REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

Priročnik kibernetske varnosti

KOLOFON

Avtorji:

Ivana Boštjančič Pulko, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
Gorazd Božič, Nacionalni odzivni center za kibernetsko varnost (SI-CERT)
dr. Denis Čaleta Institut za korporativne varnostne študije (ICS-Ljubljana)
Matic Čaleta, Institut za korporativne varnostne študije (ICS-Ljubljana)
Borut Jakopin, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
mag. Polona Jerina, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
Matjaž Mravljak, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
Maja Obreht, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)

Recenzenti:

Ivana Boštjančič Pulko (URSIV), Sebastjan Čagran (URSIV), Borut Jakopin (URSIV), mag. Polona Jerina (URSIV), Urban Kunc (URSIV), mag. Matjaž Mravljak (URSIV), Žiga Novak, (URSIV), Maja Obreht (URSIV), mag. Melita Šinkovec (URSIV)

Založnik	Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
Jezikovni pregled	Neža Šuligoj
Oblikovanje & Grafična podoba	Robert Mostar
Oblika izdaje	Elektronska izdaja
Datum izdaje	februar 2025
Elektronski naslov založnika	gp.uiv@gov.si

Vsebine za Sekcijo 1 so prispevali predstavniki URSIV in SI-CERT, vsebine za Sekcijo 2 in Sekcijo 3 sta prispevala predstavnika ICS-Ljubljana.

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID 226661635

ISBN 978-961-96923-0-1 (PDF)

POZDRAVNI NAGOVOR DIREKTORJA URSIV DR. UROŠA SVETETA

Spoštovani,

nahajamo se v času, ko digitalni svet postaja neločljiv del našega vsakdana. Tehnologija poganja naše gospodarstvo, povezuje ljudi in ustvarja priložnosti, ki si jih še pred leti nismo mogli niti zamisliti. A z vsemi temi priložnostmi prihajajo tudi tveganja. Kibernetska varnost ni le tehnična nuja, temveč postaja temeljna vrednota vsake družbe, ki stremi k razvoju, napredku in zaupanju v digitalno prihodnost.

Najboljši način napovedovanja prihodnosti je njeno ustvarjanje, je zapisal Peter Drucker, utemeljitelj sodobne vede o upravljanju. Ta misel povzema vodilo in prizadevanja Urada Vlade Republike Slovenije za informacijsko varnost (URSIV). Stremimo k oblikovanju nacionalnega sistema, ki bo v času hitrega digitalnega napredka čim bolj odporen na kibernetske grožnje. Ključna stvar pri vzpostavljanju tega sistema pa je izgradnja učinkovitega sodelovanja med deležniki, ki oblikujejo nacionalni sistem kibernetske varnosti.

Pričujoč priročnik je eden izmed korakov URSIV k tesnejšemu povezovanju različnih sektorjev, vključno z javnim, zasebnim in civilno družbo, ki tvorijo živahen ekosistem kibernetske varnosti v Republiki Sloveniji. Predstaviti vam želimo URSIV kot krovno nacionalno entiteto za vzpostavitev učinkovitega sistema kibernetske varnosti, strukturo in procese zagotavljanja kibernetske varnosti, pravni okvir, tako slovenski kot mednarodni, projekte ter nenazadnje tudi vizijo za skupno ustvarjanje prihodnosti.

Kibernetska varnost je praksa zaščite omrežij, sistemov, podatkov in informacijskih tehnologij pred kibernetskimi napadi, nepooblaščenim dostopom, poškodbami, krajo, ali motnjami delovanja. Kibernetska varnost vključuje tehnološke, procesne in človeške dejavnike ter uporablja različne tehnologije, politike in prakse za zaščito pred kibernetskimi grožnjami.

Naša vizija za Slovenijo je jasna: postati želimo država, kjer varnost in digitalna inovacija hodita z roko v roki. Slovenija želi povezati talente, institucije in gospodarstvo v učinkovit nacionalni kibernetski ekosistem. Naša prizadevanja temeljijo na zaupanju, sodelovanju in odgovornosti – tako med državo, kot tudi med podjetji, raziskovalnimi ustanovami ter posamezniki.

Stremimo k okolju, kjer bomo državljani, podjetja in institucije varno delovali v digitalnem svetu ter skupaj z vami pišemo zgodbo o varnem in uspešnem digitalnem jutri.

Dr. Uroš Svete

Ljubljana, februar 2025

KAZALO VSEBINE

KAZALO SHEM

STROKOVNE KRATICE IN POJASNILA

AES: Napredni standard šifriranja

AI: Umetna inteligenca

AIGC: Vsebina, ustvarjena z umetno inteligenco

API: Programski vmesnik za aplikacije

BCMS: Sistem za upravljanje neprekinjenega poslovanja

BCP: Načrt za neprekinjeno poslovanje

BIA: Analiza vpliva na poslovanje

Black box: Testiranje brez poznavanja notranje strukture ali delovanja sistema.

CEN: Evropski odbor za standardizacijo

CENELEC: Evropski odbor za elektrotehniško standardizacijo

CIA: Centralna obveščevalna agencija

CISA: Agencija za kibernetsko in infrastrukturno varnost

CISSP: Certificirani strokovnjak za varnost informacijskih sistemov

CSIRT: Ekipe za odzivanje na računalniške incidente

CTF: Ujemi zastavo (tekmovanje v kibernetski varnosti)

CTI: Kibernetsko-obveščevalni podatki

DDoS: Porazdeljen napad za onemogočanje storitev

DHCP: Protokol za dinamično dodeljevanje naslovov IP

DIN: Nemški inštitut za standardizacijo

DLP: Preprečevanje izgube podatkov

DNS: Sistem domenskih imen

DPIA: Ocena vpliva na varstvo podatkov

2FA: Dvofaktorska avtentikacija

EDR: Zaznavanje in odzivanje na končnih točkah

ENISA: Evropska agencija za kibernetsko varnost

ESG: Okoljski, družbeni in upravljavski vidiki

ETSI: Evropski inštitut za telekomunikacijske standarde

FBI: Zvezni preiskovalni urad

FISMA: Zakon o upravljanju varnosti informacij v ZDA

GDPR: Splošna uredba o varstvu podatkov

GRC: Upravljanje, tveganja in skladnost

Grey Box: Testiranje z omejenim poznavanjem notranje strukture.

HIPAA: Zakon o prenosljivosti in odgovornosti zdravstvenih podatkov

IAM: Upravljanje identitet in dostopov

IAMaaS: Upravljanje identitet in dostopov kot storitev

IBS: Informacijski bazični sistemi

ICS: Industrijski kontrolni sistemi

IDS: Sistem za zaznavanje vdorov

IEC: Mednarodna elektrotehniška komisija

IKT: Informacijsko-komunikacijske tehnologije

IOC: Indikatorji kompromitiranja

IPS: Sistem za preprečevanje vdorov

IR: Odziv na incidente

ISMS: Sistem za upravljanje informacijske varnosti

MSSP: Ponudnik storitev upravljanja varnosti

NDR: Zaznavanje in odzivanje v omrežju

NIS: Direktiva o omrežjih in informacijskih sistemih

NSA: Nacionalna varnostna agencija

NTP: Protokol za sinhronizacijo časa

OSINT: Obveščevalni podatki iz odprtih virov

PBX: Zasebna telefonska centrala

PCI: Plačilna industrija

PCIDSS: Standard varnosti podatkov v plačilni industriji

PDEU: Pogodba o delovanju Evropske unije

PHISHING: Lažno predstavljanje za krajo podatkov (ribarjenje)

RBAC: Nadzor dostopa na podlagi vlog

RDP: Protokol za oddaljeno namizje

RPO: Ciljna točka obnovitve

RSA: Rivest–Shamir–Adleman (kriptografski algoritem)

RTO: Ciljni čas obnovitve

SDLC: Življenjski cikel razvoja programske opreme

SIEM: Upravljanje informacij in dogodkov na področju varnosti

SIST: Slovenski inštitut za standardizacijo

SLA: Dogovor o ravni storitev

SOAR: Orkestracija, avtomatizacija in odziv na področju varnosti

SOC: Varnostno-operativni center

SOCaaS: Varnostno-operativni center kot storitev

SUIV: Sistem upravljanja informacijske varnosti

SUNP: Sistem upravljanja neprekinjenega poslovanja

SUVI: Sistem upravljanja varovanja informacij

SWOT: Moč, slabosti, priložnosti, grožnje

TTP: Taktike, tehnike in postopki

VAPT: Ocena ranljivosti in testiranje prodiranja

VISHING: Goljufivo predstavljanje prek telefona

VPN: Navidezno zasebno omrežje

White box: Testiranje z natančnim poznavanjem notranje strukture in delovanja sistema.

XDR: Razširjeno zaznavanje in odzivanje

ZInfV: Zakon o informacijski varnosti

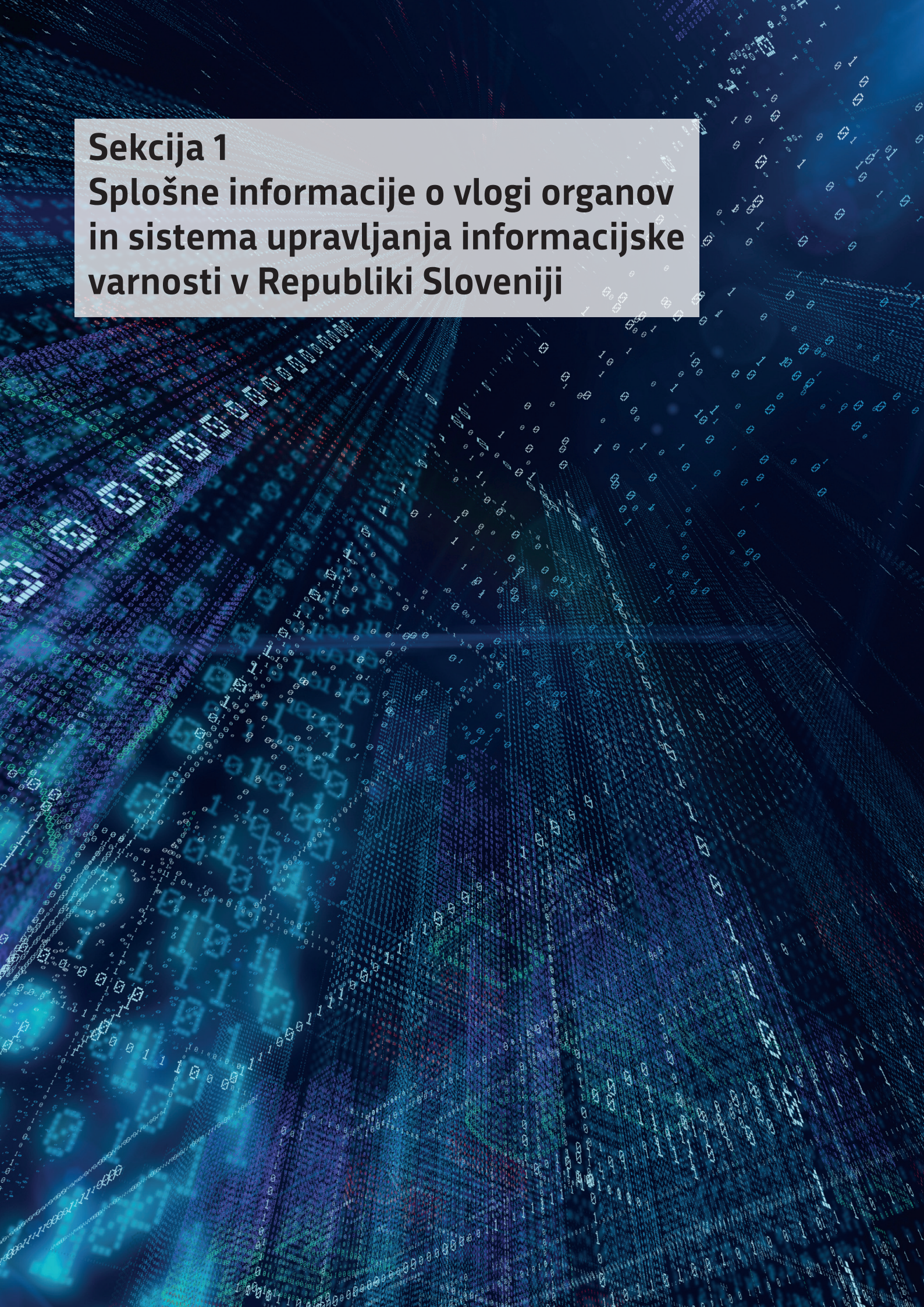
ZISSP: Zakon o informacijski varnosti in sistemski zaščiti podatkov

ZJN-3: Zakon o javnem naročanju

ZJNPOV: Zakon o javnem naročanju na področju obrambe in varnosti

ZUP: Zakon o splošnem upravnem postopku

ZVOP: Zakon o varstvu osebnih podatkov



Sekcija 1
Splošne informacije o vlogi organov in sistema upravljanja informacijske varnosti v Republiki Sloveniji

Poglavje 1
Uvodne informacije in napotila

Namesto uvoda

Urad Vlade za informacijsko varnost je sprejel odločitev o pripravi tega priročnika zaradi povečane potrebe pri zavezancih, ter na splošno za krepitve odpornosti informacijsko-komunikacijskih sistemov pred kibernetskimi incidenti v slovenskih organizacijah. Za izvedbo naloge je poleg lastnih kapacitet urada, pripravo vsebine prevzel Institut za korporativne varnostne študije.

Namen priročnika

Priročnik ima namen organizacijam in osebam odgovornim za pripravo varnostne dokumentacije podati osnovne informacije ter napotke kje pridobiti dodatne vsebine za posamezna področja, nima pa namena posredovati vzorčne dokumentacije za dosego zakonodajne skladnosti. To je naloga in obveza vsake posamezne organizacije, saj so tudi organizacije zelo raznolike.

Komu je namenjen?

Priročnik je primarno namenjen vsem zavezancem po Zakonu o informacijski varnosti, vendar pa je kot pomoč in podpora hkrati namenjen tudi vsem drugim organizacijam, ki želijo okrepiti svojo varnost informacijsko-komunikacijskih sistemov pred kibernetskimi incidenti, ter se približati zahtevam zakonodaje.

Urad Vlade za informacijsko varnost

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je pristojni nacionalni organ za informacijsko varnost, ki deluje kot samostojna vladna služba. Ima ključno vlogo pri vzpostavitvi celovite strategije informacijske in kibernetske varnosti na nacionalni ravni. Skladno z 27. členom Zakon o informacijski varnosti, pa nudi tudi podporo zavezancem, kar urad vidi tudi v pripravi in objavi tega priročnika.

Pravne podlage

Vse navedene pravne podlage so v času nastanka priročnika veljavne pravne podlage. Urad pa se zaveda, da se le-te lahko spremenijo, zato ne odgovarja za morebitne neskladnosti z bodočo zakonodajo.

Vse navedbe vezane na Zakon o informacijski varnost, bodo ustrezno posodobljene ko bo sprejet nov zakon, kar lahko vpliva na posamezna poglavja tega priročnika.

Poglavja in podane usmeritve

Priročnik ni pravno zavezujoč dokument in tudi v nobenem delu ne posega ali spreminja zakonodajnih obveznosti. V primeru morebitnih neskladnosti z zakonodajo, vedno obvelja zakonodajni oziroma pravno zavezujoč dokument npr. zakon, uredba ipd.

Priročnik je lahko napotek za vse organizacije in posameznike, ki bodo pripravljali varnostno dokumentacijo v svojih organizacijah.

Urad bo vesel vsakršne povratne informacije glede vsebin podanih v priročniku in kaj morda še manjka, kar sprejema na gp.uiv@gov.si.

Urad vidi ta priročnik kot prvi korak, ki se bo z razvojem področja in zakonodaje tudi ustrezno nadgrajeval oziroma dopolnjeval.

Poglavje 2
Predstavitev Urada Vlade Republike Slovenije za informacijsko varnost (URSIV)

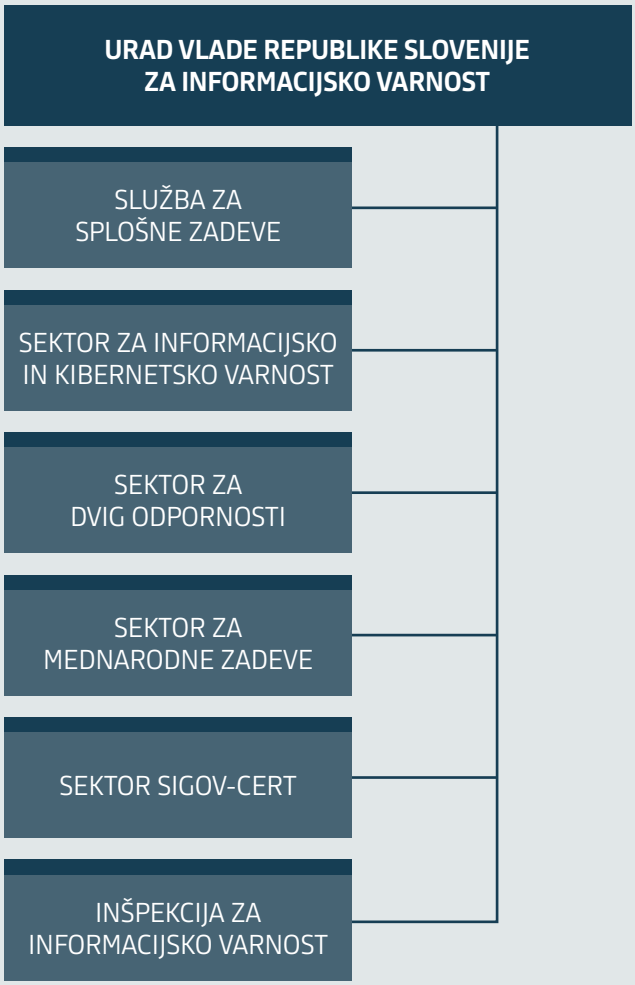
POVZETEK

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) ima osrednjo vlogo pri zagotavljanju nacionalne kibernetske varnosti. Kot samostojen organ je odgovoren za vzpostavitev strategij, usklajevanje deležnikov ter zaščito ključnih informacijskih sistemov in kritične infrastrukture. Njegova naloga vključuje pripravo zakonodajnih okvirov, mednarodno sodelovanje, izvajanje inšpekcijskega nadzora in razvoj rešitev za obvladovanje kibernetskih groženj. V sodelovanju z drugimi organi in sektorji URSIV prispeva k odpornosti Slovenije na sodobne kibernetske izzive.

KLJUČNE TOČKE:

- URSIV (ustanovitev, samostojna vladna služba)
- Nacionalna strategija kibernetske varnosti
- ZInfV (Zakon o informacijski varnosti)
- Ključne naloge (koordinacija, zakonodaja, mednarodno sodelovanje, inšpekcija)
- Kritična infrastruktura (energija, digitalna infrastruktura, zdravstvo, bančništvo)
- Mednarodni projekti (NCC-SI, Evropski izziv kibernetske varnosti, SI-EuroQCi)
- SIGOV-CERT (CSIRT, odziv na incidente)
- Izobraževanje in ozaveščanje o kibernetski varnosti
- Horizontalni pristop (koordinacija med ministrstvi, agencijami)
- Mednarodno sodelovanje (ENISA, TF-CSIRT).

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je pristojni nacionalni organ za informacijsko varnost, ki deluje kot samostojna vladna služba. Ima ključno vlogo pri vzpostavitvi celovite strategije informacijske in kibernetske varnosti na nacionalni ravni. Njegove naloge zajemajo širok spekter dejavnosti, ki so osredotočene na krepitev odpornosti kritične infrastrukture in zagotavljanje varnosti ključnih informacijskih sistemov v državi. Z vzpostavitvijo učinkovitega sistema za obvladovanje kibernetskih groženj URSIV aktivno prispeva k zagotavljanju varnosti posameznikov, podjetij in javnih institucij.



Shema1: Organizacijska struktura URSIV (Vir: URSIV)

Kratka zgodovina Urada

Slovenija je pomen kibernetske varnosti prepoznala v temeljnih nacionalno varnostnih dokumentih, in sicer v Resoluciji o strategiji nacionalne varnosti leta 2010 in leta 2019 (Uradni list RS, št. 59/19). Vlada Republike Slovenije je na svoji 76. redni seji, 25. februarja 2016, sprejela nacionalno strategijo kibernetske varnosti (Sklep vlade številka: 38100-12/2015/5), ki stremi k vzpostavitvi celovitega sistema kibernetske varnosti kot pomembnega elementa nacionalne varnosti.

Skladno s sprejeto strategijo je Vlada Republike Slovenije januarja 2017 sprejela odločitev, da Urad za varovanje tajnih podatkov (UVTP) prevzame naloge nacionalnega organa za kibernetsko varnost, kar se je zgodilo aprila 2017. UVTP je začasno opravljal naloge pristojnega nacionalnega organa skladno z Zakonom o informacijski varnosti (ZinfV), razen nalog upravnega odločanja in nadzora, ki jih je opravljalo ministrstvo, pristojno za informacijsko družbo (takrat MJU). UVTP je te naloge izvajal do vzpostavitve Uprave RS za informacijsko varnost (URSIV), organa v sestavi Ministrstva za javno upravo (MJU), ki je prevzela naloge nacionalnega organa na začetku leta 2020 (Uradni list RS, št. 52/2018). Urad Vlade Republike Slovenije za informacijsko varnosti je bil ustanovljen 15. julija 2021 z Odlokom o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za informacijsko varnost (Uradni list RS, št. 114/21 in 69/23). URSIV je tako 31. julija 2021 prevzel naloge Uprave RS Slovenije za informacijsko varnost, ki je delovala kot organ v sestavi Ministrstva za javno upravo.

URSIV je samostojna vladna služba in je s tem podrejen neposredno predsedniku Vlade Republike Slovenije. Ker je vladna služba, ni del nobenega izmed ministrstev Republike Slovenije, saj v sistemu deluje horizontalno. S tem, ko je Vlada Republike Slovenije oblikovala Urad Vlade Republike Slovenije za informacijsko varnosti, kot vladno službo, je prepoznala prednosti horizontalnosti vladnih služb v pravni ureditvi Republike Slovenije. Horizontalnost se nanaša na sodelovanje in usklajevanje med različnimi ministrstvi, agencijami in drugimi vladnimi organi na isti ravni hierarhije. Ta pristop omogoča bolj učinkovito delovanje državne uprave, ker spodbuja deljenje informacij in medsebojno sodelovanje. Prednosti horizontalnosti vladnih služb so v tem, da omogočajo: boljše usklajevanje politik, hitrejše in učinkovitejše reševanje problemov, povečana transparentnost in odgovornost, boljša pripravljenost na krizne situacije.

Ključne naloge

URSIV povezuje deležnike v nacionalnem sistemu informacijske varnosti in na strateški ravni koordinira operativne zmogljivosti v sistemu. Posebno pozornost posveča zavezancem po ZInfV, iz skupine ponudnikov digitalnih storitev, iz skupine organov državne uprave in iz skupine izvajalcev bistvenih storitev na področjih:

- energije,
- digitalne infrastrukture,
- oskrbe s pitno vodo in njene distribucije,
- zdravstva,
- prometa,
- bančništva,
- infrastrukture finančnega trga,
- preskrbe s hrano in
- varstva okolja.

Na zakonodajni ravni URSIV tesno sodeluje pri pripravi in izboljšavi zakonodajnih okvirjev, ki urejajo področje informacijske varnosti, ter si prizadeva za usklajevanje slovenske zakonodaje z evropskimi direktivami in standardi. S tem zagotavlja, da Slovenija ostaja v koraku z najnovejšimi zahtevami in trendi na področju kibernetske varnosti, kar je ključno za zaščito pred nenehno spreminjajočimi se grožnjami v digitalnem okolju.

URSIV tesno sodeluje z drugimi ključnimi subjekti na področju informacijske varnosti, kot so nacionalne in mednarodne organizacije, zasebni sektor ter akademske ustanove. Z vzpostavitvijo partnerskih odnosov na nacionalni in mednarodni ravni URSIV krepi zmogljivosti za odzivanje na kibernetske incidente ter razvija nove rešitve za preprečevanje in obvladovanje groženj. Zaradi vse večje mednarodne narave kibernetskih groženj je URSIV močno vključen v mednarodno sodelovanje na področju kibernetske varnosti, kjer si izmenjuje najboljše prakse in tehnološke rešitve z drugimi državami ter sodeluje v različnih mednarodnih pobudah in organizacijah. Tako zagotavlja, da je Slovenija dobro pripravljena na globalne izzive, povezane s kibernetsko varnostjo, in prispeva k skupni varnosti na ravni Evropske unije ter širše.

URSIV izvaja naloge enotne kontaktne točke za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in z evropsko mrežo skupin CSIRT ter druge naloge mednarodnega sodelovanja. Z lastno inšpekcijsko službo izvaja nadzor nad izvajanjem ZInfV. URSIV je z obveščanjem vlade in Sveta za nacionalno varnost (SNAV) o stanju povečane ogroženosti zaradi verjetnosti realizacije kritičnega incidenta ali kibernetskega napada umeščen v sistem nacionalne varnosti.

URSIV deluje tudi kot središčna točka za obveščanje javnosti in drugih deležnikov o potencialnih kibernetskih grožnjah. Z vzpostavitvijo sistemov za hitro opozarjanje in obveščanje je v primeru povečanih tveganj ali incidentov zmožen hitro reagirati ter obvestiti pristojne organe in javnost. Pri tem uporablja najnovejše tehnologije in pristope za odkrivanje, spremljanje ter analizo kibernetskih groženj. Ključni del delovanja URSIV je izobraževanje in ozaveščanje javnosti o pomembnosti kibernetske varnosti. V ta namen izvaja različne kampanje, usposabljanja in delavnice za ciljne skupine, kot so podjetja, javni sektor ter posamezniki. Tako si prizadeva za dvig splošne informacijske pismenosti in varnostne kulture, kar je ključnega pomena za zmanjševanje tveganj kibernetskih napadov.

Vloga URSIV je torej osrednja pri zagotavljanju varnosti informacijske infrastrukture Republike Slovenije, kar vključuje tako preventivne kot reaktivne ukrepe za zaščito pred kibernetskimi napadi in krepitev zavedanja o pomembnosti kibernetske varnosti na vseh ravneh družbe.

Projekti URSIV na področju kibernetske varnosti v Sloveniji

URSIV se redno udeležuje nacionalnih in mednarodnih dogodkov ter konferenc na temo kibernetske varnosti. V letu 2024 je vzpostavil Nacionalni koordinacijski center za kibernetsko varnost (NCC-SI), ki krepi raziskovanje in inovacije ter njihovo uvajanje na področje kibernetske varnosti. Z zagotavljanjem možnosti sofinanciranja iz evropskih projektov pospešuje

razvoj industrijskih, tehnoloških ter raziskovalnih zmogljivosti države.

Velik poudarek NCC-SI namenja izobraževanju s področja kibernetske varnosti. Poudarek je predvsem na mladih, ki se odločajo za poklicno pot, saj na kibernetskem področju primanjkuje strokovnjakov. V ta namen potekajo različne aktivnosti, npr. vsakoletna udeležba na evropskem tekmovanju mladih talentov v kibernetski varnosti »Evropski izziv kibernetske varnosti (European Cybersecurity Challenge)« v okviru projekta »Kibertalent«. Vanj sodi tudi usposabljanje deklet za kibernetsko varnost. Urad stremi k vzpostavitvi mrež srednjih šol za kibernetsko varnost ter sodeluje pri poletnih taborih s področja kibernetske varnosti za mlade.

URSIV podpira raziskave, razvoj in inovacije na področju kibernetske varnosti tudi s sofinanciranjem projektov. Uspešno sodeluje v konzorcijih za izvedbo projektov EU. Nekaj projektov, kjer je URSIV sodeloval:

- »SI-EuroQCi« za vzpostavitev nacionalne kvantne komunikacijske infrastrukture za varno distribucijo kvantnih šifrirnih ključev.
- »Akadimos« s področja pridobivanja veščin kibernetske varnosti.
- »ALiEnS-SOC«, namenjen uporabi novih tehnologij in umetne inteligence v varnostno operativnih centrih.
- »Atlantis«, katerega cilj je povečati odpornost in kibernetsko-fizično-človeško varnost ključnih kritičnih infrastruktur EU.
- Pilotni projekt Agencije evropske unije za kibernetsko varnost (ENISA) za izvajanje storitev zagotavljanja kibernetske varnosti, ki so namenjene zavezancem, tudi upravljalcem kritične infrastrukture.
- Projekt napredne analitike podatkov in modeliranje napadov ter napadalcev na področju kibernetske varnosti v sektorjih obrambe, notranje varnosti, obveščevalne dejavnosti, zaščite in reševanja ter kritične infrastrukture. Sofinanciral ga je z Javno agencijo za znanstvenoraziskovalno in inovacijsko dejavnost (ARIS) ter Ministrstvom za obrambo.
- Projekt s področja uporabe umetne inteligence v kibernetski varnosti, ki ga je URSIV sofinanciral z ARIS.

Sektor SIGOV-CERT

SIGOV-CERT je odzivni center za incidente v informacijskih sistemih organov državne uprave. Deluje v okviru Urada Republike Slovenije za informacijsko varnost. Pristojen je za sprejem in obravnavo kibernetskih incidentov v organih državne uprave, ki upravljajo informacijske sisteme ter dele omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

SIGOV-CERT predstavlja kontaktno točko za priglasitev incidentov zavezancem po Zakonu o informacijski varnosti (ZInfV) in jim nudi metodološko pomoč pri obravnavi ter razreševanju kibernetskih incidentov. Od leta 2024 je SIGOV-CERT akreditiran v sklopu Odzivne skupine za računalniške varnostne incidente (CSIRT) TF-CSIRT Trusted Introducer (stran je v angleščini), ki omogoča zaupanje, sodelovanje in izmenjavo informacij med CSIRT ekipami v Evropi, kar pripomore k višjemu nivoju kibernetske varnosti. Prav tako je SIGOV-CERT član CSIRT mreže Agencije evropske unije za kibernetsko varnost (ENISA).

Naloge SIGOV-CERT:

SIGOV-CERT izvaja zakonsko določene naloge CSIRT organov državne uprave in še naslednje naloge:

- sprejema, obravnava in ocenjuje priglasitve incidentov zavezancev ter te podatke evidentira, hrani in varuje;
- zavezancem nudi metodološko podporo, pomoč in sodelovanje ob pojavu incidenta;
- sodeluje z nacionalnim CSIRT in s pristojnim nacionalnim organom ter jima na poziv na varen način - nudi informacije o izvajanju svojih pristojnosti na podlagi tega zakona;
- objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti organov državne uprave.

Poglavje 3
Povzetek Nacionalnega načrta za odzivanje na kibernetske incidente

POVZETEK

Nacionalni načrt za odzivanje na kibernetske incidente (NOKI) je temeljni dokument za usklajeno in sistematično obvladovanje kibernetskih incidentov na državni ravni. Določa okvir za sodelovanje vseh deležnikov, vključno z državnimi organi, lokalno samoupravo, zasebnim sektorjem in upravljavci kritične infrastrukture. S poenotenjem postopkov in metodologij, vključno z razvrščanjem incidentov, komunikacijskimi smernicami in časovnimi okviri za poročanje, NOKI omogoča učinkovito preprečevanje in obvladovanje kibernetskih groženj. Dokument, ki ga upravlja URSIV, je zasnovan na Strategiji kibernetske varnosti in Zakonu o informacijski varnosti ZInfV ter redno posodobljen glede na mednarodne standarde in potrebe.

Ključne točke:

- NOKI (strateški okvir, URSIV, koordinacija deležnikov)
- Kibernetski incidenti (opredelitev, razvrstitev, pragovi poročanja)
- Poročanje (postopki, časovni okvirji, vloge zavezancev)
- Upravljanje incidentov (priprava, zaznavanje, omilitev, okrevanje)
- Kritični incidenti (koordinacija na nacionalni ravni, mednarodno sodelovanje)
- Koordinacijska skupina za kibernetsko varnost (naloge, vodenje)
- Mednarodno sodelovanje (EU, NATO, čezmejne grožnje)
- Posodobitve NOKI (uskladitev z direktivo NIS 2, hitro spreminjajoče se okolje).

V vsakdanjem življenju se povečuje uporaba informacijskih sistemov, omrežij, pametnih naprav in interneta stvari, kar vpliva na gospodarske in negospodarske dejavnosti ter na vsakdanje življenje in blaginjo družbe. Hiter razvoj informacijsko-komunikacijskih tehnologij prinaša velike koristi, a tudi neprestane izzive v obliki kibernetskih groženj. Kibernetski incidenti so danes ena najpogostejših varnostnih groženj, kibernetska varnost pa predstavlja pomemben del nacionalno varnostnega sistema.

Nacionalni načrt za odzivanje na kibernetske incidente (v nadaljnjem besedilu NOKI) predstavlja temelj državnega sistema odzivanja na kibernetske incidente. NOKI je sprejela Vlada Republike Slovenije 18. marca 2021[1] in določila Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) za skrbnika dokumenta, ki je pooblaščen tudi za posodabljanje prilog. NOKI je javno dostopen dokument, izdelan na podlagi Strategije kibernetske varnosti in Zakona o informacijski varnosti (ZInfV) ter drugih relevantnih nacionalnih in mednarodnih predpisov.

NOKI določa skupno doktrino in strateški okvir za odzivanje celotnega kroga deležnikov, ki so vključeni v nacionalni sistem zagotavljanja kibernetske varnosti – vse ravni državnega sestava (državni organi in ustanove), lokalne samouprave, zasebni in neprofitni sektor (vključno z zasebnimi in javnimi lastniki ter upravljavci kritične infrastrukture). NOKI je zagotovil poenotenje postopkov upravljanja kibernetskih incidentov in podal smernice za usklajen odziv vseh deležnikov, s poudarkom na usklajenem komuniciranju ter preprečitvi širitve incidenta na druge subjekte. Z operacionalizacijo postopkov določenih z ZInfV, je opredelil pomembne elemente kot so pragovi kibernetskih incidentov, časovni okvirji priglasitve in poročanja o kibernetskih incidentih ter komunikacijske poti. Slednje je zlasti pomembno, kadar kibernetski incident vpliva na storitev, ki je bistvena za ohranitev ključnih družbenih oziroma gospodarskih dejavnosti po ZInfV. Zaradi vse večje potrebe po koordinaciji glede vprašanj kibernetske varnosti na nacionalnem nivoju, je NOKI zagotovil vzpostavitev Koordinacijske skupine za kibernetsko varnost in določil njeno sestavo in naloge.

Z zagotavljanjem sistematičnega in usklajenega odziva na nacionalni ravni, NOKI opredeljuje vloge različnih deležnikov, ki jih naslavlja prek različnih področij. Z uvedbo poenotene homogene taksonomije, ki kibernetske incidente klasificira glede na nevarnost in vpliv, je NOKI uvedel opredelitev kibernetskih incidentov ter njihovo vrednotenje. NOKI je tudi določil enotno metodologijo poročanja in spremljanja kibernetskih incidentov ter opredelil posamezne postopke glede na vrednotenje incidenta in tip zavezanca. Določene so bile tudi ustrezne komunikacijske poti, prek katerih se izvaja priglasitev, poročanje in koordinacija za izvajanje postopkov odziva na različne kategorije ter stopnje incidentov. S celotnim naborom navedenih ukrepov je bila vzpostavljena podlaga za enotno in koordinirano odzivanje vseh relevantnih deležnikov na državni ravni v primeru lažjih, kot tudi kritičnih kibernetskih incidentov.

V nadaljevanju je predstavljena struktura NOKI, ki je po uvodu in predstavitvi namena sledeča:

Opredelitev in stopnje kibernetskih incidentov

- Opredelitev: Incident je vsak dogodek, ki ima dejanski negativni učinek na varnost omrežij in informacijskih sistemov. Incidenti so razvrščeni glede na tip in njihov vpliv, oziroma učinek na omrežne ter informacijske sisteme.

- Stopnje: Incidenti so kategorizirani kot lažji, težji in kritični, z določenimi merili za določanje praga za obvezno poročanje na podlagi vnaprej opredeljenih kazalnikov. Stopnja kazalnikov in njihova interakcija določata, ali je kibernetski incident pod pragom obvezne-

[1] 2022-03-NOKI.pdf (gov.si)

ga poročanja in kakšni so postopki deležnikov kibernetske varnosti.

Poročanje o kibernetskih incidentih

- Zaznavanje in poročanje: Kibernetski incidenti se razvrščajo v kategorije od C6 do C1, glede na odnos med napadenim deležnikom (žrtvijo kibernetskega incidenta) in stopnjo nevarnosti (učinkom kibernetskega incidenta). Podrobno so določeni postopki za zaznavanje in poročanje o incidentih, vključno s priglasitvijo ter pripravo vmesnih in končnih poročil.
- Komunikacija: Opredeljene so smernice za obveščanje javnosti, pri čemer se komuniciranje o kibernetskem incidentu prilagaja glede na kategorijo kibernetskega incidenta.

Upravljanje kibernetskih incidentov

- Upravljanje kibernetskih incidentov je organiziran sklop ukrepov in aktivnosti, ki so usmerjeni v čim boljšo zaščito oziroma preprečevanje nastanka kibernetskih incidentov. Sestavljeno je iz več faz: priprava, zaznavanje, zadrževanje, omilitev, okrevanje in aktivnosti po incidentu.
- V posameznih fazah upravljanja kibernetskih incidentov so zapisane pristojnosti, odgovornosti in naloge, ki jih izvajajo deležniki. Opredeljene so naloge različnih subjektov, vključno z URSIV, SI-CERT, SIGOV-CERT, SOC in AKOS.

Odzivanje na kritične kibernetske incidente na državni ravni

- Nacionalna raven: Koordinacija upravljanja kritičnega kibernetskega incidenta (C1 ali C2, za katerega obstaja dejanska nevarnost, da preide v C1), se prenese na URSIV. Za usklajevanje kibernetske varnosti na državni ravni je pristojna Koordinacijska skupina za kibernetsko varnost, ki se srečuje na rednih in izrednih zasedanjih ter jo vodi direktor URSIV.
- Mednarodno sodelovanje: Mehanizmi odzivanja in pomoči na mednarodni ravni (predvsem EU in NATO) predstavljajo koristno orodje v primeru kritičnih incidentov, kibernetskih napadov večjih razsežnosti ter kibernetskih incidentih s čezmejnimi učinki.

Priloge NOKI so tabele in obrazci za poročanje ter diagrami s prikazi postopkov za obvladovanje incidentov.

Državni sistem odzivanja na kibernetske incidente je kompleksen proces, ki zahteva veliko znanja in zavedanja ter usklajenega delovanja vseh relevantnih deležnikov. Uspešno odzivanje na kibernetske incidente med drugim zahteva sistematične, hitre in učinkovite ukrepe, ki so jasno opredeljeni. NOKI je zato ključnega pomena za zagotavljanje kibernetske varnosti v Republiki Sloveniji. Pomembno je, da so vsi deležniki seznanjeni s postopki, zahtevami in nalogami, ki morajo biti predmet rednih izobraževanj ter preverjanj v obliki vaj in usposabljanj.

Veljavni NOKI že zdaj predvideva redne (vsaj vsake tri leta) posodobitve zaradi hitro spreminjajoče se krajine kibernetskega varnostnega okolja, potrebe po usklajevanju z mednarodnimi akti in nacionalno zakonodajo, na katerih tudi temelji. Posodobitev načrta bo zlasti treba opraviti po sprejemu novega Zakona o informacijski varnosti, ki bo v slovenski pravni red prenesel zahteve evropske direktive NIS 2.

Poglavje 4
Vloga SI-CERT: nacionalnega odzivnega centra za kibernetsko varnost

POVZETEK

SI-CERT je nacionalni odzivni center za kibernetsko varnost, ki zagotavlja tehnično pomoč pri reševanju incidentov, kot so vdori, računalniške okužbe in druge zlorabe. Besedilo opisuje postopke za prijavo incidentov in poudarja sodelovanje centra z različnimi organizacijami na nacionalni ter mednarodni ravni. Prav tako se osredotoča na zakonodajne obveznosti prijave incidentov za določene subjekte in nudi napotke za učinkovito odzivanje na kibernetske grožnje. SI-CERT ima ključno vlogo pri ozaveščanju o varni rabi interneta in sodeluje v projektih za izboljšanje kibernetske varnosti.

Ključne točke:

- Vloga in pristojnosti SI-CERT
- Postopki za prijavo kibernetskih incidentov
- Poročanje (postopki, časovni okvirji, vloge zavezancev)
- Aktivnosti SI-CERT pri odzivu na kibernetske incidente (priprava, zaznavanje, omilitev, okrevanje)
- Projekti in vzvodi za povečanje osveščanja uporabnikov.

Nacionalni odzivni center za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team) opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT izvaja nacionalni program ozaveščanja Varni na internetu in sodeluje v projektu SAFE-SI. SI-CERT deluje v okviru javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije).

Delovanje centra SI-CERT je opredeljeno v 28. členu Zakona o informacijski varnosti.

SI-CERT ima na voljo različne kontaktne elektronske naslove:

- cert@cert.si za sporočanje kibernetskih incidentov,
- press@cert.si za novinarska vprašanja in
- info@cert.si za vsa ostala vprašanja.

Mednarodno sodelovanje

SI-CERT je član CSIRT mreže po Direktivi NIS, svetovnega združenja odzivnih in varnostnih centrov FIRST (Forum of Incident Response and Security Teams), član skupine nacionalnih odzivnih centrov pri CERT/CC, član delovne skupine evropskih odzivnih centrov TF-CSIRT in je akreditiran v programu Trusted Introducer.

Storitve odzivnega centra SI-CERT so na voljo širši javnosti. SI-CERT aktivnosti v celoti financira Urad Vlade Republike Slovenije za informacijsko varnost, pristojni nacionalni organ za informacijsko varnost.

Prijava incidenta – splošna navodila

SI-CERT je nacionalni odzivni center za kibernetsko varnost. Ob zaznanem varnostnem incidentu pošljite prijavo z elektronskim sporočilom na naslov cert@cert.si in nudili vam bomo pomoč pri preiskavi incidenta.

Prijavi priložite natančen opis dogajanja in vse relevantne dnevniške izseke (ang. log files), vzorce škodljive kode, podtaknjene vsebine na spletni strani ipd. Če pošiljate občutljive podatke in vas skrbi možnost prestrezanja na poti, lahko sporočila zašifrirate s programom PGP (Pretty Good Privacy) ali GPG (GNU Privacy Guard) tako, da uporabite SI-CERT javni PGP ključ. Na enak način nam posredujte tudi vzorce škodljive kode ali prestreženi zlonamerni promet okuženih sistemov, saj lahko sicer kakšen od poštnih strežnikov na poti sporočilo zaustavi zaradi protivirusne zaščite. Če niste vešči postopkov šifriranja in digitalnega podpisovanja s PGP, lahko podatke pošljite v ZIP arhivu, zaščitenim z geslom.

Prostovoljna in obvezna priglasitev incidenta

Zakon o informacijski varnosti (ZInfV) določa v 13. in 14. členu zakona obvezo priglasitve incidenta na SI-CERT za vse zavezance, ki so bili določeni po sklepu Vlade RS kot izvajalci bistvenih storitev ali ponudniki digitalnih storitev. Podobno določa za operaterje elektronskih komunikacij Zakon o elektronskih komunikacijah (ZEKom-2) v 118. členu. Zakon o varovanju osebnih podatkov (ZVOP-2) pa v 23. členu določenim upravljalcem osebnih podatkov nalaga "smiselno uporabo določb o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost."

Vsi ostali poslovni subjekti, javne ustanove in fizične osebe lahko podajo prostovoljno prijavo incidenta na SI-CERT. Namen prijave je strokovna pomoč pri identifikaciji težave, pomoč pri njeni odpravi, zamejitvi in odpravi posledic. SI-CERT ni organ pregona, zato je pri sumu kaznivega dejanja potrebna prijava hkrati tudi policiji. Če gre za sum zlorabe osebnih podatkov, podajte tudi prijavo Informacijskemu pooblaščencu. SI-CERT ima z obema organoma vzpostavljeno operativno sodelovanje za skupno preiskovanje, kadar je to potrebno.

SI-CERT zaradi kadrovskih omejitev ne more nuditi telefonske podpore pri prostovoljnih prijavah incidentov. Prosimo vas, da prijavo oddate po elektronski pošti, pred tem pa preverite, ali je vaš primer že opisan in so na voljo navodila za ukrepanje (glej "Kdaj pomoč poiščete sami" v nadaljevanju).

Kdaj prijaviti incident na SI-CERT

Primer incidenta	Pričakovane aktivnosti SI-CERT
Okužba računalnika (izsiljevalski virusi, bančni trojanci, ciljani napadi, agenti za pošiljanje neželene elektronske pošte).	Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami. Svetovanje o ukrepih za sanacijo stanja.
Opažen vdor v strežnik (razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca).	Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.
Phishing elektronska sporočila (potvorjena elektronska sporočila, ki vas napeljujejo, da vpišete geslo na lažno spletno stran).	Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev ter javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.
Napad onemogočanja (poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja).	Ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta in obveščanje ponudnikov o zlorabljeni infrastrukturi ter njeni zaščiti.
Ranljive ali izpostavljene storitve (vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja).	Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.
Izguba gesel ali kraja omrežne identitete (zloraba preko phishing napada ali okužbe računalnika).	Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in možni identifikaciji storilca.

Shema 2: Kdaj prijaviti incident na SI-CERT (vir: SI-CERT)

Kaj lahko pričakujete po oddani prijavi

Iz SI-CERT vam bomo odgovorili v najkrajšem možnem času z obrazložitvijo incidenta in napotki, kako ukrepati naprej. V večini primerov lahko pričakujete odgovor v nekaj urah, v skoraj vseh primerih pa v manj kot 48 urah, pri čemer upoštevamo vrsto in nujnost incidenta, kot ju določimo po interni triažiter glede na zakonske obveznosti. Glede na vrsto incidenta bomo po potrebi stopil v stik s tujimi odzivnimi centri, kadar pa bo potrebno, vas bomo napotili na ali pa sami kontaktirali druge pristojne ustanove.

Kdaj pomoč poiščete sami

Splet predstavlja nove priložnosti tudi za spletne goljufe. Podatke in nasvete za njihovo prepoznavo smo zbrali v programu ozaveščanja Varni na internetu, kjer lahko sami najdete dovolj napotkov za ustrezno ukrepanje, saj zaradi obilice pojavitev na vse priglasitve goljufij vsakemu prijavitelju posebej ne moremo odgovoriti. Tveganja za tovrstne zlorabe boste lahko bistveno zmanjšali sami, če se prijavite na novičnik, v katerem obveščamo javnost o aktualnih opaženih goljufijah.

Vrsta goljufije	Vir dodatnih informacij
Sumljive ponudbe (ponudbe o hitrem zaslužku ali kreditih, loterijske nagrade, brezplačne vinjete ali telefoni, neverjetno poceni spletni nakupi, dediščine neznanih sorodnikov ...).	Varni na internetu https://varninainternetu.si
Spletna goljufija (lažne spletne trgovine, prevare pri prodaji in nakupih preko spletnih posrednikov, nigerijske ter ljubezenske prevare, izsiljevanje z domnevnimi intimnimi posnetki).	

Shema 3: Vrste goljufij in viri informacij (vir: SI-CERT)

Več o spletnih goljufijah

Podatke in nasvete za njihovo prepoznavo smo zbrali v programu ozaveščanja Varni na internetu, kjer lahko sami najdete dovolj napotkov za ustrezno ukrepanje, saj zaradi obilice pojavitev na vse priglasitve goljufij vsakemu prijavitelju posebej ne moremo odgovoriti. Tveganja za tovrstne zlorabe boste lahko bistveno zmanjšali sami, če ostanete obveščeni preko novičnika, v katerem obveščamo javnost o aktualnih opaženih goljufijah.

Navodila za zavezance

S sprejetjem Zakona o informacijski varnosti (ZInfV) leta 2018, ki je v slovenski pravni red prenesel Direktivo o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (direktiva NIS), je SI-CERT določen za nacionalno skupino CSIRT, katere naloge so opredeljene v 28. členu ZInfV. Kot ključne naloge v vlogi nacionalne skupine CSIRT izpostavljamo sprejem prijav incidentov, ki jih priglasijo zavezanci, in nudenje metodološke pomoči pri obvladovanju incidentov, saj pravilno in pravočasno odzivanje na kibernetske incidente bistveno prispeva k zagotavljanju visoke stopnje kibernetske varnosti v državi.

V vlogi zavezancev, ki imajo dolžnost priglasitve kibernetskih incidentov nacionalni CSIRT skupini, so tri skupine subjektov:

- Zavezanci po Zakonu o informacijski varnosti (ZInfV) so tako izvajalci bistvenih storitev (priglasitev v skladu s 13. členom ZInfV) kot ponudniki digitalnih storitev (priglasitev v skladu s 14. členom ZInfV), ki morajo nacionalnemu CSIRT brez nepotrebnega odlašanja priglasiti incidente s pomembnim negativnim vplivom na delovanje bistvenih storitev, ki jih zagotavljajo. Pri določitvi, ali bi incident imel pomemben negativen vpliv, se upoštevajo dejavniki, ki so navedeni v Uredbi o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev.
- Zavezanci po Zakonu o elektronskih komunikacijah (ZEKom-2); namen ZEKom-2, ki je uveljavil Direktivo (EU) 2018/1972 o elektronskih komunikacijah, je ojačati varnost javnih komunikacijskih omrežij in storitev subjektov, ki z vidika države in družbe zagotavljajo kritične storitve, kar ima pomen tudi za nacionalno varnost. Skladno s to zavezo in zaradi večje učinkovitosti in takojšnjega razreševanja varnostnih incidentov morajo operaterji o varnostnem incidentu takoj obvestiti AKOS in SI-CERT (nacionalno skupino CSIRT). Pogoji, kdaj gre za takšne varnostne incidente, so določeni v 118. členu ZEKom-2.
- Zavezanci po Zakonu o varstvu osebnih podatkov (ZVOP-2); Zakon o varstvu osebnih podatkov prenaša evropsko splošno uredbo o varstvu podatkov (GDPR) v slovensko zakonodajo in tudi ureja nacionalne posebnosti varstva osebnih podatkov. V 23. členuZVOP-2 so opredeljene posebne obdelave osebnih podatkov, upravljavcem ta člen nalaga smiselno uporabo določbe o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

Kako prijaviti incident na SI-CERT

Zaznani incident zavezanci v čim krajšem času, brez nepotrebnega odlašanja priglasite po elektronski pošti na naš naslov cert@cert.si.

Podatke lahko zašifrirate s SI-CERT javnim PGP ključem. Če niste vešči postopkov šifriranja in digitalnega podpisovanja s PGP, lahko občutljive podatke pošljite v ZIP arhivu, ki ga zaščitite z geslom. V primeru želje ali zahteve po uporabi druge vrste šifriranja in/ali digitalnega podpisovanja, nam to posebej sporočite.

V primeru posredovanja vzorcev škodljive kode ali druge zlonamerne ali sumljive vsebine, morate to pred pošiljanjem zašifrirati. V nasprotnem primeru sporočilo ne bo dostavljeno, zaradi detekcije škodljive vsebine na poštnem strežniku.

Obrazci za poročanje

- Zavezanci, kot jih določa metodologija po ZInfV, pri sporočanju incidentov sledijo Nacionalnemu načrtu odzivanja na kibernetske incidente (NOKI), ki je vodilo zavezancev, komu, kdaj in kako priglasiti kibernetski incident znotraj svojih sistemov. Zavezanci lahko v komunikaciji s SI-CERT prostovoljno uporabijo obrazec Priloga E iz NOKI.
- Operaterji elektronskih komunikacij v skladu z ZEKom-2 incident priglasijo prek obrazca, predpisanega s strani AKOS Poročilo o varnostnem incidentu
- Upravljavci pri sporočanju kršitev varnosti osebnih podatkov na področju posebnih obdelav sledijo določbam po ZInfV in pri priglasitvi incidenta lahko uporabijo obrazec Priloga E iz NOKI.

Dodatni napotki

- Prijava naj poleg ključnih podatkov o zaznanem incidentu (čas zaznave incidenta, opis, kaj se je zgodilo, vpliv incidenta na delovanje storitve ipd.), vsebuje še vse relevantne dnevniške izseke (ang. log files), vzorce škodljive kode, podtaknjene vsebine na spletni strani ipd.
- Če je možno, naj bodo poslani podatki v formatu, ki omogoča čim lažjo strojno obdelavo (txt, csv, json, xml, log ...). Izogibajte se formatom, ki niso namenjeni strojni obdelavi (pdf, xlsx, jpg, png ...).
- V primeru potrebe po pošiljanju večje količine podatkov, nam to posebej sporočite, da vam pošljemo povezavo na spletno stran, na kateri boste lahko varno odložili večje datoteke.
- Po prejemu prijave lahko z naše strani pričakujete odgovor s potrdilom o prejemu prijave. Odgovor v zadevi vsebuje unikatno oznako (primer: \[SI-CERT#187654\]). Če je le možno, naj vsa nadaljnja komunikacija glede istega incidenta v zadevi sporočila ohrani to oznako.

Prostovoljna prijava

Zavezanci lahko na SI-CERT priglasite tudi incident ali varnostni dogodek, ki po pomembnosti ne zadostuje kriterijem za obvezno poročanje, bi pa podatki o incidentu lahko koristili širši skupnosti. Tako prijavo obravnavamo kot prostovoljno priglašeno prijavo. Med take primere lahko spadajo:

- e-naslov, ki vsebuje škodljivo kodo;
- kakršenkoli phishing napad (tudi neuspešen);
- zaznane okužbe spletnih strani;
- skeniranje omrežja, poskusi vdorov, ali kakršenkoli drug škodljiv ali sumljiv promet iz slovenskih IP naslovov;
- skeniranje omrežja ali poskusi vdorov, ki odstopajo od običajnih zaznav;
- novi, neznani in neobičajni vzorci napadov.

Deljenje informacij v CSIRT skupnosti

SI-CERT vse informacije, povezane s prijavljenimi kibernetskimi incidenti, tako prostovoljnimi kot s strani zavezancev, obravnava kot zaupne.

Skladno z ustaljenimi postopki delovanja odzivnih centrov pa lahko določene kazalnike zlorab (ang. indicators of compromise, IoC) delimo še v širši CSIRT skupnosti.

Pri tem uporabljamo protokol TLP (ang. Traffic Light Protocol), ki je postal de-facto standard pri izmenjavi informacij.

Oznaka	Pomen
RED RDEČA	**Informacija ni za razkritje, omejeno le na prisotne** Naslovniki ne smejo deliti informacije izven okvirja samega sestanka ali pogovora, v katerem je bila informacija posredovana. Informacija TLP:RED se mora posredovati ustno ali osebno.
AMBER RUMENA	**Razkritje omejeno na organizacije udeleženih** Naslovniki lahko delijo informacijo samo znotraj svoje organizacije. Pošiljatelj lahko dovoli izmenjavo tudi s partnerskimi organizacijami naslovnika, ko je poznavanje informacije nujno pri zaščiti in preprečevanju nadaljnje škode.
GREEN ZELENA	**Razkritje omejeno na skupnost ali sektor** Naslovniki lahko delijo informacijo po potrebi znotraj svoje organizacije ter znotraj svoje skupnosti ali sektorja, vendar pa ne po komunikacijskih kanalih, ki so dostopni tudi širši javnosti (objava na javno dostopnih mestih).
WHITE BELA	**Razkritje ni omejeno** Naslovniki lahko informacijo prosto delijo naprej.

Shema 4: Protokol TLP (ang. Traffic Light Protocol) je de-facto standard pri izmenjavi informacij (Vir: SI-CERT)

Izmenjava informacij o kibernetskih grožnjah

MISP (Malware Information Sharing Platform) je odprtokodna platforma za izmenjavo informacij o kibernetskih grožnjah. Prek platforme MISP partnerji izmenjujemo informacije o kazalnikih zlorab (IoC), pridobljenih z analizo škodljive kode ali zajemom in analizo sumljive omrežne dejavnosti. Tako pridobljeni indikatorji so ključnega pomena pri pravočasnem odkrivanju in proaktivni zajezitvi omrežnih zlorab ter tudi za povezovanje posameznih, z analizo pridobljenih indikatorjev z že znanimi omrežnimi zlorabami in okužbami.

Na SI-CERT upravljamo centralno vozlišče MISP v državi in smo dobro povezani v mednarodno skupnost. S priklopom na platformo MISP organizacije pridobijo brezplačen dostop do širokega nabora indikatorjev zlorab, ki jih lahko uporabijo za iskanje korelacij znotraj sistema SIEM ali pa zgolj kot dodatna pravila na požarni pregradi ali obogatitev filtrov poštnega strežnika.

Zavezanci se lahko za priklop na MISP obrnejo z elektronskim sporočilom na info@cert.si.

Poglavje 5
Predstavitev inšpekcijskih pregledov in priporočila na podlagi prakse (inšpekcijske izkušnje)

POVZETEK

V pričujočem poglavju so izpostavljene tiste ugotovitve, ki jih Inšpekcija za informacijsko varnost pri Uradu Vlade RS za informacijsko varnost najpogosteje zaznava pri izvedbi ustreznih nadzorov zavezancev v Republiki Sloveniji. Informacija se podaja kot pomemben pripomoček in napotilo za stare ter nove zavezance na podlagi Zakona o informacijski varnosti, da bodo lahko še bolj uspešno zagotovili uskladitev svojih procesov in varnostnih zahtev znotraj svojih organizacijskih okolij.

Ključne točke:

- Vloga in pristojnosti Inšpekcije za informacijsko varnost
- Postopki za pripravo na izvajanje inšpekcijskih postopkov pri zavezancih
- Glavne ugotovitve ob izvedenih inšpekcijskih postopkih (primeri dobrih praks in napotil za večjo pozornost na posameznih področjih).

V inšpekcijah, ki jih izvaja Inšpekcija za informacijsko varnost pri Uradu Vlade RS za informacijsko varnost, so najpogosteje zaznane nepravilnosti ali pomanjkljivosti pri zavezancih po Zakonu o informacijski varnosti:

Zavezanec ima pomanjkljivo izdelano zakonsko predpisano dokumentacijo ali pa navedene dokumentacije sploh nima.

Glede na to, v katero vrsto zavezancev spadajo na podlagi prvega odstavka 5. člena Zakona o informacijski varnosti, bi morali zavezanci imeti izdelano varnostno dokumentacijo v skladu z eno od uredb, ki veljajo za tovrstne zavezance (IBS, ODU ali povezani subjektu). Inšpekcija ugotavlja, da imajo zavezanci pogosto pomanjkljivo dokumentacijo (npr. manjkajo posamezni elementi, dokumentacija ne odraža dejanskega stanja SUNP in SUVI, dokumentacija ne podpira aktivnosti zavezanca) ali je celo sploh nimajo.

Zavezanec nima izdelanega popisa (ključnih) informacijskih virov/sistemov, ima pa izdelano analizo obvladovanja tveganj.

Popis sredstev znotraj SUVI je eden ključnih elementov za pripravo analize obvladovanja tveganj. Šele ko so določena sredstva prepoznana in popisana, je mogoče prepoznati možne grožnje za izgubo zaupnosti, celovitosti in razpoložljivosti sredstev, prepoznati morebitne njihove ranljivosti in oceniti stopnjo vpliva uresničitve groženj. Brez popisa sredstev tudi ni mogoče izdelati seznama ključnih, krmilnih in nadzornih informacijskih sistemov ter presoditi, ali je zagotavljanje storitev odvisno od posameznega sredstva. Analiza tveganj, izdelana brez popisa sredstev, je zato zelo verjetno izdelana pavšalno in je sama sebi namen. Pogosto so popisi sredstev sicer narejeni, vendar kot parcialne rešitve samo za ozke segmente poslovanja, za katere se je velikokrat izkazalo, da niso povezani z izvajanjem bistvenih storitev.

Poudarjamo, da je po izvedenem popisu sredstev treba tega tudi redno periodično posodabljati. Neizveden ali neposodobljen popis informacijskih sredstev pomeni, da bo na primer upravljanje in preprečevanje izrab tehničnih ranljivosti zelo oteženo. Nemogoče je namreč spremljati ranljivosti za informacijska sredstva, če ta sploh niso prepoznana oziroma popisana. Posledično zavezanci za morebitne ranljivosti izvejo šele po obvestilu SI-CERT ali zunanjih ponudnikov storitev, če je obveščanje seveda sploh izvedeno (pogosto ni).

Zavezanec nima izvedenih popisov poslovnih procesov (ali pa so ti izvedeni samo delno).

Enako, kot velja za popis sredstev, velja tudi za popis procesov. Brez popisa poslovnih procesov in prepoznave kritičnosti določenih procesov ni mogoče izdelati ter upravljati sistema neprekinjenega poslovanja, niti ni mogoče izvesti ocene vpliva na poslovanje.

Zavezanec nima izdelane ocene vpliva na poslovanje (BIA analiza), ima pa izdelano politiko/načrt neprekinjenega poslovanja.

Ocena vpliva na poslovanje oz. BIA analiza je eden ključnih elementov za pripravo politike neprekinjenega poslovanja, saj zajema določitev ciljnih časovnih okvirov za obnovitev procesov in ciljnih točk za obnovitev podatkov ter navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje. Hkrati je tudi temelj za navedbo ukrepov, ki zagotavljajo neprekinjeno poslovanje in minimalno raven poslovanja. Brez BIA analize ni mogoče realno oceniti, s katerimi ukrepi zavezanec zagotavlja neprekinjeno poslovanje in kako ga zagotavlja, niti ni mogoče realno določiti minimalne ravni poslovanja. Politika neprekinjenega poslovanja, izdelana brez BIA analize, je zato zelo verjetno pomanjkljiva ali pavšalno izdelana.

Zavezanec, ki izvaja storitve katerih zahtevana je (izredno) visoka razpoložljivost, nima vzpostavljene (ustrezne) sekundarne lokacije.

Nekateri zavezanci morajo storitve zagotavljati v zelo visoki razpoložljivosti, 24 ur na dan, sedem dni v tednu. Če so storitve odvisne od informacijskih sredstev (in skoraj gotovo so), bo zavezanec brez ustrezne sekundarne loka-

cije težko zagotavljal storitve v primeru izpada primarne lokacije, ki se lahko zgodi iz različnih razlogov (naravne nesreče, kot so poplave, potresi, požari, sabotaže ali druge vrste namernih poškodovanj). Taki zavezanci morajo zato zagotavljati ustrezno sekundarno lokacijo, ki bo zagotavljala nemoteno izvajanje storitev v primeru, da to na primarni lokaciji ni več mogoče.

Zavezanec ni opredelil varnostnih zahtev za ključne dobavitelje informacijske opreme, ki se uporablja za zagotavljanje bistvenih storitev.

Izvajanje kritičnih (bistvenih) procesov, s katerimi se zagotavlja neprekinjeno izvajanje bistvenih storitev, je pogosto odvisno od opreme ali storitev tretjih oseb, torej tudi pogodenih dobaviteljev. Zavezanci naj zato določijo kritičnost vsakega dobavitelja za poslovanje, pri čemer naj analiza upošteva možne posledice v primeru motenj v storitvah dobavitelja (med te spadajo tudi morebitne motnje pri dobavi opreme) ali celo za primer, da so te storitve onemogočene (npr. stečaj oziroma prenehanje poslovanja dobavitelja). Za ključne dobavitelje je nato treba opredeliti varnostne zahteve, tega pa zavezanci pogosto ne storijo. Dobro definirane varnostne zahteve zagotavljajo, da zavezanec dobi varno strojno in programsko opremo brez potencialnih ranljivosti. Pri strojni opremi naj gredo zahteve v smeri overjanja izvora (varnost dobavne verige), zahtevanje dokazil o izvajanju testiranj, prilaganje certifikatov za skladnost z varnostnimi standardi in podobno. Pri programski opremi naj gredo zahteve v smeri zagotavljanja sodobnih varnostnih funkcionalnosti (npr. t.i. »military grade« šifriranje), zagotavljanja podpore pri odpravi napak in ranljivosti, zagotavljanja rednih posodobitev ter vključene zaščite pred nepooblaščenim dostopom.

Ker zavezanci za IT področje pogosto najemajo zunanje ponudnike storitev, je ključno, da so v takem primeru varnostne zahteve zaglavne dobavitelje opredeljene v internih aktih in vključene v pogodbe (sporazum o ravni storitev). Zavezanci pogosto tega ne opredelijo. Za informacijsko varnost je odgovoren zavezanec tudi v primeru, ko izvajanje informacijskih storitev najemajo pri zunanjem ponudniku storitev.

Zavezanec ni predpisal in izvajal testov postopkov upravljanja izrednih dogodkov, ki imajo negativen vpliv na izvajanje bistvenih storitev.

Na izvajanje bistvenih storitev ali storitev, ki jih morajo neprekinjeno zagotavljati različni subjekti, lahko vplivajo različni dogodki. Na splošno ne zadostuje, da jih zavezanci samo opredelijo v predpisanih internih aktih, saj brez občasnega testiranja postopkov zavezanec težko predvideva, kako bodo vplivali na izvajanje bistvenih storitev, na poslovne procese ali na zagotavljanje neprekinjenega poslovanja. Zavezanci pogosto takšnih testov niti ne predpišejo, ali pa jih predpišejo in jih ne izvajajo (npr. imajo na lokaciji zagotovljen generator ter UPS za primer izpada električne energije, vendar ne testirajo, za kakšen obseg nalog in za koliko časa zadostujeta). Pomembno je, da zavezanci periodično takšne teste tudi izvedejo, saj bodo lažje zagotovili izvajanje storitev v realnih dogodkih.

Zavezanec ni redno izvajal (v skladu z navodili oziroma priporočili proizvajalcev opreme) posodobitev ključnih informacijskih sistemov (strežnikov, aplikacij, omrežne opreme, ipd.).

Neposodobljeni informacijski sistemi bistveno povečujejo tveganje za kibernetske napade, saj so izpostavljeni znanim ranljivostim, ki jih lahko izkoristijo različni akterji. Posledica so lahko v takšnim primerih izjemno hude, saj lahko vodijo v prekinitev zagotavljanja storitev, izgube podatkov, izgube nadzora nad sistemi in posledično velikih stroškov ter izgube ugleda. Zato je ključno, da se posodobitve izvajajo redno in pravočasno.

Zavezanec ni zagotovil ohranjanja dnevniških zapisov o delovanju vseh ključnih informacijskih sistemov in delov omrežja, ki so

bistvenega pomena za delovanje bistvenih storitev, za obdobje najmanj šest mesecev (na območju R Slovenije).

Definiranje ključnih informacijskih sistemov in delov omrežja je pomembno tudi ker je treba za te sisteme, če so bistvenega pomena za delovanje bistvenih storitev, zagotoviti dnevniške zapise (loge) za obdobje najmanj šest mesecev, pri čemer se morajo hraniti na območju Republike Slovenije. Pogosto pri zavezancih ugotavljamo, da takšnih zapisov sploh ni, ni vseh potrebnih zapisov, ali da se hranijo premalo časa.

Zavezanec ni preverjal kakovosti izdelave varnostnih kopij.

Varnostno kopiranje je eden ključnih mehanizmov za zagotavljanje razpoložljivosti podatkov v primeru nepredvidenih dogodkov. Zavezanci ga sicer zagotavljajo na različne načine, precej redkeje pa preverjajo kakovost izdelanih kopij. Če zavezanec namreč vsaj občasno ne izvede testa oz. simulacije obnove podatkov iz obstoječih kopij, bo težko vedel, ali je obnova sploh mogoča. Zavezanci naj zato poleg varnostnega kopiranja periodično izvajajo tudi obnovo z namenom, da preverijo, ali so varnostne kopije ustrezne in dovolj kakovostne, da omogočajo obnovo podatkov v primeru nepredvidenega dogodka.

Zavezanci sicer prepoznajo odgovorne osebe za neprekinjeno poslovanje, niso pa ti ključni kadri prepoznani v podpornih procesih (ni zagotovljene dosegljivosti potrebnega ključnega kadra izven delovnega časa).

Mogoča posledica takšnega ravnanja je, da zavezancu ključni kader ne bo na voljo ob morebitnih incidentih ali podobnih dogodkih. Zato je vprašljivo, ali bo zavezanec res lahko zagotavljal neprekinjeno poslovanje v takšnih primerih in na določene neželene dogodke reagiral učinkovito in pravočasno.

Zavezanci ne izvajajo rednega izobraževanja zaposlenih na področju informacijske varnosti in ne zagotavljajo zadostnega usposabljanja ter izpopolnjevanja za ključni IT kader.

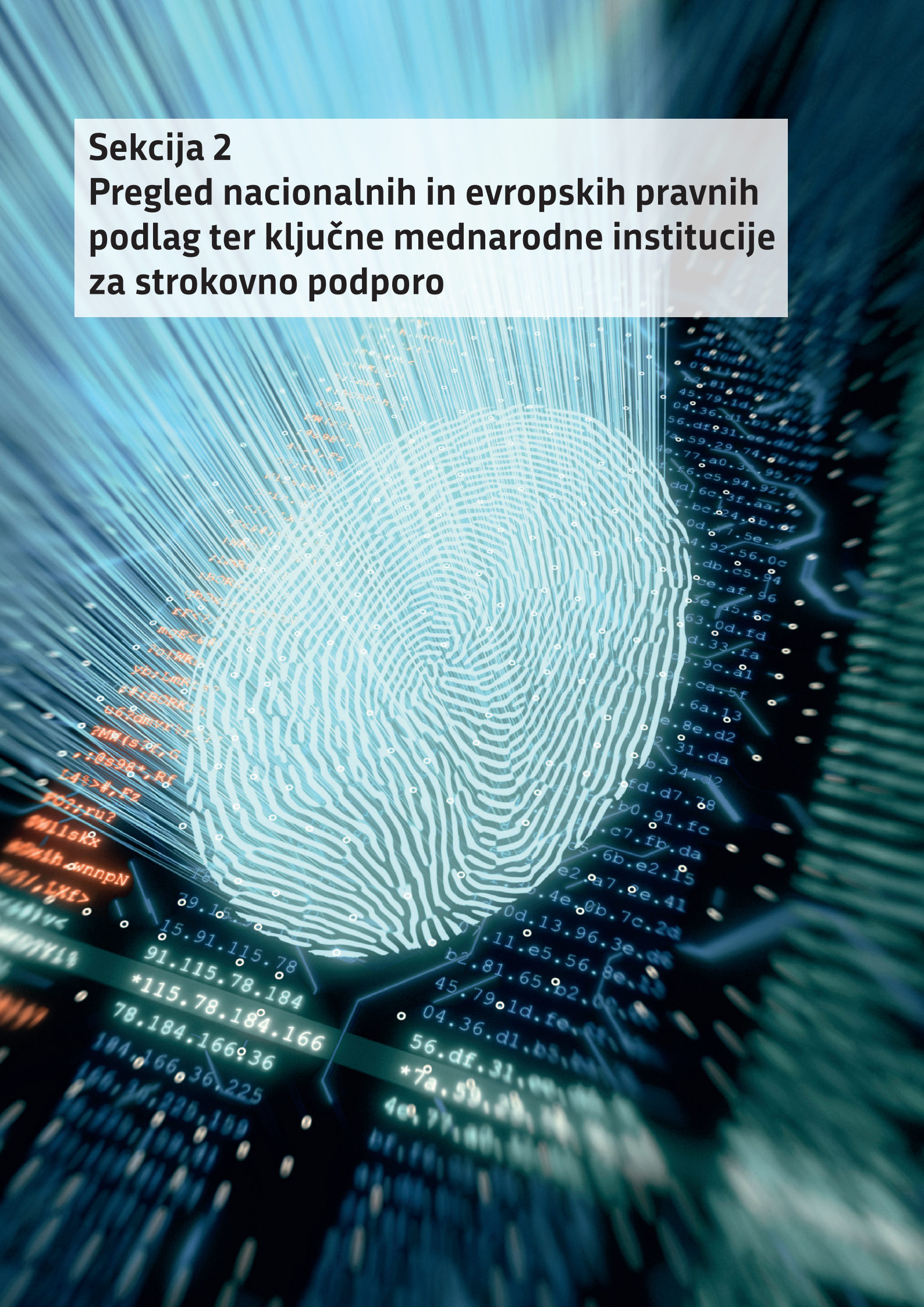
Strokovnjaki na področju kibernetske varnosti stalno opozarjajo, da smo ljudje najšibkejši člen v verigi kibernetska varnosti. Veliko škodljivih dogodkov bi se dalo preprečiti z ustreznim usposabljanjem zaposlenih, saj se incidenti pogosto začnejo na podoben način. Izobraževanje zaposlenih je zato ključnega pomena pri prepoznavanju tovrstnih dejanj, zlasti phishinga in drugih podobnih oblik socialnega inženiringa. Menimo, da bi morali biti zaposleni bolj ozaveščeni o posledicah, ki jih lahko povzročijo morebitna tvegana dejanja (npr. odpiranje škodljivih priponk, uporaba svojih naprav za službene namene in obratno, ipd.).

Poudariti je treba zlasti to, da zavezanci pogosto ne namenjajo dovolj pozornosti niti usposabljanju in izpopolnjevanju ključnega IT kadra, temveč so ti kadri prepuščeni lastni iniciativi in lastni volji. Poudarjamo, da je področje kibernetske varnosti take narave, da zahteva stalno usposabljanje in izpopolnjevanje, kar bi morali zavezanci upoštevati že v fazi načrtovanja proračunov.

Zavezanci nimajo potrebnega kadra/znanja za izvajanja dolžnega nadzorstva nad izvajanjem storitev zunanjih ponudnikov (ni mogoče obvladovanje tveganj dobavne verige).

S prejšnjo točko – izvajanje rednega izobraževanja in izpopolnjevanja kadra – je povezano tudi izvajanje nadzorstva nad izvajanjem storitev zunanjih ponudnikov. Dobavne verige ni mogoče nadzirati, če zavezanci nimajo kadra in/ali znanja, da to izvajajo. S tem ostane tveganje, povezano s celotno dobavno verigo, praktično neobvladovano ali nenadzorovano.

Sekcija 2
Pregled nacionalnih in evropskih pravnih podlag ter ključne mednarodne institucije za strokovno podporo



Poglavje 6
Pregled in predstavitev nacionalnih pravnih podlag ter ključnih poudarkov

POVZETEK

Poglavje ponuja pregled ključnih zakonodajnih aktov in smernic, ki urejajo področje informacijske varnosti v Republiki Sloveniji. Zakon o informacijski varnosti (ZInfV) določa pravne podlage za zaščito omrežij in informacijskih sistemov ter pristojnosti zavezancev, kot so izvajalci bistvenih storitev, izvajalci digitalnih storitev in ostali zavezanci. Integracija Direktive NIS-2 bo prinesla novosti v nacionalni zakonodaji, vključno s strožjimi standardi in razširjenim področjem uporabe. Prav tako uredbe, kot so tiste o varnostni dokumentaciji, zagotavljajo jasne okvirje za izvajanje varnostnih ukrepov. Poglavje poudarja pomembnost usklajevanja z evropskimi standardi in prilagodljivost zakonodaje glede na hitro spreminjajoče se grožnje.

Ključne točke:

- Zakon o informacijski varnosti (ZInfV)
- Direktiva NIS-2 in njen vpliv
- Uredbe o varnostni dokumentaciji
- Zakon o kritični infrastrukturi (ZKI)
- Strategija kibernetske varnosti
- Zakon o elektronskih komunikacijah (ZEKom-2)
- Pristojnosti nacionalnih organov in CSIRT
- Usklajevanje z EU standardi
- Prilagodljivost zakonodaje na nove grožnje.

Razumljivo je, da so zavezanci, ki so ključni za neprekinjeno delovanje širše družbene skupnosti tako pomembni, da jih zakonodajalec obravnava neposredno in posredno v posameznih pravnih predpisih. Zaradi navedenega je pričujoče poglavje usmerjeno v pregled trenutno veljavnih zakonskih aktov, ki bodo omogočali razumeti normativni okvir, pristojnosti in nenazadnje tudi odgovornosti za ureditev varnosti ter zagotavljanje neprekinjenosti delovanja ključnih procesov v teh organizacijah. Pomembno je tudi zavedanje, da se zakonodajni okvir na tem področju zaradi dinamičnih sprememb v mednarodnem in posledično nacionalnem okolju, vseskozi spreminja. Trenutno v Republiki Sloveniji poteka integracija nove EU direktive NIS-2[2] v nacionalni pravni red, kar bo posledično pomenilo, da bo do konca leta sprejet nov Zakon o informacijski varnosti[3]. V pregledu pomembnih zakonskih predpisov smo se v zaključku tega poglavja dotaknili tudi tistih pravnih predpisov, ki posredno ali v kombinaciji z osnovnimi pravnimi predpisi s področja informacijske varnosti vplivajo tudi na izvajalce bistvenih storitev.

Pri pripravi pregleda in predstavitve nacionalnih pravnih podlag ter ključnih poudarkov s področja informacijske varnosti v Sloveniji je pomembno, da se osredotočite na zakonodajo, uredbe ter smernice, ki pokrivajo to področje.

V nadaljevanju navajamo najpomembnejše pravne predpise:

Temeljni zakoni in predpisi

I **Zakon o informacijski varnosti (ZInfV)** (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-10 in 49/23)- Temeljni zakon, ki ureja področje informacijske varnosti v Sloveniji.

Ta zakon ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij ter informacijskih sistemov v Republiki Sloveniji. Tiso bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah in zagotavljajo bistvene storitve za ohranitev ključnih družbenih ter gospodarskih dejavnosti v Republiki Sloveniji. Določa minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona. Prav tako ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost, enotne kontaktne točke za informacijsko varnost, nacionalne skupine za obravnavo incidentov s področja varnosti elektronskih omrežij ter informacij (nacionalni CSIRT) in skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (CSIRT organov državne uprave) na področju zagotavljanja informacijske varnosti.

V 5. členu ZInfV so podrobno določeni zavezanci in področja, na katerih delujejo omenjeni zavezanci.

(1) Zavezanci po tem zakonu so:

- izvajalci bistvenih storitev,
- ponudniki digitalnih storitev,
- organi državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljevanju: organi državne uprave), in
- državni organi, organi lokalnih skupnosti, javne agencije in nosilci javnih pooblastil ter drugi subjekti, ki niso organi državne uprave iz prejšnje alineje ali izvajalci bistvenih storitev iz prve alineje tega odstavka in se povezujejo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom (v nadaljevanju: povezani subjekti).

(2) **Izvajalci bistvenih storitev** so subjekti, ki delujejo na naslednjih področjih:

[2] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 201/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2)

[3] Osnutek si lahko ogledate na tej povezavi https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16290

1. energija,
2. digitalna infrastruktura,
3. oskrba s pitno vodo in njena distribucija,
4. zdravstvo,
5. promet,
6. bančništvo,
7. infrastruktura finančnega trga,
8. preskrba s hrano in
9. varstvo okolja.

V 6. členu je opredeljen postopek določitev izvajalcev bistvenih storitev

(1) Za namen določitve izvajalcev bistvenih storitev Vlada Republike Slovenije določi seznam bistvenih storitev iz predpisa, ki ureja standardno klasifikacijo dejavnosti.

(2) Posameznega izvajalca bistvenih storitev na podlagi meril iz 7. člena tega zakona določi vlada.

(3) Ne glede na določbo prejšnjega odstavka vlada kot izvajalce bistvenih storitev določi tudi tiste upravljavce kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo področje kritične infrastrukture, in nosilce obrambnega načrtovanja, ki so določeni v skladu s predpisi, ki urejajo področje obrambe, katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov.

(4) Če izvajalec zagotavlja bistveno storitev v Republiki Sloveniji in še kateri drugi državi članici EU, se pristojni nacionalni organ pred določitvijo izvajalcev bistvenih storitev iz drugega odstavka ali prejšnjega odstavka tega člena v skladu z Direktivo 2016/1148/ES posvetuje s pristojnim nacionalnim organom države članice EU, kjer izvajalec takšne storitve zagotavlja.

V 7. členu tega zakona so še podrobneje opredeljena zakonska merila – metodologija za določitev kdo je izvajalec bistvenih storitev

(1) Pri določitvi izvajalcev bistvenih storitev iz drugega odstavka 5. člena tega zakona se upošteva naslednja merila:

- subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih oziroma gospodarskih dejavnosti;
- zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov ter
- incident bi imel pomemben negativen vpliv na zagotavljanje te storitve.

(2) Pri določanju, kako pomemben je negativen vpliv iz tretje alineje prejšnjega odstavka, se upoštevajo vsaj trije od naslednjih med področnih dejavnikov:

1. število uporabnikov, ki so odvisni od storitve subjekta;
2. odvisnost drugih področij iz drugega odstavka 5. člena tega zakona od storitve subjekta;
3. stopnja in trajanje vpliva, ki bi ga incidenti lahko imeli na gospodarske ter družbene dejavnosti ali javno varnost;
4. tržni delež subjekta;
5. geografska razširjenost, kar zadeva območje, ki bi ga incident lahko prizadel;
6. pomen subjekta za ohranitev zadostne ravni storitve, ob upoštevanju razpoložljivosti alternativnih načinov za zagotavljanje storitve.

(3) Pri odločanju, ali bi incident imel pomemben negativen vpliv, se upoštevata vsaj dva od naslednjih področnih dejavnikov:

- število uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvene storitve;
- trajanje incidenta;
- geografska razširjenost, kar zadeva območje, na katerega vpliva incident.

(4) Metodologijo za določitev izvajalcev bistvenih storitev podrobneje določi vlada.

11. člen opredeljuje varnostne zahteve, ki jih morajo zagotoviti izvajalci bistvenih storitev

(1) Izvajalci bistvenih storitev skladno z metodologijo iz tretjega odstavka 12. člena tega zakona, določijo svoje ključne, krmilne in nadzorne informacijske sisteme ter dele omrežja, s katerimi zagotavljajo izvajanje bistvenih storitev.

(2) Izvajalci bistvenih storitev izvedejo analizo, oceno in vrednotenje tveganj ter na tej osnovi pripravijo in izvedejo potrebne ukrepe za obvladovanje tveganj glede varnosti omrežij ter informacijskih sistemov, ki jih uporabljajo pri bistvenih storitvah.

(3) Izvajalci bistvenih storitev sprejmejo ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost tistih omrežij ter informacijskih sistemov, ki se uporabljajo za zagotavljanje bistvenih storitev, da bi zagotovili neprekinjeno izvajanje teh storitev.

(4) Če izvajalci bistvenih storitev za opravljanje svoje dejavnosti črpajo vhodne podatke in informacije iz ključnih delov nacionalno varnostnega sistema, vzpostavijo vse potrebne varnostne zahteve ob soglasju pristojnega ministrstva za posamezni ključni del nacionalno varnostnega sistema.

V 12. členu pa je določena **varnostna dokumentacija in varnostni ukrepi**, ki jih tukaj ne bomo posebej navajali, saj bodo podrobno opisani v 11. poglavju tega priročnika.

V 13. členu so opredeljene **dolžnosti in obseg priglasitve incidentov**. Podrobno smo to že predstavili v poglavju 4, kjer je predstavljena vloga SI-CERT.

Za opredelitev ostalih podrobnosti si lahko ogledate celotno vsebino zakona.

II. Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov (Uradni list RS, št. 118/23)

Ta uredba podrobneje določa vsebino in strukturo predpisane dokumentacije povezanih subjektov, metodologijo za pripravo analize obvladovanja tveganj informacijske varnosti z oceno sprejemljive ravni tveganj, način izvajanja obveznosti povezanega subjekta na področju informacijske varnosti, minimalni obseg varnostnih ukrepov glede informacijske varnosti ter pripravo navodil in postopkov za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave.

III. Uredba o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 98/23)

Ta uredba podrobneje določa vsebino in strukturo varnostne dokumentacije, metodologiji za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja in pripadajočih podatkov ter minimalni obseg in vsebino varnostnih ukrepov organov državne uprave.

IV. Uredba o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23)

Ta uredba podrobneje določa vsebino in strukturo varnostne dokumentacije, metodologijo za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja in pripadajočih podatkov ter minimalni obseg in vsebino varnostnih ukrepov izvajalcev bistvenih storitev.

V. Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev (Uradni list RS, št. 39/19)

Ta uredba določa tiste storitve iz Uredbe o standardni klasifikaciji dejavnosti (Uradni list RS, št. 69/07 in 17/08; v nadaljnjem besedilu: SKD), ki se za potrebe izvajanja Zakona o informacijski

varnosti (Uradni list RS, št. 30/18) štejejo za bistvene, in metodologijo za določitev izvajalcev bistvenih storitev, vključno z vrednotenjem med področnih in področnih dejavnikov.

Za izvajalce bistvenih storitev je to zelo pomemben dokument in dodatno pojasnjuje vrednotenje področnih in med področnih dejavnikov med posameznimi sektorji.

VI. Odlok o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za informacijsko varnost (Uradni list RS, št. 114/21 in 69/23)

S tem odlokom se ustanovi Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu: urad) ter se v skladu s tem odlokom, Zakonom o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21; v nadaljnjem besedilu: zakon) in z drugimi predpisi določijo njegove naloge in organiziranost.

VII. Strategija kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti (februar 2016)

S pomočjo strategije kibernetske varnosti Slovenija krepi svoj sistem zagotavljanja kibernetske varnosti, hkrati pa to področje tudi sistemsko ureja. Okrepitev celotnega sistema je nujna zaradi vedno večjega pomena kibernetske varnosti za nemoteno delovanje sistemov, od katerih je odvisno delovanje celotne družbe. Prav tako državo k temu spodbujajo in hkrati zavezujejo nacionalni ter mednarodni strateški dokumenti. Učinkovit sistem zagotavljanja kibernetske varnosti ni in ne more biti poceni, temveč je neprimerljivo cenejši, kot bi bilo odpravljanje posledic, ki bi lahko nastale ob varnostnih incidentih, če takega sistema ne bi bilo. Strategija vsebuje pregled obstoječega stanja na področjih, pomembnih za zagotavljanje kibernetske varnosti, opredeljuje vizijo ter zastavlja cilje. Prav tako opredeljuje področja, na katerih se bo udejanjala, in tveganja, ki nastopajo v kibernetskem prostoru. Strategija predlaga način, kako naj bo sistem zagotavljanja kibernetske varnosti organiziran, in potrebne ukrepe za uresničitev zastavljenih ciljev.

VIII. Zakon o elektronskih komunikacijah (ZEKom-2) (Uradni list RS, št. 130/22 in 18/23 – ZDU-10)

Ta zakon ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev, ureja zagotavljanje univerzalne storitve, zagotavljanje konkurence, upravljanje radiofrekvenčnega spektra ter elementov oštevilčenja, ureja učinkovitejšo gradnjo in postavitev elektronskih komunikacijskih omrežij ter souporabo obstoječe fizične infrastrukture, določa pogoje za omejitev lastninske pravice, določa pravice uporabnikov, ureja varnost omrežij in storitev, vključno v luči tveganj, ki jih prinašajo nove tehnologije ter delovanje v stanjih ogroženosti, zagotavlja uresničevanje in ureja varovanje pravice do komunikacijske zasebnosti uporabnikov javnih komunikacijskih storitev, ureja reševanje sporov na področju tega zakona, ureja pristojnosti, organizacijo in delovanje Agencije za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju: agencija) kot neodvisnega regulativnega organa ter pristojnosti drugih organov, ki opravljajo naloge po tem zakonu, ter druga vprašanja, povezana z elektronskimi komunikacijami.

V tem poglavju je zlasti pomembno VIII. poglavje Varnosti omrežij in storitev ter delovanje v stanjih ogroženosti, ki je posebej pomembno za telekomunikacijske operaterje.

Zakon o kritični infrastrukturi (ZKI) (Uradni list RS, št. 75/17, 189/21 – ZDU-1M in 102/24 – ZKI-1)

Ta zakon ureja ugotavljanje in določanje kritične infrastrukture Republike Slovenije, načela ter načrtovanje zaščite kritične infrastrukture, naloge organov in organizacij na področju kritične infrastrukture ter obveščanje, poročanje, zagotavljanje podpore odločanju, varovanje podatkov in nadzor na področju kritične infrastrukture.

Ta zakon je pomemben za tiste organizacije, ki so določene tako v kategorijo izvajalcev bistvenih storitev, kakor tudi upravljalcev kritične infrastrukture.

OPOMBA: V postopku sprejema je nov Zakon o informacijski varnosti s katerim bo Republika Slovenija v pravni red prenesla določila EU direktive NIS-2. V osmem poglavju bodo podrobneje predstavljene novosti, ki jih prinaša omenjena EU direktiva in se bodo ob sprejemu odrazile tudi v novem Zakonu o informacijski varnosti. Ravno tako je bil sprejet nov Zakon o kritični infrastrukturi, ki bo v nacionalni pravni red prenesel EU Critical Entities Resilience Directive (CER Directive - EU Directive 2022/2557), ki še tesneje povezuje področja kritične infrastrukture in kibernetske varnosti.

Poglavje 7
Pregled in predstavitev evropskih pravnih podlag ter ključnih poudarkov

POVZETEK

Evropska unija je skozi pravne in strateške ukrepe oblikovala celovit okvir za kibernetsko varnost, ki naslavlja hitro spreminjajoče se digitalne grožnje. Ključni dosežki vključujejo sprejetje Direktive NIS (2016), ki je prvič postavila pravne temelje za zaščito kritičnih sektorjev, ter njeno nadgradnjo z Direktivo NIS-2 (2022), ki širi področje uporabe na dodatne sektorje, uvaja strožje zahteve in spodbuja čezmejno sodelovanje. EU Cybersecurity Act (2019) uvaja certifikacijski sistem za IKT izdelke, storitve in procese, kar zagotavlja usklajenost varnostnih standardov po celotni EU. ENISA, kot centralni organ za kibernetsko varnost, podpira izvajanje teh ukrepov, spodbuja ozaveščenost ter krepi operativne zmogljivosti držav članic. Skupni cilj teh strategij je povečati odpornost kritične infrastrukture, izboljšati sodelovanje in zagotoviti varen digitalni prostor za vse državljane in organizacije.

Ključne točke:

- Pravna podlaga: Direktiva NIS (2016)
- Razširitev in nadgradnja: Direktiva NIS-2 (2022)
- Standardizacija: EU Cybersecurity Act
- Osrednja vloga: ENISA (Agencija za kibernetsko varnost)
- Krepitev odpornosti kritične infrastrukture
- Varovanje dobavnih verig in IKT sektorja
- Mednarodno sodelovanje in kibernetska diplomacija
- Evropski sistem zgodnjega opozarjanja: Kibernetski ščit (AI)
- Strateško usklajevanje držav članic
- Vzpostavitev zaupanja v digitalne ekosisteme.

Da bi pridobili celovito razumevanje strategij Evropske unije (EU), ki se nanašajo na vzpostavitev zakonodajnega in regulativnega okvira za kibernetsko varnost, se je nujno treba poglobiti v zapleten razvoj sistema kibernetske varnosti EU. Ta zgodovinski kontekst zagotavlja ključno osnovo za razumevanje kasnejših priporočil in najboljših praks, ki so bile oblikovane na podlagi neposrednih izkušenj ter spoznanj, pridobljenih iz različnih kontekstov.

Razvoj režima kibernetske varnosti EU je dokaz njegove prilagodljivosti kot odziv na dinamično pokrajino digitalnih groženj. Pot se je začela s porajajočimi se prizadevanji za obravnavo kibernetskih groženj s postopnimi pobudami v posameznih državah članicah. Ko sta se resnost in kompleksnost kibernetskih napadov stopnjevala, se je pojavilo kolektivno spoznanje – potreba po usklajenem pristopu za učinkovito reševanje teh izzivov.

To spoznanje je doseglo vrhunec z oblikovanjem strategije kibernetske varnosti EU, ki je bil temeljni mejnik. Direktiva o varnosti omrežij in informacij (NIS), sprejeta leta 2016, je določila prelomen pravni okvir, ki je določal ukrepe kibernetske varnosti v bistvenih sektorjih. Ta direktiva je poudarila medsebojno povezanost kritične infrastrukture in vzpostavila trden mehanizem poročanja za incidente, izboljšala zavedanje o razmerah ter spodbudila kulturo preglednosti.

Najnovejši korak prizadevanj EU za kibernetsko varnost se odraža v novi direktivi NIS-2, ki bi jo morale vse države članice EU sprejeti in objaviti ukrepe, potrebne za uskladitev z direktivo NIS 2. Ob upoštevanju »stanja« in, kjer je primerno, ustreznih evropskih ter mednarodnih standardov in stroškov izvajanja, navedeni ukrepi zagotavljajo raven varnosti omrežij ter informacijskih sistemov, ki ustreza povzročenim tveganjem. Pri ocenjevanju sorazmernosti teh ukrepov je treba ustrezno upoštevati stopnjo izpostavljenosti subjekta tveganjem, velikost subjekta in verjetnost pojava incidentov ter njihovo resnost, vključno z njihovim družbenim in gospodarskim učinkom.

Ukrepi temeljijo na „pristopu vseh nevarnosti“, katerega cilj je zaščititi omrežne in informacijske sisteme ter fizično okolje teh sistemov pred incidenti, ki vključujejo „vsaj“ naslednje:

(a) politike o analizi tveganja in varnosti informacijskega sistema;

(b) obravnavanje incidentov;

(c) neprekinjeno poslovanje, kot je upravljanje varnostnih kopij in obnova po katastrofi ter krizno upravljanje;

(d) varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, v zvezi z odnosi med vsakim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;

(e) varnost pri pridobivanju, razvoju in vzdrževanju omrežij ter informacijskih sistemov, vključno z obravnavanjem ranljivosti in razkritjem;

(f) politike in postopke za ocenjevanje učinkovitosti ukrepov za obvladovanje tveganja kibernetske varnosti;

(g) osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;

(h) politike in postopke v zvezi z uporabo kriptografije ter po potrebi šifriranja;

(i) varnost človeških virov, politike nadzora dostopa in upravljanje sredstev;

(j) uporaba večfaktorske avtentikacije ali rešitev za stalno avtentikacijo, zaščitene glasovne, video in besedilne komunikacije ter zaščitenih komunikacijskih sistemov v sili znotraj subjekta, kjer je primerno.

Na tej podlagi je EU marljivo črpala iz izkušenj in spoznanj iz resničnega sveta, da bi izboljšala svoj okvir kibernetske varnosti. Priporočila in najboljše prakse so natančno zbrali iz različnih sektorjev, industrij ter zainteresiranih strani. Ta ponavljajoč se proces vključuje stalen dialog, ki vključuje povratne informacije javnih in zasebnih subjektov.

Praktičnost teh priporočil je poudarjena tako, da temeljijo na dejanskih scenarijih, kar zagotavlja, da odmevajo s kompleksnostjo, s katero se soočajo različna ciljna okolja. S sintetiziranjem spoznanj iz različnih kontekstov želi EU razviti prilagodljive strategije, ki bodo poskrbele za edinstvene izzive, ki jih predstavljajo različni sektorji, hkrati pa se bodo držale splošnih načel odpornosti, sodelovanja in trdnega obvladovanja tveganja.

I. Politika kibernetske varnosti in zakonodajni okviri

Kibernetska varnost gre z roko v roki z razvojem tehnologije in posledično digitalno preobrazbo družbe. Danes so digitalizacija, digitalna identiteta, zasebnost, varstvo podatkov ter, kar je ključnega pomena, spreminjajoči se izzivi v varnosti in varnosti naših družb zelo pomembni pri oblikovanju politik ter so povezani s kibernetsko varnostjo.

Verjetno so najpomembnejši akterji na področju kibernetske varnosti države same po sebi. To pomeni, da se vse začne s kratkoročno ali srednjeročno strateško vizijo in načrtom države ter povezanimi ukrepi za njeno uresničitev (ENISA, 2020b). Ob upoštevanju tega bi morala biti osnovna prednostna naloga vlad oblikovanje celovite strategije kibernetske varnosti – skupaj z ustreznimi viri za financiranje pobud – ki določa pristojni organ, odgovoren za nacionalni položaj kibernetske varnosti v državi. Nekatere države članice imajo na primer strateški cilj povečati delež bruto domačega proizvoda zaradi digitalnega gospodarstva, pri čemer priznavajo, da sta njihov prihodnji razvoj in rast odvisna od njihove sposobnosti varovanja digitalnega gospodarstva. To zahteva ustrezno vlaganje in izvedbo strukturnih reform.

Glede na to, da digitalna transformacija ne pozna meja, se je kibernetska varnost internacionalizirala. Izzivi, s katerimi se sooča mednarodna skupnost, vključujejo prihodnje mednarodno sodelovanje pri predpisih o kibernetski varnosti, standardizaciji, čezmejnem pregonu kibernetske kriminalitete in mednarodnem pravu ter o tem, kako se odzvati na vse več hibridnih groženj.

Kibernetska varnost je horizontalna razsežnost, ki podpira prednostno nalogo Komisije, da zgradi „Evropo, primerno za digitalno dobo“.

V zadnjem desetletju je EU obravnavala široko paleto ukrepov kibernetske varnosti, katerih nadaljnje podrobnosti so navedene v tabeli 1. Zlasti od leta 2016 se je poudarek na kibernetski varnosti znatno povečal s sprejetjem direktive NIS, ki spodbuja industrijo in ustreznih akterjev za zmanjšanje ranljivostiter krepitev odpornosti. To je bilo dopolnjeno s podpisom javno-zasebnega partnerstva med EU in Evropsko organizacijo za kibernetsko varnost (ECSO) za podporo vsem vrstam projektov ter pobud za razvoj kibernetske varnosti v EU (Fovino, 2020).

Skupno sporočilo o kibernetski varnosti iz leta 2017 (EC, 2017c) predstavlja najobsežnejši del oblikovanja politike EU v zvezi s kibernetsko varnostjo, ki združuje ukrepe v tri stebre evropske politike kibernetske varnosti: odpornost, odvračanje in obramba.

„Akt o kibernetski varnosti“ (ES, 2017d) se osredotoča na opredelitev certifikacijskih procesov in standardov za kibernetsko varnost za izdelke IKT ter daje trajni mandat ENISA, Agenciji EU za kibernetsko varnost. Kar zadeva hibridne (kibernetske) grožnje, sta bili aprila 2016 objavljeni skupni sporočili Evropskemu parlamentu in Svetu z naslovom „Skupni okvir za boj proti hibridnim grožnjam“ (EU, 2016) ter „Povečanje odpornosti in krepitev zmogljivosti za obravnavo hibridne grožnje« junija 2018 (EC, 2016a).

Podobno bo „Cyber Diplomacy Toolbox“ zagotovil sredstva za usklajevanje odziva držav članic EU na zlonamerne kibernetske dejavnosti na ravni EU. Drugi dopolnilni ukrepi vključujejo „načrt“, priporočilo o obravnavi hudih, obsežnih kibernetskih incidentov, ustanovitev Evropskega kompetenčnega centra za kibernetsko varnost za usklajevanje mreže kompetenčnih centrov za kibernetsko varnost in posebne smernice o tem, kako obravnavati ukrepe kibernetske varnosti v omrežjih 5G (Fovino, 2020).

Direktiva o varnosti omrežij in informacijskih sistemov – Direktiva NIS

Direktiva o varnosti omrežij in informacijskih sistemov – Direktiva NIS (EC, 2016b) – je vseevropska zakonodaja o kibernetski varnosti, katere cilj je zagotoviti zmogljivosti kibernetske varnosti na enaki ravni razvoja v vseh državah članicah EU. Zagotavlja učinkovito izmenjavo informacij in sodelovanje, vključno s čezmejno izmenjavo informacij, s čimer prispeva k ustvarjanju višje ravni kibernetske varnosti v EU.

Direktiva NIS operaterjem bistvenih storitev (OES) in ponudnikom digitalnih storitev (DSP) nalaga nove zahteve glede varnosti omrežij ter informacij. Oba sta odgovorna za prijavo večjih varnostnih incidentov. Predmet uredbe so tudi DSP, ki še niso vzpostavljeni, a še vedno delujejo v EU. Tudi če OES in DSP oddajo vzdrževanje svojih informacijskih sistemov tretjim osebam, jih Direktiva NIS šteje za odgovorne za vse varnostne incidente. Poleg tega morajo OES in DSP poročati o vseh pomembnih incidentih pristojnim organom ali skupinam za odzivanje na incidente z računalniško varnostjo (CSIRT). Pomemben incident kibernetske varnosti določa število uporabnikov, ki jih je prizadela kršitev varnosti, in dolgotrajnost ter geografski doseg incidenta.

Države članice EU morajo vzpostaviti strategijo Direktive NIS, ki poleg nacionalnih pristojnih organov (NCA) in enotnih kontaktnih točk (SPOC) vključuje ustanovitev skupin CSIRT. Takšni viri so odgovorni za obravnavanje kršitev kibernetske varnosti na način, ki zmanjša vpliv. Poleg tega se vse države članice EU spodbuja k izmenjavi informacij o kibernetski varnosti.

Na splošno Direktiva NIS zagotavlja pravne ukrepe, ki povečujejo raven kibernetske varnosti v EU z zagotavljanjem:

- Izmenjava informacij, saj morajo države članice ustanoviti skupine CSIRT in pristojni nacionalni organ NIS.
- Sodelovanje z ustanovitvijo skupine za sodelovanje za podporo in olajšanje strateškega sodelovanja ter izmenjave informacij med državami članicami. NIS Cooperation group je skupina za strateško sodelovanje, kjer države članice EU sodelujejo, izmenjujejo informacije in se dogovarjajo o tem, kako dosledno izvajati direktivo NIS po vsej EU. Skupina za sodelovanje NIS daje tudi strateško usmeritev osnovni mreži EU CSIRT. Člani NIS Cooperation Group so predstavniki ustreznih nacionalnih ministrstev in nacionalnih agencij za kibernetsko varnost.
- Ozaveščenost o varnosti s spodbujanjem kulture varnosti v ključnih sektorjih za gospodarstvo in družbo EU, ki so močno odvisni od IKT, kot so energija, promet, voda, bančništvo, infrastrukture finančnih trgov, zdravstvo in digitalne infrastrukture.

Zadnji korak Komisije EU – Direktiva NIS 2

Direktiva NIS zahteva občasno pregledovanje njenega delovanja. V zvezi s tem je bilo v 3. četrtletju 2020 odprto posvetovanje, rezultati tega posvetovanja pa so bili uporabljeni za vrednotenje in oceno učinka Direktive NIS. Kot rezultat pregleda je bila sprejeta nova zakonodajna direktiva NIS-2. Polno ime je »Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 in o razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2)«.

Natančneje, NIS 2 se osredotoča na razširitev direktive NIS in zagotavlja naslednje:

Večje zmogljivosti

- Uvaja strožje ukrepe nadzora in izvršbe.
- Predvideva seznam upravnih sankcij, kot so globe za kršitev obveznosti upravljanja tveganja kibernetske varnosti in poročanja.

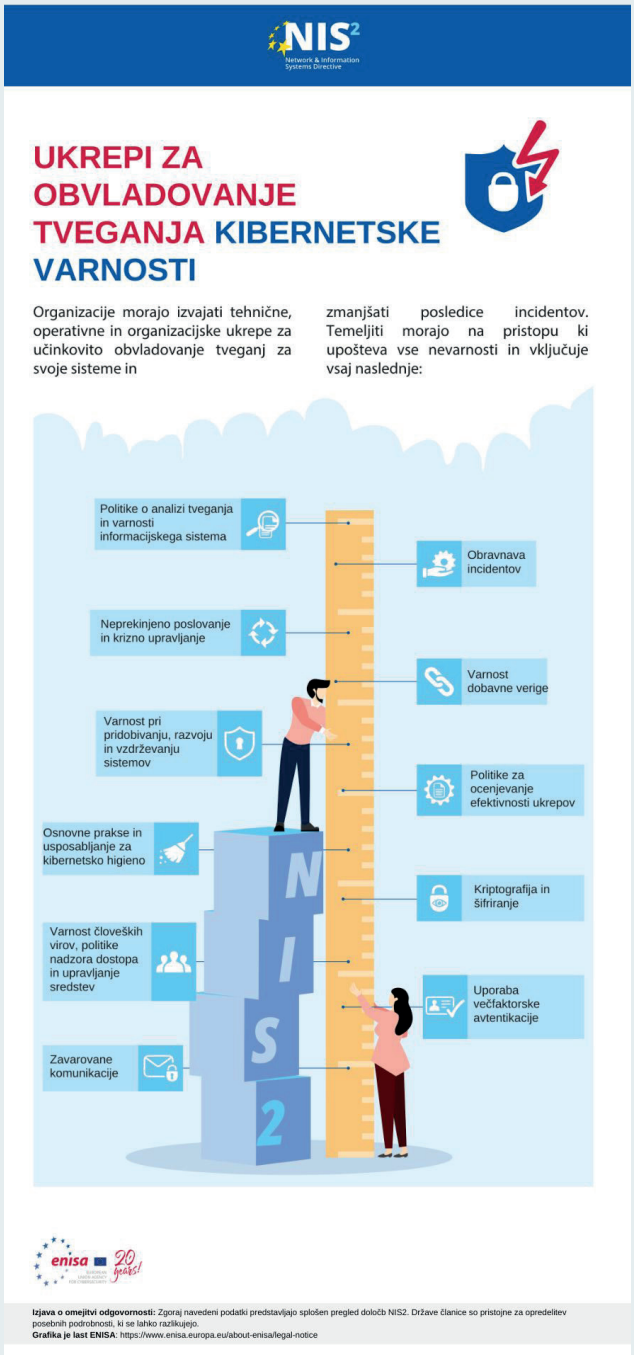
Povečano sodelovanje

- Vzpostavlja evropsko mrežo povezovalnih organizacij za kibernetske krize (EU-CyCLONe) za podporo usklajenega upravljanja obsežnih kibernetskih varnostnih incidentov in kriz na ravni EU.
- Spodbuja izmenjavo informacij in sodelovanje med organi držav članic prek okrepljene vloge skupine za sodelovanje.

- Vzpostavlja usklajeno razkritje ranljivosti za na novo odkrite ranljivosti po vsej EU.

Okrepljeno obvladovanje tveganja kibernetske varnosti

- Zvišuje varnostne zahteve s seznamom osredotočenih ukrepov, vključno z odzivom na incidente in kriznim upravljanjem, obravnavanjem ranljivosti ter razkritjem, testiranjem kibernetske varnosti in učinkovito uporabo šifriranja.



Shema 5: Ukrepi za obvladovanje tveganj kibernetske varnosti po NIS 2 (Vir: URSIV)

- Povečuje kibernetsko varnost dobavne verige za ključne informacijske in komunikacijske tehnologije.
- Uvaja odgovornost vodstva družbe za skladnost z ukrepi za obvladovanje tveganj kibernetske varnosti.
- Poenostavlja obveznosti poročanja o incidentih z natančnimi določbami o procesu poročanja, vsebini in časovnici.

Poleg tega NIS 2 razširja področje uporabe direktive na več sektorjev in storitev, kot so:

- ponudniki javnih elektronskih komunikacijskih omrežij ali storitev;
- digitalne storitve, kot so platforme storitev socialnega mreženja in podatkovni centri;
- ravnanje z odpadnimi vodami in odpadki;
- prostor;
- proizvodnja nekaterih kritičnih izdelkov (kot so zdravila, medicinske naprave, kemikalije);
- poštne in kurirske storitve;
- hrana;
- javna uprava.

Ena najpomembnejših sprememb, ki jih prinaša direktiva NIS 2, je opredelitev novega področja uporabe. Dejansko, kjer je Direktiva NIS v svoje področje uporabe vključila operaterje bistvenih storitev in ponudnike digitalnih storitev, Direktiva NIS 2 prinaša nadomestitev teh z dvema novima kategorijama subjektov. Natančneje, člen 2. predloga Komisije bi določil, da se Direktiva NIS 2 uporablja za nekatere „**javne** in **zasebne bistvene subjekte**“, ki delujejo v sektorjih, navedenih v Prilogi I Direktive NIS 2 (energija, promet, bančništvo, infrastrukture finančnih trgov, zdravstvo, pitna voda, odpadna voda, digitalna infrastruktura, javna uprava in prostor) ter nekaterim „**pomembnim subjektom**“, ki delujejo v sektorjih, navedenih v Prilogi II Direktive NIS 2 (poštne in kurirske storitve, ravnanje z odpadki, proizvodnja, proizvodnja ter distribucija kemikalij, proizvodnja, predelava in distribucija hra-

ne, proizvodnjater digitalni ponudniki). Poleg tega je uvedeno pravilo o omejitvi velikosti, v skladu s katerim vsi srednji in veliki subjekti, kot so opredeljeni v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij, ki delujejo v zgoraj omenjeni sektorji, bi samodejno spadali v področje uporabe direktive NIS 2 (uvodna izjava 8. direktive NIS 2) (Baldin, 2021; ECSO, 2020).

Poleg tega Direktiva NIS 2 med drugim:

- od držav članic zahteva, da sprejmejo nacionalno strategijo kibernetske varnosti (členi 5–11 Direktive NIS 2);
- krepi sodelovanje med državami članicami z omogočanjem strateškega sodelovanja in izmenjave informacij (12. do 16. člen Direktive NIS 2);
- krepi varnostne zahteve z obveznostjo držav članic, da vsem zajetim subjektom naložijo obveznosti kibernetske varnosti, in poenostavi obveznosti poročanja (členi 17 do 23 direktive NIS 2);
- omogoča izmenjavo informacij med zajetimi subjekti (26. in 27. člen Direktive NIS 2); in
- oblikuje strožje nadzorne ukrepe, zahteve za izvrševanje ter usklajene minimalne sankcije (28. do 34. člen Direktive NIS 2) (Baldin, 2021).

II. Strategija EU za kibernetsko varnost

Cilj strategije EU za kibernetsko varnost je podpirati skupno odpornost Evrope na kibernetske grožnje in zagotoviti, da lahko vsi državljani ter podjetja izkoristijo uporabo zaupanja vrednih in zanesljivih digitalnih storitev, aplikacij ter orodij. Varuje globalni in odprt internet ter zagotavlja varnost in zaščito evropskih vrednot ter temeljnih pravic vsakogar. V okviru strategije EU za kibernetsko varnost so obravnavana tri glavna področja ukrepov EU.

Odpornost, tehnološka suverenost in vodstvo

Vključuje reformo varnostnih pravil v zvezi z omrežnimi in informacijskimi sistemi, da se poveča raven kibernetske odpornosti kritičnih javnih in zasebnih sektorjev, kot so bolnišnice, energetska omrežja, železnice, podatkovni centri, javne uprave, raziskovalni laboratoriji in proizvodnja kritičnih medicinskih naprav in zdravil ter druge kritične infrastrukture in storitve. Takšne infrastrukture morajo ostati neprepustne v hitro spreminjajočem se in kompleksnem okolju groženj. To se izvaja z Direktivo o ukrepih – revidirano Direktivo NIS ali »NIS 2« – za visoko skupno raven kibernetske varnosti po vsej EU.

Predlaga se tudi vzpostavitev mreže varnostno-operativnih centrov (SOC) po vsej EU, ki bi izkoriščala umetno inteligenco (AI). Ta mreža SOC bo oblikovala „kibernetski varnostni ščit“ za EU, ki bo lahko dovolj zgodaj zaznal znake kibernetskega napada in omogočil proaktivno ukrepanje. Dodatni ukrepi bodo vključevali namensko podporo malim in srednje velikim podjetjem, izpopolnjevanje delovne sile, privabljanje ter ohranjanje strokovnjakov za kibernetsko varnost in vlaganje v raziskave ter inovacije, ki so odprte, konkurenčne in temeljijo na odličnosti.

Operativna zmogljivost za preprečevanje, odvračanje in odzivanje

V postopnem in vključujočem procesu z državami članicami je v pripravi nova skupna kibernetska enota. Cilj je zbližati organe EU in organe držav članic, odgovorne za preprečevanje, odvračanje ter odzivanje na kibernetske napade, da se okrepi njihovo sodelovanje. Poleg tega so predlagani predlogi za preprečevanje, odvračanje, odvračanje in učinkovito odzivanje na zlonamerne kibernetske dejavnosti, zlasti tiste, ki vplivajo na kritične infrastrukture, dobavne verige, demokratične institucije ter procese. EU si prizadeva tudi za nadaljnjo krepitev sodelovanja na področju kibernetske obrambe in razvoj najsodobnejših zmogljivosti za kibernetsko obrambo, pri čemer izkorišča delo Evropske obrambne agencije ter spodbuja države članice, da v celoti izkoristijo Stalno strukturno sodelovanje in Evropski obrambni sklad.

Sodelovanje za napredek globalnega in odprtega kibernetskega prostora

EU nadalje podpira sodelovanje z mednarodnimi partnerji za krepitev svetovnega reda, ki temelji na pravilih, spodbujanje mednarodne varnosti in stabilnosti v kibernetskem prostoru ter zaščito človekovih pravic in temeljnih svoboščin na spletu. Da bi pospešila mednarodne standarde, ki odražajo te temeljne vrednote EU, bo EU spodbujala tudi sodelovanje z Združenimi narodi in drugimi ustreznimi forumi, okrepila orodje EU za kibernetsko diplomacijo ter povečala prizadevanja za krepitev kibernetskih zmogljivosti v tretjih državah z razvojem zunanje kibernetske zmogljivosti EU Agenda gradnje. EU bo oblikovala tudi mrežo kibernetske diplomacije EU po vsem svetu, da bi promovirala svojo vizijo kibernetskega prostora.

EU je prav tako zavezana podpreti novo strategijo kibernetske varnosti s povečano ravnjo naložb, predvidenih v naslednjih sedmih letih, prek programa Digitalna Evropa in Horizon Europe ter načrta za oživitev Evrope. Cilj je doseči do 4,5 milijarde EUR skupnih naložb iz EU, držav članic in industrije v okviru strokovnega centra za kibernetsko varnost in mreže usklajevalnih centrov ter zagotoviti, da večji del doseže MSP.

Poleg tega je namenjen krepitvi industrijskih in tehnoloških zmogljivosti EU na področju kibernetske varnosti s projekti, ki jih skupaj podpirata proračun EU ter nacionalni proračuni. V zvezi s tem ima EU priložnost združiti svoja sredstva, da bi okrepila svojo strateško avtonomijo in spodbudila svoj vodilni položaj na področju kibernetske varnosti v celotni digitalni dobavni verigi v skladu z vrednotami ter prednostnimi nalogami EU.

III. EU Cybersecurity Act

EU Cybersecurity Act (Zakon EU o kibernetski varnosti) (EC, 2019c) je začel veljati 27. junija 2019. Gre za obsežen sveženj ukrepov, katerih cilj je okrepiti odpornost proti kibernetskim napadom v Evropski uniji (EU). Gre za pomemben korak k varnosti na evropskem enotnem digitalnem trgu in večjemu zaupanju v internet stvari (IoT). Gre za pravni okvir, ki usklajuje testne postopke za certificiranje proizvodov, storitev in procesov na ravni EU.

Natančneje, zakon EU o kibernetski varnosti vključuje:

- Trajni mandat za Agencijo EU za kibernetsko varnost (ENISA), ki predvideva znatno povečanje finančnih in človeških virov agencije. V zvezi s tem ima ENISA omogočeno, da poveča zmogljivosti kibernetske varnosti v Evropski uniji in spodbuja pripravljenost. ENISA naj bi delovala tudi kot neodvisen kompetenčni center. Cilj je dvojen, ozaveščati državljane in podjetja ter podpreti institucije EU in države članice pri izvajanju političnega okvira ter ustreznih pogojev na področju kibernetske varnosti.
- Vzpostavitev okvira EU za certificiranje varnosti IKT za izdelke, storitve in procese. To vključuje obsežen nabor pravil, tehničnih zahtev, standardov in postopkov na ravni EU za vrednotenje lastnosti kibernetske varnosti izdelkov, storitev ali procesov. Certifikati veljajo v vseh državah članicah EU in zagotavljajo informacije o izpolnjenih varnostnih zahtevah IKT. Podjetja, ki poslujejo v EU, bodo imela koristi od tega, da bodo morale svoje izdelke, postopke in storitve IKT certificirati samo enkrat, ter da bodo njihovi certifikati priznani po vsej EU. ENISA bo imela ključno vlogo pri vzpostavitvi in vzdrževanju evropskega certifikacijskega okvira za kibernetsko varnost s pripravo tehnične podlage za posebne sheme certificiranja. ENISA bo skrbela za obveščanje javnosti o certifikacijskih shemah in izdanih certifikatih preko namenskega portala.
- Na podlagi novih pravil o telekomunikacijah (Kodeks elektronskih komunikacij) morajo države članice zagotoviti ohranitev celovitosti in varnosti javnih komunikacijskih omrežij, ter da operaterji sprejmejo tehnične in organizacijske ukrepe za obvladovanje morebitnih varnostnih tveganj v omrežjih ter storitvah. Določa tudi, da imajo pristojni nacionalni regulativni organi pooblastila,

vključno s pooblastilom za izdajanje zavezujočih navodil in zagotavljanje skladnosti z njimi. Poleg tega lahko države članice splošnim pooblastilom za operaterje določijo pogoje v zvezi z varnostjo javnih omrežij pred nepooblaščenim dostopom zaradi varovanja zaupnosti komunikacij.

- Akt EU o kibernetski varnosti prvič določa »zasnovo zasnove« in »privzeto varnost« kot regulativni načeli za varnostno pomembne izdelke. V zvezi s tem spodbuja proizvajalce ali ponudnike, vključene v načrtovanje in razvoj izdelkov, storitev ali procesov IKT, da izvajajo ukrepe v najzgodnejših fazah procesa načrtovanja ter razvoja. To omogoča zaščito varnosti teh izdelkov, storitev ali procesov na najvišji možni ravni, tako da je pojav kibernetskih napadov predviden in minimiziran.

Tisti, za katere se pričakuje, da bodo imeli koristi od zakona EU o kibernetski varnosti, vključujejo:

- Državljani in končni uporabniki, ki jim bo omogočeno bolj poučeno odločanje o nakupu glede izdelkov in storitev, ki jih uporabljajo.
- Prodajalci in ponudniki izdelkov ter storitev, ki bodo deležni stroškovnih in časovnih prihrankov, saj bodo opravili enoten postopek za pridobitev evropskega certifikata, ki je veljaven in jim omogoča konkurenčnost v vseh državah članicah.
- Vlade, ki bodo bolje opremljene za sprejemanje bolj informiranih odločitev o nakupu izdelkov in storitev IKT.

Opozoriti je treba, da so sheme certificiranja, ustvarjene v skladu z Zakonom EU o kibernetski varnosti, prostovoljne. To praktično pomeni, da se lahko prodajalci odločijo, ali želijo, da so njihovi izdelki certificirani pod njimi. Vendar pa zakon o kibernetski varnosti predvideva, da lahko Komisija oceni učinkovitost in uporabo sprejetih evropskih certifikacijskih shem za kibernetsko varnost. Na ta način lahko oceni, ali bi morala posebna evropska certifikacijska shema za kibernetsko varnost postati obvezna prek ustrezne zakonodaje EU, da se zagotovi ustrezna raven kibernetske varnosti izdelkov, storitev in procesov IKT.

V skladu z aktom EU o kibernetski varnosti se uveljavljajo vloga in odgovornosti Agencije EU za kibernetsko varnost (ENISA). Natančneje, glavne naloge ENISA v okviru novega mandata so:

- **Podpora izvajanju politik** na področju kibernetske varnosti, zlasti direktive o omrežnih in informacijskih sistemih (NIS), kot tudi drugih političnih pobud z elementi kibernetske varnosti v različnih sektorjih (npr. energija, promet, finance).
- **Zgradite strokovno znanje** o kibernetski varnosti, na primer z usposabljanji, da bi pomagali izboljšati zmogljivosti javnih organov EU in nacionalnih javnih organov.
- **Analiza trga** glede standardizacije in certificiranja kibernetske varnosti.
- **Zagotavljanje operativnega sodelovanja in kriznega upravljanja**, namenjenega krepitvi obstoječih preventivnih operativnih zmogljivosti ter podpiranju operativnega sodelovanja kot sekretariat mreže CSIRTs. ENISA bo tudi nudila pomoč državam članicam pri obravnavi incidentov in imela vlogo pri usklajenem odzivu EU na obsežne čezmejne kibernetske incidente.
- **Usklajeno razkrivanje ranljivosti**, kjer bo državam članicam in institucijam, agencijam in organom Unije pomagalo pri vzpostavitvi ter izvajanju politik razkritja ranljivosti na prostovoljni osnovi.

Viri:

- Baldin, A. (2021). EU: Towards the adoption of the NIS 2 Directive. OneTrust DataGuidance, December 2021. Retrieved from https://www.dataguidance.com/opinion/eu-towards-adoption-nis-2-directive

- Council of the European Union (2020). Council Resolution on Encryption: Security through encryption and security despite encryption. Retrieved from https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf
- EC (2016a). Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats – a European Union Response, JOIN(2016) 18 Final. European Commission, 6 April 2016. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
- EC (2016b). The Directive on Security of Network and Information Systems (NIS Directive). European Commission and European Parliament, 5 July 2016. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis-directive
- EC (2017a). Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises. European Commission. Retrieved from https://eur-lex.europa.eu/eli/reco/2017/1584/oj
- EC (2017b). Cybersecurity in the European Digital Single Market. European Commission, Directorate-General for Research and Innovation, 24 March 2017. Retrieved from https://doi.org/10.2777/466885
- EC (2017c). Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, JOIN(2017) 450 Final. European Commission, 13 September 2017. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=-JOIN:2017:450:FIN
- EC (2017d). Proposal for a Regulation of the European Parliament and of the Council on ENISA and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ('Cybersecurity Act'), COM(2017) 477 Final. European Commission, 13 September 2017. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN
- EC (2019c). EU Cybersecurity Act - Regulation (EU) 2019/881 of the European Parliament and of the Council. European Commission. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- EU (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 01 Final. European Parliament, Council of the European Union, European Economic and Social Committee, and Committee of the Regions. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001
- Fovino, I. N. (2020). Cybersecurity – our digital anchor, a European perspective. European Commission, Joint Research Centre, Ispra - Italy, Luxembourg: Publications

Poglavje 8
Pregled področij delovanja Evropske agencije za kibernetsko varnosti (ENISA)

POVZETEK

ENISA predstavlja ključni steber pri zagotavljanju kibernetske varnosti na ravni EU. Skozi svoja poročila, smernice in analize organizacijam omogoča učinkovito prepoznavanje in obvladovanje kibernetskih groženj. Širok nabor dokumentov, od poglobljenih analiz trenutnih in prihodnjih groženj do dobrih praks za varnost dobavnih verig, pomaga izvajalcem bistvenih storitev in nacionalnim organom pri prilagajanju na kompleksne izzive. Posebna pozornost je namenjena sektorsko specifičnim priporočilom za področja, kot so zdravstvo, promet in umetna inteligenca.

Ključne točke:

- Poročilo o grožnjah za leto 2024
- Ocena zrelosti izobraževanja o kibernetski varnosti
- Napovedovanje kibernetskih groženj za leto 2030
- Dobre prakse za krizno upravljanje
- Varnost dobavnih verig in IoT
- Smernice za varnost umetne inteligence
- Analize in poročila za posamezne izpostavljene sektorje.

V nadaljevanju je predstavljenih nekaj primerov dokumentov in študij, ki so lahko uporabne za pridobitev dodatnih informacij ali znanja s področja informacijske varnosti za izvajalce bistvenih ali pomembnih storitev s strani ENISA:

- 2024 Report on the State of the Cybersecurity in the Union: Ta dokument je prvo poročilo o stanju kibernetske varnosti v Uniji, ki ga je sprejela ENISA v sodelovanju s skupino za sodelovanje NIS in Evropsko komisijo, v skladu z 18. členom Direktive (EU) 2022/2555 (v nadaljevanju NIS2).Namen poročila je oblikovalcem politik na ravni EU zagotoviti na dokazih temelječ pregled trenutnega stanja na področju kibernetske varnosti in zmogljivosti na ravni EU ter nacionalni in družbeni ravni ter priporočila politike za odpravo ugotovljenih pomanjkljivosti in povečanje ravni kibernetske varnosti po vsej Uniji.
- Cybersecurity Awareness Raising: The ENISA-Do-It-Yourself Toolbox: AR-in-a-Box je celovita rešitev za dejavnosti ozaveščanja o kibernetski varnosti, zasnovana za potrebe javnih organov, operaterjev bistvenih storitev ter velikih in malih zasebnih podjetij. Zagotavlja teoretično in praktično znanje o tem, kako oblikovati in izvajati učinkovite programe ozaveščanja o kibernetski varnosti, vključno z:
  - Smernice za ustvarjanje programov ozaveščanja po meri za interno uporabo znotraj organizacije.
  - Smernice za ustvarjanje ciljno usmerjenih kampanj za ozaveščanje zunanjih deležnikov.
  - Navodila za izbiro ustreznih orodij in kanalov za učinkovito doseganje ciljne publike.
  - Navodila za razvoj ključnih kazalnikov uspešnosti za oceno učinkovitosti programa ali kampanje.
  - Priročnik za razvoj komunikacijske strategije, ki je ključna za doseganje ciljev ozaveščanja.
  - Kviz za ozaveščanje, s katerim preverimo razumevanje in zadrževanje ključnih informacij.
  - Igra za ozaveščanje v različnih različicah in slogih, skupaj z vodnikom o igranju.

  Z AR-in-a-Box ENISA organizacijam zagotavlja bistvena orodja in vire za učinkovito dvigovanje ozaveščenosti o kibernetski varnosti v okviru njihovega delovanja ter ponuja dinamično rešitev, ki se bo redno posodabljala in obogatila.
- Annual Report - Trust Services Security Incidents 2023: Poročilo ENISA za leto 2023 o varnostnih incidentih v storitvah zaupanja predstavlja sedmi krog poročanja o varnostnih incidentih za sektor storitev zaupanja v EU, pri čemer analizira temeljne vzroke, statistiko in trende. Gre za zbirni pregled prijavljenih kršitev za leto 2023, ki jih je 27 držav članic EU in 3 države EGP posredovalo ENISA in Komisiji.
- Cyber Europe 2024 - After Action Report: Poročilo po ukrepanju ponuja pregled izdaje vaje Cyber Europe iz leta 2024, ki je bila izvedena junija in je bila namenjena odkrivanju vrzeli ter povečanju pripravljenosti in odpornosti na kibernetsko varnost.
- ENISA Threat Landscape 2024: Leta 2024 je bilo ugotovljenih sedem glavnih groženj kibernetski varnosti, pri čemer so grožnje zoper razpoložljivost na vrhu lestvice, sledijo pa ji izsiljevalska programska oprema in grožnje zoper podatke, poročilo pa ponuja ustrezen poglobljen potop v vsako od njih z analizo več tisoč javno prijavljenih kibernetskih incidentov ter dogodkov.
- Cybersecurity Education Maturity Assessment: Namen te študije ENISA je razviti model ocenjevanja zrelosti za oceno stopnje izobrazbe o kibernetski varnosti vsake države članice v osnovnih in srednjih šolah ter zagotoviti celovit pregled EU. Poleg tega si ENISA prizadeva zbirati in deliti priporočila ter najboljše prakse med državami, skupaj s kvantitativnimi ocenami zrelosti.
- Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report: To je druga ponovitev študije »ENISA Foresight Cybersecurity Threats for 2030«, ki predstavlja celovito analizo in oceno nastajajočih gro-

ženj kibernetski varnosti, predvidenih za leto 2030. Poročilo ponovno ocenjuje predhodno ugotovljenih prvih deset groženj in ustrezne trende, medtem ko raziskuje razvoj teh groženj v obsegu tekočega leta.

- Best Practices for Cyber Crisis Management: Ta študija poudarja zapletenost pojma kibernetske krize in stopnjo subjektivnosti, ki jo vključuje. Povzdigovanje obsežnega kibernetskega incidenta v kibernetsko krizo je odvisno predvsem od politične odločitve in je v veliki meri odvisno od stopnje tveganja, ki so ga države članice EU (MS) pripravljene tolerirati (t. i. „nagnjenost k tveganju").
- NIS Investments Report 2023: Namen tega poročila je oblikovalcem politik zagotoviti dokaze za oceno učinkovitosti obstoječega okvira kibernetske varnosti EU, zlasti s podatki o tem, kako so operaterji osnovnih storitev (OES) in ponudniki digitalnih storitev (DSP) opredeljeni v direktivi Evropske unije o varnosti omrežij ter informacij (Direktiva NIS) vlagajo svoje proračune za kibernetsko varnost in kako je Direktiva NIS vplivala na to naložbo. Ta četrta ponovitev poročila predstavlja podatke iz 1.080 OES/DSP iz vseh 27 držav članic EU.
- Foresight 2030 Threats: Ta publikacija povzema prihajajoče izzive in ponuja oceno tveganj. Ali smo pripravljeni oblikovati kibernetsko varno prihodnost, ki je pred nami?
- Good Practices for Supply Chain Cybersecurity: Poročilo ponuja pregled trenutnih praks kibernetske varnosti dobavne verige, ki jim sledijo bistveni in pomembni subjekti v EU, na podlagi rezultatov študije ENISA iz leta 2022, ki se je osredotočala na naložbe proračunov za kibernetsko varnost med organizacijami v EU.
- Multilayer Framework for Good Cybersecurity Practices for AI: V tem poročilu predstavljamo razširljiv okvir za usmerjanje nacionalnih organov za konkurenco in deležnikov umetne inteligence glede korakov, ki jih morajo upoštevati, da zavarujejo svoje sisteme, operacije ter procese umetne inteligence z uporabo obstoječega znanja in najboljših praks ter prepoznavanjem manjkajočih elementov. Ogrodje je sestavljeno iz treh plasti (temeljev kibernetske varnosti, kibernetske varnosti, specifične za umetno inteligenco, in sektorske specifične kibernetske varnosti za umetno inteligenco) in je namenjeno zagotavljanju postopnega pristopa k sledenju dobrim praksam kibernetske varnosti, da bi zgradili zaupanja vredne dejavnosti v zvezi z umetno inteligenco.
- Cybersecurity and privacy in AI - Forecasting demand on electricity grids: To poročilo omogoča boljšo oceno resničnosti, da umetna inteligenca prinaša svoj nabor groženj, kar posledično vztraja pri iskanju novih varnostnih ukrepov za boj proti njim. Na koncu je treba opozoriti, da ta priročnik močno poudarja vprašanja zasebnosti na enak način kot vprašanja kibernetske varnosti, pri čemer je zasebnost eden najpomembnejših izzivov, s katerimi se današnja družba sooča. Varnost in zasebnost sta tesno povezani, vendar sta obe enako pomembni, zato je treba za vsako uporabo vzpostaviti ravnotežje. Posledično, kot je razvidno iz tega poročila, lahko prizadevanja za optimizacijo varnosti in zasebnosti pogosto pridejo na račun delovanja sistema.
- Cybersecurity Support Action: Podporni ukrep ENISA za kibernetsko varnost zagotavlja naknadne in predhodne storitve ter pomoč subjektom iz direktive NIS 2 držav članic.
- Risk Management Standards: Namen tega dokumenta je zagotoviti skladen pregled objavljenih standardov, ki obravnavajo vidike obvladovanja tveganja, in nato opisati metodologije in orodja, ki jih je mogoče uporabiti za uskladitev s temi standardi ali njihovo izvajanje.
- Guidelines for Securing the Internet of Things: Ta študija ENISA opredeljuje smernice za zavarovanje dobavne verige za IoT. ENISA je s prispevki strokovnjakov za IoT ustvarila varnostne smernice za celotno življenjsko dobo: od zahtev in zasnove do dostave ter vzdrževanja za končno uporabo in

odlaganja. Študija je bila razvita za pomoč proizvajalcem interneta stvari, razvijalcem, integratorjem in vsem zainteresiranim stranem, ki so vključene v dobavno verigo interneta stvari, pri sprejemanju boljših varnostnih odločitev pri gradnji, uvajanju ali ocenjevanju tehnologij interneta stvari.

- Good Practices for Security of IoT - Secure Software Development Lifecycle: Ta študija ENISA uvaja dobre prakse za varnost interneta stvari, s posebnim poudarkom na smernicah za razvoj programske opreme za varne izdelke in storitve interneta stvari skozi njihovo življenjsko dobo. Vzpostavitev varnih razvojnih smernic v celotnem ekosistemu IoT je temeljni gradnik za varnost IoT. Z zagotavljanjem dobrih praks o tem, kako zavarovati proces razvoja programske opreme IoT, se ta študija ukvarja z enim vidikom za doseganje varnosti že po zasnovi, kar je ključno priporočilo, ki je bilo poudarjeno v študiji ENISA Baseline Security Recommendations, ki se je osredotočala na varnost ekosistema IoT s horizontalnega vidika.

Sektorsko usmerjene študije in dokumenti:

- Securing Smart Airports: Kot odgovor na nove nastajajoče grožnje, s katerimi se soočajo pametna letališča, to poročilo ponuja vodnik za letališke odločevalce (CISO, CIO, IT direktorje in vodje operacij) ter letališke strokovnjake za varnost informacij, pa tudi ustrezne nacionalne organe in agencije, ki so pristojni kibernetske varnosti za letališča. Na podlagi poglobljenega pregleda obstoječega znanja in potrditvenih intervjujev s strokovnjaki za zadevo to poročilo izpostavlja ključne prednosti pametnih letališč. Na podlagi tega je bila izvedena podrobna analiza in preslikava groženj s posebnim poudarkom na ranljivostih pametnih komponent.
- Port Cybersecurity - Good practices for cybersecurity in the maritime sector: To poročilo, ki je bilo razvito v sodelovanju z več pristanišči EU, namerava zagotoviti uporabno osnovo, na kateri lahko CIO in CISO subjektov, vključenih v pristaniški ekosistem, zlasti pristaniških organov ter upravljavcev terminalov, gradijo svojo strategijo kibernetske varnosti. Študija navaja glavne grožnje, ki predstavljajo tveganje za pristaniški ekosistem, in opisuje ključne scenarije kibernetskih napadov, ki bi lahko vplivali nanje. Ta pristop je omogočil identifikacijo varnostnih ukrepov, ki jih morajo vrata uvesti, da bi se bolje zaščitila pred kibernetskimi napadi. Glavni opredeljeni ukrepi naj bi služili kot dobre prakse za osebe, odgovorne za izvajanje kibernetske varnosti. Študija je lahko koristna za druge deležnike v širši skupnosti znotraj pristaniškega ekosistema, kot so ladjarske družbe in oblikovalci pomorske politike.
- Guidelines - Cyber Risk Management for Ports: Namen tega poročila je upravljavcem pristanišč zagotoviti dobre prakse za oceno kibernetskega tveganja, ki jih lahko prilagodijo katerikoli metodologiji ocenjevanja tveganja, ki ji sledijo. Da bi to dosegli, to poročilo uvaja štirifazni pristop k obvladovanju kibernetskega tveganja za pristaniške operaterje, ki sledi skupnim načelom obvladovanja tveganja in je preslikan v korake metodologije ocenjevanja tveganja, ki je določena v Kodeksu ISPS ter ustreznem EU zakonodajo za varnost pristanišč in pristaniških zmogljivosti. Za vsako od teh faz to poročilo zagotavlja uporabne smernice za pomoč upravljavcem pristanišč pri njihovih prizadevanjih, navaja pogoste izzive, povezane z izvajanjem ustreznih dejavnosti, dobre prakse, ki jih lahko posamezne organizacije takoj sprejmejo in prilagodijo, ter kartiranje navedenih dobrin prakse za vsako fazo z ustreznimi izzivi, ki jih obravnavajo.
- Telecom Security Incidents 2021: To poročilo zagotavlja anonimizirane in združene informacije o večjih telekomunikacijskih varnostnih incidentih v letu 2021. Letni povzetek za leto 2021 vsebuje poročila o 168 incidentih, ki so jih predložili nacionalni organi iz 26 držav članic EU (MS) in dveh držav EFTE.
- ENISA Transport Threat Landscape: To poročilo je prva analiza kibernetske grožnje

prometnega sektorja v EU, ki jo je izvedla Agencija Evropske unije za kibernetsko varnost (ENISA). Namen poročila je prinesti nove vpoglede v realnost prometnega sektorja s kartiranjem in preučevanjem kibernetskih incidentov od januarja 2021 do oktobra 2022. Opredeljuje glavne grožnje, akterje in trende na podlagi analize kibernetskih napadov, usmerjenih v letalski, pomorski, železniški in cestni promet v obdobju skoraj dveh let.

- Railway Cybersecurity - Good Practices in Cyber Risk Management: Namen tega poročila je referenčna točka za trenutne dobre prakse za pristope obvladovanja kibernetskega tveganja, ki se uporabljajo v železniškem sektorju. Ponuja vodnik za prevoznike v železniškem prometu in upravljavce infrastrukture za izbiro, kombiniranje ali prilagajanje metod obvladovanja kibernetskega tveganja potrebam njihove organizacije. Gradi na poročilu ENISA iz leta 2020 o kibernetski varnosti v železniškem sektorju (ENISA, 2020), ki je ocenilo raven izvajanja ukrepov kibernetske varnosti v železniškem sektorju. To poročilo vsebuje smernice, ki jih je mogoče uporabiti, navaja skupne izzive, povezane z izvajanjem ustreznih dejavnosti, in opisuje dobre prakse, ki jih lahko posamezne organizacije brez težav sprejmejo ter prilagodijo. Poleg tega je na voljo seznam koristnega referenčnega gradiva, skupaj s praktičnimi primeri in veljavnimi standardi.
- Health Threat Landscape: To je prva analiza kibernetske grožnje zdravstvenega sektorja v EU, ki jo je izvedla Agencija Evropske unije za kibernetsko varnost (ENISA). Namen poročila je prinesti nove vpoglede v realnost zdravstvenega sektorja s kartiranjem in preučevanjem kibernetskih incidentov od januarja 2021 do marca 2023. Opredeljuje glavne grožnje, akterje, vplive in trende na podlagi analize kibernetskih napadov na zdravstvene organizacije v dvoletnem obdobju.

V pričujočem poglavju smo podali nekaj izpostavljenih mednarodnih organizacij in virov, ki bodo lahko služili za razširitev potrebnega okvir znanja vsem strokovnjakom, ki se bodo v organizacijah ukvarjali z uvajanjem določil direktive NIS-2 ter Zakona o informacijski varnosti. Seveda se je potrebno zavedati, da je to samo del možnih referenčnih publikacij.

Viri:

- Evropska unija, Evropska agencija za kibernetsko varnost (ENISA): https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_sl?utm

Poglavje 9
Predstavitev mednarodnih standardov in drugih okvirjev za področje informacijske in kibernetske varnosti

POVZETEK

Mednarodni standardi predstavljajo ključni okvir za zagotavljanje informacijske in kibernetske varnosti. Najbolj uveljavljeni so standardi organizacije ISO, ki jih v Sloveniji podpira Slovenski inštitut za standardizacijo (SIST). Poleg ISO/IEC standardov, kot so 27001, 27002 in 22301, igrajo pomembno vlogo tudi drugi okviri, kot so NIST, DIN in panogi specifični standardi PCI DSS ter HIPAA. Ti standardi omogočajo sistematičen pristop k obvladovanju tveganj, zaščiti informacij in neprekinjenemu poslovanju. Praktična uporaba teh standardov ne le zagotavlja skladnost z zakonodajo, temveč tudi povečuje odpornost organizacij na kibernetske grožnje. Implementacija mora biti prilagodljiva in usmerjena v učinkovitost.

Ključne točke:

- Standard ISO/IEC 27001
- Standard ISO/IEC 27002
- Standard ISO 22301
- Standarda ISO 31000 in ISO 31010
- SIST – Slovenski inštitut za standardizacijo
- Standardi za neprekinjeno poslovanje
- Varnostna dokumentacija in upravljanje tveganj.

Treba se je zavedati, da je področje informacijske in kibernetske varnosti zelo močno podprto z dogovorjenimi ter splošno uporabljenimi standardi. V EU so najbolj razširjeni standardi Mednarodne standardizacije organizacije ISO (International Standardization Organization), katere polnopravni član je tudi Slovenski inštitut za standardizacijo (SIST). Omenjena ustanova je v Republiki Sloveniji tudi pooblaščena za zastopanje Slovenije pri mednarodnih organizacijah kot so ISO Mednarodna standardizacijska organizacija (International standardization organization), IEC Mednarodna elektrotehnična komisija (International Electrotechnical Commission), CEN Evropski komite za standardizacijo (European Committee for Standardization), CENELEC Evropski komite za elektrotehniško standardizacijo (European Committee for Electrotechnical Standardization) in ETSI (Evropski institut za standardizacijo telekomunikacij (European Telecommunications Standards Institute)). V mednarodnem okolju sicer poznamo tudi druge standardizacijske organe, ki so uveljavljeni tudi na področju informacijske in kibernetske varnosti, kot na primer NIST Nacionalni institut za standardizacijo in tehnologijo (National Institute of Standards and Technology) iz ZDA ali DIN Nemški institut za standardizacijo (Deutschen Institut für Normung). Nekatere panoge poznajo še standarde, specifične za to panogo, na primer PCI DSS (payment card industry data security standard) na področju kartičnega in plačilnega prometa ali HIPAA (health insurance portability and accountability act) na področju zdravstva.

Za podporo in razumevanje potrebnih ukrepov zavezancev po ZINFV, na podlagi Zakona o informacijski varnosti so pomembni predvsem naslednji standardi, na katerih tudi smiselno temeljijo zahtevani ukrepi v omenjenih zakonskih ter podzakonskih predpisih.

Ti pomembni standardi so naslednji:

- ISO/IEC 27001: Sistemi upravljanja informacijske varnosti (predvsem pomemben pri delu dokumentacije povezane z zagotavljanjem sistema upravljanja informacijske varnosti; v praksi se uporabljajo kratice SUVI, SUIV in ISMS);
- ISO/IEC 27002: Kodeks ravnanja za nadzor informacijske varnosti (predvsem pomemben pri delu dokumentacije povezane z zagotavljanjem SUVI);
- ISO 22301: standard za sisteme upravljanja neprekinjenega poslovanja (predvsem pomemben pri delu dokumentacije povezane z zagotavljanjem sistema upravljanja neprekinjenega poslovanja; v praksi se uporabljata kratici SUNP in BCMS);
- ISO 31000: Splošne smernice za obvladovanje tveganj (pomemben za oba dela SUVI in SUNP);
- ISO 31010: Tehnike ocenjevanja tveganj (pomemben za oba dela SUVI in SUNP).

ISO/IEC 27001 in **ISO/IEC 27002** sta mednarodno priznana standarda za upravljanje in zagotavljanje informacijske varnosti v organizacijah. Spodaj je podroben pregled teh standardov in njihove vloge pri zagotavljanju varnosti informacij z učinkovitimi nadzornimi in upravljalnimi sistemi.

ISO/IEC 27001: Sistemi upravljanja informacijske varnosti (SUVI)

ISO/IEC 27001 je standard, ki določa zahteve za vzpostavitev, izvajanje, vzdrževanje in stalno izboljševanje SUVI. Cilj SUVI je zaščititi zaupnost, celovitost in razpoložljivost informacij z uporabo procesa obvladovanja tveganj ter zagotavljanjem zaupanja zainteresiranim stranem, da so tveganja ustrezno obvladana.

Ključni elementi ISO/IEC 27001:

1. Kontekst organizacije:
   - razumevanje organizacije in njenega konteksta,
   - razumevanje potreb in pričakovanj zainteresiranih strani,
   - določitev obsega SUVI.

2. Vodenje:
   - vodstvo in zavezanost,
   - politika informacijske varnosti,
   - organizacijske vloge, odgovornosti in pooblastila.
3. Načrtovanje:
   - ukrepi za obvladovanje tveganj in priložnosti,
   - cilji informacijske varnosti in načrtovanje za njihovo dosego,
   - načrtovanje sprememb.
4. Podpora:
   - viri,
   - usposobljenost,
   - zavedanje,
   - komunikacija,
   - dokumentirane informacije.
5. Delovanje:
   - operativno načrtovanje in nadzor,
   - ocena in obravnava tveganj,
   - upravljanje sprememb.
6. Ocenjevanje uspešnosti:
   - spremljanje, merjenje, analiza in vrednotenje,
   - notranja revizija,
   - pregled vodstva.
7. Izboljšave:
   - neskladnosti in korektivni ukrepi,
   - stalno izboljševanje.

ISO/IEC 27002: Kodeks ravnanja za nadzor informacijske varnosti

ISO/IEC 27002 je dopolnilni standard k ISO/IEC 27001. Ponuja smernice za organizacijske standarde informacijske varnosti in prakse upravljanja informacijske varnosti, vključno z izbiro, uvedbo ter upravljanjem nadzorov, ob upoštevanju tveganj informacijske varnosti v okolju organizacije.

Ključni elementi ISO/IEC 27002:

1. Politike informacijske varnosti:
   - usmeritve za upravljanje informacijske varnosti.
2. Organizacija informacijske varnosti:
   - notranja organizacija,
   - mobilne naprave in delo na daljavo.
3. Varnost človeških virov:
   - pred zaposlitvijo,
   - med zaposlitvijo,
   - prenehanje in sprememba zaposlitve.
4. Upravljanje sredstev:
   - odgovornost za sredstva,
   - klasifikacija informacij,
   - ravnanje z mediji.
5. Nadzor dostopa:
   - poslovne zahteve za nadzor dostopa,
   - upravljanje uporabniškega dostopa,
   - odgovornosti uporabnikov,
   - nadzor dostopa do sistemov in aplikacij.
6. Kriptografija:
   - kriptografski nadzori.
7. Fizična in okoljska varnost:
   - varna območja,
   - varnost opreme.
8. Operativna varnost:
   - operativni postopki in odgovornosti,
   - zaščita pred zlonamerno programsko opremo,
   - varnostne kopije,
   - zapisovanje in spremljanje,
   - nadzor operativne programske opreme,
   - upravljanje tehničnih ranljivosti,
   - premisleki za revizijo informacijskih sistemov.
9. Varnost komunikacij:
   - upravljanje varnosti omrežja,
   - prenos informacij.

10. Pridobivanje, razvoj in vzdrževanje sistemov:
    - varnostne zahteve informacijskih sistemov,
    - varnost v procesih razvoja in podpore,
    - testni podatki.
11. Odnosi z dobavitelji:
    - informacijska varnost v odnosih z dobavitelji,
    - upravljanje storitev dobaviteljev.
12. Upravljanje incidentov informacijske varnosti:
    - upravljanje incidentov informacijske varnosti in izboljšave.
13. Vidiki informacijske varnosti pri obvladovanju poslovne kontinuitete:
    - kontinuiteta informacijske varnosti,
    - redundantnosti.
14. Skladnost:
    - skladnost z zakonskimi in pogodbenimi zahtevami,
    - pregledi informacijske varnosti.

Integracija ISO/IEC 27001 in ISO/IEC 27002

- ISO/IEC 27001 se osredotoča na del sistema upravljanja, ki podrobno opisuje, kako vzpostaviti SUVI, ki zagotavlja, da se varnostni ukrepi nenehno izboljšujejo in prilagajajo spreminjajočemu se okolju groženj.
- ISO/IEC 27002 zagotavlja specifične nadzore, ki jih lahko organizacije uvedejo za obvladovanje ugotovljenih tveganj, in ponuja podrobne smernice za izvajanje varnostnih ukrepov, ki podpirajo SUVI.

Praktična uporaba

Primer scenarija:

1. Izvajanje SUVI (ISO/IEC 27001):
    - Določite obseg SUVI glede na kontekst in zainteresirane strani.
    - Razvijte politiko informacijske varnosti.
    - Izvedite oceno tveganj za prepoznavanje groženj, ranljivosti in vplivov.
    - Izberite nadzore na podlagi ISO/IEC 27002 za obvladovanje ugotovljenih tveganj.
    - Uvedite nadzore in razvijte podporne postopke.
    - Spremljajte in pregledujte učinkovitost nadzorov.
    - Izvedite notranje revizije in preglede vodstva.
    - Nenehno izboljšujte SUVI na podlagi ugotovitev revizij in spreminjajočih se okolij tveganj.
2. Uporaba nadzorov (ISO/IEC 27002):
    - Nadzor dostopa: Uvedite politike za upravljanje uporabniškega dostopa, ki zagotavljajo, da imajo uporabniki ustrezne pravice dostopa.
    - Kriptografija: Uporabljajte šifriranje za zaščito občutljivih podatkov med prenosom in shranjevanjem.
    - Fizična varnost: Zagotovite varnost podatkovnih centrov z ustreznimi fizičnimi nadzori dostopa in okoljskimi zaščitami.
    - Upravljanje incidentov: Vzpostavite postopke za poročanje, odzivanje in odpravljanje incidentov.

Sledenje strukturiranemu pristopu, ki ga predpisujeta ISO/IEC 27001 in izvajanje podrobnih nadzorov iz ISO/IEC 27002, lahko organizacije, kot je Elektro Gorenjska, učinkovito upravljajo in izboljšajo svojo informacijsko varnost ter zagotovijo robustno zaščito pred spreminjajočimi se grožnjami.

ISO 22301: Sistem upravljanja neprekinjenega poslovanja

ISO 22301 je mednarodni standard za sisteme upravljanja neprekinjenega poslovanja (SUNP). Ta standard organizacijam pomaga pri načrtovanju, vzpostavitvi, izvajanju, vzdrževanju in nenehnem izboljševanju sistema, ki ščiti pred, zmanjšuje verjetnost nastanka, pripravlja na, se odziva na in okreva po motnjah, ko se zgodijo.

Ključni elementi ISO 22301:

1. Kontekst organizacije:
   - Razumevanje organizacije in njenega konteksta: Identificiranje notranjih in zunanjih vprašanj, ki lahko vplivajo na sposobnost organizacije za doseganje ciljev SUNP.
   - Razumevanje potreb in pričakovanj zainteresiranih strani: Identificiranje ključnih zainteresiranih strani in njihovih zahtev v zvezi z zagotavljanjem neprekinjenega poslovanja.
   - Določitev obsega SUNP: Določitev meja in uporabnosti sistema upravljanja neprekinjenega poslovanja v organizaciji.
2. Vodenje:
   - Vodstvo in zavezanost: Najvišje vodstvo mora izkazati vodstvo in zavezanost glede SUNP.
   - Politika neprekinjenega poslovanja: Razvijanje in implementacija politike neprekinjenega poslovanja.
   - Organizacijske vloge, odgovornosti in pooblastila: Določitev odgovornosti in pooblastil za vodenje ter izvajanje SUNP.
3. Načrtovanje:
   - Ukrepi za obvladovanje tveganj in priložnosti: Identificiranje in obravnavanje tveganj ter priložnosti, ki lahko vplivajo na doseganje ciljev SUNP.
   - Cilji neprekinjenega poslovanja in načrtovanje za njihovo dosego: Določanje ciljev za doseganje želenih rezultatov neprekinjenosti poslovanja in načrtovanje potrebnih ukrepov.
   - Načrtovanje sprememb: Upravljanje sprememb, ki vplivajo na SUNP.
4. Podpora:
   - Viri: Zagotavljanje potrebnih virov za vzpostavitev, izvajanje, vzdrževanje in izboljševanje SUNP.
   - Kompetentnost: Zagotavljanje usposobljenosti osebja, ki deluje v okviru SUNP.
   - Zavedanje: Povečanje zavedanja o politikah neprekinjenega poslovanja in posameznih odgovornostih.
   - Komunikacija: Vzpostavitev procesov za notranjo in zunanjo komunikacijo v zvezi z SUNP.
   - Dokumentirane informacije: Vzpostavitev in vzdrževanje dokumentiranih informacij, ki so potrebne za SUNP.
5. Delovanje:
   - Operativno načrtovanje in nadzor: Vzpostavitev in izvajanje operativnih kontrol za doseganje ciljev neprekinjenega poslovanja.
   - Analiza vpliva na poslovanje (BIA) in ocena tveganj: Izvedba BIA in ocena tveganj za prepoznavanje ter določanje prednostnih področij za zagotavljanje neprekinjenega poslovanja.
   - Strategije in rešitve za neprekinjeno poslovanje: Razvijanje strategij in rešitev za obvladovanje ugotovljenih tveganj.
   - Načrti neprekinjenega poslovanja: Priprava in vzdrževanje načrtov za obvladovanje motenj.
   - Programi ozaveščanja in usposabljanja: Izvajanje programov za ozaveščanje in usposabljanje zaposlenih o SUNP.
   - Vaje in testiranje: Redno izvajanje vaj in testiranje načrtov za neprekinjeno poslovanje.
6. Ocenjevanje uspešnosti:
   - Spremljanje, merjenje, analiza in vrednotenje: Spremljanje in merjenje učinkovitosti SUNP, analiza rezultatov ter vrednotenje doseganja ciljev.
   - Notranja revizija: Izvajanje rednih notranjih revizij za preverjanje skladnosti in učinkovitosti SUNP.

- Pregled vodstva: Redni pregledi s strani vodstva za oceno uspešnosti SUNP in določitev priložnosti za izboljšave.

7. Izboljšave:

   - Neskladnosti in korektivni ukrepi: Obvladovanje neskladnosti in izvajanje korektivnih ukrepov.

   - Nenehno izboljševanje: Iskanje priložnosti za stalno izboljševanje SUNP.

Integracija ISO 22301 z drugimi standardi, kot sta ISO/IEC 27001 in ISO/IEC 27002

Integracija ISO 22301 z drugimi varnostnimi standardi, kot sta ISO/IEC 27001 (informacijska varnost) in ISO/IEC 27002 (kontrole informacijske varnosti), lahko prinese večje koristi za celovito upravljanje varnosti in kontinuitete v organizaciji. Integracija teh standardov lahko vključi naslednje korake:

1. Harmonizacija politik in ciljev:

   - Usmerjanje politik informacijske varnosti in neprekinjenega poslovanja k skupnim ciljem ter strategijam.

2. Skupni procesi ocenjevanja tveganj:

   - Uporaba enotnega pristopa k ocenjevanju tveganj, ki pokriva tako informacijsko varnost kot neprekinjeno poslovanje.

3. Konsolidacija dokumentacije:

   - Združitev dokumentacije, kjer je to mogoče, da se prepreči podvajanje in poveča učinkovitost upravljanja.

4. Usklajevanje vlog in odgovornosti:

   - Določitev jasnih vlog in odgovornosti, ki podpirajo tako informacijsko varnost kot neprekinjeno poslovanje.

5. Skupne vaje in testiranje:

   - Izvajanje združenih vaj in testiranj za preverjanje učinkovitosti načrtov za informacijsko varnost ter zagotavljanje neprekinjenega poslovanja.

Vzpostavitev sistema upravljanja sistema neprekinjenega poslovanja v skladu z ISO 22301, skupaj z integracijo drugih standardov za informacijsko varnost, lahko organizacijam, ki so določeni kot zavezanci, pomaga pri zagotavljanju celovite zaščite pred motnjami in varnosti informacij. To bo omogočilo učinkovito obvladovanje tveganj, povečalo odpornost na incidente in zagotovilo hitro ter učinkovito okrevanje po motnjah.

Implementacija ISO 31000 in ISO 31010

ISO 31000 in ISO 31010 sta ključna standarda za obvladovanje tveganj, kjer ISO 31000 ponuja splošne smernice za obvladovanje tveganj, ISO 31010 pa podrobneje opisuje tehnike ocenjevanja tveganj. Njuna integracija v poslovne procese organizacije, kot so zavezanci lahko bistveno izboljša sposobnost za identifikacijo, oceno in obvladovanje tveganj.

Koraki za implementacijo ISO 31000 in ISO 31010

1. Vzpostavitev konteksta organizacije:

   - Razumevanje notranjega in zunanjega okolja: Analiza notranjih dejavnikov (npr. kultura, struktura, procesi) in zunanjih dejavnikov (npr. regulative, tržni pogoji).

   - Opredelitev obsega obvladovanja tveganj: Določitev področja uporabe sistema upravljanja tveganj (RMS).

2. Vodenje in zavezanost:

   - Zavezanost vodstva: Zagotovitev podpore najvišjega vodstva in določitev jasnih odgovornosti ter pooblastil za obvladovanje tveganj.

   - Razvoj politike obvladovanja tveganj: Določitev smernic in ciljev za obvladovanje tveganj.

3. Načrtovanje:

   - Ukrepi za obvladovanje tveganj: Identifikacija tveganj in priložnosti, razvoj načrtov za zmanjšanje tveganj.

- Določitev kriterijev za tveganja: Določitev meril za ocenjevanje tveganj glede na verjetnost in vpliv.

4. Implementacija in delovanje:
   - Vzpostavitev strukture za obvladovanje tveganj: Vključevanje obvladovanja tveganj v obstoječe procese in sisteme.
   - Izvajanje procesov za obvladovanje tveganj: Uporaba ISO 31010 tehnik za identifikacijo, analizo in vrednotenje tveganj.
5. Spremljanje in pregled:
   - Spremljanje učinkovitosti: Redno spremljanje in pregledovanje RMS za zagotavljanje učinkovitosti ter skladnosti.
   - Notranje revizije: Redne revizije za preverjanje skladnosti z ISO 31000 in ISO 31010 standardi.
6. Nenehno izboljševanje:
   - Identifikacija priložnosti za izboljšave: Stalno iskanje načinov za izboljšanje RMS.
   - Izvajanje izboljšav: Implementacija sprememb na podlagi rezultatov spremljanja in pregledov.

Podrobnosti o tehnikah ocenjevanja tveganj po ISO 31010

Identifikacija tveganj:

- Brainstorming: Skupinsko ustvarjanje idej za identifikacijo možnih tveganj.
- SWOT analiza: Analiza močnih in šibkih točk ter priložnosti in groženj.
- Kontrolni seznami: Uporaba seznamov za sistematično preverjanje morebitnih tveganj.

Analiza tveganj:

- Kvalitativna analiza: Ocena tveganj glede na verjetnost in vpliv z uporabo lestvic.
- Kvantitativna analiza: Kvantificiranje tveganj z uporabo matematičnih modelov (npr. Monte Carlo simulacije).

Vrednotenje tveganj:

- Primerjava z merili za tveganje: Primerjava ugotovljenih tveganj s kriteriji, določenimi v začetni fazi.
- Razvrstitev tveganj: Razvrstitev tveganj po prioriteti glede na njihovo pomembnost za organizacijo.

Obvladovanje tveganj:

- Izogibanje tveganjem: Izogibanje dejavnostim, ki povzročajo tveganje.
- Zmanjšanje tveganj: Uvedba ukrepov za zmanjšanje verjetnosti ali vpliva tveganja.
- Prenos tveganj: Prenos tveganja na tretjo osebo (npr. zavarovanje).
- Sprejemanje tveganj: Sprejemanje tveganja, ko je verjetnost in vpliv v mejah sprejemljivega.

Primer integracije v posamezno organizacijo

- Vzpostavitev politike obvladovanja tveganj: Razvoj in odobritev politike, ki jo podpira najvišje vodstvo.
- Analiza tveganj v IT in OT okolju: Izvedba SWOT analize za identifikacijo tveganj povezanih z IT in OT sistemi.
- Vzpostavitev kontrolnih mehanizmov: Uvedba kontrolnih seznamov in redno izvajanje notranjih revizij.
- Izvedba scenarijskih analiz: Priprava scenarijev za simulacijo možnih incidentov in oceno njihovega vpliva.
- Nenehno spremljanje in izboljševanje: Redno spremljanje učinkovitosti uvedenih ukrepov in prilagajanje strategij obvladovanja tveganj.

Implementacija ISO 31000 in ISO 31010 v posamezni organizaciji bo zagotovila celovit in strukturiran pristop k obvladovanju tveganj. To bo organizaciji omogočilo učinkovito prepoznavanje, ocenjevanje in obvladovanje tveganj, s čimer se bo povečala odpornost na potencialne grožnje ter izboljšala stabilnost in uspešnost poslovanja.

Napotila za prakso

- Uvajanje standardov v redno poslovanje je vsekakor priporočljiv korak, ki bo vsem organizacijam, ki so ali bodo v prihodnje sodile v okvir zavezancev za izvajanje bistvenih storitev, močno olajšal uvajanje zakonskih zahtev na področju Zakona o informacijski varnosti.
- Varnostne standarde uvajajte v svoje organizacijske procese zaradi izboljšanja ravni varnosti in ne zato, da dobite ustrezno potrdilo o skladnosti s standardom.
- Pri uvajanju bodite pragmatični in uporabljate zdrav razum v smeri zagotavljanja učinkovitosti predvidenih standardizacijskih ukrepov.
- Pri uvajanju ne komplicirajte z uvajanjem standardov iz različnih standardizacijskih okolij, temveč se odločite za en okvir in tega uveljavite v celoti.
- Standarde lahko pridobite preko SIST.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO 31000:2018: Risk management — Guidelines
- ISO 31010:2019 : Risk management — Risk assessment techniques
- ISO 28000:2022: Security and resilience — Security management systems — Requirements
- ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements
- ISO 9001:2015: Quality management systems — Requirements

Sekcija 3
Napotki za sistemski pristop pri vzpostavitvi učinkovitega sistema informacijske varnosti

Poglavje 10
Napotki za pripravo dokumentacije skladne z zakonom: priprava krovne varnostne politike

POVZETEK

Priprava krovne varnostne politike je ključnega pomena za organizacije, ki želijo izpolnjevati zakonske zahteve s področja informacijske varnosti in zagotavljati skladnost z Zakonom o informacijski varnosti ter evropskimi smernicami, kot je NIS-2. Takšna politika določa splošna načela, cilje in postopke za zaščito informacij ter upravljanje tveganj. Poleg vzpostavitve sistemov SUVI in SUNP je treba izvesti analizo tveganj, pripraviti načrte za odzivanje na incidente in obnovitev sistemov ter oblikovati varnostne ukrepe. V pomoč organizacijam pri oceni ravni kibernetske varnosti je na voljo samo ocenitveno orodje, ki pokriva 19 ključnih tematskih področij. Dokumentacija mora biti celovita, strukturirana in prilagojena specifikam organizacije.

Ključne točke:

- Krovna varnostna politika
- Sistem upravljanja varnosti informacij (SUVI) in Sistem upravljanja neprekinjenega poslovanja (SUNP)
- Analiza tveganj
- Načrt neprekinjenega poslovanja
- Načrt obnovitve sistemov
- Načrt odzivanja na incidente
- Samoocenitveno orodje
- Varnostni ukrepi
- Skladnost z NIS-2
- Organizacijska odgovornost.

Namen krovne varnostne politike je, da se določi splošne smernice, načela in zahteve za varovanje informacij ter informacijskih sistemov v organizaciji. Cilj krovne varnostne politike je zagotoviti celovit, strukturiran in jasen okvir za upravljanje vseh vidikov varnosti ter upravljanja tveganj z vidika vseh nevarnosti, ki pretijo informacijskim in omrežnim sistemom.

V skladu z zakonskimi zahtevami in pričakovanimi standardi zagotavljanja informacijske varnosti morajo izvajalci zavezanci za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov vzpostaviti ter vzdrževati dokumentiran sistem upravljanja varovanja informacij (SUVI)[4] in sistem upravljanja neprekinjenega poslovanja (SUNP)[5], ki mora obsegati najmanj:

1. analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj;
2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja;
3. seznam njegovih ključnih, krmilnih in nadzornih informacijskih sistemov ter delov omrežja in pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev;
4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje;
5. načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT;
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja ter informacijskih sistemov, ki upoštevajo področne posebnosti.

Za ustrezno začetno oceno nivoja urejenosti procesov informacijske varnosti v vaših organizacijah pa je URSIV pripravil poseben samoocenitveni vprašalnik, ki vam pomaga izvesti začetno oceno kibernetske varnosti. To je lahko ustrezna in učinkovita podlaga za nadaljevanje potrebnih ukrepov dograditve sistema upravljanja varnosti informacij ter sistema upravljanja neprekinjenega poslovanja.

Omenjeni vprašalnik temelji na orodju, ki obsega 238 kontrolnih točk razdeljenih v 19 tematskih sklopov.

Ti sklopi so:

[4] **Sistem za upravljanje varovanja informacij (SUVI)** je proces, s katerim rešujemo vse izzive varovanja informacij in predstavlja temelj za zmanjševanje informacijskih tveganj. Varovanje informacij in podatkov predstavlja nabor tehničnih ter organizacijskih ukrepov, katerih cilj je varovanje in zagotavljanje celovitosti, razpoložljivosti, uporabnosti, dostopnosti ter zaupnosti informacij in podatkov, ki jih obdeluje ter pripravlja organizacija in zagotavljanje njegovega neprekinjenega delovanja. Upravljanje informacijske varnosti mora biti vedno usklajeno z drugimi organizacijskimi procesi.

[5] **Sistem upravljanja neprekinjenega poslovanja (SUNP)** je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organizacije, da pripravi načrt za primere prekinitev in motenj pri poslovanju ter se nanje odzove z namenom zagotovitve storitev na sprejemljivi, vnaprej določeni ravni, in vključuje pripravo in uporabo načrtov obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov.

1) Upravljanje kibernetske varnosti in obvladovanje tveganj	11) Delo na daljavo
2) Popis strojne in programske opreme	12) Uporaba kriptografije
3) Varna konfiguracija naprav in aplikacij	13) Usposabljanje in ozaveščanje
4) Nadzor nad aplikacijami in storitvami	14) Obvladovanje tveganj dobavne verige
5) Upravljanje računov in nadzor dostopov	15) Tehnična ocena kibernetske varnosti
6) Preverjanje pristnosti uporabnika	16) Fizična varnost
7) Varnost omrežja	17) Varnostno kopiranje podatkov
8) Zaščita pred zlonamerno programsko opremo	18) Ravnanje z incidenti
9) Vzdrževanje in analiza dnevnikov dogodkov	19) Neprekinjeno poslovanje in okrevanje po nesrečah
10) Varnost spletnih aplikacij	

Shema 6: Vsebinski sklopi samo-ocenitev začetnega stanja kibernetskega stanja v organizaciji (Vir: URSIV)

Orodje je namenjeno predvsem izvajalcem bistvenih storitev, organom državne uprave in povezanim subjektom, ki so zavezanci po Zakonu o informacijski varnosti, zato se priporoča uporaba orodja v povezavi s postopkom ocene tveganj v organizaciji in pri prepoznavanju tehničnih, organizacijskih ter upravljavskih šibkih točk (slabosti), ki lahko vplivale na izpostavljenost organizacije večjim tveganjem.

Glavni cilji uporabe omenjenega orodja so:

- Praktični pristop merljivemu ocenjevanju ravni kibernetske varnosti organizacije na podlagi ocene specifičnih področij.
- Pomoč organizacijam pri ugotavljanju slabosti, ki bi lahko povečale izpostavljenost grožnjam, obenem pa jim orodje omogoča možnost izbora ustreznih tehničnih in organizacijskih ukrepov, ki lahko zmanjšajo tveganja.
- Služi kot osnovno orodje za odločanje na podlagi dokazov v zvezi s kibernetsko varnostjo.
- Poenostavljen pristop k splošni skladnosti z regulativnimi ali drugimi zahtevami.

Za pregled priprave ustrezne varnostne dokumentacije vam v nadaljevanju ponujamo »kontrolni seznam«, ki vam bo v veliko pomoč pri celoviti pripravi potrebne varnostne dokumentacije, da boste skladni z zahtevami Zakona o informacijski varnosti, posledično pa tudi z evropsko direktivo NIS-2.

Člen[6]	Namen
3	**Vsebina in struktura varnostne dokumentacije**
3.1	Vzpostavljen in vzdrževan SUVI
3.2	Vzpostavljen in vzdrževan SUNP
3.3	SUVI in SUNP podpisana s strani zakonitega zastopnika IBS
4	**Analiza obvladovanja tveganj**
4.1	Navedba uporabljene metodologije za izvedbo analize, biti mora primerljiva, verodostojna in ponovljiva v skladu s pravili stroke
4.2	Navedba sredstev znotraj SUVI in upravljavcev/odgovornih za sredstva
4.3	Navedba možnih groženj tem sredstvom
4.4	Navedba ranljivosti sredstev, ki bi jih grožnje lahko prizadele
4.5	Navedba vpliva uresničitve groženj na zaupnost, celovitost in razpoložljivost sredstev
4.6	Ocena vpliva na opravljanje bistvenih storitev v primeru kršitve informacijske varnosti zaradi izgube zaupnosti, celovitosti, razpoložljivosti in avtentičnosti
4.7	Ocena verjetnosti, da nastane kršitev informacijske varnosti
4.8	Ovrednotenje ravni tveganj
4.9	Določitev in obrazložitev sprejemljive ravni tveganj
4.10	Navedba ukrepov za odpravo ali zmanjšanje tveganj na sprejemljiv nivo
5	**Politika neprekinjenega poslovanja**
5.1	Navedba ciljev in načel za zagotavljanje neprekinjenega poslovanja (neprekinjenega izvajanja bistvenih storitev)
5.2	Navedba postopkov neprekinjenega poslovanja, ki se izdelajo na podlagi popisa poslovnih procesov
5.2	Popis poslovnih procesov
5.3	Ocena vpliva na poslovanje, zajema navedbo možnih dogodkov (odpovedi informacijskih sistemov, pomanjkanje zaposlenih, izpad posamezne lokacije znotraj organizacij, odpovedi storitev pogodbenih izvajalcev)
5.4	Določitev minimalne ravni poslovanja
5.5.	Navedba ukrepov za zagotavljanje neprekinjenega poslovanja, ki se izdelajo na podlagi ocene vpliva na poslovanje in minimalne ravni poslovanja
5.6	Določitev vlog in odgovornosti za izvajanje politike neprekinjenega poslovanja ter njeno posodabljanje
6	**Seznam ključnih, krmilnih in nadzornih informacijskih sistemov**
6.1	Navedba sredstev znotraj SUVI, od katerih je odvisno zagotavljanje bistvenih storitev
6.2	Opredelitev ključnih, krmilnih in nadzornih informacijskih ter omrežnih sistemov in določitev njihovih upravljavcev
7	**Načrt obnovitve delovanja informacijskih in omrežnih sistemov**
7.1	Opis postopkov za obnovitev delovanja informacijskih sistemov iz člena 6
7.2	Opis odgovornosti za postopke obnovitve
8	**Načrt odzivanja na incidente informacijske varnosti**

[6] Člen se nanaša in povezuje z Uredbo o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave

8.1	Opis orodij in infrastrukture za zaznavanje ter odziv na incidente
8.2	Opis sistema za zbiranje in zavarovanje dokazov o incidentu, vključno z dnevniškimi zapisi ter revizijskimi sledmi (če te obstajajo)
8.3	Opis politik in postopkov za odziv na incidente, obravnavo in analizo incidentov, vključno z evidentiranjem odzivnih aktivnosti
8.4	Opis odgovornosti oseb/organizacijskih enot, ki se bodo vključile v aktivnosti odzivov/obravnave/analize incidentov
8.5	Opis postopkov in odgovornosti za poročanje o incidentih znotraj ter zunaj organizacije
8.6	Opis protokola obveščanja nacionalnega CSIRT o incidentu (zajema najmanj oceno števila prizadetih uporabnikov bistvene storitve, oceno trajanja incidenta, navedbo kazalnikov zlorabe, če ti obstajajo, oceno geografske razširjenosti območja vpliva incidenta, oceno morebitnega čezmejnega vpliva incidenta, oceno morebitnega medpodročnega vpliva incidenta, opis pomembnosti vpliva incidenta na neprekinjeno izvajanje bistvenih storitev)
9	**Načrt varnostnih ukrepov**
9.1	Navedba ukrepov, ki so učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje
9.2	Navedba ukrepov, ki so prilagojeni tako, da se organizacija usmeri v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost in se izogibajo podvajanjem
9.3	Navedba ukrepov, ki so skladni tako, da se prednostno obravnavajo osnovne in skupne varnostne ranljivosti organizacije kljub področnim posebnostim
9.4	Navedba ukrepov, ki so sorazmerni s tveganji tako, da se izogibajo čezmerni obremenitvi posamezne organizacije
9.5	Navedba ukrepov, ki so konkretni tako, da organizacija te ukrepe izvaja, in da ukrepi prispevajo k informacijski varnosti
9.6	Navedba ukrepov, ki so preverljivi tako, da se na zahtevo pristojnega organa lahko predložijo dokazila o njihovi izvedbi
9.7	Navedba ukrepov, ki so vključujoči tako, da so upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo informacijskih sistemov
10.1	**Metodologija za pripravo analize obvladovanja tveganj**
10.1.1	Organizacija navede metodologijo z opredelitvijo lestvic in atributov ocenjevanja, po kateri bo izvedla analizo obvladovanja tveganj
10.1.2	Izvede popis sredstev znotraj SUVI in določi njihove upravljavce/odgovorne osebe za ta sredstva
10.1.3	Prepozna možne grožnje za izgubo zaupnosti, celovitosti in razpoložljivosti sredstev
10.1.4	Prepozna ranljivost sredstev, ki bi jih grožnje lahko prizadele
10.1.5	Oceni stopnjo vpliva uresničitve groženj na zaupnost, celovitost in razpoložljivost sredstev zaradi ranljivosti
10.1.6	Oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi
10.1.7	Ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev
10.1.8	Določi oceno sprejemljive ravni tveganja glede na vrednotenje ugotovljenih tveganj
10.2	**Metodologija za določitev ključnih, krmilnih in nadzornih informacijskih sistemov**
10.2.1	Na podlagi popisanih sredstev znotraj SUVI organizacija presodi, ali je zagotavljanje bistvenih storitev odvisno od posameznega sredstva znotraj SUVI

10.2.2	Za sredstva, od katerih je odvisno zagotavljanje bistvenih storitev, organizacija presodi, katero od teh sredstev je bistveno za delovanje glavne storitve
10.3	Analiza obvladovanja tveganj in določitev ključnih, krmilnih ter nadzornih informacijskih sistemov mora temeljiti na postopkih, ki so dosledni, primerljivi in verodostojni
10.4	Analiza obvladovanja tveganj in določanje ključnih, krmilnih in nadzornih informacijskih sistemov IBS izvaja v rednih časovnih presledkih, ali kadar so predlagane, ali nastanejo bistvene spremembe v okviru SUVI
11	**Minimalni obseg in vsebina varnostnih ukrepov**
11.1	Zagotavlja podporo vodstva organizacije pri zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja organizacije
11.2	Zagotavlja integriteto kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve
11.3	Zagotavlja notranji pregled SUVI in SUNP najmanj enkrat letno ter kadar so predlagane ali nastanejo bistvene spremembe
11.4	Zagotavlja upravljanje ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov z določitvijo odgovornosti za njihovo zaščito
11.5	Zagotavlja ohranjanje dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja
11.6	Zagotavlja upravljanje prometa in komunikacij
11.7	Zagotavlja opredelitev varnostnih zahtev za ključne dobavitelje organizacije
11.8	Zagotavlja fizično in tehnično varovanje dostopov do prostorov, kjer so ključni, krmilni ter nadzorni informacijski sistemi organizacije
11.9	Zagotavlja varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti IBS
11.10	Zagotavlja preverjanje identitete uporabnikov
11.11	Zagotavlja upravljanje in preprečevanje izrabe tehničnih ranljivosti
11.12	Zagotavlja raven dostopnosti informacij in upravlja pooblastila za dostop
11.13	Zagotavlja zaščito pred zlonamerno programsko kodo
11.14	Zagotavlja evidentiranje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev
11.15	Zagotavlja zaznavanje poskusov vdorov in preprečevanje incidentov

Shema 7: Vsebinski pregled zakonsko predvidene dokumentacije (vir: ICS)

Posebno pozornost je treba pri pripravi dokumentov nameniti razumevanju dveh sistemov SUVI in SUNP, ki sta med seboj sicer ločena, tudi skozi različne standarde, ki podpirajo vzpostavitev obeh procesov, vendar sta na drugi strani komplementarna ter močno prepletena. To razumevanje je ključno, da bo priprava ustrezne varnostne dokumentacije učinkovita, celovita, in da bo zajela vse vidike, ki so pomembni za učinkovito ter varno delovanje informacijskih sistemov v organizacijah in zagotavljanje neprekinjena delovanja tistih delov, ki so opredeljeni kot ključni za zagotavljanje izvajanja bistvenih ali pomembnih storitev.

V nadaljevanju vam posredujemo še koračni prikaz izdelave potrebne dokumentacije za uskladitev z zahtevami Zakona o informacijski varnosti.

Krovna varnostna politika

Krovna varnostna politika je temeljni dokument, ki opredeljuje načela, cilje, odgovornosti in postopke za zagotavljanje informacijske varnosti v organizaciji. Njen namen je zagotoviti skladnost z zakonodajo, vključno z Zakonom o informacijski varnosti, in določiti okvir za izvajanje varnostnih ukrepov in postopkov.

Priprava Krovne varnostne politike bi morala v grobem vsebovati naslednja temeljna področja:

1. Splošna varnostna politika

Namen in obseg: Določite namen in obseg varnostne politike, vključno z njeno uporabo za vse zaposlene, izvajalce ter partnerje.

Varnostni cilji: Opredelite glavne varnostne cilje, kot so ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij.

Odgovornosti: Dodelite odgovornosti za upravljanje informacijske varnosti na vseh ravneh znotraj organizacije.

Skladnost: Zagotovite skladnost z ustreznimi zakoni, predpisi in standardi (npr. ISO 27001).

2. Politika varnosti podatkov

Razvrščanje podatkov: Ustanovite shemo za razvrščanje podatkov glede na občutljivost in pomembnost.

Ravnanje s podatki: Določite postopke za varno ravnanje, shranjevanje, prenos in uničenje podatkov.

Šifriranje: Naročite uporabo šifriranja za občutljive podatke tako v mirovanju kot med prenosom.

Nadzor dostopa: Uvedite nadzor dostopa za omejevanje dostopa do podatkov na podlagi načela najmanjših privilegijev.

3. Politika nadzora dostopa

Avtentikacija uporabnikov: Določite zahteve za mehanizme avtentikacije uporabnikov, kot so gesla, večfaktorska avtentikacija in biometrične kontrole.

Avtorizacija: Opredelite postopke za dodeljevanje, spreminjanje in preklic dostopnih pravic do sistemov ter podatkov.

Upravljanje računov: Uvedite postopke za upravljanje uporabniških računov, vključno z rednimi pregledi dostopnih pravic in pravočasno odstranitvijo dostopa za odpuščene zaposlene.

4. Politika omrežne varnosti

Segmentacija omrežja: Opredelite omrežno arhitekturo, vključno s segmentacijo omrežij za omejevanje širjenja morebitnih varnostnih incidentov.

Požarni zidovi in zaznavanje vdorov: Opisujte uporabo požarnih zidov, sistemov za zaznavanje vdorov (IDS) in sistemov za preprečevanje vdorov (IPS) za zaščito omrežja.

Poskrbite za varnost na omrežnem nivoju z onemogočanjem neuporabljenih vrat na omrežnih napravah in servisih, ki jih ne uporabljate. Naprave redno posodabljajte, saj s tem odpravite morebitne ranljivosti. Poskrbite za varnostne kopije konfiguracij omrežnih naprav, da boste lahko v primeru odpovedi naprave hitro zagotovili ponovno delovanje nove naprave. Zagotavljajte redundanco omrežja, če je to nuj-

no za izvedbo vaših kritičnih procesov. Dokumentirajte spremembe konfiguracij in vzpostavite sistem upravljanja procesa sprememb. Če je mogoče, spremembe konfiguracij predhodno testirajte v ne-produkcijskem okolju.

Oddaljen dostop: Vzpostavite smernice za varen oddaljen dostop do omrežja, vključno z uporabo virtualnih zasebnih omrežij (VPN).

Spremljanje in beleženje: Uvedite stalno spremljanje in beleženje omrežnih dejavnosti za zaznavanje ter odzivanje na varnostne incidente.

5. Politika zaščite končnih točk

Protivirusna in programska oprema za odkrivanje škodljivih kod: Zahtevajte namestitev in redno posodabljanje protivirusne ter programske opreme za odkrivanje škodljivih kod na vseh končnih točkah.

Upravljanje popravkov: Določite postopke za pravočasno uporabo varnostnih popravkov in posodobitev na končnih napravah.

Šifriranje naprav: Naročite uporabo šifriranja na vseh mobilnih in prenosnih napravah.

Politike uporabe: Ustanovite smernice za sprejemljivo uporabo končnih naprav, vključno s prepovedjo nepooblaščenih namestitev programske opreme.

6. Politika obnovitve po nesrečah in zagotavljanje neprekinjenosti poslovanja

Ocena tveganj: Redno izvajajte ocene tveganj za prepoznavanje morebitnih groženj poslovanju.

Načrtovanje obnovitve: Razvijajte in vzdržujte načrt za obnovitev po nesrečah ter načrt za neprekinjeno poslovanje, ki opredeljujeta postopke za odzivanje na motnje in okrevanje po njih.

Postopki varnostnega kopiranja: Določite postopke za varnostno kopiranje ključnih podatkov in sistemov, vključno s frekvenco ter mesti shranjevanja varnostnih kopij.

Testiranje in vaje: Redno preizkušajte in posodabljajte načrte za obnovitev po nesrečah ter neprenehno poslovanje prek vaj in simulacij. Redno preverjajte, ali je iz varnostnih kopij mogoče uspešno izvesti obnovitev.

7. Politika varstva osebnih podatkov

Načela varstva podatkov: Upoštevajte načela varstva podatkov, kot so zakonitost obdelave, načelo najmanjše obdelave podatkov, omejitev namena in transparentnost. Prva tri načela zagotavljajo, da se obdelujejo le tisti osebni podatki, s katerimi je mogoče doseči namen obdelave. Evidenca dejavnosti obdelav in vzpostavitev postopkov za uveljavljanje pravic posameznikov pa zagotavljata transparentnost obdelave osebnih podatkov.

Dobra praksa je, da imenujete pooblaščeno osebo za varstvo podatkov, tudi če vas zakon o varstvu osebnih podatkov in GDPR ne zavezujeta k imenovanju. Če pri obdelavi osebnih podatkov obstaja tveganje za kršitev pravic v zvezi z osebnimi podatki, izvedite oceno učinka in se posvetujte s pooblaščeno osebo za varstvo podatkov.

Pravice posameznikov: Uvedite postopke za omogočanje uresničevanja pravic posameznikov, vključno z dostopom, popravkom, omejitvijo obdelave in izbrisom podatkov.

Obveščanje o kršitvah: Vzpostavite protokol za pravočasno obveščanje o kršitvah varstva podatkov prizadetim posameznikom in regulatornim organom.

Zunanji izvajalci: Zagotovite, da zunanji obdelovalci podatkov izpolnjujejo zahteve varstva podatkov preko pogodbenih dogovorov in rednih revizij.

8. Politika varnostnega izobraževanja in ozaveščanja

Programi usposabljanja: Razvijajte in izvajajte redne programe usposabljanja za vse zaposlene, vključno z ozaveščanjem o pogostih grožnjah ter varnih praksah.

Ozaveščevalne kampanje: Izvajajte stalne kampanje za ozaveščanje o pomenu informacijske varnosti.

Simulacije spletnega ribarjenja: Izvajajte simulacijske vaje za prepoznavanje in odzivanje na poskuse spletnega ribarjenja.

Poročanje o incidentih: Spodbujajte kulturo varnosti s promoviranjem poročanja o sumljivih dejavnostih in potencialnih varnostnih incidentih.

9. Politika upravljanja tretjih strank

Ocena dobaviteljev: Izvajajte temeljite ocene dobaviteljev in izvajalcev za zagotavljanje, da izpolnjujejo varnostne standarde organizacije.

Pogodbene zahteve: V pogodbe s tretjimi strankami vključite specifične varnostne zahteve in odgovornosti.

Spremljanje in revizija: Redno spremljajte in revidirajte skladnost tretjih strank z varnostnimi politikami ter postopki.

Postopki prekinitve: Vzpostavite postopke za varno prekinitev odnosov s tretjimi strankami, vključno z vračilom ali uničenjem občutljivih podatkov.

10. Politika razvoja programske opreme

Varnost v razvojnem življenjskem ciklu: Integrirajte varnost v vse faze življenjskega cikla razvoja programske opreme (SDLC), od zasnove do uvedbe.

Pregled kode: Uvedite redne preglede kode in statične analize kode za prepoznavanje ter odpravljanje varnostnih ranljivosti.

Testiranje: Izvajajte temeljito varnostno testiranje, vključno z vdornim testiranjem in oceno ranljivosti, pred uvedbo programske opreme. Če je le mogoče, ločite testno okolje od produkcijskega.

Upravljanje popravkov: Zagotovite pravočasne posodobitve in popravke za odpravljanje varnostnih ranljivosti v programski opremi.

S temi podrobnimi navodili lahko organizacije ustvarijo celovito krovno varnostno politiko, ki je skladna z zakonskimi zahtevami in najboljšimi praksami ter zagotavljajo robustno zaščito svojih informacijskih sredstev. Priprava krovne varnostne politike zahteva celovit pristop, ki vključuje analizo tveganj, določitev varnostnih ciljev, vzpostavitev odgovornosti in uvedbo tehničnih ter organizacijskih ukrepov. Pomembno je, da politika ni zgolj dokument, temveč živi del organizacijske kulture, ki se redno pregleduje in prilagaja spreminjajočim se varnostnim izzivom ter regulatornim zahtevam.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- ISO 31000:2018: Risk management — Guidelines
- ISO 31010:2019 : Risk management — Risk assessment techniques
- Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov: Uradni list RS, št. 118/23: https://pisrs.si/pregledPredpisa?id=URED8925&utm=
- Urad Vlade RS za informacijsko varnost https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/
- Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-10 in 49/23): https://pisrs.si/pregledPredpisa?id=ZAKO7707&utm_

Poglavje 11
Predstavitev ključnih korakov upravljanja kibernetske oziroma informacijske varnosti

POVZETEK

Upravljanje kibernetske in informacijske varnosti je ključnega pomena za zaščito organizacijskih informacijskih sistemov in podatkov pred nenehno spreminjajočimi se grožnjami. Poglavje zajema celovit pregled ključnih korakov, od prepoznavanja varnostnih zahtev, identifikacije tveganj, razvoja strategije upravljanja, implementacije ukrepov, izobraževanja zaposlenih, nadzora in odziva na incidente, rednega testiranja ter priprave na obnovo po incidentu. Poudarjena je potreba po povezovanju z mednarodnimi standardi, kot je standard ISO/IEC 27002, ter pomembnost sodelovanja vseh ravni organizacije, vključno z vodstvom in zaposlenimi. Uspešno upravljanje zahteva stalno prilagajanje novim izzivom, redno ocenjevanje učinkovitosti varnostnih ukrepov ter vzpostavitev celovitih načrtov za neprekinjeno poslovanje in odzivanje na incidente.

Ključne točke:

- Upravljanje kibernetske varnosti
- Identifikacija in analiza tveganj
- Strategija upravljanja tveganj
- Implementacija varnostnih ukrepov
- Izobraževanje in ozaveščanje zaposlenih
- Nadzor in odzivanje na incidente
- Redno testiranje in ocenjevanje ukrepov
- Priprava na obnovo po incidentih
- Povezovanje s standardom ISO/IEC 27002
- Neprekinjeno poslovanje in krizni načrti.

1. Uvod v upravljanje kibernetske varnosti

V sodobnem poslovnem okolju, kjer informacijski sistemi podpirajo ključne poslovne procese, je učinkovito upravljanje kibernetske varnosti postalo nuja. Pomen prepoznavanja varnostnih zahtev je zato ključen del tega procesa. Organizacija mora najprej prepoznati in oceniti svoje specifične varnostne potrebe. Ti izzivi niso zgolj tehnični, temveč se navezujejo na različne poslovne, pravne in regulativne dejavnike, ki oblikujejo varnostne zahteve.

Glavni viri varnostnih zahtev vključujejo:

- **Ocenjevanje tveganj**: Organizacije morajo analizirati grožnje, ki lahko vplivajo na njihove informacijske sisteme. Ta analiza vključuje prepoznavanje ranljivosti v sistemih, ocenitev potencialnih vplivov in opredelitev resnosti tveganj. Učinkovita ocena tveganj omogoča pripravo prioritetne lestvice ukrepov in zagotovi, da se omejena sredstva usmerijo v reševanje najbolj kritičnih težav.
- **Pravne in regulativne zahteve**: Zakonodaja in regulativa se na področju varnosti informacij nenehno razvijata. Podjetja morajo biti skladna z nacionalnimi in mednarodnimi (evropskimi) pravnimi podlagami in/ali z različnimi varnostnimi standardi, ki se uporabljajo v njihovi panogi. Upoštevanje teh podlag zagotavlja, da podjetje ne le varuje svoje podatke, temveč se tudi izogiba morebitnim kaznim/globam zaradi neskladnosti.
- **Cilji in načela upravljanja**: Pomembno je, da organizacije določijo jasno strukturo ciljev glede upravljanja informacij. To vključuje vzpostavitev postopkov za varovanje občutljivih podatkov, opredelitev odgovornosti in določanje načinov za spremljanje ter preverjanje skladnosti z varnostnimi politikami.

Povezava z SIST EM ISO/IEC 27002:

Standard ISO/IEC 27002 predstavlja temeljni vir smernic za vzpostavitev ustreznih kontrol in mehanizmov za zaščito pred varnostnimi tveganji. Standard omogoča organizacijam prilagoditev kontrol glede na lastne potrebe in jih usmerja pri izbiri potrebnih varnostnih ukrepov. Poleg tega ponuja okvir za vzpostavitev učinkovitih postopkov za spremljanje in odzivanje na varnostne incidente. Uvedba oziroma upoštevanje teh smernic omogoča organizacijam, da ostanejo proaktivni pri obvladovanju varnostnih tveganj, kar poveča odpornost na zunanje in notranje grožnje.

2. Identifikacija tveganj

Identifikacija tveganj je osnova za vzpostavitev učinkovitega sistema kibernetske varnosti. Gre za postopek, pri katerem organizacija prepozna in oceni grožnje, ki bi lahko ogrozile njene informacijske sisteme ter podatke. Pri identifikaciji tveganj je pomembno, da podjetje upošteva celoten spekter potencialnih nevarnosti, saj te izhajajo iz različnih virov, od zunanjih napadov do notranjih napak ali malomarnosti zaposlenih.

Postopek identifikacije tveganj vključuje več ključnih korakov:

- **Zbiranje informacij o obstoječih grožnjah**: Organizacije morajo redno spremljati razvoj kibernetskih groženj, tako na globalni kot nacionalni ravni. To vključuje analizo preteklih varnostnih incidentov v industriji/sektorju, kot tudi reden pregled lastnih informacijskih sistemov.
- **Prepoznavanje ranljivosti**: Ranljivosti v informacijskih sistemih so tista šibka mesta, kjer lahko pride do vdora ali izgube podatkov. Te ranljivosti so lahko tehnične narave, kot so nezakrpane programske opreme, ali pa izhajajo iz neustreznih varnostnih praks znotraj organizacije.
- **Ocena resnosti in verjetnosti tveganj**: Ko so tveganja prepoznana, jih je treba oceniti glede na njihovo verjetnost in možne posledice. Tveganja, ki predstavljajo veliko grožnjo, je treba obravnavati prednostno, saj lahko njihova realizacija povzroči organizaciji znatno škodo.

Učinkovita identifikacija tveganj omogoča organizacijam, da oblikujejo ustrezne strateške

varnostne ukrepe, ki so usmerjeni v preprečevanje in blaženje potencialnih škod. To je nenehen proces, ki zahteva stalno prilagajanje in izboljševanje, saj se narava groženj neprestano spreminja.

3. Razvoj strategije upravljanja tveganj

Ko so tveganja prepoznana in ocenjena je naslednji korak oblikovanje strategije za njihovo upravljanje. Razvoj strategije upravljanja tveganj je ključnega pomena, saj mora zagotoviti, da se ukrepi osredotočijo na najpomembnejše grožnje, in da so stroškovno učinkoviti. V tem koraku organizacija določi prioritetne naloge, metode in vire, ki so potrebni za obvladovanje tveganj.

Koraki pri razvoju strategije:

- **Določitev ciljev in prioritet**: Strategija mora temeljiti na jasnih ciljih, ki so povezani z zaščito ključnih informacijskih virov. Organizacija mora določiti, kateri podatki in sistemi so najbolj občutljivi ter katere grožnje predstavljajo največje tveganje.
- **Izbira metod upravljanja tveganj**: Na voljo so različne metode za obvladovanje tveganj, vključno z izogibanjem tveganjem, zmanjševanjem njihovega vpliva, prenosom tveganj na tretje strani (npr. zavarovalnice) ali sprejemanjem tveganj v primerih, ko so posledice sprejemljive. Za več informacij o posameznih metodah si lahko ogledate poglavje 14: Napotki za pripravo ukrepov za obvladovanje tveganj.
- **Ocena stroškov in virov**: Pri razvijanju strategije je pomembno, da se oceni tudi stroškovna učinkovitost posameznih varnostnih ukrepov. Organizacija mora presoditi, ali so viri (tako finančni kot kadrovski) razporejeni optimalno glede na stopnjo tveganj.

Strategija upravljanja tveganj se mora prilagajati spremembam v poslovnem okolju in slediti razvoju tehnologij. Poleg tega mora vključevati redno ocenjevanje in testiranje učinkovitosti ukrepov, kar zagotavlja, da je organizacija pripravljena na nove ter razvijajoče se grožnje.

4. Implementacija varnostnih ukrepov

Ko je strategija pripravljena, sledi njena implementacija, ki je ključnega pomena za zaščito informacijskih sistemov pred kibernetskimi grožnjami. Ta korak vključuje tako tehnične kot organizacijske ukrepe, ki morajo biti natančno izvedeni, da zagotovijo največjo možno zaščito.

Glavne komponente implementacije:

- **Tehnološki ukrepi**: Sem spadajo uporaba požarnih zidov, naprednih sistemov za zaznavanje vdorov (IDS), šifriranje podatkov ter protivirusni programi. Ti ukrepi so prva obrambna linija pred zunanjimi grožnjami.
- **Organizacijski ukrepi**: Varnostne politike, kot so pravilniki o uporabi gesel, dostop do podatkov in postopki za obravnavo varnostnih incidentov so prav tako ključni elementi zaščite. Pomembno je, da so zaposleni seznanjeni z varnostnimi pravili, in da organizacija zagotovi redno izobraževanje na tem področju.
- **Redno testiranje in nadzor**: Sistemi, ki so bili implementirani, morajo biti redno preverjani in testirani, da se zagotovi njihova učinkovitost. To vključuje izvajanje varnostnih preizkusov, kot so vdorni (penetracijski) testi ter spremljanje dnevniških zapisov, da se čim prej odkrijejo morebitne neskladnosti.

Implementacija varnostnih ukrepov zahteva tesno sodelovanje različnih oddelkov znotraj organizacije. Poleg IT oddelka je nujno, da so v ta proces vključeni tudi zaposleni z oddelka za človeške vire, pravne službe in vodstvo, saj je kibernetska varnost v rokah celotne organizacije, odgovornost pa nosi vodstvo.

5. Izobraževanje in usposabljanje zaposlenih

Človeški dejavnik ostaja eden najpomembnejših, vendar tudi najšibkejših elementov kibernetske varnosti v organizacijah. Veliko varnostnih incidentov izhaja iz napak zaposlenih, ki zaradi pomanjkljivega znanja ali nepazljivosti omogočijo zlorabo sistemov ali izpostavijo ob-

čutljive podatke. Zato je ključnega pomena, da organizacija vzpostavi celovit in učinkovit program izobraževanja, ozaveščanja ter usposabljanja zaposlenih. Ta mora biti zasnovan tako, da ne gre zgolj za enkratno izobraževanje, temveč za neprekinjen proces, ki se prilagaja novim izzivom in grožnjam.

Začeti je treba s temeljitim uvajanjem vseh novih zaposlenih, kjer se jih seznani z osnovnimi varnostnimi politikami organizacije, pravilno uporabo tehnologije, kot so gesla, VPN-ji in večfaktorska avtentikacija. Vendar to ni dovolj. Zaposlene je treba redno osveščati o novih grožnjah, kot so lažno predstavljanje (ang. phishing) napadi, socialni inženiring, izsiljevalska programska oprema, saj so te taktike vedno bolj sofisticirane in pogosto izkoriščajo ravno pomanjkanje zavedanja pri uporabnikih.

Usposabljanje mora vključevati praktične primere in simulacije, kjer zaposleni lahko preizkusijo svoje odzive na potencialne kibernetske grožnje. Na primer, simulirani napadi lažnega predstavljanja (ang. Phishing) lahko služijo kot uporabno orodje, da se pokažejo slabosti v obstoječih procesih in se hkrati okrepi pripravljenost zaposlenih na resnične napade. Redni seminarji, delavnice in dostop do spletnih tečajev morajo biti del vsakdanje prakse, saj le tako lahko organizacija zagotovi, da so zaposleni vedno korak pred napadalci.

Poleg tehničnih vidikov je pomembno tudi, da usposabljanje vključuje širšo ozaveščenost o odgovornosti zaposlenih. Na vseh ravneh podjetja se mora vzpostaviti varnostna kultura, kjer vsak posameznik razume svojo vlogo pri zaščiti podatkov in sistemov. Le tako lahko podjetje učinkovito zmanjšuje človeška tveganja in krepi svojo celotno varnostno kulturo.

6. Nadzor in odziv na incidente

Kibernetska varnost ni statičen proces, temveč zahteva nenehen nadzor in hitro ukrepanje ob morebitnih incidentih. Varnostni incidenti se lahko pojavijo kadarkoli, ne glede na to, kako robustni so preventivni ukrepi. Zato je ključno, da organizacija vzpostavi sistem za stalno spremljanje svojih informacijskih sistemov. To vključuje uporabo naprednih tehnologij, kot so orodja za zaznavanje vdorov (IDS), ki nenehno spremljajo promet v omrežju in opozarjajo na sumljive dejavnosti, ter sisteme za preprečevanje vdorov (IPS), ki lahko proaktivno blokirajo zaznane grožnje. Pomembno je tudi redno spremljanje dnevniških zapisov s pomočjo rešitev za upravljanje varnostnih informacij in dogodkov (SIEM), ki omogočajo sledenje ter analizo dogodkov v omrežju v realnem času. Poleg tega se uporabljajo požarni zidovi (Firewall) in rešitve za zaznavanje ter odzivanje na končnih točkah (EDR) in omrežju (NDR) za dodatno zaščito.

Ko pride do varnostnega incidenta, mora biti organizacija pripravljena na hiter in učinkovit odziv. To pomeni, da je treba imeti vnaprej pripravljen načrt za odzivanje na incidente, ki jasno določa korake, odgovornosti in postopke, ki jih je treba izvesti. Odzivni načrti morajo vključevati takojšnje ukrepe za omejevanje škode, kot je na primer izolacija okuženega sistema ali prekinitev dostopa do ogroženih podatkov, ter obveščanje vseh prizadetih strani, tako znotraj organizacije kot tudi zunaj nje.

Pomembno je, da odziv na incidente ni le tehnična naloga IT oddelka, temveč celostni proces, ki vključuje tudi pravne, komunikacijske in vodstvene vidike. Če gre za večji incident, ki lahko vpliva na ugled podjetja ali vključuje osebne podatke, mora biti pripravljen tudi komunikacijski načrt, kako obvestiti stranke, partnerje, javnosti in regulatorje. Po zaključku incidenta pa je treba izvesti temeljito analizo dogodka, da se ugotovi, kaj je šlo narobe, katere ranljivosti so bile izkoriščene in kako lahko organizacija izboljša svoje varnostne ukrepe.

Uspešen nadzor in odziv na incidente omogočata organizaciji, da minimizira škodo in prepreči, da bi posamezni incidenti imeli dolgoročne negativne posledice na poslovanje. Varnost je le tako celovito vzpostavljena, če podjetje učinkovito prehaja med preventivnimi in reaktivnimi ukrepi.

Organizacije uporabljajo različna orodja, kot so sistemi za zaznavanje vdorov (IDS), SIEM:

varnostno-informacijski in dogodkovni sistem (Security Information and Event Management) ter protivirusne rešitve, da spremljajo dogajanje v omrežju. Prav tako je ključnega pomena, da podjetje vzpostavi odzivni načrt, ki določa, kako bodo različni oddelki reagirali v primeru napada. Pomembna je tudi jasna koordinacija med vsemi enotami organizacije, ki so v takšen odziv vključene, ta mora potekati po vnaprej določeni poti in iz ene točke. Ta načrt vključuje naslednje korake:

- prva reakcija na incident (prepoznavanje, izolacija),
- analiza in ocena škode,
- omejitev nadaljnjih posledic (zapiranje ranljivosti),
- obnova podatkov in sistemov,
- učinkovita komunikacija s strankami in deležniki.

7. Redno testiranje in ocenjevanje

V kibernetski varnosti ni nič bolj nevarnega kot občutek lažne varnosti. Tudi najbolj napredni varnostni sistemi in kontrole se lahko sčasoma izkažejo za neučinkovite, še posebej, če jih organizacija ne testira ter ocenjuje redno. Grožnje se nenehno razvijajo, kar pomeni, da se morajo varnostni ukrepi stalno prilagajati novim izzivom. Zato je redno testiranje varnostnih ukrepov ključnega pomena za zagotavljanje, da so še vedno ustrezni in učinkoviti

Vdorni (Penetracijski) testi so ena izmed najbolj uporabljenih metod za preverjanje varnosti. Zunanji strokovnjaki ali specializirane ekipe znotraj organizacije simulirajo napade na sisteme, da bi odkrili morebitne ranljivosti. Ti testi so izjemno dragoceni, saj omogočajo, da podjetje odkrije šibke točke v svojih sistemih, preden jih odkrijejo dejanski napadalci. Poleg tega vdorni (penetracijski) testi pomagajo oceniti, kako dobro delujejo odzivni načrti in koliko so zaposleni pripravljeni na morebitne incidente.

Poleg testov je pomembno tudi redno ocenjevanje učinkovitosti obstoječih varnostnih politik in postopkov. Organizacija mora redno pregledovati svoje varnostne strategije in jih prilagajati glede na nove grožnje ali spremembe v notranjem ter zunanjem okolju. Pri tem je ključnega pomena, da se zbirajo povratne informacije od vseh oddelkov znotraj organizacije. Tisti, ki delajo neposredno s podatki in sistemi, so pogosto najboljši vir informacij o tem, kje so ranljivosti ter kako bi lahko izboljšali obstoječe procese.

Z rednim testiranjem in ocenjevanjem se organizacija ne le izogne potencialnim grožnjam, temveč tudi ohranja proaktivno držo pri upravljanju svoje kibernetske varnosti. To je najboljši način, da ostane korak pred napadalci in hkrati ohrani zaupanje strank ter partnerjev

8. Priprava na obnovo po incidentu

Tudi z najboljšimi varnostnimi ukrepi se organizacije soočajo z dejstvom, da varnostni incidenti lahko kljub vsemu še vedno nastopijo. Zato je ključnega pomena, da so podjetja pripravljena na obnovo po incidentu, saj lahko hitro in učinkovito ukrepanje bistveno zmanjša posledice za poslovanje. Proces obnove ne vključuje le tehnične plati, temveč mora biti organizacija pripravljena tudi na pravne, komunikacijske in poslovne izzive, ki jih incidenti prinašajo. Obnova po incidentu je tesno povezana z neprekinjenim poslovanjem. Za več informacij o oceni vpliva na poslovanje in ukrepih za zagotavljanje neprekinjenega poslovanja si lahko ogledate poglavje 15: Napotki za pripravo ocene vpliva na poslovanje in ukrepov zagotavljanja neprekinjenega poslovanja.

Prvi korak v obnovi po incidentu je vzpostavitev natančnega načrta za obnovitev sistemov in podatkov. Ta načrt mora zajemati pomembne časovne odzive za ponovno vzpostavitev delovanja prizadetih sistemov, postopek za obnavljanje varnostnih kopij podatkov in aplikacij, ponovni zagon sistemov ter preverjanje, ali so bili sistemi po incidentu ustrezno očiščeni ter

zaščiteni pred nadaljnjimi napadi. Zato mora organizacija vzpostaviti redne varnostne kopije, ki se izvajajo samodejno in na več varnostnih lokacijah, saj je obnova pogosto odvisna od dostopa do neokrnjenih kopij podatkov.

Priprava na obnovo po incidentu vključuje tudi razvoj kriznih načrtov za komunikacijo z zaposlenimi, strankami in javnostjo. V primeru večjega varnostnega incidenta, kot je izguba osebnih podatkov ali napad z izsiljevalsko programsko opremo, je treba pravočasno in natančno obvestiti vse prizadete strani ter tudi pristojne državne organe. Neuspešno komuniciranje lahko še poveča škodo, saj lahko izguba zaupanja strank in poslovnih partnerjev traja dolgo po tem, ko je incident že tehnično rešen.

Pomemben del načrta za obnovo je tudi analiza incidenta. Organizacija mora po vsakem incidentu izvesti temeljito preiskavo, da ugotovi, kaj je šlo narobe, kako je napadalec pridobil dostop in kateri ukrepi so bili neučinkoviti. Ta analiza služi kot osnova za izboljšanje varnostnih politik in postopkov, da bi preprečili ponovitev podobnih incidentov v prihodnosti. To je dinamičen proces, kjer se organizacija uči iz svojih napak in prilagaja svojo strategijo kibernetske varnosti.

Priprava na obnovo po incidentu ni le tehnično vprašanje, temveč tudi vprašanje celotne organizacijske pripravljenosti. Le podjetja, ki imajo vzpostavljen celovit in podroben načrt za obvladovanje kriznih situacij, lahko ohranijo stabilnost ter zmanjšajo vpliv varnostnih incidentov na svoje poslovanje.

Viri:

- ENISA (December 2016): Technical Guidelines for the implementation of minimum security measures for Digital Service Providers. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/@@download/fullReport
- Čaleta, D. in drugi (2019) Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture, MORS-Ljubljana
- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- Urad Vlade RS za informacijsko varnost https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/
- Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-10 in 49/23): https://pisrs.si/pregledPredpisa?id=ZAKO7707&utm_

Poglavje 12
Napotki za izdelavo analize tveganj informacijske varnosti

POVZETEK

Izdelava analize tveganj informacijske varnosti je ključnega pomena za vzpostavitev učinkovitega sistema varovanja informacijskih sredstev organizacije. Poglavje ponuja celovit pregled postopka, ki vključuje prepoznavanje, oceno in obvladovanje tveganj. Poudarjen je pomen metodološke doslednosti, sodelovanja različnih oddelkov ter usklajenosti z zakonodajnimi zahtevami in mednarodnimi standardi, kot je standard ISO 27005. Analiza tveganj služi kot temelj za učinkovito načrtovanje varnostnih ukrepov, hkrati pa omogoča prilagodljivost na hitro spreminjajoče se grožnje. Posebej izpostavljena je potreba po vključevanju vodstva ter oblikovanju realističnih načrtov za obvladovanje tveganj, ki so usklajeni z razpoložljivimi viri.

Ključne točke:

- Priprava in načrtovanje
- Identifikacija sredstev in groženj
- Identifikacija ranljivosti in ocena vpliva
- Ocena tveganj in resnosti (verjetnosti)
- Strategije upravljanja tveganj
- Implementacija in spremljanje ukrepov
- Prilagoditev zakonskim zahtevam
- Uporaba mednarodnih standardov in metodologij
- Integracija analize tveganj v sistemu upravljanja varnosti informacij (SUVI) in sistemu upravljanja neprekinjenega poslovanja (SUNP).

Izdelava analize tveganj informacijske varnosti je ključni korak za zagotovitev ustrezne zaščite informacijskih sredstev organizacije. S spodnjimi napotki boste lažje izvedli celovit postopek analize tveganj, ki vam bo pomagal prepoznati, oceniti in upravljati tveganja v vašem informacijskem okolju. Ocenjevanje tveganj ima pomembno mesto tako v sistemu upravljanja varnosti informacij (SUVI), kakor tudi v sistemu upravljana neprekinjenega poslovanja (SUNP).

Na podlagi zakonskih zahtev[7] je treba izvesti analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj (v nadaljevanju: analiza obvladovanja tveganj), ki mora zajemati najmanj:

- navedbo uporabljene metodologije za izvedbo analize obvladovanja tveganj, ki mora biti primerljiva, verodostojna in ponovljiva v skladu s pravili stroke,
- navedbo sredstev znotraj SUVI in upravljavce teh sredstev oziroma odgovorne osebe za ta sredstva,
- navedbo možnih groženj tem sredstvom,
- navedbo ranljivosti sredstev, ki bi jih grožnje lahko prizadele,
- navedbo vpliva uresničitve groženj na zaupnost, celovitost in razpoložljivost sredstev zaradi opredeljenih ranljivosti,
- oceno vpliva na opravljanje bistvenih storitev v primeru kršitve informacijske varnosti zaradi izgube zaupnosti, celovitosti ali razpoložljivosti,
- oceno verjetnosti, da nastane kršitev informacijske varnosti,
- ovrednotenje ravni tveganj,
- določitev in obrazložitev sprejemljive ravni tveganj,
- navedbo ukrepov za odpravo ali zmanjšanje tveganj nad sprejemljivo ravnjo.

Zavezanec analizo obvladovanja tveganj pripravi tako, da:

- navede metodologijo z opredelitvijo lestvic in atributov ocenjevanja, po kateri bo izvedel analizo obvladovanja tveganj v skladu z Uredbo,
- izvede popis sredstev znotraj SUVI in določi njihove upravljavce oziroma odgovorne osebe za ta sredstva,
- prepozna možne grožnje za izgubo zaupnosti, celovitosti in razpoložljivosti sredstev iz prejšnje točke,
- prepozna ranljivost ključnih informacijskih sredstev, ki bi jih identificirane grožnje lahko prizadele,
- oceni stopnjo vpliva uresničitve groženj na zaupnost, celovitost in razpoložljivost ključnih informacijskih sredstev,
- oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi,
- ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev ter
- določi oceno sprejemljive ravni tveganja glede na vrednotenje ugotovljenih tveganj.

Zavezanec seznam svojih ključnih, krmilnih in nadzornih informacijskih sistemov pripravi tako, da:

- na podlagi popisanih sredstev znotraj SUVI presodi, ali je zagotavljanje bistvenih storitev odvisno od posameznega sredstva znotraj SUVI, in
- na podlagi posameznih sredstev znotraj SUVI, od katerih je v skladu s prejšnjo alinejo odvisno zagotavljanje bistvenih storitev, presodi, katero od teh sredstev je ključno za delovanje bistvene storitve.

[7] Podrobneje glej Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, Ur. l. RS 8/23.

Zavezanec izvede analizo obvladovanja tveganj ter določi ključne, krmilne in nadzorne informacijske sisteme tako, da bodo rezultati teh postopkov dosledni, primerljivi ter verodostojni.

Zavezanec izvaja analizo obvladovanja tveganj in določa ključne, krmilne ter nadzorne informacijske sisteme v rednih časovnih presledkih, ali kadar so predlagane, ali nastanejo bistvene spremembe v okviru SUVI.

Pomembno je razumevanje, da je za učinkovitost analiziranja tveganj največkrat treba opraviti dve analizi ocenjevanja tveganj. Prvo v okviru SUVI, kot je razloženo v zgornjih zahtevah zakonodajalca, kjer je fokus analize tveganj prvenstveno usmerjen v ključne krmilne in nadzorne informacijske sisteme, pri SUNP pa je analiza širše zasnovana in usmerjena predvsem v tiste bistvene procese v organizaciji, ki so nujni za celovito delovanje organizacije ter je zaradi njihovega učinka na delovanje organizacije tudi treba, da ves čas neprekinjeno delujemo.

V nadaljevanju bomo podali nekaj dodatnih pojasnil, ki jih lahko uporabite pri izvedbi procesov analiziranja tveganj v vaših organizacijah. Za pomoč se lahko oprete na določene standarde, ki v svojem obsegu opredeljujejo korake za izvedbo analize tveganj. Posebej pa bomo predstavili tudi določene modele in metode, ki se uporabljajo na področju analiziranja tveganj.

Koraki za izdelavo analize tveganj informacijske varnosti

1. **Priprava in načrtovanje**
   - **Določitev obsega analize**: Opredelite, katere informacijske sisteme, podatke in procese boste vključili v analizo.
   - **Vzpostavitev ekipe za analizo tveganj**: Sestavite multidisciplinarno ekipo, ki vključuje strokovnjake za informacijsko varnost, IT, pravne zadeve, poslovne procese in druge relevantne oddelke.
   - **Določitev metodologije**: Izberite in dokumentirajte metodologijo, ki jo boste uporabili za analizo tveganj (npr. ISO 27005).
2. **Identifikacija sredstev in groženj**
   - **Identifikacija informacijskih sredstev**: Naredite popis vseh informacijskih sredstev, kot so podatki, strojna in programska oprema, omrežja, aplikacije ter podporna infrastruktura.
   - **Določitev lastnikov sredstev**: Identificirajte odgovorne osebe za vsako sredstvo.
   - **Identifikacija groženj**: Zberite informacije o možnih grožnjah, ki bi lahko vplivale na varnost vaših informacijskih sredstev (npr. kibernetski napadi, naravne nesreče, notranje grožnje).
3. **Identifikacija ranljivosti in ocena vpliva**
   - **Identifikacija ranljivosti**: Preglejte varnostne kontrole in postopke ter določite potencialne ranljivosti, ki bi jih grožnje lahko izkoristile.
   - **Ocena vpliva**: Določite, kako bi izkoriščena ranljivost vplivala na zaupnost, celovitost in razpoložljivost vaših informacijskih sredstev. Uporabite merila, kot so finančne posledice, pravne posledice, vpliv na poslovne operacije in ugled organizacije.
4. **Ocena tveganj**
   - **Ocena verjetnosti**: Določite verjetnost, da se bo določena grožnja realizirala in izkoristila ranljivost.
   - **Ocena resnosti**: Kombinirajte verjetnost in vpliv, da ocenite resnost vsakega tveganja. To lahko storite z uporabo matrike tveganj (npr. nizko, srednje, visoko tveganje).

5. **Upravljanje tveganj**

   - **Določitev strategij za obvladovanje tveganj**: Izberite ustrezne ukrepe za zmanjšanje, sprejetje, prenos ali izogibanje tveganjem.

   - **Izdelava načrta ukrepov**: Dokumentirajte ukrepe, odgovorne osebe, roke in vire, potrebne za izvajanje izbranih strategij.

   - **Implementacija ukrepov**: Uvedite izbrane ukrepe za obvladovanje tveganj.

6. **Spremljanje in pregledovanje**

   - **Nadzor in spremljanje**: Nenehno spremljajte tveganja in učinkovitost uvedenih ukrepov.

   - **Redno pregledovanje**: Periodično pregledujte in posodabljajte analizo tveganj, zlasti ob pomembnih spremembah v informacijskem okolju, procesih ali grožnjah.

Priporočene metode in orodja:

- **Metodologije**: ISO 27005, NIST SP 800-30, OCTAVE.

- **Orodja**: Risk Management Framework (RMF), orodja za oceno tveganj (npr. FAIR, CRAMM).

Pravilno izvedena analiza tveganj informacijske varnosti je temelj za učinkovito upravljanje varnostnih groženj in zaščito informacijskih sredstev organizacije. S sistematičnim pristopom boste lahko prepoznali in ocenili tveganja ter uvedli ustrezne ukrepe za njihovo obvladovanje, kar bo prispevalo k večji odpornosti vaše organizacije proti kibernetskim grožnjam in drugim varnostnim incidentom.

V nadaljevanju se oglejmo kratko predstavitev določenih metodologij in orodij za izvedbo ocenjevanja tveganj. Pri analizi lahko uporabljate eno metodologijo ali pa, glede na specifičnost vaših organizacij, kombinacijo večjih metodologij ali orodij. Pomembno je samo, da je analiza izvedena z jasno postavljenimi kriteriji, in da jo je možno v vsakem trenutku ponoviti prek jasno določenega metodološkega aparata.

A. ISO 27005 - Smernice za upravljanje tveganj informacijske varnosti

ISO/IEC 27005 je mednarodni standard, ki nudi smernice za upravljanje tveganj informacijske varnosti. Namenjen je podpori zahtevam iz standarda ISO/IEC 27001 in pomaga organizacijam pri implementaciji sistema upravljanja varnosti informacij (ISMS). Ta standard opisuje proces upravljanja tveganj, ki omogoča organizacijam, da prepoznajo, ocenijo in obvladajo tveganja, povezana z varnostjo informacij.

Ključni koraki v procesu upravljanja tveganj po ISO 27005:

1. **Vzpostavitev konteksta**

   - **Opredelitev obsega**: Določite, katere dele organizacije, poslovne procese, informacijska sredstva in lokacije bo obsegala analiza tveganj.

   - **Kontekst organizacije**: Razumevanje notranjega in zunanjega konteksta, vključno s poslovnimi cilji, zakonskimi zahtevami, regulativami ter pričakovanji deležnikov.

   - **Kriteriji tveganja**: Opredelite kriterije za ocenjevanje tveganj, vključno s toleranco do tveganj in merili za sprejemanje tveganj.

2. **Identifikacija tveganj**

   - **Identifikacija sredstev**: Zberite informacije o vseh informacijskih sredstvih, ki so v obsegu analize, vključno z lastniki sredstev.

   - **Identifikacija groženj**: Prepoznajte potencialne grožnje, ki lahko vplivajo na vaša sredstva (npr. kibernetski napadi, naravne nesreče).

   - **Identifikacija ranljivosti**: Ugotovite ranljivosti, ki jih lahko grožnje izkoristijo.

- **Identifikacija posledic**: Določite možne posledice realizacije groženj, vključno z vplivi na zaupnost, celovitost in razpoložljivost informacij.

3. **Ocena tveganj**

   - **Analiza tveganj**: Ocenite verjetnost in vpliv posameznih tveganj. To lahko storite z uporabo kvalitativnih, kvantitativnih ali polkvalitativnih metod.

   - **Ocena tveganj**: Določite stopnjo tveganja za vsako grožnjo glede na kombinacijo verjetnosti in vpliva.

4. **Obvladovanje tveganj**

   - Možnosti obvladovanja tveganj: Določite možne ukrepe za zmanjšanje, prenos, sprejetje ali izogibanje tveganjem.

   - Izbira ukrepov: Izberite najprimernejše ukrepe za obvladovanje vsakega tveganja glede na kriterije tveganj in poslovne cilje.

   - Načrt obvladovanja tveganj: Pripravite načrt, ki vključuje izbrane ukrepe, roke za izvedbo, odgovorne osebe in potrebne vire.

5. **Spremljanje in pregledovanje tveganj**

   - Nenehno spremljanje: Spremljajte tveganja in učinkovitost uvedenih ukrepov.

   - Redno pregledovanje: Periodično pregledujte in posodabljajte analizo tveganj glede na spremembe v informacijskem okolju, poslovnih procesih ali novih grožnjah.

   - Poročanje o tveganjih: Poročajte vodstvu in drugim relevantnim deležnikom o stanju tveganj ter učinkovitosti ukrepov.

ISO/IEC 27005 zagotavlja strukturiran pristop k upravljanju tveganj informacijske varnosti, kar pomaga organizacijam pri zaščiti njihovih informacijskih sredstev in izpolnjevanju zahtev standarda ISO/IEC 27001. S pravilno implementacijo teh smernic lahko organizacije bolje prepoznajo, ocenijo in obvladajo varnostna tveganja, kar prispeva k večji odpornosti proti kibernetskim grožnjam ter zagotavljanju neprekinjenega poslovanja.

B. Okvir za upravljanje tveganj (RMF)

Okvir za upravljanje tveganj (RMF) je strukturiran pristop za identifikacijo, oceno, obvladovanje in spremljanje tveganj v organizaciji. RMF pomaga organizacijam pri sistematičnem obravnavanju tveganj, ki lahko vplivajo na njihovo delovanje, varnost in skladnost z zakonodajo.

Ključni koraki RMF

1. **Priprava in organizacija**

   - Določitev ciljev: Jasno opredeliti cilje upravljanja tveganj, ki jih želi organizacija doseči.

   - Vzpostavitev ekipe: Oblikovati večfunkcionalno ekipo za upravljanje tveganj, ki vključuje predstavnike iz različnih delov organizacije.

   - Opredelitev obsega: Določiti obseg in meje procesa upravljanja tveganj.

2. **Identifikacija tveganj**

   - Zbiranje informacij: Uporabiti različne vire za zbiranje podatkov o možnih tveganjih, kot so notranji pregledi, ankete, intervjuji in analize podatkov.

   - Prepoznavanje tveganj: Identificirati vsa možna tveganja, ki lahko vplivajo na doseganje ciljev organizacije.

3. **Analiza tveganj**

   - Ocenjevanje verjetnosti in Vpliva: Oceniti verjetnost pojava vsakega tveganja in njegov potencialni vpliv na organizacijo.

   - Razvrščanje tveganj: Razvrstiti tveganja glede na njihovo resnost in pomembnost za organizacijo.

4. **Ocena tveganj**

   - Vrednotenje tveganj: Ugotoviti, katera tveganja so sprejemljiva in katera zah-

tevajo ukrepanje. To vključuje primerjavo ocenjenih tveganj z določenimi kriteriji sprejemljivosti.

5. **Obvladovanje tveganj**
   - Razvoj strategij: Oblikovati strategije za zmanjšanje, prenos, sprejemanje ali izogibanje tveganjem.
   - Izvajanje ukrepov: Izvesti načrtovane strategije in ukrepe za obvladovanje tveganj.
6. **Spremljanje in pregled**
   - Nenehno spremljanje: Nenehno spremljati tveganja in učinkovitost sprejetih ukrepov.
   - Redni pregledi: Periodično pregledovati in posodabljati okvir za upravljanje tveganj glede na spremembe v notranjem ter zunanjem okolju organizacije.
7. **Komunikacija in poročanje**
   - Obveščanje deležnikov: Redno obveščati ključne deležnike o stanju tveganj in izvedenih ukrepih.
   - Dokumentacija: Vzdrževati ustrezno dokumentacijo o vseh korakih in odločitvah v procesu upravljanja tveganj.

Prednosti RMF

- Strukturiran pristop: Zagotavlja sistematičen in dosleden pristop k upravljanju tveganj.
- Izboljšana odločanja: Omogoča bolje informirane odločitve glede obvladovanja tveganj.
- Povečana odpornost: Prispeva k večji odpornosti organizacije proti nepričakovanim dogodkom.
- Skladnost: Pomaga organizacijam pri izpolnjevanju zakonskih in regulativnih zahtev.

Okvir za upravljanje tveganj (RMF) je ključen za učinkovito upravljanje tveganj v organizaciji. S strukturiranim pristopom k prepoznavanju, ocenjevanju, obvladovanju in spremljanju tveganj pomaga organizacijam zaščititi svoje cilje, izboljšati varnost ter zagotoviti skladnost z zakonodajo.

C. ISO 31010 – Obvladovanje tveganj: Tehnike ocenjevanja tveganj

IEC 31010:2009 je mednarodni standard, ki ponuja smernice in orodja za oceno tveganj. Podpira širši okvir ISO 31000, ki se osredotoča na načela in smernice za obvladovanje tveganj. Standard IEC 31010 ponuja celovit pregled različnih tehnik, ki jih je mogoče uporabiti za prepoznavanje, analizo in vrednotenje tveganj znotraj organizacije.

Glavni cilji

- Podpora ISO 31000: Zagotavljanje podrobnih smernic o metodah ocenjevanja tveganj kot dopolnilo širšemu okviru obvladovanja tveganj.
- Izboljšanje odločanja: Izboljšanje sposobnosti organizacij za sprejemanje informiranih odločitev s pomočjo razumevanja in obvladovanja tveganj.
- Spodbujanje doslednosti: Standardizacija pristopa k ocenjevanju tveganj v različnih industrijah in sektorjih.

Struktura IEC 31010:2009

1. **Uvod**: Razloži namen, obseg in strukturo standarda ter poudarja njegov odnos do ISO 31000.
2. **Koncepti ocenjevanja tveganj**: Določa ključne izraze in koncepte, povezane z ocenjevanjem tveganj, kar zagotavlja skupno razumevanje.
3. **Proces ocenjevanja tveganj**: Opisuje korake v procesu ocenjevanja tveganj, vključno z identifikacijo, analizo in vrednotenjem tveganj.
4. **Tehnike ocenjevanja tveganj**: Ponuja podrobne opise različnih tehnik in orodij, ki jih je mogoče uporabiti v različnih fazah procesa ocenjevanja tveganj.

Proces ocenjevanja tveganj

1. **Identifikacija tveganj:**
   - Identificiranje potencialnih dogodkov, ki bi lahko vplivali na doseganje ciljev.
   - Tehnike: Možganska nevihta, Delphi tehnika, kontrolni seznami, HAZOP (Hazard and Operability Study / Študija nevarnosti in delovanja).
2. **Analiza tveganj:**
   - Razumevanje narave identificiranih tveganj in določanje njihovega potencialnega vpliva ter verjetnosti.
   - Tehnike: SWOT analiza (prednosti, slabosti, priložnosti, nevarnosti), FMEA (Failure Modes and Effects Analysis / Analiza načinov odpovedi in učinkov), analiza drevesa napak, analiza drevesa dogodkov.
3. **Vrednotenje tveganj:**
   - Primerjava rezultatov analize tveganj z merili tveganja, da se določi pomen tveganj.
   - Tehnike: Matrika tveganj, analiza stroškov in koristi, večkriterijska analiza odločanja.

Tehnike za ocenjevanje tveganj

IEC 31010:2009 navaja številne tehnike, ki so primerne za različne vrste tveganj in kontekste. Nekatere ključne tehnike vključujejo:

1. **Možganska nevihta:**
   - Sodelovalna tehnika za ustvarjanje idej in prepoznavanje tveganj.
   - Prednosti: Spodbuja ustvarjalnost in različne poglede.
   - Slabosti: Brez ustreznega vodenja lahko postane neosredotočena.
2. **Delphi tehnika:**
   - Uporablja vrsto vprašalnikov za zbiranje mnenj strokovnjakov in doseganje soglasja o tveganju.
   - Prednosti: Strukturirana in sistematična.
   - Slabosti: Časovno zahtevna in zahteva sodelovanje strokovnjakov.
3. **Kontrolni seznami:**
   - Uporablja vnaprej določene sezname potencialnih tveganj na podlagi preteklih izkušenj in industrijskih standardov.
   - Prednosti: Enostavna in hitra.
   - Slabosti: Morda ne zajame edinstvenih ali novih tveganj.
4. **HAZOP (Hazard and operability study):**
   - Sistematična tehnika za prepoznavanje in ocenjevanje potencialnih nevarnosti v procesih.
   - Prednosti: Temeljita in podrobna.
   - Slabosti: Zahtevna glede virov.
5. **SWOT analiza:**
   - Identificira notranje prednosti in slabosti, ter zunanje priložnosti in nevarnosti.
   - Prednosti: Celovit pogled na strateški položaj organizacije.
   - Slabosti: Lahko je subjektivna.
6. **FMEA (Failure Modes and Effects Analysis):**
   - Analizira potencialne načine odpovedi in njihove vplive na sisteme ali procese.
   - Prednosti: Preventivni pristop.
   - Slabosti: Lahko je kompleksna in podrobna.
7. **Analiza drevesa napak:**
   - Grafična tehnika za prepoznavanje osnovnih vzrokov odpovedi sistema.
   - Prednosti: Vizualna in sistematična.
   - Slabosti: Zahteva strokovno znanje za izdelavo drevesa napak.

8. **Analiza drevesa dogodkov:**
    - Ocenjuje izide začetnih dogodkov s pomočjo drevesnega diagrama.
    - Prednosti: Jasna vizualizacija zaporedja dogodkov.
    - Slabosti: Lahko postane kompleksna z več vejami dogodkov.

Upoštevanje pri implementaciji

- **Kontekst in obseg**: Izbira ustreznih tehnik ocenjevanja tveganj mora upoštevati specifičen kontekst organizacije in obseg obvladovanja tveganj.
- **Strokovnost in viri**: Učinkovito ocenjevanje tveganj zahteva zadostno strokovnost, vire in vključenost deležnikov.
- **Nenehno izboljševanje**: Ocenjevanje tveganj je stalen proces, organizacije pa naj redno pregledajo in posodobijo svoje tehnike ter prakse ocenjevanja tveganj.

IEC 31010:2009 je ključni standard za organizacije, ki želijo izboljšati svoje procese ocenjevanja tveganj. Z zagotavljanjem celovitega nabora tehnik pomaga organizacijam sistematično identificirati, analizirati in vrednotiti tveganja, kar podpira boljše odločanje ter obvladovanje tveganj.

D. Korelacija med standardi IEC 31010:2009 in ISO 27005

Pregled

IEC 31010:2009 in ISO 27005 sta dva pomembna standarda na področju obvladovanja tveganj. Medtem ko IEC 31010:2009 zagotavlja smernice za različne tehnike ocenjevanja tveganj je ISO 27005 specifično osredotočen na upravljanje tveganj informacijske varnosti znotraj okvira ISO/IEC 27001.

IEC 31010:2009

- **Namen**: Ponuja smernice za izbor in uporabo sistematičnih tehnik za oceno tveganj.
- **Uporaba**: Široka uporaba v različnih sektorjih za oceno vseh vrst tveganj.
- **Vsebina**: Vključuje številne tehnike, kot so možganska nevihta, Delphi tehnika, FMEA, SWOT analiza, analiza drevesa napak in dogodkov itd.

ISO 27005

- **Namen**: Zagotavlja smernice za upravljanje tveganj informacijske varnosti.
- **Uporaba**: Specifično za informacijsko varnost, podpira izvajanje ISO/IEC 27001.
- **Vsebina**: Poudarja identifikacijo, analizo, vrednotenje in obravnavo tveganj informacijske varnosti.

Korelacija in dopolnjevanje

1. **Okvir in pristop:**
    - **IEC 31010:2009** ponuja širok spekter tehnik, ki se lahko uporabijo v katerem koli kontekstu upravljanja tveganj.
    - **ISO 27005** uporabi te tehnike v specifičnem kontekstu informacijske varnosti, s poudarkom na zaščiti zaupnosti, celovitosti in razpoložljivosti informacij.
2. **Identifikacija tveganj:**
    - **ISO 27005** sledi strukturi ISO/IEC 27001 za identifikacijo groženj in ranljivosti.
    - **IEC 31010:2009** ponuja različne metode, kot so možganska nevihta in Delphi tehnika, ki se lahko uporabijo za identifikacijo tveganj v kontekstu informacijske varnosti, kar dopolnjuje pristop iz ISO 27005.
3. **Analiza tveganj:**
    - **ISO 27005** predlaga analizo verjetnosti in vpliva tveganj na informacijsko varnost.
    - **IEC 31010:2009** ponuja orodja, kot so FMEA in analiza drevesa napak, ki se lahko uporabijo za podrobnejšo analizo teh tveganj.
4. **Vrednotenje tveganj:**
    - **ISO 27005** poudarja primerjavo analiziranih tveganj z merili za sprejemljivost tveganj.

- **IEC 31010:2009** nudi tehnike, kot so SWOT analiza in večkriterijska analiza odločanja, za vrednotenje tveganj ter pomoč pri odločanju.

5. **Obravnava tveganj:**

   - **ISO 27005** ponuja strategije za obvladovanje tveganj, kot so zmanjšanje, prenos, sprejemanje ali izogibanje tveganjem.

   - **IEC 31010:2009** daje širši nabor tehnik, ki jih lahko uporabimo pri oblikovanju strategij za obravnavo tveganj.

Sinergija med standardi

- **Dopolnjevanje tehnik**: ISO 27005 se zanaša na smernice in tehnike iz IEC 31010:2009 za izvajanje svojih korakov ocenjevanja tveganj. Kombinacija teh standardov omogoča organizacijam celovit in strukturiran pristop k upravljanju tveganj informacijske varnosti.

- **Prilagodljivost in uporabnost**: Uporaba tehnik iz IEC 31010:2009 omogoča prilagoditev in izboljšanje procesa upravljanja tveganj, opisanega v ISO 27005, glede na specifične potrebe ter kontekst organizacije.

- **Izboljšanje zmogljivosti upravljanja tveganj**: Integracija teh dveh standardov krepi zmogljivost organizacije za prepoznavanje, analiziranje, vrednotenje in obvladovanje tveganj na sistematičen ter celovit način.

Korelacija med IEC 31010:2009 in ISO 27005 zagotavlja organizacijam robusten okvir za obvladovanje tveganj. IEC 31010:2009 ponuja širok spekter tehnik, ki jih ISO 27005 vključuje v svoj specifični kontekst informacijske varnosti, kar omogoča organizacijam, da učinkovito prepoznajo in obvladujejo tveganja ter zaščitijo svoje informacijske vire.

E. Metodologija OCTAVE (Operativno kritična ocena groženj, sredstev in ranljivosti)

Metodologija OCTAVE je celovit okvir, zasnovan za oceno in načrtovanje informacijske varnosti na podlagi tveganj. Omogoča organizacijam prepoznavanje, prednostno obravnavo in upravljanje tveganj informacijske varnosti. OCTAVE je še posebej primeren za velike organizacije, vendar ga je mogoče prilagoditi tudi za manjše entitete.

Ključne komponente OCTAVE

1. **Organizacijski pogled (Faza 1)**

   - **Cilj**: Identificirati ključna sredstva in varnostne zahteve, povezane z njimi.

   - **Dejavnost**i:

     - **Identifikacija ključnih sredstev**: Določiti, katere informacije in sistemi so ključnega pomena za organizacijo.

     - **Prepoznavanje groženj**: Prepoznati potencialne grožnje tem sredstvom iz notranjih in zunanjih virov.

     - **Določanje varnostnih zahtev**: Ugotoviti varnostne potrebe in pričakovanja za vsako ključno sredstvo.

2. **Tehnološki pogled (Faza 2)**

   - **Cilj**: Oceniti infrastrukturo in identificirati ranljivosti, ki bi lahko vplivale na ključna sredstva.

   - **Dejavnost**i:

     - **Identifikacija ključnih komponent**: Narediti seznam ključnih komponent IT infrastrukture, ki podpirajo ključna sredstva.

     - **Ocenjevanje ranljivosti**: Oceniti ranljivosti teh komponent, vključno z ranljivostmi programske opreme, strojne opreme in omrežja.

     - **Analiza tehnoloških tveganj**: Ugotoviti potencialna tveganja, povezana z identificiranimi ranljivostmi.

3. **Strateški pogled (Faza 3)**

   - **Cilj:** Razviti načrt za zmanjševanje tveganj in strategijo za obravnavo ugotovljenih tveganj.

- **Dejavnosti**:
  - **Dajanje prednosti tveganjem**: Razvrstiti ugotovljena tveganja glede na njihov potencialni vpliv in verjetnost.
  - **Razvoj strategij za zmanjševanje tveganj**: Ustvariti strategije za zmanjšanje ali upravljanje najvišjih tveganj.
  - **Načrt implementacije**: Pripraviti načrt za izvajanje teh strategij, vključno z dodelitvijo odgovornosti in časovnimi roki.

Podrobni koraki metodologije

1. **Priprava**
   - **Zbiranje ekipe**: Oblikovati večfunkcionalno ekipo s predstavniki iz različnih delov organizacije.
   - **Določitev obsega**: Jasno opredeliti obseg ocenjevanja, vključno s sredstvi, sistemi in procesi, ki jih je treba oceniti.
2. **Identifikacija in vrednotenje sredstev**
   - **Inventar sredstev**: Narediti podroben popis vseh ključnih sredstev v opredeljenem obsegu.
   - **Vrednotenje sredstev**: Oceniti vrednost vsakega sredstva glede na njegov pomen za delovanje in cilje organizacije.
3. **Prepoznavanje groženj**
   - **Identifikacija virov groženj:** Določiti potencialne vire groženj, kot so kibernetski napadi, notranje grožnje, naravne nesreče itd.
   - **Značilnosti groženj**: Opisati naravo vsake grožnje, vključno z njenim potencialnim vplivom in verjetnostjo.
4. **Identifikacija ranljivosti**
   - **Tehnične ocene**: Uporabiti orodja in tehnike, kot so skeniranje ranljivosti, penetracijsko testiranje ter pregled kode za identifikacijo slabosti.
   - **Dokumentacija ranljivosti**: Zabeležiti vse ugotovljene ranljivosti, pri čemer je treba upoštevati njihovo resnost in potencialni vpliv.
5. **Analiza tveganj**
   - **Kombinacija groženj in ranljivosti**: Analizirati, kako lahko določene grožnje izkoristijo ugotovljene ranljivosti za vpliv na ključna sredstva.
   - **Ocenjevanje vpliva in verjetnosti**: Oceniti potencialni vpliv in verjetnost vsakega scenarija tveganja.
6. **Prednostna obravnava tveganj**
   - **Razvrščanje tveganj**: Dati prednost tveganjem glede na njihov ocenjeni vpliv in verjetnost.
   - **Osredotočanje na najpomembnejša tveganja**: Usmeriti pozornost in vire na najpomembnejša tveganja.
7. **Načrtovanje zmanjševanja tveganj**
   - **Razvoj ukrepov za zmanjšanje**: Oblikovati strategije za zmanjšanje ali upravljanje prednostnih tveganj. To lahko vključuje uvedbo novih varnostnih kontrol, izboljšanje obstoječih ukrepov ali razvoj načrtov za nepredvidene dogodke.
   - **Dodeljevanje odgovornosti**: Dodeliti odgovornosti za izvajanje ukrepov za zmanjšanje tveganj določenim posameznikom ali ekipam.
   - **Ustvarjanje časovnega načrta**: Vzpostaviti časovni načrt za izvajanje strategij zmanjševanja tveganj.
8. **Implementacija in spremljanje**
   - **Izvajanje ukrepov za zmanjšanje tveganj**: Izvesti načrtovane dejavnosti za zmanjšanje tveganj.
   - **Spremljanje učinkovitosti**: Nenehno spremljati učinkovitost izvedenih ukrepov in jih po potrebi prilagajati.

- **Pregled in posodabljanje**: Periodično pregledovati oceno tveganj in strategije zmanjševanja, da se zagotovi njihova ustreznost ter učinkovitost.

Prednosti OCTAVE

- **Celovit pristop**: Upošteva tako organizacijske kot tehnološke perspektive.
- **Prilagodljivost**: Lahko se prilagodi organizacijam različnih velikosti in kompleksnosti.
- **Vključevanje deležnikov**: Vključuje različne dele organizacije, kar zagotavlja celovito razumevanje tveganj in njihovih vplivov.
- **Osredotočenost na ključna sredstva**: Daje prednost prizadevanjem za zaščito sredstev, ki so najpomembnejša za poslanstvo in delovanje organizacije.

Metodologija OCTAVE zagotavlja strukturiran pristop k prepoznavanju in upravljanju tveganj informacijske varnosti. S tem, ko združuje organizacijski kontekst s tehnološkimi ocenami, pomaga organizacijam razviti robustne varnostne strategije, ki ščitijo njihova ključna sredstva in zagotavljajo dolgoročno operativno odpornost.

F. Orodja za oceno tveganj

1. FAIR metodologija za ocenjevanje tveganj informacijske varnosti (Factor Analysis of Information Risk)

FAIR je metodologija za ocenjevanje tveganj informacijske varnosti, ki temelji na kvantitativnem pristopu. FAIR pomaga organizacijam razumeti, oceniti in meriti tveganja v smislu finančnih izgub.

- **Identifikacija in klasifikacija**: Identifikacija informacijskih sredstev in njihovih ranljivosti.
- **Ocena verjetnosti in vpliva**: Kvantitativna ocena verjetnosti groženj in potencialnega vpliva na sredstva.
- **Izračunavanje izgube**: Izračunavanje pričakovane letne izgube (ALE) na podlagi ocenjene verjetnosti in vpliva.

2. CRAMM (CCTA Risk Analysis and Management Method / Analiza tveganja in metoda upravljanja)

CRAMM je orodje za ocenjevanje tveganj, ki vključuje sistematičen pristop k analizi varnostnih tveganj in določanju ustreznih varnostnih ukrepov.

- **Faza 1: Ocena vrednosti sredstev**: Določanje vrednosti informacijskih sredstev in njihovih kritičnih značilnosti.
- **Faza 2: Identifikacija groženj in ranljivosti**: Identifikacija groženj in ranljivosti, ki lahko vplivajo na sredstva.
- **Faza 3: Analiza tveganj**: Kvantitativna ocena tveganj na podlagi identificiranih groženj in ranljivosti ter določanje ustreznih varnostnih ukrepov.

RMF je ključni okvir za upravljanje tveganj, ki omogoča organizacijam strukturiran in sistematičen pristop k obvladovanju tveganj informacijske varnosti. Orodja za oceno tveganj, kot sta FAIR in CRAMM, ponujajo različne metodologije za kvantitativno ter kvalitativno analizo tveganj, kar pomaga organizacijam pri sprejemanju informiranih odločitev glede varnostnih ukrepov.

Zaključek

V omenjenem poglavju smo vam poskušali prikazati okvirne zakonske zahteve na področju ocenjevanja tveganj in jih podpreti z dodatnimi informacijami možnih metodologij ter orodij, ki jih lahko uporabite pri tem zahtevnem procesu. Od učinkovite in predvsem realistične izvedbe ocenjevanja tveganj je v nadaljevanju korakov zagotavljanja SUVI ter tudi SUNP odvisna uporabnost takšnih analiz in podatkov, ki so lahko pomembna podlaga za načrtovanje investicij v organizaciji. Izpostaviti velja učinkovito in realno načrtovanje potrebnih

virov za ustrezno obvladovanje ter upravljanje z varnostnimi tveganji, in pomembnost vključenosti odgovornih oseb v organizaciji pri tem postopku.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO 31010:2019 : Risk management — Risk assessment techniques
- ISO 31000:2018: Risk management — Guidelines
- Čaleta, D. in drugi (2019) Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture, MORS-Ljubljana).
- Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov: Uradni list RS, št. 118/23: https://pisrs.si/pregledPredpisa?id=URED8925&utm=
- Urad Vlade RS za informacijsko varnost https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/
- Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-10 in 49/23): https://pisrs.si/pregledPredpisa?id=ZAKO7707&utm_

Poglavje 13
Napotki za pripravo ukrepov za obvladovanje tveganj

POVZETEK

Priprava ukrepov za obvladovanje tveganj je ključen proces za zagotavljanje varnosti informacijskih sistemov, podatkov in poslovnih procesov v organizaciji. Poglavje obravnava celovit pristop k identifikaciji, analizi in obvladovanju tveganj, s poudarkom na integraciji organizacijskih, človeških, fizičnih in tehnoloških kontrol. Te kontrole zagotavljajo temelje za razvoj učinkovitih varnostnih strategij, prilagojenih specifičnim potrebam organizacije.

Poseben poudarek je namenjen vzpostavitvi organizacijskih kontrol, kot so jasne politike, opredeljene odgovornosti in upravljanje dostopov, ki omogočajo strukturiran pristop k obvladovanju tveganj. Človeške kontrole so ključne za usposabljanje in ozaveščanje zaposlenih, saj človeški dejavnik pogosto predstavlja največje tveganje. Fizične kontrole obravnavajo zaščito kritičnih prostorov in opreme, medtem ko tehnološke kontrole pokrivajo tehnične vidike, kot so zaščita omrežij, šifriranje in obvladovanje ranljivosti.

Ključne točke:

- Organizacijske kontrole
- Človeške kontrole
- Fizične kontrole
- Tehnološke kontrole
- Identifikacija tveganj
- Odgovornosti in postopki
- Preventivni ukrepi
- Odziv na incidente
- Učenje iz incidentov.

1. Uvod v obvladovanje tveganj

Za uspešno obvladovanje tveganj v organizaciji je nujno vzpostaviti celovit sistem nadzora, ki zajema vse ključne kontrole, opisane v standardu ISO/IEC 27002. Obvladovanje tveganj vključuje identifikacijo, analizo in odziv na varnostna tveganja, ki lahko ogrozijo informacijske sisteme, podatke ali poslovne procese organizacije. Da bi bilo obvladovanje tveganj celovito in učinkovito, je treba uvesti različne tipe kontrol, ki pokrivajo organizacijske, človeške, fizične ter tehnološke vidike informacijske varnosti.

V nadaljevanju so predstavljene glavne vrste kontrol, ki jih je treba vzpostaviti za celovito obvladovanje tveganj v organizaciji, skupaj z nekaterimi ključnimi ukrepi, ki določajo konkretne postopke znotraj teh kontrol. Nabor kontrol, ključnih za posamezno organizacijo, pa mora določiti vsaka organizacija z ozirom na svoje potrebe in ključne procese poslovanja.

Organizacijske kontrole

Organizacijske kontrole so osnova za vzpostavitev učinkovitih politik in procesov, ki urejajo informacijsko varnost na ravni celotne organizacije. Te kontrole zagotavljajo jasne odgovornosti, postopke in so del standarda za upravljanje z informacijamiter tveganji. Med ključnimi organizacijskimi kontrolami, ki jih določa standard ISO 27002, so (za podrobnejše poznavanje tematike, je treba pregledati celoten nabor kontrol v standardu):

- **Politike za informacijsko varnost:** Uvedba celovitih varnostnih politik, ki opredeljujejo cilje in smernice za varovanje informacij v organizaciji.
- **Vloge in odgovornosti za informacijsko varnost:** Določitev odgovornih oseb in oddelkov za izvajanje varnostnih politik ter postopkov.
- **Razmejevanje nalog:** Zagotavljanje, da so naloge, ki lahko vodijo do konfliktov interesov, razdeljene med različne osebe ali oddelke.
- **Upravljanje odgovornosti:** Jasna opredelitev odgovornosti vodstva pri zagotavljanju, da so varnostne politike ustrezno izvajane in nadzorovane.
- **Povezovanje z organi in interesnimi skupinami:** Vzpostavitev stikov z zunanjimi organi in strokovnimi skupinami, ki lahko nudijo podporo pri obvladovanju varnostnih incidentov ali groženj.
- **Obveščanje o grožnjah:** Zbiranje in analiziranje informacij o potencialnih grožnjah za boljšo zaščito pred varnostnimi incidenti.
- **Varnost v projektih:** Zagotavljanje, da se varnostni vidiki vključijo že v fazi načrtovanja projektov, zlasti pri uvajanju novih tehnologij ali sistemov.
- **Inventarizacija informacijskih sredstev:** Vzpostavitev natančnega inventarja vseh informacij in povezanih sredstev, ki so pomembna za delovanje organizacije.

Človeške kontrole

Človeške kontrole se osredotočajo na varnostne ukrepe, ki vključujejo zaposlene in druge osebe, povezane z organizacijo. Vključujejo ukrepe za usposabljanje, preverjanje in zagotavljanje, da zaposleni delujejo skladno z varnostnimi politikami. Ključne človeške kontrole so:

- **Preverjanje zaposlenih:** Izvajanje preverjanj preteklosti novih zaposlenih, da se zagotovi, da nimajo zgodovine, ki bi lahko predstavljala varnostno tveganje.
- **Pogoji zaposlitve:** Zagotovitev, da so varnostne zahteve jasno vključene v pogodbe o zaposlitvi.
- **Ozaveščanje in usposabljanje o varnosti:** Redna usposabljanja in izobraževanja zaposlenih glede varnostnih postopkov ter prepoznavanja varnostnih groženj.
- **Disciplinarni postopki:** Vzpostavitev jasnih pravil glede disciplinskih ukrepov v primeru kršenja varnostnih pravil.

- **Odgovornosti po prenehanju delovnega razmerja:** Zagotovitev, da zaposleni po prenehanju delovnega razmerja nimajo več dostopa do občutljivih informacij in sistemov.
- **Pogodbe o zaupnosti:** Vsi zaposleni in pogodbeniki morajo podpisati pogodbe o zaupnosti, da bi preprečili nepooblaščeno razkritje občutljivih informacij.

Fizične kontrole

Fizične kontrole se nanašajo na zaščito fizičnih prostorov in opreme pred nepooblaščenim dostopom, poškodbami ali uničenjem. Te kontrole vključujejo ukrepe za omejitev fizičnega dostopa do kritičnih območij in zagotovitev, da so vsa informacijska sredstva ustrezno zaščitena. Ključne fizične kontrole vključujejo:

- **Fizični varnostni perimetri:** Vzpostavitev varnostnih perimetrov okrog objektov in območij, ki vsebujejo občutljive informacije ali opremo.
- **Nadzor dostopa v prostore:** Omejevanje dostopa do prostorov na podlagi identifikacijskih metod, kot so kartice za dostop, biometrija ipd.
- **Zavarovanje pisarn, prostorov in objektov:** Fizično varovanje prostorov s ključavnicami, alarmnimi sistemi in drugimi varnostnimi ukrepi.
- **Varovanje pred fizičnimi in okoljskimi grožnjami:** Ukrepi za zaščito pred nevarnostmi, kot so požari, poplave ali druge naravne nesreče.
- **Politika čiste mize in zaslona:** Zaposleni morajo zagotoviti, da so mize vedno pospravljene, in da so zasloni zaklenjeni, ko niso v uporabi.

Tehnološke kontrole

Tehnološke kontrole zajemajo ukrepe, povezane z zaščito informacijskih sistemov, omrežij in podatkov. Te kontrole vključujejo tako preventivne kot reaktivne ukrepe za zagotovitev, da so informacijski sistemi zaščiteni pred tehničnimi ranljivostmi in kibernetskimi grožnjami. Ključne tehnološke kontrole so:

- **Uporabniške naprave:** Zagotavljanje varnosti vseh končnih uporabniških naprav, kot so prenosni računalniki, pametni telefoni in tablice.
- **Pravice privilegiranega dostopa:** Ustrezno upravljanje privilegiranih uporabniških računov, ki imajo večji dostop do sistemov.
- **Zaščita pred zlonamerno programsko opremo:** Vzpostavitev zaščite pred virusi, trojanskimi konji in drugo zlonamerno programsko opremo.
- **Upravljanje tehničnih ranljivosti:** Redno preverjanje in posodabljanje sistemov za odpravljanje ranljivosti.
- **Varnost omrežja:** Uvedba varnostnih ukrepov, kot so požarni zidovi in sistemi za zaznavanje vdora, za zaščito omrežij pred zunanjimi napadi.
- **Uporaba kriptografije:** Zavarovanje občutljivih podatkov z uporabo kriptografskih metod, kot sta šifriranje in digitalni podpisi.

2. Identifikacija tveganj

Proces identifikacije tveganj je osnova za vzpostavitev učinkovitega sistema obvladovanja tveganj. Identifikacija tveganj zajema prepoznavanje vseh možnih groženj, ki lahko vplivajo na informacijske sisteme, procese in poslovanje organizacije. Ta proces se mora začeti že v fazi načrtovanja varnostnih politik, saj je učinkovita identifikacija tveganj ključna za ustrezno zaščito organizacijskih virov. Organizacije, ki zanemarjajo ta korak, se pogosto soočajo z nepričakovanimi incidenti, katerih vpliv je lahko zelo negativen.

Identifikacija tveganj se ne sme omejevati zgolj na tehnične vidike varnosti. Poleg tehničnih ranljivosti, kot so šibkosti v programski opremi ali nezadostno zavarovani sistemi, je treba upoštevati tudi človeški dejavnik, ki pogosto predstavlja največje tveganje. Zaposleni, ki niso dovolj ozaveščeni o varnostnih praksah

in kulturi, lahko nehote povzročijo varnostne vrzeli, kar napadalcem omogoča lažji dostop do informacijskih virov. Za podrobnejše informacije o obvladovanju teh tveganj si lahko ogledate poglavja 13, 14 in 15.

Pri identifikaciji tveganj je ključno, da organizacija vzpostavi učinkovit proces za oceno verjetnosti, s katero se lahko določeno tveganje materializira. Na primer, tveganje za kibernetski napad je v določeni industriji morda zelo visoko, medtem ko je v drugih sektorjih bolj verjetno, da bodo informacije ogrožene zaradi notranjih napak ali neustreznega upravljanja dostopa do podatkov.

Ključni koraki v procesu identifikacije tveganj:

- **Identifikacija virov tveganj:** Viri tveganj lahko vključujejo zunanje grožnje (napadalci, naravne nesreče) in notranje ranljivosti (napake v sistemih, človeške napake).
- **Ocenjevanje resnosti tveganj:** Vsako identificirano tveganje je treba oceniti glede na njegovo verjetnost in morebitni vpliv na poslovanje.
- **Sistematična analiza tveganj:** Na podlagi ocene verjetnosti in vpliva organizacija določi, katera tveganja so najpomembnejša ter zahtevajo takojšnje ukrepanje.

Ena izmed največjih napak, ki jih lahko organizacija naredi pri upravljanju tveganj, je podcenjevanje določenih groženj, še posebno tistih, ki na prvi pogled niso tako očitne. Zato je priporočljivo, da se v proces identifikacije vključijo strokovnjaki z različnih področij – od IT strokovnjakov do vodij poslovnih procesov. Sodelovanje različnih oddelkov in nivojev v organizaciji omogoča bolj celovito prepoznavanje tveganj.

3. Vzpostavitev odgovornosti in postopkov

Vzpostavitev jasnih odgovornosti in postopkov za obvladovanje tveganj je temelj učinkovitosti varnostnega sistema organizacije. Vodstvo mora jasno določiti odgovornosti posameznih oddelkov in zaposlenih, da bi zagotovili hiter ter ustrezen odziv na varnostne incidente. Brez natančno določenih vlog in nalog lahko pride do zamud pri ukrepanju, kar povečuje možnost škode.

Organizacija mora začeti s pripravo natančnega načrta, ki opredeljuje odgovornosti za ključne naloge, kot so spremljanje tveganj, prijava incidentov, izvajanje zaščitnih ukrepov in poročanje o napredku pri varovanju informacijskih virov. Ta načrt naj vključuje tudi postopke za redno preverjanje izvajanja varnostnih politik ter oceno uspešnosti ukrepov.

Jasno opredeljene odgovornosti morajo zajemati vse ravni organizacije. Na strateški ravni mora biti vodstvo odgovorno za sprejemanje ključnih odločitev glede upravljanja tveganj, vključno z razporejanjem proračuna za varnostne ukrepe in odobritvijo strateških pobud. Na operativni ravni pa morajo biti IT strokovnjaki in drugi zaposleni, ki so neposredno vključeni v obvladovanje tveganj, zadolženi za tehnične rešitve, kot so izvajanje popravkov, spremljanje sistemov ter izvajanje varnostnih preverjanj.

Postopki vzpostavitve odgovornosti vključujejo:

- **Vzpostavitev jasnih komunikacijskih poti:** Pomembno je, da vsi zaposleni vedo, kdo je odgovoren za kaj in kako komunicirati v primeru incidentov.
- **Redno preverjanje izvajanja postopkov:** Organizacije morajo vzpostaviti sistem za nadzor izvajanja varnostnih politik, da zagotovijo, da so postopki v skladu s predpisi in/ali standardi.
- **Prilagajanje postopkov glede na nove grožnje:** Glede na razvoj tehnologij in novih varnostnih tveganj morajo organizacije redno prilagajati oziroma posodabljati svoje postopke za obvladovanje tveganj.

Tako vzpostavljeni postopki omogočajo hitro odzivanje na morebitne varnostne incidente, zmanjšujejo tveganje napačnega upravljanja in zagotavljajo večjo učinkovitost varnostnega sistema.

4. Načrtovanje ukrepov za obvladovanje tveganj

Načrtovanje ukrepov za obvladovanje tveganj je ključnega pomena za uspešno obvladovanje incidentov in zmanjšanje njihovega vpliva na organizacijo. To zahteva skrbno preučitev vseh potencialnih tveganj, s katerimi se lahko organizacija sooči, in pripravo načrta, ki predvideva odziv na vsak scenarij.

Proces načrtovanja se začne z oceno tveganj, ki jih je organizacija identificirala v prejšnjih fazah. Na podlagi te ocene mora organizacija razviti strategije, ki vključujejo tako preventivne ukrepe kot tudi načrte za odzivanje na incidente. Načrtovanje ukrepov vključuje tako tehnične rešitve kot tudi organizacijske in procesne ukrepe.

Preventivni ukrepi vključujejo vzpostavitev varnostnih kontrol, kot so omejevanje dostopa do kritičnih informacij, redno preverjanje sistemov in vzpostavitev varnostnih politik, ki zmanjšujejo verjetnost nastanka incidentov. Načrti za odziv na incidente pa vključujejo postopke za hitro zaznavanje, obvladovanje in obnavljanje po incidentih.

Načrtovanje mora vključevati tudi vzpostavitev postopkov za redno spremljanje in posodabljanje varnostnih politik. To pomeni, da se organizacija ne sme zadovoljiti s trenutno varnostno postavitvijo, ampak mora nenehno prilagajati svoje varnostne ukrepe glede na nove grožnje in tehnologije. V tem kontekstu ima pomembno vlogo tudi izobraževanje zaposlenih, ki morajo biti redno obveščeni o spremembah v varnostnih politikah.

5. Beleženje in poročanje o incidentih

Beleženje in poročanje o varnostnih incidentih predstavlja ključen vidik uspešnega obvladovanja tveganj. Varnostni incidenti se lahko zgodijo kadarkoli in lahko vključujejo širok spekter dogodkov, od manjših kršitev varnosti do resnih napadov, ki lahko ogrozijo celotno organizacijo. V tem kontekstu je pomembno, da organizacija vzpostavi sistematičen pristop k beleženju vseh dogodkov, povezanih z incidenti, saj to omogoča natančno analizo in oceno tveganj ter načrtovanje ukrepov za preprečevanje podobnih dogodkov v prihodnosti. Za več informacij si oglejte poglavje 23.

Proces beleženja vključuje zapisovanje vseh pomembnih informacij o incidentu, kot so datum in čas, vrsta incidenta, prizadeti sistemi, vpletene osebe ter odziv organizacije. Podrobno beleženje je bistveno ne le za notranje analize, temveč tudi za poročanje zunanjim deležnikom, kot so regulatorji ali stranke, ki so lahko prizadete zaradi incidenta.

Osnovni elementi beleženja incidentov vključujejo:

- **Identifikacija incidenta:** V tem koraku se zabeležijo osnovni podatki o tem, kdaj je bil incident zaznan, katera informacijska sredstva so bila prizadeta in kakšne so bile prve zaznane posledice.
- **Odziv in ukrepanje:** Pomembno je dokumentirati, kakšni so bili prvi odzivi na incident, kateri ukrepi so bili sprejeti in kdo je bil odgovoren za ukrepanje.
- **Ocena škode:** Beleženje mora vključevati oceno vpliva incidenta, vključno s finančnimi in operativnimi posledicami.
- **Popravni ukrepi:** V zadnji fazi je treba dokumentirati, kakšni so bili popravni ukrepi, ki jih je organizacija sprejela, da bi preprečila prihodnje podobne dogodke.

Poročanje o incidentih je prav tako ključno, saj omogoča pravočasno obveščanje vseh ustreznih deležnikov. Notranje poročanje zagotavlja, da so vsi vpleteni oddelki obveščeni in pripravljeni na nadaljnje ukrepanje. Zunanje poročanje je običajno potrebno v primeru večjih incidentov, kjer je treba obvestiti regulatorje, stranke ali partnerje. Poročanje mora biti natančno in podprto z vsemi ustreznimi podatki, saj lahko slabo poročanje povzroči nepotrebne zaplete ali pravne posledice.

Vse to poudarja pomembnost vzpostavitve jasnih postopkov za beleženje in poročanje, ki vključujejo tako tehnične kot organizacij-

ske vidike. Le s skrbno dokumentacijo lahko organizacija zagotoviti, da se bo iz preteklih incidentov kaj naučila in izboljšala svoje varnostne ukrepe.

6. Odziv na varnostne incidente

Odziv na varnostne incidente zahteva hitro, natančno in organizirano ukrepanje. Ključ do uspešnega odziva je, da ima organizacija vnaprej vzpostavljene jasne postopke in določene odgovorne osebe, ki omogočajo nemoten potek aktivnosti, ko se incident zgodi. Varnostni incidenti so lahko zelo različni po svoji naravi – od majhnih notranjih kršitev do velikih zunanjih napadov, kot so porazdeljena zavrnitev storitve (DDoS). napadi, izsiljevalski programi ali kraje podatkov. Ne glede na vrsto incidenta pa je ključnega pomena, da je odziv organizacije hiter in učinkovit, saj lahko vsak zamik poveča škodo organizaciji.

Odziv se začne z zgodnjim odkrivanjem incidenta, ki je odvisno od sposobnosti organizacije za spremljanje svojih sistemov. Dobro vzpostavljen nadzorni sistem lahko hitro zazna nenavadne aktivnosti, kar omogoča, da organizacija hitro ukrepa in omeji širjenje škode. Pomembno je tudi, da se incidenti ocenijo glede na njihov možen vpliv na sisteme in procese v organizaciji. Nekateri incidenti zahtevajo le manjše tehnične popravke, medtem ko so drugi resnejši in zahtevajo aktivacijo kriznih načrtov.

Ključni koraki v odzivu na varnostne incidente vključujejo:

- **Hitro zaznavanje in izolacija:** Ko je incident zaznan, je ključno hitro omejiti njegov vpliv. To lahko vključuje izklop prizadetih sistemov, omejitev dostopa do določenih podatkov ali celo začasno prekinitev določenih operacij.
- **Komunikacija znotraj in zunaj organizacije:** V primeru resnejših incidentov je zlasti pomembno, da so vsi ključni deležniki obveščeni. To vključuje notranje ekipe, ki so odgovorne za obvladovanje incidenta, pa tudi zunanje partnerje, regulatorje in stranke.
- **Forenzična analiza:** Po prvih odzivih je treba izvesti forenzično analizo, da se ugotovi vzrok incidenta. To vključuje pregled log datotek, analizo prometa in preverjanje ranljivosti, ki so bile izkoriščene.
- **Obnova in povrnitev sistemov:** Po tem, ko je incident zajezen in analiziran, je treba vzpostaviti sistem nazaj v normalno delovanje. To vključuje povrnitev podatkov iz varnostnih kopij, ponovno konfiguracijo sistemov in preverjanje, da so vse ranljivosti odpravljene.

Odziv na incidente ne vključuje samo tehničnih ukrepov, temveč tudi koordinacijo med različnimi oddelki in/ali zunanjimi deležniki. Prav tako je pomembno, da organizacija po zaključku incidenta izvede notranjo oceno svojih zmogljivosti za odzivanje, da ugotovi, ali so bili postopki učinkoviti, in kje so potrebne izboljšave.

7. Učenje iz incidentov

Učenje iz varnostnih incidentov je proces, ki omogoča organizacijam, da na podlagi preteklih izkušenj izboljšajo svoje varnostne politike in postopke. Po vsakem varnostnem incidentu bi morala organizacija opraviti temeljito analizo dogajanja, da prepozna šibke točke v svojih sistemih in operativnih postopkih. Učenje iz incidentov je ključnega pomena za izboljšanje pripravljenosti na prihodnje grožnje.

Organizacije, ki se učijo iz preteklih napak, so bolje pripravljene na nove izzive in lahko hitreje prilagodijo svoje varnostne strategije. To pomeni, da po vsakem incidentu poteka podrobna analiza, ki zajema vse faze dogodka – od prvega zaznavanja do končne obnovitve sistemov. Ta analiza omogoča prepoznavanje vzorcev, ki lahko kažejo na ponavljajoče se na-

pake ali ranljivosti, ki jih je treba odpraviti.

Poleg tega proces učenja iz incidentov vključuje tudi izmenjavo znanja med oddelki znotraj organizacije in/ali po potrebi s pogodbeni izvajalci, ki so lahko tudi del odzivanja na incidente. Tehnične ekipe, ki so neposredno vključene v obvladovanje incidentov, morajo svoje ugotovitve deliti z vodstvom in drugimi oddelki, da se zagotovi, da vsi razumejo vzroke ter posledice incidenta. Pomemben del tega procesa je tudi posodabljanje varnostnih politik na podlagi pridobljenih izkušenj.

Učenje iz incidentov vključuje:

- **Analizo vzrokov:** Prepoznavanje tehničnih in organizacijskih pomanjkljivosti, ki so omogočile incident, ter oblikovanje priporočil za izboljšave.
- **Pregled ukrepov:** Ocena učinkovitosti ukrepov, ki so bili sprejeti med incidentom, in ugotavljanje, ali so bili postopki dovolj hitri ter učinkoviti.
- **Prilagajanje varnostnih politik:** Na podlagi analize incidenta organizacija prilagodi svoje varnostne politike, da prepreči ponovitev podobnih dogodkov.

Na koncu je ključno, da se organizacija zave, da učenje iz incidentov ni enkraten dogodek, temveč stalna praksa. Incidenti se lahko ponavljajo, če se organizacija ne uči iz preteklih napak in ne prilagodi svojih varnostnih ukrepov ter postopkov. Zato je pomembno, da so vsi deležniki vključeni v ta proces, in da se pridobljeno znanje deli ter uporablja za stalno izboljševanje varnostnega sistema v organizaciji.

Viri:

- Čaleta, D. in drugi (2019) Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture, MORS-Ljubljana
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- Združenje bank Slovenije, Smernice upravljanja tveganj (2022): https://www.zbs-giz.si/wp-content/uploads/2023/01/SmerniceUpravljanjaTveganj_2022.pdf?utm
- Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-10 in 49/23): https://pisrs.si/pregledPredpisa?id=ZAKO7707&utm_

Poglavje 14
Napotki za pripravo ocene vpliva na poslovanja in ukrepov zagotavljanja neprekinjenega poslovanja (Business Impact Analysis - BIA)

POVZETEK

Ocena vpliva na poslovanje (BIA) je osnova za vzpostavitev robustnega sistema zagotavljanja neprekinjenega poslovanja ter varnosti informacij. Poglavje obravnava metodološki pristop k analizi vplivov motenj na ključne poslovne procese, vključuje korake za identifikacijo kritičnih funkcij ter poudarja pomen načrtovanja časovnih okvirov in analize odvisnosti. Proces vključuje sodelovanje ključnih deležnikov in upošteva najboljše prakse ter standard ISO 22301.

Ključne točke:

- Namen izdelave BIA
- Priprava in načrtovanje
- Zbiranje informacij
- Identifikacija kritičnih funkcij
- Analiza vplivov
- Vrednotenje časovnih okvirov
- Analiza odvisnosti
- Dokumentiranje rezultatov
- Pregled in potrditev
- Razvoj načrta za neprekinjenost poslovanja.

Izdelava ocene vpliva na poslovanje je eden izmed najbolj ključnih korakov pri izgradnji celovitega in na realnih temeljih postavljenega sistema zagotavljanja varnosti informacij ter predvsem zagotavljanja ustrezne neprekinjenosti delovanja tistih ključnih procesov in funkcij, ki so ključne za delovanje posamezne organizacije. Čeprav je ta korak v domeni procesa sistema upravljanja neprekinjenosti poslovanja (SUNP) je dejansko osnovni temelj za celovito pripravo varnostne dokumentacije in sistemskih ukrepov na področju zagotavljanja varnosti informacij.

Bistvenega pomena, da znaš v organizaciji jasno opredeliti točno določene metodološke korake, bistvene procese, tehnologije in sisteme, katerih nedelovanje ima največji negativni poslovni učinek na organizacijo.

Pomembno, da je metodologija v naprej jasno postavljena in so z njo seznanjeni vsi, ki bodo sodelovali pri procesu ocenjevanja vplivov na poslovanje organizacije. Za kvalitetno in realno oceno mora biti v proces vključen zelo širok krog ključnih vodstvenih kadrov v organizaciji. Največkrat je zelo priporočljivo, da posebej pri tem procesu pomagajo zunanji usposobljeni strokovnjaki, ki so sposobni korigirati izvajanje celotnega procesa in v določenih primerih neodvisno, jasneje pogledati na realnost izvedenih analiz. Dejstvo je sicer, da strokovnjaki znotraj organizacije najbolj podrobno poznajo svoje procese v organizacijah. Na drugi strani pa to lahko prinaša določene izzive s stališča nerealnosti ocen in favoriziranja svojega procesa, ki lahko prinese silosne pristope k ocenjevanju in s tega stališča izkrivljeno analizo. To lahko v nadaljevanju negativno vpliva na celotno izvedbo procesa ustreznega načrtovanja varnostnih ukrepov in potrebnih virov za zagotovitev le tega.

Za konec naj poudarimo še dva zelo pomembna dejavnika:

- Vse analize je treba ustrezno dokumentirati, kar omogoča, da se v vsakem trenutku v nadaljnjih fazah še vedno lahko vrnete v proces določitve BIA in spremenite ali dopolnite kakšne pomembne ugotovitve, ki se pokažejo v kasnejših fazah procesa.
- Prioritizacija je ključen moment, ki nam dejansko pomaga izluščiti tiste bistvene procese ali sisteme, njihov vpliv ima največji učinek na delovanje organizacije.

V nadaljevanju si oglejmo nekaj najpomembnejših korakov pri izdelavi ocene vpliva na poslovanja (BIA):

1. Namen same izdelave BIA

Metodologija izdelave BIA je ključna za prepoznavanje in vrednotenje vpliva, ki ga imajo motnje na poslovne funkcije organizacije. BIA omogoča razvoj učinkovitih strategij za neprekinjenost poslovanja in obnovo po motnjah. Tukaj je podrobno opisana metodologija za izvedbo BIA.

2. Koraki pri Izvedbi BIA

2.1 Priprava in načrtovanje

- Določitev ciljev: Opredelite glavne cilje BIA, kot so prepoznavanje kritičnih poslovnih funkcij, ocena vpliva motenj in določitev prednostnih nalog za obnovo.
- Obseg BIA: Določite obseg BIA, vključno z oddelki, procesi in sistemskimi viri, ki bodo vključeni v analizo.
- Sestava tima: Ustanovite tim za izvedbo BIA, ki vključuje predstavnike vseh ključnih poslovnih enot in strokovnjake za neprekinjenost poslovanja.

2.2 Zbiranje informacij

- Informacijska sredstva: Izvedite popis informacijskih sredstev, s katerimi se izvajajo procesi (strojna, programska oprema, podatkovne baze, drugi resursi). Sredstva se kategorizirajo po smiselnih sklopih (npr. vse končne naprave uporabnikov brez administratorskega dostopa, mobilni telefoni uporabnikov ...).

- Intervjuji: Izvedite strukturirane intervjuje z vodji poslovnih enot in ključnimi zaposlenimi za pridobitev vpogleda v poslovne procese ter njihovo kritičnost.
- Vprašalniki: Pripravite in distribuirajte vprašalnike za zbiranje podatkov o poslovnih funkcijah, vključno s potrebnimi viri ter vplivi motenj.
- Dokumentacija: Preglejte obstoječo dokumentacijo, kot so poslovni načrti, procesne mape in pretekli incidenti.

2.3 Identifikacija kritičnih poslovnih funkcij

- Seznam funkcij: Ustvarite izčrpen seznam vseh poslovnih funkcij in procesov znotraj organizacije.
- Kritičnost: Razvrstite funkcije glede na njihovo kritičnost, pri čemer upoštevate, kako pomembne so za doseganje poslovnih ciljev.

2.4 Analiza Vplivov

- Finančni vplivi: Ocenite finančne posledice motenj za vsako poslovno funkcijo, vključno z izgubo prihodkov, dodatnimi stroški in denarnimi kaznimi.
- Operativni vplivi: Ocenite operativne vplive, kot so izguba produktivnosti, motnje v dobavni verigi in zmanjšana kakovost storitev.
- Vplivi na ugled: Ocenite vpliv motenj na ugled organizacije, vključno z zaupanjem strank in skladnostjo z regulativnimi zahtevami.

2.5 Vrednotenje časovnih okvirov

- Maksimalni sprejemljivi čas neizpolnjevanja (maximum tolerable period of disruption - MTPD): Določite MTPD za vsako kritično funkcijo – največji čas, ki lahko preteče, preden je delovanje funkcije obnovljeno brez povzročanja nesprejemljive škode.
- Ciljni čas obnovitve (recovery time objective - RTO): Določite RTO – časovni okvir, v katerem je treba obnoviti funkcijo, da se prepreči nesprejemljiv vpliv na poslovanje.
- Ciljni čas za obnovo podatkov (recovery point objective - RPO): Določite RPO – največja količina podatkov, ki se lahko izgubi zaradi motnje.

2.6 Analiza odvisnosti

- Notranje odvisnosti: Prepoznajte odvisnosti med različnimi poslovnimi funkcijami znotraj organizacije.
- Zunanje odvisnosti: Prepoznajte odvisnosti od zunanjih dobaviteljev, partnerjev in storitev.

2.7 Dokumentiranje rezultatov

- Poročilo BIA: Pripravite podrobno poročilo o BIA, ki vključuje vse zbrane podatke, ocene vplivov in časovne okvire za obnovo.
- Vizualizacije: Ustvarite grafične prikaze, kot so tabele, grafikoni in diagrami za ponazoritev rezultatov BIA.

2.8 Pregled in potrditev

- Notranji pregled: Izvedite notranji pregled poročila BIA s strani ključnih deležnikov in vodstva.
- Potrditev: Pridobite formalno potrditev BIA s strani vodstva organizacije.

2.9 Razvoj načrta za neprekinjenosti poslovanja (BCP)

- Strategije za obnovo: Na podlagi rezultatov BIA razvijte strategije za obnovo kritičnih poslovnih funkcij.
- Postopki: Pripravite podrobne postopke za obnovo, vključno z viri in odgovornostmi.
- Testiranje: Redno testirajte BCP za preverjanje njegove učinkovitosti in prilagajanje glede na spremembe v poslovnem okolju.

Izdelava BIA je bistven korak v procesu zagotavljanja neprekinjenosti poslovanja. Metodologija, ki vključuje pripravo in načrtovanje, zbiranje informacij, identifikacijo kritičnih funkcij, analizo vplivov, vrednotenje časovnih okvirov, analizo odvisnosti, dokumentiranje rezultatov, pregled ter potrditev in razvoj načrta za neprekinjenost poslovanja, omogoča organizacijam, da se učinkovito pripravijo na motnje ter hitro obnovijo ključne poslovne funkcije.

S to metodologijo lahko organizacije vzpostavijo robusten okvir za oceno vpliva na poslovanje in načrtovanje neprekinjenosti poslovanja v skladu z najboljšimi praksami ter standardom ISO 22301.

Predstavljamo vam možen model vprašalnika, ki vas bo vodil skozi proces ocenjevanja posameznih identificiranih procesov znotraj BIA. Glede na poslovno dejavnost ali sektor vaše organizacije se lahko posamezni deli vprašalnika dopolnijo ali spremenijo, predvsem pri velikosti finančnih posledic, ki so značilne za vašo dejavnost. Okvir pa vseeno služi kot uporaben pripomoček pri učinkoviti in realni izvedbi BIA.

Shema 8: Vprašalnik za pridobitev podatkov za oceno vplivov prekinitev na poslovanje (vir: ICS)

VPRAŠALNIK ZA PRIDOBITEV PODATKOV ZA OCENO VPLIVOV PREKINITEV NA POSLOVANJE.	
Vprašalnik je namenjen zbiranju podatkov za kritične poslovne funkcije, ki podpirajo kritični poslovni proces.	
Poslovna funkcija:	
Kritični poslovni proces:	**Kontaktna oseba:**
Datum:	Štev**ilo zaposlenih v poslovni funkciji:**
SPLOŠNO	
Opis poslovne funkcije:	
Opredelite odvisnosti poslovne funkcije od drugih poslovnih procesov/funkcij podjetja, njihovih storitev ali izdelkov. Kako je od funkcije odvisen kritični poslovni proces? Kateri drugi procesi/funkcije so še odvisni od funkcije?	
Ocenite kolikšen je toleriran čas nedelovanja funkcije (čas, po preteku katerega se lahko pokažejo resne negativne posledice pri delovanju kritičnega poslovnega procesa).	

Ali je možno blaženje posledic prekinitve funkcije z ročnimi ali alternativnimi postopki? Katerimi? Ali je vpeljan dokumentiran rezervni postopek?
Ali v funkciji obstajajo točke ene napake, kjer je delovanje funkcije lahko prekinjeno z enim samim dogodkom (npr. odsotnost določenega zaposlenega, okvara dela opreme, nerazpoložljivost informacij)? Opišite. Navedite tudi pomembne podatke, ki obstajajo samo v eni kopiji.
Opredelite čase največje obremenjenosti funkcije (tudi dnevna oz. tedenska nihanja), če obstajajo, oziroma kdaj funkcija ni v obratovanju.
Ali bi bilo funkcijo možno izvajati s preusmeritvijo dela na druge oddelke organizacije? Katere?
Katere zakonske, pogodbene in druge obveznosti mora poslovna funkcija izpolnjevati v določenih intervalih oz. rokih? Katera poročila poslovanja so potrebna glede na zakonodajo ali poslovanje?
Ali imate s prekinitvijo ali grožnjo prekinitve poslovne funkcije že izkušnje? Kakšne?
ČASOVNI VPLIV

Vprašanje	1 dan	7 dni	14 dni	30 dni
1) Če bi prišlo do prekinitve poslovne funkcije za zgoraj navedeni čas, koliko bi potrebovali za okrevanje poslovne funkcije? A. Ogromno, B. veliko, C. malo, D. neznatno.				
☐ osebja				
☐ opreme				
☐ zalog				
☐ računalniških zmogljivosti				

1) Če bi prišlo do prekinitve poslovne funkcije za navedeni čas, koliko bi bilo treba ob ponovni vzpostavitvi za odpravo zamud? A. Zamud ne bi bilo mogoče nadoknaditi, B. zelo veliko dela, C. malo dela, D. zamude se ne bi poznale.				
2) Če bi prišlo do prekinitve poslovne funkcije in bi izgubili podatke zadnjega poslovanja za navedeni čas, kako bi označili to izgubo? A. Katastrofalna izguba, B. zelo opazna izguba, C. majhna izguba, D. neznatna izguba.				
3) Če bi prišlo do prekinitve poslovne funkcije za navedeni čas, kako bi to vplivalo na kritični poslovni proces, ki ga funkcija podpira? A. Katastrofalen vpliv, B. zelo opazen vpliv, C. majhen vpliv, D. neznaten vpliv.				
4) Če bi prišlo do prekinitve poslovne funkcije za navedeni čas, kolikšno škodo bi povzročil izpad? A. Velika (nad 200.000 EUR), B. srednja (100.000 - 200.000 EUR), C. majhna (od 50.000 – 100.000 EUR), D. ni neposredne finančne škode.				
5) Če bi prišlo do prekinitve poslovne funkcije za navedeni čas, do kakšnih zakonskih ali pogodbenih kazni bi lahko prišlo? A. Velike (nad 10.000 EUR), A. srednje (1.000 - 10.000 EUR), B. majhne (do 1.000 EUR), C. ni pravnih posledic.				

Viri:

- ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements

Poglavje 15
Napotki za krizno upravljanje in pripravo obnovitvenih načrtov

POVZETEK

Krizno upravljanje in priprava obnovitvenih načrtov sta ključna procesa, ki omogočata pravočasno in usklajeno odzivanje na krizne situacije ter zmanjšanje vpliva na delovanje organizacije. Smernice zajemajo vse ključne faze kriznega upravljanja, od priprave na možne krizne dogodke, prek hitrega in učinkovitega odzivanja, do postopne obnove normalnega delovanja. Poseben poudarek je na oblikovanju celovitih obnovitvenih načrtov, ki vključujejo tako strateške kot operativne vidike. Integracija standardov ISO 22301 in ISO 27031 omogoča vzpostavitev strukturiranega okvira, ki združuje poslovne potrebe in tehnične zahteve, kar povečuje odpornost organizacije proti različnim vrstam groženj, od naravnih nesreč do kibernetskih napadov.

Ključne točke:

- Faze kriznega upravljanja
- Komunikacijski načrt
- Vloge in odgovornosti
- Načrtovanje obnovitvenih procesov
- Testiranje in izboljšave
- Integracija standardov ISO 22301 in ISO 27031.

Uvod

Pričujoče poglavje prinaša pomembne informacije, vezane na razumevanje obsega kriznega upravljanja in ključne korake, ki jih obsega ta pomembni proces za zagotavljanje neprekinjenosti delovanja organizacij v primeru kriz. V nadaljevanju podrobno predstavlja ključne korake za pravilno pripravo oblik in procesov obnovitvenih načrtov, ki so pomembni za ukrepanje v času aktiviranja kriznega načrta. Na koncu pa podrobneje pojasnjuje integrativni pristop med dvema pomembnima standardoma ISO 22301 in ISO 27031, ki urejata področje neprekinjena poslovanja in bi zaradi napačnega razumevanja pri uporabnikih lahko prinesli določeno zmedo. Pomembno je zavedanje ustreznih integrativnih pristopov in upoštevanja posebnosti, ki jih predstavljajo vaše organizacije. Načrtovanje upravljanja kriznih dogodkov in načrtovanja ustreznega odzivanja je lahko učinkovito samo v primeru, da so bili izvedeni vsi predhodni koraki. V teh pa ima ključno mesto ustrezna ocena učinkov na poslovanje (BIA) in ustrezna analiza tveganj tako, da se res identificira tiste procese, ki so bistveni za zagotavljanje neprekinjenega delovanja posamezne organizacije.

NAPOTKI ZA KRIZNO UPRAVLJANJE

Krizno upravljanje je proces priprave, odzivanja in obnavljanja po izrednih dogodkih, ki lahko vplivajo na delovanje organizacije. Učinkovito krizno upravljanje pomaga organizacijam zmanjšati vpliv kriz in hitreje obnoviti normalno delovanje.

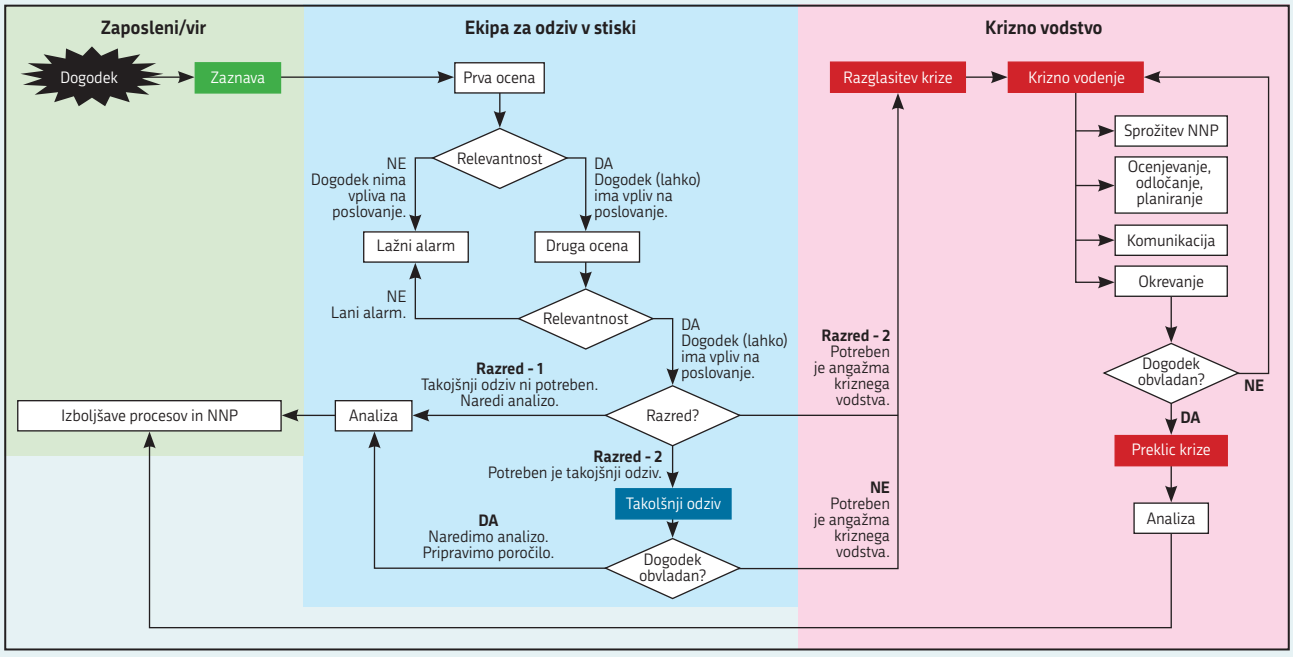
1. Faze kriznega upravljanja

Priprava:

- Analiza tveganj: Identificirajte potencialne grožnje in ranljivosti, ki bi lahko povzročile krizo v organizaciji.
- Načrtovanje: Razvijte krizne načrte, ki vključujejo postopke za odzivanje na različne vrste kriz/incidentov, določite vloge in odgovornosti ter vzpostavite komunikacijske strategije.
- Usposabljanje in ozaveščanje: Redno usposabljajte osebje o kriznih postopkih in povečajte njihovo ozaveščenost o potencialnih grožnjah.

Odzivanje:

- Aktiviranje kriznega načrta: Ob izbruhu krize takoj aktivirajte krizni načrt in obvestite ključne deležnike.



Shema 9: Upravljanje kriznih dogodkov v sistemu zagotavljanja neprekinjenega poslovanja (vir: ICS)

- Vzpostavitev kriznega tima: Sestavite krizni tim, ki bo koordiniral odzivanje na krizo.
- Komunikacija: Zagotovite jasno in pravočasno komunikacijo z notranjimi ter zunanjimi deležniki.
- Operativni ukrepi: Izvedite potrebne ukrepe za zaščito ljudi, premoženja in informacijskih virov.

Obnova:

- Ocena škode: Ocenite obseg škode in določite prednostne naloge za obnovo.
- Obnovitveni ukrepi: Izvedite ukrepe za obnovo kritičnih funkcij in sistemov.
- Analiza po krizi: Opravite analizo odzivanja na krizo in identificirajte priložnosti za izboljšanje.

Izboljšave:

- Pregled načrtov: Na podlagi pridobljenih izkušenj pregledujte in posodobite krizne načrte.
- Stalno usposabljanje: Nadaljujte z usposabljanjem osebja in organiziranjem vaj za preverjanje pripravljenosti.
- Izboljšave procesov: Implementirajte ugotovitve iz analiz in vaj v obstoječe postopke ter načrte.

2. Ključni elementi kriznega načrta

Komunikacijski načrt

- Notranja komunikacija: Vzpostavite jasne komunikacijske linije znotraj organizacije.
- Zunanja komunikacija: Razvijte strategije za obveščanje javnosti, strank, dobaviteljev in drugih deležnikov.

Vloga	Zadolžitve	Pooblastila
Krizni vodja	- Vodi in koordinira delovanje kriznega vodstva. - S svojimi odločitvami zagotavlja, da se bo lahko poslovanje podjetja uspešno nadaljevalo tudi v prihodnje. - Informira vodstvo podjetja o stanju krize.	- Razglasitev krize - Sprejem strateških odločitev glede odziva na krizo.
Koordinator	- Zagotavlja ustrezen in učinkovit odziv ekip. - Je osrednja koordinacijska točka za ekipe. - Zagotavlja učinkovito komuniciranje med ekipami in kriznim vodstvom.	- V nujnih primerih: Vodenje delovanje kriznega vodstva. - Dajanje informacij ekipam. - Analiziranje delovanja ekip in uvajanje dodatnih ukrepov.
Informator	- Zbira in beleži ključne informacije, potrebne za vodenje krize. - Zagotavlja ažurne in točne informacije glede na trenutno stanje krize. - Skrbi za prikaz odnosov in informacij med ključnimi dogodki. - Zagotavlja, da so informacije ekipi na voljo v jasni in jedrnati obliki.	- Upravljanje z informacijskimi viri.
Koordinator za stike z javnostmi	- Zagotavlja komuniciranje z javnostmi (**zunanjimi in notranjimi**).	- Dajanje informacije za javnosti. - Aktiviranje stikov z javnostmi. - Izbira informacij za različne javnosti.
Logistik	- Vzpostavi in upravlja krizni štab (storitve IT, električna energija, ogrevanje in razsvetljava, oprema, pisalne potrebščine, ipd.). - Skrbi za dobro počutje ekip (pijača, hrana, ipd.).	- Zagotavljanje vseh potrebnih virov za krizni štab in ekipe.
Specialisti (npr. pravna služba, varovanje, VZD)	- Na zahtevo kriznega vodstva zagotavljajo strokovno znanje in tehnično podporo. - Na svojem področju delujejo v skladu z razumevanjem širše slike v zvezi s kriznim dogajanjem.	- Koordiniranje ekip s svojega ekspertnega področja.

Shema 10: Krizno vodstvo in opis ključnih vlog ter pooblastil (vir: ICS)

- Medijska komunikacija: Pripravite izjave za medije in določite govorce za krizne situacije.

Vloge in odgovornosti

- Krizni tim: Določite člane kriznega tima in njihove vloge.
- Vodstvo: Vzpostavite jasne odgovornosti za odločanje in usmerjanje med krizo.
- Operativno osebje: Opredelite naloge operativnega osebja za odzivanje in obnovo.

Viri in oprema

- Zmogljivosti: Identificirajte potrebne vire in opremo za odzivanje na različne vrste kriz.
- Dostopnost: Zagotovite, da so viri in oprema dostopni ter pripravljeni za uporabo v vsakem trenutku.

Evakuacijski načrt

- Evakuacijske poti: Določite evakuacijske poti in zbirna mesta.
- Usposabljanje: Redno izvajajte vaje za evakuacijo in preverjanje evakuacijskih postopkov.

3. Vaje in testiranje

- Redne vaje: Organizirajte redne krizne vaje, da preverite učinkovitost kriznih načrtov.
- Simulacije: Izvajajte simulacije različnih kriznih scenarijev za izboljšanje pripravljenosti.
- Ocena uspešnosti: Po vsaki vaji ocenite uspešnost odzivanja in identificirajte priložnosti za izboljšanje.

Krizno upravljanje je bistvenega pomena za zagotavljanje odpornosti organizacije na različne vrste kriz. S pravilno pripravo, učinkovitim odzivanjem, hitro obnovo in nenehnimi izboljšavami lahko organizacije zmanjšajo vpliv kriz ter zagotovijo kontinuiteto poslovanja. Učinkovito krizno upravljanje zahteva skrbno načrtovanje, jasno določene odgovornosti, stalno usposabljanje in redno preverjanje ustreznosti teh načrtov. Z integracijo najboljših praks in standardov, kot sta ISO 22301 ter ISO 27031, lahko organizacije zagotovijo, da so pripravljene na različne krizne situacije, kar jim omogoča hitrejše okrevanje in zmanjšanje negativnih vplivov na poslovanje.

NAČRTOVANJE OBNOVE V PROCESIH UPRAVLJANJA NEPREKINJENEGA POSLOVANJA (BCM)

Načrtovanje obnove je ključna sestavina upravljanja neprekinjenega poslovanja (BCM). Zagotavlja, da organizacija lahko nadaljuje z delovanjem med in po motnji, s čimer se zmanjša vpliv na njeno delovanje, ugled ter deležnike. Ta razdelek razširja temeljne vidike načrtovanja obnove znotraj procesov BCM, s poudarkom na pomembnosti strukturiranega in celovitega pristopa.

1. Pomen načrtovanja obnove

Načrtovanje obnove je pomembno za:

- Zmanjšanje izpadov: Zagotavljanje, da se ključne poslovne funkcije hitro obnovijo, da se zmanjšajo operativne motnje.
- Zaščito prihodkov: Zmanjšanje finančnih izgub z ohranjanjem ključnih operacij in storitev.
- Varovanje ugleda: Ohranitev zaupanja strank in deležnikov z dokazovanjem odpornosti.
- Skladnost: Izpolnjevanje zakonskih, regulativnih in pogodbenih obveznosti v zvezi z neprekinjenim poslovanjem ter obnovo po nesrečah.

2. Ključne sestavine načrtovanja obnove

Analiza vpliva na poslovanje (BIA)

Temelj učinkovitega načrtovanja obnove je temeljita analiza vpliva na poslovanje (BIA). Vključuje:

- Identifikacijo kritičnih funkcij: Določanje, katere poslovne funkcije so ključne za preživetje organizacije.

- Oceno vplivov: Vrednotenje možnega vpliva motenj na te funkcije v smislu finančne izgube, operativnega izpada in škode za ugled.
- Določanje ciljev časa obnove (RTO): Postavljanje RTO-jev za določitev najdaljšega sprejemljivega izpada za vsako kritično funkcijo.
- Cilje točke obnove (RPO): Določanje največje dopustne izgube podatkov, merjeno v času.

Ocena tveganja

Razumevanje tveganj, ki lahko vodijo do poslovnih motenj, je ključnega pomena. To vključuje:

- Identifikacijo groženj: Prepoznavanje potencialnih groženj, kot so naravne nesreče, kibernetski napadi, okvare opreme in človeške napake.
- Oceno ranljivosti: Vrednotenje ranljivosti organizacije na te grožnje.
- Razvoj strategij za ublažitev: Ustvarjanje strategij za zmanjšanje verjetnosti in vpliva teh groženj.

Razvoj obnovitvenih strategij

Strategije obnove je treba prilagoditi specifičnim potrebam organizacije in njenim kritičnim funkcijam. Te strategije vključujejo:

- Preventivne ukrepe: Uvajanje ukrepov za preprečevanje motenj, kot so redno vzdrževanje, robustni kibernetski protokoli in usposabljanje zaposlenih.
- Strategije ublažitve: Razvoj načrtov za zmanjšanje vpliva motenj, kot so diverzifikacija dobaviteljev, vzpostavitev alternativnih delovnih ureditev in vzdrževanje redundantnih sistemov.
- Podrobni obnovitveni postopki: Izdelava podrobnih postopkov za obnovo vsake kritične funkcije, vključno z razporeditvijo virov, dodelitvijo nalog in časovnicami.

Komunikacijski načrt

Učinkovit komunikacijski načrt zagotavlja, da so vsi deležniki obveščeni in usklajeni med motnjo. To vključuje:

- Notranjo komunikacijo: Zagotavljanje, da so zaposleni seznanjeni s svojimi vlogami in odgovornostmi med motnjo.
- Zunanjo komunikacijo: Komuniciranje s strankami, dobavitelji, regulatorji in mediji za upravljanje pričakovanj ter ohranjanje zaupanja.

Testiranje in vzdrževanje

Redno testiranje in vzdrževanje obnovitvenega načrta je bistveno za zagotavljanje njegove učinkovitosti. To vključuje:

- Redne vaje: Izvajanje rednih vaj in simulacij za testiranje obnovitvenega načrta ter prepoznavanje morebitnih pomanjkljivosti.
- Pregledi načrta: Redni pregledi in posodobitve obnovitvenega načrta, da odražajo spremembe v organizaciji, njenem delovanju ter zunanjem okolju.
- Učne lekcije: Vključevanje lekcij, pridobljenih iz testiranj in dejanskih motenj, v obnovitveni načrt za nenehno izboljševanje njegove učinkovitosti.

Usposabljanje in ozaveščanje

Zagotavljanje, da so vsi zaposleni usposobljeni in seznanjeni z obnovitvenim načrtom, je ključnega pomena. To vključuje:

- Usposabljanje zaposlenih: Redno usposabljanje zaposlenih, da razumejo svoje vloge v obnovitvenem procesu.
- Programi ozaveščanja: Izvajanje programov ozaveščanja za poudarjanje pomena načrtovanja obnove in spodbujanje kulture odpornosti.

Poslovno kritična funkcija	Zabeleži se **ime poslovno kritične funkcije** oz. oddelka.
Ciljni čas okrevanja	Zabeleži se **najdaljši sprejemljiv čas**, v katerem mora biti izredni dogodek naslovljen in vsi relevantni kritični podprocesi ponovno vzpostavljeni.
Aktivacija načrta neprekinjenega poslovanja	Določi se **funkcija in oseba**, ki sproži aktivacijski načrt v primeru izrednega dogodka.
TAKOJŠNJI ODZIV V STISKI	
Dogodek	Zabeleži se kritični **dogodek**, ki se obvladuje.
Vloga	Opredeli se **vloga** (in **ime** posameznika), ki je odgovorna za izvedbo spodnjih korakov za takojšnji odziv v stiski.
Zadolžitve	Določijo se posamezni **koraki** v določenem **vrstnem redu**, ki so potrebni za takojšnji odziv na dogodek, ter **roki** (reakcijski čas) v katerih morajo biti izpeljani. Koraki vsebujejo informacije o **ključnih sredstvih, virih, informacijah**, ki so potrebne za zmanjšanje posledic dogodka in takojšnji odziv za ponovno vzpostavitev relevantnih kritičnih procesov. Koraki vsebujejo informacije o **ključnih (notranjih in zunanjih) deležnikih**, ki morajo biti obveščeni o dogodku in/ali odzivu ali pa so neposredno vpleteni v definirane korake (npr. drugi oddelki v podjetju, zunanji izvajalci, dobavitelji, mediji). Koraki vsebujejo navodila za **dokumentiranje** dogajanja in sprejetih odločitev.
OKREVALNI POSTOPKI	
Dogodek	Zabeleži se kritični **dogodek**, ki se obvladuje.
Vloga	Opredeli se **vloga** (in **ime** posameznika), ki je odgovorna za izvedbo spodnjih korakov za okrevanje.
Zadolžitve	Določijo se posamezni **koraki** v določenem **vrstnem redu**, ki so potrebni za okrevanje oz. povrnitev v prvotno stanje, ter **roki** (reakcijski čas) v katerih morajo biti izpeljani. Koraki vsebujejo informacije o **ključnih sredstvih, virih, informacijah**, ki so potrebne za zmanjšanje posledic dogodka in povrnitev relevantnih kritičnih procesov v prvotno stanje. Koraki vsebujejo informacije o **ključnih (notranjih in zunanjih) deležnikih**, ki morajo biti obveščeni o dogodku in/ali postopkih za okrevanje ali pa so neposredno vpleteni v definirane korake (npr. drugi oddelki, zunanji izvajalci, dobavitelji, mediji). Koraki vsebujejo navodila za **dokumentiranje** dogajanja in sprejetih odločitev.

Shema 11: Vzorec odzivnih in okrevalnih postopkov v načrtu neprekinjenega poslovanja (vir: ICS)

Razširjeni pristopi k načrtovanju obnove

Uporaba in vključevanje naprednih tehnologij ter inovativnih rešitev, kot so umetna inteligenca (AI), strojno učenje (ML) in avtomatizacija, lahko znatno izboljša zmogljivosti načrtovanja obnove:

- AI in ML: Te tehnologije lahko analizirajo velike količine podatkov za prepoznavanje vzorcev in napovedovanje potencialnih motenj.
- Avtomatizacija: Avtomatizacija nalog, kot so varnostno kopiranje podatkov in sprožanje obnovitvenih postopkov, zmanjšuje čas izpada ter človeške napake.

Sodelovanje z zunanjimi partnerji

Sodelovanje z zunanjimi partnerji in dobavitelji je ključnega pomena za uspešno načrtovanje obnove:

- Pogodbe o ravni storitev (SLA): Določanje SLA-jev z dobavitelji za zagotavljanje pravočasnega in zanesljivega odziva med motnjami.
- Redna komunikacija: Vzpostavljanje rednih komunikacijskih kanalov z dobavitelji in partnerji za usklajevanje obnovitvenih dejavnosti.

Uporaba scenarijev in simulacij

Scenariji in simulacije so učinkovite metode za testiranje ter izboljšanje načrtov obnove:

- Simulacije na podlagi scenarijev: Izvajanje simulacij na podlagi različnih scenarijev motenj za preverjanje pripravljenosti in prilagodljivosti načrtov.
- Lekcije iz preteklih incidentov: Analiza preteklih incidentov za prepoznavanje izboljšav v postopkih obnove.

Vključevanje ključnih deležnikov

Vključevanje ključnih deležnikov v proces načrtovanja obnove je bistvenega pomena za zagotavljanje celovite in učinkovite priprave:

- Deležniki: Identifikacija in vključevanje vseh ključnih notranjih ter zunanjih deležnikov, kot so vodstvo, zaposleni, dobavitelji in regulatorji.
- Redni sestanki: Organiziranje rednih sestankov in delavnic z deležniki za usklajevanje ter izboljšanje načrtov obnove.

Učinkovito načrtovanje obnove je temelj upravljanja neprekinjenega poslovanja. Z natančnim razumevanjem kritičnih funkcij organizacije, oceno tveganj, razvojem robustnih obnovitvenih strategij in vzdrževanjem celovitega komunikacijskega načrta lahko organi-

Pridobitev podpore vodstva.
Določitev obsega, oblike, ciljev in termina testiranja.
Ugotovitev omejitev ob izvedbi.
Ponovno ovrednotenje obsega, oblike, ciljev in termina glede na omejitve.
Objava obsega, oblike, ciljev in termina testiranja.
Določitev ekip/udeležencev testiranja.
Določitev ekipe za razvoj scenarija.
Razvoj scenosleda dogodkov v scenariju.
Priprava sporočil, mini scenarijev in podatkov za preizkus.
Priprava rekvizitov, pripomočkov, diagramov, slike.
Razvoj orodij za pomoč pri izvedbi testiranja.
Vzpostavitev nadzorne skupine testiranja in izbor ocenjevalcev.
Obvestilo udeležencem o terminu, obsegu, namenu in omejitvah testiranja.
Obvestilo zaposlenim in (po potrebi) javnosti in medijem o vaji.
Kritično ocenjevanje testiranja na podlagi povratnih informacij organizatorjev in udeležencev.
Izdelava poročila, ovrednotenje (ugotavljanje pomanjkljivosti) in dokumentiranje izvedenega testiranja.
Revizija načrtov, postopkov, sredstev, opreme in nadaljnje testiranje na podlagi zaključkov.

Shema 12: Načrtovanje testiranja scenarijev na področju zagotavljanja neprekinjenega poslovanja (vir: ICS)

zacije zagotovijo svojo odpornost ob motnjah. Redno testiranje, vzdrževanje in usposabljanje dodatno povečujejo pripravljenost organizacije, zagotavljajo hitro ter učinkovito obnovo po motnji in s tem varujejo njeno delovanje, ugled ter deležnike. Napredne tehnologije, sodelovanje z zunanjimi partnerji, uporaba scenarijev in simulacij ter vključevanje ključnih deležnikov prispevajo k celovitemu in prilagodljivemu pristopu k načrtovanju obnove, kar omogoča organizacijam, da se uspešno spopadajo s sodobnimi izzivi ter grožnjami.

INTEGRACIJA ISO STANDARDOV (INTEGRATIVNI PRISTOP STANDARDOV ISO 22301 IN ISO 27031)

Sledenje mednarodnim standardom, kot sta ISO 22301 za upravljanje neprekinjenega poslovanja in ISO 27031 za pripravljenost IKT za neprekinjeno poslovanje, lahko izboljša učinkovitost načrtovanja obnove. Ti standardi zagotavljajo okvir za vzpostavitev, izvajanje, vzdrževanje in izboljšanje načrtov neprekinjenega poslovanja.

V sodobnem poslovnem okolju je zagotavljanje neprekinjenega poslovanja in pripravljenosti informacijskih ter komunikacijskih tehnologij (IKT) ključno za odpornost organizacij. Standarda ISO 22301 in ISO 27031 ponujata celovite smernice za upravljanje neprekinjenega poslovanja ter pripravljenost IKT sistemov. Skupaj ustvarjata integrativni pristop, ki pomaga organizacijam obvladovati tveganja, zmanjšati izpade in zagotavljati poslovno kontinuiteto.

Pregled Standardov

- ISO 22301 - Sistem upravljanja neprekinjenega poslovanja (BCMS)
- ISO 22301 je mednarodni standard, ki določa zahteve za vzpostavitev, implementacijo, vzdrževanje in nenehno izboljševanje sistema upravljanja neprekinjenega poslovanja (BCMS). Poudarja pomen analize vplivov na poslovanje (BIA), strategij za neprekinjeno poslovanje in pripravljenost na izredne dogodke.

ISO 27031 - Pripravljenost IKT za neprekinjeno poslovanje

ISO 27031 zagotavlja smernice za načrtovanje, implementacijo, delovanje in izboljševanje pripravljenosti IKT sistemov za zagotavljanje neprekinjenega poslovanja. Standard se osredotoča na vzpostavitev odpornosti IKT sistemov, testiranje obnovitvenih načrtov in vzdrževanje pripravljenosti.

Integrativni Pristop (Skupni cilji in področja)

Pogled na oba ključna standarda, ki ju dopolnjuje še veliko dodatnih standardov, pa nam poda osnovi pregled oz. usmeritev na proces integracije. Oba standarda se osredotočata na zagotavljanje neprekinjenega poslovanja in odpornosti na motnje. Njuna integracija omogoča celovit pristop k obvladovanju tveganj, saj združuje procese za neprekinjeno poslovanje (ISO 22301) in pripravljenost IKT sistemov (ISO 27031). Organizacije se lahko certificirajo zgolj po ISO 22301 in ISO 27001, ostali pripadajoči standardi so dodatne usmeritve ter pojasnila za področje upravljanja neprekinjenega poslovanja ali upravljanja področje IKT storitev in sistemov.

Proces Integracije

A.1. Analiza Vplivov na Poslovanje (BIA)

- ISO 22301: Poudarja pomembnost BIA za identifikacijo kritičnih poslovnih funkcij in njihovih zahtev za obnovitev.
- ISO 27031: Dopolnjuje BIA z osredotočanjem na kritične IKT sisteme in infrastrukturo, ki podpira poslovne funkcije.

A.2. Razvoj Strategij za neprekinjeno poslovanje

- ISO 22301: Vzpostavlja strategije za neprekinjeno poslovanje, vključno z obnovitvenimi načrti in pripravljenostjo na izredne dogodke.
- ISO 27031: Dopolnjuje te strategije z načrti za obnovitev IKT sistemov, vključno s testiranjem in vzdrževanjem teh načrtov.

A.3. Implementacija in vzdrževanje

- ISO 22301: Usmerja implementacijo BCMS in zagotavlja stalno vzdrževanje pripravljenosti organizacije.
- ISO 27031: Osredotoča se na implementacijo načrtov za obnovitev IKT sistemov in njihovo redno vzdrževanje, kar vključuje usposabljanje zaposlenih ter redno testiranje.

A.4. Testiranje in Izboljšave

- ISO 22301: Poudarja pomembnost rednega testiranja načrtov za neprekinjeno poslovanje in nenehno izboljševanje na podlagi povratnih informacij.
- ISO 27031: Zagotavlja smernice za testiranje obnovitvenih načrtov IKT sistemov in nenehno izboljševanje na podlagi rezultatov testov ter analize incidentov.

A.5. Komunikacija in Ozaveščanje

- ISO 22301: Usmerja komunikacijo z notranjimi in zunanjimi deležniki glede načrtov za neprekinjeno poslovanje.
- ISO 27031: Dopolnjuje komunikacijske strategije z vidika pripravljenosti IKT sistemov in vloge ključnih deležnikov pri zagotavljanju odpornosti.

A.6. Prednosti Integrativnega Pristopa

- Celovitost: Združuje poslovne procese in IKT pripravljenost za celovit pristop k obvladovanju tveganj ter zagotavljanju neprekinjenega poslovanja.
- Učinkovitost: Omogoča učinkovitejše načrtovanje, implementacijo in vzdrževanje strategij za neprekinjeno poslovanje ter obnovitev IKT sistemov.
- Skladnost: Povečuje skladnost z regulativnimi zahtevami in najboljšimi praksami na področju neprekinjenega poslovanja ter kibernetske varnosti.
- Odpornost: Krepi odpornost organizacije proti različnim vrstam motenj, od naravnih nesreč do kibernetskih napadov.

Integracija standardov ISO 22301 in ISO 27031 predstavlja učinkovit ter celovit pristop k zagotavljanju neprekinjenega poslovanja in pripravljenosti IKT sistemov. Organizacije, ki implementirajo ta integrativni pristop so bolje pripravljene na obvladovanje tveganj, zagotavljanje odpornosti in hitro obnovitev po motnjah, kar je ključnega pomena za dolgoročni uspeh ter stabilnost. ISO 27031 namreč predstavlja celovit okvir za vzpostavitev, implementacijo, vzdrževanje in izboljševanje pripravljenosti IKT za neprekinjeno poslovanje. Organizacije, ki sledijo tem smernicam, lahko zagotovijo, da njihovi IKT sistemi ostanejo operativni tudi v času motenj, s čimer podpirajo neprekinjeno poslovanje in povečujejo odpornost proti različnim tveganjem ter grožnjam.

Viri:

- ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements
- ISO/IEC 27031:2011: Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)

Poglavje 16
Napotki za pripravo politike in postopkov za oceno učinkovitosti varnostnih ukrepov

POVZETEK

Priprava politike in postopkov za oceno učinkovitosti varnostnih ukrepov je ključna za zagotavljanje prilagodljivega in proaktivnega sistema varovanja informacijskih virov. Smernice zajemajo določitev ciljev, obsega in strukture politik, spremljanje učinkovitosti ter redne revizije za skladnost z aktualnimi predpisi in standardi. Poudarjen je pomen meril uspešnosti, informacijskih sistemov za spremljanje ter rednega izboljševanja ukrepov, da organizacija ostaja odporna na nove grožnje.

Ključne točke:

- Določanje ciljev in obsega ocenjevanja
- Struktura politike ocenjevanja varnostnih ukrepov
- Upravljanje tveganj in določitev meril za učinkovitost
- Izvajanje postopkov ocenjevanja
- Vloga informacijskega sistema za spremljanje in poročanje
- Redno spremljanje in izboljševanje politik
- Zagotavljanje skladnosti in revizija.

1. Uvod v ocenjevanje učinkovitosti varnostnih ukrepov

Ocenjevanje učinkovitosti varnostnih ukrepov je ključnega pomena za zagotavljanje, da organizacija ustrezno ščiti svoje informacijske vire in občutljive podatke pred vedno večjimi ter bolj kompleksnimi grožnjami. Varnostno okolje se nenehno spreminja, zato morajo biti varnostni ukrepi proaktivni, prilagodljivi in vedno usklajeni s cilji organizacije. Proces ocenjevanja učinkovitosti vključuje redne preglede tehničnih, organizacijskih in človeških varnostnih ukrepov ter preverjanje, ali ti ukrepi še naprej ustrezno ščitijo pred aktualnimi grožnjami, kot so zlonamerna programska oprema, napadi na omrežja in notranje varnostne grožnje.

Uvedba učinkovitih postopkov ocenjevanja pomaga organizaciji zmanjšati tveganja, zlasti tista, povezana z iztekom veljavnosti obstoječih varnostnih kontrol, ki so postale zastarele ali neučinkovite. Ocena učinkovitosti tako prispeva k nenehnemu izboljševanju varnostne politike in postopkov ter podpira organizacijo pri oblikovanju strategij obvladovanja varnostnih tveganj. Kljub temu pa uspešno izvajanje ocenjevanja zahteva tudi podporo vodstva, saj je brez ustrezne podpore organizacija izpostavljena večjim tveganjem in manj učinkovitim varnostnim procesom. Cilj je vzpostaviti proaktiven sistem, ki je prilagodljiv in zmožen zaščititi organizacijo pred razvojem novih groženj ter ranljivostmi.

2. Določanje ciljev in obsega ocenjevanja

Cilji ocenjevanja učinkovitosti varnostnih ukrepov so zasnovani na potrebah organizacije, pri čemer je pomembno, da se osredotočajo na varovanje zaupnosti, integritete, avtentičnosti in razpoložljivosti podatkov. Ključna vprašanja pri določanju ciljev vključujejo opredelitev, kaj organizacija želi doseči z ocenjevanjem, in katere specifične varnostne komponente je treba oceniti. Na primer, organizacija lahko kot cilje določi zmanjšanje števila varnostnih incidentov, povečanje ozaveščenosti zaposlenih ali izboljšanje odziva na incidente. Določitev obsega ocenjevanja je prav tako temeljnega pomena in zahteva temeljito analizo vseh informacijskih sistemov, infrastrukture, procesov ter človeških virov, ki so kritični za varnost organizacije. V obseg morajo biti vključeni vsi elementi, ki imajo potencialen vpliv na varnost, vključno z informacijskimi tehnologijami, fizično infrastrukturo, zaposlenimi, partnerji in zunanjimi dobavitelji. Pravilno določeni cilji in obseg so temelj za uspešno izvedbo ocenjevanja, saj zagotavljajo, da so vključeni vsi bistveni vidiki varnosti, organizacija pa se lahko prilagaja spremembam v zakonodaji ali poslovnih procesih, ki lahko vplivajo na njene kritične varnostne potrebe.

3. Struktura in razvoj politike ocenjevanja varnostnih ukrepov

Politika ocenjevanja varnostnih ukrepov mora biti strukturirana in zasnovana tako, da omogoča jasno definicijo odgovornosti, postopkov ter smernic, ki se uporabljajo za oceno učinkovitosti. Vključevati mora smernice o merilih uspešnosti in postopkih, ki so potrebni za učinkovito ocenjevanje. Poleg tega mora politika opredeliti, kdo je odgovoren za spremljanje učinkovitosti, kako se rezultati ocen analizirajo in kako se obravnavajo povratne informacije. Struktura politike mora biti dovolj prilagodljiva, da omogoča prilagoditev glede na spremembe v varnostnem okolju. Politika ocenjevanja je pomembno orodje za zagotavljanje skladnosti s standardi in zakonodajo, saj določa okvir, v katerem se izvajajo vse aktivnosti ocenjevanja. Politiko mora odobriti vodstvo organizacije, da zagotovi ustrezno podporo in usklajenost z organizacijskimi cilji. Priporočljivo je, da se politika redno preverja in posodablja, da ostane skladna z najnovejšimi standardi, zakonodajo ter poslovnimi potrebami organizacije.

4. Upravljanje tveganj in določitev meril za učinkovitost

Upravljanje tveganj je ključno za vzpostavitev meril učinkovitosti varnostnih ukrepov, saj organizacija s tem določi sprejemljivo raven tveganja in prilagodi varnostne kontrole.

Merila učinkovitosti morajo temeljiti na ključnih kazalnikih uspešnosti (KPI), ki omogočajo spremljanje varnostnih ukrepov na podlagi merljivih podatkov, kot so hitrost odziva na incidente, raven zaščite pred nepooblaščenim dostopom, število zaznanih incidentov in uspešnost sanacije škode.

Kazalniki uspešnosti varnostnih ukrepov naj bodo oblikovani na način, da omogočajo sistematično spremljanje ključnih varnostnih vidikov organizacije in omogočajo primerjavo trenutne učinkovitosti z določeno ciljno ravnjo varnosti. Merila uspešnosti prav tako omogočajo upravljavcem tveganj, da prepoznajo morebitna področja za izboljšanje in po potrebi prilagodijo vire ter načine izvajanja varnostnih ukrepov. Tako lahko organizacija usmeri svoja sredstva v izboljšave, kjer so pomanjkljivosti kritične in kjer se pojavljajo največja tveganja.

5. Izvajanje postopkov ocenjevanja varnostnih ukrepov

Pravilno izvajanje postopkov ocenjevanja zahteva predhodno določen načrt in opredelitev vseh korakov, ki zagotavljajo, da so vsi varnostni ukrepi ustrezno pregledani. Vključevanje zunanjih strokovnjakov ali avditorjev zagotavlja objektivnost in nepristranskost ocenjevanja. Pomembno je, da ocenjevanje vključuje tako tehnične zaščitne ukrepe (npr. požarne zidove, varnostno konfiguracijo sistemov) kot tudi organizacijske ukrepe, kot so izobraževanja zaposlenih, postopki za odzivanje na incidente in pravila za ravnanje z občutljivimi informacijami.

Izvajanje ocenjevanja naj poteka sistematično in v skladu s cilji politike ter obsegom ocenjevanja. Postopki vključujejo zbiranje podatkov, analiziranje rezultatov in izdelavo poročil z oceno učinkovitosti ukrepov. Na podlagi teh ugotovitev se nato oblikujejo priporočila za izboljšave, ki lahko vključujejo posodobitev obstoječih varnostnih politik, zagotovitev dodatnih resursov ali uvedbo dodatnih ukrepov. Redno ocenjevanje je ključno za zagotovitev, da so varnostni ukrepi vedno prilagojeni aktualnim grožnjam.

6. Vloga informacijskega sistema za spremljanje in poročanje

Informacijski sistem za spremljanje in poročanje je ključno orodje za zbiranje, analiziranje ter spremljanje varnostnih incidentov in aktivnosti, povezanih z varnostnimi kontrolami. Sistem omogoča avtomatizirano spremljanje groženj in nepravilnosti, s čimer omogoča takojšnjo zaznavo potencialnih varnostnih incidentov ter hitro odzivanje nanje. Redna analiza podatkov, zbranih prek sistema, omogoča prepoznavanje vzorcev, ki kažejo na prisotnost groženj, kar olajša določitev potrebnih prilagoditev in izboljšav. Učinkovit informacijski sistem omogoča tudi sprotno poročanje, kar vodstvu in odgovornim osebam zagotavlja aktualen pregled nad stanjem varnosti. S tem se izboljša preglednost, vodstvu pa omogoči sprejemanje informiranih odločitev. Poleg tega sistem omogoča sledljivost in dokumentacijo, ki so ključne za revizijske namene in za dokazovanje skladnosti z regulativnimi zahtevami. Vloga informacijskega sistema za spremljanje in poročanje je torej osrednja pri vzdrževanju visokega nivoja varnosti ter prilagajanju varnostnih ukrepov na podlagi aktualnih podatkov. Pomembno pa je zagotoviti ustrezne kompetence za učinkovito upravljanje s takšnim orodjem, saj je človeški faktor tukaj še vedno ključen.

7. Redno spremljanje in izboljševanje politik ter postopkov

Za vzdrževanje učinkovitih politik in postopkov je nujno redno spremljanje njihove učinkovitosti ter skladnosti z aktualnimi predpisi ali standardi. Načrt za redne revizije in preglede omogoča, da organizacija pravočasno prepozna morebitne pomanjkljivosti ter priložnosti za izboljšave. Redno spremljanje zagotavlja, da se organizacija proaktivno odziva na nove varnostne izzive, pridobljene izkušnje pa se uporabijo za nadaljnje izboljšanje obstoječih politik in postopkov.

Vključevanje povratnih informacij od zaposlenih in drugih vključenih strani omogoča organizaciji natančno oceno, kako učinkovite so

trenutne varnostne politike ter prakse. Prilagoditev politike na podlagi povratnih informacij in rezultatov preteklih ocenjevanj zagotavlja, da ostaja politika ustrezna ter prilagojena trenutnim varnostnim zahtevam. Redne izboljšave politik in postopkov omogočajo, da organizacija ohranja visoko raven varnosti ter skladnost z regulativnimi zahtevami.

8. Zagotavljanje skladnosti in revizija

Zagotavljanje skladnosti je ključno za vzdrževanje ustreznosti varnostnih ukrepov, saj omogoča, da se varnostne politike in postopki izvajajo v skladu z notranjimi ter zunanjimi zahtevami. Redne revizije pomagajo prepoznati pomanjkljivosti v trenutnih postopkih in omogočajo organizaciji oceno, ali varnostni ukrepi še zadostujejo za doseganje ciljev. Notranje preglede dopolnjujejo neodvisne revizije, ki prinašajo dodatno objektivnost in zagotovilo, da so postopki ustrezni.

Organizacija lahko sodeluje z neodvisnimi tretjimi osebami za izvedbo revizij in pregledov varnostnih postopkov, kar prispeva k dodatnemu zaupanju v učinkovitost politik ter skladnost z zakonodajnimi zahtevami. Pravilna struktura revizijskih postopkov zagotavlja, da so varnostni ukrepi vedno ustrezno preverjeni in posodobljeni glede na nove zahteve ali tveganja.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- Evropska unija, Evropska agencija za kibernetsko varnost (ENISA): https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_sl?utm
- Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov: Uradni list RS, št. 118/23: https://pisrs.si/pregledPredpisa?id=URED8925&utm=
- Urad Vlade RS za informacijsko varnost https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/
- Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-10 in 49/23): https://pisrs.si/pregledPredpisa?id=ZAKO7707&utm_

Poglavje 17
Napotki glede varnosti pri nabavi, razvoju, integraciji, vzdrževanju omrežnih in informacijskih sistemov ter odstranjevanju sistemov iz produkcije

POVZETEK

Poglavje obravnava ključne varnostne prakse pri celotnem življenjskem ciklu omrežnih in informacijskih sistemov. Poudarja pomen varnosti pri nabavi, integraciji, razvoju in vzdrževanju teh sistemov ter zagotavljanju ustrezne zaščite pri odstranjevanju iz produkcije. Smernice vključujejo določitev strogih varnostnih zahtev, preverjanje ponudnikov, vključevanje varnosti že v fazi načrtovanja, redne posodobitve, spremljanje sistemov in učinkovito upravljanje dostopov. Poseben poudarek je namenjen segmentaciji omrežij, ki povečuje varnost z ločevanjem sistemov glede na funkcionalnost in občutljivost podatkov.

Ključne točke:

- Pridobivanje omrežnih in informacijskih sistemov
- Razvoj sistemov z vgrajeno varnostjo (Security by Design)
- Vzdrževanje in posodabljanje sistemov
- Upravljanje dostopov in avtorizacija
- Segmentacija omrežja za povečano varnost.

1. Pridobivanje omrežnih in informacijskih sistemov

Pridobivanje omrežnih in informacijskih sistemov zahteva premišljeno izbiro, kjer sta varnost in zanesljivost ključnega pomena. Najprej je pomembno, da se osredotočimo na izbiro ponudnikov, ki izpolnjujejo stroge varnostne standarde. Ponudniki morajo imeti ustrezne certifikate, kot so družina standardov ISO/IEC 27001 ali NIST, ki potrjujejo njihovo zavezanost k varnosti. Pomembno je tudi preveriti njihovo zgodovino na področju odpravljanja ranljivosti in varnostnih incidentov ter njihove sposobnosti zagotavljanja rednih posodobitev in popravkov. Sodelovanje s ponudnikom mora temeljiti na jasnih pogodbah, kjer so opredeljene njihove odgovornosti, vključno s tem, kako bodo obravnavane morebitne varnostne pomanjkljivosti in šibke točke. Ključni del teh dogovorov je SLA (Service Level Agreement) ali pogodba o ravni storitev, ki jasno določa pričakovanja med ponudnikom opreme in storitev ter naročnikom. SLA vključuje opredelitev odzivnih časov za odpravo napak, glede dobave opreme in rezervnih delov, razpoložljivost storitev ter postopke v primeru motenj ali incidentov. To zagotavlja hitro in učinkovito ukrepanje v primeru težav ter motivira ponudnika, da spoštuje dogovorjene standarde, kar je ključno za varnost in zanesljivost sistema.

Pred uvedbo novega sistema je nujno opraviti oceno vseh varnostnih tveganj in vplivov na poslovanje organizacije, kar je ključen korak za prepoznavanje možnih varnostnih groženj, ranljivosti ter vplivov na poslovanje in nemoteno zagotavljanje storitev. Ocena mora biti celovita in zajemati tako tehnične kot poslovne vidike, saj vsaka uvedba nove tehnologije neposredno vpliva na celotno varnost organizacije. Sodelovanje strokovnjakov iz različnih področij omogoča, da se tveganja pravilno prepoznajo, in da se pripravijo ustrezne strategije za njihovo zmanjšanje. To je še posebej pomembno, ker se s tem zagotovijo temelji za varno delovanje sistema in se zmanjšajo možnosti za nepredvidene težave.

Ob pridobivanju novih sistemov je nujno jasno opredeliti varnostne zahteve ali standarde, ki jih mora sistem izpolnjevati. Med varnostnimi zahtevami so zahteve, kot je zagotavljanje zaupnosti (npr. uporaba šifriranja), zagotavljanje avtentičnosti (npr. uporaba večfaktorske avtentikacije), zagotavljanje celovitosti (npr. prepoznavanja nepooblaščenih sprememb v sistemskih datotekah), zagotavljanje razpoložljivosti (npr. podvojeni elementi). Specifikacije morajo biti natančno določene in vključevati postopke ravnanja v primeru zaznane ranljivosti ter odzivanje na varnostne incidente. Poleg tehničnih zahtev je pomembno tudi, da so vpeljani ustrezni varnostni protokoli in politike, ki so skladni z zakonodajo ter najboljšimi praksami. Ustrezno upoštevanje varnostnih standardov in dobrih praks že v razvoju (npr. OWASP Application Security Verification Standard - ASVS) zagotavlja, da bo sistem odporen na potencialne grožnje, ter da bo organizacija pripravljena na učinkovito upravljanje varnostnih izzivov.

2. Razvoj omrežnih in informacijskih sistemov

Razvoj omrežnih in informacijskih sistemov zahteva, da varnost ni nekaj, kar se doda na koncu, temveč je vgrajena v vsak korak razvoja. Zasnova sistema mora upoštevati načelo „Security by Design“, kar pomeni, da se varnostne funkcije vgradijo že v začetni fazi načrtovanja. Vsak del sistema, od aplikacij do omrežne infrastrukture, mora biti zasnovan s poudarkom na zaščiti pred potencialnimi grožnjami, kar se ugotovi z ustrezno analizo tveganj in rednim spremljanjem poročil o zaznanih ranljivostih. Tak pristop omogoča, da se ranljivosti (šibke točke) odkrijejo in odpravijo že v zgodnjih fazah, kar bistveno zmanjša tveganje za morebitne napade po uvedbi sistema v produkcijo. Pri mrežnih aplikacijah, ki podpirajo delovanje bistvenih storitev je pomembno zagotoviti možnost preverjanja teh aplikacij že v fazi razvoja. V tem okviru je pomemben dostop do izvorne kode in dokumentacija vseh sestavnih programskih delov ter odvisnosti aplikacije z drugimi programi (kosovnica – Software Bill of Material), saj to omogoča celovit pregled in preverjanje varnosti aplikacij

že v fazi razvoja. Še posebej je treba biti pozoren pri uporabi odprte kode, saj lahko vsebuje zlonamerno kodo, stranska vrata ali ranljivosti, ki niso odpravljene.

Ključni del razvoja je tudi natančno testiranje varnosti. Testiranje ni zgolj enkraten postopek, temveč kontinuiran proces, ki mora spremljati razvoj skozi vse njegove faze. Varnostni testi, simulacije napadov in ocene ranljivosti so le nekateri od načinov, s katerimi se preverja odpornost sistema. Pomembno je, da teste izvajajo izkušeni strokovnjaki, ki lahko identificirajo tudi manj očitne šibke točke in ranljivosti. Testiranje ne sme biti omejeno le na tehnične komponente – preveriti je treba tudi procese, ki podpirajo delovanje sistema, kot so varnostni postopki, ki jih upoštevajo razvijalci in uporabniki.

Šifriranje podatkov je še en ključen element pri razvoju varnega sistema. Vsi podatki, ki se shranjujejo ali prenašajo, morajo biti zaščiteni s sodobnim kriptografskim algoritmom, ki zagotavlja, da so informacije dostopne in berljive le pooblaščenim uporabnikom. Uporaba naprednih šifrirnih algoritmov, kot so AES in RSA, zagotavlja visoko stopnjo varnosti, vendar je treba poskrbeti tudi za ustrezno upravljanje s šifrirnimi ključi, saj neustrezno ravnanje lahko ogrozi celoten sistem. Pomembno je, da so šifrirni mehanizmi učinkoviti in se ne upočasnjujejo kritični procesi, kar zahteva skrbno načrtovanje ter integracijo šifriranja že v začetnih fazah razvoja.

Vključitev modernih rešitev za zaščito, kot so sistemi za zaznavanje in preprečevanje vdorov (IDS/IPS), napredna avtentikacija ter tehnologije strojnega učenja za prepoznavanje neobičajnih vedenj v omrežju dodatno izboljšajo varnost sistema. Takšne rešitve omogočajo proaktivno zaznavanje groženj in hitro odzivanje na incidente. Z uvajanjem naprednih zaščitnih mehanizmov v fazi razvoja je možno ustvariti robustne sisteme, ki se lahko učinkovito upirajo sodobnim kibernetskim grožnjam in varujejo podatke ter procese znotraj organizacije.

Pri razvoju sistemov mora torej biti varnost vseprisotna, skrbno integrirana v vsako fazo, saj le tako lahko dosežemo visoko stopnjo zaščite in zanesljivosti, kar je ključno za uspešno delovanje vsake sodobne organizacije.

3. Vzdrževanje omrežnih in informacijskih sistemov

Vzdrževanje omrežnih in informacijskih sistemov je ključno za ohranjanje njihove varnosti ter operativnosti skozi celotno življenjsko dobo. Čeprav lahko kakovostna zasnova in razvoj zmanjšata število varnostnih težav, so redne vzdrževalne aktivnosti tiste, ki dolgoročno zagotavljajo odpornost sistemov pred novimi grožnjami ter ranljivostmi. To vključuje redno spremljanje ranljivosti (npr. prek objav proizvajalca, spletnih forumov), izvajati preverjene in redne posodobitve, stalen nadzor ter spremljanje in pravilno izvajanje ter preverjanje varnostnih kopij.

Redne posodobitve sistemov in programske opreme so osnova za vzdrževanje varnosti. Proizvajalci programske opreme redno izdajo popravke, ki odpravljajo odkrite ranljivosti in izboljšujejo delovanje sistema. Pomembno je, da so posodobitve predhodno preverjene v testnem okolju, so načrtovane in izvedene pravočasno, saj zamuda pri implementaciji popravkov lahko pomeni odprta vrata za kibernetske napade. Organizacije bi morale vzpostaviti avtomatizirane sisteme za posodabljanje, kadar je to mogoče, in izvajati redne preglede za zagotovitev, da vsi elementi sistema delujejo z najnovejšimi varnostnimi izboljšavami, vendar hkrati ne negativno vplivajo na druge povezane sisteme ter aplikacije.

Nadzor in spremljanje omrežja sta ključna elementa pri vzdrževanju varnosti. Sistem za spremljanje mora biti sposoben zaznati nenavadne aktivnosti, kot so poskusi nepooblaščenega dostopa, nenadni skoki v prometu ali komunikacije z znanimi nevarnimi naslovi IP. Vpeljava rešitev, kot so SIEM (Security Information and Event Management) sistemi, omogoča združevanje in korelacijo podatkov

iz različnih sistemov ter njihovo analizo v realnem času, kar omogoča hitro prepoznavanje in odzivanje na varnostne incidente. Redno spremljanje varnostnih dogodkov omogoča pravočasne intervencije in preprečuje širjenje potencialnih varnostnih incidentov.

Varnostne kopije so temelj za varstvo podatkov in zagotavljanje neprekinjenega poslovanja v primeru varnostnih incidentov, kot so napadi z izsiljevalsko programsko opremo ali okvare strojne opreme. Pri izdelavi varnostnih kopij je treba upoštevati pravilo 3-2-1, ki priporoča, da imate vsaj tri kopije svojih podatkov, shranjene na dveh različnih medijih, pri čemer je ena kopija shranjena na lokaciji, ki je fizično ločena od primarne. To pomeni, da poleg glavne kopije na delovnih strežnikih ali računalnikih obstajata še dve dodatni kopiji, na primer ena na lokalnem NAS strežniku in druga v oblaku ali na fizičnem disku, ki se hrani na ločeni lokaciji.

Pomembno je, da so varnostne kopije redno preizkušene, da se zagotovi njihova obnovljivost, saj so le tako uporabne v kriznih situacijah. Poleg tega je smiselno uporabljati šifrirane kopije podatkov, da so zaščitene tudi v primeru fizičnega dostopa nepooblaščenih oseb. Uvajanje avtomatiziranih postopkov za izdelavo kopij zagotavlja, da varnostne kopije niso prepuščene človeški napaki, in da se podatki varno arhivirajo v rednih intervalih.

Vzdrževanje sistemov ni zgolj tehnična naloga, temveč celostna aktivnost, ki zahteva sodelovanje različnih oddelkov znotraj organizacije, z jasno določenimi postopki in odgovornostmi. Pravilno vzdrževanje zagotavlja, da sistemi ostajajo varni in operativni, ter da lahko organizacija hitro in učinkovito obnovi svoje delovanje v primeru nepredvidenih dogodkov.

4. Upravljanje dostopov in avtorizacija

Upravljanje dostopov in avtorizacija sta ključna stebra varnosti v omrežnih ter informacijskih sistemih, saj neposredno vplivata na to, kdo lahko dostopa do katerih podatkov in sistemov ter pod kakšnimi pogoji. Natančno načrtovanje in implementacija teh mehanizmov sta nujna za zaščito pred notranjimi ter zunanjimi grožnjami in zagotavljanjem, da občutljivi podatki ostanejo varni.

Sistemi za upravljanje identitet in dostopa (IAM) omogočajo centralizirano upravljanje uporabniških pravic ter dostopov in zagotavljajo, da imajo uporabniki dostop le do tistih informacij, ki jih nujno potrebujejo za opravljanje svojega dela. Z vzpostavitvijo pravil o najmanjših privilegijih (princip least privilege) je mogoče zagotoviti, da uporabniki in sistemi delujejo z minimalnimi potrebnimi dovoljenji, kar zmanjšuje tveganje zlorabe. Ključno je tudi, da se dostopi redno preverjajo, posodabljajo ali ukinjajo, zlasti ko uporabniki spremenijo svoje delovne vloge ali zapustijo organizacijo. Implementacija teh rešitev vključuje uporabo avtentikacije, avtorizacije in kontrole dostopa na osnovi vlog (RBAC), ki omogočajo boljši nadzor ter sledljivost uporabniških aktivnosti.

Pri varnosti gesel ne gre več zgolj za priporočanje dolgih in kompleksnih gesel, temveč za celovito strategijo, ki vključuje večfaktorsko avtentikacijo (MFA). Močna gesla so še vedno pomembna, vendar sama po sebi ne zagotavljajo zadostne zaščite pred napadi, kot so ribarjenje (phishing), napad z uporabo surove sile (brute force) napadi ali kraja poverilnic. Uvedba večfaktorske avtentikacije, ki združuje nekaj, kar uporabnik ve (geslo), nekaj, kar ima (mobilni telefon ali generiran varnostni ključ), in nekaj, kar je (biometrični podatki, kot so prstni odtis ali prepoznava obraza), znatno povečuje stopnjo zaščite. MFA zmanjšuje tveganje za nepooblaščen dostop, saj napadalcu ni dovolj le ukrasti geslo, temveč mora premagati tudi druge varnostne ovire.

V okviru upravljanja dostopov je pomembno tudi redno spremljanje in beleženje uporabniških dejavnosti, tako pri dostopu do sistema, podatkov ali v omrežnem prometu. Beleženje in analiza prijav, poskusov prijav, sprememb pravic dostopa (še posebej za dostop do ključnih sistemov) ter drugih ključnih dogodkov omogočata hitro prepoznavanje sumljivih dejavnosti. Sistemi morajo biti zasnovani tako, da ob ne-

običajnih poskusih prijave ali dostopa sprožijo alarme in varnostne postopke, kar omogoča hitro ukrepanje. Vzpostavitev revizijskih sledi (audit trails) je prav tako ključnega pomena, saj omogoča preglednost in zagotavlja, da so vsi dostopi sledljivi ter pregledani, kar olajša preiskave ob morebitnih varnostnih incidentih.

Skrbno načrtovano in izvedeno upravljanje dostopov ter avtorizacije je torej bistvenega pomena za varnost organizacije. Ne gre le za tehnične rešitve, temveč za stalno prizadevanje za ohranjanje visokih varnostnih standardov, prilagajanje novim grožnjam in zagotavljanje, da varnostni postopki ustrezajo aktualnim potrebam ter tveganjem.

5. Dobra segmentacija omrežja

Segmentacija omrežja je ena izmed najpomembnejših praks za zagotavljanje varnosti v informacijskih sistemih. S segmentacijo se omrežje razdeli na manjše, ločene dele, kar omogoča boljši nadzor nad prometom in zmanjšuje površino, ki jo lahko napadalci izkoristijo. Dobro segmentirano omrežje ne le preprečuje širjenje morebitnih napadov, temveč tudi izboljšuje upravljanje z varnostjo in povečuje odpornost sistema.

Prvi korak k učinkoviti segmentaciji omrežja je razdelitev na varnostne cone. Te cone določajo, kateri deli omrežja imajo dostop do določenih podatkov in sistemov. Varnostne cone so lahko razdeljene glede na občutljivost podatkov (npr. javna, interna, zaupna) ali glede na funkcionalnost sistemov (npr. razvojno, testno, produkcijsko okolje). Na primer:

- **Javna cona:** Vsebuje strežnike, ki so dostopni iz interneta, kot so spletni strežniki. To je najbolj izpostavljena cona, ki zahteva najstrožje nadzorne mehanizme.
- **Interna cona:** Vsebuje sisteme, do katerih imajo dostop le zaposleni. Ta cona vključuje notranje storitve, kot so e-pošta in datotečni strežniki.
- **Zaupna cona:** Vsebuje kritične sisteme in podatke, kot so baze podatkov s finančnimi informacijami ali osebni podatki strank. Dostop do te cone mora biti strogo omejen in skrbno nadzorovan.

Po vzpostavitvi varnostnih con je ključna uporaba požarnih zidov, varnostnih pravil in drugih kontrolnih mehanizmov za nadzor dostopa med segmenti. Požarni zidovi omogočajo filtriranje prometa med conami na podlagi vnaprej določenih pravil, kar preprečuje nepooblaščen dostop do občutljivih podatkov. Poleg požarnih zidov se lahko uporabljajo tudi sistemi za zaznavanje in preprečevanje vdorov (IDS/IPS), ki spremljajo promet med segmenti ter samodejno blokirajo potencialno nevarne dejavnosti. Uporaba pravil za filtriranje prometa zagotavlja, da lahko sistemi med seboj komunicirajo le v skladu z varnostnimi politikami organizacije.

Strog nadzor prometa med segmenti je še en pomemben varnostni ukrep. Manj kot je povezav med različnimi segmenti, manj možnosti imajo napadalci za premikanje znotraj omrežja v primeru vdora. To se doseže z omejevanjem potrebnih komunikacij na minimum in z določitvijo specifičnih pravil, ki dovoljujejo promet samo za specifične aplikacije ali storitve. Na primer, dostop iz segmenta, kjer so uporabniške delovne postaje do zaupne cone mora biti strogo nadzorovan, in običajno se mora izvajati samo prek ustrezno avtoriziranih aplikacij ali namenskih delovnih postaj.

Za dodatno varnost je smiselno implementirati tudi segmentacijo na nivoju mikrosegmentacije, kjer se omejitve dostopa določajo celo znotraj posameznih segmentov. Mikrosegmentacija omogoča zelo podroben nadzor nad tem, kateri deli aplikacij lahko komunicirajo med seboj, kar dodatno zmanjša možnosti za širjenje napadov. Treba se je zavedati, da zelo podrobna segmentacija zahteva večje napore pri upravljanju omrežja, vendar je varnost na drugi strani neprimerno višja. Za za-

vezance, ki so pomembni za delovanje širše družbene skupnosti je segmentacija ključna pri zagotavljanju varnosti omrežij. Ločenost omrežij z požarnimi zidovi, kjer so jasno določene pravice za prehod oziroma dostop, bistveno povečuje varnost celotnega sistema.

Dobra segmentacija omrežja tako ne le omejuje dostopa do kritičnih virov, temveč tudi izboljšuje zaznavanje napadov in zmanjšuje potencialne škode. To je ena izmed najbolj učinkovitih strategij za zaščito omrežij pred vedno bolj sofisticiranimi kibernetskimi grožnjami.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls

Poglavje 18
Ključni nasveti upravljanja s kibernetskimi incidenti in preprečevanja izrabe prepoznanih tehničnih ranljivosti

POVZETEK

Učinkovito upravljanje kibernetskih incidentov in preprečevanje zlorabe tehničnih ranljivosti zahteva dobro pripravljenost, jasno določene odzivne procese ter preventivne ukrepe. Krizni načrti in organizacija odzivnih ekip omogočajo hitro ukrepanje ob incidentih, medtem ko redna usposabljanja in sodelovanje na vajah izboljšujejo odzivnost na grožnje. Preventivne aktivnosti, kot so redno posodabljanje sistemov, izvajanje vdornih testiranj ter segmentacija omrežij, zmanjšujejo možnosti za zlorabe. Ključnega pomena je tudi učinkovito krizno komuniciranje z deležniki in pravočasno obveščanje pristojnih institucij, kar omogoča celovit pristop k obvladovanju kibernetskih groženj.

Ključne točke:

- Priprava kriznih načrtov in odzivnih procesov
- Jasna organizacija in vloge odzivnih ekip
- Usposabljanje in udeležba na vajah
- Redno posodabljanje in upravljanje varnostnih popravkov
- Izvajanje vdornih testiranj in preverjanje varnostnih ranljivosti
- Segmentacija omrežja in zaščita ključnih sistemov
- Krizno komuniciranje in obveščanje ključnih strank
- Povezovanje s CSIRT-i in drugimi institucijami.

Pripravljenost in krizni načrt kot temelj učinkovitega upravljanja kibernetskih incidentov

V današnjem digitalnem svetu, kjer se podjetja in organizacije soočajo z nenehno prisotnostjo kibernetskih groženj, je učinkovito upravljanje kibernetskih incidentov ključnega pomena. Ključ do uspešnega obvladovanja takšnih situacij se skriva v dobro sestavljenih načrtih odzivanja na krize oziroma načrtih kriznega upravljanja, ki opredeljujejo postopke, pristojnosti in naloge pri odzivanju na kibernetske incidente. Takšni načrti niso zgolj dokumenti; so strateški vodniki, ki usmerjajo celotno organizacijo v času kriznih razmer.

Prvi in najpomembnejši korak pri upravljanju s kibernetskimi incidenti je vzpostavitev jasnih ter natančno določenih odzivnih načrtov. Ti načrti morajo vsebovati podrobna navodila o tem, kaj storiti ob pojavu kibernetskega incidenta, kdo so ključne osebe, ki sodelujejo pri reševanju situacije, in kako hitro ter učinkovito zagotoviti nadaljnje delovanje poslovnih procesov. Jasno določene vloge in odgovornosti so ključne; vsak član odzivne ekipe mora natančno vedeti, kaj je njegova naloga ter kako naj se odzove v primeru incidenta. Posebno pozornost je treba nameniti tudi določitvi kontaktnih oseb, ki so odgovorne za vodenje in usmerjanje odzivnih ukrepov ter obveščanje ključnih deležnikov v organizaciji. Vloga kontaktne osebe je pomembna zlasti v kriznih situacijah, saj je od njihove sposobnosti hitrega in učinkovitega odločanja odvisen uspeh obvladovanja incidenta.

Da bi bili odzivni načrti učinkoviti, morajo biti vključene osebe ustrezno usposobljene in redno izobražene o najnovejših kibernetskih grožnjah ter postopkih odzivanja. Redno usposabljanje omogoča zaposlenim, da se hitro in pravilno odzovejo na različne situacije, kar zmanjšuje morebitno škodo za organizacijo. Vse to prispeva k večji odpornosti sistema, hitrejši vzpostavitvi delovanja po incidentu in zmanjšuje tveganje za resne posledice ob pojavu kibernetskega incidenta.

Organizacija odziva: Reakcijski čas in vloge odgovornih oseb pri nepredvidljivih incidentih

Pri upravljanju kibernetskih incidentov je izjemno pomembna učinkovita organizacija odziva, saj je prav odzivni čas tisti, ki pogosto določi obseg škode in uspešnost ukrepanja. Ko se pojavi kibernetski incident, je reakcijski čas ključen za omejevanje posledic in ponovno vzpostavitev normalnega delovanja sistema. Zlasti je pomembno, da je ekipa, ki je odgovorna za odziv na incidente, ustrezno usposobljena za hitro in pravilno ukrepanje tudi v primerih nepredvidljivih situacij, ki niso zapisane v odzivnih načrtih.

Usposobljenost ekipe za ravnanje ob incidentih je ključna, saj se grožnje nenehno spreminjajo, zlonamerni akterji pa pogosto presenetijo z novimi, še nepoznanimi metodami. Ne glede na to, kako dobro so načrti pripravljeni, vedno obstajajo scenariji, ki so težko predvidljivi in zahtevajo hitro prilagajanje ter kreativno razmišljanje. Pri takšnih incidentih je reakcijski čas še bolj ključnega pomena, saj mora ekipa hitro identificirati obseg incidenta, oceniti vpliv na druge informacijske sisteme in storitve ter takoj začeti z izvajanjem ukrepov za zajezitev incidenta. Usposobljenost članov ekipe je ključna, saj morajo biti sposobni hitro oceniti situacijo in se odločiti za ustrezne ukrepe v zelo kratkem času. Za učinkovito upravljanje incidentov je nujna jasna in dobro organizirana struktura odgovornosti znotraj podjetja. Pomembno je, da je natančno določeno, kdo je odgovoren za spremljanje in obvladovanje posameznih delov sistema, kot so omrežja, strežniki ali aplikacije. Skrbništvo nad temi sistemi običajno opravljajo notranji zaposleni ali zunanji pogodbeni izvajalci, ki so zadolženi za vzdrževanje teh informacijskih sredstev. Vloga operativnega centra (VOC) je pri tem specifična – VOC ni skrbnik informacijskih sredstev, temveč je odgovoren za nenehno spremljanje omrežnega prometa in zaznavanje potencialnih varnostnih groženj. V primeru zaznane anomalije ali kibernetskega napada VOC obvesti interno ekipo in takoj sodeluje pri usklajevanju odzivnih ukrepov. Tes-

na in usklajena komunikacija med VOC centri ter notranjimi zaposlenimi omogoča hitrejše odločitve in zmanjšuje možnost napak, ki bi lahko še poslabšale situacijo.

Zaradi nepredvidljive in kompleksne narave kibernetskih incidentov je nujno, da je vzpostavljen seznam oseb, ki so potrebne pri upravljanju z incidenti in se zanje pripravi stalna pripravljenost/dosegljivost. Ob tem morajo biti komunikacijski kanali med notranjimi ekipami in VOC centri vedno odprti ter učinkoviti, z namenom hitrega prenosa informacij. Pomembno je tudi, da so vnaprej opredeljeni odzivni postopki, ki vključujejo seznam kontaktnih oseb, naloge in pristojnosti ter protokole komuniciranja. Slednje omogoča, da v primeru incidenta vsi napori lahko takoj usmerijo v reševanje situacije.

Poleg odzivne ekipe, ki je zadolžena za neposredno upravljanje incidentov, so v proces vključene še druge ključne skupine z natančno določenimi vlogami. Kontaktne osebe v vodstvu podjetja imajo nalogo spremljati širšo strategijo odziva in zagotavljati usklajenost ukrepov s poslovnimi cilji ter zakonodajnimi zahtevami. Odzivna skupina na taktični ravni, ki deluje neposredno na terenu, izvaja operativne ukrepe za obvladovanje in omejevanje incidenta ter skrbno dokumentira vse ključne postopke. Vključen je tudi VOC (operativni center), ki zaznava in spremlja nenavadne aktivnosti ter prvi obvešča odzivno ekipo o morebitnih grožnjah, sodeluje pri usklajevanju takojšnjih ukrepov in zagotavlja dodatno podporo. Poleg teh skupin ima pomembno vlogo tudi ekipa za odnose z javnostmi (PR), ki komunicira z zunanjimi deležniki, mediji in javnostjo ter usmerja objave, da se ohrani ugled podjetja in vzpostavi zaupanje.

Identifikacija in ocena vpliva incidenta: Ključni koraki ter obveščanje vodstva

Identifikacija kibernetskega incidenta je eden najpomembnejših korakov pri odzivanju, saj omogoča hitro oceno vpliva na sisteme, procese in storitve ter opredelitev nadaljnjih ukrepov. Ko se pojavi incident, je ključno, da se čim prej ugotovi, kaj se je zgodilo, kateri deli sistema so prizadeti, katere informacije ali podatki so morda izgubljeni ali ogroženi, obseg nedelovanja storitev, obseg prizadetih subjektov zaradi nedelovanja storitve, morebiten vpliv incidenta na druge dele organizacije, morebiten vpliv na druge sektorje, ali celo čezmejen vpliv incidenta. Ta proces identifikacije pomaga pri razumevanju narave in obsega incidenta ter je temelj za nadaljnje odločanje o ukrepih za odpravljanje posledic, vključno z vzpostavitvijo in polnim delovanjem sistema po kibernetskem incidentu.

Prvi korak v procesu identifikacije je natančna ocena, kateri deli sistema so napadeni in ali so ogroženi kritični podatki. Pomembno je tudi hitro ugotoviti, ali incident vpliva na ključne poslovne procese ali operacije, ki so bistvene za nadaljnje delovanje podjetja in so bili identificirani v okviru analize učinka poslovanja (BIA). Pri tem je ključna tudi ocena vpliva incidenta na zaupnost, celovitost, razpoložljivost in avtentičnost podatkov v informacijskem sistemu. S pravilno identifikacijo je mogoče hitreje določiti, kateri deli sistema potrebujejo takojšnjo pozornost za odpravljanje težav.

Ko so prizadeti deli sistema identificirani, je naslednji korak določitev prioritet pri odpravljanju posledic. V tej fazi je ključna ocena, kateri procesi, prepoznani kot ključni v analizi učinka poslovanja (BIA), so najbolj pomembni za nemoteno poslovanje in morajo biti čim prej obnovljeni. Odpravljanje težav se običajno usmeri na sisteme, ki so neposredno povezani z zagotavljanjem ključnih storitev, varnostjo podatkov ali operacijami, katerih zaustavitev bi imela največje posledice za podjetje. S pravilno določitvijo prioritet je mogoče učinkoviteje porabiti omejene vire, kot so čas, tehnična podpora in usposobljenost ekipe, da bi čim prej obnovili najbolj kritične funkcije.

Poleg tehničnega odziva na incident je izjemno pomembno tudi pravilno in hitro obveščanje pristojnih odločevalcev, oziroma vodstva. Vodstvo podjetja mora biti natančno in ažurno obveščeno o stanju sistema, prizadetih procesih ter posledicah incidenta. To vključuje obveščanje o tem, kateri ključni poslovni procesi so začasno zaustavljeni, kakšen je vpliv na operacije in kakšne posledice lahko pričakuje-

jo v kratkoročnem ter dolgoročnem obdobju. Hitro in jasno komuniciranje z vodstvom omogoča, da se tudi sprejmejo strateške odločitve glede usmerjanja virov, notranjega ter zunanjega komuniciranja in nadaljnjih korakov za okrevanje po incidentu.

Ozaveščanje in usposabljanje: Vloga kibernetskih vaj in hitrega prenosa informacij

Ena izmed ključnih komponent učinkovitega upravljanja kibernetskih incidentov je neprestano usposabljanje in udeležba na vajah s področja zagotavljanja kibernetske varnosti. Ni dovolj, da so odgovorne osebe pripravljene samo teoretično – potrebna je praktična izkušnja, ki jih usposobi za resnične razmere. Vaje, ki simulirajo realne incidente, so izjemno pomembne za preizkušanje odzivnosti, izboljšanje reakcijskega časa in usklajenosti celotne ekipe. Take vaje morajo potekati na vseh nivojih: od internih vaj znotraj podjetja, sektorskih vaj, ki vključujejo določeno industrijo, do nacionalnih in mednarodnih vaj, ki zajemajo širše sodelovanje z drugimi organizacijami ter državami.

1. **Kibernetske vaje na različnih nivojih:**

- **Interni nivo:** Simulacije znotraj podjetja so ključne za preverjanje, kako se odzivna ekipa in vsi zaposleni odzivajo na incident. Te vaje omogočajo, da se preveri učinkovitost odzivnih načrtov, identificirajo morebitne pomanjkljivosti in izboljšajo komunikacijski protokoli znotraj podjetja.
- **Sektorski nivo:** Sodelovanje na sektorskih vajah, kot na primer v energetiki, financah ali zdravstvu, omogoča podjetjem, da preizkusijo svoje reakcije v širšem kontekstu industrije, kjer so izpostavljeni specifičnim grožnjam in tveganjem.
- **Nacionalni nivo:** Nacionalne vaje vključujejo sodelovanje z državnimi organi in drugimi ustanovami, kar omogoča boljše razumevanje državnih odzivnih protokolov in krepitev nacionalne kibernetske odpornosti.
- **Mednarodni nivo:** Mednarodne vaje združujejo organizacije in države z vsega sveta, kar udeležencem omogoča vpogled v globalne kibernetske grožnje ter razvoj mednarodnega sodelovanja in izmenjave znanja.

2. **Igranje vlog – priprava na resnične dogodke:**

   Igranje vlog je še ena pomembna metoda usposabljanja, kjer odgovorne osebe simulirajo konkretne kibernetske incidente in se učijo, kako se nanje odzvati v praksi. Tako se lahko preizkusijo v različnih scenarijih, od kraje podatkov, napadov z izsiljevalsko programsko opremo do vdorov v omrežja. Take vaje povečajo samozavest ekip, saj niso le pripravljene na papirju, temveč imajo tudi dejansko izkušnjo z odzivanjem na incident. To pomeni, da bodo ob morebitnem resničnem napadu delovali hitreje, bolj usklajeno in učinkovito.

3. **Ozaveščanje in usposabljanje vseh zaposlenih:**

   Kibernetska varnost ni le odgovornost odzivnih ekip. Ključnega pomena je, da so vsi zaposleni v podjetju ustrezno ozaveščeni in usposobljeni. Vsak zaposleni je potencialna vstopna točka za napadalce, zato mora poznati osnovne postopke obveščanja in vedeti, koga kontaktirati v primeru zaznave nenavadnega dogodka. Izobraževanja morajo vključevati praktične primere, kot so prepoznavanje lažnih elektronskih sporočil, pravilno ravnanje ob odkritju zlonamerne programske opreme in navodila za varno ravnanje s podatki.

Zelo pomembno je tudi, da se zaposleni ne bojijo priznati, če so storili napako, kot je na primer klik na sumljivo povezavo ali prenos zlonamerne datoteke. Ključna je hitrost prenosa informacij do odgovornih oseb, saj je lahko vsaka sekunda odločilna pri zajezitvi škode. Zaposleni morajo vedeti, da je njihovo obveščanje v takih situacijah prioriteta, in da prikrivanje incidenta lahko privede do veliko hujših posledic za celotno podjetje. Namen preiskave kibernetskega incidenta je analiza vzrokov in posledic incidenta ter s tem izboljšanje varnostnih ukrepov in preprečevanje prihodnjih incidentov, ne pa iskanje krivca, katerega napačni klik je povzročil incident.

Preventiva: Ukrepi za zmanjšanje posledic kibernetskih incidentov

Da bi preprečili kibernetske napade in izrabo prepoznanih tehničnih ranljivosti je ključno, da podjetje izvaja celovite preventivne ukrepe. Kibernetska varnost ni le odzivanje na incidente, temveč predvsem proaktivno delovanje, ki zmanjšuje možnosti za vdor ali zlorabo. Tukaj je nekaj ključnih korakov, ki jih podjetje lahko implementira za izboljšanje svoje obrambne drže.

1. **Redno posodabljanje in upravljanje z varnostnimi popravki (patch management)**

Posodabljanje sistemov in programske opreme je eden izmed najpomembnejših korakov pri preprečevanju kibernetskih napadov. Napadalci pogosto izkoriščajo ranljivosti v zastareli programski opremi, zato je nujno, da so sistemi redno posodobljeni z najnovejšimi varnostnimi popravki. Patch management, torej sistematično uvajanje popravkov je ključnega pomena za zapiranje varnostnih vrzeli. Ranljivosti, ki so odkrite v programski opremi, morajo biti čim prej odpravljene, saj lahko že en nezaščiten element predstavlja vstopno točko za napad.

2. **Redna izvajanja vdornih testiranj**

Vdorna testiranja, znana tudi kot penetracijski testi, so simulirani napadi na sisteme, ki pomagajo identificirati morebitne ranljivosti, preden jih napadalci lahko izkoristijo. Testi se izvajajo z namenom, da se preveri odpornost sistemov in odkrivanje šibkih točk v varnostni infrastrukturi. Pomembno je, da se rezultati teh testiranj ne ustavijo le pri poročilih – odkrite ranljivosti morajo biti tudi dejansko odpravljene, saj le tako podjetje resnično izboljšuje svojo varnostno stanje. Več o pomenu vdornih testiranj in podrobnostih izvedbe si lahko preberete v poglavju 20.

3. **Menjava gesel in upravljanje z dostopi**

Gesla so še vedno eden najpogostejših načinov zaščite sistemov, a tudi eden najpogosteje zlorabljenih elementov varnosti. Podjetje mora vzpostaviti politike redne menjave gesel, uporabo močnih gesel ter dvostopenjsko avtentikacijo, ki dodatno varuje dostop do občutljivih podatkov. Uporaba gesel naj bo podprta tudi z dobro urejenimi dostopnimi pravicami, kar pomeni, da ima vsak zaposleni dostop samo do tistih podatkov in sistemov, ki jih potrebuje za svoje delo.

4. **Varnostne politike in redno usposabljanje**

Vzpostavitev jasnih varnostnih politik, ki določajo ravnanje z občutljivimi podatki, uporabo službenih naprav in dostopov do omrežij, je ključna za zmanjševanje tveganj. Poleg tega morajo zaposleni redno prejemati usposabljanja in posodobitve glede varnostnih praks, saj je človeški faktor pogosto najšibkejši člen. Zaposleni morajo razumeti, kako pomembno je varnostno ravnanje pri vsakodnevnih nalogah, in kako lahko s svojimi dejanji zmanjšajo možnosti za napad.

5. **Dodatni preventivni ukrepi**

- **Šifriranje podatkov:** Zavarovanje podatkov s šifriranjem zagotavlja, da so informacije zaščitene tudi v primeru, če so napadalci uspeli pridobiti dostop.
- **Varnostne kopije:** Redne varnostne kopije pomembnih podatkov zagotavljajo, da lahko podjetje hitro obnovi sisteme v primeru napada, kot so ransomware napadi.
- **Nadzor omrežnega prometa:** Uvedba naprednih sistemov za nadzor omrežja lahko pomaga pri hitrem zaznavanju nenavadnih aktivnosti, ki bi lahko kazale na kibernetski napad.
- **Uporaba dobrih antivirusnih programov:** Zmogljivi antivirusni programi so osnovna obramba pred zlonamerno programsko opremo. Pomembno je izbrati rešitve, ki vključujejo zaščito v realnem času in redno posodabljanje, da se ujamejo nove grožnje.
- **Endpoint Detection and Response (EDR) sistemi:** EDR rešitve omogočajo napredno zaznavanje in odzivanje na grožnje na končnih točkah (kot so računalniki, strežniki ter mobilne naprave). Sproti spremljajo dogajanje na končnih točkah, zazna-

vajo sumljive aktivnosti in omogočajo hitro ukrepanje, kar pripomore k boljšemu nadzoru nad dogajanjem v omrežju.

- **Segmentacija omrežja:** Dobra segmentacija omrežja omogoča ločevanje pomembnih procesov in kritičnih sistemov v ločene segmente z omejenim dostopom. S tem se zmanjšuje tveganje, da bi se napad ali zlonamerna programska oprema hitro razširila po celotnem omrežju. Kritični sistemi, kot so finančni ali proizvodni procesi, morajo biti strogo ločeni in zaščiteni z dodatnimi varnostnimi ukrepi.

S temi preventivnimi ukrepi lahko podjetje bistveno zmanjša tveganje za kibernetske napade in zlorabe, hkrati pa okrepi svojo odpornost na kibernetske grožnje. Ključ je v proaktivnem delovanju, kjer se ranljivosti redno odkrivajo, rešujejo in preprečujejo, preden postanejo resna grožnja.

Obveščanje pristojnih institucij in ključnih strank ob kibernetskih incidentih

Ko pride do kibernetskega incidenta, je hitro in pravilno obveščanje ključnega pomena za omejevanje škode ter zagotavljanje varnosti. Ena od najpomembnejših nalog je pravočasno obveščanje pristojnih državnih in drugih ustreznih institucij za obravnavo kibernetskih groženj, kot so nacionalni ter sektorski CSIRT-i v Sloveniji, med njimi SI-CERT (Slovenian Computer Emergency Response Team). CSIRT-i delujejo kot osrednje točke za obravnavo kibernetskih groženj in incidentov ter podjetjem nudijo podporo pri odzivanju na kibernetske napade. Pravočasno obveščanje ustreznih CSIRT-ov omogoča, da se potrebni ukrepi sprejmejo hitreje, kar lahko pomaga pri omejevanju širjenja incidenta in zmanjšanju škode. Več podrobnosti o obveščanju CSIRT-ov in njihovih postopkih si lahko preberete v poglavju 4.

Poleg obveščanja državnih institucij je izjemno pomembno tudi, da podjetje takoj obvesti svoje ključne stranke, še posebej tiste, ki so neposredno odvisne od njihovih storitev. V primeru incidentov, ki vplivajo na kritične sektorje, kot so zdravstvo, energetika, finance ali druge vitalne dejavnosti, je ključno, da so stranke obveščene o morebitnih motnjah in vplivih na storitve. Hitro obveščanje omogoča, da stranke prilagodijo svoje delovanje in v čim krajšem času vzpostavijo nadomestne rešitve, kar je še posebej pomembno pri kriznih storitvah, kjer je lahko vsak trenutek dragocen.

Krizno komuniciranje z vsemi prizadetimi deležniki je temelj učinkovitega upravljanja incidentov. V takih situacijah mora podjetje vzpostaviti jasne in odprte komunikacijske kanale, da zagotovi transparentnost ter pravočasne informacije. To ne vključuje le tehničnih podrobnosti o incidentu, temveč tudi oceno vpliva na stranke in načrtovane ukrepe za odpravo težav. Dobra krizna komunikacija zmanjšuje negotovost med prizadetimi in krepi zaupanje v podjetje, saj stranke vidijo, da se incident aktivno obvladuje.

Več informacij o najboljših praksah kriznega komuniciranja in obveščanja ključnih strank, zlasti v kriznih sektorjih, najdete v poglavju 25, kjer so predstavljeni konkretni primeri in smernice za učinkovito obvladovanje takih situacij.

Viri:

- ISO 22398:2013: Societal security — Guidelines for exercises
- Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov: Uradni list RS, št. 118/23: https://pisrs.si/pregledPredpisa?id=URED8925&utm=
- Vlada RS, Nacionalni načrt odzivanja na kibernetske incidente (NOKI, 2022): https://www.gov.si/assets/vlade-sluzbe/URSIV/Datoteke/Dokumenti/2022-03-NOKI.pdf?utm

Poglavje 19:
Predstavitev korakov izvedbe vdornih testiranj

POVZETEK

Vdorni testi (penetracijsko testiranje) so nepogrešljiv del varnostnega načrta vsake organizacije, ki želi oceniti in izboljšati odpornost svojih informacijskih sistemov proti kibernetskim grožnjam. Testiranje omogoča simulacijo metod in tehnik, ki jih uporabljajo zlonamerni akterji, da bi identificirali in izkoristili ranljivosti. Rezultati testiranja zagotavljajo vpogled v varnostno stanje organizacije in ponujajo konkretne smernice za izboljšanje varnosti.

Ključne točke:

- Pomen vdornega testiranja za varnost informacijskih sistemov
- Pogostost izvajanja vdornih testiranj
- Oblike vdornih testov: zunanje, notranje, OT, aplikacije
- Metodološki pristopi: Black box (testiranje brez poznavanja notranje strukture ali delovanja sistema), Grey box (testiranje z omejenim poznavanjem notranje strukture) in White box (Testiranje z natančnim poznavanjem notranje strukture in delovanja sistema)
- Izbira ustreznega izvajalca testiranj in certifikati
- Določanje obsega testiranja
- Priprava in kakovost poročil
- Slabe prakse pri vdornem testiranju
- Socialni inženiring: vrste napadov in preprečevanje
- Dinamična usposabljanja za zaposlene.

Kaj je vdorni test test?

Penetracijski test, znan tudi kot vdorno testiranje, je izvedba postopkov in metod, ki jih uporabljajo zlonamerni akterji, da bi odkrili ranljivosti, ki bi jih lahko izkoristili. Gre za napad na varnostne mehanizme sistemov, aplikacij ali omrežij, pri čemer se preverja, kako bi se sistem odzval na dejanski napad. Vdorno testiranje izvajajo izkušeni strokovnjaki za varnost, ki uporabljajo enake metode kot kibernetski kriminalci, da ocenijo, kako varni so sistemi organizacije.

Vdorni test vključuje več ključnih faz:

- **Zbiranje informacij**: Cilj te faze je pridobiti čim več podatkov o ciljnem sistemu, vključno z možnimi vstopnimi točkami, omrežno topologijo, konfiguracijo storitev in drugimi relevantnimi informacijami. Zbiranje informacij lahko vključuje pasivne metode, kot je iskanje javno dostopnih informacij, in aktivne metode, kot so skeniranje omrežij ter storitev.
- **Identifikacija ranljivosti**: S pomočjo specializiranih orodij in tehnik se identificirajo šibke točke, ki bi jih napadalci lahko izkoristili za nepooblaščen dostop ali povzročitev škode. Pri tem so običajno uporabljeni tako avtomatizirani skenerji kot tudi ročno preverjanje, kar poveča natančnost identifikacije.
- **Izkoriščanje ranljivosti**: V tej fazi se izbrane ranljivosti poskuša izkoristiti na varen način, da se simulira potencialni napad in oceni, kakšne bi lahko bile posledice uspešnega vdora. Namen izkoriščanja je oceniti resnični vpliv ranljivosti na sistem in identificirati, do katerih podatkov ali funkcionalnosti lahko dostopa napadalec.
- **Ocena posledic in poročanje:** Izvajalci pripravijo podrobno poročilo, ki vključuje vse faze testiranja, odkrite ranljivosti, njihovo stopnjo tveganja in priporočila za izboljšanje varnosti. Kakovostno poročilo mora biti jasno, strukturirano in praktično uporabno, da naročniku omogoča učinkovito odpravljanje ranljivosti.

Primarni namen vdornega testiranja je najti varnostne pomanjkljivosti in omogočiti njihovo odpravo. Poleg tega testiranje organizacijam pomaga razumeti, kako zlahka bi lahko zlonamerni napadalci ogrozili njihove sisteme. Vdorni testi so pomemben proces pri oblikovanju strategij kibernetske obrambe in zmanjševanju tveganj, saj organizacijam omogočajo realen vpogled v stanje njihove varnosti.

Pomen vdornega testiranja za varnost informacijskih sistemov v organizaciji

Za izvajalce bistvenih storitev je kibernetska varnost ključnega pomena, saj je večina njihovih storitev neposredno odvisna od varnosti informacijskih sistemov. Napadi na te sisteme lahko povzročijo resne posledice, vključno z motnjami v delovanju, izgubo občutljivih podatkov, finančnimi izgubami in resno škodo za ugled organizacije.

V praksi se pogosto srečujemo s scenariji, kjer so varnostne pomanjkljivosti prisotne zaradi napačnih konfiguracij, zastarelih sistemov, neprimernih nastavitev pravic dostopa ali nezadostnega nadzora nad aplikacijami. Vdorni test omogoča pravočasno odkrivanje takih šibkosti, kar zmanjšuje možnosti za uspešen napad in zagotavlja, da so sistemi organizacije varni ter skladni z zakonodajnimi zahtevami.

Pogostost izvajanja vdornih testov

Pogostost izvajanja vdornih testov je odvisna od več dejavnikov, vključno s stopnjo tveganja, pogostostjo sprememb v IT okolju in specifičnimi potrebami organizacije. Priporočljivo je, da organizacije izvajajo vdorne teste vsaj enkrat letno in ob vseh večjih spremembah, ko se sistem posodablja, uvajajo nove aplikacije ali spreminjajo varnostne zahteve. Na podlagi rezultatov testiranj se izvajajo popravki in ponovni testi, kar pomaga zagotoviti neprekinjeno varnost. Prav tako se organizacije odločajo za periodična testiranja, ki omogočajo reden vpogled v stanje sistemov.

Poleg tega organizacije pogosto pripravijo letni ali večletni (dvo- ali triletni) načrt vdornih testiranj, kar je usklajeno tudi s priporočili iz točke 5.35 v Anexu A standarda ISO 27001.

Nekateri dodatni scenariji, ko je vdorno testiranje priporočljivo, vključujejo:

- **Ob večjih posodobitvah:** Ko se implementirajo pomembne spremembe v omrežju, aplikacijah ali infrastrukturi.
- **Po varnostnih incidentih:** Da se preveri, ali so uvedeni popravki in ukrepi učinkoviti ter ali obstajajo dodatne ranljivosti, ki so bile prej spregledane.
- **Pri spremembi poslovnih procesov:** Če nova poslovna funkcionalnost vključuje uporabo novih tehnologij, mobilnih aplikacij ali oblačnih storitev je smiselno izvesti testiranje, da se preveri varnost teh novosti.
- **Pri uvajanju novih partnerstev ali povezav z zunanjimi sistemi:** Da se preveri, ali povezave ne uvajajo dodatnih varnostnih tveganj.

Poleg rednih testiranj je priporočljivo izvesti vdorno testiranje po večjih spremembah v IT infrastrukturi, kot so uvedba novih tehnologij, migracija na oblak ali sprememba omrežnih konfiguracij. Organizacije z visoko stopnjo izpostavljenosti, kot so finančne institucije, vladne agencije in ponudniki kritične infrastrukture, naj razmislijo o pogostejšem testiranju, tudi večkrat letno.

Oblike vdornih testov

Vdorno testiranje je prilagodljivo in se lahko izvaja na različne načine, odvisno od specifičnih potreb organizacije. Spodaj so opisane glavne oblike testiranj:

1. **Zunanje testiranje:** Osredotoča se na zunanje komponente sistema, kot so spletni strežniki, požarni zidovi, VPN-ji in druge storitve organizacije, ki so dostopne iz interneta. Cilj je odkriti ranljivosti, ki bi jih lahko izkoristil napadalec izven organizacije. Testiranje običajno vključuje preverjanje odprtih vrat, napačno konfiguriranih storitev, preverjanje stanja verzij programske opreme, preverjanje varnosti podatkovnih prenosov in drugih izpostavljenih ranljivosti.
2. **Notranje testiranje:** Izvajanje napadov znotraj organizacije, kjer ima napadalec že dostop do omrežja. Ta vrsta testiranja je zlasti pomembna za odkrivanje ranljivosti, ki izhajajo iz napak v konfiguraciji, nezadostnih pravic dostopa ali pomanjkljivih varnostnih ukrepov znotraj organizacije. Notranje testiranje pogosto izpostavi varnostne pomanjkljivosti, ki bi lahko bile posledica slabo urejenega upravljanja identitet, neprimernih pravic dostopa ali neustrezno zaščitenih občutljivih podatkov.
3. **OT (Operational Technology) omrežja:** Ta testiranja se izvajajo na sistemih, ki so ključni za operativne procese, kot so industrijski nadzorni sistemi, SCADA in druge oblike industrijske avtomatizacije. Varnost teh sistemov je ključna za zagotavljanje nemotenega delovanja procesov, zato je pomembno, da se preverijo ranljivosti, ki bi lahko vplivale na operativno učinkovitost in varnost. Testiranje OT omrežij zahteva posebne pristope, saj se prepletajo s fizičnimi procesi, ki jih napaka lahko neposredno prizadene.
4. **Pregled mobilnih aplikacij:** Namenjeno identifikaciji varnostnih pomanjkljivosti v mobilnih aplikacijah, ki so dostopne na pametnih napravah. To vključuje pregled kode, preverjanje varnosti komunikacij med aplikacijo in strežnikom ter preverjanje zaščite podatkov v aplikaciji. Pomembno je preveriti, da aplikacije ne izpostavljajo občutljivih podatkov uporabnikov, kako učinkovito uporabljajo preverjanje poverilnic in šifriranje ter ali imajo zaščito pred povratnimi inženirskimi analizami.
5. **Pregled aplikacij:** Pregled spletnih in namiznih aplikacij vključuje preverjanje ranljivosti, kot so vnos SQL kode (SQL injection), napačno upravljanje sej, nepravilno preverjanje identitete uporabnikov in druge pomanjkljivosti, ki bi lahko vodile do nepooblaščenega dostopa ali kraje podatkov. Testiranje aplikacij je ključno za zagotavljanje varnosti aplikacij, saj izpostavi ranljivosti, ki lahko nastanejo zaradi napak v

kodeksu ali napačne integracije varnostnih funkcij.

6. **Pregled izvorne kode:** Analiza izvorne kode aplikacij vključuje najprej avtomatizirano pregledovanje, s čimer je mogoče odkriti napake v programski kodi, ki lahko predstavljajo varnostne ranljivosti. Gre za poglobljen proces, v katerem se nato uporabljajo tudi metode ročnega preverjanja, da se odkrijejo težave, ki jih avtomatizirana testiranja morda ne bi zaznala. Ta pristop zagotavlja visoko stopnjo varnosti, saj analiza poteka neposredno na ravni izvorne kode. Ta vrsta testiranja omogoča zgodnje odkrivanje in odpravljanje ranljivosti, še preden aplikacija doseže produkcijsko okolje.

Metodološki pristopi k vdornemu testiranju

Vdorno testiranje se lahko izvaja na več načinov, odvisno od stopnje dostopa, ki ga imajo ekipe do informacij o testiranem sistemu:

1. **Black Box Testing:** Pri tej metodi se izvaja napad, kjer napadalec nima nobenih informacij o tarči. Ekipa deluje kot zunanji napadalec, ki poskuša pridobiti dostop s pomočjo javno dostopnih informacij in orodij. Ta pristop omogoča preverjanje, kako ranljiv je sistem za napadalce brez vedenja o sistemu in je še posebej učinkovit pri odkrivanju ranljivosti, ki so posledica napačnih konfiguracij ali nezadostno zaščitenih zunanjih storitev.
2. **Grey Box Testing:** Pri tej metodi ima testirna ekipa delne informacije o sistemu, kot so uporabniški dostopi, dokumentacija omrežij ali arhitektura sistema. S tem se poveča učinkovitost testiranja, saj ekipa lahko ciljno išče ranljivosti na podlagi pridobljenih informacij. Grey Box metoda je optimalna kombinacija, saj omogoča testiranje z določenimi informacijami, hkrati pa simulira napade z določeno stopnjo notranjega dostopa, kot bi jih lahko izvedli zaposleni z omejenimi pravicami.
3. **White Box Testing:** Izvajalci imajo popoln dostop do informacij o sistemu, vključno z izvorno kodo, konfiguracijami in topologijo omrežja. Ta pristop omogoča najcelovitejšo analizo varnostnih pomanjkljivosti, saj lahko ekipa preizkusi vse možne scenarije napadov znotraj sistema. Gre za temeljit pristop, ki omogoča odkrivanje tudi najmanjših napak v izvorni kodi ali sistemskih nastavitvah, ki bi sicer lahko ostale spregledane.

Izbira ustreznega izvajalca vdornih testiranj

Izbira izvajalca za vdorno testiranje je ključnega pomena za uspeh in kakovost testiranja. Pri izbiri je pomembno preveriti njihove izkušnje, reference in usposobljenost. Ključno je, da izberete izvajalca, ki ima izkušnje s testiranjem v vaši industriji, razume specifične varnostne izzive in se ujema s sistemi, ki jih želite testirati, saj morajo imeti temu ustrezne certifikate. Dober izvajalec bo imel ekipo strokovnjakov z različnimi znanji in certifikati, kot so Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), GIAC Penetration Tester (GPEN), CompTIA PenTest+ ter Certified Information Security Manager (CISM), ki nudijo vpogled v njihovo usposobljenost in uporabo priznanih metod. Poleg certifikatov je pomembno tudi poznavanje vodil, kot je OWASP Top 10, ki opredeljuje najpogostejša varnostna tveganja pri spletnem razvoju in je ključna referenca za prepoznavanje ranljivosti v aplikacijah.

Poleg strokovnosti in tehničnega znanja je pomembno preveriti tudi pristop izvajalca k izvedbi testiranja. Dober izvajalec bo zagotovil ročne preglede ranljivosti poleg avtomatiziranih pregledov, saj je ročno testiranje ključno za odkrivanje kompleksnejših ranljivosti, ki jih avtomatizirana orodja morda ne zaznajo. Pomembno je, da izvajalec upošteva specifične zahteve in omejitve organizacije ter ponudi prilagojeno rešitev.

Treba je tudi preveriti kakovost poročil, ki jih izvajalec pripravlja. Poročila morajo biti jasna, strukturirana in vsebovati praktična priporočila. Kakovost poročila je pogosto dober pokazatelj strokovnosti in zanesljivosti izvajalca.

Določanje obsega testiranja

Pred začetkom testiranja je ključno jasno definirati obseg testiranja, ki mora vključevati določitev ciljev, omejitev in vrst testiranj. Obseg testiranja mora biti usklajen s potrebami organizacije in specifičnimi tveganji, ki jih želite nasloviti. V praksi se obseg pogosto definira z določitvijo natančnih parametrov, kot so obseg IP-naslovov (IP range), vrsta aplikacij ali specifične komponente, ki jih želite preizkusiti, kar omogoča bolj ciljno usmerjeno testiranje.

Pri določitvi obsega je pomembno tudi, da se dogovorite o časovnem okviru, dovoljenjih za dostop do sistemov in morebitnih omejitvah, kot so občutljivi podatki ali kritične komponente sistema, pri čemer je treba poskrbeti, da pregled ne povzroči izpada ali motenj v delovanju. Definiranje obsega je tudi priložnost, da se organizacija pogovori o pričakovanjih glede poročanja, sledenja najdenim ranljivostim in načinu podajanja priporočil.

Kvalitetna priprava obsega testiranja omogoča, da izvajalec razume, kaj je treba testirati in kakšne rezultate pričakujete. Tako se zmanjšajo možnosti za nesporazume glede pričakovanj, obenem pa se zagotovi, da bo testiranje osredotočeno na najbolj kritične vidike varnosti.

Kakšna morajo biti poročila?

Poročila o vdornem testiranju so ključni del procesa, saj zagotavljajo vpogled v najdene ranljivosti, ocenjujejo tveganja in predlagajo ukrepe za izboljšanje varnosti. Kvalitetno poročilo mora vključevati jasno in razumljivo predstavitev ugotovitev, oceno vpliva ranljivosti, podrobno razlago uporabljene metodologije in konkretna priporočila za odpravo pomanjkljivosti.

Poročila morajo biti prilagojena uporabnikom, ki bodo z njimi delali – od tehničnih ekip, ki bodo odpravljale ranljivosti, do vodstva, ki mora razumeti širšo sliko varnostnih tveganj. Pomembno je, da poročilo vključuje tudi jasno razmejitev med ranljivostmi, ki jih je mogoče takoj popraviti, in tistimi, ki zahtevajo dolgoročnejše načrtovanje ter naložbe. Poročilo mora biti več kot le tehnični dokument – mora služiti kot osnova za odločanje in načrtovanje ukrepov za izboljšanje varnosti.

Slabe prakse pri vdornem testiranjih

Slabe prakse pri vdornem testiranjih lahko bistveno zmanjšajo učinkovitost in zanesljivost ugotovitev, kar vodi v napačne varnostne ukrepe. Ena najpogostejših slabih praks je izvajanje zgolj avtomatiziranih testiranj, brez ročne potrditve ranljivosti. Avtomatizirana orodja pogosto zaznajo številne ranljivosti, a brez ročnega preverjanja ostanejo mnoge kompleksnejše pomanjkljivosti neopažene, ali pa so zaznave napačne. Takšen pristop lahko daje lažen občutek varnosti, saj nekatere ranljivosti zahtevajo bolj poglobljeno analizo, ki jo lahko zagotovi le usposobljen strokovnjak.

Druga pogosta težava pri testiranju varnosti je prevelik poudarek na številu odkritih ranljivosti namesto na njihovi kritičnosti in jasnosti rešitev. Pogosto se namreč dogaja, da organizacije zmotno verjamejo, da obsežna poročila z dolgim seznamom ranljivosti pomenijo temeljitejše testiranje. V praksi pa so kakovost poročila, jasnost opisa ranljivosti in praktična priporočila za njihovo odpravo tisto, kar dejansko prinaša vrednost. Na primer, dolgotrajno navajanje manj pomembnih ranljivosti lahko vodi do zanemarjanja ključnih, kritičnih pomanjkljivosti.

Pomanjkanje jasnih smernic za odpravljanje ranljivosti, nepregledna struktura poročila in površno obravnavanje ključnih ranljivosti lahko zmanjšajo praktično uporabnost poročila za varnostne ekipe ter otežijo načrtovanje izboljšav varnosti.

Pomembno je, da organizacija od izvajalca zahteva jasno metodologijo, ki vključuje tako avtomatizirane kot ročne preglede, jasna in uporabna poročila ter konkretna priporočila za odpravo težav, razvrščena glede na kritičnost. Izvajalci morajo biti sposobni zagotoviti smiselne vpoglede in rešitve, ne zgolj generičnih rezultatov.

Socialni inženiring in usposabljanje

Socialni inženiring se pri vdornih testiranjih pogosto uporablja kot metoda za pridobitev začetnih dostopov ali občutljivih informacij, ki omogočajo nadaljnje preizkušanje varnosti sistemov. Predstavlja eno največjih groženj kibernetski varnosti, saj izkorišča človeški vidik, ki je pogosto najšibkejši člen v varnostni verigi. Pri socialnem inženiringu napadalci manipulirajo z zaposlenimi, da pridobijo dostop do občutljivih informacij, omrežij ali fizičnih prostorov. Učinkovitost socialnega inženiringa je odvisna od tega, kako dobro se napadalec pripravi in prilagodi svoje tehnike specifičnim značilnostim podjetja. Pomembno je, da izvajalci socialnega inženiringa opravijo temeljito predhodno raziskavo, preden začnejo s testiranjem, saj s tem bistveno povečajo uspešnost svojih napadov.

Ena od ključnih faz priprave je zbiranje informacij o podjetju, kot so njegovi poslovni procesi, organizacijska struktura, javno dostopne kontaktne informacije in morebitne specifične interne politike. S tem pristopom se lahko izvajalec osredotoči na izdelavo bolj usmerjenih napadov, kot so e-poštna sporočila ali SMS-ji, ki so prilagojeni podjetju in njegovim zaposlenim. Personalizacija sporočil, kot je uporaba specifičnih terminov, imen projektov ali drugih podrobnosti, ki so značilne za podjetje, bistveno poveča verjetnost, da bodo zaposleni na takšna sporočila tudi odgovorili. Zelo splošna in generična sporočila pogosto izzovejo sum, medtem ko se prilagojena sporočila zdijo legitimna ter so veliko bolj učinkovita.

Socialni inženiring vključuje različne tehnike, kot so e-poštni napadi (phishing), SMS sporočila (smishing), lažni telefonski klici (vishing) in fizični vdori.

E-poštni napadi (Phishing email) so ena najpogostejših metod socialnega inženiringa, kjer napadalec pošlje e-pošto, ki na videz prihaja iz zaupanja vrednega vira. Takšna sporočila pogosto vsebujejo povezave do lažnih prijavnih strani. Pri usmerjenih napadih, imenovanih tudi spear-phishing, napadalec uporablja informacije, pridobljene med predhodnim raziskovanjem, da naredi e-poštno sporočilo čim bolj verodostojno in specifično za prejemnika. Na primer, sporočilo lahko simulira notranjo komunikacijo med oddelki ali vsebuje informacije o aktualnih projektih, kar zmanjša sum zaposlenega.

SMS napadi (Smishing) so podobni phishing napadom, vendar uporabljajo kratka sporočila SMS. V tem primeru napadalec pošlje sporočilo, ki vsebuje zlonamerno povezavo ali navodila za posredovanje osebnih podatkov. Takšne napade je težje prepoznati, saj sporočila pogosto simulirajo komunikacijo od mobilnih operaterjev, bank ali drugih ponudnikov storitev, ki redno komunicirajo prek SMS-jev. Prilagojena vsebina sporočil, ki vključuje specifične informacije o podjetju, močno poveča uspešnost teh napadov, saj se zdi, da prihajajo iz zanesljivega vira.

Lažni telefonski klici (Vishing) vključujejo uporabo telefonije za pridobivanje občutljivih informacij, kot so gesla ali finančni podatki. Napadalci se pogosto predstavljajo kot IT podpora, bančni uslužbenci ali drugi uradni predstavniki, ki nujno potrebujejo dostop do določenih informacij. Poleg zbiranja podatkov lahko napadalec zahteva tudi dovoljenje za vzpostavitev oddaljene povezave, na primer s pomočjo RDP (Remote Desktop Protocol) seje, kar mu omogoča neposreden dostop do računalnika žrtve. Vishing napadi so še posebej nevarni, ker se zanašajo na neposredno interakcijo z zaposlenimi, ki so lahko pod pritiskom, da odgovarjajo na prošnje, saj napadalec pogosto ustvari občutek nujnosti ali krize.

Fizični vdori so še ena oblika socialnega inženiringa, kjer napadalec fizično vstopi v poslovne prostore organizacije, bodisi da dostopa do notranjih omrežij, občutljivih dokumentov ali da fizično namesti zlonamerno opremo, kot je beležnik tipkanja (keylogger) ali USB naprave. Napadalci se lahko predstavljajo kot dostavljavci, vzdrževalno osebje ali celo kot zaposleni, da bi pridobili dostop do varovanih območij. Testiranje fizičnih vdorov pomaga organizacijam oceniti, kako učinkoviti so njihovi fizični

varnostni ukrepi, kot so dostopne kontrole, varnostne kamere in ozaveščenost zaposlenih o nevarnosti nepooblaščenega dostopa.

Za uspešno zaščito pred socialnim inženiringom pa zgolj tehnični varnostni ukrepi niso dovolj; ključnega pomena je tudi stalno usposabljanje zaposlenih. Pomembno je, da se izvajajo redna predavanja in izobraževanja, ki obravnavajo različne tehnike socialnega inženiringa ter načine, kako jih prepoznati in se jim izogniti. Vendar pa morajo biti ta izobraževanja dinamična in interaktivna, da zares pritegnejo pozornost udeležencev ter jih spodbudijo k sodelovanju. Klasična predavanja brez interakcije pogosto ne dosežejo želenega učinka, saj se pomembne informacije hitro pozabijo.

Usposabljanja morajo aktivno vključevati zaposlene z uporabo vprašanj, diskusij in praktičnih primerov, ki simulirajo resnične napade. Dodatno vrednost lahko prinesejo platforme, ki omogočajo sprotno izvajanje kvizov med predavanji, s čimer se poslušalci spodbujajo k aktivnemu sodelovanju. Takšni kvizi pomagajo preveriti razumevanje in takojšnjo uporabo naučenih vsebin, kar je ključnega pomena za utrjevanje znanja. Dinamična usposabljanja z uporabo resničnih primerov in simulacij omogočajo zaposlenim, da se bolje seznanijo z načini napadov, ter kako naj ustrezno reagirajo v takšnih situacijah.

V končni fazi socialni inženiring ni le tehnični izziv, temveč predvsem psihološka igra, kjer zmagujejo tisti, ki znajo najbolje manipulirati z informacijami in človeškim vedenjem. Organizacije, ki razumejo pomembnost stalnega usposabljanja in dinamične prilagoditve varnostnih politik, imajo veliko boljšo možnost, da se učinkovito zaščitijo pred tovrstnimi napadi.

Viri:

- Marta Barceló, Pete Herzog (2010). OSSTMM 3 – The Open Source Security Testing Methodology Manual. https://www.isecom.org/OSSTMM.3.pdf
- NACIONALNI NAČRT ODZIVANJA NA KIBERNETSKE INCIDENTE: https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Dokumenti/2022-03-NOKI.pdf
- P. Vats, M. Mandot and A. Gosain, „A Comprehensive Literature Review of Penetration Testing & Its Applications," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2020, pp. 674-680, doi: 10.1109/ICRITO48877.2020.9197961.
- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)

Poglavje 20
Napotki pri izvajanju in upravljanju varnostnih kopij, vključno z dnevniškimi zapisi

POVZETEK

Učinkovito upravljanje varnostnih kopij je ključno za zaščito podatkov in zagotavljanje nemotenega poslovanja. Pravilna izbira podatkov, določitev frekvence kopiranja ter uporaba primernih metod (popolne, diferencialne, inkrementalne kopije) zmanjšujejo tveganja za izgubo podatkov. Pomembna je geografska redundanca z lokalno in oddaljeno lokacijo hranjenja, pri čemer je treba upoštevati zakonodajne zahteve. Priprava dokumentacije in standardiziranih postopkov za arhiviranje ter redno testiranje obnovitve podatkov omogočata hitro in učinkovito ukrepanje ob incidentih. Beleženje dnevniških zapisov zagotavlja sledljivost ter omogoča hitro odkrivanje in odpravljanje težav.

Ključne točke:

- Izbira kritičnih podatkov za varnostne kopije
- Dnevno, tedensko in mesečno kopiranje glede na naravo podatkov
- Popolne, diferencialne in inkrementalne varnostne kopije
- Lokalna hramba in oblačne storitve z geografsko redundanco
- Preverjanje celovitosti kopij s kontrolnimi vsotami in integracijskimi testi
- Standardizirani postopki za arhiviranje in obnovitev podatkov
- Protokoli za različne scenarije, kot so kibernetski napadi ali popolne okvare
- Testiranje postopkov obnovitve, vključujoč simulacije okvar
- Beleženje dnevniških zapisov: status, napake in spremembe v podatkih
- Skladnost z zakonodajo (npr. Zakon o varstvu osebnih podatkov) pri shranjevanju kopij.

1. Izbira podatkov za varnostne kopije

Ko govorimo o varnostnih kopijah, je bistvenega pomena, da pravilno izberemo podatke, ki jih želimo arhivirati. Vsaka organizacija, še posebej tista, ki upravlja kritične storitve, mora skrbno določiti, kateri podatki so ključni za nemoteno delovanje in katere bi lahko obnovili brez večjih posledic. Kritični podatki, kot so finančne evidence, vse vrste osebnih podatkov, prometni ali lokacijski podatki, baze strank, konfiguracije sistemov, dnevniški zapisi, podatki o zaposlenih, intelektualna lastnina, pa tudi operativne informacije so navadno na vrhu seznama za varnostne kopije.

Pri izbiri podatkov za varnostno kopiranje je treba upoštevati tudi stopnjo občutljivosti podatkov in njihovo pravno regulacijo. Za izvajalce kritičnih storitev je zlasti pomembno zagotoviti celovitost in razpoložljivost teh podatkov, saj so lahko motnje usodne za poslovanje. Varnostne kopije morajo zato vključevati vse podatke, potrebne za hitri povratek v normalno delovanje ob morebitnih izpadih ali incidentih. Prav tako pa je treba poskrbeti, da so varnostno kopirani podatki pravilno zaščiteni pred nepooblaščenim dostopom.

Ko se odločamo, katere podatke bomo varnostno kopirali, je smiselno vzpostaviti jasno politiko varnostnega kopiranja. Ta politika določa kriterije, na podlagi katerih se določijo pomembni podatki za varnostno kopiranje. Kriteriji so lahko različni in temeljijo na naravi podatkov, njihovi pomembnosti za poslovanje ter stopnji občutljivosti. Pogosto se uporabijo kategorije, kot so „visoko kritični podatki," „podatki srednje pomembnosti" in „manj pomembni podatki." Tako je možno optimizirati porabo virov za varnostno kopiranje in zagotoviti, da se največji poudarek namenja podatkom, ki so ključni za delovanje.

Za izvajalce kritičnih storitev, kjer je vsaka minuta nedelovanja lahko draga, je bistveno, da politika varnostnega kopiranja omogoča hitro in zanesljivo obnovitev podatkov. V tem kontekstu je treba tudi zagotoviti, da so varnostne kopije shranjene na več lokacijah, ki morajo biti strogo izbrane z upoštevanjem zakonodaje. Pomembno je, da se podatki hranijo na nadomestnih lokacijah znotraj Republike Slovenije, oziroma če dovoljuje zakonodaja znotraj EU, s posebnim poudarkom na geografski ločenosti.

2. Perioda varnostnega kopiranja

Ena izmed ključnih odločitev pri vzpostavljanju učinkovitega sistema varnostnih kopij je določitev frekvence, s katero se bodo podatki varnostno kopirali. Perioda varnostnega kopiranja mora temeljiti na več dejavnikih, kot so narava podatkov, pogostost njihovega spreminjanja in pomembnost za poslovanje. V praksi se najpogosteje uporabljajo dnevne, tedenske in mesečne periodičnosti.

Dnevno, tedensko, mesečno varnostno kopiranje

- **Dnevno varnostno kopiranje** je najpogosteje uporabljena oblika, zlasti v okoljih, kjer se podatki pogosto spreminjajo. To je smiselna izbira v organizacijah, kjer so podatki izjemno dinamični, kot so finančne institucije, kjer se transakcije izvajajo neprestano.
- **Tedensko varnostno kopiranje** lahko zadostuje za manj dinamična okolja, kjer podatki ne doživljajo toliko sprememb dnevno. Tedenske kopije omogočajo zmanjšanje obremenitev omrežja in prostora za shranjevanje, vendar še vedno zagotavljajo relativno hitro obnovitev.
- **Mesečno varnostno kopiranje** se uporablja predvsem za arhivske namene ali za shranjevanje podatkov, ki se ne spreminjajo pogosto, a so kljub temu pomembni za dolgoročno hrambo. To je koristno zlasti za dokumentacijo in zgodovinske zapise.

Določanje ustrezne frekvence glede na naravo podatkov

Izbor frekvence varnostnega kopiranja mora temeljiti na natančni oceni pomembnosti podatkov. Bolj kot so podatki kritični za poslovanje in pogosteje kot se spreminjajo, bolj

pogoste morajo biti varnostne kopije. Tukaj je smiselno izdelati analizo tveganja, ki upošteva verjetnost izgube podatkov in posledice za poslovanje v primeru izgube.

Kriteriji za določanje frekvence:

- Ali se podatki spreminjajo dnevno, tedensko ali mesečno?
- Kakšne so zahteve za hitro obnovitev podatkov?
- Kako pogosto so potrebni varnostni pregledi in preizkušanje kopij?

Samodejno ali ročno varnostno kopiranje

Samodejno varnostno kopiranje je danes standard v večini organizacij, saj omogoča zanesljivost in manjšo možnost človeških napak. Samodejni postopki so programirani tako, da se izvedejo v vnaprej določenih intervalih, brez potrebe po ročnih posegih. To je uporabno zlasti za velike sisteme, kjer je ročno varnostno kopiranje neizvedljivo ali preveč zamudno.

V določenih primerih pa lahko ročno varnostno kopiranje še vedno pride v poštev. Na primer, pri občasnem kopiranju specifičnih podatkovnih zbirk ali arhivov, kjer avtomatizacija ni potrebna. Poleg tega je lahko ročni nadzor koristen pri izdelavi kopij pred pomembnimi sistemskimi spremembami ali nadgradnjami.

3. Načini in tehnologije varnostnega kopiranja

Pri načrtovanju varnostnih kopij je pomembno izbrati primeren način kopiranja, ki bo zagotavljal tako varnost kot učinkovitost pri shranjevanju podatkov. Tehnologije varnostnega kopiranja so zasnovane z namenom optimizacije porabe prostora, časa in sistemskih virov. Najpogostejši načini varnostnega kopiranja so popolne, diferencialne in inkrementalne varnostne kopije, pri čemer ima vsak od teh načinov svoje prednosti ter omejitve.

Popolne (celovite) varnostne kopije

Popolna varnostna kopija pomeni, da se celoten sistem ali podatkovni niz kopira v celoti. Vse datoteke, mape in baze podatkov se shranijo na ciljno lokacijo. Prednost popolnih varnostnih kopij je preprosta in zanesljiva obnova podatkov, saj vsebujejo celoten nabor informacij. Pomanjkljivost pa je, da popolne kopije zahtevajo veliko prostora za shranjevanje in dolge časovne okvire za izvedbo, zlasti v okoljih z velikimi količinami podatkov.

Ključne značilnosti popolnih varnostnih kopij:

- Celoten nabor podatkov se shrani na enkrat.
- Omogoča najhitrejšo obnovo v primeru incidenta.
- Zahteva večjo količino prostora za shranjevanje.

Diferencialne varnostne kopije

Diferencialna varnostna kopija zajame samo tiste datoteke, ki so bile spremenjene od zadnje popolne varnostne kopije. To omogoča zmanjšanje prostora, potrebnega za shranjevanje, saj kopije ne vključujejo vseh podatkov, temveč samo spremembe. Obnova iz diferencialnih kopij je še vedno relativno hitra, saj zahteva le zadnjo popolno varnostno kopijo in zadnjo diferencialno kopijo.

Diferencialne varnostne kopije so primerne za okolja, kjer spremembe niso pogoste, vendar še vedno zahtevajo stalno nadgradnjo varnostnih kopij.

Inkrementalne varnostne kopije

Inkrementalna varnostna kopija shranjuje samo tiste podatke, ki so bili spremenjeni od zadnje varnostne kopije – bodisi popolne, diferencialne ali inkrementalne. To je najučinkovitejši način kopiranja, ko gre za porabo prostora in čas kopiranja, vendar pa ima največje pomanjkljivosti pri obnovi. Obnovitev iz inkrementalnih kopij zahteva dostop do vseh prejšnjih inkrementalnih kopij, kar lahko povzroči daljši čas obnovitve in večjo zapletenost postopka.

Prednosti in slabosti inkrementalnih kopij:

- Minimalna poraba prostora.
- Najhitrejša izdelava varnostnih kopij.
- Daljša in kompleksnejša obnova podatkov.

Varnostno kopiranje v oblak ali lokalno shranjevanje

Sodobne rešitve za varnostno kopiranje se v veliki meri naslanjajo na varnostno kopiranje v oblaku, ki omogoča geografsko ločenost in redundanco podatkov. Kopiranje v oblaku ponuja skalabilnost in fleksibilnost, saj omogoča shranjevanje velikih količin podatkov brez potrebe po fizičnih strežnikih na lokaciji. Pomembno je poudariti, da morajo biti podatki, zlasti za izvajalce kritičnih storitev, shranjeni na nadomestnih lokacijah znotraj Republike Slovenije oz. če dovoljuje zakonodaja znotraj EU. Izogibanje shranjevanju podatkov zunaj EU je ključnega pomena zaradi varnostnih in pravnih tveganj. Za nekatere podatke je že v predpisih določeno, kjer se smejo in kje se ne smejo obdelovati ali hraniti (Zakon o varstvu osebnih podatkov (Ur.l.RS, še. 163/22) npr. v 23. členu določa posebne kategorije podatkov, ki se ne smejo hraniti izven ozemlja Republike Slovenije, kar velja tudi za varnostne kopije teh podatkov). Pred odločitvijo, kje boste hranili varnostne kopije, se zato prepričajte, ali za vrsto podatkov, ki jih obdelujete, veljajo kakšna posebna pravila ali zahteve.

Lokalno shranjevanje pa še vedno ostaja pomembno v številnih organizacijah, kjer se uporablja za hitrejši dostop do podatkov in krajše čase obnovitve. Pri tem načinu je pomembno poskrbeti, da so podatki zaščiteni in da obstaja ustrezen sistem za nadzor ter preverjanje celovitosti varnostnih kopij.

4. Lokacija arhiviranja varnostnih kopij

Lokacija arhiviranja varnostnih kopij je eden najpomembnejših dejavnikov, ki vpliva na varnost in zanesljivost shranjenih podatkov. Izbira prave lokacije za hrambo varnostnih kopij mora temeljiti na več kriterijih, kot so dostopnost, geografska ločenost, pravna skladnost ter zaščita pred fizičnimi in kibernetskimi grožnjami. Lokacije se lahko razlikujejo glede na to, ali gre za lokalno ali oddaljeno hrambo podatkov, pri čemer vsaka možnost ponuja svoje prednosti in slabosti.

Lokalne varnostne kopije

Lokalne varnostne kopije se shranjujejo na fizičnih napravah, ki so nameščene neposredno znotraj infrastrukture organizacije. To omogoča hitrejši dostop do podatkov, kar je zlasti pomembno pri obnovi v nujnih primerih. Lokalna hramba je tudi koristna za organizacije, ki želijo imeti popoln nadzor nad fizično varnostjo svojih podatkov, saj ni odvisna od tretjih strank.

Vendar pa lokalne varnostne kopije predstavljajo tveganje, če se uporabljajo kot edina oblika shranjevanja podatkov. V primeru večje katastrofe, kot so požar, poplava ali kibernetski napad, lahko pride do izgube tako primarnih podatkov kot tudi lokalnih varnostnih kopij. Zato se pogosto priporoča uporaba kombinacije lokalnih in oddaljenih kopij.

Oddaljene varnostne kopije

Oddaljene varnostne kopije predstavljajo drugo plast zaščite, saj se shranjujejo na lokacijah, ki so geografsko ločene od primarnih sistemov. To zmanjšuje tveganje, da bi bile varnostne kopije uničene skupaj s primarnimi podatki v primeru lokalnih nesreč. Oddaljena hramba je lahko izvedena preko oblačnih storitev ali s fizičnim prenosom podatkov na oddaljene strežnike.

Pomembno je, da se pri oddaljenih kopijah upošteva zakonodaja o hrambi podatkov, zlasti pri občutljivih informacijah. Za izvajalce kritičnih storitev je nujno, da so podatki shranjeni v skladu s predpisi, s poudarkom na varnosti in zasebnosti. Zbiranje in shranjevanje podatkov na lokacijah izven EU lahko privede do resnih pravnih zapletov ter povečanja tveganj.

Izbira med lastnim podatkovnim centrom in oblačnimi storitvami

Odločitev med shranjevanjem podatkov v lastnem podatkovnem centru ali uporabo oblačnih storitev je odvisna od več dejavnikov, kot

so stroški, zmogljivosti in nadzor nad podatki. Lastni podatkovni centri omogočajo večji nadzor nad varnostnimi postopki in fizično zaščito, vendar so lahko dragi za vzdrževanje ter upravljanje, zlasti za manjše organizacije.

Oblačne storitve ponujajo prilagodljivost in skalabilnost, saj omogočajo hitro povečevanje prostora za shranjevanje brez potrebe po večjih kapitalskih naložbah. Prednost oblačnega varnostnega kopiranja je tudi, da zagotavlja geografsko ločenost in redundanco brez potrebe po dodatni fizični infrastrukturi. Vendar pa je pri oblačnih rešitvah ključnega pomena izbrati ponudnika, ki shranjuje podatke znotraj EU in zagotavlja skladnost s slovensko ter evropsko zakonodajo o varstvu podatkov. Pri izbiri ponudnikov oblačnih storitev je potrebno upoštevati tudi vrsto in občutljivost podatkov, ki se bodo shranjevala pri ponudniku, zakonodajna tveganja povezana z lastništvom ali matično državo ponudnika, zmožnostjo prehoda k drugemu ponudniku, raven zrelosti ponudnika pri zagotavljanju varnosti storitev (npr. izkazuje skladnost z evropsko priznanimi varnostnimi standardi ter certifikacijskimi shemami).

Geografska redundanca in zunanje lokacije

Geografska redundanca pomeni, da so varnostne kopije shranjene na več lokacijah, ki so geografsko ločene. To je ključnega pomena za zagotavljanje kontinuitete poslovanja v primeru naravnih nesreč, okvar strojne opreme ali drugih motenj. Redundantne lokacije morajo biti izbrane tako, da zmanjšujejo tveganje izgube podatkov, pri tem pa je pomembno upoštevati varnostne standarde in zakonske zahteve.

Izvajalci kritičnih storitev morajo biti posebej pozorni na lokacijo shranjevanja varnostnih kopij. Redundantna hramba podatkov mora biti organizirana znotraj EU, saj to zagotavlja večjo pravno zaščito in skladnost z zakonodajo. Hranjenje podatkov na lokacijah izven EU lahko predstavlja dodatna tveganja, zato se takšne prakse običajno odsvetujejo.

5. Preverjanje celovitosti in kakovosti varnostnih kopij

Vzpostavitev varnostnih kopij je le prvi korak v zagotavljanju zaščite podatkov. Da bi bile varnostne kopije dejansko uporabne in zanesljive, je ključnega pomena redno preverjanje njihove celovitosti ter kakovosti. Brez preverjanja in testiranja lahko kopije vsebujejo napake ali manjkajoče podatke, kar lahko povzroči resne težave, ko je potrebna obnova.

Pomen rednega preverjanja varnostnih kopij

Redno preverjanje varnostnih kopij je bistvenega pomena, saj lahko le tako zagotovimo, da so podatki pravilno shranjeni in dostopni za obnovo. Če se varnostne kopije ne preverjajo sistematično, obstaja nevarnost, da bi bile poškodovane, nepopolne ali celo nedosegljive v kritičnih trenutkih. Pogostost preverjanja je odvisna od narave podatkov in sistema kopiranja, vendar se na splošno priporoča, da se preverjanje izvaja vsaj tedensko ali mesečno, odvisno od frekvence varnostnega kopiranja.

Preverjanje celovitosti podatkov ne vključuje samo tehničnega pregleda, ampak tudi analizo ali so varnostne kopije v skladu s poslovnimi in zakonskimi zahtevami. Podjetja, ki upravljajo z občutljivimi podatki, morajo upoštevati pravne zahteve glede varnosti, skladnosti in shranjevanja podatkov, zlasti izvajalci kritičnih storitev.

Orodja in metode za preverjanje celovitosti podatkov

Za preverjanje celovitosti varnostnih kopij obstajajo različna orodja in metode, ki so zasnovana tako, da prepoznajo morebitne napake ter zagotovijo, da so varnostne kopije popolne. Med najbolj uporabljena orodja spadajo integracijski testi, ki preverjajo, ali so podatki pravilno preneseni in shranjeni, ter orodja za preverjanje kontrolnih vsot (hashing), ki omogočajo natančno prepoznavo sprememb v podatkih.

Kontrolne vsote so koristne zlasti za zagotovitev, da se datoteke niso spremenile ali poškodovale med procesom varnostnega kopiranja. S primerjanjem izvornih in varnostno kopira-

nih datotek lahko sistem zazna tudi najmanjše spremembe, kar omogoča hitro ukrepanje v primeru težav.

Orodja za preverjanje celovitosti vključujejo:

- **Ciklično preverjanje redundance - CRC** (Cyclic Redundancy Check), ki zazna napake pri prenosu podatkov.
- **Integracijski testi**, ki preverjajo, ali je sistem v celoti usklajen s pričakovanim stanjem varnostnih kopij.
- **Digitalni podpisi in certifikati**, ki zagotavljajo, da podatki niso bili spremenjeni in da izvirajo od zaupanja vrednega vira.

Mobilne in prenosne naprave

Mobilne in prenosne naprave lahko razširijo nabor storitev, ki jih ponuja upravljavec podatkov, vendar povečajo tveganje za krajo ter nenamerno izgubo podatkov. V primeru mobilnih naprav, kot so pametni telefoni ali tablice, jih uporabniki morda uporabljajo tudi v osebne namene, zato je potrebna posebna previdnost pri zagotavljanju, da poslovni podatki niso ogroženi. Pomembno je upoštevati naslednja pravila:

- **Q.1**: Postopki za upravljanje mobilnih in prenosnih naprav morajo biti definirani ter dokumentirani z jasnimi pravili za njihovo pravilno uporabo.
- **Q.2**: Mobilne naprave, ki jim je dovoljen dostop do informacijskega sistema, morajo biti predhodno registrirane in predhodno avtorizirane.
- **Q.3**: Mobilne naprave morajo biti predmet enake ravni postopkov nadzora dostopa (do sistema obdelave podatkov) kot ostala terminalska oprema.
- **Q.4**: Vloge in odgovornosti v zvezi z upravljanjem mobilnih in prenosnih naprav morajo biti jasno opredeljene.
- **Q.5**: Organizacija mora biti sposobna oddaljeno izbrisati osebne podatke (v zvezi z obdelavo podatkov) na mobilni napravi, ki je bila kompromitirana.
- **Q.6**: Mobilne naprave morajo podpirati ločevanje med zasebno in poslovno uporabo naprave prek varnih programskih zabojnikov.
- **Q.7**: Mobilne naprave morajo biti fizično zaščitene pred krajo, kadar niso v uporabi.
- **Q.8**: Upoštevati je treba dvofaktorsko avtentikacijo za dostop do mobilnih naprav.
- **Q.9**: Osebni podatki, shranjeni na mobilni napravi (kot del obdelave podatkov organizacije), morajo biti šifrirani. (ENISA, 2016)

Preizkušanje obnovljivosti varnostnih kopij

Preizkušanje obnovljivosti je prav tako ključen del zagotavljanja kakovosti varnostnih kopij. Organizacije morajo redno izvajati teste, ki simulirajo izgubo podatkov in preizkusijo postopek njihove obnovitve. Taki testi ne le preverjajo tehnično delovanje varnostnih kopij, temveč tudi usposobljenost osebja in učinkovitost procesov, ki so vzpostavljeni za hitro obnovo.

6. Priprava dokumentacije in postopkov arhiviranja

Učinkovito izvajanje varnostnih kopij ne vključuje zgolj tehničnega postopka kopiranja podatkov, temveč tudi pripravo natančne dokumentacije in jasnih postopkov, ki opredeljujejo arhiviranje ter obnavljanje podatkov. Organizacije, zlasti izvajalci kritičnih storitev, morajo imeti jasno opredeljene procese in protokole, ki omogočajo hitro ter zanesljivo odzivanje na morebitne incidente ali katastrofe. Dobra dokumentacija zagotavlja, da so vsi postopki jasni, hitro izvedljivi, ponovljivi in ustrezno prilagojeni specifičnim potrebam organizacije.

Pomen natančne dokumentacije

Natančna dokumentacija o varnostnih kopijah je ključnega pomena za zagotavljanje skladnosti postopkov in hitre ter učinkovite obnove podatkov v primeru okvar ali izgube podatkov. Dokumentacija mora vsebovati natančne podatke o tem, katere vrste podatkov se kopirajo, kako pogosto se varnostne kopije izvajajo, kam se kopije shranjujejo in kako dolgo se hranijo.

Vse informacije o postopkih varnostnega kopiranja morajo biti dostopne vsem ključnim deležnikom, ki sodelujejo pri upravljanju IT infrastrukture. Dokumentacija mora vključevati tudi podrobnosti o orodjih, programski opremi in strojni opremi, ki se uporabljajo za varnostne kopije, in kontaktne informacije za vse ključne osebe, ki so odgovorne za nadzorovanje ter vzdrževanje sistema varnostnih kopij.

Standardni postopki za arhiviranje in obnovitev

Vzpostavitev standardnih postopkov za arhiviranje in obnovitev podatkov je eden ključnih vidikov uspešnega upravljanja varnostnih kopij. Standardizirani postopki omogočajo enoten pristop k shranjevanju podatkov in s tem zmanjšujejo možnosti za napake ali izpade pri obnovi podatkov.

Takšni postopki vključujejo:

- **Natančen urnik arhiviranja**, ki določa frekvenco in čas izvajanja varnostnih kopij.
- **Navodila za obravnavo napak** pri varnostnih kopijah, vključno s protokoli za odpravljanje težav.
- **Jasna navodila za obnavljanje podatkov**, ki morajo biti dovolj podrobna, da omogočajo obnovo podatkov v različnih scenarijih, od manjših okvar do popolnega izpada.

Poleg tega morajo biti vsi postopki redno posodobljeni in prilagojeni spremembam v IT infrastrukturi ali zakonskih zahtevah. Standardizacija zagotavlja tudi skladnost s predpisi in olajšuje izvajanje varnostnih pregledov ter revizij.

Ustvarjanje protokolov za različne scenarije (npr. katastrofalna okvara)

V pripravo dokumentacije spada tudi razvoj podrobnih protokolov za različne scenarije, kot so delni izpadi sistemov, okvare strojne opreme, katastrofalna okvara, kibernetski in drugi napadi, ki bi lahko povzročili izgubo celotnih podatkovnih sistemov. Organizacija mora pripraviti načrt za obnovitev podatkov v vsakem izmed teh scenarijev, pri čemer je pomembno, da so protokoli oblikovani tako, da zagotavljajo hiter odziv in zmanjšanje izpadov.

Primeri scenarijev, za katere je treba pripraviti protokole:

- **Delna okvara**: Postopki za obnovo posameznih podatkov ali manjših delov sistema.
- **Popolna okvara sistema ali uničenje podatkov**: Protokoli za obnovo celotnega sistema iz varnostnih kopij, vključno z nadomestnimi lokacijami.
- **Kibernetski napad**: Načrti za hitro izolacijo okuženih sistemov in varno obnovitev podatkov iz nepoškodovanih kopij.

Sistematično oblikovani protokoli omogočajo hitrejše in učinkovitejše reakcije na nepredvidene dogodke ter pripomorejo k zmanjšanju škode in čimprejšnji vzpostavitvi normalnega delovanja.

7. Postopki za obnovitev podatkov iz varnostnih kopij

Eden najpomembnejših korakov pri upravljanju varnostnih kopij je oblikovanje jasnih in učinkovitih postopkov za obnovitev podatkov. Organizacije se morajo zavedati, da so varnostne kopije koristne le, če so podatki zlahka in hitro obnovljivi. Postopki za obnovitev morajo biti zato skrbno načrtovani in redno testirani, da se zagotovi, da bodo v primeru nujnih situacij zanesljivi ter dostopni.

Načrtovanje obnovitve

Načrtovanje postopka za obnovitev podatkov je več kot zgolj tehnična operacija – gre za celovit postopek, ki vključuje jasna navodila, dodeljevanje odgovornosti in opredelitev ključnih virov. Pomembno je, da vsak korak v postopku obnovitve temelji na specifičnih potrebah organizacije, kot so kritičnost podatkov in tveganja, ki jih prinaša morebitna izguba teh podatkov.

Pri načrtovanju obnovitve je treba upoštevati:

- **Vrste podatkov**, ki jih je treba obnoviti: Načrti za obnovitev morajo določati, kateri podatki imajo najvišjo prioriteto in morajo biti obnovljeni najprej.
- **Lokacije varnostnih kopij**: Redundantne lokacije in dostopnost do teh podatkov sta ključni za hitro obnovo.
- **Viri za obnovitev**: Vključno z IT osebjem, programsko opremo in strojno opremo, ki je potrebna za obnovitev podatkov.

Načrt mora vključevati tudi različne scenarije, od delnih okvar do popolnih izpadov, saj bodo potrebni različni pristopi glede na obseg izgube podatkov.

Testiranje obnovitvenih postopkov

Obnova podatkov mora biti redno testirana, da se zagotovi, da vsi procesi delujejo pravilno in da lahko osebje hitro ter učinkovito izvede obnovitev, kadar je to potrebno. Testiranje omogoča odkrivanje morebitnih napak v postopku, kot so manjkajoče kopije, poškodovani podatki ali neskladnost z najnovejšimi spremembami v IT sistemih.

Priporočljivo je izvajati testiranja v različnih scenarijih, ki simulirajo različne vrste okvar, kot so delni izpadi strojne opreme, izgube omrežne povezave ali kibernetski napadi. Takšna testiranja omogočajo organizacijam, da ocenijo čas in vire, ki so potrebni za uspešno obnovitev podatkov, ter prilagodijo postopke, če se odkrijejo pomanjkljivosti.

Testiranje obnovitvenih postopkov naj vključuje:

- **Redne simulacije okvar**: Te simulacije pomagajo preizkusiti učinkovitost sistema in usposobljenost osebja.
- **Preizkus dostopa do podatkov**: Preverjanje, ali so varnostne kopije dejansko dosegljive in v ustreznem stanju za obnovo.
- **Pregledovanje napak in izboljšav**: Analiza rezultatov testiranj, da se ugotovijo pomanjkljivosti in predlagajo izboljšave.

Časovni okvirji za obnovitev v nujnih primerih

V nujnih primerih je čas ključni dejavnik, saj lahko izguba dostopa do podatkov hitro povzroči resne motnje v poslovanju. Zato morajo biti časovni okvirji za obnovitev natančno opredeljeni in prilagojeni glede na kritičnost podatkov. Pri tem se pogosto uporabljajo koncepti RPO – Točka obnovitve sistemov (Recovery Point Objective) in RTO – Ciljni čas okrevanja (Recovery Time Objective), ki določata, koliko podatkov se lahko izgubi brez hujših posledic ter koliko časa lahko traja obnova, preden pride do motenj v poslovanju.

Časovni okvirji za obnovitev morajo vključevati:

- **Kratkoročne cilje**: Na primer obnovitev ključnih poslovnih podatkov v nekaj urah ali manj.
- **Dolgoročne cilje**: Kot je popolna obnova vseh sistemov, ki lahko traja več dni ali celo tednov, odvisno od obsega izpada.
- **Vloge in odgovornosti**: Kdo je odgovoren za določene korake v procesu obnovitve in kako poteka komunikacija med oddelki.

Določen in testiran časovni okvir za obnovitev je bistven za učinkovito ter pravočasno reševanje v kriznih situacijah, kar omogoča organizacijam, da zmanjšajo izgube in se čim prej vrnejo k normalnemu delovanju.

8. Beleženje dnevniških zapisov (logiranje) pri varnostnem kopiranju

Beleženje in redno pregledovanje dnevniških zapisov pri izvajanju varnostnih kopij je pomemben vidik spremljanja učinkovitosti in zanesljivosti postopkov varnostnega kopiranja. Dnevniški zapisi omogočajo pregled nad tem, kdaj so bile varnostne kopije izvedene, ali so bile uspešne in ali je prišlo do morebitnih napak med postopkom kopiranja.

Pomen dnevniških zapisov

Dnevniški zapisi zagotavljajo sledljivost vseh dejanj, povezanih z varnostnimi kopijami. Čeprav niso v središču pozornosti pri vsako-

dnevnih aktivnostih, so ključni, ko gre za odpravljanje težav ali preverjanje skladnosti z internimi politikami ali zakonskimi predpisi. V primeru neuspelih varnostnih kopij ali napak, ki se pojavijo med postopkom, omogočajo natančno analizo in ugotavljanje vzrokov, kar posledično vodi do hitrejše odprave težav.

Katera dejanja je treba beležiti?

Med varnostnim kopiranjem je smiselno beležiti naslednje podatke:

- **Čas začetka in konca varnostnega kopiranja**: Ti podatki omogočajo pregled nad tem, kdaj je bil postopek sprožen in koliko časa je trajal.
- **Status varnostnih kopij**: Ali so bile kopije uspešno ustvarjene ali je prišlo do napak med procesom.
- **Spremembe v podatkovnih zbirkah**: Beleženje tega, kateri podatki so bili kopirani ali spremenjeni je pomembno za celovit pregled nad tem, ali je bilo kopiranje popolno.
- **Opozorila in napake**: Vsakršna opozorila ali napake, ki se pojavijo med postopkom varnostnega kopiranja so ključna za pravočasno ukrepanje.
- **Uporaba dnevnikov za diagnostiko težav pri varnostnem kopiranju**

V primeru težav z varnostnimi kopijami so dnevniki nepogrešljivi pri ugotavljanju vzrokov za napake. Na primer, če pride do prekinitve omrežja med postopkom varnostnega kopiranja ali če varnostna kopija ni bila dokončana zaradi pomanjkanja prostora, dnevniški zapisi jasno prikažejo, kdaj in zakaj je prišlo do težave. To omogoča hitro ukrepanje in zmanjšuje tveganje za izgubo podatkov.

Vendar pa je pomembno, da se dnevniki ne hranijo predolgo, saj lahko postanejo preobsežni in težko obvladljivi. Organizacije bi morale imeti jasno politiko, ki določa, kako dolgo se dnevniki hranijo in kdo ima dostop do njih, da se zagotovi ustrezna zaščita informacij.

Viri:

- ENISA (2016) Guidelines for SMEs on the security of personal data processing: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing/@@download/fullReport
- ENISA 12 Steps to securing your business: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport

Poglavje 21
Predstavitev ključnih storitev varnostno operativnih centrov

POVZETEK

Varnostno operativni centri (SOC) so ključni za zagotavljanje kibernetske varnosti organizacij, saj omogočajo neprekinjeno spremljanje, zaznavanje in odzivanje na grožnje ter proaktivno obvladovanje ranljivosti. SOC vključuje storitve, kot so zbiranje obveščevalnih podatkov o grožnjah, upravljanje ranljivosti, izvajanje varnostnih politik in ozaveščanje uporabnikov. Pri izbiri ponudnika SOC-a je treba upoštevati strokovnost ekipe, hitrost odzivanja, tehnološko opremljenost in skladnost z zakonodajo EU. Zunanji SOC prinaša prednosti, kot so znižanje stroškov, dostop do vrhunske tehnologije in izboljšanje kibernetske odpornosti podjetja.

Ključne točke:

- Spremljanje varnostnih dogodkov v realnem času (SIEM in avtomatizacija)
- Zaznavanje anomalij in prepoznavanje groženj
- Upravljanje varnostnih incidentov (zajezitev, sanacija in obnova)
- Zbiranje obveščevalnih podatkov o grožnjah (OSINT in komercialni viri)
- Redno skeniranje ranljivosti in upravljanje varnostnih popravkov
- Razvoj in spremljanje skladnosti varnostnih politik
- Usposabljanje uporabnikov in simulacije napadov ribarjenja (phising)
- Izboljšanje kibernetske odpornosti z vajami in simulacijami
- Stalno svetovanje in prilagojeno poročanje naročnikom
- Skladnost z zakonodajnimi zahtevami in varnostnimi standardi (ISO 27001, NIST)
- Izogibanje ponudnikom SOC izven EU zaradi pravnih tveganj.

1. Pomen varnostno operativnih centrov (SOC) v sodobnem poslovanju

Varnostno operativni centri (SOC) so v današnjem poslovnem okolju postali nepogrešljiv element učinkovitega upravljanja kibernetskih groženj. Glede na naraščajoče število digitalnih napadov podjetja prepoznavajo, da je proaktivna varnostna strategija ključnega pomena za zaščito podatkov in kritičnih sistemov. SOC omogoča organizacijam neprekinjeno spremljanje varnostnih dogodkov, s čimer pomaga pravočasno zaznati in preprečiti potencialne napade.

Vloga SOC-a se je skozi čas iz pasivnega spremljanja varnostnih dogodkov razvila v proaktivno analizo tveganj in groženj. Tako danes SOC ne deluje več zgolj kot opazovalec, temveč postane aktivni igralec v kibernetski varnosti, ki skozi analitične postopke nenehno izboljšuje obrambne zmogljivosti podjetja. Podjetja se zavedajo, da je stalna prisotnost usposobljenih strokovnjakov SOC-a neprecenljiva za prepoznavanje nevarnosti, ki jih lahko sicer spregledajo.

Vloga kibernetske varnosti pri zaščiti poslovnih procesov

Kibernetska varnost danes ni več zgolj tehnična nuja, temveč poslovna funkcija, ki ima neposreden vpliv na kontinuiteto poslovanja in ugled podjetja. Nevarnosti, kot so vdori v informacijske sisteme, kraja podatkov ali sabotaža procesov, lahko resno ogrozijo delovanje organizacij. V tem kontekstu SOC igra ključno vlogo, saj zagotavlja, da so poslovni procesi ves čas zaščiteni pred nenehno spreminjajočimi se grožnjami.

Sodobni poslovni procesi so globoko integrirani z digitalno infrastrukturo, kar pomeni, da je varnost teh sistemov neposredno povezana s stabilnostjo in uspešnostjo podjetja. Prekinitev poslovnih procesov zaradi kibernetskih napadov lahko povzroči ogromne finančne izgube, pa tudi nepopravljivo škodo ugledu podjetja. Z vzpostavitvijo učinkovitega SOC-a se organizacija ne le zaščiti pred takšnimi dogodki, temveč tudi zagotovi, da je pripravljena na hiter in usklajen odziv v primeru morebitnega incidenta.

2. Ključne storitve varnostno operativnih centrov

Varnostno operativni center (SOC) je nepogrešljiv element v obrambnem sistemu organizacije, ki se osredotoča na uporabo ljudi, procesov in tehnologije za neprekinjeno spremljanje ter izboljševanje varnostnega stanja. Hkrati preprečuje, odkriva, analizira in se odziva na kibernetske incidente. Naloge SOC-a lahko razdelimo na več ključnih področij:

2.1 Spremljanje in zaznavanje

Neprekinjeno spremljanje

- **Spremljanje v realnem času**: SOC uporablja sisteme za upravljanje varnostnih informacij in dogodkov (SIEM) ter druga orodja za spremljanje omrežij, sistemov in podatkov organizacije ter zaznavanje varnostnih groženj v realnem času.
- **Upravljanje opozoril**: Ekipa SOC-a upravlja in prioritetno obravnava varnostna opozorila, ki jih generirajo različna varnostna orodja, da zagotovi pravočasen pregled ter odziv na morebitne grožnje.

Zaznavanje groženj

- **Zaznavanje anomalij**: Prepoznavanje nenavadnih vzorcev ali vedenj, ki lahko kažejo na varnostno grožnjo ali kompromis.
- **Signature-based detection (prepoznavanje na podlagi podpisov)**: Uporaba vnaprej določenih podpisov za zaznavanje znanih groženj, kjer se za prepoznavanje groženj uporabljajo specifični vzorci, ki so bili prej identificirani.
- **Vedenjska analiza**: Uvajanje tehnik za analizo vedenja z namenom zaznave groženj, ki temeljijo na odklonih od običajnega delovanja.

2.2 Odziv na incidente

Raziskovanje incidentov

- **Upravljanje opozoril**: Prvotna triaža varnostnih opozoril za določitev njihove veljavnosti in resnosti.
- **Analiza vzrokov**: Raziskovanje in analiza varnostnih incidentov za določitev njihovega izvora, vpliva ter osnovnega vzroka.

Koordinacija odziva

- **Upravljanje incidentov**: Razvoj in izvedba načrtov za odzivanje na incidente, ki vključujejo zajezitev, odstranitev in obnovitvene ukrepe.
- **Komunikacija**: Koordinacija komunikacije z relevantnimi deležniki med in po incidentu, vključno z internimi ekipami ter zunanjimi partnerji.

2.3 Obveščanje o grožnjah

Zbiranje obveščevalnih podatkov o grožnjah

- **Odprti viri informacij (Open source intelligence-OSINT)**: Zbiranje podatkov o grožnjah iz javno dostopnih virov.
- **Komercialni viri groženj**: Naročanje na komercialne vire informacij o grožnjah za pridobivanje ažurnih informacij o novih grožnjah.
- **Izmenjava in sodelovanje**: Sodelovanje v skupnostih za izmenjavo obveščevalnih podatkov o grožnjah z namenom izmenjave informacij s partnerji v industriji.

Analiza groženj

- **Kontekstualna analiza**: Analiza obveščevalnih podatkov o grožnjah za razumevanje konteksta in morebitnega vpliva na organizacijo.
- **Iskanje groženj**: Proaktivno iskanje skritih groženj, ki bi lahko ušle običajnim mehanizmom zaznavanja.

2.4 Upravljanje ranljivosti

Ocenjevanje ranljivosti

- **Skeniranje**: Redno izvajanje skeniranja ranljivosti za prepoznavanje varnostnih slabosti v sistemih in omrežjih organizacije.
- **Ocena tveganja**: Ocenjevanje tveganja, povezanega z ugotovljenimi ranljivostmi, na podlagi njihove resnosti in morebitnega vpliva.

Upravljanje popravkov

- **Načrtovanje sanacije**: Razvoj in izvajanje načrtov za sanacijo ugotovljenih ranljivosti.
- **Izvajanje popravkov**: Pravočasna izvedba popravkov in posodobitev za zmanjšanje tveganja.

2.5 Varnostne politike in skladnost

Razvoj politik

- **Varnostne politike**: Razvoj in vzdrževanje varnostnih politik ter postopkov, ki so usklajeni z industrijskimi standardi in zakonskimi zahtevami.
- **Nadzor skladnosti**: Spremljanje skladnosti z varnostnimi politikami in zakonskimi predpisi za zagotavljanje upoštevanja zahtev.

Revizije in poročanje

- **Varnostne revizije**: Redno izvajanje varnostnih revizij za oceno učinkovitosti varnostnih ukrepov in prepoznavanje področij za izboljšave.
- **Poročanje**: Priprava in distribucija rednih varnostnih poročil za vodstvo ter druge deležnike, ki poudarjajo ključne kazalnike, incidente in trende.

2.6 Ozaveščanje o varnosti in usposabljanje

Usposabljanje uporabnikov

- **Programi ozaveščanja**: Razvoj in izvajanje programov ozaveščanja o varnosti za izobraževanje zaposlenih o najboljših varnostnih praksah ter grožnjah.
- **Simulacije phishing (ribarjenje) napadov**: Izvajanje simulacij phishing napadov za preverjanje in izboljšanje sposobnosti zaposlenih pri prepoznavanju ter odzivanju na takšne napade.

Razvoj spretnosti

- **Nadaljnje izobraževanje**: Omogočanje stalnega usposabljanja in strokovnega razvoja za zaposlene v SOC-u, za namen kontinuirane seznanitve z najnovejšimi varnostnimi tehnologijami in grožnjami.

2.7 Avtomatizacija

Orkestracija, avtomatizacija in odzivanje na varnostne dogodke (SOAR)

- **Avtomatizacija**: Uvajanje orodij za avtomatizacijo ponavljajočih se nalog in izboljšanje odzivnih časov.
- **Scenariji odziva**: Razvoj avtomatiziranih scenarijev odziva za pogoste incidente, kar zagotavlja dosledno in učinkovito obvladovanje dogodkov.

2.8 Sodelovanje in koordinacija

Koordinacija med oddelki

- **Medsektorske ekipe**: Tesno sodelovanje z drugimi oddelki (IT, pravni, kadrovski idr.) za zagotavljanje usklajenega pristopa k varnosti.
- **Ekipe za odzivanje na incidente**: Vzpostavitev in vzdrževanje ekip za odzivanje na incidente, ki vključujejo predstavnike različnih oddelkov, da se omogoči celovito obvladovanje incidentov.

Zunanji partnerji

- **Sodelovanje z organi pregona**: Koordinacija z organi pregona pri incidentih, ki vključujejo kriminalne dejavnosti.
- **Upravljanje tretjih ponudnikov**: Upravljanje odnosov s tretjimi ponudniki varnostnih storitev kot zagotovilo, da ustrezajo varnostnim standardom organizacije.

SOC je ključni del kibernetske strategije organizacije, zadolžen za spremljanje, zaznavanje, odzivanje in ublažitev varnostnih groženj. S celovitim pristopom, ki vključuje neprekinjeno spremljanje, odzivanje na incidente, zbiranje in analizo groženj, upravljanje ranljivosti, zagotavljanje skladnosti, avtomatizacijo ter sodelovanje, SOC zagotavlja robustno in prilagodljivo varnostno stanje organizacije.

3. Kaj naročniki lahko pričakujejo?

Prilagoditev storitev glede na poslovne potrebe

Ena izmed najpomembnejših prednosti varnostno operativnih centrov (SOC) je sposobnost prilagoditve storitev specifičnim potrebam podjetja. Nobeno podjetje ni enako kot drugo, in tudi kibernetske grožnje se razlikujejo glede na vrsto dejavnosti, infrastrukturo ter občutljivost podatkov, ki jih podjetje upravlja. SOC ponuja storitve, ki so oblikovane po meri vsakega naročnika – od majhnih podjetij, ki potrebujejo osnovno varnostno zaščito, do velikih korporacij, ki zahtevajo napredne rešitve za nadzor in obrambo.

Prilagoditev storitev zajema vse, od specifičnih politik nadzora, integracije z obstoječimi sistemi, do uvedbe specializiranih orodij in rešitev. SOC omogoča, da podjetje izbere tiste storitve, ki najbolj ustrezajo njihovim operativnim in varnostnim potrebam, s čimer se zagotavlja optimizacija varnostnih ukrepov ter učinkovitost obrambe. Ta prilagodljivost je zlasti pomembna v sektorjih, kot so finance, zdravstvo ali trgovina, kjer so zahteve glede varnosti izjemno visoke.

Stalno svetovanje in poročanje

SOC ne deluje zgolj kot pasivni opazovalec, temveč kot aktiven partner v kibernetski varnosti podjetja. Stalno svetovanje naročnikom je eden ključnih stebrov uspešnega delovanja

SOC-a. To vključuje redna srečanja in posvetovanja, kjer se skupaj pregledujejo trenutne varnostne politike, incidenti, zaznane grožnje in izboljšave varnostnih praks.

Poleg tega SOC naročnikom zagotavlja redna poročila, ki vsebujejo analize o varnostnih dogodkih, ranljivostih in splošnem stanju varnosti znotraj podjetja. Ta poročila ne le pripomorejo k boljšemu razumevanju kibernetske varnosti, temveč omogočajo tudi pripravo ustreznih ukrepov za prihodnost. Poročila so običajno prilagojena glede na potrebe naročnika – lahko so bolj tehnična, namenjena IT oddelku, ali pa bolj strateška, namenjena višjemu vodstvu podjetja.

Skladnost z zakonodajnimi in varnostnimi standardi

Varnostno operativni centri igrajo tudi pomembno vlogo pri zagotavljanju skladnosti podjetja z zakonodajnimi predpisi in varnostnimi standardi. Na področjih, kot so zdravstvo, finance ali telekomunikacije, so podjetja zavezana strogi zakonodaji. SOC skrbi, da so vse storitve in ukrepi skladni s temi predpisi, kar podjetju zagotavlja mirno poslovanje brez skrbi glede pravnih posledic.

SOC nenehno spremlja spremembe v zakonodaji in svetuje podjetjem, kako se prilagoditi novim zahtevam. Poleg tega so varnostne rešitve, ki jih uvaja SOC, v skladu z industrijskimi standardi, kot so ISO 27001 in NIST, kar zagotavlja, da so sistemi zaščiteni skladno z najboljšimi praksami. Skladnost ni zgolj formalnost, ampak ključni del kibernetske varnosti, saj pomaga podjetjem pri vzdrževanju ugleda in zaupanja strank.

Izboljšanje kibernetske odpornosti podjetja

Eden izmed glavnih ciljev varnostno operativnega centra je izboljšanje celotne kibernetske odpornosti podjetja. SOC ne deluje zgolj reaktivno – s tem, ko ščiti pred trenutnimi grožnjami – ampak tudi proaktivno, saj pomaga podjetju krepiti svojo varnostno infrastrukturo in se pripravljati na prihodnje napade. Kibernetska odpornost vključuje več vidikov: hitrejši odziv na incidente, zmanjšanje ranljivosti ter vzpostavitev robustnih varnostnih sistemov, ki lahko prenesejo vse večje pritiske kibernetskih napadov.

SOC sodeluje z naročnikom pri razvijanju in testiranju varnostnih scenarijev, simuliranju napadov ter izvajanju vaj za obvladovanje incidentov, kar omogoča boljšo pripravljenost ekipe na realne napade. V praksi to pomeni, da podjetje postaja vse bolj odporno na napade, saj ima ustrezno infrastrukturo, procese in ekipo, ki lahko hitro ter učinkovito ukrepa. Izboljšana kibernetska odpornost je temelj dolgoročnega poslovnega uspeha v digitalnem svetu, kjer je varnost podatkov ena izmed najpomembnejših poslovnih prioritet.

4. Na kaj biti pozoren pri izbiri SOC?

Strokovnost in izkušnje ekipe

Ko izbirate varnostno operativni center (SOC), je strokovnost ekipe ključni dejavnik, ki ga morate upoštevati. Učinkovitost SOC-a je namreč neposredno povezana s kompetentnostjo in izkušnjami varnostnih strokovnjakov, ki nadzirajo ter upravljajo vašo varnostno infrastrukturo. Pomembno je preveriti, ali ima ekipa ustrezno tehnično usposobljenost, certifikate na področju kibernetske varnosti (kot so CISSP, CEH, CISM) in dolgoletne izkušnje pri delu z različnimi podjetji ter sektorji.

Izkušena ekipa ne samo bolje zaznava in obvladuje varnostne incidente, temveč je tudi bolj pripravljena na sodelovanje pri dolgoročnem strateškem svetovanju. Pri izbiri SOC-a je priporočljivo tudi preveriti, kako pogosto se njihovi strokovnjaki udeležujejo izobraževanj in nadgrajujejo svoje znanje o najnovejših grožnjah ter tehnologijah. Strokovnjaki, ki so ves čas v koraku z najnovejšimi trendi, so ključni za uspešno zaščito vaših sistemov.

Zmožnost hitrega odzivanja in učinkovitost storitev

Hitrost odzivanja je eden najpomembnejših dejavnikov pri oceni kakovosti SOC-a. Varnostni incidenti se lahko zgodijo nepričakovano,

in ko pride do napada, je vsaka sekunda ključnega pomena. SOC, ki ima dobro uveljavljene postopke za hitro zaznavanje in odzivanje, lahko občutno zmanjša škodo, ki bi jo napad lahko povzročil.

Upoštevajte:

- Kako hitro SOC zazna sumljive dejavnosti.
- Kako hitro se ekipa lahko aktivira in ukrepa po zaznavi incidenta.
- Kakšen je časovni okvir za popolno sanacijo napada.

SOC mora imeti tudi postopek za obvladovanje več incidentov hkrati, saj se lahko podjetja soočajo z več napadi iz različnih smeri. Pomembno je tudi, da SOC nenehno optimizira svoje odzivne zmogljivosti in uporablja avtomatizirana orodja, ki omogočajo hitrejše obravnavanje groženj.

Transparentnost in razpoložljivost poročil

Transparentnost je temelj zaupanja med naročnikom in SOC-om. Pri izbiri ponudnika SOC-a je nujno, da je naročniku omogočen jasen vpogled v vse aktivnosti, ki jih SOC izvaja za zaščito podjetja. To vključuje redno poročanje o stanju varnosti, obvladovanju incidentov, analizah ranljivosti in vseh preventivnih ukrepih, ki jih SOC uvaja.

Kakovost poročil je prav tako pomembna kot njihova frekvenca. Dobra poročila niso zgolj tehnični zapisi, ampak jasno prikazujejo glavne ugotovitve, nevarnosti in priporočila za izboljšanje varnostne strategije. Poročila morajo biti prilagojena različnim ciljnim skupinam v podjetju – od tehničnega osebja, ki potrebuje natančne podatke, do vodstvene ekipe, ki potrebuje bolj strateške vpoglede.

Pri izbiri SOC-a preverite, kako pogosto ponujajo poročila in ali so ta prilagojena vašim specifičnim potrebam. Dober SOC bo omogočil ne samo redna poročila, temveč tudi dostop do podatkov v realnem času prek posebnih nadzornih plošč (dashboardov), kjer lahko spremljate ključne varnostne kazalnike.

Tehnološka opremljenost in podpora

SOC mora biti opremljen z naprednimi tehnologijami, ki omogočajo učinkovit nadzor in zaščito pred kibernetskimi grožnjami. Pri izbiri SOC-a preverite, ali uporabljajo sodobne varnostne rešitve, kot so sistemi za upravljanje varnostnih informacij in dogodkov (SIEM), napredna orodja za odkrivanje groženj (Threat Intelligence), rešitve za analitiko velikih podatkov ter avtomatizirana orodja za odziv na incidente.

- Dobra tehnološka opremljenost SOC-a pomeni:
- Uporabo orodij, ki so prilagojena vašim poslovnim potrebam.
- Sposobnost integracije z vašimi obstoječimi sistemi in rešitvami.
- Uporabo napredne umetne inteligence in strojnega učenja za prepoznavanje kompleksnih groženj.

SOC mora poleg tega nuditi neprekinjeno tehnično podporo, ki vam je na voljo, kadarkoli jo potrebujete. Hitrost in kakovost tehnične podpore sta ključni, zlasti, kadar se soočate s kritičnimi incidenti. Pred izbiro SOC-a preverite, ali ponujajo podporo 24/7 in ali imajo dobro razvite komunikacijske kanale, prek katerih lahko hitro pridobite pomoč ter odgovore na svoja vprašanja.

5. Prednosti sodelovanja z zunanjim SOC

Strokovnost brez dodatnih stroškov zaposlovanja

Ena največjih prednosti sodelovanja z zunanjim varnostno operativnim centrom (SOC) je dostop do visoko usposobljenih strokovnjakov brez potrebe po internem zaposlovanju dodatnega osebja. Gradnja lastnega SOC-a zahteva najem številnih specializiranih strokovnjakov, od varnostnih analitikov, forenzikov, do strokovnjakov za odzivanje na incidente, kar lahko predstavlja veliko finančno breme za podjetje. Zunanji SOC pa podjetju omogoča takojšnji dostop do celotne ekipe izkušenih strokov-

njakov, ki imajo potrebno znanje, certifikate in izkušnje za obvladovanje vseh varnostnih izzivov.

Podjetje se tako izogne stroškom zaposlovanja, usposabljanja in nenehnega nadgrajevanja znanja svojih zaposlenih. Namesto tega lahko zunanji SOC nemoteno zagotovi vse potrebne storitve, kar organizacijam omogoča, da se osredotočijo na svoje osnovne poslovne dejavnosti, medtem ko strokovnjaki skrbijo za kibernetsko varnost. Ta model je zlasti privlačen za manjša in srednje velika podjetja, ki nimajo resursov za vzdrževanje celovite varnostne ekipe, a vseeno potrebujejo visoko raven zaščite.

Zmanjšanje stroškov lastne infrastrukture

Vzpostavitev in vzdrževanje lastnega SOC-a ni samo vprašanje človeških virov, temveč tudi velikih investicij v tehnologijo ter infrastrukturo. Zunanji SOC odpravi potrebo po investicijah v lastne varnostne sisteme, kot so draga orodja za upravljanje varnostnih informacij (SIEM), sistemi za nadzor omrežja in drugi specializirani varnostni mehanizmi.

Poleg začetnih stroškov vzpostavitve lastne varnostne infrastrukture je tu tudi stalni strošek vzdrževanja in posodabljanja teh sistemov. Z zunanjim SOC-om podjetje plača zgolj za storitve, ki jih dejansko potrebuje, brez dodatnih skritih stroškov. Poleg tega se izognejo stroškom, povezanim z amortizacijo opreme in nadgradnjami. Ta prilagodljivost omogoča, da podjetja znižajo svoje operativne stroške in se hkrati izognejo obremenitvi z visokimi investicijami v tehnologijo, ki hitro zastara.

Nenehna nadgradnja storitev in tehnologij

V kibernetski varnosti je ključnega pomena, da se sistemi in procesi nenehno posodabljajo, saj se grožnje razvijajo z neverjetno hitrostjo. Zunanji SOC ponuja stalno izboljševanje storitev in tehnologij, saj je njegova naloga, da zagotovi najsodobnejše varnostne rešitve za svoje naročnike. Ker zunanje varnostne ekipe sodelujejo z različnimi naročniki, so izpostavljene različnim vrstam groženj in napadov, kar jim omogoča hitrejše prepoznavanje novih taktik napadalcev ter učinkovito prilagajanje varnostnih ukrepov.

SOC-i vlagajo v napredno tehnologijo, avtomatizacijo in umetno inteligenco, kar omogoča boljše zaznavanje ter preprečevanje napadov. Pri tem so zunanje ekipe ves čas na tekočem z najnovejšimi varnostnimi trendi in grožnjami, zaradi česar lahko hitro prilagodijo svoje storitve, kar pa podjetju omogoča, da ostaja pred napadalci. Stalna nadgradnja tehnologij in storitev pri zunanjem SOC-u zagotavlja, da naročniki prejemajo vrhunsko zaščito brez potrebe po dodatnih investicijah.

Poleg tehnološke nadgradnje pa zunanji SOC ponuja tudi nadgradnjo znanja. Njihovi strokovnjaki so usposobljeni za reševanje najkompleksnejših varnostnih vprašanj, saj se nenehno izobražujejo in certificirajo v skladu z najnovejšimi standardi v industriji. Sodelovanje z zunanjim SOC-om tako zagotavlja, da so vaši sistemi vedno zaščiteni z najboljšimi praksami in tehnologijami, ki so na voljo.

6. Sklep

Pomen dolgoročne kibernetske odpornosti

V sodobnem poslovnem svetu, kjer se grožnje iz digitalnega prostora nenehno razvijajo, postaja kibernetska odpornost podjetij eden izmed ključnih dejavnikov njihovega dolgoročnega uspeha. Varnostno operativni centri (SOC) igrajo ključno vlogo pri vzpostavitvi in ohranjanju te odpornosti, saj omogočajo stalno spremljanje ter zaščito pred vse kompleksnejšimi kibernetskimi napadi. Ni več dovolj zgolj reaktivno ukrepanje – podjetja, ki želijo ohraniti svojo konkurenčnost in zaupanje strank, morajo postati proaktivna v svoji obrambi.

Dolgoročna kibernetska odpornost vključuje zmožnost hitrega okrevanja po varnostnih incidentih, a hkrati tudi stalno prilagajanje in nadgrajevanje varnostnih ukrepov. To pomeni, da podjetja potrebujejo SOC, ki ne zagotavlja

zgolj trenutne zaščite, temveč nenehno izboljšuje in prilagaja varnostne rešitve na podlagi aktualnih groženj. Zmožnost hitrega prepoznavanja napadov, učinkovito odzivanje in izboljšanje sistemov po vsakem incidentu so temelji, na katerih gradimo dolgoročno kibernetsko odpornost.

Izbira pravega ponudnika SOC-a kot ključ za varnost poslovanja

Izbira pravega ponudnika SOC-a je strateška odločitev, ki lahko odločilno vpliva na varnost poslovanja podjetja. Pomembno je, da podjetja izberejo SOC, ki razume njihove specifične varnostne potrebe, ima izkušeno ekipo strokovnjakov ter uporablja najsodobnejše tehnologije. Zunanja ekipa mora biti sposobna nuditi hitro in učinkovito podporo, hkrati pa zagotoviti visoko raven transparentnosti pri svojem delu. Učinkovit SOC-a ni zgolj ponudnik storitev, ampak partner, ki aktivno sodeluje pri oblikovanju varnostne strategije in izboljševanju kibernetske odpornosti.

Pri izbiri ponudnika SOC-a je treba biti pozoren tudi na geografsko lokacijo in upravljanje centra. SOC, ki je v celoti ali deloma v upravljanju izven Republike Slovenije ali celo izven Evropske unije, lahko predstavlja določena tveganja. Evropska zakonodaja, kot je GDPR, zahteva strogo zaščito podatkov, pri čemer je pomembno, da je SOC skladno z evropskimi standardi varstva osebnih podatkov. SOC, ki je podvržen zakonodaji izven EU, lahko izpostavi podjetje tveganjem, povezanim z dostopom do podatkov s strani tujih državnih institucij ali drugačno obravnavo varnostnih praks. Zato je ključnega pomena, da podjetja izberejo SOC, ki deluje v skladu s predpisi in standardi Evropske unije ter zagotavlja visoko raven varstva podatkov.

Na koncu je izbira pravega ponudnika SOC-a pomemben korak k zagotavljanju varnosti in stabilnosti poslovanja. Partnerstvo s strokovno usposobljenim in zaupanja vrednim SOC-om je temelj dolgoročne varnosti podjetja, saj zagotavlja, da so vaši sistemi zaščiteni pred vedno bolj naprednimi grožnjami v digitalnem svetu.

Viri:

- ENISA (2020): How to set up CSIRT and SOC (https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc)
- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)

Poglavje 22
Predstavitev aktualnih pristopov in orodij za spremljanje informacijskih sistemov v organizacijah, zaznavanje poskusov vdorov ter preprečevanje kibernetskih incidentov

POVZETEK

Besedilo obravnava sodobne pristope in orodja za spremljanje informacijskih sistemov, zaznavanje poskusov vdorov in preprečevanje kibernetskih incidentov. Izpostavlja pomen neprekinjenega spremljanja sistemov s pomočjo naprednih tehnologij, kot so sistemi za odkrivanje (IDS) in preprečevanje vdorov (IPS), rešitve za upravljanje varnostnih dogodkov (SIEM) ter analitika na osnovi umetne inteligence. Obravnava tudi vlogo varnostno operativnih centrov (SOC), odzivnih ekip za incidente (CSIRT) ter pomen rednih varnostnih pregledov in izobraževanja zaposlenih za zmanjšanje tveganj.

Ključne točke:

- Uporaba sistemov za odkrivanje in preprečevanje vdorov (IDS/IPS)
- Napredna analiza podatkov z umetno inteligenco in strojno učenje
- Implementacija rešitev za upravljanje informacij o varnostnih dogodkih (SIEM)
- Vloga varnostno operativnih centrov (SOC)
- Ključna naloga odzivnih ekip za hitro ukrepanje ob incidentih (CSIRT)
- Izvajanje rednih varnostnih pregledov in vdornih testiranj
- Uporaba avtomatizacije za proaktivno zaznavanje groženj
- Usposabljanje zaposlenih za prepoznavanje socialnega inženiringa
- Vključevanje naprednih tehnologij v celovito varnostno infrastrukturo
- Preprečevanje kibernetskih incidentov s kombinacijo tehnoloških in človeških virov.

1. Pomen nadzora in varnosti v sodobnih informacijskih sistemih

V današnjem digitalno usmerjenem svetu so informacijski sistemi hrbtenica vsake sodobne organizacije. Varnost teh sistemov je zato ključna za zaščito občutljivih podatkov, intelektualne lastnine in poslovnih operacij. Pomembno je razumeti, da vsaka ranljivost v teh sistemih predstavlja potencialno nevarnost za delovanje podjetja, kar lahko privede do motenj, finančne škode in izgube ugleda.

Sodobne organizacije se soočajo z naraščajočo kompleksnostjo kibernetskih groženj, ki postajajo vse bolj izpopolnjene in težje zaznavne. Kibernetski kriminalci uporabljajo napredne tehnike, kot so socialni inženiring, napadi ribarjenja in zlonamerna programska oprema, ki lahko zlahka zaobidejo osnovne varnostne ukrepe. Nenehno spreminjajoči se kraji, načini in vektorji kibernetskih groženj zato zahtevajo od podjetij, da vlagajo v prilagodljive ter napredne varnostne rešitve.

Nadzor in spremljanje informacijskih sistemov postajata vse bolj nujna, saj omogočata proaktivno zaznavanje anomalij ter hitro odzivanje na sumljive aktivnosti. Zgodnje odkrivanje varnostnih incidentov lahko prepreči večje kibernetske katastrofe. Investicije v varnostne rešitve, kot so sistemi za odkrivanje vdorov (IDS), sistemi za upravljanje varnostnih dogodkov (SIEM) in napredna orodja za analizo podatkov, postajajo prednostna naloga.

Med ključne izzive, s katerimi se organizacije soočajo pri zagotavljanju kibernetske varnosti, sodi tudi pomanjkanje usposobljenega kadra. Mnoge organizacije se soočajo z vrzeljo v znanju in veščinah, ki so potrebne za upravljanje ter spremljanje informacijskih sistemov. Poleg tega se morajo podjetja spopadati z nenehno spreminjajočimi se predpisi in standardi varnosti, ki jih je treba dosledno upoštevati.

Za uspešno varovanje informacijskih sistemov morajo organizacije prepoznati potrebo po vzpostavitvi robustnih varnostnih strategij, ki združujejo napredne tehnologije z dobro usposobljenimi varnostnimi strokovnjaki. Vlaganje v to področje je dolgoročna naložba, ki organizacijam omogoča vzdrževanje operativne učinkovitosti in zaščito pred vse bolj zapletenimi grožnjami.

2. Pristopi k spremljanju informacijskih sistemov

Spremljanje informacijskih sistemov v organizacijah je ključno za proaktivno zaznavanje groženj in zaščito pred kibernetskimi napadi. Različni pristopi in orodja omogočajo različne nivoje nadzora, od preprostega spremljanja, do naprednega odkrivanja ter preprečevanja groženj. Z naraščajočim obsegom in sofisticiranostjo kibernetskih groženj postaja uporaba teh tehnologij nujna.

Sistem za odkrivanje vdorov (IDS)

Sistem za odkrivanje vdorov (IDS) je eno izmed osnovnih orodij za zaznavanje kibernetskih groženj. IDS deluje kot pasivni nadzornik, ki analizira omrežni promet in sistemske aktivnosti, pri čemer išče vzorce ali nepravilnosti, ki bi lahko nakazovali na potencialni poskus vdora. IDS sistemi uporabljajo vnaprej določene vzorce (signaturne sisteme) ali analizo obnašanja za zaznavanje sumljivih aktivnosti. Njihova glavna prednost je možnost zaznavanja neznanih napadov na podlagi nenavadnega vedenja, vendar pa zaradi pasivnega pristopa ne preprečijo napada – zaznajo ga in sprožijo opozorilo.

Sistem za preprečevanje vdorov (IPS)

Sistem za preprečevanje vdorov (IPS) je naslednji korak v evoluciji varnostnih rešitev, saj ne le zaznava sumljive aktivnosti, temveč tudi aktivno ukrepa. IPS sistemi delujejo v realnem času in so zasnovani tako, da preprečijo potencialne napade, še preden ti dosežejo ciljno infrastrukturo. To dosežejo z blokiranjem prometa, ki ga prepoznajo kot grožnjo, ali s preusmeritvijo na varne poti. Pomembno je, da IPS sistemi delujejo brez večjih vplivov na delovanje omrežja, saj lahko preveč agresivni varnostni ukrepi vplivajo na normalne poslovne procese. Učin-

kovit IPS sistem zato zagotavlja ravnovesje med zaščito in operativno učinkovitostjo.

Napredna analiza podatkov

Napredna analiza podatkov postaja ena ključnih komponent v kibernetski varnosti. Uporaba umetne inteligence (AI) in strojnega učenja (ML) omogoča odkrivanje vzorcev napadov, ki jih klasični sistemi morda ne bi zaznali. AI in ML lahko analizirata velike količine podatkov v realnem času in prepoznata subtilne nepravilnosti, ki bi lahko nakazovale na potencialne grožnje. Sposobnost teh sistemov, da se učijo iz zgodovinskih podatkov in prilagajajo novim napadom, omogoča napredno zaščito, saj se kibernetski napadi nenehno razvijajo.

Varnostno operativni centri (SOC)

Za nekatere organizacije so lastni varnostno operativni centri (SOC) nepogrešljivi del kibernetske zaščite. SOC centri so namenjeni 24-urnemu nadzoru nad informacijskimi sistemi in omogočajo hitro odzivanje na varnostne incidente. Strokovnjaki, ki delajo v teh centrih, uporabljajo različna orodja in tehnike za spremljanje omrežij, strežnikov ter aplikacij in zaznavanje sumljivih aktivnosti. SOC center je pogosto tudi ključna točka za koordinacijo odzivov na incidente in za izdelavo poročil o varnostnih dogodkih, kar omogoča stalno izboljševanje varnostnih politik organizacije.

Z uporabo kombinacije teh pristopov lahko organizacije vzpostavijo robustno varnostno infrastrukturo, ki omogoča tako zgodnje zaznavanje kot aktivno preprečevanje kibernetskih incidentov.

3. Tehnologije za zaznavanje poskusov vdorov

Zaznavanje poskusov vdorov v informacijske sisteme je osrednji element kibernetske varnosti, saj omogoča zgodnje prepoznavanje groženj in hitro ukrepanje. Sodobne organizacije uporabljajo številna orodja, ki omogočajo napredno spremljanje omrežij in dogodkov v realnem času, kar je ključno za učinkovito preprečevanje večjih kibernetskih incidentov.

Sistemi za spremljanje omrežij so namenjeni analizi omrežnih tokov v realnem času in omogočajo prepoznavanje nenavadnega vedenja, ki bi lahko nakazovalo na poskus vdora. Delujejo kot osrednji mehanizem za nadzor podatkovnih tokov med napravami znotraj omrežja, s ciljem zaznati odstopanja od običajnih vzorcev. Ena izmed ključnih prednosti teh sistemov je njihova sposobnost prepoznavanja nepravilnosti, kot so nenavadno veliki podatkovni tokovi ali poskusi dostopa do strežnikov, kar so lahko zgodnji znaki kibernetskega napada. Ti sistemi uporabljajo različne pristope, vključno z analizo vedenjskih in prometnih vzorcev, ki omogočajo odkrivanje sumljivih aktivnosti. Ker nadzor omrežja poteka neprekinjeno, lahko organizacije hitro reagirajo na odstopanja v prometu in vedenju.

SIEM (Security Information and Event Management) rešitve predstavljajo ključni del kibernetske infrastrukture za zbiranje in centralizirano analizo varnostnih dogodkov v realnem času. Te rešitve združujejo podatke iz različnih virov znotraj organizacije, kot so omrežne naprave, strežniki in aplikacije, kar omogoča celovit pregled nad stanjem varnosti. SIEM rešitve omogočajo napredno analizo dogodkov, pri čemer uporabljajo algoritme za prepoznavanje morebitnih varnostnih incidentov ali nepravilnosti, ki bi lahko nakazovale na grožnjo. Pomembno je tudi, da omogočajo hitrejše in učinkovitejše odzivanje na incidente, saj so vse informacije združene na enem mestu.

- **Zbiranje podatkov**: SIEM rešitve zbirajo podatke iz različnih naprav, aplikacij, strežnikov in omrežnih elementov, kar omogoča široko sliko varnostnega dogajanja.
- **Analiza podatkov**: Orodja nato uporabijo napredne algoritme za analizo teh podatkov in zaznavanje morebitnih groženj ali odstopanj, ki nakazujejo na varnostne incidente.
- **Centralizacija in odziv**: Ena glavnih prednosti SIEM rešitev je njihova sposobnost združevanja vseh varnostnih podatkov na

enem mestu, kar omogoča hitrejše in bolj učinkovito odzivanje na incidente.

Varnostna programska oprema, kot so antivirusni programi, požarni zidovi in orodja za zaznavanje zlonamerne programske opreme, prav tako igrajo ključno vlogo pri zaščiti pred kibernetskimi grožnjami. Antivirusni programi so zasnovani za prepoznavanje in odstranjevanje znanih vrst zlonamerne programske opreme, pri čemer redno posodabljajo svoje baze podatkov z novimi grožnjami, da zagotovijo ustrezno zaščito. Požarni zidovi delujejo kot prva obrambna linija med notranjim omrežjem in zunanjimi viri, saj nadzorujejo ter filtrirajo promet, preprečujejo pa dostop sumljivim povezavam. Programska oprema za zaznavanje zlonamerne programske opreme je ključna za prepoznavanje in odstranjevanje groženj, kot so virusi, črvi, trojanski konji ter druge vrste škodljive programske opreme.

Kombinacija teh tehnologij omogoča organizacijam vzpostavitev učinkovite zaščite pred kibernetskimi grožnjami. Pomembno je, da se te rešitve integrirajo v celovit varnostni sistem, ki vključuje tako napredno zaznavanje kot odzivanje na potencialne incidente, kar omogoča zaščito pred vedno bolj zapletenimi napadi.

4. Preprečevanje kibernetskih incidentov

Preprečevanje kibernetskih incidentov je ena ključnih strategij, ki zagotavlja varnost informacijskih sistemov. Organizacije, ki si prizadevajo vzpostaviti robusten obrambni sistem, se morajo zavedati, da je aktivno preprečevanje groženj enako pomembno kot odzivanje nanje. To vključuje tako tehnološke rešitve kot tudi procese in človeške vire.

Redne varnostne ocene so bistvene za prepoznavanje in odpravljanje potencialnih ranljivosti v informacijskih sistemih. Organizacije morajo izvajati redne varnostne preglede in vdorne teste, da bi preverile, kako odporni so njihovi sistemi proti morebitnim napadom. Takšne ocene zagotavljajo, da so organizacije v koraku z najnovejšimi grožnjami in ranljivostmi, ki jih lahko kibernetski napadalci izkoristijo. Vdorni testi, znani tudi kot etično hekanje, omogočajo simulacijo resničnih napadov na sistem in tako pomagajo pri odkrivanju šibkih točk, še preden jih napadalci odkrijejo sami.

Odzivne ekipe za incidente, poznane kot CSIRT (Computer Security Incident Response Teams), so posebej usposobljene ekipe, katerih glavna naloga je hitro in učinkovito odzivanje na kibernetske incidente. CSIRT ekipe igrajo ključno vlogo pri omejevanju škode, ki jo lahko povzroči varnostni dogodek, kot je vdor ali napad. Njihova naloga ni le reševanje takojšnjih posledic, temveč tudi analiza incidenta, da bi se iz njega naučili in izboljšali prihodnje preventivne ukrepe. Ključnega pomena je, da imajo te ekipe jasno določene postopke in orodja, s katerimi lahko ukrepajo hitro ter učinkovito, saj lahko vsak trenutek zamude prinese večjo škodo.

Izobraževanje zaposlenih je še ena pomembna komponenta pri preprečevanju kibernetskih incidentov. Zaposleni predstavljajo prvo obrambno linijo pred številnimi oblikami kibernetskih napadov, zlasti pred tistimi, ki vključujejo socialni inženiring, ribarjenje ali manipulacijo znotraj podjetja. Zato je ključno, da so redno usposobljeni za prepoznavanje sumljivih dejavnosti, kot so nenavadne e-pošte ali poskusi dostopa do zaupnih informacij. Usposabljanje naj vključuje simulacije napadov, redne tečaje ter opomnike o najboljših praksah pri uporabi gesel, varni uporabi interneta in prepoznavanju zlonamernih dejavnosti. S tem organizacije zmanjšajo tveganje človeške napake, ki pogosto predstavlja najšibkejši člen v verigi kibernetske varnosti.

Preprečevanje kibernetskih incidentov zahteva celovit pristop, ki združuje tehnične varnostne rešitve, proaktivne preglede in usposobljeno osebje. Uspešna strategija temelji na kombinaciji tehnologij, ki omogočajo stalno spremljanje in preprečevanje, ter človeških virov, ki so ustrezno pripravljeni na prepoznavanje in preprečevanje groženj.

Viri:

- ENISA (December 2016): A good practice guide of using taxonomies in incident prevention and detection. https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
- ENISA (December 2016): Technical Guidelines for the implementation of minimum security measures for Digital Service Providers. https://www.enisa.europa.eu/publications/minimum-security-measures-for--digital-service-providers/@@download/fullReport

Poglavje 23
Poudarki in predlogi ter obvezni elementi pri sklepanju pogodb z zunanjimi izvajalci

POVZETEK

Pogodbe z zunanjimi izvajalci so temelj učinkovitega sodelovanja med organizacijami in izvajalci. Ključno je natančno opredeliti obseg storitev, časovne okvirje, kakovostne standarde, finančne pogoje, varovanje zaupnih informacij ter določiti odgovornosti in postopke za reševanje sporov. Poseben poudarek je na zagotavljanju skladnosti z zakonodajo (npr. GDPR) ter določitvi pravic intelektualne lastnine. Jasno opredeljene določbe zmanjšujejo tveganja in omogočajo uspešno dolgoročno sodelovanje.

Ključne točke:

- Natančna določitev obsega storitev
- Časovni okvirji in ključni mejniki
- Standardi kakovosti in postopki nadzora
- Finančni pogoji in plačilni roki
- Varovanje zaupnih informacij in osebnih podatkov
- Pravice do intelektualne lastnine
- Odgovornosti strank in zavarovanja
- Postopki za reševanje sporov
- Skladnost z GDPR in drugimi predpisi
- Protikorupcijske klavzule.

Pogodbe z zunanjimi izvajalci so ključni del poslovnih sodelovanj, saj opredeljujejo pogoje in obveznosti obeh strank. Besedilo se osredotoča na ključne poudarke in obvezne elemente, ki jih je treba upoštevati pri sklepanju takih pogodb. Med najpomembnejšimi elementi so natančna določitev obsega storitev, jasni časovni okvirji in ključni mejniki, določanje ustreznih standardov kakovosti, finančni pogoji ter varovanje zaupnih informacij in intelektualne lastnine. Poleg tega besedilo obravnava odgovornosti strank, zahteve glede zavarovanj in postopke za reševanje morebitnih sporov, s čimer pomaga zagotavljati uspešno sodelovanje ter zmanjševati tveganja med naročnikom in izvajalcem.

1. Določitev obsega storitev

Določitev obsega storitev je kritičen element pogodbe z zunanjim izvajalcem, saj opredeljuje, kaj točno se pričakuje od izvajalca, v kakšnem obsegu in v kakšnem časovnem okviru. Pogosto se dogaja, da je ta del premalo natančno opredeljen, kar lahko privede do nejasnosti, slabe izvedbe projekta in nesoglasij med naročnikom ter izvajalcem. Da bi se izognili takim težavam, mora pogodba vključevati zelo podroben opis nalog, ki jih bo izvajalec opravljal, skupaj z jasno določitvijo mejnika začetka in konca posameznih aktivnosti.

Pri določanju obsega storitev je pomembno, da obe strani natančno opredelita pričakovanja glede izvedbe del. Naročnik mora zagotoviti, da so v pogodbi vključene vse specifične naloge in funkcionalnosti, ki jih potrebuje, medtem ko izvajalec prispeva svojo strokovnost pri oblikovanju izvedljivih rešitev. Obseg mora biti dokumentiran na način, da ni dvoumnosti glede tega, kaj je vključeno v pogodbo in kaj ni, kar ščiti obe strani pred prihodnjimi nesporazumi. V pogodbi naj bo določeno tudi, pod kakšnimi pogoji in v kakšnem obsegu (če sploh) sme izvajalec za izvedbo posameznih sklopov pogodbe najeti podizvajalca.

Pomemben element je tudi določitev prilagodljivosti obsega. Pogosto se med izvajanjem projektov pojavijo nepredvidene okoliščine ali dodatne zahteve naročnika, ki lahko vplivajo na obseg dela. V pogodbi mora biti natančno določeno, kako se bodo te spremembe obravnavale in kakšni so postopki za usklajevanje sprememb obsega dela, bodisi z aneksi k pogodbi bodisi z internimi dogovori med strankami.

Poleg tega mora pogodba vključevati jasne metode za spremljanje in nadzor nad izvajanjem storitev. To lahko vključuje postopke poročanja, redna srečanja za pregled napredka ali vnaprej dogovorjene revizijske točke, kjer naročnik preveri, ali izvajalec izpolnjuje pričakovanja.

2. Časovni okvirji in mejniki

Časovni okvirji in mejniki so osrednji del vsake pogodbe, ki določajo dinamiko izvajanja projekta. Natančno določeni časovni roki zagotavljajo, da tako naročnik kot izvajalec delujeta usklajeno in v skladu s pričakovanji. Pogodba mora vsebovati jasne določbe o začetku in zaključku vsakega posameznega koraka ali faze projekta ter definirati ključne mejnike, na podlagi katerih se bo ocenjevalo napredovanje projekta.

Določitev mejnika v pogodbi pomeni opredelitev pomembnih točk v času izvajanja projekta, ko mora izvajalec predstaviti določene dosežke ali zaključene faze dela. Ti mejniki omogočajo naročniku, da preveri, ali izvajalec dela napreduje v skladu s pričakovanji, in ali je kakovost opravljenih del na ustrezni ravni. Mejniki prav tako pomagajo strukturirati projekt na manjše dele, kar omogoča boljše upravljanje časa in virov, tako za naročnika kot za izvajalca.

Pogodba mora vsebovati tudi določila za obvladovanje zamud, ki lahko nastanejo iz različnih razlogov, kot so tehnične težave, sprememba obsega dela ali nepričakovane okoliščine, kot so naravne nesreče ali pandemije. Pri zamudah je nujno, da pogodba določa, kako se bodo te obravnavale, kakšne so pravne posledice in kakšni so postopki za prilagoditev časovnih rokov. Možno je vključiti tudi določbe o finančnih sankcijah za primer, da izvajalec ne doseže dogovorjenih rokov.

Prav tako je priporočljivo vključiti določila o tem, kako bo nadomestilo prilagojeno, če pride do pospešenega izvajanja del, zlasti, če izvajalec uspe zaključiti določen projekt pred rokom. S tem se spodbuja pozitivna dinamika izvajanja in motivacija za hitrejše zaključke, ne da bi to vplivalo na kakovost storitev.

Če je del pogodbe tudi nadaljnje vzdrževanje, je treba v pogodbi določiti tudi časovne okvirje izvedbe morebitnih nadgradenj, odprave napak in dosegljivost oziroma odzivnost izvajalca.

3. Kakovost in standardi

Kakovost storitev, ki jih zagotavlja zunanji izvajalec, je ena izmed ključnih determinant uspešnosti projekta. Natančno določeni standardi kakovosti v pogodbi zagotavljajo, da storitve izpolnjujejo pričakovanja naročnika in so v skladu z industrijskimi normami ali posebnimi specifikacijami projekta. V kolikor standardi niso jasno opredeljeni, obstaja tveganje, da bo izvedba del odstopala od pričakovanj, kar lahko privede do konfliktov med naročnikom in izvajalcem.

V pogodbo je treba vključiti jasne zahteve glede kakovosti, pri čemer je priporočljivo upoštevati tako splošne industrijske standarde kot tudi specifične zahteve naročnika, ki se lahko nanašajo na tehnične parametre, funkcionalnost, zmogljivost ali uporabnost končnega izdelka. V določenih primerih je smiselno uporabiti referenčne standarde ali certifikate kakovosti, ki so priznani na področju specifičnih storitev (na primer ISO standardi ali drugi strokovni normativi).

Ključno je tudi, da pogodba vključuje postopke za spremljanje kakovosti in redna preverjanja, ki omogočajo sprotno zaznavanje morebitnih napak ali neskladnosti z določenimi standardi. Taka preverjanja so lahko v obliki revizij, testiranj, ali vmesnih poročil, kjer izvajalec predstavi dosežke in rezultate dela. Določiti je treba tudi postopke za odpravljanje napak ali popravke, kjer se določi, v kakšnem roku mora izvajalec popraviti morebitne napake in kakšne so sankcije za neizpolnjevanje dogovorjenih standardov.

Poleg tega je pomembno, da so v pogodbo vključene določbe, ki omogočajo prilagoditev standardov kakovosti glede na spremembe obsega projekta ali tehnološke napredke, ki lahko vplivajo na izvedbo storitev. S tem se omogoča fleksibilnost pri prilagajanju kakovostnih zahtev, ki sledijo hitremu razvoju na področju storitev ali tehnologij.

4. Finančni pogoji in plačilni roki

Finančni pogoji in plačilni roki so eden izmed ključnih elementov vsake pogodbe, saj neposredno vplivajo na uspešno izvedbo storitev ter zaščito interesov tako naročnika kot izvajalca. Pregledni in natančno opredeljeni finančni pogoji zmanjšujejo tveganje za nepričakovane stroške ali finančne težave, ki bi lahko nastale zaradi nesoglasij glede plačil.

Pogodba mora natančno določiti skupno ceno storitev, ki jih bo izvajalec zagotovil, ter način obračunavanja teh storitev. Najpogosteje se uporabljajo različni modeli obračunavanja, kot so fiksna cena, plačilo po dejanskih urah ali plačilo po doseženih rezultatih (npr. fazni mejniki). Pri izbiri primernega modela je treba upoštevati obseg in naravo storitev ter možne spremembe, ki bi lahko vplivale na finančno strukturo.

V pogodbo je treba vključiti tudi določbe o pogojih in rokih plačila, ki jasno določajo, kdaj in pod kakšnimi pogoji bo izvajalec prejel plačilo. Natančno določeni plačilni roki omogočajo izvajalcu načrtovanje finančnih sredstev in zagotavljajo stabilno izvajanje storitev. Prav tako je pomembno opredeliti morebitne dodatne stroške, ki se lahko pojavijo med projektom, kot so na primer nepredvidene spremembe obsega del, zahteve po dodatnih storitvah ali prilagoditvah.

Poleg tega mora pogodba določati tudi mehanizme za obravnavanje zamud pri plačilih. Vključiti je treba določila o zamudnih obrestih ali drugih finančnih sankcijah, ki izvajalca zaščitijo pred morebitnimi finančnimi tveganji v primeru neplačila s strani naročnika. Smiselno je vključiti tudi določbe o vmesnih plačilih, zlasti pri daljših projektih, kjer se lahko

izvajalec srečuje z večjimi stroški še pred zaključkom projekta.

5. Varovanje zaupnih informacij in intelektualna lastnina

Sodelovanje z zunanjimi izvajalci pogosto vključuje izmenjavo zaupnih informacij, ki lahko vključujejo poslovne skrivnosti, strateške podatke ali tehnične specifikacije. Pogodba mora zato vsebovati zelo natančna določila glede varovanja zaupnih informacij, s čimer se zagotavlja, da bo izvajalec ustrezno ravnal z občutljivimi podatki naročnika.

Poleg tega je ključno, da pogodbe vključujejo določbo, ki zagotavlja, da so zunanji izvajalci ustrezno usposobljeni in ozaveščeni glede vprašanj kibernetske varnosti. Tako je nujno zagotovilo, da imajo tretje stranke dostop do potrebnega znanja o varnostnih vprašanjih, kar pomaga preprečevati morebitne grožnje in neskladnosti z varnostnimi standardi. To vključuje redno usposabljanje izvajalcev in preverjanje njihove skladnosti z varnostnimi praksami.

Pogodba mora vsebovati določbe, ki jasno definirajo, katere informacije veljajo za zaupne, kako bo izvajalec z njimi ravnal, kdo bo imel dostop do teh informacij in kakšni so ukrepi za njihovo zaščito. Prav tako je treba določiti obdobje, v katerem bo izvajalec dolžan varovati zaupne podatke, ter določiti morebitne sankcije za kršitev teh določil. Vključitev klavzule o zaupnosti lahko dodatno zaščiti interese naročnika, zlasti v primerih, ko je treba izvajalcu omogočiti dostop do poslovnih skrivnosti. Če je mogoče, v pogodbo vključite tudi pravila oziroma postopke v primeru morebitnega razkritja zaupnih informacij in roke, v katerih je treba obveščati o morebitnem razkritju zaupnih informacij.

Če pogodba obsega obdelavo podatkov, je treba z njo zagotoviti, da so izvajalci (in tudi morebitni podizvajalci) zavezani k enakim standardom varovanja podatkov ter zaupnih informacij, kot veljajo za naročnika. To vključuje npr. čezmejno hrambo ali obdelavo, roke hrambe in logiranje oz. vodenje dnevnikov zapisov. Če se v okviru pogodbe obdelujejo osebni podatki, veljajo za izvajalca in morebitne podizvajalce enaki kriteriji, kot za naročnika. Pogodba mora v tem primeru vsebovati tudi določila, ki izvajalca oz. morebitne podizvajalce zavezujejo k tem enakim kriterijem.

Prav tako je treba jasno opredeliti, komu pripada intelektualna lastnina, ustvarjena v okviru sodelovanja. V določenih primerih je lahko intelektualna lastnina, kot so programska oprema, tehnične rešitve ali inovacije, ključna konkurenčna prednost naročnika, zato mora pogodba jasno določiti, kdo ima pravico do uporabe teh inovacij. Lahko se določi, da pravice pripadajo naročniku, izvajalec pa ima omejeno licenco za njihovo uporabo v obdobju trajanja pogodbe.

6. Odgovornosti in zavarovanje

Določitev odgovornosti med naročnikom in izvajalcem je pomemben del pogodbe, saj zagotavlja jasno razumevanje, kdo nosi odgovornost za določene naloge, stroške ali morebitne težave, ki se lahko pojavijo med izvajanjem storitev. Pogodba mora natančno opredeliti odgovornosti vsake stranke, saj nejasno določene odgovornosti lahko vodijo do pravnih sporov ali nepričakovanih stroškov za katerokoli stranko.

Odgovornosti vključujejo tako finančno kot tudi pravno odgovornost za morebitne napake, neskladnosti z dogovorjenimi standardi ali škodo, povzročeno med izvajanjem storitev. Natančno določen obseg odgovornosti zmanjšuje tveganje za pravne spore in omogoča strankam, da razumejo, katera tveganja morajo upravljati. Poleg tega mora pogodba vključevati določbe, ki omejujejo odgovornost posamezne stranke v primerih, kjer je to mogoče (npr. zavarovanja odgovornosti). Če pogodba dopušča, da izvajalec za izvedbo določenega sklopa najame podizvajalca, naj pogodba vsebuje tudi odgovornosti za morebitne podizvajalce.

Poleg tega je zelo priporočljivo, da pogodba vključuje zahteve po ustreznem zavarovanju, ki ga mora izvajalec imeti, da bi zaščitil na-

ročnika pred morebitnimi finančnimi posledicami napak, nesreč ali drugih nepredvidenih dogodkov. Zavarovanja, kot so splošno odgovornostno zavarovanje, zavarovanje za napake in izpustitve ter druge vrste, zagotavljajo, da bo izvajalec finančno zmožen pokriti morebitne odškodninske zahtevke.

7. Reševanje sporov

Tudi pri najboljših pogodbah se lahko pojavijo nesoglasja ali spori med naročnikom in izvajalcem. Pogodba mora zato vsebovati jasno določene mehanizme za reševanje sporov, ki omogočajo hitrejše, cenejše in učinkovitejše reševanje sporov, preden ti prerastejo v dolgotrajne sodne postopke.

Običajno pogodbe vključujejo postopke mediacije ali arbitraže, ki omogočajo hitro rešitev nesoglasij z vpletenostjo nevtralne tretje osebe. Mediacija ponuja možnost neformalnega reševanja sporov, kjer stranke dosežejo dogovor s pomočjo posrednika. Arbitraža je bolj formaliziran proces, kjer stranke soglašajo, da bodo spor rešile pred arbitrom, katerega odločitev je zavezujoča. Ena izmed prednosti arbitraže je hitrost in zaupnost postopka v primerjavi z dolgotrajnimi ter javnimi sodnimi postopki.

Poleg tega mora pogodba določati, katera jurisdikcija bo pristojna za reševanje sporov in katero pravo se bo uporabljalo. To je zlasti pomembno pri mednarodnih pogodbah, kjer se lahko pojavijo pravna vprašanja glede pristojnosti in uporabe različnih pravnih sistemov. Natančno določeni postopki za reševanje sporov zmanjšujejo tveganje za dolgotrajne pravne postopke in omogočajo obema stranema, da se osredotočita na uspešno izvajanje pogodbe.

Pogoste napake pri sodelovanju z zunanjimi izvajalci

Kljub skrbno pripravljenim pogodbam in določenim varnostnim ukrepom se v praksi še vedno pojavljajo nekatere pogoste napake, ki lahko negativno vplivajo na sodelovanje z zunanjimi izvajalci. Naročniki morajo biti pozorni na naslednje:

1. **Nejasno opredeljen obseg storitev**: Ena izmed najpogostejših napak je pomanjkljivo ali nejasno opredeljen obseg storitev, kar pogosto privede do nesporazumov med strankami. Pomembno je, da pogodba jasno določa, kaj je zajeto v obsegu storitev in kaj ni, da se preprečijo poznejša nesoglasja.
2. **Neustrezno spremljanje izvajalcev**: V številnih primerih naročniki ne izvajajo rednega nadzora nad napredkom in kakovostjo storitev zunanjih izvajalcev. Pomembno je, da so vzpostavljeni mehanizmi za sprotno preverjanje, kot so redni pregledi, poročila in nadzorne točke, ki omogočajo spremljanje skladnosti s pogodbo.
3. **Nevarnost odtekanja ključnih podatkov**: Ena izmed največjih nevarnosti pri sodelovanju z zunanjimi izvajalci je tveganje odtekanja ključnih podatkov podjetja. Zunanji izvajalci pogosto pridobijo dostop do občutljivih informacij, kot so poslovne skrivnosti, tehnične specifikacije, podatki o strankah ali finančne informacije. Če izvajalec nima vzpostavljenih ustreznih varnostnih ukrepov, obstaja resna grožnja, da bi lahko prišlo do nepooblaščenega dostopa ali zlorabe teh podatkov.
4. **Pomanjkanje dogovora o intelektualni lastnini**: Nejasna ali nepopolna določila o pravicah intelektualne lastnine lahko povzročijo pravne spore glede lastništva inovacij, rešitev ali programske opreme, ustvarjene v okviru projekta. Zato je nujno, da so te določbe jasno opredeljene.
5. **Nepravočasna plačila in finančna neskladja**: Težave z zamudami pri plačilih ali nejasnimi finančnimi dogovori so pogosta ovira pri uspešnem sodelovanju. Pomembno je, da so plačilni pogoji jasno opredeljeni, in da so v primeru zamud predvidene sankcije.
6. **Neurejeni postopki za prekinitev sodelovanja**: Pogodbe pogosto ne vsebujejo ustreznih določil o tem, kako bo potekala prekinitev sodelovanja ali prenos storitev

nazaj k naročniku. Ta vidik je ključen, da se zagotovi, da občutljivi podatki ostanejo zaščiteni, in da prekinitev ne vpliva na poslovanje naročnika.

Naročniki, ki se izognejo tem pogostim napakam, bodo bolj uspešno obvladovali tveganja in vzpostavili trdne temelje za dolgoročno sodelovanje z zunanjimi izvajalci.

Kot pomemben del sporazumov med naročnikom in izvajalcem mora biti vključena tudi naslednja vsebina:

GDPR

Skladno z zakonom, ki ureja varstvo osebnih podatkov, pogodbeni stranki soglašata, da morebitnih osebnih podatkov ne bosta uporabljali v nasprotju z določili tega zakona. Pogodbeni stranki bosta tudi zagotavljali pogoje in ukrepe za zagotovitev varstva osebnih podatkov ter preprečevali morebitne zlorabe, v smislu določil navedenega zakona.

Pogodbene stranke se zavezujejo, da bodo ves čas strogo varovale kot poslovno skrivnost vse podatke in informacije v zvezi z delom ter poslovanjem pogodbenih strank, ki jih bodo na kakršenkoli način pridobile pri delu oziroma v zvezi z delom po tej pogodbi. Pogodbene stranke se zavezujejo, da bodo ves čas varovale tudi osebne podatke pridobljene pri delu oziroma v zvezi z delom po tej pogodbi v skladu z nacionalno zakonodajo, ki ureja varstvo osebnih podatkov in v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov – GDPR).

Pogodbene stranke bodo seznanile zaposlene navedene v tej pogodbi in druge kadre pogodbenih strank, ki bodo sodelovali pri izvajanju te pogodbe z določilom 7. člena GDPR in pridobile njihovo privolitev za obdelavo njihovih osebnih podatkov za namen izvajanja te pogodbe.

Naročnik bo osebne podatke obdeloval za čas trajanja pogodbe in jih bo hranil še deset (10) let po izteku pogodbenega razmerja, izključno na ozemlju RS.

Izvajalec se s to pogodbo zaveže, da bo vse podatke, dejstva in listine naročnikov, s katerimi se bo seznanil v zvezi z izvedbo dela po tej pogodbi, skrbno varoval in jih ne bo razkril tretji osebi ali uporabil v svojo korist, ne v času trajanja te pogodbe, niti kadarkoli po njenem prenehanju. Izvajalec z zavezo seznani pri njemu zaposlene. Za morebitne kršitve je izvajalec odškodninsko odgovoren.

PROTIKORUPCIJSKA KLAVZULA – NIČNOST

V primeru, da se ugotovi, da je pri izvedbi naročila, na podlagi katerega je podpisana ta pogodba ali pri izvajanju te pogodbe kdo v imenu ali na račun druge pogodbene stranke, predstavniku ali posredniku naročnika ali drugega organa ali organizacije iz javnega sektorja obljubil, ponudil ali dal kakšno nedovoljeno korist za pridobitev tega posla ali za sklenitev tega posla pod ugodnejšimi pogoji ali za opustitev dolžnega nadzora nad izvajanjem pogodbenih obveznosti ali za drugo ravnanje ali pridobitev nedovoljene koristi predstavniku organa, posredniku organa ali organizacija iz javnega sektorja, drugi pogodbeni stranki ali njenemu predstavniku, zastopniku, posredniku, je ta pogodba nična.

Naročnik bo v primeru ugotovitve o domnevnem obstoju dejanskega stanja iz prvega odstavka tega člena ali obvestila Komisije za preprečevanje korupcije ali drugih organov, glede njegovega domnevnega nastanka, pričel z ugotavljanjem pogojev ničnosti pogodbe iz prejšnjega odstavka tega člena oziroma z drugimi ukrepi v skladu s predpisi Republike Slovenije.

Viri:

- ENISA (December 2016): Technical Guidelines for the implementation of minimum security measures for Digital Service Providers. https://www.enisa.europa.eu/publications/minimum-security-measures-for--digital-service-providers/@@download/fullReport

Poglavje 24
Ključni nasveti za krizno komuniciranje

POVZETEK

Predstavljeni so ključni vidiki uspešnega kriznega komuniciranja, ki vključujejo pripravo kriznega načrta, hitro in usklajeno komuniciranje ter transparentnost in prilagodljivost. Organizacija mora proaktivno obravnavati krizne situacije z jasnimi sporočili, uporabo več kanalov in učinkovitim upravljanjem negativnih odzivov. Pomembno je tudi stalno spremljanje odzivov ter prilagajanje strategij glede na razvoj situacije, kar pomaga pri ohranjanju zaupanja deležnikov in omejevanju škode.

Ključne točke:

- Krizni komunikacijski načrt
- Identifikacija možnih kriz
- Pristojne osebe in odgovornosti
- Hitro in dosledno komuniciranje
- Uporaba več komunikacijskih kanalov
- Transparentnost in jasnost sporočil
- Upravljanje negativnih odzivov
- Redno obveščanje deležnikov
- Spremljanje in prilagajanje strategij
- Ohranjanje zaupanja deležnikov.

1. Pripravite krizni komunikacijski načrt

Vsaka organizacija se lahko kadarkoli znajde v krizni situaciji, ki zahteva hitro, premišljeno in usklajeno komuniciranje. Krizni komunikacijski načrt je bistven za zagotovitev, da bodo vsi procesi komuniciranja potekali brez zastojev in napak. Ta načrt mora biti natančno strukturiran in dostopen vsem ključnim osebam znotraj organizacije. Vključevati mora jasne protokole za možno krizo – od tega, kdo je odgovoren za določene naloge, do tega, kako in kdaj se posamezne informacije posredujejo javnosti.

V okviru kriznega načrta je nujno, da organizacija predhodno preuči vse možne scenarije kriznih situacij, vključno z notranjimi in zunanjimi grožnjami ter določi postopke za hitro ukrepanje. Dobra priprava zmanjša tveganje napačnih informacij in omogoča takojšnje usklajeno delovanje med ključnimi oddelki. Tako bo v primeru krize organizacija imela na voljo jasno začrtan načrt ukrepanja, ki ga lahko nemudoma uporabi.

1.1 Identifikacija možnih kriz

Preden pride do krizne situacije, je pomembno prepoznati vzroke za morebitno krizo. To vključuje analizo notranjih ranljivosti, kot so tehnične napake ali notranji konflikti, pa tudi zunanje grožnje, kot so naravne nesreče, gospodarski vzroki ali negativna medijska poročanja. Identifikacija teh scenarijev ni enkraten proces – treba je nenehno spremljati in posodabljati ugotovitve na podlagi novih informacij in sprememb v okolju. Sistematičen pristop k identifikaciji kriz omogoča oblikovanje specifičnih odgovorov za vsak scenarij, kar poveča pripravljenost organizacije in zmanjša tveganje improviziranih, nepremišljenih odločitev, ko se kriza dejansko zgodi. Organizacija, ki je sposobna prepoznati zgodnje znake krize, bo bolj proaktivna pri ukrepanju, kar bo zmanjšalo posledice.

1.2 Določanje pristojnih oseb

Krizno komuniciranje zahteva jasne vloge in odgovornosti. Pri oblikovanju načrta je ključno, da se določi, kdo bo vodil krizno komuniciranje, saj mora biti odgovorna oseba hitro dostopna in pripravljena sprejemati odločitve pod pritiskom.

Poleg glavne osebe, ki bo komunicirala z mediji in javnostjo, je treba določiti tudi druge podporne vloge – od oseb, ki bodo zbirale podatke in spremljale odzive javnosti, do tehnične podpore, ki bo zagotavljala, da bodo vsi komunikacijski kanali delovali brezhibno. Jasno določene odgovornosti bodo omogočile, da se bo vsak član ekipe osredotočil na svojo nalogo, kar bo povečalo učinkovitost in zmanjšalo verjetnost napak.

2. Prvi odziv ob krizi

Ko nastopi kriza, se najprej določi vse vpletene strani in na koga bo situacija vplivala. Preden se obvesti javnost, se vedno obvesti zaposlene in vpletene strani. Preučiti je treba vsa znana dejstva in predvideti njihove posledice. Na podlagi tega organizacija določi tri ključna sporočila za javnost. Vsako ključno sporočilo naj bo ena misel.

3. Komunicirajte hitro in dosledno

V krizni situaciji je čas ključnega pomena. Organizacije, ki se ne odzovejo hitro in odločno, tvegajo, da bodo informacije, resnične ali napačne, prišle v javnost, preden bodo same sploh lahko podale svoj uradni odziv. Prvi vtis, ki ga javnost dobi, pogosto oblikuje nadaljnje razumevanje situacije, zato je pomembno, da organizacija deluje hitro in zbrano. Pomembno je tudi, da so vsa sporočila dosledna, ne glede na komunikacijski kanal.

Ko se zgodi kriza, morajo biti informacije posredovane čim hitreje, vendar brez žrtvovanja natančnosti. Prvi odzivi naj bodo kratki, jedrnati in naj se osredotočajo na dejstva – kaj se je zgodilo, kdo je prizadet, kaj se bo naredilo, da se situacija reši. Čeprav popolne informacije morda še niso na voljo, mora organizacija vzpostaviti zaupanje z zagotavljanjem, da bo javnost sproti obveščena o nadaljnjih korakih.

3.1 Uporaba več kanalov

V sodobnem svetu krizno komuniciranje zahteva uporabo več komunikacijskih kanalov, da se informacije hitro in učinkovito razširijo med vse ključne deležnike. Družbeni mediji, spletna stran, tradicionalni mediji in neposredna komunikacija z zaposlenimi so le nekateri od kanalov, ki jih mora organizacija uporabiti za hitro ter natančno posredovanje informacij.

Prav tako je nujno, da je ton komuniciranja prilagojen vsakemu kanalu posebej. Na družbenih omrežjih, kjer odzivi potekajo v realnem času, je treba odgovarjati hitreje in bolj neposredno, medtem ko so uradne izjave za medije pogosto bolj strukturirane ter formalne. Večkanalni pristop omogoča, da organizacija doseže širše občinstvo in s tem zmanjša tveganje širjenja napačnih informacij ali govoric.

3.2 Jasnost komuniciranja

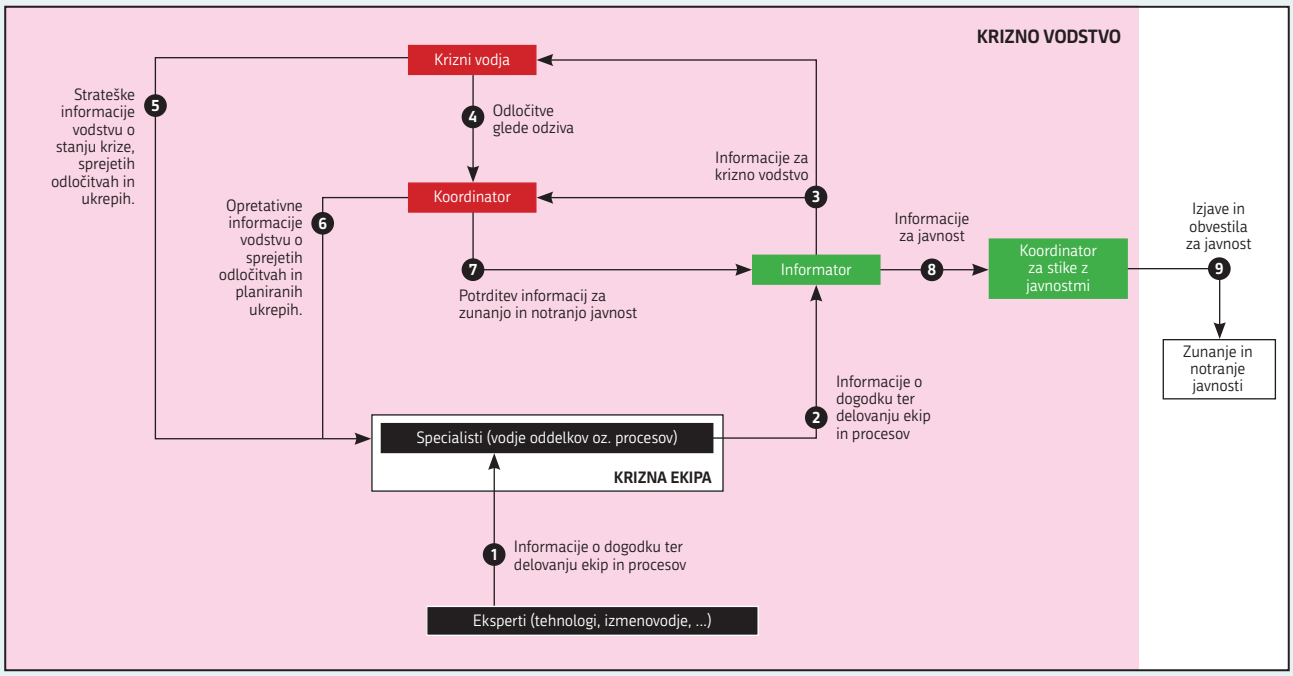
Vsebina sporočil naj bo razumljiva in kratka. V mislih je treba imeti, komu je sporočilo namenjeno. Če je namenjeno širši javnosti, je treba strokovne izraze in postopke ustrezno poimenovati ter opisati na preprost in razumljiv način.

Kadar organizacija daje ustno izjavo, naj bo oseba mirna in spoštljiva. Oblikuje naj cele stavke, s ključnimi sporočili, ki bi jih organizacija rada posredovala javnosti. Govori naj počasi, prijazno in v vsebino naj vključi pohvalo svoje ekipe. Ob negativnem vprašanju naj v izjavi ne ponovi negativnih fraz, ampak poda pozitivno vsebino. Novinarjevo vprašanje si je dobro v mislih preoblikovati v takšno obliko, da lahko nanj oseba poda pozitiven odgovor. Intervjuje in izjave je priporočljivo snemati za arhiv.

3.3 Doslednost v sporočilih

Ko govorimo o kriznem komuniciranju, je doslednost ključnega pomena. Vsako sporočilo, ne glede na to, ali gre za interno ali eksterno komunikacijo, mora biti usklajeno z glavnimi cilji organizacije in strategijo za reševanje krize. Neskladja v sporočilih lahko povzročijo zmedo in škodijo ugledu organizacije.

Zato je pomembno, da so vsi vpleteni v krizno komuniciranje obveščeni o osrednjem sporočilu, ki ga želi organizacija posredovati, in da tega sporočila ne spreminjajo brez odobritve vodje kriznega komuniciranja. Organizacije, ki ohranjajo doslednost v svojih sporočilih, bodo bolje nadzorovale situacijo in se izognile nadaljnjim zapletom.



Shema 13: Tok informacij v kriznem vodstvu (vir: ICS)

4. Poudarite transparentnost

Transparentnost v krizni komunikaciji je temeljna za ohranjanje zaupanja med vsemi deležniki – naj bodo to zaposleni, stranke, partnerji ali širša javnost. V situacijah, ko je stres na vrhuncu, sta odprta in iskrena komunikacija ključna faktorja za ohranitev integritete ter verodostojnosti organizacije. Javno priznanje težave ali krize ni znak šibkosti, temveč odgovornega in profesionalnega pristopa k obvladovanju razmer. Vendar pa je transparentnost več kot le preprost dostop do informacij. Gre za zavezanost k pravočasnemu, natančnemu in popolnemu obveščanju javnosti o dogajanju ter ukrepih, ki jih organizacija izvaja za obvladovanje krize. Čeprav morda v začetnih fazah krize ni na voljo vseh podrobnosti, morajo organizacije sporočiti, kaj vedo, kaj ne vedo in kaj nameravajo narediti v prihodnje, da bodo zagotovile rešitev situacije.

3.1 Sprejemanje odgovornosti

Sprejemanje odgovornosti je pogosto eden najtežjih, a hkrati najpomembnejših vidikov krizne komunikacije. Organizacija, ki jasno in brez ovinkarjenja prizna svoje napake ali odgovornost za situacijo, bo pridobila večje zaupanje javnosti, kot tista, ki poskuša krivdo prevaliti drugam ali se izgovarjati.

Pomembno je poudariti, da sprejemanje odgovornosti ne pomeni priznanja poraza. Nasprotno, gre za pokazatelja močne vodstvene strukture, ki se zaveda svojih obveznosti do strank in družbe. Poleg tega je organizacija, ki prevzame odgovornost, bolj pripravljena na ukrepanje in odpravo težav, kar vodi do hitrejše rešitve krize.

3.2 Redno obveščanje

Rednost obveščanja je ključna za preprečevanje širjenja govoric in napačnih informacij, ki lahko dodatno poslabšajo krizo. Z jasno določenimi časovnimi okviri za posodabljanje informacij, organizacija ohranja nadzor nad dogajanjem in zmanjšuje negotovost med deležniki. Zaposleni in javnost morajo vedeti, kdaj lahko pričakujejo nove informacije. Tudi če v določenem trenutku ni bistvenih sprememb, je pomembno, da organizacija vzpostavi vzorec obveščanja in tako pokaže, da krizo aktivno obvladuje. Če organizacija ostane tiho, lahko pomanjkanje informacij sproži špekulacije, ki bi lahko še dodatno poslabšale situacijo.

4. Bodite pripravljeni na negativne odzive

V kriznih situacijah so negativni odzivi neizogibni. Zaposleni, stranke, mediji in širša javnost lahko izrazijo svoje nezadovoljstvo, jezo ali frustracijo, zlasti, če se počutijo zapostavljene ali slabo obveščene. Organizacije morajo biti pripravljene na obvladovanje teh odzivov na način, ki pomirja in ponovno vzpostavlja zaupanje. Pripravljenost na negativne odzive pomeni imeti jasno strategijo, kako se bo organizacija soočila s kritikami in jih upravljala v realnem času.

Negativni odzivi lahko prihajajo z različnih strani – od objav na socialnih omrežjih, do uradnih novinarskih poročil. Ključno je, da organizacija te odzive obravnava neposredno, brez odlašanja in ne ignorira težav ali poskuša utišati kritik. Tak pristop bi lahko še bolj poslabšal situacijo in povzročil dolgoročne poškodbe ugleda.

4.1 Upravljanje s komentarji in kritikami

Prva in najpomembnejša stvar pri obravnavanju negativnih komentarjev je priznavanje težave. Organizacije, ki kritike poskušajo prezreti ali jih obravnavajo z defenzivnim tonom, se pogosto znajdejo v še večjih težavah. Priznanje, da je kriza prizadela ljudi in da imajo pravico izraziti svoje mnenje, je prvi korak k pomiritvi situacije.

Ko gre za neposredne komentarje – naj gre za družbene medije, e-pošto ali druge oblike javnih odzivov – mora organizacija imeti jasno strategijo za obvladovanje teh komunikacij. Pomembno je, da se odzivate hitro, vendar s premišljenostjo, da sporočilo ne bo zvenelo neiskreno ali avtomatizirano. Vsak odgovor mora pokazati, da organizacija razume pomisleke in jih jemlje resno.

4.2 Ohranjanje mirnosti in profesionalnosti

Pri odzivanju na negativne odzive je nujno, da organizacija ohranja mirnost in profesionalen ton, tudi če so komentarji ostri ali čustveni. Pomembno je, da zaposleni, ki so odgovorni za komunikacijo, ostanejo osredotočeni na reševanje težave in ne na čustveni odziv. Profesionalen in miren pristop pripomore k zmanjšanju napetosti ter prepreči, da bi se situacija še dodatno zaostrila.

Tudi v primerih, ko so kritike neupravičene ali preveč čustvene, se mora organizacija izogibati defenzivnemu ali napadalnemu tonu. Zmernost in objektivnost bosta pomagala ohranjati ugled podjetja in pokazala, da organizacija situacijo obvladuje na zrel ter odgovoren način.

5. Spremljajte odzive in prilagajajte strategijo

V kriznih situacijah je sposobnost hitrega prilagajanja izjemno pomembna. Načrti in strategije, pripravljeni vnaprej, so ključni, vendar je dinamika vsake krize nepredvidljiva. Razmere se lahko spremenijo v trenutku, zato mora organizacija nenehno spremljati odzive in biti pripravljena prilagoditi svojo komunikacijsko strategijo, če ugotovi, da ne dosega želenih rezultatov. Spremljanje odzivov vključuje aktivno opazovanje vseh kanalov, na katerih se odvija komunikacija – to vključuje družbene medije, spletne strani, forume, tradicionalne medije in tudi neposredne povratne informacije zaposlenih ter strank. Nenehno ocenjevanje odzivov vam omogoča, da razumete, kako javnost doživlja vaša sporočila, in hkrati prepoznate morebitne šibke točke v vaši komunikaciji.

5.1 Analiza odzivov v realnem času

V kriznih trenutkih je analiza odzivov javnosti v realnem času neprecenljiva. Organizacija mora biti sposobna hitro obdelati podatke, ki prihajajo iz različnih virov, in ugotoviti, kako se odziva javnost. Z uporabo orodij za spremljanje medijev in družbenih omrežij lahko hitro zaznate trende ter prepoznate morebitna vprašanja, ki zahtevajo takojšnjo pozornost.

Analitična orodja, ki omogočajo vpogled v razpoloženje javnosti, lahko pomagajo pri prepoznavanju morebitnih težav, ki jih morda sprva niste opazili. Če se negativni odzivi začnejo kopičiti ali se pojavijo napačne informacije, je pomembno, da organizacija nemudoma ukrepa in prilagodi svojo strategijo za komuniciranje, da prepreči širjenje napačnih podatkov.

5.2 Prilagoditve strategije

Ko spremljate odzive, je pomembno, da ste pripravljeni prilagoditi svojo strategijo, če ugotovite, da vaše trenutne metode ne delujejo. To morda pomeni spremembo načina, kako sporočate informacije ali pa preusmeritev pozornosti na bolj kritična področja, ki so bila sprva spregledana.

Prilagoditve strategije ne smejo biti le reaktivne, ampak tudi proaktivne. Na primer, če ugotovite, da določene informacije niso bile ustrezno posredovane določenim deležnikom, je smiselno nemudoma izboljšati komunikacijo in pojasniti nesporazume. Organizacije, ki se hitro in učinkovito prilagajajo, lahko omilijo vpliv krize ter sčasoma celo pridobijo ugled kot prilagodljive in odzivne entitete.

Na koncu je uspešno krizno komuniciranje odvisno od zmožnosti hitrega odziva, vendar tudi od pripravljenosti, da se sproti učimo in izboljšujemo. Z vztrajnim spremljanjem odzivov in sprotnim prilagajanjem strategije bo organizacija ostala korak pred krizo ter omejila njen negativen vpliv.

KLJUČNI KORAKI

1. **Pripravite krizni komunikacijski načrt**
   - **Identifikacija možnih kriz.**
   - **Določanje pristojnih oseb;** kdo bo vodil krizno komuniciranje in podporne vloge (zbiranje podatkov, spremljanje odziva javnosti, tehnična podpora).
   - **Zajeti ključne korake.**

2. Ko nastopi krizna situacija

1. Aktiviranje pristojnih oseb.
2. Določiti vpletene strani -> na koga bo situacija vplivala.
3. Preučitev dejstev -> posledice.
4. Obveščanje zaposlenih.
5. Obveščanje vpletenih strani.
6. Tri ključna sporočila za javnost.
7. Prvi odziv hiter in dosleden – primerna komunikacija; stavki kratki, jedrnati in osredotočeni na dejstva – kaj se je zgodilo, kdo je prizadet, kaj se bo naredilo, da se situacija reši.
8. Spremljanje odziva in prilagajanje strategije.

3. Komuniciranje

Uporaba več kanalov:
- neposredna komunikacija z zaposlenimi,
- ustaljena komunikacija s vpletenimi stranmi,
- družbeni mediji,
- spletna stran,
- tradicionalni mediji.

Jasno komuniciranje:
- odprta in iskrena komunikacija,
- razumljiva, dosledna in kratka sporočila,
- strokovne izraze in postopke ustrezno poimenovati ter poenostaviti,
- ustna izjava: govorec miren in prijazen -> podati ključna sporočila ter pozitivno vsebino,
- težavo dobro priznati in sprejeti odgovornost, ampak se osredotočiti na rešitve,
- redno obveščanje zaposlenih, vpletenih strani in javnosti.

4. Negativni odzivi

- Priznati težavo ali izziv.
- Podati obrazložitev.
- Brez branjenja - izogibati defenzivnemu ali napadalnemu tonu.
- Mirnost in profesionalnost.
- Osredotočenost na reševanje težave.
- Zmernost in objektivnost.

Viri:

- ENISA (AVGUST 2016): Strategies for Incident Response and Cyber Crisis Cooperation. https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation/@@download/fullReport
- ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements

Poglavje 25
Napotki za varovanje podatkov - osebnih in drugih občutljivih podatkov

POVZETEK

Poglavje obravnava ključne vidike varovanja osebnih in občutljivih podatkov, vključno z zagotavljanjem skladnosti z zakonodajo, kot je GDPR, in najboljšimi praksami za tehnično ter fizično zaščito podatkov. Poudarjen je pomen ozaveščanja zaposlenih, prepoznavanja socialnega inženiringa ter priprave odzivnega načrta za primere incidentov. Namen je ponuditi celovite smernice za zaščito podatkov, ki pripomorejo k zmanjšanju tveganj ter preprečevanju zlorab in kršitev varnosti.

Ključne točke:

- Pravni okvir in skladnost z zakonodajo
- GDPR in nacionalni predpisi
- Zaupnost, celovitost in razpoložljivost podatkov
- Tehnični ukrepi: šifriranje, nadzor dostopa, revizije
- Fizična zaščita podatkov
- Ozaveščanje in usposabljanje zaposlenih
- Prepoznavanje socialnega inženiringa
- Odzivni načrt za varnostne incidente
- Poročanje o kršitvah varnosti
- Redne analize in posodobitve ukrepov.

1. Uvod

V današnjem digitalno prepletenem svetu postaja varovanje osebnih in drugih občutljivih podatkov ena ključnih odgovornosti tako za podjetja kot posameznike. Z vse večjo količino podatkov, ki se zbirajo in obdelujejo, raste tudi tveganje za zlorabe, nepooblaščene dostope ter kršitve zasebnosti. Osebni podatki, kot so ime, naslov, kontaktni podatki, zdravstveni zapisi in finančne informacije, predstavljajo neprecenljivo vrednost, ne samo za posameznika, temveč tudi za organizacije, ki te podatke upravljajo.

Poleg osebnih podatkov obstajajo tudi druge občutljive informacije, ki lahko vključujejo poslovne skrivnosti, intelektualno lastnino, finančne podatke ali transakcije, podatke o strankah ali celo strateške načrte organizacij. Zloraba takih informacij lahko vodi do finančne škode, izgube zaupanja strank in celo pravnih posledic. Zato je ključnega pomena, da vsaka organizacija vzpostavi robustne varnostne politike, ki ščitijo podatke pred grožnjami.

V tem dokumentu so predstavljeni ključni napotki za učinkovito varovanje podatkov, ki vključujejo pravni okvir, tehnične in fizične varnostne ukrepe ter pomen ozaveščanja zaposlenih. Namen besedila je zagotoviti jasna in uporabna navodila, ki bodo pripomogla k zmanjšanju tveganj ter zaščiti podatkov pred morebitnimi zlorabami.

2. Pravni okvir in skladnost z zakonodajo

Varovanje osebnih in občutljivih podatkov ni zgolj etična dolžnost, temveč tudi pravna obveznost, ki izhaja iz različnih zakonodajnih okvirov. Eden najpomembnejših zakonov na področju varstva osebnih podatkov v Evropski uniji je Splošna uredba o varstvu podatkov (GDPR). Uredba določa pravila in obveznosti za podjetja ter organizacije, ki zbirajo, obdelujejo ali hranijo osebne podatke državljanov EU. Njena glavna načela vključujejo preglednost, zakonitost, varnost in omejevanje namena obdelave podatkov.

GDPR zahteva, da podjetja zagotovijo, da se osebni podatki obdelujejo na pravičen, zakonit in pregleden način. Poleg tega določa, da morajo biti vsi osebni podatki zavarovani pred nepooblaščenim dostopom in uporabo, podjetja pa morajo vzpostaviti ustrezne tehnične ter organizacijske ukrepe za varstvo teh podatkov. Pomembno je poudariti, da kršitve zakonodaje, kot je GDPR, lahko vodijo do visokih glob, izgube zaupanja strank in resnih pravnih posledic.

Poleg GDPR so lahko pomembni tudi nacionalni zakoni o varstvu osebnih podatkov, ki jih je treba upoštevati, saj ti pogosto dopolnjujejo ali še natančneje določajo zahteve za specifična področja, kot so zdravstveni, finančni ali javni sektor. Organizacije morajo zato redno spremljati zakonodajne spremembe in zagotavljati skladnost z vsemi predpisi, ki vplivajo na njihovo dejavnost. V Sloveniji velja ZVOP-2, ki dopolnjuje GDPR in se obvezno uporablja skupaj z njo.

Med druge občutljive podatke štejemo tudi podatke, ki jih opredeljujejo drugi predpisi:

- poslovna skrivnost na podlagi Zakona o poslovni skrivnosti,
- tajni podatek na podlagi Zakona o tajnih podatkih,
- zaupne informacije na podlagi Zakona o bančništvu.

Pri varovanju občutljivih podatkov je prav tako pomembno upoštevati zahteve, povezane z dolžnostmi obveščanja ob kršitvah podatkov. V primeru kršitve je podjetje dolžno o tem obvestiti pristojne organe, in če je treba, tudi posameznike, katerih podatki so bili prizadeti. Skladnost z zakonodajo in transparentnost v komunikaciji ob takšnih dogodkih sta ključni za ohranitev zaupanja strank ter omejitev potencialne škode.

3. Ključna načela varstva podatkov

Za učinkovito varovanje osebnih in občutljivih podatkov morajo organizacije spoštovati osnovna načela, ki zagotavljajo zaupnost, celovitost ter razpoložljivost podatkov. Ta načela so temeljni stebri vsake varnostne strategije in pomagajo preprečevati nepooblaščene dostope, izgubo podatkov ter druge grožnje, po-

vezane s kibernetskimi napadi in notranjimi napakami.

- **Zaupnost** podatkov pomeni, da so osebni in občutljivi podatki dostopni samo tistim, ki so za to pooblaščeni. Organizacije morajo vzpostaviti politike dostopa, ki temeljijo na principu najmanjših pravic, kar pomeni, da zaposleni dostopajo le do tistih podatkov, ki jih potrebujejo za svoje delo. Zaupnost se zagotavlja tudi s šifriranjem podatkov, tako med prenosom kot v mirovanju, kar preprečuje nepooblaščenim osebam branje podatkov tudi v primeru njihovega prestrezanja.
- **Celovitost** podatkov zagotavlja, da se podatki nepooblaščeno ne spreminjajo. To načelo je ključno za preprečevanje napak, ki bi lahko povzročile izgubo pomembnih informacij ali poškodovale podatke. Redne varnostne kopije, digitalni podpisi in mehanizmi za preverjanje integritete podatkov so ključni ukrepi, ki pomagajo pri zagotavljanju, da so podatki točni, popolni ter veljavni skozi celoten cikel njihove obdelave. Del celovitosti je tudi neovrgljivost (ang. non-repudiation), ki zagotavlja, da je podatek res prišel od osebe, ki se predstavlja za naslovnika.
- **Razpoložljivost** podatkov pomeni, da so podatki dostopni in uporabni za pooblaščene uporabnike, kadar je to treba. Učinkovito varovanje podatkov vključuje tudi zaščito pred izgubo zaradi tehničnih napak, naravnih nesreč ali kibernetskih napadov, ki lahko preprečijo dostop do podatkov. Tukaj pridejo v poštev varnostne kopije, robustni sistemi za obnovo podatkov in redundantni strežniki, ki zagotavljajo, da so podatki na voljo tudi v primeru okvare ali napada.

4. Ukrepi za tehnično zaščito podatkov

Tehnični ukrepi za zaščito podatkov so ključnega pomena za preprečevanje nepooblaščenega dostopa, zlorab in izgube podatkov. Organizacije morajo implementirati celovit nabor varnostnih ukrepov, ki zagotavljajo zaupnost, celovitost in razpoložljivost podatkov. Ti ukrepi vključujejo šifriranje podatkov, vzpostavitev sistemov za nadzor dostopa, redne varnostne preglede in uporabo naprednih orodij za zaznavanje ter preprečevanje vdorov.

- **Šifriranje podatkov** je eden izmed najosnovnejših, a hkrati najučinkovitejših ukrepov za varovanje podatkov. Z njim se podatki kodirajo na način, da so nečitljivi za nepooblaščene osebe. Šifriranje je ključnega pomena tako pri prenosu podatkov (na primer med dvema strežnikoma ali med uporabnikom in aplikacijo) kot tudi v mirovanju, ko so podatki shranjeni na diskih ali v oblačnih okoljih. Z uporabo močnih šifrirnih algoritmov lahko podjetja znatno zmanjšajo tveganje za krajo ali zlorabo podatkov, tudi če pride do njihovega prestrezanja ali izgube naprav.
- **Dostopni kontrolni sistemi**: nadzor dostopa je temelj varovanja občutljivih podatkov. Organizacije morajo zagotoviti, da imajo do podatkov dostop samo tiste osebe, ki to potrebujejo za opravljanje svojega dela. To vključuje uporabo mehanizmov za preverjanje identitete, kot so dvofaktorska avtentikacija (2FA), ter vzpostavitev jasnih pravil za dodeljevanje in odvzemanje dostopnih pravic. Sistem za nadzor dostopa bi moral biti zasnovan na principu najmanjših privilegijev, kar pomeni, da ima vsak uporabnik dostop samo do tistih podatkov, ki so nujno potrebni za opravljanje njegove naloge.
- **Redne varnostne revizije in ocene tveganja**: tehnični ukrepi morajo biti redno preverjani in prilagajani glede na nove grožnje ter tehnološke spremembe. Redne varnostne revizije omogočajo organizacijam, da odkrijejo morebitne ranljivosti v svojih sistemih, prepoznajo neustrezne prakse in implementirajo izboljšave. Ocene tveganja so prav tako bistven del tega procesa, saj pomagajo določiti, kateri podatki so najbolj kritični za poslovanje in katere grožnje so najbolj verjetne ter jih je treba obravnavati prednostno.

5. Fizična zaščita občutljivih podatkov

Poleg tehničnih ukrepov je enako pomembna tudi fizična zaščita podatkov, saj lahko do uhajanja podatkov pride tudi zaradi fizičnih vdorov ali neustrezno varovanih prostorov in naprav. Učinkovita fizična varnost vključuje tako zaščito strojne opreme kot tudi ustrezno ravnanje z dokumentacijo, ki vsebuje občutljive podatke. Organizacije morajo zagotoviti, da so vse fizične naprave, ki hranijo ali obdelujejo podatke, ustrezno varovane, dostop do teh naprav pa omejen le na pooblaščene osebe.

Strežniške sobe in podatkovni centri so srce digitalne infrastrukture vsake organizacije, saj shranjujejo ključne podatke in omogočajo njihovo obdelavo. Fizična zaščita teh prostorov mora vključevati omejen dostop do tehničnega osebja s preverjanjem identitete, uporabo nadzornih sistemov, kot so kamere in varnostne ključavnice, ter omejevanje fizičnega dostopa do strežnikov. Hkrati je treba zagotoviti, da so prostori primerno zaščiteni pred naravnimi nesrečami, kot so poplave, požari ali potresi, z vzpostavitvijo varnostnih mehanizmov, kot so protipožarne zaščite in redundantne električne napajalne rešitve.

Čeprav večina občutljivih podatkov danes obstaja v digitalni obliki, pa so tiskani dokumenti še vedno pomemben del vsakodnevnega poslovanja, zlasti v nekaterih panogah, kot so bančništvo, zdravstvo in pravne storitve. Zaupni dokumenti morajo biti shranjeni v zaklenjenih omarah ali trezorjih, ki so dostopni le pooblaščenim osebam. Organizacije morajo vzpostaviti politiko ravnanja s tiskano dokumentacijo, ki vključuje pravilno označevanje zaupnih dokumentov, varno shranjevanje in redno uničevanje zastarelih ali nepotrebnih dokumentov z uporabo uničevalcev papirja, ki zagotavljajo, da dokumenti ne morejo biti obnovljeni.

6. Ozaveščanje zaposlenih in usposabljanje

Eden najpogosteje spregledanih vidikov varovanja podatkov je človeški dejavnik. Tudi najbolj napredni tehnološki in fizični ukrepi lahko postanejo neučinkoviti, če zaposleni niso dovolj ozaveščeni in usposobljeni glede pravilnega ravnanja z občutljivimi podatki. Ozaveščanje zaposlenih o potencialnih nevarnostih in najboljših praksah za varovanje podatkov je zato nujen del vsake varnostne strategije.

Redna in ciljno usmerjena usposabljanja zaposlenih so ključnega pomena za vzdrževanje visoke stopnje varnosti. Zaposleni morajo biti obveščeni o trenutnih grožnjah, kot so phishing napadi, socialni inženiring in zlonamerna programska oprema. Poleg tega je nujno, da razumejo pomen pravilnega ravnanja z občutljivimi podatki, vključno z varnim shranjevanjem, deljenjem in uničevanjem teh podatkov. Usposabljanja naj bodo prilagojena vlogam zaposlenih znotraj organizacije – na primer, tehnično osebje potrebuje bolj poglobljeno tehnično znanje, medtem ko so splošni zaposleni lahko bolj osredotočeni na prepoznavanje in preprečevanje socialnega inženiringa. Socialni inženiring je ena najpogostejših tehnik, s katero hekerji manipulirajo z ljudmi, da pridobijo dostop do občutljivih podatkov. Ta oblika napada se pogosto začne z na videz nedolžnim e-poštnim sporočilom ali telefonskim klicem, ki od zaposlenega zahteva razkritje zaupnih informacij ali dostop do notranjih sistemov. Organizacije morajo zato svoje zaposlene naučiti, kako prepoznati znake socialnega inženiringa, kot so nenavadne prošnje za informacije, pritiski po hitrem ukrepanju ali sumljive povezave v e-poštnih sporočilih. Ključno je, da imajo zaposleni jasna navodila, kam se obrniti v primeru, ko prejmejo sumljivo zahtevo.

Napadalci se v fazi poizvedovanja poslužujejo tudi informacij iz odprtih virov (ang. OSINT, open source intelligence), zato je ključnega pomena tudi ozaveščanje o podatkih in informacijah, ki jih posameznik sam (vede ali nevede) deli na družabnih omrežjih, na drugih podobnih spletnih platformah oziroma na spletu nasploh.

7. Incidenti in odzivni načrt

Kljub najboljšim prizadevanjem za varovanje podatkov se včasih zgodi, da pride do varnostnih incidentov. Učinkovit odziv na incident je ključnega pomena za omejevanje škode, hitro obnovitev sistemov in zmanjšanje posledic za poslovanje ter zaupanje strank. Zato je bistveno, da imajo organizacije pripravljen in jasno določen odzivni načrt, ki ga redno preizkušajo ter posodabljajo.

Odzivni načrt za varnostne incidente mora zajemati jasne postopke za ravnanje v primeru kršitve varnosti podatkov. Pomembno je, da so določene odgovorne osebe in timi, ki bodo vodili odziv na incident, ter da so vzpostavljeni jasni protokoli za obveščanje ključnih deležnikov, vključno z vodstvom, tehničnimi ekipami in pravnimi strokovnjaki. Načrt mora vključevati postopke za takojšnjo omejitev škode, kot je izolacija prizadetih sistemov, onemogočanje dostopa nepooblaščenim uporabnikom in zavarovanje podatkov. Hkrati je pomembno, da so vsi zaposleni seznanjeni s tem, kako naj poročajo o morebitnih varnostnih incidentih in kakšni koraki sledijo, če opazijo sumljivo dejavnost.

V skladu z zakonodajo, kot je GDPR, so organizacije dolžne poročati o kršitvah osebnih podatkov v roku 72 ur po tem, ko so kršitev zaznale, če gre za kršitev, ki lahko predstavlja tveganje za pravice in svoboščine posameznikov. Zato je nujno, da organizacija hitro identificira, katere podatke je incident prizadel, in pripravi ustrezno poročilo za pristojne nadzorne organe. V nekaterih primerih bo treba o kršitvi obvestiti tudi prizadete posameznike, kar zahteva transparentno in natančno komunikacijo o tem, kakšne podatke so pridobili nepooblaščeni subjekti ter kakšni so možni ukrepi za zaščito prizadetih oseb. Po obvladovanju incidenta je pomembno opraviti podrobno analizo vzrokov, ki so pripeljali do kršitve. S tem organizacija pridobi vpogled v morebitne ranljivosti v svojih varnostnih postopkih in sistemih. Na podlagi teh ugotovitev je mogoče sprejeti izboljšave, ki vključujejo dodatne tehnične in organizacijske ukrepe za preprečevanje podobnih incidentov v prihodnosti. Redno testiranje in nadgrajevanje odzivnega načrta je ključno za učinkovito obvladovanje prihodnjih incidentov.

Viri:

- ENISA (Januar 2017) : Guidelines for SMEs on the security of personal data processing. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
- ENISA (Januar 2018): Handbook on Security of Personal Data Processing. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
- Informacijski pooblaščenec RS: https://www.ip-rs.si/

Poglavje 26
Napotki za upravljanje in hrambo dnevniških zapisov

POVZETEK

Besedilo poudarja pomen pravilnega upravljanja in hrambe dnevniških zapisov, ki so ključni za varnost, skladnost z zakonodajo in uporabo pri forenzičnih preiskavah. Predstavljene so najboljše prakse za beleženje, analizo, varno hrambo, arhiviranje in uničenje dnevnikov. Poseben poudarek je na skladnosti z zakonodajo in standardi, kot je ISO 27001, ter zagotavljanju varnosti podatkov in vzpostavljanju zaupanja med deležniki.

Ključne točke:

- Dnevniški zapisi
- Forenzične preiskave
- Beleženje in analiza dogodkov
- Centralizirano upravljanje dnevnikov
- Varna hramba in šifriranje
- Geografska lokacija hrambe
- Arhiviranje in uničenje podatkov
- Skladnost z zakonodajo (ZInfV, GDPR)
- Standard ISO 27001
- Zaupanje in varnost podatkov.

1. Uvod v dnevniške zapise

Dnevniški zapisi so nepogrešljiv element varnostnega sistema, saj zagotavljajo sledi dogodkov in aktivnosti, ki potekajo znotraj informacijskih sistemov. Ti zapisi niso zgolj tehnični dnevnik aktivnosti; predstavljajo ključni vir informacij za analizo in oceno varnostnih tveganj, forenzične preiskave ter odpravljanje napak v sistemih. Bistveno je razumeti, da dnevniki niso zgolj za notranjo uporabo tehničnih ekip. Njihova pomembnost se odraža tudi pri izpolnjevanju zakonodajnih zahtev in zagotavljanju skladnosti s standardi. Organizacije, ki ne upravljajo pravilno z dnevniki, tvegajo izgubo dragocenih informacij, ki bi lahko bile ključne za reševanje incidentov ali dokazovanje skladnosti z zakonodajo. Poleg tega so pravilno vzdrževani dnevniki osnova za vzpostavitev zaupanja med poslovnimi partnerji in strankami.

V tem kontekstu postaja jasno, da učinkovito upravljanje dnevniških zapisov zahteva strateški pristop. Ne gre zgolj za tehnično beleženje dogodkov, temveč za vzpostavitev postopkov, ki zagotavljajo varno in zanesljivo hrambo podatkov ter njihovo pravočasno analizo.

2. Zakaj so dnevniški zapisi pomembni?

Pomen dnevniških zapisov daleč presega zgolj tehnično vlogo beleženja dogodkov. Njihova vrednost se izraža v več različnih vidikih, ki vplivajo na celovito varnost, zanesljivost in skladnost z zakonodajo v organizacijah.

Prvi ključni razlog je zagotavljanje sledi dogodkov za potrebe forenzičnih analiz. Brez dnevniških zapisov bi bila preiskava morebitnih varnostnih incidentov precej otežena, saj ne bi bilo mogoče natančno rekonstruirati dogajanja v informacijskem sistemu. Tako v primeru vdorov, zlonamernih aktivnosti ali celo tehničnih napak lahko dnevniki razkrijejo natančne korake, ki so vodili do incidenta. V primeru zlonamernih napadov so tovrstni podatki ključni za ugotavljanje načina dostopa, obsega škode in potencialnih slabosti v sistemu.

Poleg forenzičnih namenov pa dnevniški zapisi omogočajo tudi sprotno spremljanje delovanja sistema. Organizacije, ki spremljajo dnevnike v realnem času, lahko hitro zaznajo nepravilnosti, kot so povečano število napak, poskusi dostopa do občutljivih podatkov ali sistemske napake, ki lahko vodijo v večje težave. Varnostne ekipe se pogosto zanašajo na te podatke, da identificirajo potencialne grožnje, preden te prerastejo v večje incidente.

Nenazadnje je hramba in analiza dnevniških zapisov tesno povezana z zakonodajnimi ter regulativnimi zahtevami. Organizacije, ki delujejo v sektorjih, kot so finance, zdravstvo ali energetika, morajo pogosto dokazovati skladnost z zakonodajo in varnostnimi standardi, kot je ISO 27001. Dnevniki so lahko dokaz, da so bili varnostni protokoli ustrezno izvajani, da ni bilo nepooblaščenih dostopov do podatkov, in da je bil sistem ves čas ustrezno zaščiten. Pomanjkanje teh zapisov lahko vodi v pravne težave in visoke kazni.

3. Najboljše prakse za upravljanje dnevniških zapisov

Upravljanje dnevniških zapisov ni samo tehnična naloga, temveč zahteva skrbno načrtovanje in implementacijo ustreznih postopkov. Tukaj so nekatera ključna priporočila, kako zagotoviti, da so dnevniki koristni, varni in dostopni, ko jih potrebujete.

- **Redna analiza dnevniških zapisov**: Za zagotovitev varnosti je priporočljivo, da se dnevniki ne zgolj beležijo, temveč tudi redno analizirajo. Organizacije lahko vzpostavijo avtomatizirane procese, ki v realnem času analizirajo dnevnike in sprožijo alarm v primeru sumljivih aktivnosti. Tak pristop omogoča hitro odzivanje na morebitne grožnje.
- **Samodejno beleženje pomembnih dogodkov**: Sistemi naj bodo konfigurirani tako, da samodejno beležijo pomembne dogodke, kot so prijave, poskusi dostopa, napake sistema in spremembe konfiguracij. Ročno beleženje je nepraktično in ne-

zanesljivo, zato je nujno, da se ti procesi avtomatizirajo.

- **Centralizirano zbiranje zapisov**: V velikih organizacijah, kjer obstajajo številni sistemi in platforme, je priporočljivo zbirati dnevnike iz različnih virov v centraliziranem sistemu za upravljanje dnevnikov. Centralizacija olajša pregled nad celotno infrastrukturo in omogoča hitrejše zaznavanje anomalij.

Za učinkovito upravljanje dnevniških zapisov je torej pomembno upoštevati načela avtomatizacije, centralizacije in rednega spremljanja. Le tako lahko zagotovite, da bodo dnevniki uporabni tako za operativne kot za forenzične potrebe.

4. Hramba dnevniških zapisov

Hramba dnevniških zapisov je ključni element upravljanja, saj morajo biti ti podatki varno shranjeni za določeno časovno obdobje, odvisno od zakonodajnih in operativnih zahtev posamezne organizacije. Pravilna hramba ni samo vprašanje varnosti, temveč tudi vprašanje skladnosti z zakonodajo.

Trajanje hrambe

Pri določanju obdobja hrambe dnevniških zapisov je treba upoštevati naravo podatkov, pravne zahteve in potrebe podjetja. Na primer, finančne institucije so pogosto dolžne hraniti dnevnike za daljša obdobja, v nekaterih primerih celo več let, medtem ko lahko druge industrije zahtevajo krajše obdobje hrambe. Ključno je, da se vsakodnevno upravljanje podatkov prilagodi specifičnim potrebam, saj lahko pretirano dolga hramba dnevnikov brez pravega razloga privede do nepotrebnih stroškov in preobremenitve sistemov.

Varna hramba

Zagotavljanje varnosti pri hrambi dnevnikov je ključnega pomena. Dnevniki pogosto vsebujejo občutljive podatke, kot so informacije o prijavah uporabnikov, dostopih do sistemov in napakah. Zato je treba te podatke shranjevati na zanesljivih in varovanih lokacijah, dostop do njih pa omejiti na pooblaščene osebe. Šifriranje dnevniških zapisov je ena od najboljših praks, ki zagotavlja, da tudi v primeru vdora v sistem ti podatki ostanejo varni.

Geografska lokacija hrambe

Geografska lokacija, kjer se hranijo dnevniki je prav tako pomembna. Priporočljivo je, da se dnevniki hranijo v zanesljivih in varnih podatkovnih centrih, pri čemer je zlasti pomembna redundantnost – hranjenje dnevniških zapisov na več lokacijah zagotavlja, da podatki ne bodo izgubljeni v primeru naravnih nesreč ali drugih nepredvidenih dogodkov. V skladu s 17. členom Zakona o informacijski varnosti (ZInfV) je zahtevano, da se ohranjanje dnevniških zapisov zagotovi na ozemlju Republike Slovenije, kar dodatno pripomore k varnosti in skladnosti z zakonskimi določili.

5. Pravilno arhiviranje in uničenje dnevniških zapisov

Za dolgoročno varnost je izjemno pomembno, da organizacije vzpostavijo jasne postopke za arhiviranje in uničenje dnevniških zapisov. Napačno upravljanje lahko vodi do nepotrebnih tveganj, kot so izguba podatkov, neskladnost z regulativnimi zahtevami ali celo vdori, če podatki niso ustrezno zaščiteni.

Arhiviranje

Ko dnevniki niso več potrebni za vsakodnevno spremljanje, jih je treba pravilno arhivirati. Arhiviranje je postopek premika dnevniških zapisov iz aktivne uporabe v varno shrambo. Organizacije bi morale vzpostaviti jasne smernice, ki določajo, kateri zapisi bodo arhivirani, za koliko časa in na kakšen način bodo ti podatki dostopni. Pri tem je treba paziti, da so arhivirani dnevniki zaščiteni pred nepooblaščenim dostopom in shranjeni na varnih ter zanesljivih lokacijah, da preprečimo izgubo podatkov.

Poleg tega mora biti dostop do arhiviranih dnevnikov omejen na pooblaščeno osebje. Vsak dostop bi moral biti zabeležen, da se zagotovi sledljivost in preglednost. To je zlasti pomembno v primerih, ko se dnevniki upora-

bljajo kot dokazno gradivo pri pravnih postopkih ali forenzičnih preiskavah.

Postopki uničenja

Ko dnevniki presežejo obdobje hrambe, jih je treba varno uničiti. Pomembno je, da postopek uničenja sledi ustaljenim varnostnim protokolom, in da se zagotovi, da uničenje podatkov poteka nepopravljivo, brez možnosti kasnejše obnove. To vključuje uničenje varnostnih kopij in arhivov.

Uničenje dnevniških zapisov se mora izvajati v skladu z zakonodajnimi zahtevami, zlasti tistimi, ki so povezane z varovanjem osebnih podatkov. Na primer, organizacije, ki hranijo osebne podatke, morajo biti zlasti pozorne na to, da se podatki uničijo v skladu s pravili o varstvu podatkov, kot jih določa GDPR. Nepravilno uničenje ali pozabljeno uničenje starih dnevnikov lahko privede do varnostnih incidentov ali pravnih posledic, zato je ta postopek kritičen za vsako organizacijo.

6. Skladnost z zakonodajo in varnostnimi standardi

Skladnost z zakonodajo in varnostnimi standardi je eden izmed najpomembnejših vidikov upravljanja dnevniških zapisov, saj imajo organizacije dolžnost, da zaščitijo občutljive podatke in preprečijo zlorabe. Varnostni standardi, kot je ISO 27001, postavljajo jasna pravila, kako je treba ravnati z dnevniki, da bi se zagotovila ustrezna varnost in zaščita podatkov.

Uporaba standardov, kot je ISO 27001

Poleg skladnosti z zakonodajo morajo organizacije slediti tudi varnostnim standardom, kot je ISO 27001, ki določa sistematičen pristop k upravljanju informacij in varnostnih procesov. Ta standard zahteva, da se vzpostavijo in dokumentirajo postopki za upravljanje dnevniških zapisov, kar vključuje natančno opredelitev, kako ter kje se dnevniki hranijo, kdo ima dostop do njih, in kako se obdelujejo ter uničujejo.

Skladnost z ISO 27001 pomaga organizacijam tudi pri vzpostavljanju zaupanja med strankami in poslovnimi partnerji, saj zagotavlja, da so varnostni ukrepi na najvišji ravni. To je zlasti pomembno v kritičnih sektorjih, kjer je varnost podatkov ključnega pomena.

Viri:

- ENISA (December 2016): Technical Guidelines for the implementation of minimum security measures for Digital Service Providers. https://www.enisa.europa.eu/publications/minimum-security-measures-for--digital-service-providers
- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls

Poglavje 27
Napotki glede fizičnega varovanja prostorov

POVZETEK

Besedilo obravnava ključne elemente učinkovitega fizičnega varovanja prostorov, kot so analiza tveganj, določitev varnostnih ciljev in politik, nadzor dostopa, video nadzor, fizične pregrade ter požarna varnost. Poseben poudarek je na uporabi tehničnih rešitev, kot so elektronski sistemi za nadzor dostopa in skladnosti z zakonodajo ter standardi, kot je ISO/IEC 27002. Cilj je zagotoviti celovito zaščito premoženja, zaposlenih in informacijskih virov.

Ključne točke:

- Fizično varovanje prostorov
- Analiza tveganj in ocena groženj
- Varnostni cilji in politike
- Nadzor dostopa (biometrija, elektronske kartice)
- Video nadzor (strategija, zakonodaja)
- Fizične pregrade (ograje, varovana vrata)
- Požarna varnost (sistemi za zaznavanje dima, evakuacija)
- Skladnost z zakonodajo in standardi (ISO/IEC 27002)
- Tehnični sistemi in integracija
- Usposabljanje zaposlenih.

Fizična varnost prostorov je ključni vidik vsake organizacije, saj varuje pred različnimi fizičnimi grožnjami, kot so kraje, nepooblaščen dostop in naravne nesreče. V sodobnih podjetjih, kjer so občutljivi podatki in ključna oprema glavni, je zagotavljanje ustrezne fizične varnosti bistvenega pomena za ohranjanje nemotenega delovanja in s tem skladnosti s sistemom zagotavljanja neprekinjenega delovanja .

Fizična varnost je dobro opredeljena tudi v standardu **ISO/IEC 27002**, ki ponuja smernice za zaščito prostorov, infrastrukture in informacijskih sistemov. Skladnost s temi smernicami zagotavlja celovit pristop k zmanjšanju tveganj ter zaščiti ključnih virov.

1. Analiza tveganj in ocena groženj

Učinkovito fizično varovanje prostorov se vedno začne z natančno analizo tveganj in oceno groženj. Ta korak organizacijam omogoča razumevanje potencialnih nevarnosti, ki bi lahko ogrozile varnost objektov, sredstev in zaposlenih. Pomembno je, da se ta analiza izvaja redno, saj se grožnje nenehno spreminjajo – od novih tehnik vlomov do naravnih nesreč, kot so poplave in potresi, ki lahko ogrozijo delovanje prostorov.

Pri analizi tveganj je treba upoštevati specifične značilnosti objekta in okolja. Na primer, v urbanih okoljih so pogostejša tveganja, povezana s kriminalom, medtem ko so v bolj oddaljenih območjih lahko večje nevarnosti povezane z dostopnostjo in odzivnostjo na incidente. Poleg tega je ključno, da se identificirajo kritične točke ranljivosti, kot so vhodi, izhodi, skladišča, IT-sobe in parkirišča, ki pogosto predstavljajo cilje napadov.

Po končani analizi je priporočljivo pripraviti poročilo, ki vsebuje predloge za izboljšave ter prednostno lestvico ukrepov. To omogoča jasno sliko o tem, kje so potrebne največje naložbe v varnost, in pomaga določiti odgovornosti v podjetju. Ocena groženj je tudi temelj za oblikovanje kasnejših varnostnih politik in ciljev, ki jih je treba postaviti znotraj organizacije.

2. Določitev varnostnih ciljev in politik

Po zaključku analize tveganj sledi določitev varnostnih ciljev in politik, ki organizaciji omogočajo usmerjanje naporov na ustrezna področja. Varnostni cilji morajo biti jasno definirani, konkretni in merljivi, da se lahko učinkovito spremlja njihova implementacija in uspešnost. Določitev teh ciljev je odvisna od specifičnih potreb organizacije in ugotovitev analize tveganj.

Glavni varnostni cilji lahko vključujejo:

- Varovanje zaposlenih in premoženja organizacije zaradi vseh fizičnih vplivov (požar, potres, poplave ter ostalo).
- Preprečevanje nepooblaščenega dostopa do varovanih območij.
- Zmanjševanje tveganj, povezanih z notranjimi grožnjami (zaposleni, pogodbeni izvajalci).
- Zaščita vitalnih sredstev, kot so podatki in pomemba infrastruktura.

Na podlagi teh ciljev je treba vzpostaviti varnostne politike, ki služijo kot okvir za vedenje zaposlenih, obiskovalcev in varnostnega osebja. Politike morajo pokrivati širok spekter varnostnih področij – od upravljanja z dostopi do ravnanja v izrednih situacijah. Ključno je tudi, da so te politike žive in prilagodljive, saj varnost ni statičen proces. Z novimi grožnjami in tehnološkimi rešitvami se morajo varnostne politike stalno posodabljati, kar zahteva tesno sodelovanje med varnostnim vodstvom ter preostalimi oddelki v podjetju.

3. Nadzor dostopa

Nadzor dostopa predstavlja temeljni element fizičnega varovanja, saj omogoča učinkovito omejevanje gibanja oseb znotraj določenih območij. V sodobnem okolju obstajajo številne tehnologije za nadzor dostopa, ki omogočajo visoko raven prilagodljivosti in varnosti. Uporaba elektronskih sistemov, kot so pametne kartice ali biometrični sistemi, omogoča ne le preprečevanje nepooblaščenega dostopa,

temveč tudi natančno sledenje, kdo in kdaj je vstopil v določen prostor.

Ključne tehnologije za nadzor dostopa vključujejo:

- **Elektronske kartice in bralniki**: Omogočajo enostavno in varno upravljanje z dostopi. Te kartice so pogosto opremljene s funkcijo beleženja vstopov, kar omogoča natančen nadzor nad gibanjem oseb. Navedeni sistemi morajo biti ustrezno certificirani, elektronske kartice pa morajo omogočati ustrezno šifriranje, ki ga ni mogoče zlorabiti oz. spreminjati s strani nepooblaščenih oseb.
- **Biometrični sistemi**: Prepoznava prstnih odtisov, obrazov ali šarenice ponuja visoko raven zaščite, saj je biometrične podatke izredno težko ponarediti. Za uvedbo teh sistemov je treba predhodno izvesti temeljito DPIA (oceno učinkov na varovanje osebnih podatkov) in pridobiti ustrezno mnenje Informacijskega pooblaščenca.
- **PIN-kodni sistemi**: Čeprav so manj varni v primerjavi z biometričnimi sistemi, so še vedno učinkoviti, zlasti če so PIN kode redno posodobljene.

Nadzor dostopa ni le tehnološki izziv, temveč zahteva tudi jasno definirane protokole za upravljanje dostopa. Na primer določitev, kdo ima dostop do katerih območij in v kakšnih okoliščinah, mora biti jasno dokumentirano. Redno je treba izvajati tudi preglede sistema, da se zagotovi brezhibno delovanje in posodabljanje dostopov skladno s kadrovskimi spremembami.

Načrtovanje in izvedbo vgraditve omenjenih sredstev tehničnega varovanja lahko izvajajo le za to ustrezno usposobljene ter licencirane organizacije, ki imajo ustrezno licenco na podlagi zakona o zasebnem varovanju.

4. Video nadzor in tehnični sistemi

Video nadzor predstavlja ključno orodje za zagotavljanje fizične varnosti v vsakem objektu. Kamere so v preteklosti služile predvsem kot odvračalno sredstvo, vendar se z razvojem tehnologij zdaj uporabljajo kot aktivno orodje za sledenje, odkrivanje in analizo sumljivih dejavnosti. Pomembno je, da so kamere nameščene na strateških točkah – vhodi in izhodi, hodniki, parkirišča ter skladišča, kjer je tveganje za incidente največje.

Pri implementaciji video nadzora je treba upoštevati več dejavnikov:

- **Kakovost posnetkov**: Kamere z visoko ločljivostjo omogočajo prepoznavo oseb in podrobnosti, kar je ključno pri preiskovanju incidentov.
- **Shranjevanje posnetkov**: Posnetke je treba hraniti varno in v skladu z zakonodajo. Pri tem je pomembno, da so ti šifrirani in dostopni le pooblaščenim osebam.
- **Integracija s senzorji gibanja in alarmi**: Napredni sistemi video nadzora so povezani s senzorji, ki ob zaznavanju nenavadnih gibanj sprožijo takojšnje ukrepe. Takšni sistemi omogočajo hitrejšo zaznavo potencialnih groženj.
- **Oddaljen nadzor**: Z modernimi tehnologijami lahko varnostno osebje spremlja posnetke v realnem času prek oddaljenega dostopa, kar omogoča hiter odziv tudi v primeru, ko so osebno odsotni.

Video nadzor ima tudi svojo pravno komponento, ki jo organizacije ne smejo zanemariti. Pomembno je, da se video nadzor izvaja skladno z lokalno zakonodajo o zasebnosti, kar vključuje pravilno obveščanje zaposlenih in obiskovalcev o obstoju kamer ter primerno upravljanje posnetkov. Organizacija mora glede na oceno ogroženosti zagotoviti varnostno kopiranje podatkov video nadzornega sistema in pristope kontrole. Varnostne kopije se potrebuje za rekonstrukcijo dogodkov in jih je treba hraniti na ustrezni sekundarni lokaciji ter primerno urediti prenosno povezavo oz. kopiranje teh.

Signali vseh tehničnih sredstev morajo biti ustrezno po varnih povezavah speljani v ustrezne varnostno-nadzorne centre, kjer se na

podlagi sprejetih signalov tudi izvede ustrezna intervencija na mestu sprožitve signala ali zaznave nepooblaščenega gibanja.

5. Fizične pregrade in zaščitni elementi

Fizične pregrade predstavljajo prvi sloj obrambe pred nepooblaščenim vstopom v varovane prostore. Te pregrade so zasnovane tako, da otežijo ali preprečijo dostop do zaščitenih območij, bodisi skozi fizične ovire bodisi s tehničnimi sistemi, ki preprečujejo dostop. Kvalitetno zasnovan sistem fizičnega varovanja se začne že pri urejanju dostopa v samo organizacijo. To pomeni ustrezno varovano in zaščiteno recepcijo, ki predstavlja prvo in zelo pomembno vstopno točko v organizaciji. Največkrat se že po prvem stiku, ki se začne s fizičnim dostopom na recepciji organizacije, da zaključiti kakšno pozornost organizacija namenja procesom varovanja.

Najpogostejše fizične pregrade vključujejo:

- **Ograje in zidove**: Zaščita zunanjih obodov je temeljni del varovanja. Ograje morajo biti dovolj visoke in trdne, da odvračajo morebitne vlomilce. Pomembno je tudi, da se ti objekti redno vzdržujejo.
- **Varovana vrata in okna**: Posebna varnostna vrata in okna, opremljena z ojačanim steklom ali rešetkami, predstavljajo dodatno oviro pred fizičnim vdorom. Poleg tega lahko uporaba varnostnih ključavnic ali kodnih sistemov še dodatno poveča zaščito.
- **Senzorji in alarmi**: Ti tehnični sistemi dopolnjujejo fizične pregrade in so ključni za zaznavo poskusov vdora. Senzorji gibanja, alarmi na oknih in vratih ter tlačne plošče omogočajo zgodnje opozarjanje na sumljive dejavnosti.

Pri načrtovanju fizičnih pregrad je pomembno, da niso zasnovane le kot pasivne ovire, temveč so del širšega varnostnega sistema, ki vključuje tudi tehnologije za zaznavanje in odziv. Fizične pregrade morajo biti usklajene s potrebami objekta, da ne ovirajo normalnega delovnega procesa, vendar še vedno zagotavljajo visoko stopnjo zaščite.

Požarna varnost

Požarna varnost je eden izmed ključnih vidikov fizičnega varovanja prostorov, saj lahko požari povzročijo nepopravljivo škodo na premoženju, infrastrukturi in ogrozijo človeška življenja. Pri oblikovanju učinkovitega načrta za požarno varnost je treba upoštevati tako preventivne kot odzivne ukrepe, ki zmanjšujejo tveganje za nastanek požara in omogočajo hitro ukrepanje v primeru požarnega incidenta.

Preventivni ukrepi

Preprečevanje požara vključuje vrsto ukrepov, katerih cilj je zmanjšanje možnosti za nastanek izrednih dogodkov v prostorih. Med ključne preventivne ukrepe spadajo:

- **Namestitev protipožarnih sistemov**: To vključuje avtomatske gasilne sisteme, kot so brizgalniki (sprinklerji), ki se sprožijo ob zaznavi visokih temperatur. Sem vključujemo tudi ustrezno postavitev požarnih central, ki morajo biti pravilno povezane, da se prek njih posreduje signal na za to ustrezne odzivne službe ali centre (možno je, da so ti signali vezani na Varnostno operativne centre varnostnih služb, ki varujejo omenjene objekte ali direktno na pristojne lokalne gasilske enote).
- **Sistem za zaznavanje dima**: Detektorji dima so ključni za zgodnje odkrivanje požara in aktiviranje alarmov, ki omogočajo pravočasno evakuacijo.
- **Požarne lopute, povezave s prezračevanjem objektov**.
- **Varnostno shranjevanje nevarnih snovi**: Materiali, ki lahko povzročijo požar, morajo biti ustrezno shranjeni v ognjevarnih prostorih.
- **Redno vzdrževanje električnih napeljav**: Nepravilno vzdrževane ali poškodovane električne napeljave so pogost vzrok za požare, zato je redno pregledovanje nujno.

Poleg preventivnih ukrepov, ki so vezani na zgoraj navedene aktivnosti je treba izvajati tudi druge fizične preventivne ukrepe, ki so povezani z usposabljanjem osebja za različne situacije, kot na primer za situacije v glavnih pisarnah ob možnih tveganjih bioagensov ali drugih kemičnih substanc in podobnih situacij. Za to mora biti del teh aktivnosti povezan tudi z delom ustreznih postopkov v sklopu zaščite in reševanja ter upoštevanih zahtev uredbe o zaščitnih sredstvih za zaposlene in njihovo usposabljanje za uporabo teh zaščitnih sredstev. Omenjeni ukrepi niso omejeni samo na biološke ali kemijske sestavine, temveč so sem vključeni tudi postopki v primeru najave bombne grožnje in odzivi vseh potrebnih v organizaciji na omenjena tveganja.

Evakuacija in odziv

V primeru požara je hitra in organizirana evakuacija ključna za varnost oseb v objektu. Pomembno je, da so evakuacijski načrti jasno prikazani in redno preizkušeni. Ti načrti morajo vključevati:

- **Jasno označene evakuacijske poti**: Izhodi v sili morajo biti vedno dostopni, ustrezno označeni in redno preverjani.
- **Izobraževanje zaposlenih**: Zaposlene je treba redno izobraževati o postopkih evakuacije in uporabi gasilnih aparatov.
- **Namestitev gasilnih aparatov**: Na strateških točkah v objektu morajo biti nameščeni gasilni aparati, ki so primerni za različne vrste požarov (električni, kemični, itd.).

Vzdrževanje požarne varnosti

Redni pregledi in vzdrževanje protipožarnih sistemov so nujni za zagotavljanje njihove brezhibnosti. Priporočljivo je, da se izvajajo periodični preizkusi delovanja vseh sistemov za zaznavanje dima, brizgalnikov ter gasilnih aparatov. Poleg tega je pomembno, da se vzpostavi natančen načrt za izvajanje požarnih vaj in usposabljanj, da bodo vsi zaposleni ter obiskovalci seznanjeni s pravilnim ravnanjem v primeru požara.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls

Poglavje 28
Napotki za pripravo javnih naročil

POVZETEK

Besedilo obravnava ključne korake in varnostne usmeritve za pripravo javnih naročil, s poudarkom na zakonodajnih zahtevah, varovanju dobavne verige ter zagotavljanju skladnosti z varnostnimi standardi in predpisi. Poudarjen je pomen natančne opredelitve potreb, izbire zanesljivih ponudnikov, zaščite občutljivih informacij ter učinkovitega spremljanja in nadzora nad izvajanjem pogodbenih obveznosti.

Ključne točke:

- Javno naročanje (ZJN-3, ZJNPOV)
- Opredelitev potreb in ciljev naročila
- Zahteve za ponudnike (reference, standardi, ISO 27001, ISO 28000)
- Varovanje dobavne verige (ocena tveganj, pogodbeni mehanizmi)
- Postopek priprave in izvajanja naročila (ocene, razpis, ocenjevanje ponudb)
- Skladnost s predpisi (GDPR, standard ISO 27002, standard ISO 22301)
- Varovanje informacij in nadzor dostopa
- Upravni in tehnični nadzor nad izvajalci
- Pogodbene klavzule (zaupnost, pravica do revizije, protikorupcijska določila)
- Zaključevanje razmerja z izvajalcem (uničenje podatkov, prenos pravic).

Zaradi zahtevnosti poslovnega okolja je danes praktično nemogoče, da organizacija izvaja vse potrebne procese z lastnimi viri. To pomeni, da je treba za zagotavljanje celovitosti poslovanja posegati po storitvah zunanjih izvajalcev, ki jih organizacija na podlagi ustreznih postopkov angažira za izvedbo določenih strokovnih aktivnosti ali dobavo potrebne tehnologije. Na področju informacijske varnosti in pomanjkanja ustreznega kadrovskega potenciala je najemanje zunanjih izvajalcev zelo pogosta stalnica. V pričujočem poglavju bomo podali nekaj osnovnih napotil, ki so pomembne za razumevanje korakov naročanja storitev in blaga po postopkih javnega naročanja. Poleg tega pa bomo podali bistvene varnostne usmeritve, ki jih je treba smiselno upoštevati pri izbiri, sklepanju sporazumov, nadzoru nad zunanjimi izvajalci in zagotavljanju sodelovanja, ki bo zagotovil, da so ključne informacije lastne organizacije ustrezno obvladovane.

Zavedati se moramo, da je javno naročanje treba izvajati na podlagi Zakona o javnem naročanju (ZJN-3). Vendar je treba pri tem uporabiti pravo mero previdnosti, katere informacije se odkrivajo v fazi izvedbe naročila. Zakonska podlaga določa več možnosti kot so dvofazni postopek in ostalo, kjer se najprej preveri ustrezne prijavitelje in šele za tem odpre potrebne informacije za oddajo naročila. V teh primerih vendarle govorimo o ključnih organizacijah v Republiki Sloveniji, ki zagotavljajo izvajanje bistvenih storitev in so informacije o njihovih informacijskih sistemih smatrane kot zelo pomembne. Seveda zakonodaja za posebne primere dopušča tudi možnost uporabe dodatnih specifičnih predpisov kot so Zakon o javnem naročanju na področju obrambe in varnosti (ZJNPOV), kjer so postopki za izvedbo naročil izvedeni po posebnih korakih, ki zagotavljajo dodatno varnost informacij. Tako ZJNPOV kot ZJN-3 omogočata tudi izjemo javnega naročanja na podlagi 346. člena Pogodbe o delovanju EU (PDEU), pri čemer so države članice upravičene zavarovati informacije, za katere država meni, da bi bilo njihovo razkritje v nasprotju z bistvenimi interesi njene varnosti in/ali sprejeti ukrepe, za katere meni, da so potrebni za zaščito bistvenih interesov njene varnosti.

Priprava javnih naročil je ključnega pomena za zagotavljanje poštenega, preglednega in učinkovitega postopka, ki omogoča izbiro najprimernejšega ponudnika za specifične potrebe organizacije. Spodnji napotki vključujejo osnovne korake za pripravo javnih naročil, s poudarkom na varovanju dobavne verige ter zahteve za ponudnike.

1. Opredelitev potreb in ciljev javnega naročila

Pred pripravo razpisa je treba natančno opredeliti cilje, obseg in specifične zahteve javnega naročila. Vključimo sledeče:

- **Opredelitev predmeta naročila:** Opredelite podrobno vrsto blaga, storitev ali del, ki so predmet javnega naročila, ter njihov namen.
- **Tehnične specifikacije:** Zberite in določite vse tehnične zahteve ter standarde, ki jih mora izpolnjevati predmet naročila (npr. skladnost z ISO standardi).
- **Kriteriji za izbiro:** Na podlagi specifičnih potreb določite objektivne kriterije za ocenjevanje ponudb, kot so kakovost, cena, čas dostave, tehnična podpora, trajnost ipd.

2. Zahteve za ponudnike

Zagotoviti moramo skladnost ponudnika z zahtevami iz vsakokratno veljavnega zakona s področja javnega naročanju in jasno opredeliti tudi zahteve za sodelovanje, saj le tako jamčimo, da so izbrani ponudniki zanesljivi ter sposobni izpolniti zahteve naročila:

- **Izkušnje in reference:** Zahtevajte, da ponudniki dokažejo svoje izkušnje z relevantnimi referencami, ki potrjujejo njihovo usposobljenost in uspešno izvedbo podobnih projektov.
- **Finančna stabilnost:** Preverite finančno stabilnost ponudnikov, saj je to pomembno za zmanjšanje tveganja v dobavni verigi.

- **Certifikati in standardi:** Zahtevajte veljavne certifikate, ki izkazujejo skladnost ponudnikov s standardi, kot so ISO 9001 (kakovosti), ISO 27001 (informacijska varnost) in ISO 22301 (kontinuiteta poslovanja).
- **Kadrovska usposobljenost:** Zahtevajte podatke o ključnem osebju, ki bo zadolženo za izvedbo projekta, in dokazila o njihovih kvalifikacijah ter izkušnjah.

3. Varovanje dobavne verige

Varovanje dobavne verige postaja ključno področje pri javnih naročilih, saj zagotavlja varnost, kakovost in odpornost storitev ter izdelkov v celotnem življenjskem ciklu. Pomembni koraki vključujejo:

- **Ocenjevanje dobaviteljev:** Izvedite oceno dobaviteljev glede njihovih ukrepov za zagotavljanje varnosti storitev ali izdelkov, ki vam jih dobavljajo, zlasti to velja pri občutljivih področjih (npr. IT infrastruktura, občutljivi podatki).
- **Politika obvladovanja tveganj:** Zahtevajte od ponudnikov, da predložijo svoje politike za obvladovanje tveganj v dobavni verigi, vključno z načrti za kontinuiteto poslovanja v primeru motenj.
- **Pogodbeni mehanizmi:** V pogodbe vključite klavzule, ki omogočajo redno ocenjevanje skladnosti z varnostnimi standardi dobavne verige, in določite sankcije v primeru neskladnosti.
- **Pregled dostopa do informacij:** Določite ukrepe za nadzor dostopa do občutljivih informacij v dobavni verigi. Zahtevajte, da ponudniki zagotovijo ustrezne varnostne postopke in omejitve dostopa.

4. Postopek priprave in izvajanja javnega naročila

Za zagotovitev popolne preglednosti in skladne izvedbe celotnega procesa je priporočljivo slediti naslednjim korakom:

- **Ocena vrednosti**: Izbira vrste postopka javnega naročanja je odvisna od ocene vrednosti, ki se pripravi v skladu z metodologijo, predvideno v veljavni zakonodaji s področja javnega naročanja.
- **Izogibanje drobljenju javnih naročil**: Drobljenje lahko nastopi, kadar posamezne storitve ali predmeti dobave niso neposredno med seboj povezani, sodijo pa med isto vrsto dobav ali storitev. Poljubna ali strokovno neutemeljena delitev naročila, s katerio bi se dosegla umetna razdelitev (drobljenje) z namenom izogibanja se uporabi pravil javnega naročanja, ni skladna s cilji in polnim učinkom zakonodaje na področju javnega naročanja, tako na evropski kot tudi nacionalni ravni.
- **Priprava razpisa:** Razpis pripravite na podlagi zgoraj navedenih zahtev in smernic ter ga objavite na ustreznih platformah za javna naročila.
- **Predložitev ponudb:** Določite jasne roke in pogoje za predložitev ponudb ter poskrbite za način, ki omogoča transparentno zbiranje ponudb.
- **Ocenjevanje ponudb:** Pripravite postopek ocenjevanja ponudb na podlagi vnaprej določenih kriterijev in po potrebi uporabite metodologijo ponderiranja. Vključi naj se tudi oceno tveganj za dobavno verigo in zanesljivost ponudnikov.
- **Dodelitev naročila:** Izberite najboljšega ponudnika v skladu z ocenjenimi kriteriji, z njim sklenite pogodbo in poskrbite za redno spremljanje njegovega delovanja.

5. Spremljanje in nadzor pogodbe

Za uspešno izvajanje javnega naročila je treba vzpostaviti mehanizme za spremljanje in nadzor:

- **Redno poročanje:** Zahtevajte redna poročila ponudnikov o napredku in skladnosti z določili pogodbe.

- **Obvladovanje sprememb:** Zagotovite, da so vsi pomembni vidiki pogodbe zabeleženi in redno posodobljeni glede na spremembe v dobavni verigi.
- **Ocena uspešnosti dobavne verige:** Na koncu projekta izvedite analizo uspešnosti dobavne verige in ugotovite, ali so bili doseženi vsi cilji glede varnosti, kakovosti ter pravočasnosti dobave. Določeno pomoč vam lahko nudi standard ISO 28000:2022.

6. Pomen skladnosti s predpisi in standardi

Skladnost s predpisi in standardi, kot so Zakon o javnem naročanju, GDPR ter standardi ISO (skupina 27000 in skupina 28000), je bistvena za zagotavljanje zakonitega in varnega postopka. Pred pripravo javnega naročila preverite skladnost z aktualnimi zakonodajnimi zahtevami in vključite ustrezne smernice ter klavzule v razpisno dokumentacijo. Ta metodološki okvir za pripravo javnih naročil omogoča učinkovito izvajanje postopkov in zagotavlja varnost ter zanesljivost dobavne verige, s čimer organizacija izboljša varnost svojih projektov in poslovanja.

V nadaljevanju je podanih nekaj bistvenih zahtev, ki jih predvideva standard ISO 27002:2022 (5.20) in jih je možno aplicirati na katerikoli postopek naročanja določenih storitev ali opreme pri zunanjih izvajalcih:

- identifikacija in dokumentiranje vrst dobaviteljev (npr. storitve IKT, logistika, komunalne storitve, finančne storitve, komponente IKT infrastrukture), ki lahko vplivajo na zaupnost, celovitost in razpoložljivost informacij organizacije;
- vzpostavitev načina za ocenjevanje in izbiro dobaviteljev glede na občutljivost informacij, izdelkov ter storitev (npr. z analizo trga, referencami strank, pregledom dokumentacije, ocenami na lokaciji, certifikati);
- ocenjevanje in izbira izdelkov ali storitev dobavitelja, ki imajo ustrezne varnostne ukrepe za varovanje informacij, ter pregled teh ukrepov; pozornost namenite zlasti natančnosti in popolnosti varnostnih ukrepov, ki jih dobavitelj izvaja za zagotavljanje celovitosti svojih informacij in procesiranja informacij ter s tem varnosti informacij organizacije;
- določitev informacij, IKT storitev in fizične infrastrukture organizacije, do katerih imajo dobavitelji lahko dostop, možnost nadzora, upravljanja ali uporabe;
- določitev vrst komponent IKT infrastrukture in storitev, ki jih zagotavljajo dobavitelji ter lahko vplivajo na zaupnost, celovitost in razpoložljivost informacij organizacije;
- ocenjevanje in upravljanje tveganj informacijske varnosti, povezanih z:
  - uporabo informacij organizacije in drugih povezanih sredstev s strani dobaviteljev, vključno s tveganji, ki lahko izhajajo iz morebitnega zlonamernega ravnanja osebja dobavitelja;
  - okvarami ali ranljivostmi izdelkov (vključno s programsko opremo in njenimi podkomponentami), ali storitvami, ki jih zagotavljajo dobavitelji;
- nadzorom skladnosti z uveljavljenimi zahtevami informacijske varnosti za posamezne vrste dobaviteljev in tipe dostopa, vključno s pregledi tretjih strani ter validacijo izdelkov;
- omiljevanjem neskladnosti dobavitelja, ne glede na to, ali je bila ta odkrita skozi nadzor ali z drugimi sredstvi;
- upravljanje z incidenti in nepredvidenimi dogodki, povezanimi z izdelki in storitvami dobaviteljev, vključno z odgovornostmi tako organizacije kot dobaviteljev;
- odpornost, in če je potrebno, ukrepi za okrevanje ter nepredvidene situacije, ki zagotavljajo razpoložljivost informacij dobavitelja in procesiranja informacij ter s tem razpoložljivost informacij organizacije;
- zavedanje in usposabljanje osebja organizacije, ki sodeluje z osebjem dobavitelja, glede ustreznih pravil sodelovanja, speci-

fičnih politik, procesov in postopkov ter vedenja, odvisno od vrste dobavitelja in ravni dostopa dobavitelja do sistemov ter informacij organizacije;

- upravljanje potrebnega prenosa informacij, drugih povezanih sredstev in vsega, kar je potrebno spremeniti, ter zagotavljanje, da se varnost informacij ohranja skozi celotno obdobje prenosa;
- zahteve za zagotavljanje varnega zaključka razmerja z dobaviteljem, vključno z:
  - odprava pravic dostopa;
  - ravnanje z informacijami;
  - določitev lastništva intelektualne lastnine, razvite med sodelovanjem;
  - prenosljivost informacij v primeru spremembe dobavitelja ali notranjega obvladovanja;
  - upravljanje z dokumentacijo;
  - vrnitev sredstev;
  - varno uničenje informacij in drugih povezanih sredstev;
  - trajne zahteve po zaupnosti;
- nivo varnosti osebja in fizične varnosti, ki se pričakuje od osebja ter objektov dobavitelja.

Pogodbe z dobavitelji bi morale biti vzpostavljene in dokumentirane, da se zagotovi jasno razumevanje med organizacijo ter dobaviteljem glede obveznosti obeh strank za izpolnjevanje ustreznih zahtev informacijske varnosti (ISO 27002:2004 – 5.21).

Naslednji pogoji se lahko upoštevajo za vključitev v pogodbe, da zadostijo ugotovljenim zahtevam informacijske varnosti:

- opis informacij, ki jih je treba zagotoviti ali dostopati, ter metode zagotavljanja ali dostopa do teh informacij;
- klasifikacija informacij v skladu s klasifikacijskim sistemom organizacije;
- usklajevanje med lastnim klasifikacijskim sistemom organizacije in klasifikacijskim sistemom dobavitelja;
- pravne, zakonske, regulativne in pogodbene zahteve, vključno z varstvom podatkov, ravnanjem z osebnimi podatki, pravicami intelektualne lastnine ter avtorskimi pravicami in opis, kako se bo zagotovilo, da so ti pogoji izpolnjeni;
- obveznost vsake pogodbene stranke, da uvede dogovorjen sklop kontrol, vključno z nadzorom dostopa, pregledom uspešnosti, spremljanjem, poročanjem in revizijo ter skladnost obveznosti dobavitelja z informacijskimi varnostnimi zahtevami organizacije;
- pravila sprejemljivega ravnanja z informacijami in drugimi povezanimi sredstvi, vključno z nepotrebnim ravnanjem, če je to treba;
- postopki ali pogoji za avtorizacijo in odstranitev avtorizacije za uporabo informacij ter drugih povezanih sredstev organizacije s strani osebja dobavitelja (npr. prek izrecnega seznama osebja dobavitelja, pooblaščenega za uporabo informacij in drugih povezanih sredstev organizacije);
- zahteve glede varnosti informacij v zvezi z IKT infrastrukturo dobavitelja; zlasti minimalne zahteve glede varnosti informacij za vsako vrsto informacij in vrsto dostopa, ki naj služijo kot osnova za posamezne pogodbe z dobavitelji, odvisno od poslovnih potreb in kriterijev tveganja organizacije;
- odškodnine in odpravljanje posledic za neizpolnitev zahtev s strani izvajalca;
- zahteve in postopki za upravljanje incidentov (zlasti obveščanje ter sodelovanje med odpravljanjem incidentov);
- zahteve za usposabljanje in zavedanje o specifičnih postopkih ter zahtevah informacijske varnosti (npr. za odzivanje na incidente, postopke avtorizacije);

- relevantne določbe za podizvajalce, vključno s kontrolami, ki jih je treba uvesti, kot so dogovor o uporabi poddobaviteljev (npr. zahteva, da so podvrženi istim obveznostim kot dobavitelj, zahteva po seznamu poddobaviteljev in obveščanje pred vsako spremembo);
- relevantni kontaktni podatki, vključno s kontaktnim osebjem za vprašanja informacijske varnosti;
- morebitne zahteve za preverjanje ozadja, kjer je to pravno dovoljeno, za osebje dobavitelja, vključno z odgovornostmi za izvajanje preverjanja in postopki obveščanja, če preverjanje ni bilo zaključeno ali če rezultati vzbudijo dvome ali skrb;
- dokazi in mehanizmi zagotavljanja tretjih strank za ustrezne zahteve informacijske varnosti, povezane s procesi dobavitelja, ter neodvisno poročilo o učinkovitosti kontrol;
- pravica do revizije procesov in kontrol dobavitelja v zvezi s pogodbo;
- obveznost dobavitelja, da periodično predloži poročilo o učinkovitosti kontrol in dogovor o pravočasnem odpravljanju ustreznih vprašanj, ki so bila navedena v poročilu;
- postopki za reševanje napak in konfliktov;
- zagotavljanje varnostnih kopij, usklajenih z potrebami organizacije (glede na frekvenco, vrsto in lokacijo shranjevanja);
- zagotavljanje dostopnosti alternativnega objekta (tj. lokacije za obnovo po katastrofi), ki ni izpostavljen enakim grožnjam kot primarni objekt, ter upoštevanje rezervnih kontrol (alternativne kontrole) v primeru neuspeha primarnih kontrol;
- vzpostavitev postopka za upravljanje sprememb, ki zagotavlja pravočasno obveščanje organizacije in možnost, da organizacija ne sprejme sprememb;
- fizične varnostne kontrole, ki so primerne glede na klasifikacijo informacij;
- kontrole prenosa informacij za zaščito informacij med fizičnim ali logičnim prenosom;
- določbe o prenehanju obveznosti ob zaključku pogodbe, vključno z upravljanjem evidenc, vrnitvijo sredstev, varnim uničevanjem informacij in drugih povezanih sredstev ter kakršnimikoli trajnimi obveznostmi glede zaupnosti;
- zagotavljanje metode za varno uničenje informacij organizacije, ki jih hrani dobavitelj, takoj, ko te informacije niso več potrebne;
- zagotavljanje podpore pri predaji drugim dobaviteljem ali sami organizaciji ob zaključku pogodbe;
- varstvo osebnih podatkov, če je to primerno;
- protikorupcijska klavzula in primeri ničnosti pogodbe.

Ukrepi se smiselno uporabljajo glede na velikost organizacij in specifike naročila storitev ter opreme. Pri izvedbi naslanjanja na zunanje izvajalce je treba najprej uporabljati pristop dobrega gospodarja, ki bo zagotovil, da boste poskrbeli za varnost ključnih informacij o vaših ključnih procesih in infrastrukturi.

Viri:

- SIST ISO/IEC 27001:2023: Informacijska varnost, kibernetska varnost in varovanje zasebnosti — Sistemi upravljanja informacijske varnosti — Zahteve (ISO/IEC 27001:2022)
- ISO 28000:2022: Security and resilience — Security management systems — Requirements
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV