KONCEPT KIBERNETSKE VARNOSTI V INDUSTRIJSKIH OKOLJIH

Avtor: Matjaž Demšar

Visoka šola za poslovne vede, Management in informatika (2. stopnja)

Povzetek

Kibernetska varnost s tehnološkim napredkom ter spremljajočo digitalizacijo prihaja v ospredje aktivnosti, povezanih z varnostjo in varovanjem informacij. V IT okoljih, torej poslovnih okoljih organizacij je pristop k varnosti urejen s pomočjo splošno veljavnih standardov in varnostnih ogrodij, ter vključuje postopke in orodja, s katerimi organizacije lahko dosežejo zahtevani nivo varnosti. V proizvodnih okoljih, znanih tudi pod kratico OT (ang. Operational technology) pa je situacija drugačna – zaradi zgodovinskih posebnosti ta okolja niso šla v razvoj varnostnih rešitev istočasno kot poslovna, poleg tega pa specifične lastnosti posameznih okolij predstavljajo precejšnjo oviro pri vpeljevanju standardiziranih rešitev. To srečevanje obeh svetov, t.j. IT in OT pojmujemo kot konvergenco IT in OT; trenutno gre za eno od najbolj aktualnih tem v industrijskih podjetjih, saj s srečevanjem različnim filozofij prihaja tako do negativnih, kot pozitivnih posledic. Na področju poznavanja IT tehnologij so praviloma informatiki v prednosti, a brez dobrega poznavanja OT tehnologij so posledice napak lahko katastrofalne. V članku je predstavljena tematika konvergence IT in OT, ter metoda, kako zagotoviti, da vsak od deležnikov v tem odnosu prispeva svoj del k zagotavljanju ustreznega nivoja kibernetske varnosti v teh okoljih.

Ključne besede: konvergenca IT in OT, kibernetska varnost v industriji, 62443

Uvod

Za proizvodna okolja oziroma okolja OT je zelo značilna visoka stopnja specifičnosti oziroma heterogenosti, ki je posledica tega, da je vanje vključeno večje število naprav, ki opravljajo specifične funkcije, prav tako pa je v implementaciji takšnih rešitev lahko vključeno večje število partnerjev, t.j. sistemskih integratorjev, ki stroje oziroma proizvodne linije izdelajo, pri tem pa vanje tudi vgradijo večje število IT naprav, kot so računalniki, omrežna oprema ter prikazovalniki, ki pa s to vgradnjo dobijo nov namen in so tako del neke večje celote. Stroji in proizvodne linije so certificirani kot končni izdelki, kar pomeni, da spreminjanje oziroma izločevanje komponent praviloma ni možno, oziroma iz vidika standardizacije oziroma homologacije pomeni ustvarjanje novega tipa stroja oziroma naprave. Vrsta in tip teh naprav se razlikuje od panoge do panoge, pogosto pa tudi znotraj posameznih panog prihaja do razlik zaradi konkurenčnih razlik med samimi ponudniki.

Zaradi konvergence IT in OT prihaja do konfliktnih idej, kako zaščititi industrijske naprave na najboljši možen način – IT ima na razpolago pester nabor rešitev, storitev ali aktivnosti, ki poskrbijo za varnost, so pa vsi ti izdelki namenjeni poslovnim okoljem, njihova implementacija

v industrijskih okoljih pa lahko pripelje do izredno hudih neželenih posledic za okolje, zdravje in družbo.

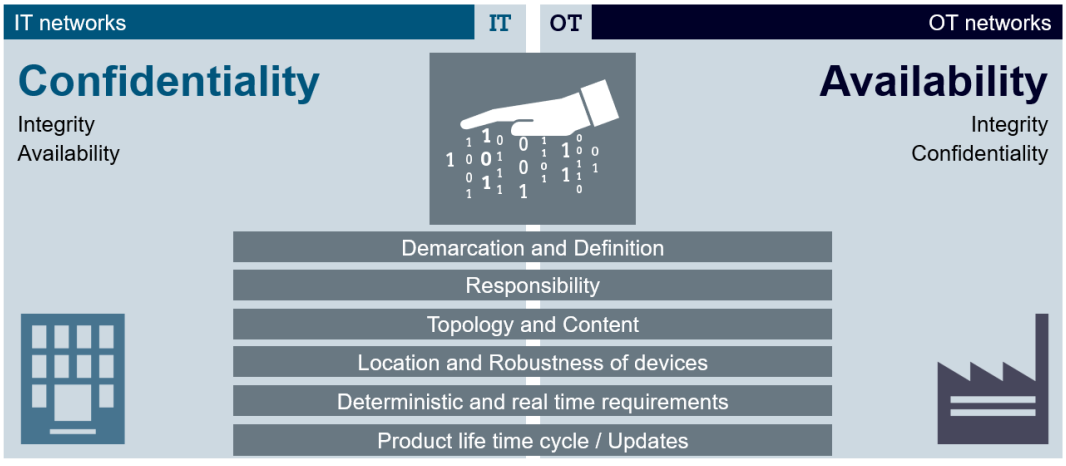
V nadaljevanju so izpostavljene najpomembnejše razlike med okolji, s katerimi se strokovnjaki za omrežja srečujejo pri delu v proizvodnih okoljih, ter koncept kibernetske varnosti za proizvodno okolje.

Koncept varovanja

Akronim »CIA« v IT konceptu varnosti pomeni prioriteto zaporedja lastnosti podatkov, ki jih z uporabo varnostnih mehanizmov varujemo. V IT okoljih tako največjo prioriteto predstavlja zaupnost, oziroma angleško »Confidentiality«. Zaupnost naših in podatkov naših strank je kritičnega pomena, saj njihovo razkritje lahko predstavlja poslovno in pravno tveganje. Sledita mu tako integriteta, oziroma angleško »Integrity«, ter razpoložljivost oziroma angleško »Availability«. Integriteta pomeni, da podatki po končanem prenosu ostanejo v enaki obliki in se njihova vsebina ni spremenila. Razpoložljivost pa je njihova dejanska razpoložljivost, kot odraz delovanja prenosnega omrežja.

V primeru OT omrežja je to zaporedje ravno obratno - zaupnost ter razpoložljivost imata obrnjeni mesti. To je rezultat tega, da je v industriji najbolj pomembno obvladovanje strojev in procesov, med tem ko je sama zaupnost veliko manj pomembna. Oblika podatkov v OT prometu je namreč odvisna od procesa in sama po sebi ne predstavlja tako velikega tveganja v primeru prestrezanja in razkritja, saj podatek sam po sebi ne nosi tako kritične vrednosti, kot v IT okoljih.

Slika 1: Koncept varovanja v IT in OT (vir: Siemens Customer Services).



Glavne razlike med IT in OT

Na Sliki 1 je prikazan osnovni koncept pristopa k varovanju. V spodnjem delu je izpostavljenih pa nekaj glavnih razlik med okoljema, ki so opisane spodaj.

Osnovna definicija

IT je skupni pojem za nabor tehnologij za obdelovanje informacij, vključno s programsko, strojno, komunikacijsko opremo ter spremljajočimi storitvami. IT na splošno ne vključuje naprav, ki ne ustvarjajo podatkov za poslovno uporabo v organizaciji. (Gartner, 2022)

OT pojem predstavlja opremo, strojno in programsko, ki zazna ali povzroči spremembo, neposredno ali skupaj s povezano industrijsko opremo, viri, procesi ali dogodki. (Gartner, 2022)

Zgornji dve definiciji prihajata iz Gartnerjevih slovarjev, ter predstavljata najkrajši možen opis tehnologij. Dodatno si lahko tehnologiji predstavljamo tako, da ena skrbi samo za prenos podatkov in povezljivost, medtem ko druga spreminja in krmili druge naprave. Zaradi digitalizacije se pa meja med njima včasih zabriše, kar bomo videli kasneje.

Odgovornost

V IT okoljih glede odgovornosti ni dosti povedati, vsaj na prvi pogled. Praviloma gre za zaščito podatkov zaposlenih in podjetja, ter delitev odgovornosti za te naloge med zaposlene v podjetju, mogoč je pa tudi prenos odgovornosti na zunanje osebe, tako preko t.i. »outsourcing« pogodb, kot preko zavarovanja, kjer je to mogoče. Osebje, ki upravlja z okoljem, ima ustrezne kompetence na IT področju.

V OT okoljih gre pa poleg zaščite podatkov tudi za varnost ljudi in strojev; ti so namreč v primeru incidenta lahko neposredna ali posredna tarča. Odgovornosti se v OT okoljih praviloma ne da prenašati na zunanje osebe, vsaj ne končne odgovornosti v primeru incidentov. Poleg tega pa so za upravljanje OT naprav, ki se nahajajo v samih tovarnah praviloma zahtevane drugačne kompetence, ki obsegajo znanja s področja strojništva oziroma elektrotehnike, v izogib nesrečam pri delu z napravami.

Topologija in vrsta podatkov

V IT okoljih se srečujemo s prometom, ki je organiziran vertikalno, na relaciji odjemalec-strežnik. Prenaša se večja količina poslovnih podatkov (dokumenti, aplikacijski podatki, zvok in video), tako da je zasedena precejšnja pasovna širina, prav tako pa je v uporabi veliko število povezav, ki so organizirane v hierarhični arhitekturi.

OT okolja imajo pogosto precej horizontalne komunikacije, neposredno med samimi napravami. Preko omrežja se prenašajo majhni paketi, tako da je pasovna širina relativno nizka. Število povezav je prav tako precej manjše, kot v IT. Podatki v prenosu so po navadi razne procesne vrednosti, podatki senzorjev, ali pa paketi industrijskih protokolov z raznimi krmilnimi vrednostmi.

Kar se tiče te razlike, so podatki v IT po navadi precej bolj zanimivi za prestrezanje, saj gre za berljive informacije, medtem ko OT podatki predstavljajo vrednosti, ki brez potrebnega konteksta in znanja niso enostavno berljivi.

Lokacija opreme in robustnost

V IT okoljih je oprema nameščena oziroma hranjena v nadzorovanem in stabilnem okolju. Temperaturno območje je po navadi stabilno in v razponu, ki je primerno za vsakodnevno bivanje in zadrževanje oseb. Take razmere so zelo ugodne za opremo, ki tako ni pod posebnim stresom. OT oprema pa mora biti nameščena v bližini samih strojev, kar pomeni, da se pogosto nahaja v okoljih, ki zahtevajo najmanj ustrezno IP (an. Ingress Protection) zaščito, po navadi pa se soočajo še s korozivnimi okoljem, visokimi ali izredno nizkimi temperaturami ter vrsto drugih fizikalnih ali kemičnih dejavnikov, ki lahko vplivajo na zanesljivost delovanja.

Determinizem

Determinizem pomeni sposobnost, da napovemo prihodnje dogodke oziroma se ti zgodijo v znanem trenutku. Sicer je pojem malce široko razložen, pomeni pa, kar se OT okolja tiče, da lahko predvidimo, kdaj bi nek paket prispel do svojega cilja. Ta lastnost je pomembna predvsem v scenarijih krmiljenja naprav, ki delujejo po principih zaprte zanke – signali potujejo po napravi in skrbijo za usklajenost posameznih delov. Determinizem se doseže z uporabo posebnih industrijskih komunikacijskih protokolov, ki delujejo na 2. in 3. nivoju OSI modela, potrebujejo pa tudi posebno opremo. Medtem ko v IT omrežjih VoIP komunikacija, ki predstavlja eno najbolj kritičnih glede odzivnosti omrežja, potrebuje čase ciklov v okolici 10 ms, se v IRT (Izohroni realno časovni) komunikaciji dela s cikli, ki so lahko v okolici 32 µs (32000 ciklov na sekundo). Vsakršne motnje ali prekinitve v tej komunikaciji imajo lahko za posledico precejšnjo škodo ali poškodbe. Ta vrsta komunikacija se uporablja po navadi v scenarijih, kjer se krmili večje sinhronizirane motorje; primer je recimo papirniška industrija, ali pa jeklarstvo – valjarne različnih vrst pločevine, ter za določene vrste robotov.

Življenjski cikel opreme

V IT okoljih se oprema obravnava kot zaključena končna točka (ang. Endpoint) ali del infrastrukture in procesi se odvijajo tako, da se strojna in programska oprema redno osvežuje, oziroma nadgrajuje. Življenjska doba je pogosto vezana tudi na amortizacijsko dobo, po izteku katere pogosto nova oprema predstavlja cenejšo možnost. Zaradi takšnega pristopa je precej poenostavljeno tudi vzdrževanje opreme, hkrati s tem pa je tudi okolje veliko bolj homogeno.

V OT po drugi strani pa je okolje precej bolj razgibano. Kot omenjeno že v uvodu, so IT komponente tu vgrajene v večje celote, stroje oziroma proizvodne linije. Te naprave pa imajo precej daljšo življenjsko dobo, praviloma daljšo od 15 let, v določenih industrijah pa tja do 40 let. Gre za izredno drage naprave, ki se amortizirajo daljše obdobje, pogosto pa zaradi njihove velikosti menjava ni finančno upravičena. Zaradi tega se lahko pripeti, da so v OT okolju prisotne zelo heterogene naprave, različnih proizvajalcev, ter različnih starosti. Programska oprema v teh primerih je pogosto preveč zastarela, da bi bilo posodabljanje še smiselno, tako da so potrebni drugačni varnostni ukrepi

Standardi, ki urejajo varnost

Za celovito upravljanje okolij v IT se uporablja vrsta standardov, ki imajo tudi različne vloge in so na različne načine vpeti v organizacije. Vključeni so lahko predpisovalno ali pa informativno – to v praksi pomeni, da se organizacija po nekem standardu lahko certificira pri zunanji organizaciji, ali pa postopke samo vpelje, ter procese upravlja skladno s priporočili. Tu noben pristop nima bistvene prednosti pred drugim in vsaka organizacija lahko ubere pot. Pri tem je seveda odvisna tudi od morebitnih predpisov, ki so vezani na panogo v kateri deluje in upoštevanje določenih standardov predpisujejo.

IT in OT se v principu pristopa, z uporabo standardov in predpisov ne razlikujeta, prav tako ne v postopkih ocene tveganja, ki se uporabijo za ocene tveganja in priprave uravnoteženih protiukrepov za obvladovanje le-teh. Razlike so najbolj vidne pri standardih, ki so osnova za pripravo, uvedbo, vodenje in izboljševanje sistema upravljanja informacijske varnosti. V IT je tako glavna osnova družina standardov ISO/IEC 27000, na kateri temelji precejšnji del prakse. V OT je varnost v največji meri urejena z uporabo IEC 62443, oziroma posameznih poglavij, ki so pripoznani kot veljavni mednarodni standardi, urejajo pa predvsem vzpostavitev sistema kibernetske varnosti za sisteme industrijske avtomatizacije, ter varnostne nivoje opreme oziroma ukrepov. Dve poglavji standarda IEC 62443 se pa ukvarjata z razvojem strojne in programske opreme za industrijska okolja in omogočata proizvajalcem, da skladnost svojih izdelkov in procesov certificirajo. Tudi ISO/IEC 27000 družina ima standard; ISO/IEC 27019, ki definira razlike med IT in OT okolji, ter ponuja načine za preverjanje ustreznosti ukrepov za del industrijskih okolij, natančneje oskrbo z električno energijo, ne ponuja pa načina za vzpostavitev sistema kibernetske varnosti. (ISO/IEC 27019:2017, 2022)

Razmišljanje o ločnici med IT in OT nas lahko hitro napelje k sklepu, da sta ISO/IEC 27001 in IEC 62443 namenjena vsak svojemu okolju. V nekaterih delih to sicer drži, praksa pa kaže, da je znanje v organizacijah, ki imajo vpeljan ISO/IEC 27001 veliko lažje prenesti v vpeljevanje IEC 62443. (ISA, 2021)

Varnostni koncept za OT okolja

Globinska obramba

Obramba je močna toliko, kot je močen njen najšibkejši člen. To je pravilo, ki velja v vrsti različnih scenarijev, ne samo vojaških, od koder pojem izvira. Za boljše razumevanje si lahko obrambo predstavljamo kot utrdbo iz srednjega veka. V primeru, da smo zavarovani samo z enim zidom, napadalci ne potrebujejo veliko, da ga na enem mestu predrejo in pride do nas. V kolikor pa je naša utrdba sestavljena iz več elementov, mora pa napadalec najprej preplavati jarek z vodo (v katerem lahko tudi ždijo dodatne nevarnosti), nato pa se mora šele spopasti z zidom, pri čemer je omejen z orodjem, ki ga lahko prinese s seboj. Ko predre ta zid, ga čaka še manjši notranji zid, z ozkimi prehodi, na koncu pa še vrsta utrjenih stavb, od katerih vsaka predstavlja utrjeno točko. Verjetno ni potrebno dodatno razlagati, kateri od gradov je težje osvojljiv. Podoben pristop ubira tudi varovanje industrijskih okolij s pomočjo globinske obrambe – sestavljen je iz slojev

varnostnih ukrepov, ki se pričnejo takoj ob prihodu na območje objekta, se nadaljujejo v posameznih stavbah in skrbijo za varnost pristopa na območje, kot tudi gibanja med posameznimi deli objektov. Danes to srečamo v praktično vsaki organizaciji, ki ima organiziran program varnosti. V primeru kibernetske varnosti so to dopolnilni ukrepi, ki zagotavljajo varnost fizičnih pristopov. Varnost namreč ne pomaga dosti, v kolikor napadalec pridobi fizičen dostop do samih naprav.

Slika 2: Koncept globinske obrambe.

Drugi sloj globinske varnosti je omrežna varnost. Tu se nahajajo ukrepi, vezani na zaščite samih dostopov do sistemov preko omrežja. Ukrepi se nanašajo predvsem na topologijo omrežij, kjer je pogosta uporaba segmentacije omrežij na celice, ki so definirane tako, da omogočajo čim višjo stopnjo varnosti in zmožnost nadaljevanja oziroma obvladovanja procesa ali njegovih delov kljub incidentom. Zaradi zagotavljanja tega je v sklopu ukrepov potrebna tudi fizična segmentacija omrežja, glede na ocenjene stopnje tveganja, opisane kasneje. Dodatni ukrepi so prav tako uporaba industrijskih požarnih pregrad, ter različnih implementacij VPN dostopov, prilagojenih za industrijska okolja.

Tretji nivo predstavlja integriteto sistemov. To so sistemi, ki predstavljajo jedro OT okolja, na njih pa tečejo aplikacije, ki upravljajo s stroji oziroma proizvodnim procesom. Ukrepi, s katerimi se tu najpogosteje zagotavlja varnost so pa:

- Utrjevanje sistemov
- Upravljanje posodobitev
- Zaznava vdorov oziroma anomalij
- Avtentikacija in kontrola dostopa do sistemov
- Zaščita znanja

Ukrepi so precej podobni tistim v IT, ob tem da je potrebno upoštevati posebnosti posameznega okolja. Spodaj so opisane posebnosti, ki vplivajo na uvajanje ukrepov.

Utrjevanje sistemov

Utrjevanje sistemov pomaga zmanjšati površino napada, oziroma potencialno tveganje, tako da se izključi nepotrebne storitve, zapre omrežna vrata, ki niso v uporabi, ter odstrani nepotrebne programe. Sisteme se lahko utrdi z namestitvijo t.i. »whitelisting« programov, ki pomagajo pri varovanju zastarelih operacijskih sistemov (poskrbijo, da operacijski sistem zažene samo programe, ki so na dovoljenem seznamu – od tu ime »whitelisting«), na OT specifični opremi se uveljavijo priporočene varnostne nastavitve, nastavijo gesla. To so nekateri od najpogosteje uporabljenih ukrepov, podrobnejše informacije pa se najdejo na straneh, namenjenih varnosti, kot so npr. Center for Internet Security (Center for Internet Security, 2022), ali pa National Institute for Standards and Technology (NIST, 2022).

Upravljanje posodobitev

Posodobitve so kritičen element kibernetske varnosti, je pa njihovo nameščanje pogosto pogojevano s tem, da se zmanjša neželen vpliv na IT okolje. Občasno se lahko zgodi, da popravek povzroči tudi neželene napake, tako da je tudi pri nameščanju popravkov potrebno implementirati ukrepe za zmanjševanje tveganja, kot so testno nameščanje, preverjanje popravkov v laboratorijskem okolju, ter priprava postopkov za povrnitev prejšnjega stanja, v primeru, da se pojavijo težave po namestitvi. (Abrams, 2022)

V OT okolju večina ukrepov, navedenih zgoraj ni izvedljivih, zaradi posebnosti okolja; testni scenariji niso možni, ker ni moč zagotoviti kopij strojev, ki bi služile samo za testiranje. Prav tako v določenih situacijah izpadov delovanja ni možno tolerirati, ker predstavljajo prevelik strošek ali preveliko tveganje. To posebnost je potrebno upoštevati pri pripravi načrta posodabljanja. Obstajajo posebne storitve, ki jih zagotavljajo večji ponudniki in sicer preverjanje kombinacij programske opreme in različic popravkov, ki delujejo skupaj. Na podlagi teh testov se potem izdajajo matrike kompatibilnosti oziroma informacije, ki uporabnikom pomagajo upravljati s popravki v OT okolju.

Zaznava vdorov oziroma anomalij

V IT se poleg tradicionalnih protivirusnih programov vedno bolj uveljavljajo rešitve za zaznavo in preprečevanje vdorov, v zadnjem času pa se nadgrajujejo tudi z rešitvami, ki s pomočjo umetne inteligence zaznavajo tako globalne trende, kot trende v omrežjih. Podobne rešitve se uveljavljajo tudi v OT okoljih, vendar je tu potrebna previdnost pri implementaciji, saj ti sistemi ne smejo vplivati na delovanje sistemov. Predvsem je tu pomembno, da rešitev ne posega v delovanje sistemov, tako preko samodejnih ukrepov, ki jih lahko rešitve za preprečevanje vdorov (IPS) izvajajo, ter preko lažno pozitivnih označitev delov programov za nadzor kot neželene aktivnosti. Tveganje se pojavi predvsem pri programih za upravljanje procesov, PCS/DCS (ang. Process Control System, ali Distributed Control System) ter sistemih za nadzor in pridobivanje

podatkov, SCADA (an. Supervisory Control And Data Acquisition), ki delujejo na specifične načine in med delovanjem lahko izkazujejo vedenje, ki pri nekaterih protivirusnih programih ali sistemih za zaznavo vdorov povzroči nepredvidljivo reakcijo.

V OT okolju se tako lahko uporablja preverjeno programsko opremo, ki je testirana za združljivost, pri namestitvi se pa upošteva posebnosti posameznega sistema.

Avtentikacija in kontrola dostopa do sistemov

Avtentikacija je področje, kjer pogosto prihaja do največjih nerazumevanj med IT in OT strokovnjaki. V OT okolju namreč zaradi kritičnosti dostopa do nadzora procesov postopki avtentikacije potekajo drugače, predvsem zaradi tega, ker je potrebno zmanjšati tveganje za proces. Politike gesel, ki so v IT eden najbolj osnovnih ukrepov za zagotavljanje varnosti, v OT lahko povzročijo katastrofo, če dostop do upravljanja procesa ni mogoč takrat, ko je to potrebno. Zaradi tega se v OT lahko uporabi drugačne mehanizme avtentikacije, ki ne ovirajo kritičnega dostopa do naprave, hkrati pa omogočajo podrobno sledenje dostopov.

Zaščita znanja

Programska koda, ki upravlja s proizvodnimi procesi, praviloma vsebuje znanje, ki je zaščiteno z avtorskimi pravicami, oziroma predstavlja intelektualno lastnino. Dostop do te kode, ter njen ogled je potrebno nadzorovati, ob tem, da se ta nahaja na samih napravah, ne v centralni lokaciji. Obstajajo sicer rešitve za varnostno kopiranje in hrambo ter nadzor različic, a koda mora biti na napravi, kjer proces teče. Tam pa je lahko izpostavljena nepooblaščenim osebam, v kolikor niso implementirani zadostni zaščitni ukrepi. Ti vključujejo mehanizme, ki so po navadi sicer odvisni od proizvajalca do proizvajalca, vključujejo pa lahko razširjene mehanizme, kot je npr. kriptografija.

Načrtovanje ukrepov

Načrtovanje ukrepov, povezanih z zaščito industrijskega okolja temelji na uporabi priporočil in standardov, ki se nanašajo na posamezno okolje. V odsotnosti konkretnih napotkov, ki so sicer na voljo za specifične panoge, kot so recimo kritična infrastruktura, jedrske elektrarne, farmacevtska industrija ipd. je najboljša začetna točka uporaba standarda ISO/IEC 62443. Ta vsebuje najboljše smernice za pripravo sistema upravljanja s kibernetsko varnostjo v industrijskih okoljih. Stopnja potrebne zaščite sistemov temelji na oceni tveganja, ki se izdela za posamezen del proizvodnje, temelji pa na kombinaciji grožnje, ter možnosti, da pride do njenega udejanja. Glede na to oceno se potem izdela načrt ukrepov za zaščito, ki mora doseči ustrezno varnostno stopnjo. (IEC, 2013) Te so štiri, z oznakami od SL-1 do SL-4, pomenijo pa naslednje:

Tabela 15: Stopnje varnosti po ISO/IEC 62443.

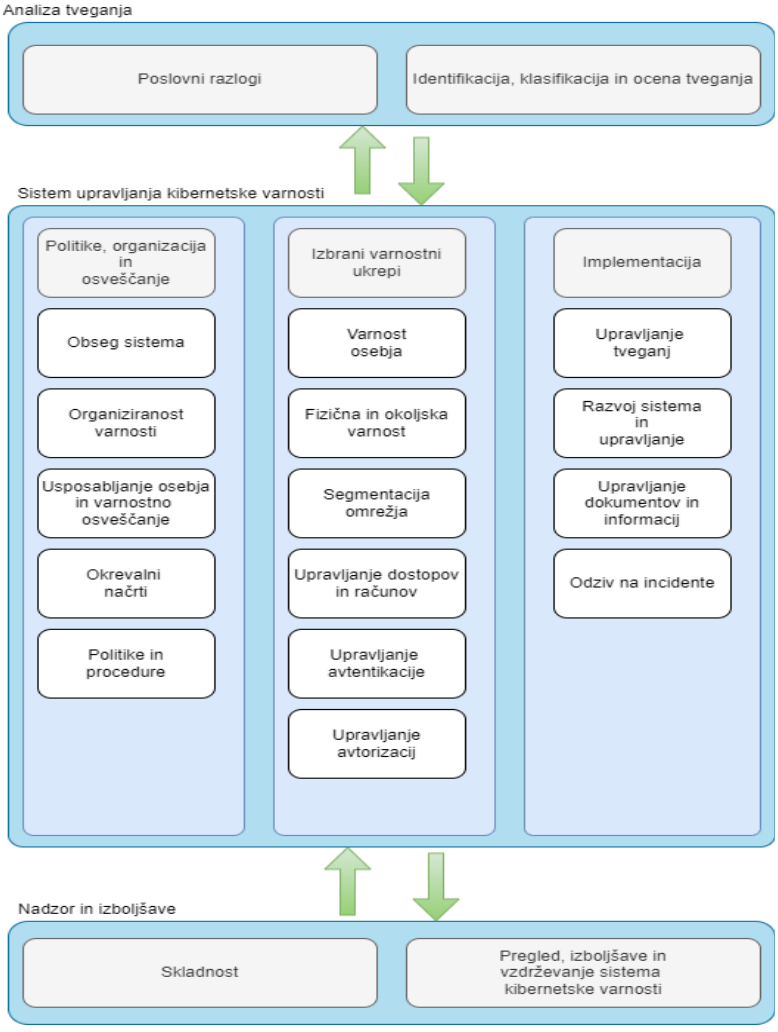
SL-0	Zaščita ni potrebna. Ta stopnja se ne upošteva pri navajanju
SL-1	Zaščita pred nehotenimi incidenti in nesrečami

SL-2	Zaščita pred osnovnim napadom, z nizko motivacijo napadalca, nizkim nivojem znanja in malo razpoložljivimi sredstvi
SL-3	Zaščita pred naprednim napadom, povprečno motiviranim napadalcem, s specifičnim ICS/SCADA znanjem in srednjo količino sredstev
SL-4	Zaščita pred naprednim napadom, visoko motiviranim napadalcem s specifičnim ICS/SCADA znanjem in veliko količino sredstev

Stopnje zaščite same po sebi še niso dovolj za uspešno zaščito. Pri vzpostavitvi sistema upravljanja kibernetske varnosti se uporabijo napotki , vsebovani v ISO/IEC 62443-2-1, ki predpisujejo način vzpostavitve in upravljanja s kibernetsko varnostjo za sisteme v avtomatizaciji (IACS) (IEC, 2010)

Na spodnji sliki so prikazani gradniki sistema za upravljanje s kibernetsko varnostjo.

Slika 46: Diagram sistema upravljanja kibernetske varnosti.



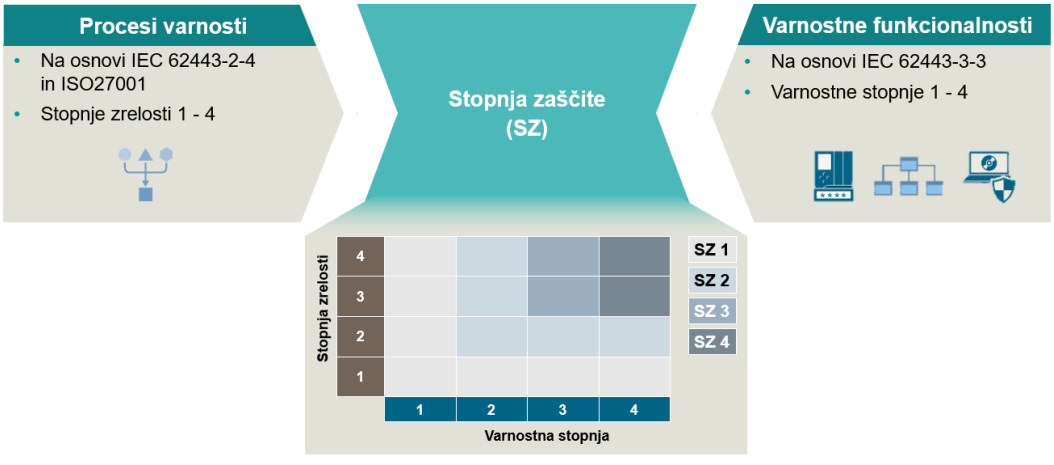
Življenjski cikel kibernetske varnosti se prične še predno je oprema na lokaciji stranke. Trendi groženj, ki se pojavljajo v zadnjih letih, govorijo v prid t.i konceptom »zero trust« oziroma »chain of trust«. Ti se nanašajo na celovito upravljanje varnosti, ki presega meje okolja, kjer bo uporabljen nek izdelek - pokriva tako tudi razvoj in izdelavo. Standard ISO/IEC 62443 vsebuje nekaj poglavij, ki se nanašajo na to in s svojimi smernicami urejajo način, kako zadostiti tem potrebam, ter zagotoviti ustrezno sledljivost. Prvo je poglavje 2-4 ISO/IEC 62443. To je namenjeno upravljanju zrelosti procesov na strani dobavitelja, zrelost pa deli v štiri stopnje. (IEC 62443-2-4, 2017)

Tabela 16: Stopnje zrelosti procesov dobaviteljev, po standardu ISO/IEC 62443-2-4.

Stopnja zrelosti 1	Začetna: Dobavitelji razvoj izvajajo ad-hoc in pogosto ne dokumentirajo rešitev ali pa jih pomanjkljivo.
Stopnja zrelosti 2	Upravljana: Dobavitelj upravlja razvoj skladno z zapisanimi smernicami. Osebje prikaže ustrezno znanje in usposabljanje. Proces je ponovljiv.
Stopnja zrelosti 3	Definirano: Proces je ponovljiv v celotni dobaviteljski organizaciji. Procesi so dokazljivo upravljani.
Stopnja zrelosti 4	Izboljševanje: Dobavitelji uporabljajo metrike procesa za nadzor učinkovitosti in dokazujejo nenehne izboljšave.

S pomočjo ocene stopnje zrelosti lahko določimo skupno oceno stopnje zaščite, ki je rezultat tako varnostne stopnje, kot stopnje zrelosti, prikazana je pa na Slika 47.

Slika 47: Prikaz stopnje zaščite.



Poleg zgoraj omenjenih standardov je potrebno za razumevanje kibernetske varnosti v industrijskih okoljih poznati tudi dva standarda, ki usmerjata razvoj programske in strojne opreme. Prvi je IEC 62443-4-1, ki ureja področje varnostnih vidikov razvoja in življenjski cikel. Z njegovo pomočjo se lahko ureja varnost pri razvoju programske opreme, strojne programske kode ter vseh ostalih izdelkov, kjer se uporablja proces, katerega rezultat je v obliki programske

opreme. Napadi, ki smo jim priča v zadnjih letih kažejo, da je pri varnosti potreben celovit pristop – najbolj predani napadalci lahko programsko kodo napadejo še, ko je v fazi razvoja in si tako zagotovijo stranski vhod v sisteme, ki so sicer postavljeni v skladu z vsemi varnostnimi predpisi, a je razvoj potekal brez nadzora skozi celoten življenjski cikel. Prav tako podoben vektor vdora je skozi posodobitve programske opreme na račun zaupanja do dobavitelja. Namen standarda IEC 62443-4-1 je tako zagotoviti ureditev procese razvoja, ki upoštevajo varnostne smernice skozi celoten potek aktivnosti in tako zmanjšajo tveganja na račun napak pri razvoju. (IEC, 2018)

Drugi standard, ki pa ureja področje strojne opreme, je pa IEC 62443-4-2. Namen tega standarda je vzpostavitev tehničnih zahtev, ki jim mora oprema zadostiti, da ustreza zahtevam posameznega sistema za upravljanje kibernetske varnosti. Zahteve standarda se tesno vežejo na stopnje varnosti, ki jih predpisuje standard IEC 62443-3-3. (IEC, 2013) (IEC, 2019)

Zaključek

V nalogi je bil predstavljen koncept kibernetske varnosti za industrijska okolja. Ta se v najbolj kritičnih točkah razlikujejo od IT, ob tem, da je pa zaradi digitalizacije in prehoda v Industrijo 4.0 veliko opreme, tako strojne kot programske prenesene v ta okolja. Žal pa zaradi tega prenosa pogosto prihaja do nejasnosti glede odgovornosti, ter pristopa k sami varnosti, kar lahko prinaša težave tako IT kot OT osebju, na koncu pa celotni organizaciji. Dodaten vidik tveganja na tem področju so tudi sami ponudniki opreme, ki pogosto s svojim pristopom poskušajo reševati težave, katerim so namenjeni organizacijski ukrepi, na ta način pa se lahko določena tveganja narobe razumejo, posledično pa obvladujejo na nepravilne načine.

Razvoj standardov, tako v IT, kot tudi v OT okolju, prinaša napredek glede tega, kako znanja in kompetence čim bolje aplicirati na reševanje konkretnih izzivov, s katerimi se srečujejo proizvodna podjetja, vzpostavljanje njihove širše prepoznavnosti pa naloga, vseh, ki se z njimi srečujejo v praksi.

Viri in literatura

Abrams, L. (13. 1 2022). Microsoft pulls new Windows Server updates due to critical bugs. Pridobljeno iz Bleeping Computer: https://www.bleepingcomputer.com/news/microsoft/microsoft-pulls-new-windows-server-updates-due-to-critical-bugs/

Center for Internet Security. (23. 1 2022). Center for Internet Security. Pridobljeno iz Center for Internet Security: https://www.cisecurity.org/

IEC. (2010). IEC 62443-2-1: Security for Industrial Automation and Control Systems, Part 2-1: Establishing an Industrial Automation and Control Systems Security Program. IEC.

IEC. (2013). IEC 62443-3-3: Security for Industrial Automation and Control Systems, Part 3-3: System security requirements and security levels. IEC.

IEC. (2018). IEC 62443-4-1: Security for Industrial Automation and Control Systems, Part 4-1:Secure product development lifecycle requirements. IEC.

IEC. (2019). IEC 62443-4-2: Security for Industrial Automation and Control Systems, Part 4-2: Technical security requirements for IACS components. IEC.

IEC 62443-2-4. (8 2017). Security for industrial autoamtion and control systems - Part 2-4: Security program requirements for IACS service providers.

ISA. (20. 7 2021). White Paper: Applyiing ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments. Pridobljeno 18. 8 2021 iz https://www.isa.org/news-press-releases/2021/july/new-white-paper-applying-iso-iec-27001-2-and-the-i

ISO/IEC 27019:2017. (6. 8 2022). Pridobljeno iz ISO: https://www.iso.org/standard/68091.html

NIST. (23. 1 2022). Industrial Control Systems Cybersecurity. Pridobljeno iz National Institute for Standards and Technology: https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity