ORGANIZACIJSKI VIDIKI VAROVANJA INFORMACIJSKIH SISTEMOV (I)

Tomaž Poštuvan

Povzetek

Prispevek o organizacijskih vidikih varovanja informacijskih sistemov obravnava področje, ki je tudi pri nas vedno bolj pomembno. Vsaka organizacija ima premoženje, ki je lahko običajen denar ali pa so to naslovi strank oz. informacije o dogajanjih na trgu in borzi. Če so kakšni od teh podatkov nenadoma nedostopni ali ukradeni, lahko to povzroči neprijetnosti, izgubo denarja ali pa celo bankrot. Zato je podatke potrebno varovati.

Abstract

The paper discusses an area, which is of outmost importance to all the organizations. Every organization possesses assets that include money, customer adresses and marketing informations. If some or all of those assets are either unavailable for use or stolen, the organization might suffer inconvenience, loss of money or maybe even go out of business. Therefore, data must be secure.

■ ■ ■

UVOD

Vseprisotnost računalniških informacijskih sistemov v današnji družbi močno izpostavlja vprašanje njihove varnosti oziroma zaščite pred malomarnostjo ali nepooblaščenimi uporabniki. Omenjeni sistemi imajo veliko materialno in drugačno vrednost, zaradi česar obstaja tudi temu primerno tveganje izgub zaradi malomarnosti ali protizakonitih dejanj. Prav zaradi pomembnosti vprašanja je varovanje in zaščita podatkov danes posebna stroka, ki se na sistematičen način ukvarja s področjem vsestranske zaščite informacijskih sistemov. Takoj naj pojasnimo, da pod pojmom informacijski sistem mislimo na računalniški informacijski sistem oziroma informacijski sistem, katerega bistveni sestavni del je računalniška tehnologija.

Velja poudariti, da je varovanje podatkov pomembno tudi iz splošno civilizacijskih razlogov in ne le zaradi materialne vrednosti, ki jo imajo informacijski sistemi oziroma shranjeni podatki. Danes je zasebnost uveljavljena civilizacijska vrednota, ki je v večini držav na ustrezen način tudi ustavno in zakonsko varovana. Zaradi tega je primerno varovanje podatkov, ki se nanašajo na posameznike, obveznost vseh lastnikov in uporabnikov informacijskih sistemov. Seveda pa je obveza varovanja materialne vrednosti informacijskih sistemov in podatkov del običajnega delokroga vodstva organizacije, ki je lastnik takega sistema.

Varovanje podatkov oziroma njihova varnost ima več vidikov, od katerih tu omenjamo dva: tehnični in organizacijski. Tehnična stran obsega vse tehnične probleme zagotavljanja varnosti in načine njihovega reševanja, organizacijska pa zbirko metod, načel, napotkov in podobno, ki zagotavlja, da se varovanje podatkov kot ena od nalog podjetja ali organizacije izvaja zanesljivo in učinkovito. V tem sestavku se ukvarjamo predvsem z drugo, organizacijsko stranjo zaščite podatkov, čeprav bomo nekaj prostora namenili tudi tehničnim vprašanjem.

1. Problem varnosti informacijskih sistemov

Problem z varnostjo informacijskih sistemov je zelo enostaven - to je problem ljudi. Rešitev problema je prav tako zelo enostavna - ljudje naj kontrolirajo ostale ljudi v računalniškem okolju. Misel "Računalniki ne kradejo, ljudje pa" stoji na trdni osnovi. Eden od ljudi, ki se ukvarjajo z varnostjo v enem večjih računalniških podjetij v ZDA je rekel, da še nikoli v svojih tridesetletnih izkušnjah nadzorovanja in preiskovanja računalniških goljufij ni naletel na primer, ko za prevaro niso bili odgovorni določeni ljudje [3, stran 3]. Program varnosti podatkov mora večino naporov usmerjati v nadzorovanje ljudi, če želi biti uspešen.

Eden od kriterijev pomembnosti varnosti informacijskega sistema je tudi narava posla, s katerim se organizacija ukvarja. Zadnje čase, ko se organizacije vključujejo v informacijske tokove, se zavedajo nujnosti zaščite informacij. V nekaterih organizacijah sicer še vedno mislijo, da je programska oprema strošek, ne pa premoženje organizacije, vendar so na srečo taka v manjšini. Zapisani ali ne, podatki (in z njimi programska oprema) so glavno premoženje organizacije.

Svet varnosti informacijskih sistemov je velik in še raste. Varnost organizaciji sicer ne bo prinesla denarja v klasičnem smislu, vendar bo povečala posredni dobiček zaradi zmanjšanja stroškov in preprečevanja odtekanja informacij.

1.1 Kako razmišljati o varnem sistemu ?

Odgovornost za varnost podatkov na vsak način nosi vodstvo organizacije in sicer za varovanje premoženja, izdelavo sistemov za notranjo kontrolo, ki varujejo premoženje ter za ugotavljanje, če premoženje sploh še obstaja. Bolj pomembni kot so podatki, večja je potreba po izpolnitvi te vrste odgovornosti.

Nekdo se bo vprašal : "Kaj vodstvo organizacije dela, da bi izpolnilo svojo odgovornost do varnosti?". Tudi vodstvo se mora vprašati, kaj dela za varnost sistema, preden začne kritizirati program varnosti kot neučinkovit.

Poglejmo nekaj vprašanj, ki se nanašajo na varnost in lahko vodstvo organizacije spravijo v zadrego :

- **Ali vodstvo aktivno sodeluje v programu varnosti?** Aktivna udeležba pomeni veliko vloženega časa, določanje strategije, povpraševanje ostalih delavcev o njihovem vložku ... Samo podpora in odobravanje nista dovolj.
- **Ali je vodstvo spoznalo njegove glavne šibke točke?** Če se šibke točke ne odkrijejo, to avtomatično pomeni, da se strategija varnosti ne more primerno sestaviti.
- **Če so šibke točke znane, ali poznamo njihov relativni pomen?** Velikost sredstev, ki bodo namenjena določeni šibki točki, je odvisna od možnosti, da pride do incidenta ravno pri njej. Sistem je tako varen, kot je varen njegov najšibkejši člen.
- **Ali uporabljene rešitve delujejo?** Vodstvo ima za nalogo tudi ocenitev učinkovitosti programa, sicer se lahko denarna sredstva, ki so za varnost zelo velika, trošijo nenamensko.

Začetek kateregakoli programa za varnost je ocena trenutnega stanja. Dokler ne vemo, kje smo, ne bomo nikoli vedeli, kam moramo iti. Obstajata dve poti za ugotovitev, kako varen je informacijski sistem. Prvi pristop je natančna, v globino usmerjena ocena, ki opozori na konkretne grožnje in na primerne protiukrepe za zmanjšanje teh groženj. Ta pristop zahteva strokovno usposobljeno ekipo, ki natančno pozna informacijski sistem v organizaciji. Drugi pristop je bolj površen - pokazati na tista področja, kjer nevarnost obstaja in za varnost ni dovolj dobro poskrbljeno.

Prvi pristop je ekvivalenten natančnemu pregledu kardiovaskularnega sistema z EKG, stresnimi testi, merjenjem količine holesterola itd., medtem ko drugi pristop ustreza ogledu karakteristik, ki vodijo k problemom s srcem - diete, visokega pritiska, kajenja itd. Obe metodi sta napovedovalca srčnih težav, nobena ni popolnoma zanesljiva, vendar je prva bolj natančna in je verjetnost pravilne napovedi večja.

Vodstvo organizacije nosi osnovno odgovornost za varnost sistema, da pa bo informacijski sistem tudi resnično varen, mora pomagati sleherni zaposleni. Moramo razlikovati med odgovornostjo vodstva za program varnosti in odgovornostjo delavcev za posamezne aktivnosti v okviru programa.

2. Kako velik je problem varnosti ?

Vsak program varnosti se mora začeti z ugotovitvijo trenutnega stanja v organizaciji. Le-to nam predstavlja neke vrste začetno točko za njegovo izboljšanje.

2.1 Trenutno stanje v organizaciji

Trenutno stanje v organizaciji je natančen pregled programa varnosti informacijskega sistema v določenem trenutku. Namenjeno je odgovoru na dve vprašanji : (1) Kaj delamo za varnost podatkov ? (2) Kako učinkovit je naš program varnosti ?

Pregled stanja organizacije naj bi napravili neodvisni ljudje, saj bi s tem odpadli vsi predsodki, ki se lahko pojavljajo v organizaciji, če bi pregled delali notranji sodelavci.

Obstajata dve kategoriji informacij, ki jih je treba zbrati: prva je vezana na sam proces varnosti in vključuje strategije, metode, procedure in tehnike, ki jih potrebujemo za varovanje računalniških sredstev. Druga kategorija pa vključuje varnostne dokumente - informacije o poskusih vdora oz. samih vdorih v sistem. Če je mogoče, naj bi bile izgube tudi ocenjene.

Kakšna je potreba po pregledu stanja organizacije? Delavci, ki delajo v organizaciji daljše obdobje, s časom dobijo določene izkušnje in jih je zelo težko prepričati, da so možna tudi druga dejstva, ki so bolj pravilna. Neki strokovnjak za varnost je dejal, da v skoraj vseh organizacijah velja ti. **dvajsetletno pravilo**, ki pravi, da če se neki neprijeten dogodek ni zgodil v zadnjih dvajsetih letih, potem je verjetnost, da se tudi v bodoče ne bo zgodil, enaka ena [3, stran 22]. To pa seveda ni nujno. Edina rešitev, ki vodstvo prepriča v nasprotno, je prikaz dejstev. V svetu varnosti je tak pristop nujen.

2.2 Ključni koraki zbiranja informacij o stanju organizacije

Zbiranje informacij o stanju podatkov ni nujno časovno potratna stvar. Cilj je zbrati tisto, kar lahko zberemo razmeroma enostavno. Trije ključni vidiki so :

- Kaj zbirati
- Od koga bomo dobili informacijo
- Točnost zbranih informacij

Zbiranje informacij o stanju v organizaciji mora biti

končano v enem tednu (razen v velikih organizacijah, kjer se lahko zbiranje malce zavleče). Postopek je sestavljen iz naslednjih šestih točk: :

1. Določitev skupine za zbiranje
2. Določitev zahtev in ciljev zbiranja
3. Načrt zbiranja informacij
4. Učenje članov skupine
5. Zbiranje informacij
6. Analiza in poročilo o stanju v organizaciji

Določitev skupine za zbiranje

Za člane skupine morajo biti izbrani tisti delavci, ki se zavedajo problema varnosti in bodo lahko rezultate uporabili za njeno izboljšanje. Vodstvo organizacije mora poudariti važnost in cilje zbiranja informacij, da tudi ostali začnejo na varnost gledati z drugačnimi očmi.

Idealna ekipa je sestavljena iz treh do sedmih ljudi, število članov pa naj bo zaradi morebitnega preglasovanja liho.

Določitev zahtev in ciljev zbiranja

Na prvem sestanku skupine se morajo določiti zahteve in cilji zbiranja. Dve vrsti ciljev sta posebej pomembni: (1) zbrati informacije o trenutnih ukrepih za varnost in (2) zbrati informacije o učinkovitosti odkrivanja in preprečevanja varnostnih incidentov. Zahteve morajo odgovoriti na vprašanja Zakaj, Kaj, Kdo, Kdaj, Kje in Kako lahko pride do napadov na informacijski sistem.

Načrt zbiranja informacij

Pri postavitvi varnostnega sistema je potrebno poskrbeti za to, da se informacije o njegovi kvaliteti zbirajo med njegovim rednim delovanjem in da niso potrebni naknadni in dodatni ukrepi za analizo njegovega delovanja. Če pa se zgodi, da povratni mehanizmi še ne delujejo, se gleda na eni strani dejansko stanje (kdo je odgovoren, kateri viri so varovani, katere metode se uporabljajo), po drugi strani pa tudi, kakšno je stališče zaposlenih. Če se nevarnosti incidenta zavedajo, potem je verjetnost, da bo do njega prišlo, manjša.

Učenje članov skupine

Skupina, ki bo zbirala informacije, in tudi ljudje, ki bodo informacije nudili, bi morali biti seznanjeni s tem, kaj se od njih pričakuje. Najmanj, kar morajo vedeti, je, da se zbiranje sploh opravlja, kako zbrati potrebne informacije in jih ločiti od nepotrebnih ter kakšna točnost zbiranja je potrebna.

Zbiranje informacij

Zbiranje mora biti končano v najkrajšem možnem času, pomeni, v nekaj delovnih dneh. Odgovornost, da je zbiranje v tem času dejansko končano, pade na člane skupine.

Analiza in poročilo o stanju v organizaciji

Rezultat analize stanja v organizaciji mora biti pregled, kateri elementi varnosti v organizaciji pomenijo največjo potencialno nevarnost. Najboljše analize so tiste, ki potrdijo mnenja članov skupine, ki so jih dobili ob samem zbiranju. Rezultati, ki nasprotujejo mnenju naročnika študije, bodo zelo težko dobili zeleno luč. Zato je bolje, da so usmerjeni k nadgradnji obstoječega sistema kot njegovi zamenjavi.

Ko smo informacije zbrali, imamo podlago za izboljšanje programa - trenutno stanje lahko služi kot primerjava. Študija služi dvema namenoma: (1) Program za varnost usmerja od besed k dejanjem. Čeprav nekatera dejstva temeljijo na odnosu ljudi, so statistična podlaga za nadaljnje študije. (2) Meri učinkovitost sprememb. Če se koristnost sprememb ne da izmeriti, nikoli ne vemo, ali je bila sprememba dovolj učinkovita.

2.3 Ovrednotenje stroškov varovanja informacijskih sistemov

Ocenjene izgube, povezane z varnostjo podatkov in informacijskih sistemov v celoti, so zelo velike (v ZDA so ocenjene na več kot 40 milijard USD letno (povzeto po [1])). Glavna komponenta cene varnosti je cena nadzornih ukrepov in v zvezi s tem se pojavljata dve vprašanji : (1) Ali bi bilo ceneje, če bi izgubili del podatkov kot pa plačali za nadzor in (2) Ali so stroški, ki nastajajo zaradi varnosti, upravičeni - ali se varnost izboljšuje ali ne ?

Strošek varnosti v organizaciji je ponavadi neznan. En del gre v projekte, en del v skupno učenje delavcev, nekaj za sprotno delo ... Vsebuje pa tri specifične komponente: (1) preventivne stroške, (2) stroške odkrivanja incidentov in (3) stroške izgub. Vsota vseh treh komponent je skupen strošek organizacije.

Preventivni stroški

Preventivni stroški so stroški, zaradi katerih se incident sploh ne zgodi. Vsebujejo postavitev odgovorne osebe za varnost, šolanje zaposlenih, preverjanje varnosti, razvoj varnih programov, shranjevanje računalniških medijev in nabavo sistema za varnost podatkov. Cilj te vrste stroškov je oteževanje možnega incidenta.

Stroški odkrivanja incidentov

Ti stroški so namenjeni odkritju incidenta (ko se je ta že zgodil) preden lahko pride do kakšne večje škode. Ukrepi vključujejo postavljanje gesel, preverjanje, če je zahtevana akcija dovoljena, opremo za nadzor, kontrolo dostopov in nenazadnje tudi fizično kontrolo. Kljub incidentu so varnostni ukrepi še vedno dokaj učinkoviti, saj denimo brez gesla vdiralec ne more priti nikamor. Ponavadi so preventivni stroški in stroški odkrivanja incidentov povezani med seboj.

Na primer, mnogi terminali so nastavljeni tako, da

se po nekaj napačnih vnosih gesla zaklenejo in nadaljnji dostop do sistema nekaj časa ni več možen.

Stroški izgub

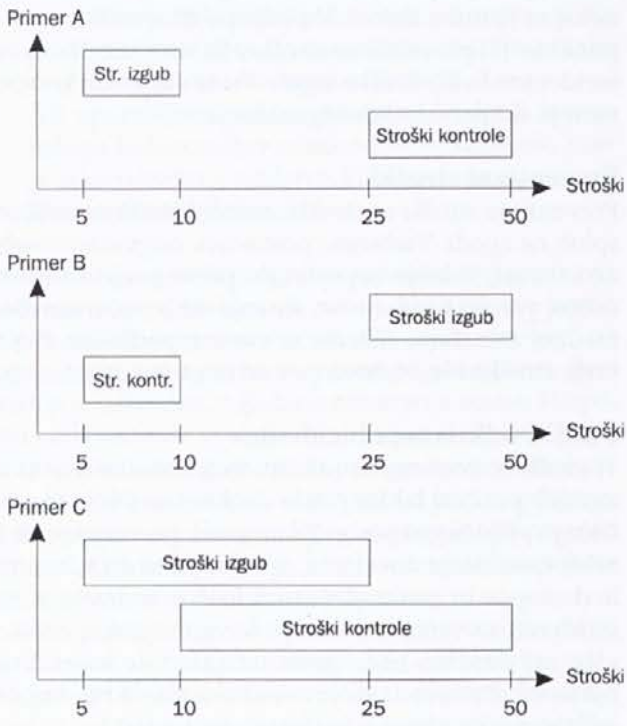
Izgube podatkov so posledica nepravilnih oz. nezadostnih preventivnih ukrepov in ukrepov odkrivanja. Izgube so dveh vrst : fizične izgube (npr. izguba traku, CD-ROMa) in programske izgube (izguba podatkov, manipulacija s transakcijami).

2.4 Izračun stroškov varnosti

Koncept stroškov varnosti ponavadi zajema čim cenejše ukrepe, ki bi preprečili čimveč možnih različic vdorov v sistem, se pravi zmanjšanje verjetnosti vdora na določeni točki.

Eden takih zelo enostavnih in učinkovitih ukrepov je na primer zmanjšanje števila zaposlenih, ki imajo dostop ali pa celo zmanjšanje vstopnih točk v sistem. Ko je koncept določen, ostane končna odločitev na vodstvu, ki zanjo tudi odgovarja.

Stroški varnosti vsebujejo stroške izgub in stroške nadzora. Odločitev o nakupu sistema varnosti postane zelo lahka, ko so stroški enkrat znani. Večina organizacij napravi bilanco enkrat letno, zato se enkrat letno tudi odloča o velikosti proračuna. Takrat je idealen trenutek za določitev stroškov varnosti informacijskega sistema. Stroške protiukrepov lahko izračunamo precej enostavneje kot pa stroške morebitnih groženj. Izziv osebju je torej čim točnejša ocena stroškov morebitnih varnostnih incidentov. Na sliki 1 so trije primeri, ki ponazarjajo razmerje med izgubami zaradi vdorov in stroški za protiukrepe.



Slika 1. **Stroški izgub proti stroškom kontrole**

Primer A kaže, da so stroški izgub precej manjši, kot pa bi znašali stroški kontrole aktivnosti. V tem primeru, tudi če smo se pri oceni izgub zmotili za 50 %, bomo še vedno raje utrpeli izgubo, ker so stroški kontrole previsoki. Primer B je nasprotje primera A. Tudi v tem primeru pa velja, da če smo se lahko zmotili za 50 %, je odločitev še vedno nedvoumna. Zadnji primer odgovorne sili v zadrego, saj se stroški izgub in kontrole med seboj prekrivajo. Če so stroški izgub previsoko in stroški kontrole prenizko ocenjeni, potem bi bila kontrola ekonomsko upravičena, v obratnem primeru pa ne.

Ti trije primeri kažejo, da se morajo stroški izračunati v dveh korakih. V prvem koraku naj bo izračun bolj površen (dovolj dober za primera A in B), če pa pride do primera C, naj se v drugem koraku natančnost poveča. Edini pogoj za izračun na tem nivoju pa je, da je natančnost pri obeh izračunih enaka, ne da se stroški kontrole izračunajo do zadnjega tolarja, stroški izgub pa ostanejo v milijonih.

2.4 Stroški izgub in protiukrepi

Tehnologijo izračuna potencialnih izgub zaradi varnosti že stoletja uporabljajo zavarovalnice. Spremenljivki računa sta frekvenca pojavljanja izgube in enkratna izguba (izguba ob enem vdoru). Rezultat bo pričakovana letna izguba in se izračuna kot :

Pričakovana letna izguba =
= frekvenca pojavljanja x enkratna izguba

Kako si s to formulo lahko pomagamo? Denimo, da smo banka, ki posluje s kreditnimi karticami. Ena od možnih izgub je nesolventnost stranke - stranka kartico uporabi za nakup, vendar nima pokritja. Izgube lahko nastanejo tudi zaradi ponarejenih ali ukradenih kartic. Izračuna se po zgornji formuli, za vrednosti spremenljivk pa se uporabijo podatki o prejšnjih, recimo ukradenih karticah. Povprečna izguba pri teh karticah je bila 10.000 SIT in če predvidevamo, da se bo to zgodilo 5000-krat letno, je pričakovana letna izguba 50 milijonov SIT.

Izračun pričakovane letne izgube je orodje, s katerim si lahko pomagamo pri oceni stroškov za varnost in ekonomičnost nakupa. Po drugi strani pa je zelo težko pravilno oceniti izgube, ki nastanejo zaradi kraje računalniških programov in podatkov. Vrednost programa se ponavadi grobo izračuna kot 30$ - 50$ na programsko vrstico izvorne kode, vrednost podatkov pa bodisi kot strošek za nadomestitev ukradenih podatkov (npr.ponovno vnašanje imen in priimkov strank) bodisi kot vrednost izgube posla, če je škoda na podatkih nepopravljiva. V drugem primeru je vrednost izgubljenih podatkov seveda precej višja.

Za zmanjšanje frekvence pojavljanja izgube obstajata dve metodi : (1) zmanjšanje priložnosti izgube z omejevanjem dostopa do podatkov ljudem, ki jih ne potrebujejo in (2) zmanjšanje verjetnosti izgube, denimo s preverjanjem vnosa ključev - s tem se verjetnost izgube zmanjša na kakovost programa za preverjanje ključa. Tudi enkratna izguba se lahko zmanjša in to bodisi z zavarovanjem, ki izgubo v celoti pokrije, bodisi z decentralizacijo, na primer razdelitvijo računalniškega centra na dve enoti, tako da katastrofa v eni enoti ne vpliva na delo v drugi.

Stroški preventivnih in kurativnih protiukrepov morajo biti v sorazmerju s stroški izgub. To so stroški za njihov razvoj ter sami operativni stroški. Prvi so enkratni (zato jih je tudi lažje izračunati), medtem ko je treba na druge računati vsakič sproti in so odvisni tudi od števila poskusov vdora.

V tem poglavju sem opisal proces ocene izgub v primerjavi z verjetnostjo vdora v sistem in posledic kontrole aktivnosti, ki izgube zmanjšujejo. Proces se lahko ponavlja toliko časa, da se dobi optimalna mešanica in so kontrole najučinkovitejše. Podrobneje je postopek ugotavljanja velikosti problema varnosti opisan v [3].

3. Kako napraviti sistem varen?

Program za varnost informacijskega sistema naj bo, če je le mogoče, zaključen del širšega sistema, ki varuje celotno organizacijo. Nima namreč smisla zapravljati velike vsote denarja za zaščito enega dela, če je na drugi strani organizacije do informacij možno priti brez posebnega napora, ker v nekem oddelku zaščite sploh nimajo. Mnogo vodilnih oseb trpi za ti. "bankirskim sindromom". Ko bankir odpre novo banko, zgradi v kleti trezor, zaščiten z debelim jeklenim zidom, vhod vanj je možen samo na en način, pa še za to je treba poznati več kombinacij varnostnih kod. Ta trezor pa pomeni le 0.5 % celotnega premoženja, 99.5 % pa je v računalniku, do katerega je možen dostop prek terminalov. Kriminalci ta sindrom poznajo in si rečejo: "Zakaj bi tvegal življenje za drobiž iz trezorja, če lahko to precej lažje naredim s pritiskom na nekaj tipk".

Varovanje organizacije se mora vedno začeti na vrhu, nato pa se polagoma spuščati do posameznih enot. Varovanje računalniških virov sicer jamči za več kot povprečno zaščito, vendar naj bi to vseeno ne bil edini vir, vreden pozornosti.

3.1 Strategija vodenja in ključni faktorji uspeha

Prvi korak k programu varnosti je izjava vodstva o nameri in potrebi. Nato je dobro, če vprašamo o njihovih vidikih tudi zaposlene, kajti program ne bo dosti pomagal, če zaposleni sprejemajo varnost kot nebodigatreba in vsakič ko pride do posla, ki ga je treba napraviti hitro, pozabijo na varnost. Šele takrat, ko so morebitni spori z zaposlenimi rešeni, pride trenutek za izdelavo strategije.

Strategija seveda ne more biti enaka za vse organizacije; razlikuje se glede na dejavnost, s katero se organizacija ukvarja, želje vodstva in nenazadnje tudi na zakone, ki se nanašajo na varnost. Predlagana strategija varnosti ne sme ščititi samo računalniških virov, ampak celotno organizacijo (varnostni ukrepi v trezorju so še vedno nujni).

Kriteriji, s pomočjo katerih vodstvo lahko oceni pravilnost strategije, se imenujejo ključni faktorji uspeha (Critical Success Factors). Ključni faktorji uspeha za program računalniške varnosti organizacije se morajo osredotočiti na naslednja štiri področja:

- Uporabnost sistema glede na velikost in porazdeljenost sistema viri vključujejo strojno in programsko opremo, podatke in dokumentacijo, komunikacije, okolje in vzdrževanje. Izguba podatkov napravi sistem v celoti neuporaben, medtem ko pri izgubi komunikacij sistem še vedno deluje, le oddaljeni računalniki ostanejo mrtvi.
- Celovitost sistema. Izraz "celovitost sistema" se najpogosteje uporablja za podatke, na katerih sistem deluje. Zmanjšanje celovitosti ima lahko različne posledice, od napačne akcije zaradi nepravilnih podatkov pa celo do zaustavitve delovanja.
- Zaupanje v sistem. Izguba zaupanja je najresnejša posledica nezanesljivega sistema. Do tega pride zaradi naključne ali namerne prekinitve delovanja ali zaradi nepooblaščenega dostopa. Te vrste izgub so ponavadi obravnavane prioritetno, saj rešitev tega problema večkrat reši tudi kakšnega od ostalih.

Ključni faktorji uspeha za računalniško varnost morajo imeti štiri osnovne značilnosti. Prvič, uresničevati morajo resnični namen vodstva organizacije. Če vodstvo v faktorje ne verjame, potem ne bo niti podprlo namestitve programa niti ga ne bo zanimalo, če je bil dosežen kakšen uspeh. Drugič, biti morajo dokumentirani, sicer podrejeni ne bodo imeli od njih nobene koristi pri namestitvi. Tretjič, biti morajo merljivi. Če pomena faktorjev ne moremo izmeriti, potem so neuporabni. In četrtič, kriteriji morajo biti dosegljivi. Na primer, faktor, ki pravi, da nikakor ne sme priti do vdora v sistem, je nedosegljiv.

Naloga vodstva, ko so ključni faktorji uspeha podani, je, da jih preuči in napravi plan, ki je ponavadi sestavljen iz petih točk :

1. **Postavitev odgovorne osebe za varnost.** Namen postavitve odgovorne osebe je v tem, da postane odgovoren za varnost posameznik. Veliko organizacij je poskušalo s skupino ljudi, pa se ni obneslo. Naloge odgovorne osebe so : definiranje ključnih

faktorjev uspeha, zagotovitev, da ima vsak oddelek nekoga, ki je odgovoren za varnost, analiza in predlog aktivnosti ter potrebnega denarja za naslednje leto in zagotovitev usposabljanja novih zaposlenih.

2. **Izbira skupine, ki se bo ukvarjala z varnostjo.** Ker je računalniška obdelava podatkov prisotna v celotni organizaciji, bi bilo nerealno pričakovati od ene same osebe, da lahko primerno planira, nameša in nadzoruje potrebe po varnosti na vseh področjih organizacije. Zato se ponavadi določi skupina uporabnikov (liho število), ki skrbijo za celotno organizacijo.
3. **Določitev kriterijev za oceno programa varnosti.** Kriteriji za ocenjevanje so nujni zato, da se lahko preveri, če je informacijski sistem tako varen, kot je potrebno. Kvaliteta programa je odgovornost tistih, ki so program namestili.
4. **Zagotovitev denarja za podporo prvih treh aktivnosti.** Mnogi programi za varnost trpijo pomanjkanje sredstev. Vodstvo ponavadi sicer stoji za programom, pri denarju pa se vse skupaj ustavi. V varnosti pa velja : "Dobiš tisto, kar plačaš." Računalniška varnost mora opravičiti svoj obstoj, ko se to enkrat zgodi, pa se morajo zanjo najti tudi denarna sredstva.
5. **Osebna angažiranost v programu.** Vodstvo organizacije mora ne samo verjeti v program varnosti, ampak biti vanj tudi osebno vključeno. Če vodilna oseba pride na sestanek o varnosti, prikazuje rezultate delničarjem itd, potem vsi vedo, da je varnost za organizacijo pomembna in se navadno tako tudi obnašajo. Čas je za vodilno osebo najpomembnejši vir in mora biti smotrno porabljen, toda ena ura mesečno je nekakšen minimum, ki lahko zaposlene prepriča, da je varnost pomembna.

3.2 Ustvarjanje motiviranosti med delavci.

Nelogično in neupravičeno bi bilo pričakovati, da bodo zaposleni avtomatično pomagali pri vzpostavitvi sistema varnosti, takoj ko se bo vodstvo za to odločilo. Motiviranost pa se s skrbno načrtovanim planom lahko ustvari in s tem doseže namen.

Ustvarjanje motiviranosti vsebuje **princip spremembe vedenja**, pomeni, da bo učenec sposoben napraviti neko novo dejanje.

Ljudje imajo do varnosti različne poglede. Nekateri so skrbni in želijo varovati premoženje delodajalcev, medtem ko drugi mislijo češ, saj so bogati in ne bodo pogrešali nekaj ukradenega premoženja. Znanstveniki so se ukvarjali s spremembo vedenja precej časa, da so prišli do ugotovitve, da velja naslednja formula [3, stran 92]:

Sprememba vedenja =
= sprememba posameznika + sprememba okolja

Formula kaže, da je vedenje posameznika odvisno od njegovega odnosa in od vpliva okolja, v katerem se nahaja.

Ustvarjanje motiviranosti je sprememba vedenja. Dosežemo jo lahko tako, da spremenimo posameznika, okolje ali celo oboje. Psihologi trdijo, da je precej lažje spremeniti okolje kot posameznika. Temu pravijo "mafijski sindrom ", kjer človeka okolje (množica drugih ljudi, ki delajo isto) naravnost sili k temu, da napravi kriminalno dejanje. Torej bomo najprej poskušali spremeniti okolje tako, da bo naklonjeno varnosti (povabilo delavca na tečaj, kosilo z direktorjem - naj se delavec počuti pomembnega), nato pa še posameznika.

Naštel bom pet principov sprememb vedenja, ki lahko ustvarijo motiviranost ljudi za varnost in jih obravnavajo kot aktivne subjekte :

1. **Delegiranje odgovornosti navzdol.** Delegiranje odgovornosti navzdol ima dva cilja - obogatitev dela podrejenih, da se čutijo pomembnejše in več prostega časa vodstva, ki se lahko posveti drugim stvarem. Metode, ki se jih moramo držati pri delegiranju odgovornosti, so določitev nalog (vse naloge morajo biti neodvisne, da jih lahko opravi en sam človek), vedeti je treba, katera znanja so potrebna za izvršitev naloge (naloga ne sme biti dana človeku glede na položaj v organizaciji) ter kateri človek še ima dovolj znanja za izpolnjevanje nalog varnosti.
2. **Odgovornost posameznika za varnost.** Lastništvo varnosti je ena ključnih lastnosti spremembe vedenja posameznika. Taka odgovornost pomeni, da bodo zaposleni imeli važno vlogo pri določanju, kakšne vrste varnost je potrebna in seveda tudi pri sami namestitvi. Vodstvo se bo sicer še vedno odločilo, kaj je potrebno, zaposleni pa bodo predlagali, kako se bo to tudi dejansko uporabljalo. Ponavadi se sestavijo skupine nekaj ljudi, ki skupaj najdejo rešitev določenega problema in jo predstavijo vodstvu. Le-to si mora vzeti vsaj eno uro tedensko na člana take skupine, sicer pa je odgovornost v celoti na strani skupine.
3. **Osebna podpora rezultatov dela.** Ena od težav pri varnosti je, da se nikoli ne ve, ali je bilo kaj narejenega. Recimo, nekdo, ki veliko časa vloži v izboljšave varnosti, je kritiziran, ker porabi preveč procesorskega časa, ne dobi pa nobene podpore svojemu delu s strani vodstva. Za spremembo vedenja pa je zelo pomembno, da posameznik sam ve, da dela nekaj koristnega - v to pa ga mora prepričati nadrejeni s spodbujanjem in svojo podporo rezultatom.
4. **Sistem nagrajevanja.** Ljudje naj bodo nagrajeni, če delajo tisto, kar vodstvo želi. Če je večja varnost v interesu organizacije, potem naj bodo ljudje, ki se z njo ukvarjajo in dosegajo rezultate, primerno nagrajeni. Nagrade niso nujno denarne, saj je dovolj

nagrad, ki delavcu pokažejo, da je naredil nekaj koristnega za organizacijo, npr. pohvala pred ostalimi delavci, nagradno udeleževanje seminarjev, napredovanje v službi ...

5. **Osebni nadzor vodstva.** Prevečkrat so naloge dane delavcem na način, ki pomeni bodisi, da bodo "splavali" (napravili nalogo) ali pa "utonili". Na žalost pa to ni pravi način, ki bi povečeval motiviranost, saj je stalno prisoten strah, kaj pa če naloge ne bom naredil. Zaposlenega je treba najprej naučiti, kaj naloga sploh zahteva in se prepričati, da ima dovolj znanja za njeno rešitev. Tudi potem je treba vsaj na toliko in toliko časa pogledati, kako mu gre od rok in mu morebiti pomagati. Za to je ponavadi odgovoren vodja varnosti.

(se nadaljuje)

Literatura :

[1] *M.A.L. Farr : Security for Computer Systems, Hotspur Press, 1974*

[2] *Jan Hruska : Computer Security Solutions, Blackwell Scientific Publications, 1990*

[3] *William E. Perry : Management Strategies for Computer Security, Butterworth Publishers, 1985*

[4] *D.W. Davies : Security for Computer Networks, John Wiley & Sons, 1984*

[5] *Paul J. Fortier : Handbook of LAN Technology, McGraw-Hill, 1992*

[6] *Mario Korva : Šifriranje - kriptoalgoritmi, CIFRA d.o.o., 1994*

[7] *Roger M. Needham : Denial of service , Communications of the ACM, November 1994*

◆

Tomaž Poštuvan je diplomiral leta 1993, trenutno pa je zaposlen kot mladi raziskovalec na Fakulteti za računalništvo in informatiko. Njegovo delovno področje so prevajalniki (v tem okviru tudi pripravlja magistrsko delo), sicer pa se je precej ukvarjal tudi z varnostjo oz. zaupnostjo podatkov v računalniških sistemih.

◆

Vabilo avtorjem

Uredniški odbor revije Uporabna informatika načrtuje razširitev obsega revije oziroma večjo pogostost izhajanja. Rezultati ankete med bralci revije so pokazali, da si želijo med drugim prispevke z naslednjih področij: ocena orodij in različnih rešitev, predstavitve primerov iz prakse, predstavitev rešenih informacijskih problemov, pregled stanja na nekaterih področjih v Sloveniji.

S tem vabilom se posebej obračamo na informatike v praksi, da s članki v naši reviji predstavijo svoje ugotovitve in izkušnje.

Navodila za prispevke objavljamo na zadnji strani revije. Prispevke bomo začenši z letošnjim letnikom tudi honorirali.