



# Varnost IT ni samoumevna

Najšibkejši člen v varnostni verigi je vedno človek, ki je vselej prva tarča napada

**Brez padala si je težko zamišljati varen skok iz letala, prav tako kot si je težko zamišljati varen avtomobil brez zavor. Podobno težko je v sodobnem času pričakovati varno poslovanje brez vzpostavljenega sistema vodenja varovanja informacij. Za ustrezno varnost poslovanja in varovanje ključnih informacij danes namreč ni dovolj zgolj nakup nekaj »črnih škatel« in njihov priklop na elektriko.**

Sodobno podjetje za učinkovito poslovanje potrebuje celovite, neokrnjene in razpoložljive informacije. Strateško obvladovanje informacijskih tveganj je zato ključnega pomena za njegov obstoj in nemoteno delovanje. Le tako lahko podjetje doseže neprekinjeno poslovanje, zmanjša poslovna tveganja, zniža stroške, povezano z informacijsko varnostjo, obvaruje dobro ime na konkurenčno neizprosni trgu ter si zagotovi skladnost z veljavno področno zakonodajo in vsemi zahtevami nadzornih ustanov.

## Pravilen pristop = tehnologija + znanje

Poleg naprednih tehnoloških rešitev, ki ščitijo informacijsko premoženje, morajo podjetja oziroma zaposleni v njih osvojiti še ustrezna znanja, kako varnostne tehnologije uporabljati. Le takrat bodo slednje tudi dejansko ščitile intelektualno lastnino podjetja. »Uporaba sodobnih varnostnih rešitev sama po sebi še ni dovolj. Podjetje mora sprejeti in izvajati politike varovanja informacij, skrbeti za izobraževanje zaposlenih o nevarnostih ter uveljavljati dobre prakse pri konfiguracijah naprav. Vloga implementatorja rešitev je zato še kako pomembna,« razlaga Matej

Saksida, vodja področja informacijske zaščite v podjetju S & T Slovenija.

Vpeljava standardov in načel dobrih praks na področju varovanja informacij izboljšuje delovanje organizacije in omogoča racionalizacijo notranjih procesov ter tehnologije. Vse naštetu pripomore k boljšemu varovanju informacijskih sredstev, zagotavlja neprekinjeno poslovanje in povečuje učinkovitost celotnega poslovanja. Ob tem strokovnjaki podjetja opominjajo tudi, da naj bo raven varnosti ustrežna oziroma prenosorazmerna s pomenom tistega, kar varujemo, sicer lahko varovanje ovira poslovanje ali je samo sebi namen. Varnost je konec koncev kompromis in posledično je vložek vanjo odvisen od vrednosti informacij in podatkov, ki jih je treba varovati.

## Ljudje so pot do informacij

Najšibkejši člen v varnostni verigi je vedno človek uporabnik. On je tisti, ki ima dostop do podatkov in informacij, zato je tudi prva tarča napada. Zelo pogoste so zlorabe identitet, ki napadalcem omogočajo protipravno pridobitev ključnih podatkov. »Ozaveščanje in izobraževanje zaposlenih sta ključnega pomena in dejstvo je, da prinašata rezultate, bližnjic tu preprosto ni. Podjetje mora seveda poskrbeti za ustrezno varnostno tehnologijo, nadzor nad informacijami ter njihovo upravljanje. Sestavni del varovanja informacij so tako, poleg nepogrešljive varnostne tehnologije, še notranji varnostni akti ter procedure, pravila varne rabe interneta ... Eden izmed pristopov k varovanju informacij se glasi tudi 'Prepovej vse, kar ni dovoljeno', vendar mora za tako rešitev izvajalec, ki je odgovoren za implemen-

tacijo varnostnih rešitev in sistemov, zelo dobro poznati delovanje podjetja ter uporabnikov, da ne bi s tem onemogočal dela in oviral pravzaprav osnovne dejavnosti podjetja. Temeljita analiza stanja je nujna za postavitev dobrih temeljev, učinkovite varnostne pristope opisuje Miro Faganel, vodja oddelka varnost in komunikacije v S & T Slovenija.

Praksa s področja varovanja informacij ne navdaja z optimizmom. Tako ima povprečno podjetje, ki izgubi vse podatke, le šest odstotkov možnosti, da informacijsko nesrečo preživi. Še bolj zgovoren je podatek, da informacijsko nesrečo v kar 87 odstotkih primerov povzročijo privilegirani uporabniki (menedžerji, direktorji, vodje oddelkov) sami ali pa njihovo identiteto zlorabi zunanji ali notranji napadalec. Nedolžne ovčice niso niti preostali zaposleni. V raziskavi nizozemskega varnostnega podjetja je kar 59 odstotkov zaposlenih priznalo, da bi ob odpustitvi z delovnega mesta s seboj odneslo podatke zaupne narave. Izmed njih bi jih kar 67 odstotkov te podatke uporabilo za pridobitev nove službe v konkurenčnem podjetju.

## Statistika ne laže

Ne le mehki pristopi napadalcev, tudi »grobi« digitalni napadi na podjetja se še vedno dogajajo. Za boljši vpogled v stanje vdorov v informacijske sisteme podjetij in krajo podatkov si velja ogledati letna poročila družbe Verizon, ki v navezi s tajno službo ZDA obdeluje podatke o varnostnih zlorabah na območju ZDA. V poročilu 2010 Data Breach Investigations Report, ki analizira številne zbrane podatke o napadih, napadalcih in žrtvah, je mogoče zaslediti, da se število

notranjih napadov znatno povečuje. Hkrati so notranji napadalci tudi precej uspešnejši od zunanjih, saj navadno zelo dobro vedo, katere podatke iščejo, kje jih bodo našli, kako so ti varovani in kako jih bodo odtujili.

Močno povečan obseg kraj podatkov, ki jih zakrivijo zaposleni, ima za posledico tudi povečan delež zlorab uporabniških privilegijev, zato varnostni strokovnjaki podjetjem svetujejo vpeljava bolj strogih in omejujočih varnostnih politik ter nadzora nad njihovim izvajanjem. »Orodja za zaščito končnih točk so zgledno učinkovita – administrator ve, kaj uporabnik dela, in lahko prepreči neavtorizirano odtujevanje podatkov. Dober informacijski sistem bo za vsako digitalno informacijo imel ustrezno revizijsko sled in omogočal sledljivost. Zelo pomembna je tudi delitev vlog na izvajalce in nadzornike ter uporabnike. V slovenskih podjetjih se te funkcije združujejo, kar z vidika varnosti seveda ni najprimernejše. Dejstvo je, da je v domačih podjetjih le malo ljudi, ki bi bili nosilci varnostnih znanj. Tu podjetjem lahko pomaga zunanji izvajalec,« dodaja Faganel.

## Napadalci so uspešni

Napadalci so v zadnjih letih izredno uspešni pri napadih s pomočjo socialnega

inženiringa, s katerimi žrtev prepričajo, da jim bodisi sama pošlje/izroči podatke bodisi da jim posreduje dostop do njih. Uspešnost teh napadov spodbuja njihovo širjenje, v tem letu lahko pričakujemo podvojitve njihovega obsega.

Čeprav obseg hekerskih napadov nasploh upada, pa so ti še vedno zelo »učinkoviti«, saj so neposredni hekerski napadi in napadi s pomočjo izvajanja škodljivi-

vih kod uspešni v kar 95 odstotkih primerov. V recesiji narašča tudi kriminalna aktivnost, zato podjetja v ZDA opažajo tudi več fizičnih napadov (vlomov), katerih posledice so tudi kraje računalniške opreme in podatkov na vanjo vgrajenih nosilcih podatkov.

### Kraja je prevečkrat mala malica

Še vedno pa recepti napadalcev ostajajo zelo podobni, saj je večina podatkov odtujena z različnih strežnikov in aplikacij. Žal je ustreznih »varovalk« v podjetjih premalo, saj poročilo družbe Verizon razkriva, da kar 85 odstotkov napadov od napadalcev ni zahtevalo večjih podvigov in obsežnih znanj, ob tem pa bi bilo mogoče skoraj vse napade iz te kategorije preprečiti z vpeljavo dobrih varnostnih politik, ki bi jih zaposleni tudi upoštevali. Neredko se podjetja sploh ne zavedajo, da so bila napadena in so jim bili odtujeni podatki, temveč za zlorabo izvedo šele, ko jih

na to opozori drugo podjetje ali organizacija. Napadalci so večinoma finančno motivirani, na kar kažejo tudi pogoste kraje podatkov o plačilnih karticah (če jih podjetje zaradi narave svoje dejavnosti hrani) oziroma podatkov, s pomočjo katerih je mogoče sorazmerno enostavno in hitro pridobiti finančno korist.

### Igra mačke in miši

Varnost IT v podjetjih ni slaba, prav dobra pa tudi ne. K sreči pa napadalci v tej »igri« vseeno niso toliko pred podjetji, da bi bil ves trud za

izboljšanje informacijske varnosti zaman. Namreč, več kot informatiki in zaposleni vedo o nevarnostih, ki preživijo nanje in njihove podatke, bolj pozorni bodo na različne anomalije, napake in druge nepravilnosti, posledično pa jih bo tudi težje pretentati in iz njih izvabiti razkritje poslovnih informacij tretjim osebam.



► Politika varovanja informacij je izhodiščni segment celostnega varovanja podatkov. Analizi dejanske ravni varnosti v organizaciji sledi proučitev potencialnih varnostnih tveganj ter določitev potreb po varovanju. Opredeljena notranja politika varovanja nato služi kot krovna strategija in vodilo pri izvajanju vseh varnostnih procedur.

Stran / Page: 23

Doseg / Reach: 47000

Država / Country: SLOVENIA

Površina prispevka / Size: 824 cm2

3 / 3



► »Uporaba sodobnih varnostnih rešitev sama po sebi še ni dovolj. Podjetje mora sprejeti in izvajati politike varovanja informacij,« pravi **Matej Saksida**, vodja področja informacijske zaščite v podjetju S & T Slovenija.



► »Dober informacijski sistem bo za vsako digitalno informacijo imel ustrezno revizijsko sled in omogočal sledljivost,« pravi **Miro Faganel**, vodja oddelka varnost in komunikacije v S & T Slovenija.

**s&t**  
Consulting. Integration. Outsourcing.

#### KDO SE SKRIVA ZA VARNOSTNIMI VDORI?

Vrsta napada/vdora	Pogostost v letu 2009 (v %)	Sprememba glede na leto 2008 (v %)
Napadi od zunaj	70	-9
Napadi od znotraj	48	0,26
Za vdor je kriv poslovni partner	11	-23
V napadu/vdoru je udeleženih več strani	27	-19

Vir: Verizon 2010 Data Breach Investigations Report, oktober 2010.

#### KAKO PRIDE DO VARNOSTNIH VDOROV?

Vrsta napada/vdora	Pogostost v letu 2009 (v %)	Sprememba glede na leto 2008 (v %)
Zloraba uporabniških privilegijev	48	26
Napadi hakerjev	40	-24
Uporaba škodljivih kod	38	0
Uporaba tehnik socialnega inženiringa	28	16
Fizični napad na podjetje	15	6

Vir: Verizon 2010 Data Breach Investigations Report, oktober 2010.

#### SPLOŠNA DEJSTVA O NAPADIH IN VDORIH V POSLOVNIH OKOLJIH

Dejstvo	Pogostost v letu 2009 (v %)	Sprememba glede na leto 2008 (v %)
Tarča napadov in zlorab so strežniki.	98	-1
Gre za lažje izvedljive napade.	85	2
Zlorabo je odkrila šele tretja stran.	61	-8
Žrtve imajo dokaze o napadu.	86	0
Kraj podatkov bi se lahko izognili zgolj z uveljavljanjem preprostih kontrol.	96	9
Žrtve zlorab plačilnih kartic niso imele urejene združljivosti z varnostnim standardom PCI DSS.	79	Ni podatka.

Vir: Verizon 2010 Data Breach Investigations Report, oktober 2010.