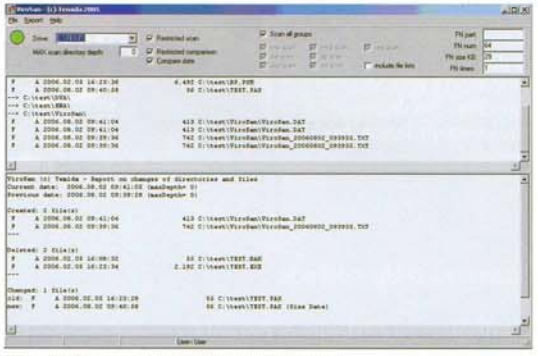
# Ustavite odtok podatkov

**Poslovanje podjetij je odvisno od "mehkih" virov – informacij, ki vključujejo strateški "know-how" podjetja ter podpirajo poslovne odločitve. Ponavadi jih ne bomo našli ovrednotene po računovodskih standardih, kljub temu pa prosto upravljanje takih virov pomeni pomembna tveganja za poslovanje. Obvladovanje takih tveganj od podjetja zahteva vpeljavo ustreznih varnostnih politik. V grobem ima podjetje tri možnosti: nima varnostne politike, ima jo, a ni zapisana, ali ima jo in je tudi zapisana. Izkaže pa se, da čim bolj je podjetje urejeno, tem bolj je urejeno tudi področje varnosti.**

**Stojan Košti, dr. Bojan Cestnik**

Z uvedbo sistema varovanja podjetje ohranja svojo konkurenčno prednost. Zato tveganja obravnavamo tako z vidika poslovne priložnosti (kontinuiteta zagotavljanja informacij in možnost za povečanje donosa) kot z vidika nevarnosti (dogodek z negativnimi posledicami). Ker sta dejavnika enako pomembna pri poslovanju, je treba vzpostaviti procese proaktivnega ocenjevanja tveganj in njihovega upravljanja. Ob zavedanju, da neko tveganje obstaja, leto bodisi sprejmemo ali pa ga obvladujemo z ukrepi za njegovo zmanjševanje. Proces takega obvladovanja tveganj mora biti skladen s specifičnimi poslovnimi cilji podjetja.

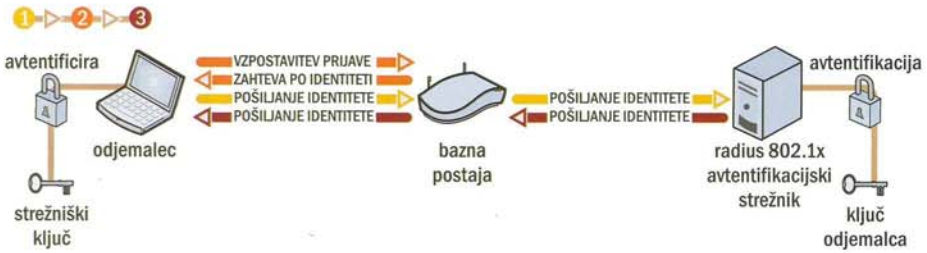


Sistem ViroSan za nadzor vsebine pomnilniških nosilcev

### Raziščite svoje možnosti

Računalniška varnost je širok pojem in zajema cel spekter, od fizičnega do logičnega varovanja dostopov do sistemov, aplikacij in podatkov. Na prvem mestu je treba pri izvajanju učinkovite varnostne politike določiti pravila fizičnega dostopa do računalniške opreme in omogočiti in uveljaviti njihovo izvajanje. V ta sklop spadajo sistemi zaklepanja in nadzorovanja dostopov v prostore z računalniško opremo, pa tudi sistemi za shranjevanje varnostnih kopij podatkov v smislu zagotovitve nepretrganega poslovanja. Prav tako spadajo v to skupino varovanja dostopov do krajevnih računalnikov iz zunanjega omrežja.

Druga ključna prvina varnostne politike je varovanje informacij. Te so aktivno in marsikdaj najpomembnejše premoženje podjetja. Preden lahko od zaposlenih pričakujemo ustrezno varovanje in upravljanje informacij, morajo le-ti razumeti njihovo vrednost in sprejeti odgovornost pri delu z njimi. Stopnja varnosti informacij mora biti premo sorazmerna z vrednostjo informacij, pri čemer vrednost navadno ocenimo v finančnem smislu, kot jo, na primer, povzroči napačna raba, razkritje, nepravilnost ali celo izguba informacije. Zato je za vzpostavitev primerne ravni zaščite pomembna klasifikacija informacij v podjetju. Pri tem si pomagamo z ocenami, ki temeljijo na vprašanjih, kolikšna je škoda v primeru posredovanja napačnih informacij, nepooblaščenega razkritja ali izgube informacij in drugo. Na taki podlagi rangiramo informacije in se odločimo, katera tveganja so sprejemljiva in katera je smotrno obvladovati.




Metodologija PDCA

Varnostne politike podjetja navadno nastanejo kot posledica poslovnih zahtev in zagotavljajo učinkovitost poslovanja, sledijo zakonskim in pogodbenim zahtevam ter zagotavljajo zmanjšanje tveganj v podjetju. Pristop k informacijski zaščiti je zato širši in ni omejen zgolj na tehnični vidik.

### Opazujte svoje hibe

Po podatkih Security Institute and Resource centra iz ZDA so še vedno poglavitna grožnja informacijski zaščiti (dve tretjini) napake zaposlenih pri uporabi informacijskih sistemov in različna opuščanja varnostnih mehanizmov. Nekaj več kot 10 % težav nastane zaradi površnost in nepoštenosti zaposlenih, s tem v povezavi pa nadaljnjih 10 % problemov nastane zaradi nezadovoljstva zaposlenih. Problemi, povezani z upravljanjem fizične informacijske infrastrukture, prav tako vodijo do resnih problemov. V skupnem odstotku groženj predstavljajo v povprečju manj kot 10 %. Šele na zadnjem mestu so problemi, ki jih povzročajo razni hekerji z vdori v informacijski sistem.

Kljub temu da prav slednjim namenjamo največjo pozornost, pa predstavljajo ti problemi okrog 5 % delež v skupni sliki tveganj. Prav zato se velja podrobneje posvetili tveganjem, ki jih za informacijsko varnost predstavljajo pogosto prezrti notranji dejavniki podjetja.

### Preštejte svoje vrste

Kot najpomembnejše pri ocenjevanju tveganj smo že omenili postavljanje pravih vprašanj. Zgled takega vprašanja je, kaj pomeni za podjetje, če neki informacijski vir ni dostopen določen čas (eno uro, en dan, en teden itd.). Koliko izgube (škode) v tem času to povzroči podjetju? Pri tem si pomagamo s seznamom procesov, informacij in njihovih virov, ki so navadno del poslovne dokumentacije podjetja. Za vsako entiteto s tega seznama razmislimo, kako in s kakšno verjetnostjo lahko odstopa od želenega stanja in kakšno škodo povzroči tako odstopanje. Pri obvladovanju tveganj navadno izhajamo iz kakovostne ocene tveganja - tveganja pod določeno mejo sprejmemo, nad to mejo pa obvladujemo. Za obvladovanje vzpostavimo nadzorstva, katerih namen je zmanjšanje tveganja na sprejemljivo raven. Pri tem je najpomembneje, da ves postopek ocene tveganj ustrezno dokumentiramo. Katero orodje uporabimo, je stvar izbire, navadno pa zadošča že navadna preglednica.

Omeniti velja še stroškovni vidik obvladovanja tveganj. Pri tem lahko razmišljamo podobno kot pri zavarovanju osebnega avtomobila. Ni smiselno potrošiti vsa sredstva za zavarovanje, ker potem ne bomo imeli denarja za nakup goriva in izvedbo potovanj in bo moral avto počivati v garaži. Prav tako verjetno ni smiselna druga skrajnost: ves denar namesto za zavarovanje namenimo za potovanja. Prava odločitev je kompromis nekje med obema skrajnostma. Kje, je odločitev vsakega posameznika, oziroma ko govorimo o nadzorstvih za obvladovanje tveganj, vsakega vodstva podjetja.

### Prevzemite krmilo

Zaradi občutljivosti področja upravljanja informacij je priporočljiva vzpostavitev enotnega nadzora dostopa uporabnikov do aplikacij - uporabnik tako uporablja eno ime in geslo za vse aplikacije. Pri oblikovanju in spreminjanju gesel v razumni meri upoštevajmo priporočila standarda BS 7799. Vsi sistemi in aplikacije naj imajo vgrajene mehanizme za zapisovanje posegov (t. i. dnevniške oz. log datoteke), ki naj bodo standardizirani za vse aplikacije v podjetju. Z namestitvijo sistemov za spremljanje revizijskih sledi v uporabljenih računalniških programih (npr. LogAn) si nato precej olajšamo delo pri odkrivanju vsebinskih napak in problemov.

Opravljajmo periodično preverjanje vsebine računalniških nosilcev. Z nameščenimi pregledovalniki (npr. SnapShot, ViroSan, WINAFV32, FSUM, SFV Checker ...) sledimo vsem spremembam (kdo, kdaj, kaj), ki se v nekem obdobju zgodijo na nekem nosilcu (slika 1). Tako lahko celo ugotovimo, ali se je v sistem pretihotapil kak virus, črv ali vohunski program. Sistem namreč ustvari podatkovne slike celotnega nosilca v nekem obdobju in vsebine medsebojno primerja. Največja dodana vrednost takega spremljanja pa je možnost časovnega ugotavljanja posegov (namernih ali nenamernih) s strani uporabnikov sistema.

### Postavljajte jasna pravila

Upravljanje tveganj mora biti na prvem mestu celovito, vštevši fizično varnost, računalniško varnost in, kot najpomembneje, varnost informacij. Pomembno je, da so varnostne politike napisane, saj imajo le tako tudi pravno veljavo ob njihovem morebitnem neupoštevanju.

Eden izmed načinov pristopa k upravljanju tega področja je projektni pristop, pri katerem se osredotočimo predvsem na doseganje želenih rezultatov. Poleg izdelave varnostnega načrta je na mestu predvsem učinkovita izvedba varnostnih politik, standardov, procedur in navodil. Aktivni pristop in odgovornost za izvajanje varnostnega programa mora zajemati vse zaposlene. Pri tem je poglavitno razumevanje, zakaj je treba vzeti izvajanje informacijske varnosti resno, kaj bomo s tem pridobili in kako nam bo spoštovanje varnostnih standardov pomagalo pri našem delu. Spoštovanje in izvajanje varnostnih politik mora postati obveza vseh zaposlenih v podjetju.

Nadzor in upravljanje informacijskega sistema v povezavi z učinkovitim obvladovanjem informacijskih tveganj v podjetju mora postati stalen proces. Problemov se lotimo z izbiro ustrezne metodologije s področja upravljanja varnosti informacij. Med bolj znanimi je PDCA (Plan-Do-Check-Act), ki jo priporoča tudi varnostni standard BS 7799-2-2003 (slika 2).

Ne glede na velikost podjetja z uporabo spleta, e-pošte in drugih informacijskih virov, ki jih uporabljajo zaposleni pri svojem delu, podjetje tvega svoje vire, prihodnost in ugled. Nenamerna ali namerna zloraba teh virov nam lahko povzroči hude glavobole. Podjetja, ki se tega zavedajo, zato izdelajo celovite in razumljivo napisane politike ter za izvajanje politik svoje zaposlene tudi ustrezno izobražujejo. *

## Sedem koristnih lastnosti

1. Varnostne politike naj bodo zapisane.
2. Izobražujte zaposlene o tveganjih, politikah in varnosti.
3. Pripravite smernice za ohranjanje sporočil e-pošte in takojšnjega sporočanja.
4. Postavite pravila sprejemljive uporabe za osebne potrebe.
5. Obravnavajte zadeve v zvezi z lastništvom in zasebnostjo.
6. Vzpostavite pravila izražanja.
7. Podprite svoje elektronske politike z ustrezno tehnologijo.

## Sedem pomembnih malenkosti

1. Ozrite se po že zapisanih politikah.
2. Cilji in poslanstvo podjetja morajo postati aktivni del politike.
3. Naj bodo varnostne politike videti kot varnostne politike.
4. Zavedajte se, da 100 % varnosti ni.
5. Pazite na razumljivost.
6. Držite se bistva. Politike naj ne bodo predolge.
7. Poročajte zaposlenim in jih izobražujte.