Na vaša pitanja odgovara Enimark Ponjević, direktor poduzeća General Security

Sigurnost informacija

Opet smo svjedoci mnogih primjera curenja informacija, kao npr. registra branitelja, pitanja s državne mature, pa čak i informacija o osiguranju Predsjednika Republike. Čuo sam da bi takve stvari trebali rješavati stručnjaci za sigurnost i upravljanje kriznim situacijama. Moje poduzeće nema kapaciteta za zapošljavanje takve osobe, zato me zanima Vaš odgovor na pitanje „Koja je njihova uloga i koje konkretne korake trebam očekivati od njih u zaštiti svog poduzeća?" *Roman R., Zagreb*

Sigurnost informacija i sprječavanje njihovog curenja? Pa to mi zvuči otprilike kao "pojedi juhu s vilicom"!

Nije nemoguća misija, nego treba znati! Prvo namotajte rezance na vilicu kao da jedete špagete, a onda popijte preostalu juhu. Ono što vam se prelilo preko brade i umazalo košulju – e to Vam je curenje informacija. Nemate iskustvo, praksu i mislite da to može svatko pa ćete, nakon što pročitate ovaj članak do kraja, odlučiti malo "dotegnuti šarafe" u Vašoj tvrtki po principima sigurnosti koji slijede. Pa hajde…

SVEDITE RIZIKE NA MINIMUM

Sigurnost informacija i Vaših informacijskih sustava ovisi o tome s kolikom se vjerojatnošću možete pouzdati u njihovu dostupnost, ispravnost i samu tajnost. Kako bi se rizik "curenja" sveo na minimum, potrebno je uspostaviti formalne propise za sigurno uklanjanje osjetljivih medija te provedba tih propisa treba biti provjerena i dokumentirana. Na listu dokumenata za sigurno uklanjanje svakako stavite papirnate dokumente, snimljeni glas, indigo papir, traku za printer, magnetni medij, optički medij, sistemsku dokumentaciju itd.

Uspostavite i procedure za rukovanje informacijama kako biste ih zaštitili od neovlaštenog otkrivanja i zlouporabe. Ograničavajte pristup i održavajte popis ovlaštenih primaoca podataka. Jasno označavajte sve kopije i zaštitite podatke u skladu s njihovom osjetljivošću uz minimalnu distribuciju.

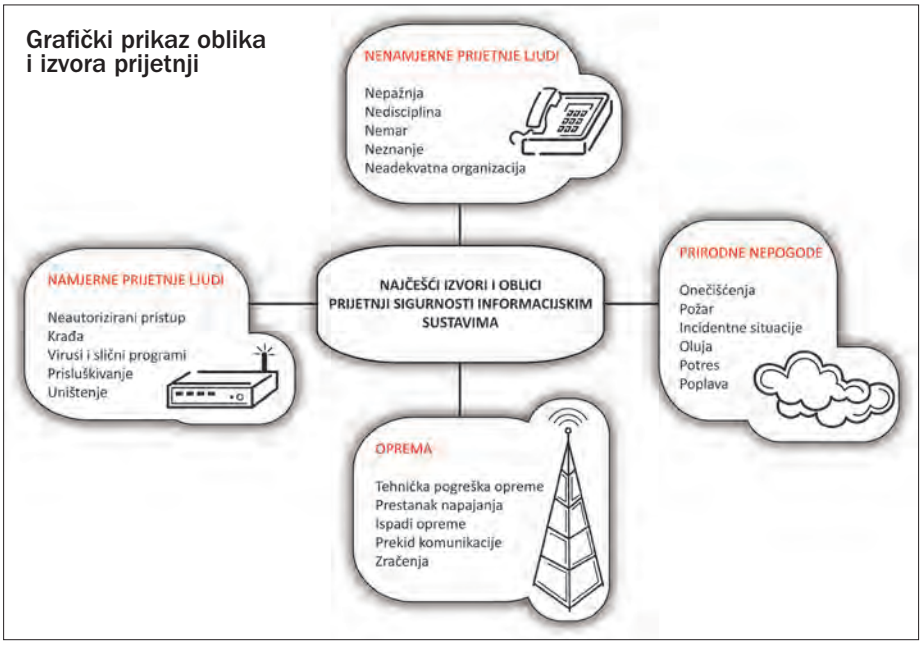
Najčešći oblici i izvori prijetnji sigurnosti informacijskih sustava su namjerne i nenamjerne prijetnje ljudi, zatajenje opreme i prirodne nepogode.

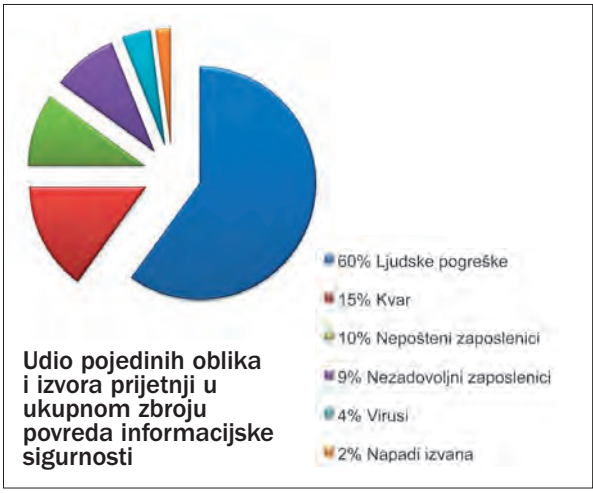
Needucirani zaposlenici zadaju najviše problema u zaštiti informacijskih sustava, bez obzira radi li se o ovlaštenim ili neovlaštenim korisnicima. Oni svojim postupcima slučajno brišu ili mijenjaju podatke, nepažljivo rukuju resursima i ugrožavaju sigurnost informacija u najvećem postotku od ukupnog broja incidenata.

Vrlo često su nesvjesni pomagači zlonamjernim korisnicima za izvršavanje napada, ne znajući da im pružaju potrebne podatke. Ova tehnika napada je danas vrlo aktualna i zove se "Socijalni inženjering". Ako smatrate da prijetnje Vašim sigurnosnim sustavima najčešće dolaze izvana (hakeri), istraživanja su pokazala da probleme sigurnosti najviše uzrokuju greške Vaših zaposlenika, zatim kvar opreme, slijede zaposlenici koji svoj položaj koriste za vlastitu korist i zaposlenici koji na ovakav način izražavaju svoje nezadovoljstvo prema poduzeću ili nadređenoj osobi.

Najrjeđi, ali napadi koji uzrokuju najviše štete su napadi "izvana", od kojih se morate braniti kontrolom prometa s interneta, sprječavanjem instaliranja špijunskih programa u operacijski sustav i kriptiranjem podataka. Kriptografske metode osiguravaju i pomažu u ostvarenju tajnosti izvornog

Grafički prikaz oblika i izvora prijetnji





Udio pojedinih oblika i izvora prijetnji u ukupnom zbroju povreda informacijske sigurnosti

Sigurnost informacija i Vaših informacijskih sustava ovisi o tome s kolikom se vjerojatnošću možete pouzdati u njihovu dostupnost, ispravnost i samu tajnost. Kako bi se rizik "curenja" sveo na minimum, potrebno je uspostaviti formalne propise za sigurno uklanjanje osjetljivih medija te provedba tih propisa treba biti provjerena i dokumentirana.

teksta sprječavajući uvid u njegov sadržaj. Osiguravaju Vam i autentičnost izvornog teksta, tj. vjerodostojnost sadržaja poruke, kao i njezin integritet u smislu sprječavanja neovlaštenog mijenjanja sadržaja izvornog teksta, te njegovo oštećenje ili uništenje.

Smjestite opremu na kojoj se čuvaju podaci u posebnu prostoriju sa kontroliranom vlagom i temperaturom te uvedite kontrolu pristupa uz definirane sankcije onima koji se ne pridržavaju propisanih pravila.

UGOVORI O POVJERENJU

Sa svojim djelatnicima, partnerima, kao i s vanjskim suradnicima sklopite ugovore o povjerenju, sa svrhom da na temelju zakona zaštitite podatke i vrijednosti od kopiranja, uništavanja, zamjene i ostalih neželjenih radnji. Ugovor o povjerenju treba sadržavati sljedeće podatke:

- što treba zaštititi,
- očekivano trajanje ugovora,
- što je potrebno poduzeti prilikom raskida ugovora,
- odgovornost i radnje odgovornih kako bi se spriječilo neovlašteno širenje informacija,
- koja prava imaju ovlašteni pri uporabi informacija,
- prava provjere, kontrole i nadgledanja pri uporabi osjetljivih informacija,
- procese za obavještavanje i prijavu neovlaštenog širenja informacija ili otkrivanje povjerljivih informacija,
- popis informacija koje moraju biti uništene, promijenjene ili vraćene pri prekidu ugovora,
- radnje koje je potrebno poduzeti ukoliko dođe do nepoštivanja ugovora.

UGOVORI O ZAPOSLENJU ILI SURADNJI

Održavanje opreme ste povjerili stručnjacima iz Vašeg poduzeća ili imate vanjskog partnera? Svejedno, obratite pozornost da pristup opremi mora biti strogo kontroliran i dokumentiran. Zahtijevajte sklapanje posebnih ugovora o zaposlenju ili suradnji, koji definiraju procedure u pogledu sigurnosti i imaju za cilj smanjiti rizik od ljudske pogreške, krađe, prijevare i zlouporabe resursa Vašeg informacijskog sustava. Tim ugovorima mora prethoditi provjera kandidata ili tvrtke partnera na temelju raspoloživih referenci poslovanja, karaktera, na temelju dostupnih CV-a kao i kontrole dostavljenih podataka, potvrda o izobrazbi i profesionalnim kvalifikacijama, dokazima identiteta i provjerama da li je kandidat kazneno gonjen.

Prije dodjeljivanja prava pristupa osjetljivim informacijama, pružite im uvid u obliku smjernica o tome što od njih očekujete ovisno o njihovim ulogama i pokušajte osigurati potrebnu razinu svijesti o potrebi za sigurnošću.

Poduzmite sve ove predradnje prije sklapanja ugovora o radu ili suradnji te osigurajte da sadrži definirane sve mjere sigurnosti koje stvaraju preduvjet za kvalitetan raskid istog tog ugovora.

RASKID UGOVORA

Radnje i odgovornosti kod prekida radnog odnosa, raskida ugovora s partnerskom tvrtkom ili promjene radnog mjesta moraju biti jasno propisane. Zaposlenik, partner ili treća strana mora vratiti u Vaš posjed sve materijalne vrijednosti koje je dobio na korištenje tijekom radnog odnosa. Isto tako, morate im oduzeti sva prava pristupa informacijama i resursima, tražite povrat svih ključeva, pametnih kartica, imovine na korištenju te o primopredaji sačinite zapisnik. Zahvalite na suradnji i ispratite ih do vrata. Uz malo sreće, to bi moglo značiti da ste sačuvali informacije Vaše tvrtke i dobro odradili posao do samoga kraja.

Da se poslužimo nogometnim rječnikom - za uspješno vođenje Vaše tvrtke odaberite najbolji mogući tim igrača raznih profila. S njima ćete dobro pokriti teren Vaših poslovnih interesa i svi izgledi za velike pobjede su na Vašoj strani. Masa koja Vam daje podršku loviti će Vaš pogled i tapšati Vas po ramenu. Budite hladni i pametni u završnici akcije koja donosi pobjedu. I zapamtite, nije gol kada loptom zatresete mrežu Vašeg protivnika, nego tek ako sudac nakon toga pokaže na centar terena. PS