CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

Sigurnije poslovanje na Internetu

Partner

Poslovni dnevnik
PRVE DNEVNE POSLOVNE NOVINE U HRVATSKOJ

Sadržaj

Impressum

Hrvatska akademska i istraživačka mreža CARNet

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Josipa Marohnića 5, Zagreb
tel: 01 6661 616
fax: 01 6661 615
http://www.CARNet. hr

Nacionalni CERT

Nacionalni CERT+

Suradnici:
Mladen Štifić (tekst);
Sebastijan Čamagajevac (ilustracije)

Partner

Poslovni dnevnik
PRVE DNEVNE POSLOVNE NOVINE U HRVATSKOJ

Uvod

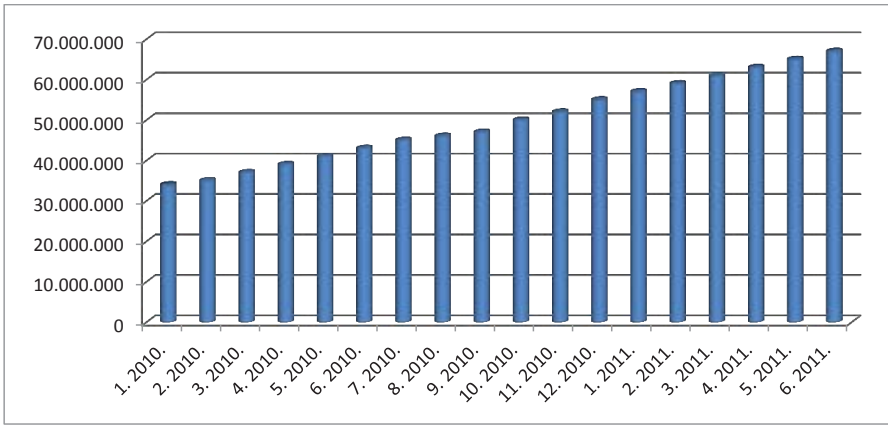
Ako pretpostavimo da su računala i pristup Internetu integralni dio Vašeg poslovanja, neovisno o djelatnošću kojom se Vaša tvrtka bavi, teško da ćemo pogriješiti. Uz brojne prednosti koje donose nove tehnologije i Internet, suočavamo se i s nekim novim rizicima za poslovanje.

Nacionalni CERT je organizacija s misijom prevencije i zaštite od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Ova knjižica izrađena je s motivom podizanja ukupne razine svijesti o informacijskoj sigurnosti kroz edukaciju poslovnih subjekata. Kako je područje našeg djelovanja sigurnost javnih informacijskih sustava (računala dostupnih putem Interneta), sadržaj pred Vama ograničen je na taj aspekt sigurnosti Vaše tvrtke.

Osigurati IT infrastrukturu tvrtke nije nimalo slično zaštiti kućnog računala. Rizik od prekida rada ili gubitka podataka, pogotovo ako su prihodi uz njih izravno vezani, daleko je izraženiji. Ako raspolažete podacima klijenata, povjerljivost tih podataka je osjetljiva. Ako nudite usluge putem Interneta, njihova dostupnost je svakako kritična. Ispravan rad računala unutar Vaše poslovne mreže također može biti ključan. Pored toga, računala tvrtke uglavnom su dostupna većem broju ljudi, neka možda čak i Vašim klijentima. Samim time, sigurnost svih navedenih sustava ovisi i o uspješnom ograničavanju aktivnosti koje su na njima dopuštene.

Uspješna briga o računalnoj sigurnosti tvrtke podrazumijeva praćenje razvoja sigurnosnih standarda i tehnologija. Poželjno je unutar tvrtke imati osobu čiji je to zadatak, a Vama savjetujemo da u skladu s izloženošću računalno sigurnosnim rizicima procijenite razumno ulaganje u zaštitu.

Prijetnje na Internetu

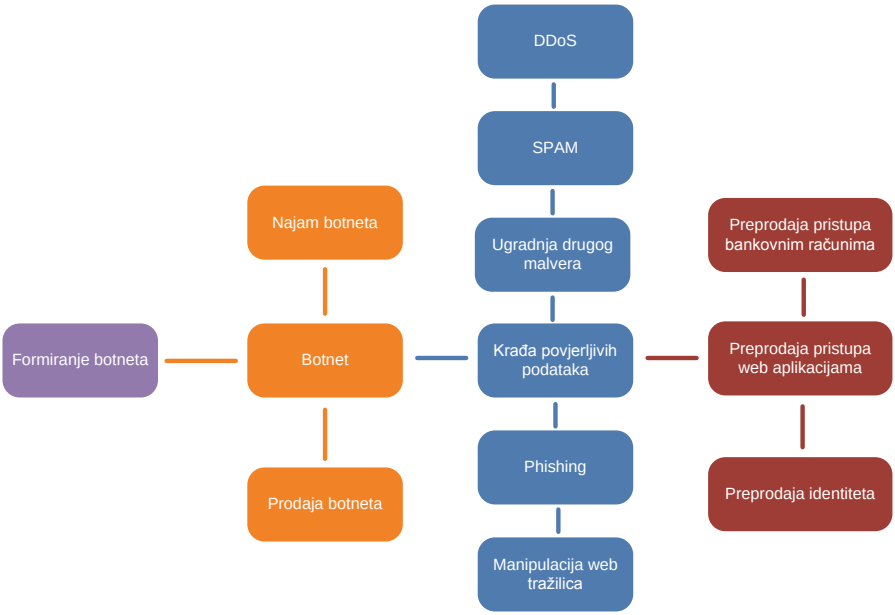


Broj uzoraka malvera u bazi antivirusnog alata od početka 2010. godine

Izvor: McAffee

Uvjerljivo najzastupljenija prijetnja računalima spojenima na Internet u trenutku pisanja ovog teksta je malver. Motivi autora i širitelja malvera uglavnom su neki oblik financijske dobiti. Takav malver zovemo crimeware. Većina malvera organizira zaražena računala u hijerarhijske mreže kojima je moguće upravljati. Te mreže nazivamo botnetovima, a malver koji se izvršava na zaraženim računalima botovima. Također je uobičajeno računalo zaraženo botom zvati zombie računalo.

Razlog takve organizacije je specifična ekonomija autora i korisnika botnetova. Autori kôda malvera svoje uratke prodaju u obliku softvera za izradu botneta (botnet kit) ili botnet sami uspostavljaju i održavaju pa prodaju kontrolu nad određenim brojem zaraženih računala i pripadajući upravljački softver.



Botnetovi svojim krajnjim korisnicima omogućavaju različite kriminalne aktivnosti:

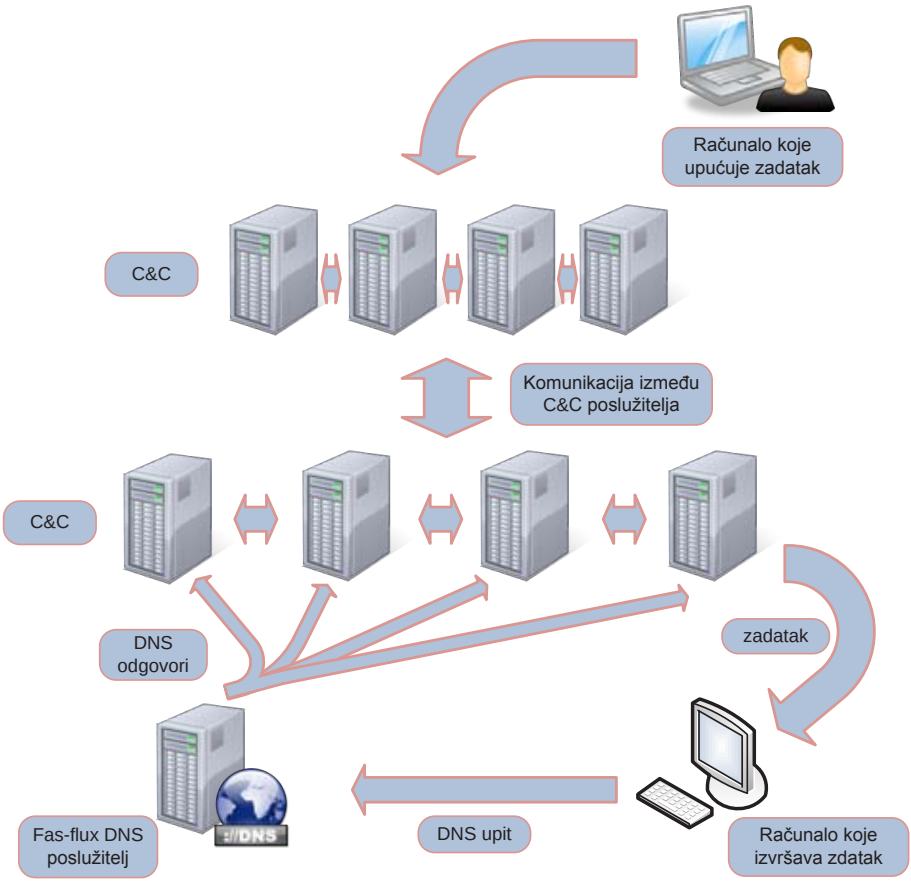
- DDoS napad
- Krađu povjerljivih informacija (npr. kreditne kartice)
- Phishing
- Slanje neželjenih poruka (SPAM)
- Širenje drugog malvera
- Posluživanje malicioznih web stranica
- Razne oblike prevara

Tipičan botnet sastoji se od najmanje dva različita oblika softvera: samog bota koji obavlja zadatke i kontrolnog centra (C&C) koji mu te zadatke upućuje. Često je kontrolni sloj botneta sastavljen od mnoštva računala organiziranih u sofisticirane slojeve. Takva arhitektura otežava otkrivanje računala s kojeg zadaci izvorno stižu, odnosno služi za zaštitu kontrolnog centra i kriminalaca koji njima upravljaju.

Kako računala u kontrolnom sloju ima više, kada neko od njih prestane biti dostupno (npr. s njega je malver uklonjen), bot automatski nastavlja preuzimati zadatke sa sljedećeg. Kako bi ovaj proces bio dovoljno brz i botnet otporan na gašenje, koristi se metoda fast-flux.

Fast flux je metoda postavljanja DNS poslužitelja koji za isto simboličko ime odgovara nizom različitih IP adresa. DNS odgovori označeni su kao kratkotrajno važeći (kratak TTL). Iza svake od tih adresa nalazi se računalo koje obavlja neku od funkcija unutar botneta (npr. poslužuje kôd malvera ili prosljeđuje C&C zadatke botovima).

Među najraširenijim modernim botovima nalazimo Conficker, Zeus, SpyEye i TDSS (autor Zeusa je navodno izvorni kôd predao autoru SpyEye-a i povukao se). Zeus i SpyEye u različitim verzijama predstavljaju botnet kitove i poznati su po specijalizaciji za presretanje bankovnih transakcija. Računalo zaraženo Zeusom korisniku prikazuje uobičajen tijek korištenja elektroničkog bankarstva, dok u pozadini transakciju izmjenjuje u prijenos sredstava na neki drugi bankovni račun. Novac s tog računa podiže osoba regrutirana kao money mule, zadržava proviziju i prosljeđuje dalje, sve dok novac ne stigne do napadača.



Malver na radnim stanicama u internim poslovnim mrežama

Osim već opisanih botova, na radne stanice, mahom opremljene Windows operativnim sustavom, stižu i drugi oblici malvera. Mnogima je cilj praćenjem tipkovnice ukrasti lozinke i brojeve kreditnih kartica, no u porastu su i drugi načini zlouporabe, npr. ransomware.

Ransomware – malver koji onemogućava normalan rad računala, prijeti uništavanjem podataka ili lažno detektira drugi malver kako bi korisnika prinudio da napadaču uplati određen iznos novca.

Normalan rad računala ne znači da ono nije zaraženo malverom! Ako je cilj autora malvera ostati neotkriven, računalo ničime neće odavati znakove da je zaraženo!

Malver na poslužiteljima

Kako se na poslužiteljima uglavnom nalazi drugačija programska podrška nego na radnim stanicama, malver koji na njima pronalazimo drugačije je strukture i namjene. Meta su mahom PHP CMS web aplikacije na Apache web poslužitelju te .net platforma na IIS web poslužiteljima.

Na datotečni sustav web poslužitelja, uz legitimnu web stranicu Vaše tvrtke napadač može postaviti phishing stranicu, kôd malvera, web trgovinu s lijekovima i slično, a da to ne ometa normalan rad Vaše web aplikacije. Sporan sadržaj posluživat će se s drugih domena koje vode na Vašu IP adresu ili će biti skrivene u strukturi direktorija web aplikacije. Također, vaš poslužitelj može postati jedno od računala u botnet strukturi, pohranjujući ukradene podatke (dropzone) ili prosljeđujući upute C&C-a botovima.

Ako je Vaš poslužitelj postao meta ovakvog napada, to ćete obično saznati na način da korisnici pri posjeti Vaše web stranice naiđu na upozorenje kako se radi o opasnom odredištu. Razlog tome je što je neka od organizacija u suradnji s proizvođačem web preglednika Vašu web stranicu postavila na crnu listu kako bi se zaustavilo širenje opasnog sadržaja.

Ukloniti maliciozan sadržaj s web poslužitelja nije dovoljno! Ako ne pronađete način na koji je sadržaj dospio na Vaš poslužitelj, napadač će ga unutar nekoliko minuta vratiti, možda čak pod drugim imenom kako biste ga još teže pronašli.

Vektori širenja malvera

Napadačima je najjednostavnije zaraziti računalo ako mogu pronaći neki sigurnosni propust u programskoj podršci. Ako web preglednik omogući preuzimanje i pokretanje programa bez intervencije korisnika, govorimo o napadu naziva drive-by-download. Ako pak web aplikacija zbog loše provjere omogući izvršavanje stranog kôda, napadač može steći pristup datotečnom sustavu Vašeg web poslužitelja. Od takvih napada možemo se štititi

redovnim ažuriranjem programske podrške, no takva zaštita nije dovoljna zbog zero day sigurnosnih propusta.

0 day: proizvođači softvera ne uspijevaju uvijek držati korak s autorima malvera; ponekad autori malvera iskoriste propust za koji još nije objavljena zakrpa proizvođača ili čak propust koji do tada nije poznat pa proizvođač nije ni mogao pripremiti zakrpu.

Kako su krajnji korisnici obično dovoljno "slaba karika" u smislu njihove svijesti o računalnoj sigurnosti, mnogi napadači koriste prvenstveno ljudski faktor za distribuciju malvera. Tako ćemo poveznice na malver pronaći u statusima na Facebooku, objavama na Twitteru, komentarima na blogovima, IM i e-mail porukama pa čak i SMS-ovima.

Primjer ransomwarea nalazimo u obliku lažnog antivirusnog softvera. Maliciozna web stranica vizualnim trikom prikaže upozorenje da je pronađen virus te traži od korisnika da preuzme antivirusni program koji će ga očistiti. Preuzeti program je zapravo malver koji najčešće potpuno blokira računalo i traži od korisnika uplatu kako bi normalno nastavio s radom.

Za korisnike dovoljno educirane da takve programe ne pokreću, smišljaju se kreativnije metode. Tako na statusu prijatelja na Facebooku možete vidjeti poveznicu na neki zanimljiv video, a stranica koja navodno poslužuje video zahtjeva preuzimanje dodatka za web preglednik (koji je zapravo malver). Napadači također vrebaju na nestrpljive obožavatelje popularnih emisija te putem P2P* mreža (npr. BitTorrent) objavljuju lažne video sadržaje s nazivom još neobjavljene epizode. Kada se video pokrene, na ekranu se nalazi uputa da je za gledanje potrebno preuzeti poseban softver te poveznica na kojoj se taj softver nalazi. Softver je, naravno, malver.

Malver se osim ovim putevima širi još i elektroničkom poštom s privitkom ili poveznicom na maliciozan dokument te na brojne druge načine. Poznavati trenutno prisutne oblike socijalnog inženjeringa nije dovoljno, jer napadači stalno smišljaju nove, računajući na našu sposobnost da stare trikove prepoznamo. Učinkovitije je primijeniti isključiv kriterij, ne pokretati ništa što nismo očekivali, a kada nismo sigurni, izravno se obratiti osobi koja nam sadržaj navodno šalje. Na primjer, ako nam je poruka stigla od banke, nazvati njihov info telefon i zatražiti od službenika da nam potvrdi da su oni poslali poruku.

Ove prijetnje čine dodatni motiv ograničavanju aktivnosti djelatnika na računalima izvan okvira njihovih poslovnih zadataka te utvrđivanju jasne procedure za zadatke koji jesu po-

slovni. Djelatnici će na taj način lakše primijetiti kada prime poruku koja se ne uklapa u njihov uobičajen rad i biti skloniji savjetovati se s kolegama.

Ne postoji garancija da je računalo na kojem antivirusni softver nije pronašao prijetnju zaista sigurno. Ukoliko sumnjate da je računalo kompromitirano, upotrijebite pričuvnu kopiju čitavog sadržaja čvrstog diska (image backup). Vodite računa da koristite pričuvnu kopiju načinjenu prije nego što je računalo postalo kompromitirano te ju prije primjene provjerite ažurnim antivirusnim softverom. Prije ponovnog uključenja računala u mrežu primijenite sve u međuvremenu izašle zakrpe.

Osim malvera, sigurnost računala može doći u pitanje napadima usmjerenima na Vaše resurse i dostupnost javnih usluga. Neželjena pošta može poskupiti ili ograničiti funkcionalnost naše komunikacije, a DoS napadi onemogućiti našim klijentima korištenje naše web stranice ili druge usluge.

DDoS (Distributed Denial of Service), napad uskraćivanjem usluge, izvodi se u pravilu iz botneta. Brojna zombie računala upućena su da pristupaju usluzi i maksimalno opterećuju poslužitelj kako bi ga onemogućila u pružanju usluge stvarnim korisnicima.

Rizici i posljedice incidenata na Internetu

Kako se računala bave obradom informacija, računalna sigurnost primarno se odnosi na kontrolu protoka informacija i njihovu dostupnost. Velik dio brige odnosi se na zaštitu povjerljivosti osjetljivih podataka, područje koje sigurnosni stručnjaci nazivaju Data Leakage Protection (eng. zaštita od curenja podataka).

Sami najbolje možete procijeniti koje su informacije unutar Vaše tvrtke povjerljive, no možemo prepoznati neke uobičajene kategorije:

- Autentikacijski podaci (lozinke, tajni ključevi)
- Osobni podaci zaposlenih i klijenata
- Računovodstveni podaci (plaće, poslovne transakcije)
- Poslovne tajne (korespondencija, intelektualno vlasništvo)

Podaci mogu "curiti" iz različitih izvora, a Internet se u praksi pokazao kao posebno interesantan medij za krađu povjerljivih ili osobnih podataka. Najizloženija su neadekvatno zaštićena računala i mreže tvrtki te tvrtke čiji se zaposlenici ne pridržavaju sigurnosnih procedura. Izložene su i tvrtke čije su mreže povezane s poslovnim partnerima a da ta povezanost nije adekvatno ograničena i zaštićena.

Važno je razumjeti da tehničke mjere zaštite (sigurnosni uređaji, dizajn mreže) nisu dovoljne, stoga je nužna edukacija djelatnika s pristupom osjetljivim informacijama.

Phishing (eng. fishing – pecanje) je postupak masovnog slanja poruke u kojoj se napadač lažno predstavlja u ime nekog našeg pružatelja usluge (web trgovina, banka) i od nas traži pristupne podatke.

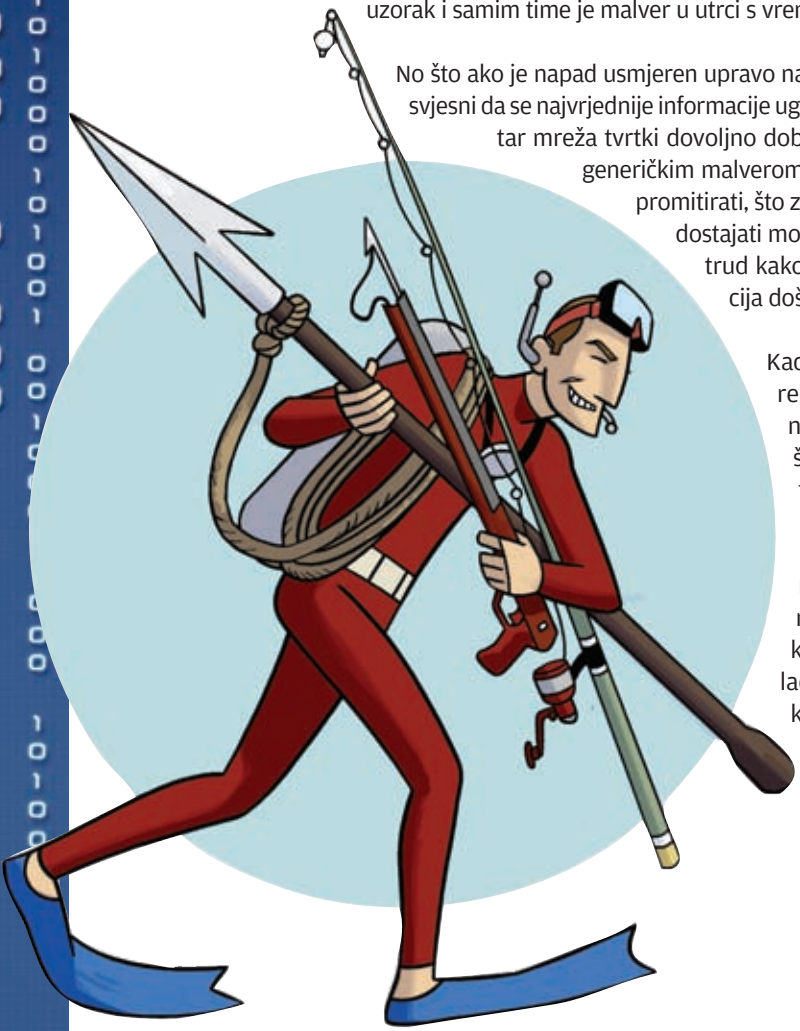
Ako ste žrtva phishinga (odnosno, ako je zaposlenik Vaše tvrtke na phishing stranicu upisao povjerljive podatke), uz dobru komunikaciju unutar organizacije možda ćete za incident saznati na vrijeme i spriječiti veću štetu. No prođe li incident neprimijećeno, napadač koji nakon stjecanja pristupa Vašim računalima malver dobro sakrije može informacije prikupljati neograničeno dugo bez vidljivog znaka.

Rootkit – softver posebno namijenjen skrivanju i zaštiti malicioznog kôda manipulacijom operativnog sustava; uklanja maliciozni proces s popisa procesa koji se izvršavaju i štiti svoje datoteke.

Targeted attack (eng. ciljani napad) – kompromitiranje sigurnosti točno određenog pojedinca ili organizacije napadom posebno podešenim za izabranu žrtvu u unaprijed pripremljenom scenariju.

Generički malver, široko distribuiran s namjerom kompromitiranja što većeg broja računala na Internetu, često će nastojati u što kraćem roku izvući materijalnu korist za napadača; na ovakav malver sigurnosna zajednica relativno brzo može reagirati jer im je dostupan uzorak i samim time je malver u utrci s vremenom.

No što ako je napad usmjeren upravo na Vas? Kriminalci su svjesni da se najvrjednije informacije uglavnom nalaze unutar mreža tvrtki dovoljno dobro zaštićenih da ih generičkim malverom nije moguće kompromitirati, što znači da im neće nedostajati motiva uložiti dodatan trud kako bi do tih informacija došli.



Kada napadač odabere konkretnu žrtvu, nastojat će prikupiti što više informacija te pomoću njih izvesti uvjerljiv socijalni inženjering. Kombiniranjem potrage za ranjivostima tehničke prirode i manipulacije zaposlenicima koji znaju povjerljive podatke, nastojat će steći što veće ovlasti.

Spear phishing (eng. ribolov harpunom) je postupak ciljanog slanja phishing poruka posebno skrojenih za odabranu žrtvu. Specijalni oblik spear phishinga, kada se napadaju čelne osobe velikih organizacija nazivamo whaling (eng. kitolov)

Žrtve phishinga mogu biti i Vaši klijenti, ukoliko pružate uslugu kojoj se pristupa putem interneta, a zaštićena je nekom od metoda autentikacije. Napadač će se u tom slučaju Vašem klijentu predstaviti kao Vi i zatražiti pristupne podatke. Svoje klijente možete u velikoj mjeri zaštititi na način da ih unaprijed upozorite na tu mogućnost i obvežete se da od njih nikada nećete putem elektroničke pošte i sličnim načinima tražiti autentikacijske podatke.

Podsjetimo da su podaci koji se nalaze na računalima Vašeg poduzeća vjerojatno osjetljivi čak i ako nemate posebno vrijedne dokumente. Vaši računovodstveni podaci, podaci klijenata i pristupni podaci vaše elektroničke pošte svakako mogu prouzročiti konkretnu štetu ako se nađu u krivim rukama.

Web defacement – zamjena sadržaja web stranice drugim po izboru napadača.

Web aplikacije koje nisu adekvatno zaštićene relativno su jednostavan vektor napada. Napadač Vam može narušiti ugled širenjem malvera pomoću Vaše web stranice ili zamijeniti čitav sadržaj nekim uvredljivim. Ako poželi, može čak i neprimjetno zamijeniti jedan podatak na stranici, kao što je broj telefona ili sadržaj neke vijesti. Ovisno o tome koliko je Vaše poslovanje vezano uz web stranicu tvrtke, šteta može biti relativno mala ili vrlo ozbiljna. Kompromitiranje baze podataka web aplikacije u kojoj se nalaze osjetljivi podaci Vaših klijenata u pitanje može dovesti i kontinuitet poslovanja.

Ponovit ćemo da napadač, ako želi, može Vaše podatke prikupljati tajno i zatim zametnuti trag svoje prisutnosti, što znači da poslovne tajne mogu „curiti“ a da Vi za to nikada ne saznate, no da ipak na neki posredan način zbog toga trpite štetu. S druge strane, ako ste obvezani ugovorom o tajnosti štititi informacije pod Vašom kontrolom, odgovornost može biti još veća.

Ostvari li napadač administrativni pristup ključnim računalima i na njima pronađe privatne ključeve za pristup drugim uslugama (npr. VPN pristup mreži poslovnog partnera), bit ćete prisiljeni opozvati sve izdane certifikate i možda privremeno obustaviti važne usluge.

Od DDoS napada nije se moguće u potpunosti i trajno zaštititi, no moguće je povećati otpornost do razine na kojoj napad možda neće biti isplativ. Bez ikakve zaštite uslugu je mo-

guće onesposobiti i sa samo jednog računala (DoS) i time takav napad postaje dovoljno jednostavan da se radi o stvarnoj i stalnoj prijetnji. Posljedice ovise o vezanosti napadnute usluge za naše poslovanje – ako poslužujemo uslugu kod koje je stalna dostupnost važna, potencijalna šteta je vrlo značajna.

Pouka svih ovih prijetnji je da je sanacija i najblažih posljedica kompromitirane sigurnosti često značajno skuplja i teža od ulaganja potrebnih da bi se rizici umanjili. Neadekvatna sigurnost donosi kontinuirani trošak saniranja manje važnih sustava i visok rizik ispada ključnih sustava ili kompromitiranja osjetljivih podataka pa sve do rizika totalne štete i onemogućenja nastavka poslovanja. Na Vama je da racionalno odmjerite ulaganja u sigurnost zavisno o osjetljivosti usluga i podataka kojima raspolažete te postojećih rizika.

Rizici vezani uz "cloud computing"

"Cloud computing" – istovremeno korištenje resursa velikog broja računala pod kontrolom pružatelja usluga.

Usluge smještaja naših aplikativnih rješenja ili podataka u oblak (cloud) postaju sve primamljivije u usporedbi s korištenjem vlastite opreme. Uklonjeni su troškovi i rizici održavanja, a količina računalnih resursa može se dokupljivati ili otkazivati po potrebi. Također nam omogućavaju jednostavno eksperimentiranje novim, zahtjevnim uslugama uz minimalna ulaganja ili pružaju smještaj velikih količina podataka.

Iako su prednosti značajne, odlučivanju za i odabiru pojedinog "cloud" rješenja potrebno je ozbiljno pristupiti. Podaci kojima naša aplikacija upravlja mogu biti povjerljivi, dostupnost

usluge kritična, a moguće je i da korištenje “clouda” nije usklađeno s ugovornim ili zakonskim obvezama koje imamo.

Ako u “cloudu” pohranjujemo povjerljive podatke, posebno ako ga koristimo kao odredište pričuvnih kopija (backup) svoje tvrtke, moramo postaviti sljedeća pitanja:

1. Koristi li pružatelj cloud usluge enkripciju za zaštitu naših podataka?
2. Je li kontrola kriptografskog ključa kod nas ili kod pružatelja usluga?
   Jamči li tvrtka sigurnost i dostupnost
3. podataka priznatim certifikatom?
4. Jamči li tvrtka dostupnost podataka
   čak i u slučaju propasti?
5. Ako nas zakon ili ugovor obvezuje da podatke držimo isključivo unutar Republike Hrvatske ili u okviru nekih odabranih zemalja, možemo li takvu uslugu ostvariti?

Vrlo je važno odabrati “cloud” usluge od provjerenog pružatelja jer o njihovoj sigurnosti ovisi naša sigurnost. Danas je moguće vrlo povoljno zakupiti usluge od vrhunskih pružatelja certificiranih od strane neovisnih tijela.

Standarde sigurnosti “cloud” usluga među ostalima postavljaju organizacije CSA (Cloud Security Alliance) i IETF (Internet Engineering Task Force). Izvan tih tijela poznat je certifikat PCI DSS (Payment Card Industry Data Security Standard). Različiti pružatelji usluga imat će različite certifikate, no uvijek provjerite izdaje li ih priznata organizacija.

Izrada sigurnosne politike

Sigurnost tvrtke je lanac osjetljiv na najslabije karike, te manjak dosljednosti u primjeni propisanih sigurnosnih mjera čini ostale postojeće mjere neučinkovitima. Dovoljna je samo jedna radna stanica na kojoj nisu primijenjene aktualne zakrpe da bi napadač tim putem mogao steći privilegije korisnika tog računala.

Dosljednost je najlakše osigurati izradom sigurnosne politike. Radi se o internom dokumentu Vaše tvrtke koji propisuje kriterije i sve aktivnosti o kojima ovisi računalna sigurnost. Sigurnosna politika specificira i načine na koje će se ona provoditi.

Da bismo znali napisati odmjerenu sigurnosnu politiku, prvo moramo imenovati rizike i prijetnje te procijeniti ozbiljnost posljedica sigurnosnih incidenata na poslovanje. Kada smo to učinili, imamo osnovu po kojoj možemo procijeniti ulaganja i stupanj zaštite pojedinih resursa.

Ako tvrtka već radi po ranije ustanovljenoj sigurnosnoj politici i želite napraviti reviziju, u svoj rad uključite i plan prelaska na nov način rada – navike zaposlenih mogu predstavljati problem u prelasku na nove procedure. Vodite računa o edukaciji i kontroli.

Menadžment mora biti upućen u izradu i krajnji oblik sigurnosne politike, razumjeti je te biti spreman dati podršku njenoj provedbi. Ponovit ćemo: sigurnosna politika je učinkovita samo onda kada se provodi dosljedno.

Kako bismo lakše pristupili izradi dokumenta, na raspolaganju su nam već propisani standardi i uobičajena poslovna praksa, koja proizlazi npr. iz ISO/IEC 27000 obitelji standarda. Nije nam nužni cilj standarde zadovoljiti u cijelosti, već iz njih preuzeti dio koji se odnosi na naše poslovanje i koristiti ih kao pomoć u definiranju rješenja.

Jedna od stavki sigurnosne politike treba biti i propisan način i učestalost revizije tog dokumenta kako rješenja ne bi zastarjela i na taj način ometala poslovanje ili izgubila na učinkovitosti. U istom dijelu potrebno je definirati način i učestalost provjere ranjivosti sustava unutar tvrtke.

Sigurnosna politika mora biti prilagođena poslovnim potrebama tvrtke te u njenoj izradi trebaju sudjelovati djelatnici iz više odjela. Treba biti opisan i način prijave i rješavanja incidenata. Odgovornosti nad resursima moraju biti jasno podijeljene kako bi se u slučaju kompromitacije lakše našlo izvorište.

Pristup posebno osjetljivim resursima treba biti opisan u obliku procedura. Način korištenja Interneta i sigurnosni kriteriji trebaju biti jasno opisani i prilagođeni ciljevima poslovanja tvrtke i krajnjim korisnicima (npr. zaposlenicima).

Politika treba izričito zabraniti neovlašteno pristupanje tuđim sustavima, preuzimanje ilegalnog ili nelicenciranog softvera, pokretanje malicioznog softvera te iznošenje privatnih podataka o zaposlenicima i poslovanju na društvenim mrežama.

Postupak u slučaju kršenja pravila politike također u njoj mora biti opisan kako bi se unaprijed moglo osigurati njeno daljnje poštivanje.

Zaštita mreže, usluga, radnih stanica i poslužitelja

Primjena sigurnosne politike ključ je uspješne zaštite računala i mreže Vaše tvrtke. Tehničke mjere koje opisujemo u ovom poglavlju imat će željeni učinak tek uz pretpostavku da se sigurnosna politika dosljedno provodi.

Zaštita radnih stanica i poslužitelja započinje redovitim otklanjanjem poznatih ranjivosti za koje su dostupne zakrpe proizvođača. Redovnom primjenom zakrpa značajno smanjujemo izloženost računala automatiziranim napadima, odnosno robotima koji te ranjivosti aktivno traže. Najizloženija računala ovakvim napadima su poslužitelji javnih usluga (kao što je web), no ranjivost svakog računala u mreži potencijalna je točka rizika.

Radne stanice, računala na kojima Vaši zaposleni svakodnevno obavljaju svoj posao vrlo su osjetljiv dio ukupne IT infrastrukture. Iako se u pravilu nalaze u dijelu mreže izoliranom od pristupa s Interneta, činjenica da radnje na njima iniciraju korisnici otvara velike mogućnosti napadačima. Važno je da sav softver koji dolazi u dodir s vanjskim sadržajima redovito ažurirate: web preglednik, aplikacije za pregled dokumenata (Word, PDF) i naravno, sam operacijski sustav.

Nakon uspostave automatskog ažuriranja softvera, računala je potrebno dodatno zaštititi antivirusnim alatima. S obzirom da se novi malver pojavljuje svake sekunde, presudno je i da antivirusni softver ima kontinuiran i nesmetan pristup Internetu. Također je važno da korisnici prepoznaju ispravan rad antivirusnog alata i razumiju njegova upozorenja; na taj se način mogu obraniti od lažnih antivirusnih alata ili primijetiti kada zaštita nije uključena. Koliko god dobro zaštitili računala, nije mudro pretpostaviti da su ona potpuno sigurna i da do kompromitacije ne može doći. Važno je maksimalno ograničiti što malver može činiti u slučaju da dospije na računalo. To postižete ograničavanjem ovlasti lokalnog korisnika i pristupa računala drugim resursima na mreži.

Sukladno činjenici da potpuna sigurnost ne postoji, sljedeća razina zaštite odnosi se na međusobno izoliranje pojedinih resursa. U prvom redu to činite segmentiranjem mreže – stvaranjem posebnih međusobno odijeljenih cjelina sa strogo kontroliranim pristupom. Uobičajena je praksa javne usluge posluživati iz segmenta nazvanog DMZ (DeMilitarized Zone), kojem je moguće protokolom usluge pristupiti izvana, no unutar kojeg računala nemaju pristup ostatku interne mreže. Imamo li različite usluge koje ne dijele iste resurse ili zbog sigurnosnih razloga moraju biti mrežno odvojene, moguće je definirati i više takvih zona.

Zadaću dijeljenja mreže u tehničkom smislu mogu obavljati za to specijalizirani uređaji. Gotovo svaki moderni samostojeći vatrozid dolazi s više mrežnih sučelja koja se mogu definirati na način primjeren ovoj namjeni. Istovremeno, uređaj obavlja filtriranje i inspekciju sveg prometa koji kroz njega prolazi.

Klasičan vatrozid omogućava filtriranje prometa na razini TCP/IP protokola, no mnogi moderni, NG (Next Generation) vatrozidi mogu interpretirati i protokole na aplikacijskoj razini te aktivno uklanjati maliciozan promet.

Neki mrežni uređaji omogućavaju i kontrolu brzine protoka podataka ovisno o usluzi i korisniku, tako da je na taj način moguće ograničiti usluge koje ometaju poslovno važnije procese.

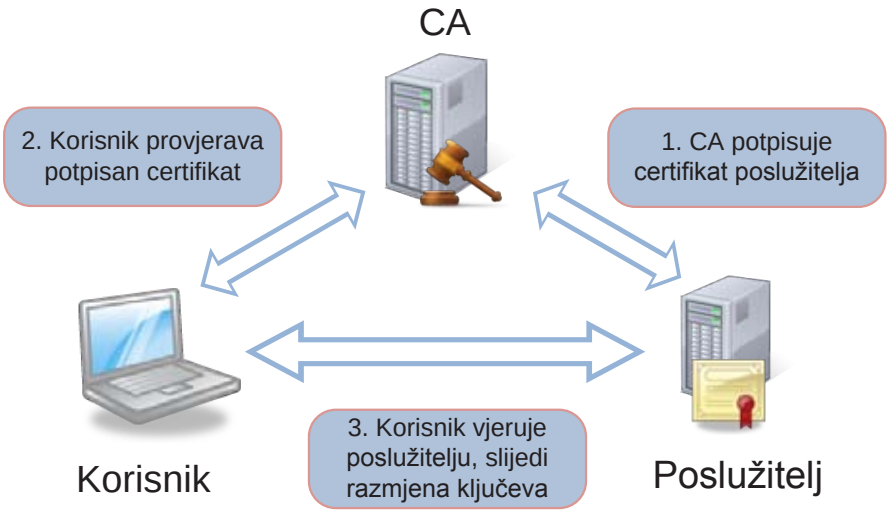
Neke usluge koje javno poslužujemo mogu imati različite zadaće u internoj mreži i izvan nje, na Internetu. Na primjer, poslužitelj elektroničke pošte na javnoj mreži ne mora pohranjivati primljenu poštu niti je činiti dostupnom internim korisnicima, već to može obavljati drugi, bolje zaštićeni poslužitelj. Na sličan način, javni DNS poslužitelj ne mora korisnicima s Interneta odavati imena i IP adrese internih računala. Takav dizajn zovemo split DNS.

Kao još jedan primjer ovakve arhitekture, web poslužitelj možemo zaštititi tako da ispred njega postavimo reverse proxy: poslužitelj koji dostupnim čini samo javni dio web aplikacije te sâm nema pristupa bitnim drugim resursima, kao što je interna baza podataka.

Veći dio malicioznog prometa s kojim se susrećemo ima prepoznatljive karakteristike. Postoje uređaji i softver čija je zadaća prepoznati ih. Ako je funkcija uređaja samo obavijestiti nas o takvim događajima, uređaj se zove IDS (Intrusion Detection System). Ako pak istovremeno uklanja sporan promet, zovemo ga IPS (Intrusion Prevention System).

Razmjena povjerljivih podataka s drugim računalima na Internetu ponekad je nužnost. Kada to činimo, podatke šaljemo kroz javnu mrežu i riskiramo mogućnost da ih netko na njihovom putu prikupi. Takav napad zove se Man in the Middle i možemo ga efikasno onemogućiti korištenjem enkripcije. Sva razmjena povjerljivih podataka trebala bi se obavljati SSL ili nekim drugim protokolom koji podržava enkripciju podataka u prometu.

SSL je široko prihvaćen protokol čije implementacije obuhvaćaju ključne elemente sigurnosti razmjene podataka: povjerljivost, cjelovitost, autentičnost i neporecivost. Ove četiri karakteristike osigurane su korištenjem asimetrične enkripcije (PKI). Certifikati potpisani od strane organizacije od povjerenja garantiraju nam identitet poslužitelja s kojim komuniciramo, a asimetrični algoritam rješava problem razmjene kriptografskog ključa.



SSL omogućava administrativni pristup poslužiteljima uz korištenje certifikata umjesto lozinki. Korištenje certifikata u praksi se pokazuje kao bolja metoda u usporedbi s lozinkama, jer je za pristup tajnom ključu na lokalnom računalu često potrebno značajno više truda nego za otkrivanje lozinke.

Sigurnost računala ne odnosi se samo na mogućnost njihove kompromitacije. Pod tim pojmom podrazumijevamo i dostupnost ključnih resursa o kojima Vaše poslovanje ovisi. Za usluge koje javno poslužujete važno je unaprijed procijeniti i opisati prihvatljivo vrijeme nedostupnosti u slučaju incidenta, bez obzira radilo se o kvaru ili nekom drugom problemu. Jednom kada ste definirali što je za Vas prihvatljivo vrijeme nedostupnosti, možete sukladno tome izraditi plan prevencije i postupanja u slučaju da se kvar dogodi.

Prevenciju nedostupnosti usluge ostvarujemo postavljanjem zamjenskog poslužitelja i uspostavom plana stavljanja tog zamjenskog poslužitelja u rad. Potrebno je također implementirati i redundantno mrežno-sigurnosno rješenje vezano uz uslugu. Kada dostupnost usluge nije kritična, dovoljno je imati spremno zamjensko računalo i pričuvnu kopiju – kroz nekoliko sati posluživanje će se nastaviti. No ako je usluga kritična, prelazak na drugo računalo mora biti obavljen brzo i automatski – što znači da drugo računalo čitavo vrijeme mora biti spremno za rad. Takvo računalo zovemo redundantnim poslužiteljem, jer u svakodnevnim uvjetima ne obavlja korisnu zadaću. Automatsko prebacivanje posluživanja s računala u kvaru na zamjensko zovemo failover.

Moguće je uspostaviti arhitekturu u kojoj dva poslužitelja istovremeno poslužuju istu uslugu te raspoređuju posao među sobom – load balancing (eng. uravnoteživanje opterećenja). U tom slučaju ispad jednog od njih ne prekida dostupnost već samo ograničava performanse. Razmislite koja od navedenih arhitektura najbolje osigurava Vaše ciljeve.

Računalna oprema koja dijeli lokaciju ili priključak na električnu energiju također dijeli i neke rizike. Razmislite o scenariju u kojem je Vaše poslovanje prekinuto zbog nekog događaja koji istovremeno onesposobljava Vašu glavnu i redundantnu opremu. Podatke možete zaštititi povremenim pohranjivanjem pričuvnih kopija na drugu sigurnu lokaciju (fizičku ili na Internetu, npr. u oblaku). Nakon toga, ponovna uspostava usluga mora slijediti prioritete Vašeg poslovanja: kritične usluge bez kojih poslovanje nije moguće morate moći uspostaviti u kratkom vremenu i to tako da one mogu funkcionirati bez svih dodatnih resursa koje ste izgubili. Takav plan nazivamo Disaster Recovery.

Tehnička rješenja koja se navode u ovom poglavlju sa sobom nose izdatke koji su možda preveliki za Vaš budžet. Jedna od mogućnosti koja Vam se uz neke kompromise pruža je korištenje SecaaS (Security as a Service) usluga. Te usluge uglavnom pokrivaju promet elektroničke pošte i pristup Vaših računala webu i to tako da se filtriranje obavlja na udaljenim računalima pružatelja usluge. Na taj način smanjujete ukupan Internet promet te možete koristiti manje fizičkih poslužitelja unutar vlastite mreže. SecaaS doduše ne može zaštititi specifične web aplikacije Vaše tvrtke ni spriječiti socijalni inženjering.

Osnove sigurnosti web poslužitelja

Web Vaše tvrtke konstantno je izložen pokušajima kompromitiranja, bez obzira nalazi li se poslužitelj unutar Vaše mreže ili koristite hosting uslugu. Svaka web aplikacija izložena je napadima na više razina:

- Operacijski sustav
- Web poslužitelj
- Web aplikacija

Ranjivost na bilo kojoj od ovih razina može napadaču omogućiti neovlašten pristup. Ako koristite hosting, pružatelj usluge preuzima brigu o prve dvije razine, no sigurnost web aplikacije ostaje na vama. Koristite li pak neku od gotovih web aplikacija, dio odgovornosti je i dalje na Vama, jer morate redovito primjenjivati zakrpe te slijediti sigurnosne preporuke kao što je korištenje dovoljno složenih lozinki.

Razvijate li svoju web aplikaciju, sigurnost je stavka koju razvojni inženjeri moraju uzeti u obzir od samog početka projekta. Naknadno ugrađivanje sigurnosnih mjera kao da se radi o dodatnom modulu softvera gotovo sigurno neće rezultirati dobrim rješenjem. U razvojnom timu važno je imati osobu koja je stručna u području sigurnosti web aplikacija te joj dati položaj u timu koji osigurava provedbu dizajna koji preporučuje.

Osim što je aplikaciju potrebno od početka osmisliti vodeći računa o sigurnosti, daljnji kontinuirani razvoj mora uključivati korak provjere očuvanja uspostavljene razine zaštite. Također je važno povremeno provjeravati sigurnost aplikacije korištenjem specijaliziranih alata za provjeru ranjivosti ili revizijom stručne osobe.

Provjeru ranjivosti moguće je izvesti iz pozicije korisnika usluge u realnom scenariju. Na taj način ocijenit će se stvarna mogućnost iskorištenja poznatih ranjivosti od strane vanjskog napadača, ali samo uz pretpostavku da se napadač koristi unaprijed poznatim metodama.

Ovakvu uslugu nudi i Nacionalni CERT na web stranici
http://www.cert.hr/provjera_ranjivosti

Detaljniju provjeru moguće je napraviti korištenjem istih alata, ali uz puni pristup poslužitelju, bez ikakve zaštite koja bi filtrirala promet. Na taj način možemo otkriti ranjivosti koje možda nisu na jednostavan način iskoristive s javne mreže, no koje bi napadač uz više truda ipak mogao zloupotrijebiti. Te provjere poželjno je obaviti prije puštanja usluge u javnost te za njih i eventualne ispravke uračunati vrijeme.

Nakon provjere i uspostave usluge, web aplikaciju moguće je dodatno zaštititi specijaliziranim vatrozidom. Vatrozide ove namjene zovemo WAF (Web Application Firewall). Ti uređaji omogućavaju nam ograničavanje komunikacije web korisnika s našim poslužiteljem unutar okvira predviđenog normalnim radom web aplikacije te preventivno filtriranje poznatog malicioznog prometa.

Najčešće sigurnosne propuste u izradi web aplikacija možete unaprijed izbjeći ako ih u fazi razvoja imate na umu:

- Lozinke korisnika moraju u bazi biti jednosmjerno kriptirane (hashing) uz korištenje aktualnog algoritma i dodatnog slučajnog podatka (salt).
- Sve prosljeđivanje parametara od korisnika ka aplikaciji mora biti ograničeno na skup vrijednosti koji je za tu namjenu predviđen, posebno s obzirom na duljinu
- Parametri koje zadaje korisnik ne smiju izravno utjecati na učitavanje dodatnog koda ili preuzimanje datoteka/zadataka s datotečnog sustava ili iz vanjskih izvora
- Parametri koje aplikacija prosljeđuje bazi podataka moraju proći kroz algoritam za uklanjanje/kodiranje specijalnih znakova
- Struktura direktorija mora biti zaštićena od pisanja, a tamo gdje to mora biti omogućeno zaštićena od izvršavanja koda

Mobilni pristup internim računalima putem Interneta

Zaposlenici mnogih tvrtki danas obavljaju dio svojih zadataka van ureda. Pri tome koriste prijenosna računala, pametne telefone ili web aplikacije. U ovom se poglavlju posvećujemo pristupu internoj mreži putem Interneta i to s računala koje je zaposlenicima ustupila tvrtka (prijenosnicima i pametnim telefonima). Naša je preporuka da se internoj mreži ne pristupa s privatnih računala jer u tom slučaju tvrtka ne može adekvatno provoditi sigurnosnu politiku.

Čim računalo izađe iz tvrtke, podaci na njemu izloženi su dodatnim rizicima. Najjednostavniji primjer je krađa, u kojem slučaju su svi podaci na računalu i sve što se s njega može činiti bez autentikacije dostupni kradljivcu. Podatke je od tog rizika moguće zaštititi enkripcijom: korištenjem enkripcije direktorija ugrađene u operativni sustav ili hardverske enkripcije dostupne na nekim modelima prijenosnih računala.

Podatke je nužno zaštititi i na prijenosnim medijima kao što su USB memorije.

Za pristup internoj mreži svakako treba koristiti enkripciju i dvostruku autentikaciju. Poželjno je korištenje neke od VPN (Virtual Private Networking) tehnologija te za autentikaciju koristiti digitalni certifikat te po mogućnosti jednokratnu lozinku. Segment mreže u koji korisnik dolazi kroz VPN također je potrebno ograničiti tako da su u njemu moguće samo radnje koje su udaljenim korisnicima zaista nužne. Preporučamo da je spajanje u VPN samo "predvorje" pristupa štićenim resursima te da se za daljnji pristup konkretnim štićenim računalima i resursima treba koristiti dodatna autentikacija.

Uz sve ove razine zaštite, prijenosno računalo i dalje predstavlja rizik, pogotovo zbog dolaska u doticaj s nezaštićenim mrežama i većom izloženošću malveru. Dobar način ograničavanja štete u slučaju kompromitacije je korištenje virtualnog računala čije se stanje nakon korištenja vraća na početne postavke. Za takva virtualna računala potrebno je uspostaviti proceduru ažuriranja virtualnog operativnog sustava te preuzimanje ažurirane inačice na prijenosna računala prije iznošenja s radnog mjesta.

Zaključak

Unatoč prijetnjama kojima je suvremena tvrtka danas izložena na Internetu moguće je rizik koji one donose svesti na poslovno prihvatljivu razinu. Rješenja za većinu poznatih problema sigurnosni stručnjaci već znaju.

Važno je razumjeti da sigurnost kao gotov proizvod ne postoji. Povremen ili stalan nadzor kvalificirane osobe je nužan kako biste uopće mogli osvijestiti rizike i ispravno odlučiti. Također, bez provedivih i zapisanih pravila ponašanja (sigurnosne politike), većina tehničkih mjera „pada u vodu". Netko se treba sjetiti promijeniti lozinke nakon odlaska zaposlenika.

Da je knjižica koju držite u rukama dvije godine starija, velik dio teksta bio bi drugačiji. Postoje načini razmišljanja i tehnička pravila koja u sigurnosti uvijek vrijede, no prijetnje i dostupna rješenja stalno se mjenjaju.

O sigurnosnim problemima najviše smisla ima brinuti prije nego što se dogode. To je jedini trenutak u kojem je moguće izbjeći štetu.

Nacionalni CERT

Pojmovnik

bot – vrsta malvera specijalizirana za izvršavanje zadataka primljenih s udaljene lokacije

botnet – više računala na kojima je aktivan bot povezana u koordiniranu mrežu

certifikat – kriptografski dokument kojim se garantira identitet računala s kojim komuniciramo

command & control (C&C) – računalo na kojem se nalazi softver za prosljeđivanje zadataka zombie računalima

crimeware – oblik malvera specijaliziran za kriminalne aktivnosti

(D)DoS – (Distributed) Denial of Service – napad iz jednog ili više (Distributed) izvora čija je posljedica uskraćivanje usluge ostalim korisnicima

DMZ – DeMilitarized Zone – mrežni segment u koji smještamo javne poslužitelje; vidi stranica 19

failover – vidi stranica 22

fast-flux – vidi stranica 2

IDS – Intrusion Detection System vidi stranica 20

IPS – Intrusion Prevention System vidi stranica 20)

malver – općeniti naziv za zlonamjeran softver

phishing – vidi stranica 11

SSL – Secure Sockets Layer – vidi stranica 20

redundancija – vidi stranica 22

rootkit – vidi stranica 11

SecaaS – Security as a Service (sigurnost kao usluga) – vidi stranica 22

VPN – Virtual Private Network – tehnologija povezivanja udaljenih mreža u jednu cjelinu kriptografskom komunikacijom putem Interneta

WAF – Web Application Firewall – vidi stranica 24

zombie računalo – računalo zaraženo malverom koje izvršava zadatke upućene iz kontrolnog centra

Izdavač: 24 sata d.o.o., Oreškovićeva 6H/1, Zagreb, tel: 01/6326 000, fax: 01/6362 060, e-mail: redakcija@poslovni.hr; **Tisak:** Tiskara Vjesnik, Slavonska avenija 4, Zagreb