(n)eVarnost

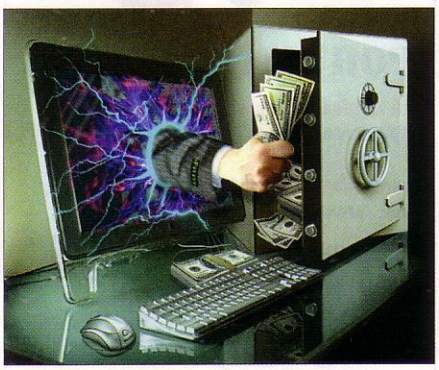
Ukradli so mi identiteto?!

..Koliko škode nam v resnici lahko povzroči ukradeno osebno geslo ter kako se pripraviti na najhujše? Kako zaščititi tehnologijo pred krajo, podatke pa pred zlorabo?..

Najbolj pogoste varnostne luknje

Danes uporabljamo računalnike vsak dan za najrazličnejša opravila – za delo, za upravljanje financ, za iskanje prostih delovnih mest, za nakupovanje in celo za spoznavanje novih ljudi. Medtem ko brezskrbno dan za dnem deskamo po svetovnem spletu, na nas skrivoma preži na milijone spletnih kriminalcev. Medtem ko so jih še pred nekaj leti »gnali« motivacija, dokazovanje in politična opredelitev, je danes zgodba povsem drugačna. Velika večina spletnih kriminalcev ima namreč pogosto en sam cilj: čim hitreje obogateti.

Ker je naš računalnik priključen na internet, nas lovke spletnega kriminala lahko kaj hitro ujamejo. Manjša nepazljivosti in klik na napačno priponko sta namreč že dovolj, da v trenutku ostanemo brez denarja, pomembnih dokumentov ali celo osebnih podatkov. Te za nameček lahko kriminalci uporabijo celo za izvajanje najhujših oblik kriminala – od prevar do umorov in ugrabitev. Zagotovo mislite, da je možnost, da postanete žrtev spletnega kriminala izredno majhna. Če sodite po tem, da internet danes uporablja že več kot dve milijardi ljudi, morda res. Če pa gledate na to iz vidika, da se spletni kriminalci zadržujejo predvsem na mestih, kjer smo tudi mi največ prisotni (na primer družabna omrežja), potem se ta možnost precej poveča. Pri tem se morate seveda vedno zavedati tega, da vam ena napaka lahko za zmeraj spremeni življenje.



Zaradi ene nepazljivosti lahko ostanemo brez vsega!

Najboljša obramba pred spletnim kriminalom je seveda ozaveščenost. Bolj kot poznamo nevarnosti, ki nam prežijo na svetovnem spletu, manjša je možnost, da se bomo ujeli v past. Spletni prevaranti, tatovi in drugi nepridipravi imajo namreč zelo bujno domišljijo in veliko zelo posrečenih idej, kako brez veliko truda priti do tujega denarja. V nadaljevanju si zato poglejmo ključne grožnje, ki nam trenutno prežijo na svetovnem spletu.

Elektronska pošta

Elektronska pošta je med nami prisotna že dolgih 40 let. Ker skoraj vsak računalničar uporablja elektronski poštni predal, ne preseneča, da je še vedno izjemno priljubljena med spletnimi kriminalci. Ker je veliko računalničarjev naivnih in ne razmišlja preveč o tem, kaj počnejo, ko odpirajo priponke ali klikajo na povezave v elektronski pošti, je ta vrsta »napada« še vedno izjemno uspešna. Medtem ko so v preteklosti kriminalci prevzeli nadzor nad računalnikom s pomočjo okuženih datotek, danes prevladuje napad na ljudi. Med njimi najdemo tako lažje »kopije« spletnih strani (na primer spletnega bančništva) kot razne nagradne igre, ker nam vedno obljubljajo bajne vsote denarja. Kaj storiti? Preprosto. Ne odpirajmo vseh prilog in ne klikajmo na vse povezave znancev ali neznancev, če ne vemo, zakaj smo jih prejeli. Poleg tega imejmo posodobljen operacijski sistem in programsko opremo ter nameščen kakovosten protivirusni program oziroma celovito zaščito pred računalniško nesnago.

Elektronska pošta je kot nalašč za napad na nevešče uporabnike.

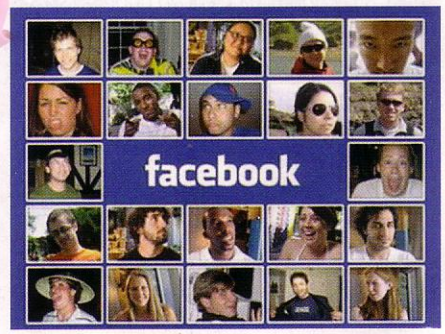
Pornografske, hekerske in piratske spletne strani

Pornografske, hekerske in piratske spletne strani so zelo dobro obiskane. Zaradi tega nepridipravi na teh mestih spretno podtikajo okuženo programsko opremo. Ob pogledu na nagce in nagice, napredna hekerska orodja in brezplačno programsko opremo smo namreč veliko manj pozorni na to, kaj in kako klikamo po takšnih straneh in kakšne vrste datotek s tem zaženemo. Take spletne strani imajo pogosto vgrajeno tako škodljivo programsko kodo, ki se samodejno zažene že ob samem obisku spletne strani. Na kaj moramo tu paziti? Predvsem na to, da ne klikamo nepremišljeno, ko se nam pri poskusu predvajanja kakega videoposnetka pojavi zahteva po namestitvi dodatnega programa ali kodeka. Pozorni moramo biti tudi v primeru, da nas spletna stran želi preusmeriti na drugo stran. Tudi pojav neželenih oken po vsej verjetnosti kaže na to, da stran ni varna. Ker ni zagotovil, da se na teh straneh kljub previdnosti ne boste okužili, vam priporočamo, da se jih izogibate, koliko se le da.

Pornografske, hekerske in piratske spletne strani so pravo leglo škodljivih programskih kod.

Družbena omrežja

Danes družbena omrežja uporablja že skoraj milijarda uporabnikov. Ker je med njimi veliko takih, ki nimajo niti osnovnega znanja s področja informacijske varnosti, so ta pravi raj za spletne kriminalce. Razlog za to tiči predvsem v tem, da je tu komunikacija zelo osebna in vsebuje visoko stopnjo medsebojnega zaupanja. Ko prejmemo sporočilo na svoj profil, je to precej drugače, kot če prejmemo anonimno sporočilo prek ele-



Uporabniki družbenih omrežij pogosto preveč zaupajo nepoznanim sogovornikom.

ktronske pošte ali nezaželeno sporočilo. In ravno to je tisto, kar spletni kriminalci s pridom izkoriščajo. Spletni kriminalci uporabnike poskušajo pretentati s povezavami na okužene spletne strani, z lažnimi videoposnetki, datotekami in podobno. Nekateri gredo še tako daleč, da si ustvarijo lažen profil, pridobijo naše zaupanje in od nas skozi pogovor poskušajo izvleči podatke zaupne narave, kot so domači naslov, telefonska številka, geslo in podobno. Ti napadi so zelo učinkoviti in jih je zelo težko odkriti. Več o tem, kako jih prepoznati in kako ravnati, bomo spregovorili v nadaljevanju.

Druge spletne nevarnosti

Na svetovnem spletu preži toliko nevarnosti, kolikor je spletnih kriminalcev. Spletni prevaranti, tatovi in drugi nepridipravi imajo namreč zelo bujno domišljijo. Ti nas namreč poskušajo pretentati še z okrajšanimi spletnimi naslovi, škodljivimi kodeki, ponarejenimi rezultati iskanja, lažnimi videopredvajalniki, lažnimi aplikacijami za družabno omrežje Facebook, lažnimi protivirusnimi programi, lažnimi opozorili in še bi lahko naštevali. Zaradi tega je zelo priporočljivo, da imamo, poleg osnovnega znanja s področja računalniškega kriminala, na računalniku nameščeno celovito zaščito pred spletnimi grožnjami. Ta nam bo pomagala obiti marsikatero čer pri deskanju po svetovnem spletu. V nadaljevanju si zato poglejmo, katera programska zaščita nam tu lahko priskoči na pomoč.

Programska zaščita pred spletnimi grožnjami

Protivirusna zaščita

Protivirusna zaščita je namenjena predvsem tistim, ki neradi raziskujejo po svetovnem spletu in so dovolj spretni pri prepoznavanju spletnih groženj. Ta namreč nudi zaščito le pred škodljivimi programskimi kodami kot so trojanski konji, računalniški virusi, vohunski programi in podobne. Protivirusna zaščita nas varuje tako pred nevarnostmi na svetovnem spletu kot tistimi, ki so skriti v priponkah oziroma datotekah. Maloprodajne cene komercialnih protivirusnih programov, kot so F-Secure, Nod32, Panda in drugi, se pri nas gibljejo okoli 40 evrov. Na voljo imamo seveda tudi brezplačne (Avast, Comodo AVG in druge). Brez protivirusne zaščite se načeloma da preživeti, vendar moramo biti pri deskanju po svetovnem spletu zelo previdni. Da pri tem ne govorimo o priponkah v e-sporočilih. Če ste se že odločili tvegati, vam priporočamo, da si računalnik enkrat tedensko »pregledate« z oblačnimi protivirusniki, kot je na primer Panda Cloud Antivirus (http://goo.gl/9Bza).

Celovita zaščita pred spletnimi grožnjami

Programske opreme, ki nudijo celovito zaščito pred spletnimi grožnjami, se pogosto imenujejo Internet Security. Te nam poleg protivirusne zaščite nudijo še zaščito pri brskanju po spletnih straneh. Funkcija zaščite brskanja nam namreč jasno sporoči, katere spletne strani so varne in katerih se je bolje izogniti. Zlonamerne spletne

Celovita zaščita nas obvaruje pred številnimi spletnimi nevšečnostmi.

strani so pogosto blokirane samodejno. Zraven je ponavadi na voljo še požarni zid in starševski nadzor, ki otroke varuje pred neprimerno spletno vsebino. Zaradi dodatnih funkcionalnosti so te rešitve nekoliko dražje. Maloprodajne cene komercialnih celovitih varnostnih rešitev, kot so F-Secure, Nod32, Panda in druge, se pri nas gibljejo okoli 55 evrov (cene se močno razlikujejo med različnimi proizvajalci).

Plačljiva ali brezplačna zaščita?

Če potrebujete popolno zaščito pred spletnimi nevarnostmi, ni dileme, saj tu prevladujejo plačljive rešitve. Pri protivirusnih rešitvah pa je slika nekoliko drugačna. Če gre verjeti najnovejši raziskavi neodvisne spletne strani Virus Bulletin VB100 (http://goo.gl/eUWQl), so brezplačne protivirusne rešitve povsem enakovredne plačljivim. Med vodilnimi brezplačnimi rešitvami najdemo Avast! in Aviro. Med plačljivimi pa vodilna mesta zavzemajo BitDefender, F-secure, G Data in še kdo bi se našel. Če menite, da polne zaščite pred spletnimi nevarnostmi ne potrebujete, vam priporočamo, da si namestite vsaj brezplačno protivirusno rešitev.

Ranljivost operacijskih sistemov

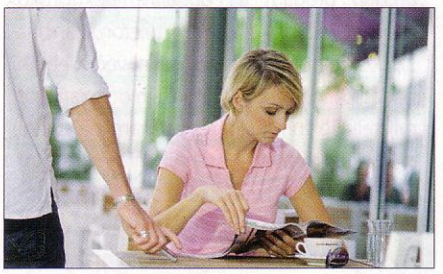
Vsi operacijski sistemi, brez izjeme, so ranljivi. Pri več milijonih vrstic je namreč že tako rekoč samoumevno, da bodo programerji naredili kakšno napako. Koliko teh napak pa bodo kriminalci odkrili in jih zlorabili za nelegalno pridobitev dostopa do naših podatkov, je pač odvisno od tega, koliko potencialnih žrtev uporablja nek operacijski sistem.

Klasični operacijski sistemi

Ker danes več kot 88 odstotkov računalničarjev uporablja operacijski sistem Windows, spletni kriminalci zanj skoraj vsako minuto pripravijo novo škodljivo programsko kodo. V zadnjem času med spletnimi kriminalci močno pridobiva na priljubljenosti Applov operacijski sistem MacOS. Tega namreč že uporablja skoraj vsak deseti računalničar. Zato ne preseneča, da vse več programskih hiš zanj pripravlja celovite protivirusne zaščite. Linux je prav tako ranljiv, vendar se tu napadalci usmerjajo na področje strežniških sistemov. Kljub temu je pogosto predvsem od nas uporabnikov odvisno, ali nas bodo spletni kriminalci pretentali. Ti nas namreč ne bodo poskušali le okužiti s škodljivimi kodami, ampak bodo od nas želeli pridobiti podatke zaupne narave kot so številka kreditne kartice, domači naslov, uporabniško ime in geslo in podobno. To pa bodo pridobili tako, da nas bodo preusmerili na lažno spletno stran ali preko pogovora na družbenih omrežjih. Varnost torej še zdaleč ni odvisna le od operacijskega sistema in varnostne opreme, ki je na njem nameščena.

Mobilni operacijski sistemi

Ker vse več uporabnikov za dostop do interneta uporablja mobilne naprave, so se kriminalci seveda temu prilagodili. Trenutno je najbolj priljubljena tarča mobilni operacijski sistem Android, saj povpraševanje po mobilnih napravah, opremljenih z njih, strmo narašča. Že večkrat se je celo zgodilo, da so strokovnjaki za varnost odkrili okuženo programsko opremo kar na porta-



Mobilne naprave so lahka tarča za uličnе nepridiprave.

lu Android Market. Tu gre za precej nevarne škodljive programske kode, katerih namen je predvsem kraja podatkov, vsebin kratkih sporočil SMS, prisluškovanje pogovorom in podobno. To sicer ne velja za Applov operacijski sistem iOS (mobilnik iPhone in tablica iPad), saj so aplikacije, preden so objavljene na portalu iTunes, preverjene s strani Applovih programerjev. Izven tega portala pa je zgodba povsem drugačna. Na spletu namreč najdemo kar veliko programov, ki so okuženi s škodljivimi kodami. Predvsem gre tu za programe, ki so namenjeni odklepanju. Tu sicer velja poudariti, da so tako pri Androidu kot pri iOSu škodljivim kodam najbolj izpostavljeni tisti, ki imajo tako imenovane »super pravice«. Tu imajo namreč škodljive kode neposreden dostop do »jedra« sistema. Zaradi

Marko Malovrh, direktor, Sismentor d. o. o.

Za dostop do različnih storitev, ki nam jih nudi ITK tehnologija, potrebujemo uporabniško ime in geslo. Dobro geslo je sestavljeno iz vsaj desetih črk in številk ter posebnih znakov. Ker si je taka gesla težko zapomniti, ljudje pogosto za več storitev uporabljajo isto geslo. Še več: povprečno geslo je dolgo 6 znakov, običajno je povezano z dejstvi iz uporabnikovega življenja (imena otrok, rojstni datumi, imena hišnih ljubljenčkov, naslovi ipd.), te informacije pa uporabniki delijo z »znanci« na socialnih omrežjih, kar lahko ugotavljanje gesla še poenostavi.

S poznavanjem uporabniškega imena in gesla lahko pridobimo dostop do računalniškega sistema, računalniškega omrežja, zaupnih informacij, elektronske pošte, elektronskega bančništva, ...

Izgubo gesla bi v vsakodnevnem življenju lahko primerjali z izgubo ključa vhodnih vrat. Nepošten najditelj, ki ve, kje stanujemo, lahko ključ uporabi za vstop v stanovanje, pridobitev npr. ključev našega avtomobila, bančnih kartic, drugih dragocenosti, ...

Nekaj priporočil za »domače« uporabnike: preden prodam ali podarim elektronsko napravo (računalnik, mobilni telefon, dlančnik ...), poskrbim za to, da na njih ni več osebnih podatkov, na socialnih omrežjih dodajam kot prijatelje le ljudi, ki jih res poznam, na spletu ne razkrivam preveč osebnih informacij). Kot vodilo lahko služi misel, kako bi se na tako ponudbo odzvali v »realnem« življenju?

Podjetja lahko odtok gesel/informacij preprečijo z ustrezno varnostno politiko, izobraževanjem uporabnikov ter s programskimi orodji, ki so na voljo.

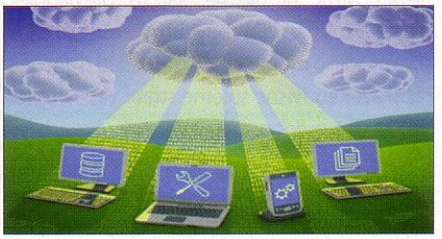
tega se vse bolj priporoča, da se tudi na mobilno napravo namesti ustrezno varnostno rešitev. Te je vsaj za operacijski sistem Android na voljo izjemno veliko (na primer AVG Antivirus, Lookout Security & Antivirus, GuardX Antivirus, Zoner AntiVirus Free in še mnogo več). Seveda tudi tu varnost ni odvisna le od operacijskega sistema in varnostne opreme, ki je na njem nameščena.

Kje so podatki bolj varni

Danes lahko naše podatke hranimo na številnih mestih. Lahko jih imamo shranjene na lokalnem diskovju, pomnilniškem ključku USB ali zunanjem disku, strežniku in celo v oblaku. Verjetno ste se že večkrat vprašali, kje so naši podatki najbolj varni? Ker največ nevarnosti preži na svetovnem spletu, bi lahko rekli, da so naši podatki najbolj varni na pomnilniškem ključku USB in zunanjem disku, ko ta dva seveda nista priključena v računalniški sistem. Če jih prenašamo naokrog, je seveda podatke pametno imeti šifrirane. Tak način shranjevanja podatkov se seveda priporoča predvsem za podatke občutljive narave, ki jih ne potrebujemo pri vsakdanjem delu.

Varnost podatkov na osebnem računalniku in strežniku je v največji meri seveda odvisna od skrbnika sistema. Več kot je ta strokovno podkovan (tudi s področja varovanja informacij), večja je verjetnost, da bodo podatki ostali na varnem. Za kritične dokumente in prenosne naprave se seveda tudi tu priporoča uporaba šifrirnih mehanizmov. Žal tudi hranjenje podatkov na osebnih računalnikih in strežnikih ni več primerno iz praktičnega stališča, saj je narava dela postala taka, da podatke potrebujemo tudi takrat, ko smo na poti. Poleg tega morajo biti ti na voljo kjerkoli in kadarkoli. Ker vzdrževanje takih sistemov zahteva veliko denarja, časa in znanja, se vse več posameznikov in podjetij odloča za hranjenje podatkov v oblakih.

Računalništvo v oblaku (angl. cloud computing) podjetjem in posameznikom nudi prilagodljivo alternativo nakupu aplikacij, storitev in infrastrukture. Tu uporabnik najame prostor glede na trenutne potrebe, ki so lahko tudi povsem



Oblak je relativno varno mesto za hranjenje naših podatkov.

nepričakovane. Ko kapacitet ne potrebuje več, jih lahko preprosto sprosti. Na svetovnem spletu najdemo bogato paleto ponudnikov oblačnih storitev za shranjevanje podatkov, in sicer Dropbox, Fabasoft, ADrive, SugarSync, OpenDrive in še bi lahko naštevali. Kratek pregled desetih najboljših ponudnikov tovrstnih storitev je na voljo na spletnem naslovu http://goo.gl/GMdu. Cene za najem prostora so relativno ugodne (na primer preračunanih 180 evrov za letni najem 250 GB prostora).

Kljub temu, da so cene najema »oblačnega prostora« relativno zelo ugodne in so ti sistemi praviloma zelo zanesljivi, moramo vseeno sami poskrbeti za varnost naših podatkov. Priporočamo vam, da si vedno naredite kopijo vaših podatkov na računalnik ali zunanji trdi disk. Če bo ponudnik oblačnih storitev prenehal s ponujanjem storitve ali bo zaradi napake izgubil vse naše podatke (to se je mimogrede že večkrat zgodilo – na primer podjetju Vodafone), bomo podatke še vedno imeli na voljo. Tu lahko uporabimo zunanji trdi disk CloudBox podjetja LaCie, ki podatke shranjuje tako na lokalni ravni kot strežniku v oblaku. Ker ni nikakršnega zagotovila, da zaposleni pri ponudniku oblačnih storitev ne pregledujejo vsebine datotek svojih strank ali te izročajo organom pregona na zahtevo (to je mimogrede v ZDA obvezno), vam priporočamo, da vse pomembne podatke šifrirate. Za to lahko uporabite brezplačno programsko orodje TrueCrypt (http://goo.gl/1K9r). Geslo naj bo dolgo vsaj 23 znakov. Če boste na oblačni prostor shranjevali osebne podatke, pazite, da se ti hranijo znotraj meja Evropske unije in da ponudnik ustrezno skrbi za varovanje informacij (npr. standard 27001:2005). V nasprotnem primeru vas utegne doleteti zelo visoka kazen s strani našega informacijskega pooblaščenca.

Varnost arhiviranja podatkov in podatkovnih centrov

Kot smo lahko že predhodno spoznali, je varnost podatkov zelo pomembna. Zamislite si samo, kaj bi se zgodilo, če bi v trenutku izgubili vse vaše podatke. Žal to ni nemogoče, saj za izgubo podatkov pogosto zadošča le okvara strojne in programske opreme ali človeška napaka. Če nismo povsem prepričani, da to lahko počnemo v lastni režiji (to velja predvsem za podjetja), bo bolje, če to zaupamo zunanjim pogodbenim podjetjem. Ti bodo namreč poskrbeli za ustrezno in cenovno ugodno arhiviranje podatkov. Pri tem je pomembno, da tovrstno podjetje jamči za nespremenljivost ter varnost shranjenih elektronskih dokumentov oziroma podatkov in tudi omejuje vsakršen nepooblaščen dostop do teh dokumentov. Zato je zelo pomembno, da preden podatke nekomu zaupamo, preverimo njegovo »zanesljivost« (na primer z zunanjo revizijo). Zanesljivost lahko podjetje dokazuje tudi z ustreznimi standardi (na primer 27001:2005).

Podjetje, ki se ukvarja s hranjenjem podatkov, mora imeti seveda na voljo poseben prostor. Ta mora zadostovati protivlomnim, protipotresnim in tudi protipožarnim ter protipoplavnim kriteri-

Naše podatke zaupajmo le preverjenim ponudnikom storitev zunanjega izvajanja!

jem. Pogosto se podjetja odločijo kar za posebne varne prostore v obliki kontejnerjev, ki jih je mogoče postaviti v poljuben prostor, zanje pa proizvajalec jamči odpornost na vse mogoče neugodne vplive. Dobra praksa veleva, da ima podjetje še rezervno lokacijo (ali dve) v primeru večjih katastrof (rušilni potres, naravne nesreče večjega obsega in podobno). Tu so seveda v največji prednosti ponudniki storitev računalništva v oblaku, saj ti imajo strežnike razpršene tako rekoč povsod po svetu in imajo na voljo najizkušenejše strokovnjake (na primer Google). Kljub temu ne smemo zanemariti človeškega faktorja. Varne sobe postanejo brez vrednosti, če bodo do podatkov nepooblaščeno dostopali ali jih celo posredovali tretjim osebam ravno zaposleni. Zato podjetja, ki se ukvarjajo z arhiviranjem podatkov, zaposlene varnostno preverijo pred nastopom službe in tudi še po zaposlitvi. Tudi tu se zato priporoča, da podjetje to skladnost dokazuje z ustreznimi standardi (npr. 27001:2005). Dokazovanje skladnosti lahko preverimo tudi tako, da naročimo revizijo ali ponudniku pošljemo ustrezen vprašalnik. Tu previdnost nikoli ni odveč, saj jim bomo verjetno zaupali tudi podatke, ki so ključni za poslovanje.

Katera slovenska banka je za e-poslovanje »najbolj« varna?

Številne slovenske banke komitentom ponujajo storitve elektronskega bančništva (nekatere celo mobilno bančništvo). Ker na svetovnem spletu preži veliko nevarnosti, verjetno nam ni vseeno, kateri banki zaupamo naš težko zaslužen denar. Katera slovenska banka pa je »najbolj« varna? Slovenske banke imajo lasten informacijski sistem zelo dobro »zavarovan«. K temu jih namreč zavezuje tako slovenska zakonodaja kot evropske direktive (na primer Basel II). Poleg tega morajo še opravljati redne notranje in zunanje presoje s področja varovanja informacij.

Katera slovenska banka pa je »najbolj« varna za komitenta oziroma uporabnika storitev? To je tista, ki komitentu nudi dovolj zaščitnih mehanizmov, da ta ne postane žrtev vse bolj prebrisanih spletnih nepridipravov. Med trenutno najbolj varnimi spletnimi bančništvi gre izpostaviti Klik NLB. Ta namreč z več različnimi varnostnimi elementi poskrbi za visok nivo varnosti spletnega poslovanja. Tu za vstop potrebujemo kvalificirano digitalno potrdilo (ta mora biti na pametnem USB ključku ali pametni kartici). Že na vstopni strani se nam prikaže osebno sporočilo, kar preprečuje, da bi postali žrtev ponarejene spletne strani oziroma ribarjenja. Uporabniki NLB Klika imajo možnost celo naročila na prejemanje SMS sporočil ob vsakokratnem vstopu v NLB Klik. Tu je na voljo še dodatno osemmestno varnostno geslo na papirju. Če izvajamo plačilo mimo seznama hitrih plačil, bo NLB Klik od nas zahteval vnos dveh naključno določenih znakov varnostnega gesla. To velja tudi v primeru prenosov med računi, naročil nakazil v tujino, nakazovanju denarja po sistemu Western Union in nekaterih naročil. Večino teh funkcionalnosti moramo seveda vključiti sami.

Kaj je najbolj pomembno, ko se odločamo za elektronsko bančništvo? Predvsem to, da od banke zahtevamo, da za vstop v portal nujno potrebujemo digitalno potrdilo in da je to shranjeno na pametnem USB ključku ali pametni kartici. Digitalnega certifikata nikoli ne smemo imeti shranjenega na trdem disku računalnika, saj se lahko kriminalec kaj hitro dokoplje do njega. Če že ne gre drugače, naj bo geslo daljše od 23 znakov. Nikar pa se ne odločajte za banke, kjer za dostop do vašega bančnega računa potrebujete le uporabniško ime in geslo (na primer Bank@Net od NKBM). Čeprav kriminalec tu ne bo mogel izvajati plačil, bo natančno vedel za stanje na računu, opravljene transakcije in še mnogo več. Digitalni certifikat seveda še ni dovolj. Poleg tega zahtevajte še zunanji varnostni element v fizični obliki (na primer ključek RSA). S tem boste kriminalcu preprečili, da bo v vašem imenu izvedel določeno transakcijo.

Za varnost elektronskega bančništva moramo seveda poskrbeti tudi uporabniki sami. Na računalnik je potrebno redno nameščati varnostne popravke tako operacijskega sistema kot programov. Poleg tega je potrebno imeti nameščeno kakovostno protivirusno programsko opremo, ki jo redno posodabljamo in z njo dnevno pregledujemo računalnik. Tudi požarni zid je zelo priporočljiv. Na osebnem računalniku za vsakodnevno delo uporabljajmo uporabniški profil, ki onemogoča nameščanje programske opreme in spremembe sistemskih nastavitev računalnika (omejen račun). Dostop do našega osebnega računalnika omogočimo samo tistim osebam, ki jim zaupamo. Pozorni moramo biti na lažne bančne spletne strani (ribarjenje) in na to, da ne klikamo na povezave od »bank«, ki se nahajajo v elektronskih sporočilih. Po elektronskih sporočilih nikoli ne pošiljajmo našega uporabniškega imena in gesla za dostop do portala spletnega bančništva. Nekateri strokovnjaki za varovanje informacij celo priporočajo, da za dostop do elektronskega bančništva uporabljamo navidezen operacijski sistem, ki je nastavljen na način, da se sprememb ne shranjuje. Na ta način bomo preprečili, da bi do elektronskega bančništva dostopali z okuženim računalnikom. Previdnost naj torej ne bo nikoli odveč.

Varnost e-poslovanja

Varnost e-poslovanja je vedno vprašljiva. Tu se moramo namreč zavedati, da kadar kupujemo na spletu, nam nihče ne more zagotoviti stoodstotne varnosti, saj so nepridipravi vedno korak pred snovalci varnostnih rešitev. Kljub temu lahko na svetovnem spletu nakupujemo z dovolj visoko mero varnosti, pod pogojem, da smo pred samim nakupom izdelka ali storitve pozorni na t. i. sumljive elemente na spletni strani. Tehnologija nam namreč ne more biti vedno v pomoč!

Silvester Drobnič, vodja prodaje, CHS d. o. o.

Virtualizacija strežnikov in delovnih postaj je enostavno rečeno ločitev strojne opreme od operacijskih sistemov. Kljub ločitvi ostanejo vprašanja varnosti na virtualnih strežnikih in delovnih postajah enako pomembna. Virtualno okolje ima svoje značilnosti, ki jih mora varnostna programska oprema upoštevati. Symantec, ki je vodilni ponudnik varnostnih rešitev za delovne postaje in strežnike, je ravnokar izdal novo verzijo varnostne rešitve za podjetja, Symantec Endpoint Protection 12, ki celovito pokriva zaščito delovnih postaj in strežnikov pred virusi in ostalimi najnovejšimi tehnikami vdorov. V novi različici je zmanjšana obremenitev strojne opreme do 70 %, kar je izredno pomembno za virtualna okolja zaradi potrebne zmogljivosti strežnikov. V SEP12 je vgrajena možnost časovno razpršenega izvajanja nadgradenj in skeniranj, ker se s tem močno razbremeni strojna oprema, na kateri teče množica delovnih postaj in strežnikov. SEP12 je možno brezplačno testirati in s tem preveriti ustreznost delovanja v konkretnem virtualnem okolju.

Preverite prodajalca

Če kupujemo izdelke in storitve v Sloveniji, smo lahko relativno varni. Če gre za spletne strani, kot so na primer Računalniške novice, Mimovrste, Enaa in druge, namreč ni bojazni, da nas bodo ogoljufali. Poleg tega nam tu država nudi veliko pravne varnosti (na primer Zveza potrošnikov Slovenije). Če kupujemo v tujini, velja predhodno preveriti, ali podjetje, kjer nameravamo izdelek ali storitev kupiti, uporablja za spletno stran in elektronsko pošto enako domensko ime ter da pri registraciji domene ni »skrilo« svojih podatkov. Pri tem si lahko pomagamo z brezplačnim spletnim orodjem za pregledovanje osnovnih podatkov o domenah, ki se imenuje WHOIS DomainTools in se nahaja na strani http://goo.gl/D5JW.

Kupovanje izdelkov in storitev preko spletnega portala eBay je iz določenih vidikov varnejše kot preko običajnih spletnih trgovin (predvsem, ko

Aleš Gerkman, direktor, GenLan d. o. o.

Vsi v informatiki se zavedamo, da je ključnega pomena pri razvoju sodobne družbe zagotavljanje istovetnosti osebe, ki želi dostopati do varovanih vsebin in storitev prek lokalnih omrežij ali spleta. Ta zavest raste tudi med *ljudmi, kraja identitete in zlorabe pri* naročanju blaga in storitev ter uporabi e-bančništva je vsepovsod prisotna tema. Vsi si želimo varnosti, ta pa je pogojena z zanesljivo identifikacijo oz. avtentikacijo.

Ključna ovira pri uvajanju identifikacijskih rešitev je odločitev za stroškovno neučinkovit sistem tako pri implementaciji kot vzdrževanju in uporabi, pogosto spregledana napaka pa je tudi odločitev za uporabniku neprijazno rešitev, ki ga odvrača od ponudnikove storitve. Veseli me, da smo se v našem podjetju že pred leti odločili za lasten razvoj SMS avtentikacije, ki rešuje vse prej naštete težave, ob tem pa obema, organizaciji ter uporabniku njenih storitev, nudi še nepoznano raven varnosti in udobja. V zadovoljstvo mi je, da naš produkt SecureKey uporabljajo varnostno najzahtevnejše organizacije in je dokazan v svetovnem vrhu identifikacijskih rešitev.

gre za nakupe storitev in blaga iz tujine). Na spletni strani lahko kupci določenega izdelka ali storitve namreč podajo povratno informacijo o kakovosti izdelka in zanesljivosti prodajalca. Kolikor je velika večina kupcev zadovoljna, bomo po vsej verjetnosti z nakupom zadovoljni tudi

Kupovanje na spletni strani eBay je dovolj varno!

mi. To je seveda mogoče le tedaj, ko gre za izdelke, ki se prodajajo v večji količini (na primer procesorji, pomnilniki, digitalni fotoaparati in podobno). Dobra stran portala eBay je tudi ta, da so zaupanja vredni prodajalci označeni z »nalepko« eBay Top-rated sellers. Tu gre za prodajalce, ki imajo oceno zadovoljstva med 4 in 5 (na lestvici od 1 do 5) za kakovost storitev, hitro dostavo in natančnost opisa blaga ali storitve. Poleg tega morajo imeti prometa za več kot 3.000 ameriških dolarjev in morajo izdelek prodati vsaj 100 kupcem. Prodajalce, ki izpolnjujejo pogoje, še dodatno preverijo zaposleni eBaya.

Zaupajte le v spletne strani z varno povezavo

Če vnašamo osebne podatke in/ali plačujemo določen izdelek ali storitev s plačilno kartico, moramo najprej preveriti, ali prenos podatkov *poteka v varnem načinu. To je v spletnem br*skalniku razvidno na dveh mestih. Pri večini brskalnikov se v spodnjem desnem kotu okna prikaže ključavnica (preko nje so dostopni podatki o digitalnem certifikatu), besedilo v naslovni vrstici brskalnika pa se mora začeti s »https://« in ne zgolj s »http://«. Pri digitalnem certifikatu moramo nujno preveriti ime izdajatelja oziroma overitelja digitalnih potrdil, ime domene, za katero certifikat velja, časovno veljavnost certifikata ter varnostne algoritme, ki so bili uporabljeni (na primer RSA dolžine 1024 bitov). Če poteka prenos podatkov s strežnikom v varnem šifriranem načinu, to nepridipravom prepreči oziroma oteži krajo osebnih podatkov, ki potujejo med našim računalnikom in strežnikom. Pod pogojem, da računalnik ni okužen. Tu moramo upoštevati enaka priporočila kot pri spletnem bančništvu.

Uporabljajte alternativna plačilna sredstva

Če se le da, se pri plačilu blaga in storitev izogibajmo uporabe plačilnih kartic, kjer imamo privarčevan denar ali pa imamo odobreno negativno stanje. Za spletno nakupovanje vam priporočamo uporabo »namenskih« plačilnih kartic, ki nimajo odobrenega negativnega stanja in na njih imejmo le toliko denarja, kot ga potrebujemo za določen nakup. Za plačevanje blaga in storitev se lahko odločimo tudi za t. i. predplačniške kartice, med katerimi sta v Sloveniji najbolj razširjeni PayPal in Paysafecard. PayPal lahko uporabljamo za prodajo in nakup izdelkov ali storitev preko interneta (največ na spletni preprodajalni novih in rabljenih stvari eBay). Sistem nam omogoča, da lahko opravimo nakup s komerkoli, ki ima odprt račun PayPal.

Paysafecard (http://goo.gl/Qd6yL) pa je predplačniška kartica, s katero lahko hitro, varno in enostavno plačujemo na spletu in pri tem celo ne potrebujemo kreditne kartice ali bančnega računa. S karticami Paysafecard lahko plačujemo v spletnih trgovinah, ki Paysafecard sprejemajo kot plačilno sredstvo (okoli 3.500 spletnih trgovin). Med spletnimi trgovci so največji ponudniki spletnih iger, spletnega telefoniranja kot tudi prenašanja glasbe. Stanje na predplačniški kartici lahko napolnimo z vplačilom na pooblaščenih prodajnih mestih, z nakazilom na tekoči račun in celo z Moneto preko kratkih sporočil SMS. Na kartico naložimo le toliko denarja, kot ga v nekem določenem trenutku potrebujemo.

Kako zaščititi domače brezžično omrežje ter zakaj?

Danes je že tako rekoč vsaka domača naprava opremljena z brezžičnim omrežjem (prenosni računalnik, pametni mobilni telefon, televizija, *predvajalnik večpredstavnostnih vsebin, igralne* konzole, hladilniki in še mnogo več). Zato je še kako pomembno, da ustrezno zaščitimo domače brezžično omrežje. V nasprotnem primeru se lahko kaj hitro zgodi, da bomo postali tarča nepridipravov. Ti se lahko namreč do naših podatkov ali naprav zlahka dokopljejo z uporabo namenske programske opreme. Ta omogoča spreminjanje IP in MAC naslovov, razbijanje šifrirnih ključev in napad Man-in-the-middle, pri katerem se napadalec vsem računalnikom, ki komunicirajo med seboj, izdaja za upravičenega prejemnika podatkov. Morda nas bo obiskal celo »sosed« (ali več od njih), ki si bo želel »sposoditi« našo povezavo v svetovni splet.

Če že uporabljate brezžično omrežje, naj bo to varno!

Kako najhitreje do varnega brezžičnega omrežja?

Preden pričnemo uporabljati brezžično omrežje, je potrebno nujno zamenjati privzeto administratorsko geslo na usmerniku z drugim, primerno kakovostnim geslom (dolžine vsaj osem znakov in tremi različni znaki). Priporoča se tudi izklop funkcionalnosti, ki onemogoča oddaljeno upravljanje usmerjevalnika z računalnikov zunaj lokalnega omrežja.

Naslednji korak je zamenjava imena brezžičnega omrežja (SSID) s poljubnim drugim imenom. Da ta ne bo viden vsem, se priporoča izklop oddajanja SSID med delovanjem usmernika. Tako omrežje namreč ne bo več samodejno vidno na seznamu omrežij in se bodo morali uporabniki vanj prijavljati ročno. To bo precej otežilo delo spletnim nepridipravom.

Za zagotavljanje varne povezave in preprečitev, da bi se drugi priključevali v naše brezžično omrežje, moramo seveda vključiti še šifriranje podatkov. V ta namen vam priporočamo upora-

bo šifrirnega mehanizma WPA-PSK ali WPA2. Tu seveda moramo poskrbeti za dovolj varno geslo. Če katera izmed naprav ne podpira šifrirnih mehanizmov WPA-PSK ali WPA2, nam preostane še WEP, ki pa je žal ranljiv. No, vseeno je bolje uporabljati ranljiv protokol kot pa odprto povezavo.

Če želimo varnost še dodatno povečati, omogočimo prijavo v brezžično omrežje le znanim napravam. To storimo tako, da v usmerniku omogočimo filtriranje MAC naslovov, ki so unikatni za vsako omrežno kartico. Pametno je tudi izključiti storitev Dynamic Host Configuration Protocol (DHCP), ki omogoča, da se napravi pri vzpostavitvi povezave z omrežjem samodejno dodeli IP naslov. Vse naprave, ki se povezujejo v omrežje, naj imajo statičen IP. Morda tu velja razmisliti še o tem, da brezžični usmerjevalnik postavimo tako, da bo signal zunaj domačih oziroma poslovnih prostorov čim slabši. Za poslovne uporabnike pa je primerna tudi še zagotovitev dodatne zaščite s pomočjo pametnih kartic ali zaščitnih ključev USB.

Zakaj in kje se lahko izobrazimo s področja varnosti?

Človek je vedno bil in vedno bo prva in zadnja obramba na področju varovanja informacij. Že neštetokrat se je v praksi pokazalo, da visoka tehnologija ne pripomore k večji varnosti, če ljudje niso ustrezno ozaveščeni oziroma izobraženi. Nevarnosti na zaposlene prežijo na vsakem koraku in sicer od nezaželene elektronske pošte, okuženega promocijskega materiala in prestrezanja ključnih informacij na javnih mestih pa vse do kraje prenosnih računalnikov v avtomobilih in napadov na družbenih omrežjih. Učinkovitost napada na ljudi oziroma spletna uporaba socialnega inženiringa za krajo zaupnih podatkov se je pred časom pokazala v primeru napada na podjetje RSA, ki proizvaja in trži varnostne sisteme. Tu so kriminalci napredne varnostne sisteme prelisičili na način, da so dvema skupinama zaposlenim poslali sporočilo z zadevo »Plan zaposlovanja 2011«. V njem je bila pripeta okužena datoteka. Čeprav je varnostni sistem podjetja RSA pošto označil kot neželeno (SPAM), je enega izmed zaposlenih sporočilo vseeno zamikalo in je »sprožil« okuženo datoteko. Na ta način je spletni kriminalec dobil najvišje pravice na sistemu in iz njega odtujil zaupne podatke o sistemu za avtentikacijo SecurID. Čeprav je podjetje RSA sprva zatrjevalo, da napad ni bil uspešen, je na koncu vseeno priznalo, da uporaba sistema SecurID zaradi napada ni več varna. Za odpravo škode je moralo podjetje odšteti na sto tisoče ameriških dolarjev. Analogen primer je bil v Sloveniji, ko so spletni kriminalci s pomočjo socialnega inženiringa in elektronske pošte dvema komitentoma z bančnih računov pobrali okoli 20 tisoč evrov.

Ker bodo kriminalci v prihodnje še bolj osredotočeni na zaposlene, bodo organizacije morale poskrbeti, da zaposlenim zagotovijo ustrezno izobraževanje in »urjenje« tako iz področja informacijske varnosti kot veljavne zakonodaje. Ustrezno izobraževanje je namreč predpogoj za uspešno implementacijo politik varovanja informacij v poslovne procese in spoštovanje veljavnih zakonskih določil. Proces izobraževanja je potrebno razumeti v najširšem smislu. To vključuje pripravo splošnih priročnikov in navodil za delo, specializiranih navodil ali procedur za izvajanje specifičnih nalog, osnovno izobraževanje zaposlenih ob nastopu delovnega razmerja ter redna letna izobraževanja in izobraževanja po potrebi (na primer pri implementaciji novih varnostnih mehanizmov). Celovito izobraževanje zaposlenih mora vključevati tudi seznanjanje z že znanimi ranljivostmi in tveganji za organizacijo, na koga se lahko obrnejo v primeru vprašanj in kakšno je pravilno ravnanje v primeru »izbruha« nesreče.

Izobraževanje s področja varovanja informacij lahko poteka na več načinov. Ker je časa za izobraževanje relativno malo, se priporoča, da zaposlene v okviru predavanj ali delavnic izobražuje

Če uporabniki ne bodo ozaveščeni, vam tehnologija ne bo v nikakršno pomoč!

zunanji partner. Na ta način bodo zaposleni v relativno kratkem času osvojili vsa znanja, ki so potrebna za učinkovito obrambo pred spletnim kriminalom. V Sloveniji je veliko število podjetij, ki se ukvarjajo z izobraževanjem s področja varovanja informacij. Med njimi izstopajo S&T Slovenija (http://goo.gl/QBBVs), FMC (http://goo.gl/Aqkuv), Palsit (http://goo.gl/ynRpW), B2 (http://goo.gl/slGLU) in še bi lahko naštevali.

Kako vam lahko na Facebooku ukradejo identiteto?

Družbena omrežja so med spletnimi deskarji vse bolj priljubljena. Mnogim so namreč v veliko pomoč predvsem pri ohranjanju osebnih, poslovnih in družinskih stikov. Trenutno najbolj priljubljeno družbeno omrežje Facebook uporablja že več kot 750 milijonov uporabnikov, pri čemer njihovo število še vedno narašča. Priljubljenost socialnih omrežij žal s pridom vse bolj izkoriščajo spletni kriminalci. Ti namreč na njih lahko na sila preprost in hiter način pridobijo veliko uporabnih informacij za organiziranje in izvedbo raznovrstnih kriminalnih dejanj.

Da bi se lahko učinkoviteje zoperstavili sodobni obliki spletnega kriminala in da ne bi prav vi postali žrtev socialnega inženiringa in podjetju ali sebi povzročili nepopravljivo škodo, smo pri Računalniških novicah pripravili izobraževalni webinar z naslovom »Kako vam lahko na Facebooku ukradejo identiteto?«. Na webinarju bodo prikazane najpogostejše tehnike, ki jih kriminalci uporabljajo na področju socialnega inženiringa, praktični primer uporabe socialnih omrežij za pridobitev zaupnih podatkov, ki so potrebni za izvedbo vdora v informacijski sistem ter načini, kako se lahko tem napadom učinkovito zoperstavimo. V svet hekanja s pomočjo družbenih omrežij vas bo popeljal Matej Saksida, priznan strokovnjak s področja varovanja informacij. Strokovnjak bo odgovoril tudi na vsa vaša vprašanja s področja varovanja informacij in ljudi. Več informacij o webinarju in prijave so na voljo na spletnem naslovu http://goo.gl/cniZU.

Aleš TRONTELJ, direktor, SG BIRO d. o. o.

V času, ko se vsak dan srečujemo z vlomi in ropi je pomembno, da tudi sami poskrbimo za varnost. Majhni predmeti, kot so mobilniki, prenosniki, tablični računalniki in ostala IT oprema, so privlačna in pogosta tarča tatov. Veliko lahko storimo, če stvari shranjujemo na varnih mestih. V našem podjetju se vsakodnevno srečujemo s strankami, ki jim je bilo odtujeno premoženje. Največkrat je težava v premajhni skrbnosti. Veliko naredi preventiva. Na tem področju se v Sloveniji naredi premalo. Ker sledimo trendom v svetu, uvajamo inovativne varnostne ideje. Skupaj s slovensko policijo začenjamo s projektom forenzičnega označevanja predmetov. Namenjeno je odvračanju potencialnih storilcev, saj označeni predmeti in sledi unikatne DNA snovi na storilcu služijo kot neizpodbitno dokazno sredstvo v sodnih postopkih. Odsevne nalepke na predmetih in opozorilni znaki na objektih opozarjajo, da je premoženje zaščiteno z DNA snovjo. Delujejo preventivno in odvračajo tatove. Opažamo povečano število uporabnikov forenzičnega označevanja pri preventivnih dejavnostih v zvezi z vlomi, tatvinami, ... V državah, v katerih uporabljajo forenzično označevanje, je upad tatvin kar za 85 %!