Prof. dr Dušanka Stojanović, Tehnološki fakultet Banja Luka
Mr Vesna Marić, Ekonomski fakultet Banja Luka

BEZBJEDNOST MREŽNIH KOMPONENTI POSLOVNIH UPRAVLJAČKIH INFORMACIONIH SISTEMA

UVOD

Ukupna količina podataka stvorenih tokom 1999. godine iznosila je oko 1,5 eksabajtova (10^{l8}), Čak 93% ove količine informacija čine digitalni podaci. To je, začuđujuće, enorman broj. On odgovara milijardi i po gigabajta. To znači da na svakog stanovnika naše planete dolazi 250 megabajta informacije, bez obzira na njegovu starost, dakle, računajući i svakog novorođenog stanovnika Zemlje. Šta to znači za nas i posao koji obavljamo? Sve je u vezi sa informacijama. One su danas naša realnost - to je nova svjetska ekonomija. Šta zapravo imamo? S jedne strane imamo buduće zahtjeve za obradu podataka, a s druge ljude koji treba da pristupe tim podacima. Informacije koje ne možemo da prebacimo s jednog mjesta na drugo, bezvrijedne su. Zato je suštinski posao da korisnici mogu da pristupe svojim podacima ma gdje se oni nalazili, ali, ujedno, da ti podaci budu bezbjedni.

Kao decentralizirana rješenja organizacije poslovnih upravljačkih informacionih sistema, s kojima se i u zaštiti eksperimentisalo na početku sedamdesetih godina, nisu ostvarila očekivanja stručnjaka i korisnika. Istraživački napori se usmjeravaju u pronalaženju mogućnosti direktnog povezivanja ne samo glavnog računara s udaljenim perifernim uređajima već i većeg broja računara međusobno. Tako nastaje koncept *mreže računara.* Do krajnosti pojednostavljeno rečeno, nastojalo se učiniti sve da računari uključeni u mrežu "govore istim jezikom" i da budu bezbjedni. Ovo zato što lični podaci u mreži nikad nisu bili izloženi tuđim pogledima kao danas. Iako su nezavisni kontrolori i stroži zakoni na vidiku, samozaštita nesumnjivo ostaje najbolji vid odbrane. "Internet je veća opasnost za privatnost od svih tehnologija s kojima smo se dosad susretali. On povezuje vaše ime sa svim onim što ste kupili ili pročitali".[148]

[148] Ričard Smit, američki borac za zaštitu privatnosti.

1. PRIVATNOST U DVADESETPRVOM VIJEKU

Neodgovarajuća sigurnost jedan je od najvećih problema kod pretvaranja Interneta u komercijalno tržište. Budući da su incidenti zbog narušavanja sigurnosti na Internetu vrlo česti, razumljivo je da se mnoga preduzeća i korisnici teško odlučuju za uključeno (on-line) izvođenje finansijskih ili drugih povjerljivih transakcija.

Danas postoje dva osnovna pristupa osiguranju elektronskog trgovanja. Prvi se usmjerava na zaštitu resursa štiteći pojedine poslužitelje i mrežna sjedišta. Ta zaštita pristupa uglavnom se obavlja vatrenim zidovima (firewalls) ili drugim sredstvima "osiguranja perimetra".[149]

Drugi pristup je baziran na osiguranju transakcija. Osiguranje transakcija bavi se sprečavanjem neovlašćenog slušanja ili prisluškivanja komunikacije kupac - prodavač provjerom, kako bi obe strane znale s kim razgovaraju, integritetom poruka, tako da se sadržaj poruka ne može mijenjati, i nepobitnim bilježenjem transakcije u obliku priznanice ili potpisa.

Jedan od načina da se postigne takva sigurnost jeste *sigurnost zasnovana na kanalu* koja osigurava kanal duž kojeg se transakcija odvija. *Sigurnost zasnovana na dokumentu* bazira se na zaštiti dokumenata koji provode transakciju. Dva nova standarda bave se zaštitom zasnovanom na kanalu i na dokumentu. Sistem SSL (Secure Socket Layer) tvrtke Netscape Communicationsa jeste vodeća tehnika zasnovana na kanalu. Glavni pristup zasnovan na dokumentu jeste sistem SHTTP (Secure Hypertext Transport Protocol) iz tvrtke Enterprise Integration Technologies, koja je vodeći pokrovitelj CommerceNeta, neprofitnog konzorcija.

U međuvremenu se preduzeća na Internetu pripremaju na podršku za oba zaštitna protokola.[150]

[149] Vidi „Barricading the Net“,Byte,IV.95,i „Cach on the Wirehead, IV. 95.

[150] „Pratićemo što kupci žele“,kaže Bill Rollinson,suosnivač i potpredsjednik prodaje Internet Shoping Networka. Moraćemo podržati razna rešenja,a prvenstveno SSL i SXHTTP pomoću dva poslužitelja. Imaćemo zaglavlje koje će usmjeravatai transakciju na odgovarajući server.“

2. SIGURNOSNI PROBLEMI U INTERNET-U

Internet predstavlja prostor u kojem su uočljivi brojni tipovi napada na sigurnost obuhvaćenih subjekata. lako su mnoge od takvih opasnosti vrlo malo vjerovatne, ipak s njima uvijek treba računati i vjerovati da se to "meni ne može dogoditi".[151]

Rizici u elektronskom poslovanju mogu se svrstati u 4 osnovne kategorije:

1) gubitak integriteta podataka - napadač mijenja, krade ili uništava naše poslovne podatke ili pak stvara (podmeće nam) lažne informacije,
2) ugrožavanje privatnosti podataka - privatni podaci o fizičkim iii pravnim osobama dospjevaju u ruke neovlašćenih korisnika,
3) nemogućnost korišćenja određene usluge - djelovanjem napadača korisnik se dovodi u poziciju da ne može, privremeno ili trajno koristiti Internetsku uslugu koja mu je potrebna,
4) gubitak kontrole - Internetske usluge koriste se na dopušteni način, ali nekontrolisano, čime se neko drugi ugrožava ili mu se nanosi šteta.

Sigurnosne mjere primijenjene u Internetu, tj. u elektronskom poslovanju mogu se svrstati u 5 kategorija:

- postupci autorizacije,
- mjere kriptografske zaštite,
- postupci autentifikacije,
- mjere zaštite privatnosti.

[151] CERT (Computer Emergency Response Team), u sklopu američkog Ministarstva odbrane, bavi se istraživanjem tzv. komjuterskog ili informacionog kriminala, prevencijom te vrste kriminala, te poduzimanjem istražnih postupaka u slučaju otkrivanja delikata. Stručnjaci CERT-a proveli su u januaru 1999. Godine eksperiment kojim su, uz dopuštenje vlasnika, simulirali različite oblike napada na „živa“ Internetska Web mjesta, ne uništavajući i niti kradući, pri tom njihove podatke. Rezultati su se pokazali više nego zabrinjavajućim: samo oko 2% Web mjesta uspjelo je uopšte otkriti, odnosno zapaziti napade, a tek oko 2 promila je moglo tačno utvrditi šta je zapravo učinjeno.

2.1. Postupci autorizacije

Autorizacija je provjera ovlašćenosti i obavlja se određenim programima u računaru određenog Web mjesta, a osnovni je cilj takvih programa tačno provođenje pravila o tome što korisnik Web mjesta smije, a što ne smije raditi. Provjera se obavlja na osnovu identifikacije kojom se korisnik predstavlja Web mjestu.

2.2. Mjere kriptološke zaštite

Mjere kriptološke zaštite koriste metode kojima će se partnerima u komunikaciji obezbijediti tajnost, tj. onemogućiti neovlašćene ili neželjene korisnike da razumiju poruke koje se razmjenjuju. Kriptiranje se obavlja utvrđenim postupcima koji se nazivaju kriptološkim algoritmima. Svaki kriptološki algoritam možemo transformisati u računarski program; zato se zaštita poruka (podataka) ostvaruje jednostavno i brzo pomoću računara. Izbor kriptološkog algoritma određen je ključem (eng. Key) i ključeva može biti više. Danas su u upotrebi dva kriptografska sistema: *simetrični sistemi* (s tajnim ključem) i *asimetrični sistemi* (sa javnim ključem). U elektronskom poslovanju vlasnici Web mjesta moraju omogućiti svojim korisnicima kriptografsku zaštitu podataka koje mu oni moraju poslati uvijek kad oni imaju karakter tajne ili kad to korisnik iz bilo kog razloga zahtijeva.

2.3. Postupci autentifikacije

Autentifikacija je postupak provjere vjerodostojnosti podataka. Ona je u elektronskom poslovanju nužna, jer se uvijek mora provjeravati odgovara li primljena poruka sadržaju zaista poslate poruke ili je možda tokom prenosa neko neovlašćen, uprkos svim mjerama zaštite, ipak promjenio njezin sadržaj. U tu svrhu na Internet-u se koristi tehnika digitalnog potpisa (Digital Signature). Ta tehnika će se primjenjivati kad su poruke, koje se razmjenjuju, duže (npr. poruke u elektronskoj pošti). Tada se svodi sve na to da se samo mali dio poruke kriptuje, i taj dio se, u zaštićenom obliku, dodaje osnovnoj poruci u obliku tzv. digitalnog potpisa. Dakle, digitalni potpis i nema vezu sa vlastitim potpisom, osim što je jednoznačan kao i on. Jednoznačnost digitalnog potpisa osigurava se slučajnim izborom uzorka poruke koji se kriptuje na mjestu slanja.

Primalac poruke ne može falsifikovati potpis jer ne zna kako je stvoren, što onda čini osnovu za provjeru autentičnosti potpisa, a time i cjelokupne poruke.[152]

2.4. Mjere antivirusne zaštite

Zašto se provodi antivirusna zaštita? Računarski virusi i crvi su programi, programske rutine ili segmenti koji se "lijepe" na regularne korisničke ili sistemske programe, a imaju osobinu razmnožavanja, uzrokujući poteškoće pri radu informatičke opreme, te oštećenje i/ili uništenje datoteka progama i/ili podataka.

Virusi se "lijepe" na računarski program u vrijeme njegovog izvođenja, tako da mogu preuzeti kontrolu pri svakom njegovom sljedećem izvođenju. Zavisno o tome kako su oblikovani, oni se mogu odmah manifestovati ("javiti") i/ili reprodukovati u novoj okolini ili neko vrijeme ostati pritajeni (kad se nazivaju "logičkim bombama" - Logical Bomb).

Crvi su programi koji se ponašaju vrlo slično virusima, ali je razlika u tome što se virusima može zaraziti samo onaj računar u kojeg su oni unijeti s podacima stvorenim na nekom drugom inficiranom računaru, dok crvi "vrebaju", poput nekih drumskih razbojnika, u mreži i "lijepe" se na izvorno nezaražene podatke tokom prenosa.[153]

Danas su razvijene dvije grupe mjera antivirusne zaštite:

a) mjere preventivne antivirusne zaštite,
b) mjere kurativne antivirusne zaštite.

Najbolji efekat daju mjere preventivne antivirusne zaštite (po onoj staroj uzrečici "bolje spriječiti, nego liječiti"). Među njima posebno su značajne:

[152] Programi za primjenu tehnike digitalnog potpisa će biti ugrađen u novi Microsoftov operativni sistem Windows 2000, koji je još u fazi testiranja.

[153] Prvi crv koji je izazvao planetarni upozorenje bio je onaj što ga je u Noći vještica 1988. godine „lansirao" student univerziteta Cornell Robert T. Morris i koji je pokrao oko 2000 mreženih računara. Optužen je i priznao svoj čin, ali je rekao kako ga nije izvršio sa zlom namjerom, tj. da nije mogao pretpostaviti posljedice koje će izazvati. Osuđen je samo na uslovnu kaznu u trajanju od 3 godine. Ipak ostaje pitanje: koliko je je poslije bilo onih kojima je Morris dao „dobru ideju" i kakve su oni sve štete izazvali?

- izbjegavanje upotrebe računarskih programa nepoznatog ili sumnjivog porijekla, tj. izvora;
- izbjegavanje presnimavanja Shareware i Freeware programa iz Interneta, ako oni nisu licencirani, tj. ako se ne zna ko im je autor;
- izbjegavanje upotrebe opreme za koju nije izvjesno je li licencirana virusom ili nije;
- redovno stvaranje rezervnih kopija podataka i programa, te njihovo čuvanje na fizički sigurnom mjestu;
- obavezna upotreba antivirusnih programa prije početka ili povremeno tokom rada.[154]

Tehnički najjednostavniji, ali obično i najskuplji postupak, je tzv. reformatiranje svih aktivnih nosilaca podataka i računarskih memorija (magnetni diskovi, diskete), odnosno njihovo čišćenje od svih postojećih sadržaja, pa onda i od virusa.

Nažalost, čak i reformatiranje nosilaca podataka i memorija u nekim posebno teškim slučajevima infekcije nije potpuno sigurna metoda antivirusne zaštite. Tada je nužno primjenjivati tzv. antivirusne lijekove (engl. Antivirus Remedy), odnosno programe koji, uz pronalaženje virusa, podrazumijevaju aktivnosti otklanjanja šteta što ih je virus izazvao ("liječenje od bolesti"). [155]

2.5. Mjere zaštite privatnosti

Poznati primjer ugrožavanja privatnosti vremenom su postali tzv. ''kolačići" (engl. Cookies). "Kolačić" je segment podataka koji Internetski potražilac postavlja na klijentskom računaru na zahtjev poslužioca Weba. Obično se to radi kad se nekom Web mjestu neki korisnik prijavljuje prvi put. Web poslužilac će "zapamtiti" klijentova pitanja i prepoznati ih kad on sljedeći put "posjeti" to Web mjesto. Konstantnim ažuriranjem, provjeravanjem i analizom "kolačića" vlasnik Web poslužioca, odnosno mjesta može trajno prikupljati informacije o određenom ili svim klijentima u čije

[154] Danas zasigurno najpopularniji antivirusni programi su oni iz grupe NortonAntiVirus. Mogu se nabaviti na mnogim prodajnim Web mjestima (vlasnik autorskih prava je kompanija Symatec).
[155] I u ovom slučaju obično će biti od koristi neki od programa iz već pomenute grupe NortonAntiVirus.

računare je ugradio "kolačiće". Izvorna namjera "kolačića" je bila poštena u namjeri - trebalo je da oni pomognu pri elektronskom trgovanju na dva načina:

1. olakšavajući kupcu pronalaženje traženih, preciznih i ažurnih informacija o ponudi određenih prodajnih mjesta i
2. olakšavajući prodavaocu informisanje potencijalnih kupaca o novostima u vlastitoj ponudi.

Međutim. vremenom se pokazalo da ”kolačići" mogu hiti moćno sredstvo "špijunaže i ugrožavanja privatnosti klijenata, jer neki drugi korisnici Interneta o njima mogu znati "saznati previše" i izvrgavati ih različitim neugodnostima, pa čak i do ucjene i prijetnje. Zato danas "kolačići imaju nepotrebnu negativnu reputaciju, ali Internetski trgovci poštenih namjera mogu ih uspješno koristiti za istraživanje tržišta.[156]

3. PRIJETNJA ZA BUDUĆNOST - ZLONAMJERAN SOFTVERSKI KOD

Zlonamjeran kod ugrađen u softver nije novina. Korisnici uvijek rizikuju da preuzmu virus ili trojanca koji se krije u serveru i igrama na Internetu.. I u programima koji se dobijaju lijepo upakovani povremeno se pojavi "napadač". Međutim, hakerisanje[157] po Mikrosoftovom izvornom kodu već je prouzrokovalo zabrinutost da sljedeća meta napada može da bude ovaj popularni softver. Ako softverske kompanije ne povećaju bezbjednost, može se desiti da uz nov program za računovodstvo kao poklon dobijemo i štetočinski virus.

[156] Problemi ugrožavanja privatnosti korisnika Interneta doveli su do osnivanja neovisne, neprofitne organizacije nazvane TRUSTe, čiji je osnovni cilj razvijanje povjerenja korisnika u Internet-u poduzimanjem raznih mjera zaštite njihove privatnosti. TRUSTe izdaje certifikate i on se izdaje kao svojevrsna potvrda, znak ili pečat, nazvan trustmark, a služi kao dokaz da se organizacija (ili osoba) koja ga je dobila prethodno obavezala na pridržavanje kodeksa o zaštiti privatnosti klijenata formulisanog od strane TRUSTe-a i omogućavanje trajnog nadzora neovisnih promatrača nad njezinim poslovanjem.

[157] Hakeri i krekeri nisu ništa drugo do napadači na sigurnost ostalih interentskih korisnika, dakle najobičniji kriminalci. Samo ih tako treba shvatati i tretirati!

ZAKLJUČAK

Kao glavni pravci budućeg razvoja poslovne informatike pokazuju se područja vjestačke inteligencije, neuronskih mreža, multimedijskih sistema, bežičnih komunikacija, virtuelne (prividne) stvarnosti i sistema za podršku odlučivanju. I u svim njima neodgovarajuća sigurnost jedan je od najvećih problema i današnjice i bliske budućnosti.

I na kraju, budući da živimo u dinamičnom svijetu u kojem se iz dana u dan javljaju najrazličitiji i stalno novi problemi, pitanje lične sigurnosti pojedinaca, poslovne sigurnosti privrednih subjekata i opšte nacionalne sigurnosti nameću se same od sebe. Internet kao fenomen novijeg datuma i sam donosi brojne bezbjedonosne probleme i rizike koji prije nisu postojali ili se barem za njih nije znalo. Problem je veći što u Internet-u nema nikakvog formalnog autoriteta koji bi sistemski radio na prevenciji i suzbijanju nedopuštenih, nemoralnih ili opasnih aktivnosti - nema barem za sada, nikakve "Internetske krimpolicije“, čiji bi zadatak bila briga o sigurnosti cjelokupne Internetske korisničke zajednice, na čemu se u budućnosti mora raditi.

LITERATURA

1. D. Stojanović Primjena kriptozaštite u sigurnom informacijskom sistemu, doktorska disertacija, ETF Zagreb. 1989.
2. D. Ajduković (Stojanović) Kampjuterski informatički sistem u funkciji kriptozaštite, Banja Luka, 1993.
3. D, Stojanović, M Stojanović, S. Stević, D. Vejnović Šifrom protiv kompjuterskog terora, Udruženje defendologa RS i GLAS srpski, B. Luka, 1998,
4. Ž, Panian Pravna zaštita podataka, IDI, Zagreb, 1976.
5. D, Stojanović, V. Marić Organizacioni aspekti zaštite u informacionim sistemima, XXVI jugoslovenski simpozijum o operacionim istraživanjima, ZBORNIK RADOVA, Beograd, 1999. str. 169-173.
6. M. Mihaljević, D. Stijović, S. Popadić, B. Marić Elektronska trgovina, elektronski novac i kriptografske tehnike, INFO, 1999. (jedan osvrt na savremene trendove)