

KOMPJUTERSKI KRIMINAL

sa posebnim osvrtom na malu privredu

Марко Милојевић
Извршни директор
ФЛ Инжењеринг Информатика и Инфотехника Београд
Милешевска 6, 11000 Београд, СЦГ
fling@EUnet.yu

Pojavljivanjem novih tehnologija kod nas, neminovno je došlo i do olakšanja u komunikacijama. Prvobitan fax aparat zamenio je računar sa telefonskim posrednikom - modemom, a sve u cilju što bržeg, efikasnijeg i sigurnijeg komuniciranja sa, nekada službom platnog prometa i danas, bankama. U novonastaloj situaciji mali privrednici u Srbiji odlično su se snašli. Uvek je postojao neko da pokaže, prenese znanje, pomogne. S' obzirom na date okolnosti ljudi su se adaptirali na računar i njegove mogućnosti u jako malom vremenskom periodu. Nebitno koje struke, da li piljar, apotekar ili inženjer tek, u svakoj kancelariji, radnji, ordinaciji, mogli ste zapaziti komunikacionu napravu koja je radila svoj posao - operisala sa novcem.

O sigurnosnim manama takvog sistema nije bilo govora, niti je iko postavljao pitanja o mogućem postojanju problema takve prirode. Arhitektura prvobitnog sistema komunikacije datog na korišćenje privredi Srbije u smislu povezivanja sa službom platnog prometa bila je neranjiva samim tim što se zasnivala na direktnoj, telefonskoj komunikaciji korisničkog računara sa centralnim serverom SPP-a. Sa jedne strane imali ste računar sa telefonskim posrednikom i aplikacijom koju je privrednik dobijao na osnovu zahteva računskoj službi SPP-a, a sa druge SPP sam koji je omogućio telefonski pristup vlasniku računa istom. Ceo sistem eliminisao je fizičko odlaženje do nadležnog SPP-a i čekanje u redovima zarad predavanja virmana kojime bi se transfer novca izvršio.

Sistem, dakle, nije bio povrediv upadima i zloupotrebama u bilo kom pogledu samom prirodom ostvarene veze, ali je imao mnogo mana koje su tadašnji korisnici sve više počeli da uviđaju. Prvo, nije bilo moguće u nedogled širiti broj korisnika jer je sama veza omogućavala tek nekoliko korisnika konektovanih na server istovremeno. Dok oni ne bi završili svoje upite, novi se nisu mogli konektovati.

Izmenom zakona koja se odnosi na platni promet, banke su ponovo dobile puni bonitet rada sa privredom i samim tim, pojavio se vrlo realan zahtev za povezivanje velikog broja korisnika na takođe, veliki broj banaka. Rešenje ovoga puta nije moglo biti jednostavno, ne samo zbog velikog broja zahteva korisnika koji su morali biti obrađeni u što kraćem roku, već i zbog internog povezivanja među samim bankama. Pribeglo se rešenju korišćenja postojeće infrastrukture za tako obiman zahtev. Postojeća infrastruktura je, naravno, Internet, sa svim svojim prednostima i manama. Prednosti smo naveli, a mane ćemo pokušati da prepoznamo i klasifikujemo.

Ono što, zbog navedenog iskustva sa SPP-om u ranijem poslovanju, privrednik u Srbiji ne može odmah da prepozna jeste vid komunikacije i rizik njenog korišćenja. Sama činjenica da zloupotrebe elektronskog računa u prethodnom poslovanju nije bilo daje jedan privid

sigurnosti korisniku novog sistema. Za njega je to jedna nova aplikacija, vizuelno lepša od prethodne i neki novi broj telefona. Svest da u njoj, za razliku od prethodne, postoji potencijalna opasnost od deset miliona subjekata koji su kadri napasti u svakom trenutku i postići neki od željenih ciljeva koji nisu uvek finansijska sredstva, ne postoji kod prosečnog korisnika. Baš zbog pomenutih raznolikosti profila, vrlo je redak prosečan korisnik koji prepoznaje istinske opasnosti koje se kriju iza upotrebe najrasprostranjenije infrastrukture na planeti. O njima sada više neće biti reči, jer detaljnu specifikaciju opasnosti moramo ostaviti za jedan drugi skup koji će se time baviti. Ono na čemu ćemo se ovde bazirati biće upozorenje da takve opasnosti postoje i da svest o njima mora postati sveprisutna.

Sam termin "kompjuterski kriminal" našem čoveku pravi viziju neke čudne osobe koja ne izlazi iz svog stana, ima naočare velike dioptrije usled preteranog gledanja u ekran i sposoban je da sa malo truda dođe do sredstava koja su mu potrebna za život. To je vizija koju su u domaćoj svesti stvorile filmska industrija i nedostatak realnih slučajeva koji bi ukazali da je stvarnost drugačija. Ono na šta ću ja posebno skrenuti pažnju jeste činjenica da kompjuterski kriminal sam za sebe retko može opravdati svoje postojanje.

Vratimo se na temu domaćih banaka i elektronskog poslovanja. Sistem je osmišljen po ugledu na već postojeća svetska rešenja. Korisnik dobija broj telefona i digitalni sertifikat koji mu, po uspešnom ostvarivanju veze, omogućuje da se predstavi serveru banke koja će mu potom pružiti mogućnost obavljanja svih vidova operacija sa računom, kao da se nalazi u poslovnici banke sa virmanima i pečatom. Osnovni problem koji se javlja u ovom vidu komunikacije nije samo elektronsko rešenje. Čitavi timovi eksperata sakupili su se da bi omogućili nastanak jednog takvog ličnog sertifikata visoke kriptacije kakav je dostupan našem tržištu. U tom pogledu ne zaostajemo za tehnološki najrazvijenijim zemljama sveta od kojih smo preuzeli i implementirali rešenje. Razlika između nas i pomenutih je upravo svest na koju toliko skrećem pažnju. Nije problem, dakle, u načinu kodiranja, pristupu, zaštiti servera banke... Problem je u spoju klasičnog i elektronskog kriminala. Da pojasnim: čistog elektronskog upada u potpuno nepoznati sistem nije bilo od 1997. godine. Od 1997. do danas desilo se mnogo kriminalnih dela, od krađe intelektualne svojine do prave, velike pljačke novca. Nijedan slučaj nije doveden do svoje završne, dramatične faze samo posredstvom nezavisnog genija, hakera koji je uspeo sam da zaobiđe sve sisteme zaštite, već je delo najmanje dva učesnika od kojih je jedan snabdeo kriminalni akt vitalnim podacima. Da li je to u pitanju amater, službenik u banci kome je dostupan šifarnik ili beskrupulozni ulični nasilnik koji je do digitalnog sertifikata došao silom sasvim je irelevantno. Ono što je prepoznatljiva srž svakog uspelog napada jeste upravo taj spoj tradicionalnog i modernog, virtualnog kriminala.

Vodeći ovom temom, zatražio sam od svoje banke, u trenutku dobijanja mogućnosti elektronskog povezivanja, jedno obaveštenje. Na postavljeno pitanje na koji telefon mogu hitno javiti da se svaki elektronski transfer sa mog računa obustavlja, odgovoreno mi je brojem telefona i radnim vremenom od 08 do 18h. Tu se svaka priča o elektronskom transferu završava. Moje preduzeće danas funkcioniše tako što se virmani popunjavaju ručno i vrlo tradicionalno odnose na šalter banke. Bilo koji amaterski napad ostavlja dovoljno mesta najprosečnijem kriminalcu da izvrši transfer sa bilo koje lokacije samo uz pomoć digitalnog sertifikata do koga je mogao doći na više načina: pljačkom mojih poslovnih prostorija, koja se već događala; fizičkim napadom na osobu koja je zadužena za sertifikat, van kancelarije; i sl.

Dovođenje banaka na nivo svesti o postojanju problema samo je jedan korak. Formiranje zakona koji bi se eksplicitno bavio kompjuterskim kriminalom već je mnogo više. Postojanje ovlašćenog interventnog ekspertskeg tima sposobnog da, u sprezi sa organima zakona i telekomunikacionim kućama, u najkraćem mogućem roku sagleda pričinjenu štetu i locira počinioca, ultimatno je rešenje koje svaka razvijena država već poseduje.