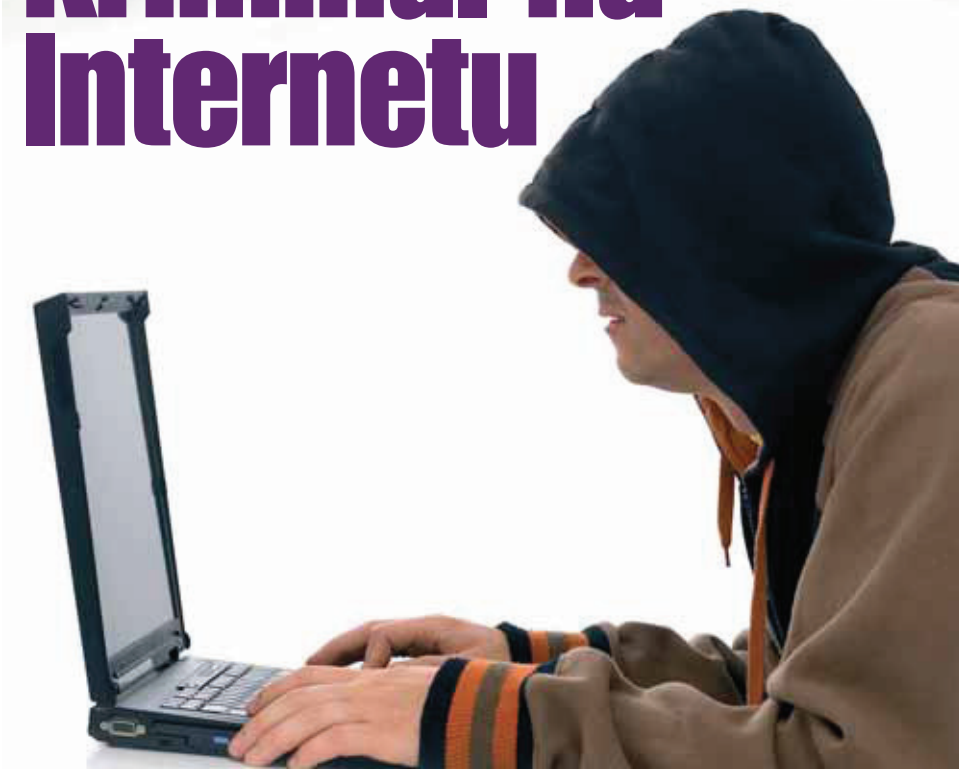
Dože Tokić, dipl. ing.

Računalni kriminal, cyber kriminal, e-kriminal ili elektronički kriminal su pojmovi koji se odnose na kriminalne aktivnosti gdje je računalo ili mreža izvor, alat, meta ili mjesto kriminalnih aktivnosti. Ove kategorije nisu tijesno vezane samo za sebe, odnosno one mogu biti u interakciji s drugim oblicima kriminala. Ukratko, kriminalna aktivnost može potpadati pod više kategorija.

Kriminal na Internetu



Iako se spomenuti pojmovi koriste za opisivanje kriminalnih aktivnosti u kojima je računalo ili mreža nužan dio kriminalne aktivnosti, ovi pojmovi se tako ponekad koriste za opisivanje tradicionalnih kriminalnih aktivnosti, kao što je prijevara, krađa, ucjena, krivotvorenje i utaja, gdje se računala ili mreže koriste za pomaganje zabranjenih aktivnosti. Kako uporaba računala raste, tako i računalni kriminal postaje sve važniji.

VRSTE RAČUNALNOG KRIMINALA

- **Zloćudni/Maliciozni;** kad je softver napravljen da bi se infiltrirao i oštetio računalni sustav bez da korisnik za to zna ili pristane na to. Ovaj izraz je općeniti izraz koji koriste računalni profesionalci da bi označili veliki broj različitih oblika napadnog, neprijateljskog, dosadnog softvera ili programskog koda. Velik broj korisnika računala nije upoznat s ovim pojmom i svodi ovakav čin neprijateljstva pod pojam "računalnih virusa".
- **Denial-Of-Service napad;** pokušaj da se računalni izvor (sadržaj, skup informacija) napravi nedostupnim korisnicima kojima je namijenjen. Iako se metode, motivi i cilj DoS napada razlikuju, općenito se sastoji od usklađenih, zlonamjernih pokušaja jedne ili više osoba da spriječe neki Internet servis ili stranicu da efikasno funkcionira ili da je privremeno ili trajno onesposobe za upotrebu. Izvođači DoS napada tipično ciljaju sajtove ili servise koji udomljavaju web servere visokog stupnja sigurnosti kao što su banke, poslužitelji za plaćanje kreditnim karticama ili čak DNS root serveri.
- **Hakiranje;** ima više različitih značenja na području računalnih znanosti i tehnologije. Može se odnositi na pametnu ili brzu zakrpu za rješavanje problema računalnog programa, ili na nespretno ili neelegantno rješenje problema. Pojam se isto tako koristi za opisivanje modifikacija programa ili uređaja koji daju korisniku pristup mogućnostima koje mu na drugi način ne bi bile dostupne. Većina korisnika računala ovaj pojam je poznat kao čin ilegalnog ulaska u računalo, poznatog kao "krakiranje".
- **Računalni virus;** računalni program koji ima sposobnost kopirati samog sebe i zaraziti tuđe računalo bez dopuštenja ili znanja korisnika tog računala.
- **Cyber terorizam;** kontroverzan pojam. Općenito se odnosi na djela koja čine pripadnici bilo kojih poznatih, terorističkih organizacija, a s ciljem stvaranja uzbune ili panike.
- **Informacijsko ratovanje;** uporaba informacija za ostvarivanje natjecateljske prednosti nad protivnikom. Ovdje je upletena cijela skupina taktičkih informacija, uz činjenicu da je informacija onog tko je širi istinita, šireći propagandu ili dezinformacije da bi se utjecalo na moral neprijatelja i javnosti, potkopavanjem kvalitete informacije protivničke strane i sprečavanje protivnika u procesu prikupljanja informacija.
- **Virtualno uznemiravanje;** korištenje informacijske i komunikacijske tehnologije, posebno Interneta, od strane individualaca ili grupe, da bi se uznemiravao drugi individualac, grupa ili organizacija. Ponašanje uključuje lažno optuživanje, nadziranje, slanje prijetnji, krađu identiteta, oštećivanje podataka ili opreme, seksualno uznemiravanje, prikupljanje informacija da bi se kasnije iskoristile za uznemiravanje.
- **Prevara i krađa identiteta;** pojam koji se koristi da bi se opisala prevara koja je povezana s krađom novca ili nabavkom drugih dobara pretvarajući se da ste netko drugi. Ovaj pojam je relativno nov i često je predmet zabune, jer se povezuje s krađom identiteta, međutim, ovdje se radi samo o korištenju tuđeg identiteta.
- **Phishing;** jedan od oblika prijevare koji podrazumijeva skup aktivnosti kojima ne-

ovlašteni korisnici korištenjem lažnih poruka elektroničke pošte ili instant poruka pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka poput korisničkog imena, lozinke, detalja vezanih za kreditnu karticu, a sve pod krinkom vama povjerljive fizičke osobe. Najčešće poruke dolaze s domena popularnih socijalnih web stranica (Youtube, Facebook, Myspace), aukcijskih stranica (eBay), *on-line* banaka (PayPal) ili IT administratora (Yahoo, ISP, itd.) jer su isti najmanje sumnjivi.

● **Virtualni kriminal;** odnosi se na virtualni kriminalni čin koji se zbiva u masovnim on-line igrama. Veliko vrijeme i trud koji se investira u nasilne računalne igre može dovesti do toga da isti "preraste" u stvarno kriminalno djelo u realnom svijetu, ili čak da igrač izgubi sposobnost razlučivanja stvarnog od virtualnog svijeta.

● **Krađa brojeva kreditnih kartica;** samo se 3% ukupnog broja prevara odnosi na kartično poslovanje, tako da možemo smatrati on-line plaćanje kreditnim karticama sigurnim procesom kupovine. Treba istaknuti da je zbog potencijalne krađe podataka s kreditne kartice zabrinuto više od 50% *on-line* kupaca, iako je manje od 2% iskusilo tu neugodnost. Istraživanja su pokazala da je učestalost krađe kartičnih podataka identična postotku krađa koje se rade licem u lice, putem pošte ili telefona. Najbolja isplativost ovakvih kriminalnih radnji dokazuje postojanje web stranica gdje se može generirati cjelokupan lažan identitet i broj kartice. Ukoliko sumnjate da postoji mogućnost prevare, limitirajte iznos isplate vaše kartice, ili pak poništite karticu i zatražite izdavanje nove.

Savjeti Poslovnog savjetnika

1. Redovito nadograđujte svoj operativni sustav novim "zakrpama". Isto radite i s drugim programima koje posjedujete. Ukoliko se radi o velikoj tvrtki i nije vam neophodan Internet, rezervirajte nekoliko računala za Internet, odnosno fizički odvojite vaše povjerljive podatke od Interneta.
2. Programi koji koriste vatrozid su efikasni u borbi protiv upada. Posebno efikasni su se pokazali hardverski vatrozid uređaji. Obavezna je uporaba antivirusnih programa i *antispyware* programa.
3. Poštivanje sigurnosne politike tvrtke će isto tako pospješiti sprečavanje kriminalnih radnji nad računalnim sustavom.
4. Zatražite savjetovanje s tvrtkama koje se bave sigurnosnim konzaltingom kojih, specijaliziranih samo za to područje, kod nas u Hrvatskoj nema, pa ćete pomoć morati potražiti kod tvrtki koje se bave projektiranjem, ugradnjom i administriranjem računalnih mreža neovisno o tome imate li dva ili tisuću umreženih računala.

POZNATI HAKERSKI UPADI

● **Ian Murphy**, tzv. *"Captain Zap"*, prva je osoba osuđena zbog računalnog kriminala. On i njegova tri prijatelja su provalili u AT&T-ov (najveća telekomunikacijska tvrtka u SAD-u) računalni sustav i pomakli su satove koji mjere utržak, tako da je sustav naplaćivao skuplju tarifu razgovora noću, a preko dana jeftiniju. Uhićen je 1981., osuđen 1982., i prema njemu je snimljen film *"Sneakers"*. Murphy od tada vodi tvrtku koja se bavi sigurnosnim savjetovanjem, IAM/Secure Data Systems.

● Iako se brže širio od Melissa virusa koji se pojavio samo godinu dana ranije, brisao je slikovne i zvučne zapise s inficiranih računala. Virus se sam slao na sve mail adrese koje je žrtva imala u Outlook Expressu. Zanimljivo, zarazio je samo računala s Windows platformom i to korisnike Outlook programa što je izazvalo, po prvi put, veliku galamu na Microsoft da ne posvećuje pažnju sigurnosti. Mail je stizao na adresu potencijalne žrtve s bezazlenim natpisom **"ILOVEYOU"** u subjektnoj liniji i virusnim kodom koji je bio prikačen za mail. Ni dan danas nije sigurno tko je autor virusa, samo se zna da je širenje započelo u Aziji i kroz 24 sata zahvatilo cijeli svijet.

● Slučaj zadarskih hakera nije toliko poznat u svijetu koliko je kod nas. Zbio se 1996. godine kad je troje maloljetnika navodno provalilo u Pentagonove tajne datoteke (navodno nuklearno postrojenje Anderson prema tvrdnjama američkog ministarstva obrane). Oprema trojice zadrana je zaplijenjena. Američko ministarstvo obrane je izjavilo da je počinjena šteta od pola milijuna dolara, a prema nekim navodima oni su poslužili jednom ruskom hakeru da zavara agente SAD-a i provali u računalo dok su se zabavljali sa "zadarskim hakerima".

PS

Tvrtka Cisco objavila je drugi dio studije trenutnog stanja sigurnosti podataka u korporacijama

Korporacije zbog nepažnje gube podatke, ali i klijente

Istraživanje otkriva da zaposlenici često nisu svjesni korporativnih politika te skreće pozornost na činjenicu da svaka četvrta kompanija nema definirane sigurnosne politike.

Tvrtka Cisco objavila je drugi dio globalnog istraživanja o "curenju" kompanijskih podataka, u kojemu navodi spoznaje o učestalosti primjene i učinkovitosti korporativnih sigurnosnih politika te razloge zbog kojih ih se zaposlenici pridržavaju ili ih krše. Istraživanje omogućuje timovima zaduženima za informacijsku tehnologiju širom svijeta da bolje razumiju faktore rizika kod zaposlenika kako bi mogli uspješno prilagoditi kompanijske politike u skladu s realnim potrebama korisnika u obavljanju radnih zadataka.

Postoji nekoliko faktora koji utječu na odluku zaposlenika da se pridržava korporativnih sigurnosnih politika odnosno da ih krši:

● **svijest zaposlenika o politikama:** jedno od najvažnijih otkrića ovog istraživanja je da postoji veliki nesrazmjer između broja zaposlenika i broja IT stručnjaka koji su svjesni postojanja sigurnosnih politika. Ovisno o državi u kojoj se nalaze, broj IT stručnjaka koji su svjesni određenih sigurnosnih politika bio je 20-30% viši u odnosu na zaposlenike koji su ih svjesni. Najveći nesrazmjer (31%) zabilježen je u SAD-u, Brazilu i Italiji;

● **komunikacija:** ukupno 11% zaposlenika navelo je da IT služba nikada ne komunicira ili ne educira zaposlenike o sigurnosnim politikama. Ovaj je problem naročito prisutan u Europi gdje je u Velikoj Britaniji (25%) i Francuskoj (20%) zabilježen najveći broj zaposlenika koji su potvrdili ovu tvrdnju;

● **ažuriranje politika:** 3 od 4 IT stručnjaka (77%) vjeruje kako sigurnosne politike treba češće ažurirati, dok isto to misli tek polovica zaposlenika (47%). U Kini (91%) i Indiji (89%) IT stručnjaci najviše su podržali takvo mišljenje;

● **primjerenost:** većina zaposlenika smatra da sigurnosne politike poduzeća nisu primjerene. To je slučaj u 8 od 10 država obuhvaćenih ovim istraživanjem; s takvim stajalištem ne slažu se jedino zaposlenici u Njemačkoj i SAD-u;

● **nepridržavanje:** prema mišljenju IT stručnjaka, zaposlenici krše politike iz niza različitih razloga, od neshvaćanja razmjera sigurnosnog rizika do ravnodušnosti. Međutim, prema mišljenju zaposlenika najvažniji razlog nepridržavanja politika je to što smatraju da politike nisu u skladu s njihovim realnim potrebama u obavljanju radnih zadataka. Ukupno 42% zaposlenika slaže se s tom tvrdnjom na globalnoj razini.