# KODEKS PONAŠANJA ZA BEZBRIŽNO UČEŠĆE U INTERNET SVIJETU

***Prof. dr Vesna Aleksić Marić, dipl. ekon.***
***Ekonomski fakultet u Banja Luci***

***Prof. dr Dušanka Stojanović, dipl. inž.***
***Tehnološki fakultet u Banja Luci***

*Moderne organizacije su suočene s brojnim sigurnosnim prijetnjama. Danas postoje različite preporuke i standardi koji daju smjernice za očuvanje informaticke sigurnosti. U ovom radu opisano je uspostavljanje sistema upravljanja sigurnošcu informacija u skladu s preporukama normi ISO/IEC 17799 i ISO/IEC 27001.*
*U radu su obrađene metode napada, oblici ugrožavanja i vrste prijetnji kojima su izložene računarske mreže, kao i moguće metode i tehnička rješenja za zaštitu mreža. Analizirani su efekti prijetnji kojima mogu biti izložene računarske mreže i informacije koje se preko njih prenose. Opisana su određena tehnička rješenja koja obezbjeđuju potreban nivo zaštite računarskih mreža, kao i mjere za zaštitu informacija koje se preko njih prenose. Navedeni su standardi koji se odnose na metode i procedure kriptozaštite informacija u računarskim mrežama. U radu je naveden primer zaštite jedne lokalne računarske mreže.*

*Ključne riječi: računarske mreže, ugrožavanje mreža, prijetnje mreži, protivmjere, zahtijevi za zaštitu, tajnost informacija, autentičnost, integritet, autorizacija prava korisnika,*

# CODEX MORALS AFTER CARELESSLY INVOLVEMENT AT THE INTERNET WORLD'

*Modern organisations are faced with a numerous security threats. Today, there are different recommendations and standards that offer guidelines for protecting organization's information security. This paper describes the implementation of information security management system according to ISO/IEC 17799 and ISO/IEC 27001 standards.*

*In this paper different methods of attacks, threats and different forms of dangers to thecomputer networks are described. The possible models and technical solutions for networks protection are also given. The effects of threats directed to the computer networks and their information are analyzed certain technical solutions that provide necessary protection level of the computer networks as well as measures for information protection are also described.*

*The standards for methods and security procedure for the information in computer networks are enlisted. There is also an example of protecting one local data network (in this paper).*

*Key words: computer networks, endanger of networks, network threats, countermeasures, protection demands, information confidentiality, authenticity, integrity,*

## *UVOD*

Internet čine međusobno spojene računarske mreže rasprostranjene cijelim svijeta, te tako predstavlja vrlo veliku svjetsku mrežu. Svaki pojedinac ima širok spektar mogućnosti rada na Internetu zbog čega Internet u svojoj osnovi nije siguran. Međutim, pošto Internet nije samo svjetska mreža računara, već i velika neformalna zajednica ljudi, potrebno je posjedovati kodeks ponašanja kojim se želi omogućiti bezbrižno učešće u Internet svijetu.Takva

Kontakt: Prof. dr Vesna Aleksić-Marić, dipl. ekon.
Ekonomski fakultet u Banja Luci
Majke Jugovića 4, 78 000 Banja Luka
E-mail : vesna.m@inecco.net

pravila se zove "netiquette", a svaka povreda tih pravila se naziva "abuse" radnja. Prilikom dobijanja korisničkog računa od ISP-a, svaki pojedinac automatski podliježe tim pravilima, te u skladu s tim i mogućim sankcionisanjem prilikom povrede istih. Brigu o lijepom ponašanju svojih korisnika nadgleda ISP-ova abuse služba (služba za pritužbe). Ukoliko primjetite bilo koji oblik nedozvoljenog i neprihvatljivog ponašanja, potrebno je isti prijaviti nadležnoj abuse službi.

Međutim, do narušavanja sigurnosti računara i računarskih sistema dolazi i zbog još nekih razloga. Prvi razlog čine greške u samim proizvodima, dok je drugi razlog loša konfiguracija i održavanje proizvoda od strane korisnika. Iako korisnik nije direktno i svjesno pričinio štetu, to ga neće osloboditi krivice zbog neznanja. Dakle, svaki korisnik mora paziti na svoje ponašanje na Internetu, ali također i paziti i brinuti o sigurnosti vlastitog računara kako ne bi došlo do propusta.

Prijava bi trebala sadržati slijedeće podatke:

- IP adresa napadača
- datum, tačno vrijeme i vremensku zonu napada
- kratki opis incidenta(najčešće se navodi u naslovu poruke)
- izvod iz log datoteke
- adresu elektronske pošte dojavljivača incidenta.

Svaki davalac Internet usluga ima svoju Abuse službu (abuse eng. zloupotreba, kršenje sklopljenog dogovora ). Abuse služba bavi se zapremanjem i obradom prijava u koje su uključeni korisnici pružaoca Internet usluga kojima Abuse služba pripada.

Abuse služba ima za cilj zapremanje i obrađivanje prijava vezanih uz računarsko sigurnosne incidente i zloupotrebu resursa kao što su:

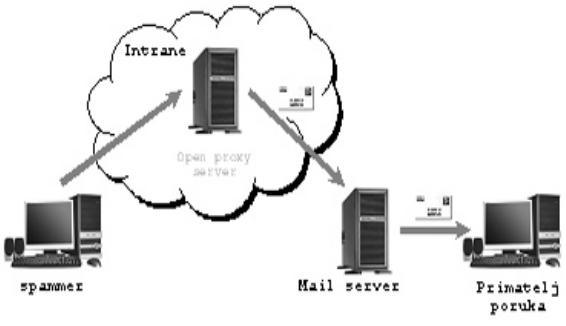
- spam
- netiquette
- virusi / crvi / trojanci
- povreda autorskih prava
- komercijalno korištenje
- neovlašteni pristup
- provale
- DoS
- DDoS

***OPEN PROXY – širenje malicioznih programa***

Pojam "Open proxy" u "abuse svijetu" predstavlja prekršaj računara/poslužioca koji je postao distributer neželjene pošte ( spam ) i drugih mailcioznih programa (virusa, crva, trojanskih konja).

Spam mail (Junk mail, neželjena pošta) je poruka najćešce reklamnog sadržaja. Putem e - maila dolaze obavještenja i reklame za proizvode za koje nikad niste izrazili interes, lažne poruke koje vode na stranice pornografskog sadržaja (na kojima gotovo uvijek možete pokupiti dialer, itd). Primjer iz svakodnevnog života koji bi najjednostavnije mogao dočarati spam jest dobijanje reklamnih papirića gotovo svakodnevno u naše poštanske sandučiće. Zabrinjavajuća je činjenica kako tri četvrtine svih e-mail poruka na Internetu su spam poruke, a svoj prilog sve većem broju spam poruka dali su i crvi koji se neumorno šire po Internetu, prikupljaju sve veći broj e-mail adresa te šalju neželjene poruke. Bitno je naglasiti kako je jedan od "najboljih" načina širenja malicioznih programa, koji šire spam, putem računara koji je zaražen malicioznim programom koji računar pretvara u odlazni poštanski poslužioc ( SMTP, outgoing mail server ), te na taj način lažno emituje veliki broj spam-a. I ne samo spam-a, već i samoga sebe kako bi pronašao druge potencijalne računare za pretvaranje u "open proxy"

Način na koji funkcioniše "open proxy" incident možete pogledati na slijedećoj slici:




*Slika1.*

Ukoliko počnete primati spam mailove, potrebno je zaglavlje (header) poruke poslati nadležnoj službi koja će upozoriti korisnika čije je računar slalo spamove da provjeri sigurnosni nivo svoga računara. Jedina zaštita od potencijalne zaraze s malicioznim programima koji kreiraju "open proxy" problem jest vatreni zid ( firewall ).

Zaglavlje poruke otkriva abuse službi IP adresu računara koji je emitovao spam kako bi mogla utvrditi ko je korisnik čije je računar izvršilo incident. Zaglavlja poruke u komercijalnim poštanskim klijentima se najčešće dohvati kombinacijom s tastature Ctrl+U , ili biranjem sa View ili Edit pa Header. Primjer jednog headera spam maila (obratite pažnju na crvene dijelove heareda maila):

Received: from nj-71-48-188-75.dyn.sprint-hsd.net (nj-71-48-188-75.dyn.sprint-hsd.net [71.48.188.75]) by nesto.srce.hr (8.13.4/8.13.4/Debian-3) with SMTP id j8C9Gim3022331 for <nesto@nesto.hr>; Mon, 12 Sep 2005 11:16:53 +0200
Received: from mail pickup service by 71.48.188.75 with Microsoft SMTPSVC; Mon, 12 Sep 2005 11:09:46 +0100
Received: from pszypoc ([176.180.234.63]) by 114.129.96.70 (8.12.53/8.12.60/YUA-6.27) with ESMTP id h8YItFBf6931524 for <nesto@nesto.hr>; Mon, 12 Sep 2005 08:08:46 -0200
Received: from 24.200.84.135 by 32.150.50.234 with Microsoft SMTPSVC(6.0.0553.6292); Mon, 12 Sep 2005 03:12:46 -0700
From: Mona <marshan@messiah-memphis.org>
To: nesto@nesto.hr
Subject: penny stox zfll
Date: Mon, 12 Sep 2005 13:08:46 +0300
Message-ID: <4974239.1319472968.15563676839@posey-bmzmqrg24282203878769.%FROM_DOMAIN>
Mime-Version: 1.0
Content-Type: multipart/alternative; boundary="--007325307507944"
X-Spam-Status: No, Hits=2.591 required=5
X-Scanned-By: MIMEDefang 2.51 on 161.53.2.69 Status: RO Content-Length: 2005 X-UID: 1856 X-Keywords: ----007325307507944
Content-Type: text/plain;
Content-Transfer-Encoding: 7Bit SRGX - Hot STock for your Attention sufficeidentifydaybed

Crveni dijelovi prikazuju odakle je doputovao mail, te prikazuje kad je upućen mail, te u kojoj vremenskoj zoni pripada kako bi abuse služba znala tačno o kojem se korisniku radi. Nadležnu abuse službu za određene domene možete potražiti na WHOIS servisu[1].

Prikaz maila prijave abuse službi zbog širenja virusa:

### *Povreda autorskih prava*

U prethodnom dijelu članka koje je govorilo o "netiquettu", bilo je riječi o autorskim pravima. No, u "abuse svijetu" povredom autorskih prava se najčešće misli na uobičajenu pojavu skidanja pjesama i filmova preko Interneta, pribavljanja ilegalnih distribucija programa, te distribucija svega navedenoga. Poznati su P2P (peer-to-peer) programi uz čiju pomoć se sav sadržaj čija su autorska prava povrijeđenja distribuira nelegalno među sudionicima Interneta. Povreda ovih prava je izrazito osjetljive prirode obzirom na to da autori direktno ekonomski gube, te i sami angažuju kompanije koje se bave praćenjem povrede autorskih prava i hvatanjem distributera zaštićenog sadržaja. I u Republici Srpskoj je povećan broj povrede autorskih prava obzirom na povećanu dostupnost broadband pristupa Internetu.

Povreda autorskih prava (bilo da se radi o presnimavanju softvera, muzike ili nečeg drugog) po zakonima BiH može biti krivično djelo, prekršaj, a možete se suočiti i s građanskom parnicom za naknadu štete, ako vlasnik autorskog prava pokrene tužbu.

Iako sve to iz pozicije običnog korisnika računara zvuči pomalo nevjerojatno, u BiH je bilo slučajeva ljudi u čijim je domovima policija obavila pretragu nakon što je njihovu adresu pronašla kod nekog pirata. Samo jedna kopija npr. presnimljenog softvera teoretski može dovesti čak i do krivične odgovornosti. To znači: krivični dosje, novčana kazna, te (što će mnoge najviše zaboliti) oduzimanje računara i ilegalnih sadržaja.

### *Prekršaj*

Evo jednog primjerka povrde autorskih prava zbog skidanja filma "The Stepford Wives". Kao što je prethodno pomenuto, brojne autorske kuće angažuju posebne firme koje će pratiti i "hvatati" one koji krše autorska prava njihovih klijenata. U ovom slučaju, abuse služba je primila prijavu od BayTSP, Inc. u ime Paramouth Pictures o ilegalnoj ditribuciji filma njihovog klijenta, te očekuje sankcioniranje prestupnika[2].

Original Message -----
From: <xxx-alert@nesto.cac.psu.edu>
To: <abuse@nesto.hr>
Sent: Thursday, mjesec 16, 20xx 10:07 PM
Subject: Virus received from xxx.xxx.yyy.yyy

This is an automatically generated message.
Please inform us if abuse@nesto.hr is not the correct abuse address by replying to this email with CHANGE in the subject line, and supplying the correct address.

[This is infected email number 1 we have received from xxx.xxx.yyy.yyy]

A message containing a virus originated from a system on your network.
Please contact the owner and ask them to clean up their system.
Sophie found the W32/Netsky-C virus.
Here are the message headers:
---

Return-Path: <posalo@nesto.com>
Received: from psu.edu (nesto1234.nesto.mreza.hr [xxx.xxx.yyy.yyy]) by tr11n05.aset.psu.edu (amavis-milter) id hgfkfhsdhf837mn8232;
Thu, 16 Dec 2004 16:07:44 EST
From: poslao@netko.com
To: nije@bitno.edu
Subject: Re: Re: Re: Re:
Date: Thu, 16 mjesrc 20xx 22:07:42 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----
=_NextPart_000_0005_00005800.00001C74"
X-Priority: 3
X-MSMail-Priority: Normal

Evo kako izgleda prijava:

Dear Sir or Madam:
BayTSP, Inc. ("BayTSP") swears under penalty of perjury that Paramount Pictures Corporation ("Paramount") has authorized BayTSP to act as its non-exclusive agent for copyright infringement notification.
BayTSP's search of the protocol listed below has detected infringements of Paramount's copyright interests on your IP addresses as detailed in the attached report.
BayTSP has reasonable good faith belief that use of the material in the manner complained of in the attached report is not authorized by Paramount, its agents, or the law. The information provided herein is accurate to the best of our knowledge.
Therefore, this letter is an official notification to effect removal of the detected infringement listed in the attached report. The Berne Convention for the Protection of Literary and Artistic Works, the Universal Copyright Convention, as well as bilateral treaties with other countries allow for protection of client's copyrighted work even beyond U.S. borders. The attached documentation specifies the exact location of the infringement.
We hereby request that you immediately remove or block access to the infringing material, as specified in the copyright laws, and insure the user refrains from using or sharing with others Paramount's materials in the future (see, 17 U.S.C. §512).
Further, we believe that the entire Internet community benefits when these matters are resolved cooperatively. We urge you to take immediate action to stop this infringing activity and inform us of the results of your actions. We appreciate your efforts toward this common goal.
Please send us a prompt response indicating the actions you have taken to resolve this matter. Please reference the Notice ID number above in your response.
Nothing in this letter shall serve as a waiver of any rights or remedies of Paramount with respect to the alleged infringement, all of which are expressly reserved. Should you need to contact me, I may be reached at the following address:
Mark Ishikawa
Chief Executive Officer
BayTSP, Inc.
PO Box 1314
Los Gatos, CA 95031
v: 408-341-2300
f: 408-341-2399
paramount-picture@copyright-compliance.com

### *Skeniranje portova i ostali incidenti*

Port skeniranje je tehnika koja se koristi kod provjere računarskog operativnog sistema kako bi se utvrdilo koji su TCP/IP portovi (ulazi) otvoreni. Analogija portu jest poziv na jedan telefonski broj (centralu) i preusmjeravanje na lokalni broj. Uz pomoć portova se omogućuje spajanje s više IP adresa TCP/IP protokolom na isti poslužioc. Standardni TPC/IP stack omogućuje 65535 različitih portova, koji se dijele na tri grupe:

- poznati portovi : 0 - 1023
- registrirani portovi : 1024 - 49151
- dinamički (privatni) portovi : 49152 - 65535

Evo popisa nekih od najčešće korištenih portova:

| |
|---|
| **echo** 7/tcp |
| **discard** 9/tcp |
| **qotd** 17/tcp #quote |
| **ftp-data** 20/tcp |
| **ftp** 21/tcp |
| **ssh** 22/tcp # SSH Remote Login Protocol |
| **telnet** 23/tcp |
| **smtp** 25/tcp #mail |
| **time** 37/tcp #timeserver |
| **domain** 53/tcp # name-domain server |
| **gopher** 70/tcp # Internet Gopher |
| **finger** 79/tcp |
| **www** 80/tcp # WorldWideWeb HTTP |
| **www** 80/udp # HyperText Transfer Protocol |
| **pop3** 110/tcp # POP version 3 |
| **sunrpc** 111/tcp # RPC 4.0 portmapper TCP |
| **auth** 113/tcp #authentication tap ident |
| **nntp** 119/tcp # USENET News Transfer Protocol |
| **ntp** 123/udp # Network Time Protocol |
| **imap2** 143/tcp # Interim Mail Access Proto v2 |
| **snmp** 161/udp # Simple Net Mgmt Proto |
| **irc** 194/tcp # Internet Relay Chat |
| **irc** 194/udp |
| **ldap** 389/tcp # Lightweight Directory Access Protocol |
| **https** 443/tcp # Secure HTTP |
| **mysql** 3306/tcp # MySQL |
| **ircd** 6667/udp # Internet Relay Chat |
| **webcache** 8080/tcp # WWW caching service |

*pgp public key is available on the key server at ldap://keyserver.pgp.com

Note: The information transmitted in this Notice is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, reproduction, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from all computers.
This infringement notice contains an XML tag that can be used to automate the processing of this data. If you would like more information on how to use this tag please contact BayTSP.
Infringed Work: Stepford Wives, The
Infringing FileName: Movie_The Stepford Wives (1974).avi
Infringing FileSize: 734992384
Protocol: OpenNap
Infringers IP Address: 193.198.xxx.xx
Infringer's User Name: Looser
Infringer's DNS Name: stroj.domena.hr
Initial Infringement Timestamp: 24 mjesec 20xx 12:38:59 GMT
Recent Infringement Timestamp: 24 mjesec 20xx 13:43:07 GMT

Što se tiče direktnog skeniranja portova, nerijetko se događa kako računari/poslužioci koji su zaraženi malicioznim programima (virusima, crvima, trojanskim konjima) koriste tehniku skeniranja portova kako bi se umnožili i raspodijelili na druge računare na mreži, te tako širili svoje štetno djelovanje. Skeniranjem portova se utvrđuje ranjivost, "otvorenost" računara za ubacivanje zlonamjernog kôda. Najbolja zaštita Vašeg računara je pomoću vatrenog zida (firewalla), međutim, sve pokušaje skeniranja iznimno je bitno prijaviti nadležnoj abuse službi kako bi ista upozorila vlastitog korisnika na sigurnosni propust koji se javlja s njegovog računara (bilo to namjerno ili nenamjerno). Log zapise iz Vašeg vatrenog zida potrebno je dostaviti u prijavi nadležnoj abuse službi.
Skeniranje portova samo po sebi nije zlonamjerna akcija jer postoje programi pomoću kojih administratori provjeravaju ranjivost svojih poslužioca. Prikupljanje informacija o ranjivosti računara na mreži i iskorištavanje istih informacija radi nanošenja štete je kažnjivo i spada u teže prekršaje svih abuse službi[1].

**Primjer jedne prijave abuse službi zbog skeniranja porta 7748:**

Subject: Scanning from xxx.53.xxx.xxx
From: cert@cert.dk
Date: Sat, 11 mjesec 20xx 21:08:21 +0100
To: abuse@nesto.hr

Dear Administrator,

We recieved a complaint about networkscan from IP 161.53.xxx.xxx. Please see the attached set of logs from the security software. It might be that your host has been taken over by intruders. Please disconnect IMMEDIATELY this host and investigate its security status. Otherwise please identify your customer operating from the above address at the time mentioned, and terminate immediately his hacking activities.
Please prevent him from continuing these kind of activities in the future as well.
This incident has been assigned the following number:

DK*CERT#xxxxxx

For future reference, please include this number in the subject line of your e-mail.

Best regards,

DK*CERT Abuse Team,
DK*CERT UNI*C

If nothing else mentioned below, timezone is believed to be UTC+0100(CET)

Evo još nekih najčešćih abuse radnji:

DoS/DDoS napadi. DoS dolazi od Denial of Service, odnosno napad uskraćivanjem usluga. Radi se o vrsti napada u kojem se obično namjernim generisanjem velike količine mrežnog saobraćaja nastoji zagušiti mrežna oprema i poslužioci. Isti postaju toliko opterećeni da više nisu u stanju procesirati legitimni saobračaj što na kraju ima za posljedicu da legitimni korisnici ne mogu koristiti mrežne usluge poput maila weba i sl. DDoS dolazi od Distributed Denial of Service, a radi se o obliku napada uskraćivanjem usluga u kojem su izvori zagušujućeg mrežnog saobračaja distribuirani na više mjesta po Internetu. Najčešće se radi o računarima na koja je prethodno provaljeno kako bi ih se iskoristilo za napad na druge mreže ili računare na Internetu[1].

[1] Slijedi prijava jednog DDoS napada slanjem UDP paketa:

Hi,
I wanted to let you know that one of our webservers received a ddos attack from one of the boxes hosted on your network, you might want to check it:
Date: 21.mjesec.20xx

04:35:31.422783 161.53.xxx.xxx.33259 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.422791 161.53.xxx.xxx.33259 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.422795 161.53.xxx.xxx.33259 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.422804 161.53.xxx.xxx.33259 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.422844 161.53.xxx.xxx.33259 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.422853 161.53.xxx.xxx.33259 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.423105 161.53.xxx.xxx.33258 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:35:31.423114 161.53.xxx.xxx.33258 > 69.31.xxx.xxx.pop3: udp 10 (DF)
04:37:58.411008 161.53.xxx.xxx.33253 > 69.31.xxx.xxx.domain: 12337 op6$ [b2&3=0x3233] [13879a] [13365q] [14393n] Type0 (Class 0)? .[|domain] (DF)
04:37:58.411012 161.53.xxx.xxx.33253 > 69.31.xxx.xxx.domain: 12337 op6$ [b2&3=0x3233] [13879a] [13365q] [14393n] Type0 (Class 0)? .[|domain] (DF)
04:37:58.411061 161.53.xxx.xxx.33253 > 69.31.xxx.xxx.domain:

*Phishing***.** Phishing označava skup aktivnosti kojima neovlašteni korisnici korištenjem lažnih poruka elektronske pošte i lažnih web stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih ličnih podataka. Ovo najčešće, zbog neznanja, zna biti veliki financijski šok prilikom otkrivanja prevare. Naime, osobe koje nisu upućene u nesigurnost Interneta kao javnog servisa znaju ostavljati brojeve kreditnih kartica na takozvane "povjerljive" web sadržaje koji iskoriste primljene informacije, te finacijski oštete posjetioca "povjerljivih" web stranica.

### *PROCJENA RANJIVOSTI ILI UPRAVLJANJA RANJIVOSTIMA*

U čemu je razlika između procjene ranjivosti ("Vulnerability Assessment) i upravljanja ranjivostima ("Vulnerability Management")? Procjena ranjivosti je tehnička aktivnost koja se obično provodi ne prečesto, ponekad i neredovno. Obuhvata provjeru prisutnosti eventualnih tehničkih nedostataka i ranjivosti na mrežnim resursima, a ponajprije se provodi na perimetarskom dijelu informacionog sistema. Ako se provodi kako treba, procjena ranjivosti će u jednom trenutku dostići kritičnu tačku: broj resursa koje treba provjeriti naglo raste, frekvencija provjere zauzima nerijetko i nedeljnu dinamiku, u provjeru se uključuju i druga mjesta u organizacionoj hijerarhiji (ne samo mrežni tehničari već i vođe sigurnosti, revizori, rukovodioci, administratori nemrežnih sistema...), provjera se počinje provoditi i na internim resursima... Procjena ranjivosti kao tehnička aktivnost prelazi u proces i nastaje upravljanje ranjivostima.

Izvještaji o utvrđenim ranjivostima prelaze u detaljan "workflow" koji uključuje i osobe nadležne za implementaciju popravaka, vlasnike resursa, a ponekad i revizore. Upravljanje ranjivostima reflektuje se i na "compliance" proces.

### *Čiji je zadatak provjeravati sigurnosne mjere?*

Svaki program upravljanja informacionom sigurnošću biće nekompletan (i nedjelotvoran) ako ne uključuje i redovnu provjeru ispravnosti i pridržavanja propisanih mjera. Redovna provjera (naziva se i "auditing", "assessment"...) jedna je od ključnih aktivnosti složenog procesa koji svim zaintereseranim stranama mora pružiti garanciju o adekvatnosti i djelotvornosti sigurnosnih procesa. Nije jedini - postoje i druge aktivnosti kako kroz horizontalni tako i kroz vertikalni pogled - no svakako je najkompleksniji i s najintenzivnijim doticajima prema komplementarnim aktivnostima. Provjera sigurnosnih mjera se kod nas najčešće percipira kroz dva izvođenja. Jedan oblik susrećemo preko revizija poslovnih sistema, čiji plan realizacije mora obuhvatiti i provjeru rada informacionih sistema, te daje ocjenu o potencijalnim nedostacima koji mogu uticati na izvedbu poslovnog sistema. Drugi oblik susrećemo preko tzv. penetracijskih testiranja. Ova izvedba obično nije formalno pozicionirana kao poslovna revizija, a svojim je obuhvatom usmjerena prije svega na tehnički aspekt nekog dijela informacionog sistema.

I to je, manje-više sve. No, provjera sigurnosnih mjera mora biti definisana sveobuhvatnije. Područja primjene danas su raznolikija od revizijskih aktivnosti i testiranja novih aplikacija. Pojavom regulatornih propisa, definicijom sigurnosnih standarda ili barem isticanjem smjernica o sigurnosnim mjerama, odgovornošću uprava kompanija za djelotvornost sigurnosnog sistema i nekim drugim pokretačkim momentima, sigurnosna provjera je aktivnost za koji uprave kompanija moraju biti i te kako zainteresirani.

Provjera sigurnosnih mjera mora krenuti od dobre definicije samih sigurnosnih mjera. One moraju biti dobro strukturirane već u fazi njihovog donošenja, propisivanja i izvođenja, a nakon toga treba se osigurati mehanizam njihove kontinuirane provjere, poređenja s očekivanim ili prihvatljivim rezultatima, te generisati smislene indikatore koji će ukazivati na odstupanja ili će omogućiti mjerenje djelotvornosti pridržavanja sigurnosnih mjera.

Provjera sigurnosnih mjera mora biti dio nadležnosti i odgovornosti poslovne cjeline koja upravlja informacijskom sigurnošću i pri tome je veoma važno očuvati neovisnost od dijela organizacie koji operativno provodi pojedine sigurnosne mjere (čitaj, dakle, od službe informatike).

---

12337 op6$ [b2&3=0x3233] [13879a] [13365q] [14393n] Type0 (Class 0)? .[|domain] (DF)
04:37:58.411067 161.53.xxx.xxx.33253 > 69.31.xxx.xxx.domain: 12337 op6$ [b2&3=0x3233] [13879a] [13365q] [14393n] Type0 (Class 0)? .[|domain] (DF)
04:37:58.411076 161.53.xxx.xxx.33253 > 69.31.xxx.xxx.domain: 12337 op6$ [b2&3=0x3233] [13879a] [13365q] [14393n] Type0 (Class 0)? .[|domain] (DF) --

Best Regards,

Nemojte zaboraviti da provjera sigurnosnih mjera mora imati dodir s procesom provjere i otklanjanja računarskih ranjivosti ("Vulnerability Management"), s testiranjem aplikativnih sistema u razvojnom ciklusu, s internom revizijom, s "compliance" incijativama, s upravljanjem operativnim rizicima, s forenzičkim aktivnostima...

Stoga, provjera sigurnosnih mjera mora postati dobro definisan proces koji neće biti izolovan od drugih cjelina (a naročito ne od službe informatike). Potrebno je očuvati nevisnost, vjerodostojnost i preciznost provjera, obuhvatiti organizacione, administrativne i tehničke sigurnosne mjere, a indikatori i izvještaji moraju biti dostupni svim poslovnim cjelinama koje, svaka na svoj način, doprinose ukupnom uspjehu programa informacione sigurnosti.

### *A zašto obratiti pažnju na ethical hacking*

Ovom pribjegavamo baš iz razloga svega gore uznesenog. Da zaključimo: Nevjerovatno, ali gotovo uvijek dolazi do povreda tajnosti, cjelovitosti i dostupnosti računarskih podataka programa ili sistema. Uvijek moramo imati na umu sljedeće:

(1) Ko uprkos zaštitnim mjerama neovlašteno pristupa računarskom sistemu…

(2) Ko s ciljem onemogućava ili otežava rad ili korištenje računarskih podataka ili programa, računarskog sustema ili računarskih komunikacija…

(3) Kazniće se ko neovlašteno ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ili nedostupnim tuđe računarske podatke ili programe

(4) Kazniće se ko presretne ili snimi nejavni prenos računarskih podatka koji mu nisu namijenjeni prema računarskom sistemu, iz njega ili unutar njega, uključujući i elektromagnetske emisije računarskog sistema koji prenosi te podatke, ili ko omogući nepozvanoj osobi da se upozna s takvim podacima

(5) Ko neovlašteno izrađuje, nabavlja, uvozi, rasparčava, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računarske podatke ili programe stvorene ili prilagođene za činjenje krivičnog djela iz stava 1., 2., 3. ili 4. ovoga clanka…

Zato je i opravdano dalje postaviti i proučiti šta je ethical hacking ?

***Ethical hacking*** (white hat hacking) je prema tome:

- istraživački rad (eng. security research) koji podrazumjeva:

- pronalaženje sigurnosnih propusta u operativnim sistemima, komercijalnim i open-source aplikacijama…

  - u skladu s profesionalnom etikom

    RFP policy (http://www.wiretrip.net/rfp/policy.html)

    Symantec (http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf)

- komercijalni penetracijski testovi/ispitivanja sigurnosti

  - u strogo kontrolisanim uslovima u skladu s opsegom i metodologijom ispitivanja

Ethical hacking zahtijeva sveobuhvatno tehničko znanje, nužan profesionalan pristup i prezentaciju rezultata prilagođenih managementu, kao i penetracijske testove/ethical hacking u skladu s poslovnim zahtjevima i procjenom rizika - neizostavan dio procesa upravljanja informacionom sigurnošću.

### *ŠTA JE INFORMACIONA SIGURNOST?*

Informacija je imovina i kao takvu ju je potrebno skladno zaštititi, kako bi se omogućilo normalno poslovanje organizacije. Taj zahtjev postaje sve važniji zbog distribuiranosti poslovne okoline, jer su u takvom okruženju informacije izložene većem broju prijetnji i ranjivosti. Informacije se javljaju u više oblika. Mogu biti zapisane na papiru, pohranjene u elektronskom obliku, sačuvane na filmu, mogu se prenositi poštom ili elektronskim putem. Bez obzira u kojem je obliku pohranjena informacija, ona uvijek mora biti skladno zaštićena.

Pod pojmom informacione sigurnosti podrazumijeva se zaštita informacija od velikog broja pretnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat od investicija. Informaciona sigurnost se postiže primjenom odgovarajućih kontrola, koje se odnose na sigurnosnu politiku, procese, procedure, strukturu organizacije i funkcije sklopovske i programske opreme. Navedene kontrole je potrebno osmisliti, implementirati, nadzirati, pregledavati i poboljšavati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahtjeva organizacije.

### *Zašto je važna informacijska sigurnost?*

Informacije i pripadni procesi, sistemi i mreže su važan dio poslovne imovine. Definisanje, implementacija, održavanje i poboljšavanje informacione sigurnosti može biti od presudne važnosti kako bi se ostvarila i zadržala konkurentnost, osigurao dotok novca i profitabilnost, kako bi se zadovoljile zakonske norme i osigurao poslovni ugled. Organizacije se suočavaju s brojnim sigurnosnim prijetnjama poput računarskih prevara, špijunaže, sabotaže, vandalizma, požara, poplave i sl. Šteta nanesena organizaciji u obliku zloćudnog koda, računarskog hakerisanja i uskraćivanja usluge je sve prisutnija pojava. Informaciona sigurnost je jednako važna javnim i privatnim organizacijama. Povezanost javnih i privatnih računarskih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uslovima oblici centralizovane kontrole nisu djelotvorni. Upravljanje informacionom sigurnošću zahtjeva učestvovanje svih zaposlenih u organizaciji, a često je potrebna pomoć konsultanata izvan granica organizacije.

### *Definisanje sigurnosnih zahtjeva*

Tri glavne kategorije za definiranje sigurnosnih zahtjeva su:

- Procjena rizika, uzimajući u obzir poslovnu strategiju organizacije i njezine ciljeve. Kroz procjenu rizika se identifikuju prijetnje imovini organizacije i njezina ranjivost. Također, određuje se vjerojatnoća pojave prijetnji i njihov uticaj na organizaciju ukoliko se te prijetnje realizuju.
- Legalne, ustavne, zakonske i ugovorne obveze koje organizacija mora zadovoljiti.
- Skup ciljeva, načela i poslovnih zahtjeva organizacije.

### *Procjena rizika*

Sigurnosni zahtjevi se identifikuju metodičkom procjenom sigurnosnih rizika. Proširenje sigurnosnih kontrola mora biti proporcionalno šteti koju sigurnosni propusti nanose organizaciji. Rezultati procjene rizika pomažu u određivanju prioriteta i prikladnih akcija kod upravljanja sigurnosnim rizicima. Procjena rizika se mora provoditi periodično kako bi se u procjenu uključile bilo kakve promjene koje bi mogle uticati na rizik.

### *Izbor odgovarajućih kontrola*

Nakon što se identifikuju sigurnosni zahtjevi i napravi procjena rizika, potrebno je izabrati i implementirati prikladne kontrole kako bi se rizik sveo na prihvatljiv nivo. Izbor kontrola ovisi o organizaciji, odnosno prihvatljivosti rizika i načinu upravljanja rizikom, ali i o nacionalnim i međunarodnim zakonskim pravima i obvezama.

### *Početna tačka u postizanju informacione sigurnosti*

Kontrole presudne za organizaciju sa zakonske tačke gledišta su:

a) zaštita informacija i tajnosti ličnih podataka;
b) čuvanje organizacijskih izvještaja;
c) poštivanje prava intelektualnog vlasništva.

Kontrole koje u praksi postižu dobre rezulate kod implementacije informacione sigurnosti su:

a) sigurnosna politika;
b) podjela odgovornosti informacione sigurnosti;
c) svijest o informacionoj sigurnosti, edukacija i trening;
d) ispravno procesiranje podataka u aplikacijama;
e) upravljanje ranjivostima;
f) upravljanje poslovnim kontinuitetom;
g) upravljanje sigurnosnim incidentima i poboljšanjima sistema.

## *PROCJENA I OBRADA RIZIKA*

### *Procjena rizika*

Procjena rizika je postupak identifikovanja, kvantifikovanja i utvrđivanja prioriteta rizika u ovisnosti o kriterijima za prihvaćanje rizika i ciljevima organizacije. Rezultat procjene rizika daje smjernice u upravljanu sigurnosnim rizicima i implementaciji kontrola za odbranu od rizika. Proces procjene rizika i izbor odgovarajućih kontrola se, po potrebi, provodi više puta da bi se obuhvatili svi dijelovi organizacije. Procjena rizika uključuje sistemski pristup procjenjivanju magnitude rizika (analiza rizika) i poredjenje procijenjenog rizika i kriterija rizika kako bi se utvrdila važnost rizika (evaluacija rizika). Procjena rizika se izvodi periodično zbog promjene sigurnosnih zahtjeva, tj. promjene imovine, prijetnji, ranjivosti, napada i evaluacije rizika. Procjena sigurnosnog rizika mora imati jasno definisan domet kako bi bila

efektivna. Takođe, mora uključivati odnose s rizikom u drugim područjima, ako je to prikladno. Domet procjene rizika može biti cijela organizacija, dio organizacije, pojedinačni informacioni sistem, pojedinačna komponenta sistema ili neka usluga koju nudi sistem.

### *Obrada rizika*

Prije nego se pristupi obradi rizika, potrebno je odrediti kriterije za prihvaćanje rizika. Rizik se prihvaća ukoliko je, na primjer, procijenjeni rizik mali ili trošak obrade rizika nije prihvatljiv organizaciji. Za svaki procijenjeni rizik mora se donijeti odluka o obradi rizika. Neki od postupaka obrade rizika su sljedeći:

a) primjena odgovarajuće kontrole kako bi se reducirao rizik;

b) svjesno i objektivno prihvaćanje rizika kako bi se ispoštovala sigurnosna politika i kriteriji prihvaćanja rizika;

c) izbjegavanje rizika nedopuštanjem akcija koje mogu prouzrokovati pojavu rizika;

d) prebacivanje rizika na neke druge stranke, tj. dobavljače ili lica koja osiguravaju instituciju;

Ako je donesena odluka o implementaciji kontrole, onda kontrole trebaju osigurati da se rizik reducira na prihvatljiv nivo, uzimajući u obzir:

a) zahtjeve i ograničenja nacionalnih i međunarodnih zakona i propisa;

b) organizacione ciljeve;

c) operativne zahtjeve i ograničenja;

d) trošak implementacije mora biti proporcionalan organizacionim zahtjevima i ograničenjima;

e) trošak implementacije kontrole mora biti proporcionalan šteti koju organizaciji može prouzrokovati sigurnosni propust.

Već pri postupku specificiranja i dizajniranja sistema potrebno je razmotriti koje kontrole su prikladne za taj sistem. Ukoliko se to ne učini, mogu se javiti propusti u vidu nedjelotvorne kontrole ili dodatnog troška. U najgorem slučaju može biti nemoguće uvesti sigurnosnu kontrolu u kasnijim fazama izgradnje sistema. Potrebno je imati na umu da ne postoji skup kontrola koji bi u potpunosti bio djelotvoran pa je potrebno dodatnim nadzorom, evaluacijom i poboljšavanjem kontrola povećati njihovu efikasnost.

### *SECURITY POLICY*

Sigurnosna politika je važan korak za ugradnju sistema za upravljanje informacionom sigurnošću unutar neke organizacije. Sigurnosna politika je u stvari hijerarhijski organizovan skup dokumenata koji na apstraktnom nivou pokrivaju bitne vidove informacione sigurnosti. Politike su dokumenti koji opisuju sigurnost na opštem nivou i ne daju detaljne tehničke specifikacije za njenu stvarnu implementaciju. Osnovni element svake politike je odluka. Politika određuje smjer u kojem je potrebno razvijati implementaciju sigurnosti na pojedinom nivou. Hijerarhijski najviši, a ujedno i najopštiji, je krovni dokument sigurnosne politike. Krovni dokument sigurnosne politike predstavlja odluku uprave i definiše opšti smjer u kojem je potrebno razvijati sistem upravljanja informacionom sigurnošću. Na osnovu krovnog dokumenta sigurnosne politike izrađuju se ostale politike koje definišu vidove sigurnosti unutar pojedinih segmenata informacionog sistema organizacije ili nje same.

Kreiranje sigurnosne politike ili politike u svrhu zaštite može se izvršiti (implementirati) u tri koraka:

- indentfikacija resursa,
- analiza prijetnji i
- eliminacija prijetnji.

Sada ćemo detaljnije opisati pojedini korak, koji čini zapravo jedan dokumnet na osnovu kojeg organizacije grade svoje zaštitne sisteme.

### *Indentifikacija resursa*

Prvi preduslov za uspješno upravljanje sigurnošću e-sistema podrazumijeva identifikaciju resursa, koji su dio tog sistema. Bez precizne identifikacije resursa nije moguće provesti njihovu kvalitetnu zaštitu. Kroz proces identifikacije resursa potrebno je pobrojati sve resurse unutar e-sistema, te procijeniti njihovu relativnu vrijednost za organizaciju. Da bi se mogla odrediti vrijednost resursa za organizaciju, potrebno je poznavanje poslovnih procesa koji se odvijaju u organizaciji. Na osnovu toga je kasnije u procesu upravljanja rizikom, odnosno prilikom analize rizika moguće djelotvorno ocijeniti potreban nivo zaštite za svaki pojedini resurs, bitan za funkcionisanje poslovnih procesa unutar organizacije.

Kvalitetnom identifikacijom resursa nužno je postići sljedeće zahtjeve:

- Ustanoviti vlasnike poslovnih procesa, odnosno odgovorne osobe.
- Identifikovati pojedine resurse bitne za funkcionisanje poslovnih procesa.
- Procijeniti vrijednost resursa.
- Ustanoviti njihovo fizičko ili logičko mjesto u sistemu.
- Napraviti odgovarajuću dokumentaciju.

***Podjela resursa***

Podjelu resursa moguće je napraviti prema raznim pravilima. U informacionim sistemima resurse je ugrubo moguće podijeliti u sljedeće kategorije:

- Informacije (baze podataka, dokumentacija, autorska djela, unutrašnje procedure, sigurnosne politike,itd.).
- Programska podrška (aplikacije, operativni sistemi, razvojni alati itd.).
- Oprema (računarska oprema, mrežno-komunikaciona oprema, mediji za pohranjivanje podataka i ostala oprema nužna za rad informacionog sistema).
- Servisi (računarski i komunikacioni, te opšti servisi, kao što su na primjer grijanje, osvjetljenje itd.).

***Analiza prijetnji***

Jednom indentifikovani resursi kao potencijalni na kojima se mogu desiti ili izvršiti napadi, trebala bi se analizirati zbog svih mogućih prijetnji koje su usmjerene prema tim resursima.Za pomoć u pronalaženju "svih" mogućih prijetnji i na kraju ponuda riješenja koje bi dovelo do njihova otklanjanja, dolazi od strane "policymakers-a", koji bi trebali ne samo istražiti kako svaki resurs može biti meta napada, nego i od kuda sve te prijetnje mogu doći, koja je namjera napadača. Međutim, moramo pomenuti da pojedine vrste napada uzrokuju različite oblike narušavanja sigurnosti. Navodimo samo neke od njih da i sam čitalac stekne nekakav osjećaj o kakvim je zapravo napadima riječ; gdje ih je moguće izvršiti, što oni zaparvo uzrokuju, te na kraju koji se zahtijevi postavljaju da bi se uspješno spriječile pojednine slabosti.

1.) U normalnim uslovima komunikacioni kanal prenosi nesmetano informacije iz izvorišta u odredište.Najjednostavniji način napada na sigurnost je prisluškivanje(eng. eavesdropping) ili presretanje (eng. intecepti on). Ako izvršimo klasifikaciju napada onda ovo možemo smjestiti u skup pasivnih napada (eng. Passiv attack), jer uljez (eng. Attacker, intruder) ne djeluje aktivno na informaciju. Prisluškivanjem se djeluje na povjerljivost (eng. confidentiality), odnosno tajnost(eng. secrecy) informacija.U ostalim načinima napada uljez mora djelovati na informacije, te se oni nazivaju aktivnim napadima (eng. Active attacks).

2.) Nadalje, možemo navesti da uljez može djelovati tako da prekine komunikacioni kanal između izvorišta i odredišta. Ta vrsta napada se naziva prekidanje(eng. Interruption), koje narušava raspoloživost (eng. availability) informacija. Još jedan mogući primjer koji narušava raspoloživost - uljez naprosto preplavi mrežu beskorisnim sadržajem (spam), čime dovodi mrežu u stanje zagušenja, te time i nemogućnosti dostupa do određenih usluga.

3.) Medjutim, uljez može prekinuti komunikacioni kanal i lažno se predstavljajući kao izvorište, promjeniti sadržaj poruke.Takva vrsta napada je promjena sadržaja poruke(eng. modification), koja narušava besprijekornost (eng. integrity) informacija.

4.) Uljez isto tako može uspostaviti komunikacioni kanal s odredištem i lažno se predstavljajući kao izvorište, slati mu izmišljene poruke. Takav napad se naziva izmišljanje poruka (eng. fabrication) koji narušva, kao i promjena sadržaja, besprijekornost ili integritet (eng. integrity) informacija.

5.) Posebni oblik narušavanja sigurnosti mogao bi biti takav, da ovlašteni korisnik opovrgava poruku koju je ranije poslao tvrdeći da je ona izmišljotina uljeza. Takav napad se naziva poricanje (eng. repudiation).

6.) Uljez isto može promjeniti adresu web stranice u DNS-u koja ima isti izgled kao web stranica pravog vlasnika, gdje se korisnik prilikom, recimo plaćanja računa, zapravo misleći da komunicira sa serverom banke na kojoj plaća račune, zapravo slijedeći proceduru plaćanja koja je između ostalog i davanje broja kartice, uljez iskoristi taj trenutak i uzme broj kartice korisnika koji od tog trenutka postaje sasvim bespomoćan. Gore smo naveli samo neke od mogućih scenarija i njegovih posljedica.

### *Eliminacija prijetnji*

Tek nakon indentifikacije resursa i analize prijetnji može se okrenuti na pronalaženje solucija za "eliminisanje" tih prijetnji. Naime, riječ eliminacija smo stavili pod navodnike, jer ipak nije moguće „zakrpiti" sve rupe koje se kriju u sistemu.Uvijek postoje neki propusti ili uvijek postoji domišljenost napadača (uljeza) da nanese štetu drugome, a ako je moguće u korist sebi. Na ono na što se obraća pažnja, je prevencija napada u smislu da napadač nemože ostvariti svoje zamisli, te nanijeti štetu drugome. Veliku ulogu u tom naravno igraju i vrste sistema koje navodimo: 1.)vojni informacioni sistemi, 2.)bankovni informacioni sistemi, 3.)zdravsteni i bolnički informacioni sistemi, 4.)infromacioni sistemi državnih institucija, 5.)informacioni sistemi osiguravajućih društava, 6.)poslovni informacioni sistemi državnih subjekata. Navedeni sistemi svojim redoslijedom naznačavauju i važnost (prioritet) u kreiranju politika zaštite. Između ostalog, osim nekakvih prioriteta, i financijska moć same organizacije utiče na donošenje politika zaštite. Znači, ukoliko preduzeće nemože preuzeti sve troškove jedne takve zaštite onda se mora suočiti sa određenim stepenom rizika. Sada ono mora ili samo odlučiti ili se pouzdati na osnovu nekih statističkih podataka koje resurse i do kojeg stepena sigurnosti ih osposobiti da obavljaju svoju funkciju zaštite.

Međutim, ovo što ćemo sada navesti, možda prelazi okvire same politike zaštite jer kao što smo naveli na početku, politika zaštite ne daje konkretna riješenja za uklanjanje problema, već na osnovu nje vrše to neke druge organizacije, koje na osnovu donešenih politika same donose najbolja riješenja u svrhu njihova ostvarenja.

U prethodnom pododjeljku (analiza prijetnji) smo naveli neke moguće napade, te njihove posljedice. Iz navedenih primjera se može ustanoviti da se sigurnost sistema zasniva na ispunjavanju u grubo, triju sigurnosnih zahtijeva (još jednom napomenimo da su zahtijevi povezani sa vrstom usluge, te mogućih napada na dotičnu uslugu, a ovo je samo jedan od recimo takvih primjera).To su: povjerljivost ili tajnost(informacije u sistemu smiju biti pristupačne samo ovlaštenim korisnicima), raspoloživost(informacije moraju uvijek biti na raspolaganju ovlaštenim korisnicima), besprijekornost (informacije u sistemu mogu mijenjati samo zato ovlašteni korisnici). Ovlašteni korisnici se moraju jednoznačno moći prepoznati. Jednoznažno prepoznavanje ovlaštenih korisnika obavlja se postupkom autentifikacije. Dodatno za osiguranje besprijekornosti autentifikujemo se ovlaštenim korisnicima, postupkom autorizacije – ona dozvoljava pristup samo određenim sadržajima. Dakle, kada se govori o sigurnosti onda se pominju ključne riječi kao što su: povjerljivost ili tajnost, raspoloživost, besprijekornost, autentifikacija, autorizacija, neporecivost.

Riješenja otklanajanja prijetnji (napada) može se riješiti hardverski, softverski ili u kombinaciji. Svi gore navedeni zahtijevi, osim raspoloživosti, mogu se dosta uspiješno riješti ili zadovoljiti uvođenjem kriptovanja.

### *UMJESTO ZAKLJUČKA (Top 10 savjeta)*

Ljudi su različiti. Ono što neko smatra normalnim, drugome se možda neće svidjeti. Upravo zbog toga moramo voditi računa jedni o drugima, a to znači biti spremni na međusobnu toleranciju, te na odgovornost za ono što radimo. Upravo zbog toga stvorene su određene norme kojih bi se trebalo pridržavati. Pojava spama u zadnjih nekoliko godina samo je pojačala potrebu pridržavanja pravila internetskog bontona.

Email shvatite kao mogućnost slanja poruke namijenjene jednoj osobi, odnosno kao neku vrstu dijaloga. Koristite ga kada trebate prenijeti informacije koje nisu od značaja za veći broj ljudi. Objavljivanje sadržaja maila trećim licima nije dozvoljeno, osim uz saglasnost oba sagovornika. Vlasništvo nad svakom mail porukom je ravnopravno podijeljeno izmedu pošiljaoca i primaoca. Sadržajem se može raspolagati samo uz obostranu saglasnost, osim ako se ne žalite administratoru na sadržaj poruke, kada vam ne treba suglasnost pošiljaoca.

Ako ste dobili dozvolu da mail proslijedite trećim ljudima, ne mijenjajte njegov sadržaj. Prema dogovoru, poruku možete skraćivati, tj. izbacivati nepotrebne dijelove, ali tako da ne narušite značenje prenošenog teksta.

Budite korak ispred računarskih problema! Informišite se i djelujte preventivno!

Redovno ažurirajte sigurnosne alate i operativni sistem.

1. Kreirajte sigurnosne kopije važnijih datoteka.
2. Ne zaobilazite sigurnosne dijaloge.
3. Koristite alternativne aplikacije.

4. Redovno mijenjati lozinke.
5. Pažljivo rukujte sa zaglavljem poruke elektronske pošte.
6. Čuvajte svoju privatnost i lične informacije.
7. Kreirajte i upotrebljavajte korisnički račun sa smanjenim ovlastima.
8. Ne odgovarjte na spam poruke (html image trick).
9. Redovno proveravajte postavke Dial-Up Networking ili Network Connecti-ons.

1. Redovno ažurirajte sigurnosne alate i operativni sistem. Redovno ažuriranje se odnosi i na vaš operativni sistem (najčešće Windows) i na aplikacije koje često koristite, posebno aplikacije koje imaju pristup Internetu. Najbolje je da redovno posjećujete stranice proizvođača sigurnosnih alata ili jednostavno koristite automatsko ažuriranje dostupno u većini antivirusnih alata (automatic update).

2. Kreirajte sigurnosne kopije važnijih datoteka. Time se osiguravate od gubitka podataka u slučaju nestanka struje, kvara računara ili napada nekog malicioznog programa.

3. Ne zaobilazite sigurnosne dijaloge. Kada odgovarate na sigurnosne upite, razmislite znate li šta je uzrokovalo pokušaj komunikacije te kakve posljedice ima radnja koju upravo poduzimate. Ako ne znate, pokušajte saznati.

4. Koristite alternativne aplikacije. Upotrebom alternativnih aplikacija i web brower-a u svako-dnevnom radu značajno smanjujete izloženost napadima. Alternativne aplikacije neće biti bez propusta, no njihovi propusti će u manjem broju biti poznati i korišteni pri izradi novih virusa, crva, spywarea i sličnih nametnika. Uz alterna-tivne aplikacije, za iznimne slučajeve, korisno je zadržati i one najrašireni je.

5. Redovno mijenjajte lozinke. Lozinke koje koristite za pristup Internetu, elektronskoj pošti ili internetskim stranicama koje omogućavaju online trgovinu ne smiju biti predvidljive. Dobra metoda postavljanja lozinke je skraćenica od 6 - 8 znakova (izaberite neku rečenicu koja će samo vama biti smislena) uz ubacivanje 2 - 4 interpunkcijska znaka ili broja. Također, poželjno je koristiti različite lozinke za različite resurse: npr. jednu za elektronsku poštu za Inernet bankarstvo, jednu za posao i sl.

6. Pažljivo rukujte s zaglavljem poruke elektro-nske pošte. Potrebno je biti siguran u njihov izvor i sadržaj. Razmislite od koga vam dolazi to zaglavlje, jeste li ga zatražili i znate li čemu služe datoteke s primljenim nastavkom. Ukoliko vam je nastavak nepoznat, trebate postupiti oprezno i provjeriti je li poruka poslata od nekoga kome vjerujemo.

7. Čuvajte svoju privatnost i lične informacije. Vaša fizička ili elektronska adresa, podaci o dobi, polu, potrošačkim navikama i mnoge druge, na prvi pogled, malo vrijedne informacije na crnom tržištu imaju svoju cijenu. Stoga svoje podatke u web formulare upisujte samo kada je to nužno i na stranicama čija je sigurnost i povjerljivost provjerena. Redovno brišite History vašeg web brower-a odnosno zapis adresa koje ste posjetili. To je posebno poželjno nakon trgovine putem Interneta jer stranice koje ste posjetili oglašivačima govore mnogo o vašim potrošačkim navikama. Svoju adresu ele-ktronske pošte ne objavljujte javno. Ako iz nekog razloga vaša adresa ipak mora biti objavljena na internetskim stranicama, onda to učinite tako da ona bude kriptirana. Na taj ćete način onemogućiti barem neke jednostavnije spammerske alate.Sigurnost protoka podataka između vas i stranice na koju ih upisujete označava simbol lokota u statusnoj liniji vašeg web brower-a i https umjesto http protokola u adresnoj liniji.

8. Kreirajte i upotrebljavajte korisnički račun sa smanjenim ovlastima. Korisnički račun sa smanjenim ovlastima najbolje je koristiti kada se spajate na Internet. Time znatno smanjujete mogućnost da netko preuzme kontrolu nad vašim računarom.

9. Ne odgovarajte na spam poruke (html image trick). Ne odgovarajte na spam poruke koje završavaju uputama kako se odjaviti s takvih mailing lista čime ćete prestati primati neželjene poruke. Pokušate li se na taj način odjaviti sa spammerskih lista, učinit ćete upravo suprotno. Dobije li spammer vaš zahtjev za odjavom s liste, to će mu samo biti potvrda da je adresa koju je negdje pribavio ispravna te da, što je možda još i važnije, poruke koje na nju stižu neko zaista čita.

10. Redovno provjeravajte postavke Dial-Up Networking ili Network Conne-ctions. Zbog specifičnih nametnika koji se preko Internet Explorera instališu na vaš računar i mijenjaju neke od postavki (najčešće Internet Settings), umjesto broja dial-up pristupa vašeg ISP-a, može se dogoditi da "svojevoljno" birate premi-um rate number neke daleke zemlje, zbog čega će se vaši telefonski računi višestruko uvećati.

***LITRATURA***

[1] *S.P. Miller, B.C. Neuman, J.I. Schiller, J.H. Saltzer*: "*Kerberos Authentication and Authorization System*", *Project Athena tehnical plan*, *section E.2.1*, 27. listopada 1988, ftp://athena.dist.mit.edu/pub/kerberos/doc/techplan.ps

[2] *J.G. Steiner, C. Neuman, J.I.Schiller*: "*Kerberos: An Authentication Service for Open Network Systems*", 30. ožujka 1988, ftp://athena.dist.mit.edu/pub/kerberos/doc/usenix.ps

[3] *B.C. Neuman, T. Ts'o*: "*Kerberos: An Authentication Service for Computer Networks*", USC/ISI Technical Report number ISI/RS-94-399, IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994, http://nii.isi.edu/publications/kerberos-neuman-tso.html

[4] *B. Ediger*: "*10 Reasons why OSF DCE sucks*", 1999., http://www.cnn.net/~bediger/anti_dce.html

[5]*P. Blackburn*: "*AFS distributed filesystem FAQ*", verzija 1.113, 26. siječnja 2000., http://www.angelfire.com/hi/plutonic/afs-faq.html

[6]"*How to Kerberize Your Site*", http://www.epm.ornl.gov/~jar/HowToKerb.html

[7] *M.Vandenwauver, R.Govaerts, J.Vandewalle*: "*Security of Client-Server Systems*", , *Information Security - from Small Systems to Management of Secure Infrastructures*, J.P. Eloff and R. von Solms, Ed., IFIP Press, May 1997, pp. 39-54., http://www.esat.kuleuven.ac.be/cosic/sesame/papers/wg11.2-7/index.html

[8] *N.Itoi, P.Honeyman*: "*Pluggable Authentication Modules for Windows NT*", 4. kolovoza 1998.,http://www.personal.engin.umich.edu/~itoi/ni_pam_usenix.pdf

Konferencije:

[9] InfoSeCon 2005, Information Security Conference Dubrovnik (Cavtat), Croatia; 6. - 9. lipnja 2005.

[10] Annual FIRST Conference on Computer Security Incident Handling, 2005 in Singapore

[11] 5th Workshop on Privacy Enhancing Technologies, Dubrovnik (Cavtat), Croatia; 30. svibnja - 1. lipnja 2005.