CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Pregled svjetskih organizacija u području informacijske sigurnosti

CCERT-PUBDOC-2008-08-238

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Upravljanje informacijskom sigurnošću složen je i zahtjevan posao, za kojeg još ne postoji dovoljno stručnjaka. U Hrvatskoj nema specijaliziranih škola ili smjerova za obuku stručnjaka za informacijsku sigurnosti. Zato se tim poslom uglavnom bave informatičari tehničkog usmjerenja, koje su organizacije poslale na dodatna školovanja, a ponekad i stručnjaci pravnog ili menadžerskog obrazovanja.

Uspješnost obavljanja tog posla uvelike ovisi o informiranju i praćenju novosti iz nekoliko različitih područja. Okolina u kojoj posluju današnje organizacije vrlo se brzo mijenja, pa je nužno pratiti zbivanja i reagirati na njih. Mijenjaju se uvjeti poslovanja, stanje na tržištu, pojavljuju se nove tehnologije, nove prijetnje, novi zakoni i propisi.

U dokumentu su navedeni izvori informacija koje bi svaki profesionalac koji se bavi računalstvom, a posebno informacijskom sigurnošću, trebao redovito pratiti. Odabrane su tvrtke i neprofitne organizacije koje su se specijalizirale za informacijsku sigurnosti i predstavljaju ozbiljne i pouzdane izvore informacija.

Informacijska sigurnost uobičajeno se definira kao briga za povjerljivost, cjelovitost i dostupnost informacija. Povjerljivost informacija ponekad je propisana zakonskom regulativom. Ponekad proizlazi iz poslovnih zahtjeva, iz ovisnosti poslovanja o zaštiti informacija koje su vrijedne i kritične za opstanak organizacije, ili su zaštićene kao autorska djela odnosno intelektualno vlasništvo. Zakonska regulativa integralni je dio brige za sigurnost, te zahtjeve zakonodavaca treba uključiti u sustav upravljanja informacijskom sigurnošću. Zato će se u dokumentu navesti mjesta na kojima su dostupne informacije o zakonima koji propisuju zaštitu podataka i informacijskih sustava.

Međunarodni standardi, odnosno norme, koji se odnose na informacijsku sigurnost izrađeni su kako bi organizacijama pomogli da uspostave sustav upravljanja informacijskom sigurnošću. Organizacije koje se potrude i steknu certifikate koji potvrđuju sukladnost sa zahtjevima međunarodnih normi, mogu na taj način zadovoljiti zahtjeve zakonodavca, a istovremeno steći povjerenje poslovnih partnera i kupaca, što im daje poslovnu prednost na kompetitivnom tržištu. Radi toga se spomenute organizacije kod kojih čitatelj može pronaći norme i standarde informacijske sigurnosti te mnoštvo korisnih uputa i savjeta o tome kako uspostaviti sustav upravljanja informacijskom sigurnošću.

Zapošljavanje osoblja s certifikatima iz područja informacijske sigurnosti također je jedan od zahtjeva koji doprinosi poboljšanju informacijske sigurnosti, te je radi toga navedena i referenca na listu certifikata koji su trenutno aktualni i poželjni.

Na kraju dokument donosi i izvore informacija koji su uže tehnički usmjereni, bilo da se radi o stranicama proizvođača programa i računalnog sklopovlja, antivirusnim tvrtkama, ali i organizacijama koje su specijalizirane za informacijsku sigurnosti, te nude mnoštvo novosti, testova, upozorenja na najnovije ranjivosti i slične teme.

Etičko hakiranje zasebna je disciplina unutar spektra poslova vezanih za informacijsku sigurnost. Hakeri se druže na mreži s kolegama, razmjenjuju znanje i alate, tvoreći zasebnu kulturu koja je zatvorena i teško prima nove članove. Oni su neka vrsta elite, a istovremeno i gerile, istovremeno komuniciraju i prikrivaju tragove, koriste zatvorene komunikacijske kanale i neprestano mijenjaju mjesta sastanka. Njihova je najnovija dostignuća teško pratiti, jer hakeri predstavljaju pokretnu metu i teško im je ući u trag.

Izraz haker isprva je označavao entuzijasta, željnog znanja, koji teži znanju i spreman je neprestano učiti. Nažalost, s pojavom elektroničkog kriminala, izraz je počeo dobivati negativne konotacije. Prvi hakeri razvijali su besplatna programska rješenja, nastojeći zaobići ekskluzivizam komercijalnih alata i omogućiti svima da koriste dobrobiti novih tehnologija. Kasnije se nekolicina počela baviti kriminalom, pa su ih, da bi se razlikovali od dobronamjernih tehnoloških fanatika, počeli nazivati *crackerima*. No taj se izraz nije udomaćio, pa su se pojavili novi izrazi: *etički haker* je na strani dobra, kao i *White Hat haker*, dok je *Black Hat haker* na strani zla i nudi svoje usluge za novac (ili neku drugu protuuslugu). I jedni i drugi otkrivaju ranjivosti i propuste u programskim rješenjima, a razlikuju se po tome što će sa tom spoznajom učiniti. U tom smislu je izraz „haker“ neutralan, tj. označava samo zagriženog stručnjaka, entuzijasta. Bavljenje informacijskom sigurnošću podrazumijeva i uvid u svijet *hakera/crackera*, bez obzira na boju šešira koji nose.

2. Legislativa i regulativa

ICT je djelatnost koja je svakim danom sve više „regulirana“, što znači da se povećava broj zakona, vladinih uredbi i smjernica kojima je propisana razina informacijske sigurnosti. „Compliance“, tj. poštivanje regulative, dio je zahtjeva koji se stavlja pred organizacije, a zahtjevi koje treba ispuniti ovise o području djelatnosti organizacije.

Republika Hrvatska žurno usklađuje svoje propise sa legislativom članica Europske unije i NATO saveza, što je jedan od uvjeta za pridruživanje tim organizacijama.

Krovne organizacije za pojedine vrste poslovanja zadužene su za propisivanje minimalnih standarda informacijske sigurnosti i rokova za njihovu primjenu. Narodna banka Hrvatske već je objavila niz obvezujućih smjernica. Očekuje se da svoj dio posla napravi i HANFA, koja bi trebala propisati uvjete kojih se moraju pridržavati tvrtke izlistane na burzi. Novoosnovani Zavod za sigurnost informacijskih sustava propisati će standarde za tijela državne vlasti i lokalne samouprave.

2.1. Strategija razvoja informacijske sigurnosti u Hrvatskoj

Središnji državni ured ze e-Hrvatsku „obavlja upravne i stručne poslove koji se odnose na razvitak informacijskog sustava državne uprave te uspostavu tehnološke i sigurnosne informatičke infrastrukture u tijelima državne uprave“. 2003. godine ovaj je ured osmislio program e-Hrvatska, koji predstavlja strateški okvir za razvoj informacijske sigurnosti u Republici Hrvatskoj. Plan je pokrivao razdoblje do 2007. godine, no njegova se provedba nastavlja i dalje. Svrha djelatnosti ureda je pretvaranje Hrvatske u informacijsko društvo, pa je tako jedan od njihovih projekata i Hitro.hr, koji bi trebao omogućiti građanima i poslovnim subjektima da na jednom mjestu zatraže i brzo dobiju usluge od tijela državne vlasti. E-uprava, e-pravosuđe, e-zdravstvo, e-obrazovanje i e-poslovanje dijelovi su cjelovitog sustava elektroničkih javnih usluga koji bi trebao biti interoperabilan i omogućiti integraciju u međunarodne programe, kao dio približavanja Hrvatske Europskoj uniji i NATO paktu.

2005. godine Središnji državni ured za e-Hrvatsku donio je Nacionalni program informacijske sigurnosti u Republici Hrvatskoj koji određuje strateški okvir za upravljanje informacijskom sigurnošću. Dostupan je na adresi:

http://www.e-hrvatska.hr/sdu/Dokumenti/StrategijeIPrograma.html

Radi se o dokumentu kojeg treba imati „pri ruci“, jer je u njemu oslikan cjelovit sustav zaštite informacija na svim razinama društvene organizacije, te navedena državna tijela čija je zadaća donošenje zakona, propisivanje standarda, edukacija specijalista i stanovništva, te provođenje i nadzor provođenja propisanih mjera.

Provedba je planirana u tri cjeline.

- Skupinu A čine tijela središnje izvršne vlasti i nacionalne sigurnosti:
  - Vlada i njezini uredi,
  - ministarstva,
  - diplomatska predstavništva i
  - obavještajne agencije
- Skupinu B čine ostala tijela državne vlasti:
  - Sabor,
  - pravosuđe,
  - Hrvatska narodna banka,
  - javni sektor i
  - lokalna samouprava

- Skupina C je privatni sektor:
  - Pravne osobe
  - i trgovačka društva bez obzira na tip vlasništva (privatno, državno ili miješano)

2.2. Zakoni i uredbe iz područja informacijske sigurnosti

Narodne novine nisu organizacija koje se bavi informacijskom sigurnošću, ali su primarni izvor za pronalaženje zakona i uredbi koje donose sabor i vlada, te krovne organizacije za pojedine djelatnosti poput Narodne banke Hrvatske. Pravnici uz svaki zakon navode broj Narodnih novina i godinu objavljivanja, pa su uz pomoć tih informacija u stanju pronaći tekst zakona. No tehničari će pojedine zakone potražiti uz pomoć Google tražilice. Ako im bar otprilike znaju naziv, u polje za pretraživanje dovoljno je upisati:

```
site:nn.hr Zakon o tajnosti podataka
```

Članke i komentare pronaći će na taj način da se pretraživanje ne ograniči na stranicu Narodnih novina, već se u polje za pretraživanje upiše samo naziv.

Pri tome propisi i zakoni te vladine uredbe s kojima bi se trebalo upoznati su:

2.2.1. Legislativa koja se odnosi na sve organizacije

- Zakon o elektroničkom potpisu (NN 10/02)
- Zakon o zaštiti osobnih podataka (NN 103/03)
- Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN 139/04)
- Zakon o pravu na pristup informacijama (NN 172/03)
- Zakon o elektroničkoj ispravi (NN 150/05)

2.2.2. Tijela državne vlasti i lokalne samouprave

- Zakon o sigurnosnim službama (NN 32/02)
- Zakon o informacijskoj sigurnosti (NN 79/07)
- Zakon o sigurnosno-obavještajno sustavu (NN 32/02)
- Zakon o tajnosti podataka (NN 79/07)
- Uredba o mjerama informacijske sigurnosti (NN 46/08)
- Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima (NN 72/07)
- Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima (NN 102/07)
- Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost (NN 100/08)

2.2.3. Banke i kreditne organizacije

- Odluka o primjerenom upravljanju informacijskim sustavom (HNB, NN 80/07)
- Smjernice za adekvatno upravljanje rizikom eksternalizacije (HNB listopad 2005.)
- Smjernice Za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika (HNB ožujak 2006.)
- Smjernice za ovladavanje rizikom informacijskog sustava u kreditnim unijama (HNB studeni 2007)

2.2.4. Ostale financijske institucije

- Pravilnik o detaljnom obliku i najmanjem opsegu te sadržaju revizorskog pregleda i revizorskog izvješća društava za osiguranje (NN 76/06)
- Pravilnik o uvjetima za obavljanje poslova ovlaštenog društva (NN 14/07)
- Pravilnik kojim se uređuje poslovanje društva za upravljanje investicijskim fondovima (NN 25/07)

U ovom popisu nedostaje jedan zakon koji na prvi pogled nije izravno vezan uz informacijsku sigurnost. Zakon o zaštiti i spašavanju (NN 174/04) u članku 18 propisuje da sve pravne osobe moraju pripremiti planove kontinuiteta poslovanja.

3. Međunarodne norme

Najvažniji međunarodni standardi iz područja informacijske sigurnosti su:

- ISO 27001 ISMS Requirements
- ISO 17799 Code of Practice for IT sec management
- BS 7799-3 Information security risk management
- BS 25999-1 Code of practice for business continuity management
- BS 25999-2 Specification for business continuity mangement

3.1. British Standards Institute

Velika Britanija prednjači u izradi međunarodnih normi, pa su mnoge ISO norme nastale iz britanskih, tako na primjer ISO 17799 potiče od britanskog standarda BS 7799. Stoga je posve opravdano na prvom mjestu ukazati na organizaciju BSI, *British Standards Institute*. Osim što nude na prodaju britanske i međunarodne standarde, BSI sudjeluje u njihovu razvoju, bavi se edukacijom, procjenom primjene standarda, certificiranjem organizacija i testiranjem proizvoda. Web adresa BSI organizacije je:

http://bsi-global.com

3.2. NIST

U SAD-u nacionalna organizacija za standarde je NIST, *National Institute of standards and Technology*, dostupna na adresi http://www.nist.gov. Njihova podružnica za računalnu sigurnost održava *Computer Security Resource Center*, http://csrc.nist.gov, gdje se nudi niz korisnih sadržaja.

Između ostalog, mogu se besplatno preuzeti „draftovi"ili nacrti razvojne verzije dokumenata koji obrađuje konkretne teme iz sigurnosti, na primjer:

- Draft SP 800-68 Rev 1, Guide to Securing Microsoft Windows XP Systems for IT Professionals
- Draft SP 800-121, Guide to Bluetooth Security
- Draft SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy
- SP 800-39 DRAFT Managing Risk from Information Systems: An Organizational Perspective

Nacrti se javno objavljuju kako bi ih svi zainteresirani mogli komentirati i tako doprinijeti kvaliteti konačne verzije. Konačne verzije dokumenata više nisu besplatne, moraju se kupiti.

3.3. Zavod za norme

Hrvatski zavod za norme usvojio je ISO 27001 kao hrvatsku normu HRN/ISO 27001:2006. Kopija norme, nažalost zasad samo na engleskom, može se kupiti u Zavodu, u Vukovarskoj 78. Planiraju uvesti i e-prodaju, ali je programsko rješenje još u razvoju. Više informacija na dostupne su na službenim web stranicama:

http://www.hzn.hr

3.4. Zavod za ispitivanje kvalitete (ZIK)

Unutar Zavoda djeluje odjel za informacijsku sigurnost, koji između ostalog objavljuje međunarodne norme i nudi obuku stručnih kadrova. ZIK je ovlašten od strane Britanskog instituta za standarde za prevođenje i distribuciju hrvatskih verzija normi.

Norme koje se mogu nabaviti preko ZIK-a su:

- BS/ISO/IEC 27001
- BS/ISO/IEC 17799
- BS 7799-3
- BS 25999-1
- BS 25999-2

Vrijedi spomenuti da se u ZIK-u može nabaviti prijevod knjige Alana Caldera iz IT Governance tvrtke: „Devet koraka do uspjeha, ISO 27001: Pregled primjene“.

4. Certifikati za različita područja informacijske sigurnosti

Profesionalci koji se bave informacijskom sigurnošću lakše će se zaposliti ili pronaći bolje plaćen posao ukoliko se pobrinu da steknu neki od certifikata koji potvrđuju njihovu stručnost. S druge strane, tvrtke koje nude konzultantske usluge iz područja informacijske sigurnosti također žele zaposliti certificirane profesionalce, jer to potencijalnim kupcima pruža povjerenje i olakšava dobivanje natječaja. Teret izgradnje informacijskog društva iznijeti će certificirane organizacije koje zapošljavaju certificirane stručnjake – tako, čini se, izgleda put u budućnost informacijskog društva.

Mnoštvo različitih organizacija i proizvođača opreme izdaju brojne certifikate vezane za različita područja informacijske sigurnosti. Iscrpan popis sigurnosnih certifikata nalazi se na stranicama organizacije IT Governance:

http://www.itgovernance.co.uk/training.aspx

5. Organizacije koje se bave informacijskom sigurnošću

U nastavku je izdvojeno nekoliko organizacija koje su stekle reputaciju i predstavljaju ozbiljan i pouzdan izvor informacija vezanih uz informatičku sigurnosti.

5.1. CERT

Computer Emergency Response Team je naziv za ekipu stručnjaka koji rješavaju sigurnosne incidente. Veće tvrtke mogu imati svoje timove, no CERT-ovi postoje i na razini grupacija (na primjer CARNetov CERT za akademsku zajednicu), te na nacionalnoj razini.

Zadaća je nacionalnih CERT-ova višestruka: oni prikupljaju podatke o sigurnosnim prijetnjama i incidentima, sudjeluju u rješavanju incidenata, pri izradi zakona i propisa iz područja informacijske sigurnosti, educiranju korisnika itd.

Uz CARNetov CERT, iz kojeg će se razviti i hrvatski nacionalni CERT, vrijedno je pratiti i stranice CERT-ova informatički razvijenih zemalja.

- CARNetov CERT: http://www.cert.hr
- USA CERT: http://www.us-cert.gov
- Australski CERT: http://www.auscert.org.au
- Britanski CERT: http://www.ukcert.org.uk/

5.2. SANS Institute

Među organizacijama koje se bave informacijskom sigurnošću s pretežno tehničkog stajališta, na prvom mjestu valja spomenuti SANS Institute. Naziv je skraćenica od *SysAdmin, Audit, Network, Security*. Osnovan je 1989. kao „kooperativna istraživačka i obrazovna organizacija".

Između mnogobrojnih djelatnosti instituta, najvažnije su:

- Treninzi iz informacijske sigurnosti – niz intenzivnih višednevnih tečajeva iz područja kao što su sigurno administriranje sustava, otkrivanje upada (Intrusion detection), hakerske tehnike itd.
- Certifikacijski program GIAC – cijenjeni certifikati iz područja sigurnog administriranja sustava, upravljanja, nadzora i sigurnosti softvera.

- Projekt sigurnosne politike – predlošći za izradu sigurnosne politike
- Internet Storm Center – Internetski sustav ranog uzbunjivanja: web stranica na kojoj se može pratiti trenutno stanje opasnosti na Internetu, predstavljeno bojama kao na semaforu. Storm center prati zbivanja na Internetu, priprema top listu najvećih prijetnji, te mjeri vrijeme koliko nezakrpan sustav može izdržati na Internetu, prije nego ga preuzmu napadači.
- ISC održava i top listu najvećih sigurnosnih rizika: http://www.sans.org/top20
- ISC Neprekidno mjeri vrijeme preživljavanja umreženih računala bez instaliranih zakrpa kao što je vidljivo na:

  http://isc.sans.org/survivaltime.html

Iako se radi o organizaciji koja posluje na komercijalnoj osnovi, na stranicama SANS-a pruža se i niz besplatnih usluga, poput pretplate na mailing liste, objavljenih različitih korisnih dokumenata i studija i dr.

5.3. IT Governance

IT Governance je tvrtka specijalizirana za pružanje usluga iz područja upravljanja IT službom, upravljanja rizikom, usklađivanja s regulativom, vođenja projekata i informacijske sigurnosti. Uz edukaciju i savjetovanje razvili su i zapaženu izdavačku djelatnost. Jedan od njihovih autora je poznati stručnjak za upravljanje informacijskom sigurnošću Alan Calder, autor nekoliko cijenjenih knjiga o standardima ISO 27001 i 17799. Razvili su i program koji olakšava uvođenje sustava upravljanja informacijskom sigurnošću, na primjer alate za procjenu rizika i izradu sigurnosne politike. Web adresa IT Governance tvrtke je:

http://www.itgovernance.co.uk

5.4. Secunia

Secunia je Danska tvrtka poznata po tome što prati ranjivosti za preko 12.000 različitih programa i operacijskih sustava. Secunia okuplja istraživače koji redovito testiraju ranjivosti, dokumentiraju ih, objavljuju analize i savjetuju kako se zaštiti. Nezavisni su i drže do reputacije beskompromisnih istraživača, koji usude objaviti detalje o ranjivosti usprkos protivljenju proizvođača programa u kojem je propust pronađen. Ranjivosti dobivaju oznaku SAxxxx (Secunia Advisory i redni broj), nakon čega se mnogi drugi izvori referenciraju na njihovu analizu.

Nudi se pretplata na mailing listu, pa će informacije o novim ranjivostima stizati svakodnevno, ili u tjednim sažecima.

Secunia nudi i sigurnosne programe, na primjer *Security Scanner*, koji napravi izvještaj o ranjivom softveru koji je instaliran na osobnim računalima u lokalnoj mreži. Također, nude i komercijalnu uslugu provjere ranjivosti.

http://secunia.com

5.5. Packet Storm

Portal koji se može koristiti u svrhu dobivanja izvornog koda *exploita* - programa koji iskorištavaju ranjivosti nekog programa. Stranica će biti korisna savjetnicima za sigurnost, koji će uz pomoć izvornog koda moći organizirati testiranje ranjivosti u svojim organizacijama, programerima kako bi naučili zaštititi svoje programe i etičkim hakerima koji mogu postojeće tehnike iskoristiti za otkrivanje novih ranjivosti. Radi se zapravo o „groblju“ *exploita*, jer ogromna većina više ne radi tamo gdje su primijenjene zakrpe. Na adresi http://packetstormsecurity.org/ nalazi se mnoštvo opisanih materijala. *Exploiti* su skupljeni pod naslovom „assessment“, grupirani prema operacijskom sustavu. Ostatak su različiti dokumenti, na

primjer savjeti kako se zaštiti, sigurnosna dokumentacija i slično. Dakle, osobama kojima je potreban virus i/ili trojanski kod određenih karakteristika, Packet Storm je dobro mjesto za početak pretrage.

5.6. SecuriTeam

Sličan site je i SecuriTeam, koji se diči sloganom: „Free//Accurate//Independent“. Na naslovnici objavljuju vijesti o najnovijim propustima koji su otkriveni u programima, povremeno s izvornim kodom za iskorištavanje ranjivosti (exploit), ali ovdje je moguće pronaći i korisne alate za provjeru ranjivosti raznih servisa, na primjer *PorkBid*, koji testira NDS servis, *ProxyStrike* za provjeru web servisa, ili popularni alat *NetCat* kojem je dodana podrška za SSL. SecuriTeam ne vjeruje da se sigurnost postiže prikrivanjem informacija, pa se ne ustručavaju objaviti programe za iskorištavanje ranjivosti kao npr. „Kaminsky DNS cache poisoning exploit“. Kaminsky je u ljeto 2008. uzbudio duhove otkrivši ranjivosti u DNS servisu, koje se mogu iskoristiti za *phishing*. SecuriTeam nudi i mogućnost pretplate na mailing listu.

SecuriTeam preporuča se svim praktičarima informacijske sigurnosti, kao izuzetno vrijedan izvor svježih informacija o ranjivostima, koda kojim se ranjivost može provjeriti i korisnih programskih alata za testiranje sigurnosti, provjeru rada protokola i slično.

http://www.securiteam.com

6. Proizvođači programa i sklopovlja računala

Vrijedan izvor informacija predstavljaju i tvrtke koje proizvode programe i računalne komponente. Na njihovim stranicama objavljuju se informacije o ranjivostima i načinima obrane, od instalacije zakrpa do promjena u konfiguraciji ili privremenog zaustavljanja pojedinih nesigurnih servisa.

Namjerno je odlučeno iste spomenuti iza nezavisnih organizacija koje otkrivaju i analiziraju ranjivosti, jer proizvođači komercijalnog softvera u pravilu kasne s objavom ranjivosti. To je donekle razumljivo, jer proizvođači moraju obaviti vlastitu analizu, ispraviti pogreške u programima, dokumentirati izmjene u kodu, izraditi zakrpe i obavijestiti javnost. Obično najprije izdaju umirujuću izjavu za javnost, tvrdeći da ranjivost nije tako opasna kao što tvrde istraživači, ili da još ne postoji *exploit* za tu ranjivost, i slično. Ponekad se razvija napetost između nezavisnih istraživača i proizvođača koji zahtijevaju da se ranjivost prvo prijavi njima, pa tek onda javno objavi. Međutim nezavisni istraživači tvrde kako javnim objavljivanjem znatno ubrzavaju izdavanje zakrpa, izražavajući na taj način nezadovoljstvo brzinom kojom se greške ispravljaju.

Od komercijalnih proizvođača programa u ispravljanju grešaka mnogo su brži proizvođači besplatnih - *open source* rješenja. To je razumljivo, jer ne moraju slijediti stroge procedure kao njihovi kolege iz komercijalnog sektora. Otvaranjem koda čak se potiče korisnike da traže greške i prijavljuju ih, tako da je broj ispravaka obično veći, što ne znači da je otvoreni softver a priori lošije kvalitete, nego da je u otvorenom kodu s vremenom sve manje skrivenih ili neotkrivenih grešaka.

O programima i sklopovlju kojeg čitatelj koristi ovisit će i čije web stranice bi bilo poželjno da pratiti. Ovdje su navedeni proizvođači koji su svojim proizvodima zauzeli većinski dio tržišta pa su time zanimljivi većem broju čitatelja.

6.1. Microsoft

Windowse koriste praktički svi, a njihovo korištenje nosi sa sobom i određene rizike. Microsoft mjesečno izdaje nove zakrpe, ponekad i češće, ukoliko se radi o ozbiljnim sigurnosnim problemima. Praćenje sigurnosnih novosti vezanih uz ovaj popularnih OS i njegove aplikacije mora biti dnevna rutina. Obavijesti su dostupne na:

http://www.microsoft.com/technet/security

6.2. Cisco

Najznačajniji proizvođač mrežno-komunikacijske opreme također je na udaru hakera.

Cisco Security Center na adresi:

http://tools.cisco.com/security/center/home.x

pomaže mrežnim administratorima u nastojanju da zaštite Ciscovu mrežnu opremu.

6.3. Linux

Mnogo je različitih distribucija Linuxa, ali postoji jedno središte koji se bavi sigurnošću Linuxa bez obzira na distribuciju - Linux Security, dostupan na adresi:

http://www.linuxsecurity.com

6.3.1. Debian

Debian Linux poznat je po brzim ispravcima otkrivenih grešaka. Debian ima svoj sigurnosni centar, gdje se objavljuju vijesti o novim ranjivostima i savjeti kako se zaštiti:

http://www.debian.org/security/

6.3.2. Red Hat

Red Hat izdaje Linux za poslovne korisnike, Red Hat Enterprise Linux. Uz sam programski dio, nudi kao dodatnu uslugu i profesionalnu podršku, a dio podrške su i sigurnosni savjeti. RHEL Advisory Center je dostupan na adresi:

https://rhn.redhat.com/errata

6.4. Proizvođači antivirusnih programa

Na stranicama proizvođača antivirusnog programa nalazi se mnoštvo korisnih sadržaja, od opisa novih virusa, učestalosti njihova pojavljivanja, do uputa za uklanjanje. Nazivi virusa ponekad variraju od jednog do drugog proizvođača. Nakon otkrivanja novih virusa mora se što prije objaviti potpis za njegovo prepoznavanje, pa nema uvijek prilike za usuglašavanje naziva. Radi toga je preporučljivo da korisnici prate informacije na stranicama onog proizvođača čiju antivirusnu zaštitu koriste, iako je ponekad nužno potražiti dodatne upute na stranicama konkurencije. Najpoznatiji proizvođači AV zaštite su:

- Sophos: http://www.sophos.com
- Norton: http://www.symantec.com/norton/antivirus
- Trend Micro: http://www.trendmicro.com
- F-Secure: http://www.f-secure.hr
- Panda: http://www.pandasecurity.com

7. E-časopisi koji prate informacijsku sigurnost

Svakodnevno praćenje svih nabrojenih web odredišta odnijelo bi dobar dio radnog dana. Mnogi si to ne mogu priuštiti. Za njih je možda bolje da se pretplate na sigurnosne rubrike nekog od ozbiljnih časopisa, čiji novinari prate događanja i izvještavaju o svim značajnim novostima. U nastavku poglavlja opisani su najznačajniji.

7.1. Computerworld

Takav časopis je i *Computerworld*, koji nudi besplatnu pretplatu na sažetke članaka iz pojedinih tematskih cjelina. Novinari vrlo dobro poznaju područje o kojem pišu, a autori su često i ICT stručnjaci. Kada se obrađuje neka tema, iznose se različita, često sukobljena mišljenja, tako da čitatelj može steći širok pogled na problematiku i sam odlučiti kojoj se strani prikloniti. Web adresa ovog zanimljivog e-časopisa je:

http://www.computerworld.com

7.2. CSO, Security and Risk

Tvrtka IDG, izdavač Computerworlda, izdaje i specijalizirani časopis namijenjen voditeljima sigurnosti:

http://www.csoonline.com

7.3. Portal za informacijsku sigurnost

Čitateljima zanimljiv može biti i domaći izvor informacija, portal za informacijsku sigurnost dostupan na adresi:

http://sigurnost.info

Autori nisu profesionalni novinari, već stručnjaci koji su zaposleni na poslovima vezanim za informacijsku sigurnost, konzultanti i edukatori, pravnici koji prate zakonsku regulativu. Iako je prvenstveno namijenjen menadžerima, pokriva i tehničke teme u rubrikama „Podzemlje novog doba“ i „Na prvim linijama“, gdje se iznose konkretna iskustva iz prakse. Širok dijapazon tema pokriva područja od zakonske regulative, kontinuiteta poslovanja, međunarodnih normi, pogled managementa na sigurnost i slično. Portal prenosi i vijesti iz područja informacijske sigurnosti.

7.4. Ostali časopisi

Time naravno nisu navedeni svi dobri e-časopisi. U nastavku slijedi i nekoliko vrijednih spomena:

- The Register - http://www.theregister.co.uk/, poznat po ciničnim komentarima, uostalom logo im je lešinar!
- Dark Reading – http://www.darkreading.com, vijesti iz cyber podzemlja
- Network World – http://www.networkworld.com, rubrika *Security*

7.5. Blogovi

Blogovi su također zanimljiv izvor informacija. Neformalniji, izravniji, omogućuju istraživačima da prezentiraju svoja otkrića na način koji će možda više cijeniti njihove kolege. Na blogovima su česte osobne primjedbe i komentari koji ne bi prošli redakcijsku cenzuru. Poznatiji blogovi iz područja informatičke sigurnosti mogu se pronaći na:

- Bejtlich - http://taosecurity.blogspot.com/
- Matasano - http://www.matasano.com/log
- Kaminsky - http://www.doxpara.com/
- Rutkowska - http://theinvisiblethings.blogspot.com/
- Nod32 blog - http://www.eset.com/threat-center/blog
- Kaspersky blog - http://www.viruslist.com/en/

8. Hakerske konferencije

Iako su hakeri „sramežljivi" i ne vole publicitet, ipak se pojavljuju, zajedno sa stručnjacima za informacijsku sigurnost, na dvije konferencije gdje prezentiraju svoja najnovija otkrića. Prezentacije su konkretne, demonstriraju se najnovije ranjivosti i načini njihova iskorištavanja. Nezavisni hakeri tu su u boljem položaju jer se na njih ne vrše pritisci da se uzdrže od otkrivanja ranjivosti. Istraživači zaposleni u tvrtkama koje se bave sigurnošću ponekad su izloženi pritiscima, čak su u opasnosti da izgube posao. Ipak, želja za otkrivanjem ranjivosti, koliko god se time ugrožavala reputacija proizvođača, na kraju krajeva je korisna i doprinosi poboljšanju sigurnosti.

Obje su konferencije tehnički orijentirane, tako da ih mogu pratiti samo vrlo obrazovani tehničari. Radi se o:

- Black Hat Conference, dostupna je na stranici http://www.blackhat.com.
- Defcon Konferencija održava se Las Vegasu, Nevada: http://www.defcon.org

9. Zaključak

Profesionalci koji se bave informacijskom sigurnošću moraju se kontinuirano obrazovati i pratiti novosti iz različitih područja. Osim tehničkih znanja, poput razvoja novih tehnologija, pojave novih ranjivosti, prijetnji i načina napada, moraju pratiti zakonsku regulativu, te razvoj međunarodnih normi upravljanja informacijskom sigurnošću, a istovremeno stjecati i razvijati upravljačke vještine. Dokument navodi brojne izvore kvalitetnih informacija, tako da će svatko moći izabrati nešto za sebe, ovisno o užoj specijalizaciji unutar područja informacijske sigurnosti. Ograničen opseg ovakvog dokumenta ne dozvoljava navođenje svih postojećih izvora. Internet je dinamično okruženje, svakodnevno se pojavljuju novi izvori potencijalno vrijednih informacija, a neki od starih izvora prestaju postojati. Iz toga proizlazi potreba daljnjeg održavanja ovog dokumenta. Ovdje navedeni izvori informacija, bez obzira na ograničenost izbora, prevelik su zalogaj za jednog čovjeka, tako da zapravo nije moguće, uz sve ostale dnevne obaveze, svakodnevno praćenje svih novosti. Zato svaki pojedinac, prema vlastitim potrebama/mogućnostima te željama za profesionalno usavršavanje, treba izabrati „svoje“ izvore i njih redovito pratiti.

10. Reference

[1] Secunia: http://en.wikipedia.org/wiki/Secunia, kolovoz 2008.

[2] Black Hat: http://en.wikipedia.org/wiki/Black_hat, kolovoz 2008

[3] Hacker: http://en.wikipedia.org/wiki/Hacker, rujan 2008

[4] SANS Institute: http://en.wikipedia.org/wiki/SANS_Institute, travanj 2008

[5] Exploit: http://en.wikipedia.org/wiki/Exploit_(computer_security), rujan 2008

[6] CERT: http://www.cert.org/, rujan 2008

[7] Computerworld: http://www.computerworld.com/, rujan 2008

[8] Narodne novine: http://www.nn.hr/, kolovoz 2008

[9] HITRO.HR: http://www.hitro.hr/, kolovoz 2008

[10] e-Hrvatska: http://e-hrvatska.hr/, rujan 2008