Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 005.8
DOI: https://doi.org/10.24867/14GI08Smitran

BEZBJEDNOST INFORMACIONIH SISTEMA

INFORMATION TECHNOLOGY SECURITY

Dejna Šmitran, Slobodan Morača, Fakultet tehničkih nauka, Novi Sad

Oblast: INDUSTRIJSKI MENADŽMENT

Kratak sadržaj: *Ovaj rad u sebi objedinjuje nekoliko krucijalnih aspekata računarskih mreža, počevši od organizacije i administracije virtuelne privatne mreže, do zaštite sistema i bezbednosti podataka. Organizacija mreže se bavi hardverskim i softverskim rješenjima koja su potrebna da bi se mreža realizovala po zahtijevima korisnika. Administraciju mreže čine njeno održavanje, nadgledanje i unapređivanje kako bi ona bila dugotrajna i efikasna, te na taj način zadovoljavala najviše IT standarde. Zaštitu sistema i bezbednost podataka čine sva hardverska i softverska rješenja neophodna da spriječe i otklone potencijalne prijetnje po sigurnost i bezbjednost sistema.*

Ključne riječi: *Računarska mreža, IT standard, bezbjednost podataka, sigurnost informacionih sistema*

Abstract: *This paperwork incorporate several crucial aspects of networks, starting at organization and administration of virtual private network, all the way to IT security and data safety. Network organization engage in hardware and software solutions that are needed to accomplish network by customer demands. Network's administration includes maintenance, surveillance and advancement so that network would be longlasting and well-used, and in that way to satisfy all the highest IT standards. System protection and data security inculdes all hardware and software solutions which are needed to prevent and banish potencial data's security and safety threats.*

Key words: *IT network, IT standard, data safety, IT Security*

1. UVOD

Izuzetno rapidan i brz razvoj informacionih tehnologija doveo je do globalizacije svjetskog tržišta, velike konkurencije, brzog protoka informacija i podataka, stvaranja novih i boljih mrežnih sistema ali isto tako i novih i boljih vrsta napada i na privatne informacije ili tajne podatke.

IT predstavlja nezaobilazan faktor modernog menadžmenta, i njihova primjena u poslovanju organizacija i kompanija doprinosi bržem nalaženju i rješavanju problema, te omogućava kvalitetnu i ekonomičnu podršku poslovanju.

NAPOMENA
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Slobodan Morača, van. prof.

Računarske mreže se uglavnom baziraju na Internet tehnologijama i protokolima koji su podložni mogućim napadima koji narušavaju bezbjednost podataka i identiteta subjekata.

Ključni problem leži u činjenici da podaci kruže i egzistiraju u elektronskom obliku koji nije neposredno vidljiv i zbog toga postaju izloženi novim vrstama napada, a osnovni razlozi za to leže u samim osnovnim karakteristikama arhitekture računarskih mreža Internet/ Intranet tipa.

2. BEZBJEDNOST INFORMACIONIH SISTEMA

Bezbjednost je oblik administracije mreže, nadležan da osigura da podatke, vodove i opremu na mreži koriste samo ovlašteni korisnici na ovlaštene načine. Konkretnije, obezbjeđenje treba da osigura dostupnost, povjerljivost i integritet [1].

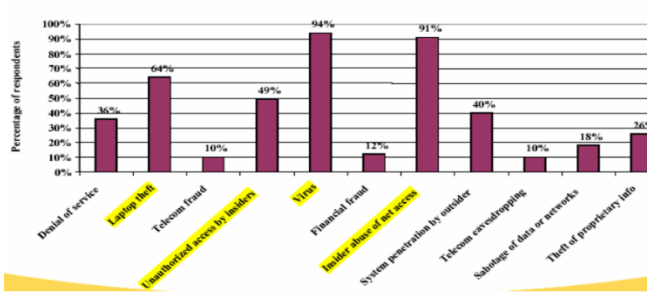
Već 70ih godina pokrenut je istraživački projekat koji se smatra začetnikom cybersecurity-a. Bob Thomas je stvorio računarski program koji je mogao da pomjeri ARPANET - The Advanced Research Projects Agency Network (mreža naprednih istraživačkih projekata), ostavljajući trag gdje god da se nadje, te je Thomas taj program nazvao „CREEPER“, zbog ispisane poruke koju je ostavljao prilikom prolaska kroz mrežu „CREEPER SAM: UHVATITE ME AKO MOŽETE“. Rai Tomlinson – čovjek koji je izmislio e-poštu je kasnije dizajnirao program koji je Creeper podigao na viši nivo, čineći ga prvim računarskim crvom. On je tada napisao drugi program nazvan Reaper koji je hvatao Creeper i brisao ga, te je na taj način pružio prvi primjer za antivirusni softver. U to vrijeme je ovaj eksperiment otkrio mnoge nedostatke u mrežnoj sigurnosti. Određene grupe ljudi su to prepoznale i počeli su da traže načine da se uvuku u njihove redove i ukradu važne podatke – to su bili prvi hakeri na svijetu. Prekretnicu informacione bezbjednosti obilježio je Morrisov crv 1988.godine. Dizajniran je tako da se širi mrežama i ugrađuje se u terminale koristeći poznatu grešku koju na kraju sam kopira. Cilj Morris crva bio je da prepozna područja koja nedostaju u mrežnom sistemu, a štite od hakerskih upada. Međutim crv je bio preagresivan i samim tim uništavao računare u koje se ubacivao što je dovelo do neispravnosti i ogromne štete. Sve ovo rezultiralo je formiranjem CERT-a (Computer Emergency Response Team) koji je trebao da spriječi ponavljanje ovakvih sajber napada.

Sprovođenje bezbjednosnih mjera je trajan proces – neko je rekao da je jedini potpuno bezbjedan računar onaj koji ne sadrži podatke, nije uključen u mrežu, nije priključen

na električno napajanje, nema priključenu tastaturu i zaključan je u podrumu [2].

3. TRENDOVI U SISTEMIMA ZAŠTITE SAVREMENIH RAČUNARSKIH MREŽA

Računarske mreže, s jedne strane omogućavaju povećanje efikasnosti rada, ali s druge strane predstavljaju kritičnu tačku bezbjednosti date organizacije, gledajući sa stanovišta bezbjednosti informacija.
U svetu postoji veliki broj različitih pregleda i analiza opasnosti korišćenja računarskih mreža na bazi Internet tehnologija izrađenih od strane relevantnih institucija. Jedna takva analiza ukazuje na tipove napada, u procentima prijavljenih napada, Slika 1.



Slika 1. Vrste napada na računarske mreže

Prema jednom sličnom pregledu američkog instituta za zaštitu računara (Computer Security Institute (CSI)'s 2000 Computer Crime and Security Survey) koji je obuhvatao velike korporacije, 70% razmatranih subjekata je prijavilo detektovane neautorizovane pristupe u svojim mrežama u prethodnoj godini [3].
Takođe, prema istoj analizi, u prethodnih 5 godina, 66 razmatranih subjekata je prijavilo ukupan gubitak proizveden krađom osetljivih korporacijskih informacija u iznosu od $66 708 000, a 54 razmatrana subjekta su prijavila ukupan gubitak proizveden finansijskom proneverom u iznosu od $53 996 000.
Ova analiza je takođe potvrdila sledeće trendove u korišćenju računarskih mreža Internet tipa u poslednje vrijeme:

- Razvoj sve šireg spektra mogućih napada,
- Napadi na korporacijske računarske mreže Internet tipa mogu biti eksterni i interni.
- U poslednje vreme su zabeleženi veoma veliki finansijski gubici prouzrokovani napadima na računarske mreže Internet tipa,
- Uočeno je da primjena samo komercijalnih tehnologija zaštite informacija ne može uvek predstavljati pouzdano rešenje odbrane od potencijalnih napada već da se ponekad mora koncipirati i primjeniti slojevita i sveobuhvatna politika zaštite koja će pored komercijalnih tehnologija zaštite obavezno uključiti i primjenu kvalitetnijih, sopstveno realizovanih mehanizama zaštite, kao i mehanizama kontrole pristupa i organizacionih elemenata zaštite date računarske mreže.

Sa druge strane, SANS Institut je obavio istraživanja koja su rezultovala u definisanju tri liste osnovnih grešaka koje omogućavaju različite vrste napada na mreže Internet tipa i pojedinačne radne stanice u mreži.
Prva lista se odnosi na krajnje korisnike i definiše sledećih pet najvećih bezbjednosnih grešaka:

- Otvaranje nezahtjevanog e-mail priloga (attachment) dobijenog od nepoverljivog izvora,
- Propust da se instaliraju bezbednosni patch-evi standardnih Internet programskih paketa, kao i novih definicija (upgrade) antivirusnih programa,
- Instaliranje i download-ovanje screen saver-a i igara od nepoverljivih izvora,
- Nekreiranje i netestiranje back-up operacija,
- Korišćenje modema dok ste vezani u lokalnoj računarskoj mreži (LAN).

Druga lista se odnosi na korporacijske uprave (management) i definiše sledećih sedam najvećih bezbednosnih grešaka koje utiču na slabosti korporacijske računarske mreže:
-Neobezbeđenje odgovarajućeg broja službenika koji treba da uspostave i održavaju sistem zaštite u okviru korporacije,
-Primjena samo organizacionih vidova zaštite bez primene (i bez prihvatanja neophodnosti primene) mehanizama zaštite informacija,
-Rješavanje samo pojedinačnih bezbednosnih problema bez primene mera i stvaranja uslova za kreiranje kompletnog sistema zaštite koji bi osigurao rešenje najšireg spektra bezbjednosnih problema,
-Korišćenje samo mrežnih barijera (firewall) u korporacijskoj računarskoj mreži,
-Neshvatanje koliko vrijede intelektualno vlasništvo i poslovna reputacija firme,
-Primjena kratkotrajnih rešenja pojedinačnih situacija što dovodi do brzog umnožavanja bezbjednosnih problema,
-Pretvaranje da će se bezbjednosni problemi riješiti sami od sebe ako se ignorišu.

Treća lista se odnosi na informatičke profesionalce i definiše sledećih deset najvećih bezbjednosnih grešaka:
-Priključivanje računarskog sistema na internet bez prethodne primene svih neophodnih bezbednosnih mera da se to učini,
-Priključivanje test i razvojnih sistema na internet sa default lozinkama,
-Propust da se sistem ažurira sa rešenjima nekih bezbednosnih problema,
-Korišćenje nekriptovanih protokola za upravljanje sistemima, ruterima i firewall-ovima,
-Davanje korisnicima lozinki preko telefona i njihovo menjanje bez prethodne autentikacije osobe koja zahteva izmenu,
-Propust pri održavanju i testiranju procedure back-up-a sistema,
-Korišćenje nepotrebnih internet servisa,
-Primjena mrežnih barijera sa pravilima koja ne osiguravaju bezbjedno osetljivi dolazeći i odlazeći saobraćaj,
-Propust u implementaciji i ažuriranju softverskog paketa za detekciju virusa,

-Propust u edukaciji korisnika u odnosu na to šta je potrebno učiniti kada se uoči potencijalni bezbednosni problem.

4. BEZBJEDNOSNI ZAHTIJEVI I PRINCIPI

Najbitniji i najvažniji principi bezbjednosti, odnosno bezbjednosni zahtijevi su:

-***Tajnost*** *(privacy, confidentality)* – predstavlja, najprostije rečeno obezbjeđivanje sigurnog komunikacionog kanala između učesnika u elektronskoj transakciji.

-***Integritet*** *(data integrity)* – verifikacija da nije došlo do narušavanja integriteta podataka za vrijeme njihovog prenosa.

-***Autentikacija*** *(authentication)* – obezbjeđivanje da su učesnici u transakciji oni za koje se predstavljaju, odnosno sprečavanje lažnog predstavljanja učesnika u komunikaciji.

-***Neporecivost*** *(non-repudiation)* – obezbjeđivanje da učesnici u transakciji ne mogu poreći svoje učešće.

-***Dostupnost*** *(availability)* – podrazumijeva da su infromacije/servisi dostupni kada je to potrebno, tj. kada to zahtjeva autorizovani korisnik.

-***Kontrola pristupa*** *(access control)* – spriječava neautorizovan pristup resursima.

-***Pouzdanost*** *(realiability)* – otpornost na otkaze.

-***Audit*** – audit informacije moraju biti sačuvane kako bi akcije koje su ugrozile sigurnost naknadno mogle biti istražene [4].

5. PRIJETNJE ZA BEZBJEDNOSNI SISTEM I RIZICI OD NAPADA

Rizik se uglavnom smanjuje na jedan od četiri moguća načina:

1. *Smanjivanje provođenjem sigurnosnih kontrola* – ovim se načinom primjenjuju sigurnosne kontrole koje smanjuju vjerovatnost ostvarivanja prijetnje ili smanjuju njezin utjecaj
2. *Izbjegavanje rizika* - bilo koja akcija kod koje se mijenjaju poslovne aktivnosti ili način vođenja poslovanja kako bi se spriječila pojava rizika
3. *Prenošenje rizika* – ovim se načinom uglavnom pokrivaju rizici kod kojih bi primjena sigurnosnih kontrola bila neekonomična, pa se pribjegava prenošenju rizika na drugu organizaciju
4. *Prihvatanje rizika* - odabirom ove opcije organizacija svjesno prihvata vrijednovani rizik i ne namjerava ništa dodatno preduzimati kako bi ga smanjila

Sigurnosne kontrole je najbolje izabrati kroz zakone, standarde, smjernice i okvire koji se danas koriste u području informacione bezbjednosti.

U svjetskim okvirima je to ISO/IEC 27001:2005.

6. ISO 27000-IMPLEMENTACIJA SISTEMA UPRAVLJANJA INFORMATIČKOM BEZBJEDNOŠĆU U ORGANIZACIJI PO STANDARDU ISO/IEC 27001:2005

Međunarodni standard ISO/IEC 27001 je pripremljen da obezbjedi jedan model za uspostavu, implementaciju, operativni rad, nadzor, pregled, održavanje i poboljšavanje Sistema za upravljanje informatičkom bezbednošću (ISMS – Information Security Management System). Usvajanje ISMS sistema treba da bude strateška odluka za jednu organizaciju. Dizajn i implementacija ISMS sistema u organizaciji je pod uticajem njenih potreba i ciljeva, bezbjednosnih zahtjeva, procesa koji se izvršavaju, kao i uslovljen veličinom i strukturom organizacije.

Procesni prilaz upravljanju informatičke bezbednosti koji je predstavljen u ISO 27001 standardu naglašava važnost:

-Razumijevanja zahtijeva za informatičkom bezbednošću u organizaciji, kao i potrebe da se uspostavi politika i ciljevi informatičke bezbednosti;
-Implementacije i primjene kontrola za upravljanje rizicima informatičke bezbjednosti u organizaciji u kontekstu sveukupnih poslovnih rizika organizacije;
-Nadzora i pregleda performansi i efektivnosti ISMS sistema;
-Kontinualnog poboljšanja na bazi objektivnog mjerenja.

ISO/IEC 27001 standard usvaja "Plan-Do-Check-Act" (PDCA) model, slika 6.1, koji se primenjuje da struktuira sve ISMS procese. Naime, ISMS sistem uzima kao ulaz zahtijeve za informatičkom bezbjednošću, kao i očekivanja zainteresovanih strana, i kroz neophodne akcije i procese proizvodi izlaze informatičke bezbjednosti koji zadovoljavaju pomenute zahtijeve i očekivanja.

Dakle, danas aktuelni standardi u domenu informatičke bezbjednosti su:

- **ISO/IEC 27002: 2005** – Information Technology – Security Techniques – Code of practice for information security management (nekada 17799 standard),

o Obezbeđuje smernice najboljeprakse za ISMS sistem

o Definiše skup ciljeva kontrola, kontrola, kao i smernica za implementaciju.
o Ne može se koristiti za ocenjivanje i sertifikaciju.

- **ISO/IEC 27001:2005** – Information Technology – Security Techniques – Information Security Management Systems – Requirements

o Definiše specifične zahteve za uspostavu, implementaciju, operativni rad, nadzor, pregled, održavanje i poboljšanje dokumentovanog ISMS sistema.
o Izrađen da osigura adekvatne bezbednosne kontrole da zaštiti informaciona dobra i dokumentuje ISMS sistem.

- Može se koristiti za ocenjivanje i sertifikaciju.

6.1. Uspostava i upravljanje ISMS sistemom
Uspostava ISMS (Plan)

U cilju uspostave ISMS sistema organizacija treba da izvrši sledeće aktivnosti:

a) **Definiše okvir i granice ISMS** i to u skladu sa karakteristikama svog poslovanja, organizacije, lokacijom, imovinom i tehnologijama, uključujući i relevantne detalje;
b) **Definiše ISMS politiku** u skladu sa karakteristikama svog poslovanja, organizacije, lokacijom, imovinom i tehnologijama;
c) **Definiše pristup ocjenjivanju rizika** u organizaciji
d) **Identifikuje** rizike
e) **Analizira i evaluira** rizike
f) **Identifikuje i evaluira opcije tretmana** rizika
g) **Selektuje ciljeve kontrola, kao i same kontrole, za tretman** rizika
h) **Dobije odobrenje od menadžmenta** za predložene preostale (rezidualne) rizike
i) **Dobije autorizaciju** od strane menadžemnta da implementira i pusti u operativni rad ISMS sistem
j) **Pripremi Izjavu o primjenljivosti** (Statement of Applicatbility)

Da bi se ISMS sistem uveo u fazu operativnog rada potrebno je izvršiti sljedeće korake:

a) Formulisati plan tretiranja rizika, gdje se utvrđuju podudarne upravne akcije, resursi, odgovornosti i prioriteti za upravljanje rizicima informaticke bezbjednosti.

b) Plan tretiranja rizika treba da se sprovede u djelo radi postizanja utvrđenih ciljeva kontrola. Oni obuhvataju i razmatranje budžeta, ali i dodjeljivanje zadataka i odgovornosti.
c) Takođe, da bi se zadovoljili postavljeni ciljevi kontrola potrebno je i odabrane kontrole sprovesti u djelo.
d) Potrebno je odrediti način na koji se mjeri učinkovitost izabranih kontrola, ili njihovih grupa, te utvrditi kako treba da se koriste ove mjere da bi se ocjenila učinkovitost kontrola, i da bi se dobili komparativni rezultati.
e) Zaposleni treba da prođu kroz određene programe i obuke, da bi se podigla njihova svijest o informatičkoj sigurnosti.
f) Organizacija rukovodi operativnim radom ISMS sistema
g) Rukovodi i resursima koji su potrebni za ISMS sistem
h) U djelo se sprovode sve one kontrole koje omogućavaju brzu identifikaciju sigurnosnih događaja,

7. ZAKLJUČAK

Kako postoji već određeni broj standarda u području zaštite informacionih resursa, potrebno je sistemski pristupiti procesu njihove evaluacije i sertifikacije. U skladu sa tim, kao zaključak se nameće da je proces sertifikacije potrebno započeti usvajanjem standarda ISO/IEC 27001 kao osnovnog standarda za implementaciju, kontrolu, unapređenje i sertifikaciju sistema informacione sigurnosti (ISMS - Information Security Management System), iz kojeg treba da uslijedi sertifikacija specifičnih podučja informacionih resursa na višem nivou.
Standardom ISO/IEC 27001 se, u cilju uspostavljanja sveobuhvatnog sistema zaštite informacionih resursa, determiniše sistem za zaštitu informacija, odgovornost rukovodećih ljudi, determinišu procedure unutrašnje provjere sistema za zaštitu informacija, zatmi procedure provjere valjanosti sistema za zaštitu informacija, te procedure vezane za poboljšanja na sistemu za zaštitu informacija. Kada je u pitanju usvajanje navedenog standarda u Bosni i Hercegovini, može se zaključiti je to trenutno stanje dosta nepovoljno u odnosu na zemlje razvijenih regija u svijetu obzirom da samo dvije organizacije imaju usvojen standard ISO/IEC 27001.

8. LITERATURA

[1] Feibel, W. (1995). *Novell's Complete Encyclopedia of Networking* . San Jose: Novell Press.

[2] Collings, T., & Wall, K. (2002). Obezbjedjivanje sistema. U *Red Hat Linux networking and System Administration* (str. 9). Wiley Publishing, Inc.

[3] *5 things you need to know about Data Privacy*. (2020, 12 16). Preuzeto sa Data Privacy Management: https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

[4] Sigurnost na internetu. (2020). Banja Luka, BiH, RS.

Kratka biografija

Dejna Šmitran je rođena i odrasla u Gradišci, RS, BiH. Osnovne akademske studije je završila u Novom Sadu na Fakultetu tehničkih nauka, gdje upisuje i master studije. Trenutno je zaposlena u Ministarstvu unutrašnjih poslova RS, Uprava za informaciono-komunikacione tehnologije.