FBIM TRANSACTIONS
DOI 10.12709/fbim.01.01.02.09

EKSTERNA I INTERNA ZAŠTITA ELEKTRONSKIH INFORMACIJA

EXTERNAL AND INTERNAL ELECTRONIC INFORMATION SECURITY

Milorad Markagić
Univerzitet odbrane, Vojna akademija, Beograd, Srbija

JEL category: **D8, D82, D85**

Apstrakt
Savremena komunikacija među pojedincima i institucijama, kroz evoluciju tehnoloških sredstava postaje sve dinamičnija, a protok informacija koje su najčešće u digitalnom obliku meri se ogromnim količinama. Nezamislivo je da se bilo koji vid savremenog poslovanja odvija bez korišćenja računarske opreme i mrežnih i telekomunikacionih resursa. Osim velikih koristi, lakšeg i bržeg prenosa i pojednostavljenosti komunikacije, na polju informacije, kroz prostor generisanja, obrade i prenosa informacija, provlače se i zlonamerne manipulacije, krađe i uništenje informacija.

Ključne reči:
informacija, zaštita, računarske mreže, računarski sistemi, telekomunikacije

Abstract:
Contemporary communications between individuals and institutions, through evolution of technological resources, becomes more dynamic. Information flow, mostly digital, reaches unexpected proportions. It is unthinkable that any aspect of modern business could be carried out without the use of computer equipment and ICT resources. Besides the great benefit of easier and faster transmission and simplicity of communication in the field of information through space of generating, processing and transmitting, there are malicious manipulations, theft and destruction of the information.

Keywords:
information,security,computer networking,computer systems, telecommunications

1 UVOD

Svrha svakodnevne komunikacije za lične ili poslovne potrebe, kao i savremeno poslovanje danas je apsolutno nezamislivo bez upotrebe savremenih informaciono-telekomunikacionih tehnologija (IKT) i globalnih mreža. Jedan od najvažnijih resursa ovoga doba svakako jesu i informacije od kojih umnogome zavisi pravovremena komunikacija subjekata i uspešno poslovanje kompanija.

Adresa autora:
Milorad Markagić
milmarkag@yahoo.com

Kako pojednci, tako i kompanije se sve više otvaraju u povezivanju svojih IKT resursa sa okruženjem ili na globalnom nivou.

Pitanje savremenog sveta nije ko ima kapital, ko vlada resursima, već ko vlada informacijama. Može se reći da onaj ko vlada informacijama, vlada i resursima.

Vrtoglav je rast globalnih društvenih mreža, koje pored prvobitne namene- masovnih, brzih i jeftinijih ličnih kontakata, sve više dobijaju značaj i primenu u marketinško-ekonomskim, poltičkim, obrazovnim, naučnim, obaveštajnim i drugim poljima delovanja ljudskog društva.

Masovna primena, niska cena i relativno lak pristup globalnim mrežama neminovno pored svih prednosti doprinosi i pojavi brojnih bezbednosnih pretnji.

Računarske prevare, špijunaže, sabotaže, krađe novca, krađe identiteta, izazivanje panike, unošenje nemira, širenje defetizma, zloupotreba mreža u terorističkim akcijama i još ogroman broj drugih nezakonskih i nepravilnih primena savremenih vidova komunikacije nanose ogromnu, a često i nemerljivu i trajno nepovratnu štetu pojedincima ili kompanijama, a svedoci smo u skorije vreme i celovitim promenama društvenih sistema i uređenja.

Takođe je sve masovnija primena bezrazložnog uskraćivanja usluga preko globalnih mreža putem unošenja zloćudnih kodova, računarskog hakerisanja ili jednostavnim fizičkim ili elektronskim uništenjem podataka i resursa.

Ovo navodi na zaključak da informacije moraju biti adekvatno zaštićene. Bezbednost i zaštita informacija, očuvanje poverljivosti i integriteta, nužan su segment razmatranja i praktične primene od izvora do odredišta infrmacije.

Ovo treba shvatiti ne samo kao potrebu upotrebe odgovarajućih softverskih rešenja koje nude savremene IKT, već i permanentnu brigu o uticaju korisnika tehničkih sredstava.

2 PRETNJE INFORMACIJAMA I IKT SISTEMIMA

Pretnje informacijama i IKT sistemima su mnogobrojne, često neprimetne subjektima a mogu se manfestovati u više pojavnih oblika. Pri razmatranju izvora pretnji posebnu pažnju treba pokloniti sledećim segmentima:

- pretnje izvorima informacija u otvorenom ili digitalnom obliku (baze podataka i sami podaci, dokumenta sistema, uputstva, pravila, nastavni planovi, programi i materijali, operativne i sistemske procedure, sistem zapisa),
- pretnja fizičkim (hardverskim) resursima (kompjuterska oprema, kompjuterski uređaji, delovi uređaja -procesori, monitori i sl, modemi, ruteri, svičevi, telefoni, magnetni medijumi (eksterni diskovi, CD iili DVD ili flash memorije, sistemi za napajanje, hlađenje),
- pretnja softverskim resursima (aplikativni i sistemski, alati za razvoj softvera)
- pretnja uslugama (usluge obrade podataka, komunikacione usluge) i
- pretnja pojedincu (znanje i veštine osoblja tehničkog, operatvnog, marketing, finansijskog, itd...).

2.1 Napadi na informacije i IKT sisteme

Polazeći sa stanovišta ko, kada, gde i kako može i vrši napade osnovna podela napada na informacije, a pre svega na IKT sisteme bila bi na: struktuirani i nestruktuirani napad.

2.1.1 Nestrukturirani (neplanirani, slučajni) napad

Najčešći i najmasovniji vid napada na informacije i IKT sisteme, koji se obavljaju bez unapred definisanog cilja, bez posebne motivacije i bez očekivane materijalne ili druge dobiti.

Izvode ih najčešće amateri koji nisu detaljno upućeni u programe i hardvarsku strukturu IKT sisema ili ih izvorna informacija ne dotiče u nekom posebnom smislu.

Takođe su mogući napadi između jedinki u smislu zabave ili napadi unutar kompanije sa ciljem trenutnog dolaska do određene informacije, bez dalje upotrebe ili zloupotrebe saznanja.

Zaštitita od ovih napada je relativno laka. Postoji niz postupaka i softversko-tehnoloških rešenja

kojima se napadaču blokira pristup kako na fizičkom nivou, tako i na aplikativno-softverskom nivou.

2.1.2 Strukturirani (zlonamerni, planirani) napad

Ovu vrstu napada karakteriše pojava da su izvršioci unapred planiranim, osmišlenim ciljevima, spremni da upotrebe sve raspoložive resurse i kapacitete radi dolaska do informacija. Napadači su vrlo osposobljeni, dobro tehnološki opremljeni i motivisani za izvršenje napada.

Korišćenjem savremenih alata, napadaju informaciju od njenog generisanja u fizičkom obliku i/ili dorade u elektronskom obliku na samom računaru, prilikom njene obrade i transfera kroz računarsku ili telekomunikacionu mrežu.

Mete napada najčešće su državne institucije, finansijski sektori, bezbednosne strukture, vojni i policijski resursi, ali i privatne i državne kompanije koje raspolažu nekim vidom tajnih podataka.

Ovakvi napadi su veoma retko usmereni na pojedinca, personalni računar ili pristup mreži, ali je pojava upada u globalne mreže sa ciljem njihovog rušenja ili krađe podataka pogodno tle i za gubitak ličnih informacija.

Znatan je materijalni učinak napadača kada vrši ovaj vid napada, bilo da je u pitanju napad na javno publikovane informacije (rušenje sajtova), pribavljanja protivpravne materijalne koristi, zloupotrebe IKT sistema u cilju vršenja krivičnih dela sajber terorizma, zloupotrebe dece ili napad na globalnu mrežu koju koristi veliki broj pojedinaca.

Sa druge strane gubici pojedinca ili kompanije su ogromni. Veoma često dolazi do gubitka informacija, novčanih sredstava, ali i trajnog onesposobljavanja računarskih mreža i sistema.

Iako su nestruktuirane pretnje mnogobrojnije, struktuirane pretnje su višestruko opasnije i nose sa sobom puno veću cenu oporavka sistema.

Osnovni problem bezbednosti jeste što je veoma nizak nivo poznavanja zaštite na internom nivou, a u kompanijama se poslovi bezbednosti oslanjaju na sprovođenje pojedinih tehničkih mera i IT sektor koji najčešće ima jednog ili dva zaposlena radnika. Ovakvim nedovoljnim poklanjanjem pažnje resursi su lako ranjivi i kroz strukturirani napad napadač lako dolazi do informacija i podataka.

2.2 Uzroci oštećenja i gubitka informacija

Postoji čitav niz uzroka zbog kojih dolazi do gubitka ili oštećenja informacija, a koje izazivaju izvori ili korisnici informacija. Ukažimo samo na nekoliko najznačajnijih:

- Slaba ili nepostojeća evidencija poverljivih podataka i informacija. Ako evidencija i postoji nju retko ili nikako ne koristi širi krug interesenata,
- Neadekvatna kontrola pristupa informacijama, koja se manifestuje kroz pojavu da veliki broj nepozvanih lica ima pristup i mogućnst korišćenja poverljivih podataka i informacija,
- Neadekvatna zaštita informacije na fizičkom nivou (papirna ili elektronska forma na izvoru), gde se sa izradom Planova, projekata, finansijskim izveštajima i sl. upoznaje veći broj ljudi od neophodnihm
- Čuvanje informacija na desktop nezaštićenim ili prenosivim računarima, koje najčešće koristi više pojedinaca kako za ličnu upotrebu, tako i u kompanijama i institucijama,
- Gubitak prenosivih računara na kojima se čuvaju podaci, koje najčešće pojedinci koriste i za službene i za lične potrebe,
- Nepostojanje ili neažurne evidencije o broju i korisnicima računara, kao najčešći oblik zloupotrebe u internim prevarama, jer se računari nabavljaju, daju na korišćenje ili rashoduju često bez adekvatne prateće dokumentacije,
- Nepoznavanje zaposlenih koji imaju pristup infrmacijama, gde se osim stručnih karakteristika ostale osobine zaposlenika veoma malo ili uopšte ne poznaju,
- Neadekvatna izrada kopije podataka, tako da se često bez potrebe poverljive informacije

kopiraju na više mesta, više računara ili prenosivih medija,

- Izrađena kopija podataka se neadekvatno čuva i dostupna je nepozvanim licima,
- Nepostojanje evdencije o prenosivim medijima na kojima se obrađuju i čuvaju informacije,
- Nepostojanje kriptološke zaštite informacija,
- Nabavka softvera pod povoljnijim uslovima, bez procene kvaliteta i rizika,
- Korišćenje besplatnih verzija, krekovanih ili piratskih verzija softvera,
- Slaba antivirusna zaštita računara i mreža,
- Nezainteresovanost ili nestručnost menadžmenta za bezbednost IKT sistema, pri čemu se za poslove zaštite angažuje mali broj zapošljenih, a rukovodstvo bude uključeno tek kada dođe do nekog incidenta,
- Mali broj stručnih lica u oblasti bezbednosti,
- Mali broj stručnih lica u IT sektorima,
- Neobezbeđivanje zamenjivosti kadra,
- Slaba edukacija korisnika informacija,
- Izostanak ili nepotpuna kontrola korisnika itd.

Imajući u vidu da se oštećenje i gubitak informacija najčešće dešavaju kombinacijom nekoliko pobrojanih činioca (Petrovic, Cekerevac, & Grubor, 2005), logično se nameće zaključak da je zaštita veoma kompleksna celina i aktivnost u koju moraju biti uključeni svi koji barataju informacijama.

3 INTERNA ZAŠTITA INFORMACIJA I IKT SISTEMA

Sprovođenje interne i eksterne zaštite informacija i IKT sistema neodvojivi su i međuzavisni procesi, ali radi lakšeg uvida u ciljeve i metode prikazane su kao posebne celine. (Ewell, 2009)

Odgovarajuće upravljanje bezbednošću informacija sprovodi se primenom tehničkih rešenja, odgovarajuće opreme i proizvoda ali i permanentnom edukacijom osoblja.

Veoma važan segment jeste primena odgovarajućih kontrola koje se odnose na politiku bezbednosti i sigurnosti, poslovne procese, procedure, strukturu organizacije i funkcije hardvera i softvera.

Neophodno je da se definišu postupci rada sa informacijama, da se isti dokumentuju i budu dostupni korisnicima, upravljačkim organima i organima zaduženim za prenos i skaldištenje informacija.

Na nivou kompanje potrebno je preduzeti niz radnji, postupaka i aktivnosti kojima se može sprečiti negativan uticaj sredine na kvalitet i tok informacija. Osnovni elementi bili bi sadržani u sledećem:

- zaštititi informacije od neovlašćeng pristupa, kako bi informacijom ili podatkom upravljalo i koristilo samo osoblje koje ima direktan dodir sa predmetnom materijom,
- održavati poverljivost informacija, gde svakoj informaciji treba odrediti nivo i stepen tajnosti, rok čuvanja i upotrebe i rok i način uništenja,
- zaštittiti integritet informacija,
- omogućiti pristup i mogućnost izmene informacija samo ovlašćenim licima, čime se izbegava dodir trećim licima, a samim tim umanjuje ili neutrališe mogućnost krađe istih,
- usaglasiti zahteve sa zakonskom regulativom i tehničkim mogućnostima, pre svega angažovanjem stručnih lica iz oblasti prava, informacionih tehnologija i sektora bezbednosti,
- izraditi politiku i plan bezbednosti informacija i IKT sistema, učiniti ih javno dostupnim, upoznati zapošljene sa pravima, obavezama i sankcijama u slučaju nepoštovanja procedura,
- vršiti stalnu nadogradnju, kontrolu, testiranje i obezbediti zamenjivost opreme koja se koristi pri izradi. Čuvanju ili prenosu informacija,
- vršiti permanentnu edukaciju korisnika, kroz zajedničke ili posebne oblike osposobljavanja,
- sankcionsati prekršioce politike i procedura, uz preduzimanje svih zakonskih mera i mera propisanih internim uputstvima kompanije,

- vršiti zaštitu i čuvanje podataka kroz 'backup', čime se izbegava trajni gubitak informacije u slučaju otkaza i kvarova delova IKT sistema,
- regulisati načine korišćenja i čuvanja laptop računara, sa težištem zabrane korišćenja istih u višenamemske svrhe i izdvajanjem službenih od privatnih računara i podataka,
- regulisati čuvanje podataka i informacija, bilo da se radi o izvornom ili elektronskom obliku,
- vršiti permanentnu kontrolu raspoloživosti i pristupu informacijama, kroz redovne i vanredne kontrole i nenajavljene obilaske mesta izrade i čuvanja nformacija,
- preduzimati mere fizičko-tehničke zaštite, sa ciljem zaštite od neovlašćenog pristupa prostorijama opremi i dokumentaciji i
- vršiti kontrolu korišćenja Interneta i elektronske pošte, naročito kada je pojava da se jedan računar koristi i zaposlovne i za privatne potrebe.

Angažovanjem menadžmenta (Perera, 2008) (ISO, 2013), zaposlenih u IT i sektoru bezbednsti, neophodno je pored ovih aktivnosti, permanentno raditi sa korisnicima informacija na svim nivoima, izvršiti podelu obaveza i odgovornosti i vršiti interne i eksterne provere znanja, karakteristika i postupaka istih.

4 EKSTERNA ZAŠTITA INFORMACIJA I IKT SISTEMA

Kada su kompanije, veliki javni sistemi ili državni organi u pitanju, u delu koji bi se bavio eksternom zaštitom informacija najvažniju ulogu ima osoblje iz IKT sistema koje pored ostalh postupaka treba da sprovede i sedeće aktivnosti:

1. Prevencija delovanja virusa, crva, trojanaca, i drugih malicioznih programa.

   Postiže se korišćenjem legalnih softvera, njihovim neprekidnim ažuriranjem i korišćenjem kvalitetnih antivirusnih programa.

2. Detekcija delovanja virusa, crva, trojanaca, i drugih malicioznih programa.

   Ukoliko i pored svih postavljenih zaštita, maliciozni programi prodru u sistem, njihova rana detekcija u cilju sprovođenja mera za otklanjanje posledica

   Monitoringom i alertingom smanjuje se vreme potrebno za detekciju problema, a samim tim je reakcija brža, efikasnija i sprečavaju se veći gubici informacija.

3. Korišćenje softverskih alata

   Korišćenje niza softverskog alata koji je dostupan u samim operativnim sistemima, njihovom nadogradnjom i praćenjem učinka smanjuje se mogućnost gubitka informacija.

4. Zabrana ili ograničavanje pristupa mrežama

   Posebno je karakteristično za velike kompanije sa velikim brojem računara u operativnoj upotrebi, a koje često isti računar koriste za ličnu upotrebu, internu komunikaciju i povezivanje na globalnu mrežu. Menadžment u saradnji sa organima zaduženim za poslove bezbednosti i IT sektorom reguliše ko, kada i kojim javnim mrežama može pristupiti.

5. Administriranje prava

   Ostvrtom na predhodnu činjenicu upotrebe jednog računara za više konekcija, neophodno je da se administratorskim pravima ograniči i interna komunikacija u segmentima ili u celini, a u zavisnosti od značaja radnog mesta korisnika.

6. Kriptozaštita

   U savremenom vidu prenosa informacija, (Markagić, 2011) nezamislivo je da se bilo koji vid komunikacije gde su sadržane poverljive informacije obavlja u izvornom, odnosno otvorenom obliku.

   Za konkretnu zaštitu delova ili cele informacije, što je i najčešći slučaj, na raspolaganju je veliki broj kriptografskih algoritama, javno dostupnih i testiranih u praktičnoj primeni.

   Korišćenjem pouzdanog algoritma uz primenu kvaltetnog kriptografskog ključa često je napadaču onemogućen dolazak do informacija.

S druge strane veoma mali broj pojedinaca i institucija poseduje kadar opremu ali ne raspolaže dovoljnim vremenskim resursima za izvođenje kriptoanalize, te kriptovane informacije često i ne budu predmet razmatranja.

Bez obzra na sve izneto nikada ne treba zanemariti činjenicu: *Čovek je osnovna, ali često i najslabija karika bezbednosti.* (Nikolić, 2012)

5 ZAKLJUČAK

Bio je ovo pokušaj da se kroz sagledavanje načina prenosa, ranjivosti i gubitaka informacija, ukaže na nekoliko mogućih vidova interne i eksterne zaštite istih.

Činjenica je da se svaki deo pomenut u tekstu može i mora posmatrati kroz multidisciplinarni pristup, uz poznavanje više naučnih oblasti, te da je ovo samo jedan vid razmatranja zaštite.

Ključne vrednosti bezbednosti informacija i IKT sistema nisu i nikako ne smeju biti predmet razmatranja i delovanja samo uskog kruga stručnih lica, već celokupnog kadra uključenog u generisanje, korišćenje, transfer i zaštitu informacija svih oblika. Nezamenjljiva je uloga top menadžmenta u kreiranju politike i plana zaštite.

Savremeni vidovi komunikacije i razvoj globalne mreže, laka dostupnost informacijama i softverskim rešenjima, sa jedne strane doprinose kvalitetnijoj komunikaciji, a sa druge strane predstavljaju pogodno tlo za zloupotrebu informacija i IKT sistema.

6 Citirani radovi

Ewell, C. V. (2009, 06). A method[ology] to the madness. *Information Security, 11*(6), 21-30.

ISO. (2013). *ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.* Retrieved from ISO 27001 security: http://www.iso27001security.com/html/27001.html

Markagić, M. (2011). *Kriminal u sajber prostoru i informaciona bezbednost.* Beograd: NIC Odbrana.

Nikolić, D. Ž. (2012, 07 12). *Unutrašnji izvor ugrožavanja - pretnja informacionim sistemima.* Retrieved from ITveštak: http://www.itvestak.org.rs/ZITEH_12/radovi-12/Unutrasnji%20izvor%20ugrozavanja%20-%20pretnja%20IS.pdf

Perera, D. (2008, 07 26). *ISO/IEC 27001 Information security management system.* Retrieved from Daminda: http://www.daminda.com/downloads/ISO27001.pdf

Petrovic, S., Cekerevac, Z., & Grubor, G. (2005). Security System Engineering Capability Maturity Model in the ICT Security. *Proceedings - X International Scientific Conference CRISES SITUATIONS SOLUTION IN THE SPECIFIC ENVIRONMENT* (p. 8). Žilina: FSI University of Žilina. Retrieved 03 12, 2013

Datum prve prijave: 04.02.2013.
Datum prijema korigovanog članka: 29.03.2013.
Datum prihvatanja članka: 09.04.2013.

Kako citirati ovaj rad?

Style – **APA** Sixth Edition:

Markagić, M. (2013, 07 15). Eksterna i interna zaštita elektronskih informacija. (Z. Čekerevac, Ed.) *FBIM Transactions*, 1(2), 85-91.

Style – **Chicago** Fifteenth Edition:

Markagić, Milorad. "Eksterna i interna zaštita elektronskih informacija." Edited by Zoran Čekerevac. FBIM Transactions (MESTE) 1, no. 2 (07 2013): 85-91.

Style – **GOST** Name Sort:

Markagić Milorad Eksterna i interna zaštita elektronskih informacija [Journal] = Zaštita elektronskih informacija // FBIM Transactions / ed. Čekerevac Zoran. - Belgrade : MESTE, 07 15, 2013. - 2 : Vol. 1. - pp. 85-91. - ISSN 2334-704X (Online); ISSN 2334-718X.

Style **Harvard** Anglia:

Markagić, M., 2013. Eksterna i interna zaštita elektronskih informacija. *FBIM Transactions,* 15 07, 1(2), pp. 85-91.

Style – **ISO 690** – Numerical Reference:

Eksterna i interna zaštita elektronskih informacija. **Markagić, Milorad.** [ed.] Zoran Čekerevac. 2, Belgrade : MESTE, 07 15, 2013, FBIM Transactions, Vol. 1, pp. 85-91. ISSN 2334-704X (Online); ISSN 2334-718X.