BEZBEDNOST PODATAKA NA INTERNETU

DATA SECURITY AT THE INTERNET

PhD, Srđan Tomić, profesor[255]
PhD, Brankica Pažun, docent[256]
MSc, Damir Ilić, saradnik u nastavi[257]

Apstrakt: *Sajber bezbednost više ne može da se posmatra odvojeno od bezbednosti u realnom svetu. Ipak, zbog specifičnosti vezanih za tehnologiju, vrste, počinioce i žrtve ovakvih napada pitanje sajber bezbednosti zahteva posebnu brigu svih koji se bave Internetom. Sajber bezbednost je u žiži interesovanja savremenog društva zahvaljujući nagloj ekspanziji broja korisnika Interneta. Prateći efekat nagle integracije Interneta u skoro sve oblike ljudske delatnosti je povećana ranjivost savremenog društva od sajber napada. Internet je deo kritične globalne infrastrukture i mnogi drugi bitni servisi savremenog društva (e-Trgovina, e-Bankarstvo…) sve više zavise od Interneta i česta su meta sajber napada.*

Ključne reči: *bezbednost, internet, e-trgovina*

Abstract: *Cyber security can no longer be considered separately from safety in the real world. However, due to the specifics related to technology, types, perpetrators and victims of these attacks the issue of cyber security requires special care of all who deal with the Internet. Cyber security is a major focus of modern society, thanks to the rapid expansion of the number of Internet users. Following the impact of the rapid integration of the Internet in almost all areas of human activity has increased the vulnerability of modern society against cyber-attacks. The Internet is a critical part of the global infrastructure and many other important services of modern society (e-commerce, e-banking ...) are increasingly dependent on the Internet and are often the targets of cyber-attacks.*

Key words: S*ecurity, Internet, e-Commerce*

UVOD

Bezbednosne mere predstavljaju skup aktivnosti koje se preduzimaju da bi se obezbedili podaci. Ni jedne bezbednosne mere ne mogu osigurati 100% bezbednost sistema. U velikom broju slučajeva, obim i kvalitet ovih mera zavisi od količine sredstava koja su uložena u njih. Veoma često ta sredstva nisu velika tako da i mere koje se preduzimaju ne mogu da pruže adekvatnu zaštitu. Međutim treba znati da šteta koja nastaje posle, kada neko ugrozi bezbednost sistema, je po pravilu znatno veća nego što je ulaganje u dobar sistem zaštite. Sami rukovodioci ovo shvataju tek kad se napad na informacioni sistem

[255] Fakultet za inženjerski menadžment, Bulevar vojvode Mišića 43, Beograd
[256] Fakultet za inženjerski menadžment, Bulevar vojvode Mišića 43, Beograd
[257] Fakultet za inženjerski menadžment, Bulevar vojvode Mišića 43, Beograd

dogodi, ali je to po običaju uvek prekasno. Što se tiče izbora zaštitnih mera koje će se preuzeti, on zavisi od brojnih faktora. Kao što su:

- Opšti atributi PIS
- osobine lokacije PIS
- grana delatnosti korisnika PIS
- veličina organizacije i njena struktura
- složenost opreme i postupaka u PIS
- karakteristike krajnjih korisnika
- karakteristike podataka

2. Posebni atributi PIS
   - karakteristike izvora saobraćaja
   - karakteristike OSI modela, izuzimajući protokole sedmog nivoa
   - sistem prenosa, multipleksiranje i komutacije
   - mrežni operativni sistemi
   - terminali, računari, radne stanice i druga oprema
3. Posebni atributi PIS specijalnog sistema
   - topologija mreže
   - mobilnost korisnika
   - širina propusnog opsega komunikacionog kanala
   - stepen grešaka
   - vreme prenosa podataka
   - vreme obrade podataka
   - stabilnost telekomunikacione infrastrukture
   - organizacija upravljanja

Na kraju, može se izvesti zaključak da ne postoji univerzalni skup bezbednosnih mera koji može da obezbedi apsolutnu sigurnost PIS. Čak se može reći da svaki PIS treba da ima svoju univerzalnu zaštitu koja će na najbolji mogući način biti prilagođena njegovim potrebama.

Doc. dr Brankica Pažun *je diplomirala i magistrirala iz oblasti informacionih tehnologija na Fakultetu organizacionih nauka. Kao stipendista Ministarstva spoljnih poslova Italije završila je master studije u Rimu, na Univerzitetu Tor Vergata, iz oblasti razvojne ekonomije i međunarodne saradnje, a potom doktorirala na Fakultetu za međunarodnu ekonomiju. Uporedo sa angažovanjem u softverskoj industriji i u sistemu Ujedinjenih nacija (UN HABITAT) radi kao predavač na Institutu Vinča – Škola računara Vinča u sastavu Univerziteta u Beogradu. Akademsku karijeru započinje 2009. u zvanju asistenta na Fakultetu za poslovne studije, a 5 godina kasnije kao docent na Fakultetu za inženjerski menadžment, na katedri za informacione tehnologije. Autor je i koautor preko 35 naučnih radova i autor jednog udžbenika.*

BEZBEDNOST INFORMACIONIH SISTEMA SERIJE STANDARDA ISO 27001

Menadžment sistem bezbednosti informacija (ISMS – Information Security Management System) definisan je međunarodnim standardom ISO/IEC 27001 koje su zajedno razvile dve vodeće organizacije za standardizaciju: ISO - The International Organization for Standardization i IEC - The International Electrotechnical Commision.

Jedan od ključnih resursa u savremenom poslovanju predstavljaju informacije. Finansijski podaci, podaci o načinu rada organizacije, kontakti sa korisnicima, podaci o zaposlenima, podaci o proizvodima i tehnologijama, ugovori, zapisi, itd. samo su mali deo u moru

informacija sa kojima raspolaže savremena organizacija. Bezbednost ovih informacija je od ključnog značaja za njihov opstanak. Prema najnovijim istraživanjima, nakon gubitka informacija 43% kompanija se trajno zatvara, 51% se zatvori posle dve godine, dok svega 6% uspe da nastavi sa poslovanjem.

Po poslednjem istraživanju Pricewaterhouse Coopers u saradnji sa CIO magazinom iz 2010. godine, napad na podatke se značajno povećao, i glavni cilj napada na informacije u organizacijama su baze podataka. Serija standarda iz familije ISO/IEC 27000 razvijena je u cilju odgovora na potrebe organizacija za uspostavljanjem sistemskog upravljanja bezbednošću informacija i informacionih sistema. Serija standarda koji se odnose na menadžment sistem bezbednosti informacija su:

- ISO/IEC 27001:2005 – Zahtevi
- ISO/IEC 27000:2009 – Osnove i rečnik pojmova
- ISO/IEC 27002:2005 – Kodeks postupaka za upravljanje bezbednošću informacija
- ISO/IEC 27003:2010 – ISMS uputstvo za primenu
- ISO/IEC 27004:2009 - Merenja u menadžmentu bezbednosti informacija
- ISO/IEC 27005:2008 - Menadžment rizika bezbednosti informacija

Damir Ilić *je diplomirao, a zatim i stekao akademski naziv Master inženjer menadžmenta na Fakultetu za inženjerski menadžment. Saradnik je u nastavi i rukovodilac Službe kontrole kvaliteta na Fakultetu za inženjerski menadžment. U fokusu njegovog istraživanja su upravljanje projektima, kontrola kvaliteta i informacione tehnologije u odbrambenoj industriji.*

Standard ISO/IEC 27001:2005, koji se implementira u organizacije, je primenjiv za različite veličine i tipove organizacija, od banaka, osiguravajućih društava, vlada i njenih organizacija, do zdravstvenih organizacija, državnih i privatnih preduzeća. Zainteresovane strane čine klijenti, vlasnici, zaposleni, isporučioci, poslovni partneri i društvo u celini, s obzirom da se informacije u okviru organizacije tiču svih pojedinačno.

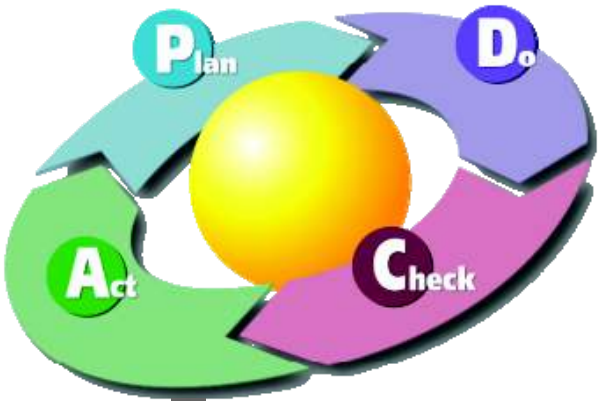
Prednosti implementacije standarda ISO/IEC 27001:200534:

- *u okviru organizacije se formulišu zahtevi i ciljevi za zaštitom i bezbednosti informacija,*
- *efektivno se upravlja rizicima bezbednosti,*
- *obezbeđuje se usklađenost sa zakonskim i ostalim zahtevima,*
- *definiše se novi proces bezbednosti informacionih sistema,*
- *definiše se status bezbednosti informacija i aktivnosti koji one nose,*
- *definiše stepen usklađenosti sa politikom, direktivama i standardima organizacije,*
- *obezbeđuje relevantne informacije o bezbednosti informacija korisnicima,*
- *smanjenje incidenata i bolje razumevanje uzročnika,*
- *razvija se svest zaposlenih u smislu značaja zaštite informacija,*
- *obezbeđuje se jasan protok i raspoloživost informacija i dr.*

Poštujući procesni pristup, standard ISO/IEC 27001:2005 definiše zahteve za uspostavljanje, primenu, monitoring, preispitivanje, održavanje i unapređenje dokumentovanog menadžment sistema bezbednosti informacija. Uspešno dizajniran i implementiran menadžment sistem bezbednosti informacija, koji obuhvata ljude, procese i IT sistem, pruža sigurnost i uverenje korisnicima i poslovnim partnerima da je bezbednost informacija na listi prioriteta poslovanja, da se prema njima postupa profesionalno i odgovorno.

Kao i kod drugih ISO standarda, ISO/IEC 27001 usvaja P-D-C-A model koji se primenjuje u strukturu ISMS procesa. Kao ulazi u sistem, predstavljeni su zahtevi i očekivanja za bezbednost informacija svih zainteresovanih strana i kroz sve neophodne akcije i procese se obezbeđuje ispunjenje ovih očekivanja i zahteva.

ISO 27001 standard objavljen je u oktobru 2005. godine i suštinski je zamenio stari BS 7799 – 2 standard. To je specifikacija za ISMS sistem za upravljanje bezbednošću informacija. BS 7799 je prvi put objavljen 90 - ih godina, i bio dugogodišnji standard kao kodeks ponašanja. Danas više od hiljadu ovih sertifikata su prisutni u celom svetu. ISO 27001 je poboljšan sadržaj BS 7799 – 2 i usklađen je sa drugim standardima.
Cilj standarda je da se "obezbedi model za uspostavljanje implementacije, rukovanje, praćenje, pregled, održavanje i unapređenje sistema za upravljanje bezbednošću informacija". Standard definiše svoj "procesni pristup" kao "primena sistema procesa unutar organizacije, zajedno sa identifikacijom i interakcijom ovih procesa i upravljanje njima". To koristi PDCA (Plan – Do – Check – Act) tj. (Planiraj – Uradi – Proveri – Poboljšaj) model za strukturu procesa, i održava principe iznete u OECG smernicama.



Slika 1: PDCA (Demingov) ciklus

Politika sistema menadžmenta za bezbednost informacija, zajedno sa ciljevima sistema menadžmenta za bezbednost informacija, i definisanim merama na unapređenju sistema u pogledu poboljšanja bezbednosti informacija, čine "Plan-Planiraj" deo sistema menadžmenta za bezbednost informacija, prema zahtevima standarda ISO 27001. Na osnovu iskazanih zahteva korisnika i kroz uspostavljanje politike ISMS organizacija, ulazi u fazu uspostavljanja,odnosno planiranja sistema za upravljanje bezbednošću informacija.

Sledeća faza je sprovođenje „Plan – Planiraj". Struktura i odgovornosti, obuka, kompetentnost i svest, dokumentacija i kontrola dokumenata, kontrola nad operacijama i spremnost na reagovanje u vanrednim situacijama i odgovor na njih čine "Do-Uradi" deo sistema menadžmenta za bezbednost informacija prema zahtevima standarda ISO 27001.

Treća faza je preispitivanja ISMS-a na osnovu definisanih procedura za preispitivanje, merenje efektivnosti upravljačkih mehanizama, sprovođenja internih provera, ažuriranje planova za snižavanje rizika itd.
Na kraju, "Act-Deluj" deo sistema menadžmenta za bezbednost informacija prema zahtevima standarda ISO 27001 se ostvaruje kroz preispitivanje od strane rukovodstva, koje zaokružuje ceo ciklus performansi sistema menadžmenta, i vraća ga na planiranje, koje treba da rezultuje kontinualnim poboljšanjem.

ISO/IEC 27001 je službena grupa specifikacija na osnovu kojih organizacije imaju pravo da traže postupak sertifikacije, naravno ukoliko su primenile taj standard na sistem upravljanja bezbednosti informacija. Ovaj standard propisuje zahteve za ustanovljavanje, implementaciju, kontrolu i unapređenje ISMS-a, sistema za upravljanje bezbednošću informacija. Standard je primenljiv na sve vrste organizacija (komercijalne, neprofitne, državne institucije, itd.) i sve veličine organizacija, od malih do velikih svetskih organizacija.
Standard se sastoji od 5 delova:

- Sistem za zaštitu informacija,
- Odgovornost rukovodećih ljudi,
- Unutrašnje provere sistema za zaštitu informacija,
- Provera valjanosti sistema za zaštitu informacija,
- Poboljšanja na sistemu za zaštitu informacija.

U standardu su navedeni ciljevi provere koje je potrebno ostvariti, i provere koje je potrebno sprovesti, kako bi se ostvarili ti isti ciljevi. Postoje institucije akreditovane za sertifikaciju prema ISO/IEC 27001 standardu, ali isto tako i veliki broj organizacija koje su sertifikovale svoje informacione sisteme prema ISO/IEC 27001 standardu, ili standardima pojedinih država. Sertifikacija je izbor organizacije, ali treba spomenuti, da poslovni partneri ponekad traže da organizacija s kojom sarađuju ima sertifikat.

Doc. dr Srđan Tomić
Doktorirao na temu: "Menadžment kvaliteta sa posebnim osvrtom na međunarodne i evropske standarde sistema menadžmenta kvaliteta" na Fakultetu za inženjerski internacionalni menadžment, stekao naziv magistra na temu: „Komparativni pristup menadžmenta u pivarstvu" i diplomirao na temu: „Menadžment u automobilskoj industriji" na Fakultetu za inženjerski internacionalni menadžment.
Na Fakultetu za inženjerski menadžment predaje predmete Osnove menadžmenta, Kontrola kvaliteta i Upravljanje kvalitetom.

ORGANIZACIONE KORISTI OD PRIMENE SERIJE STANDARDA ISO 27001

Značajne su koristi koje model za uređenje sistema za bezbednosti informacija ISO 27001, ostvaruje organizacijama, koje se odluče da ga implementiraju, pre svega, u smislu poboljšanja svojih organizacionih performansi.

Implementacijom ISO 27001 standarda i sertifikacijom takvog sistema, organizacije ostvaruju brojne dobiti od kojih su neke:

- kod potencijalnih ili postojećih korisnika se stvara poverenje u informacioni sistem,

- obezbeđuje se da organizacija ima potpuno komplementaran sistem sa pravnom regulativom, koja je vezana za informacione tokove,
- obezbeđuje se i sistem, koji je posebno orijentisan na upravljanje rizikom,
- obezbeđuje se naprednije razumevanje informacionih tokova u organizaciji,
- ostvaruje se bolja analiza troškovi / dobiti,
- ostvaruje se lakši proces monitoringa,
- moguće je povećati preventivno,
- smanjenje incidenata i bolje razumevanje uzročnika,
- razvija se svest zaposlenih u smislu značaja zaštite informacija,
- obezbeđuje se jasan protok i raspoloživost informacija i dr.

ZAKLJUČAK

Danas kada je upotreba računara, informacionih sistema i Interneta gotovo neizbežna u poslovanju, učenju, pronalaženju informacija itd. neophodno je koristiti zaštitu od raznih malicioznih softvera, napadača na korporativne i privatne podatke, koja se ogleda primenom kriptografskih i nekriptografskih mehanizama u više slojeva arhitekture informacionih sistema.

Ono što je danas aktuelno kao metod napada u bliskoj budućnosti može biti modifikovana ili skroz zamenjena novom metodom koja zaobilazi postojeće sisteme zaštite. Stoga zaštita informacionih sistema ima i jako bitan zadatak praćenja svih novih metoda koje se koriste i koje bi mogle da se koriste od strane napadača.

REFERENCES

[1] Čerić, V., Varga, M., ur., Informacijska tehnologija u poslovanju, Sveučilište u Zagrebu, Element, Zagreb, 2004.
[2] Muller, J., Srića, V., Upravljanje odnosom s klijentima, MEP, 2005.
[3] Spremić, M., Menadžment i elektroničko poslovanje, Narodne novine d.d., Zagreb, 2004.
[4] Norton, Peter; »Nova unutrašnjost PC-a«; Kompjuter Biblioteka Čačak, Sams 2003.
[5] Mesmer, Hans-Peter; »PC hardver do kraja«; Kompjuter Biblioteka Čačak, Addison-Njesley 2002.
[6] Prof. dr Nikola Bračika "Poslovna Informatika",Čačak 2007.
[7] Rečnik komunikacionih tehnologija, Hari Njutn, Čačak 2005.
[8] Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet, Dutton, William H.; Dopatka, Anna; Law, Ginette; Nash, Victoria, Division for Freedom of Expression, Democracy and Peace, United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris, 2011., str. 103, ISBN 978-92-3-104188-4
[9] "INTERNET POLITICS" autora Andrew Chadwick-a, Oxford University Press, 2006.
[10]Stankić R. „Informatika u turizmu", Visoka turistička škola, 2008.
[11] Keković Z. „Sistemi bezbednosti", Fakultet bezbednosti, 2009.
[12] Milosavljević M. „Osnovi bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, 2006.