7. Naučno-stručni skup sa međunarodnim učešćem
"KVALITET 2011", Neum, B&H, 01 - 04 juni 2011.

MJERENJE EFIKASNOSTI SISTEMA UPRAVLJANJA INFORMACIONOM SIGURNOSTI ANALIZOM FIZIČKE KONTROLE PRISTUPA ZAŠTIĆENIM PROSTORIJAMA

MEASURING INFORMATION SECURITY MANAGEMENT SYSTEM EFFICIENCY THROUGH PHYSICAL ACCESS CONTROL ANALYSIS OF PROTECTED AREA

Enver Delić, dipl.oec.
mr.sc. Agić Dragana, dipl.iur
Institut za privredni inženjering, d.o.o., Zenica
Fakultetska 1, Zenica, Bosna i Hercegovina

Doc. Dr. Sabahudin Jašarević, dipl.inž.maš.
Univerzitet u Zenici
Mašinski fakultet u Zenici
Fakultetska 1, Zenica, Bosna i Hercegovina

REZIME

Podaci su najznačajniji resurs organizacija zasnovanih na znanju. Organizacije koje se bave sigurnošću i standardizacijom su davno uvidjele posljedice koje može izazvati curenje povjerljivih podataka i kroz različite standarde (NIST 800, PCI DSS, HIPAA, ISO 27000) omogućile firmama i javnim institucijama, koje posjeduju podatke koje žele da zaštite, da ih čuvaju u skladu sa najboljim svjetskim praksama.

Uvođenje sistema upravljanja zaštitom informacija po standardu ISO/IEC 27001:2005 podrazumijeva kontinuirano mjerenje efikasnosti i efektivnosti pojedinih kontrola i cjelokupnog sistema. Pravilna implementacija sistema nadzora fizičkog pristupa omogućava dobivanje preciznih metrika koje pružaju osnov za daljnja unapređenja sistema.

Ključne riječi: ISO 27001:2005, informacija, zaštita, ranjivost, efikasnost, mjerenje

SUMMARY

The data are the most important resource of organizations based on knowledge. Organizations that deal with security and standardization long realized the consequences that may cause leakage of confidential data and through different standards (NIST 800, PCI DSS, HIPAA, ISO 27000), they enable companies and public institutions that have information that they want to protect, to keep them in line with best international practices.

Implementation of information security management standard ISO/IEC 27001:2005 means the continuous measurement of the efficiency and effectiveness of individual controls and the overall system. Proper implementation of physical access control system provides to obtain accurate metrics that provide a basis for further system improvement.

Keywords: ISO 27001:2005, information, security, vulnerability, efficiency, measuring

1. UVOD

Zaštita povjerljivih podataka u modernom poslovanju se susreće sa sve većim izazovima. Razvojem modernih sredstava komunikacije i prijenosa podataka, reducirana je mogućnost nadzora nad podacima koji su od firme označeni kao interni ili povjerljivi. Najčešće se radi o ugovorima, tehnologijama, ličnim podacima, transakcijama i drugim podacima čije bi otkrivanje konkurenciji ili javnosti, kao i njihov gubitak ili neautorizovana promjena izazvali posljedice na poslovanje organizacije, kako kroz gubitak reputacije, tako i kroz direktne finansijske gubitke.

Organizacije koje se bave sigurnošću i standardizacijom su davno uvidjele posljedice koje može izazvati curenje povjerljivih podataka i kroz različite standarde (NIST 800, PCI DSS, HIPAA, ISO 27000) omogućile firmama i javnim institucijama koje posjeduju podatke koje žele da zaštite da ih čuvaju u skladu sa najboljim svjetskim praksama.

Cilj standarda ISO/IEC 27001:2005 je da obezbijedi uspostavu, implementaciju, nadziranje, održavanje i poboljšavanje sistema upravljanja informacionom sigurnošću (*Information security management system*, u daljem tekstu - ISMS). Prihvatanje ovog standarda je strateška odluka svake organizacije. Za razliku od drugih standarda koji pokrivaju ovu oblast ISO/IEC 27001:2005 se lako prilagođava veličini i potrebama organizacije.

Standard ISO/IEC 27001 je usklađen sa zahtjevima definisanim kroz standard ISO 9001 kako bi se sigurnost informacija shvatila kao kontinuirani proces a ne kao jednokratan zahvat. To je vidljivo i po tome što standard zahtjeva da se uspostava sistema za upravljanje sigurnošću informacija bazira na Demingovom ciklusu PDCA (*plan–do–check–act*, prev.engl.: planiraj-uradi-provjeri-reaguj).

Primjenom ovog sistema moramo uspostaviti i metrike za mjerenje efikasnosti i efektivnosti kako pojedinih implementiranih kontrola, tako i sveukupnog sistema.

2. USPOSTAVLJANJE KONTROLA

U okviru Instituta za privredni inženjering, koji ima ovlasti Vlade Federacije Bosne i Hercegovine da vrši nadzor svih stanica tehničkih pregleda u Federaciji Bosne i Hercegovine, smješten je centralni serverski sistem kojim se upravlja podacima prikupljenim na stanicama tehničkog pregleda u Federaciji Bosne i Hercegovine (sistem a|TEST). Ove informacije su označene povjerljivim od strane IPI-Instituta za privredni inženjering, a u skladu sa zahtjevima Zakona o zaštiti ličnih podataka, te je menadžment Instituta odlučio da se uspostavi sistem zaštite ovih podataka u skladu sa standardom ISO/IEC 27001:2005.
Evaluacijom obavljene analize rizika utvrđene su kontrole koje bi trebalo implementirati kako bi se reducirao nivo rizika od ozbiljnih prijetnji koje mogu iskoristiti određene ranjivosti sistema.

Rizik	Kontrola
Krađa podataka Krađa opreme Korupcija podataka Nedozvoljena obrada podataka Nedozvoljeno korištenje opreme Namjerno uništenje opreme Nenamjerno uništenje opreme Zloupotreba privilegija Krivotvorenje privilegija	Uspostavljena kontrola pristupa resursima i izvršena edukacija zaposlenika. Uspostavljeno sigurno područje u slojevima sa protuprovalnim otvorima, alarmom i videonadzornim sistemom. Uspostavljen kontinuiran nadzor od strane zaposlenika i evidencija ulaska i izlaska iz sigurnog područja. Softverski nadzor IT resursa, njihove dostupnosti, rada i izmjena.

Implementirane kontrole su usklađene u skladu sa preporukama standarda ISO/IEC 27002 definisanim u aneksima 9, 11 i 13:

A.9	**Fizička sigurnost i sigurnost okruženja**
A.9.1	**Sigurna područja**
A.9.1.1	Perimetar fizičke sigurnosti
A.9.1.2	Kontrola fizičkog pristupa
A.9.1.3	Zaštita ureda, prostorija i opreme
A.9.1.4	Zaštita od vanjskih prijetnji i prijetnji okruženja
A.9.1.5	Rad u sigurnim područjima
A.9.1.6	Javni pristup, područja za isporuku i utovar
A.11	**Kontrola pristupa**
A.11.1	**Poslovni zahtjevi za kontrolu pristupa**
A.11.1.1	Politika kontrole pristupa
A.11.2	**Upravljanje pristupom korisnika**
A.11.2.1	Registracija korisnika
A.11.2.2	Upravljanje privilegijama
A.11.2.3	Upravljanje korisničkim lozinkama
A.11.2.4	Pregledavanje korisničkih prava pristupa
A.13	**Upravljanje incidentima informacione sigurnosti**
A.13.1	**Izvještavanje o sigurnosnim događajima i ranjivostima**
A.13.1.1	Izvještavanje o događajima informacione sigurnosti
A.13.1.2	Izvještavanje o sigurnosnim slabostima
A.13.2	**Upravljanje incidentima informacione sigurnosti i poboljšavanja**
A.13.2.1	Odgovornosti i procedure
A.13.2.2	Učenje na incidentima informacione sigurnosti
A.13.2.3	Prikupljanje dokaza

3. EFIKASNOST USPOSTAVLJENIH KONTROLA

S ciljem analize efikasnosti sprovedenih mjera i adekvatnog reagovanja, neophodno je uspostaviti određene metrike. Obzirom da je pristup prostoriji u kojoj se vrši prikupljanje i obrada podataka (u daljem tekstu: zaštićena prostorija) dozvoljen samo ograničenom broju autorizovanih osoba, mjerenjem broja ulazaka zabilježenih na videonadzornom sistemu i upoređivanjem sa brojem evidentiranih ulazaka možemo izmjeriti efikasnost kontrola i aneksa 9. i 11. Ukoliko neautorizovana lica pokažu interes za ulazak u serversku prostoriju u istu mogu ući samo nakon što dobiju odobrenje nadređenih kroz poseban računarski program i pošto potpišu izjavu o tajnosti, kojom se obavežu da neće odavati podatke koje bi mogli vidjeti u serverskoj prostoriji. Dodatna iskoristiva metrika je i upoređivanje broja ulazaka lica bez autorizacije sa ukupnim ulascima u zaštićen prostor. Dodatno se može iskoristiti broj vanrednih ulazaka sa brojem popunjenih formulara o incidentima kako bi se izmjerila efikasnost kontrole uspostavljene s ciljem upravljanja incidentima kako je definisano u aneksu 13 standarda ISO/IEC 27001:2005: „A.13 Upravljanje incidentima informacione sigurnosti“.

Za mjerenje koristimo sljedeće formule:

1. *(Broj ulaza zabilježenih od strane zaposlenika) * 100 / broj ulaza zabilježenih na videonadzornom sistemu.*

Očekivani nivo efektivnosti je 100% i za svaki nedostatak su predviđene sankcije u skladu sa poslovnikom organizacije.

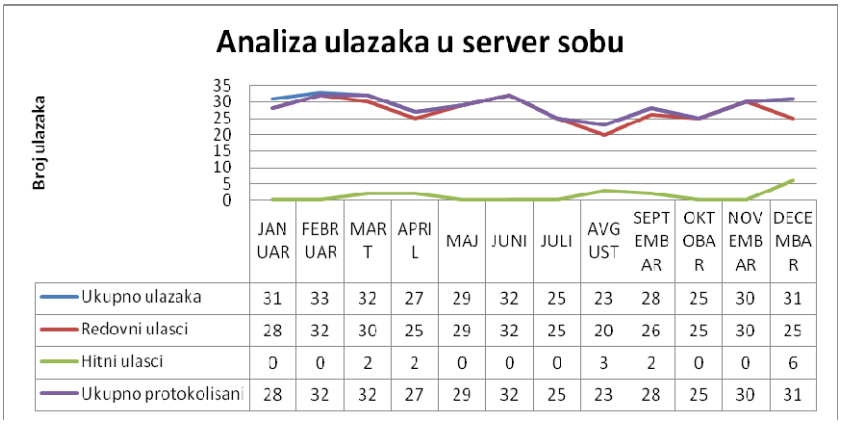
2. (*Broj autorizovanih lica koja su ušla) * 100 / ukupan broj lica zabilježenih na videonadzornom sistemu.*
Očekivani nivo efektivnosti je takođe 100% i za svaki nedostatak su predviđene sankcije u skladu sa poslovnikom organizacije.

*3. (Broj ukupnih ulaza - broj redovnih ulazaka) * 100 / broj izvještaja o incidentima*
Očekivani nivo efektivnosti je takođe 100% osim ukoliko se radi o ponavljajućem incidentu za koji je popunjen jedan izvještaj o incidentu.

Rezultati ovih mjerenja se analiziraju na mjesečnom nivou i na osnovu njih se poduzimaju odgovarajuće akcije („*Do*“ korak Demingovog ciklusa).

S ciljem prezentacije rezultata prikazujemo podatke za 2010. godinu. Obzirom da nije zabilježen nijedan neautorizovan ulazak, te podatke nismo prikazali.

Mjesec 2010 godina	Broj ulazaka koje bilježi videonadzorni sistem	Broj ulazaka koje bilježi ovlašteno lice			Procenat redovnih u odnosu na ukupne ulaske	Procenat evidentiranih u odnosu na ukupne ulaske
		redovno	vanredno	ukupno		
JAN	31	28	0	28	100%	90,32%
FEB	33	32	0	32	100%	96,96%
MART	32	30	2	32	93,75%	100%
APRIL	27	25	2	27	92,59%	100%
MAJ	29	29	0	29	100%	100%
JUNI	32	32	0	32	100%	100%
JULI	25	25	0	25	100%	100%
AVG	23	20	3	23	86,96%	100%
SEPT	28	26	2	28	92,86%	100%
OKT	25	25	0	25	100%	100%
NOV	30	30	0	30	100%	100%
DEC	31	25	6	31	80,64%	100%



Slika 1. Analiza ulazaka u server sobu tokom 2010. godine

Iz rezultata vidimo da je uvođenje mjerenja efikasnosti sprovođenja kontrole poboljšalo njenu implementaciju. Početkom mjerenja smo imali nekoliko ulazaka u sobu bez evidentiranja razloga ulaska kod administrativnog radnika, što je sankcionisano u skladu sa internim pravilnikom organizacije. Ove mjere su dovele do punog pridržavanja propisanih procedura za fizički pristup server sobi.

4. ZAKLJUČAK

Uspostavljanjem sistematičnog mjerenja efikasnosti, na samom početku su ustanovljene neke slabosti poput neevidentiranog ulaska u zaštićen prostor, što je uklonjeno brzo implementiranim korektivnim akcijama. Određene kontrole zahtijevaju maksimalnu efikasnost zbog rizika koji predstavljaju prijetnje koje bi mogle da iskoriste određene ranjivosti sistema. Zahtjev menadžmenta da nivo efikasnosti ne smije biti ispod 100% je omogućio potpunu efikasnost primijenjenih kontrola u kratkom periodu i reducirao potrebu za implementacijom dodatnih kontrola koje bi reducirale nivo rizika.

Menadžment je, na osnovu ovih i drugih rezultata, u periodu od marta do decembra 2010. godine, ISMS, koji je uspostavljen s ciljem čuvanja podataka koji se prikupljanju, obrađuju i distribuiraju u sistemu a|TEST, ocijenio efikasnim.

5. LITERATURA

[1] K. Thesis and P. Doctor, “Risks in Networked Computer Systems,” Doctor, 2008.
[2] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology,” Nist Special Publication.
[3] BSI, BS 7799-3:2006 Information security management systems – security risk management, 2006.
[4] International Organization for Standardization, ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements, 2005.
[5] International Organization for Standardization, ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management, 2005.
[6] International Organization for Standardization, ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management, 2004
[7] International Organization for Standardization, ISO 9001:2008, Quality management systems — Requirements, 2008.