NADZOR ISMS-A I ISO/IEC 27001:2005

ISMS MONITORING AND ISO/IEC 27001:2005

Enver Delić, dipl.oec. ISO/IEC 27001 Lead Auditor
IPI – Institut za privredni inženjering
Zenica

Adnan Stroil, dipl.el.ing.
a|NET
Zenica

Elvis Pivić, ISO 9001 Interni Auditor
a|NET
Zenica

REZIME
Nadzor informacionog sistema je jedan od zahtjeva aneksa A standarda ISO/IEC 27001. Pored toga što nadzire dostupnost, integritet i povjerljivost štićenih podataka, omogućava nam neporecivost korisničkih akcija.

Ključne riječi: ISO/IEC 27001, ISMS, nadzor

SUMMARY
Information security monitoring is a part of theinformation security management system based on ISO/IEC 27001. Besides monitoring confidentiality, integrity and availability of protected information it helps us eliminate deniability of user actions.

Ključne riječi: ISO/IEC 27001, ISMS, monitoring

1.POTREBA ZA NADZOROM ISMS-A

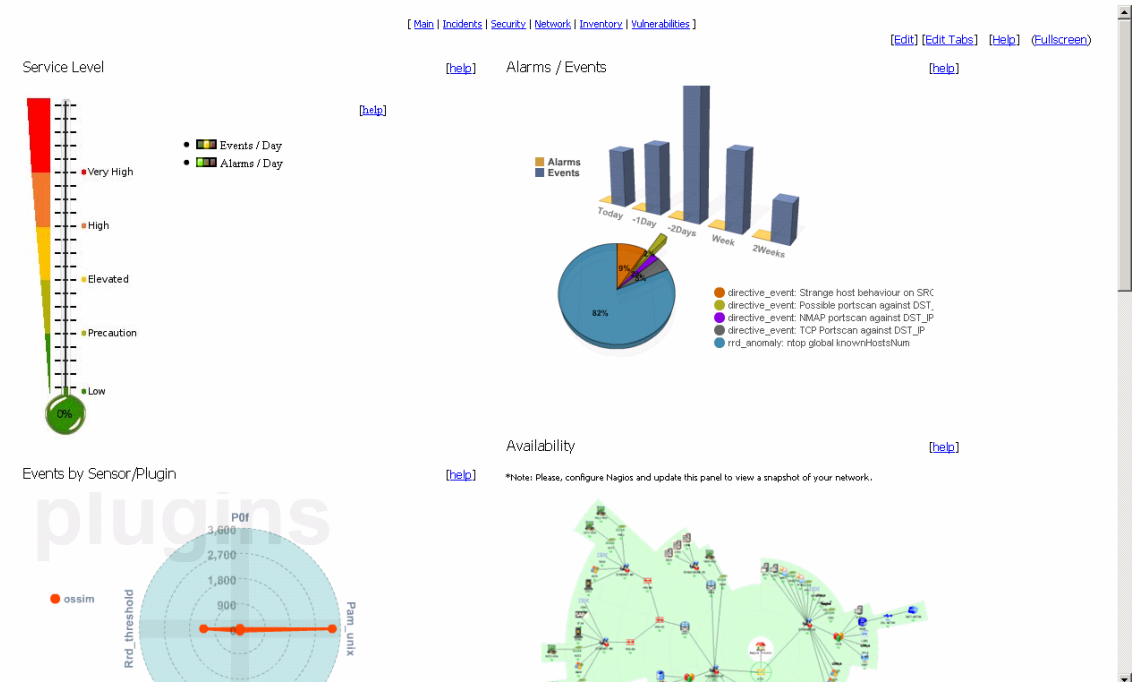
Sanja Meseldžija-Gvožđar, blagajnica i kontrolorka blagajne u filijali "Raiffeisen banke" u Banja Luci počinila je kaznena djela pronevjera i falsificiranje ili uništavanje poslovnih ili trgovačkih knjiga ili isprava na taj način što je od 25. decembra 2006. do 28. septembra 2007. obavljajući poslove vršila nezakonite novčane transakcije čime je protupravno prisvojila oko 2.252.000 KM, na štetu "'Raiffeisen banke". Odgovorni u banci su posumnjali da nešto nije u redu tek nakon što se gospođa Meseldžija-Gvožđar prestala pojavljivati na poslu. Nakon što je uhapšena i osuđena na osam godina i četiri mjeseca zatvora, sudija je upozorio i upravu banke na neadekvatne sigurnosne kontrole.

Terry Childs, 43-godišnji administrator gradske mreže San Franciska je, nezadovoljan izdvajanjima za održavanje mreže, preoteo kompletnu mrežu koja je služila za distribuciju i pohranu službene elektronske pošte, platnih lista, policijskih, zatvorskih i medicinskih dokumenata. Childs je ukinuo pristup svim drugim administratorima i samo je njegov „superkorisnički" account mogao administrirati brojne servere i usluge ove mreže. Tek nakon što je gradonačelnik San Franciska posjetio Childsa u zatvoru, ovaj mu je vratio lozinke. Da se desio bilo kakav veći problem tokom tih dana, šteta je mogla biti multimilionska. Velika sreća je što novac nije bio motiv ovom kriminalcu, jer su on ili potencijalni saučesnici imali ekskluzivan pristup osjetljivim ugovorima i ostalim dokumentima.
Najveća prijetnja po sigurnost neke kompanije su njeni uposlenici. Iako čine samo 20% incidenata, načine 80% štete. Hakeri vam mogu uništiti sistem na različite načine, ali redovan i pravilno izveden backup gotovo u potpunosti eliminišu ovu prijetnju i svode je na par sati nedostupnosti koliko je potrebno da se sistem ponovo podigne. Međutim, nezadovoljni uposlenici mogu napraviti mnogo veće štete. Nijedan od ova dva slučaja se ne bi desio, ili bi štete bile neuporedivo manje da su na vrijeme aktivirani alarmi koji bi upozorili na prekoračenje ovlasti. Kvalitetan nadzorni sistem je jedina kontrola koja može, ako ne eliminisati, a onda znatno umanjiti poriv za malicioznim aktivnostima ljudi, obzirom da se mogućnost otkrivanja tih aktivnosti drastično povećava.

2. NADZORNI SISTEM UNUTAR PROJEKTA A|TEST IPI – INSTITUTA ZA PRIVREDNI INŽENJERING

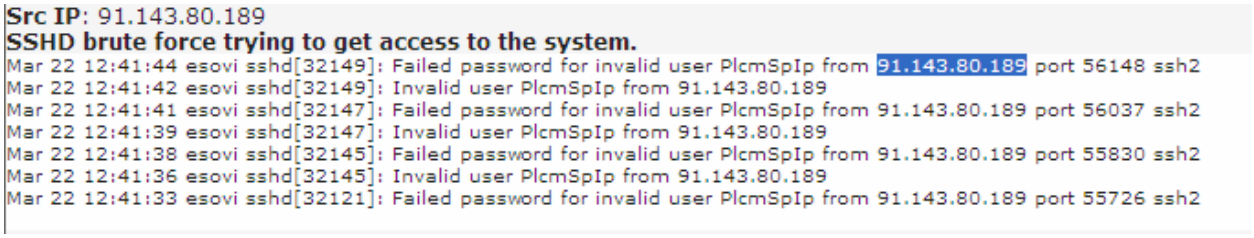
„Institut za privredni inženjering" Zenica se bavi istraživanjem i eksperimentalni razvojem, planiranjem i projektovanjem, konsaltingom i edukacijom. IPI – Institut čine dvije jedinice: poslovna jedinica „*Inžinjering*" i poslovna jedinica „*Centar za vozila*".
PJ Inženjering
Aktivnosti ove poslovne jedinice su sljedeće:
Izrada: studija i elaborata, razvojnih i biznis planova, programa, projekata i druge tehničke dokumentacije; konsalting: o tehničko-tenološkim i ekonomsko-finansijskim pitanjima, uvođenju i razvoju proizvoda, izboru opreme i investiranju, tržišnom nastupu i promocionim aktivnostima;
PJ Centar za vozila
Odlukom Vlade FBiH, između Federalnog ministarstva prometa i komunikacija i IPI – Instituta za privredni inžinjering, sklopljen je Ugovor o međusobnim pravima i obavezama, a kojim su na IPI – Institut preneseni sljedeći poslovi:
Stručno osposobljavanje kontrolora tehničke ispravnosti vozila, voditelja stanica tehničkog pregleda i drugih osoba koje rade na stručnim poslovima tehničkog pregleda; periodična provjera znanja kontrolora tehničke ispravnosti vozila i drugih osoba koje rade na stručnim poslovima tehničkog pregleda; kontrola izvršenog baždarenja opreme kojom se vrši kontrola tehničke ispravnosti vozila ; obrada podataka i izrada analiza iz oblasti tehničkog pregleda vozila; izrada pisanih uputstava, informacija i stručnih publikacija iz oblasti tehničkog pregleda vozila; uvezivanja stanica za tehnički pregled vozila i drugih zainteresovanih subjekata u jedinstven informatički sistem, vezan za poslove tehničkog pregleda vozila; praćenje propisa iz oblasti kontrole ispavnosti vozila koje donose susjedne zemlje, Evropska unija i druge međunarodne organizacije; saradnja sa stručnim, naučnim organizacijama, institutima, preduzećima i drugim pravnim licima iz oblasti tehničkog pregleda vozila.
Najkompleksnija obaveza iz prenesenih oblasti je dizajn, implementacija i razvoj informacionog sistema koji će se razviti pod imenom a|TEST čiji je cilj prikupljanje podataka o registrovanim vozilima i njihovim vlasnicima sa stanica tehničkog pregleda u realnom

vremenu, obrada tih podataka i pružanje statističkih informacija ovlaštenim subjektima. Dio informacija, koje su se odlukom Vlade prikupljale i analizirale, je zaštićen Zakonom o zaštiti ličnih podataka koji je stupio na snagu 2006. godine.
Analizom rizika, koristeći prilagođenu metodologiju instituta CERN zaključili smo da su ljudi, kako uposlenici, tako i treća lica, najosjetljivija karika u sistemu. Kako bi smanjili mogućnost zloupotrebe na razumnu mjeru implementirali smo niz kontrola. Prije svega, sve osobe koje makar i samo potencijalno mogu doći u kontakt sa povjerljivi podacima uključujući uposlenike IPI-ja i treća lica sa kojima postoje sporazumi o saradnji su dužne potpisati sporazum o povjerljivosti gdje su navedene njihove obaveze, odgovornosti i sankcije koje će trpjeti u slučaju kršenja sporazuma. Korisnici pristupaju na sistem koristeći vlastito korisničko ime i lično su odgovorni za čuvanje svoje lozinke. Kako bi zaposlenici bili svjesni svojih odgovornosti i obaveza održana su dva treninga u kojima su pokriveni osnovni aspekti zaštite sigurnosti informacija, uključujući i politike korištenja računara, izbora sigurne lozinke i „politike čistog stola“. Znatno je reduciran broj ljudi unutar IPI- Instituta za privredni inženjering koji mogu imati pristup povjerljivim podacima, a uz to nijedna osoba pojedinačno ne može mijenjati, brisati ili dodavati podatke bez direktnog nadzora još jednog lica. Osobe koje vrše nadzor također nemaju direktan uvid u povjerljive podatke. Rukovodioci Instituta uopšte ne posjeduju privilegije koje bi im omogućile pristup ovim podacima. Kako bi obeshrabrili bilo kakav pokušaj zloupotrebe implementirali smo plan nadzora rada sistema koji pored informacija o radu sistema, iskorištenosti i dostupnosti resursa i pokušajima napada hakera izvana kontroliše i sve aktivnosti administratora sistema, osoba koje unose podatke i organizacija koje preuzimaju obrađene podatke. Čak se i rad saradnika za nadzor redovno nadzire. Tako prikupljeni zapisi se čuvaju 10 godina i zaštićeni su od vanjskih uticaja backup-om i enkripcijom.
Zahvaljujući posebno prilagođenoj aplikaciji za nadzor stanja resursa rukovodioci mogu imati prikaz svih značajnih događaja na jednom ekranu (Slika 1) a saradnik za sigurnost informacija ima pristup detaljnijim izvještajima sa informacijama o pokušajima neovlaštenog korištenja sistema, otkrivenim propustima na korištenim aplikacijama, dostupnosti i procentu iskorištenosti svakog pojedinog resursa.



Slika 1

Pored toga, za incidente najvišeg nivoa je implementirana trenutna dojava problema putem e-maila i SMS-a saradniku za sistem upravljanja sigurnošću informacija kako bi se odmah mogle poduzeti kontra mjere. Sam software posjeduje mogućnost aktivnog odgovora na predefinisane prijetnje ukoliko se pokaže potreba za tim. Struktura aplikacije i pravila na osnovu kojih se definiše nivo rizika se mijenjaju u skladu sa novim prijetnjama, pa se prijetnjama koje, po provedenoj analizi rizika, povećavaju ranjivost sistema dodjeljuje veća vrijednost kako bi aplikacija povećala pretpostavljeni nivo rizika i adekvatno kategorizirala novu prijetnju.
Zahvaljujući prikupljenim podacima možemo da pokrenemo akciju protiv nepoznatog zlonamjernog lica (Slika 2).



Slika 2

Iz dobijene IP adrese možemo vidjeti izvor napada (Slika 3):

Slika 3

Sada kad imamo detaljne informacije o porijeklu i vrsti napada možemo kontaktirati odgovarajuće autoritete u zemlji porijekla napada i preduzeti mjere kako se napad ne bi ponovio. Ukoliko je napad izveden unutar sistema odmah dobijamo ime korisnika i mjesto odakle je napad izvršen.

Kroz alate za nadzor lako je kontrolisati aktivnosti zaposlenika, pogotovu onih sa većim ovlastima. Sistem automatski pravi kategorije poduzetih akcija i ukoliko je urađeno nešto izvan standardnih operativnih zahvata, sistem poduzetu aktivnost izdvaja. Sedmičnom revizijom se analiziraju vanredne akcije, provjerava se razlozi za njihovo poduzimanje i u skladu sa tin informacijama poduzimaju odgovarajuće akcije. Očito je da pored povjerljivosti, integriteta i dostupnosti podataka dosta pažnje mora biti posvećeno i *neporecivost.* Zahvaljujući tome što se svi zapisi čuvaju do deset godina, tačno se zna ko je, kada, kako i tačno šta uradio, i ne postoji mogućnost prebacivanja ili izbjegavanja odgovornosti.

3. ZAKLJUČAK

Iako su namijenjeni analizi neovlaštenih pristupa sistemu, sistemi za detekciju neovlaštenih upada (Intrusion detection system, IDS) vrlo dobro rade i posao alarmnog sistema u slučaju podizanja privilegija korisnika, pojave rootkit aplikacija ili drugih malicioznih aplikacija. Zahvaljujući radu IT stručnjaka IPI – Instituta za privredni inženjering i a|NET d.o.o., postojeći sistem nadzora implementiran na projektu a|TEST je maksimalno prilagođen potrebama aplikacije a|TEST i zakonskim i ugovornim zahtjevima i trenutno je jedan od najboljih i najsvestranijih nadzornih sistema u Bosni i Hercegovini. Sistemi za detekciju neovlaštenih upada (Intrusion detection system, IDS) su postali praktično neophodan alat za integralni nadzor sistema i odlično se uklapaju u zahtjeve standarda ISO/IEC 27001.

4. LITERATURA

[1] „Blagajnici banjolučke Raiffeisen banke osam i pol godina zatvora - Vijesti.net“, Index.HR, Banja Luka 2008, http://www.index.hr/vijesti/clanak/blagajnici-banjolucke-raiffeisen-banke-osam-i-pol-godina-zatvora/408411.aspx

[2] BS7799-1 1999: Information Security Management-Part1: Code of Practice for Information Security Management. BS 7799-1, British Standards Institution, BSI (London)

[3] Clyde, R. A., 2002. The Focused Information Security Management Architecture. Infopro Weekly

[4] ISO/IEC 17799. 2000. Information technology-code of practice for information security management. BSI (London).

[5] ISO/IEC 27001. 2005. Information technology - Security techniques - Information security management systems - Requirements.

[6] ISO/IEC FDIS 17799. 2005. Information techniques-Security techniques-Code of practice for information security management (2nd edition). British Standards Institution.

[7] „S.F. officials locked out of computer network“, SF Gate, San Francisko 2008 http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL

[8] Zakon o izmjeni Zakona o slobodi pristupa informacijama u Bosni i Hercegovini (2006. godina).,

[9] Zakon o zaštiti ličnih podataka (Službeni glasnik Bosne i Hercegovine br. 49/06).