Mr Dejan Vuletic,
kapetan I klase,
Institut za strategijska istraživanja
Beograd

STANDARDI ZA UPRAVLJANJE SIGURNOŠCU PODATAKA

UDC: 006.4 : 004.6

Rezime:

U radu su analizirani osnovni pojmovi vezani za upravljanje sigurnošcu podataka. Ukazano je na potrebu i znacaj standardizacije u oblasti informaciono-komunikacionih tehnologija, narocito prema standardima Medunarodne organizacije za standardizaciju (International Standardization Organization – ISO). U završnom delu rada prikazane su proaktivne i reaktivne aktivnosti u upravljanju sigurnošcu podataka.

Kljucne reci: podaci, standardi, upravljanje sigurnošcu podataka.

STANDARDS FOR MANAGEMENT DATA SECURITY

Summary:

In this article basic notions of management data security are analyzed. We indicated demand and importance of standardization in information-communication technology domain, especially according to International Standardization Organization. In the final part of the article we illustrated both proactive and reactive activities in management data security.

Key words: data, standards, management data security.

Uvod

Standardi za upravljanje sigurnošcu podataka se, prema nameni, mogu podeliti na: standarde za sigurnost proizvoda, standarde za sigurnost procesa i standarde sigurnosti sistema [4].

Standardi koji osiguravaju sigurnost proizvoda definišu pravila pod kojima se može izdati sertifikat koji daje punu garanciju da je neki proizvod ili usluga sigurna. Nakon dve decenije razvoja i zajednickih napora, pre svega Japana, SAD, Kanade, Evropske unije i medunarodne zajednice, usvojen je standard ISO/IEC 15408 (Security Evaluation Criteria).

U podrucju standarda za sigurnost procesa najznacajniji je ISO/IEC (TR) 13335-x Uputstva za upravljanje sigurnošcu informacione tehnologije (Guidelines for the Management of IT Security – GMITS). Taj standard se sastoji od niza tehnickih izveštaja koji služe kao uputstvo za implementaciju sistema upravljanja sigurnošcu podataka resursa i sprovodenje postupka samoocenjivanja.

Standardi ISO/IEC

Medunarodna organizacija za standardizaciju (International Standardization Organization – ISO) i medunarodna elektrotehnicka komisija (International Electrotechnical Commission – IEC) konstituisale su združeni tehnicki komitet (Joint Technical Committee – JTC),

ciji je zadatak donošenje standarda iz oblasti informaciono-komunikacionih tehnologija. Britanski institut za standarde pripremio je, a ISO i IEC su usvojili medunarodni standard ISO/IEC 17799 cija je najnovija verzija objavljena 2005. godine. Ocekuje se da ce navedeni standard 2007. godine zameniti standard ISO 27002 [3], a predstavljace skup pravila namenjenih obezbedenju visokog nivoa upravljanja sigurnošcu podataka (informacija).

Pored standarda ISO/IEC 17799, odnosno ISO 27002, objavljeni su ili su u razvoju sledeci, sa aspekta upravljanja sigurnošcu, znacajni standardi:

– ISO 27001 – Information Security Management System (ISMS) requirements.

Ovaj standard objavljen je u oktobru 2005. godine, a zasnovan je na britanskom standardu BS 7799-2. Definiše zahteve koje mora da ispuni sistem za upravljanje sigurnošcu podataka, da bi akreditovana organizacija mogla da ga sertifikuje [2];

– ISO 27004 – Information Security Management Metrics and Measurement.

Ovaj standard je još uvek u razvoju i ocekuje se da ce biti objavljen 2007. godin?. Treba da pomogne organizacijama u merenju i izveštavanju o efikasnosti njihovih sistema za upravljanje sigurnošcu podataka obuhvacenih postupcima upravljanja sigurnošcu (definisanih u ISO 27001) i kontrolama (obuhvacenih u ISO 27002);

– ISO 27005 – Information Security Risk Management.

Ocekuje se da ce biti objavljen 2008. ili 2009. godine. Zasnivace se na britanskom standardu BS 7799-3, koji je objavljen u martu 2006. godine. Ovaj standard ce obuhvatati procenu rizika, sprovodenje odgovarajucih kontrola, nadgledanje i ponovnu procenu rizika u toku rada ili periodicno, održavanje i stalno unapredenje sistema kontrole i drugo.

Model sistema upravljanja sigurnošcu podataka, koji podržava standard ISO/IEC 17799 primenljiv je za organizacije svih tipova i velicina, a može se prilagoditi razlicitim geografskim, kulturnim i socijalnim uslovima. Ovaj standard zadovoljava potrebe razlicitih organizacija širom sveta, osiguravajuci im zajednicki okvir za bavljenje pitanjima u vezi sa sigurnošcu podataka [4].

Standard ISO/IEC 17799 bavi se problematikom definisanja politike sigurnosti i primene opšte dobre prakse upravljanja sigurnošcu podataka. Termin „politika racunarske sigurnosti“ definiše se kao direktiva rukovodstva da se formira plan zaštite podataka, utvrde ciljevi i odrede odgovornosti [8]. Taj standard pruža dragocenu pomoc kao pregled visokog nivoa koji menadžmentu kompanije omogucava da sagleda i razume problematiku upravljanja sigurnošcu podataka u sopstvenoj organizaciji [4].

Upravljanje sigurnošcu podataka u racunarskim sistemima može se, uslovno, podeliti na dva dela – proaktivno i reaktivno delovanje.

Proaktivnim delovanjem se, prvenstveno, onemogucava, otežava ili sprecava neovlašcenim licima da dodu do sadržine podataka ili dokumenata.

Reaktivnim delovanjem obezbeduje se da sistem povrati osnovne servise (odredene nivoe integriteta, poverljivosti, performansi i drugih kvalitativnih svojstava).

Proaktivno delovanje

Najbolji metod eliminisanja ili ublažavanja rizika jeste proaktivno delovanje koje se obezbeduje višestrukim sferama.

Model ešelonirane višeslojne zaštite podataka realizuje se modelom zaštitnih prstenova (sfera) koji cine:

– sfera fizicke zaštite (onemogucava fizicki pristup napadaca);

– tehnicka sfera (sistemi za detekciju i sprecavanje napada i dr.);

– kadrovska sfera (pravilan izbor kadrova i obezbedenje optimalnih uslova rada);

– organizaciona sfera (mere i aktivnosti, nadležnosti i obaveze korisnika i izvršilaca, kao i pristup resursima),

– normativna sfera (zakoni, uputstva, planovi i druge regulative koje obavezuju i propisuju izvršenje neke radnje i nacin izvršenja te radnje).

Standard ISO 17799 reguliše, sa aspekta proaktivnog delovanja, znacajne mere [1].

U delu „Kontrolisanje pristupa mreži“ navodi se da treba kontrolisati pristup internim i eksternim mrežnim uslugama (servisima).

Delovi „Politika koriscenja mrežnih usluga (servisa)“ i „Ogranicenje pristupa informacijama“ upozoravaju da korisnicima treba obezbediti direktan pristup samo onim uslugama za koje imaju odobrenje za koriscenje. To kontrolisanje je posebno važno kod mrežnog povezivanja sa osetljivim ili kriticnim poslovnim aplikacijama ili sa korisnicima na mestima velikog rizika, npr. javnim ili spoljnim podrucjima koja su izvan kontrole i upravljanja sigurnošcu u organizaciji.

Deo „Politika u pogledu elektronske pošte“ reguliše da organizacije treba da projektuju jasnu politiku u pogledu elektronske pošte (zaštitu od sadržaja pridodatih elektronskoj pošti, uputstva kada ne treba koristiti elektronsku poštu i sl.).

Deo „Nadgledanje pristupa i koriscenja sistema“ ukazuje na to da sisteme treba nadgledati, kako bi se otkrila odstupanja od politike kontrole pristupa i zapisali uocljivi dogadaji, da bi se obezbedili dokazi za slucajeve incidenata u pogledu sigurnosti.

Deo „Kriptografske kontrole“ realizuje se s ciljem da se zaštiti poverljivost, verodostojnost ili celovitost informacija. Kriptografske sisteme i postupke treba primenjivati radi zaštite podataka za koje se smatra da su u opasnosti i kojima druge kontrole ne pružaju dovoljnu zaštitu.

Deo „Samozaštita zapisa u organizaciji“ ukazuje na to da važne zapise u nekoj organizaciji treba zaštititi od gubljenja, uništenja i falsifikovanja. Vremenski period i sadržaj podataka koji se cuvaju mogu biti predvideni regulativom. Zapise treba razvrstati u kategorije tipova zapisa, npr. zapise u bazama podataka, zapisnike o transakcijama, zapise o proverama i operativnim procedurama, svaki sa detaljima o periodu cuvanja i tipu medijuma na kojima se oni cuvaju. Sistem za skladištenje podataka treba odabrati tako da se potrebni podaci mogu pretraživati na nacin koji je zakonski i sudski prihvatljiv, npr. da se svi potrebni zapisi mogu izvuci u prihvatljivom roku i formatu. Sistemi za skladištenje i rad sa podacima treba da osiguraju jasnu identifikaciju zapisa i njihov statutarni ili regulativni period cuvanja. Sistem mora do-

zvoljavati odgovarajuce uništavanje zapisa po isteku tog perioda ako organizaciji više nisu potrebni.

Da bi se ispunile ove obaveze, unutar organizacije treba preduzeti sledece korake:

– izdati uputstvo o cuvanju, skladištenju, postupanju i odbacivanju zapisa i informacija;

– izraditi nacrt – termin plana za cuvanje, kojim se identifikuju najvažniji tipovi zapisa i period u kojem ih treba sacuvati;

– održavati inventarski popis izvora kljucnih informacija;

– uvesti odgovarajuce kontrole radi zaštite najvažnijih zapisa i informacija od gubljenja, uništenja i falsifikovanja.

U novije vreme posebno znacajan segment zaštite podataka predstavljaju odredena hardverska i softverska rešenja za detekciju i sprecavanje napada. Proizvodaci racunarske opreme sve više isticu mere sigurnosti. Tako je Bil Gejts istakao da ce prioritet u razvoju Microsoft proizvoda ubuduce imati zaštita [7].

Reaktivno delovanje

Kada pored proaktivnog delovanja dode do incidenta, organizacije moraju biti spremne da se suprotstave brzo i efikasno, da bi se minimizirao negativan uticaj i prikupili neophodni podaci koji bi doveli do pocinioca kriminalne radnje.

Ne ulazeci u uzroke incidenta, nakon njega sledecih šest koraka znatno ce pomoci da se upravlja brzo i efikasno [6]:

– zaštita života i bezbednosti ljudi;

– lokalizovanje oštecenja;

– procena oštecenja;

– utvrdivanje uzroka oštecenja;

– oporavak oštecenja, i

– razmatranje reakcije (odgovora) i ažuriranje politike.

Mnoge kompanije, organizacije i vladine agencije imaju implementirane kapacitete za odgovore na incident (incident management), fokusirajuci se, pre svega, na sledece aspekte [5]:

– efikasan odgovor (obuhvata: pripremu, identifikovanje, zadržavanje, eliminisanje, oporavak i pracenje);

– centralizaciju (za izveštavanje, suprostavljanje incidentu i sl.),

– poboljšanje svesti korisnika.

Kada se napad desi, ili sistem bude kompromitovan, veoma je važno prikupiti podatke (dokaze) o tome šta se desilo. U odredenim granicama racunari i ostali mrežni uredaji (npr. sistemi za detekciju upada) sposobni su da zabeleže aktivnosti koje su se dogodile u njihovim granicama ili prošli kroz njih. Ta evidencija je neophodan element procesuiranja odgovornih lica.

Zavisno od procenjenih rizika, nužno je da svaka organizacija sacini „plan upravljanja kontinuitetom poslovanja“. Upravljanje kontinuitetom poslovanja treba da obuhvati kontrole za identifikovanje i smanjivanje rizika, za ogranicavanje posledica incidenata i da osigura da se važne operacije pravovremeno ponovo zapocnu. Postupak upravljanja kontinuitetom poslovanja treba uvesti kako bi se smanjile posledice štetnih dogadaja na prihvatljiv nivo kombinovanjem kontrola za prevenciju i za oporavak. Usled razlicitih promena rizika, loših procena ili drugih faktora, planove za kontinuitet poslovanja treba održavati kroz redovno preispitivanje i ažuriranje, kako bi se osigurala njihova

efikasnost. Kada je sacinjen takav plan, od strategijskog znacaja, neophodno ga je primenjivati u praksi [1].

Zakljucak

Baze podataka veoma su ranjive i izložene ozbiljnim potencijalnim opasnostima. Apsolutna sigurnost podataka nije moguca. U skladu sa potencijalnim opasnostima moguce je jedino upravljati sigurnošcu podataka, a rizike svoditi na minimum.

Upravljanje sigurnošcu podataka otežavaju stalne promene rizika s obzirom na to da se nijedan incident ne može predstaviti kao tipican. To je konstantan proces koji zahteva saradnju svakog dela i clana organizacije.

Sve je veci broj organizacija u kojima, pored vodeceg službenika bezbednosti (Chief Security Officer – CSO), post?ji, kao zasebna funkcija, vodeci službenik informacione bezbednosti (Chief Information Security Officer – CISO). Vodeci službenik informacione bezbednosti pripada top-menadžmentu organizacije i bavi se razradom i realizacijom politike bezbednosti. Pored vodeceg službenika informacione bezbednosti, sve je cešca i funkcija menadžera službe IB (Business Information Security Officer – BISO), koji se bavi praktic nom realizacijom politike bezbednosti na nivou neke organizacione celine (npr. plansko-ekonomskog, marketinga ili odeljenja IT).

Upravljanje sigurnošcu podataka prerasta u zasebnu delatnost sa široko razgranatom lepezom profesija i sa sve vecim brojem ljudi koji ce profesionalno raditi na tim pitanjima.

Literatura:

[1] ISO/IEC 17799 Information technology – Code of practice for information security management, 2005.
[2] ISO 27001 – Information Security Management System (ISMS) requirements, http://www.iso27001/security.com/html/iso27001.html
[3] ISO 27002, http://www.iso27001/security.com/html/iso27002.html
[4] Kukrika, M.: Upravljanje sigurnošcu informacija, INFOhome Press, Beograd, 2002.
[5] Schweitzer, D.: Incident Response: Computer Forensics Toolkit, Wiley Publishing, Indianapolis, 2003.
[6] Security Risk Management Guide, Microsoft Corporation, 2004 (ažurirana marta 2006), http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/
[7] Shinder, D.: Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, Inc., Rockland (USA), 2002.
[8] Swanson, M.; Guttman, B.: Generally Accepted Principles and Practices for Securing Information Technology Systems, National Institute of Standards and Technology, Gaithersburg, 1996.