MEHARI 2010
Pregled

Mart 2010.godine

Radna grupa za metodologiju

Molimo da vaše komentare i pitanja ostavite na forumu:
http://mehari.info/

UDRUŽENJE ZA INFORMACIONU BEZBJEDNOST FRANCUSKE
CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS
11 Rue De Mogador, 75009 PARIS
Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e-mail: clusif@clusif.fr
Web: http://www.clusif.fr

ZAHVALNOST

CLUSIF se specijalno zahvaljuje gospodinu Žan Filipu Žoasu (Jean-Philippe Jouas) za njegov izuzetan doprinos, gospodinu Aleksandru Bratiću za ovaj prevod i gospodinu Zoranu Jasaku za korekciju prevoda, kao i članovima Komisije za metodologiju koji su učestvovali u realizaciji ovog dokumenta:

Žan Filip	Žoa	Odgovoran za provođenje metode
Jean-Philippe	Jouas	Odgovoran za radne principe grupe, mehanizme i bazu znanja za MEHARI
Žan Lui	Rul	Odgovoran za radnu grupu MEHARI dokumentacija
Jean-Louis	Roule	
Dominik	Bu	BUC S.A.
Dominique	Buc	
Olivije	Korbi	Docapost
Olivier	Corbier	
martin	Ganje	hydroQuébec
martine	Gagné	
mois	Hazan	ministarstvo usluga Vlade Kvebeka (ministère des Services
moïse	Hazzan	Gouvernementaux du Québec)
Žerar	moline	molines Consultants
Gérard	molines	
Šantal	Pino	AGRm
Chantale	Pineault	
Luk	Polan	CRIm
Luc	Poulin	
Pjer	Sasvil	ministarstvo usluga Vlade Kvebeka (ministère des Services
Pierre	Sasseville	Gouvernementaux du Québec)
Klod	Talon	ministarstvo obrazovanja, rekreacije i sporta Kvebeka (ministère
Claude	Taillon	de l'Éducation, du Loisir et du Sport du Québec)
mark	Tubul	BULL SA
marc	Touboul	

Sadržaj

1. UVOD

MEHARI metodologija je napravljena i neprekidno se aktuelizira da bi služila kao pomoć šefovima službi informacione sigurnosti (Chief Information Security Officer – CISO) za obavljanje svakodnevnih zadataka i upravljanje segmentom informacione sigurnosti. Ovaj pregled je namijenjen šefovima službi informacione sigurnosti (CISO), a takođe i revizorima, rukovodiocima informacionih sistema (CIO) ili risk menadžerima koji dijele uglavnom iste ili slične probleme ili izazove.

Cilj ovog dokumenta je da opiše kako se MEHARI koristi. Detaljniji opisi metodologije i odgovarajućih alata nalaze se u drugim dokumentima dostupnim iz CLUSIF-a:

- MEHARI: Koncept i funkcionalne specifikacije,
- MEHARI vodič:
  - analiza uloga i klasifikacija,
  - procjena servisa sigurnosti i
  - analiza rizika,
- MEHARI Referentni priručnik službe sigurnosti,
- MEHARI baza znanja.

Glavni cilj MEHARI-JA je da osiguri procjenu rizika i metod upravljanja u domenu zaštite informacija, u skladu sa zahtjevima ISO/IEC 27005:2008 standarda i da osigura skup alata i elemenata neophodnih za sprovođenje standarda[1].

Dodatni ciljevi su:

- Obezbjeđivanje direktne i individualne analize rizičnih situacija opisanih u scenarijima,
- Obezbjeđivanje kompletnog seta alata koji je specifično dizajniran za upravljanje sigurnošću na kratak, srednji i dugi rok, i koji je prilagodljiv različitim akcijama i terminima završetka.

Svakako, MEHARI obezbjeđuje konzistentnu metodologiju sa odgovorajućom bazom znanja kako bi bio od pomoći šefovima službi informacione sigurnosti, generalnim menadžerima, menadžerima sigurnosti ili ljudima koji su zaduženi za upravljanje rizicima u njihovim svakodnevnim zadacima i aktivnostima.

Povezanost MEHARI-ja sa ISO/IEC 27000 opisana je na kraju dokumenta.

[1] Alati i prateća sredstva, koje obezbjeđuje MEHARI opisani su i nabrojani u dokumentu MEHARI *Koncept i funkcionalna specifikacija*

2. UPOTREBA MEHARI-JA

MEHARI je iznad svega metod za procjenu i upravljanje rizikom.

U praksi, ovo znači da su MEHARI i baza znanja koja stoji iza njega dizajnirani za preciznu analizu rizika i rizičnih situacija opisanih kroz scenarija.

U svakodnevnim aktivnostima, upravljanje segmentom informacione sigurnosti je aktivnost koja se mijenja i evoluira tokom vremena. Korektivne akcije su različite u zavisnosti da li je organizacija uradila nešto u domenu informacione sigurnosti ili su postojale značajne investicije u vidu vremena i truda.

U uspostavljanju informacione sigurnosti preporučuje se da se napravi presjek stanja postojećih sigurnosnih mjera, politika i organizacije i uporedi se sa preporučenom praksom, kako bi se jasno definisala neusaglašenost na kojoj će se raditi.

Nakon ovakve procjene i odluke o uvođenju informacione donose se odluke o konkretnim akcijama. Ovakve odluke koje se obično grupišu u planove, korporativna pravila, politike ili radni okvir za informacionu sigurnost, trebale bi biti donešene na osnovu strukturiranog pristupa. Ovaj pristup može biti baziran na analizi rizika kako se zahtijeva u ISO/IEC 27001 kao dio ISMS (ISMS : Information Security management System). Ostala sredstva, kao što su testiranje performansi informacione sigurnosti bilo interno, profesionalno ili ukoliko to radi eksterni konsultant.

U ovoj fazi bez specifične analize rizika, mora biti riješeno pitanje uloga u informacionoj sigurnosti. Veoma često, kada je odluka o ulogama donijeta, osoba koja donosi konačnu odluku za određivanje budžeta neće biti u nedoumici “da li je ovo zaista potrebno?”. Zbog nepostojanja preliminarne procjene i odluke o ulogama uključenih u infomacionu sigurnost, mnogi projekti vezani za informacnionu sigurnost su odloženi ili zatvoreni.

Često kasnije, ali ponekad u samom početku uvođenja informacnione sigurnosti, dovodi se u pitanje stvarni rizik koji je identifikovan u kompaniji. Ovo je često formulisano u pitanjima sličnim sljedećim: “Da li su svi rizici kojima kompanija može biti izložena identifikovani i da li postoji garancija da su nivoi identifikovanog rizika prihvatljivi?”

Ovakva pitanja mogu se pojaviti na korporativnom nivou ili u vezi sa određenim projektom. Potrebna je metodologija rada koja uključuje i analizu rizika.

MEHARI se zasniva na principu da alati i informacije koji se zahtijevaju u svakoj fazi razvoja informacione sigurnosti moraju biti konzistentni. Treba razumjeti da rezultati dobijeni u pojedinoj fazi mogu biti ponovno korišteni od strane drugih alata ili u okviru drugog procesa u kompaniji.

Različiti alati i moduli MEHARI metodologije dizajnirani su da prate direktne i individualne analize rizika, mogu biti korišteni odvojeno jedni od drugih u bilo kojoj fazi razvoja informacione sigurnosti, koristeći različite pristupe upravljanja i mogu garantovati konzistentnost rezultata i odluka.

Svi ovi alati i moduli, kratko opisani u nastavku, čine konzistentnu metodu procjene rizika sa pratećim alatima, modulima za analizu uloga i nadgledanje kvaliteta sigurnosnih mjera itd.

2.1. Analiza ili procjena rizika

Analiza rizika je izraz koji se spominje u skoro svakoj publikaciji koja se bavi domenom informacione sigurnosti, kao inicijalna metoda za sigurnosne zahtjeve i standarde propisane od strane ISO/IEC. Međutim, u većini slučajeva desi se greška da se ne dogovori podrazumijevana metoda rada.

Već više od 15 godina MEHARI obezbjeđuje strukturirani pristup za procjenu rizika[2], baziran na nekoliko jednostavnih principa.

Rizična situacija može biti opisana pomoću više faktora:

- Strukturni (organizacioni) faktori, koji ne zavise od sigurnosnih mjera, ali zavise od bazičnih aktivnosti organizacije, okruženja i sadržaja.
- Faktori ublažavanja rizika koji su u direktnoj zavisnosti od sigurnosnih mjera.

U stvari, analiza uloga u procesu informacione sigurnosti je neophodna kako bi se odredio maksimalni uticaj posljedica rizične situacije. Ovo je tipično strukturni faktor dok će procjena sigurnosti biti korištena za ocjenu ublažavanja rizika.

MEHARI uključuje kvalitativnu i kvantitativnu procjenu ovih faktora, i pomaže pri procjeni nivoa rizika. Kao rezultat toga, MEHARI integriše alate (kao što su kriteriji za procjenu, formule itd.) i bazu znanja (posebno za određivanje sigurnosnih mjera) koji su osnovne komponente za minimalni okvir propisan sa ISO/IEC 27005.

2.1.1 Sistematična analiza rizičnih situacija

Da bi se pravilno odgovorilo na pitanje "koji su rizici u okviru organizacije i da li je nivo rizika prihvatljiv ili ne" potreban je strukturirani pristup kako bi se identifikovale sve potencijalne rizične situacije kao i individualna analiza najkritičnijih situacija i nakon toga identifikacija akcija kako bi se redukovao rizik.

Pristup koji obezbjeđuje MEHARI baziran je na osnovi znanja koja se odnosi na rizične situacije i automatizovane procedure za evaluaciju faktora koji odlikuju svaki rizik koji daje mogućnost određivanja njihovog nivoa. Dodatno, metoda pomaže pri selekciji odgovorajućeg plana ublažavanja rizika.

Za ocjenu rizika postoje dvije opcije:

- Korištenje skupa funkcija baze znanja (za Microsoft Excell ili Open Office) pruža mogućnost integracije MEHARI modula (klasifikacija sredstava iz analize uloga, analize informacione sigurnosti). Ove funkcije daju mogućnost procjene aktuelnog nivoa i mjere za smanjenje rizika
- Softverska aplikacija (kao što je RISICARE[3]) koja ima raznovrsniji korisnički interfejs i koja omogućuje simulacije i dalju optimizaciju.

[2] Detaljan opis modela rizika se nalazi u dokumentu *MEHARI Fundamentalni principi i funkcionalne specifikacije.*

[3] Od proizvođača softvera BUC S.A.

2.1.2 Spontana analiza rizičnih situacija

Isti set alata može biti korišten u svakom momentu u različitim pristupima upravljanja informacionom sigurnošću.

U nekim slučajevima upravljanja informacionom sigurnošću, gdje upravljanje rizicima nije glavni cilj i gdje se informacionom sigurnošću upravlja kroz reviziju ili referentnim okvirom za sigurnost, postojaće specifični slučajevi u kojima pravila ne mogu biti primijenjena. Spontana analiza rizika može biti korištena kako bi se donela odluka o daljoj metodologiji rada.

2.1.3 Analiza rizika u novim projektima

Modeli i mehanizmi analize rizika mogu biti korišteni u upravljanju projektima, kako bi se ocijenio nivo rizika i donela odluku koje mjere će biti korištene u ublažavanju rizika.

2.2. Procjene informacione sigurnosti

MEHARI kroz dijagnostički upitnik o kontrolama sigurnosti omogućuje ocjenu nivoa kvaliteta mehanizama i rješenja koja su implementirana kako bi se redukovao rizik[4].

2.2.1 Pregled ranjivosti, element analize rizika

MEHARI omogućava struktuirani model rizika koji uzima u obzir i "faktore smanjenja rizika" u cilju unapređenja sigurnosti servisa.

Rezultat ocjene ranjivosti će biti važan izvor informacija za analizu rizika kako bi se postiglo da sigurnosni servisi ispunjavaju njihovu ulogu – suštinska stvar za kredibilitet i pouzdanost analize rizika.

Suštinska prednost MEHARI-ja je mogućnost da ocijeni trenutni nivo rizika kao i nivo rizika u budućnosti koji je baziran na ekspertskoj bazi znanja, ocjenjujući kvalitet mjera sigurnosti, bez obzira da li su one operativne ili su donijete odluke o implementaciji.

2.2.2 Plan sigurnosti baziran na pregledu ranjivosti

Mogući pristup je da se napravi akcioni plan, direktno kao rezultat ocjenjivanja statusa sigurnosnih servisa.

Proces unapređenja informacione sigurnosti koji je zasnovan na već objašnjenom veoma je jednostavan: potrebno je provesti ocjenjivanje i odlučiti se za unapređenje svih servisa koji su ispod propisanog nivoa sigurnosti.

MEHARI upitnik može biti korišten u ovakvoj vrsti pristupa.

Preliminarne analize biznis uloga, takođe, trebaju biti planirane čime se obezbeđuje veza ka ovom modulu MEHARI-ja. Analiza uloga omogućava određivanje zahtijevanog nivoa kvaliteta za relevantne servise sigurnosti i, shodno tome, mogućnost ignorisanja drugih dijelova procjene.

[4] Sigurnosne mjere i kontrole su grupisane u podservisima, servisima i konačno u sigurnosnim domenima.

2.2.3 Pomoć baze znanja u kreiranju referentnog okvira za informacionu sigurnost

Baza znanja koju koristi MEHARI može biti korištena za direktno kreiranje referentnog okvira za informacionu sigurnost (ili sigurnosne politike) koji će sadržati i opisati set sigurnosnih pravila i instrukcije na koji način se kompanija može držati tih pravila.

Ovaj pristup je često korišten u organizacijama ili kompanijama sa određenim brojem organizacionih jedinica ili lokacija. U ovakvim slučajevima su u pitanju velike multinacionalne kompanije sa velikim brojem lokacija ili članova grupe. Isto tako lako se primenjuje na kompanijama srednje veličine sa velikim brojem filijala i poslovnica. U ovakvim slučajevima teško je efikasno obavljanje procjene rizika.

Izrada okvira za informaciou sigurost

MEHARI upitnici za procjenu informacione sigurnosti su dobra baza za menadžere informacione sigurnosti za odlučivanje šta će biti primenjeno u njihovoj kompaniji.

Upravaljanje izuzecima od pravila

Kreiranje seta pravila, kroz radni okvir za informacionu sigurnost, često nije usaglašen sa izazovima lokalne implementacije tako da mora postojati svijest o odstupanjima i tim razlikama se mora upravljati.

Korištenje baze znanja sa konzistentnim setom alata i analičkom metodologijom omogućava da se pravilno upravlja lokalnom divergencijom. Razlika zbog koje nastaju odstupanja može biti pokrivena specifičnom analizom rizika koja će se odnositi na direktne razloge odstupanja.

2.2.4 Oblasti pokrivene modulom pregleda ranjivosti

Sa aspekta analize rizika, u smisu identifikovanja rizičnih situacija i želje da se pokriju svi neprihvatljivi nivoi rizika, MEHARI nije ograničen samo na domen informacionih tehnologija (IT).

Modul ocjenjivanja pokriva, pored informacionog sistema, sve dijelove organizacije i zaštitu lokacija, u smislu radnog okruženja, zakonskih i regulatornih aspekata.

2.2.5 Pregled: modul ocjenjivanja

Treba imati na umu da modul pregleda ranjivosti omogućava širi aspekt i konzistentnost u ocjenjivanju informacione sigurnosti. Ova osobina može biti korištena u različitim pristupima, detaljnim i preciznim analizama i može biti korištena u svim fazama unapređenja svijesti o informacionoj sigurnosti, kao i samoj organizaciji informacione sigurnosti.

2.3. Analiza uloga

Osnovna uloga sigurnosti je zaštita sredstava kompanije.

Kakva god da je orijentacija strategije informacione sigurnosti, postoji princip oko koga se slažu svi menadžeri – mora postojati ravnoteža između ulaganja u informacionu sigurnost na jednoj strani i važnosti odgovarajućih biznis uloga. To znači da je razumijevanje biznis uloga

osnova i takva analiza uloga u informacionoj sigurnosti zaslužuje visok prioritet i strukturirani metod procjene.

Cilj analize uloga u informacionoj sigurnosti je da odgovori na dvostruko pitanje:

“Šta se može desiti, i ako se desi koliko će biti ozbiljno?”

Ovo pokazuje da se u oblasti informacione sigurnosti, uloge označavaju kao posljedice događaja koje ometaju željene operacije kompanije ili organizacije.

MEHARI obezbjeđuje modul analize uloga, opisan u MEHARI-JU: Analiza uloga i klasifikacija, koji daje dvije vrste rezultata.

Vrijednosna skala kvarova i zastoja

Identifikacija kvarova ili potencijalnih događaja je proces koji počinje sa aktivnostima kompanije i podrazumijeva identifikaciju mogućih kvarova i zastoja u operativnim procesima. Rezultati su :

- Opis mogućeg kvara
- Definicija parametara koji utiču na nivo ozbiljnosti svakog kvara
- Procjenu kritičnih vrijednosti parametara koji mijenjaju nivo ozbiljnosti kvara

Ovaj set rezultata čini vrijedosnu skalu kvarova i zastoja.

Klasifkacija informacija i sredstava

Obično se u informacionoj sigurnosti govori o klasifikaciji infomacija i klasifikaciji sredstava.

Ovakva klasifikacija se sastoji u definisanju, za svaki tip informacije i svaki tip sredstava i za svaki kriterij klasifikacije (dostupnost, integritet i tajnost mada se mogu koristiti drugi kriteriji kao što je sledljivost / neporecivost), reprezentativnih pokazatelja ozbiljnosti uticaja gubitka informacija ili sredstva.

Klasifikacija informacija i sredstava za informacione sisteme je vrijednosna skala kvarova i zastoja koja je definisana ranije u pokazatelje osjetljivosti povezane sa sredstvima informacionih tehnologija (IT).

Izražavanje uloga informacione sigurnosti

Vrijednosna skala kvarova i zastoja, klasifikacija informacija i sredstava su dva različita načina opisivanja uloge informacione sigurnosti.

Prva je mnogo detaljnija i daje više informacija za šefove službi informacione sigurnosti CISO (CISO), druga je uopštenija i korisnija za kampanje podizanja svijesti o informacionoj sigurnosti i komunikaciju.

2.3.1 Analiza uloga, baza za analizu rizika

Jasno je da je ovaj modul ključni faktor u analizi rizika. Bez usaglašavanja o posljedicama potencijalnih kvarova ne može se pravilno ocijeniti nivo rizika.

MEHARI je striktan metod za ocjenu uloga i klasifikovanje sredstava koji daje objektivne i racionalne rezultate.

2.3.2 Analiza uloga u informacionoj sigurnosti: Temelj strateškog planiranja akcionih planova

Analiza uloga je potrebna za uvođenje bilo koje forme planova informacione sigurnosti.

Koji god pristup da se koristi, u jednom momentu sredstva će morati da se dodjeljuju kako bi se akcioni planovi implementirali i neizbježno će se pojaviti pitanje investicija.

Sredstva i fondovi koji će biti dodijeljeni informacionoj sigurnosti su, kao i polise osiguranja, u direktnoj srazmjeri sa rizikom. Ukoliko ne postoji dogovor o potencijalnim problemima i kvarovima, veoma je vjerovatno da budžet za informacionu sigurnost neće biti dodijeljen.

2.3.3 Klasifikacija: osnovni element za informacionu sigurnost

Reference radnog modela, politike informacione sigurnosti i odgovarajući pristup upravljanju informacionm sigurnošću su već pomenuti u ovom dokumentu.

U praksi kompanije koje upravljaju sigurnošću na osnovu skupa pravila u obavezi su da istaknu u svojim pravilima i procedurama akcije koje se obavljaju u funkciji povjerljivosti informacija koje se u tim akcijama obrađuju. Najčešće se to radi kroz klasifikaciju informacija i popis IT sredstava. MEHARI-jev modul analiza uloga u informacionoj sigurnosti obezbjeđuje navedenu klasifikaciju i sistematizaciju.

2.3.4 Analiza uloga u informacionoj sigurnosti: baza planiranja informacione sigurnosti

Sam proces analize uloga inforamacione sigurnosti zahtijeva doprinos operativnih menadžera, vrlo često dolazi do potrebe za hitnu akciju. Iskustvo pokazuje da, kada se radi intervju sa top menadžmentom, bez obzira na veličinu preduzeća, i kada oni objasne njihov stav i mišljenje o ozbiljnim zastojima, dolazi do saznanja da postoje problemi koji ranije nisu identifikovani i čije rješavanje zahteva hitne akcije.

Akcioni planovi mogu biti odmah napravljeni, koristeći direktan pristup koji se bazira na dva seta ekspertize: sprovedeno od osoblja koje se bavi poslovnim procesom koji izvršavaju operativni menadžeri i analiza sigurnosnih rješenja, izvršena od strane eksperata za informacionu sigurnost.

2.4. Generalni pregled korištenja MEHARI-JA

Jasno je da je glavna orijentacija MEHARI-ja analiza i ublažavanje rizika. Njegova baza znanja, mehanizmi i alati kreirani su za tu svrhu.

Takođe, kreatori metodologije su imali na umu potrebu za strukturiranim metodama za analizu i ublažavanje rizika i u zavisnosti od veličine kompanije postoje:

- Stalna metodologija rada – uputstvo za posebne grupe
- Metodologija rada koja se koristi paralelno sa drugim metodama upravljanja

- Metoda rada koja se povremeno koristi kako bi se dopunile redovne prakse

MEHARI obezbjeđuje različite pristupe i alate za analizu rizika kada je to potrebno.

MEHARI metodologija čiju bazu znanja čine uputstva i procedure koje opisuju različite module (uloge, rizike, ranjivosti) postoji kako bi bila od pomoći ljudima koji su uključeni u proces informacione sigurnosti na bilo koji način (CISO, risk menadžeri, revizori, CIO, u njihovim različitim akcijama i zadacima.

3. MEHARI I ISO/IEC 27000 STANDARD

Često postavljano pitanje je: kako MEHARI odgovara internacionalnim standardima posebno ISO/IEC 27000 seriji.

Namjera je da se objasni kako MEHARI odgovara ISO 27001, 27002 i 27005 standardima u smislu kompatibilnosti i ciljeva.

3.1. Odgovarajući ciljevi ISO/IEC (ISO/IEC) 27001, 27002, 27005 i MEHARI

3.1.1 Ciljevi ISO/IEC 27002:2005 standarda

Standard propisuje da organizacija treba identifikovati zahtjeve za informacionu sigurnost kroz tri glavna izvora :

- Analizu rizika,
- Zakonskim, statutarnim, regulatornim ili ugovornim zahtjevima
- Skupom principa, ciljeva i zahtjeva koje važe za informacije koje nastaju da bi podržale operativne zadatke

Koristeći ovo kao bazu, kontrolne tačke mogu biti izabrane i implementirane koristeći listu u sekciji "kodeks prakse za upravljanje informacionom sigurnošću" u standardu ili iz nekog drugog kontrolnog seta tačaka (§4.2).

NB: U okviru 27002: 2005 predviđeno je da standard pruža "uputstva i opšte principe za iniciranje, implementaciju, održavanje i unapređenje upravljanja informacionom sigurnošću" što znači da se ISO standard može posmatrati kao polazna tačka. Međutim ISO/IEC 27001 propisuje da svako odstupanje mora biti opravdano i prihvatljivo kada se dodaju kontrolne tačke (Dodatak A - A.1).

ISO 27002 standard obezbjeđuje skup uputstava koje organizacija može koristiti. Međutim, spisak nije konačan i dodatne mjere mogu biti zahtijevane. Međutim, ne preporučuje se metodologija za stvaranje kompletnog sistema upravljanja informacionom sigurnošću.

Na drugoj strani, svaki dio objašnjenja najbolje prakse sadrži uvod i komentare o namjeri ciljeva, što može biti velika pomoć.

NB: ISO (ISO) standard, takođe, predviđa u svom okviru koji se može koristiti da "pomogne izgradnji povjerenja u inter-organizacione aktivnosti". Ovo nije uključeno slučajno i donosi bitan aspekat koje bi pristalice standarda trebalo promovisati, što je to evaluacija (čak i certifikacija) za perspektive informacione sigurnosti, partnera i dobavljača.

3.1.2 Ciljevi ISO/IEC 27001:2005

Jasan cilj ISO/IEC 27001 je da "osigura model za kreiranje i administraciju korporativnog sistema upravljanja infromacionom sigurnošću **ISMS"** i kako bi ga koristili "interno, treća strana, uljučujući certifikaciona tijela".

Cilj evaluacije i certifikacije stavlja fokus na formalne aspekte (dokumentaciju i registraciju odluka, deklaraciju o primjenjivosti, registar i dr.) i kontrole (analize, revizije itd.).

Jasno je da kod ovog pristupa informacionoj sigurnosti analiza rizika mora biti urađena kako bi se ispitali rizici kojima bi organizacija mogla biti izložena i odabrane odgovarajuće mjere za redukovanje rizika na prihvatljiv nivo (paragraf 4.2.1)

ISO/IEC 27001 propisuje da bi analiza rizika trebala biti urađena ali da nije dio standarda. Takođe, nije ponuđena odgovarajuća metoda ako se ne uzima u obzir PDCA (PDCA-Plan, Do, Check, Act) rekurzivni proces modela kao što je definisano u uspostavi ISMS.

Svakako, preporuka "najbolje prakse" koja može biti korištena u redukovanju nivoa rizika je "usaglašena sa onim iz ISO/IEC 27002:2005", dok dodatna lista kontrola postoji u dodacima.

Prema ISO/IEC 27001 osnova procjene upravljanja informacionom sigurnošću nije toliko stvar znanja ili to da li su odluke koje su donesene odgovoarajuće i prilagođene potrebama kompanije, već da revizor ili certifikovani revizor može procijeniti da li su odluke zaista implementirane.

3.1.3 Ciljevi ISO/IEC 27005:2008

Cilj ovog standarda nije da konstituiše metod za risk menadžment već da odredi minimalni radni okvir i opiše zahtjeve za proces analize rizika, za identifikaciju prijetnji i identifikovanje ranjivosti kako bi se odredio nivo rizika i onda biti u poziciji da se odabere model remedijacije i pratećih planova usmjerenih na evaluaciju i poboljšanje situacije.

Standard propisuje da analiza rizika mora biti odabrana u skladu sa ovim zahtjevima kako bi se izbjeglo korištenje nedosljedne ili pojednostavljene metode, u poređenju sa onim što je bila ideja autora standarda.

3.1.4 Ciljevi MEHARI-JA

MEHARI je konzistentan set alata i metodologije za upravljanje informacionom sigurnošću i odgovarajućih mjera baziran na tačnoj analizi rizika. Fundamentalni principi MEHARI-JA:

- Predstavljanje risk modela rizika (kvalitativni, kvantitativni)
- Razmatranje efikasnosti mjera informacione sigurnosti koje su primijenjene ili planirane
- Mogućnost da procijeni preostali nivo rizika koji ostaju posle primenjenih mjera

Ovi principi su obavezne komponente koji se dopunjuje sa zahtjevima ISO/IEC 27000 standarda i posebno ISO/IEC 27005.

3.1.5 Poređenje ciljeva MEHARI-JA SA ISO/IEC 27001 i 27002 standardima

Ciljevi MEHARI-JA i pomenutih ISO standarda su veoma različiti.

- MEHARI ima za cilj da osigura sredstva i metode koje se mogu koristiti da se izaberu najpogodnije mjere sigurnosti za datu organizaciju i da procijeni preostale rizike kada te mjere postanu operativne. Ovo nije primarni cilj ISO standarda.
- ISO standardi obezbeđuju skup najboljih praksi koje se svakako veoma korisne ali ne i nužno odgovarajuće za pitanja informacione sigurnosti u okviru organizacije; one su korisne da pokriju sve aspekte informacione sigurnosti, planiranje i reviziju, eksternu ili internu.

MEHARI Referentni priručnik službe sigurnosti daje elemente koji mogu biti korišteni za izradu radnog okvira za informacionu sigurnost i može se porediti sa ISO/IEC 27002. Jasno je da MEHARI pokriva širi okvir od ISO standarda i da pokriva osnovne aspekte informacione sigurnosti kako u tako i van informacionih sistema.

3.2. Kompatibilnost između ova dva pristupa

MEHARI pristup je potpuno podudaran sa ISO 27002 zato što, bez obzira što nemaju iste ciljeve, relativno je lako prezentirati rezultate MEHARI analize u pogledu na ISO 27002 indikatore.

MEHARI odgovara potrebama koje su izražene u oba standarda ISO 27001 i 27002 za analizu rizika i definisanje mjera koje se trebaju implementirati.

3.2.1 Kompatibilnost sa ISO/IEC 27002:2005 standardima

Standardne kontrolne tačke ili najbolja praksa ISO standarda su najčešće generalne ili organizacione mjere ponašanja dok MEHARI pored njih naglašava potrebu za mjerama čija će efikasnost biti garantovana.

Uprkos ovim razlikama, MEHARI pregled ranjivosti pruža dodatne tabele za prikazivanje indikatora usklađenosti sa krahom koji se koriste u ISO 27002:2005 standardima, takođe, korisne za one koji trebaju pokazati usklađenost sa navedenim standardom. Treba pomenuti da su MEHARI upitnici za reviziju dizajnirani i napravljeni tako da omoguće operativnim menadžerima efektivni pregled ranjivosti i utvrde kapacitete svakog servisa sigurnosti kako bi umanjili rizik.

3.2.2 Kompatibilnost sa ISO/IEC 27001 standardom

MEHARI može lako biti integrisan u PDCA (PDCA: Plan – Do – Check – Act) proces, kako je propisano u ISO/IEC 27001, posebno faza ‘PLAN’ (§4.2.1). MEHARI kompletno pokriva opis zadataka koji omogućavaju stvaranje ISMS baze.

Za DO fazu (§4.2.2), koja ima za cilj da implementira i upravlja ISMS, MEHARI pruža korisne početne elemente kao što su izrada planova za upravljanje rizicima uz davanje prioriteta direktno povezanim za klasifikaciju rizika i uspješnost mjera u toku njihovog korištenja.

Za CHECK fazu (§4.2.3) MEHARI predviđa elemente koje omogućavaju procjenu preostalog rizika i poboljšanja u mjerama sigurnosti. Pored toga, sve promjene u okruženju (uloge, prijetnje, rešenja i organizacija) mogu se lako ponovo ocijeniti ciljanim revizijama koje koriste incijalne MEHARI revizije, tako da planovi sigurnosti mogu biti revidirani i razvijeni tokom vremena.

Za ACT fazu (§4.2.4) MEHARI implicitno poziva na kontrole i kontinuirano unapređenje informacione sigurnosti; time obezbjeđuje da su ispunjeni ciljevi sigurnosti. U ove tri faze, kada MEHARI nije u fokusu, bitno doprinosi njihovom izvršenju i obezbeđuje njihovu efikasnost.

3.2.3 Kompatibilnost sa ISO/IEC 27005:2008 standardima

Radni okvir uspostavljen od strane ovog novog standarda je potpuno primenjiv na način na koji MEHARI omogućava upravljanje rizicima, na primjer:

- Proces analize rizika, ocjene, i tretman rizika (uzet iz ISO 13335)
- Identifikacija primarnih sredstava i klasifikacija nivoa vezanih za njih, nakon analize uloga
- Identifikacija prijetnji, uključujući njihov nivo (prirodne izloženosti), za koji MEHARI ima precizniji opis scenarija rizika.
- Identifikacija i kvantifikacija efikasnosti sigurnosnih mjera (ili kontrola) u redukciji ranjivosti
- Kombinacija ovih elemenata za procjenu nivoa rizika na skali sa 4 nivoa
- Sposobnost da se direktno izabere mjera sigurnosti potrebna za smanjenje rizika

Odatle MEHARI nije lako integrisati u ISMS proces, koji je promovisan od strane ISO 27001 ali je potpuno u skladu sa ISO 27005 zahtjevima za metodu upravljanja rizicima.

L'ESPRIT DE L'ÉCHANGE

UDRUŽENJE ZA INFORMACIONU SIGURNOST FRANCUSKE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 Rue de mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

Download CLUSIF productions at:

www.clusif.fr