МЕХАРИ 2010

Преглед

Март 2010.године

Радна група за методологију

Молимо да ваше коментаре и питања оставите на форуму:
http://mehari.info/

УДРУЖЕЊЕ ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ ФРАНЦУСКЕ

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

ЗАХВАЛНОСТ

ЦЛУСИВ (CLUSIF) се специјално захваљује господину Жан Филипу Жоасу (Jean-Philippe Jouas) за његов изузетан допринос, господину Александру Братићу (за све сугестије око овог превода можете послати директно на имејл acobratic@yahoo.com) за овај превод и господину Зорану Јасаку (jasak_z@bih.net.ba) за корекцију превода, као и члановима Комисије за методологију који су учествовали у реализацији овог документа:

Жан Филип Jean-Philippe	Жоа Jouas	Одговоран за провођење Методе Одговоран за радне принципе групе, механизме и базу знања за МЕХАРИ
Жан Луи Jean-Louis	Рул Roule	Одговоран за радну групу МЕХАРИ документација
Доминик Dominique	Бу Buc	BUC S.A.
Оливије Olivier	Корби Corbier	Docapost
Мартин Martine	Гање Gagné	HydroQuébec
Моис Moïse	Хазан Hazzan	Министарство услуга Владе Квебека (Ministère des Services Gouvernementaux du Québec)
Жерар Gérard	Молине Molines	Molines Consultants
Шантал Chantale	Пино Pineault	AGRM
Лук Luc	Полан Poulin	CRIM
Пјер Pierre	Сасвил Sasseville	Министарство услуга Владе Квебека (Ministère des Services Gouvernementaux du Québec)
Клод Claude	Талон Taillon	Министарство образовања, рекреације и спорта Квебека (Ministère de l'Éducation, du Loisir et du Sport du Québec)
Марк Marc	Тубул Touboul	BULL SA

Садржај

1. **Увод**

МЕХАРИ методологија је направљена и непрекидно се актуелизује да би служила као помоћ шефовима службе информационе безбедности (Chief Information Security Officers - CISO) при обављању свакодневних задатака и при управљању информационом безбедношћу. Овај преглед је намењен шефовима служби информационе сигурности (CISO), али такође и ревизорима, руководиоцима информационих система (CIO), или риск менаџерима који деле углавном исте или сличне проблеме или изазове.

Циљ овог документа је да опише како се МЕХАРИ користи. Детаљнији описи методологије и одговарајућих алата налазе се у другим документима доступним из Клузива (CLUSIF-а.):

- МЕХАРИ: Концепт и функционалне спецификације,
- МЕХАРИ водич:
    - анализа улога и класификација,
    - процена сервиса сигурности и
    - анализа ризика,
- МЕХАРИ Референтни приручник службе сигурности,
- МЕХАРИ база знања.

Главни циљ МЕХАРИ-ЈА је да обезбеди процену ризика и метод управљања у домену безбедности информација, у складу са захтевима ИСО/ИЕЦ (ISO/IEC) 27005:2008 стандарда, као и да обезбеди скуп алата и елемената неопходних за спровођење стандарда[1].

Додатни циљеви су:

- Обезбеђивање директне и индивидуалне анализе ризичних ситуација описаних у сценаријима,
- Обезбеђивање комплетног сета алата који је специфично дизајниран за управљање безбедношћу на кратак, средњи и дуги рок, и који је прилагодљив различитим акцијама и терминима завршетка.

Свакако, МЕХАРИ обезбеђује конзистентну методологију са одговорајућом базом знања како би био од помоћи шефовима служби информационе безбедности, генералним менаџерима, менаџерима сигурности или људима који су задужени за управљање ризицима у њиховим свакодневним задацима и активностима.

Повезаност МЕХАРИ-ја са ИСО/ИЕЦ (ISO/IEC) 27000 описана је на крају документа.

[1] Алати и пратећа средства, које обезбеђује МЕХАР-и описани су и набројани у документу *МЕХАРИ: концепт и функционална спецификација*

2. УПОТРЕБА МЕХАРИ-ЈА

МЕХАРИ је изнад свега метод за процену и управљање ризиком.

У пракси, ово значи да су МЕХАРИ и база знања која стоји иза њега дизајнирани за прецизну анализу ризика и ризичних ситуација описаних кроз сценарија.

У свакодневним активностима, управљање информационом безбедношћу је активност која се мења и еволуира током времена. Корективне акције су различите у зависности да ли је организација урадила нешто у домену информационе безбедности или да ли су постојале значајне инвестиције у виду времена и труда.
У успостављању информационе безбедности препоручује се да се направи пресек стања постојећих безбедносних мера, политика и организације и упореди се са препорученом праксом, како би се јасно дефинисала неусаглашеност на којој ће се радити.

Након овакве процене и одлуке о увођењу информационе безбедности доносе се одлуке о конкретним акцијама. Овакве одлуке које се обично групишу у планове, корпоративна правила, политике или радни оквир за информациону безбедност требале би бити донешене на основу структурираног приступа. Овај приступ може бити базиран на анализи ризика како се захтева у ИСО/ИЕЦ (ISO/IEC) 27001 као део ИСМС (ISMS (Information Security Management System)). Остала стредства као што су тестирање перформанси информационе безбедности, било интерно, професионално или уколико то ради екстерни консултант.

У овој фази без спеифичне анализе ризика, питање улога у информационој безбедности мора бити решено. Веома често, када је одлука о улогама донета, особа која доноси коначну одлуку за одређивање буџета неће бити у недоумици "да ли је ово заиста потребно?". Због непостојања прелиминарне процене и одлуке о улогама укључених у инфомациону безбедност, многи пројекти везани за информацниону безбедност су одложени или затворени.

Често касније, али понекад у самом почетку увођења информацнионе безбедности, доводи се у питање стварни ризик који је идентификован у компанији. Ово је често формулисано у питањима сличним следећим: "Да ли су сви ризици којима компанија може бити изложена идентификовани и да ли постоји гаранција да су нивои идентификованог ризика прихватљиви?"

Оваква питања могу се појавити на корпоративном нивоу или у вези са одређеним пројектом. Потребна је методологија рада која укључује и анализу ризика.

МЕХАРИ се заснива на принципу да алати и информације који се захтевају у свакој фази развоја информационе безбедности морају бити конзистентни. Треба разумети да резултати добијени у појединој фази могу бити поновно коришћени од стране других алата или у оквиру другог процеса у компанији.

Различити алати и модули МЕХАРИ методологије дизајнирани су да прате директне и индивидуалне анализе ризика, могу бити коришћени одвојено једни од других у било којој фази развоја информационе безбедности, користећи различите приступе управљања и могу гарантовати конзистентност резултата и одлука.

Сви ови алати и модули – кратко описани у наставку – сачињавају конзистентну методу процене ризика са пратећим алатима, модулима за анализу улога и надгледање квалитета сигурносних мера итд.

2.1. Анализа или процена ризика

Анализа ризика је израз који се спомиње у скоро свакој публикацији која се бави информационом сигурношћу, као иницијална метода за сигурносне захтеве и стандарде прописане од стране ИСО/ИЕЦ (ISO/IEC). Међутим у већини случајева деси се грешка да се не договори подразумевана метода рада.

Већ више од 15 година, МЕХАРИ обезбеђује структурирани приступ за процену ризика[2], базиран на неколико једноставних принципа.

Ризична ситуација може бити описана помоћу више фактора:

- Структурни (организациони) фактори, који не зависе од сигурносних мера, али зависе од базичних активности организације, окружења и садржаја.
- Фактори ублажавања ризика који су у директној зависности од сигурносних мера.

У ствари, анализа улога у процесу информационе безбедности је неопходна како би се одредио максимални утицај последица ризичне ситуације. Ово је типично структурни фактор, док ће процена безбедности бити коришћена за оцену ублажавања ризика.

МЕХАРИ укључује квалитативну и квантитативну процену ових фактора, и помаже при процени нивоа ризика. Као резултат тога, МЕХАРИ интегрише алате (као што су критеријуми за процену, формуле итд.) и базу знања (посебно за одређивање сигурносних мера) који су основне компоненте за минимални оквир прописан са ИСО/ИЕЦ (ISO/IEC) 27005

2.1.1 Систематична анализа ризичних ситуација

Да би се правилно одговорило на питање "који су ризици у оквиру организације и да ли је ниво ризика прихватљив или не" потребан је структурирани приступ како би се идентификовале све потенцијалне ризичне ситуације, као и индивидуална анализа најкритичнијих ситуација, и након тога идентификација акција како би се редуковао ризик.

Приступ који обезбеђује МЕХАРИ базиран је на основи знања која се односи на ризичне ситуације и аутоматизоване процедуре за евалуацију фактора који одликују сваки ризик који даје могућност одређивања њиховог нивоа. Додатно, метода помаже при селекцији одговорајућег плана ублажавања ризика.

За оцену ризика постоје две опције:

- Коришћење скупа функција базе знања (за Микрософт Ексел (Microsoft Excell)

[2] Детаљан опис модела ризика се налази у документу *МЕХАРИ Фундаментални принципи и функционалне спецификације.*

или Опен офис (Open Office)) пружа могућност интеграције МЕХАРИ модула (класификација средстава из анализе улога, анализе информационе безбедности). Ове функције дају могућност процене актуелног нивоа и мере за смањење ризика

- Или софтверска апликација (као што је РИЗИКЕР (RISICARE[3])) која има разноврснији кориснички интерфејс и која омогућује симулације и даљу оптимизацију.

[3] Од произвођача софтвера БУК С.А.(BUC S.A.)

2.1.2 Спонтана анализа ризичних ситуација

Исти сет алата може бити коришћен у сваком моменту у различитим приступима управљања информационом сигурношћу.

У неким случајевима управљања информационом безбедношћу где управљање ризицима није главни циљ и где се информационом безбедношћу управља кроз ревизију или референтним оквиром за безбедност, постојаће специфични случајеви у којима правила не могу бити примењена. Спонтана анализа ризика може бити коришћена како би се донела одлука о даљој методологији рада.

2.1.3 Анализа ризика у новим пројектима

Модели и механизми анализе ризика могу бити коришћени у управљању пројектима, како би се оценио ниво ризика и донела одлуку које мере ће бити коришћене у ублажавању ризика.

2.2. Процене информационе безбедности

МЕХАРИ кроз дијагностички упитник о контролама сигурности омогућује оцену нивоа квалитета механизама и решења која су имплементирана како би се редуковао ризик[4].

2.2.1 Преглед рањивости, елемент анализе ризика

МЕХАРИ омогућава структуирани модел ризика који узима у обзир и "факторе смањења ризика" у циљу унапређења сигурности сервиса.

Резултат оцене рањивости ће бити важан извор информација за анализи ризика у циљу обезбеђивања да сигурносни сервиси испуњавају њихову улогу – суштинска ствар за кредибилитет и поузданост анализе ризика.

Суштинска предност МЕХАРИ-ја је могућност да оцени тренутни ниво ризика, као и ниво ризика у будућности који је базиран на експертској бази знања, оцењујући квалитет мера безбедности, без обзира да ли су оперативне или су донете одлуке о имплементацији.

2.2.2 План безбедности базиран на прегледу рањивости

Могући приступ је да се направи акциони план, директно као резултат оцењивања статуса сигурносних сервиса.

Процес унапређења информационе безбедности који је заснован на горе објашњеном веома је једноставан: потребно је спровести оцењивање и одлучити се за унапређење свих сервиса који су испод прописаног нивоа сигурности.

МЕХАРИ упитник може бити коришћен у оваквој врсти приступа.

[4] Сигурносне мере и контроле су груписане у подсервисима,сервисима и коначно у сигурносним доменима.

Прелиминарне анализе бизнис улога, такође, треба да буду планиране чиме се обезбеђује веза ка овом модулу МЕХАРИ-ја. Анализа улога омогућава одређивање захтеваног нивоа квалитета за релевантне сервисе безбедности, и сходно томе, могућност игнорисања других делова процене.

2.2.3 Помоћ базе знања у креирању референтног оквира за информациону безбедност

База знања коју користи МЕХАРИ може бити коришћена за директно креирање референтног оквира за информациону безбедност (или сигурносне политике) који ће садржати и описати сет сигурносних правила и инструкције на који начин компанија може да се држи тих правила.

Овај приступ је често коришћен у организацијама или компанијама са одређеним бројем организационих јединица или локација. У оваквим случајевима су у питању велике мултинационалне компаније са великим бројем локација или чланова групе. Али се исто тако лако примењује на компанијама средње величине са великим бројем филијала и пословница. У оваквим случајевима тешко је ефикасно обављање процене ризика.

Израда оквира за информациоу безбедост

МЕХАРИ упитници за процену информационе сигурности су добра база за менаџере информационе сигурности за одлучивање шта ће бити примењено у њиховој компанији.

Управљање изузецима од правила

Креирање сета правила, кроз радни оквир за информациону безбедност често није усаглашен са изазовима локалне имплементације, тако да мора постојати свест о одступањима и тим разликама се мора управљати.

Коришћење базе знања са конзистентним сетом алата и аналичком методологијом омогућава да се правилно управља локалном дивергенцијом. Разлика због које настају одступања може бити покривена специфичном анализом ризика која ће се односити на директне разлоге одступања.

2.2.4 Области покривене модулом прегледа рањивости

Са аспекта анализе ризика, у смису идентификовања ризичних ситуација и жеље да се покрију сви неприхватљиви нивои ризика, МЕХАРИ није ограничен само на домен информационих технологија (ИТ).

Модул оцењивања покрива, поред информационог система, све делове организације и заштиту локација, у смислу радног окружења, законских и регулаторских аспеката.

2.2.5 Преглед: Модул оцењивања

Треба имати на уму да модул прегледа рањивости омогућава шири аспект и конзистентност у оцењивању информационе безбедности. Ова особина може бити коришћена у различитим приступима, детаљним и прецизним анализама и може бити коришћена у свим фазама унапређења свести о информационој сигурности, као и самој организацији информационе сигурности.

2.3. Анализа улога

Основна улога безбедности је заштита средстава компаније.

Каква год да је оријентација стратегије информационе безбедности, постоји принцип око кога се слажу сви менаџери - мора постојати равнотежа између улагања у информациону безбедност на једној страни и важности одговарајућих бизнис улога. То значи да је разумевање бизнис улога основа и таква анализа улога у информационој безбедности заслужује висок приоритет и структурирани метод процене.

Циљ анализе улога у информационој безбедности је да одговори на двоструко питање:

“Шта се може десити, и ако се деси колико ће бити озбиљно?”

Ово показује да се у области информационе безбедности, улоге означавају као последице догађаја које ометају жељене операције компаније или организације.

МЕХАРИ обезбеђује модул анализе улога, описан у МЕХАРИ-ЈУ: Анализа улога и класификација, који даје две врсте резултата:

Вредносна скала кварова и застоја

Идентификација кварова или потенцијалних догађаја је процес који почиње са активностима компаније и подразумева идентификацију могућих кварова и застоја у оперативним процесима. Резултати су :

- Опис могућег квара
- Дефиниција параметара који утичу на ниво озбиљности сваког квара
- Процену критичних вредности параметара који мењају ниво озбиљности квара

Овај сет резултата чини вредосну скалу кварова и застоја.

Класифкација информација и средстава

Обично се у информационој безбедности говори о класификацији инфомација и класификацији средстава.

Оваква класификација се састоји у дефинисању, за сваки тип информације и сваки тип средстава и за сваки критеријум класификације (доступност, интегритет и тајност, мада се могу користити други критеријуми као што је следљивост / непорецивост), репрезентативних показатеља озбиљности утицаја губитка информација или средства.

Класификација информација и средстава за информационе системе је вредносна скала кварова и застоја која је дефинисана раније у показатеље осетљивости повезане са средствима информационих технологија (ИТ).

Изражавање улога информационе безбедности

Вредносна скала кварова и застоја, класификација информација и средстава су два различита начина описивања улоге информационе безбедности.

Прва је много детаљнија и даје више информација за шефове служби информационе сигурности ЦИСО (CISO), друга је уопштенија и кориснија за капмање подизања свести о информационој безбедности и комуникацију.

2.3.1 Анализа улога, база за анализу ризика

Јасно је да је овај модул кључни фактор у анализи ризика. Без усаглашавања о последицама потенцијалних кварова не може се правилно оценити ниво ризика.

МЕХАРИ је стриктан метод за оцену улога и класификовање средстава који даје објективне и рационалне резултате.

2.3.2 Анализа улога у информационој безбедности: Темељ стратешког планирања акционих планова

Анализа улога је потребна за увођење било које форме планова информационе безбедности.

Који год приступ да се користи у једном моменту средства ће морати да се додељују како би се акциони планови имплементирали и неизбежно ће се појавити питање инвестиција.

Средства и фондови који ће бити додељени информационој безбедности су, као и полисе осигурања, у директној сразмери са ризиком. Уколико не постоји договор о потенцијалним проблемима и кваровима, веома је вероватно да буџет за информациону безбедност неће бити додељен.

2.3.3 Класификација: основни елемент за информациону сигурност

Референце радног модела, политике информационе безбедности и одговарајући приступ управљању информационм сигурношћу су већ поменути у овом документу.

У пракси компаније које управљају безбедношћу на основу скупа правила у обавези су да истакну у својим правилима и процедурама акције које се обављају у функцији поверљивости информација које се у тим акцијама обрадјују. Најчешће се то ради кроз класификацију информација и попис ај ти (IT) средстава. МЕХАРИ-јев модул анализа улога у информационој безбедности обезбеђује горе наведену класификацију и систематизацију.

2.3.4 Анализа улога у информационој безбедности: база планирања информационе безбедности

Сам процес анализе улога инфорамационе безбедности захтева допринос оперативних менаџера, врло често долази до потребе за хитну акцију. Искуство показује да, када се ради интервју са топ менаџментом, без обзира на величину предузећа, и када они објасне њихов став и мишљење о озбиљним застојима, доводи до сазнања да постоје

проблеми који раније нису идентификовани и чије решавање захтева хитне акције. Акциони планови могу бити одмах направљени, користећи директан приступ који се базира на два сета експертизе: спроведено од особља које се бави пословним процесом који извршавају оперативни менаџери и анализа сигурносних решења, извршена од стране експерата за информациону безбедност.

2.4. Генерални преглед коришћења МЕХАРИ-ја

Јасно је да је главна оријентација МЕХАРИ-ја анализа и ублажавање ризика. Његова база знања, механизми и алати креирани су за ту сврху.

Такође, креатори методологије су имали на уму потребу за структурираним методома за анализу и ублажавање ризика и у зависности од величине компаније постоје:

- Стална методологија рада – упутство за посебне групе
- Методологија рада која се користи паралелно са другим методама управљања
- Метода рада која се повремено користи како би се допуниле редовне праксе

МЕХАРИ обезбеђује различите приступе и алате за анализу ризика када је то потребно.

МЕХАРИ методологија чију базу знања чине упутства и процедуре које описују различите модуле (улоге, ризике, рањивости) постоји како би била од помоћи људима који су укључени у процес информационе безбедности на било који начин (ЦИСО (CISO), риск менаџери, ревизори, ЦИО (CIO)), у њиховим различитим акцијама и задацима.

3. МЕХАРИ И ИСО/ИЕЦ (ISO/IEC)27000 СТАНДАРД

Често постављано питање је: како МЕХАРИ одговара интернационалним стандардима посебно ИСО/ИЕЦ (ISO/IEC) 27000 серији.

Намера је да се објасни како МЕХАРИ одговара ИСО (ISO) 27001, 27002 И 27005 стандардима у смислу компатибилности и циљева.

3.1. Одговарајући циљеви ИСО/ИЕЦ (ISO/IEC) 27001, 27002, 27005 и МЕХАРИ

3.1.1 Циљеви ИСО/ИЕЦ (ISO/IEC) 27002:2005 стандарда

Стандард прописује да организација треба да идентификује захтеве за информациону безбедност кроз три главна извора :

- Анализу ризика,
- Законским, статутарним, регулаторним или уговорним захтевима
- Скупом принципа, циљева и захтева које важе за информације које настају да би подржале оперативне задатке

Користећи ово као базу, контролне тачке могу бити изабране и имплементиране користећи листу у секцији "кодекс праксе за управљање информационом сигурношћу", у стандарду или из неког другог конролног сета тачка (§4.2).

НБ: У оквиру 27002: 2005 предвиђено је да стандард пружа "упутства и опште принципе за иницирање, имплементацију, одржавање и унапређење управљања информационом безбедношћу" што значи да се ИСО (ISO) стандард може посматрати као полазна тачка. Међутим, ИСО/ИЕЦ (ISO/IEC) 27001 прописује да свако одступање мора бити оправдано и прихватљиво када се додају контролне тачке (Додатак А - А.1).

ИСО *(ISO)* 27002 стандард обезбеђује скуп упутстава које организација може користити. Међутим, списак није коначан и додатне мере могу бити захтеване. Међутим, не препоручује се методологија за стварање комплетног система управљања информационом безбедношћу.

На другој страни, сваки део објашњења најбоље праксе садржи увод и коментаре о намери циљева, што може бити велика помоћ.

НБ: ИСО (ISO) стандард, такође, предвиђа у свом оквиру који се може користити да "помогне изградњи поверења у интер-организационе активности". Ово није укључено случајно и доноси битан аспекат које би присталице стандарда требало да промовишу, што је то евалуација (чак и сертификација) за перспективе информационе безбедности, партнера и добављача.

3.1.2 Циљеви ИСО/ИЕЦ 27001:2005

Јасан циљ ИСО/ИЕЦ 27001 је да "обезбеди модел за креирање и администрацију корпоративног система управљања инфромационом безбедношћу **ИСМС(ИСМС)"** и како би га користили "интерно, трећа страна, укључујући сертификациона тела".

Циљ евалуације и сертификације ставља фокус на формалне аспекте (документацију и регистрацију одлука, декларацију о примењивости, регистар и др.) и контроле (анализе, ревизије. итд.).

Јасно је да код овог приступа информационој безбедности анализа ризика мора бити урађена како би се испитали ризици којима би организација могла бити изложена и одабране одговарајуће мере за редуковање ризика на прихватљив ниво (параграф 4.2.1)

ИСО/ИЕЦ (ISO/IEC) 27001 прописује да би анализа ризика требала бити урађена али да није део стандарда, такође, није понуђена одговарајућа метода ако се не узима у обзир ПДЦА (PDCA-Plan, Do, Check, Act) рекурзивни процес модела као што је дефинисано у успостављању ИСМС.

Свакако, препорука "најбоље праксе" која може бити коришћена у редуковању нивоа ризика су "усаглашене са оним из ИСО/ИЕЦ 27002:2005", док додатна листа контрола постоји у додацима.

Према ИСО/ИЕЦ (ISO/IEC) 27001 основа процене управљања информационом безбедношћу није толико ствар знања или то да ли су одлуке које су донесене одговоарајуће и прилагођене потребама компаније, већ да ревизор или сертификовани ревизор може проценити да ли су одлуке заиста имплементиране.

3.1.3 Циљеви ИСО/ИЕЦ (ISO/IEC) 27005:2008

Циљ овог стандарда није да конституише метод за риск менаџмент већ да одреди минимални радни оквир и опише захтеве за процес анализе ризика, за идентификацију претњи и идентификовање рањивости како би се одредио ниво ризика и онда бити у позицији да се одабере модел ремедијације и пратећих планова усмерених на евалуацију и побољшање ситуације.

Стандард прописује да анализа ризика мора бити селектована у складу са овим захтевима како би се избегло коришћење недоследне или поједностављене методе, у поређењу са оним што је била идеја аутора стандарда.

3.1.4 Циљеви МЕХАРИ-ЈА

МЕХАРИ је конзистентан сет алата и методологије за управљање информационом безбедношћу и одговарајућих мера базиран на тачној анализи ризика. Фундаментални принципи МЕХАРИ-ЈА:

- Представљање риск модела модела ризика (квалитативни, квантитативни)
- Разматрање ефикасности мера информационе безбедности које су примењене или планиране
- Могућност да процени преостали ниво ризика који остају после примењених мера

Ови принципи су обавезне компоненте који се допуњује са захтевима ИСО/ИЕЦ (ISO/IEC) 27000 стандарда и посебно ИСО/ИЕЦ (ISO/IEC) 27005.

3.1.5 Поређење циљева МЕХАРИ-ЈА СА ИСО/ИЕЦ (ISO/IEC) 27001 и 27002 стандардима

Циљеви МЕХАРИ-ЈА и поменутих ИСО стандарда су веома различити..

- МЕХАРИ има за циљ да обезбеди средства и методе кое се могу користити да се изаберу најпогоднije мере безбедности за дату организацију и да процени преостале ризике када те мере постану оперативне. Ово није примарни циљ ИСО стандарда.
- ИСО стандарди обезбеђују скуп најбољих пракси које се свакако веома корисне али не и нужно одговарајуће за питања информационе безбедности у оквиру организације, оне су корисне да покрију све аспекте информационе безбедности, планирање и ревизију, екстерну или интерну.

МЕХАРИ Референтни приручник службе сигурности даје елементе који могу бити коришћени за израду радног оквира за информациону безбедност и може се поредити са ИСО/ИЕЦ (ISO/IEC) 27002. Јасно је да МЕХАРИ покрива шири оквир од ИСО стандарда и да покрива основне аспекте информационе безбедности како у, тако и ван информационих система.

3.2. Компатибилност између ова два приступа

МЕХАРИ приступ је потпуно подударан са ИСО 27002 зато што, без обзира што немају исте циљеве, релативно је лако презентовати резултате МЕХАРИ анализе у погледу на ИСО 27002 индикаторе.

МЕХАРИ одговара потребама које су изражене у оба стандарда ИСО 27001 и 27002 за анализу ризика и дефинисање мера које се требају имплементирати.

3.2.1 Компатибилност са ИСО/ИЕЦ (ISO/IEC) 27002:2005 стандардима

Стандардне контролне тачке или најбоља пракса ИСО стандарда су најчешће генералне мере понашања или организационе, док МЕХАРИ поред њих наглашава потребу за мерама чија ће ефикасност бити гарантована.

Упркос овим разликама, МЕХАРИ-јев преглед рањивости пружа додатне табеле за приказивање индикатора усклађености са крахом који се користе у ИСО 27002:2005 стандардима, такође, корисне за оне који треба да покажу усклађеност са наведеним стандардом. Треба поменути да су МЕХАРИ упитници за ревизију дизајнирани и направљени тако да омогуће оперативним менаџерима ефективни преглед рањивости и утврде капацитете сваког сервиса сигурности како би умањили ризик.

3.2.2 Компатибилност са ИСО/ИЕЦ (ISO/IEC) 27001 стандардом

МЕХАРИ може лако бити интегрисан у ПДЦА (PDCA: Plan – Do – Check – Act) процес као што је прописано у ИСО/ИЕЦ 27001, посебно фаза 'ПЛАН' (§4.2.1). МЕХАРИ комплетно покрива опис задатака који омогућавају стварање ИСМС базе.

За 'ДУ' (DO) (фазу (§4.2.2), која има за циљ да имплементира и управља ИСМС, МЕХАРИ пружа корисне почетне елементе као што су израда планова за управљање ризицима уз давање приоритета директно повезаним за класификацију ризика и успешност мера у току њиховог коришћења.

За 'ЧЕК' (CHECK) фазу (§4.2.3), МЕХАРИ предвиђа елементе које омогућавају процену преосталог ризика и побољшања у мерама сигурности. Поред тога све промене у окружењу (улоге, претње, решења и организација) могу се лако поново оценити циљаним ревизијама које користе инцијалне МЕХАРИ ревизије, тако да планови сигурности могу бити ревидирани и развијени током времена.

За 'АКТ' (ACT) фазу (§4.2.4), МЕХАРИ имплицитно позива на контроле и континуирано унапређење информационе сигурности; тиме обезбеђује да су испуњени циљеви безбедности. У ове три фазе, када МЕХАРИ није у фокусу, битно доприноси њиховом извршењу и обезбеђује њихову ефикасност.

3.2.3 Компатибилност са ИСО/ИЕЦ (ISO/IEC) 27005:2008 стандардима

Радни оквир успостављен од стране овог новог стандарда је потпуно примењив на начин на који МЕХАРИ омогућава управљање ризицима, на пример:

- Процес анализе ризика, оцене, и третман ризика (узет из ИСО(ISO) 13335)
- Идентификација примарних средстава и класификација нивоа везаних за њих, након анализе улога
- Идентификација претњи, укључујући њихов ниво (природне изложености), за који МЕХАРИ има прецизнији опис сценарија ризика.
- Идентификација и квантификација ефикасности сигурносних мера (или контрола) у редукцији рањивости
- Комбинација ових елемената за процену нивоа ризика на скали са 4 нивоа
- Способност да директно изаберете мере безбедности потребне за смањење ризика

Одатле МЕХАРИ није лако интегрисати у ИСМС процес, који је промовисан од стране ИСО (ISO) 27001 али је потпуно у складу са ИСО 27005 захтевима за методу управљања ризицима.

L'ESPRIT DE L'ÉCHANGE

УДРУЖЕЊЕ ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ ФРАНЦУСКЕ

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