MEHARI 2010

Przegląd

Styczeń 2010

Metody grup roboczych

Pytania i komentarze proszę umieszczać na stronie:
http://mehari.info/

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.asso.fr
Web: http://www.clusif.asso.fr

PODZIĘKOWANIA

CLUSIF pragnie podziękować w szczególności Jean-Philippe'owi Jouas za nieoceniony wkład, Jean-Louis'owi Roule za tłumaczenie oraz członkom Metody Grup Roboczych, którzy przyczynili się do powstania tego dokumentu:

CLUSIF pragnie podziękować również Panu Imed'owi El Fray, Zespół Ochrony Informacji, Wydział Informatyki, Zachodniopomorski Uniwersytet Technologiczny - ZUT www.wi.zut.edu.pl, który realizował to tłumaczenie.

Jean-Philippe	Jouas	Przewodniczący Metody Grup Roboczych Odpowiedzialny za koordynowanie zasad prac Metody Grup Roboczych, tworzenie mechanizmów i baz wiedzy MEHARI
Jean-Louis	Roule	Odpowiedzialny za dokumentację pracy Metdy Grup Roboczych MEHARI
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministerstwo Usług Rządowych Québec'u
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministerstwo Usług Rządowych Québec'u
Claude	Taillon	Ministerstwo Edukacji, Sportu i Rekreacji Québec'u
Marc	Touboul	BULL SA

ZAWARTOŚĆ DOKUMENTU

WPROWADZENIE

Metodologia MEHARI została zaprojektowana i jest na bieżąco rozwijana, aby wspierać przedsięwzięte zadania przez Głównych Administratorów Bezpieczeństwa Informacji (GABI) w zarządzaniu i nadzorowaniu bezpieczeństwem informacji. Owe wprowadzenie jest skierowane głównie do nich, lecz również do Audytorów, Administratorów Bezpieczeństwa Informacji (ABI) oraz zarządzających ryzykiem i do wszystkich, których łączy duża grupa podobnych wyzwań.
Głównym celem dokumentu jest opisanie, w jaki sposób MEHARI może zostać wykorzystana. Bardziej szczegółowe opisy metodologii oraz związane z nią narzędzia udostępnione są w odrębnych dokumentach Clusif, a w szczególności:

- MEHARI: Koncepcje i specyfikacje funkcjonalne,
- MEHARI przewodnik: do
    - identyfikacji i klasyfikacji zasobów,
    - oceny usług bezpieczeństwa, i
    - analizy ryzyka,
- MEHARI Instrukcja obsługi dla usług bezpieczeństwa,
- Baza wiedzy MEHARI.

Głównym celem MEHARI jest udostępnienie metody analizy ryzyka i zarządzania nim, głównie w dziedzinie ochrony informacji – zgodnie z wymaganiami normy ISO/IEC 27005:2008 – udostępniwszy niezbędne ku temu narzędzia[1].

Dodatkowe cele:

Umożliwić bezpośrednią, indywidualną ocenę ryzyk, opisanych za pomocą scenariuszy.

Dostarczyć kompletny zestaw narzędzi zaprojektowanych specjalnie do krótko-, średnio- i długoterminowego zarządzania bezpieczeństwem, niezależnie od stopnia dojrzałości organizacji i dający się dostosować do różnych typów przedsięwziętych przez nią działań.

MEHARI dostarcza spójnej z bazą wiedzy metodologii, by wspomóc prace Głównych Administratorów Bezpieczeństwa Informacji (GABI), Administratorów Bezpieczeństwa Informacji (ABI), Audytorów oraz innych borykających się z problemem redukcji ryzyka.

Zestawienie zgodności MEHARI ze standardami ISO/IEC 27000 zostało opisane w końcowej części niniejszego dokumentu.

[1] Narzędzia i powiązane z nimi środki, dostarczane przez MEHARI jako dodatek na zgodności z normą, zostały opisane w dokumencie MEHARI: *koncepcje i specyfikacje funkcjonalne*

WYKORZYSTANIE MEHARI

MEHARI przed wszystkim jest wiodącą metodą analizy i oceny ryzyka.

W praktyce wyraża się to faktem, że MEHARI wraz z bazą wiedzy zostały zaprojektowane do dokładnej analizy ryzyka na podstawie opisanych scenariuszy.

Zarządzanie bezpieczeństwem jest procesem, który ewoluuje z biegiem czasu. Działania korygujące zależą od działań, które organizacja podejmuje (bądź nie) w tej dziedzinie.
Czyniąc pierwszy krok w dziedzinie bezpieczeństwa, niezbędnym jest dokładne określenie stanu bezpieczeństwa panującego w organizacji, a następne porównanie go do „*wzorca dobrych praktyk w dziedzinie bezpieczeństwa*" , aby znaleźć luki, które należy wyeliminować.

Następstwem wykonanej oceny i podjęcia decyzji o wdrożeniu w organizacji wymagań bezpieczeństwa, jest poczynienie konkretnych decyzji odnośnie podejmowanych działań. Takie decyzje, które zwykle grupowane są w plany, procedury, polityki, czy pewien schemat bezpieczeństwa, do którego organizacja będzie się odnosić, powinny zostać utworzone według określonego podejścia. Powinno ono być oparte o analizę ryzyka, zgodnie z wymogami ISO/IEC 27001 w części ISMS (System Zarządzania Bezpieczeństwem Informacji). Istnieją również inne rozwiązania oparte na „*wzorcu*" (lub standardzie) bez względu na to czy wzorzec jest wewnętrzny, wykorzystujący wiedzę i doświadczenie profesjonalistów czy ekspertów z zakresu bezpieczeństwa IT.

Na tym etapie, nie mówiąc o analizie ryzyka, należy postawić pytanie, jakie zasoby należy chronić. Często zdarza się, że mimo iż zostały podjęte już odpowiednie decyzje, osoba odpowiedzialna za asygnowanie budżetu zadaje pytanie, "czy rzeczywiście jest to niezbędne?". Z powodu braku wstępnej analizy stanu[2] bezpieczeństwa organizacji i ogólnego konsensusu, wiele projektów związanych z bezpieczeństwem systemów jest porzucanych lub ulega znacznym opóźnieniom.

Często się zdarza, że później poddawane są w wątpliwość środki przedsięwzięte przeciw danemu ryzyku, które dotyczą daną organizacji, co często wyrażane jest zapytaniem: "Czy na pewno zostały rozpoznane wszystkie ryzyka i czy jest pewność, że poziomy zabezpieczeń są wystarczające?". To pytanie może zostać zadane zarówno na poziomie korporacyjnym, jak i w odniesieniu do konkretnego projektu. Potrzebna jest metodologia, która umożliwi analizę ryzyka.

MEHARI zostało opracowane zgodnie z założeniem, że niezbędne narzędzia na każdym etapie poprawy (rozwoju) bezpieczeństwa, muszą być spójne. Zgodnie z tym, wyniki uzyskane w jednej fazie muszą móc być później ponownie wykorzystane w organizacji.

Zróżnicowane narzędzia i moduły związane z metodologią MEHARI, zaprojektowane, by wspomóc bezpośrednią i indywidualną ocenę ryzyka, mogą być używane osobno w różnych fazach, wykorzystujących różne podejścia zarządzania i gwarantują spójność wszystkich podjętych decyzji.

Wszystkie te narzędzia i moduły – opisane w skrócie poniżej – tworzą spójną metodę oceny ryzyka wraz z narzędziami i modułami służącymi do analizy i diagnostyki aktualnego i przyszłego stanu bezpieczeństwa.

[2] Analiza stanu: identyfikacja i ocena poziomów dysfunkcji, klasyfikacja zasobów, analiza zagrożeń,…

2.1. Analiza (lub ocena) ryzyka

Analiza ryzyka jest cytowana w różnych książkach i artykułach związanych z bezpieczeństwem systemów IT jak również w normach ISO/IEC serii 27000. Pomimo, że niektóre z tych książek czy norm traktowane są jako wzorce (niekiedy wytyczne) wymagań związanych z bezpieczeństwem, to jednak większość z nich nie wspomina lub milczy na temat metod stosowanych lub wspomagających analizę ryzyka.

Od ponad 15 lat, MEHARI dostarcza ustrukturyzowanego podejścia do analizy ryzyka[3], bazując na kilku prostych zasadach.

Biorąc pod uwagę najważniejsze, sytuacja określona jako „ryzykowna" może być charakteryzowana przez następujące czynniki:

- czynniki strukturalne (lub organizacyjne), które nie zależą od przedsięwziętych środków bezpieczeństwa[4], lecz działań wewnątrz organizacji, jej otoczenia i jej działalności,

- czynniki redukujące ryzyko, które są bezpośrednią funkcją implementowanych środków bezpieczeństwa.

W szczególności analiza stanu bezpieczeństwa jest konieczna, aby wyznaczyć maksymalne konsekwencje powstałe w wyniku zajścia danego zdarzenia (sytuacji). Jest to typowy czynnik strukturalny, podczas gdy diagnostyka ryzyka będzie wykorzystana do oceny czynników redukujących ryzyko.

MEHARI umożliwia jakościową i ilościową ocenę tych czynników, i w rezultacie uczestniczy w ocenie poziomów (wag) ryzyka. Tym samym, MEHARI integruje narzędzia (takie jak kryteria, formuły obliczeniowe, itp.) i bazy wiedzy (głównie do diagnostyki stanu bezpieczeństwa), które są niezbędnymi dodatkami minimalnej ramy wyznaczonej przez ISO/IEC 27005.

2.1.1 Systematyczna analiza ryzyka

Aby odpowiedzieć na pytanie „jakie ryzyka dotyczą organizacji i czy są one akceptowalne?", potrzebne jest ustrukturyzowane podejście umożliwiające identyfikację wszystkich potencjalnych ryzyk, przeanalizowanie najbardziej krytycznych z nich i następnie podejmowanie działań, prowadzących do zminimalizowania ryzyka do akceptowalnego poziomu.

MEHARI umożliwia realizację wyżej opisanego podejścia, a bazy wiedzy są rozwijane tak aby odpowiedzieć na te wymagania. W użyciu MEHARI akcent położony jest na zapewnienie, że każde z krytycznych ryzyk jest brane pod uwagę i jest pokryte przez odpowiedni plan działania.

Podejście MEHARI oparte jest na wiedzy na temat ryzyka, mechanizmów (zautomatyzowanych procedur, itp.) oceny czynników charakteryzujących każde z ryzyk oraz ocenę jego poziomu (nadanie mu wagi). Dodatkowo, metoda ta dostarcza wsparcia w wyborze odpowiednich planów poddawania działaniu tych ryzyk.

Żeby ocenić ryzyko, proponuje się dwie opcje:

- Wykorzystać zbiór funkcji z bazy wiedzy (w Microsoft Excel lub Open Office) umożliwiających integrację wyników z modułów MEHARI. Przy użyciu tych funkcji możliwe jest dalsze ocenę obecnego stanu ryzyk i zaproponowanie dodatkowych

[3] Szczegółowy opis modelu ryzyka dostępny w *MEHARI :* Koncepcje i specyfikacje funkcjonalne.
[4] Środków bezpieczeństwa: środki zaradcze redukujące wpływ podatności systemu IT

środków, celem ich ograniczenia.

- Albo aplikację (jak np. RISICARE[5]), która udostępnia bogatszy interfejs i umożliwia symulacje, wizualizacje oraz dalszą optymalizację ryzyka.

2.1.2 Wyrywkowa analiza ryzyka

Te same narzędzia mogą zostać wykorzystane w dowolnym momencie w innych podejściach związanych z zarządzaniem bezpieczeństwem.

W niektórych podejściach związanych z zarządzaniem bezpieczeństwem, gdzie zarządzanie ryzykiem nie jest głównym celem, i gdzie bezpieczeństwo jest zarządzane przez audyty, często zdarzają się przypadki, że nie można zastosować pewnych reguł. Wyrywkowa analiza ryzyka może zostać wykorzystana, aby zadecydować o najlepszym rozwiązaniu dla danej sytuacji.

2.1.3 Analiza ryzyka w nowych projektach

Modele i mechanizmy analizy ryzyka MEHARI mogą być zastosowane w zarządzaniu projektami, aby analizować ryzyka i podejmować odpowiednie działania im przeciwdziałające.

2.2. Ocena bezpieczeństwa

MEHARI integruje kwestionariusze dotyczące bezpieczeństwa, pozwalając na ocenę jakości mechanizmów i rozwiązań wykorzystanych do redukcji ryzyka[6].

2.2.1 Przegląd podatności, jako elementu analizy ryzyka

MEHARI udostępnia ustrukturyzowany model ryzyk, który bierze pod uwagę czynniki redukcji ryzyka, w postaci usług bezpieczeństwa.

Wynik analizy podatności będzie istotnym punktem wejściowym do analizy ryzyka zapewniając, że usługi bezpieczeństwa rzeczywiście spełniają swoją rolę, co jest niezbędne dla wiarygodności oraz rzetelności analizy ryzyka.

Podstawową siłą MEHARI jako metody analizy i oceny ryzyka jest możliwość oceny obecnego poziomu ryzyka, jak również jego przyszłego poziomu, na podstawie eksperckiej bazy oceniającej jakość środków bezpieczeństwa, zarówno powziętych, jak i planowanych.

2.2.2 Plany zabezpieczeń bazujące na przeglądzie podatności

Jednym z możliwych podejść jest tworzenie planów działań bezpośrednio na podstawie oceny stanu bezpieczeństwa.

Proces zarządzania bezpieczeństwem wykonywany według tego podejścia jest zdecydowanie prostszy: przeprowadzamy ocenę stanu bezpieczeństwa, a następnie decydujemy się na poprawę wszystkich usług bezpieczeństwa, które nie są na zadowalającym poziomie jakości.

Kwestionariusze MEHARI do oceny (diagnostyki) stanu bezpieczeństwa mogą zostać wykorzystane przy tym podejściu.

Użycie wstępnej analizy stanu bezpieczeństwa jest gorąco zalecane w połączeniu z innym modułem Mehari, przedstawionym w dalszej części niniejszego dokumentu. Analiza stanu

[5] BUC S.A.

[6] Kontrola bezpieczeństwa, lub środki, są zgrupowane w pod usługach, potem w usługach i na końcu w domenach bezpieczeństwa.

bezpieczeństwa pozwala natomiast określić wymagania jakości usług bezpieczeństwa, w tym wybór tylko tych właściwych usług, które podlegają audytowi podczas oceny.

2.2.3 Wsparcie bazy wiedzy w tworzeniu polityki bezpieczeństwa (struktura odniesienia do bezpieczeństwa)

Moduł oceny ryzyka oparty jest na bazie wiedzy, w której zawarte są usługi bezpieczeństwa (zwane dalej Instrukcją Obsługi dla Usług Bezpieczeństwa). Baza określa dla każdej z usług efekt końcowy (co wykonuje), do czego jest potrzebna (co zwalcza), mechanizmy i rozwiązania wspomagające usługi oraz elementy, które należy brać pod uwagę podczas oceny jakości tych usług.

Unikatowa baza wiedzy MEHARI może zostać użyta bezpośrednio do budowy pewnych wzorców (polityki) bezpieczeństwa, które będą zawierać i opisywać zbiór zasad i instrukcji zawiązanych z bezpieczeństwem, i które organizacja powinna respektować.

To podejście jest często używane w organizacjach i korporacjach posiadających wiele niezależnych jednostek organizacyjnych. Jest to głównie przypadek wielkich międzynarodowych korporacji z dużą liczbą oddziałów, lecz również sprawdza się przy średnich i małych przedsiębiorstwach, posiadających lub nie dużą liczbę regionalnych agencji. W takich przypadkach trudne jest zwielokrotnienie oceny czy analizy ryzyka.

Budowa polityki bezpieczeństwa

Kwestionariusze oceny MEHARI z zawartością posiadanych objaśnień są dobrą podstawą dla pracy administratorów, audytorów, itp. bezpieczeństwa informacji, którzy decydują co powinno zostać implementowane w ich organizacji.

Zarządzanie wyjątkami wynikające z reguł

W tworzeniu zbioru reguł przy pomocy polityki bezpieczeństwa, często napotyka się na trudności podczas próby implementacji na płaszczyźnie lokalnej, więc wymagana jest umiejętność zarządzania wyjątkami.

Fakt użycia spójnej bazy wiedzy z narzędziami i metodą analizy ryzyka MEHARI, pokazuje, że można zarządzać lokalnymi trudnościami analizując żądania związane z wyjątkami poprzez analizę ryzyka skupioną na oczywistych trudnościach.

2.2.4 Domeny bezpieczeństwa pokryte przez moduł oceny podatności

Z punktu widzenia analizy ryzyka, w zakresie ustalenia wszystkich przyczyń ryzyka oraz potrzeby przeciwdziałaniu wszystkich nieakceptowanych ryzyk, MEHARI nie jest ograniczona jedynie do systemów informatycznych.

Kwestionariusze oceny ryzyka MEHARI pokrywają ponadto systemy informacyjne i komunikacyjne, zarządzanie organizacją, ochronę fizyczną całej siedziby, jak również środowisko pracy użytkowników i aspekty przepisowe i prawne.

2.2.5 Ogólny przegląd modułu oceny stanu bezpieczeństwa

Ważne jest aby zapamiętać, że moduł oceny podatności MEHARI daje szeroki i spójny obraz na temat bezpieczeństwa. Może to zostać wykorzystane w różnorakich podejściach i analizach – na wszystkich fazach (oraz stopniach ich dojrzałości) związanych z zapewnieniem bezpieczeństwa w organizacji.

2.3 Analiza stanu bezpieczeństwa

Bezpieczeństwo dotyczy ochrony zasobów. Bez względu na orientację czy politykę w dziedzinie bezpieczeństwa, jest jedna podstawowa reguła, z którą zgadzają się wszyscy menadżerowie: zawsze musi być równowaga pomiędzy inwestowanymi środkami w bezpieczeństwo a istotą (wysokością zaistnienia możliwych strat) zagrożenia, itp. bezpieczeństwa.

Znaczy to, że właściwa znajomość stanu bezpieczeństwa organizacji jest nieodzowna, a analiza tego stanu zasługuje na wysoki priorytet i rygorystyczną metodę oceny.

Celem analizy stanu bezpieczeństwa w organizacji jest odpowiedź na podwójne pytanie:

"Co może się stać i jeśli się stanie, jak poważny będzie skutek?"

Pokazuje to, że w dziedzinie bezpieczeństwa, stan bezpieczeństwa postrzegany jest jako konsekwencje zdarzeń, które zakłócają właściwe działanie organizacji.

MEHARI integruje moduł analizy stanu bezpieczeństwa – opisany w „*Przewodniku identyfikacji i klasyfikacji zasobów"* – dostarczający dwóch rodzajów wyników:

- Skalę wartości dysfunkcji,
- Klasyfikację informacji i zasobów systemu IT

Skala wartości dysfunkcji

Identyfikacja możliwych dysfunkcji w procesie operacyjnym lub potencjalnych zdarzeń, których możemy się obawiać jest podejściem, które przeprowadza się na poziomie działalności organizacji. Wynikiem identyfikacji jest:

- Opis wszystkich możliwych dysfunkcji
- Definiowanie parametrów, które mają wpływ na wagę każdej dysfunkcji z osobna.
- Ocena progu krytyczności wartości tych parametrów, które umożliwiają przeniesienie wagi dysfunkcji z jednego poziomu na drugi.

Ten zbiór wartości współtworzy odpowiednią skalę wartości dysfunkcji.

Klasyfikacja informacji i zasobów

W dziedzinie bezpieczeństwa informacji, naturalną rzeczą jest mówić o klasyfikacji informacji oraz klasyfikacji zasobów systemów IT.

Taka klasyfikacja polega na definiowaniu, dla każdego typu informacji, zasobu systemu IT, kryterium klasyfikacji (dostępność, integralność i poufność, choć mogą być stosowane również inne, tj. autentyczność i niezaprzeczalność), jako wskaźników określających wagę naruszenia każdego z nich.

Klasyfikacja informacji i zasobów, dla systemów informacyjnych, jest skalą wartości dysfunkcji, zdefiniowaną wcześniej i przetransponowaną na wskaźniki wrażliwości związane z tymi informacjami i zasobami.

Wyrażanie stanu bezpieczeństwa

Skala wartości dysfunkcji oraz klasyfikacja informacji i zasobów są dwoma odrębnymi sposobami wyrażania stanu bezpieczeństwa.

Pierwszy jest bardziej szczegółowy i dostarcza więcej informacji Głównemu Administratorowi Bezpieczeństwa Informacji (GABI), drugi z kolei jest bardziej globalny i

użyteczny np. w kampanii dotyczącej podniesienia poziomu świadomości, lecz mniej szczegółowy.

2.3.1 Analiza stanu bezpieczeństwa, podstawy analizy ryzyka

Analiza stanu bezpieczeństwa jest kluczowym modułem analizy ryzyka i bez konsensusu odnośnie konsekwencji potencjalnych dysfunkcji, nie jest możliwe ocenienie poziomów ryzyka.

Siła MEHARI z kolei polega na udostępnianiu rygorystycznej metody oceny stanu bezpieczeństwa i klasyfikacji zasobów, która daje obiektywne i racjonalne wyniki.

2.3.2 Analiza stanu bezpieczeństwa: wsparcie dla każdego planu działania

Oczywiste jest, że analiza stanu bezpieczeństwa jest często konieczna w celu wdrożenia każdego planu bezpieczeństwa. W rezultacie, jakiekolwiek zastosowane podejście, w którymś momencie wymaga alokacji pewnych środków na wdrożenie planów działań, co skutkuje nieuchronnie zadaniem pytania o sens takiej inwestycji (poddawanie w wątpliwość sensu wdrożenia te planów).

Znaczy to, że środki finansowe przeznaczone na zabezpieczenia organizacji są takie jak w przypadku polisy ubezpieczeniowej, bezpośrednio będącej w ścisłej zależności od poziomu ryzyka. Jeżeli nie będzie konsensusu odnośnie obaw związanych z potencjalnymi dysfunkcjami, istnieje małe prawdopodobieństwo, że takie środki zostaną przeznaczone na zabezpieczenia.

2.3.3 Klasyfikacja: element zasadniczy polityki zabezpieczeń

Powoływaliśmy się już na nią w dokumencie polityki bezpieczeństwa oraz związane z nim podejście do zarządzania bezpieczeństwem.

W praktyce, organizacje, które zarządzają bezpieczeństwem poprzez zbiór pewnych reguł (zasad), zmuszone są różnicować je w zależności od wrażliwości przetwarzanych informacji. Często odnosi się to do klasyfikacji informacji oraz zasobów IT.

Moduł identyfikacji i klasyfikacji MEHARI umożliwia wykonanie takiej klasyfikacji.

2.3.4 Analiza stanu: podstawa planowania zabezpieczeń

Proces analizy stanu, wymagający współpracy personelu operacyjnego, często prowadzi do potrzeby podjęcia natychmiastowych działań.

Doświadczenie pokazuje, że gdy spotkaliśmy się z personelem operacyjnym na wysokim stanowisku w organizacji (niezależnie rzecz jasna od wielkości organizacji) i chcieliśmy aby wypowiadał się, co według niego jest poważną dysfunkcją, prowadziło to do uświadomienia potrzeb bezpieczeństwa personelu i tym samy przyspieszenia jego reakcji.

Plany działania mogą być bezpośrednio budowane, przy użyciu lekkiego podejścia, bazującego na połączeniu dwóch ekspertyz: tej powiązanej z zawodem osoby odpowiedzialnej za działania operacyjne i tej powiązanej z rozwiązaniami eksperta związanymi z bezpieczeństwem.

2.4 Ogólne podsumowanie na temat użycia metody MEHARI

Jest jasne, że główną orientacją MEHARI jest analiza i redukcja ryzyka, a jego bazy wiedzy, mechanizmy oraz narzędzia wsparcia są specjalnie tworzone w tym celu.

Ponad to, jasne jest że twórcy tej metodologii, chcąc zaspokoić zapotrzebowanie na strukturalizowaną metodę analizy i redukcji ryzyka, zaproponowali, że może ona być według organizacji:

- Metodą ciągłej pracy – jako przewodnik dla specjalistycznych grup,
- Metodą ciągłej pracy używaną równolegle z innymi praktycznymi metodami zarządzania bezpieczeństwem,
- Metodą pracy okazjonalną, będącą jako dodatek do regularnych praktyk (uzupełnieniem dla innych metod zarządzania bezpieczeństwem).

Pamiętając o tym, MEHARI dostarcza zbioru pojęć i narzędzi, które umożliwiają analizę ryzyka wtedy, kiedy jest to potrzebne.

MEHARI jest metodologią opracowaną przez Clusif w postaci plików do pobrania ze strony zawierający bazy wiedzy, podręczniki umożliwiające lepiej zrozumieć rożne moduły zawarte w metodzie (dysfunkcje, zasoby, zagrożenie, podatności, ryzyka, środki zaradcze). Metoda istnieje po to, aby wspomagać pracę specjalistów związanych z zarządzaniem bezpieczeństwem informacji w wypełnieniu ich pracy.

MEHARI I NORMY ISO/IEC SERII 27000

Często zadawane jest pytanie: w jakim stopniu MEHARI odpowiada międzynarodowym normom, a w szczególności normie ISO/IEC serii 27000.

Celem tej części dokumentu jest wyjaśnienie, w jaki sposób MEHARI spełnia normy ISO 27001, 27002 oraz 27005, w zakresie kompatybilności i celów.

3.1. Cele zabezpieczeń ISO/IEC 27001, 27002, 27005 i MEHARI

3.1.1 Cele zawarte w ISO/IEC 27002:2005

Norma ta postuluje, iż organizacje powinny identyfikować wymagania bezpieczeństwa przy użyciu trzech głównych źródeł:

- Analizy ryzyka,
- Prawnych, regulacyjnych, statutowych lub kontraktowych wymagań,
- Zbioru zasad, celów i wymagań stosowanych do przetwarzania informacji niezbędnej do funkcjonowania organizacji.

Używając tego jako podstawy, można wybierać punkty kontrolne i implementować je, zgodnie z listą dostarczoną w sekcji „**Praktyczne zasady zarządzania bezpieczeństwem informacji**", lub rozpocząć z dowolnym zbiorem (zestawem) punktów kontrolnych. (§4.2).

Uwaga: w zakresie wersji 27002:2005, postulowane jest, aby norma zapewniała „wytyczne i ogólne zasady inicjalizacji, implementacji, utrzymywania i ulepszania zarządzania bezpieczeństwem informacji", co oznacza, że norma ISO może być postrzegany jako punkt startowy. Jednakże, ISO/IEC 27001 postuluje (§1.2), że każde odstępstwo musi być uzasadnione oraz że akceptowalne jest dodawanie punktów kontrolnych (Appendix A - A.1).

Norma ISO 27002 dostarcza zbioru wytycznych i zasad, które mogą zostać wykorzystane przez organizacje. Zaznacza jednak, że lista ta nie jest wyczerpująca i dodatkowe środki mogą być konieczne. Jednakże, żadna metodologia nie jest proponowana do analizy i oszacowania kompletnego systemu zarządzania bezpieczeństwem.

Z drugiej strony, każda część przewodnika dobrych praktyk zawiera wstępy i komentarze, zakreślające zamierzone cele, co może okazać się niezwykle przydatne.

Uwaga: norma ISO postuluje w swoim zakresie, że może być wykorzystana do „pomocy w budowaniu zaufania w działalności między organizacjami". Nie zostało to zamieszczone tam przypadkowo gdyż rzuca to światło na bardzo ważny aspekt promowany przez twórców normy. Jest nim ocena (a nawet certyfikacja) partnerów i dostawców, z punktu widzenia bezpieczeństwa informacji.

3.1.2 Cele ISO/IEC 27001:2005

Wyraźnym celem ISO/IEC 27001 jest „dostarczenie modelu umożliwiającego tworzenie i administrację systemem zarządzania bezpieczeństwem informacji w organizacji (SZBI)" oraz aby system ten był „stosowany wewnątrz, bądź przez strony trzecie, w tym centra certyfikacyjne włącznie".

Te wymagania odnośnie oceny i certyfikacji prowadzą do położenie akcentu na formalnych aspektach (dokumentacje, zapis każdej decyzji, deklaracji stosowania, rejestrowania, itd.) i na kontroli (wywiady, audyty, itd.).

Jasnym jest, że istota podejścia do bezpieczeństwa domniemywa, że powinna zostać przeprowadzona analiza wymagań, a następne analiza ryzyka na, które firma lub organizacja może być narażona oraz wybór odpowiednich środki redukujących ryzyko do akceptowalnego poziomu (paragraf 4.2.1).
ISO/IEC 27001 wskazuje, że powinna zostać wykorzystana metoda analizy ryzyka dla realizacji SZBI w ramach rekursywnego modelu PDCA (*Plan* (Planuj), *Do* (Wykonuj), *Check* (Sprawdzaj) i *Act* (Działaj)) lecz żadna konkretna metoda nie jest częścią normy, ani żadna nie jest sugerowana, pominąwszy integrację rekursywnego modelu PDCA.

Dodatkowo, rekomendacje lub „*dobre praktyki"* mogące zostać wykorzystane do redukcji ryzyka są „wymienione w ISO/IEC 27002:2005", dla których lista punktów kontrolnych znajduje się w aneksie.

Zgodnie z ISO/IEC 27001, podstawą **oceny systemu zarządzania bezpieczeństwem** nie jest wiedza, ani weryfikacja, czy podjęte decyzje były odpowiednie i dostosowane do potrzeb organizacji, lecz sprawdzenie, czy po podjęciu decyzji, audytor lub osoba certyfikująca mogą być pewni, że podjęte decyzje rzeczywiście będą stosowane.

3.1.3 Cele ISO/IEC 27005:2008

Celami tej normy nie jest stworzenie pełnej metody zarządzania ryzykiem, lecz ustalenie minimalnych ram oraz narzucenie wymagań zarówno dla procesu, który należy śledzić jak i identyfikacji zagrożeń i podatności umożliwiającej estymację ryzyk i oszacowanie ich poziomu, aby następnie móc wybrać sposób postąpienia z nimi w celu poprawienia sytuacji (plany, środki zapewniające bezpieczeństwo, wskaźniki, itd.).

Norma zaleca, by metoda analizy ryzyka była dobierana zgodnie z jej wytycznymi, tak aby uniknąć korzystania ze zbyt uproszczonych metod lub dalekich od wytycznych norm.

3.1.4 Cele MEHARI

MEHARI jest spójnym zbiorem samowystarczalnych narzędzi i metod do zarządzania i nadzoru nad bezpieczeństwem zorientowanych na precyzyjną analizę ryzyka. Fundamentalny aspekty związany z MEHARI:

- model ryzyka (ilościowy i jakościowy),
- wydajność środków bezpieczeństwa, zarówno obecnych, jak i planowanych, które muszą być brane pod uwagę podczas procesu ich oceny ilościowego,
- możliwość oceny i symulacji efektów implementowanych środków zaradczych na poziomie ryzyka szczątkowego.

są obowiązkowym uzupełnieniem wymogów stawianych przez normy ISO/IEC serii 27000, a w szczególności ISO/IEC 27005.

3.1.5 Porównanie celów MEHARI ze normami ISO/IEC 27002 i ISO/IEC 27001

Wstępne cele MEHARI z jednej strony i wyżej wymienione normy ISO z drugiej strony są radykalnie różne.

- MEHARI udostępnia narzędzia i metody, które mogą zostać wykorzystane przy wyborze najodpowiedniejszych środków bezpieczeństwa zarówno technicznych jak i ekonomicznych dla danej organizacji oraz umożliwia oceny ryzyka szczątkowego, gdy owe środki zostaną już implementowane, co stanowczo nie jest podstawowym celem żadnego ze standardów ISO.
- normy ISO wyżej wymienione, dostarczają zbioru najlepszych praktyk, które są z pewnością użyteczne, lecz niekoniecznie dostosowane do wymogów organizacji. Są one równie użyteczne jako środek opiniotwórczy odnośnie dojrzałości planów związanych z bezpieczeństwem informacji, podmiotów w aspekcie ich autonomii wewnętrznej lub partnerów.

Instrukcja obsługi dla usług bezpieczeństwa MEHARI, która dostarcza szczegółowych elementów mogących być użytymi do budowy struktury bezpieczeństwa, może być porównana ze normą ISO/IEC 27002. Jest jasne jednak, iż dostarczane usługi w Mehari są szersze aniżeli norma ISO i obejmuje istotne aspekty bezpieczeństwa poza systemami informacyjnymi.

3.2. Zgodność pomiędzy podejściami

Podejście MEHARI można całkowicie pogodzić z ISO 27002, ponieważ, mimo iż nie mają zbieżnych celi, łatwo jest przedstawić (jeśli to jest potrzebne) wyniki analiz MEHARI w zgodzie z wyznacznikami organizacji, z celami kontrolnymi zawartymi w ISO 27002.

MEHARI odpowiada potrzebom wyrażonym w obu normach ISO 27001 i 27002, odnośnie analizy ryzyka, by zdefiniować środki zaradcze, które powinny zostać poddane implementacji.

3.2.1 Kompatybilność ze normą ISO/IEC 27002:2005

Standardowe „*Punkty kontrolne*" lub „*najlepsze praktyki"* zawarte w normie ISO są głównie środkami ogólnymi (organizacyjnymi lub behawioralnymi), podczas gdy MEHARI, rozszerzając je, podkreśla potrzebę środków, których efektywność związaną z redukcją podatności można zagwarantować.

Pomimo tych różnic, MEHARI posiada tabele zgodności, które umożliwiają dostarczenie wyników w postaci wskazówki (punkty kontrolne) ujęte w normie ISO 27002:2005, dla tych, którzy mają szczególną potrzebę udowodnić zgodność ich postępowania z normą.

Warto dodać tutaj, że kwestionariusze audytów MEHARI zostały zaprojektowane i utworzone w taki sposób, aby umożliwić audytorom itd. efektywne przeprowadzenie analizy podatności i wydedukowanie zdolności każdej z usług bezpieczeństwa do redukcji ryzyk.

3.2.2 Zgodność ze standardem ISO/IEC 27001

Łatwo jest integrować MEHARI z modelem PDCA (planuj, wykonuj, sprawdzaj i działaj) zdefiniowanym w normie ISO/IEC 27001, a w szczególności:

- Faza „PLAN" (§4.2.1), MEHARI spełnia w całości opis zadań, które umożliwiają utworzenie baz SZBI.

- faza „DO” (§4.2.2), której celem jest implementacja i administracja systemem SZBI, MEHARI dostarcza użytecznych elementów startowych, takich jak: plany budowy zarządzania ryzykiem z priorytetami bezpośrednio uzależnionymi od klasyfikacji ryzyk oraz narzędzi pomiaru postępów podczas ich wykorzystywania.
- faza „CHECK” (§4.2.3), MEHARI dostarcza elementów, które umożliwiają określenie ryzyka szczątkowego w wyniku oceny (audytu) środków bezpieczeństwa oraz wprowadzonych ulepszeń w tychże środkach. Dodatkowo, wszystkie zmiany środowiskowe (dysfunkcje, zagrożenia, rozwiązania itd.) mogą zostać z łatwością ponownie przeszacowane przez ukierunkowane audyty, które korzystają z wyników wstępnych audytów realizowanych przez MEHARI, dzięki czemu plany zabezpieczeń mogą zostać zrewidowane i ewoluowane z czasem.
- faza „ACT”, MEHARI z natury rzeczy nawołuje do prowadzenia kontroli i ciągłych usprawnień zabezpieczeń, zapewniając tym samym, że cele redukcji ryzyka zostaną osiągnięte.

MEHARI, nie będąc w sercu tych procesów, wielce się przyczynia do ich realizacji i zapewnia ich efektywność.

3.2.3 Kompatybilność ze normą ISO/IEC 27005:2008

Struktura ustanowiona przez normę ISO jest w pełni zbieżna ze sposobem, w jaki MEHARI umożliwia zarządzanie ryzykiem, w szczególności dla:

- Procesu analizy, oceny i postępowania z ryzykiem (wzięte z ISO 13335),
- Identyfikacji podstawowych i pomocniczych zasobów i ich poziomu klasyfikacji w wyniku analizy stanu bezpieczeństwa,
- Identyfikacji zagrożeń, uwzględniając ich poziomy (podatność naturalna), dla których MEHARI jest dokładniejsza, zwłaszcza w opisie scenariuszy ryzyka,
- Identyfikacji i kwantyfikacji efektywności istniejących środków bezpieczeństwa (kontrolnych) ukierunkowanych na redukcję powiązanych podatności,
- Kombinacji tych elementów dla określenia (oceny) wagi scenariuszy ryzyk według czterostopniowej skali.
- Selektywny wybór środków bezpieczeństwa podlegających integracji w planach redukcji ryzyka.

Zatem, metoda MEHARI nie tylko łatwo integruje się z ISMS, tak jak jest to opisane w normie ISO 27001, lecz również w pełni spełnia dyktowane wymagania przez ISO 27005 odnośnie metod zarządzania ryzykiem.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Download CLUSIF productions at:
www.clusif.asso.fr