MEHARI 2007

نظرة عامة

MEHARI هي العلامة التجارية المسجلة من قبل CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Semard, 75009 PARIS

رقم الهاتف : 80 08 25 153 33+ رقم الفاكس: 88 08 25 53 1 33+

البريد الإلكتروني: clusif@clusif.asso.fr

موقع الانترنت : http://www.clusif.asso.fr

 © CLUSIF 2007

تعبير عن شكر

تود CLUSIF أن تشكر جان فيليب Jean-Philippe Jouas وجان لوي Jean-Louis Roule، مؤلفي هذه النظرة العامة عن منهج MEHARI لإدارة أمن المعلومات ، اللذان سمحا بنشرها من قبل CLUSIF.
كما تود CLUSIF أن تشكر كلاود اوسمبا Claude Essomba من شركة Getsec Inc. و رشدي أحمد عثمان Roshdi Osman اللذان قاما بترجمة هذه الوثيقة وفقا لنظام مبادئ المصادر المفتوحة

يرجى إرسال أي أسالة أو تعليقات إلى: MEHARI-2007-2@clusif.asso.fr

فهرس المحتويات

1. المقدمة
2. استخدامات MEHARI
2،1. التقييمات الأمنية
2.1.1 تقييم الضعف الأمني هو أحد عناصر تحليل المخاطر
2.1.2 الخطط الأمنية بناء على تقييم الضعف الأمني 6
2.1.3 الدعم المقدم من قواعد المعرفة في خلق إطار مرجع للأمن
2.1.4 المجالات التي يشملها نموذج التقييم
2.1.5 نظرة عامة لنموذج التقييم

2،2. تحليل الأصول والأملاك المعرضة للخطر
2.2.1 تحليل المخاطر ، أساسا لتحليل المخاطر
2.2.2 تحليل المخاطر الأمنية : حجر الزاوية في أي عمل التخطيط الاستراتيجي
2.2.3 التصنيف : عنصر أساسي لسياسة الأمن
2.2.4 تحليل المخاطر الأمنية: أساس التخطيط الأمني

2،3. تحليل المخاطر
2.3.1 تحليل المخاطر : هو معونة للتخطيط الاستراتيجي
2.3.2 تحليل منهجي للحالات التي تنطوي على مخاطر
2.3.3 تحليل غير منهجي أو تلقائي وسريع للحالات التي تنطوي على مخاطر
2.3.4 تحليل المخاطر في المشاريع الجديدة
2،4. لمحة عامة عن استخدامات MEHARI

3. MEHARI والمعايير الدولية

3،1. أهداف المنظمات الدولية للتوحيد القياسي ISO 17799 ، IEC/ISO 27001 وMEHARI
3.1.1 أهداف مقياس IEC/ISO 17790:2005 و 17799:2005 معيار
3.1.2 أهداف مقياس IEC/ISO 27001
3.1.3 أهداف MEHARI
3.1.4 مقارنة بين أهداف MEHARI و ISO 17799 و IEC/ISO 27001
3،2. التوافق بين المقاييس
3.2.1 توافق مقياس MEHARI مع مقياس ISO 17799
3.2.2 توافق مقياس MEHARI مع مقياس ISO 27001

 © CLUSIF 2007

1. المقدمة

صمم MEHARI أصلا لمساعدة رؤساء أمن المعلومات (CISOs) في مهام إدارة أمن نظم المعلومات.

هذه النظرة العامة تستهدف أساسا رؤساء و ضباط أمن المعلومات (CISOs) و أيضا مراجعي الحسابات Auditors و مديري المخاطر Risk Managers اللذان يحظون بنفس القدر من التحديات.
والهدف الرئيسي من هذه الوثيقة هو أن تصف لنا باختصار كيف يمكن أن نستخدم منهجية MEHARI.
كما يمكن الحصول على وصف أكثر تفصيلا لمنهجيه وما يرتبط بها من أدوات في وثائق أخرى متاحة من CLUSIF ، على وجه الخصوص
الوثائق أدناه:

- MEHARI : المفاهيم والآليات ،
- MEHARI : تحليل المخاطر و دليل التصنيف
- MEHARI : دليل التقييم للخدمات الأمنية
- MEHARI : دليل تحليل المخاطر ،
- MEHARI قواعد المعرفة والأدلة المرجعية (خدمات الأمن وسيناريوهات المخاطر).

تهدف MEHARI إلى توفير مجموعة من الأدوات المصممة خصيصا لإدارة أمن المعلومات ، التي تضم مجموعة من الإجراءات الإدارية لكل منها هدف محدد.

وهذه بعض الأمثلة :

- وضع خطط أمنية ، أو خطط استراتيجيه ،
- تنفيذ سياسات الأمن أو القواعد التي سيتم جمعها معا تحت مصطلح " الإطار المرجعي لأمن المعلومات " ،
- تنفيذ عمليات تقييم سريعة أو تفصيلية للحالة الأمنية ،
- تقييم المخاطر وإدارتها
- ضمان إدراج الأمن في إدارة المشاريع الأنمإءية ،
- التوعية الأمنية والدورات التدريبية ،
- إدارة الأمن التنفيذي ومراقبة أو رصد للإجراءات التي ارتكبت.

هذه الأمثلة ، وما شابهها من الإجراءات الإدارية يمكن أن تنفذ سوية في نفس الوقت أو في أوقات متفرقة من قبل فئات محددة و مختلفة أو من قبل مجموعة واحدة ، تبعا لمتطلبات محددة أو دائمة.
وبالمثل ، هذه الإجراءات يمكن أدائها سواء بشكل مستقل أو باعتبارها جزءا من برنامج أوسع و أشمل.
نفس الإجراءات الإدارية يمكن أن تنفذ بطرق مختلفة ، ويتوقف ذلك على عدد من العوامل مذكورة أدناه :

- النضج ، من حيث الأمن ، من قبل المنظمة وموظفيها ،
- مستوى تدخل المدراء و الوحدة الإدارية في اتخاذ القرارات الأمنية•

ثقافة وفهم المؤسسة أما هرمية والتكنوقراطية (وجود قواعد وتطبق) ، أو ، على العكس من ذلك كسلطة غير مركزية.
ونظرا لهذه الاختلافات، فان المطلب الرئيسي لأي منهج أمني هو أن يأتي مرافقا لمجموعة من الأدوات الملائمة لكل حالة، وهذه الأدوات يجب أن تكون متناسقة ومتكاملة بين بعضها البعض
لتسمح للحركة من أداة إلى أخرى دون ازدواجية وتكرارية المهام أو عبء العمل الزائد.
MEHARI توفر منهجيه ثابتة ومنسجمة مصحوبة بقواعد المعرفة و البيانات المناسبة لمساعدة رئيس موظفي الأمن (CISOs) ، والمدراء العامين ومديري

الأمن ، أو غيرها من الأشخاص المناط بهم في مهمة الحد من المخاطر على اختلاف مهامهم وأعمالهم.

تقدم هذه الوثيقة نظرة عامة للكيفية و الحيثية التي يمكن بها أستخدام MEHARI.

في نهاية هذه الوثيقة يوجد وصف موجز للمعايير الدولية ذات العلاقة بهذا الصدد إضافة إلي علاقة MEHARI بهذه المعايير الدولية،

2. استخدامات MEHARI

MEHARI هي قبل كل شيء طريقة لتحليل وإدارة المخاطر.
وفي الممارسة العملية هذا يعني أن MEHARI والمعارف و القواعد المرتبطة بها قد تم تصميمهم للتحليل الدقيق للمخاطر دون فرض تحليل وإدارة المخاطر كمهام ذات أولوية.
و في التعبير و التعريف اليومي وإدارة المخاطر هي وظيفة أو نشاط يتطور مع مرور الوقت.
تختلف القرارات و الإجراءات وفقا لما أنجزته المؤسسة في مجال أمن المعلومات

في اتخاذ الخطوات الأولى في مجال أمن المعلومات لا شك انه من المستحسن إجراء تقييم للحالة الأمنية و السياسات الأمنية القائمة في الوقت الراهن وتقيمها ومقارنتها بأفضل المعايير المتفق عليها عالميا بغرض توضيح الفرق وفهم ما يتبقي أن تفعله المنظمة لتوافق المعايير العالمية.

وبعد عملية تقييم الوضع الأمني للمؤسسة لابد من اتخاذ قرارات صارمة. مثل هذه القرارات عادة التي عادة ما تصنف ضمن مخططات أو قواعد الشركات السياسية والأمنية أو إطار الأمن المرجعي ، ينبغي اتخاذها باستخدام نهج منظم.
وهذا النهج يمكن أن يستند إلى تحليل المخاطر، أو أن يتضمن مفهوم الخطر، رغم أن ذلك ليس إلزاميا. وتوجد وسائل أخرى ، مثل القياس ، سواء تم إجراءه من قبل الشركة نفسها أو من كوادر خارجية محترفة في هذا المجال أو من قبل الاثنين معا.

و صحيح في هذه المرحلة أنه وبدون ذكر عملية تحليل المخاطر ينبغي أن نجد إجابة لكمية وقيمة الأملاك و الأصول المعرضة للخطر.
وفي كثير من الأحيان نجد أن الشخص المسئول عن تخصيص ميزانية الشركة قد اتخذ قرارا مسبقا لذلك عاد يطرح هذا السؤال:"هل هذا ضروري حقا؟".

نظرا لعدم وجود تقييم أولي أو أتفاق عام بشأن قيمة الأملاك و الأصول المعرضة للخطر فان العديد من المشاريع الأمنية يتم التخلي عنها أو يتم تأخيرها.

و في كثير من الأحيان تجد المؤسسة منذ البداية أو حتى في وقت لاحق أن الخطر الحقيقي الذي يواجهها موضع تساؤل.

وهذا الوضع كثيرا ما يصاغ بعبارات مشابهة لهذا: " هل تم تحديد وحصر جميع المخاطر التي يمكن أن تتعرض لها المنظمة؟ وهل تم التأكد من أن هذه المخاطر في مستويات مقبولة؟".
ولذلك يتعين وجود منهجيه تشمل عملية تحليل المخاطر.
MEHARI تأسست على مبدأ ن الأدوات اللازمة في كل مرحلة من مراحل التنمية والأمن يجب أن تكون متناسقة ثابتة.
وبناء على هذا الأساس ينبغي أن يكون مفهوما أن أي نتائج ولدت في مرحلة من المراحل يجب أن تكون قابلة لإعادة الاستخدام من قبل أدوات أخرى في وقت لاحق أو في أماكن أخرى في المنظمة.
الأدوات والنماذج المختلفة من منهجيه MEHARI والتي تم تصميمها لترافق عملية تحليل المخاطر يمكن أن تستخدم بصورة منفصلة عن بعضها البعض في أي

خطوة من خطوات التنمية الأمنية. كما أن استخدام مناهج أدارية مختلفة يضمن اتساق القرارات الناتجة.
كل هذه الأدوات والوحدات – والمذكورة أجازا أدناه - تضم الأدوات اللازمة لتقييم الحالة الأمنية، نموذج للتحليل الأملاك والأصول المعرضة للمخاطر، مع أدوات تدعم هذه المنهجية.

2،1. التقييمات الأمنية

منهجية MEHARI تحتوي علي طريقتين أو نموذجين لتقييم المخاطر :
1- النموذج الأول هو لإجراء تقييم سريع و غير مفصل.
-- النموذج الثاني هو لإجراء تقييم أكثر تفصيلا.
النموذج الأول مازال قيد الإنشاء

وفي كل حالة ،الهدف هو تقييم مستوى الأمن. ومن ناحية عملية فأن هذا التقييم يدل و يحكم على خدمات الأمن. ومن الواضح أن النتائج سوف تعتمد على عمق التقييم.
فإذا كان التقييم سريعا تكون النتائج أقل دقة وأما إذا كان مفصلا تكون النتائج أكثر موثقيه ويمكن الاعتماد عليها.
وفي التقييم السريع أو المفصل فان النواحي الأمنية التي يتم تقييمها هي نفسها بغض النظر عن نوع التقييم.
ولكن في حالة التقييم السريع فان الهدف من الأسئلة هو معرفة ما إذا كانت النواحي الأمنية قد كان قد تم تنفيذها دون التحقق منها أو من وجود نقاط الضعف.
وبهذا المعنى، فان كل جوانب الضعف التي تم تحديدها هي بالتأكيد من نقاط الضعف.
لكن القوة المحتملة قد لا تكون القوة فيها.
التقييم التفصيلي يهدف إلي إيجاد ومعرفة نقاط الضعف في كل ناحية من النواحي الأمنية كل على حدة.
وبذلك فان التقييم التفصيلي يشكل قاعدة الخبرة ، والتي يمكن استخدامها في تحليل المخاطر.
يسمح التوافق بين هذين النموذجين (السريع و التفصيلي) لنا باستخدام النموذج السريع كنقطه بداية وانطلاق، وبعد ذلك استخدام النموذج التفصيلي للتأكد من أي نقطة قد تحتاج إلى تأكيد.
هذان النموذجان يمكن استخدامهما في مجموعة متنوعة من الطرق.

2.1.1 التقييم الأمني من عناصر تحليل المخاطر

توفر MEHARI طريقة متناسقة ومتوافقة لتحليل المخاطر.
وفي الوقت الراهن يكفي أن نعرف أن نموذج المخاطر يأخذ في الاعتبار عوامل الحد من المخاطر.
ولهذا فان النموذج التفصيلي سيكون مدخلا هاما لعملية تحليل المخاطر لضمان أن تفي الأجهزة الأمنية بدورها وهذه تعتبر نقطة جوهريه بالنسبة لمصداقية عملية تحليل المخاطر.

2.1.2 الخطط الأمنية على أساس تقييم الضعف الأمني

أحد الطرق الشائعة والمتبعة بكثرة هي أن تبنى خطط العمل مباشرة نتيجة للتقييم حالة الأمن.

عملية إدارة الأمن التابعة لهذا النهج تعد عملية بسيطة للغاية لأنها تعني أن نقوم بعملية تقييم أمني ثم نقوم بتحسين كل الخدمات التي ليس لديها ما يكفي من مستوى الجودة بناء على نتيجة التقييم.
استخدام تحليل أولي للمخاطر الأمنية ومن المخطط أيضا ل، ومن ثم توفير وصله إلى هذا النموذج من MEHARI (الوارد وصفها في وقت لاحق من هذه الوثيقة).
المراحل المختلفة والنصائح المتعلقة بتنفيذ هذا الشكل من أشكال ألإدارة يرد وصفها في MEHARI -- تقييم دليل للخدمات الأمنية.

2.1.3 الدعم المقدم من قواعد المعرفة في إيجاد إطار مرجعي للأمن

نموذج التقييم المفصل يستفيد من خدمات الأمن و قواعد المعارف (موثق في MEHARI -- الدليل المرجعي لخدمات الأمن).
ويصف هذا لكل خدمة الأتي:

- الغرض منها
- ماتستخدم ضده
- حلول وآليات دعم الخدمة
- تلك العناصر التي ينبغي النظر فيها عند تقييم نوعية الخدمة.

قاعدة المعرفة الفريدة من نوعها يمكن استخدامها مباشرة لإيجاد إطار مرجعي للأمن (أو السياسات الأمنية) التي ستتضمن وتصف مجموعة القواعد والتعليمات الأمنية التي يتعين على المؤسسة أو المنظمة أتباعها.
هذا النهج كثيرا ما يستخدم في المنظمات أو المؤسسات التي لها عدد من الوحدات التنفيذية المستقلة أو المواقع المنفصلة. وهذا هو عادة شأن وحال الشركات الكبيرة المتعددة الجنسيات والتي لها عدد من الشركات الأخرى التابعة لها.
ولكن بنفس السهولة ينطبق هذا النهج على الشركات المتوسطة الحجم ذات عدد كبير من الفروع أو الوكالات الإقليمية.
وفي مثل هذه الحالات من الصعب علينا عمليا القيام بالعديد من التقييمات أو تحليلات المخاطر.

بناء إطار الأمن المرجعي
أسئلة الاستبيان و تقييم الحالة الأمنية وقبل كل شيء الدليل المرجعي للأجهزة والخدمات الأمنية وما يحتويه من توضيحات إضافية
هما من الأساسيات العملية التي
توفر أساسا جيدا لمديري الأمن حيث تمكنهم من تقرير ما ينبغي أن يطبق في المنظمة من نواحي أمنية.

إدارة الاستثناءات من القواعد:
إنشاء مجموعة من القواعد من خلال إطار الأمن المرجعي يأتي في كثير من الأحيان ضد صعوبات في تنفيذ ذلك تجب أدارة التنازلات والاستثناءات من القواعد. استخدام قاعدة معارف متماسكة و متناسقة مع مجموعة من أدوات التحليل المنهجي يمكن من أدارة الاختلافات المحلية.
طلبات الاستثناء يمكن تغطيتها عن طريق عملية تحليل المخاطر المحددة تركز على الصعوبات الناتجة.

2.1.4 المجالات التي يشملها نموذج التقييم الأمني

من وجهة نظر تحليل المخاطر، من حيث تحديد جميع الحالات التي تنطوي على مخاطر والرغبة في تغطية جميع المخاطر غير المقبولة، MEHARI لا يقتصر ببساطة على أنها المجال.

ويغطي التقييم الوحدة ، وبصرف النظر عن نظام المعلومات ، التنظيم العام ، وحماية الموقع في العام ، فضلا عن بيئة العمل والجوانب القانونية والتنظيمية.

2.1.5 نظرة عامة لنموذج التقييم الأمني

الشيء الوحيد الذي لابد أن يؤخذ في الاعتبار عن نموذج التقييم الأمني هو أنه يقدم رؤية واسعة ورأي ثابت عن الأمن.
ولذلك يمكن استخدام نموذج التقييم الأمني في طائفة متنوعة من الطرق في تقييم عمق التحليل الأمني كما يمكن استخدامه في جميع مراحل نضج المؤسسة في التوعية والنظام الأمني.

2،2. تحليل المخاطر

الهدف الأساسي من نظام الأمن هو حماية الأملاك الموجودة.
ومهما كانت توجهات السياسة الأمنية فهناك مبدأ واحد يتفق عليه جميع مديري الأمن وهو انه يجب أن يكون هناك توازن عادل بين الاستثمارات في مجال الأمن من ناحية وأهمية ومقدار المخاطر نفسها من ناحية أخرى.
وهذا يعني أن الفهم الصحيح للمصالح المعرضة للخطر أمر أساسي
ولهذا فان عملية تحليل المخاطر الأمنية تستحق أولوية عالية المستوى وتتطلب وجود طريقة منظمة للتقييم.
والهدف من تحليل المخاطر الأمنية هو الرد على السؤال المزدوج:
"ماذا يمكن أن يحدث، وإذا حدث ذلك، هل سيكون خطيرا؟"
وهذا يدل على انه في مجال الأمن فان المخاطر المترتبة ينظر إليها على أنها من الأحداث التي تعكر المسار المقصود لعمليات المؤسسة أو المنظمة.

MEHARI توفر نموذج لتحليل المخاطر وهذا النموذج قد تم وصفه في MEHARI:
تصنيف وتحليل المخاطر ، التي تنتج نوعين من النتائج:

- معيار لتقييم الخلل الوظيفي
- تصنيف المعلومات و الأصول التقنية

معيار تقييم الخلل الوظيفي
معرفة و تحديد الخلل الوظيفي و
الأعطال المحتملة هي عملية تبدأ مع أنشطه المؤسسة وتتكون من تحديد الخلل الوظيفي في العمليات التنفيذية. وهذه العملية تؤدي إلى الأتي:

- وصف للأنواع الأعطال المحتملة
- وضع تعريف للمعايير التي تؤثر على خطورة كل عطل
- إجراء تقييم للقيمة الحرجة لتلك المعايير و التي تغيير مستوى الجدية للأعطال المحتملة

تصنيف المعلومات والأصول
ومن المعتاد ، انه في نظام الأمن ، التحدث عن تصنيف المعلومات و تصنيف الأصول.
وهذا التصنيف يحدد لكل نوع من أنواع المعلومات و الأصول ولكل معيار من معايير التصنيف (Availability, Integrity and Confidentiality)
مؤشرات تمثل جدية المعيار المتأثر وتحدد احتمالية فقدان المعلومات.

التعبير عن المعلومات والأصول، لنظم المعلومات، هو عطل قيمة النطاق المحدد في وقت سابق من ترجمتها إلى حساسية المؤشرات المرتبطة أنها الأصول.
وإذ تعرب عن المخاطر الأمنية

وقد عطل قيمة النطاق وتصنيف المعلومات والأصول متميزتين السبل للتعبير عن المخاطر الأمنية.
الأول هو أكثر تفصيلا وتوفر المزيد من المعلومات لCISOs. هذا الأخير هو أكثر عالمية وأكثر فائدة لحملات التوعية والاتصال، ولكن اقل دقة.

2.2.1 تحليل ألأصول أساسا لتحليل المخاطر

ومن الواضح أن هذا المبدأ هو أساسي في عملية تحليل المخاطر. فبدون اتفاق مشترك بشان الآثار المترتبة عن الأخطاء المحتملة لا يمكننا إصدار حكم بشأن مستويات المخاطر.

2.2.2 تحليل ألأصول من ناحية أمنية هو حجر الزاوية في أي تخطيط الاستراتيجي و كما ورد في المقدمة فأن تحليل ألأصول في كثير من الأحيان يكون لازما لتنفيذ أي شكل من أشكال الخطة الأمنية.
و على نحو فعال أيا كان النهج الذي يستخدم فعند نقطة ما يتحتم علينا أن نخصص لها الأصول والأموال لتنفيذ خطط العمل. وحتما فان مبرر لمثل هذا الاستثمار سيكون موضع للتساؤل.
الأصول والأموال التي سوف تخصص للأمن حالها كحال تلك التي تخصص للتأمين فكلهما لهما علاقة مباشرة لمقدار و نسبة الخطر.
وإذا لم يكن هناك اتفاق مشترك بشأن الخلل الوظيفي المحتمل فمن المستبعد جدا أن يتم تخصيص الميزانيات والأموال.

2.2.3 التصنيف: عنصر أساسي لسياسة الأمن

الإطار والمرجع الأمني والسياسات الأمنية وما يرتبط بها من نهج في إدارة الأمن تم ذكرها مسبقا في هذه الوثيقة.
في الممارسة العملية فان الشركات التي تدير الأمن من خلال مجموعة من القواعد ملزمة للتمييز بين القواعد نفسها و بين الإجراءات التي يتعين أن تقوم بها بوصفها وظيفة من وظائف حساسية المعلومات التي يتم معالجتها.
ومن المعتاد أن تتم الإشارة إلى تصنيف للمعلومات الأصول التكنولوجية.
نموذج MEHARI لتحليل الأصول والمخاطر يوفر وسيلة لأداء هذا التصنيف.

2.2.4 تحليل المخاطر و الأصول الأمنية هو أساس التخطيط الأمني:

عملية تحليل المخاطر الأمنية والتي من الواضح أنها تتطلب مساهمه الإدارة التنفيذية كثيرا ما تؤدي إلى ضرورة اتخاذ إجراءات فورية.
وتبين التجربة انه عندما يتم أجراء مقابلات لمستوى الأعلى لإدارة العمليات ، مهما كان حجم المنظمة ، وعندما يوضح المدراء أرائهم فان هذا يؤدي إلى وجود احتياجات أمنية لم تعتبر في السابق والتي تتطلب استجابات فورية.
وبعد ذلك يمكن وضع خطط العمل مباشرة وذلك باستخدام نهج سريع أو مباشر بناء على الجمع بين مجموعتين من الخبرة:
الخبرة الأولى للمهنة في حد ذاتها مقدمة من الإدارة التنفيذية والخبرة الثانية هي تلك التي تتمثل في الحلول الأمنية التي يقدمها خبراء الأمن.

2،3. تحليل المخاطر

تتم الإشارة إلي تحليل المخاطر في كل نشرة أو وثيقة بخصوص الأمن باعتبارها القوة الدافعة في مجال الأمن.
ومع ذلك ، فان معظم الأشخاص يخفقون ويتناسون مناقشة الأساليب التي ينبغي استخدامها لأجراء عملية .
منذ أكثر من عشر سنوات قدمت MEHARI نهج منظما لتقييم المخاطر استنادا إلى مبادئ قليلة و بسيطة.
حاله الخطورة يمكن وصفها من عوامل مختلفة:

- الهيكلي (أو التنظيمية (العوامل، التي لا تعتمد على التدابير الأمنية، ولكن على النشاط الأساسي للمنظمة، والبيئة، والسياق.
- الحد من خطر العوامل التي هي بشكل مباشر على تنفيذ التدابير الأمنية.

MEHARI تمكن التقييم الكمي والنوعي لهذه العوامل و بالتالي تساعد في تقييم مستويات المخاطر.
وفي الواقع فان التحليل الأمني للمخاطر والأصول المعرضة لها يستخدم لتحديد مستوى الحد الأقصى من الخطورة المترتبة على الوضع خطر.
وهذا عادة عامل من العوامل الهيكلية في حين إن تقييم الحالة الأمنية سوف يستخدم لتقييم عوامل الحد من المخاطر.

2.3.1 تحليل المخاطر هو معونة للتخطيط الاستراتيجي:

تحديد عوامل الحد من المخاطر هو في حد ذاته وظيفة من وظائف التدابير الأمنية ويوفر الأساس المنهجي لبناء الخطة الأمنية ألاستراتيجيه أو الخطة الرئيسية.
و للمساعدة في هذا الشأن توفر MEHARI هيكلة وتنظيم لنهج التخطيط الأمني. ويستند هذا النهج إلى قاعدة معارف ومعلومات لحالات الخطر.
وإجراءات أوتوماتيكية لتقييم عوامل الحد من المخاطر.
ودعما للنهج تتوفر أداة حاسوبيه (برنامج كمبيوتر) تخفف علي المستخدم عبء الاضطرار إلى إجراء حسابات وتوفر أيضا محاكاة للظروف المحتملة و والتحسينات في الأداء.

وهذا الاستخدام لمنهج MEHARI يركز على تحسين التدابير الأمنية عامة بهدف الحد من المخاطر.

2.3.2 تحليل منهجي للحالات التي تنطوي على مخاطر

وعلى نفس الأساس المنهجي يتوفر نهجا مختلفا بعض الشيء وينص على : تحديد جميع الحالات التي تنطوي على مخاطر محتملة وتحليل تلك الحالات الأشد خطورة وتحديد الإجراءات اللازمة للحد من تلك المخاطر أو كبتها إلى مستوى مقبول.
ونهج MEHARI يوفر ويدعم هذا النهج من خلال ما يحتويه نهج MEHARI من قواعد المعرفة.
وهذا الاستخدام لنهج MEHARI يركز على ضمان أن تكون كل حاله من حالات المخاطر الحرجة قد تم تحديدها وتغطيتها بخطة عمل تنفيذية.

2.3.3 التحليل العفوي للحالات التي تنطوي على مخاطر

نفس مجموعة الأدوات التي يمكن أن تستخدم في أي لحظة في نهج إدارة الأمن الأخرى. في الحالات التي سبق وصفها حيث أن الأمن تتم أدارته من خلال عمليات مراجعة أو من خلال الأطر المرجعية الأمنية.
وستكون هناك دائما حالات محددة لا يمكن أن تطبق فيها هذه القواعد. وفي هذه الحالات يمكن أن يستخدم التحليل العفوي أو الغير منهجي لتحليل المخاطر.

2.3.4 تحليل المخاطر في المشاريع الجديدة

نموذج تحليل المخاطر يمكن استخدامه في إدارة المشاريع.
عند القيام بوضع خطة للحد من المخاطر التي تتضمنها المشاريع الجديدة وتقرر التدابير التي ينبغي استخدمها نتيجة لذلك.

2،4. لمحة عامة عن استخدامات MEHARI

ومن الواضح ، أن التوجه الرئيسي لنهج MEHARI هو تحليل المخاطر والحد منها. حيث أنشئت قواعد المعارف والآليات والأدوات التابعة لنهج MEHARI لهذا الغرض.
وفي أذهان مصممي نهج MEHARI أن الحاجة إلى أسلوب منظم لتحليل المخاطر والحد منها تتوقف على المنظمة أو المؤسسة في النواحي التالية :

- أسلوب عمل دائم - المبادئ التوجيهية لمجموعة متخصصة ،
- طريقة عملية تستخدم جنبا إلى جنب مع غيرها من الممارسات الإدارية لأمن ،
- طريقة عملية تستخدم أحيانا لتكمل الممارسات العادية.

و مع أخذ هذا في الاعتبار فأن MEHARI توفر مجموعة من المناهج والأدوات التي تمكن من تحليل المخاطر عند الحاجة.
منهجيه MEHARI تضم قواعد المعرفة، والتوجيهات والمراجع التي من شأنها أن تصف مختلف النماذج المتعلقة بالنظام الأمني (كالأملاك و المخاطر و أوجه الضعف الأمني)
ومن هنا لمساعدة الأشخاص المسئولين عن إدارة الأمن (CISOs، ومديري المخاطر، ومراجعي الحسابات، Auditors.) ، في مختلف المهام والأعمال.

3. MEHARI والمعايير الدولية

سؤال كثيرا ما يطرح هو: كيف يتطابق منهج MEHARI مع المعايير الدولية - - وخاصة المنظمة الدولية للتوحيد القياسي ISO13335،ISO17799 و ISO/IEC 27001.

وهنا لن نقوم بالمقارنة المباشرة بين منهجيةMEHARI وتلك المعايير والأدوات البارزة والشهيرة في هذا اليوم.

فالقصد من هذه الوثيقة هو بالأحرى شرح كيفية توافق منهجيةMEHARI مع معايير المنظمة الدولية للتوحيد القياسي ISO من حيث التوافق بين الأهداف.

معيار ISO13335 يشمل نموذجا لإدارة المخاطر التي تمت الإشارة إليها في منهجية MEHARI. وتتوافق منهجية MEHARI توافقا تاما مع نموذج ISO لإدارة المخاطر حيث توفر MEHARI طريقة منهجية وأدوات وفقا لما يقضي به معيارISO.

وسوف نناقش هنا معيار ISO17799و معيار ISO/IEC 27001 وارتباطهما وعلاقتهما بنهج MEHARI.

3،1. أهداف المنظمة الدولية للتوحيد القياسي ISO17799 و ISO/IEC 27001 منهجية MEHARI :

3.1.1 أهداف معيار ISO/IEC 17799:2005

ينص هذا المعيار أن المنظمة أو المؤسسة ينبغي أن تحدد احتياجاتها ومتطلباتها الأمنية باستخدام ثلاثة مصادر رئيسية هي:

- تحليل المخاطر.
- المتطلبات القانونية والتأسيسية والتنظيمية و الشروط التعاقدية.
- مجموعة من المبادئ والأهداف والمتطلبات لمعالجة المعلومات والتي قد تم وضعها من قبل المنظمة أو المؤسسة لدعم عملياتها.

وباستخدام هذا باعتباره أساسا يمكن اختيار ووضع نقاط مراقبة وتحكم من خلال استخدام القائمة المنصوص عليها في البند بعنوان "دليل ممارسات أدارة أمن المعلومات"

أو من أي مجموعة أخرى من نقاط المراقبة (المادة 4.2).

ملاحظه : في نطاق 17799 : 2005 تم النص على أن يوفر المعيار "المبادئ التوجيهية والمبادئ العامة للبدء في تنفيذ وصيانة وتحسين أدارة أمن المعلومات"

ألأمر الذي يعني أن المنظمة الدولية للتوحيد القياسي ISO يمكن أن ينظر إليها على أنها نقطة بدأ و انطلاق.

غير أن معيار ISO/IEC 27001 27001 ينص في المادة (1.2) على انه يتوجب أن يكون أي استثناء مبرر ومقبول (الملحق A - A.1).

معيار ازو ISO17799 يقدم مجموعة من المبادئ التوجيهية التي يمكن أن تستخدمها المنظمة أو المؤسسة.

والمعيار يشير إلى أن القائمة ليست شاملة أو كاملة ولذلك فأن التدابير التكميلية قد تكون مطلوبة.

ومع ذلك لا يوصي المعيار بمنهجيه معينة لوضع نظام كامل لإدارة الأمن. ومن ناحية أخرى فإن كل جزء من المعيار يتضمن دليل ومقدمات وتعليقات عن الأهداف المنشودة. وهذا يمكن أن يكون مفيدا جدا.
ملاحظه : معيار ايزو ISO ينص أيضا في مضمونه أنه يمكن استخدامه "للمساعدة على بناء الثقة في الأنشطة المشتركة بين المنظمات".
وشملت هذه ليست مِن قبيل الصدفة فهذا يبرز جانبا أساسيا من جوانب التي يروج لها مؤيدي المعيار وهو جانب التقييم الأمني (أو حتى الحصول على شهادة) من الناحية الأمنية من الشركات المتحالفة والموردين.

3.1.2 أهداف المنظمة الدولية للتوحيد القياسي ISOاو IEC27001

الهدف واضح من المنظمة الدولية للتوحيد القياسي ISO و IEC27001 هو "توفير نموذج لإنشاء وإدارة معلومات الشركات ونظام إدارة الأمن (ISMS)" والتي يمكن استخدامها سواء داخليا أو استخدامها من قبل أطراف ثالثة ومؤسسات أخرى بما فيها سلطات التصديق".
أهداف عمليات التقييم وإصدار الشهادات تضع تركيزا قويا على الجوانب الشكلية (تقييد و تسجيل الوثائق والقرارات، وإعلان الانطباق، والسجلات، وما إلى ذلك) و التحكم و السيطرة (استعراضات، ومراجعة الحسابات، وما إلى ذلك).
ومن الواضح أن أساس المعالجة الأمنية يعني أن تحليل المخاطر وينبغي أن ينفذ لبحث المخاطر التي تواجهها و تتعرض لها المنظمة واختيار التدابير المناسبة للحد من المخاطر على مستوى وحد مقبول (الفقرة 4.2.1).

معيار ISO/IEC27001 ينص على أن طريقة ما لتحليل المخاطر ينبغي أن تستخدم، ولكنه ليس جزءا من معيار أن يقترح طريقة محددة. بصرف النظر عن اندماج PDCA (PLAN, DO, Check, Act)
وهزه عملية تكرارية من النموذجي من شأنها أنشاء نظام أل ISMS. أيضا فان التوصيات لأفضل الممارسات والتي يمكن استخدامها للحد من المخاطر. توافق تلك التوصيات المدرجة في معيار ISO/IEC17799:2005
وحسب المنظمة الدولية للتوحيد القياسي ISO/IEC27001 فأن أساس تقييم نظام أدارة الأمن ليس يعتمد بالكثير علي المعرفة أو التحقق من ما أذا كانت القرارات التي بذلت مناسبة وملائمة لاحتياجات المنظمة وإنما للتأكد من انه بمجرد أن القرارات اتخذت فأن نظام الإدارة مثله مثل مراجع حسابات أو القائم بالتصديق فقط ينبغي عليه التأكد من أن هذه القرارات قد نفذت فعلا.

3.1.3 أهداف MEHARI

MEHARI هي مجموعة متناسقة من الأدوات والأساليب لإدارة الأمن استنادا إلى تحليل المخاطر. الجانبين الأساسيين في منهج MEHARI هما : نموذج المخاطر (بناء على التحليل النوعي أو الكمي)
ونموذج الإدارة الأمني القائم على أساس تحليل المخاطر ليس له ما يعادله في أي من عناصر المنظمة الدولية للتوحيد القياسي ISO 17799 أو في نظام ISO/IEC 27001

3.1.4 مقارنة بين أهداف MEHARI والمنظمة الدولية للتوحيد القياسي ISO 17799 و ISO/IEC 27001

أهداف MEHARI والمنظمة الدولية للتوحيد القياسي للمعايير ISO المذكورة أعلاه هي مختلفة جذريا.

• MEHARI يهدف إلى توفير الأدوات والأساليب التي يمكن استخدامها لاختيار أنسب التدابير الأمنية لمنظمة بعينها. هذا ليس على الإطلاق هو الهدف المعلن لمعايير المنظمة الدولية للتوحيد القياسي.
• معايير المنظمة الدولية للتوحيد القياسي توفر مجموعة من أفضل الممارسات، التي هي بالتأكيد مفيدة جدا ، ولكنها ليست بالضرورة ملائمة لما هو على المحك في المنظمة ، ومفيدة لتغطية جوانب النضج في الأمن ، أو أمن المعلومات والتخطيط ، أو الوحدات الداخلية المستقلة أو الشركاء.
والنقطة الوحيدة في MEHARI والتي يمكن مقارنتها بالمنظمة الدولية للتوحيد القياسي ISO17799) هي الدليل المرجعي للخدمات الأمن التي تقدمه MEHARI. ويقدم هذا الدليل عناصر مفصلة على نحو فعال يمكن أن تستخدم لبناء إطار للأمن.
و حول هذه النقطة فمن الواضح أن تغطية MEHARI أوسع نطاقا من تغطية المنظمة الدولية للتوحيد القياسي حيث تشمل تغطية MEHARIالجوانب الأساسية للأمن.

3،2. التوافق بين الأنظمة والنهج المختلفة

نهج MEHARI يتفق تماما مع المنظمة الدولية للتوحيد القياسي ISO17799 و على الرغم من أنهما لا يملكون نفس الأهداف المعلنة فأنه من السهل نسبيا تمثل نتائج تحليل MEHARI من حيث مؤشرات المنظمة الدولية للتوحيد القياسي ISO17799.
MEHARI تستجيب للحاجة التي تعرب عنها معايير المنظمة الدولية للتوحيد القياسي لتحليل المخاطر وتحديد التدابير التي ينبغي تنفيذها.

3.2.1 التوافق مع معيار ازو ISO17799

نقاط المراقبة المتوفرة في معيار المنظمة الدولية للتوحيد القياسي هي نقاط عامة كتدابير تنظيمية أو سلوكيه في حين أن MEHARI تشدد على الحاجة إلى الكفاءة في التدابير التقنية التي يمكن أن تكون مضمونة النتائج .
ومن أجل ذلك فأن النتائج ستكون مختلفة اختلافا جذريا في هذين المنهجين.
ورغم من هذه الاختلافات فأن MEHARI 2007 من خلال نظامها لاستعراض الضعف تعرض لنا جداول مؤشرات متناسقة ومتوافقة مع تلك المستخدمة في المنظمة الدولية للتوحيد القياسي 17799:2005 يمكن استخدامها لمن لهم حاجة إلى إثبات امتثالها لذلك المعيار.
ومن المفيد الإشارة هنا إلى أن الاستبيانات المتعلقة بمراجعة الحسابات في نهج MEHARI جرى تصميمها لتمكين الإدارة التنفيذية لإجراء عملية استبيان و استعراض الضعف بكفاءة
واستنتاج قدرة كل أداره للحد من هذه المخاطر.

3.2.2 التوافق مع معيار ازو 27001

MEHARI يمكن بسهولة أن تدمج في عملية المنظمة الدولية للتوحيد القياسي و IEC27001 ولا سيما 'خطة' المرحلة (القسم 4.2.1).

 © CLUSIF 2007

MEHARI تشمل وصفا كاملا للمهام التي تمكن من إنشاء قواعد ISMS وفي مرحلة العمل'DO Phase' (القسم 4.2.2) والذي يهدف إلى إدارة وتنفيذ ISMS فان MEHARI توفر عناصر من قبيل بناء خطط لإدارة المخاطر ، مع تحديد الأولويات المرتبطة ارتباطا مباشرا بعملية تصنيف المخاطر وتقييم العمليات أثناء الاستخدام.

وفي مرحلة 'التحقق' المرحلة (القسم 4.2.3) ، MEHARI توفر العناصر التي تمكن من تقييم المخاطر المتبقية ، والتحسينات التي أدخلت في التدابير الأمنية.

وبالإضافة إلى ذلك ، أي تغييرات تطرأ على البيئة (المخاطر والتهديدات والحلول ومنظمة) يمكن بسهولة عن طريق إعادة تقييم عمليات مراجعة الحسابات التي استهدفت استخدام نتائج الأولية MEHARI مراجعة الحسابات. وهكذا يمكن أن تكون الخطط الأمنية المنقحة وتتطور مع مرور الوقت.

أما مرحلة 'التنفيذ' المرحلة (القسم 4.2.4)، فأن MEHARI تدعو إلي أهمية ضوابط الأمن والتحسين المستمر لها وبالتالي فإنها تضمن بلوغ الهدف المقصود في عملية الحد من الخطر.

في كل هذه المراحل الثلاث و في حين أن MEHARI ليست في صميم العمليات، فإنها تساهم إلى حد كبير في تنفيذها وتضمن الكفاءة لها.