مهاری ۲۰۱۰

مرور

آوریل ۲۰۱۰

گروه کاری روش‌ها

لطفاً پرسش‌ها و نظرات خود را به سخنگاه زیر ارسال نمایید:
http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador, 75009 PARIS

mail: clusif@clusif.fr _Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e

Web: http://www.clusif.fr

قدردانی

با تشکر از ژان لویی رائول (Louis Roule_Jean) برای ترجمه‌ی انگلیسی و مسئولیت گروه کاری مستندات *مهاری* و همچنین مهران طریحی (Mehran Toreihi) (شرکت داده پردازان آبشار) و سید علیرضا مهدوی اردستانی (Seyyed Alireza Mahdavi Ardestani) (شرکت داده پردازان آبشار) برای ترجمه و ویرایش سند به زبان فارسی.

فهرست مطالب

۱ـ مقدمه

متدولوژی *مهاری* در اصل به این منظور طراحی شده و بطور مستمر به‌روزرسانی می‌شود که مأموران ارشد امنیت اطلاعات[1] را در مدیریت امنیت اطلاعات کمک نماید.
این مستند به منظور استفاده این گروه از افراد در نظر گرفته شده است ولیکن، افراد دیگری مانند ممیزان، مأموران ارشد اطلاعات[2] و مدیران ریسک نیز که با چالش‌های مشابهی روبرو هستند، می‌توانند از آن بهره ببرند.
هدف اصلی در این مستند بیان این مطلب است که چگونه می‌توان از *مهاری* استفاده کرد. جزئیات بیشتر در رابطه با این متدولوژی و ابزارهای مشابه در مستندات دیگری ارائه شده است که از طریق سایت CLUSIF[3] در دسترس است. بعضی از این مستندات عبارتند از:

- *مهاری*: ویژگی‌های کارکردی و مفاهیم،
- راهنماهای *مهاری* برای:
  - طبقه‌بندی و تحلیل ذینفعان،
  - ارزیابی خدمات امنیتی و
  - تحلیل ریسک،
- راهنمای مرجع *مهاری* در رابطه با خدمات امنیتی،
- پایگاه دانش *مهاری*.

اولین هدف *مهاری* فراهم کردن یک روش ارزیابی و مدیریت در حوزه‌ی امنیت اطلاعات است که منطبق با نیازمندی‌های ISO/IEC 27005:2008 باشد و مجموعه‌ای از ابزارها و عناصر مورد نیاز برای پیاده‌سازی آن را فراهم نماید.
دیگر اهداف عبارتند از:

- امکان تحلیل مستقیم و یک‌به‌یک وضعیت‌های ریسک با استفاده از سناریوها،
- تدارک مجموعه‌ای از ابزارها به‌منظور طراحی مدیریت امنیت، در قالب بازه‌های کوتاه، متوسط و بلند مدت به‌طوری‌که با سطوح مختلف بلوغ سازمانی و همچنین اقدامات و فعالیت‌های مختلف سازگار باشد.

در واقع، *مهاری* یک متدولوژی پایدار، به همراه پایگاه دانشی است که مدیران ارشد امنیت اطلاعات، مدیران عمومی و مدیران امنیت و یا تمام کسانی که در مباحث کاهش ریسک نقش دارند را در انجام فعالیت‌ها و وظایفشان یاری می‌رساند.
ارتباط مهاری با استانداردهای سری ISO/IEC 27000 در انتهای این مستند اشاره شده است.

[1] CISO
[2] CIO
[3] http://clusif.asso.fr/

۲ـ موارد استفاده‌ی *مهاری*

مهاری یک روش ارزیابی و مدیریت ریسک است.
در عمل، مفهوم این موضوع این است که *مهاری* و پایگاه‌های دانش مربوط به آن، به منظور تحلیل دقیق وضعیت‌های ریسک از طریق سناریوهای تعریف شده، طراحی شده است.
در ادبیات روزمره، مدیریت امنیت، فعالیت یا عملکردی است که به مرور زمان خود را نشان می‌دهد. فعالیت‌های اصلاحی هم بر حسب اینکه سازمان تا چه حد در این حوزه تلاش کرده باشد متفاوت است.
اولین گام در امنیت این است که معیارها و سیاست‌های فعلی سازمان شناسایی شده و با بررسی و مقایسه‌ی آنها با به‌روش‌ها، فاصله‌ی حالت فعلی تا حالت آرمانی بدست آید که به این فرآیند تحلیل شکاف می‌گویند.
بعد از ارزیابی وضعیت فعلی و تصمیم گیری در خصوص پیاده‌سازی امنیت در سازمان، نوبت به تصمیم‌گیری در مورد مجموعه‌ای از فعالیت‌های زنجیره‌ای است. این تصمیمات که معمولاً در قالب‌هایی مانند طرح‌ها، قوانین سازمانی، سیاست‌ها و یا چارچوب مرجع امنیت قرار می‌گیرند باید در قالب یک رهیافت ساختیافته انجام شوند. این رهیافت می‌تواند همانند الزام بخشی از سیستم مدیریت امنیت اطلاعات (ISO/IEC 27001) مبتنی بر ارزیابی ریسک باشد. روش‌های دیگری نیز وجود دارند که می‌توانند به صورت داخلی، تخصصی یا ترکیبی اجرا شوند مانند محک‌زدن[۴].
در این مرحله بدون توجه به بحث ارزیابی ریسک باید سؤالات ذینفعان پاسخ داده شود. اغلب شخص اصلی تصمیم‌گیرنده که مسئول اختصاص بودجه نیز است علیرغم اینکه تصمیم اتخاذ شده است این پرسش را مطرح می‌کند که «آیا این موضوع واقعاً لازم است؟». با توجه به فقدان ارزیابی اولیه و توافق عمومی ذینفعان بسیاری از پروژه‌های امنیتی متوقف یا با تأخیر مواجه شده و می‌شوند.
معمولاً پس از گذشت زمانی و یا حتی بعد از مشخص کردن رهیافت اولیه، سؤالی اساسی مطرح می‌شود بدین مضمون که «آیا تمامی مخاطرات سازمان شناسایی شده‌اند و آیا این اطمینان وجود دارد که سطح آنها قابل پذیرش باشد؟». این سؤال به طور کل یا در قالب یک پروژه و یا در سطح عمومی سازمان بیان می‌شود. در این لحظه یک روش تحلیل و ارزیابی ریسک ضروری به نظر می‌رسد.
متدلوژی *مهاری* بر اساس این اصل بنا نهاده شده است که ابزارهایی که در هر مرحله از توسعه‌ی امنیت مورد نیاز هستند باید به نحوی سازگار باشند که هر نتیجه‌ای که در هر مرحله بدست آید باید توسط دیگر ابزارها در سازمان قابل استفاده‌ی مجدد باشد.
ابزارها و پیمانه‌های گوناگون در مجموعه‌ی متدلوژی *مهاری* به گونه‌ای طراحی شده اند تا علاوه بر تحلیل یک‌به‌یک مخاطرات، به گونه‌ای ارزیابی را انجام دهند که در هر مرحله از توسعه‌ی امنیت، علیرغم استفاده از رهیافت‌های گوناگون مدیریتی، سازگاری نتایج تصمیمات را تضمین نمایند.

۲ـ۱ تحلیل یا ارزیابی ریسک

تحلیل ریسک تقریباً در تمامی متون و مستندات امنیتی به عنوان نیروی محرک نیازمندی‌های امنیتی ارائه شده است که نمود اصلی آن در استانداردهای ISO/IEC به چشم می‌خورد.
در هر حال، اکثر این مستندات، موضوع اینکه چه روشی باید استفاده شود را اشاره نکرده‌اند.
برای بیش از پانزده سال است که *مهاری* یک روش ساختیافته برای ارزیابی ریسک بر اساس چند اصل ساده ارائه کرده است[۵].
وضعیت ریسک توسط چند شاخص زیر مشخص می‌شود:

[4] Benchmarking

[۵] توضیح تفصیلی روش ریسک در مستند «اصول بنیادین *مهاری* و ویژگی‌های کارکردی» تشریح شده است.

- فاکتورهای ساختاری (سازمانی) که با معیارهای امنیتی مرتبط نیستند ولیکن با فعالیت‌های اصلی سازمان یا محیط و پیرامون آن در ارتباط باشند.
- فاکتورهای کاهش ریسک که به صورت مستقیم مربوط به معیارهای پیاده‌سازی امنیت هستند.

در واقع، ارزیابی ذینفعان در حوزه‌ی امنیت به منظور تشخیص حداکثر سطح اهمیت در شرایط پیامد ریسک ضروری است. این موضوع در اصل یک فاکتور ساختاری است در حالیکه ارزیابی امنیتی به منظور شناسایی فاکتورهای کاهش ریسک استفاده می‌شود. *مهاری* امکان ارزیابی کیفی و کمّی این فاکتورها را همراه با ارزیابی سطوح ریسک به عنوان نتایج ارائه می‌کند. بدین منظور، *مهاری*، ابزارها (مثلاً معیارهای ارزیابی، فرمول‌ها و غیره) و پایگاه‌های دانش (بالاخص برای شناسایی معیارهای امنیتی) را یکپارچه می‌کند که این موضوع برای حداقل چارچوب ارائه شده توسط ISO/IEC 27001 یک اصل است.

۲ـ۱ـ۱ تحلیل سیستماتیک وضعیت ریسک

به منظور پاسخ به سؤال «ریسک‌های سازمان چه هستند و آیا در وضعیت پذیرش قرار دارند یا خیر؟» نیاز به یک روش ساختیافته است تا تمامی وضعیت‌های بالقوه‌ی ریسک را شناسایی کرده، حیاتی‌ترین آنها را یک‌به‌یک تحلیل کرده و سپس، فعالیت‌هایی که به منظور کاهش آنها به سطح قابل قبول باشند را شناسایی نماید.

رهیافت ارائه شده توسط *مهاری* مبتنی بر پایگاه دانش وضعیت ریسک و رویه‌های خودکار به منظور ارزیابی فاکتورهای تعیین کننده‌ی هر ریسک و سپس ارزیابی سطح آنها است. علاوه بر این، روش *مهاری* در انتخاب طرح‌های برخورد با ریسک نیز کمک و راهنمایی‌هایی فراهم می‌کند.

به منظور ارزیابی مخاطرات دو روش پیشنها شده است.

- استفاده از مجموعه‌ای از توابع در پایگاه دانش (برای Excel یا Open Office) که این امکان را فراهم می‌کند که ماژول‌های *مهاری* (مثلاً دسته‌بندی دارایی‌ها در ارزیابی ذینفعان، تشخیص امنیت) یکپارچه‌سازی شوند.
- استفاده از یک نرم‌افزار کاربردی (مثل RISICARE[۶]) که با استفاده از یک واسط کاربری قوی‌تر امکاناتی مانند شبیه‌سازی‌ها، نمایش‌های بصری و بهینه‌سازی‌های دیگر را فراهم می‌کند[۷].

۲ـ۱ـ۲ تحلیل فوری وضعیت ریسک

در دیگر رهیافت‌های مدیریت امنیت، در هر لحظه می‌توان از مجموعه ابزار مشابه استفاده کرد.

در برخی از شرایط در مدیریت امنیت، هنگامی که مدیریت ریسک هدف اصلی نبوده و امنیت توسط ممیزی‌ها و با چارچوب‌های مرجع امنیت مدیریت می‌شود، اغلب موارد خاصی وجود دارند که قوانین، قابل اعمال نمی‌باشند. تصمیم‌گیری در مورد بهترین گزینه می‌تواند توسط تحلیل ریسک فوری انجام شود.

۲ـ۱ـ۳ تحلیل ریسک در پروژه‌های جدید

مدل تحلیل ریسک و مکانیزم‌های آن می‌تواند در مدیریت پروژه به منظور برنامه‌ریزی مخاطرات و تصمیم‌گیری در مورد اینکه چه معیارهایی به عنوان نتیجه استفاده شوند بکارگیری شود.

---

[۶] محصول BUC S. A.

[۷] نرم‌افزار مدیریت امنیت اطلاعات بادبان با واسط کاربری فارسی و کاملاً بومی توسط شرکت داده پردازان آبشار توسعه داده شده است که مبتنی بر چهارچوب ISO/IEC 27005 فرآیند سیستم مدیریت امنیت اطلاعات و همچنین مدیریت ریسک امنیت اطلاعات را بسیار تسهیل می‌کند – مترجم.

۲ـ۲ ارزیابی‌های امنیتی

مهاری توسط پرسش‌نامه‌های شناسایی‌کننده کنترل‌های امنیتی موجود یکپارچه می‌شود و امکان ارزیابی سطح کیفی مکانیزم‌ها و راه‌حل‌هایی که در کاهش ریسک هدف گذاری شده‌اند را فراهم می‌کند[۸].

۲ـ۲ـ۱ مرور آسیب‌پذیری، یکی از عناصر تحلیل ریسک

مهاری یک مدل ریسک ساختیافته را ارائه می‌کند که در آن فاکتورهای کاهش ریسک را تحت قالب خدمات امنیتی در نظر می‌گیرد. نتایج ارزیابی آسیب‌پذیری، یک ورودی مهم برای تحلیل ریسک بوده تا بدین وسیله اطمینان حاصل شود که خدمات امنیتی نقش خود را به‌طور کامل ایفا می‌کنند که این موضوع خود یکی از نکات الزامی در اعتبار و اطمینان تحلیل ریسک است.
یکی از نقاط قوت *مهاری*، توانایی آن در ارزیابی سطح ریسک‌های فعلی و همچنین آینده، بر اساس یک پایگاه‌دانش خبره است که سطح کیفی معیارهای امنیتی را در قالب عملیاتی یا تصمیم‌گیری شده ارزیابی می‌کند.

۲ـ۲ـ۲ طرح‌های امنیت مبتنی بر بازنگری‌های آسیب‌پذیری

یک رهیافت ممکن این است که طرح‌های عملیاتی را مستقیماً بر اساس نتایج ارزیابی وضعیت خدمات امنیت ایجاد کرد.
فرآیند مدیریت امنیتی که پس از این رهیافت در نظر گرفته می‌شود بسیار ساده است: یک ارزیابی را اجرا کنید و تصمیم‌گیری کنید تا تمامی خدماتی که سطح کیفی مطلوبی ندارند را بهبود دهید.
پرسش‌نامه‌های تشخیص *مهاری* در این رهیافت مورد استفاده قرار می‌گیرند.
به منظور برقراری ارتباط با ماژول *مهاری* باید یک تحلیل اولیه از کسب و کار برنامه‌ریزی شود. این تحلیل سبب خواهد شد که سطح کیفی مورد نیاز در رابطه با خدمات امنیتی مرتبط و متعاقباً انصراف از بقیه موارد به عنوان بخشی از ارزیابی مشخص شود.

۲ـ۲ـ۳ پشتیبانی فراهم شده در پایگاه‌دانش به منظور ایجاد یک چارچوب مرجع امنیت

پایگاه‌دانش منحصر به فرد *مهاری* می‌تواند برای ایجاد یک چارچوب مرجع امنیت (یا سیاست‌های امنیتی) به صورت مستقیم مورد استفاده قرار گیرد. این چارچوب دربردارنده‌ی مجموعه قوانین و دستورالعمل‌هایی است که سازمان از آن پیروی می‌کند. این رهیافت معمولاً در سازمان‌هایی با سایت‌ها یا واحدهای عملیاتی مستقل مورد استفاده قرار می‌گیرد. این مورد معمولاً در شرکت‌های بزرگ چند ملیتی با تعدادی مجموعه‌ی وابسته وجود دارد اما می‌تواند به آسانی برای شرکت‌های متوسط با تعداد زیادی شعب و نمایندگی‌های منطقه‌ای بکارگیری شود. در این مورد انجام چندین تحلیل و ارزیابی ریسک بسیار مشکل است.

ساخت چارچوب مرجع امنیت

پرسش‌نامه‌های ارزیابی *مهاری* یک پایه‌ی کاری مناسب برای مدیران امنیت به حساب می‌آید تا بتوانند تصمیم‌گیری کنند که چه چیز باید در سازمانشان بکارگیری شود.

مدیریت استثناءها در قوانین

ایجاد یک مجموعه از قوانین در چارچوب مرجع امنیت معمولاً با مشکلات پیاده‌سازی محلی همراه است، بنابراین باید موارد استثناء و عدول از قوانین مدیریت شود.
استفاده از یک پایگاه‌دانش یکپارچه با مجموعه‌ای از ابزارها و متدلوژی تحلیل پایدار این امکان را فراهم می‌کند که انحرافات محلی مدیریت شوند. درخواست‌های مربوط به استثناءها می‌تواند توسط یک تحلیل ریسک خاص با تمرکز بر مشکلات شناسایی شده پوشش داده شود.

[۸] کنترل‌های امنیتی یا معیارها در زیر خدمات، خدمات و در نهایت حوزه‌های امنیتی گروه بندی می‌شوند.

۲ـ۲ـ۴ حوزه‌هایی که توسط ماژول ارزیابی آسیب‌پذیری پوشش داده می‌شود

از نقطه نظر تحلیل ریسک، بر طبق شناسایی تمامی وضعیت‌های مخاطره و تصمیم برای پوشش دادن تمامی ریسک‌های غیر قابل پذیرش، *مهاری* صرفاً به حوزه‌ی فناوری اطلاعات محدود نمی‌شود.
ماژول ارزیابی، صرف‌نظر از سیستم اطلاعاتی، کلیت سازمان و محافظت از سایت در حالت عمومی و همچنین محیط کاری و جنبه‌های قانونی و وابسته به قانون را پوشش می‌دهد.

۲ـ۲ـ۵ مروری بر ماژول ارزیابی

نکته‌ی مهمی که در مورد ماژول ارزیابی آسیب‌پذیری باید در ذهن حک شود این است که یک دید باز و پایدار از امنیت را ارائه می‌کند. این موضوع می‌تواند در رهیافت‌های گوناگون که از نظر عمق و ریزدانگی تحلیل، تکاملی هستند مورد استفاده قرار گیرد و همچنین می‌تواند در تمامی مراحل بلوغ آگاهی امنیتی سازمان مورد استفاده قرار گیرد.

۲ـ۳ تحلیل ذینفعان

امنیت درباره‌ی محافظت از دارایی‌ها است. صرف‌نظر از رویکردهای سیاست امنیتی، یک اصل وجود دارد که تمامی مدیران در مورد آن هم‌عقیده هستند و آن این است که باید یک توازن متناسب میان سرمایه‌گذاری‌ها در بخش امنیت از یک طرف و اهمیت ذینفعان مرتبط با کسب و کار در طرف دیگر برقرار شود.
این موضوع بدین معنی است که فهم درستی از ذینفعان کسب و کار یک اصل بنیادین است و همچنین، تحلیل امنیتی ذینفعان نیازمند یک سطح اهمیت بالا و یک روش ساختیافته و مشخص ارزیابی است.
هدف از تحلیل امنیت ذینفعان پاسخ به پرسش دو وجهی زیر است:
«چه چیز ممکن است رخ دهد و اگر اتفاق بیفتد آیا جدی است؟»
در حوزه‌ی امنیت، ذینفعان به عنوان عواقب رخدادها در نظر گرفته می‌شوند که عملکرد مورد نظر را در سازمان با مشکل مواجه می‌کنند.
مهاری یک ماژول تحلیل ذینفعان ارائه می‌کند که در مستند «*مهاری*: طبقه‌بندی و تحلیل ذینفعان» تشریح شده است و دو نتیجه به دست می‌دهد:

- یک مقیاس میزان سوء عملکرد
- یک طبقه‌بندی از اطلاعات و دارایی‌های فناوری اطلاعات

مقیاس میزان سوء عملکرد

شناسایی سوء عملکردها یا رخدادهای بالقوه، فرآیندی است که با فعالیت‌های سازمان شروع شده و شامل شناسایی سوءعملکردهای محتمل در فرآیندهای عملیاتی می‌باشد. نتیجه‌ی آن عبارتست از:

- یک توصیف از انواع سوءعملکردهای ممکن
- یک تعریف از پارامترهایی که بر اهمیت هر یک از سوءعملکردها تأثیرگذارند
- یک ارزیابی از آستانه‌ی بحرانی هر یک از این پارامترها که سطح اهمیت هر یک از سوءعملکردها را تغییر می‌دهند.

این مجموعه از نتایج تشکیل دهنده‌ی مقیاس میزان سوء عملکرد است.

طبقه‌بندی اطلاعات و دارایی‌ها

در موضوع امنیت سیستم‌های فناوری اطلاعات صحبت درباره‌ی طبقه‌بندی اطلاعات و طبقه‌بندی دارایی‌های فناوری اطلاعات بسیار عادی است.

منظور از طبقه‌بندی مشخص کردن شاخص‌های نمایش‌دهنده‌ی اهمیت معیارهای تحت تأثیر فقدان دارایی یا اطلاع در مورد هر یک از انواع اطلاعات، دارایی‌های فناوری اطلاعات و معیارهای طبقه‌بندی (مانند محرمانگی، صحت، دسترس‌پذیری یا معیارهای دیگری مانند قابلیت ردگیری) است.
طبقه‌بندی اطلاعات و دارایی‌ها برای سیستم‌های اطلاعاتی عبارت از تبدیل مقیاس میزان سوءعملکرد که پیش‌تر تعریف شده است، به شاخص‌های حساسیت مرتبط با دارایی‌های فناوری اطلاعات است.

نمایش ذینفعان امنیتی

مقیاس میزان سوءعملکرد و طبقه‌بندی اطلاعات و دارایی‌ها دو روش متفاوت ذینفعان امنیتی است.
مورد پیشین بسیار جزئی‌تر بوده و اطلاعات بیشتری را برای مأموران ارشد امنیت فراهم می‌کند. مورد اخیر کلی‌تر بوده و بیشتر مناسب کمپین‌های آگاهی‌رسانی و ارتباطات بوده ولیکن سطح ریزدانگی آن کمتر است.

۲ـ۳ـ۱ تحلیل ذینفعان، پایه‌ای برای تحلیل ریسک

این ماژول یکی از ماژول‌های کلیدی در تحلیل ریسک است. بدون توافق عمومی در مورد عواقب مرتبط با نقص عملکردهای احتمالی، امکان قضاوت در مورد سطح ریسک امکان‌پذیر نمی‌باشد.
مهاری یک روش دقیق برای ارزیابی ذینفعان و طبقه‌بندی دارایی‌ها ارائه می‌کند که نتایج و خروجی‌های منطقی فراهم می‌کند.

۲ـ۳ـ۲ تحلیل امنیتی ذینفعان: بنیاد طرح‌ریزی عملیات استراتژیک

به طور واضح، تحلیل ذینفعان به منظور پیاده‌سازی هر نوع از طرح اجرا ضروری به نظر می‌رسد. هر رهیافتی که در هر زمان مورد استفاده قرار گیرد باید منابعی به منظور پیاده‌سازی طرح‌های اجرایی اختصاص داده و توجیه این سرمایه‌گذاری‌ها مورد سؤال قرار گیرد.
منابع و بودجه‌هایی که برای امنیت اختصاص می‌یابد، همانند سیاست‌های بیمه، به طور مستقیم با ریسک در ارتباط است. اگر یک اجماع آراء در مورد نقص‌های عملکرد ممکن موجود نباشد، خیلی غیرمحتمل است که بودجه‌ها اختصاص یابد.

۲ـ۳ـ۳ طبقه‌بندی: عنصری ضروری برای خط‌مشی امنیت

چارچوب مرجع امنیت، خط مشی‌های امنیتی و رهیافت‌های مربوط برای مدیریت امنیت همگی در این مستند اشاره شده‌اند.
در عمل، شرکت‌هایی که امنیت را از طریق مجموعه‌ای از قوانین مدیریت می‌کنند باید خودشان با توجه به تابعی از حساسیت اطلاعاتی که پردازش می‌کنند در این مجموعه از قوانین تمایز قائل شوند. ارجاع به طبقه‌بندی اطلاعات یا دارایی‌های سیستم فناوری اطلاعات بسیار متداول است.
ماژول تحلیل امنیت ذینفعان در *مهاری*، روش‌های اجرای این طبقه‌بندی را مشخص می‌کند.

۲ـ۳ـ۴ تحلیل امنیت ذینفعان: پایه‌ای برای طرح‌ریزی امنیت

بسیاری از فرآیندهای تحلیل امنیت ذینفعان که نیاز به مشارکت مدیران عملیاتی دارند در اغلب موارد منجر به نیاز به اقدام فوری می‌شوند.
تجربه نشان داده است هنگامی‌که با مدیریت عملیاتی سطح بالای سازمان مصاحبه می‌شود، صرف‌نظر از اندازه‌ی سازمان، هنگامی‌که آنها دیدگاه‌ها و تخمین‌های خودشان را از نقص عملکرد جدی بیان می‌کنند منجر به نیازهای امنیتی می‌شود که قبلاً در نظر گرفته نشده و نیاز به پاسخگویی سریع دارند.

طرح‌های عمل می‌توانند به صورت مستقیم و با استفاده از یک رهیافت روشن بر پایه ترکیبی از دو مجموعه از خبرگی و تخصص شامل موارد مربوط به خود که توسط مدیریت عملیاتی ارائه می‌شود و راه‌حل‌های امنیتی که توسط خبرگان امنیتی ارائه می‌شود، ایجاد شوند.

۲ـ۴ مرور عمومی بر موارد استفاده مهاری

به طور واضح، اصلی‌ترین رویکرد *مهاری*، ارزیابی و کاهش ریسک است. پایگاه‌های‌دانش آن، مکانیزم‌های آن و همچنین ابزارها به منظور همین هدف ایجاد شده‌اند.

همچنین، در ذهن طراحان این مجموعه متدلوژی، نیاز به یک روش ساختیافته برای تحلیل و کاهش ریسک با توجه به سازمان می‌تواند به صورت یکی از موارد زیر باشد:

- یک روش دائمی – راهنمایی برای یک گروه تخصصی،
- یک روش کاری قابل استفاده به صورت موازی با دیگر روش‌های مدیریت امنیت،
- یک روش کاری قابل استفاده بصورت گهگاه برای تکمیل روش‌های معمول.

با درنظر گرفتن این موضوع، *مهاری* مجموعه‌ای از رهیافت‌ها و ابزارها را فراهم می‌کند تا در هر زمان که نیاز بود، بتوان تحلیل ریسک را انجام داد.

متدلوژی *مهاری* به همراه پایگاه‌های‌دانش آن، راهنماها و مستنداتی که ماژول‌های مختلف (ذینفعان، ریسک‌ها، آسیب‌پذیری‌ها) را تشریح می‌کنند به منظور کمک به افرادی است که وظایف و فعالیت‌هایشان در جایگاه مدیریت امنیت (مأموران ارشد امنیت، مدیران ریسک، ممیزان، مأموران ارشد اطلاعات و ...) قرار دارد.

۳ـ *مهاری* و استانداردهای ISO/IEC 27000

سؤالی که اکثراً پرسیده می‌شود این است که: ارتباط *مهاری* با استانداردهای بین‌المللی به‌ویژه سری ISO/IEC 27000 چگونه است.
هدف از این قسمت توضیح این مطلب است که *مهاری* با استانداردهای ISO 27001, 27002 و 27005 از نظر اهداف و سازگاری‌ها، چگونه مرتبط می‌شود.

۳ـ۱ اهداف مربوط به ISO/IEC 27001, 27002, 27005 و *مهاری*

۳ـ۱ـ۱ اهداف استاندارد ISO/IEC 27002:2005

این استاندارد، تصریح کننده‌ی این موضوع است که سازمان باید الزامات امنیتی خود را از طریق منابع سه‌گانه‌ی زیر شناسایی نماید:

- تحلیل ریسک،
- الزامات قانونی، حقوقی، مقرراتی یا قراردادی،
- مجموعه‌ای از اصول، اهداف و الزامات که بر فرآیندهای اطلاعاتی سازمان که به منظور پشتیبانی از عملیاتش توسعه داده شده، اعمال شده‌اند.

با بکارگیری این موضوع به عنوان یک پایه، می‌توان اهداف کنترلی را با استفاده از فهرستی که در بخش «راه‌کارهای اجرایی برای مدیریت امنیت اطلاعات» در استاندارد و یا هر منبع دیگری انتخاب و پیاده‌سازی کرد (۴ـ۲).
توجه: در دامنه‌ی 27002:2005 تصریح شده است که استاندارد «راهنماها و اصول کلی برای شروع، پیاده‌سازی، نگهداری و ارتقاء مدیریت امنیت اطلاعات» فراهم می‌کند، بدین معنی که استاندارد ISO می‌تواند به عنوان یک نقطه‌ی شروع در نظر گرفته شود. درهرحال، ISO/IEC 27001 (۱ـ۲) تصریح می‌کند که هر گونه حذف، باید توجیهی داشته باشد و اضافه کردن اهداف کنترلی قابل پذیرش می‌باشد (ضمیمه الف ـ الف ۱).

استاندارد ISO 27002 تلفیقی از راهنماها را فراهم می‌کند که می‌تواند توسط سازمان مورد استفاده قرار گیرد. البته توجه می‌دهد که این فهرست کامل نبوده و ممکن است که تمهیدات تکمیلی مورد نیاز باشد. به‌هرحال، هیچ متدولوژی‌ای به منظور ایجاد یک سیستم مدیریت امنیت اطلاعات به صورت کامل توصیه نمی‌شود.
ار طرف دیگر، هر بخش از راهنمای به‌روش‌ها[۹]، شامل مقدمه‌ها و نقطه‌نظرات در رابطه با اهداف مورد نظر بوده که می‌تواند یک کمک بسیار سودمند باشد.
توجه: استاندارد ISO در بدنه‌ی خود تصریح می‌کند که می‌تواند برای «کمک به ساخت اعتماد در فعالیت‌های بین‌سازمانی» مورد استفاده قرار گیرد. این بند به صورت اتفاقی اضافه نشده است و یک جنبه‌ی اصلی را در ذهن تداعی می‌کند که از نقطه نظر امنیت اطلاعات برای تأمین‌کنندگان و شرکای تجاری، توسط پشتیبانی‌کنندگان استاندارد ترویج می‌شود و آن مفهوم، ارزیابی (یا حتی گواهینامه) است.

[۹] Best Practice

۳ـ۱ـ۲ اهداف ISO/IEC 27001:2005

هدف مشخص در ISO/IEC 27001 «تدارک مدلی برای ایجاد و راهبری یک سیستم مدیریت امنیت اطلاعات سازمانی» و «استفاده به صورت داخلی یا توسط نهادهای سوم، شامل مراکز صدور گواهینامه» است.
هدف از ارزیابی و گواهی، یک تمرکز قوی بر جنبه‌های رسمی (مستندسازی و ثبت تصمیمات، اعلام کابردپذیری، آمارثبت و ...) و کنترل (بازنگری، ممیزی و ...) است.
کاملاً واضح است که پایه‌ی رهیافت امنیتی، مشخص‌کننده‌ی این است که ریسک‌هایی که سازمان با آنها مواجه است باید در یک تحلیل ریسک شناسایی شده و معیارهای مقابله با آنها به منظور رسیدن به سطح مورد پذیرش بکارگیری شوند.
استاندارد ISO/IEC 27001 تصریح می‌کند که یک روش ارزیابی ریسک باید مورد استفاده قرار گیرد، ولیکن این موضوع بخشی از استاندارد نبوده و هیچ روش خاصی به غیر از مجتمع‌سازی چرخه‌ی PDCA (طرح‌ریزی، اجرا، بررسی، اقدام) همانند آنچه که برای ایجاد یک سیستم مدیریت امنیت اطلاعات تعریف شده، توصیه نشده است.
همچنین، توصیه‌ها یا به‌روش‌هایی که می‌توانند به منظور کاهش ریسک مورد استفاده قرار گیرند «همسو با موارد فهرست شده در ISO/IEC 2772:2005» در نظر گرفته شده، درحالی‌که، فهرستی از کنترل‌های مرتبط، در ضمایم ارائه شده است.
با توجه به ISO/IEC 27001، زیربنای ارزیابی سیستم مدیریت امنیت اطلاعات این نیست که آیا دانش یا شناخت لازم برای تصمیم‌گیری مناسب با توجه به نیازمندی‌های سازمان وجود داشته و تصمیم‌گیری‌ها به درستی انجام شده است یا نه، بلکه، تبیین کننده‌ی این موضوع است که هنگامی که تصمیمات اتخاذ شده‌اند، از نقطه نظر ممیزی یا گواهی آیا می‌توان از پیاده‌سازی و اجرای این تصمیمات اطمینان حاصل کرد.

۳ـ۱ـ۳ هدف ISO/IEC 27005:2008

اهداف و مقاصد این استاندارد ساخت یک روش ارزیابی ریسک نیست، بلکه، ایجاد یک چارچوب کمینه و توصیف نیازمندی‌های مربوط به فرآیند ارزیابی ریسک، شناسایی تهدیدات و آسیب‌پذیری‌ها به منظور تخمین ریسک، سطوح آنها و قرارگیری در وضعیتی که استراتژی برخورد با آنها و متعاقباً طرح‌ها و معیارهای هدف برای ارزیابی و بهبود وضعیت ریسک مشخص شود، است.
استاندارد اظهار می‌دارد که به منظور اجتناب از روش‌های ساده یا ناپایدار، از روش ارزیابی ریسک مطابق با الزامات این استاندارد که مورد نظر ویراستاران آن نیز بوده است، استفاده شود.

۳ـ۱ـ۴ اهداف *مهاری*

مهاری یک مجموعه از ابزارها و ویژگی‌های روشمند و پایدار برای مدیریت امنیت و تمهیدات مرتبط مبتنی بر تحلیل ریسک دقیق است. جنبه‌های اصلی *مهاری* شامل:

- روش ریسک (کمی و کیفی)،
- ملاحظات کارایی معیارهای امنیتی موجود یا برنامه‌ریزی شده،
- توانایی ارزیابی سطوح ریسک باقیمانده از معیارهای اضافی،

بوده که مکمل‌های الزامی برای نیازمندی‌های استانداردهای ISO/IEC 27000 و به‌خصوص ISO/IEC 27005 می‌باشد.

۳ـ۱ـ۵ مقایسه‌ی بین اهداف *مهاری* و استانداردهای ISO/IEC 27001 و 27002

اهداف *مهاری* و استانداردهای ISO که قبلاً به آنها اشاره شد اساساً متفاوت می‌باشد.

- هدف *مهاری* فراهم‌کردن روش‌ها و ابزارهایی برای انتخاب تمهیدات امنیتی مناسب در سازمان و ارزشیابی ریسک‌های باقیمانده در هنگام استفاده از این تمهیدات است. این موضوع جزو اهداف اصلی اشاره شده در استانداردهای ISO نیست.
- استانداردهای ISO یکسری از به‌روش‌ها را ارئه می‌کنند که مطمئناً سودمند بوده ولیکن لزوماً برای ذینفعان سازمان مناسب نبوده و مناسب جهت پوشش جنبه‌های بلوغ در امنیت، طرح‌ریزی امنیت اطلاعات، واحدهای داخلی مستقل و شرکا است.

سند «راهنمای مرجع خدمات امنیت» از *مهاری* عناصری جزئی را به صورت مؤثر تدارک می‌بیند که می‌توانند به منظور ساخت یک چارچوب در مقایسه با ISO/IEC 27002 مورد استفاده قرار گیرند. بدین صورت، مشخص است که فراگیری *مهاری* وسیع‌تر از ISO بوده و جنبه‌هایی از امنیت را فراتر از سیستم‌های اطلاعاتی پوشش می‌دهد.

۳ـ۲ سازگاری بین این رهیافت‌ها

رهیافت مهاری به طور کل قابل تلفیق با ISO/IEC 27002 است هرچند که یک هدف یکسان را دنبال نمی‌کنند ولیکن نمایش نتایج تحلیل‌های *مهاری* در قالب شاخص‌های ISO/IEC 27002 ساده است.
مهاری به نیازی که در استانداردهای ISO/IEC 27001 و 27002 تحت عنوان تحلیل ریسک اشاره شده است پاسخ داده و معیارهایی که باید تعریف شوند را مشخص می‌کند.

۳ـ۲ـ۱ سازگاری با استاندارد ISO/IEC 27002:2005

اهداف کنترلی یا همان به‌روش‌ها در ISO به صورت معیارهای عمومی، رفتاری یا سازمانی بوده و این در حالی است که در *مهاری* علاوه بر آنها، تأکید بر روی معیارهایی است که بتوان اثربخشی آنها را تضمین کرد.
علیرغم این تفاوت‌ها، بازنگری آسیب‌پذیری‌های *مهاری* یک جدول متناظر فراهم می‌کند که شاخص‌هایی را همسو با استاندارد ISO/IEC 27002:2005 مشخص می‌کند که برای افرادی که می‌خواهند سازگاری خود را با این استاندارد بیان کنند بکار می‌رود.
لازم به توضیح است که پرسش‌نامه‌های ممیزی *مهاری* به این منظور طراحی و ساخته شده‌اند که مدیران عملیاتی را قادر سازند تا بازنگری آسیب‌پذیری‌ها را به صورت اثربخش انجام داده و ظرفیت هر خدمت امنیتی را به منظور کاهش ریسک استنباط کنند.

۳ـ۲ـ۲ سازگاری با استاندارد ISO/IEC 27001

مهاری به آسانی با فرآیندهای چرخه‌ی PDCA (طرح‌ریزی ـ اجرا ـ بازبینی ـ اقدام) همانطور که در استاندارد ISO/IEC 27001 به ویژه در فاز طرح‌ریزی، اشاره شده است قابل یکپارچه‌سازی است. *مهاری* به صورت کامل، پوشش دهنده‌ی مشروح وظایفی است که به منظور ایجاد زیربنای سیستم مدیریت امنیت اطلاعات مورد نیاز است.
مهاری برای فاز اجرا که به منظور پیاده‌سازی و راهبری سیستم مدیریت امنیت اطلاعات است، عناصر شروع‌کننده‌ای مانند ساخت طرح‌های مدیریت ریسک را فراهم کرده است که به طور مستقیم با گروه‌بندی ریسک‌ها و تمهیدات بهبود مرتبط بوده و دارای اولویت هستند.

برای فاز بازبینی، *مهاری* عناصری را تدارک دیده است که ارزیابی ریسک‌های باقیمانده و بهود در تمهیدات امنیتی را میسر می‌کند. علاوه بر این، هر تغییری در محیط (ذینفعان، تهدیدات، راه‌کارها و سازمان) می‌تواند مجدداً توسط همان ممیزی‌هایی که در ابتدا از نتایج *مهاری* حاصل شده است باز ارزیابی شوند. بنابراین، طرح‌های امنیتی با گذشت زمان می‌توانند بهبود داده شده و تکامل یابند.

برای فاز اقدام، *مهاری* صراحتاً کنترل‌ها و بهبودهای امنیت مستمر را معرفی کرده است تا بدین ترتیب، اطمینان حاصل شود که اهداف کاهش ریسک برآورده شده‌اند. در این سه فاز، علیرغم اینکه *مهاری* در قلب این فرآیندها نیست، کمک شایانی به اجرا و اطمینان از کارایی آنها می‌کند.

۳-۲-۳ سازگاری با استاندارد ISO/IEC 27005:2008

چارچوبی که توسط این استاندارد تنظیم شده است می‌تواند به صورت کامل توسط *مهاری* برای مدیریت ریسک‌ها بکارگرفته شود، برای مثال:

- فرآیندهای تحلیل، ارزیابی و مقابله با ریسک (برگرفته از ISO 13335)،
- شناسایی دارایی‌های اولیه و ثانویه به همراه طبقه‌بندی سطوح مرتبط با آنها بعد از تحلیل ذینفعان،
- شناسایی تهدیدات به همراه سطح آنها که در آن *مهاری* دقت عمل بیشتری برای مشخص کردن سناریوهای ریسک دارد،
- شناسایی و تعریف کارایی تمهیدات امنیتی (یا کنترل‌ها) در کاهش آسیب‌پذیری‌ها،
- ترکیب این عناصر به منظور ارزیابی شدت سناریوهای ریسک در مقیاسی با چهار سطح،
- توانایی انتخاب مستقیم معیارهای امنیتی که برای طرح‌های مقابله با ریسک بکار می‌روند.

بنابراین، *مهاری* نه‌تنها به آسانی با فرآیندهای سیستم مدیریت امنیت اطلاعات که در ISO/IEC 27001 مشخص شده‌اند، یکپارچه‌سازی می‌شود، بلکه کاملاً با الزامات ISO/IEC 27005 به عنوان یک روش مدیریت ریسک سازگار است.

L'ESPRIT DE L'ÉCHANGE

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: