کتاب مرجع آموزش عرضی و کوتاه‌مدت

مباحث تخصصی پدافند سایبری

مؤلف : مهندس محمود خالقی‌دخت

عضو هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات

اسفند ۱۴۰۰

فصل سوّم

مخاطره سایبری

اهداف آموزشی پیش‌بینی شده برای این فصل، عبارتند از :

۱. کسب شناخت در خصوص تهدیدهای سایبری موجود علیه سرمایه‌های سایبری سازمان
۲. کسب شناخت در خصوص مخاطرات سایبری موجود علیه سرمایه‌های سایبری سازمان
۳. کسب شناخت و توانایی انتخاب روش مناسب برای ارزیابی مخاطرات امنیتی

پس از مطالعه‌ی این فصل، انتظار می‌رود با مطالب و مفاهیم زیر، مأنوس شده باشید :

۱. انواع مخاطرات سایبری موجود علیه سرمایه‌های سایبری سازمان
۲. ویژگی‌های مخاطرات سایبری
۳. روش‌های ارزیابی امنیتی فراگیر
٤. ویژگی‌های یک روش ارزیابی امنیتی مناسب برای یک سازمان

۱-۳- تعریف تهدید سایبری

تهدید[۱]، به پتانسیل بُروز یک حادثه‌ی ناخواسته اطلاق می‌گردد که ممکن است موجب وارد نمودن صدمه به یک سامانه، شخص یا سازمان شود. تهدید همچنین به هر پیشامد یا واقعه با پتانسیل وارد نمودن ضربه‌ی مضرّ به عملیات سازمانی، سرمایه‌های سازمانی، افراد، سایر سازمان‌ها یا کشور، با بهره‌گیری از یک سامانه‌ی اطلاعاتی، از طریق دسترسی غیرمجاز، نابودی، افشاء یا تغییر اطلاعات و یا ممانعت از خدمت اطلاق می‌شود. در تعریفی دیگر، به هر عامل داخلی یا

[۱] Threat

بیرونی، که قابلیت و یا نیّت نقض خط مشی امنیتی یک سرمایه سایبری، به قصد وارد نمودن ضربه به مؤلفه‌های امنیتی آن سرمایه را داشته باشد و یا اقدامی در این راستا انجام داده باشد، تهدید سایبری اطلاق می‌گردد.

انواع تهدیدهای سایبری موجود علیه شبکه‌ها، به سه دسته‌ی تهدیدهای گزنده، تهدیدهای مجرمانه و تهدیدهای ماندگار پیشرفته[۱] (APT) تفکیک می‌شوند. تهدیدهای گزنده، بیشترین فراوانی و احتمال وقوع را دارند ولی از توانایی کمی برخوردار بوده و صدمه‌ی کمی وارد می‌کنند، لیکن APTها، اگرچه کم‌ترین فراوانی و احتمال وقوع را دارند، ولی به دلیل توانایی بالا و اتّکاء به مهارت زیاد، قادر به ایجاد صدمات فاجعه‌بار و پرهزینه‌ای می‌باشند.

همان‌گونه که از تعریف تهدید سایبری استنباط می‌شود، تهدید سایبری به دو دسته‌ی کلی تهدیدهای داخلی (خودی‌ها[۲]) و تهدیدهای بیرونی قابل تفکیک است.

در کلی‌ترین حالت، انواع تهدید سایبری عبارت از منتشرکنندگان هرزنامه، هکرها[۳]، Crackerها و نویسندگان بدافزار، هکرهای دارای انگیزه سیاسی[۴]، مجرمین سایبری[۵]، Phisherها، مجرمین سازمان‌یافته سایبری[۶]، متصدیان شبکه‌های بات، نویسندگان جاسوس‌افزار، جاسوسان سایبری[۷] و تروریست‌های سایبری[۸]، مزدوران سایبری[۹] یا گروه‌های تحت حمایت پنهان دولت‌ها[۱۰] و نهایتاً دولت‌ها[۱۱] (دولت‌های متخاصم[۱۲]) می‌باشند.

۲-۳- مخاطرات امنیتی ناشی از تهدید سایبری

مخاطره در حالت عمومی، میزان قرارگرفتن یک موجودیت، تحت شرایط یا رویداد بالقوه‌ی تهدید است. مخاطره تابعی از احتمال وقوع و ضربه‌ی ناشی از وقوع آن شرایط یا رویداد است. مخاطره‌ی امنیتی[۱۳]، نتیجه‌ی عدم قطعیّت در تحقق اهداف امنیت یا میزان قرارگرفتن یک سرمایه سایبری، تحت شرایط یا رویداد بالقوه‌ی تهدید سایبری است. مخاطره‌ی امنیتی با دو ویژگی احتمال وقوع و شدّت ضربه‌ی ناشی از وقوع تهدید سایبری توصیف می‌شود. به عبارت دیگر مخاطره‌ی امنیتی، نتیجه‌ی مستقیم وجود یک یا چند تهدید امنیتی، علیه یک سرمایه‌ی سایبری است. احتمال وقوع مخاطره‌ی امنیتی، برابر با احتمال بهره‌برداری تهدید سایبری از یک یا چند آسیب‌پذیری موجود در سرمایه‌ی سایبری موردنظر است و شدّت مخاطره‌ی امنیتی، برابر با شدّت ضربه‌ی مضرّ ناشی از بهره‌برداری تهدید سایبری از آسیب‌پذیری[های] موجود در سرمایه‌ی سایبری موردنظر است.

---

۱ Advanced Persistent Threats (APT)
۲ Insiders
۳ Hackers
۴ Hacktivists
۵ Cyber Criminals
۶ Organized Cyber Criminals
۷ Cyber espionages
۸ Cyber terrorists
۹ Cyber mercenaries
۱۰ State sponsored groups
۱۱ Nation-state
۱۲ Hostile states
۱۳ Security Risk

ضربه[۱]، تأثیر مستقیم ناشی از بهره‌برداری تهدید سایبری از آسیب‌پذیری سایبری، بر سرمایه‌ی سایبری است که موجب وارد آمدن صدمه به مؤلفه‌های امنیتی آن سرمایه، اعم از محرمانگی، صحت یا دسترس‌پذیری می‌شود.

بر اساس این تعاریف، هر گاه یک یا چند تهدید سایبری علیه یک سرمایه سایبری وجود داشته باشد، آن‌گاه می‌توان گفت برای آن سرمایه سایبری، مخاطره‌ای وجود دارد که میزان آن مخاطره، با دو مؤلفه‌ی احتمال وقوع و شدت ضربه، تعیین می‌شود. بدیهی است چنانچه هیچ تهدیدی علیه یک سرمایه سایبری وجود نداشته باشد، آن سرمایه سایبری با هیچ مخاطره‌ای مواجه نیست.

یک هکر خودی (داخل سازمان)، از جمله یک کارمند ناراضی یا جاسوس، نسبت به یک هکر خارج از سازمان، دسترسی‌های بیشتری به سرمایه‌های سایبری سازمان دارد. زیرا هکر خودی در ساده‌ترین حالت، امکان دسترسی به شبکه‌ی سازمان با استفاده از حساب کاربری خود را دارد، در صورتی که یک هکر خارج از سازمان، از این امکان برخوردار نیست. به این ترتیب احتمال بهره‌برداری یک هکر خودی از آسیب‌پذیری موجود در شبکه‌ی سازمان، در حالت کلی (در صورت برخورداری از مهارت، توانایی و ابزارهای یکسان با هکر بیرونی)، بیشتر است و همین استدلال برای شدت ضربه نیز برقرار است. به عبارت دیگر، مخاطره‌ی امنیتی ناشی از یک هکر داخلی، بیش از مخاطره‌ی امنیتی ناشی از یک هکر بیرونی است.

۳-۳- ارزیابی مخاطرات امنیتی

ارزیابی امنیتی[۲] یا ارزیابی مخاطرات امنیتی[۳]، به تخمین میزان مخاطره‌ی امنیتی موجود علیه یک سرمایه سایبری یا به فرآیند مشخص‌کردن مقدار کمّی یا سطح کیفی مخاطره‌ی امنیتی آن سرمایه گفته می‌شود.

ارزیابی مخاطرات امنیتی، در کلی‌ترین حالت، می‌تواند بر اساس سه رویکرد تهدیدمحور[۴]، آسیب‌پذیری‌محور[۵] یا سرمایه‌محور[۶] (فناوری‌محور[۷]) انجام شود.

در ارزیابی مخاطرات امنیتی با رویکرد سرمایه‌محور، مخاطره‌ی امنیتی موجود علیه یک سرمایه سایبری مورد ارزیابی قرار می‌گیرد و برای این منظور، ابتدا تمام آسیب‌پذیری‌های موجود در داخل آن سرمایه سایبری و تمام تهدیدهای داخل و خارج از سازمان مورد شناسایی قرار می‌گیرند، سپس احتمال بهره‌برداری هر یک از تهدیدهای شناسایی شده از آسیب‌پذیری‌های شناسایی شده و شدّت ضربه‌ی ناشی از این بهره‌برداری احتمالی، محاسبه می‌شود و در انتها نیز میزان مخاطره‌ی ناشی از هر تهدید برای آن سرمایه سایبری، تعیین می‌شود. در صورتی که بخواهیم مخاطرات امنیتی استفاده از یک فناوری نوظهور از قبیل اینترنت اشیاء، رایانش ابری، زنجیره‌ی بلوکی، شبکه‌ی نرم‌افزارتعریف (SDN) یا نسل پنجم ارتباطات همراه (۵G) را مورد ارزیابی قرار دهیم نیز باید از این رویکرد برای ارزیابی مخاطرات امنیتی فناوری

---

۱ Impact
۲ Security Assessment
۳ Security Risk Assessment
۴ Threat-Oriented
۵ Vulnerability-Oriented
۶ Asset-Oriented
۷ Technology-Oriented

موردنظر، استفاده نمائیم. در این حالت، ابتدا لیستی از آسیب‌پذیری‌های فناوری موردنظر و لیستی از تهدیدهای موجود علیه این فناوری را احصاء می‌کنیم، سپس احتمال بهره‌برداری هر یک از تهدیدهای شناسایی شده از آسیب‌پذیری‌های شناسایی شده و شدّت ضربه‌ی ناشی از این بهره‌برداری احتمالی را محاسبه می‌کنیم و در انتها نیز میزان مخاطره‌ی ناشی از هر تهدید برای آن فناوری و میزان مخاطرات ناشی از تمام تهدیدها برای آن فناوری را تعیین می‌نمائیم.

در ارزیابی مخاطرات امنیتی با رویکرد آسیب‌پذیری‌محور، مخاطره‌ی امنیتی ناشی از یک آسیب‌پذیری مشخص موجود در یک سرمایه سایبری موردنظر می‌باشد. برای این منظور ابتدا تمام تهدیدهای داخل و خارج از سازمان مورد شناسایی قرار می‌گیرند، سپس احتمال بهره‌برداری هر یک از تهدیدهای شناسایی شده از آن آسیب‌پذیری مشخص و شدّت ضربه‌ی ناشی از این بهره‌برداری احتمالی، محاسبه می‌شود و در انتها نیز میزان مخاطره‌ی ناشی از هر تهدید برای آن سرمایه سایبری، تعیین می‌شود.

در ارزیابی مخاطرات امنیتی با رویکرد تهدیدمحور، مخاطره‌ی امنیتی ناشی از یک تهدید سایبری مشخص، برای تمام سرمایه‌های سایبری یک سازمان، مورد ارزیابی قرار می‌گیرد. برای این منظور، ابتدا تمام سرمایه‌های سایبری سازمان مورد شناسایی قرار می‌گیرند، سپس تمام آسیب‌پذیری‌های موجود در هر سرمایه سایبری شناسایی می‌شود، در ادامه احتمال بهره‌برداری تهدید مشخص موردنظر از هر یک از آسیب‌پذیری‌های شناسایی شده و شدّت ضربه‌ی ناشی از این بهره‌برداری احتمالی، محاسبه می‌شود و در خاتمه نیز میزان مخاطره‌ی ناشی از آن تهدید برای هر سرمایه‌ی سایبری سازمان و تمام سرمایه‌های سایبری سازمان تعیین می‌شود.

۴-۳- مراحل ارزیابی مخاطرات امنیتی

در تشریح روش ارزیابی مخاطرات امنیتی با رویکردهای مختلف، مراحل یکسانی برای ارزیابی مخاطرات امنیتی برشمردیم. این مراحل یکسان در شکل (۳-۱) نمایش داده شده‌اند. بر اساس این شکل، ارزیابی مخاطرات امنیتی در سه گام اصلی با عناوین «برنامه‌ریزی»، «شناسایی» و «تحلیل و تخمین» انجام می‌شود.

گام اوّل : برنامه‌ریزی

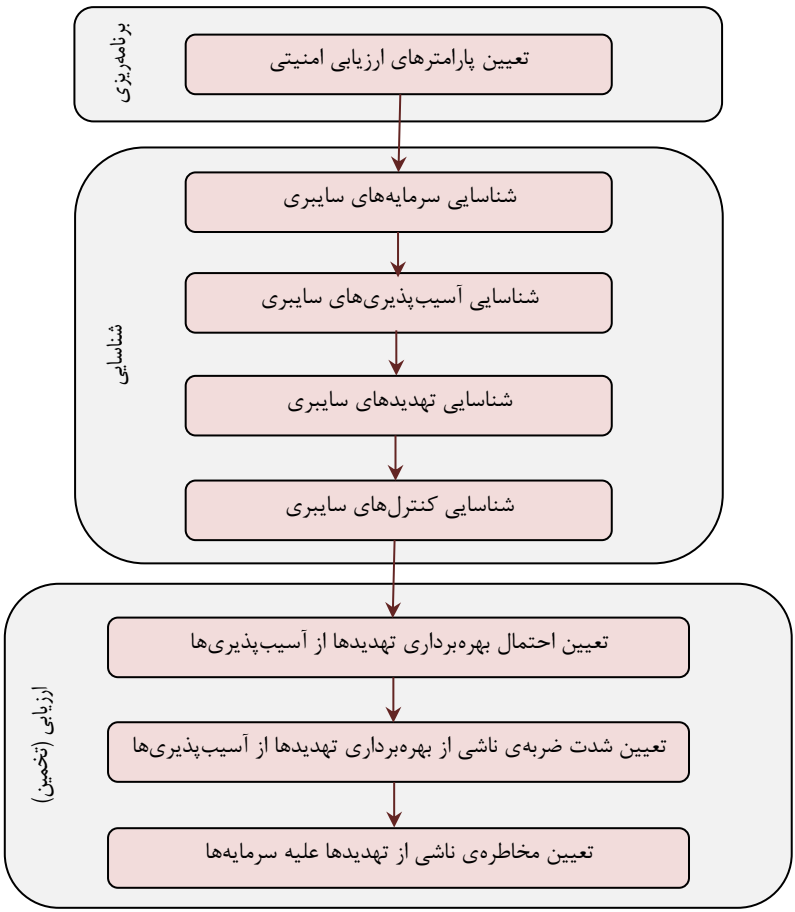
در این گام، پارامترهای ارزیابی امنیتی، از قبیل پارامترهای کلی ارزیابی (رویکرد ارزیابی، سطح ارزیابی و قلمرو ارزیابی)، پارامترهای شناسایی (رویکرد شناسایی و روش شناسایی) و پارامترهای تحلیل (رویکرد تحلیل و روش تحلیل) تعیین و بر اساس این پارامترها، روش مناسب ارزیابی امنیتی انتخاب می‌شود.

گام دوّم : شناسایی

در این گام، سرمایه‌های سایبری سازمان، آسیب‌پذیری‌های موجود در هر سرمایه سایبری، تهدیدهای موجود علیه هر سرمایه سایبری و کنترل‌های امنیتی هر سرمایه سایبری شناسایی می‌شوند.

گام سوّم : ارزیابی (تخمین)

در این گام، ابتدا احتمال بهره‌برداری تمام تهدیدهای شناسایی شده از تمام آسیب‌پذیری‌های شناسایی شده در تمام سرمایه‌های سایبری تعیین می‌شوند. در ادامه شدّت ضربه‌ی ناشی از بهره‌برداری تمام تهدیدهای شناسایی شده از تمام آسیب‌پذیری‌های شناسایی شده در تمام سرمایه‌های سایبری تعیین می‌شوند. در خاتمه نیز میزان مخاطره امنیتی ناشی از بهره‌برداری تمام تهدیدهای شناسایی شده از تمام آسیب‌پذیری‌های شناسایی شده در تمام سرمایه‌های سایبری تخمین زده می‌شوند.



شکل (۳-۱) : مراحل ارزیابی مخاطرات امنیتی

۵-۳- پارامترهای ارزیابی مخاطرات امنیتی

به‌منظور انتخاب روش مناسب برای ارزیابی امنیتی، لازم است ابتدا پارامترهای ارزیابی امنیتی را تعیین کنیم. پارامترهای ارزیابی امنیتی، در سه دسته‌ی «پارامترهای کلی ارزیابی»، «پارامترهای شناسایی» و «پارامترهای تحلیل» قابل دسته‌بندی هستند.

دسته‌ی اول : پارامترهای کلی ارزیابی

پارامترهای کلی ارزیابی، شامل سه پارامتر رویکرد ارزیابی، سطح ارزیابی و قلمرو ارزیابی است.

پارامتر (۱-۱) : رویکرد ارزیابی

ارزیابی مخاطرات امنیتی، در کلی‌ترین حالت، می‌تواند بر اساس سه رویکرد تهدیدمحور، آسیب‌پذیری‌محور یا سرمایه‌محور انجام شود. رویکرد متعارف برای ارزیابی مخاطرات امنیتی سازمان، رویکرد سرمایه‌محور است که در آن لیست سرمایه‌های سایبری تعیین می‌شود و در ادامه، به‌ازاء هر سرمایه سایبری، تمام تهدیدهای موجود علیه آن سرمایه و تمام آسیب‌پذیری‌های آن سرمایه شناسایی می‌شوند و بر اساس مراحل مطرح شده، مخاطره‌ی موجود علیه هر سرمایه تخمین زده می‌شوند. در خاتمه نیز مخاطره تجمعی موجود علیه تمام سرمایه‌ها تخمین زده می‌شوند.

پارامتر (۱-۲) : قلمرو ارزیابی

قلمرو ارزیابی، بخشی از فضای سایبر سازمان است که عملیات ارزیابی مخاطرات امنیتی، بر روی آن انجام می‌گیرد. این قلمرو، ممکن است یک سامانه‌ی اطلاعاتی، شبکه‌ی سازمان یا فرآیندهای سازمانی باشد. سرمایه‌های سایبری یک سازمان، شامل یک یا چند شبکه ارتباطی سازمانی، مجموعه‌ای از فرآیندهای سازمانی و مجموعه‌ای از سامانه‌های اطلاعاتی هستند. ممکن است بخواهیم ارزیابی مخاطرات امنیتی را برای تمام یا بخشی از این سرمایه‌ها انجام دهیم، لذا ابتدا باید قلمرو ارزیابی امنیتی را مشخص کنیم.

پارامتر (۱-۳) : سطح ارزیابی

ارزیابی امنیتی، ممکن است در یکی از سطوح راهبردی، عملیاتی و فنی انجام شود.

ارزیابی امنیتی در سطح راهبردی، صرفاً بر سرمایه‌های راهبردی، تهدیدهای راهبردی و آسیب‌پذیری‌های راهبردی تمرکز دارد. مخاطره‌ی امنیتی راهبردی، مخاطره‌ای است که در صورت وقوع، نابودی یا ایجاد اختلال اساسی و طولانی‌مدّت در عملکرد سرمایه‌های سایبری سازمان را در پی داشته باشد. در این حالت، مخاطرات امنیتی مورد توجه خواهند بود که تحمّل‌ناپذیر بوده و منجر به پیامدهای فاجعه‌بار، برگشت‌ناپذیر یا غیر قابل ترمیم شوند.

ارزیابی امنیتی در سطح عملیاتی، ارزیابی است که بر عملکرد سرمایه‌های سایبری سازمان تمرکز دارد. مخاطره‌ی امنیتی عملیاتی، مخاطره‌ای است که در صورت وقوع، ایجاد اختلال مقطعی (زمان محدود) یا موضعی (اجزاء محدود) در عملکرد یا خدمت‌رسانی سرمایه‌های سایبری سازمان را در پی داشته باشد. در این حالت، مخاطرات امنیتی مورد توجه

خواهند بود که تحمّل‌پذیر بوده و منجر به پیامدهای برگشت‌پذیر (قابل ترمیم) در عملکرد سرمایه‌های سایبری سازمان شوند.

ارزیابی امنیتی در سطح فنی، ارزیابی است که بر ویژگی‌های فنی سرمایه‌های سایبری سازمان تمرکز دارد و مخاطره‌ی امنیتی فنی نیز مخاطره‌ای است که در صورت وقوع، ایجاد اختلال در روش‌ها و تکنیک‌های فنی بکار گرفته شده در سرمایه‌های سایبری سازمان را برای یک مقطع زمانی یا محدوده‌ی منطقی، در پی داشته باشد.

دسته‌ی دوم : پارامترهای شناسایی

پارامترهای شناسایی، شامل دو پارامتر رویکرد شناسایی و روش شناسایی است.

پارامتر (۲-۱) : رویکرد شناسایی

رویکرد شناسایی سرمایه سایبری، آسیب‌پذیری سایبری، تهدید سایبری و کنترل سایبری، می‌تواند مبتنی بر اطلاعات «کتابخانه‌ای یا مستندشده» و یا مبتنی بر اطلاعات «واقعی یا وضعیت جاری» باشد. این پارامتر را با یک مثال تشریح می‌کنیم. در شناسایی آسیب‌پذیری یک سرمایه سایبری بر اساس رویکرد مبتنی بر اطلاعات کتابخانه‌ای، آسیب‌پذیری‌های سایبری آن سرمایه سایبری، از پایگاه‌های داده آسیب‌پذیری استخراج می‌شوند، لیکن برای شناسایی آسیب‌پذیری‌های سایبری یک سرمایه سایبری بر اساس رویکرد مبتنی بر اطلاعات واقعی، لازم است وضعیت جاری آن سرمایه سایبری مورد بررسی قرار گیرد. در رویکرد اول تمام آسیب‌پذیری‌های ممکن شناسایی می‌شوند ولی در رویکرد دوم تنها آسیب‌پذیری‌هایی شناسایی می‌شوند که قبلاً رفع نشده‌اند و در حال حاضر وجود دارند.

پارامتر (۲-۲) : روش شناسایی

شناسایی و جمع‌آوری اطلاعات یک سرمایه، آسیب‌پذیری یا تهدید سایبری می‌تواند با روش وارسی، اظهار یا آزمون انجام شود. در روش مبتنی بر اظهار، از فرم‌های جمع‌آوری اطلاعات، مصاحبه یا نظایر آن‌ها استفاده می‌شود. در روش مبتنی بر آزمون، یک نرم‌افزار شناسایی سرمایه سایبری مورد استفاده قرار می‌گیرد و از طریق ارسال و دریافت اطلاعات و انجام تعدادی آزمون، اطلاعات مربوط به سرمایه، آسیب‌پذیری یا تهدید شناسایی می‌شود.

دسته‌ی سوم : پارامترهای تحلیل

پارامترهای تحلیل شامل دو پارامتر رویکرد تحلیل و روش تحلیل است.

پارامتر (۳-۱) : رویکرد تحلیل

تحلیل مخاطره، با سه رویکرد کمّی، کِیفی و شبه‌کمّی انجام می‌گیرد. در رویکرد کیفی برای توصیف وضعیت مخاطره، از تعداد فرد عبارات کیفی مانند کم، زیاد، متوسط، خیلی‌کم و خیلی‌زیاد استفاده می‌شود. در رویکرد کمّی، برای توصیف وضعیت مخاطره، از مقادیر عددی استفاده می‌شود و در رویکرد شبه‌کمّی، این توصیف با بهره‌گیری از عبارات

کیفی منتسب‌شده به سطوح کمّی‌شده، بیان می‌شود. برای ارزیابی امنیتی سرمایه‌های سایبری سازمانی، بهتر است از رویکرد تحلیل شبه‌کمّی استفاده کنیم تا هم پیچیدگی تحلیل کم‌تر باشد و هم امکان کمّی‌سازی مقادیر مخاطره وجود داشته باشد. ضمناً برای ارزیابی مخاطرات امنیتی در سطح سازمانی، بهتر است تعداد سطوح مخاطره را سه سطح در نظر بگیریم ولی در ارزیابی مخاطرات امنیتی سطح ملی، باید حداقل از پنج سطح استفاده نمائیم. در تعیین تعداد سطوح ارزیابی، دو پارامتر حداقل شدن پیچیدگی عملیات و قابل‌پذیرش بودن دقت، باید مورد توجه قرار گیرند.

پارامتر (۳-۲) : روش تحلیل

روش‌ها یا تکنیک‌های زیادی برای تحلیل وجود دارند، لیکن فراگیرترین روش‌های تحلیل، عبارت از تحلیل مبتنی بر داده‌کاوی (تحلیل محتوایی)، تحلیل مبتنی بر مدل و تحلیل مبتنی بر خبرگی است.

۶-۳- آشنایی با یک روش فراگیر ارزیابی مخاطرات امنیتی

روش‌های زیادی برای ارزیابی مخاطرات امنیتی وجود دارند لیکن بر اساس پارامترهایی که در مرحله برنامه‌ریزی تعیین می‌شوند تعداد محدودی از این روش‌ها برای ارزیابی مخاطرات امنیتی سرمایه‌های سایبری موردنظر با رویکرها و روش‌های تعیین‌شده کاربرد خواهند داشت.

بالغ بر ۴۵ متدولوژی ارزیابی مخاطرات امنیتی توسط شرکت‌ها، دولت‌ها و مؤسسات استاندارد ملی و بین‌المللی ارائه شده‌اند. تعدادی از متدولوژی‌ها در کشورهای اروپایی مورد استفاده قرار می‌گیرند که توسط آژانس امنیت اطلاعات و شبکه‌ی اروپا[۱] (ENISA) به عنوان متدولوژی‌های مورد تائید جهت استفاده در کشورهای عضو اتحادیه اروپا، معرفی شده‌اند. آژانس ENISA در جایگاه مرکز مدیریت راهبردی امنیت اطلاعات و شبکه در اتحادیه اروپا قرار دارد و یک کارگروه ویژه در حوزه‌ی ارزیابی مخاطرات امنیتی دارد که هدف آن، برآورد وضعیت امنیت سایبری در برنامه‌ی Cyber Security اتحادیه اروپا است.

سازمان تحقیق و فناوری ناتو[۲] که در کنار مرکز مشارکت نخبگان دفاع سایبری[۳] (CCD-COE) ناتو، نقش مشابه ENISA در حوزه‌ی Cyber Defence را برای ناتو ایفا می‌نمایند نیز در بررسی دیگری که با هدف ایجاد یک متدولوژی مشترک برای ارزیابی مخاطرات امنیتی انجام داده است، ضمن بررسی متدولوژی‌های معرفی شده توسط ENISA، از جمله متدولوژی‌های CRAMM، Ebios، TRA، MAGERIT، نسخه اول استاندارد NIST SP ۸۰۰-۳۰ و Common

۱ European Network and Information Security Agency (ENISA)

۲ Research and Technology Organization of NATO (R&TO)

۳ Cooperative Cyber Defence Centre of Excellence (CCD-COE)

Criteria، یک چارچوب مشترک[۱]، برای ارزیابی مخاطرات امنیتی، ارائه نموده است. چارچوب پیشنهادی، بر اساس متدولوژی‌های مورد بررسی، طراحی شده است و حاوی فصل مشترک تقریباً همه‌ی روش‌های موجود است.

در میان تمام این متدولوژی‌ها، تنها یک متدولوژی وجود دارد که قابلیت ارزیابی امنیتی با هر سه رویکرد سرمایه‌محور، آسیب‌پذیری‌محور و تهدیدمحور را دارد. این متدولوژی همچنین قابلیّت استفاده‌ی هم‌زمان برای ارزیابی امنیتی در هر سه سطح فنی، عملیاتی و راهبردی، قابلیت ارزیابی امنیتی انواع قلمروها اعم از سامانه‌های اطلاعاتی، شبکه و سازمان و قابلیت ارزیابی امنیتی انواع موضوعات، اعم از تهدید، آسیب‌پذیری و مخاطره را دارد. این متدولوژی، با عنوان "راهنمای هدایت برآورد مخاطرات"، توسط مؤسسه استاندارد و فناوری ایالات متحده آمریکا، در قالب مستند ویژه‌ی NIST SP ۸۰۰-۳۰ منتشر شده است که نوعی از استانداردهای ملی ایالات متحده آمریکا تلقی می‌شوند.

در ادامه این بخش، کلیاتی از متدولوژی ارزیابی مخاطرات امنیتی ارائه شده در قالب "راهنمای هدایت برآورد مخاطرات"، معرفی شده است.

۱-۶-۳. ویژگی‌های متدولوژی NIST SP ۸۰۰-۳۰

متدولوژی ارائه‌شده در مستند ویژه‌ی شماره ۳۰-۸۰۰ مؤسسه ملی استاندارد و فناوری ایالات متحده که در سپتامبر سال ۲۰۱۲ ارائه شده است، نسخه‌ی بازنگری اوّل مستند ویژه‌ای است که با عنوان "راهنمای مدیریت مخاطرات برای سامانه‌های فناوری اطلاعات"، با همین شماره ۳۰-۸۰۰ در جولای سال ۲۰۰۲ ارائه شد. نسخه‌ی سال ۲۰۰۲ این استاندارد، صرفاً برای ارزیابی مخاطرات امنیتی در سطح فنی، در حوزه‌ی سامانه‌های اطلاعاتی با نگرش تحلیل کیفی قابل استفاده بود، لیکن متدولوژی ارائه‌شده در مستند ویژه‌ای که با عنوان "راهنمای هدایت برآورد مخاطرات"، با شماره ۳۰-۸۰۰ توسط مؤسسه ملی استاندارد و فناوری ایالات متحده در سپتامبر ۲۰۱۲ ، ارائه گردید، چند تغییر اساسی شامل افزودن قابلیّت استفاده‌ی هم‌زمان برای ارزیابی انواع موضوعات در انواع قلمروها با انواع رویکردها و در کلیه سطوح، نسبت به نسخه‌ی قبل دارد.

مدل مخاطره

در این متدولوژی، مدل مخاطره، مطابق شکل (۳-۲)، ارائه شده است. بر اساس این مدل، یک منشاء تهدید با ویژگی‌های (توانایی، انگیزه، آماج و محدوده‌ی اثر) با احتمال[۲] مشخصی یک رویداد تهدید[۳] را آغاز نموده و رشته‌ای[۴]

---

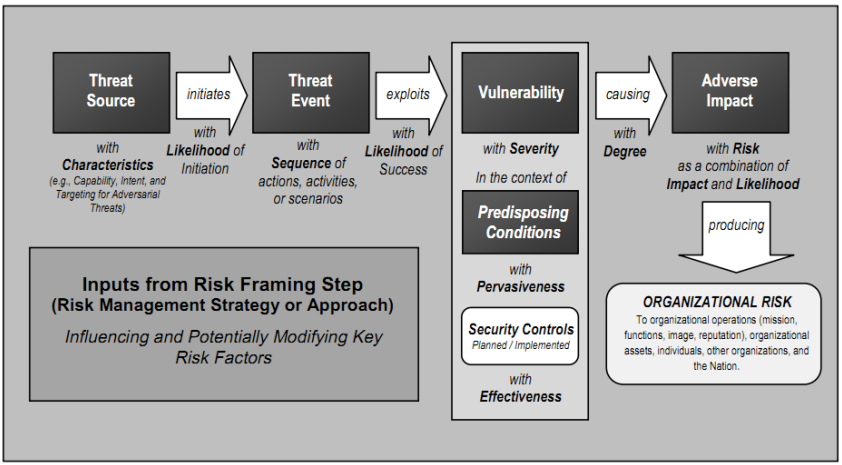
۱ Common Framework

۲ Likelihood

۳ Threat Event

۴ Sequence

از اقدام[۱]ها، فعالیت[۲]ها یا سناریو[۳]ها را انجام می‌دهد و با احتمال موفقیّت[۴]ی، از یک یا چند آسیب‌پذیری بهره‌برداری[۵] خواهد نمود. آسیب‌پذیری موردنظر، از میزانی از سختی[۶] برخوردار است و در شرایط از پیش فراهم شده[۷] (مهیّا)، با استفاده از کنترل‌های امنیتی فراگیر و اثربخش[۸] محافظت شده است. این بهره‌برداری، با درجه[۹]ای از انگیزه[۱۰] انجام شده و میزانی از مخاطره را ایجاد خواهد نمود که در صورت وقوع، ضربه[۱۱]ی مضر[۱۲]ی را وارد خواهد نمود. میزان مخاطره، ناشی از شدّت ضربه و احتمال وقوع آن می‌باشد.



شکل (۳-۲) : مدل مخاطره در متدولوژی ارزیابی مخاطرات امنیتی NIST SP ۸۰۰-۳۰

رویکرد ارزیابی

این متدولوژی، ارزیابی را به صورت هم‌زمان، با دو رویکرد کیفی و شبه‌کمّی انجام می‌دهد. تمامی ویژگی‌ها در جداولی با سطوح کیفی ۵ سطحی و مقادیر کمّی نظیر آنها در دو رنج صفر تا ۱۰۰ و صفر تا ۱۰ توصیف می‌شوند. از جمله در جدول (۳-۱)، معرفی و توصیف سطوح احتمال وقوع مخاطره در این متدولوژی، نشان داده شده است. بر اساس این

---

۱ Action
۲ Activity
۳ Scenario
۴ Success
۵ Exploit
۶ Severity
۷ Predisposing
۸ Effectiveness
۹ Degree
۱۰ Cause
۱۱ Impact
۱۲ Adverse

جدول، احتمال وقوع به ۵ سطح خیلی‌کم، کم، متوسط، زیاد و خیلی‌زیاد، تفکیک شده است که در ستون سمت چپ نمایش داده شده‌اند، همچنین در توصیف این سطوح، که در ستون سمت راست نشان داده شده است، از واژه‌های کیفی خیلی‌غیرمحتمل، غیرمحتمل، تاحدی‌محتمل، خیلی‌محتمل و تقریباًمعین (قریب‌الوقوع) استفاده شده است و رنج این سطوح در مقیاس صفر تا ۱۰۰، برای هر سطح، مشخص و در ستون دوم از سمت چپ نمایش داده شده است. بر این اساس، مثلاً سطح متوسط، از مقادیر کمّی ۲۱ تا ۷۹ را در بر می‌گیرد. همچنین در ستون سوم از سمت چپ، مقادیر متناظر سطوح مذکور، در مقیاس ۱۰ به منظور استفاده در محاسبات، مشخص شده‌اند. مثلاً برای سطح متوسط، عدد ۵ در نظر گرفته شده است.

این روش سطح‌بندی و مقداردهی به موضوعات، کامل‌ترین شیوه در میان متدولوژی‌های ارزیابی مخاطرات امنیتی است و قابلیّت استفاده تا سطح ملی را دارد و یکی از نقاط قوت و ویژگی‌های شاخص این متدولوژی محسوب می‌گردد.

جدول (۳-۱) : معرفی و توصیف سطوح احتمال وقوع مخاطره

توصیف	مقادیر شبه‌کمّی		مقادیر کیفی
وقوع رویداد تهدید توسط دشمن، تقریباًمعین (قریب‌الوقوع) است	۱۰	۹۶-۱۰۰	خیلی‌زیاد
وقوع رویداد تهدید توسط دشمن، خیلی‌محتمل است	۸	۸۰-۹۵	زیاد
وقوع رویداد تهدید توسط دشمن، تاحدی‌محتمل است	۵	۲۱-۷۹	متوسط
وقوع رویداد تهدید توسط دشمن، غیرمحتمل است	۲	۵-۲۰	کم
وقوع رویداد تهدید توسط دشمن، خیلی‌غیرمحتمل است	۰	۰-۴	خیلی‌کم

رویکرد تحلیل

این متدولوژی، تحلیل را با سه رویکرد تهدیدمحور، سرمایه‌محور و آسیب‌پذیری‌محور انجام می‌دهد.

در رویکرد تهدیدمحور، پس از مرحله‌ی شناسایی تهدیدها و شناسایی وقایع تهدید، بر توسعه‌ی سناریوهای تهدید متمرکز می‌شود و از رهگذر سناریوهای تهدید، نحوه‌ی وقوع تهدید را پیش‌بینی می‌نماید. در این رویکرد که برای برآورد تهدیدهای خصمانه استفاده می‌شود، آسیب‌پذیری‌ها از متن تهدید[۱] و ضربه[۲] بر اساس نیّت تهدید شناسایی می‌شوند.

در رویکرد آسیب‌پذیری‌محور، تحلیل با در نظر گرفتن تعدادی آسیب‌پذیری موجود در سامانه‌های اطلاعاتی یا فرآیندهای سازمانی آغاز می‌شود و در ادامه، وقایع تهدید با تلاش منشاء تهدید برای دست‌یابی به یک یا چند آسیب‌پذیری و بهره‌برداری از آنها ادامه می‌یابند.

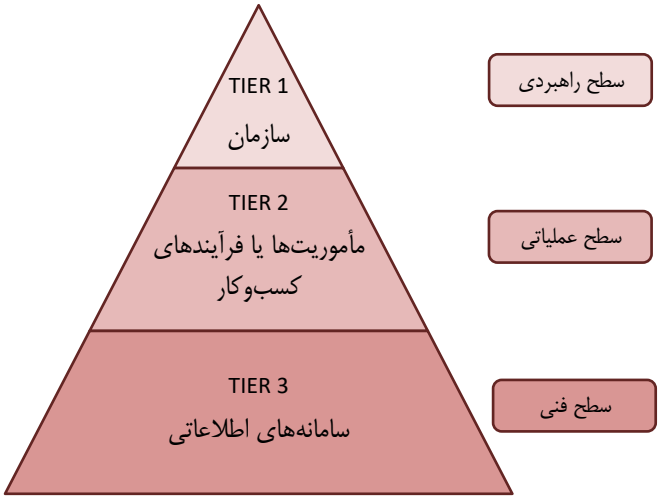
۱ Threay Context

۲ Impact

در رویکرد سرمایه‌محور نیز تحلیل با شناسایی ضربات یا پیامدهای وارده به سرمایه‌های کلیدی سازمان آغاز می‌شود و در صورت امکان با تحلیل ضربه‌ی وارده بر مأموریت سازمانی ادامه می‌یابد و نهایتاً با شناسایی وقایع تهدیدی که می‌توانند توسط منشاء تهدیدها انجام شوند و ضربات یا پیامدهای مذکور را ایجاد نمایند، خاتمه می‌یابد.

سطح ارزیابی

در این متدولوژی، مطابق شکل (۳-۳)، تهدیدها و مخاطرات امنیتی به سه رده[۱] تفکیک شده‌اند و از آنها با عناوین «راهبردی»، «عملیاتی» و «فنی» نام برده است.



شکل (۳-۳) : سطوح مخاطرات و ارزیابی مخاطرات

ارزیابی مخاطرات امنیتی در سطح فنی، بر روی سامانه‌های اطلاعاتی انجام می‌شود و مخاطرات فنی موجود علیه موجودیت یا فعالیت این سامانه‌های اطلاعاتی را شناسایی می‌کند.

ارزیابی مخاطرات امنیتی در سطح عملیاتی، بر روی مأموریت‌ها، خدمات و فرآیندهای کسب‌وکار انجام می‌گیرد و مخاطرات عملیاتی علیه تحقق مأموریت‌ها، تداوم خدمات و اجرای فرآیندهای کسب‌وکار سازمان را تعیین می‌نماید.

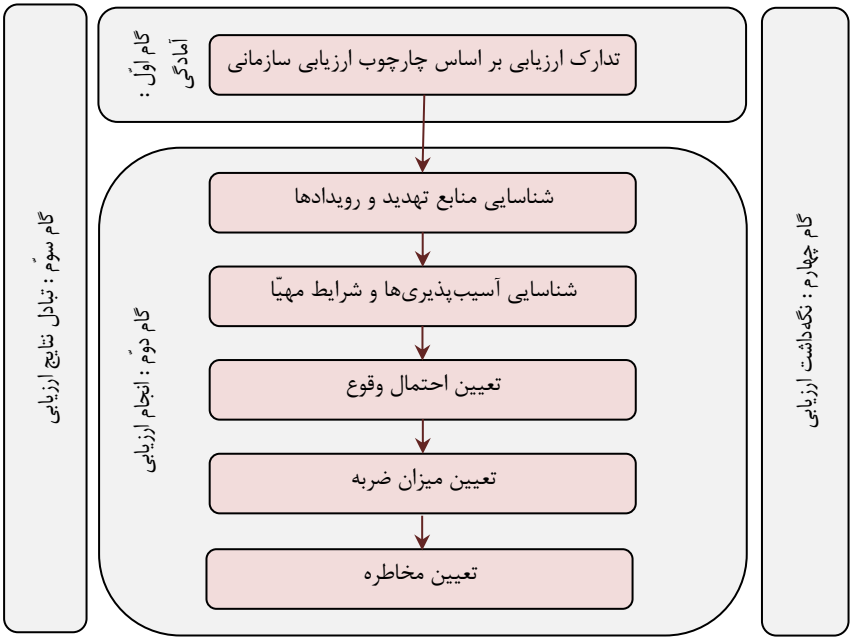
ارزیابی مخاطرات امنیتی در سطح راهبردی یا سازمانی نیز بر روی راهبردها، خط‌مشی‌ها، استانداردها، دستورالعمل‌ها و برنامه‌های سازمان انجام می‌گیرد. تمرکز این نوع ارزیابی بر مخاطرات موجود علیه موجودیت، سرمایه‌ها و پرسنل سازمان است و تأثیرات آنها را بر راهبردها و سیاست‌های سازمان مشخص می‌کند.

---

۱ TIER

۲-۶-۳. مراحل ارزیابی مخاطرات امنیتی بر اساس متدولوژی NIST SP ۸۰۰-۳۰

فصل سوم نسخه‌ی بازنگری‌شده‌ی مستند ویژه ۳۰-۸۰۰ مؤسسه ملی استاندارد و فناوری ایالات متحده، با عنوان راهنمای هدایت برآورد مخاطرات، فرآیند ارزیابی مخاطرات در متدولوژی ارائه‌شده را مطابق شکل (۳-۴)، معرفی نموده است :



شکل (۳-۴) : فرآیند ارزیابی مخاطرات

بر این اساس، فرآیند ارزیابی مخاطرات، از ۴ مرحله به شرح ذیل، تشکیل شده است :

مرحله (۱) : آماده‌سازی (تدارک) برای ارزیابی

در این مرحله، فعالیت‌های مقدماتی موردنیاز برای ارزیابی امنیتی انجام می‌شوند. نتایج این فعالیت‌ها در قالب چارچوب ارزیابی مخاطرات سازمان انجام می‌گیرند. این اقدامات، عبارتند از :

اقدام ۱-۱ : شناسایی هدف ارزیابی

هدف ارزیابی امنیتی، تصمیم‌هایی است که ارزیابی باید از آنها پشتیبانی کند. ارزیابی امنیتی ممکن است با هدف شناسایی و رفع مخاطرات خیلی‌شدید انجام شود. در این حالت، تمرکز ارزیابی بر سرمایه‌های سایبری کلیدی، آسیب‌پذیری‌های فاجعه‌بار و تهدیدهای پیشرفته‌ی مانا (APT) خواهد بود زیرا مخاطره‌ی شدید امنیتی، از دو ویژگی احتمال وقوع بسیارزیاد و شدت ضربه‌ی بسیارزیاد (فاجعه‌بار) برخوردار است. امّا چنانچه هدف ارزیابی امنیتی، شناسایی و رفع کلیه مخاطرات امنیتی غیر قابل پذیرش باشد، لازم است کلیه سرمایه‌های سایبری، کلیه آسیب‌پذیری‌های سایبری این سرمایه‌ها و کلیه تهدیدهای موجود علیه این سرمایه‌ها مورد شناسایی و تحلیل قرار گیرند و هر مخاطره‌ای که شدیدتر از حد قابل پذیرش (مثلاً شدت ۲٪ یا حداکثر ۵٪) بود، مدیریت شود. مدیریت مخاطره ممکن است از طریق رفع مخاطره، انتقال مخاطره، اجتناب از بروز مخاطره یا پذیرش مخاطره انجام گیرد.

اقدام ۱-۲ : شناسایی قلمرو ارزیابی

قلمرو ارزیابی، با توجه به کاربردپذیری سازمانی، چارچوب زمانی اثربخشی و ملاحظات فناورانه تعیین می‌شود. قلمرو ارزیابی، بخشی از سرمایه‌های سایبری سازمان است که برای تحقق هدف ارزیابی، تصمیم داریم آن‌ها را مورد ارزیابی قرار دهیم. اگرچه در حالت کلی تمام سرمایه‌های سایبری سازمان مورد ارزیابی امنیتی قرار می‌گیرند، لیکن ممکن است ارزیابی امنیتی قبلاً انجام شده باشد و پس از مدتی یک سامانه اطلاعاتی جدید بخواهد وارد شبکه سازمان شود. در این حالت لازم است پس از اتصال سامانه اطلاعاتی جدید به شبکه سازمان، این سامانه اطلاعاتی در حالت عملیاتی مورد ارزیابی امنیتی قرار گیرد. در این حالت، قلمرو ارزیابی صرفاً شامل سامانه اطلاعاتی موردنظر خواهد بود.

اقدام ۱-۳ : شناسایی الزامات و محدودیت‌های ارزیابی

در این متدولوژی، الزامات و محدودیت‌های ارزیابی، شامل منابع تهدید، وقایع تهدید، آسیب‌پذیری‌ها و شرایط مهیّا، سطوح احتمال، شدت ضربات، تحمّل مخاطره و عدم قطعیت، رویکرد ارزیابی و رویکرد تحلیل است.

اقدام ۱-۴ : شناسایی منابع اطلاعاتی مورد استفاده به عنوان ورودی ارزیابی

شامل منابع توصیفی تأمین اطلاعات تهدیدها، آسیب‌پذیری‌ها و ضربه‌های احتمالی است. خروجی این اقدام، در قالب جداولی ارائه می‌شود که به ترتیب منابع شناسایی منشاء تهدید، وقایع تهدید، آسیب‌پذیری‌ها، محاسبه‌ی ضربه و مخاطره را نشان می‌دهند.

اقدام ۱-۵ : شناسایی مدل مخاطره، رویکرد ارزیابی و رویکرد تحلیل

در این اقدام، مدل مناسب برای مخاطره و رویکرد مناسب برای ارزیابی و تحلیل، انتخاب می‌شود. این پارامترها، در بخش قبل مورد بررسی قرار گرفته‌اند.

مرحله (۲) : اجرای ارزیابی

در این مرحله، فعالیت‌های اصلی ارزیابی انجام می‌گیرد. اقدامات این مرحله، عبارتند از :

اقدام ۲-۱ : شناسایی منابع تهدید و ویژگی‌های آنها شامل قابلیّت، نیّت و هدف‌گیری برای تهدیدهای خصمانه و بُرد تأثیرات برای تهدیدهای غیرخصمانه

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

۱. شناسایی منابع تهدید (ورودی‌ها)
۲. تعیین مرتبط بودن منبع تهدید با سازمان و در قلمرو ارزیابی بودن منبع تهدید
۳. ایجاد یا به‌روزرسانی ارزیابی منابع تهدید (به تفکیک برای منابع تهدید خصمانه و منابع تهدید غیرخصمانه) برای منابع تهدید خصمانه، ابتدا قابلیت، نیت و هدف‌گیری منبع تهدید مورد ارزیابی قرار می‌گیرد و در ادامه، ارزیابی منابع تهدید انجام می‌شود. برای منابع تهدید غیرخصمانه نیز ابتدا بُرد تأثیرات منابع تهدید تعیین می‌شود و در ادامه، ارزیابی منابع تهدید صورت می‌گیرد.

اقدام ۲-۲ : شناسایی وقایع تهدید بالقوه و منابع تهدیدی که می‌توانند این وقایع را آغاز کنند

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

۱. شناسایی ورودی‌های واقعه‌ی تهدید
۲. شناسایی وقایع تهدید (به تفکیک برای منابع تهدید خصمانه و غیرخصمانه)
۳. شناسایی منابع تهدیدی که می‌توانند وقایع تهدید را آغاز کنند
٤. ارزیابی ربط وقایع تهدید به سازمان

اقدام ۲-۳ : شناسایی آسیب‌پذیری‌ها و شرایط مهیّا

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

۱. شناسایی ورودی‌های آسیب‌پذیری‌ها و شرایط مهیّا
۲. شناسایی آسیب‌پذیری‌ها، با استفاده از منابع اطلاعاتی تعیین‌شده
۳. ارزیابی شدت آسیب‌پذیری‌های شناسایی شده
٤. شناسایی شرایط مهیّا (شرایطی که فرصت بهره‌برداری تهدیدهای شناسایی شده از آسیب‌پذیری‌های شناسایی شده را فراهم می‌کند)
٥. ارزیابی فراگیری شرایط مهیّا

٦. به‌روز رسانی اطلاعات مخاطرات خصمانه یا مخاطرات غیرخصمانه

اقدام ۲-۴ : تعیین احتمال اینکه وقایع تهدید، موجب ایجاد ضربات خصمانه شوند

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

١. شناسایی ورودی‌های تعیین احتمال

٢. شناسایی فاکتورهای تعیین احتمال با استفاده از منابع اطلاعاتی تعیین‌شده (از قبیل ویژگی‌های منابع تهدید، آسیب‌پذیری‌ها و شرایط مهیّا)

٣. ارزیابی احتمال آغاز واقعه‌ی تهدید برای تهدیدهای خصمانه و احتمال وقوع واقعه‌ی تهدید برای تهدیدهای غیرخصمانه

٤. ارزیابی احتمال وقوع ضربات خصمانه در اثر وقایع تهدید، احتمال شروع یا وقوع

٥. ارزیابی احتمال کلی آغاز یا وقوع واقعه‌ی تهدید و احتمال وقوع ضربات خصمانه در اثر وقایع تهدید

٦. به‌روز رسانی اطلاعات مخاطرات خصمانه یا مخاطرات غیرخصمانه

اقدام ۲-۵ : تعیین ضربات خصمانه از وقایع تهدید

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

١. شناسایی ورودی‌های تعیین ضربه

٢. شناسایی فاکتورهای تعیین ضربه با استفاده از منابع اطلاعاتی تعیین‌شده

٣. شناسایی ضربات خصمانه و سرمایه‌های صدمه‌دیده

٤. به‌روز رسانی اطلاعات مخاطرات خصمانه یا مخاطرات غیرخصمانه

اقدام ۲-۶ : تعیین مخاطرات ناشی از وقایع تهدید برای سازمان

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

١. شناسایی مخاطره و ورودی‌های تعیین عدم قطعیّت

٢. تعیین مخاطره و به‌روز رسانی اطلاعات مخاطرات خصمانه یا مخاطرات غیرخصمانه

مرحله (۳) : تبادل نتایج ارزیابی

در این مرحله فعالیت‌های زیر انجام می‌گیرند :

اقدام ۳-۱ : مبادله‌ی نتایج ارزیابی مخاطرات با تصمیم‌سازان سازمانی برای پشتیبانی از پاسخ‌های مخاطره

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

۱. تعیین روش مناسب برای مبادله‌ی نتایج ارزیابی مخاطرات، از قبیل گزارش ارزیابی مخاطرات یا داشبورد
۲. مبادله‌ی نتایج ارزیابی مخاطرات با ذی‌نفعان سازمان

اقدام ۳-۲ : اشتراک‌گذاری اطلاعات مرتبط با مخاطره که از فرآیند ارزیابی مخاطره حاصل شده‌اند

مرحله (٤) : نگه‌داشت ارزیابی

در این مرحله، فعالیت‌هایی انجام می‌گیرند که خروجی ارزیابی مخاطرات امنیتی را همیشه به‌روز نگه‌دارند :

اقدام ۴-۱ : پایش فاکتورهای مخاطره که موجب تغییر در مخاطره برای فعالیت‌ها، سرمایه‌ها یا پرسنل سازمان می‌شوند.

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

۱. شناسایی فاکتورهای کلیدی مخاطره
۲. شناسایی فرکانس فعالیت‌های پایش فاکتورهای مخاطره

اقدام ۴-۲ : به‌روز رسانی ارزیابی مخاطره

این اقدام، شامل فعالیت‌هایی به شرح ذیل است :

۱. تائید مجدد هدف، قلمرو و سایر پارامترها، الزامات و شرایط ارزیابی امنیتی
۲. انجام فعالیت‌های ارزیابی مخاطرات
۳. مبادله‌ی نتایج ارزیابی مخاطرات با کلیه ذی‌نفعان سازمان

۷-۳- توصیه‌های ضروری

به‌منظور ارزیابی مخاطرات امنیتی فضای سایبر سازمان، لازم است :

۱. قبل از انجام هر اقدام امن‌سازی، ابتدا مخاطرات امنیتی موجود علیه سرمایه‌های سایبری سازمان خود را مورد ارزیابی قرار داده و بر اساس نتایج حاصل، دو دسته اقدام را به انجام رسانید. دسته‌ی اول، شامل اقدامات فوری است که با هدف تسکین سریع مخاطرات خیلی‌شدید صورت می‌گیرند و دسته‌ی دوم، اقدامات نظام‌مندی را در بر می‌گیرد که بر اساس آن‌ها طرح امنیتی سازمان، تهیه و اجرا می‌شود.
۲. منابع تهدید سایبری موجود علیه سرمایه‌های سایبری سازمان را شناسایی و لیستی از این منابع تهدیدها تهیه نمائید. برای این منظور، جدولی مشابه جدول (۳-۲) تشکیل دهید و تمام ستون‌های آن، از جمله ویژگی‌های منابع تهدیدها را تعیین کنید.

۳. با مطالعه‌ی راهبردها و خط مشی‌های امنیتی تدوین شده برای سازمان خود، ویژگی‌های تعیین شده برای ارزیابی مخاطرات امنیتی را استخراج و بر اساس آن‌ها، چهار دسته ویژگی ارزیابی، شناسایی، تحلیل و پیش‌بینی را تکمیل نمائید.

٤. از میان متدولوژی‌های ارزیابی مخاطرات امنیتی، متدولوژی مناسب که ویژگی‌های آن با ویژگی‌های استخراج شده، تطبیق بیشتری داشته باشد را انتخاب نمائید.

٥. مراحل انجام ارزیابی مخاطرات امنیتی بر اساس متدولوژی انتخاب شده را استخراج نموده و مقدمات انجام ارزیابی امنیتی را فراهم نمائید.

٦. بر اساس مراحل استخراج شده، ارزیابی مخاطرات امنیتی را انجام داده و نتایج را در قالب گزارش ارزیابی مخاطرات امنیتی، تدوین نمائید.

۷. برای هر یک از مخاطرات خیلی‌شدید مندرج در گزارش ارزیابی مخاطرات امنیتی، اقدامات فوری که می‌توانند منجر به تسکین فوری آن مخاطره شوند را تعیین کنید.

۸. مجموع اقدامات فوری تعیین شده را در قالب یک توصیه‌نامه، با عنوان توصیه‌نامه‌ی تسکین مخاطرات شدید، تدوین نموده و نسبت به انجام فوری آن‌ها اقدام نمائید.