کتاب مرجع آموزش عرضی و کوتاه‌مدت

مباحث تخصصی پدافند سایبری

مؤلف : مهندس محمود خالقی‌دخت

عضو هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات

اسفند ۱۴۰۰

سرشناسه	: خالقی دخت، محمود
عنوان و نام پدیدآور	: مباحث تخصصی پدافند سایبری/محمود خالقی دخت
مشخصات نشر	: تهران: سبک نو ۱۴۰۰
مشخصات ظاهری	: ۱۶۶ ص- ۱۷.۵ در ۲۴.۵-
شابک	: ۹۷۸-۶۲۲-۹۴۶۳۰-۷-۹
وضعیت فهرست نویسی	: فیپا
رده بندی کنگره	: ۱۴۰۰ ۵م/ ۴۴/ ۵۹ BP
رده بندی دیویی	: ۱۴۱/۲۹۷
شماره کتابشناسی ملی	:۶۴۴۲۵۳۰۲
اطلاعات رکورد کتابشناسی	: فیپا

سازمان پدافند غیرعامل کشور

عنوان:مباحث تخصصی پدافند سایبری

تألیف: محمود خالقی‌دخت

صفحه‌آرایی: عباس چراغ‌چشم

ناشر: سبک نو

نوبت چاپ: چاپ اول، ۱۴۰۰

تیراژ: چاپ اول ۵۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۹۴۶۳۰-۷-۹

تعداد صفحات: ۱۶۶ صفحه

فهرست

عنوان **صفحه**

فهرست اشکال

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

مقدمه

کلیّات دوره آموزشی عمومی پدافند سایبری

در نظام آموزش پدافند سایبری کشور، دوره‌های آموزشی کوتاه‌مدت و عرضی در پنج سطح با عناوین دوره‌های عمومی، مقدماتی، تخصصی فنی، تخصصی پیشرفته و مدیریت راهبردی پدافند سایبری، طراحی شده است. کتاب حاضر، به عنوان مرجع دوره آموزشی تخصصی فنی پدافند سایبری، توسط مرکز پدافند سایبری کشور، به عنوان عالی‌ترین مرجع برگزاری دوره‌های آموزش عرضی و کوتاه‌مدت پدافند سایبری در کشور، تهیه شده است. شکل (۱)، سطوح پنج‌گانه‌ی نظام آموزشی عرضی و کوتاه‌مدت پدافند سایبری و جایگاه دوره آموزشی عمومی پدافند سایبری در این نظام را نمایش می‌دهد.

شکل (۱) : سطوح نظام آموزشی عرضی و کوتاه‌مدت پدافند سایبری و جایگاه دوره آموزشی تخصصی فنی

ویژگی‌های کلّی دوره آموزش تخصصی فنی پدافند سایبری، عبارتند از :

جایگاه : دوره آموزشی تخصصی فنی پدافند سایبری، مطابق شکل (۱)، به عنوان یکی از ۵ دوره‌ی پیش‌بینی شده در نظام آموزشی پدافند سایبری کشور و سومین سطح از دوره‌های آموزشی عرضی و کوتاه‌مدت پدافند سایبری است که پس از سطوح عمومی و مقدماتی قرار دارد.

اهداف : این دوره آموزشی با هدف ایجاد توانایی به‌کارگیری موضوعات حوزه پدافند سایبری و ارزش‌گذاری سریع و دقیق این موضوعات، طراحی شده است. این دوره موجب ایجاد توانایی به‌کارگیری در حیطه‌ی شناختی، ارزش‌گذاری در حیطه‌ی عاطفی و سرعت و دقت واکنش در حیطه‌ی روانی–حرکتی می‌شود. آموزش‌های پیش‌بینی شده در این دوره، موجب خواهند شد تا فراگیران، ضمن تشخیص میزان ارزش و جایگاه موضوعات مرتبط با پدافند سایبری، توانایی واکنش دقیق و سریع در مواجهه با این موضوعات، به‌منظور دفاع در مقابل هرگونه تجاوز سایبری را کسب نمایند.

مدّت : مدّت زمان برگزاری این دوره آموزشی، ۴۰ ساعت پیش‌بینی شده است و فراگیر در صورت قبولی در آزمون انتهای این دوره، گواهی قبولی دریافت خواهد نمود. به‌منظور تصدّی هر یک از مسئولیت‌های پیش‌بینی شده در نظام پدافند سایبری کشور، دریافت این گواهی، الزامی خواهد بود.

فراگیران (مخاطبین) : دوره آموزشی تخصصی فنی پدافند سایبری، یکی از دوره‌های آموزشی الزامی برای تمام پرسنل عضو تیم امنیت فضای سایبر، عضو آزموده‌ی تیم پدافند غیرعامل، عضو آزموده‌ی تیم پدافند سایبری و مسئول تیم پدافند غیرعامل در دستگاه‌های دولتی، مجموعه‌های غیردولتی متولی زیرساخت‌های حیاتی کشور و عرضه–کنندگان خدمات سایبری عمومی است.

ویژگی‌های فراگیر : فراگیران این دوره آموزشی، علاوه بر برخورداری از ویژگی‌های شغلی مندرج در بخش مخاطبین، باید از شرایط ذیل نیز به صورت توأمان برخوردار باشند :

- **مدرک تحصیلی** کارشناسی
- **تخصّص** فنی در حداقل یکی از حوزه‌های امنیت سایبری، پدافند غیرعامل و پدافند سایبری
- **تجربه** آزموده‌شده حداقل یکی از حوزه‌های امنیت سایبری، پدافند غیرعامل و پدافند سایبری

تشخیص برخورداری از ویژگی‌های فوق، بر عهده مرکز پدافند سایبری کشور است.

برگزارکننده : دوره آموزشی تخصصی فنی پدافند سایبری، قابلیت ارائه توسط کلیه مدرسین مورد تائید معاونت آموزشی و پژوهشی مرکز پدافند سایبری کشور را دارد و به صورت دوره‌ای، توسط این مرکز نیز برگزار می‌شود.

پیش‌نیاز : فراگیران این دوره آموزشی، باید دوره‌ی آموزش مقدماتی پدافند سایبری را با موفقیّت گذرانده و گواهی این دوره را اخذ نموده باشند.

روش آموزش : محتوای دوره آموزشی تخصصی فنی پدافند سایبری، با ترکیبی از روش‌های توضیحی، طرح و پروژه، به شرکت‌کنندگان ارائه می‌گردد.

موضوعات : مخاطبین دوره آموزشی تخصصی فنی پدافند سایبری، می‌آموزند که فضای سایبر چیست؟ و چه بخش‌هایی دارد؟ هر یک از این بخش‌ها، چه آسیب‌پذیری‌هایی دارند؟ و این آسیب‌پذیری‌ها، چگونه کشف می‌شوند؟ چگونه و توسط چه مراجعی آگاهی‌رسانی می‌شوند؟ توسط چه تهدیدهایی ممکن است مورد بهره‌برداری قرار گیرند؟ و با چه روش‌هایی می‌توان میزان مخاطرات ناشی از بهره‌برداری این آسیب‌پذیری‌ها توسط تهدیدها را مورد ارزیابی قرارداد؟ امنیت هر یک از این بخش‌ها، چگونه و با بره‌گیری از چه ابزارهایی تأمین می‌شود؟ چنانچه این سازوکارهای محافظتی مفید واقع نشد و تهاجمی علیه هر بخش از فضای سایبر شکل گرفت، چه روش‌ها و ابزارهایی برای تشخیص و مواجهه با این حمله سایبری، می‌توان به‌کار گرفت؟ در چه صورتی به این تهاجم سایبری، می‌توان لفظ عملیات سایبری یا جنگ سایبری اطلاق نمود؟ عملیات سایبری با چه ابزارهایی انجام و با چه ابزارهایی تشخیص داده می‌شود؟ دفاع در مقابل عملیات سایبری، با چه روش‌هایی و با بهره‌گیری از چه سامانه‌هایی انجام می‌شود؟ برای ارتقاء آمادگی دفاعی و ایجاد بازدارندگی دفاعی، از چه شیوه‌ها و ابزارهایی می‌توان بهره برد؟ بر این اساس، موضوعات اصلی این کتاب، شامل فضای سایبر، آسیب‌پذیری سایبری، تهدید سایبری، امنیت سایبری، آمادگی امنیتی در فضای سایبر، جنگ سایبری، پدافند سایبری، قدرت آمادگی دفاعی و بازدارندگی پدافند سایبری است. تمرکز بیشتر محتوای این دوره، بر روش‌ها و ابزارهایی است که به‌کارگیری آن‌ها موجب ایجاد توانایی در انجام واکنش سریع و دقیق در مواجهه با موضوعات پدافند سایبری، توسط شما مخاطب گرامی، خواهد شد.

فصل اوّل

سرمایه سایبری

اهداف آموزشی پیش‌بینی شده برای این فصل، عبارتند از :

۱. کسب شناخت و توانایی طبقه‌بندی سرمایه‌های سایبری
۲. کسب شناخت و توانایی تعیین ارزش و حساسیّت (اهمیّت) سرمایه سایبری
۳. کسب شناخت و بهره‌گیری سریع و دقیق از پایگاه‌های داده سرمایه سایبری

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

۱. انواع سرمایه سایبری و وجوه تمایز آن‌ها
۲. روش تعیین ارزش و حساسیّت (اهمیّت) یک سرمایه سایبری
۳. روش‌های طبقه‌بندی سرمایه‌های سایبری
٤. پایگاه داده سرمایه‌های سایبری و نحوه‌ی استفاده از آن برای شناسایی و طبقه‌بندی سرمایه‌های سایبری سازمان
٥. اقدامات دوره‌ای ضروری به منظور مدیریت سرمایه‌های سایبری سازمان

۱-۱- تعریف سرمایه سایبری

سرمایه به هر موجودیتی اطلاق می‌شود که برای مالکش دارای ارزش و به واسطه‌ی آن ارزش، نیازمند محافظت باشد. بر این اساس، «سرمایه سایبری، موجودیت مرتبط با [یا بخشی از] فضای سایبر متعلق به مالک آن فضا است، که برای او دارای ارزش و نیازمند محافظت باشد».

مؤسسه بین‌المللی استاندارد، سرمایه سایبری را «هر موجودیت مشهود یا نامشهود برخوردار از ارزش برای یک سازمان» تعریف نموده است و از ماشین‌آلات، تجهیزات، اختراعات و نرم افزار به عنوان مصادیق سرمایه مشهود و از

خدمات مبتنی بر شبکه، اطلاعات سازمانی، اعتبار، وجهه، مهارت و دانش، به عنوان مصادیق دارایی نامشهود نام برده است.

مؤسسه ملی استاندارد و فناوری ایالات متحده آمریکا، سرمایه را «هر موجودیت دارای ارزش برای یک سازمان» تعریف نموده و از سازمان، پرسنل، دستگاه محاسباتی، سامانه‌ی فناوری اطلاعات، شبکه ارتباطی، نرم‌افزار، سکوی محاسبات مجازی (در رایانش و محاسبات ابری و مجازی) و سخت‌افزار، به عنوان مصادیق سرمایه‌های یک سازمان، نام برده است.

۲-۱- انواع سرمایه سایبری

سرمایه‌های سایبری، از منظرهای مختلف، قابل تفکیک و طبقه‌بندی می‌باشند. به‌منظور طبقه‌بندی سرمایه‌های سایبری، باید ابتدا لیستی از ویژگی‌های مختلف یک سرمایه سایبری را احصاء نمائیم و سپس بر اساس تمام یا بخشی از این ویژگی‌ها، به دنبال طبقه‌بندی سرمایه‌های سایبری باشیم.

تعداد زیادی ویژگی را می‌توان برای سرمایه سایبری برشمرد. ماهیت، نام و نسخه‌ی محصول، نام سازنده و فروشنده، ارزش اقتصادی، اهمیت سرمایه برای مالک، ویرایش و زبان برنامه‌نویسی برای محصولات نرم‌افزاری، شماره قطعه برای محصولات سخت‌افزاری، نمونه‌هایی از این ویژگی‌ها را تشکیل می‌دهند. از میان این ویژگی‌ها، سه ویژگی «ماهیت»، «ارزش» و «اهمیت»، مهم‌تر بوده و معمولاً مبنای طبقه‌بندی سرمایه‌های سایبری قرار می‌گیرند.

یک ویژگی شاخص سرمایه سایبری، ماهیت آن است. یک سخت‌افزار با یک نرم‌افزار، از نظر ماهیت، متفاوت است. همین تفاوت ماهیت، میان تجهیزات ارتباطی با ابزارهای رایانش و ذخیره‌سازی اطلاعات نیز قابل مشاهده است. دومین ویژگی شاخص یک سرمایه، ارزش اقتصادی آن برای مالک است. بدیهی است به هر میزان که ارزش یک سرمایه بیشتر باشد، مالک آن سرمایه، حاضر است برای محافظت از آن، هزینه‌ی بیشتری بپردازد و بر این اساس، لازم است تا این قبیل سرمایه‌ها از سایرین تفکیک شوند و بر این اساس، طبقه‌بندی سرمایه سایبری بر اساس ارزش [اقتصادی] ضرورت می‌یابد. سومین ویژگی شاخص یک سرمایه سایبری نیز نقش، اهمیت یا حساسیتی است که آن سرمایه در انجام کسب‌وکار، تحقق اهداف یا اجرای مأموریت‌های محوّل شده به سازمان مالک خود ایفا می‌نماید. لفظ «سرمایه‌های کلیدی»، به سرمایه‌هایی اطلاق می‌شود که در تحقق اهداف سازمان، نقش کلیدی داشته باشند. بر این اساس، لازم است سرمایه‌های سایبری از منظر این ویژگی شاخص نیز مورد طبقه‌بندی قرار گرفته و تفکیک شوند.

۱-۲-۱. انواع سرمایه سایبری، از نظر ماهیت

سرمایه‌های سایبری از نظر ماهیت، در کلی‌ترین حالت، به دو دسته‌ی مشهود و نامشهود یا عینی و ذهنی و یا اصلی و پشتیبان قابل تفکیک و طبقه‌بندی می‌باشند. در دسته‌بندی دیگری، این سرمایه‌ها از نظر ماهیت، به سه دسته‌ی منطقی، فیزیکی و اجتماعی طبقه‌بندی شده‌اند. برخی مراجع نیز سرمایه‌های سایبری را به سه دسته‌ی فیزیکی، انسانی و اعتباری تفکیک نموده‌اند. این دسته‌بندی‌ها هم‌پوشانی قابل توجهی دارند.

در دسته‌بندی سرمایه‌های مشهود و غیرمشهود، سرمایه‌هایی مانند انواع رایانه‌ها، تجهیزات شبکه، سامانه‌های اطلاعاتی، تجهیزات رایانشی و ذخیره‌سازی اطلاعات جزء دسته‌ی سرمایه‌های مشهود قرار می‌گیرند و اطلاعات و انواع خدمات سایبری نیز سرمایه‌های نامشهود را تشکیل می‌دهند.

در دسته‌بندی سرمایه‌های اصلی و پشتیبان، سرمایه‌های اصلی، متشکل از «اطلاعات» و «فعالیت‌ها و فرآیندهای کسب‌وکار» و سرمایه‌های پشتیبانی، شامل «سخت‌افزارها»، «نرم‌افزارها»، «شبکه»، «پرسنل»، «سایت» و «ساختار سازمانی» است.

۲-۲-۱. انواع سرمایه سایبری، از نظر حساسیّت (اهمیت)

سرمایه‌های سایبری را می‌توانیم از نظر حساسیّت (اهمیت)، در پنج سطح فاقداهمیّت، عادی (کم‌اهمیّت)، مهم (اهمیت متوسط)، حسّاس (اهمیت زیاد) و حیاتی (اهمیت خیلی‌زیاد) طبقه‌بندی نمائیم. این طبقه‌بندی، متناظر با پنج سطح طبقه‌بندی محرمانگی اطلاعات است که در آن، اطلاعات را به سطوح عادی، محرمانه، خیلی‌محرمانه، سرّی و بکلّی‌سرّی طبقه‌بندی می‌نمایند.

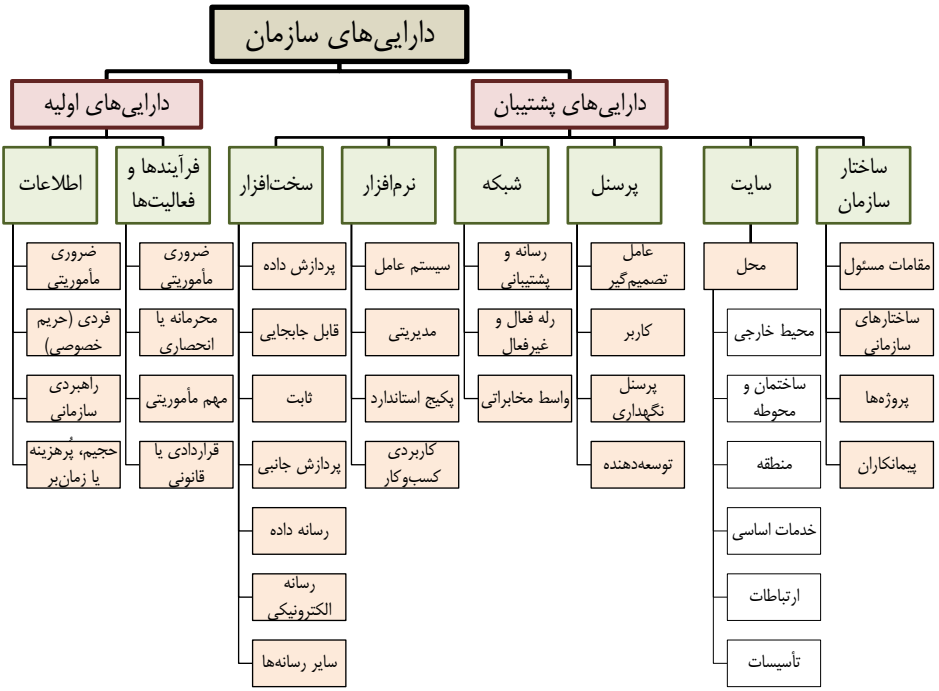
سرمایه سایبری حیاتی، به سرمایه سایبری اطلاق می‌شود که نابودی یا اختلال گسترده در عملکرد آن، منجر به بُروز پیامدهای فاجعه‌باری برای سازمان مالک آن سرمایه شود، لیکن به سرمایه سایبری که نابودی یا اختلال گسترده در آن، صرفاً موجب بُروز بُحران در آن سازمان گردد، سرمایه سایبری حسّاس اطلاق می‌شود.

۳-۲-۱. انواع سرمایه سایبری، از نظر ارزش اقتصادی

ارزش اقتصادی یک سرمایه سایبری، از دو بخش «ارزش مستقیم» و «ارزش غیرمستقیم» تشکیل می‌شود. ارزش مستقیم یک سرمایه سایبری، معادل هزینه خرید یا اکتساب آن سرمایه سایبری است و ارزش غیرمستقیم یک سرمایه سایبری نیز معادل هزینه‌هایی از قبیل هزینه نصب، راه‌اندازی، تست، تنظیم و به‌روزرسانی آن سرمایه سایبری می‌باشد. سرمایه‌های سایبری از نظر ارزش اقتصادی، به پنج سطح فاقدارزش (بسیار کم‌ارزش در مقایسه با کل سرمایه مالک)، عادی (کم‌ارزش)، ارزشمند (ارزش متوسط)، ارزش‌ویژه (پُرارزش) و ارزش‌ممتاز (بسیار پُرارزش) طبقه‌بندی می‌شوند.

۳-۱- نمونه‌های طبقه‌بندی سرمایه‌های سایبری

مؤسسه بین‌المللی استاندارد، سرمایه‌های سایبری یک سازمان را مطابق شکل (۱-۱)، طبقه‌بندی نموده است.



شکل (۱-۱) : مدل طبقه‌بندی سرمایه‌های سایبری یک سازمان، توسط مؤسسه بین‌المللی استاندارد

در این طبقه‌بندی، سرمایه‌های سایبری به دو دسته‌ی اصلی و پشتیبان تفکیک می‌شوند. در سطح دوم، دارایی‌های اصلی به «فرآیندها و فعالیت‌های مربوط به کسب‌وکار» و «اطلاعات» تفکیک شده‌اند و دارایی‌های پشتیبان نیز به «سخت‌افزار»، «نرم‌افزار»، «شبکه»، «پرسنل»، «سایت» و «ساختار سازمانی» تفکیک شده‌اند.

سرمایه‌های اصلی

فرآیندهای سازمان را می‌توان به عنوان سرمایه‌های اصلی در نظر گرفت. این سرمایه‌ها برای تنظیم خط‌مشی‌های امنیتی و نقشه راه و در جهت تداوم کسب و کار مناسب هستند. به این ترتیب، تنها کافی است فرآیندهای اصلی سازمان، شناسایی شده و در نظر گرفته شوند. سرمایه‌های اصلی خود دو نوع هستند :

۱- فرآیندها و فعالیت‌های مرتبط با کسب و کار، از قبیل :

۱-۱. فرآیندهایی که خسارت ناشی از آن‌ها، تحقق ماموریت‌های سازمان را غیرممکن می‌نماید.

۱-۲. فرآیندهایی که شامل فرآیندهای محرمانه یا فرایندهای مرتبط با فناوری انحصاری سازمان است.

۱-۳. فرآیندهایی که اگر تغییر کنند، می‌توانند تحقق ماموریت‌های سازمان را تحت تاثیر قرار دهند.

۱-٤. فرآیندهایی که رعایت آن‌ها توسط سازمان، بر اساس الزامات قراردادی، قانونی یا نظارتی، ضرورت دارد.

۲- اطلاعات، از قبیل :

۲-۱. اطلاعاتی که برای اجرای ماموریت‌ها یا کسب‌وکار سازمان، ضروری هستند.

۲-۲. اطلاعات فردی که به صورت خاص، تحت پوشش قوانین حریم خصوصی قرار دارند.

۲-۳. اطلاعات راهبردی که برای دستیابی به اهداف سازمان، در قالب برنامه راهبردی، مشخص شده‌اند.

۲-٤. اطلاعات ارزشمندی که جمع‌آوری، ذخیره‌سازی، پردازش و انتقال آنها نیاز به زمانی طولانی دارد و/یا هزینه جمع‌آوری، ذخیره‌سازی، پردازش و انتقال آنها زیاد است.

سرمایه‌های پشتیبان

سرمایه‌های پشتیبان، سرمایه‌هایی هستند که پشتیبانی از سرمایه‌های اصلی را بر عهده دارند. این سرمایه‌ها، دارای آسیب‌پذیری هستند و بسیاری از تهدیدها می‌توانند از آن‌ها به نحوی سوءاستفاده کنند که در نهایت، منجر به آسیب رساندن به سرمایه‌های اصلی (فرآیندها و اطلاعات) شوند. انواع سرمایه‌های پشتیبان، عبارتند از :

۱. سخت‌افزار

شامل تمام مؤلفه‌های فیزیکی است که از فرآیندهای سازمان پشتیبانی می‌کنند. این مؤلفه‌ها عبارتند از:

۱-۱. تجهیزات فعال مرتبط با پردازش داده : تجهیزاتی که به صورت مستقل، برای پردازش اطلاعات مورد استفاده قرار می‌گیرند.

۱-۲. تجهیزات قابل جابه‌جایی : تجهیزات کامپیوتری مانند لپ‌تاپ و دستیار دیجیتال شخصی (PDA[۱]) که از قابلیت حمل و جابجایی برخوردار می‌باشند.

۱-۳. تجهیزات ثابت : تجهیزات کامپیوتری از قبیل سرویس‌دهنده یا ایستگاه کاری[۲] که در محل استقرار سازمان مورد استفاده قرار می‌گیرند.

۱-٤. تجهیزات پردازشی جانبی : تجهیزاتی از قبیل چاپگر و دیسک سخت قابل حمل، که از طریق یک پورت مخابراتی به کامپیوتر وصل هستند تا داده‌ها را به صورت سری، موازی و یا به هر نوع دیگری، وارد کامپیوتر کرده یا از کامپیوتر انتقال می‌دهند.

۱-۵. رسانه غیرفعال داده : رسانه‌هایی که برای ذخیره‌ی داده و یا توابع، مورد استفاده قرار می‌گیرند.

---

۱ Personal Digital Assistant (PDA)

۲ Workstation

۱-٦. رسانه الکترونیکی : رسانه‌ای است که می‌تواند برای ذخیره‌سازی اطلاعات، به یک کامپیوتر یا شبکه کامپیوتری متصل شود. این نوع رسانه، علی‌رغم اندازه فشرده و کوچک، می‌تواند حاوی حجم زیادی از داده‌ها باشد. این رسانه‌ها می‌توانند توسط تجهیزات محاسبه‌گر استاندارد مورد استفاده قرار گیرند. فلاپی دیسک، دیسک فشرده، نوار مغناطیسی، دیسک سخت قابل انتقال، حافظه فلش و نوار، نمونه‌هایی از رسانه الکترونیکی می‌باشند.

۱-۷. سایر رسانه‌ها : رسانه ایستا یا رسانه غیرالکترونیکی، رسانه‌ای است که اگرچه الکترونیکی نیست، لیکن حاوی محتوای داده است. مقاله، اسلاید، مستندات و فکس، نمونه‌هایی از رسانه غیرالکترونیکی می‌باشند.

۲. نرم افزار

شامل تمامی برنامه‌هایی است که در عملیات پردازش داده مشارکت دارند. سرمایه‌های نرم‌افزاری شامل موارد زیر می‌شوند :

۲-۱. سیستم عامل : برنامه‌ی کامپیوتری است که یک پایه عملیاتی برای اجرای سایر برنامه‌ها، اعم از سرویس‌ها یا برنامه‌های کاربردی را فراهم می‌آورد. سیستم عامل شامل یک هسته اصلی و سرویس‌ها یا توابع پایه است. با توجه به معماری، یک سیستم عامل ممکن است تک هسته‌ای باشد یا از یک ریز هسته و مجموعه‌ای از سرویس‌های سیستمی ساخته شود. مولفه‌های اصلی یک سیستم عامل، شامل سرویس‌های مدیریت تجهیزات (CPU، حافظه، دیسک و اتصالات شبکه)، سرویس‌های مدیریت فرآیند و سرویس‌های مدیریت حق دسترسی کاربران[۱] است.

۲-۲. نرم‌افزار سرویس، نگهداری یا مدیریتی : این نوع نرم‌افزار، سرویس‌های سیستم عامل را به طور کامل انجام می‌دهد و به طور مستقیم در خدمت کاربران یا برنامه‌های کاربردی نیست.

۲-۳. بسته‌ی نرم‌افزاری یا نرم‌افزار استاندارد : این نوع نرم‌افزارها، محصولات کاملی هستند که تجاری‌سازی شده و شامل رسانه، نگارش و خدمات نگهداری هستند. این نرم افزارها سرویس‌هایی برای کاربران و برنامه‌های کاربردی فراهم می‌کنند، اما با این حال شخصی‌سازی نشده و خاص یک کسب و کار معین نیستند. نرم‌افزار مدیریت پایگاه داده، نرم‌افزار پیام‌رسان الکترونیکی، نرم‌افزار شبکه اجتماعی، نرم‌افزار راهنما و نرم‌افزار ارائه خدمات وب، مصادیقی از بسته‌های نرم‌افزاری می‌باشند.

۲-٤. برنامه‌های کاربردی کسب‌وکار : این برنامه ها به دو دسته تقسیم می‌شوند. دسته‌ی اول، «برنامه‌های کاربردی کسب و کار استاندارد» هستند. این نوع نرم‌افزار، نوعی نرم‌افزار تجاری هستند که به نحوی طراحی شده‌اند تا به کاربران اجازه دسترسی مستقیم به سرویس‌ها و توابعی را می‌دهند که این کاربران در زمینه کاری خود به آنها نیاز دارند. این دسته، طیف گسترده‌ای از نرم‌افزارها را در بر می‌گیرند. نرم‌افزار حسابداری، نرم‌افزار

[۱] Rights management services

کنترل ابزار ماشین، نرم‌افزار مراقبت از حقوق مشتری، نرم‌افزار مدیریت شایستگی پرسنل و نرم‌افزار اداری، نمونه‌هایی از برنامه‌های کاربردی کسب‌وکار می‌باشند. دسته‌ی دوم برنامه‌های کاربردی کسب‌وکار، «برنامه‌های کاربردی خاص کسب و کار» هستند. این دسته از نرم‌افزارها، به طور خاص، برای یک کسب‌وکار مشخص یا یک خدمت مشخص، شخصی‌سازی شده است تا خدمت مشخصی را به کاربران خاص خود، ارائه نماید. نرم‌افزار مدیریت صورتحساب مشتریان اپراتورهای مخابراتی، یکی از نرم‌افزارهای کاربردی خاص کسب‌وکار است که خدمت مدیریت صورتحساب را تنها برای مشتریان اپراتورهای مخابراتی، شخصی‌سازی نموده و ارائه می‌دهد.

۳. شبکه ارتباطی

منظور از شبکه ارتباطی، تمام ابزارهای مخابراتی است که برای اتصال کامپیوترهای دور از یکدیگر یا اتصال عناصر یک سامانه اطلاعاتی به کار می‌روند. سرمایه سایبری شبکه، شامل سه دسته تجهیزات، به شرح زیر است :

۳-۱. تجهیزات و پروتکل‌های ارتباطی پشتیبان آن‌ها : تجهیزات مخابراتی و مخابرات راه دور مورد استفاده برای ارتباط نقطه به نقطه و پخش، به همراه پروتکل‌های ارتباطی لایه ۲ و ۳ پشتیبانی کننده‌ی ارتباط این تجهیزات با یکدیگر را در بر می‌گیرد. شبکه تلفن سوئیچینگ عمومی[۱] (PSTN)، شبکه کامپیوتری سازمانی، خط اشتراک دیجیتال نامتقارن[۲] (ADSL)، پروتکل ارتباطی بی‌سیم (از قبیل پروتکل IEEE ۸۰۲,۱۱)، پروتکل ارتباطی بلوتوث و سامانه دیوار آتش[۳]، نمونه‌هایی از این نوع سرمایه سایبری می‌باشند.

۳-۲. رله فعال و غیرفعال: این دسته شامل تمامی دستگاه‌هایی است که به لحاظ منطقی در نقاط انتهایی[۴] ارتباط قرار ندارند، بلکه در طول مسیر ارتباط قرار گرفته و به مثابه رله عمل می‌کنند. رله‌ها توسط پروتکل‌های ارتباطی شبکه مشخص و توصیف می‌شوند. سوئیچ های مخابراتی و مسیریاب‌ها، نمونه‌ای از این نوع سرمایه سایبری محسوب می‌شوند. این دستگاه‌ها اغلب از راه دور مدیریت می‌شوند و معمولاً قادر به ثبت[۵] وقایع و رخدادهای بوقوع پیوسته در مسیر ارتباطی هستند.

۳-۳. واسط مخابراتی: سامانه‌های اطلاعاتی و واحدهای پردازشی، از طریق واسطهای مخابراتی به شبکه متصل می‌شوند. علاوه بر تأمین ارتباط، برخی واسطهای مخابراتی، به‌منظور اعمال پالایش روی محتوای مورد مبادله در شبکه، تولید هشدار در صورت تشخیص شرایط خاص در ارتباط و همچنین مدیریت از راه دور سامانه‌های اطلاعاتی و واحدهای پردازشی، مورد استفاده قرار می‌گیرند.

---

۱ Public Switching Telephone Network (PSTN)
۲ Asymmetric Digital Subscriber Line
۳ FireWire
۴ Logical terminations
۵ Logs

٤. پرسنل

شامل گروهی از افراد می‌شود که در فعالیت سرمایه‌های سایبری سازمان، درگیر بوده و یکی از نقش‌های ذیل را بر عهده دارند :

٤-۱. تصمیم‌ساز[۱]: عامل تصمیم‌ساز، نقشی مشابه مالک سرمایه اصلی (فرآیندها و اطلاعات) است که از جمله مدیران سازمان و مدیران پروژه آن را بر عهده دارند.

٤-۲. کاربر: پرسنلی است که یا از سرمایه سایبری موردنظر برای انجام وظایف خود استفاده می‌کند و یا از خدمات آن سرمایه سایبری، بهره‌برداری می‌نماید. پرسنل امور مالی و مدیریت منابع انسانی سازمان، به ترتیب کاربر سامانه اطلاعاتی مالی و پرسنلی سازمان محسوب می‌شوند.

٤-۳. عملیات و نگهداری : به پرسنلی اطلاق می‌شود که مسئول عملیاتی نگه‌داشتن یک سرمایه سایبری است. به‌منظور عملیاتی نگه‌داشتن یک سرمایه سایبری، از یک‌سو باید دسته‌ای اقدامات نگهداری دوره‌ای از قبیل «تهیه نسخه پشتیبان از اطلاعات»، «شناسایی و رفع آسیب‌پذیری‌ها» و نظایر این‌ها انجام شود و از سوی دیگر، باید دسته دیگری از اقدامات مراقبتی، تشخیصی و واکنشی مداوم انجام شود تا هرگونه اخلال در عملکرد سرمایه سایبری، شناسایی و رفع شود تا سرمایه موردنظر، همواره عملیاتی باقی بماند. پرسنل تیم پدافند سایبری، چنین نقشی را بر عهده دارند.

٤-٤. توسعه‌دهنده : به پرسنلی اطلاق می‌شود که مسئول توسعه برنامه‌های کاربردی سازمان است. این پرسنل، معمولاً از حق دسترسی با کم‌ترین محدودیت‌ها، به بخشی از سامانه‌های اطلاعاتی سازمان برخوردار هستند. از جمله توسعه‌دهنده برنامه‌های کاربردی کسب و کار سازمان، باید به اطلاعات سامانه‌های اطلاعاتی مختلف سازمان، دسترسی داشته باشد تا از انواع این اطلاعات، در جای مناسب، برای توسعه کسب‌وکار سازمان، بهره‌برداری نماید.

٥. محل

عبارت از موقعیت مکانی[۲] است که سرمایه‌های سایبری سازمان، ممکن است در آن‌ها قرار داشته باشند. اینموقعیت مکانی، دارای چند زیرشاخه به شرح زیر است :

٥-۱. محیط خارجی : شامل تمامی موقعیت‌های مکانی است که در آن ابزارهای امنیتی سازمان را نمی‌توان مورد استفاده قرار داد. از جمله خانه‌های پرسنل، محل استقرار سایر سازمان‌ها و به عبارت دیگر، تمامی محیط‌های خارج از سازمان، در این بخش قرار می‌گیرند.

---

۱ Decision maker
۲ Location

۵-۲. ساختمان‌ها و محوطه : عبارت از ساختمان‌های محل استقرار عموم سرمایه‌های سازمان و از جمله سرمایه‌های سایبری آن است که توسط عملکردهای مستقیم سازمان، با محوطه خارج محدود شده است. این محدودسازی ممکن است با یک مرز فیزیکی و حفاظتی از طریق موانع فیزیکی یا توسط ساختمان‌های اطراف ایجاد شود.

۵-۳. منطقه[۱] : منطقه‌ای است که به وسیله یک مرز فیزیکی حفاظت‌کننده، در درون محوطه سازمان ایجاد شده باشد. این بخش، موانع فیزیکی را دورتادور زیرساخت پردازش اطلاعات قرار می‌دهد. منطقه دسترسی رزرو شده و منطقه امن، نمونه‌هایی از مناطق ایجاد شده در داخل یک سازمان می‌باشند.

۵-٤. خدمات اساسی : تمامی خدمات مورد نیاز برای این‌که تجهیزات سازمان کار کنند و سازمان قادر به اجرای مأموریت یا کسب‌وکار خود باشد.

۵-۵. ارتباطات : خدمات ارتباطی یا رایانشی و تجهیزات مربوطه که معمولاً توسط یک اپراتور ارائه می‌شود. «ارتباطات تلفنی سازمان» که توسط خطوط تلفن به همراه PABX و شبکه تلفنی داخل سازمان برقرار می‌شوند، همچنین «ارتباطات اینترنتی سازمان» که توسط خط ارتباط با اینترنت، شبکه ارتباطی داخل سازمان، میزبان‌های اینترنتی قرار گرفته در داخل این شبکه و تارنمای (سایت وب) عرضه‌کننده خدمات سازمان در شبکه اینترنت به همراه سرویس‌دهنده پست الکترونیکی برقرار می‌شوند، نمونه‌هایی از ارتباطات سازمان را تشکیل می‌دهند.

۵-٦. تاسیسات : به سرویس‌ها و ابزارهای (منابع و سیم کشی) مورد نیاز برای تامین انرژی برای تجهیزات فناوری اطلاعات و سایر تجهیزات جانبی اطلاق می‌شود. منبع تامین توان با ولتاژ پایین، مبدل، مدار الکتریکی، منبع آب، به همراه لوله آب سرد و دستگاه‌های تهویه هوا که برای خنک کردن و تصفیه هوا مورد استفاده قرار می‌گیرند، از این دسته سرمایه می‌باشند.

٦. سازمان

منظور از سازمان، چارچوب سازمانی است که شامل تمام ساختارهای پرسنلی منتسب به یک کار خاص و روش‌های کنترل این ساختارها می‌باشد. این نوع سرمایه از چهار دسته تشکیل می‌شود :

٦-۱. سازمان مسئول: عبارت از نهاد بالادستی است که سازمان، اختیارات و مأموریت‌های خود را از آن دریافت می‌کند. این مسئله از نظر قوانین و مقررات، تصمیمات و اقدامات، محدودیت‌هایی را به سازمان تحمیل می‌کند.

٦-۲. ساختار سازمان: هر سازمان، از بخش‌های مختلفی تشکیل می‌شود که در قالب یک ساختار سازمانی، به یکدیگر مربوط بوده و تحت کنترل مدیریت سازمان اداره می‌شوند. مدیریت منابع انسانی، مدیریت فناوری

[۱] Zone

اطلاعات، مدیریت خرید، مدیریت واحد کسب و کار، خدمات ایمنی ساختمان، خدمات آتش سوزی و مدیریت حسابرسی، از جمله واحدهای تشکیل‌دهنده‌ی یک سازمان هشتند..

۶-۳. سازماندهی سیستم یا پروژه : بخشی از سازمان است که مسئول تنظیم سازمان برای اجرای موفق یک پروژه یا ارائه یک سرویس مشخص است. اگر «توسعه برنامه‌های کاربردی جدید» را به عنوان یک پروژه برای سازمان در نظر بگیریم، مدیریت فناوری اطلاعات مسئولیت اجرایی نمودن این وظیفه را بر عهده خواهد داشت.

۶-۴. پیمانکاران، تامین‌کنندگان یا سازندگان : مجموعه‌هایی هستند که در محدوده قراردادی که دارند، منابعی را برای سازمان تأمین نموده و یا خدمتی را به سازمان ارائه می‌دهند.

۴-۱- روش پیشنهادی برای طبقه‌بندی سرمایه‌های سایبری

به‌منظور شناسایی سرمایه‌های سایبری، لازم است از دسته‌بندی مبتنی بر ماهیت یا عملکرد استفاده نمود، لیکن به منظور اعمال خط مشی‌های امنیتی، استفاده از طبقه‌بندی مبتنی بر حساسیت و ارزش اقتصادی مناسب است. البته باید توجه داشت که به‌منظور ایجاد تمایز بین سرمایه‌های سایبری، لازم است اطلاعات تمام ویژگی‌های سرمایه‌های سایبری سازمان را احصاء و ذخیره نمود.

در جامع‌ترین حالت، سرمایه‌های سایبری را می‌توان به شرح ذیل، طبقه‌بندی نمود :

۱. زیرساخت سایبری

۱-۱. زیرساخت ارتباطی

کابل‌های مسی و خطوط فیبر نوری، تجهیزات دسترسی به شبکه، تجهیزات ارتباط رادیویی، تجهیزات ارتباط ماهواره‌ای، سوئیچ‌ها و مسیریاب‌های مورد استفاده در زیرساخت شبکه و تجهیزات گذرگاه ارتباط با اینترنت و انواع تجهیزات مدیریت و امنیت شبکه، نمونه‌هایی از عناصر زیرساخت ارتباطی یک سازمان را تشکیل می‌دهند.

۱-۲. زیرساخت رایانشی

تجهیزات مرکز داده، زیرساخت خدمات ابری، انواع سرویس‌دهنده‌ها و ایستگاه‌های کاری شبکه، از جمله عناصر زیرساخت رایانشی یک سازمان می‌باشند.

۱-۳. زیرساخت نرم‌افزاری

شبکه‌ی نرم‌افزار تعریف (SDN)، سیستم عامل تجهیزات ارتباطی و رایانشی و سرویس‌دهنده‌ها و میزبان‌ها، سیستم عامل نهفته و نرم‌افزارهای پایه نیز برخی عناصر زیرساخت نرم‌افزاری سازمان را تشکیل می‌دهند.

۱-۴. زیرساخت محتوایی

شبکه تحویل محتوا (CDN)، سامانه‌های ذخیره‌سازی محتوا و درگاه خدمات اینترنتی، از جمله مؤلفه‌های زیرساخت محتوایی سازمان می‌باشند.

۱-۵. زیرساخت تشکیلاتی

تشکیلات مدیریت زیرساخت، خدمات و محتوا و تشکیلات امنیت زیرساخت، خدمات و محتوا، زیرساخت تشکیلاتی مرتبط با فضای سایبر سازمان را تشکیل می‌دهند.

۲. خدمات سایبری

۲-۱. خدمات ارتباطی

خدمات ارتباطی یک سازمان، متشکل از خدمت ارتباطی بدون پروتکل، خدمت ارتباطی مبتنی بر پروتکل IP، شبکه خصوصی مجازی و خدمت ابری IaaS است.

۲-۲. خدمات رایانشی

خدمات رایانشی یک سازمان نیز متشکل از انواع خدمات میزبانی در مرکز داده، خدمات ابری PaaS و انواع خدمات اشتراک‌گذاری اطلاعات می‌باشد.

۲-۳. خدمات نرم‌افزاری پایه

خدمات نام دامنه، خدمات پیام‌رسانی، خدمات مرور وب، خدمات جویش اینترنتی، خدمات پرداخت اینترنتی، پست الکترونیکی و خدمات ابری SaaS، از جمله خدمات نرم‌افزاری پایه را تشکیل می‌دهند.

۲-٤. خدمات محتوایی

خدمت تأمین و تحویل محتوای متنی، صوتی، تصویری و ویدیوئی زنده و مبتنی بر تقاضا، انواع پایگاه‌های داده متنی، صوتی، تصویری و ویدیوئی، از جمله خدمات محتوایی را تشکیل می‌دهند.

۱-٦. پرسنل

پرسنل مرتبط با فضای سایبر سازمان، متشکل از پرسنل مدیریت زیرساخت، خدمات و محتوا، پرسنل امنیت زیرساخت، خدمات و محتوا و کاربران خدمات ارتباطی، رایانشی، نرم‌افزاری و محتوایی می‌باشد.

۳. محتوای سایبری

۳-۱. اطلاعات پیکربندی تجهیزات زیرساخت

۳-۲. اطلاعات در حال پردازش و ذخیره‌شده

۳-۳. اطلاعات تنظیمات نرم‌افزارها

۳-٤. محتوای مورد مبادله

به این ترتیب، به‌منظور شناسایی سرمایه‌های سایبری یک سازمان، باید لیستی مطابق جدول (۱-۱)، تهیه و تکمیل نمود.

جدول (۱-۱) : لیست سرمایه‌های سایبری سازمان

ماهیت		
دسته اصلی	**دسته فرعی**	**نوع**
زیرساخت سایبری	زیرساخت ارتباطی	کابل‌های مسی
		خطوط فیبر نوری
		تجهیزات دسترسی به شبکه
		تجهیزات ارتباط رادیویی
		تجهیزات ارتباط ماهواره‌ای
		سوئیچ‌ها
		مسیریاب‌ها
		تجهیزات گذرگاه ارتباط با اینترنت
		تجهیزات مدیریت شبکه
		تجهیزات امنیت شبکه
		تجهیزات کنترل صنعتی
	زیرساخت رایانشی	تجهیزات مرکز داده
		تجهیزات خدمات ابری
		سرویس‌دهنده‌ها
		ایستگاه‌های کاری
	زیرساخت نرم‌افزاری	شبکه‌ی نرم‌افزار تعریف (SDN)
		سیستم عامل تجهیزات ارتباطی
		سیستم عامل تجهیزات رایانشی
		سیستم عامل سرویس‌دهنده‌ها
		سیستم عامل میزبان‌ها
		سیستم عامل نهفته
		نرم‌افزارهای پایه
	زیرساخت محتوایی	شبکه تحویل محتوا (CDN)
		سامانه‌های ذخیره‌سازی محتوا
		درگاه خدمات اینترنتی
	زیرساخت تشکیلاتی	تشکیلات مدیریت زیرساخت
		تشکیلات مدیریت خدمات

ماهیت		
دسته اصلی	دسته فرعی	نوع
		تشکیلات مدیریت محتوا
		تشکیلات امنیت زیرساخت
		تشکیلات امنیت خدمات
		تشکیلات امنیت محتوا
خدمات سایبری	خدمات ارتباطی	خدمت ارتباطی بدون پروتکل
		خدمت ارتباطی مبتنی بر پروتکل IP
		شبکه خصوصی مجازی
		خدمت ابری IaaS
	خدمات رایانشی	خدمات میزبانی در مرکز داده
		خدمات ابری PaaS
		خدمات اشتراک‌گذاری اطلاعات
	خدمات نرم‌افزاری پایه	خدمات نام دامنه
		خدمات پیام‌رسانی
		خدمات مرور وب
		خدمات جویش اینترنتی
		خدمات پرداخت اینترنتی
		خدمات پست الکترونیکی
		خدمات ابری SaaS
	خدمات محتوایی	خدمت تأمین و تحویل محتوای متنی زنده
		خدمت تأمین و تحویل محتوای صوتی زنده
		خدمت تأمین و تحویل محتوای ویدیوئی زنده
		خدمت تأمین و تحویل محتوای ویدیوئی زنده
		خدمت تأمین و تحویل محتوای متنی مبتنی بر تقاضا
		خدمت تأمین و تحویل محتوای صوتی مبتنی بر تقاضا
		خدمت تأمین و تحویل محتوای ویدیوئی مبتنی بر تقاضا
		خدمت تأمین و تحویل محتوای ویدیوئی مبتنی بر تقاضا
		پایگاه داده متنی
		پایگاه داده صوتی
		پایگاه داده تصویری

ماهیت		
دسته اصلی	دسته فرعی	نوع
		پایگاه داده ویدیوئی
	پرسنل سایبری	پرسنل مدیریت زیرساخت
		پرسنل مدیریت خدمات
		پرسنل مدیریت محتوا
		پرسنل امنیت زیرساخت
		پرسنل امنیت خدمات
		پرسنل امنیت محتوا
		کاربران خدمات ارتباطی
		کاربران خدمات رایانشی
		کاربران خدمات نرم‌افزاری
		کاربران خدمات محتوایی
محتوای سایبری	پیکربندی تجهیزات	
	اطلاعات پردازشی و ذخیره‌ای	
	تنظیمات نرم‌افزاری	
	محتوای مبادله‌ای	
	داده‌های هویتی	

۵-۱- آشنایی با پایگاه داده سرشماری سکوی مشترک (CPE)

متولیان مدیریت امنیت و دفاع سایبری کشورها، به‌منظور برنامه‌ریزی و هدایت نظام امنیت فضای سایبر و نظام دفاع سایبری، نیازمند اطلاعات صحیح، دقیق و به‌روز از سرمایه‌های سایبری کشور خود، به‌ویژه در حوزه‌ی زیرساخت‌های حیاتی می‌باشند. برای این منظور، در اغلب کشورها، پایگاه داده سرمایه‌های سایبری شکل می‌گیرد، لیکن چنین پایگاه داده‌هایی، از محرمانگی برخوردار بوده و برای دسترسی به اطلاعات آن، کنترل‌ها و محدودیت‌هایی اعمال می‌شود.

معتبرترین پایگاه داده سرمایه‌های سایبری قابل دسترس برای عموم کاربران و متخصصین امنیت و دفاع سایبری، پایگاه داده سرشماری سکوی مشترک[۱] (CPE) است.

پایگاه داده سرشماری سکوی مشترک (CPE)، حاوی «اطلاعات محصولات و سکوهای فناوری اطلاعات در فرمت استاندارد و قابل خوانش توسط ماشین»، «مجموعه‌ای از رویه‌های مقایسه‌ی اسامی»، «یک زبان برای ساخت جملات کاربردپذیر از ترکیب نام‌های CPE با عملگرهای منطقی ساده» و «یک واژه‌نامه‌ی CPE استاندارد» است.

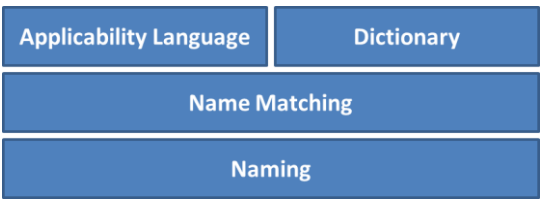
---

۱ Common Platform Enumeration (CPE)

پایگاه داده سرشماری سکوی مشترک (CPE)، توسط شرکت غیرانتفاعی MITRE ایجاد شد، لیکن از سال ۲۰۱۴، مالکیت این پایگاه داده، به همراه واژه‌نامه، ساختار استاندارد شده و مجوز تمامی نرم‌افزارها و سکوهای مورد استفاده، توسط این شرکت به مؤسسه ملی استاندارد و فناوری (NIST) ایالات متحده آمریکا منتقل شده است و اداره‌ی این پایگاه داده، که همچنان بر اساس ساختار CPE است، توسط مؤسسه NIST انجام می‌شود. این پایگاه داده، در حال حاضر، بالغ بر ۱۰۰ هزار رکورد مربوط به سرمایه‌های سایبری سرشماری شده را در خود جای داده است. به‌روز رسانی این پایگاه داده به‌صورت پیوسته در حال انجام است، به طوری که ۹ ماه اول سال ۲۰۱۸، بالغ بر ۲۷ هزار رکورد جدید متعلق به تعداد ۲۷۲ محصول جدید و تعداد ۱۵۵ فروشنده‌ی جدید به این پایگاه داده افزوده شده است و بالغ بر ۳۰ هزار رکورد نیز در آن مورد ویرایش قرار گرفته است.

۱-۵-۱. مشخصات سرشماری سکوی مشترک (CPE)

نسخه شماره ۲.۳، آخرین نسخه از مشخصات نام‌گذاری سکوی مشترک است که ساختار منطقی و استاندارد را برای نام‌گذاری رده‌های محصولات مختلف فناوری اطلاعات، به همراه روشی برای تبدیل این نام‌ها به کدهای قابل خوانش توسط ماشین و بالعکس ارائه نموده است. این نسخه، الزاماتی را برای انجام نام‌گذاری CPE محصولات مختلف فناوری اطلاعات، تعریف نموده است. ساختار پشته‌ی CPE در شکل (۱-۱) نمایش داده شده است. بر اساس این ساختار، CPE از چهار بخش با عناوین مشخصات نام‌گذاری، مشخصات تطبیق نام، مشخصات زبان کاربردپذیر و مشخصات لغت‌نامه تشکیل شده است.



شکل (۱-۳) : ساختار پشته‌ی CPE

مشخصات نام‌گذاری[۱] CPE، حاوی مفاهیم پایه و قواعد نوشتاری نام‌های مورد استفاده برای سرمایه‌های سایبری در پایگاه داده CPE، مشخصات یک نام خوش‌تعریف[۲] (WFN) و چگونگی تبدیل فرمت یک نام خوش‌تعریف به دو فرمت شناسایی‌کننده‌ی منابع یک‌شکل[۳] (URI) و رشته فرمت‌شده[۴] است.

مشخصات تطبیق نام[۵] CPE، حاوی روش‌هایی برای مقایسه‌ی نام‌های CPE است. این روش‌ها، نتیجه‌ی مقایسه را در قالب چهار گزینه‌ی برابر، زیرمجموعه، بالامجموعه و مجزّا اعلام می‌نمایند.

---

۱ Naming Specification
۲ Well-Formed CPE Name (WFN)
۳ Uniform Resource Identifier
۴ Formatted string
۵ Name Matching Specification

مشخصات لغت‌نامه[۱]، حاوی مدل داده و الزامات ایجاد و نگهداری نام‌های CPE در قالب یک لغت‌نامه است.

مشخصات زبان کاربردپذیر[۲] CPE، زبانی برای ایجاد و بهره‌گیری از عبارات زبانی کاربردپذیر[۳]، به همراه یک سکوی حاوی ترکیبی از نام‌های CPE به همراه عملگرهای «و»، «یا» و «نه» در میان آنها است.

۲-۵-۱. انواع نام‌گذاری در پایگاه داده سرشماری سکوی مشترک (CPE)

ساختار نام CPE، ترکیبی از یازده ویژگی سرمایه سایبری مورد نظر، با عناوین بخش (Part)، فروشنده (Vendor)، محصول (Product)، نسخه (Version)، به‌روز رسانی (Update)، ویرایش (Edition)، زبان (Language)، ویرایش نرم‌افزار (SW_Edition)، نرم‌افزار هدف (Target_SW)، سخت‌افزار هدف (Target_HW) و سایر (Other) است که با همین ترتیب، به دنبال یکدیگر قرار می‌گیرند و نام CPE آن سرمایه سایبری را می‌سازند. هر یک از این ویژگی‌ها، می‌تواند حداکثر یک‌مرتبه در ساختار نام CPE قرار بگیرد.

در ساختار نام‌گذاری CPE، بخش (Part)، نمایانگر آن است که این سرمایه، در کدام دسته از سرمایه‌های سایبری، طبقه‌بندی شده است. مقادیر «h» برای سخت‌افزار، «o» برای سیستم عامل و «a» برای کاربرد به این بخش از نام CPE تخصیص داده می‌شود.

در پایگاه داده سرشماری سکوی مشترک (CPE)، نمایش نام CPE، بر اساس سه فرمت نام خوش‌تعریف[۴] (WFN)، شناسایی‌کننده‌ی منابع یک‌شکل[۵] (URI) و رشته‌ی فرمت‌شده انجام می‌گیرد که همگی از ساختار ۱۱ بخشی فوق‌الذکر، تبعیت می‌نمایند و تنها نحوه‌ی قرارگیری این ۱۱ بخش در کناز یکدیگر برای ساختن نام CPE یک سرمایه سایبری، در این سه فرمت، متفاوت است.

نام‌گذاری CPE بر اساس ساختار WFN، مطابق ساختار زیر است :

wfn:[a۱=v۱, a۲=v۲, …, an=vn]

که در آن، aiها عبارت از ویژگی‌های یازده گانه می‌باشند و viها نیز عبارت از مقادیر تخصیص یافته به هر یک از این ویژگی‌ها می‌باشند.

برای مثال، نام‌گذاری مرورگر اینترنت شرکت مایکروسافت نسخه ۸.۰.۶۰۰۱ به‌روزرسانی Beta (فاقد ویرایش) بر اساس ساختار WFN، عبارت است از :

wfn:[part="a", vendor="microsoft", product="internet_explorer", version="۸\.۰\.۶۰۰۱", update="beta", edition=NA]

همچنین مرورگر اینترنت شرکت مایکروسافت نسخه ۸.* به‌روزرسانی ?SP (فاقد ویرایش و تمام زبان‌ها)

wfn:[part="a", vendor="microsoft", product="internet_explorer", version="۸\.*",

---

۱ Dictionary Specification
۲ Applicability Language Specification
۳ Applicability language statements
۴ Well-Formed CPE Name (WFN)
۵ Uniform Resource Identifier

update="sp?", edition=NA, language=ANY]

به‌منظور ذخیره‌سازی، دریافت و تغییر اطلاعات موجود در پایگاه داده CPE، بر اساس ساختار WFN، سه تابع new()، get(w, a) و set(w, a, v) مورد استفاده قرار می‌گیرند. تابع new()، منجر به ایجاد یک رکورد WFN جدید می‌شود، تابع get(w, a)، مقدار تخصیص یافته به ویژگی a در رکورد برابر ویژگی‌های w در پایگاه داده را برمی‌گرداند و تابع set(w, a, v) نیز مقدار v را در ویژگی a از رکورد برابر ویژگی‌های w ذخیره می‌کند.

برای مثال، استفاده از تابع زیر، نتیجه‌ی "microsoft" را برمی‌گرداند.

get(wfn:[vendor="microsoft",product="internet_explorer"],vendor) → "microsoft"

همچنین استفاده از تابع زیر برای تنظیم ویژگی فروشنده، نتیجه‌ی wfn:[vendor="adobe"] را برمی‌گرداند.

set(wfn:[vendor="microsoft"],vendor,"adobe") → wfn:[vendor="adobe"]

نام‌گذاری CPE بر اساس ساختار شناسایی‌کننده‌ی منابع یک‌شکل (URI)، مطابق ساختار زیر است :

cpe-name = "cpe:/" component-list
component-list = part ":" vendor ":" product ":" version ":" update ":" edition ":" lang

بر این اساس، نام‌گذاری مرورگر اینترنت شرکت مایکروسافت نسخه ۸.۰.۶۰۰۱ به‌روزرسانی Beta (فاقد ویرایش)، بر اساس فرمت شناسایی‌کننده‌ی منابع یک‌شکل (URI)، عبارت است از :

cpe:/a:microsoft:internet_explorer:۸٫۰٫۶۰۰۱:beta

همچنین نام‌گذاری CPE بر اساس ساختار رشته‌ی فرمت‌شده، مطابق ساختار زیر است :

cpe:۲٫۳: part : vendor : product : version : update : edition : language : sw_edition : target_sw : target_hw : other

و به این ترتیب، نام‌گذاری مرورگر اینترنت شرکت مایکروسافت نسخه ۸.۰.۶۰۰۱ به‌روزرسانی Beta (فاقد ویرایش)، بر اساس فرمت رشته، به شکل زیر خواهد بود :

cpe:۲٫۳:a:microsoft:internet_explorer:۸٫۰٫۶۰۰۱:beta:*:*:*:*:*:*:*

۶-۱- شناسایی و طبقه‌بندی سرمایه‌های سایبری

برای طبقه‌بندی یا دسته‌بندی سرمایه‌های سایبری، استفاده از سه ویژگی ماهیت، حساسیّت و ارزش اقتصادی، کفایت می‌کند، لیکن داشتن این سه ویژگی در مورد یک سرمایه سایبری، نمی‌تواند آن سرمایه را به صورت یکتا از بین

تمام سرمایه‌های سایبری سازمان، مشخص و متمایز نماید. به همین دلیل، برای شناسایی سرمایه‌های سایبری یک سازمان، لازم است جدولی مطابق جدول (۱-۲) تشکیل دهیم. در این جدول، شناسایی سرمایه‌های سایبری، بر اساس دسته‌بندی ماهیتی یا کارکردی انجام می‌شود، لیکن در ادامه، تمام ویژگی‌های آن سرمایه، اعم از میزان حساسیّت و ارزش اقتصادی، برای تک‌تک سرمایه‌های سایبری، احصاء و در جدول درج می‌گردد.

از آنجا که تأمین امنیت برای یک سرمایه سایبری با ارزش انجام می‌گیرد، اولین گام از امن‌سازی سرمایه‌های سایبری، گام «شناسایی و طبقه‌بندی سرمایه‌های سایبری[۱]» است.

جدول (۱-۲) : لیست سرمایه‌های سایبری شناسایی و طبقه‌بندی شده‌ی سازمان

ماهیت			ویژگی‌ها									
دسته اصلی	دسته فرعی	نوع	نام	کد[۲]	فروشنده	نسخه	ویرایش	به‌روز رسانی	زبان	میزان حساسیّت (اهمیّت)	میزان ارزش اقتصادی
زیرساخت سایبری	زیرساخت ارتباطی	کابل‌های مسی									
		خطوط فیبر نوری									
		تجهیزات دسترسی به شبکه									
		تجهیزات ارتباط رادیویی									
		تجهیزات ارتباط ماهواره‌ای									
		سوئیچ‌ها									
		مسیریاب‌ها									
		تجهیزات گذرگاه ارتباط با اینترنت									
		تجهیزات مدیریت شبکه									

[۱] Cyber Asset Identification and Classification

[۲] کد اختصاصی سرمایه، اعم از کد CPE

ماهیت			ویژگی‌ها								
دسته اصلی	دسته فرعی	نوع	نام	کد[۲]	فروشنده	نسخه	ویرایش	به‌روز رسانی	زبان	میزان حساسیّت (اهمیّت)	میزان ارزش اقتصادی
		تجهیزات امنیت شبکه									
		تجهیزات کنترل صنعتی									
	زیرساخت رایانشی	تجهیزات مرکز داده									
		تجهیزات خدمات ابری									
		سرویس‌دهنده‌ها									
		ایستگاه‌های کاری									
	زیرساخت نرم‌افزاری	شبکه‌ی نرم‌افزار تعریف (SDN)									
		سیستم عامل تجهیزات ارتباطی									
		سیستم عامل تجهیزات رایانشی									
		سیستم عامل سرویس‌دهنده‌ها									
		سیستم عامل میزبان‌ها									
		سیستم عامل نهفته									
		نرم‌افزارهای پایه									
	زیرساخت محتوایی	شبکه تحویل محتوا (CDN)									

ماهیت			ویژگی‌ها								
دسته اصلی	دسته فرعی	نوع	نام	کد [۲]	فروشنده	نسخه	ویرایش	به‌روز رسانی	زبان	میزان حساسیّت (اهمیّت)	میزان ارزش اقتصادی
		سامانه‌های ذخیره-سازی محتوا									
		درگاه خدمات اینترنتی									
	زیرساخت تشکیلاتی	تشکیلات مدیریت زیرساخت									
		تشکیلات مدیریت خدمات									
		تشکیلات مدیریت محتوا									
		تشکیلات امنیت زیرساخت									
		تشکیلات امنیت خدمات									
		تشکیلات امنیت محتوا									
خدمات سایبری	خدمات ارتباطی	خدمت ارتباطی بدون پروتکل									
		خدمت ارتباطی مبتنی بر پروتکل IP									
		شبکه خصوصی مجازی									
		خدمت ابری IaaS									
	خدمات رایانشی	خدمات میزبانی در مرکز داده									
		خدمات ابری PaaS									

ماهیت			ویژگی‌ها								
دسته اصلی	دسته فرعی	نوع	نام	کد[۲]	فروشنده	نسخه	ویرایش	به‌روز رسانی	زبان	میزان حساسیّت (اهمیّت)	میزان ارزش اقتصادی
		خدمات اشتراک- گذاری اطلاعات									
	خدمات نرم‌افزاری پایه	خدمات نام دامنه									
		خدمات پیام‌رسانی									
		خدمات مرور وب									
		خدمات جویش اینترنتی									
		خدمات پرداخت اینترنتی									
		خدمات پست الکترونیکی									
		خدمات ابری SaaS									
	خدمات محتوایی	خدمت تأمین و تحویل محتوای متنی زنده									
		خدمت تأمین و تحویل محتوای صوتی زنده									
		خدمت تأمین و تحویل محتوای ویدیوئی زنده									
		خدمت تأمین و تحویل محتوای ویدیوئی زنده									

ماهیت			ویژگی‌ها								
دسته اصلی	دسته فرعی	نوع	نام	کد [۲]	فروشنده	نسخه	ویرایش	به‌روز رسانی	زبان	میزان حساسیّت (اهمیّت)	میزان ارزش اقتصادی
		خدمت تأمین و تحویل محتوای متنی مبتنی بر تقاضا									
		خدمت تأمین و تحویل محتوای صوتی مبتنی بر تقاضا									
		خدمت تأمین و تحویل محتوای ویدیوئی مبتنی بر تقاضا									
		خدمت تأمین و تحویل محتوای ویدیوئی مبتنی بر تقاضا									
		پایگاه داده متنی									
		پایگاه داده صوتی									
		پایگاه داده تصویری									
		پایگاه داده ویدیوئی									
	پرسنل سایبری	پرسنل مدیریت زیرساخت									
		پرسنل مدیریت خدمات									
		پرسنل مدیریت محتوا									

ماهیت			ویژگی‌ها								
دسته اصلی	دسته فرعی	نوع	نام	کد[۲]	فروشنده	نسخه	ویرایش	به‌روز رسانی	زبان	میزان حساسیّت (اهمیّت)	میزان ارزش اقتصادی
		پرسنل امنیت زیرساخت									
		پرسنل امنیت خدمات									
		پرسنل امنیت محتوا									
		کاربران خدمات ارتباطی									
		کاربران خدمات رایانشی									
		کاربران خدمات نرم‌افزاری									
		کاربران خدمات محتوایی									
محتوای سایبری	پیکربندی تجهیزات										
	اطلاعات پردازشی و ذخیره‌ای										
	تنظیمات نرم‌افزاری										
	محتوای مبادله‌ای										
	داده‌های هویتی										

۷-۱- توصیه‌های ضروری

به‌منظور مدیریت صحیح سرمایه‌های سایبری، لازم است :

۱. لیست کامل و دسته‌بندی شده‌ای از کلیه سرمایه‌های سایبری سازمان، تهیه نمائید. بهتر است در این لیست، سرمایه‌های سایبری در دسته‌هایی مانند مطابق جدول (۱-۲) تفکیک شده باشند.

۲. برای هر یک از سرمایه‌های سایبری موجود در لیست، ارزش اقتصادی تقریبی، شامل هزینه‌ی خرید، تست، نصب، راه‌اندازی و ورود اطلاعات را محاسبه و درج نمائید. برای سادگی، می‌توانید ارزش اقتصادی سرمایه‌های سایبری سازمان خود را در ۵ سطح طبقه‌بندی نموده و از عبارات خیلی‌زیاد، زیاد، متوسط، کم و خیلی‌کم یا از عبارات خیلی‌پرهزینه، پرهزینه، هزینه‌متوسط، کم‌هزینه و خیلی‌کم‌هرینه برای این امر، استفاده نمائید.

۳. برای هر یک از سرمایه‌های سایبری موجود در لیست، میزان حساسیت یا اهمیت آن سرمایه در ارتباط با اجرای مأموریت‌های سازمان خود را تعیین نمائید. برای این منظور، می‌توانید از سطوح کیفی خیلی‌زیاد، زیاد، متوسط، کم و خیلی‌کم استفاده نمائید.

٤. به‌صورت مداوم و دوره‌ای، اقدام به بازنگری و به‌روزرسانی اطلاعات لیست تهیه شده از سرمایه‌های سایبری سازمان خود نمائید. زمان مناسب برای این منظور، دوره‌های زمانی سه‌ماهه است.

٥. توجه داشته باشید که لیست تکمیل‌شده‌ی سرمایه‌های سایبری، حاوی اطلاعات ارزشمندی است و در صورتی که سازمان شما از دستگاه‌های حیاتی، حساس یا مهم است، این لیست، حتماً باید جزء اسناد طبقه‌بندی شده محسوب گردد. سطح طبقه‌بندی این لیست، باید توسط خود شما و بر اساس ضوابط طبقه‌بندی اطلاعات، تعیین گردد.

فصل دوّم

آسیب‌پذیری سایبری

اهداف آموزشی پیش‌بینی شده برای این فصل، عبارتند از :

۱. کسب شناخت و توانایی تعیین شدّت آسیب‌پذیری
۲. کسب شناخت و توانایی به‌کارگیری ابزارهای پویش آسیب‌پذیری
۳. کسب شناخت و بهره‌گیری از پایگاه‌های داده آسیب‌پذیری

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

۱. انواع آسیب‌پذیری‌ها
۲. روش فراگیر تعیین شدّت آسیب‌پذیری
۳. انواع پویش‌گر آسیب‌پذیری
٤. نحوه‌ی انتخاب پویش‌گر مناسب
٥. نحوه‌ی استفاده از پویش‌گر برای شناسایی آسیب‌پذیری
٦. انواع پایگاه داده آسیب‌پذیری
۷. نحوه‌ی انتخاب پایگاه داده مناسب آسیب‌پذیری
۸. نحوه‌ی استفاده از پایگاه داده آسیب‌پذیری برای شناخت ویژگی‌ها و رفع آسیب‌پذیری‌های شناسایی شده
۹. شرایط و روش استفاده از تیم تست نفوذ برای شناسایی آسیب‌پذیری
۱۰. اقدامات دوره‌ای ضروری برای مدیریت آسیب‌پذیری سرمایه‌های سایبری سازمان

۱-۲- تعریف آسیب‌پذیری سایبری

آسیب‌پذیری، ضعفی است که در یک سرمایه سایبری یا مکانیزم‌های امنیتی آن سرمایه وجود دارد و می‌تواند توسط یک یا چند تهدید، مورد بهره‌برداری قرار گیرد. به این ترتیب، آسیب‌پذیری یک ویژگی داخلی سرمایه سایبری است و برای ترمیم یا رفع آن، باید از کنترل‌های امنیتی استفاده نمود. این کنترل‌ها، می‌توانند در داخل یا خارج از سرمایه سایبری پیاده‌سازی شوند. این‌که برای رفع آسیب‌پذیری از کدام نوع کنترل امنیتی استفاده شود، بستگی به نوع آسیب‌پذیری دارد.

۲-۲- انواع آسیب‌پذیری سایبری

آسیب‌پذیری‌ها، از نظر زمان ایجاد، منشأ یا عامل ایجاد، انگیزه‌ی ایجاد، پیامد و وضعیت کشف و استفاده، قابل دسته‌بندی می‌باشند.

۲-۳- انواع آسیب‌پذیری، از نظر زمان ایجاد

آسیب‌پذیری در داخل سرمایه سایبری ایجاد می‌شود و زمان ایجاد آسیب‌پذیری، یکی از مراحل چرخه‌ی حیات سرمایه سایبری است. چرخه‌ی حیات توسعه‌ی سامانه[۱] (SDLC)، در کلی‌ترین حالت، شامل مراحل «مطالعه»، «تعریف یا تعیین ویژگی‌ها»، «طراحی»، «پیاده‌سازی»، «یکپارچه‌سازی و تست» و «بهره‌برداری و نگهداری» است، لیکن این مراحل قابل طبقه‌بندی در سه دسته‌ی «طراحی» (شامل ۳ مرحله اول)، پیاده‌سازی (شامل مراحل ۴ و ۵) و «بهره‌برداری [و نگهداری]» نیز می‌باشند. بر این اساس، یک آسیب‌پذیری، ممکن است در مرحله‌ی طراحی، مرحله‌ی پیاده‌سازی، یا در مرحله‌ی بهره‌برداری ایجاد شده باشد.

آسیب‌پذیری ایجاد شده در مرحله‌ی طراحی، ناشی از اشتباه طراح یا ابزار طراحی است. اشتباه در طراحی معماری یک شبکه، به نحوی که منجر به فراهم نمودن امکان دسترسی غیرمجاز یک هکر بیرونی به میزبان‌های داخلی آن شبکه شود، یک آسیب‌پذیری از این نوع محسوب می‌شود. مرکز ماهر، در تاریخ ۱۳۹۴/۵/۱۷ یک آسیب‌پذیری را با کد IRCNE۲۰۱۵۰۸۲۵۹٤ منتشر نمود و اعلام کرد اطلاعات این آسیب‌پذیری، یک هفته قبل، در کنفرانس هکرهای کلاه سیاه، افشاء شده است. ماجرای این آسیب‌پذیری به سال ۱۹۹۷ برمی‌گردد که شرکت اینتل، یک پردازنده ۳۲ بیتی خود را به‌روز رسانی نمود و یک ویژگی به آن افزود. در طراحی معماری این پردازنده، اشتباهی رخ داده است که به مهاجمان اجازه می‌دهد تا روت کیتی را در میان‌افزار سطح پایین رایانه‌ای که از این پردازنده استفاده می‌کند، نصب نمایند. روت کیت نصب شده با استفاده از این آسیب پذیری، توسط محصولات امنیتی متعارف، قابل شناسایی نیست. شناسایی آسیب‌پذیری‌های ناشی از طراحی، توسط بهره‌بردار، بسیار دشوار است و معمولاً این امر، توسط آزمایشگاه‌های ارزیابی و اعتبارسنجی محصولات سایبری انجام می‌گیرد. البته مشکل اصلی این نوع آسیب‌پذیری، رفع آن است که معمولاً نیازمند بازطراحی و ارزیابی مجدد است که زمان و هزینه‌ی بالایی را در پی خواهد داشت.

---

[۱] System Development Life Cycle (SDLC)

دسته‌ی دوم آسیب‌پذیری‌ها، در اثر بروز خطا یا اشتباه، در مرحله‌ی پیاده‌سازی شبکه یا سامانه‌ی موردنظر، ایجاد می‌شوند. این نوع آسیب‌پذیری‌ها، چنانچه در مرحله‌ی تست محصول توسط سازنده یا آزمایشگاه ارزیابی و اعتبارسنجی تشخیص داده شوند، قبل از ارائه‌ی محصول به بازار، توسط سازنده رفع می‌شوند، لیکن محصول دارای این نوع آسیب‌پذیری به بازار عرضه شده و مورد بهره‌برداری قرار گیرد، پس از تشخیص آسیب‌پذیری که ممکن است توسط سازنده، آزمایشگاه ارزیابی و اعتبارسنجی یا کاربر نهایی انجام گیرد، سازنده اقدام به طراحی و ارائه وصله‌ی امنیتی برای رفع آن آسیب‌پذیری می‌کند و از طریق آگاهی‌رسانی امنیتی، کاربر را از وجود آسیب‌پذیری مطلع نموده و از او می‌خواهد که با نصب وصله‌ی امنیتی، از بروز مخاطره، پیش‌گیری نماید.

اما دسته‌ی سوم آسیب‌پذیری‌ها، ناشی از مرحله‌ی بهره‌برداری، می‌باشند. این نوع آسیب‌پذیری، ناشی از خطای مدیر شبکه یا سامانه، مدیر یا کارشناس امنیت شبکه یا سامانه و در مواردی هم کاربر نهایی، در پیکربندی، تنظیم یا استفاده از فضای سایبر، محصولات یا خدمات سایبری است. شایع‌ترین آسیب‌پذیری بهره‌برداری، استفاده از رمز عبور پیش‌فرض در محصولات سایبری خریداری شده است. متأسفانه این امر، علاوه بر عموم کاربران، حتی در میان مدیران و کارشناسان شبکه و امنیت شبکه نیز شایع است. استفاده از پروتکل ارتباطی فاقد مکانیزم‌های امنیتی، بویژه در ارتباطات بی‌سیم در محیط‌های قابل دسترس توسط مهاجمین و از جمله در مودم‌های WiFi، یا بهره‌گیری از این نوع پروتمل‌ها در ارتباط میزبان‌های پست الکترونیکی یا سامانه‌های اطلاعاتی سازمانی که اطلاعات آن‌ها از طریق شبکه‌ی اینترنت مبادله می‌شود، نمونه‌های دیگری از این نوع آسیب‌پذیری می‌باشند. تشخیص این دسته از آسیب‌پذیری‌ها، نیازمند انجام پویش امنیتی [۱] با بهره‌گیری از پویش‌گر آسیب‌پذیری [۲] یا انجام ارزیابی امنیتی عملیاتی، با بهره‌گیری از خدمات پیمانکاران دارای صلاحیت در عرضه‌ی خدمات ارزیابی امنیتی است.

۲-٤- انواع آسیب‌پذیری، از نظر منشأ یا عامل ایجاد

در کلی‌ترین حالت، منشأ ایجاد یک آسیب‌پذیری، ممکن است عوامل طبیعی (زلزله، سیل و نظایر اینها)، انسان (به‌عنوان طراح، پیاده‌ساز یا بهره‌بردار) و یا ابزار ماشینی (سخت‌افزار یا نرم‌افزار) مورد استفاده جهت طراحی، پیاده‌سازی، پیکربندی و ...، در سرمایه سایبری موردنظر باشد.

۲-۵- انواع آسیب‌پذیری، از نظر انگیزه‌ی ایجاد

آسیب‌پذیری سایبری، از نظر انگیزه‌ی ایجاد، به دو دسته‌ی عمدی و سهوی تفکیک می‌شود. آسیب‌پذیری سهوی، در اثر بُروز خطا یا اشتباه بوجود می‌آید و آسیب‌پذیری عمدی بر اساس یک نیّت بدخواهانه و با هدف بهره‌برداری بعدی توسط مهاجمی که از آن آسیب‌پذیری اطلاع دارد، ایجاد می‌شود.

۲-٦- انواع آسیب‌پذیری، از نظر پیامد

---

[۱] Vulnerability Scanning

[۲] Vulnerability Scanner

آسیب‌پذیری سایبری، از نظر پیامد، در حالت کلّی به دو دسته‌ی مخرّب و غیرمخرّب تفکیک می‌شود. آسیب‌پذیری غیرمخرّب، آسیب‌پذیری است که در صورت مورد بهره‌برداری قرار گرفتن، موجب بُروز خرابی یا نابودی سرمایه نشود. البته تخریب، یکی از پیامدهای آسیب‌پذیری محسوب می‌شود. آسیب‌پذیری ممکن است موجب «افشاء»، «دسترسی غیرمجاز»، «ممانعت از دسترسی/از کار انداختن»، «دست‌کاری/تغییر» یا «نابودی» شود. بر این اساس، آسیب‌پذیری که موجب افشاء اطلاعات می‌شود، در دسته‌بندی کلی، یک آسیب‌پذیری غیرمخرّب محسوب می‌شود.

۲-۷- انواع آسیب‌پذیری، از نظر وضعیت کشف و استفاده

آسیب‌پذیری سایبری، از نظر وضعیت کشف، به دو دسته‌ی شناخته شده (کشف شده) و ناشناخته (کشف نشده) تفکیک می‌شود. البته چرخه‌ی حیات یا مدل تعالی یک آسیب‌پذیری، از شش مرحله‌ی «ایجاد توسط منشأ»، «کشف»، «بهره‌برداری توسط مهاجم»، «افشاء وجود یا بهره‌برداری»، «عرضه‌ی وصله توسط سازنده» و «رفع / وصله‌زنی توسط استفاده‌کننده» تشکیل می‌شود. لیکن نقطه عطف این چرخه‌ی حیات، کشف شدن آسیب‌پذیری است. شکل (۲-۱)، این ۶ مرحله را در ۸ وضعیت زمانی نشان می‌دهد. از میان مراحل شش‌گانه، مرحله‌ی بهره‌برداری، از نظر زمانی، ممکن است «پس از کشف و قبل از افشاء»، «پس از افشاء و قبل از عرضه‌ی وصله» و یا حتی «پس از عرضه‌ی وصله و قبل از وصله‌زنی» اتفاق بیافتد.

شکل (۲-۱) : شش مرحله چرخه حیات آسیب‌پذیری در هشت وضعیت زمانی

۲-۸- روش‌های شناسایی آسیب‌پذیری سایبری

برای شناسایی آسیب‌پذیری سایبری، چهار روش اصلی، به شرح ذیل، وجود دارد :

۱. مراجع آگاهی‌رسانی و پایگاه‌های داده آسیب‌پذیری این مراجع
۲. پویش آسیب‌پذیری
۳. تست نفوذ

در بخش‌های بعد، این روش‌ها مورد بررسی قرار گرفته‌اند و ابزارهای قابل استفاده برای شناسایی آسیب‌پذیری بر اساس هر روش نیز معرفی شده‌اند.

٤. ارزیابی عملکرد، ارزیابی امنیتی و ارزیابی پدافندی

ارزیابی عملکرد محصولات سایبری با عنوان تائید نمونه[۱]، توسط آزمایشگاه‌های مورد تائید مراجع مقررات‌گذاری کشورها در حوزه‌ی ارتباطات و فناوری اطلاعات انجام می‌شود. در ج.ا.ایران، مرجع مقررات‌گذاری در حوزه‌ی ارتباطات و فناوری اطلاعات، کمیسیون تنظیم مقررات است که ذیل وزارت ارتباطات و فناوری اطلاعات قرار دارد.

ارزیابی امنیتی یا ارزیابی اعتماد به عملکرد[۲] توسط آزمایشگاه‌های ارزیابی امنیتی مورد تائید متولی نظام امنیت فضای تبادل اطلاعات کشورها انجام می‌گیرد که در ج.ا.ایران، مرکز مدیریت راهبردی افتا، متولی مدیریت راهبردی امنیت فضای تبادل اطلاعات کشور است.

همچنین ارزیابی پدافندی محصولات سایبری، توسط آزمایشگاه‌های مورد تائید متولیان نظام دفاع سایبری کشورها انجام می‌گیرد که در ج.ا.ایران، این مسئولیت بر عهده‌ی مرکز پدافند سایبری کشور است.

در سطح بین‌المللی، ارزیابی عملکرد و اعتماد به عملکرد محصولات سایبری، در قالب استاندارد معیارهای مشترک[۳] پیش‌بینی شده است و آزمایشگاه‌های معیارهای مشترک نیز وجود دارند. این استاندارد، ترکیبی از عملکرد و اعتماد به عملکرد محصولات سایبری را مورد سنجش قرار می‌دهد و محصول سایبری موردنظر را در یکی از ۷ سطح پیش‌بینی شده در این استاندارد، طبقه‌بندی نموده و گواهی در سطح مورد تائید به محصول سایبری اعطاء می‌نماید.

جزئیات کامل این روش شناسایی آسیب‌پذیری، در کتاب مباحث تخصصی پیشرفته پدافند سایبری، ارائه شده است.

۹-۲- پویش‌گر آسیب‌پذیری سایبری

پویش‌گرهای آسیب‌پذیری، یکی از متداول‌ترین ابزارها برای شناسایی آسیب‌پذیری‌ها می‌باشند. این ابزارها از طریق اتصال به شبکه اینترنت در خارج از سازمان یا اتصال مستقیم به شبکه ارتباطی سازمان و یا اجرا بر روی یک سامانه‌ی اطلاعاتی یا میزبان خاص، قادر به پویش آسیب‌پذیری‌های موجود در آن شبکه یا سامانه می‌باشند. پویش‌گرهای آسیب‌پذیری یک محدودیت اصلی دارند. این ابزارها، تنها قادر به شناسایی آسیب‌پذیری‌هایی می‌باشند که قبلاً کشف شده‌اند و اطلاعات آن‌ها در پایگاه‌های داده آسیب‌پذیری موجود است. در مقابل، مزیت اصلی پویش‌گرهای آسیب‌پذیری، آن است که شبکه یا سامانه‌ی در حال ارائه خدمت را مورد پویش قرار می‌دهند و برای شناسایی آسیب‌پذیری، نیازی به توقف عملکرد سرمایه سایبری موردنظر نیست. چنانچه سازمان شما در زمره‌ی دستگاه‌های حیاتی، حساس یا مهم کشور است، باید در استفاده از پویش‌گر آسیب‌پذیری، دقت کافی داشته باشید زیرا ممکن است نرم‌افزاری که شما به عنوان پویش‌گر آسیب‌پذیری می‌شناسید و استفاده می‌کنید، در واقع ابزار جاسوسی و جمع‌آوری اطلاعات دشمن باشد، لذا باید توجه داشت تنها از پویش‌گر آسیب‌پذیری مورد تائید مرکز پدافند سایبری کشور استفاده نمائید و در صورتی که تیم داخلی

---

۱ Type Approval (TA)

۲ Assurance

۳ Common Criteria (CC)

سازمان، عملیات پویش را بر عهده ندارد، حتماً در متن قرارداد پیمانکار، نام پویش‌گر آسیب‌پذیری مجاز برای استفاده توسط تیم پیمانکار نیز درج شود.

انواع مختلفی از پویش‌گرها وجود دارند. پویش‌گرهای پورت، پویش‌گرهای آسیب‌پذیری شبکه، پویش‌گرهای کاربردهای مبتنی بر وب، پویش‌گرهای امنیت پایگاه داده و پویش‌گرهای مبتنی بر میزبان، نمونه‌هایی از انواع پویش‌گرها هستند. اخیراً نیز پویش‌گری توسط مرکز امنیت اینترنت[۱] ارائه شده است که کنترل‌های امنیتی حیاتی[۲] را مورد ارزیابی قرار می‌دهد تا پدافند سایبری مؤثر را امکان‌پذیر نماید. این نوع ارزیابی، بر اساس سنجه‌های امنیتی مؤثر انجام می‌شود و پویش‌گر ارائه شده نیز میزان این سنجه‌های امنیتی را در شبکه‌ی سازمان، مورد سنجش قرار می‌دهد.

پویش‌گرهای پورت، از طریق تلاش برای برقراری ارتباط با سامانه‌ی هدف، روی تک‌تک پورت‌های پروتکل TCP/IP، شماره‌ی پورت‌های باز روی سامانه‌ی هدف که مهاجم می‌تواند روی آن‌ها، با سامانه‌ی هدف، ارتباط برقرار نموده و اقدام به تهاجم احتمالی نماید را کشف می‌کند. یک اصل برای پیکربندی امن یک سامانه، بستن تمام پورت‌های غیرضروری روی آن سامانه است. تنها باید پورت‌هایی باز بمانند که برای ارتباط مدیر یا کاربر با سامانه، ضروری هستند. نرم‌افزار NMAP، یک پویش‌گر پورت است که از طریق شناسایی سامانه‌های موجود به یک شبکه، نقشه‌ی شبکه را هم ارائه می‌نماید.

پویش‌گرهای آسیب‌پذیری شبکه، پس از اتصال به شبکه، اقدام به شناسایی تجهیزات و سامانه‌های متصل به شبکه نموده و از طریق برقراری ارتباط با تک‌تک تجهیزات و سامانه‌های شناسایی شده، اقدام به تشخیص آسیب‌پذیری‌های موجود در آنها می‌نمایند. Nessus، Qualys، SAINT، OpenVAS، INFRA Security Scanner، Nexpose و edgescan نمونه‌هایی از پویش‌گر آسیب‌پذیری شبکه می‌باشند.

پویش‌گرهای کاربردهای مبتنی بر وب، به‌منظور شناسایی آسیب‌پذیری‌های موجود در یک برنامه‌ی کاربردی مبتنی بر وب، ارائه می‌شوند. این ابزارها، از طریق وب، اقدام به برقراری ارتباط با کاربرد موردنظر نموده و با انجام تست جعبه سیاه، آسیب‌پذیری‌های موجود در آن کاربرد را شناسایی می‌نمایند. Probe.ly، Nikto، Qualys، Sucuri، High-Tech Bridge، Burp Suite، OWASP ZAP، w۳af و edgescan، نمونه‌هایی از پویش‌گرهای آسیب‌پذیری کاربردهای مبتنی بر وب هستند.

پویش‌گرهای آسیب‌پذیری پایگاه داده، ابزاری اختصاصی برای شناسایی آسیب‌پذیری‌های موجود در یک نرم‌افزار کاربردی پایگاه داده است. به علاوه برای فراهم نمودن کارکردهای بیرونی پایگاه داده از قبیل شکستن رمز عبور، این پویش‌گرها، اقدام به بررسی پیکربندی داخلی پایگاه داده می‌نمایند تا آسیب‌پذیری‌های احتمالاً قابل بهره‌برداری را شناسایی نمایند. پویش‌گر امنیتی پایگاه داده[۳] و مدیر آسیب‌پذیری پایگاه داده[۴]، دو محصول شرکت McAfee می‌باشند.

---

۱ Center fo Internet Security (CIS)

۲ Open Source Vulnerabilities Database (OSVDB)

۳ McAfee Security Scanner for Database

۴ McAfee Vulnerability Manager for Database

پویش‌گرهای مبتنی بر میزبان، روی یک ایستگاه کاری یا میزبان شبکه اجرا می‌شوند و با توجه به دسترسی کاملی که به تمام منابع میزبان دارند، تمام آسیب‌پذیری‌های موجود در میزبان را شناسایی می‌کنند. MBSA مایکروسافت، نمونه‌ای از این پویش‌گرها است.

۲-۱۰- آشنایی با نمونه‌هایی از پویش‌گرهای آسیب‌پذیری سایبری

در این بخش، تعدادی از نرم‌افزارهای پویش‌گر آسیب‌پذیری و حوزه‌ی کاربری آن‌ها، معرفی می‌شوند :

۲-۱۱- پویش‌گر آسیب‌پذیری Nessus

یک پویش‌گر امنیت شبکه برندشده و ثبت‌شده است که علاوه بر پویش و شناسایی آسیب‌پذیری، یک ابزار قدرتمند ارزیابی امنیتی و پیش‌بینی مخاطره نیز محسوب می‌شود. این پویش‌گر، قادر به شناسایی آسیب‌پذیری موجود در محدوده‌ی گسترده‌ای از انواع سیستم‌عامل‌های مختلف، پایگاه‌های داده، نرم‌افزارهای کاربردی، تجهیزات مورد استفاده در زیرساخت ابری و تجهیزات شبکه‌های مجازی و فیزیکی می‌باشد و به‌صورت هم‌زمان، توسط میلیون‌ها کاربر در سطح جهان، مورد استفاده قرار می‌گیرد.

۲-۱۲- پویش‌گر آسیب‌پذیری OpenVAS

یک پویش‌گر متن‌باز است که علاوه بر پویش و شناسایی آسیب‌پذیری، یک ابزار ارزیابی امنیتی و مدیریت آسیب‌پذیری نیز محسوب می‌شود. این پویش‌گر، سیستم‌عامل‌های مختلف را پشتیبانی می‌کند، از به‌روز رسانی مداوم برخوردار است و قادر به شناسایی آسیب‌پذیری انواع تجهیزات شبکه است.

۲-۱۳- پویش‌گر آسیب‌پذیری Retina CS

یک پویش‌گر متن‌باز و برخوردار از کنسول مبتنی بر وب است که علاوه بر پویش و شناسایی آسیب‌پذیری، یک ابزار بسیار ساده و متمرکز برای مدیریت آسیب‌پذیری نیز محسوب می‌شود. این پویش‌گر، امکان ارائه گزارش انطباق، انطباق وصله‌زنی و پیکربندی، امکان ارزیابی آسیب‌پذیری سکوهای متقابل را نیز فراهم آورده است. این ابزار، ارزیابی آسیب‌پذیری در انواع پایگاه‌های داده، کاربردهای مبتنی بر وب، ایستگاه‌های کاری و میزبان‌های ارائه خدمت در شبکه را انجام می‌دهد.

۲-۱۴- پویش‌گر آسیب‌پذیری MBSA[۱]

تحلیل‌گر امنیت پایه مایکروسافت، یک ابزار نرم‌افزاری رایگان متعلق به شرکت مایکروسافت، برای امن‌سازی رایانه‌های مبتنی بر سیستم عامل ویندوز، بر اساس سیاست‌های تعیین‌شده توسط شرکت مایکروسافت است. این ابزار، از طریق پویش به‌روزرسانی‌های انجام شده و Service Packهای نصب شده، اقدام به شناسایی پیکربندی نادرست، فقدان

[۱] Microsoft Baseline Security Analyser (MBSA)

به‌روزرسانی و فقدان نصب وصله‌های امنیتی می‌نماید. این ابزار در خاتمه‌ی پویش، اقدام به ارائه‌ی راه‌حل مناسب برای رفع آسیب‌پذیری‌های شناسایی شده نیز می‌نماید.

۲-۱۵- پویش‌گر آسیب‌پذیری Nexpose

یک ابزار پویش متن‌باز آسیب‌پذیری است. این ابزار، علاوه بر پویش آسیب‌پذیری، اقدام به انجام تعداد زیادی بررسی در شبکه می‌کند، مثلاً در صورت اتصال هر وسیله‌ی جدید به شبکه، این ابزار، اقدام به پویش خودکار آسیب‌پذیری‌های موجود در آن وسیله نموده و آنها را گزارش می‌نماید.

۲-۱۶- پویش‌گر آسیب‌پذیری Tripwire IP۳۶۰

یک محصول ارزیابی مخاطره‌ی تولید شده توسط شرکت Tripwire، به عنوان یکی از شرکت‌های پیشرو در زمینه‌ی ارزیابی امنیتی است. این محصول، آسیب‌پذیری‌ها، پیکربندی‌ها، کاربردها، میزبان‌ها، ایستگاه‌های کاری و ... را در محدوده‌ی گسترده‌ای از شبکه‌ها، شناسایی می‌کند و بر اساس استانداردهای باز، اقدام به مدیریت مخاطره می‌نماید.

۲-۱۷- پایگاه‌های داده آسیب‌پذیری سایبری

مراجع آگاهی‌رسانی حوزه‌ی امنیت و پدافند سایبری، اخبار مربوط به کشف آسیب‌پذیری‌ها، اطلاعاتی در خصوص ویژگی‌های آسیب‌پذیری‌های کشف شده و نحوه‌ی مواجهه یا رفع آن‌ها را ارائه می‌نمایند. این مراجع، عموماً اقدام به ایجاد یک پایگاه داده از آسیب‌پذیری‌ها می‌نمایند که گزارشات مربوط به کشف آسیب‌پذیری‌ها در آن ثبت می‌شود. این اقدام، با هدف تسهیل دسترسی فراگیر متخصصین و عموم بهره‌برداران به اطلاعات آسیب‌پذیری‌ها انجام می‌شود. برخی از این پایگاه داده‌ها نیز متعلق به سازندگان نرم‌افزار یا سخت‌افزارها هستند که گزارشات مربوط به آسیب‌پذیری‌های محصولات خود را در آن ثبت می‌کنند. همچنین متولیان امنیت و دفاع سایبری کشورها نیز اقدام به ایجاد این نوع پایگاه داده‌ها برای اطلاع‌رسانی هماهنگ و فراگیر در سطح ملی می‌نمایند.

ازجمله پایگاه داده‌های معتبر در زمینه آسیب‌پذیری می‌توان به پایگاه داده CVE[۱]، NVD[۲]، Security Focus و Securitytracker اشاره نمود. ضمناً تعدادی پایگاه داده تلفیقی از قبیل CVE Details، Scaprepo و Circl CVE نیز وجود دارند. این پایگاه‌ها، رکورد جدید برای آسیب‌پذیری تشکیل نمی‌دهند، بلکه از ترکیب اطلاعات رکوردهای ثبت شده در پایگاه‌های داده آسیب‌پذیری استفاده می‌نمایند.

مرکز ماهر وزارت ارتباطات و فناوری اطلاعات، یکی از متولیان نظام مقابله با حوادث رایانه‌ای در سطح ملی است که در راستای انجام این مأموریت خود، اقدام به ایجاد یک پایگاه داده از آسیب‌پذیری‌های سایبری نموده است. این مرکز، همچنین آگاهی‌رسانی در خصوص آسیب‌پذیری‌های سایبری را از طرق مختلف، از جمله ارسال پیامک، درگاه اینترنتی، شبکه اختصاصی و مکاتبات اداری، انجام می‌دهد. مرکز پدافند سایبری کشور نیز به‌عنوان متولی مدیریت راهبردی پدافند

---

[۱] Common Vulnerabilities and Exposures (CVE)

[۲] National Vulnerability Database (NVD)

سایبری در سطح ملی، اقدام به ایجاد پایگاه اطلاع‌رسانی پدافند سایبری نموده است و در راستای این مأموریت خود، پایگاه داده‌ای از آسیب‌پذیری‌های سایبری را ایجاد نموده است.

۲-۱۸- آشنایی با نمونه‌هایی از پایگاه‌های داده آسیب‌پذیری سایبری

در این بخش، تعدادی از نرم‌افزارهای پویش‌گر آسیب‌پذیری و حوزه‌ی کاربری آن‌ها، معرفی می‌شوند :

۲-۱۹- پایگاه داده آسیب‌پذیری مشترک (CVE)

تا سال ۱۹۹۹ هر پویش‌گر آسیب‌پذیری و هر سازنده‌ی محصول سایبری، خود اقدام به نام‌گذاری آسیب‌پذیری کشف شده می‌نمود تا این‌که در سال ۱۹۹۹، با حمایت US-CERT، پایگاه داده آسیب‌پذیری‌های مشترک، ایجاد شد. این پایگاه داده، حاوی اطلاعات و ویژگی‌های آسیب‌پذیری‌های کشف‌شده‌ی انواع سرمایه‌های سایبری است. پس از تشکیل وزارت امنیت داخلی و انتقال مراکز مرتبط با امنیت سایبری به این وزارت، اکنون حمایت از این پایگاه داده، توسط اداره‌ی امنیت سایبری و ارتباطات در وزارت امنیت داخلی آمریکا انجام می‌گیرد. در این پایگاه داده، برای هر آسیب‌پذیری، یک رکورد ایجاد می‌شود که حاوی ۴ فیلد اجباری «شناسه»، «توصیف»، «مراجع»، «تخصیص CNA» و «تاریخ ایجاد رکورد» و ۴ فیلد اختیاری «وضعیت»، «آراء»، «تفسیرها» و «پیشنهادها» است.

شرکت غیرانتفاعی MITRE، اداره‌ی امور پایگاه داده آسیب‌پذیری مشترک، پشتیبانی و توسعه سایت CVE، نظارت بر هیأت مدیره[۱] و متولی شماره‌گذاری CVE[۲] (CNA) را بر عهده دارد.

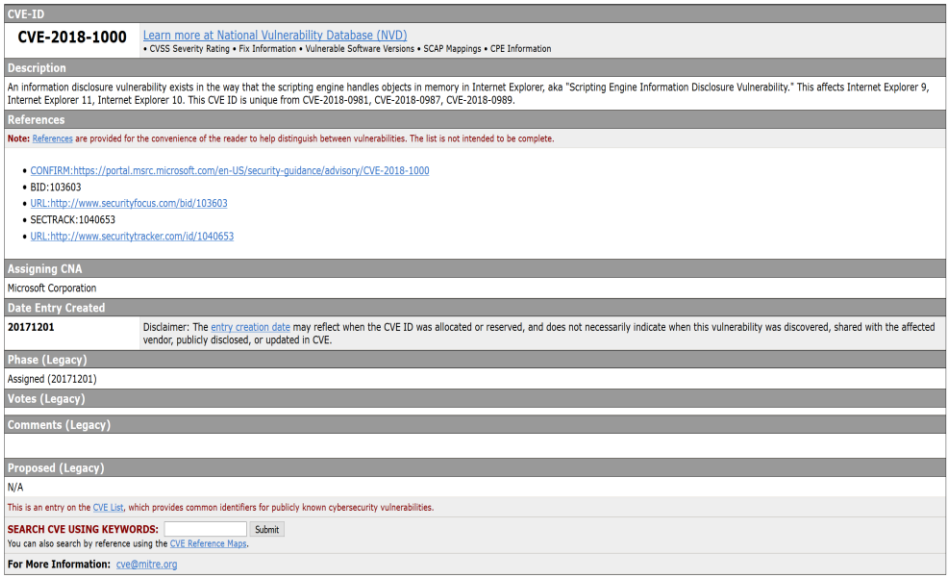
هیأت‌مدیره، متشکل از تعدادی اعضای حقوقی شامل سازمان‌های متولی امنیت سایبری و تولیدکنندگان محصولات امنیت سایبری به همراه تعدادی اعضای حقیقی از میان متخصصین امنیت سایبری است. ورودی‌های حیاتی، اهداف، ساختار و راهبردهای برنامه‌ی آسیب‌پذیری‌های مشترک، توسط هیأت مدیره و تعیین روش شماره‌گذاری شناسه‌ی CVE و فیلد تخصیص CNA به رکورد آسیب‌پذیری، توسط CNA انجام می‌شود.

شکل (۲-۲)، رکورد تشکیل شده برای آسیب‌پذیری شماره CVE-۲۰۱۸-۱۰۰۰ در پایگاه داده آسیب‌پذیری مشترک (CVE) را نمایش می‌دهد.

---

۱ CVE Board

۲ CVE Numbering Authorities (CNA)



CVE-ID

CVE-2018-1000 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An information disclosure vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engine Information Disclosure Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10. This CVE ID is unique from CVE-2018-0981, CVE-2018-0987, CVE-2018-0989.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1000
- BID:103603
- URL:http://www.securityfocus.com/bid/103603
- SECTRACK:1040653
- URL:http://www.securitytracker.com/id/1040653

Assigning CNA

Microsoft Corporation

Date Entry Created

20171201 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20171201)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

شکل (۲–۲) : رکورد آسیب‌پذیری شماره CVE-۲۰۱۸-۱۰۰۰ در پایگاه داده آسیب‌پذیری مشترک (CVE)

- در فیلد شناسه، لینک این آسیب‌پذیری در پایگاه داده‌ی NVD نیز ارائه شده است.
- در فیلد توصیف، این آسیب‌پذیری با عبارت «این آسیب‌پذیری مربوط به افشاء اطلاعات ناشی از روش بکارگرفته شده توسط موتور آغازگر مرور، برای کار با اشیاء در حافظه در مرورگر اینترنت شرکت مایکروسافت (نسخه‌های ۹، ۱۰ و ۱۱) است» توصیف شده است. در فیلد مراجع، سه لینک ارائه شده است. لینک اول به سایت مایکروسافت است، در ادامه، شناسه‌ی این آسیب‌پذیری در پایگاه داده آسیب‌پذیری SecurityFocus به همراه لینک دوم که به این پایگاه داده است، در ادامه نیز شناسه‌ی این آسیب‌پذیری در پایگاه داده آسیب‌پذیری SecurityTracker به همراه لینک سوم که به این پایگاه داده است.
- در فیلد تخصیص، CNA این آسیب‌پذیری را به شرکت مایکروسافت تخصیص داده است.
- در فیلد تاریخ ایجاد، تاریخ ۲۰۱۷/۱۲/۱ درج شده است.
- در فیلد وضعیت، اعلام شده است که این آسیب‌پذیری در تاریخ ۲۰۱۷/۱۲/۱ تخصیص داده شده است.
- فیلد آراء ، خالی است.
- فیلد تفسیرها، خالی است.
- فیلد پیشنهادها هم حاوی گزینه‌ی «هیچ پیشنهادی در دسترس نمی‌باشد» است.

پایگاه داده آسیب‌پذیری مشترک، در حال حاضر، تقریباً حاوی تعداد ۱۲۵ هزار رکورد کاندید و ثبت‌شده می‌باشد و اطلاعات کامل این رکوردها، در فرمت‌های HTML، Text، XML و Comma Separated قابل دسترس می‌باشد. تعداد آسیب‌پذیری‌های کاندید و ثبت‌شده از سال ۱۹۹۹ تا کنون، مطابق جدول (۲-۱) است.

جدول (۲-۱) : تعداد آسیب‌پذیری کاندید و ثبت‌شده در پایگاه داده آسیب‌پذیری مشترک (CVE)

سال	تعداد آسیب‌پذیری	سال	تعداد آسیب‌پذیری	سال	تعداد آسیب‌پذیری	سال	تعداد آسیب‌پذیری
۱۹۹۹	۱۵۹۸	۲۰۰۴	۹۹۹۹	۲۰۰۹	۵۱۵۲	۲۰۱۴	۹۹۹۹
۲۰۰۰	۱۲۵۴	۲۰۰۵	۴۹۰۰	۲۰۱۰	۵۳۲۹	۲۰۱۵	۹۲۶۶
۲۰۰۱	۱۵۹۴	۲۰۰۶	۷۲۵۳	۲۰۱۱	۵۳۷۴	۲۰۱۶	۱۰۰۸۸
۲۰۰۲	۲۴۴۷	۲۰۰۷	۶۷۶۱	۲۰۱۲	۶۷۰۹	۲۰۱۷	۱۰۸۹۵
۲۰۰۳	۱۶۰۵	۲۰۰۸	۷۳۱۹	۲۰۱۳	۷۴۶۴	۲۰۱۸	۱۶۳۱۵

۲۰-۲- پایگاه داده ملی آسیب‌پذیری (NVD)

پایگاه داده ملی آسیب‌پذیری، مخزن اطلاعات مدیریت آسیب‌پذیری متعلق به دولت ایالات متحده آمریکا است که با استفاده از پروتکل خودکارسازی محتوای امنیتی[۱] (SCAP) بازنمایی می‌شود. این پایگاه داده، توسط مؤسسه ملی استاندارد و فناوری (NIST) ایالات متحده آمریکا، در سال ۱۹۸۸ ایجاد و تا کنون پشتیبانی شده است. شماره‌گذاری آسیب‌پذیری در پایگاه داده ملی آسیب‌پذیری، همان شماره‌گذاری CVE است. برای آسیب‌پذیری‌های کشف‌شده طی سال‌های ۱۹۸۸ تا ۱۹۹۹ (زمان تأسیس پایگاه داده CVE)، در سال ۱۹۹۹، شناسه‌ی CVE تخصیص یافته است. بر این اساس، لیست آسیب‌پذیری‌های موجود در این پایگاه داده با پایگاه داده آسیب‌پذیری مشترک، یکسان است، لیکن رکوردی که در NVD برای یک آسیب‌پذیری تشکیل می‌شود، حاوی ۸ فیلد با عناوین «شناسه»، «توصیف کنونی» (به همراه منبع توصیف و تاریخ آخرین تغییر توصیف)، «توصیف تحلیلی» (به همراه منبع توصیف تحلیلی و تاریخ آخرین تغییر توصیف تحلیلی)، «ضربه» یا امتیاز شدت آسیب‌پذیری (به همراه جزئیات امتیاز کلیه سنجه‌ها)، «مراجع» مشاوره، راه‌حل و ابزار، «جزئیات فنی آسیب‌پذیری»، «نام و نسخه نرم‌افزار آسیب‌پذیر» و «تاریخچه‌ی تغییرات» است. شکل (۲-۳)، فیلدهای یک رکورد از پایگاه داده NVD را نمایش می‌دهد.

[۱] Security Content Automation Protocol (SCAP)

CVE-2018-9128 Detail

Current Description

DVD X Player Standard 5.5.3.9 has a Buffer Overflow via a crafted .plf file, a related issue to CVE-2007-3068.

Source: MITRE
Description Last Modified: 04/01/2018
View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 7.8 HIGH
Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 1.8

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:
Base Score: 6.8 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 8.6

Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Victim must voluntarily interact with attack mechanism
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://0day4u.wordpress.com/2018/03/30/buffer-overflow-on-dvd-x-player-standard-5-5-3-9/	Exploit, Third Party Advisory
https://www.exploit-db.com/exploits/44438/	Exploit, Third Party Advisory, VDB Entry

Technical Details

Vulnerability Type (View All)

- Buffer Errors (CWE-119)

Vulnerable software and versions Switch to CPE 2.2

Configuration 1
OR
* cpe:2.3:a:dvd-x-player:dvd_x_player:5.5.3.9:*:*:*:standard:*:*:*

* Denotes Vulnerable Software
Are we missing a CPE here? Please let us know.

Change History

2 change records found - show changes

شکل (۲-۳) : فیلدهای یک رکورد آسیب‌پذیری در پایگاه داده ملی آسیب‌پذیری (NVD)

اصلی‌ترین فیلد این پایگاه داده، فیلد ضربه یا امتیاز شدت آسیب‌پذیری است. امتیازدهی آسیب‌پذیری در این پایگاه داده، بر اساس سامانه‌ی امتیازدهی آسیب‌پذیری مشترک[۱] (CVSS) انجام می‌گیرد. این مدل امتیازدهی، توسط مؤسسه‌ی FIRST ارائه شده است و در حال حاضر، نسخه‌ی ۳,۰ این سامانه منتشر شده است. سامانه‌ی امتیازدهی آسیب‌پذیری مشترک یکی از فراگیرترین مدل‌های امتیازدهی به آسیب‌پذیری‌های کشف‌شده است. این سامانه، یک استاندارد پذیرفته‌شده‌ی فراگیر است که به تحلیل‌گران اجازه می‌دهد که به هر آسیب‌پذیری شناخته شده‌ی قرار گرفته در پایگاه داده ملی آسیب‌پذیری (NVD) و بر اساس شدّت[۲] آن آسیب‌پذیری، یک امتیاز عددی بدهند. این سامانه، شامل سه گروه سنجه‌ی پایه، موقت و محیطی است. در این سامانه به هر آسیب‌پذیری، نهایتاً یک امتیاز پایه[۳] (BS) از صفر تا ۱۰ تخصیص می‌یابد که این امتیاز، بر اساس امتیازهای داده‌شده به سنجه‌های گروه پایه، محاسبه می‌شود. سنجه‌های پایه می‌توانند به مقادیر عددی نگاشت شوند و امتیاز پایه (BS) بر اساس این مقادیر، محاسبه شود.

۲۱-۲- پایگاه داده SecurityFocus

پایگاه داده آسیب‌پذیری SecurityFocus، از سال ۱۹۹۹ تشکیل شده است و اطلاعات جامعی در خصوص آسیب‌پذیری‌های کشف‌شده، به همراه راه‌حل رفع آن‌ها ارائه می‌نماید. مانند سایر پایگاه‌های داده، برای هر آسیب‌پذیری، در این پایگاه داده، یک رکورد تشکیل می‌شود و امکان جستجوی پیشرفته برای هر سازنده، هر محصول و هر کد CVE، فراهم شده است. هر رکورد آسیب‌پذیری در این پایگاه داده، شامل ۵ بخش اصلی «اطلاعات»، «بحث»، «بهره‌برداری»، «راه‌حل» و «مراجع» است. شکل (۲-۴)، یک رکورد آسیب‌پذیری در این پایگاه داده را نشان می‌دهد که حاوی ۵ سربرگ با عناوین Info، Discussion، Exploit، Solution و References است.

سربرگ «اطلاعات»، اصلی‌ترین بخش این رکورد است که حاوی اطلاعات معرفی آسیب‌پذیری است و مطابق شکل (۲-۳)، حاوی فیلدهای «شناسه[۴] (BID)»، «کلاس»، «شناسه‌ی CVE»، «راه دور»، «محلّی»، «تاریخ انتشار»، «تاریخ به‌روزرسانی»، «اعتبار» و «آسیب‌پذیر» می‌باشد.

- فیلد شناسه (BugTraq ID) : حاوی شناسه‌ی یکتایی است که در پایگاه داده SecurityFocus، به آسیب‌پذیری تخصیص داده می‌شود. این شناسه در پایگاه داده آسیب‌پذیری مشترک (CVE) نیز با عنوان BID در رکورد آسیب‌پذیری، درج می‌شود.
- فیلد کلاس (Class) : دسته‌ی آسیب‌پذیری را مشخص می‌کند. در پایگاه داده آسیب‌پذیری SecurityFocus، آسیب‌پذیری‌ها در ۱۰ دسته با عناوین «خطای شرایط مرزی»، «خطای اعتبار دسترسی»، «خطای اعتبار ورودی»، «خطای اعتبار مبدأ»، «عدم برخورد با شرایط استثنایی»، «خطاهای وضعیت مسابقه»، «خطاهای توالی‌سازی»،

---

۱ Common Vulnerability Scoring System (CVSS)
۲ Severity
۳ Base Score (BS)
۴ Bugtraq ID (BID)

«خطاهای اتمی»، «خطاهای محیط» و «خطاهای پیکربندی» دسته‌بندی شده‌اند که در این فیلد، عنوان یکی از این دسته‌ها، ذکر می‌شود.

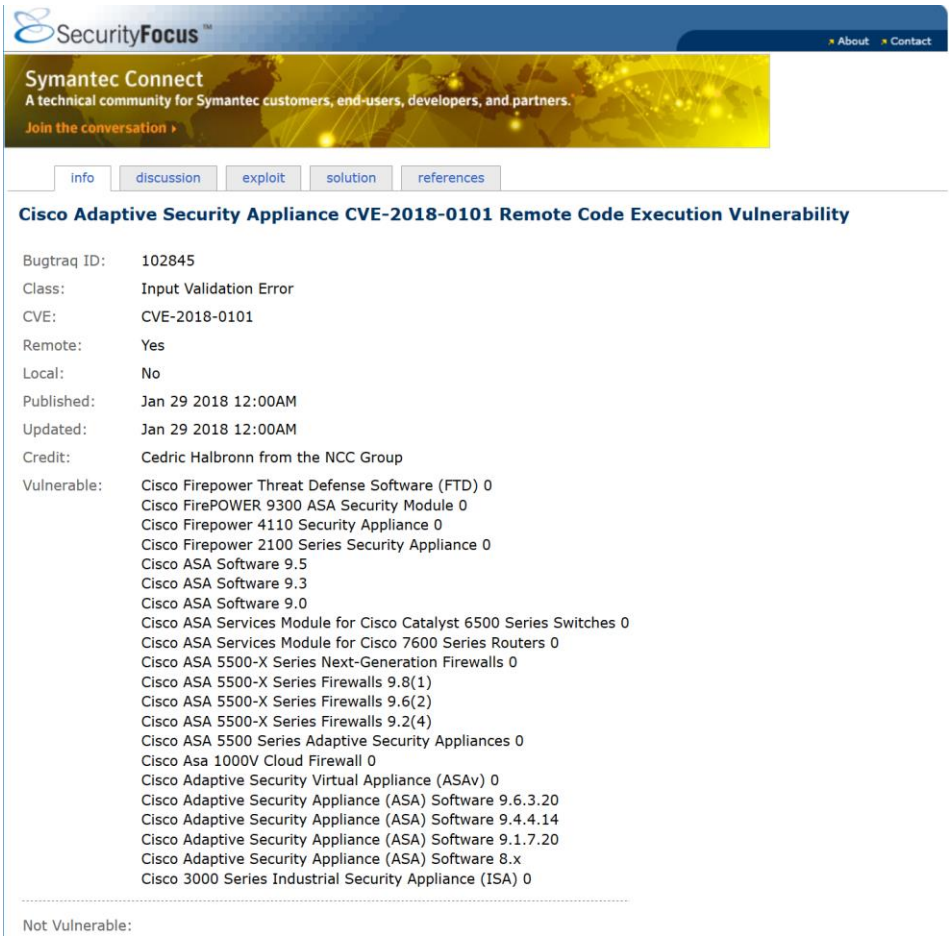
- فیلد شناسه‌ی CVE : حاوی شناسه‌ی CVE است که در پایگاه داده آسیب‌پذیری مشترک (CVE) به این آسیب‌پذیری اختصاص یافته است.
- فیلد راه دور (Remote) : نشان می‌دهد که آسیب‌پذیری از راه دور، قابل دسترس هست یا خیر.
- فیلد محلّی (Local) : نشان می‌دهد که آسیب‌پذیری به‌صورت محلی (از روی سامانه)، قابل دسترس هست یا خیر.
- فیلد تاریخ انتشار (Published) : تاریخ انتشار آسیب‌پذیری (ثبت در پایگاه داده) را نشان می‌دهد.
- تاریخ به‌روزرسانی (Updated) : تاریخ آخرین به‌روز رسانی آسیب‌پذیری و ثبت اطلاعات جدید در خصوص آن آسیب‌پذیری، در پایگاه داده را نشان می‌دهد. این تاریخ، معمولاً تاریخ ثبت راه‌حل و مراجع جدید برای دسترسی متخصصین جهت رفع آسیب‌پذیری است.
- فیلد اعتبار (Credit) : حاوی نام شخص حقیقی یا حقوقی گزارش‌کننده‌ی آسیب‌پذیری است.
- فیلد آسیب‌پذیر (Vulnerable) : حاوی نام سیستم‌عامل‌ها، تجهیزات، نرم‌افزارها و خدماتی است که از این آسیب‌پذیری برخوردار بوده و به عبارت دیگر، آسیب‌پذیر می‌باشند.

سربرگ «**بحث**»، حاوی توصیف آسیب‌پذیری و ارتباط آن با سایر آسیب‌پذیری‌های ثبت‌شده در این پایگاه داده و شناسه‌ی تخصیص یافته به این آسیب‌پذیری، توسط سازنده است.

سربرگ «**بهره‌برداری**»، حاوی اطلاعاتی در خصوص روش‌ها و ابزارهای بهره‌برداری از این آسیب‌پذیری، توسط مهاجم است.

سربرگ «**راه‌حل**»، حاوی اطلاعاتی در خصوص وصله‌های امنیتی و راهنماهایی است که توسط متخصصین، مراکز امدادرسانی و به‌ویژه سازنده‌ی محصولات برخوردار از این آسیب‌پذیری، ارائه شده‌اند.

سربرگ «**مراجع**»، حاوی لینک دسترسی به اطلاعات وصله‌های امنیتی و راهنماهایی است که توسط متخصصین، مراکز امدادرسانی و به‌ویژه سازنده‌ی محصولات برخوردار از این آسیب‌پذیری، ارائه شده‌اند.



شکل (۲-۴) : بخش Info از رکورد آسیب‌پذیری در پایگاه داده SecurityFocus

۲-۲۲- پایگاه داده Securitytracker

این پایگاه داده، در سال ۲۰۰۱، توسط شرکت Securitytracker ایجاد شده است و در حال حاضر، بیش از ۲۵ هزار آسیب‌پذیری در آن ثبت شده است. شکل (۲-۵)، نمونه‌ای از رکورد ثبت شده در پایگاه داده Securitytracker برای یک اسیب‌پذیری است. فیلدهای این رکورد، عبارتند از :

- فیلد شناسه‌ی هشدار Securitytracker : شناسه‌ی تخصیص یافته به این آسیب‌پذیری در پایگاه داده Securitytracker است.
- فیلد Securitytracker URL : حاوی URL دسترسی به اطلاعات آسیب‌پذیری، در پایگاه داده Securitytracker است.

- فیلد مرجع CVE : حاوی شناسه‌ی CVE این آسیب‌پذیری و لینک دسترسی به اطلاعات این آسیب‌پذیری در پایگاه داده CVE است.
- فیلد تاریخ : حاوی تاریخ ثبت این آسیب‌پذیری در پایگاه داده Securitytracker است.
- فیلد ضربه : حاوی ضربه‌ی ناشی از بهره‌برداری مهاجم از این آسیب‌پذیری، به همراه لینک به لیست تمام آسیب‌پذیری‌هایی است که این ضربه را امکان‌پذیر می‌نمایند.
- فیلد «راه‌حل دردسترس» و «تائید شده توسط سازنده» : به‌صورت بله/خیر مشخص می‌کند که آیا راه‌حلی برای رفع آسیب‌پذیری وجود دارد یا خیر و آیا این راه‌حل توسط سازنده مورد تائید قرار گرفته است یا خیر.
- فیلد نسخه‌ها : حاوی نسخه‌های محصولی است که این آسیب‌پذیری در آن‌ها وجود دارد.
- فیلد توصیف : حاوی تشریح آسیب‌پذیری و نام شخص حقیقی یا حقوقی است که آسیب‌پذیری را گزارش نموده است.
- فیلد ضربه : حاوی تشریح شرایط مهاجم و نحوه‌ی بهره‌برداری مهاجم از آسیب‌پذیری، برای وارد نمودن ضربه است.
- فیلد راه‌حل : حاوی راه‌حل‌های ارائه شده توسط سازنده و سایرین، به همراه لینک دسترسی به آن راه‌حل‌ها است.
- فیلد URL سازنده : حاوی URL دسترسی به راه‌حل ارائه شده توسط شرکت سازنده‌ی محصول برخوردار از آسیب‌پذیری است.
- فیلد علّت : علّت بروز یا منشأ آسیب‌پذیری را بیان می‌کند. از جمله این‌که، یک آسیب‌پذیری ممکن است ناشی از پیکربندی اشتباه باشد.
- فیلد سیستم‌عامل‌های اساسی : حاوی لیست سیستم‌عامل‌هایی است که محصول حاوی این آسیب‌پذیری، روی آن‌ها اجرا می‌شود. به عبارت دیگر، سیستم‌عامل‌هایی را نشان می‌دهد که ممکن است این آسیب‌پذیری روی آن‌ها بُروز نماید.
- فیلد تاریخچه پیام : حاوی تاریخچه‌ی گزارش و ثبت آسیب‌پذیری، به همراه راه‌حل‌های ارائه شده برای آن است.

IBM WebSphere Application Server ViewState Settings Lets Remote Users Execute Arbitrary Code on the Target System

SecurityTracker Alert ID: 1041521
SecurityTracker URL: http://securitytracker.com/id/1041521
CVE Reference: GENERIC-MAP-NOMATCH *(Links to External Site)*
Date: Aug 20 2018
Impact: Execution of arbitrary code via network, User access via network
Fix Available: Yes **Vendor Confirmed:** Yes
Version(s): 7.0, 8.0, 8.5.5
Description: A vulnerability was reported in IBM WebSphere Application Server. A remote user can execute arbitrary code on the target system.

A remote user can exploit an improper configuration of ViewState settings (if ViewState is configured to use unencrypted state information) to execute arbitrary code residing in the target server's classpath.

The JSF Sun Reference Implementation 1.2 is affected.
Impact: A remote user can execute arbitrary code that resides in the classpath on the target system.
Solution: IBM has issued a fix (Interim Fix PI99524).

The IBM advisory is available at:

https://www-01.ibm.com/support/docview.wss?uid=ibm10716525
Vendor URL: www-01.ibm.com/support/docview.wss?uid=ibm10716525 *(Links to External Site)*
Cause: Configuration error
Underlying OS: Linux (Any), UNIX (AIX), UNIX (HP/UX), UNIX (Solaris - SunOS), Windows (Any), z/OS

Message History: None.

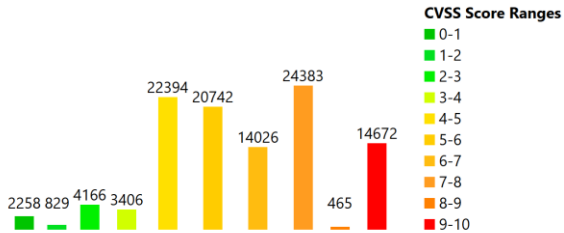
شکل (۲–۵) : رکورد یک آسیب‌پذیری نمونه، در پایگاه داده Securitytracker

۲۳-۲- پایگاه داده CVE Details

این پایگاه داده، ترکیبی از اطلاعات مندرج در تمام پایگاه‌های داده آسیب‌پذیری، نقاط ضعف و سرمایه، به همراه اطلاعات مربوط به پویش‌گرهای آسیب‌پذیری در خصوص هر آسیب‌پذیری را ارائه می‌نماید. در بخش اصلی سایت این پایگاه داده، مطابق شکل (۲–۶)، توزیع امتیاز CVSS کلیه آسیب‌پذیری‌های ثبت شده در پایگاه داده آسیب‌پذیری مشترک (CVE)، ارائه شده است.

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	2258	2.10
1-2	829	0.80
2-3	4166	3.90
3-4	3406	3.20
4-5	22394	20.90
5-6	20742	19.30
6-7	14026	13.10
7-8	24383	22.70
8-9	465	0.40
9-10	14672	13.70
Total	107341	

Weighted Average CVSS Score: **6.6**



شکل (۲–۶) : توزیع امتیاز CVSS کلیه آسیب‌پذیری‌های پایگاه داده CVE

در این پایگاه داده، اطلاعات، به تفکیک برای هر آسیب‌پذیری و هر محصول، ارائه می‌شود. شکل (۲–۷)، رکورد ثبت شده برای آسیب‌پذیری شناسه CVE-۲۰۱۸-۱۰۰۰ را نشان می‌دهد که اطلاعات ثبت شده برای آن در پایگاه داده آسیب‌پذیری مشترک (CVE)، قبلاً در شکل (۲–۲) نشان داده شد. در این رکورد، اطلاعات جامعی از قبیل کد CVE آسیب‌پذیری، توصیف، کدهای CVE آسیب‌پذیری‌های مرتبط، تاریخ ثبت و تاریخ آخرین به‌روزرسانی، راه‌حل و سایر اطلاعات منتشر شده توسط سازنده، محصولات برخوردار از این آسیب‌پذیری، کدهای بهره‌برداری، توضیحات کاربران و متخصصین، اطلاعات جزئیات آسیب‌پذیری در پایگاه داده ملی آسیب‌پذیری (NVD)، اطلاعات جزئیات آسیب‌پذیری در پایگاه داده آسیب‌پذیری مشترک (CVE)، Pluginهای موجود در پویش‌گر آسیب‌پذیری Nessus، برای کشف این آسیب‌پذیری، راهنمای FIRST برای سامانه امتیازدهی آسیب‌پذیری مشترک (CVSS)، امتیاز این آسیب‌پذیری بر اساس CVSS و جزئیات امتیاز هر یک از سنجه‌های این سامانه، نوع (کلاس) آسیب‌پذیری، لیست و نسخه تمام محصولات برخوردار از این آسیب‌پذیری به همراه اطلاعات جزئیات آسیب‌پذیری هر محصول، مراجع مربوط به هر آسیب‌پذیری به همراه شناسه‌ی آسیب‌پذیری در هر مرجع و لینک دسترسی به اطلاعات در هر مرجع و شرایط معتبر بودن آسیب‌پذیری برای هر نسخه از هر محصول، ارائه شده است.

Vulnerability Details : CVE-2018-1000

An information disclosure vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engine Information Disclosure Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10. This CVE ID is unique from CVE-2018-0981, CVE-2018-0987, CVE-2018-0989.
Publish Date : 2018-04-11 Last Update Date : 2018-05-16

Collapse All Expand All Select Select&Copy

Scroll To
Vendor Statements(0) Additional Vendor Data(0) OVAL Definitions(0) Vulnerable Products(3) # Of Vulns By Products References(3) Metasploit Modules(0)

Comments
View User Comments Add Comment

External Links
Secunia Advisories XForce Advisories Vulnerability Details at NVD Vulnerability Details at Mitre Nessus Plugins First CVSS Guide

Search Twitter Search YouTube Search Google

- CVSS Scores & Vulnerability Types

CVSS Score	2.6
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	200

شکل (۲–۷) : رکورد آسیب‌پذیری CVE-۲۰۱۸-۱۰۰۰ در پایگاه داده تلفیقی CVE Details

- Products Affected By CVE-2018-1000

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Microsoft	Internet Explorer	9				Version Details Vulnerabilities
2	Application	Microsoft	Internet Explorer	10				Version Details Vulnerabilities
3	Application	Microsoft	Internet Explorer	11				Version Details Vulnerabilities

- Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	Internet Explorer	3

- References For CVE-2018-1000

http://www.securitytracker.com/id/1040653
SECTRACK 1040653
http://www.securityfocus.com/bid/103603
BID 103603 Microsoft Internet Explorer Scripting Engine CVE-2018-1000 Information Disclosure Vulnerability *Release Date:*2018-04-10
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1000 CONFIRM

- Vulnerability Conditions

Vulnerability is valid if product versions listed below are used **TOGETHER WITH**(AND)

- Microsoft Internet Explorer 10
- Microsoft Windows Server 2012

Vulnerability is valid if product versions listed below are used **TOGETHER WITH**(AND)

- Microsoft Internet Explorer 11
- Microsoft Windows 10
- Microsoft Windows 10 1511
- Microsoft Windows 10 1607
- Microsoft Windows 10 1703
- Microsoft Windows 10 1709
- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows Rt 8.1
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Vulnerability is valid if product versions listed below are used **TOGETHER WITH**(AND)

- Microsoft Internet Explorer 9
- Microsoft Windows Server 2008 SP2

- Metasploit Modules Related To CVE-2018-1000

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

شکل (۲–۷) : ادامه‌ی رکورد آسیب‌پذیری CVE-۲۰۱۸-۱۰۰۰ در پایگاه داده تلفیقی CVE Details

در این پایگاه داده، چنانچه نام و نسخه‌ی یک محصول سایبری را وارد نمائید، لیست کلیه آسیب‌پذیری‌های آن محصول در پایگاه داده آسیب‌پذیری مشترک (CVE)، به همراه اطلاعاتی در خصوص هر آسیب‌پذیری، ارائه می‌شود.

۲-۲۴- پایگاه داده Scaprepo

این پایگاه داده، یک انباره‌ی محتوای مبتنی بر ابر و میزبانی شده توسط یک سکوی توزیع محتوا بر اساس پروتکل خودکارسازی محتوای امنیتی[۱] (SCAP) است. این پایگاه داده تلفیقی، اطلاعات سرمایه‌ها، آسیب‌پذیری‌ها و ضعف‌های امنیتی موجود در OVAL، XCCDF، CVE، CPE، CWE و CVSS را به همراه اطلاعات تکمیلی ارائه می‌نماید که تمام نیازهای متخصصین امنیت برای تشخیص آسیب‌پذیری، وصله‌زنی، تشخیص بدافزار و مدیریت حوادث رایانه‌ای را پوشش می‌دهند.

۲-۲۵- پایگاه داده Circl CVE

این پایگاه داده، امکان جستجو روی پایگاه‌های داده آسیب‌پذیری مشترک (CVE) و ضعف مشترک (CWE) را فراهم آورده است. در این پایگاه داده، جستجو بر اساس آسیب‌پذیری و بر اساس محصول قابل انجام است.

۲-۲۶- تست نفوذ و کاربرد آن در شناسایی آسیب‌پذیری سایبری

تست نفوذ[۲]، توسط یک تیم متبحّر انجام می‌شود و شباهت زیادی به یک ارزیابی امنیتی یا پویش آسیب‌پذیری غیرنظام‌مند دارد. در تست نفوذ، تیم تست با تکیه بر تجربه‌ی خود و بهره‌گیری از روش‌های خلاقانه، آسیب‌پذیری را کشف می‌کند. این روش برای کشف آسیب‌پذیری‌های ناشناخته مناسب است. قبل از تست نفوذ، حتماً باید پویش آسیب‌پذیری یا ارزیابی امنیتی عملیاتی، انجام شده باشد تا آسیب‌پذیری‌های شناخته شده کشف و رفع شوند تا حجم کار تیم تست نفوذ، کمتر و نتیجه‌ی آن، مؤثرتر شود. تست نفوذ، در اکثر موارد، روشی پرهزینه و کم‌بهره است، لیکن اگر تیم تست، خوب انتخاب شده باشد و حتی یک آسیب‌پذیری ناشناخته کشف شود، بسیار ارزشمند خواهد بود. تست نفوذ، مکمّل خوبی برای ابزارهای پویش آسیب‌پذیری نیز محسوب می‌شود زیرا در صورتی که ابزارهای پویش‌گر، به‌روز نبوده و قادر به تشخیص یک یا چند آسیب‌پذیری شناخته‌شده نبتشند و یا حتی در مواردی، عمداً کشف یک آسیب‌پذیری شناخته شده را گزارش نکنند، تیم تست نفوذ، قادر به تشخیص این موارد خواهد بود.

۲-۲۷- توصیه‌های ضروری

به‌منظور پیش‌گیری از ایجاد آسیب‌پذیری، تشخیص به‌موقع و رفع دقیق و سریع آسیب‌پذیری‌های سایبری، لازم است :

۱. محصولات و خدمات سایبری را از تولیدکننده یا عرضه‌کننده‌ی معتبر و دارای گواهی از مراجع ذی‌صلاح قانونی خریداری نمائید. در نظام پدافند سایبری کشور، اعطاء گواهی به تولیدکنندگان و عرضه‌کنندگان محصولات و خدمات، توسط مرکز پدافند سایبری کشور انجام می‌شود.

---

[۱] Security Content Automation Protocol (SCAP)

[۲] Penetration Test

۲. در انتخاب محصولات سایبری، امنیت سایبری و پدافند سایبری، یک ویژگی کلیدی را ابتدا مورد توجه قرار دهید. این ویژگی کلیدی، آن است که محصول موردنظر، حتماً دارای گواهی اعتبار عملکردی و امنیتی از مراجع ذی‌صلاح قانونی باشد. در نظام پدافند سایبری کشور، اعطاء گواهی به محصولات سایبری و پدافند سایبری، توسط مرکز پدافند سایبری کشور انجام می‌شود.

۳. در انتخاب محصولات و خدمات سایبری، به هشدارهای مراجع آگاهی‌رسانی امنیت و پدافند سایبری، به ویژه پایگاه اطلاع‌رسانی پدافند سایبری کشور و مرکز ماهر وزارت ارتباطات و فناوری اطلاعات، توجه نمائید.

٤. به‌صورت مداوم و دوره‌ای، به پایگاه‌های داده آسیب‌پذیری داخلی و خارجی معتبر، مراجعه و از آخرین اخبار آسیب‌پذیری‌های مرتبط با محصولات و خدمات سایبری مورد استفاده در سازمان خود، مطلع شوید و حتماً در اسرع وقت، نسبت به استفاده‌ی هوشمندانه از اطلاعات مندرج در این پایگاه‌های داده، اقدام نمائید. زیرا پس از افشاء یک آسیب‌پذیری، مهاجمین بلافاصله از غفلت کاربران در نصب وصله‌های امنیتی استفاده نموده و ضربات قابل توجهی به آنها وارد می‌نمایند. اگرچه این قبیل پایگاه‌های داده، تنها حاوی اطلاعات آسیب‌پذیری‌های شناخته‌شده می‌باشند، لیکن باید به این نکته توجه داشت که آسیب‌پذیری‌های شناخته‌شده‌ای که از فراوانی زیادی در یک سازمان و یا در کل کشور برخوردار باشند، در نظام پدافند سایبری، باید مورد توجه قرار گیرند.

٥. وصله‌های امنیتی ارائه شده توسط سازندگان محصولات یا عرضه‌کنندگان خدمات سایبری مورد استفاده در سازمان خود را در اسرع وقت و به‌صورت دقیق، بر اساس راهنمای ارائه شده توسط سازنده، نصب نموده و مورد بهره‌برداری قرار دهید.

٦. راهکارهای ارائه شده برای رفع یا تسکین آسیب‌پذیری توسط پایگاه اطلاع‌رسانی پدافند سایبری کشور یا مرکز ماهر وزارت ارتباطات و فناوری اطلاعات را مورد توجه و بهره‌برداری قرار دهید.

۷. به‌صورت مداوم و دوره‌ای، اقدام به پویش امنیتی کلیه بخش‌های شبکه ارتباطی و کلیه سامانه‌های اطلاعاتی سازمان خود، با بهره‌گیری از پویش‌گرهای آسیب‌پذیری مورد تائید مرکز پدافند سایبری کشور نمائید. این امر، موجب کشف آسیب‌پذیری‌های شناخته‌شده‌ای خواهد شد که در فضای سایبر سازمان شما، هنوز رفع نشده‌اند.

۸. به‌منظور کشف آسیب‌پذیری‌های ناشناخته، به‌صورت مداوم و دوره‌ای، بخش‌های کلیدی شبکه و سامانه‌های اطلاعاتی کلیدی سازمان خود را مورد تست نفوذ قرار دهید. برای این امر، حتماً از تیم‌های خبره و مورد تائید مرکز پدافند سایبری کشور، استفاده نمائید و در متن قرارداد تست نفوذ، حتماً نام ابزارهای امنیتی مورد استفاده توسط این تیم و ضرورت داشتن گواهی معتبر پدافند سایبری برای این ابزارها را درج نمائید.

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

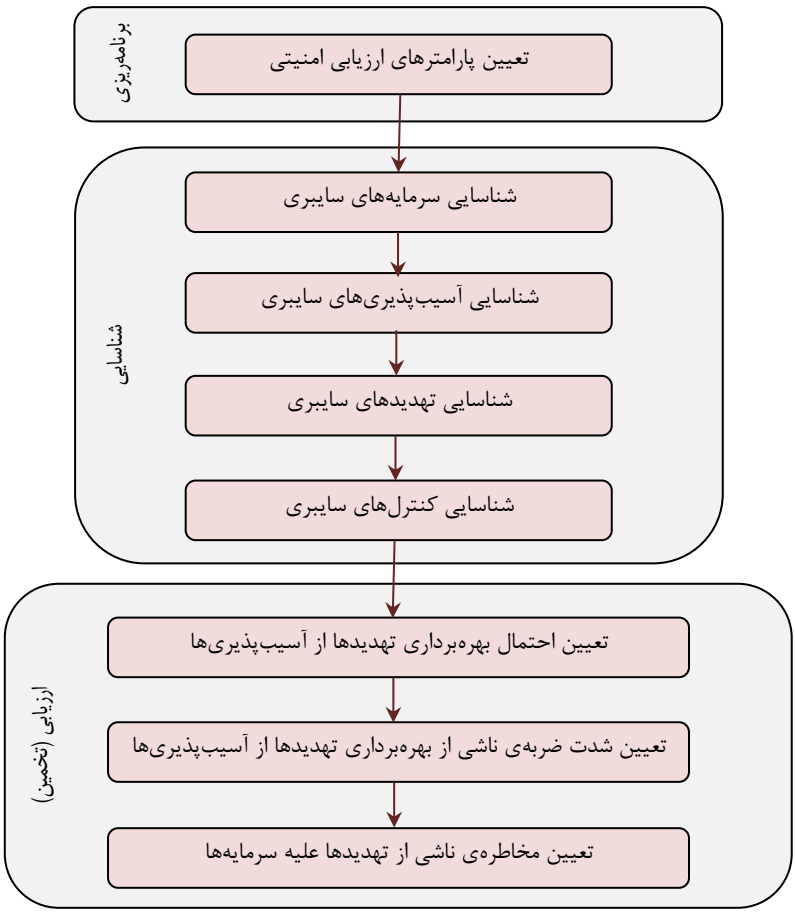
در این گام، پارامترهای ارزیابی امنیتی، از قبیل پارامترهای کلی ارزیابی (رویکرد ارزیابی، سطح ارزیابی و قلمرو ارزیابی)، پارامترهای شناسایی (رویکرد شناسایی و روش شناسایی) و پارامترهای تحلیل (رویکرد تحلیل و روش تحلیل) تعیین و بر اساس این پارامترها، روش مناسب ارزیابی امنیتی انتخاب می‌شود.

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]

---

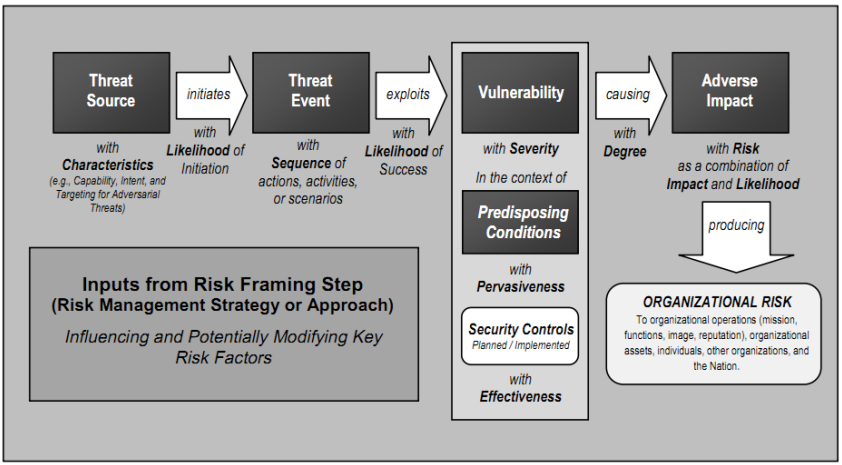
۱ Common Framework

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.

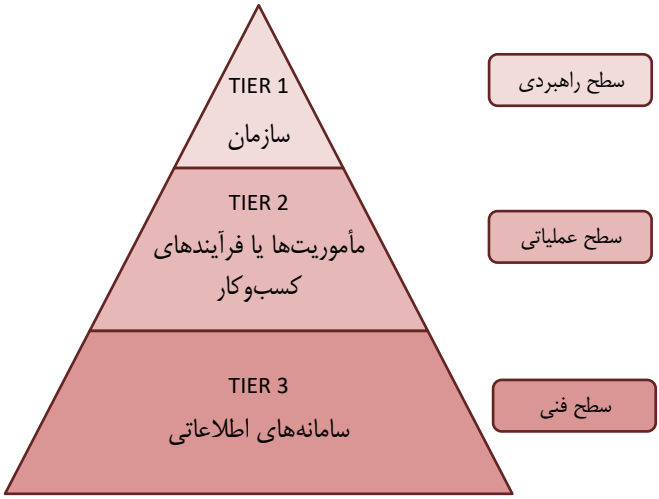
۱ Threay Context

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.

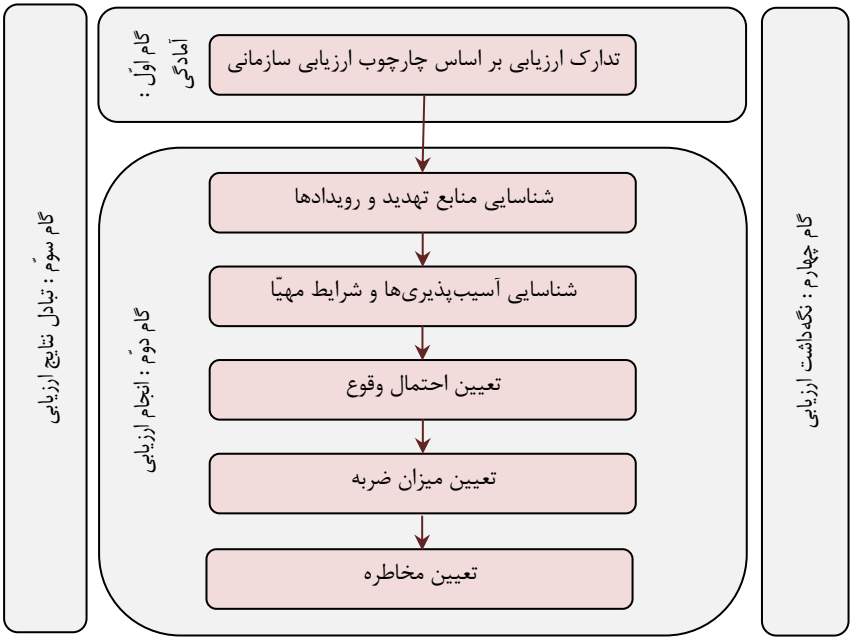
ارزیابی مخاطرات امنیتی در سطح راهبردی یا سازمانی نیز بر روی راهبردها، خط‌مشی‌ها، استانداردها، دستورالعمل‌ها و برنامه‌های سازمان انجام می‌گیرد. تمرکز این نوع ارزیابی بر مخاطرات موجود علیه موجودیت، سرمایه‌ها و پرسنل سازمان است و تأثیرات آنها را بر راهبردها و سیاست‌های سازمان مشخص می‌کند.

---

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.

فصل چهارم

امنیت سایبری

اهداف آموزشی پیش‌بینی شده برای این فصل، عبارتند از :

۱. کسب شناخت از مؤلفه‌های تشکیل‌دهنده‌ی امنیت سایبری
۲. کسب شناخت از نیازمندی‌های امنیتی
۳. کسب شناخت از ارتباط نیازمندی‌های امنیتی با مؤلفه‌های امنیت سایبری
٤. کسب توانایی تعیین نیازمندی‌های امنیتی سامانه‌های اطلاعاتی
٥. کسب توانایی تعیین نیازمندی‌های امنیتی شبکه‌های ارتباطی

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

۱. مؤلفه‌های تشکیل‌دهنده‌ی امنیت سایبری
۲. ارتباط نیازمندی‌های امنیتی با مؤلفه‌های امنیت سایبری
۳. نحوه‌ی تعیین نیازمندی‌های امنیتی بر اساس مؤلفه‌های امنیت سایبری
٤. نیازمندی‌های امنیتی گوشی تلفن هشومند همراه به عنوان یک سرمایه سایبری بسیار پرکاربرد
٥. نیازمندی‌های امنیتی یک شبکه ارتباطی انتها–به–انتها

۱-٤- تعریف امنیت سایبری

امنیت سایبری[۱]، به توانایی محافظت از یک سرمایه سایبری، در مقابل نقض خط مشی امنیتی (یا نقض مؤلفه‌های امنیت) آن سرمایه اطلاق می‌شود. اما مؤلفه‌های امنیت یک سرمایه سایبری کدام است؟ و نقض این مؤلفه‌ها چگونه انجام می‌شود؟

مؤلفه‌های امنیت سایبری، در سه سطح راهبردی، عملیاتی (اجرایی) و فنی تعریف می‌شوند.

در سطح راهبردی : برنامه راهبردی امنیت، حاوی راهبردها و خط‌مشی‌های امنیت، برنامه ارزیابی امنیتی، برنامه امن‌سازی، برنامه تشخیص و مقابله با حملات سایبری، برنامه تشخیص و مقابله با حوادث رایانه‌ای و نظایر این‌ها، مؤلفه‌های سطح راهبردی امنیت سایبری را تشکیل می‌دهند.

در سطح عملیاتی (اجرایی) : فرآیندها و رویه‌های پیکربندی امن تجهیزات و خدمات سایبری، فرآیندها و رویه‌های جذب و به‌کارگیری امن پرسنل سایبری، فرآیندها و رویه‌های خرید، نصب، راه‌اندازی و بهره‌برداری امن سامانه‌ها و خدمات سایبری و نظایر این‌ها، مؤلفه‌های سطح عملیاتی امنیت سایبری را تشکیل می‌دهند.

در سطح فنی : محرمانگی[۲]، صحت[۳] (یا یکپارچگی) و دسترس‌پذیری[۴]، مؤلفه‌های اصلی سطح فنی امنیت سایبری را تشکیل می‌دهند. در برخی دسته‌بندی‌ها، از احراز هویت[۵]، اختیاردهی[۶]، حسابرسی[۷] (پاسخ‌گویی)، کنترل دسترسی[۸]، عدم انکار[۹] و حریم خصوصی[۱۰] نیز به عنوان مؤلفه‌های سطح فنی امنیت سایبری و در برخی دیگر از دسته‌بندی‌ها با عنوان خدمات سطح فنی امنیت سایبری نام برده شده است. دلیل این امر، عدم اصالت ذاتی مؤلفه‌های دسته دوم از مؤلفه‌های دسته اول است. به عبارت دیگر، تحقق احراز هویت، اختیاردهی، حسابرسی، کنترل دسترسی، عدم انکار، حریم خصوصی و امنیت ارتباط، وابستگی ذاتی به سه مؤلفه محرمانگی، صحت و دسترس‌پذیری دارد.

تمرکز این فصل بر مؤلفه‌های سطح فنی امنیت سایبری است. اکنون با توجه به شناخت مؤلفه‌های سطح فنی امنیت، می‌توانیم امنیت سایبری را به شرح زیر، بازتعریف نمائیم :

«امنیت سایبری، به توانایی محافظت از یک سرمایه سایبری، در مقابل نقض محرمانگی، صحت و دسترس‌پذیری آن سرمایه اطلاق می‌گردد» یا در حالت کامل‌تر « امنیت سایبری، به توانایی محافظت از یک سرمایه سایبری، در مقابل نقض محرمانگی، صحت، دسترس‌پذیری، احراز هویت، کنترل دسترسی، عدم انکار، حریم خصوصی و امنیت ارتباطات آن سرمایه اطلاق می‌گردد».

«محرمانگی» در یک سرمایه سایبری، به معنای در دسترس نبودن یا افشاء نشدن اطلاعات آن سرمایه برای افراد، موجودیت‌ها و فرآیندهای غیرمجاز است. بر این اساس، «نقض محرمانگی» در یک سرمایه سایبری، به معنای در

---

۱ Cyber Security
۲ Confidentiality
۳ Integrity
۴ Availability
۵ Authentication
۶ Authorization
۷ Accounting
۸ Access Control
۹ Non Repudiation
۱۰ Privacy

دسترس قرار گرفتن یا افشاء اطلاعات آن سرمایه، برای افراد، موجودیت‌ها یا فرآیندهای غیرمجاز است. برای محافظت از محرمانگی اطلاعات، از روش‌های ساده تا پیچیده، اعم از کدگذاری، رمزنگاری و پنهان‌نگاری استفاده می‌شود. انتخاب روش تأمین امنیت، بستگی به میزان حساسیت، اهمیت یا سطح محرمانگی اطلاعات موردنظر دارد. اکنون این مسئله مطرح می‌شود که چه کسی باید تعیین کند که اساساً تأمین محرمانگی برای یک سرمایه سایبری ضرورت دارد یا خیر؟ و در صورت ضرورت، چه سطحی از محرمانگی موردنیاز است؟ بدون شک مالک سرمایه سایبری، بهترین فرد برای پاسخ به این سؤالات است. مالک سرمایه سایبری باید دو پارامتر را تعیین کند. اول این‌که آیا مؤلفه محرمانگی برای سرمایه سایبری باید تأمین شود یا خیر؟ و دوم این‌که چه سطحی از محرمانگی باید برای اطلاعات سرمایه سایبری تأمین شود؟ بر اساس پاسخ‌های ارائه شده توسط مالک سرمایه، طراح امنیت سازمان، روش تأمین محرمانگی برای سرمایه سایبری موردنظر را تعیین خواهد نمود. البته تعیین این روش، علاوه بر سؤالات مربوط به محرمانگی، به سؤالات مربوط به سایر مؤلفه‌های امنیت نیز بستگی دارد. زیرا این مؤلفه‌ها از یکدیگر مستقل نیستند و در برخی موارد، بهتر است از روشی استفاده شود که چند مؤلفه امنیت را تأمین کند یا حداقل اثر سوء در تأمین مؤلفه‌های امنیتی دیگر بر جای نگذارد.

«صحت» یک سرمایه سایبری، به معنای درستی و تمامیت سرمایه سایبری است. بر این اساس، «نقض صحت» در یک سرمایه سایبری به معنای اعمال هرگونه تغییر (افزودن، کاستن، جایگزینی، حذف و نابودی) در اطلاعات و سایر اجزاء تشکیل‌دهنده‌ی آن سرمایه سایبری، توسط افراد غیرمجاز است. روش‌های تأمین صحت اطلاعات یا یکپارچگی سامانه اطلاعاتی و شبکه ارتباطی، بسیار متنوع هستند و انتخاب روش مناسب، نیازمند پاسخ به دو سؤال مطرح شده در مؤلفه محرمانگی است. در اینجا نیز لازم است مالک سرمایه سایبری، تعیین کند که اساساً تأمین صحت برای هر یک از مؤلفه‌های سرمایه سایبری، ضرورت دارد یا خیر؟ همچنین باید تعیین کند که چه سطحی از صحت، باید برای هر یک از مؤلفه‌های سرمایه سایبری، تأمین شود؟

«دسترس‌پذیری» یک سرمایه سایبری نیز به معنای در دسترس و قابل استفاده بودن آن سرمایه برای تمام افراد، سامانه‌ها و فرآیندهای مجاز است. بر این اساس، «نقض دسترس‌پذیری» به معنای عدم امکان دسترسی به سرمایه سایبری توسط افراد، سامانه‌ها و فرآیندهای مجاز است. برای محافظت از دسترس‌پذیری یک سرمایه سایبری، لازم است اولاً منابع کافی اعم از حافظه، فضای ذخیره‌سازی، پهنای باند ارتباطی و نظایر آنها برای سرمایه سایبری پیش‌بینی شود و ثانیاً هرگونه درخواست یا دسترسی غیرمجاز و حتی در صورت لزوم، دسترسی‌های تکراری مجاز نادیده گرفته شوند. به عبارت دیگر، در تخصیص منابع به درخواست‌ها، عدالت رعایت شود.

توجه داشته باشید که اگر اطلاعات برای افراد مجاز افشاء شود، محرمانگی نقض نشده است. اگر هرگونه تغییر توسط افراد مجاز اعمال شود، صحت نقض نمی‌شود و اگر امکان دسترسی برای افراد غیرمجاز وجود نداشته باشد، دسترس‌پذیری نقض نخواهد شد. لذا در تحقق محرمانگی و صحت و دسترس‌پذیری، مجاز یا غیرمجاز بودن دسترسی، بسیار اهمیت دارد. برای تفکیک درخواست مجاز از غیرمجاز، لازم است مشخص شود که درخواست‌کننده کیست؟ چه اختیاراتی دارد؟ یا مجاز است که چه درخواست‌هایی را داشته باشد؟ اکنون چه درخواستی ارائه داده است؟ چه اقداماتی

انجام داده است؟ مثلاً چه چیزی را دیده است؟ چه چیزی را تغییر داده است؟ چه چیزی را حذف یا اضافه نموده است؟ پاسخ این سؤال‌ها، در واقع به معنای تحقق دسته دوم مؤلفه‌های فنی امنیت سایبری است.

تحقق دسته دوم مؤلفه‌های فنی امنیت، شامل احراز هویت، کنترل دسترسی، عدم انکار و حریم خصوصی، مکمل تحقق دسته اول مؤلفه‌های فنی امنیت است. اگر هویت افراد احراز گردد، اختیارات هر فرد مجاز تعیین شود و عملکرد افراد در حساب کاربری آنها ثبت و ضبط گردد. در این صورت، هم نقض محرمانگی، صحت و دسترس‌پذیری سرمایه به مراتب دشوارتر خواهد بود، هم افراد امکان انکار عملکرد خود را نخواهند داشت و پاسخ‌گو خواهند بود و هم حریم خصوصی افراد مشخص‌تر و نقض آن دشوارتر خواهد بود.

مؤلفه‌ها، معیارها یا ابعاد امنیت سایبری

محرمانگی، صحت و دسترس‌پذیری، مؤلفه‌های اصلی
و احراز هویت، کنترل دسترسی، عدم انکار و حریم خصوصی
نیز سایر مؤلفه‌های فنی امنیت سایبری را تشکیل می‌دهند.

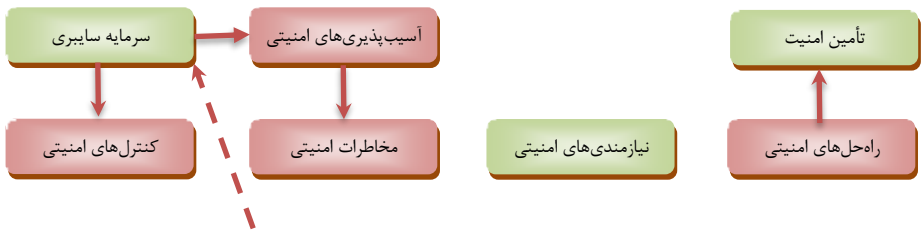
۲-٤- نیازمندی‌های امنیت سایبری

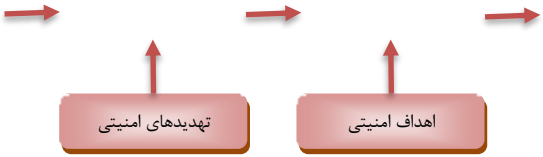
بنا به تعریف، «نیازمندی امنیتی شرطی است که ما آرزو می‌کنیم اگر روی یک پدیده محیط قرار بگیرد، موجب کاهش مخاطرات شود».

بر این اساس :

«نیازمندی امنیت سایبری، یک یا ترکیبی از مؤلفه‌های امنیتی است که ما آرزو می‌کنیم اگر روی یک سرمایه سایبری در شرایط محیطی اعمال شود، موجب کاهش مخاطرات امنیت سایبری آن سرمایه شود».

ولی چه لزومی دارد که نیازمندی‌های امنیتی یک سرمایه سایبری را تعیین کنیم؟ آیا تعیین نیازمندی‌های امنیتی یک سرمایه سایبری، در تأمین امنیت آن سرمایه به ما کمک می‌کند؟ پاسخ این سؤال، مثبت است. شکل (۴-۱)، جایگاه تعیین نیازمندی‌های امنیتی در تأمین امنیت یک سرمایه سایبری را نمایش داده است، بر اساس این شکل، نیازمندهای امنیتی، تابعی ازمخاطرات امنیتی و اهداف امنیتی می‌باشند. همچنین نیازمندی‌های امنیتی، مقدمه‌ی تعیین راه‌حل‌های امنیتی موردنیاز برای تأمین امنیت سرمایه سایبری محسوب می‌شوند.





شکل (۴-۱) : جایگاه نیازمندی‌های امنیتی در تأمین امنیت یک سرمایه سایبری

توصیف کامل شکل (۴-۱)، از گوشه سمت چپ بالای شکل آغاز می‌شود و به شرح زیر است :

هر سرمایه سایبری، از یک یا چند آسیب‌پذیری سایبری برخوردار است و توسط یک یا چند تهدید امنیتی نیز مورد تهدید قرار می‌گیرد. در مرحله توسعه سرمایه سایبری، ممکن است برای مواجهه با این تهدیدها، یک یا چند کنترل امنیتی نیز در داخل سرمایه سایبری، پیش‌بینی شده باشند. مجموعه‌ی آسیب‌پذیری‌ها، تهدیدها و کنترل‌های امنیتی برشمرده شده، موجب می‌شوند تا این سرمایه سایبری، با مخاطرات امنیتی مواجه باشد. پس از تعیین مخاطرات امنیتی موجود علیه یک سرمایه سایبری، ابتدا باید اهداف امنیتی موردنظر تعیین شوند. بر اساس هدف امنیت سایبری تعیین شده برای سرمایه سایبری موردنظر، می‌توان تشخیص داد که چه سطح [کیفی] یا چه میزان [کمّی] از امنیت، مورد انتظار است و بر اساس مخاطرات موجود، می‌توان تشخیص داد کدام‌یک از مؤلفه‌های امنیت، برای رفع مخاطرات موجود، مورد نیاز می‌باشند. به این ترتیب، بر اساس مخاطرات امنیتی موجود و اهداف امنیتی تعیین شده، نیازمندی‌های امنیتی سرمایه سایبری موردنظر، تعیین می‌شوند. در ادامه نیز راه‌حل‌های مناسبی که قادر به تأمین آن نیازمندی‌ها امنیتی باشند، شناسایی شده و مورد استفاده قرار می‌گیرند تا تأمین امنیت برای آن سرمایه سایبری، صورت پذیرد.

بر اساس توصیف فوق، «نیازمندی‌های امنیت سایبری یک سرمایه سایبری را می‌توان در قالب ترکیبی از مؤلفه‌های امنیت سایبری بیان نمود. در این ترکیب، هر مؤلفه امنیت، دارای یک ضریب کمّی یا سطح کیفی خواهد بود.»

در بخش قبل، نیازمندی امنیت سایبری را در قالب دو سؤال توصیف نمودیم و گفتیم که «مالک سرمایه، تعیین می‌کند که آیا اساساً تأمین هر یک از مؤلفه‌های امنیت سایبری، برای سرمایه سایبری موردنظر، ضرورت دارد یا خیر؟ و همچنین تعیین می‌کند که چه سطحی از این مؤلفه‌های امنیت، باید برای سرمایه سایبری موردنظر، تأمین شوند؟»

دو عبارت مندرج در دو پاراگراف فوق، کاملاً یکسان بوده و هر دو، توصیفی از نیازمندی امنیتی یک سرمایه سایبری را بیان می‌کنند.

نیازمندی‌های امنیتی یک سرمایه سایبری منفرد را می‌توان در قالب جدول (۴-۱) بیان نمود. در این جدول، مقابل هر مؤلفه فنی امنیت سایبری، دو ستون با عناوین «کاربردپذیری» و «سطح تأمین» پیش‌بینی شده است.

جدول (۴-۱) : نیازمندی‌های امنیتی یک سرمایه سایبری منفرد

مؤلفه فنی امنیت سایبری	کاربردپذیری	سطح تأمین (در صورت کاربردپذیری)
محرمانگی	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد

صحت	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد
دسترس‌پذیری	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد
احراز هویت	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد
کنترل دسترسی	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد
عدم انکار	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد
حریم خصوصی	بلی / خیر	خیلی‌کم / کم / متوسط / زیاد / خیلی‌زیاد

ستون «کاربردپذیری»، بیانگر ضرورت تأمین مؤلفه امنیت مندرج در هر سطر، برای سرمایه سایبری موردنظر است. در ستون «سطح تأمین» نیز تعیین می‌شود که چه سطحی از مؤلفه امنیت سایبری موردنظر، باید تأمین شود. میزان تأمین هر یک از مؤلفه‌های امنیت، برای هر سرمایه سایبری، به دو پارامتر اهمیت (حساسیت) آن سرمایه و نقش مؤلفه امنیتی موردنظر، در تأمین امنیت برای آن سرمایه بستگی دارد.

تنها در صورتی ستون سطح تأمین تکمیل می‌شود که در ستون کاربردپذیری، گزینه «بلی» درج شده باشد. البته در حالت ساده‌تر، دو ستون کاربردپذیری و سطح تأمین، قابل تجمیع می‌باشند. برای این منظور، می‌توان ستون کاربردپذیری را حذف نمود و در ستون سطح تأمین، به‌جای گزینه «خیلی‌کم»، از گزینه «نیاز ندارد[۱]» استفاده نمود.

تا این‌جا نحوه تعیین نیازمندی‌های امنیتی برای یک سرمایه سایبری منفرد را بررسی کردیم، اما باید توجه داشته باشیم که اغلب سرمایه‌های سایبری، بیش از یک بخش دارند و هر بخش از سرمایه موردنظر، نیازمندی‌های امنیتی متفاوتی دارد. برای نمونه، یک سامانه اطلاعاتی ممکن است از بخش‌های سخت‌افزار، سیستم‌عامل، یک یا چند نرم‌افزار کاربردی و محتوا (اطلاعات)، تشکیل شده باشد. نیازمندی‌های امنیتی یک سرمایه چندبخشی، در جدولی مشابه جدول (۲-۴) نمایش داده می‌شود.

جدول (۴-۲) : نیازمندی‌های امنیتی یک سرمایه سایبری چندبخشی

مؤلفه فنی امنیت سایبری	سطح تأمین برای بخش (۱) سرمایه سایبری	...	سطح تأمین برای بخش (n) سرمایه سایبری
محرمانگی	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد
صحت	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد
دسترس‌پذیری	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد
احراز هویت	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد
کنترل دسترسی	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد
عدم انکار	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد
حریم خصوصی	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد	...	نیاز ندارد / کم / متوسط / زیاد / خیلی‌زیاد

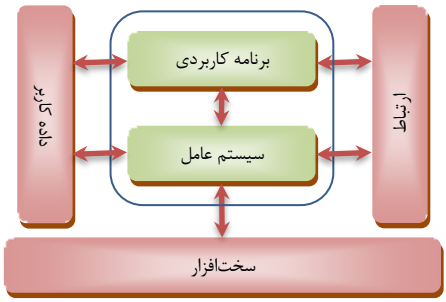
[۱] Not Required

۳-٤- نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند

یک دستگاه گوشی تلفن همراه هوشمند، ترکیبی از یک تلفن همراه و یک سامانه اطلاعاتی با قابلیت‌های فراوان محسوب می‌شود. این دستگاه، در کارکرد تلفن همراه، امکان برقراری انواع ارتباطات اعم از صوتی، تصویری و داده‌ای را فراهم می‌ورد و در کارکرد سامانه اطلاعاتی، از بخش‌های سخت‌افزاری برای پردازش و ذخیره‌سازی داده‌ها، سیستم عامل و انواع برنامه‌های کاربردی تشکیل شده است.

۱-۳-٤. سرمایه‌های سایبری گوشی تلفن همراه هوشمند

ساختار معماری گوشی تلفن همراه هوشمند، مطابق شکل (۴-۲) است. سیستم‌عامل و برنامه‌های کاربردی، کنترل‌کننده‌ی گوشی تلفن همراه هوشمند هستند. کاربران، از طریق برنامه‌های کاربردی و سیستم عامل، امکان مدیریت و بهره‌برداری از تلفن همراه هوشمند خود را می‌یابند. دسترسی به داده‌های کاربر که در انواع قالب‌های صوتی، تصویری، متنی و ویدیوئی ذخیره شده‌اند نیز از طریق برنامه‌های کاربردی و سیستم عامل انجام می‌شود. همچنین هرگونه برقراری ارتباط یا مبادله انواع داده کاربر نیز از طریق برنامه‌های کاربردی و سیستم عامل انجام می‌گیرد.



شکل (۴-۲) : معماری گوشی تلفن همراه هوشمند

به این ترتیب، لیست سرمایه‌های سایبری یک گوشی تلفن همراه هوشمند، یا بخش‌های مختلف گوشی تلفن همراه هوشمند به عنوان یک سرمایه سایبری، مطابق جدول (۴-۳)، عبارت از سه بخش، با عناوین سخت‌افزار، نرم‌افزار و داده است.

جدول (۴-۳) : سرمایه‌های سایبری گوشی تلفن همراه هوشمند

بخش	توصیف	میزان اهمیت
داده کاربر	انواع داده‌های ذخیره شده در دستگاه تلفن همراه هوشمند، شامل داده‌های دفترچه مخاطبان، داده‌های پیشینه‌ی تماس، پیام‌های متنی و چندرسانه‌ای، پست الکترونیکی، تصاویر، فایل‌های صوتی، اطلاعات بانکی، موقعیت مکانی و ...	خیلی مهم

نرم‌افزار	سیستم عامل، انواع برنامه‌های مدیریت گوشی تلفن، انواع برنامه‌های کاربردی از پیش نصب‌شده توسط سازنده و انواع برنامه‌های کاربردی نصب شده توسط کاربر	مهم
سخت‌افزار	واحد پردازش مرکزی (CPU)، حافظه دسترسی تصادفی (RAM)، باتری، واسط ارتباطی با شبکه تلفن همراه، صفحه نمایش، دوربین، میکروفن و ...	خیلی مهم و مهم

داده کاربر، بخشی از حریم خصوصی کاربر است و از این بابت، مهم‌ترین و ارزشمندترین سرمایه سایبری موجود در گوشی تلفن همراه هوشمند محسوب می‌شود. گوشی تلفن همراه هوشمند، امکانات متنوعی را برای ذخیره‌سازی، پردازش، مبادله و محافظت از داده‌های کاربر فراهم می‌کند. بخش عمده‌ای از حملات علیه گوشی تلفن همراه هوشمند نیز در واقع علیه داده‌های موجود در این گوشی انجام می‌شوند. سرقت یا دسترسی غیرمجاز به داده، سرقت شناسه، سرقت اطلاعات موقعیت کاربر و نظایر این‌ها، نمونه‌هایی از حملاتی است که می‌تواند علیه داده‌های کاربر انجام شود.

بخش‌هایی از گوشی تلفن همراه هوشمند که امکان ضبط غیرمجاز تصاویر و صدای کاربر را فراهم می‌کنند، یعنی دوربین و میکروفن گوشی نیز از اهمیت و حساسیت بسیار بالایی برخوردار می‌باشند.

۲-۳-٤. آسیب‌پذیری‌های گوشی تلفن همراه هوشمند

قبلاً دو کارکرد اصلی برای یک گوشی تلفن همراه هوشمند برشمردیم. در کارکرد «تلفن همراه هوشمند، به عنوان گوشی تلفن همراه»، تمرکز فعالیت‌های این دستگاه بر جنبه‌های ارتباطی تمرکز دارد و به همین دلیل، آسیب‌پذیری اصلی این دستگاه نیز، آسیب‌پذیری‌های ارتباطی است. در کارکرد «تلفن همراه هوشمند، به عنوان یک سامانه اطلاعاتی»، تمرکز اصلی فعالیت این دستگاه بر جنبه‌های جویش، ضبط (جمع‌آوری)، ذخیره‌سازی، پردازش، پخش (اشتراک‌گذاری) و ... انواع داده‌های متنی، صوتی، تصویری و ویدیوئی تمرکز دارد و به همین دلیل نیز آسیب‌پذیری‌های اصلی این دستگاه، ناشی از مسائل مرتبط با طراحی، پیاده‌سازی و بهره‌برداری از نرم‌افزارها و داده‌ها می‌باشند. این آسیب‌پذیری‌ها به سه دسته‌ی آسیب‌پذیری‌های ناشی از تولید، مدیریت و بهره‌برداری از این دستگاه طبقه‌بندی می‌شوند. به این ترتیب، مجموع آسیب‌پذیری‌های دستگاه تلفن همراه هوشمند را می‌توان مطابق شکل (۴-۳)، در چهار دسته‌ی ذیل، دسته‌بندی نمود :

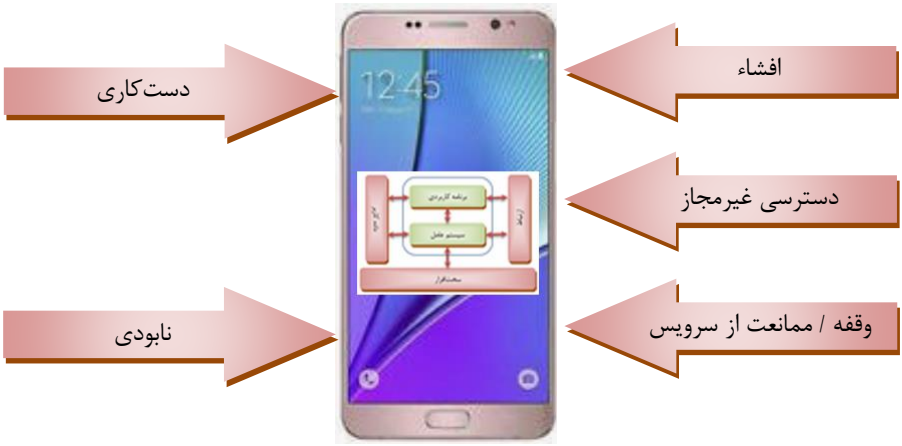
۱. «آسیب‌پذیری‌های ناشی از ارتباط ناامن با شبکه تلفن همراه» اعم از آسیب‌پذیری‌های ناشی از پروتکل ارتباط با شبکه تلفن همراه یا آسیب‌پذیری ناشی از دسترسی از راه دور به اطلاعات و نرم‌افزارهای موجود در دستگاه تلفن می‌باشند.
۲. «آسیب‌پذیری‌های ناشی از تولید سامانه» اعم از تولید سخت‌افزار و نرم‌افزار، که با عنوان نقص‌ها یا نقاط ضعف سامانه نیز شناخته می‌شوند.
۳. «آسیب‌پذیری‌های ناشی از مدیریت و تنظیم سامانه» اعم از مدیریت و تنظیم بخش‌های سخت‌افزاری و نرم‌افزاری دستگاه که تماماً توسط تنظیمات نرم‌افزاری انجام می‌شوند. این دسته، با عنوان مدیریت ناکارآمد APIها شناخته می‌شوند.

٤. «آسیب‌پذیری‌های ناشی از بهره‌برداری از سامانه» که ناشی از بهره‌برداری نادرست از امکانات و قابلیت‌های سامانه است. باتوجه به این‌که بهره‌برداری از امکانات سامانه، از طریق نرم‌افزارهای کاربردی انجام می‌شوند، این دسته از آسیب‌پذیری‌ها هم ناشی از عدم آگاهی کاربر، نسبت به نرم‌افزارهای کاربردی سامانه می‌باشند.

شکل (۴-۳) : آسیب‌پذیری‌های گوشی تلفن همراه هوشمند

۳-۴-٤. تهدیدهای موجود علیه گوشی تلفن همراه هوشمند

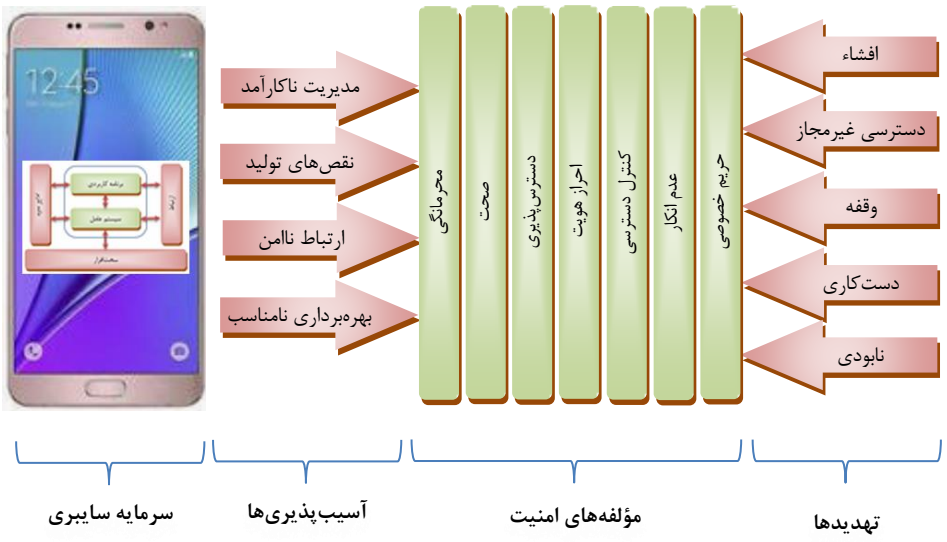
تهدیدها و حملات علیه کوشی تلفن همراه هوشمند، مانند سایر سرمایه‌های سایبری، مطابق شکل (۴-۴)، نهایتاً منجر به یک یا ترکیبی از موارد «افشاء»، «دسترسی غیرمجاز / برداشتن»، «وقفه / ممانعت از دسترسی / ازکارانداختن / غیرفعال‌کردن»، «دست‌کاری / تغییر» یا «نابودی» بخش‌هایی از [یا کل] سرمایه سایبری خواهد شد.



شکل (۴-۴) : تهدیدهای موجود علیه گوشی تلفن همراه هوشمند

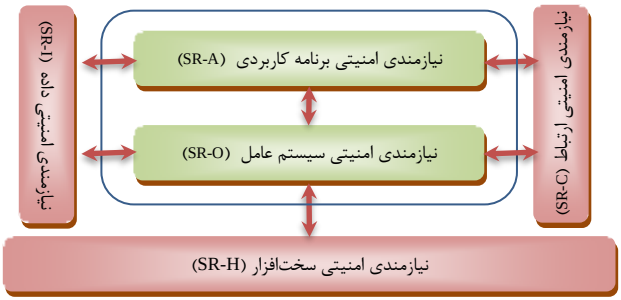
٤-٣-٤. نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند

قبلاً اشاره شد که نیازمندی‌های امنیتی هر سرمایه سایبری، به تفکیک برای بخش‌های مختلف آن سرمایه ارائه می‌شود. چنانچه بخواهیم نیازمندی‌های امنیتی گوشی تلفن همراه را تعیین کنیم، لازم است ابتدا مجموعه عوامل تأثیرگذار بر امنیت این دستگاه، شامل بخش‌ها (سرمایه‌ها)، آسیب‌پذیری‌ها، تهدیدها و مؤلفه‌های امنیتی را در قالب یک شکل مشاهده کنیم تا تصور نیازمندی‌های امنیتی را برایمان تسهیل نماید. شکل (۴-۵)، مجموعه عوامل تعیین‌کننده‌ی نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند را نمایش می‌دهد.



شکل (۴-۵) : مجموعه عوامل مؤثر بر نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند

بر این اساس، نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند، قابل دسته‌بندی در قالب ساختاری مطابق شکل (۴-۶) است.



شکل (۴-۶) : ساختار نیازمندی‌های امنیتی

به این ترتیب، نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند، شامل موارد ذیل، خواهد بود :

۱. نیازمندی‌های امنیتی سخت‌افزار (SR-H)

امنیت سخت‌افزار، شامل تأمین محرمانگی و جامعیت برای تراشه‌های ذخیره‌ساز، تراشه‌های کلید و تراشه‌های شناسه واحد می‌باشند. به‌علاوه لایه سخت‌افزار، باید مکانیزم‌های امنیتی مهم را برای لایه‌های بالاتر فراهم نماید. دسترس‌پذیری کل بخش‌های سخت‌افزاری تلفن همراه نیز پیش‌نیاز وجود دسترس‌پذیری برای سیستم عامل و برنامه‌های کاربردی است.

۲. نیازمندی‌های امنیتی سیستم‌عامل (SR-O)

سیستم عامل، قلب گوشی تلفن همراه هوشمند است و به عنوان هسته‌ی کنترل‌کننده‌ی تمام بخش‌ها عمل می‌کند. تأمین محرمانگی و جامعیت کدهای سیستم در لایه سخت‌افزار، تأمین محرمانگی و جامعیت ترافیک داده‌ها در ارتباطات، تأمین سرویس‌های امنیتی برای برنامه‌های کاربردی، احراز هویت کاربر و جداسازی دامنه‌های امنیتی باید توسط سیستم عامل انجام شوند.

دسترسی به بخش‌های خاصی از سخت‌افزار، شامل دوربین و میکروفن، باید با اعمال بالاترین سطح از مؤلفه‌های امنیتی امکان‌پذیر باشد. همچنین محرمانگی این بخش‌ها باید برای کاربران راه دور، کاملاً حفظ شود.

۳. نیازمندی‌های امنیتی نرم‌افزارهای کاربردی (SR-A)

امنیت نرم‌افزارهای کاربردی، شامل دو بخش است. بخش اول امنیت ذاتی نرم‌افزارهای کاربردی است که باید توسط تولیدکننده تأمین شود و بخش دوم، امنیت نصب، پیکربندی و بهره‌برداری از نرم‌افزارهای کاربردی است که بر عهده کاربر گوشی تلفن همراه است و باعث می‌شود تنظیمات یا بهره‌برداری به گونه‌ای انجام شود که امکان سوء استفاده از برنامه کاربردی توسط هکر محلی یا راه‌دور، امکان‌پذیر نباشد.

٤. نیازمندی‌های امنیتی داده‌های کاربر (SR-I)

داده‌های کاربر، بخشی از حریم خصوصی کاربر محسوب می‌شوند و مهم‌ترین و باارزش‌ترین بخش از گوشی تلفن همراه هوشمند را تشکیل می‌دهند. محرمانگی، صحت و دسترس‌پذیری داده‌ها باید تأمین شود. همچنین هر گونه دسترسی به داده‌های کاربر باید پس از احراز هویت و با اعمال مکانیزم‌های کنترل دسترسی انجام گیرد تا امکان انکار عملکرد از بین برود.

٥. نیازمندی‌های امنیتی ارتباطات (SR-C)

انواع داده‌ها اعم از داده‌های کنترلی، هویتی و محتوایی از انواع متنی، صوتی، تصویری و ویدیوئی از طریق درگاه ارتباطی گوشی تلفن همراه هوشمند، با شبکه و سایر مشترکین شبکه مبادله می‌شوند. تأمین محرمانگی، صحت و دسترس‌پذیری این داده‌ها از اهمیت زیادی برخوردار است. همچنین هرگونه دسترسی از راه دور، باید پس از احراز هویت و کنترل دسترسی امکان‌پذیر باشد تا عملکرد دسترسی به تنظیمات، برنامه‌ها و داده‌های کاربر، ثبت و قابل پیگرد باشند. از منظر ارتباطی، کل گوشی تلفن همراه، بخشی از حریم خصوصی کاربر محسوب می‌شود و هرگونه تلاش سایر کاربران برای دسترسی از راه دور به گوشی تلفن همراه کاربر دیگر، باید با رعایت حریم خصوصی صورت پذیرد.

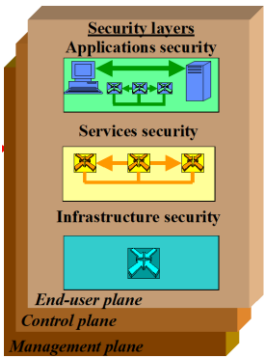
بر اساس مطالب فوق، نیازمندی‌های امنیتی یک گوشی تلفن همراه هوشمند، مطابق جدول (۴-۴) خواهد بود.

جدول (۴-۴) : سرمایه‌های سایبری گوشی تلفن همراه هوشمند

بخش	میزان	نیازمندی‌های امنیتی						
(سرمایه)	اهمیت	محرمانگی	صحت	دسترس پذیری	احراز هویت	کنترل دسترسی	عدم انکار	حریم خصوصی
سخت‌افزار (SR-H)	مهم	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	نیاز ندارد
سیستم عامل (SR-O)	مهم	زیاد	زیاد	زیاد	زیاد	زیاد	زیاد	نیاز ندارد
برنامه کاربردی (SR-A)	مهم	زیاد	زیاد	زیاد	زیاد	زیاد	زیاد	نیاز ندارد
داده کاربر (SR-I)	خیلی‌مهم	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد
ارتباط (SR-C)	مهم	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد	خیلی‌زیاد

٤-٤- نیازمندی‌های امنیتی شبکه ارتباطی

معماری امنیتی یک شبکه ارتباطی، بر اساس مدل معماری افقی–عمودی، از یک ساختار سه سطحی و سه لایه‌ای مطابق شکل (۴–۷) برخوردار است. بر اساس ساختار نمایش داده شده در این شکل، شبکه ارتباطی، از سه سطح با عناوین مدیریت، کنترل و کاربر انتهایی (کاربری) تشکیل می‌شود و هر یک از این سطوح، از سه لایه با عناوین زیرساخت، خدمت و کاربرد تشکیل می‌شوند.



شکل (۴–۷) : معماری امنیتی یک شبکه ارتباطی بر اساس مدل معماری افقی–عمودی

بر این اساس، مؤلفه‌های تشکیل‌دهنده یا سرمایه‌های سایبری یک شبکه ارتباطی که لازم است نیازمندی‌های امنیتی آن‌ها مورد توجه قرار گیرند، از ۹ بخش، با عناوین مندرج در جدول (۴–۵) تشکیل می‌شود.

جدول (۴–۵) : سرمایه‌های سایبری یک شبکه ارتباطی

سطوح / لایه‌ها	مدیریت	کنترل	کاربر انتهایی
زیرساخت	مدیریت زیرساخت شبکه و زیرساخت مدیریت شبکه	کنترل زیرساخت شبکه و زیرساخت کنترل شبکه	کاربری زیرساخت شبکه و زیرساخت کاربردهای شبکه
خدمت	مدیریت خدمات شبکه و خدمات مدیریت شبکه	کنترل خدمات شبکه و خدمات کنترل شبکه	کاربری خدمات شبکه و خدمات کاربردی شبکه
کاربرد	مدیریت کاربردهای شبکه و کاربردهای مدیریت شبکه	کنترل کاربردهای شبکه و کاربردهای کنترل شبکه	کاربری کاربردهای شبکه و کاربردهای کاربری شبکه

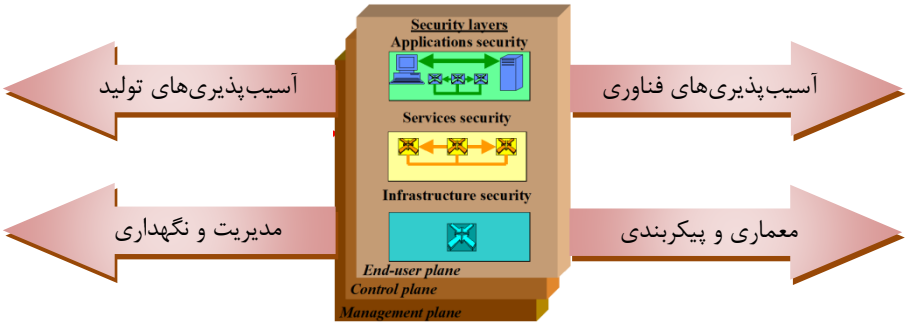
۱-٤-٤. آسیب‌پذیری‌های شبکه ارتباطی

اگر بخواهیم لیستی از آسیب‌پذیری یک شبکه ارتباطی ارائه دهیم، قطعاً این لیست، تابع نوع تجهیزاتی که در آن شبکه استفاده شده است، شرکت سازنده آن تجهیزات و تیم‌های عملیاتی که نصب، راه‌اندازی، تست و بهره‌برداری از این تجهیزات را انجام داده‌اند می‌باشد. اما آسیب‌پذیری‌های هر شبکه‌ای با هر نوع تجهیزاتی، ساخت هر شرکتی، نصب و راه‌اندازی شده توسط هر مجموعه‌ای و در حال بهره‌برداری توسط هر مجموعه‌ای، ممکن است از آسیب‌پذیری‌های طبقه‌بندی شده در فصل (۲) برخوردار باشد.

به این ترتیب، یک شبکه ارتباطی نیز مانند سایر سرمایه‌های سایبری، از مؤلفه‌هایی تشکیل می‌شود که مبتنی بر یک فناوری توسعه یافته‌اند، پس احتمالاً آسیب‌پذیری‌های ناشی از آن فناوری را در بر دارند. این مؤلفه‌ها، توسط یک شرکت سازنده و در مراحل طراحی، پیاده‌سازی، تست و ... توسعه یافته‌اند، پس احتمالاً آسیب‌پذیری‌های ناشی از توسعه محصول را هم در بر دارند. همچنین این مؤلفه‌ها بر اساس یک طراحی مشخص، تقاضا شده و توسط یک شرکت به سازمان شما فروخته شده‌اند و در سازمان شما نصب و راه‌اندازی و تست و تحویل شده‌اند، پس احتمالاً آسیب‌پذیری‌های ناشی از معماری و پیکربندی را نیز در بر دارند. نهایتاً این مؤلفه‌ها توسط یک واحد سازمانی در ساختار سازمان شما، مدیریت و نگهداری می‌شوند، پس احتمالاً آسیب‌پذیری‌های ناشی از مدیریت و نگهداری را نیز در بر خواهند داشت.

به این ترتیب، مجموع آسیب‌پذیری‌های احتمالی یک شبکه ارتباطی را می‌توان مطابق شکل (۴-۸)، در چهار دسته‌ی ذیل، دسته‌بندی نمود :

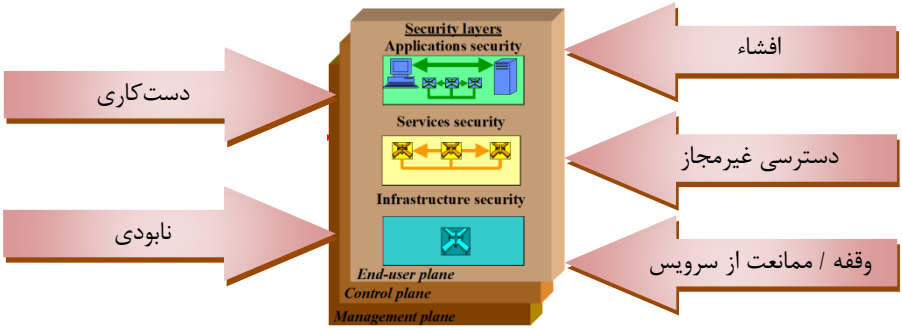
۱. آسیب‌پذیری‌های ناشی از فناوری : آسیب‌پذیری فناوری‌های ارتباطی پایه شبکه اینترنت اعم از IP V٤٫٠ یا IP V٦٫٠، فناوری‌های ارتباطات بی‌سیم، ارتباطات رادیویی یا حتی ارتباطات ماهواره‌ای مورد استفاده در شبکه، فناوری نسل پنجم ارتباطات، فناوری رایانش ابری، فناوری اینترنت اشیاء و سایر فناوری‌های مورد استفاده در شبکه موردنظر، شامل کلیه فناوری‌های مورد استفاده در لایه‌های زیرساخت، خدمت و کاربرد و سطوح مدیریت، کنترل و کاربری را در بر می‌گیرد.
۲. آسیب‌پذیری‌های ناشی از تولید : آسیب‌پذیری تولید عناصر تشکیل‌دهنده‌ی زیرساخت، خدمات و کاربردهای شبکه، اعم از عناصر تشکیل‌دهنده‌ی سطوح مدیریت، کنترل و کاربری شبکه را شامل می‌شود.
۳. آسیب‌پذیری‌های ناشی از معماری و پیکربندی : آسیب‌پذیری‌های ناشی از معماری و پیکربندی کلیه مؤلفه‌های زیرساخت، خدمت و کاربردهای شبکه در لایه‌های مدیریت، کنترل و کاربری را شامل می‌شود.
٤. آسیب‌پذیری‌های ناشی از مدیریت و نگهداری کلیه مؤلفه‌های زیرساخت، خدمت و کاربردهای شبکه در لایه‌های مدیریت، کنترل و کاربری را شامل می‌شود.



شکل (۴-۸) : آسیب‌پذیری‌های شبکه ارتباطی

۴-۴-۲. تهدیدهای موجود علیه شبکه‌های ارتباطی

تهدیدها و حملات موجود علیه یک شبکه ارتباطی، مانند سایر سرمایه‌های سایبری، مطابق شکل (۴-۹)، نهایتاً منجر به یک یا ترکیبی از موارد «افشاء»، «دسترسی غیرمجاز / برداشتن»، «وقفه / ممانعت از دسترسی / ازکارانداختن / غیرفعال‌کردن»، «دست‌کاری / تغییر» یا «نابودی» بخش‌هایی از [یا کل] سرمایه سایبری خواهد شد. البته باید توجه داشت که مهم‌ترین تهدید یک شبکه ارتباطی، نابودی یا ایجاد اختلال (ممانعت از سرویس) گسترده در آن است.

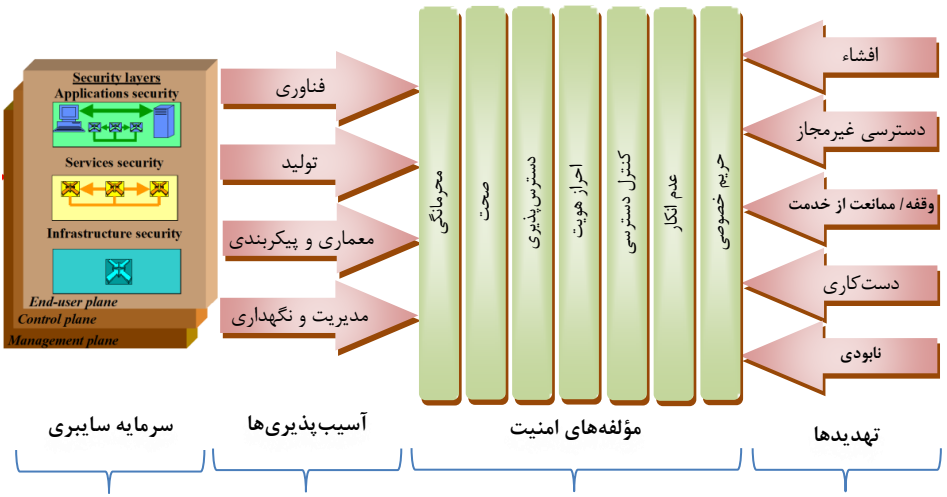


شکل (۴-۹) : تهدیدهای موجود علیه شبکه ارتباطی

۴-۴-۳. نیازمندی‌های امنیتی شبکه ارتباطی

قبلاً اشاره شد که نیازمندی‌های امنیتی هر سرمایه سایبری، به تفکیک برای بخش‌های مختلف آن سرمایه ارائه می‌شود. چنانچه بخواهیم نیازمندی‌های امنیتی یک شبکه ارتباطی را تعیین کنیم، لازم است ابتدا مجموعه عوامل تأثیرگذار بر امنیت این شبکه، شامل بخش‌ها (سرمایه‌ها)، آسیب‌پذیری‌ها، تهدیدها و مؤلفه‌های امنیتی را در قالب یک

شکل مشاهده کنیم تا تصور نیازمندی‌های امنیتی را برایمان تسهیل نماید. شکل (۴-۱۰)، مجموعه عوامل تعیین‌کننده‌ی نیازمندی‌های امنیتی یک شبکه ارتباطی را نمایش می‌دهد.



شکل (۴-۱۰) : مجموعه عوامل مؤثر بر نیازمندی‌های امنیتی شبکه ارتباطی

بر این اساس، نیازمندی‌های امنیتی شبکه ارتباطی، قابل دسته‌بندی در قالب ساختاری مطابق جدول (۴-۶) است.

جدول (۴-۶) : نیازمندی‌های امنیتی یک شبکه ارتباطی

سطوح / لایه‌ها	مدیریت	کنترل	کاربر انتهایی
زیرساخت	نیازمندی‌های امنیتی مدیریت زیرساخت شبکه و زیرساخت مدیریت شبکه (SR-IM&MI)	نیازمندی‌های امنیتی کنترل زیرساخت شبکه و زیرساخت کنترل شبکه (SR-IC&CI)	نیازمندی‌های امنیتی کاربری زیرساخت شبکه و زیرساخت کاربردهای شبکه (SR-IU&UI)
خدمت	نیازمندی‌های امنیتی مدیریت خدمات شبکه و خدمات مدیریت شبکه (SR-SM&MS)	نیازمندی‌های امنیتی کنترل خدمات شبکه و خدمات کنترل شبکه (SR-SC&CS)	نیازمندی‌های امنیتی کاربری خدمات شبکه و خدمات کاربردی شبکه (SR-SU&US)
کاربرد	نیازمندی‌های امنیتی مدیریت کاربردهای شبکه و کاربردهای مدیریت شبکه (SR-AM&MA)	نیازمندی‌های امنیتی کنترل کاربردهای شبکه و کاربردهای کنترل شبکه (SR-AC&CA)	نیازمندی‌های امنیتی کاربری کاربردهای شبکه و کاربردهای کاربری شبکه (SR-AU&UA)

به این ترتیب، نیازمندی‌های امنیتی شبکه ارتباطی، شامل موارد ذیل، خواهد بود :

۱. نیازمندی‌های امنیتی مدیریت زیرساخت شبکه و زیرساخت مدیریت شبکه (SR-IM&MI)

جدول (۴-۷) : نیازمندی‌های امنیتی مدیریت زیرساخت شبکه و زیرساخت مدیریت شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-IM&MI-۱)	اطمینان حاصل کنید که تنها پرسنل مجاز، از طریق دستگاه‌های مجاز، قادر به انجام فعالیت‌های مدیریتی تجهیزات و لینک‌های ارتباطی شبکه می‌باشند.
احراز هویت (SR-IM&MI-۲)	هویت فرد یا دستگاهی که فعالیت مدیریتی را بر روی تجهیزات و لینک‌های ارتباطی شبکه انجام می‌دهد را تصدیق نمائید.
عدم انکار (SR-IM&MI-۳)	یک رکورد شناسایی برای هر فرد یا دستگاهی که هر فعالیت مدیریتی را بر روی تجهیزات و لینک‌های ارتباطی شبکه اجرا می‌کند، فراهم کنید. این رکورد می‌تواند به عنوان اثباتی برای فعالیت مدیریتی مورد استفاده قرار گیرد.
محرمانگی (SR-IM&MI-٤)	از اطلاعات پیکربندی تجهیزات شبکه و لینک‌های ارتباطی در مقابل دسترسی یا مشاهده غیرمجاز، محافظت کنید. این شامل اطلاعات پیکربندی موجود در تجهیزات شبکه و لینک‌های ارتباطی، اطلاعات پیکربندی منتقل شده به تجهیزات شبکه و لینک‌های ارتباطی و همچنین اطلاعات پیکربندی پشتیبان است که به‌صورت برون‌خط ذخیره شده‌اند. همچنین از اطلاعات احراز هویت مدیریتی (از قبیل شناسه و گذرواژه مدیر) در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت کنید.
امنیت ارتباط (SR-IM&MI-٥)	در مورد مدیریت از راه دور تجهیزات شبکه یا لینک‌های ارتباطی، اطمینان حاصل کنید که «اطلاعات مدیریتی تنها بین ایستگاه‌های مدیریت از راه دور و تجهیزات یا لینک های ارتباطی که مدیریت می شوند، جریان دارد.»، «اطلاعات مدیریتی به هنگام که بین این نقاط پایانی جریان می یابد، منحرف یا متوقف نمی شود» و همان نوع ملاحظه برای اطلاعات احراز هویت مدیریتی (به عنوان مثال، شناسه و گذرواژه مدیر) نیز اعمال می‌شود.
صحت (SR-IM&MI-٦)	از اطلاعات پیکربندی تجهیزات شبکه و لینک‌های ارتباطی در برابر تغییر غیر مجاز، حذف، ایجاد و تکرار، محافظت کنید. این محافظت را برای اطلاعات پیکربندی مقیم در تجهیزات شبکه یا لینک‌های ارتباطی و همچنین اطلاعات پیکربندی در حال مبادله یا ذخیره‌شده در سامانه‌های برون‌خط و اطلاعات احراز هویت مدیریتی (به عنوان مثال، شناسه و گذرواژه مدیر) نیز اعمال شود.
دسترس‌پذیری (SR-IM&MI-۷)	اطمینان حاصل کنید که امکان ممانعت از مدیریت تجهیزات شبکه یا لینک‌های ارتباطی توسط پرسنل یا تجهیزات مجاز وجود ندارد. این شامل محافظت در برابر حملات فعال مانند حملات ممانعت از خدمت (DoS) و همچنین محافظت در برابر حملات غیرفعال مانند تغییر یا حذف اطلاعات احراز هویت مدیریتی (به عنوان مثال، شناسه و گذرواژه مدیر) می‌شود.
حریم خصوصی	اطمینان حاصل کنید که اطلاعاتی که می‌تواند برای شناسایی تجهیزات شبکه یا لینک‌های ارتباطی مورد استفاده قرار گیرد، برای پرسنل یا تجهیزات غیرمجاز، دسترس‌پذیر نیست. مثال‌هایی از این نوع

(SR-IM&MI-۸)	اطلاعات، شامل آدرسIP تجهیزات شبکه یا نام دامنه DNS هستند که برای مثال، امکان شناسایی تجهیزات شبکه و هدف قرار گرفتن آن‌ها توسط مهاجمان را فراهم می‌کند.

۲. نیازمندی‌های امنیتی کنترل زیرساخت شبکه و زیرساخت کنترل شبکه (SR-IC&CI)

جدول (۴–۸) : نیازمندی‌های امنیتی کنترل زیرساخت شبکه و زیرساخت کنترل شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-IC&CI-۱)	اطمینان حاصل کنید که تنها برای پرسنل و تجهیزات مجاز، امکان دسترسی به اطلاعات کنترلی مقیم در تجهیزات شبکه (به عنوان مثال، یک جدول مسیریابی) یا در سامانه‌ی ذخیره‌سازی برون‌خط، فراهم است. همچنین اطمینان حاصل کنید که تجهیزات شبکه تنها پیام‌های اطلاعات کنترلی (به عنوان مثال، به روزرسانی‌های مسیریابی) را از تجهیزات مجاز شبکه می‌پذیرد.
احراز هویت (SR-IC&CI-۲)	هویت افراد یا تجهیزات مشاهده‌کننده یا تغییردهنده‌ی اطلاعات کنترلی مقیم در تجهیزات شبکه را تصدیق کنید. هویت دستگاه ارسال‌کننده‌ی اطلاعات کنترلی به تجهیزات شبکه را نیز تصدیق نمائید. برای این منظور، ممکن است روش‌های تصدیق هویت، به عنوان بخشی از کنترل دسترسی، مورد نیاز باشند.
عدم انکار (SR-IC&CI-۳)	یک رکورد برای شناسایی هر فرد یا دستگاه مشاهده کننده یا اصلاح‌کننده‌ی اطلاعات کنترلی تجهیزات شبکه و هر عملی که اجرا می‌کند را فراهم کنید. این رکورد می‌تواند به عنوان اثباتی برای دسترسی آن فرد یا دستگاه به اطلاعات کنترلی و یا تغییر اطلاعات کنترلی توسط آن فرد یا دستگاه، مورد استفاده قرار گیرد. همچنین یک رکورد برای شناسایی دستگاه منشأ ارسال پیغام‌های کنترلی به تجهیزات شبکه و عملی که در نتیجه‌ی ارسال آن پیغام کنترلی اجرا می‌شود را فراهم کنید. این رکورد را می‌توان برای اثبات اینکه دستگاه موردنظر، منشأ ارسال پیغاام کنترلی بوده است، به کار برد.
محرمانگی (SR-IC&CI-٤)	از اطلاعات کنترلی مقیم در تجهیزات شبکه یا در ذخیره‌ساز بُرون‌خط، در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت کنید. روش‌های مورد استفاده برای تأمین کنترل دسترسی، ممکن است در فراهم کردن محرمانگی برای اطلاعات کنترلی مقیم در تجهیزات شبکه نیز نقش داشته باشند. اطلاعات کنترلی مربوط به تجهیزات شبکه را به هنگام انتقال در شبکه، در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت کنید.
امنیت ارتباط (SR-IC&CI-٥)	اطمینان پیدا کنید که اطلاعات کنترلی که از طریق شبکه منتقل می‌شوند (به عنوان مثال، به روز رسانی‌های مسیریابی)، تنها بین منبع ارسال‌کننده‌ی اطلاعات کنترلی و مقصد موردنظر

	خود جریان می‌یابند و اطلاعات کنترلی در هنگامی که بین این نقاط پایانی جریان می‌یابند، منحرف یا شنود نمی‌شوند.
صحت (SR-IC&CI-٦)	از اطلاعات کنترلی مقیم در تجهیزات شبکه، در برابر تغییر غیر مجاز، حذف، ایجاد و تکرار، محافظت کنید.
دسترس‌پذیری (SR-IC&CI-٧)	اطمینان حاصل کنید که تجهیزات شبکه، همیشه در دسترس هستند تا اطلاعات کنترلی را از منابع مجاز دریافت نمایند. این شامل حفاظت در برابر حملات عمدی مانند حملات ممانعت از خدمت و حوادث تصادفی می‌شود.
حریم خصوصی (SR-IC&CI-٨)	اطمینان حاصل کنید، اطلاعاتی که می‌تواند برای شناسایی تجهیزات شبکه یا لینک‌های ارتباطی مورد استفاده قرار گیرد، برای پرسنل غیرمجاز، موجود نمی‌باشد. برای مثال، اطلاعات آدرس IP تجهیزات و میزبان نام دامنه هکه توانایی شناسایی و هدف قرار دادن تجهیزات شبکه یا لینک‌های ارتباطی را برای مهاجمان فراهم می‌کند.

۳. نیازمندی‌های امنیتی کاربری زیرساخت شبکه و زیرساخت کاربردهای شبکه (SR-IU&UI)

جدول (۴-۹) : نیازمندی‌های امنیتی کاربری زیرساخت شبکه و زیرساخت کاربری شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-IU&UI-١)	اطمینان حاصل کنید که تنها پرسنل مجاز و ابزارهای مجاز، امکان دسترسی به داده‌های کاربر نهایی را دارند. اعم از داده‌هایی که در حال انتقال از طریق تجهیزات شبکه یا لینک‌های ارتباطی بوده و یا بر روی سامانه‌های ذخیره‌سازی برخط، مقیم می‌باشند.
احراز هویت (SR-IU&UI-٢)	هویت افراد و دستگاه‌ها، برای دسترسی به داده‌های کاربر نهایی (اعم از داده‌هایی که توسط تجهیزات شبکه یا لینک‌های ارتباطی ترانزیت می‌شوند و یا در سامانه‌های ذخیره‌سازی برون‌خط مقیم می‌باشند) را تائید نمائید. برای این منظور، ممکن است لازم باشد روش‌های تائید هویت، به عنوان بخشی از کنترل دسترسی، مورد استفاده قرار گیرند.
عدم انکار (SR-IU&UI-٣)	یک رکورد شناسایی برای هر فرد یا دستگاهی که به داده‌های کاربر نهایی (اعم از داده‌هایی که توسط تجهیزات شبکه یا لینک‌های ارتباطی انتقال داده می‌شوند و یا بر روی سامانه‌های ذخیره‌سازی برون‌خط ساکن می‌باشند) دسترسی دارد، فراهم نمائید. این رکورد باید به‌منظور اثبات دسترسی فرد یا دستگاه موردنظر، به داده‌های کاربر نهایی، مورد استفاده قرار گیرد.
محرمانگی (SR-IU&UI-٤)	از داده‌های کاربر نهایی (اعم از داده‌هایی که در حال انتقال توسط تجهیزات شبکه یا لینک‌های ارتباطی بوده و یا بر روی سامانه‌های ذخیره‌سازی برون‌خط مقیم می‌باشند)، در مقابل دسترسی

	غیرمجاز و یا مشاهده‌ی غیرمجاز، محافظت کنید. برای این منظور، می‌توان از روش‌های مورد استفاده برای کنترل دسترسی، جهت فراهم‌نمودن محرمانگی داده‌های کاربر نهایی نیز استفاده نمود.
امنیت ارتباط (SR-IU&UI-٥)	اطمینان حاصل کنید که داده‌های کاربر نهایی (اعم از داده‌هایی که توسط تجهیزات شبکه و لینک‌های ارتباطی ترانزیت می‌شوند)، در مسیر خود تا قبل از رسیدن به مقصد، منحرف نشده و چیزی مانع از رسیدن آن به مقصد نمی‌شود. به عبارت دیگر، از مبدأ تا مقصد، هیچ دسترسی غیرمجازی به داده‌های کاربر نهایی، انجام نمی‌شود.
صحت (SR-IU&UI-٦)	از داده‌های کاربر نهایی که در حال انتقال توسط تجهیزات شبکه یا لینک‌های ارتباطی بوده و یا در سامانه‌های برون‌خط ذخیره شده‌اند، در برابر تغییر مجاز، حذف، ایجاد و تکرار، محافظت کنید.
دسترس‌پذیری (SR-IU&UI-٧)	اطمینان حاصل کنید که دسترسی به اطلاعات کاربر نهایی در سامانه‌های برون‌خط، توسط پرسنل مجاز (از جمله کاربران نهایی) و دستگاه‌ها را نمی‌توان انکار کرد. این امر، شامل حفاظت در برابر حملات فعال مانند حملات ممانعت از سرویس و همچنین حفاظت در برابر حملات غیرفعال مانند اصلاح یا حذف اطلاعات تایید هویت می‌شود.
حریم خصوصی (SR-IU&UI-٨)	اطمینان حاصل کنید که تجهیزات شبکه، اطلاعات مربوط به فعالیت‌های شبکه (از جمله موقعیت جغرافیایی کاربر، وب سایت‌های مشاهده شده و غیره) را برای پرسنل غیرمجاز و تجهیزات غیرمجاز، فراهم نمی‌کنند.

٤. نیازمندی‌های امنیتی مدیریت خدمات شبکه و خدمات مدیریت شبکه (SR-SM&MS)

جدول (۴-۱۰) : نیازمندی‌های امنیتی مدیریت خدمات شبکه و خدمات مدیریت شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-SM&MS-١)	اطمینان حاصل کنید که تنها پرسنل و دستگاه‌های مجاز، می‌توانند فعالیت‌های اجرایی یا مدیریتی خدمات شبکه را انجام دهند.
احراز هویت (SR-SM&MS-٢)	هویت فرد یا دستگاهی که قصد انجام فعالیت‌های اجرایی یا مدیریتی خدمات شبکه را دارد، تائید نمائید. برای این منظور، ممکن است لازم باشد روش‌های تایید هویت، به عنوان بخشی از کنترل دسترسی مورد استفاده قرار گیرند.

عدم انکار (SR-SM&MS-۳)	یک رکورد شناسایی برای فرد یا دستگاهی که هر فعالیت اجرایی یا مدیریتی خدمات شبکه را انجام می‌دهد و عملی که انجام می‌شود فراهم نمائید. این رکورد، می‌تواند برای اثبات این‌که فرد یا دستگاهی فعالیت اجرایی یا مدیریتی انجام داده است، مورد استفاده قرار گیرد.
محرمانگی (SR-SM&MS-٤)	از پیکربندی خدمات شبکه و اطلاعات مدیریتی شبکه، در مقابل دسترسی غیرمجاز یا مشاهده‌ی غیر مجاز، محافظت نمائید. این امر لازم است برای اطلاعات مدیریتی و اطلاعات پیکربندی مقیم در تجهیزات شبکه که در سرتاسر شبکه انتقال داده می‌شوند و یا به‌صورت برون‌خط ذخیره می‌شوند، اعمال شود. همچنین از اطلاعات اجرایی یا مدیریتی شبکه (به عنوان مثال، شناسه‌ها و گذرواژه‌های کاربر و شناسه‌ها و گذرواژه‌های مدیریتی) در مقابل دسترسی غیرمجاز یا مشاهده‌ی غیرمجاز، محافظت کنید.
امنیت ارتباط (SR-SM&MS-٥)	در مورد مدیریت از راه دور یک خدمت شبکه، اطمینان حاصل کنید که اطلاعات اجرایی و مدیریتی، تنها بین ایستگاه مدیریت از راه دور و تجهیزاتی که به عنوان بخشی از خدمت شبکه مدیریت می‌شوند، جریان دارد. اطمینان حاصل کنید که اطلاعات اجرایی و مدیریتی در هنگامی که بین این نقاط پایانی جریان می‌یابد، منحرف یا متوقف نمی‌شود. همین ملاحظه برای اطلاعات تائید هویت (اعتبارسنجی) خدمت شبکه (از قبیل شناسه‌ها و گذرواژه‌های کاربر و شناسه‌ها و گذرواژه‌های مدیر اجرایی) نیز اعمال شود.
صحت (SR-SM&MS-٦)	از اطلاعات اجرایی و مدیریتی خدمات شبکه، در مقابل تغییر، حذف، ایجاد و تکرار غیرمجاز، محافظت کنید. این محافظت، برای اطلاعات اجرایی و مدیریتی مقیم در تجهیزات شبکه، در زمان مبادله در سرتاسر شبکه و یا زمان اقامت در سامانه‌های ذخیره‌سازی برون‌خط، اعمال شود. همین ملاحظه برای اطلاعات تائید هویت (اعتبارسنجی) خدمات شبکه (از جمله شناسه‌ها و گذرواژه‌های کاربر و شناسه‌ها و گذرواژه و گذرواژه‌های مدیر اجرایی) اعمال شود.
دسترس‌پذیری (SR-SM&MS-۷)	اطمینان حاصل کنید که توانایی مدیریت خدمات شبکه توسط پرسنل و دستگاه‌های مجاز را نمی‌توان انکار کرد. این امر، شامل محافظت در برابر حملات فعال از قبیل حملات ممانعت از خدمت و همچنین محافظت در برابر حملات غیرفعال از قبیل اصلاح یا حذف اطلاعات تایید هویت مدیر اجرایی شبکه (از جمله شناسه‌ها و گذرواژه‌های مدیر اجرایی) می‌شود.
حریم خصوصی (SR-SM&MS-۸)	اطمینان حاصل کنید، اطلاعاتی که می‌تواند برای شناسایی مدیریت اجرایی یا سامانه‌های مدیریتی خدمات شبکه مورد استفاده قرار گیرد، برای پرسنل غیرمجاز، در دسترس نمی‌باشند. از جمله اطلاعات آدرس IP یا نام دامنه که امکان شناسایی و هدف‌گیری سامانه‌های اجرایی خدمات شبکه را برای مهاجمان فراهم می‌کند.

۵. نیازمندی‌های امنیتی کنترل خدمات شبکه و خدمات کنترل شبکه (SR-SC&CS)

جدول (۴-۱۱) : نیازمندی‌های امنیتی کنترل خدمات شبکه و خدمات کنترل شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-SC&CS-۱)	اطمینان حاصل کنید که اطلاعات کنترل دریافت شده توسط یکی از تجهیزات شبکه برای یک خدمت شبکه، از یک مبدأ مجاز، نشأت می‌گیرد (به عنوان مثال، پیام شروع یک نشست VoIP توسط یک کاربر مجاز و یا دستگاه مجاز در شبکه ارسال شده است). این اطمینان، باید قبل از پذیرش درخواست ارسال شده، حاصل گردد. این امر، موجب محافظت از نشست، در برابر گمراه‌کردن یک پیام شروع یک نشست VoIP توسط یک دستگاه غیرمجاز، خواهد شد.
احراز هویت (SR-SC&CS-۲)	هویت منشأ اطلاعات کنترلی خدمت شبکه ارسالی به تجهیزات شبکه‌ای که در ارائه آن خدمت شبکه مشارکت دارد را تائید کنید. برای این منظور، ممکن است از روش‌های تائید هویت، به عنوان بخشی از کنترل دسترسی، استفاده شود.
عدم انکار (SR-SC&CS-۳)	برای شناسایی فرد یا دستگاه منشأ پیغام‌های کنترلی خدمت شبکه دریافت‌شده توسط یکی از تجهیزات شبکه‌ی مشارکت‌کننده در ارائه آن خدمت شبکه و تمام عملیاتی که در اثر آن پیغام‌های کنترلی انجام شده است، یک رکورد تشکیل دهید. این رکورد می‌تواند به عنوان اثباتی برای این که فرد یا دستگاه موردنظر، منشأ آن پیغام کنترلی خدمت شبکه بوده است، مورد استفاده قرار گیرد.
محرمانگی (SR-SC&CS-٤)	اطلاعات کنترلی خدمات شبکه مقیم در هر یک از تجهیزات شبکه (از جمله پایگاه داده‌های نشست IPSec)، در حال انتقال در سرتاسر شبکه یا ذخیره‌شده به‌صورت برون‌خط را در مقابل دسترسی غیرمجاز یا مشاهده، محافظت کنید.
امنیت ارتباط (SR-SC&CS-٥)	اطمینان حاصل کنید که اطلاعات کنترلی خدمت شبکه در زمان مبادله در سرتاسر شبکه ، فقط بین مبدأ اطلاعات کنترلی و مقصد موردنظر خودش جریان دارند.
صحت (SR-SC&CS-٦)	اطلاعات کنترلی خدمات شبکه‌ی مقیم در تجهیزات شبکه، در حال انتقال در شبکه، یا ذخیره شده به صورت برون‌خط را در مقابل تغییر غیرمجاز، حذف، ایجاد و تکرار، محافظت کنید.
دسترس‌پذیری (SR-SC&CS-۷)	اطمینان حاصل کنید که دستگاه‌های شبکه مشارکت کننده در یک خدمت شبکه، همیشه برای دریافت اطلاعات کنترلی از منشأهای مجاز، در دسترس می‌باشند. این امر، شامل حفاظت در برابر حملات فعال، از قبیل حملات ممانعت از خدمت است.
حریم خصوصی (SR-SC&CS-۸)	اطمینان حاصل کنید که اطلاعاتی که می‌تواند برای شناسایی تجهیزات شبکه و یا لینک‌های ارتباطی مشارکت کننده در ارائه یک خدمت، برای پرسنل یا دستگاه‌های غیرمجاز، در دسترس

	نمی‌باشند. نمونه‌ای از این نوع اطلاعات، آدرسIP یا نام دامنه تجهیزات شبکه است که می‌تواند توانایی شناسایی تجهیزات شبکه یا لینک‌های ارتباطی و هدف قرار دادن آن‌ها را برای مهاجمان فراهم کند.

٦. نیازمندی‌های امنیتی کاربری خدمات شبکه و خدمات کاربردی شبکه (SR-SU&US)

جدول (۴-۱۲) : نیازمندی‌های امنیتی کاربری خدمات شبکه و خدمات کاربردی شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-SU&US-۱)	اطمینان حاصل کنید که تنها کاربران و دستگاه‌های مجاز، امکان دسترسی و استفاده از خدمات شبکه را دارند.
احراز هویت (SR-SU&US-۲)	هویت کاربر یا دستگاه تلاش‌کننده برای دسترسی و استفاده از خدمت شبکه را تائید کنید. برای این امر، شاید لازم باشد از روش‌های تصدیق هویت، به عنوان بخشی از کنترل دسترسی، مورد استفاده قرار گیرند.
عدم انکار (SR-SU&US-۳)	برای شناسایی هر کاربر و دستگاهی به خدمات شبکه دسترسی و از آن‌ها استفاده می‌کند و همچنین همه‌ی عملیاتی که انجام می‌شود، یک رکورد تشکیل دهید. این رکورد، می‌تواند برای اثبات دسترسی و استفاده از خدمات شبکه به وسیله‌ی کاربر نهایی یا دستگاه موردنظر، استفاده شود.
محرمانگی (SR-SU&US-٤)	داده‌های کاربر نهایی که توسط یک خدمت شبکه منتقل می‌شوند، پردازش می‌شوند و یا ذخیره می‌شوند را در برابر دسترسی غیرمجاز یا مشاهده‌ی غیرمجاز، محافظت کنید.
امنیت ارتباط (SR-SU&US-٥)	اطمینان حاصل کنید که داده‌های کاربر نهایی که توسط یک خدمت شبکه انتقال داده می‌شوند، پردازش می‌شوند و یا ذخیره می‌شوند، در مسیر مبدأ تا مقصدشان، به‌واسطه‌ی دسترسی غیرمجاز، منحرف یا مسدود نمی‌شوند.
صحت (SR-SU&US-٦)	از داده‌های کاربر نهایی که توسط یک خدمت شبکه انتقال داده می‌شوند، پردازش می‌شوند و یا ذخیره می‌شوند، در مقابل تغییر، حذف، ایجاد و تکرار غیرمجاز، محافظت کنید.
دسترس‌پذیری (SR-SU&US-۷)	اطمینان حاصل کنید که دسترسی به خدمات شبکه توسط کاربران نهایی یا دستگاه‌های مجاز را نمی‌توان انکار کرد. این امر، شامل حفاظت در برابر حملات فعال مانند حملات ممانعت از خدمت و همچنین حفاظت در برابر حملات غیرفعال مانند اصلاح یا حذف اطلاعات تایید هویت کاربر نهایی (از جمله شناسه‌ها و گذرواژه‌های کاربر) می‌باشد.

حریم خصوصی (SR-SU&US-۸)	اطمینان حاصل کنید که خدمات شبکه، اطلاعات مربوط به استفاده‌ی کاربر نهایی از خدمات را (از جمله برای یک خدمت VoIP، طرفین مکالمه را) به پرسنل و دستگاه‌های غیرمجاز ارایه نمی‌کند.

۷. نیازمندی‌های امنیتی مدیریت کاربردهای شبکه و کاربردهای مدیریت شبکه (SR-AM&MA)

جدول (۴-۱۳) : نیازمندی‌های امنیتی مدیریت کاربردهای شبکه و کاربردهای مدیریت شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-AM&MA-۱)	اطمینان حاصل کنید که تنها پرسنل و دستگاه‌های مجاز، اجازه‌ی انجام فعالیت‌های اجرایی یا مدیریتی روی کاربردهای مبتنی بر شبکه (از جمله صندوق‌های پستی کاربر مدیر، برای یک کاربرد پست الکترونیکی) را دارند.
احراز هویت (SR-AM&MA-۲)	هویت فرد یا دستگاهی که تلاش می‌کند تا فعالیت‌های اجرایی یا مدیریتی روی کاربردهای مبتنی بر شبکه اجرا کند را تائید نمائید.
عدم انکار (SR-AM&MA-۳)	یک رکورد برای شناسایی فرد یا دستگاهی که هر فعالیت اجرایی یا مدیریتی مربوط به کاربردهای مبتنی بر شبکه انجام می‌دهد و کلیه عملیاتی که اجرا می شود، فراهم کنید. این رکورد می‌تواند برای اثبات انجام فعالیت اجرایی یا مدیریتی توسط آن فرد یا دستگاه، استفاده شود.
محرمانگی (SR-AM&MA-٤)	از تمامی پرونده‌هایی که در ایجاد و اجرای کاربردهای مبتنی بر شبکه استفاده می‌شوند (از جمله فایل‌های منبع، فایل‌های شیء، فایل‌های اجرایی، فایل‌های موقتی و نظایر آن‌ها)، محافظت کنید. همچنین فایل‌های پیکربندی کاربردها را در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت نمائید. این امر لازم است روی فایل‌های مقیم در تجهیزات شبکه، که از طریق شبکه انتقال داده می‌شوند، یا به‌صورت برون‌خط ذخیره می‌شوند، اعمال شود. از اطلاعات اجرایی یا مدیریتی کاربردهای مبتنی بر شبکه (از قبیل شناسه‌ها و گذرواژه‌های و شناسه‌ها و گذرواژه‌های مدیر)، در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت کنید.
امنیت ارتباط (SR-AM&MA-٥)	در مورد اجرا یا مدیریت از راه دور یک کاربرد مبتنی بر شبکه، اطمینان حاصل کنید که اطلاعات اجرایی و مدیریتی، تنها بین ایستگاه مدیریت از راه دور و دستگاه‌های مشارکت کننده در اجرای کاربرد مبتنی بر شبکه، جریان دارد. اطلاعات اجرایی و مدیریتی، به هنگام انتقال بین مبدأ و مقصد، منحرف یا متوقف نمی‌شوند.

	همین نوع ملاحظات، باید برای اطلاعات اجرایی یا مدیریتی کاربردهای مبتنی بر شبکه (از قبیل شناسه‌ها و گذرواژه‌های کاربر و شناسه‌ها و گذرواژه‌های مدیر)، اعمال شوند.
صحت (SR-AM&MA-٦)	از همه فایل‌هایی که در ایجاد و اجرای کاربردهای مبتنی بر شبکه استفاده می‌شوند (از جمله فایل‌های منبع، فایل‌های شیء، فایل‌های اجرایی، فایل‌های موقتی و نظایر آن‌ها)، محافظت کنید. همچنین فایل‌های پیکربندی کاربرد، در مقابل تغییر، حذف، ایجاد و تکرار غیرمجاز محافظت کنید. این محافظت، همچنین روی فایل‌های کاربردی مقیم در دستگاه‌های شبکه، در حال انتقال روی شبکه، یا ذخیره‌شده روی سامانه‌های برون‌خط، اعمال می‌شود. نوع مشابهی از ملاحظات، برای اطلاعات اجرایی یا مدیریتی کاربردهای مبتنی بر شبکه، اعمال می‌شود.
دسترس‌پذیری (SR-AM&MA-٧)	اطمینان حاصل کنید که توانایی اداره یا مدیریت کاربرد مبتنی بر شبکه توسط پرسنل و دستگاه‌های مجاز را نمی‌توان انکار کرد. این شامل محافظت در برابر حملات فعال مانند حملات ممانعت از خدمت و همچنین محافظت در برابر حملات غیرفعال مانند اصلاح یا حذف اطلاعات تائید هویت کاربردهای مبتنی بر شبکه از قبیل شناسه و گذرواژه کاربر می‌شود.
حریم خصوصی (SR-AM&MA-٨)	اطمینان حاصل کنید که اطلاعات قابل استفاده برای شناسایی سامانه‌های اجرایی یا مدیریت کاربردهای مبتنی بر شبکه، برای پرسنل یا دستگاه‌های غیرمجاز، قابل دسترس نباشند. نمونه‌هایی از این نوع اطلاعات، شامل آدرسIP یا نام دامنه‌ی سامانه‌ها می‌باشند. این اطلاعات، توانایی شناسایی سامانه‌های اجرایی کاربردهای مبتنی بر شبکه و هدف‌گیری آن‌ها را برای مهاجمان، فراهم می‌کند.

۸. نیازمندی‌های امنیتی کنترل کاربردهای شبکه و کاربردهای کنترل شبکه (SR-AC&CA)

جدول (۴-۱۴) : نیازمندی‌های امنیتی کنترل کاربردهای شبکه و کاربردهای کنترل شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-AC&CA-١)	اطمینان حاصل کنید که اطلاعات کنترل کاربرد دریافت شده توسط یکی از تجهیزات شبکه که در یک کاربرد مبتنی بر شبکه مشارکت دارد، از یک منشأ مجاز نشأت می‌گیرد. این اطمینان، باید قبل از پذیرش اطلاعات کنترل کاربرد فوق، انجام گیرد.
احراز هویت (SR-AC&CA-٢)	هویت منشأ اطلاعات کنترل کاربرد ارسال شده به تجهیزات شبکه که در کاربرد مبتنی بر شبکه مشارکت دارند را تایید کنید.
عدم انکار (SR-AC&CA-٣)	یک رکورد برای شناسایی فرد یا دستگاه منشأ پیغام‌های کنترلی کاربرد دریافت شده توسط یکی از تجهیزات شبکه که در برنامه کاربردی مبتنی بر شبکه مشارکت دارد و شناسایی عملیاتی

	که اجرا می‌شود، تشکیل دهید. این رکورد را می‌توان برای اثبات اینکه آن فرد یا دستگاه، منشأ ارسال پیغام کنترل کاربرد بوده است، به کار برد.
محرمانگی (SR-AC&CA-٤)	از اطلاعات کنترل کاربرد مقیم در یک دستگاه شبکه، در حال انتقال در سراسر شبکه، یا ذخیره‌شده در سامانه‌های ذخیره‌سازی برون‌خط، در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت کنید.
امنیت ارتباط (SR-AC&CA-٥)	اطمینان حاصل کنید که اطلاعات کنترلی کاربرد، از قبیل پیغام‌های گفت‌وگوی مبتنی بر SSL، که از طریق شبکه منتقل می‌شوند، تنها بین منبع اطلاعات کنترلی و مقصد موردنظر، جریان می‌یابند و اطلاعات کنترلی کاربردهای مبتنی بر شبکه، منحرف و یا مسدود نمی‌شوند.
صحت (SR-AC&CA-٦)	از اطلاعات کنترلی کاربردهای مبتنی بر شبکه مقیم در تجهیزات شبکه، در حال انتقال در شبکه، یاذخیره‌شده به‌صورت برون‌خط، در برابر تغییر، حذف، ایجاد و تکرار غیرمجاز، محافظت کنید.
دسترس‌پذیری (SR-AC&CA-٧)	اطمینان حاصل کنید که تجهیزات شبکه‌ای که در کاربردهای مبتنی بر شبکه مشارکت دارند، همیشه در دسترس هستند تا اطلاعات کنترلی را از منابع مجاز دریافت کنند. این شامل حفاظت در برابر حملات فعال مانند حملات ممانعت از خدمت است.
حریم خصوصی (SR-AC&CA-٨)	اطمینان حاصل کنید که اطلاعاتی که می‌تواند برای شناسایی تجهیزات شبکه یا لینک‌های ارتباطی مشارکت‌کننده در کاربردهای مبتنی بر شبکه به‌کار گرفته شوند، در دسترس پرسنل و دستگاه‌های غیرمجاز، نیستند. نمونه‌هایی از این نوع اطلاعات، شامل آدرسIP یا نام دامنه‌ی تجهیزات شبکه است که توانایی شناسایی تجهیزات شبکه یا لینک‌های ارتباطی و اطلاعات موردنیاز جهت هدف قرار دادن آن‌ها را برای مهاجمان فراهم می‌کند.

۹. نیازمندی‌های امنیتی کاربری کاربردهای شبکه و کاربردهای کاربری شبکه (SR-AU&UA)

جدول (۴-۱۵) : نیازمندی‌های امنیتی کاربری کاربردهای شبکه و کاربردهای کاربری شبکه

مؤلفه‌ی امنیت	توصیف
کنترل دسترسی (SR-AU&UA-١)	اطمینان حاصل کنید که تنها کاربران و دستگاه‌های مجاز، اجازه‌ی دسترسی و استفاده از کاربردهای مبتنی بر شبکه را دارند.
احراز هویت (SR-AU&UA-٢)	هویت کاربر یا دستگاه تلاش‌کننده برای دسترسی و استفاده از برنامه کاربردی مبتنی بر شبکه را تائید کنید.
عدم انکار (SR-AU&UA-٣)	یک رکورد برای شناسایی هر کاربر یا دستگاهی که به کاربردهای مبتنی بر شبکه دسترسی و از آن استفاده می‌کند، و عملیاتی که اجرا می‌شود، تشکیل دهید. این رکورد را می‌توان به عنوان

	اثباتی برای دسترسی و استفاده از کاربرد موردنظر، توسط آن کاربر نهایی یا دستگاه، مورد استفاده قرار داد.
محرمانگی (SR-AU&UA-٤)	داده‌های کاربر نهایی، اعم از شماره‌ی کارت اعتباری کاربر، که توسط یک کاربرد مبتنی بر شبکه ارسال می‌شود، مورد پردازش قرار می‌گیرد یا ذخیره می‌شود را در مقابل دسترسی یا مشاهده‌ی غیرمجاز، محافظت کنید. نوع مشابهی از ملاحظات، برای داده‌های کاربر، برای زمانی که این داده‌ها از کاربر به کاربرد مبتنی بر شبکه جریان می‌یابد، باید اعمال شود.
امنیت ارتباط (SR-AU&UA-٥)	اطمینان حاصل کنید که داده‌های کاربر نهایی که توسط یک برنامه کاربردی منتقل،پردازش یا ذخیره می‌شوند، در فاصله‌ی بین مبدأ و مقصد، با دسترسی غیرمجاز، منحرف یا متوقف نمی‌شوند. نوع مشابهی از ملاحظات، باید برای داده‌های کاربر، مادامی که این داده‌ها از کاربر به کاربرد مبتنی بر شبکه جریان می‌یابد، اعمال شود.
صحت (SR-AU&UA-٦)	از داده‌های کاربر نهایی که توسط یک برنامه کاربردی مبتنی بر شبکه ارسال، پردازش یا ذخیره می‌شود، در مقابل تغییر، حذف، ایجاد و تکرار غیرمجاز، محافظت کنید. نوع مشابهی از ملاحظات، باید برای داده‌های کاربر، در زمانی که از کاربر به سمت برنامه‌ی کاربردی مبتنی بر شبکه جریان می‌یابند، اعمال شود.
دسترس‌پذیری (SR-AU&UA-٧)	اطمینان حاصل کنید که دسترسی به برنامه‌ی کاربردی مبتنی بر شبکه توسط کاربران نهایی یا دستگاه‌های مجاز را نمی‌توان انکار کرد. این امر، شامل حفاظت در برابر حملات فعال از قبیل حملات ممانعت از خدمت و همچنین حفاظت در برابر حملات غیرفعال مانند اصلاح یا حذف اطلاعات تایید هویت کاربر نهایی، از قبیل شناسه‌ها و گذرواژه‌های کاربر می‌شود.
حریم خصوصی (SR-AU&UA-٨)	اطمینان حاصل کنید که کاربرد مبتنی بر شبکه، اطلاعات مربوط به استفاده‌ی از آن کاربرد توسط کاربران نهایی (از قبیل سایت‌های وب مشاهده شده توسط کاربر نهایی) را در اختیار پرسنل یا دستگاه‌های غیرمجاز، قرار نخواهد داد. برای مثال، افشای این اطلاعات، تنها به پرسنل انتظامی و پس از ارائه حکم بازرسی، انجام خواهد شد.

۵-٤- توصیه‌های ضروری

یک مرتبه در زمان تأمین امنیت سرمایه‌های سایبری سازمان (گام امن‌سازی) و یک مرتبه در زمان به‌کارگیری هر فناوری یا سامانه‌ی سایبری جدید در سازمان (گام پشتیبانی امنیت – مدیریت تغییرات)، لازم است موارد ذیل را به انجام رسانید :

۱. از لیست سرمایه‌های سایبری شناسایی شده یک سرمایه سایبری را انتخاب نمونه و مشخصات آن، به‌ویژه معماری سرمایه سایبری موردنظر را بررسی نمائید. در زمان به‌کار گیری یک فناوری یا سرمایه سایبری جدید در سازمان نیز معماری سرمایه سایبری موردنظر را بررسی نمائید.

۲. بر اساس معماری و ویژگی‌های سرمایه سایبری موردنظر، اجزاء تشکیل‌دهنده‌ی آن سرمایه را شناسایی نمائید. جدولی تشکیل دهید که حاوی تمام اجزاء معماری سرمایه سایبری موردنظر باشد.

۳. میزان اهمیت و ارزش هر یک از اجزاء معماری سرمایه سایبری موردنظر را مشخص نمائید و در جدولی که قبلاً تشکیل داده‌اید، آن را در مقابل جزء مربوطه، درج نمائید.

٤. لیستی از آسیب‌پذیری‌های موجود در سرمایه سایبری موردنظر را تهیه نمائید.

٥. لیستی از تهدیدهای موجود علیه سرمایه سایبری موردنظر را تهیه نمائید.

٦. تمام عوامل تعیین‌کننده‌ی نیازمندی‌های امنیتی، شامل اجزاء سرمایه سایبری، آسیب‌پذیری‌ها، تهدیدها و مؤلفه‌های امنیتی را در قالب یک شکل ترسیم نمائید و اطمینان حاصل نمائید که همه عوامل را در نظر گرفته‌اید.

۷. جدول نیازمندی‌های امنیتی سرمایه سایبری موردنظر را تشکیل دهید و در آن، مؤلفه‌های امنیتی که قابلیت مقابله با تهدیدهای موجود و جلوگیری از بهره‌برداری آن‌ها از آسیب‌پذیری‌های موجود در سرمایه سایبری موردنظر را داشته باشند، انتخاب نموده و در جدول، درج نمائید.

۸. در گام تأمین امنیت، جدول نیازمندی‌های امنیتی را مبنای انتخاب مکانیزم‌ها و ابزارهای امنیتی قرار دهید و تحقق تک‌تک این نیازمندی‌ها را در مراحل طراحی و پیاده‌سازی امنیت، بررسی و کنترل نمائید.

۹. پس از تأمین امنیت، در گام ارزیابی امنیتی دوره‌ای نیز می‌توانید از جدول نیازمندی‌های امنیتی برای کنترل جامعیت ارزیابی امنیتی بهره ببرید. ممکن است در اثر گذشت زمان، برخی کنترل‌های امنیتی پیاده‌سازی شده، بواسطه‌ی ملاحظاتی، غیرفعال یا بلااثر شده باشند.

فصل پنجم

جنگ سایبری

اهداف آموزشی پیش‌بینی شده برای این فصل، عبارتند از :

۱. کسب شناخت و توانایی تفکیک و طبقه‌بندی انواع تهاجم سایبری
۲. کسب شناخت در خصوص ابزارهای تشخیص و مقابله با انواع تهاجم سایبری و ویژگی‌های کلیدی آن‌ها
۳. کسب شناخت و بهره‌گیری از پایگاه داده حملات سایبری
٤. کسب شناخت در خصوص اشتراک‌گذاری اطلاعات تهاجم سایبری

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

۱. انواع تهاجم سایبری
۲. روش‌های فراگیر طبقه‌بندی تهاجم سایبری
۳. انواع و ویژگی‌های سامانه‌های تشخیص و مقابله با تهاجم سایبری
٤. نحوه‌ی استفاده از پایگاه داده سرشماری و طبقه‌بندی الگوی حملات مشترک
٥. ضرورت و مبانی اشتراک‌گذاری اطلاعات حملات سایبری توسط سازمان‌ها
٦. اقدامات دوره‌ای ضروری برای مدیریت حملات سایبری سازمان

۱-٥- تهاجم سایبری

حمله[۱]، یک تلاش برای «افشاء»، «سرقت»، «از کار انداختن»، «تغییر دادن»، «نابود کردن»، «کسب یا ایجاد دسترسی غیرمجاز به» یک سرمایه است. بر این اساس، حمله سایبری[۲]، فعالیتی است که از طریق فضای سایبر، با هدف

[۱] Attack
[۲] Cyber Attack

نقض امنیت یک سرمایه سایبری، اعم از «افشاء»، «سرقت»، «ایجاد اختلال»، «غیرفعال‌کردن»، «تغییر دادن»، «نابود کردن»، «کسب یا ایجاد دسترسی غیرمجاز به» یک سرمایه سایبری انجام می‌گیرد.

در فصل چهارم، از محرمانگی، یکپارچگی، دسترس‌پذیری به عنوان مؤلفه‌های اصلی امنیت و از کنترل دسترسی، تصدیق هویت، عدم انکار، امنیت ارتباط و حریم خصوصی به عنوان سایر مؤلفه‌های امنیت نام بردیم.

به این ترتیب، هر تلاشی که از طریق فضای سایبر، با هدف نقض یک یا چند مؤلفه‌ی امنیت یک سرمایه سایبری انجام شود، حمله یا تهاجم سایبری نامیده می‌شود.

۵-۲- انواع تهاجم سایبری

تهاجم سایبری ویژگی‌های متعددی دارد. مهاجم، منشأ حمله، نوع (ماهیت) حمله، هدف حمله، طرح (سناریوی) حمله، ابزار حمله، ویژگی‌های زمانی حمله اعم از مانایی و فرکانس تکرار، گستردگی (فراگیری)، پیچیدگی، شدّت یا قدرت و احتمال موفقیت حمله، ویژگی‌های اصلی تهاجم سایبری را تشکیل می‌دهند.

۵-۲-۱. انواع تهاجم سایبری از نظر مهاجم

انواع تهاجم سایبری، از نظر مهاجم به هک سایبری، هک با انگیزه‌ی خاص (رقابت، بدخواهی و سیاسی)، جرم سایبری، جاسوسی و تروریسم سایبری، نزاع و جنگ سایبری قابل طبقه‌بندی است. اصلی‌ترین تفاوت مهاجمین، تفاوت در توانایی‌ها و انگیزه‌ی مهاجم و منابع فنی، مالی و زمانی در اختیار مهاجم است. هک سایبری با ابزارهای بسیار ساده و رایگان و بدون نیاز به دانش و مهارت خاص انجام می‌شود و معمولاً هکر زمان زیادی را صرف نمی‌کند و به همین دلایل، تشخیص این نوع از حملات سایبری نیز معمولاً به سادگی، با هزینه‌ی اندک و صرف زمان بسیار کوتاه انجام می‌شود. این در حالی است که مجرمین سایبری برای انجام فعالیت‌های مجرمانه در فضای سایبر، از مهارت و توانایی بالاتری نسبت به هکرها برخوردارند، انگیزه‌ی زیادی برای تحقق اهداف خود دارند، از روش‌ها و ابزارهای پیچیده‌تری استفاده می‌کنند و سعی می‌کنند ردّ پایی از خود بر جا نگذارند و به همین دلایل، پلیس سایبری برای تشخیص جرایم سایبری، نیازمند تخصص و مهارت بالا و بهره‌گیری از ابزارها و آزمایشگاه‌های خاص کشف و تحلیل ادلّه‌ی جرم سایبری است و برای این امر، زمان و هزینه‌ی زیادی را صرف می‌کند. جدول (۵-۱)، ویژگی‌های انواع تهاجم سایبری، از نظر مهاجم را نشان می‌دهد. بر اساس محتوای این جدول، برای انواع بعدی تهاجم سایبری یعنی جاسوسی سایبری، تروریسم سایبری، نزاع سایبری و جنگ سایبری نیز هر چه پیش‌تر مهارت و توانایی‌های مهاجمین افزایش می‌یابد

جدول (۵-۱) : ویژگی‌های مهاجمین انواع تهاجم سایبری

نوع تهاجم	توانایی		منابع در اختیار مهاجم

	مهاجم	پیچیدگی تهاجم	ابزار فنی [۱]	منابع مالی [۲]	زمان صرف‌شده [۳]
نزاع و جنگ سایبری	خیلی‌زیاد (۵)	خیلی‌زیاد (۵)	خیلی‌پیچیده (۵)	خیلی‌زیاد (۵)	خیلی‌زیاد (۵)
جاسوسی و تروریسم سایبری	زیاد (۴)	زیاد (۴)	پیچیده (۴)	زیاد (۴)	زیاد (۴)
جرم سایبری	متوسط (۳)	متوسط (۳)	متوسط (۳)	متوسط (۳)	متوسط (۳)
هک سایبری با انگیزه‌ی خاص	کم (۲)	کم (۲)	ساده (۲)	کم (۲)	کم (۲)
هک سایبری	خیلی‌کم (۱)	خیلی‌کم (۱)	خیلی‌ساده (۱)	خیلی‌کم (۱)	خیلی‌کم (۱)

۲-۲-۵. انواع تهاجم سایبری از نظر هدف

در تعریف تهاجم سایبری، از «افشاء»، «سرقت»، «از کار انداختن»، «تغییر دادن»، «نابود کردن» و «کسب یا ایجاد دسترسی غیرمجاز» به عنوان اهداف تهاجم سایبری نام بردیم. اگر واژه‌ی فارسی هدف را به عنوان معنی واژه‌ی Objective یا Goal در زبان انگلیسی به کار ببریم، در این صورت هدف تهاجم سایبری یکی از موارد فوق خواهد بود. اما آنچه در عمل به عنوان هدف تهاجم سایبری مطرح می‌شود، کمی با این تعبیر متفاوت است. در عمل، واژه‌ی فارسی هدف، معمولاً به عنوان معنی واژه‌ی Target در زبان انگلیسی به کار برده می‌شود. در این کاربرد، منظور از هدف، موجودیت یا سرمایه سایبری است که مورد تهاجم سایبری قرار می‌گیرد.

حملات سایبری از نظر هدف (سرمایه سایبری هدف تهاجم)، در کلی‌ترین حالت، به دو دسته‌ی حملات رایانه‌ای و حملات شبکه‌ای تفکیک می‌شوند. حملات رایانه‌ای به حملاتی اطلاق می‌شود که علیه سامانه‌های اطلاعاتی انجام می‌شود و منظور از حملات شبکه‌ای، حملاتی است که وجه ارتباطی شبکه را مورد تهاجم قرار می‌دهند. در دسته‌بندی جزئی‌تر، حملات سایبری را می‌توان به سه دسته‌ی حملات علیه اطلاعات، سامانه‌های اطلاعاتی و شبکه تفکیک نمود، لیکن باید توجه داشت بجز در مورد اطلاعات ذخیره‌شده به عنوان پشتیبان [۴] که در محیط‌های ذخیره‌سازی منفرد و منفک از شبکه نگهداری می‌شوند، سایر مصادیق اطلاعات، معمولاً در داخل پایگاه‌های داده، سامانه‌های اطلاعاتی و یا تجهیزات شبکه نگهداری می‌شوند که می‌توان آنها را بخشی از یک سامانه اطلاعاتی در نظر گرفت و از طبقه‌بندی حملات رایانه‌ای و حملات شبکه‌ای استفاده نمود. حمله رایانه‌ای، یک سامانه اطلاعاتی، پایگاه داده و یا یک تجهیز شبکه اعم از سوئیچ، مسیریاب و نظایر این‌ها را مورد هدف قرار می‌دهد. این نوع حمله، ممکن است موجب از بین بردن اطلاعات یا دسترسی

---

[۱] ابزارهای هک معمولاً متن‌باز است و به عنوان سرگرمی توسط هکرها توسعه می‌یابند ولی ابزار جنگ سایبری، سلاح سایبری است که در قالب برنامه توسعه سلاح ارتش‌های سایبری و مبتنی بر فناوری‌های پیچیده توسعه می‌یابند

[۲] منابع مالی خیلی‌کم در محدوده‌ی چند دلار (قابل تأمین توسط هکرها) و منابع مالی خیلی‌زیاد در محدوده‌ی چند میلیون دلار (قابل تأمین توسط دولت‌ها) می‌باشند.

[۳] مجموع زمان صرف‌شده برای طراحی، تهیه مقدمات و اجرای تهاجم سایبری موردنظر است.

[۴] Backup

به داده‌ها، خرابکاری در سامانه و یا ایجاد اختلال و کاهش کارایی آن سامانه شود. ویروس، کرم، باج‌افزار، جاسوس‌افزار، اسپم، سرریز بافر و ممانعت از سرویس، مصادیقی از حملات رایانه‌ای را تشکیل می‌دهند. حملات شبکه‌ای، معمولاً علیه وجه ارتباطی شبکه انجام می‌شوند. انتشار یک کرم در شبکه، انتشار بات در شبکه، فعالیت هم‌زمان اعضای یک شبکه بات و انتشار ترافیک پرحجم علیه تعداد زیادی از سامانه‌های یک شبکه، مصادیقی از حملات شبکه‌ای می‌باشند. نمونه‌هایی از این حملات، با عنوان نمونه‌ی جنگ سایبری در کتاب مباحث مقدماتی پدافند سایبری ارائه شده است که جنگ سایبری علیه استونی و استاکس‌نت علیه ج.ا.ایران، نمونه‌هایی از آن را تشکیل می‌دهند. در حمله شبکه‌ای، ممکن است «شبکه به‌عنوان ابزاری برای انتشار ابزارهای حمله از قبیل کرم و بات یا انجام حمله استفاده شود» و یا « شبکه، هدف حمله قرار گیرد». بخشی از حملات رایانه‌ای و حملات شبکه‌ای، هم‌پوشانی دارند. مثلاً حملات رایانه‌ای که از محیط شبکه برای انجام حمله علیه یک سامانه اطلاعاتی استفاده می‌کنند، به صورت هم‌زمان، حمله رایانه‌ای و حمله شبکه‌ای تلقی می‌شوند.

دسته‌بندی‌های دیگری هم برای حملات در فضای سایبر ارائه شده است که علاوه بر حملات رایانه‌ای و حملات شبکه‌ای، شامل حملات اینترنتی،حملات سایبر–فیزیکی و حملات سایبر–اجتماعی می‌شود. حملات اینترنتی، حملاتی را در بر می‌گیرد که بر اساس ویژگی‌های خاص پروتکل HTTP، علیه سامانه‌های مبتنی بر وب انجام می‌شوند. حملات سایبر–فیزیکی، معمولاً از فضای سایبر آغاز شده و منجر به پیامد در یک سرمایه فیزیکی شده و در فضای فیزیکی خاتمه می‌یابند. نابود کردن یک خط لوله انتقال گاز از طریق صدور فرمان سایبری به شیرهای کنترل خطوط لوله، نمونه‌ای از حملات سایبر–فیزیکی است. تهاجم سایبر–اجتماعی نیز تهاجمی است که از فضای سایبر آغاز شده و موجب بروز صدمه در سرمایه‌های اجتماعی می‌شوند و به عبارت دیگر، این نوع حمله در فضای اجتماعی خاتمه می‌یابد. حملات روانی که از فضای سایبر و با انتشار محتوای هدفمند، منجر به تخریب باورها یا نابودی انسجام ملی در یک کشور می‌شوند، نمونه‌ای از تهاجم سایبر–اجتماعی است. بر این اساس، حملات در فضای سایبر، قابل دسته‌بندی در چهار دسته‌ی «حملات رایانه‌ای»، «حملات شبکه‌ای»، «حملات اینترنتی» و «حملات سایبری» می‌باشند.

۳-۲-۵. انواع تهاجم سایبری از نظر آسیب‌پذیری مورد استفاده

برای انجام یک حمله سایبری، دو شرط لازم وجود دارد. شرط لازم اول، وجود حداقل یک آسیب‌پذیری در سرمایه سایبری حمله است و شرط لازم دوم، وجود حداقل یک تهدید فعال (دارای توانایی، انگیزه، برخوردار از ابزارهای فنی، منابع مالی و زمانی) برای طراحی و اجرای حمله سایبری را تشکیل می‌دهند.

در فصل دوم، آسیب‌پذیری‌های سایبری را از نظر پیامد به دو دسته‌ی مخرّب و غیرمخرّب تفکیک نمودیم. با استناد به این طبقه‌بندی، حملات را نیز می‌توانیم به دو دسته‌ی مخرّب و غیرمخرّب طبقه‌بندی کنیم. همچنین آسیب‌پذیری‌های سایبری را از نظر وضعیت کشف، به دو دسته‌ی شناخته شده (کشف شده) و ناشناخته (کشف نشده) تفکیک نمودیم و بر اساس این طبقه‌بندی، می‌توانیم حملات سایبری را نیز به دو دسته‌ی شناخته شده و ناشناخته تفکیک

کنیم. البته منظور از حمله شناخته‌شده، حمله‌ای نیست که از آسیب‌پذیری شناخته شده استفاده می‌کند، بلکه حمله‌ای است که قبلاً حداقل یک‌مرتبه انجام شده و الگوی حمله [۱] توسط سامانه‌های تشخیص حمله، تشخیص داده شده است و در پایگاه داده حملات قرار گرفته است.

٤-۲-۵. انواع تهاجم سایبری از نظر مانایی

مانایی یا ماندگاری، به فاصله زمانی بین آغاز و پایان یک تهاجم سایبری اطلاق می‌شود. حملات سایبری از نظر مانایی، به دو دسته‌ی سریع و مانا تفکیک می‌شوند. حملات سریع، حملاتی هستند که معمولاً علیه یک سرمایه اطلاعاتی محدود و مشخص، به صورت مستقیم و یک مرحله‌ای انجام می‌شوند و در زمانی کوتاه، منجر به نتیجه شده و خاتمه می‌یابند. تشخیص این حملات، ساده است زیرا ذخیره‌سازی، تحلیل و تشخیص این نوع حملات، نیازمند حافظه و توان پردازشی کمی بوده و این حملات، به صورت برخط قابل تشخیص می‌باشند. در مقابل، حملات مانا، حملاتی هستند که در بازه‌ی زمانی طولانی، علیه یک یا چند سرمایه سایبری هدف، به صورت غیرمستقیم و در چند مرحله، به اجرا در می‌آیند. در اغلب موارد، ترافیک یا ابزار تهاجم مانا، از چند مسیر ارتباطی مختلف عبور داده می‌شود و از هر مسیر، بخشی از ترافیک یا ابزار تهاجم به سمت هدف گسیل می‌شود تا به تنهایی قابل تشخیص نباشد.

۵-۳- آشنایی با پایگاه داده سرشماری و طبقه‌بندی الگوی حمله مشترک [۲] (CAPEC)

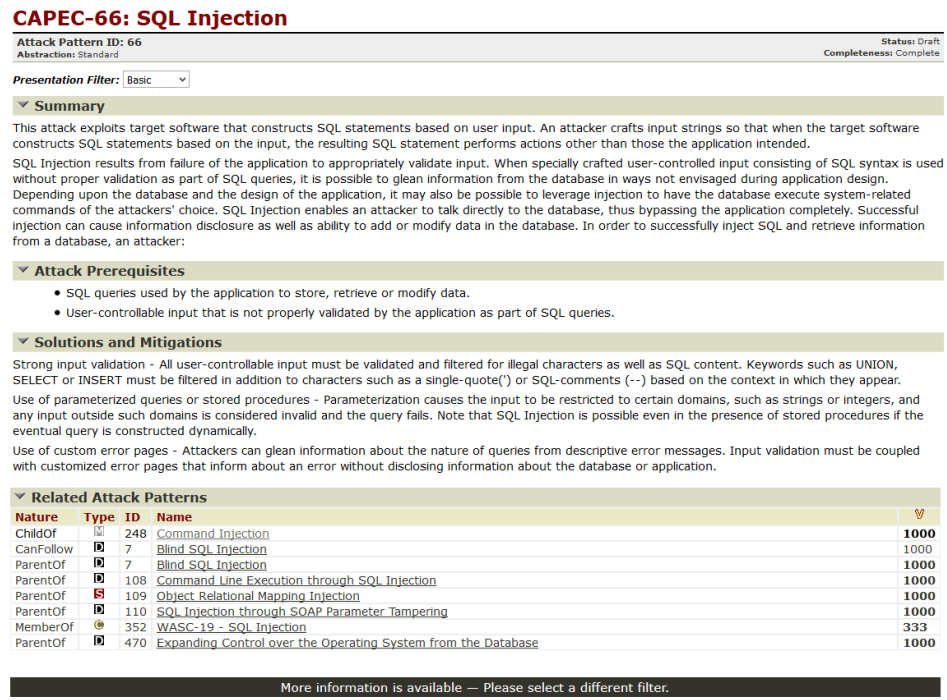
تنوع بسیار زیاد انواع دسته‌بندی حملات، موجب شده است تا پایگاه‌های داده متعدد برای حملات و کدهای بهره‌برداری ایجاد شوند. این پایگاه‌های داده، اطلاعات مربوط به حملات شناخته‌شده را در خود جای می‌دهند. اطلاعات موجود در این پایگاه‌های داده، می‌تواند توسط تحلیل‌گران، توسعه‌دهندگان، آزمون‌گران و افراد آکادمیک، برای افزایش درک حملات و بهبود روش‌های دفاعی، مورد استفاده قرار گیرد. یکی از اصلی‌ترین ویژگی‌های یک حمله، کد بهره‌برداری [۳] یا اکسپلویت آن حمله است که می‌تواند مستقیماً توسط مهاجم، مورد استفاده قرار گیرد.

پایگاه داده سرشماری و طبقه‌بندی الگوی حمله مشترک (CAPEC)، توسط شرکت غیرانتفاعی MITRE ایجاد شده است. CAPEC یک فرهنگ لغت جامع و یک طبقه‌بند کامل از حملات شناخته شده است. الگوهای حمله، ویژگی‌های مشترک حملات و رویکردهای مورد استفاده توسط مهاجمین، برای بهره‌برداری از آسیب‌پذیری‌های شناخته شده توسط مهاجمین را توصیف می‌کنند. هر الگوی حمله، دانش بخش‌های مختلف یک حمله، اعم از طراحی و اجرای حمله را به همراه توصیه‌هایی برای نحوه‌ی مواجهه با آن حمله، در خود نگهداری می‌کند.

---

۱ Attack Pattern
۲ Common Attack Pattern Enumeration and Classification (CAPEC)
۳ Exploit Code

شکل (۵–۱)، نمونه‌ای از الگوی حمله تزریق SQL ارائه شده در پایگاه داده CAPEC، با شماره CAPEC-٦٦ را نمایش می‌دهد.



CAPEC-66: SQL Injection

Attack Pattern ID: 66
Abstraction: Standard
Status: Draft
Completeness: Complete

Presentation Filter: Basic

Summary

This attack exploits target software that constructs SQL statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended.

SQL Injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. Depending upon the database and the design of the application, it may also be possible to leverage injection to have the database execute system-related commands of the attackers' choice. SQL Injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to add or modify data in the database. In order to successfully inject SQL and retrieve information from a database, an attacker:

Attack Prerequisites

- SQL queries used by the application to store, retrieve or modify data.
- User-controllable input that is not properly validated by the application as part of SQL queries.

Solutions and Mitigations

Strong input validation - All user-controllable input must be validated and filtered for illegal characters as well as SQL content. Keywords such as UNION, SELECT or INSERT must be filtered in addition to characters such as a single-quote(') or SQL-comments (--) based on the context in which they appear.

Use of parameterized queries or stored procedures - Parameterization causes the input to be restricted to certain domains, such as strings or integers, and any input outside such domains is considered invalid and the query fails. Note that SQL Injection is possible even in the presence of stored procedures if the eventual query is constructed dynamically.

Use of custom error pages - Attackers can glean information about the nature of queries from descriptive error messages. Input validation must be coupled with customized error pages that inform about an error without disclosing information about the database or application.

Related Attack Patterns

Nature	Type	ID	Name	V
ChildOf	M	248	Command Injection	**1000**
CanFollow	D	7	Blind SQL Injection	1000
ParentOf	D	7	Blind SQL Injection	**1000**
ParentOf	D	108	Command Line Execution through SQL Injection	**1000**
ParentOf	S	109	Object Relational Mapping Injection	**1000**
ParentOf	D	110	SQL Injection through SOAP Parameter Tampering	**1000**
MemberOf	C	352	WASC-19 - SQL Injection	**333**
ParentOf	D	470	Expanding Control over the Operating System from the Database	**1000**

More information is available — Please select a different filter.

شکل (۵–۱) : الگوی حمله تزریق SQL در پایگاه داده CAPEC

در این پایگاه داده، برای معرفی هر الگوی حمله، از تعدادی ویژگی استفاده شده است. این ویژگی‌ها در جدول (۵–۲) نمایش و توصیح داده شده‌اند.

جدول (۵–۲) : ویژگی‌های الگوی حملات در پایگاه داده CAPEC

ویژگی	توصیف
الف) ویژگی‌های اصلی	
۱. اطلاعات شناسایی	
Attack Pattern ID	شناسه الگوی حمله (با ساختار CAPEC-#### بیان می‌شود)
Attack Pattern Name	نام الگوی حمله (با ساختار CAPEC-####: <name> بیان می‌شود)
Pattern Abstraction level	سطح انتزاع الگو را بیان می‌کند. بسته به ویژگی‌های مورد نیاز در تعریف هر الگوی حمله، سه سطح انتزاع Meta , Standard , Detailed تعریف شده است.
۲. اطلاعات توصیفی	

Summary	توضیح حمله که به هدف حمله و ترتیب مراحل آن اشاره می‌کند.
Attack_Execution_Flow	
Related Vulnerabilities	آسیب‌پذیری‌های مورد استفاده در حمله، از قبیل CVE و US-Cert
Related Weaknesses	این مشخصه، ضعف های مورد استفاده در حمله را با توجه به استاندارد CWE مشخص می کند. در صورتی که ضعف مستقیما باعث حمله شود از نوع "targeted" است و در صورتی که احتمال حمله را افزایش دهد از نوع "Secondary" است.
Methods of Attack	بردار حمله‌ای که مورد استفاده قرار می‌گیرد.
Examples-Instances	حاوی یک یا بیش از یک مثال است. و شامل مثال توضیحی و یا اکسپولیت نمایشی از حمله مورد نظر یا آسیب پذیری های مرتبط است.
References	ارجاع به منابع خارجی برای دسترسی به اطلاعات بیشتر در مورد حمله.
۳. اطلاعات تجویزی	
Solution and mitigation	اعمال و رویکردهایی را برای کاهش اثر حمله توصیه می کند.
٤. اطلاعات مربوط به محدوده و مرزگذاری	
Typical Severity	در یک مقیاس کلی شدت و سختی یک حمله را نشان می‌دهد.(بسیار ضعیف، ضعیف، متوسط، سطح بالا، بسیار بالا)
Typical Likelihood of Exploit	احتمال موفقیت حمله را نشان می‌دهد. با سطوح بسیار ضعیف، ضعیف، متوسط، سطح بالا، بسیار بالا مشخص می شود.
Attack Prerequisites	برای اینکه حمله موفق شود چه قابلیت ها و شرایطی بایستی وجود داشته باشد و نرم افزار مورد هدف بایستی چه مشخصاتی داشته باشد و چه رفتاری از خود بروز دهد.
Attacker Skills or Knowledge Required	حمله کننده چه سطحی از مهارت و دانش برای اجرای چنین حمله ای باید داشته باشد؟ این مشخصه با سه سطح پایین، متوسط وبالا بیان می تواند بیان شود و نوع دانش مورد نیاز توضیح داده شود.
Resources Required	چه منابعی (نظیر سیکل CPU، آدرسهایIP، ابزار ها و زمان) برای اجرای حمله مورد نیاز است.
Attack Consequences Motivation	اهدافی که مهاجم سعی در بدست آوردن آن دارد.
Purposes	توصیف کلی هدف از الگوی حمله را به منظور کمک به طبقه بندی اهداف ارائه می دهد. این مشخصه شامل مجموعه ای از یک لیست از اهداف تعریف شده (مانند: شناسایی، نفوذ، بهره برداری و مبهم سازی) است که ممکن است در حال حاضر ناقص بوده و با شناسایی اهداف جدید ارتقاء یابند.
CIA Impact	سطح ضربه وارده توسط حمله به سه فاکتور امنیتی محرمانگی، صحت و دسترس‌پذیری را مشخص می کند.
Technical Context	شامل زمینه های فنی که با این الگو مرتبط است. ممکن است شامل سکو، سیستم عامل، زبان، نمونه ساختار و غیره باشد.
Keywords	این فیلد برای جستجوی راحت تر در تمام زمینه ها در نظر گرفته شده است.

Context Description	زمینه های مرتبط با حمله را مشخص می کند. این اطلاعات برای درک بهتر ماهیت این نوع از حمله مفید است.
۵. اطلاعات اداری	
Source	اطلاعات سطح بالایی از اینکه این الگو از کجا آمده و در طول تاریخ خود چگونه اصلاح شده است.
ب) ویژگی های پشتیبانی الگوهای حمله	
۱. اطلاعات توصیفی	
Injection Vector	مسیری که حمله از طریق آن صورت می گیرد را مشخص می کند.
Payload	کد، پیکربندی و سایر داده هایی که به عنوان بخشی از حمله مبتنی بر تزریق اجرا یا فعال شده را توصیف می کند.
Activation Zone	این شناسه مکان اجرای حمله را مشخص می کند. منطقه فعال سازی جایی است که مقاصد حمله‌کننده در آن بخش انجام می‌گیرد. این مناطق می توانند مفسر فرمان، کد ماشین فعال در بافر، یک مرورگر کاربر و فراخوان API سیستم باشد.
Payload Activation Impact	حمله کننده چه سطحی از مهارت و دانش برای اجرای چنین حمله ای می بایست داشته باشد؟ این مشخصه با سه سطح پایین، متوسط وبالا بیان می تواند بیان شود و نوع دانش مورد نیاز توضیح داده شود.
۲. اطلاعات تشخیصی	
Probing Techniques	تکنیک‌های کاوش شامل روش های جستجوی مهاجم برای تعیین آسیب پذیری سیستم قربانی برای دسترسی به آن است.
Indicators-Warnings of Attack	شاخص ها و اخطارهای حمله در واقع نشانه هایی هستند که هنگام بروز حمله ایجاد می شوند و توسط قربانی قابل لمس هستند.
Obfuscation techniques	این فیلد مجموعه تکنیک های مبهم سازی را نشان می دهد. یک تکنیک مبهم سازی برای پنهان کردن اینکه وضعیت حمله (قریب الوقوع ، درحال پیشرفت، رخ داده) چیست استفاده می‌شود.
۳. اطلاعات تکمیلی	
Related Attack Patterns	الگوهای حمله دیگری که به نوعی مربوط، وابسته و یا زنجیره وار با این الگوی حمله هستند را مشخص می‌کند.
Relevant Security Requirements	این شناسه نیازهای امنیتی خاص مرتبط با حمله مورد نظر را نشان می‌دهد.
Related Design Patterns	این مشخصه به پیشنهاد/عدم پیشنهاد الگوهای خاص طراحی نرم افزار جهت مقاومت بیشتر در مقابل حمله می‌پردازد.
Related Security Principles	شناسایی اصول امنیتی موجود که مربوط به شناسایی و یا کاهش حمله هستند. برای رفتارهای خوب یک اصل به عنوان یک قانون و یا استاندارد در نظر گرفته می‌شود.
Related Guidelines	شناسایی دستورالعمل‌های امنیتی موجود که مربوط به شناسایی و یا کاهش حمله هستند.
Target Attack Surface	این خصیصه مکانی را که مهاجم با سیستم هدف تعامل دارد را مشخص می‌کند.
Content History	شامل بخش‌های ارسال‌کننده (Submitter)، سازمان، تاریخ و منبع است.

Other Notes	این فیلد شامل کامنت‌های کلی است.
Relationships	ارتباط این الگوی حمله با سایر الگوهای حمله (روابطی مانند پدر و فرزندی و غیره) در این فیلد مشخص می شود.

٤-٥- روش‌های تشخیص تهاجم سایبری

مهاجم برای انجام یک حمله سایبری، از یک یا چند آسیب‌پذیری سایبری، استفاده می‌کند و برای این منظور، یک یا چند کد بهره‌برداری[۱] یا اکسپلویت را توسعه داده و یا مورد استفاده قرار می‌دهد. در نتیجه می‌توان گفت که اجرای هر حمله سایبری، وابسته به وجود یک آسیب‌پذیری است و تا زمانی که یک یا چند آسیب‌پذیری سایبری در سرمایه سایبری هدف حمله وجود نداشته باشد، اساساً حمله‌ای قابل اجرا نیست. به این ترتیب، یکی از مبانی اصلی تشخیص حمله، تشخیص آسیب‌پذیری است. یکی از روش‌های تشخیص حملات سایبری، شناسایی و تحلیل هر گونه تلاش مهاجم برای شناسایی و بهره‌گیری از آسیب‌پذیری‌های موجود در سرمایه سایبری است.

قبلاً اشاره شد که برای بهره‌گیری از هر آسیب‌پذیری، مهاجم باید از اکسپلویت یا کد سوءاستفاده از آن آسیب‌پذیری خاص، استفاده کند. اکسپلویت‌ها، کدهای مخربی هستند که با توجه به آسیب‌پذیری‌های شناخته‌شده توسعه یافته‌اند و تا زمانی‌که آن آسیب‌پذیری خاص در سرمایه سایبری هدف، برطرف نشده باشد، امکان استفاده از اکسپلویت مربوطه وجود خواهد داشت. اجرای یک اکسپلویت، به معنای انجام یک حمله سایبری با هدف «افشاء»، «سرقت»، «از کار انداختن»، «تغییر دادن»، «نابود کردن» یا «کسب یا ایجاد دسترسی غیرمجاز» است. اکسپلویت‌ها معمولاً هنگام کشف آسیب‌پذیری یا بعد از کشف آسیب‌پذیری توسعه می‌یابند. اغلب اکسپلویت‌ها توسط هکرها توسعه یافته‌اند اگرچه در موارد محدود، متخصصان امنیت نیز برای اثبات وجود یک آسیب‌پذیری مهم، اقدام به نوشتن کد اکسپلویت برای آن آسیب‌پذیری می‌نمایند. به این ترتیب، یک روش دیگر برای شناسایی حملات سایبری، تشخیص کد اکسپلویت مورد استفاده توسط مهاجم است. بر این اساس، یک روش بسیار پرکاربرد برای تشخیص حمله، استفاده از الگوی[۲] یا امضای[۳] حمله است. در این روش، الگو یا امضای کد اکسپلویت مورد استفاده برای انجام حمله، با الگوها یا امضاهای موجود در یک پایگاه داده تطبیق داده می‌شود و در صورت تطبیق با یکی از رکوردهای موجود در آن پایگاه داده، حمله‌ی در حال انجام، مورد شناسایی قرار می‌گیرد. این روش شناسایی حملات سایبری، با عنوان تشخیص مبتنی بر الگوی (امضای) حمله شناخته می‌شود. این روش تشخیص، فقط برای شناسایی حملات سایبری مناسب است که کد اکسپلویت آن‌ها در اختیار باشد (قبلاً در پایگاه‌های داده کدهای اکسپلویت یا سامانه‌های تشخیص حمله ثبت شده باشد) یا مهاجم، قبلاً با این روش، حداقل یک مرتبه اقدام به حمله نموده باشد و الگوی حمله توسط سامانه تشخیص حمله، به عنوان الگوی جدید حمله، شناسایی و در پایگاه داده الگوی حملات، ثبت شده باشد. در مقابل روش تشخیص مبتنی بر الگوی حمله، روشی با عنوان تشخیص مبتنی بر رفتار یا تشخیص مبتنی بر سوء استفاده وجود دارد که در این روش، ابتدا رفتار متعارف سامانه یا شبکه

---

۱ Exploit Code
۲ Pattern
۳ Signature

هدف تهاجم، شناسایی و ثبت می‌شود و هرگونه رفتار متفاوت با آن، به عنوان رفتار نامتعارف در نظر گرفته شده و نوعی حمله تلقی می‌گردد. پیچیدگی این روش در مقایسه با تشخیص حمله مبتنی بر الگو، بسیار بیشتر است و این روش، تنها در سامانه‌های تشخیص یادگیرنده امکان‌پذیر است.

در بخش‌های قبل، انواع حملات سایبری را به دو دسته، شامل حملات رایانه‌ای و حملات شبکه‌ای تفکیک نمودیم. به این ترتیب، دو روش پایه برای تشخیص حملات، شامل تشخیص مبتنی بر میزبان و تشخیص مبتنی بر شبکه است. تشخیص مبتنی بر میزبان، همان‌گونه که از عنوانش پیداست، از طریق قرار گرفتن روی یک سامانه اطلاعاتی، اقدام به دریافت و تحلیل تمام ورودی‌ها و خروجی‌های آن سامانه، پردازش‌های در حال انجام روی سامانه و مبادلات در حال انجام بین نرم‌افزارهای در حال اجرا یا پردازش‌های در حال انجام روی آن سامانه نموده و از این طریق، حمله علیه سامانه را تشخیص می‌دهد. در تشخیص مبتنی بر شبکه، سامانه‌ی تشخیص حمله به یک شبکه متصل شده و از طریق دریافت و تحلیل ترافیک در حال مبادله روی شبکه، اقدام به تشخیص حمله علیه شبکه یا سامانه‌های متصل به آن شبکه می‌کند. در سامانه‌های تشخیص تهاجم مبتنی بر شبکه، حجم ذخیره‌سازی و تحلیل اطلاعات بسیار زیاد است.

در بخش قبل، حملات سایبری را به دو دسته‌ی سریع و مانا تفکیک نمودیم. ویژگی کلیدی حملات سریع، کوتاه بودن بازه‌ی زمانی اجرای جمله، انجام حمله علیه یک سرمایه سایبری، اجرای حمله به صورت مستقیم، یک مرحله‌ای و از طریق یک مسیر ارتباطی است و ویژگی کلیدی حملات مانا نیز، طولانی بودن بازه‌ی زمانی اجرای حمله، انجام حمله علیه سرمایه‌های سایبری متعدد و اجرای حمله به صورت غیرمستقیم، چند مرحله‌ای و از طریق چند مسیر ارتباطی مکمّل است. برای این نوع حملات، بسته به برخورداری از ویژگی‌های طول زمانی، تعدد هدف، تعدد مراحل اجرا و تعدد مسیر حمله، علاوه بر حملات مانا، از عناوین حملات گسترده، حملات چندمرحله‌ای و حملات چندمسیره نیز استفاده می‌شود.

۵-۵- فناوری‌های تشخیص انواع تهاجم سایبری

برای تشخیص انواع حملات، اعم از حملات سریع یا مانا، حملات محدود یا گسترده، حملات یک یا چندمرحله‌ای و حملات یک یا چندمسیره، از چهار دسته سامانه‌های تشخیصی، در چهار سطح، مطابق جدول (۵-۳) استفاده می‌شود. حملات سریع توسط سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه (HIDS[۱]، HIPS[۲]، NIDS[۳] یا NIPS[۴]) با کمک انواعی از سامانه‌های تشخیصی خاص‌منظوره، نظیر سامانه دیوار آتش خاص کاربردهای وب[۵] (WAF) تشخیص داده می‌شوند. این سامانه‌ها، علی‌رغم بهره‌گیری از حجم حافظه و توان پردازشی محدود، از توانایی ذخیره‌سازی داده‌ها و تحلیل هم‌زمان تعداد قابل توجهی از حملات سریع و تشخیص قطعی وقوع این نوع از حملات برخوردار می‌باشند. اما برای تشخیص هم‌زمان تعداد زیادی از حملات مانا یا حملات چند مسیره

[۱] Host Based Intrusion Detection System (HIDS)
[۲] Host Based Intrusion Prevention System (HIPS)
[۳] Network Based Intrusion Detection System (NIDS)
[۴] Network Based Intrusion Prevention System (NIPS)
[۵] Web Application Firewall (WAF)

یا حملات گسترده و یا حملات چندمرحله‌ای، حجم حافظه و توان پردازشی بسیار زیادی موردنیاز است. به همین دلیل، سامانه‌های تشخیص نفوذ، قادر به تشخیص تعداد زیادی از این دسته حملات نیستند. برای این منظور، لازم است ترکیبی از سامانه‌های تشخیصی مختلف، در چهار سطح، مطابق آنچه در جدول (۶-۳) نمایش داده شده است، به کار گرفته شوند. در سطح اول، انواع سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه (HIDS، HIPS، NIDS یا NIPS) یا انواع خاص‌منظوره‌ی آنها نظیر سامانه دیوار آتش خاص کاربردهای وب (WAF) مورد استفاده قرار می‌گیرند. این سامانه‌ها، علاوه بر تشخیص «حملات ساده»، تشخیص «خرده‌حملات تشکیل دهنده‌ی یک حمله‌ی پیچیده» را نیز انجام می‌دهند و اطلاعات مربوط به این خرده‌حملات را برای تشخیص کامل و نهایی، در اختیار سامانه‌های سطح بعد قرار می‌دهند. در سطح دوم، مراکز عملیات امنیت [۱] (SOC) قرار دارند که با دریافت اطلاعات خرده‌حملات از سامانه‌های سطح اول و با بهره‌گیری از موتور همبستگی‌سنجی، اقدام به تشخیص همبستگی و ارتباط بین خرده‌حملات دریافتی نموده و از طریق یافتن این همبستگی‌ها، حملات طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره که مبدأ و مقصد آنها در داخل یک شبکه قرار داشته باشند را شناسایی خواهند نمود.

جدول (۵-۳) : سطوح چهارگانه تشخیص حملات مانا، گسترده، چندمرحله‌ای و چندمسیره

سطح	هدف	نوع سامانه
چهارم	تشخیص حملات مانا، گسترده، چندمرحله‌ای و چندمسیره بین زیرساخت‌های حیاتی مختلف	ISAS
سوم	تشخیص حملات مانا، گسترده، چندمرحله‌ای و چندمسیره در یک زیرساخت حیاتی	ISAC
دوم	تشخیص حملات مانا، گسترده، چندمرحله‌ای و چندمسیره در یک کلان شبکه	SOC
اول	تشخیص خرده‌حملات	HIDS، HIPS، NIDS، NIPS، WAF یا نظایر آنها

محدودیت اصلی مراکز عملیات امنیت، در تشخیص دسته‌ای از حملات طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره است که به‌صورت توزیع‌شده، از طریق عبور از چند شبکه، انجام می‌گیرند. حالتی را در نظر بگیرید که بخش‌هایی از یک حمله گسترده، از دو شبکه‌ی مرتبط به هم، عبور نموده و از طریق گذرگاه‌های مختلف، وارد شبکه هدف شود. تشخیص چنین حمله‌ای توسط مراکز عملیات امنیت این سه شبکه امکان‌پذیر نخواهد بود. این نوع از حملات پیچیده، توسط مرکز اشتراک‌گذاری و تحلیل اطلاعات [۲] (ISAC) زیرساخت ارتباطی کشور (ICT-ISAC) تشخیص داده خواهند شد. به این ترتیب، در سطح سوم شکل، سامانه‌های اشتراک‌گذاری و تحلیل اطلاعات (ISAC) قرار دارند. این

[۱] Security Operation Center (SOC)
[۲] Information Sharing and Analysis Center (ISAC)

امر، نیازمند اتصال تمام مراکز عملیات امنیت (SOC) شبکه‌های ارتباطی، به مرکز اشتراک‌گذاری و تحلیل اطلاعات زیرساخت ارتباطی کشور (ICT-ISAC) است.

به همین ترتیب، برای تشخیص حملات بین بخشی مثلاً حمله‌ای که مبدأ آن در زیرساخت ارتباطی کشور و مقصد آن در زیرساخت انرژی کشور باشد، نوع دیگری از سامانه‌های تشخیصی موردنیاز است که در سطح چهارم قرار می‌گیرند. این سامانه، با عنوان سامانه اشتراک‌گذاری و هشدار سایبری[۱] (ISAS) شناخته می‌شود. در هر کشور، یک سامانه ISAS مورد نیاز است. این سامانه علاوه بر فراهم نمودن امکان تشخیص حملات بین زیرساخت‌های حیاتی مختلف یک کشور، تشخیص وضعیت سایبری کشور را نیز بر عهده دارد.

۱-۵-۵. سامانه‌ی تشخیص و مقابله یا پیش‌گیری از حملات سایبری

ساده‌ترین سامانه‌های تشخیصی مرتبط با حملات سایبری، سامانه‌های تشخیص و مقابله با نفوذ (IDS) هستند. نوع پیشرفته‌تری از سامانه‌های تشخیصی، با عنوان سامانه‌های تشخیص و پیش‌گیری از نفوذ (IPS) شناخته می‌شوند. این سامانه‌ها از دقت بسیار زیادی برخوردار بوده و قابلیت تشخیص و اقدام پیش‌گیرانه را فراهم می‌آورند. این دو نوع سامانه، با عنوان کلی «سامانه‌های تشخیص و مقابله/پیش‌گیری از نفوذ» (IDPS) نامیده می‌شوند. IDPSها، برای تشخیص حملات در دو محیط شبکه و میزبان، طراحی و پیاده‌سازی می‌شوند. نوعی از این سامانه‌ها که تشخیص حملات در محیط شبکه را بر عهده دارند با عنوان «سامانه‌های تشخیص و مقابله/پیش‌گیری از حملات مبتنی بر شبکه» (NIDPS) و نوع دیگری که تشخیص حملات در محیط میزبان را بر عهده دارند با عنوان «سامانه‌های تشخیص و مقابله/پیش‌گیری از حملات مبتنی بر میزبان» (HIDPS) نامیده می‌شوند.

روش تشخیص در انواع سامانه‌های H/N-IDPS

تشخیص حملات سایبری توسط انواع سامانه‌های تشخیص و مقابله/پیش‌گیری از حملات مبتنی بر شبکه و میزبان، بر اساس سه روش «تشخیص مبتنی بر الگو[۲]»، «تشخیص مبتنی بر رفتار نامتعارف[۳]» و «تحلیل حالت کامل مقاوله‌نامه[۴]» انجام می‌شود.

«تشخیص مبتنی بر الگو»، ساده‌ترین روش تشخیص حملات است. در این روش، الگو یا امضای کد اکسپلویت حملات شناخته شده در یک پایگاه داده ذخیره می‌شوند و سامانه تشخیص نفوذ، برای تشخیص وجود حملات شناخته شده در ترافیک عبوری از شبکه یا ترافیک ورودی به میزبان، داده‌های در حال مبادله در ترافیک موردنظر را با الگوی تمام کدهای اکسپلویت موجود در پایگاه داده حملات، تطبیق می‌دهد و در صورت انطباق، به وجود آن حمله در ترافیک

---

[۱] Information Sharing and Alert System (ISAS)
[۲] Signature Based Detection
[۳] Anomaly Based Detection
[۴] Stateful Protocol Analysis

عبوری پی می‌برد. به این ترتیب، محدودیت اصلی روش تشخیص مبتنی بر الگو، این است که با این روش، تنها می‌توان حملات شناخته شده را تشخیص داد.

در روش «تشخیص مبتنی بر رفتار نامتعارف»، ابتدا پارامترهای توصیف‌کننده‌ی رفتار تعیین می‌شوند. سپس آستانه‌ی هر پارامتر برای رفتار متعارف تعیین می‌شود و نهایتاً در صورت عدم انطباق تعدادی از پارامترهای توصیف‌کننده‌ی رفتار شبکه یا سامانه موردنظر با مقادیر پارامترهای رفتار متعارف آن شبکه یا سامانه، این امر به عنوان یک نفوذ یا حمله تلقی می‌گردد. نوع پروتکل‌های مورد استفاده در یک شبکه و حجم ترافیک هر نوع پروتکل در ساعات مشخصی از روز، دو مورد از پارامترهای توصیف‌کننده‌ی رفتار متعارف کاربران یک شبکه را تشکیل می‌دهند. پیچیدگی اصلی روش تشخیص مبتنی بر رفتار نامتعارف، آن است که مقادیر پارامترهای توصیف‌کننده‌ی رفتار متعارف، باید برای هر شبکه، تعیین شوند. تعیین این مقادیر، برای در یک فاز با عنوان یادگیری انجام می‌شود. برای این منظور، سامانه تشخیص تهاجم، برای یک بازه‌ی زمانی مشخص، مثلاً یک یا دو ماه، در شبکه موردنظر نصب می‌شود تا مقادیر پارامترهای توصیف‌کننده‌ی رفتار متعارف را اندازه‌گیری و ثبت کند. در خاتمه فاز یادگیری، مقادیر آستانه‌ای که برای تمام پارامترهای توصیف‌کننده‌ی رفتار متعارف به دست آمده‌اند، به عنوان مقادیر آستانه‌ای ثبت می‌شوند و از این پس، مبنای تشخیص رفتار متعارف از نامتعارف قرار می‌گیرند. البته یادگیری می‌تواند در مراحل بعد نیز ادامه یابد و مقادیر آستانه‌ای پارامترها رفته رفته دقیق‌تر شوند. روش تشخیص مبتنی بر رفتار نامتعارف، نه تنها پیچیده‌تر از روش تشخیص مبتنی بر الگو است، بلکه آماده به کار شدن یک سامانه تشخیص مبتنی بر رفتار نامتعارف در یک شبکه خاص، مدت زمان قابل توجهی برای فاز یادگیری رفتار متعارف آن شبکه خاص نیاز دارد در صورتی که یک سامانه تشخیص حمله مبتنی بر الگو هیچ زمانی را برای یادگیری نیاز ندارد و بلافاصله می‌تواند عملیاتی شود. البته روش تشخیص مبتنی بر رفتار نامتعارف، در مقابل این دو اشکال یعنی «پیچیدگی تشخیص» و «زمان یادگیری»، از یک مزیت برتری‌بخش نسبت به روش تشخیص مبتنی بر الگو برخوردار است. این مزیت، «دقت تشخیص بالا» است. اشکال اساسی روش تشخیص مبتنی بر الگو، دقت پائین آن است که عملاً سامانه‌های تشخیص مبتنی بر الگو را در محیط واقعی ناکارآمد می‌کند. برای رفع این اشکال، معمولاً تمام سامانه‌های تشخیص کارآمد، از ترکیب دو روش تشخیص مبتنی بر الگو و مبتنی بر رفتار نامتعارف استفاده می‌کنند تا از مزایای برتری‌بخش هر دو روش یعنی سرعت روش مبتنی بر الگو و دقت روش مبتنی بر رفتار نامتعارف را استفاده نمایند.

در روش «تحلیل حالت کامل مقاوله‌نامه»، تحلیل رفتار در سطح نمودار حالت پروتکل ارتباطی در حال استفاده انجام می‌گیرد. یعنی به جای تحلیل پارامترهای کلی توصیف‌کننده‌ی رفتار یک شبکه، تحلیل در سطح نمودار حالت هر پروتکل ارتباطی مورد استفاده، انجام می‌گیرد. این امر، موجب افزایش شدید پیچیدگی تشخیص تهاجم می‌شود ولی در عوض، دقت را بسیار افزایش خواهد داد زیرا کوچک‌ترین تخطی از رفتار متعارف، قابل تشخیص خواهد بود. از آنجا که محصولات شرکت‌های مختلف، یک پروتکل ارتباطی را با ویژگی‌های بعضاً متفاوتی پیاده‌سازی می‌کنند، لذا استفاده از این روش در سامانه‌های تشخیص تهاجم، عملاً موجب پیچیدگی زیاد و کندی شدید عملیات تشخیص تهاجم می‌شود. به همین دلیل، از این روش تنها برای تشخیص موارد خاص یا تحلیل پروتکل‌های خاص استفاده می‌شود. در مواردی

هم به‌جای تحلیل حالت کامل، تنها برخی از حالات نمودار حالت پروتکل و یا پارامترهای کلیدی توصیف‌کننده‌ی نمودار حالت پروتکل، مورد تحلیل قرار می‌گیرند.

روش «تشخیص ترکیبی» نیز از ترکیب سه روش پیش‌گفته و با هدف بهره‌گیری از مزایای این روش‌ها، مورد استفاده قرار می‌گیرد.

در جدول (۵-۴)، ویژگی‌های سه روش «تشخیص مبتنی بر الگو»، «تشخیص مبتنی بر رفتار نامتعارف» و «تحلیل حالت کامل مقاوله‌نامه» مورد مقایسه قرار گرفته‌اند.

جدول (۵-۴) : مقایسه ویژگی‌های سه روش تشخیص مبتنی بر الگو، رفتار نامتعارف و تحلیل حالت کامل پروتکل

روش تشخیص	پیچیدگی	زمان یادگیری	دقّت
مبتنی بر الگو	کم	ندارد (صفر)	کم
مبتنی بر رفتار نامتعارف	متوسط	متوسط	متوسط
تحلیل حالت کامل پروتکل	زیاد	زیاد	زیاد
ترکیبی	متوسط	متوسط	زیاد

۲-۵-۵. مرکز عملیات امنیت (SOC)

مرکز عملیات امنیت (SOC) مجموعه‌ای از سامانه‌ها، فرآیندها و تیم‌های عملیاتی است که به‌منظور تشخیص و مقابله با حملات سایبری طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره که مبدأ و مقصد آنها در داخل یک شبکه قرار داشته باشند، به‌کار گرفته می‌شوند. مرکز عملیات امنیت، اطلاعات مربوط به خرده‌حملات تشخیص داده شده را از سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه (HIDS، HIPS، NIDS یا NIPS)، یا انواع خاص‌منظوره‌ی آنها نظیر سامانه دیوار آتش خاص کاربردهای وب (WAF)، دریافت می‌کند و از طریق تشخیص همبستگی موجود بین حملات متعدد تشخیص داده شده توسط این سامانه‌ها، حمله‌ی اصلی را تشخیص می‌دهد. منظور از حمله‌ی اصلی، حمله‌ای است که حداقل یکی از ویژگی‌های چهارگانه‌ی طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره را داشته باشد.

اهداف به‌کارگیری مرکز عملیات امنیت (SOC)

اصلی‌ترین هدف به‌کارگیری یک مرکز عملیات امنیت، تشخیص برخط حملات سایبری توزیع‌شده، اعم از حملات سایبری طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره است.

فعالیت‌های مرکز عملیات امنیت (SOC)

بر اساس ویژگی‌هایی که برای یک مرکز عملیات امنیت برشمردیم، مرکز عملیات امنیت، انجام سه فعالیت کلان ذیل را بر عهده دارد :

فعالیت کلان اوّل : جمع‌آوری و ثبت رویدادها.

مرکز عملیات امنیت، اطلاعات ورودی خود را از «انواع سامانه‌های امنیت سایبری» اعم از سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه، سامانه‌های دیوار آتش، سامانه‌های مدیریت یکپارچه تهدید و ضد بدافزارها، «انواع سامانه‌های سایبری» اعم از سوئیچ‌ها، مسیریاب‌ها، میزبان‌های خدمات کاربردی از قبیل وب و پست الکترونیکی و «انواع سامانه‌های سایبری–فیزیکی» اعم از سامانه‌های مبتنی بر کنترل صنعتی دریافت می‌کنند. از مهم‌ترین رویدادهای ورودی مرکز عملیات امنیت، می‌توان به خُرده‌حملات تشخیص داده شده توسط انواع سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه اشاره نمود. کلیه رویدادهای جمع‌آوری شده، در قالب یک پایگاه داده ذخیره می‌شوند تا متعاقباً مورد تحلیل و پردازش قرار گیرند.

مرکز عملیات امنیت، به‌منظور اجرای فعالیت «جمع‌آوری و ثبت رویدادها»، اقدام به انجام دو فعالیت «جمع‌آوری رویدادها» و «ثبت رویدادها» می‌نماید. زیرفعالیت‌های هر یک از این دو فعالیت، در جدول (۵–۵)، نمایش داده شده است.

جدول (۵–۵) : زیرفعالیت‌های «جمع‌آوری و ثبت رویدادها»

فعالیت کلان	فعالیت	عنوان زیرفعالیت	شرح زیرفعالیت
جمع‌آوری و ثبت رویدادها	جمع‌آوری رویدادها	جمع‌آوری	دریافت اطلاعات رویدادها، از عامل‌های تشخیص رویداد
		تبدیل	اعمال تغییر در الگوی رویدادهای ورودی و سازگار نمودن آن‌ها با سامانه
		دسته‌بندی	گروه‌بندی رویدادهای ورودی، بر اساس نوع مولد رویداد
		تست یکپارچگی	حصول اطمینان از عدم تغییر رویداد، در مسیر مبادله از عامل تشخیص تا سامانه
		نرمالیزه‌سازی زمانی	همسان‌سازی زمانی رویدادها نسبت به مبدأ زمان
		نرمالیزه‌سازی الگو	همسان‌سازی مؤلفه‌های رویداد از طریق تبدیل فرمت جهت ایجاد قابلیت پردازش توسط واحد تحلیل
		پالایش	پالایش رویدادها به‌منظور افزایش آنتروپی اطلاعات
		اولویت‌بندی	تعیین اولویت ثبت و بررسی رویدادها
	ثبت رویدادها	تبدیل رویداد	تغییر الگو و شکل رودیداد جهت ایجاد سازگاری
		تجمیع رویدادها	هم‌گرا نمودن اطلاعات مشابه و اختصاص شناسه مشترک
		امن‌سازی	تأمین امنیت ارتباط، از طریق اعمال رمزنگاری و اطمینان از صحت ذخیره رویدادها و کنترل دسترسی جهت دسترسی به اطلاعات رویدادها
		فشرده‌سازی	کاهش حجم اطلاعات رویدادها جهت ثبت در پایگاه داده
		چرخش	مدیریت چرخش رکوردهای موجود در صف آرشیو رویدادها جهت جلوگیری از رونویسی آن‌ها
		آرشیو	ذخیره‌سازی رویداد در پایگاه داده با فرمت استاندارد، جهت نگهداری طولانی‌مدت

فعالیت کلان دوّم : تحلیل رویدادها و تشخیص رخدادهای امنیتی.

مرکز عملیات امنیت، با تحلیل انواع رویدادهای ورودی، اقدام به تشخیص رخدادهای امنیتی می‌نماید. ورودی این فعالیت کلان، از پایگاه داده رویدادها تأمین می‌شود. مرکز عملیات امنیت، از طریق همبستگی‌سنجی رویدادهای مختلف با یکدیگر، ارتباطات و وابستگی‌های موجود بین رویدادهای مختلف را شناسایی نموده و در ادامه، رویدادهای دارای همبستگی که قابل تجمیع در قالب یک رخداد امنیتی می‌باشند را شناسایی می‌نماید. به این ترتیب، حملات طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره، از طریق همبستگی موجود بین خُرده‌حملات، شناسایی می‌شوند.

مرکز عملیات امنیت، به‌منظور اجرای فعالیت «تحلیل رویدادها و تشخیص رخدادهای امنیتی»، اقدام به انجام دو فعالیت «تحلیل رویدادها» و «تشخیص رخدادهای امنیتی» می‌نماید. زیرفعالیت‌های هر یک از این دو فعالیت، در جدول (۶-۵)، نمایش داده شده است.

جدول (۵-۶) : زیرفعالیت‌های «تحلیل رویدادها و تشخیص رخدادهای امنیتی»

فعالیت کلان	فعالیت	عنوان زیرفعالیت	شرح زیرفعالیت
تحلیل رویدادها و تشخیص رخدادهای امنیتی	تحلیل رویدادها	واکشی رویداد	واکشی رویداد از پایگاه داده رویدادها
		صحت‌سنجی رویداد	تصدیق رویداد، با استفاده از هشدار مثبت نادرست و هشدار مثبت درست
		خوشه‌یابی رویداد	
		ادغام (تجمیع) رویدادها	ترکیب رویدادهای مرتبط، به‌منظور کاهش حجم پردازش
		بازسازی ریسمان حمله	جداسازی مجموعه رویدادهای مربوط به حملات یک مهاجم به یک هدف مشخص
		بازسازی نشست حمله	برقراری ارتباط بین رویدادهای مربوط به حملات مهاجمین مختلف
		بازسازی تمرکز حمله	شناسایی میزبان‌هایی که مبدأ یا مقصد تعداد زیادی حمله بوده‌اند
	تشخیص رخدادهای امنیتی	همبستگی‌سنجی مبتنی بر قانون	تشخیص حمله‌ی شناخته شده از طریق تطبیق با الگوهای سطح بالای حملات شناخته شده (از طریق تشخیص حملاتی که از الگوهای سطح بالای مشابه برخوردار می‌باشند)
		همبستگی‌سنجی مبتنی بر ناهنجاری	تشخیص حملات ناشناخته (جدید)، تشخیص علت ریشه‌ای حمله و تشخیص سناریوی حمله‌ی جدید
		تعیین ویژگی‌های حمله	تعیین ویژگی‌های حمله، شامل مبدأ، مقصد، شدّت، پیامد، زمان وقوع و مدت حمله سایبری
		به‌روز رسانی پایگاه داده حملات	ثبت ویژگی‌های حمله‌ی تشخیص داده شده، در پایگاه داده حملات سایبری
		به‌روز رسانی پایگاه دانش حملات	به‌روز رسانی پایگاه دانش حملات، از طریق ثبت ریشه‌ی تشخیص داده شده برای حمله و سناریوی حمله‌ی جدید تشخیص داده شده در این پایگاه دانش

فعالیت کلان سوّم : واکنش به رخدادهای امنیتی.

مرکز عملیات امنیت، پس از تشخیص یک حمله سایبری، اقدام به انجام واکنش مناسب و برنامه‌ریزی شده، در مواجهه با آن حمله می‌نماید. ساده‌ترین نوع واکنش که در واقع یک واکنش مقدماتی محسوب می‌شود، صدور هشدار مبنی بر وقوع حمله است. پیغام هشدار، در حالت کلی، ممکن است برای مدیر شبکه، مدیر امنیت شبکه و نظایر آن‌ها

ارسال شود. در یک پیغام هشدار، ممکن است برخی ویژگی‌های حمله، اعم از مبدأ حمله، مقصد حمله، شدت حمله، پیامدهای وقوع حمله و نظایر آن‌ها نیز اعلام شود. پس از انجام واکنش مقدماتی، نوبت به انجام بخش اصلی واکنش می‌رسد. واکنش به یک حمله سایبری، به‌صورت نیمه‌خودکار یا تمام‌خودکار انجام می‌گیرد.

نوع اول واکنش، واکنش نیمه‌خودکار است. در این حالت، واکنش توسط عامل انسانی و بر اساس الگوی از پیش تعریف شده انجام می‌گیرد. به این ترتیب که الگوی واکنش به هر حمله، از قبل تعیین شده و در داخل یک پایگاه داده ذخیره می‌شود و مرکز عملیات امنیت، پس از تشخیص نوع حمله، الگوی واکنش به آن حمله‌ی خاص را از پایگاه داده واکشی نموده و آن الگو را در اختیار تیم انسانی مرکز عملیات امنیت قرار می‌دهد تا واکنش مناسب، بر اساس آن الگو، در مواجهه با آن حمله‌خاص، انجام گیرد.

نوع دوم واکنش، واکنش خودکار است. در این حالت، واکنش به‌صورت کام توسط ماشینی و بر اساس الگوی از پیش تعریف شده انجام می‌گیرد. به این ترتیب که الگوی واکنش به هر حمله، از قبل تعیین شده و در داخل یک پایگاه داده ذخیره می‌شود و مرکز عملیات امنیت، پس از تشخیص نوع حمله، الگوی واکنش به آن حمله‌ی خاص را از پایگاه داده واکشی نموده و آن الگو را به‌صورت گام به گام اجرا می‌کند.

بدیهی است محتوای الگوی واکنش، در این دو حالت متفاوت خواهد بود، زیرا الگوی نوع اول، باید برای انسان (مجری واکنش نیمه‌خودکار)، قابل درک و فهم باشد ولی الگوی نوع دوم، باید برای ماشین (مجری واکنش تمام‌خودکار)، قابل درک و فهم باشد.

مرکز عملیات امنیت، به‌منظور اجرای فعالیت «واکنش به رخدادهای امنیتی»، اقدام به انجام پنج فعالیت می‌نماید. لیست این فعالیت‌ها و زیرفعالیت‌های هر یک از آن‌ها، در جدول (۵-۷)، نمایش داده شده است.

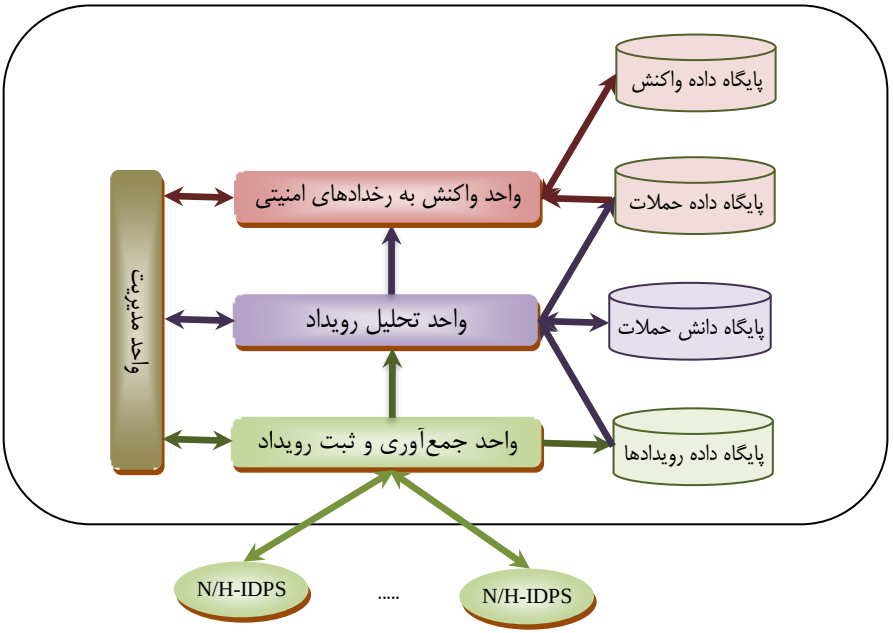
جدول (۵-۷) : زیرفعالیت‌های «واکنش به رخدادهای امنیتی»

فعالیت کلان	فعالیت	عنوان زیرفعالیت	شرح زیرفعالیت
واکنش به رخدادهای امنیتی	صدور هشدار	استخراج ویژگی‌های حمله	واکشی ویژگی‌های حمله اعم از مبدأ، مقصد، شدّت، پیامد، زمان وقوع و مدت حمله سایبری، از پایگاه داده حملات تشخیص داده شده در مرحله تحلیل و تشخیص
		صدور هشدار	تنظیم ویژگی‌های حمله، در قالب هشدار حمله سایبری
		ارسال هشدار	ارسال هشدار برای مخاطبین تعیین‌شده، از طریق کانال‌های ارتباطی تعیین‌شده و بر اساس زمان‌بندی تعیین‌شده
		تعیین نوع و نوبت واکنش	تعیین نوع و نوبت واکنش، بر اساس ویژگی‌های حمله و الگوی پاسخ تعیین شده برای آن حمله، انجام می‌گیرد
	استخراج و اعلام	استخراج الگوی واکنش	واکشی الگوی واکنش تعیین شده برای حمله‌ی تشخیص داده شده، از داخل پایگاه داده حملات سایبری

	الگوی واکنش	صدور فرمان واکنش	تنظیم ویژگی‌های الگوی واکنش، در قالب فرمان واکنش به حمله سایبری
		ارسال فرمان واکنش	ارسال فرمان واکنش به حمله سایبری، از طریق کانال‌های ارتباطی تعیین شده، برای تیم‌های واکنش تعیین شده، اعم از تیم مرکز عملیات امنیت و/یا تیم مقابله با حوادث رایانه‌ای (CERT)
	هماهنگی واکنش نیمه‌خودکار	اخذ مجوز واکنش نیمه‌خودکار	اخذ مجوز واکنش نیمه‌خودکار، از مدیریت مرکز عملیات امنیت
		اخذ الگوی جدید احتمالی	اخذ الگوی جدیدی احتمالی از تیم CERT
		صدور فرمان واکنش جدید احتمالی	تنظیم ویژگی‌های الگوی واکنش جدید احتمالی، در قالب فرمان واکنش به حمله سایبری
		ارسال فرمان واکنش جدید احتمالی	ارسال فرمان واکنش جدید احتمالی به حمله سایبری، از طریق کانال‌های ارتباطی تعیین شده، برای تیم‌های واکنش تعیین شده، اعم از تیم مرکز عملیات امنیت و/یا تیم مقابله با حوادث رایانه‌ای (CERT)
		به‌روز رسانی پایگاه داده واکنش	ثبت اطلاعات واکنش‌های در حال انجام در مقابل حملات تشخیص داده شده
	انجام واکنش خودکار	اخذ مجوز واکنش خودکار	اخذ مجوز واکنش خودکار، از مدیریت مرکز عملیات امنیت
		صدور فرمان واکنش خودکار	تنظیم فرامین مبتنی بر الگوی واکنش، جهت ارسال به تجهیزات شبکه و تجهیزات امنیت شبکه
		ارسال فرمان واکنش خودکار	ارسال فرامین واکنش خودکار، به تجهیزات شبکه و تجهیزات امنیت شبکه
		تحلیل اثربخشی واکنش خودکار	تحلیل اثربخشی واکنش خودکار، از طریق تحلیل بازخورد اقدام و هشدارهای ورودی
	اقدامات پساواکنش	محدودسازی	محدودسازی و ایزوله‌سازی بخش‌ها و خدمات آسیب‌دیده، جهت ریشه‌کنی حمله و بازیابی پیامدها توسط تیم مرکز عملیات امنیت و تیم مقابله با حوادث رایانه‌ای
		مستندسازی واکنش	مستندسازی عملیات واکنش
		تحلیل عملیات واکنش	تحلیل عملیات واکنش و پیشنهاد الگوی واکنش بهبودیافته
		به‌روزرسانی پایگاه داده واکنش	به‌روزرسانی پایگاه داده واکنش، بر اساس الگوی واکنش بهبودیافته

معماری مرکز عملیات امنیت (SOC)

معماری مرکز عملیات امنیت، در شکل (۵-۲) نمایش داده شده است. بر اساس این معماری، مرکز عملیات امنیت، از سه واحد مرکزی با عناوین «جمع‌آوری و ثبت رویداد»، «تحلیل رویداد و تشخیص رخداد امنیتی» و «واکنش به رخداد امنیتی» تشکیل شده است که توسط یک واحد مدیریت، پارامترهای این سه واحد، تنظیم شده و اقدامات مدیریت و نگهداری، روی این واحدها اعمال می‌شود.



شکل (۵-۲) : معماری مرکز عملیات امنیت (SOC)

همچنین در این معماری، سه پایگاه داده و یک پایگاه دانش، پیش‌بینی شده‌اند. پایگاه داده رویدادها، برای ذخیره‌سازی رویدادهای جمع‌آوری شده استفاده می‌شود. رویدادهای این پایگاه داده، توسط واحد جمع‌آوری و ثبت رویداد، بارگذاری شده و توسط واحد تحلیل رویداد، واکشی می‌شوند. پایگاه داده حملات، برای ذخیره‌سازی حملات شناسایی شده استفاده می‌شود. حملات تشخیص داده توسط واحد تحلیل رویداد، در داخل این پایگاه داده ذخیره می‌شوند و توسط واحد واکنش به رخدادهای امنیتی واکشی می‌شوند. پایگاه داده واکنش‌ها نیز برای ذخیره‌سازی الگوی واکنش‌هایی که باید در مواجهه با حملات انجام شوند، مورد استفاده قرار می‌گیرند. الگوهای قرار گرفته در این پایگاه داده، توسط واحد واکنش به رخدادهای امنیتی مورد استفاده قرار می‌گیرد و بر اساس تجارب حاصل از واکنش، توسط همین واحد نیز به‌روز رسانی می‌شوند. تنها پایگاه دانش موجود در این معماری، پایگاه دانش حملات است. این پایگاه دانش، حاوی هستی‌شناسی حملات است که برای تشخیص رخدادهای امنیتی از روی رویدادها، مورد استفاده قرار می‌گیرد.

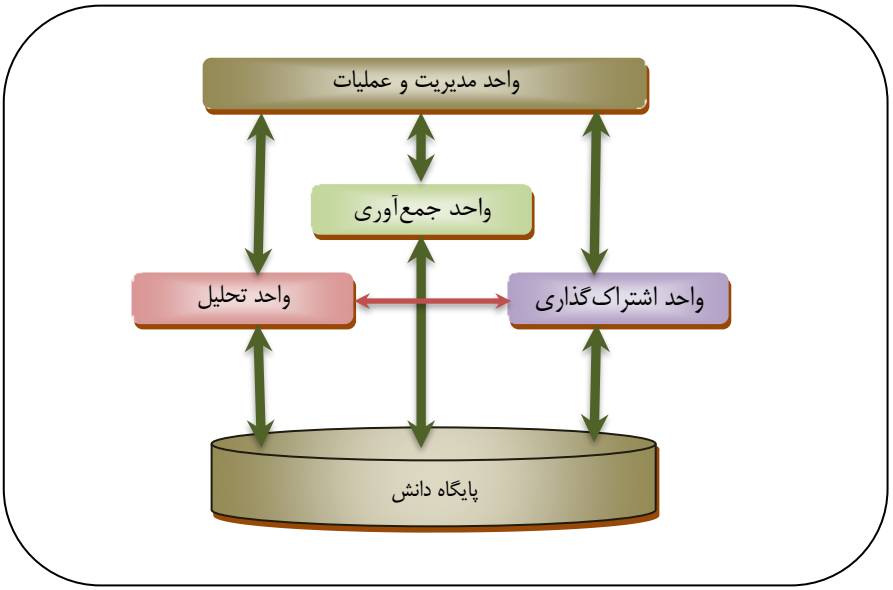
۳-۵-۵. مرکز اشتراک‌گذاری و تحلیل سایبری (ISAC)

قبلاً اشاره نمودیم که به‌منظور تشخیص تهاجم‌های پیچیده بین شبکه‌ای که مراکز عملیات امنیت (SOC) قادر به تشخیص آنها نیستند، از مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC) استفاده می‌شود. فعالیت یک مرکز اشتراک‌گذاری و تحلیل اطلاعات، مبتنی بر دریافت اطلاعات مرتبط با حملات سایبری به‌وقوع پیوسته در چندین شبکه ارتباطی است که توسط مراکز عملیات امنیت این شبکه‌ها، به اشتراک گذاشته شده‌اند. به عبارت دیگر، مراکز عملیات امنیت، پس از دریافت اطلاعات از سامانه‌های تشخیص نفوذ و تحلیل این اطلاعات، علاوه بر تشخیص قطعی برخی حملات سایبری، در مورد برخی خرده‌حملات پیچیده نیز به تشخیص غیرقطعی می‌رسند. اطلاعات مربوط به این حملات، توسط مراکز عملیات امنیت (SOC) متعدد، در یک مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)، به اشتراک گذاشته می‌شود. یکی از نتایج اشتراک‌گذاری این اطلاعات، تجمیع اطلاعات مربوط به حملات سایبری تشخیص داده شده به‌صورت قطعی یا غیرقطعی، در شبکه‌های ارتباطی متعدد است. این امر، امکان انجام تحلیل روی اطلاعات تجمیع شده و در نتیجه تشخیص حملات پیچیده بین‌شبکه‌ای را فراهم می‌آورد.

مدل مفهومی مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)

مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)، محیطی برای اشتراک‌گذاری اطلاعات حملات سایبری توسط چندین مرکز عملیات امنیت (SOC) را فراهم می‌آورد. مرکز اشتراک‌گذاری و تحلیل اطلاعات پس از «جمع‌آوری» اطلاعات حملات از مراکز عملیات امنیت متعدد (اعضای مرکز اشتراک‌گذاری و تحلیل اطلاعات)، اقدام به «اشتراک‌گذاری (تجمیع)» این اطلاعات در یک پایگاه داده نموده و از طریق «تحلیل» اطلاعات تجمیع‌شده، اقدام به «تشخیص» حملات پیچیده بین‌شبکه‌ای می‌نماید. مرکز اشتراگذاری و تحلیل اطلاعات، در پایان، اقدام به «اشتراک‌گذاری» اطلاعات حملات تشخیص داده شده، برای مشترکین خود (مراکز عملیات امنیت) می‌نماید. تمام این فعالیت‌ها با هماهنگی واحد عملیات و مدیریت ISAC انجام می‌شود. معماری مفهومی مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC) در شکل (۵-۳) نمایش داده شده است.

به این ترتیب، مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)، از یک‌سو به چندین مرکز عملیات امنیت (SOC) کمک می‌کند تا حملات پیچیده و غیرقابل تشخیص قطعی در حوزه قلمرو خود را تشخیص قطعی دهند و از سوی دیگر، با در اختیار داشتن اطلاعات تجمیعی حملات قطعی و غیرقطعی تشخیص داده شده توسط مراکز عملیات امنیت متعدد، بر وضعیت وقوع حملات سایبری در تمام این شبکه‌ها، اشراف خواهد یافت.



شکل (۵-۳) : معماری مفهومی مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)

طبقه‌بندی مراکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)

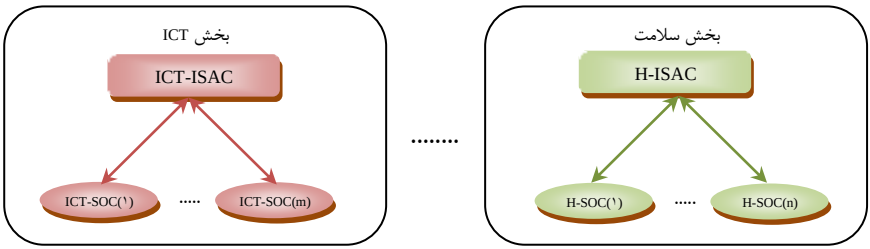
اطلاعات مراکز عملیات امنیت (SOC) هر بخش[۱]، توسط یک مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)، مورد تحلیل و پردازش قرار می‌گیرد. در کشورهای مختلف، یک مرکز اشتراک‌گذاری و تحلیل اطلاعات برای بخش ارتباطات و فناوری اطلاعات[۲] (ICT) ایجاد می‌شود که با عنوان مرکز اشتراک‌گذاری و تحلیل اطلاعات بخش ارتباطات و فناوری اطلاعات (ICT-ISAC) شناخته می‌شود. برای بخش پولی و مالی[۳]، یک مرکز اشتراک‌گذاری و تحلیل اطلاعات بخش مالی (FS-ISAC) و برای بخش سلامت[۴] نیز یک مرکز اشتراک‌گذاری و تحلیل اطلاعات بخش سلامت (H-ISAC) ایجاد می‌شود. ساختار اتصال مراکز عملیات امنیت به مراکز اشتراک‌گذاری و تحلیل اطلاعات، مطابق شکل (۵-۴) است.

بر اساس این ساختار، کلیه مراکز عملیات امنیت متصل به شبکه‌های ارتباطی بخش ICT، به ICT-ISAC متصل می‌شوند تا امکان تشخیص کامل حملات بین‌شبکه‌ای در این بخش فراهم شود. همچنین کلیه مراکز عملیات امنیت در بخش سلامت، به H-ISAC متصل می‌شوند تا حملات بین شبکه‌ای در شبکه‌های حوزه سلامت، فراهم شود. بدیهی

---

۱ Sector
۲ Information & Communication Technology (ICT)
۳ Financial
۴ Health

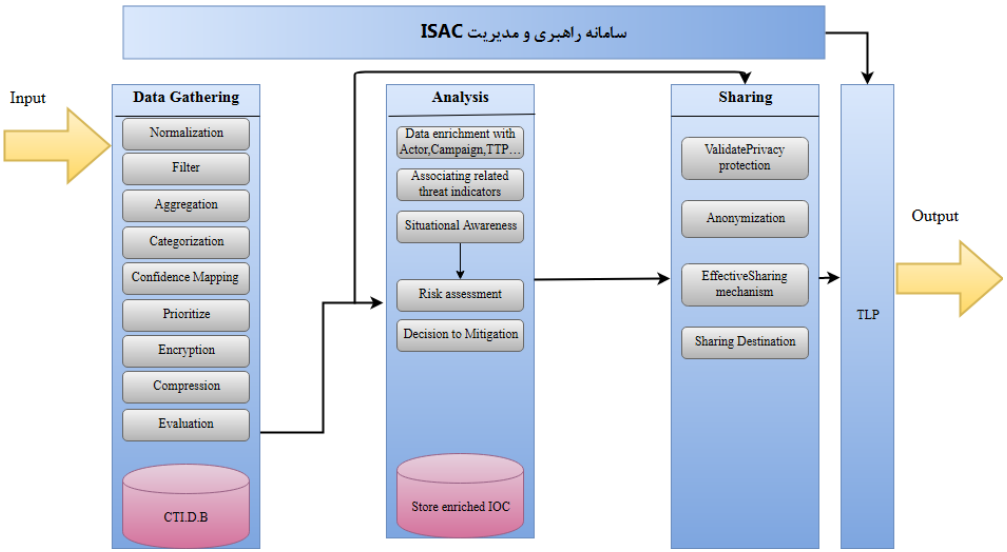
است با این ساختار، باید به تعداد زیرساخت‌های حیاتی کشور، مرکز اشتراک‌گذاری و تحلیل اطلاعات ایجاد شود تا امکان تشخیص حملات سایبری در هر بخش یا هر زیرساخت، فراهم گردد.



شکل (۵-۴) : ساختار اتصال مراکز عملیات امنیت (SOC) به مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)

معماری عملیاتی مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)

بر اساس مدل مفهومی ارائه شده، یک مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)، برای انجام پنج مأموریت خود، شامل چهار واحد کلیدی عملیاتی به همراه پایگاه دانش است. مأموریت‌های این مرکز شامل «جمع‌آوری» اطلاعات حملات از مراکز عملیات امنیت، «اشتراک‌گذاری (تجمیع)» اطلاعات دریافتی، «تحلیل» اطلاعات تجمیع‌شده، «تشخیص» حملات پیچیده بین‌شبکه‌ای و «اشتراک‌گذاری» اطلاعات حملات تشخیص داده شده است. این مأموریت‌ها توسط چهار واحد کلیدی عملیاتی یا زیرسامانه با عناوین «واحد جمع‌آوری و آماده‌سازی اطلاعات»، «واحد تحلیل و پردازش اطلاعات»، «واحد اشتراک‌گذاری و انتشار اطلاعات»، «واحد عملیات و مدیریت» به همراه یک «پایگاه دانش» اجرا می‌شوند. این واحدها، در قالب شکل (۵-۵) نمایش داده شده‌اند.



شکل (۵-۵) : معماری عملیاتی مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)

مرکز اشتراک و تحلیل اطلاعات، شامل زیرسامانه‌های زیر می‌باشد:

۱. زیرسامانه جمع‌آوری و آماده‌سازی اطلاعات

این زیرسامانه، وظیفه دریافت و آماده‌سازی داده‌های ورودی از اعضای مرکز اشتراک‌گذاری و تحلیل اطلاعات را بر عهده دارد. این اطلاعات، توسط مراکز عملیات امنیت اعضاء و بر اساس تکنیک «حالت ساختاریافته اطلاعات تهدید[۱]» (STIX) ارسال می‌شوند. داده‌های ورودی این زیرسامانه، متشکل از سرمایه‌های سایبری قرار گرفته در حوزه قلمرو هر عضو، آسیب‌پذیری‌های مربوط به این سرمایه‌ها، تهدیدهای موجود علیه این سرمایه‌ها ، حملات سایبری بوقوع پیوسته علیه این سرمایه‌ها، حوادث سایبری ناشی از این حملات و خسارت ناشی از این حوادث می‌باشند. اطلاعات حملات، خود شامل اطلاعات تشخیص قطعی برخی و اطلاعات تشخیص غیرقطعی خرده‌حملاتی از حملات پیچیده بین‌شبکه‌ای است.

زیرسامانه جمع‌آوری و آماده‌سازی اطلاعات، پس از «جمع‌آوری» داده‌ها، نسبت به انجام عملیات «نرمال‌سازی»، «فیلترکردن»، «کاهش و حذف داده‌های تکراری»، «دسته‌بندی»، «نگاشت محرمانه»، «اولویت‌دهی»، «رمزگذاری»، «فشرده‌سازی» و «اعتبارسنجی» داده‌ها اقدام می‌نماید. در صورتی که داده‌های ورودی به صورت رمزشده یا به صورت فشرده دریافت شوند، ضروری است که رمزگشایی شده و از حالت فشرده نیز خارج شوند. سپس اطلاعات، ذخیره شده و پس از انجام ارزیابی، برای تصمیم‌گیری در مورد اشتراک یا تحلیل و سپس اشتراک نتایج بدست آمده به زیرسامانه تحلیل و پردازش اطلاعات، ارسال می‌شوند.

[۱] Structured Threat Information eXpression (STIX)

۲. زیرسامانه تحلیل و پردازش اطلاعات

این زیرسامانه، وظیفه پردازش اطلاعات ورودی جهت تشخیص حملات پیچیده بین‌شبکه‌ای را بر عهده دارد. در این واحد، فعالیت‌های «غنی‌سازی داده‌ها»، « همبستگی شاخص‌های مربوط به تهدید»، «آگاهی از وضعیت امنیت»، «ارزیابی مخاطره» و «تصمیم‌گیری برای کاهش مخاطره»، انجام می‌شود. در نتیجه انجام این فعالیت‌ها نیز، کشف حملات توزیع شده ممانعت از سرویس، ایجاد آمادگی برای مواجهه با شرایط اضطراری، سنجش شدت حملات، ارائه توصیه برای اقدامات فوری، استخراج شاخص و روندها و نهایتاً تهیه گزارش‌های راهبردی محقق می‌شوند.

وظیفه این زیرسامانه، تحلیل اطلاعات سرمایه‌ها، آسیب‌پذیری‌ها، تهدیدها و مخاطرات به منظور کمک به اتخاذ تصمیم‌های عملیاتی جهت شناسایی و کاهش مخاطرات، حملات و حوادث ناشی از آنها است. این امر، با بهره‌گیری از اطلاعات موجود در «واحد پایگاه دانش» انجام می‌شود. پس از انجام تحلیل و پردازش‌های لازم، به فراخور موقعیت، «هشدار امنیتی» برای معرفی آسیب‌پذیری، تهدید، مخاطره، حمله یا حادثه امنیتی یا «گزارش تحلیلی» به‌منظور آسیب–شناسی حملات و رخدادها و تحلیل عملکرد و روشهای مقابله با آنها تولید می‌شود و به زیرسامانه «اشتراک و انتشار اطلاعات» ارسال می‌شود.

۳. زیرسامانه اشتراک‌گذاری اطلاعات

این زیرسامانه، وظیفه اشتراک‌گذاری اطلاعات حملات سایبری با اعضای مرکز اشتراک‌گذاری و تحلیل اطلاعات را بر عهده دارد. زیرسامانه اشتراک‌گذاری، ابتدا اطلاعات دریافت شده از واحد تحلیل و پردازش اطلاعات را به منظور طبقه‌بندی و تعیین حساسیت و دامنه انتشار اطلاعات، مورد بررسی قرار می‌دهد تا «مخاطبان اشتراک‌گذاری» نتیجه تحلیل و نوع دسترسی آنها، «سطح گمنام‌سازی اطلاعات» و «مکانیزم مؤثر اشتراک‌گذاری» را تعیین نماید. کلیه خروجی‌های زیرسامانه تحلیل و پردازش اطلاعات، اعم از حملات تشخیص داده شده، توصیه‌های رفع تهدید، بهترین اقدام‌ها و رویه‌ها، هشدارهای امنیتی، روش پیشنهادی برای پیکربندی امن، گزارش‌های تحلیلی و نظایر آنها، توسط این زیرسامانه، با اعضاء به اشتراک گذاشته می‌شوند.

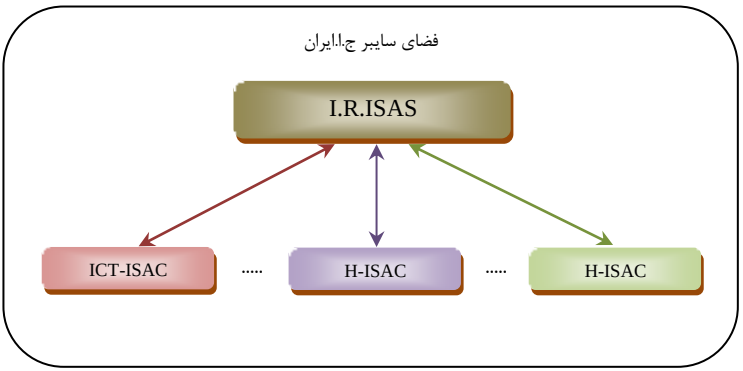
٤. زیرسامانه عملیات و مدیریت

این زیرسامانه، وظیفه تصمیم‌گیری و تصمیم‌سازی در شرایط بحران را بر عهده دارد. از زمان ایجاد مرکز اشتراک‌گذاری و تحلیل اطلاعات، زیرسامانه عملیات و مدیریت، کل فرآیند «اشتراک‌گذاری و تحلیل» انواع اطلاعات، شامل سرمایه‌ها، آسیب‌پذیری‌ها، تهدیدها، حملات و حوادث امنیتی، «سیاست‌گذاری» جهت عضوگیری، «اجرا و تغییر قوانین و مقررات»، «سازوکار تعیین نماینده مرکز»، «برگزاری کنفرانس‌ها و مجامع اطلاع‌رسانی» و «ایجاد هماهنگی با اعضا و مشترکین» و «تصمیم‌سازی در مواقع بحران»، «درخواست و تشکیل جلسه» با اعضا و شرکای موثر را هدایت و مدیریت می‌نماید.

٤-٥-٥. سامانه اشتراک‌گذاری و هشدار سایبری (ISAS)

ساختار اتصال مراکز عملیات امنیت به مراکز اشتراک‌گذاری و تحلیل اطلاعات، نمایانگر این واقعیت است که یک مرکز اشتراک‌گذاری و تحلیل بخش سلامت، امکان تشخیص حملات سایبری پیچیده بین‌بخشی یا چندبخشی که مثلاً دو بخش ICT و سلامت را درگیر نموده باشد، نخواهد داشت. زیرا بخشی از اطلاعات این حمله توسط مراکز عملیات امنیت بخش ICT و بخش دیگر، توسط مراکز عملیات امنیت بخش سلامت تشخیص داده شده است. این نوع حملات، تنها در صورتی قابل تشخیص خواهند بود که اطلاعات بخش ICT و بخش سلامت، تجمیع و تحلیل شوند.

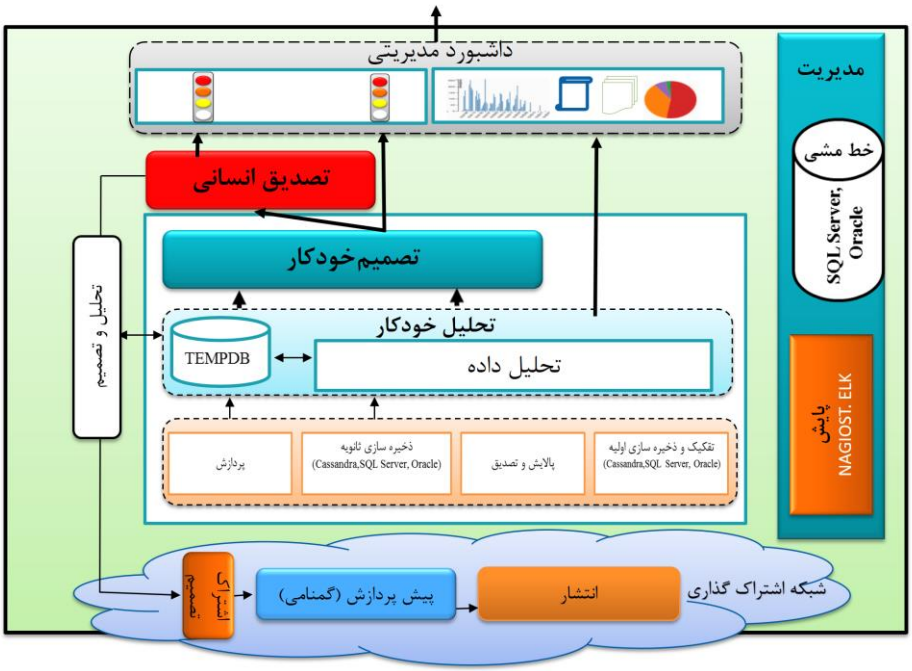
سامانه اشتراک‌گذاری و هشدار سایبری (ISAS)، برای حل این مسئله مورد استفاده قرار می‌گیرد. این سامانه، در ساختاری مطابق شکل (۵-۶)، فضا را برای اشتراک‌گذاری اطلاعات ICT-ISAC، F-ISAC، H-ISAC و ISACهای سایر زیرساخت‌های حیاتی کشور، فراهم می‌آورد.



شکل (۵-۶) : ساختار اتصال مراکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC) به سامانه اشتراک‌گذاری اطلاعات و هشدار (ISAS)

سامانه اشتراک‌گذاری اطلاعات و هشدار (ISAS) نیز مانند مرکز اشتراک‌گذاری و تحلیل اطلاعات، دو مأموریت اصلی دارد. مأموریت اول این سامانه، کمک به مراکز اشتراک‌گذاری و تحلیل اطلاعات، برای تشخیص قطعی و مواجهه با حملات پیچیده بین‌بخشی است. مأموریت دوم سامانه اشتراک‌گذاری اطلاعات و هشدار نیز اشراف بر وضعیت سرمایه‌های سایبری، آسیب‌پذیری‌ها، تهدیدها، حملات و حوادث سایبری بوقوع پیوسته یا در شرف وقوع در کل فضای سایبر ج.ا.ایران است. نتیجه اشراف بر فضای سایبر کشور، در قالب تعیین وضعیت سایبری کشور ظهور و بُروز می‌یابد. وضعیت سایبری کشور، مانند وضعیت فیزیکی، حاوی چهار وضعیت سفید، زرد، نارنجی و قرمز است.

ساختار معماری سامانه اشتراک‌گذاری اطلاعات و هشدار (ISAS)، در شکل (۵-۷) نمایش داده شده است. بر اساس این ساختار، این سامانه از پنج واحد عملیاتی با عناوین «واحد جمع‌آوری، اشتراک‌گذاری و انتشار اطلاعات»، «واحد تحلیل و پردازش اطلاعات و تصمیم‌گیری خودکار»، «واحد ارزیابی و تصدیق انسانی»، «واحد مدیریت» و «واحد بصری‌سازی و داشبورد» به همراه «پایگاه دانش» تشکیل شده است.



شکل (۵-۷) : ساختار معماری سامانه اشتراک‌گذاری اطلاعات و هشدار (ISAS)

سامانه اشتراک و تحلیل اطلاعات، شامل زیرسامانه‌های زیر می‌باشد:

۱. زیرسامانه جمع‌آوری، اشتراک‌گذاری و انتشار اطلاعات

این زیرسامانه، وظیفه دریافت داده‌های ورودی از مراکز اشتراک‌گذاری و تحلیل اطلاعات متصل به سامانه، پیش‌پردازش و به‌ویژه گمنام‌سازی اطلاعات دریافتی، انتشار (اشتراک‌گذاری) اطلاعات دریافتی از هر مرکز اشتراک‌گذاری و تحلیل اطلاعات، در بین کلیه مراکز متصل و نهایتاً اشتراک‌گذاری تصمیم اتخاذ شده توسط واحد تحلیل و پردازش و تصدیق‌شده توسط واحد ارزیابی تصدیق و تصدیق، را بر عهده دارد. داده‌های ورودی این زیرسامانه، متشکل از سرمایه‌های سایبری قرار گرفته در حوزه قلمرو هر ISAC متصل، آسیب‌پذیری‌های مربوط به این سرمایه‌ها، تهدیدهای موجود علیه این سرمایه‌ها، حملات سایبری بوقوع پیوسته علیه این سرمایه‌ها، حوادث سایبری ناشی از این حملات و خسارت ناشی از این حوادث می‌باشند.

این زیرسامانه، به منظور اشتراک‌گذاری اطلاعات تصمیم‌های حاصل شده در واحد تحلیل، پردازش و تصمیم، ابتدا اطلاعات دریافت شده را به منظور طبقه‌بندی و تعیین حساسیت و دامنه انتشار اطلاعات، مورد بررسی قرار می‌دهد تا «مخاطبان اشتراک‌گذاری» نتیجه تحلیل و نوع دسترسی آنها، «سطح گمنام‌سازی اطلاعات» و «مکانیزم مؤثر اشتراک‌گذاری» را تعیین نماید.

۲. زیرسامانه تحلیل و پردازش اطلاعات و تصمیم‌گیری خودکار

این زیرسامانه، وظیفه پردازش اطلاعات ورودی جهت تشخیص حملات پیچیده بین‌بخشی را بر عهده دارد. در این واحد، فعالیت‌های تفکیک و ذخیره‌سازی اولیه، پالایش و ذخیره‌سازی ثانویه، پردازش و تحلیل داده‌ها، تشخیص حملات پیچیده بین‌بخشی و اتخاذ تصمیم خودکار در خصوص نحوه مواجهه با آن انجام می‌شود. نتیجه این تصمیم، برای تصدیق در اختیار واحد ارزیابی و تصدیق قرار می‌گیرد.

وظیفه این زیرسامانه، تحلیل اطلاعات سرمایه‌ها، آسیب‌پذیری‌ها، تهدیدها، مخاطرات، حملات، حوادث و خسارات، به منظور کمک به اتخاذ تصمیم‌های عملیاتی جهت شناسایی و کاهش مخاطرات، حملات و حوادث ناشی از آنها است. این امر، با بهره‌گیری از اطلاعات موجود در «پایگاه دانش» انجام می‌شود. پس از انجام تحلیل و پردازش‌های لازم، به فراخور موقعیت، «هشدار امنیتی» برای معرفی آسیب‌پذیری، تهدید، مخاطره، حمله یا حادثه امنیتی یا «گزارش تحلیلی» به‌منظور آسیب‌شناسی حملات و رخدادها و تحلیل عملکرد و روشهای مقابله با آنها تولید می‌شود و به زیرسامانه «جمع‌آوری، اشتراک‌گذاری و انتشار اطلاعات» ارسال می‌شود. همچنین بر اساس اطلاعات سرمایه‌ها، آسیب‌پذیری‌ها، تهدیدها، مخاطرات، حملات، حوادث و خسارات، این زیرسامانه اقدام به «تعیین وضعیت سایبری کشور» به عنوان خروجی ویژه می‌نماید.

۳. زیرسامانه ارزیابی و تصدیق

این زیرسامانه، وظیفه ارزیابی و تصدیق تصمیم اتخاذ شده توسط واحد «تحلیل و پردازش اطلاعات و تصمیم‌گیری خودکار» را بر عهده دارد. داده‌های ورودی این زیرسامانه، علاوه بر سرمایه‌های سایبری، آسیب‌پذیری‌های مربوط به این سرمایه‌ها، تهدیدهای موجود علیه این سرمایه‌ها، مخاطرات سایبری موجود علیه این سرمایه‌ها، حملات سایبری بوقوع پیوسته علیه این سرمایه‌ها، حوادث ناشی از این حملات و خسارات ناشی از این حوادث، حاوی وضعیت سایبری کشور میز می‌باشد. ارزیابی و تصدیق وضعیت سایبری کشور، از حساسیت بسیار بالایی برخوردار است. برای نمونه، تعیین وضعیت قرمز سایبری، به معنای ورود به جنگ سایبری است. لذا لازم است ارزیابی و تصدیق وضعیت سایبری کشور، با حساسیت و بر اساس اصول قانون اساسی و قوانین موضوعه ج.ا.ایران صورت پذیرد.

٤. زیرسامانه مدیریت

این زیرسامانه، وظیفه تعیین و اعمال خط‌مشی‌ها و پایش مداوم عملکرد کلیه واحدهای عملیاتی را بر عهده دارد.

۵. زیرسامانه بصری‌سازی و داشبورد

این زیرسامانه، وظیفه بصری‌سازی آخرین وضعیت سرمایه‌های سایبری، آسیب‌پذیری‌ها، تهدیدها، مخاطرات، حملات، حوادث و خسارات به همراه وضعیت سایبری کشور و نمایش این اطلاعات، روی داشبورد مدیریتی سامانه را بر عهده دارد. وضعیت سایبری کشور، در چهار حالت سفید، زرد، نارنجی و قرمز سایبری نمایش داده می‌شود.

۶-۵- توصیه‌های ضروری

به‌منظور تشخیص به‌موقع و مقابله‌ی مؤثر با حملات سایبری، لازم است :

۱. انواع سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه (HIDS، HIPS، NIDS یا NIPS)، یا انواع خاص‌منظوره‌ی آنها نظیر سامانه دیوار آتش خاص کاربردهای وب (WAF) را در شبکه سازمان، مورد استفاده قرار دهید. هر سازمان، نیازمند بهره‌گیری از چندین سامانه از این نوع است. تعداد این سامانه‌ها، بستگی به معماری شبکه سازمان و تعداد نواحی امن ایجاد شده در شبکه سازمان دارد.

۲. یک مرکز عملیات امنیت (SOC)، به‌منظور تشخیص حملات سایبری طولانی‌مدت، گسترده، چندمرحله‌ای یا چندمسیره علیه سرمایه‌های سایبری سازمان خود، ایجاد کنید.

۳. از آن‌جا که یک مرکز عملیات امنیت، علاوه بر سامانه SOC، نیازمند بهره‌گیری از یک تیم تخصصی نیز می‌باشد، لذا به‌منظور ایجاد مرکز عملیات امنیت سازمان، لازم است توان تخصصی موردنیاز برای ایجاد این مرکز را نیز ایجاد نموده و یا به خدمت بگیرید.

۴. در صورت عدم وجود توان تخصصی موردنیاز برای ایجاد مرکز عملیات امنیت سازمانی و عدم امکان به‌خدمت گرفتن توان تخصصی موردنیاز، بهتر است از خدمات عملیات امنیت عرضه‌شده توسط تأمین‌کنندگان خدمات امنیتی مدیریت‌شده[۱] (MSSP) برای سازمان خود، استفاده نمائید. در این حالت، لازم است سامانه‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات مبتنی بر میزبان یا مبتنی بر شبکه (HIDS، HIPS، NIDS یا NIPS) نصب‌شده در شبکه سازمان خود را از راه دور، به MSSP موردنظر متصل نمائید تا رویدادهای شناسایی شده در شبکه سازمان را برای آن ارسال نمایند و MSSP اقدام به تشخیص و انجام واکنش در مواجهه با حملات سایبری انجام شده علیه سرمایه‌های سایبری سازمان شما کند.

۵. مرکز عملیات امنیت (SOC) سازمان خود را به مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC) بخش متصل کنید و از طریق به‌اشتراک‌گذاری اطلاعات حملات تشخیص داده شده توسط مرکز عملیات امنیت سازمان، به تشخیص حملات پیچیده بین‌شبکه‌ای کمک نموده و موجبات اشراف مرکز اشتراک‌گذاری و تحلیل اطلاعات مذکور بر وضعیت حملات سایبری بخش را فراهم آورید.

۶. در صورت استفاده از خدمات عملیات امنیت عرضه‌شده توسط تأمین‌کنندگان خدمات امنیتی مدیریت‌شده (MSSP) برای سازمان خود، حملات تشخیص داده شده و سایر اطلاعات موردنیاز برای مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC) بخش را تأمین کنید تا ضمن کمک به تشخیص حملات پیچیده بین‌شبکه‌ای، موجبات اشراف مرکز اشتراک‌گذاری و تحلیل اطلاعات مذکور بر وضعیت حملات سایبری بخش را فراهم آورید.

---

[۱] Managed Security Service Provider (MSSP)

فصل ششم

آمادگی دفاع سایبری

اهداف آموزشی پیش‌بینی شده برای این فصل، عبارتند از :

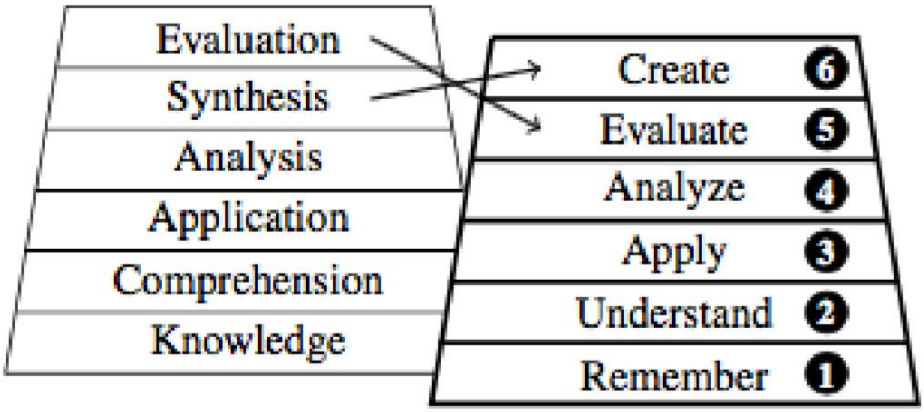
۱. کسب شناخت و توانایی تفکیک ارکان آمادگی دفاعی
۲. کسب شناخت در خصوص انواع تمرین و آزمون سایبری
۳. کسب شناخت در خصوص انواع مانور سایبری
٤. کسب شناخت در خصوص انواع شبیه‌سازهای پدافند سایبری

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

۱. مراحل تعالی قابلیت‌های پدافند سایبری
۲. ارکان تأمین آمادگی پدافند سایبری
۳. انواع و ویژگی‌های تمرین سایبری
٤. نمونه‌هایی از تمرین‌های سایبری یگان‌های دفاع سایبری کشورها
٥. انواع و ویژگی‌های آزمون سایبری
٦. نمونه‌هایی از آزمون‌های سایبری یگان‌های دفاع سایبری کشورها
۷. انواع و ویژگی‌های مانور سایبری
۸. نمونه‌هایی از مانورهای سایبری یگان‌های دفاع سایبری کشورها
۹. انواع و ویژگی‌های شبیه‌سازهای پدافند سایبری
۱۰. نمونه‌هایی از شبیه‌سازهای مورد استفاده توسط یگان‌های دفاع سایبری کشورها

۱-۶- تمرین و آزمون سایبری

طبقه‌بندی بلوم، طبقه‌بندی سطوح مختلف اهداف یادگیری شناختی است که مربیان برای دانش‌آموزان تعیین می‌کنند. این اهداف یادگیری شش سطح پیشرفته یادگیری را مشخص می‌کند. این طبقه‌بندی، مطابق آن‌چه در سمت چپ شکل (۶-۱) نمایش داده شده است، حاوی دانش، درک، کاربرد، تحلیل، ترکیب و ارزیابی است. اندرسون و همکاران، کار بلوم را بازبینی کرده‌اند و مطابق آن‌چه در سمت راست شکل (۶-۱) نشان داده شده است، طبقه‌بندی اهداف یادگیری را شامل یادآوری، فهمیدن، درخواست‌دادن، تحلیل، ارزیابی و ترکیب دانسته‌اند.



شکل (۶-۱) : اهداف آموزشی بلوم (سمت چپ) و اهداف آموزشی اندرسون (سمت راست)

در نظام پدافند سایبری کشور، بر اساس مدل‌های فوق، برای آموزش‌های عرضی پدافند سایبری، اهداف پنج‌گانه با عناوین «آگاهی یا شناخت»، «درک و فهم»، «کاربرد»، «تجزیه و تحلیل (حل مسئله)»، و «ترکیب و ارزیابی» تعیین شده است.

جدول (۶-۱) : اهداف دوره‌های آموزش کوتاه‌مدت و عرضی پدافند سایبری

سطح تعالی / اهداف	سطح (۱)	سطح (۲)	سطح (۳)	سطح (٤)	سطح (٥)
حیطه‌ی شناختی	آگاهی (شناخت)	درک/فهمیدن	کاربرد	تجزیه و تحلیل (حل مسئله)	ترکیب و ارزشیابی
حیطه‌ی عاطفی	دریافت (توجه)	واکنش (پاسخ)	ارزش‌گذاری	سازمان‌دهی	تبلور درونی (سازمان‌یافته در شخصیت)
حیطه‌ی	تقلید و آمادگی	اجرای مستقل	سرعت و دقت	هماهنگی	عادی‌شدن

روانی–حرکتی					
جمع‌بندی اهداف	آگاهی/شناخت و توجّه مقلّدانه	درک/فهم و واکنش مستقل	کاربرد و ارزش‌گذاری سریع و دقیق	حل‌مسئله به‌صورت سازماندهی‌شده و هماهنگ	هدایت متفکرانه، مبتنی بر تبلور درونی و رفتار عادی

واحدهای پدافند سایبری، به منظور کسب موفقیّت در دفاع از سرمایه‌های سایبری، باید مطابق شکل (۶–۲)، ابتدا قابلیت‌های بالقوّه‌ی خود را به توانایی تبدیل نمایند. مؤثرترین توانمندسازها برای این منظور، دوره‌های آموزشی تخصصی و مهارتی هستند.

گام بعد، تبدیل توانایی واحدهای پدافند سایبری به آمادگی است. آمادگی پدافند سایبری، به معنای آمادگی مواجهه با هرگونه حمله‌ی سایبری است. تمرین سایبری، مناسب‌ترین و مؤثرترین روش برای تبدیل توانایی به آمادگی محسوب می‌شود.

شکل (۶–۲) : مراحل تعالی قابلیت‌های پدافند سایبری

از دیگر ویژگی‌های تمرین سایبری آن است که معمولاً در محیط آزمایشگاهی و در قالب فعالیت‌های محدود انفرادی یا تیم‌های کوچک چندنفره انجام می‌شود و زمان انجام آن نیز کوتاه و در حد چند دقیقه تا چند ساعت است.

پس از کسب آمادگی پدافند سایبری، متخصصین پدافند سایبری، وارد گام بعدی تعالی خود می‌شوند. در این گام، باید آمادگی انجام عملیات پدافند سایبری آن‌ها، به کارآمدی تبدیل شود. به این معنا که در خاتمه‌ی این گام، قادر باشند تمام مأموریت‌های پدافند سایبری را به درستی، با اقدام هماهنگ در قالب یک تیم پدافند سایبری، به انجام رسانند. مؤثرترین روش برای تبدیل آمادگی به کارآمدی و اطمینان از اقدام هماهنگ و کارآمد تیم‌های پدافند سایبری، آزمون سایبری است. آزمون سایبری، در محیط آزمایشگاهی یا شبیه‌سازی شده انجام می‌شود که در آن، چند تیم یک یا چند نفره، اقدام به انجام مأموریت‌های پدافند سایبری به صورت دفاعی یا ترکیبی از تهاجمی–دفاعی می‌نمایند.

پس از طی این مراحل، واحد پدافند سایبری، نیازمند تبدیل ویژگی کارآمدی خود، به اثربخشی است. اثربخشی در عملیات پدافند سایبری، به معنای انجام عملیات پدافندی درست یا موفق است. به عبارت دیگر، اثربخشی قابلیت‌های یک واحد پدافند سایبری، تضمین کننده‌ی موفقیّت عملیات دفاعی آن واحد در مقابل هر گونه تهاجم سایبری است. مؤثرترین روش برای تبدیل کارآمدی به اثربخشی، مانور است. مانور سایبری، همانند یک عملیات سایبری واقعی، در محیطی تقریباً واقعی و در ابعاد گسترده انجام می‌شود. واحدهای مختلف آفند و پدافند سایبری، طی چند روز تا چند هفته،

در مقابل یکدیگر صف‌آرایی نموده و با استفاده از سلاح‌های آفندی و پدافندی، سعی در تهاجم و دفاع خواهند نمود. مانور سایبری، ممکن است با مشارکت یگان‌های مختلف آفندی و یگان‌های مختلف پدافندی، انجام گیرد که در این صورت، امکان اجرای عملیات مشترک سایبری نیز فراهم خواهد بود.

در سال ۲۰۰۱، برای اولین مرتبه، آکادمی خدمات نظامی ایالات متحده، آزمون دفاع سایبری[۱] (CDX) را معرفی کرد. این آزمون با هدف انجام رقابت بین آکادمی‌های نظامی، پیش‌بینی شد که در آن، تیم‌های دفاع سایبری، اقدام به طراحی و پیاده‌سازی عملیات سایبری علیه یک شبکه کامپیوتری و همچنین دفاع از این شبکه در مقابل عملیات سایبری انجام شده می‌نمودند. نخستین مسابقه دفاع سایبری دانشگاهی[۲] (CCDC) توسط مرکز تضمین زیرساخت و امنیت در دانشگاه تگزاس در آوریل ۲۰۰۵ میزبانی شد.

آزمون‌های تسخیر پرچم[۳] (CTF) یا به صورت محلی در محیطی کوچک، از قبیل دبیرستان یا دانشگاه و یا به‌صورت سراسری در یک کشور و یا به عنوان یک شایستگی چند ملیتی، به‌صورت سالیانه اجرا می‌شوند.

تمرینات شبیه سازی نیز برای شبیه‌سازی سرعت و پیچیدگی نقض امنیت سایبری طراحی می‌شوند و شامل حملات شبیه‌سازی شده سایبری می‌باشند و در حال حاضر، شبیه‌سازی در قالب یک محیط شبیه‌سازی خودکار انجام می‌گیرد که در آن، سناریوها و شبکه‌ها به آسانی قابل تغییر هستند. CyberCiege، Arena، Tracer FIRE و RangeForce، نمونه‌هایی از ابزارهای اختصاصی یا آموزشی تهیه شده برای این حوزه می‌باشند.

۲-۶- نمونه‌های تمرین، آزمون و مانور سایبری

فرماندهی سایبری ایالات متحده آمریکا، به صورت سالیانه، اقدام به برگزاری دو تمرین سایبری با عناوین پرچم سایبری[۴] و حفاظ سایبری[۵] می‌نماید. تمرین‌های پرچم سایبری و حفاظ سایبری، تمرین‌های پرچم‌دارِ فرماندهی سایبری آمریکا محسوب می‌شوند. علاوه بر این دو تمرین، واحدهای فرماندهی سایبری ایالات متحده آمریکا، به صورت منظّم، با مشارکت آژانس‌های دولتی سطح یک این کشور، در بیش از ۱۲ عنوان تمرین و مانور سایبری، شرکت می‌کنند.

برخی از این تمرین‌ها و مانورها، بر اساس اعلام نیازمندی‌های تمرینی فرماندهی‌های رزمی سایبری به آژانس امنیت ملی و برخی دیگر، بر اساس برنامه‌ریزی آژانس امنیت ملی به عنوان متولی آموزش و تمرین یگان‌های دفاع سایبری، تعیین، برنامه‌ریزی و برگزار می‌شوند.

---

۱ Cyber Defense Exercise (CDX)

۲ Collegiate Cyber Defense Competition (CCDC)

۳ Capture the Flag (CTF)

۴ Cyber Flag

۵ Cyber Guard

تمرین‌های سایبری پرچم سایبری[۱]، ائتلاف سایبری[۲] و توفان سایبری[۳]، با محوریّت آژانس امنیت ملی آمریکا برگزار می‌شوند. تمرین توفان سایبری، بخشی از نظام امنیت سایبری آمریکا محسوب می‌شود و برگزاری آن به صورت مشترک، توسط آژانس امنیت ملی (NSA) و وزارت امنیت داخلی (DHS) انجام می‌گیرد.

۳-٦- آشنایی با آزمون طوفان سایبری آمریکا

تمرین توفان سایبری که با شماره‌های (۱) تا (۶) در سال‌های ۲۰۰۶، ۲۰۰۸، ۲۰۱۰، ۲۰۱۲، ۲۰۱۶ و ۲۰۱۸ برگزار شده است، یک تمرین امنیت سایبری در سطح ملی است که متولی برگزاری آن، بخش امنیت سایبری در وزارت امنیت داخلی است و با مشارکت آژانس امنیت ملی برگزاری می‌شود. به عنوان نمونه، در تمرین توفان سایبری (۳) که از ۲۷ سپتامبر تا ۱ اکتبر ۲۰۱۰ برگزار شد، ۸ وزارت‌خانه شامل امنیت داخلی، دفاع، کشور، تجارت، انرژی، بهداشت، حمل‌ونقل و دادگستری، به همراه ۱۳ ایالت، ۱۲ شریک خارجی و تقریباً ۶۰ شرکت خصوصی مشارکت داشتند.

در تمرین توفان سایبری، تیم طراح، سناریوی تمرین را تعیین می‌کند و بازیگران شرکت‌کننده در تمرین، از سرمایه‌های سایبری در مقابل حملات سایبری شبیه‌سازی شده بر اساس این سناریو، دفاع می‌کنند.

٤-٦- آشنایی با آزمون پرچم سایبری آمریکا

مسابقه یا آزمون پرچم سایبری، یک آزمون نظامی است. از سال ۱۹۷۰ در ایالات متحده آمریکا، یک آزمون سالیانه‌ی نظامی با عنوان پرچم قرمز برگزار می‌شود. در سال ۲۰۰۸ انستیتو فناوری نیروی هوایی آمریکا، در قالب طرحی، برگزاری آزمون پرچم سایبری را پیشنهاد نمود و از سال ۲۰۱۱، این آزمون به صورت سالیانه برگزار می‌شود. آزمون پرچم سایبری، یک آزمون تاکتیکی است. در این آزمون که توسط فرماندهی سایبری و در محل نیروی هوایی در نِوادا برگزار می‌شود، تیم‌های تشکیل شده از تمامی واحدهای سایبری ارتش آمریکا، شامل فرماندهی سایبری، نیروی زمینی، نیروی هوایی، ناوگان دریایی و تفنگداران، شرکت نموده و طیف کاملی از عملیات‌های سایبری دفاعی و تهاجمی را اجرا می‌کنند. در این آزمون، علاوه بر حضور آژانس‌های مختلف سایبری آمریکا، هم‌پیمانان بین‌المللی این کشور نیز مشارکت می‌نمایند.

برای نمونه، در سومین آزمون سالیانه‌ی پرچم سایبری که از ۲۹ اکتبر تا ۸ نوامبر ۲۰۱۳ برگزار شد، ۷۰۰ نفر شرکت‌کننده حضور داشتند که در مقابل ۳۰۰ شرکت‌کننده در آزمون سال ۲۰۱۲، موجب شد تا از شبکه‌ای با ابعاد دو برابر در این مسابقه استفاده شود. در این مسابقه، نفرات شرکت‌کننده، در قالب تیم‌های مدافع و مهاجم سایبری، دسته‌بندی شده و در مسابقه شرکت می‌نمایند. در این آزمون، مانورهای سنّتی و آتش‌های جنبشی نیز در کنار عملیات سایبری، مواجهه با یک تجاوز خصمانه‌ی واقعی را تداعی می‌کند.

---

۱ Cyber Flag

۲ Cyber Coalition

۳ Cyber Storm IV

۶-۵- آشنایی با آزمون حفاظ سایبری آمریکا

حفاظ سایبری، یک آزمون سطح تاکتیکی است که با مشارکت فرماندهی سایبری آمریکا، آژانس امنیت ملّی، گارد ملّی، وزارت امنیت داخلی و پلیس فدرال (FBI) ، در محیط مجازی[۱] و در یک محدوده‌ی سایبریِ بسته، برگزار می‌شود. در این آزمون، دفاع ملّی در مقابل عملیات‌های سایبری علیه زیرساخت‌های حیاتی آمریکا، انجام می‌گیرد. هدف اصلی این آزمون، ارتقاء همکاری و آگاهی‌رسانی شغلی و افزایش قابلیت‌های سایبری وزارت دفاع و آژانس امنیت ملّی برای پشتیبانی بهتر از وزارت امنیت داخلی و پلیس فدرال، در تأمین "دفاع از سرزمین" است. مدت برگزاری این آزمون، یک هفته است. در آزمون حفاظ سایبری سال ۲۰۱۲، تعداد ۵۰۰ شرکت‌کننده از فرماندهی سایبری، یگان‌های عملیاتی دفاع سایبری (از نیروهای نظامی) و گارد ملّی حضور داشتند که ۱۰۰ شرکت‌کننده از گارد ملّی بودند. در این تمرین، محیطی تأمین می‌شود تا چندین حوادث سایبری بتوانند بر روی امکانات و موقعیت‌های مختلف، ایجاد شوند. در این تمرین، گارد ملّی یک نقش حیاتی را در دفاع سایبری از کشور، بازی‌نمود و واحدهای گارد ملّی از ۱۲ ایالت، مسئولیت دفاع از حملات سایبریِ انجام‌شده علیه زیرساخت‌های حیاتی آمریکا، از قبیل زیرساخت آب، خطوط گاز و شبکه برق را بر عهده داشتند.

آزمون حفاظ سایبری، برای دفاع در سطوح ایالتی و ملّی، در مقابل حملات سایبری است که علیه زیرساخت‌های حیاتی آمریکا انجام می‌شوند. علاوه بر فرماندهی سایبری ایالات متحده آمریکا، آژانس امنیت ملّی، وزارت امنیت داخلی و پلیس فدرال، مراکز اشتراک و تحلیل اطلاعات[۲] زیرساخت‌های حیاتی نیز مشارکت فعال دارند. این مشارکت کنندگان، عناصر نظام امنیت فضای سایبر می‌باشند که تحت مدیریت وزارت امنیت داخلی عمل می‌کنند. فرماندهی سایبری آمریکا، همچنین ابزارهای دفاع و تهاجم سایبری را توسعه داده است که مستقیماً از قابلیت بهره‌گیری توسط یگان‌های دفاع سنّتی (غیرسایبری) در عملیات‌های جنبشی، برخوردار می‌باشند.

۶-۶- آشنایی با سایر آزمون‌های یگان دفاع سایبری آمریکا

برخی آزمون‌های منظم دفاع سایبری که توسط یگان‌های مختلف دفاع سایبری ایالات متحده آمریکا اجرا می‌شوند، عبارتند از :

آزمون تصویر عملکرد مشترک[۳] (COP)

آزمون سطح ملّی با عنوان آزمون تصویر عملکرد مشترک (COP) توسط کاخ سفید و با مشارکت مرکز عملیات‌های مشترک فرماندهی سایبری، مرکز عملیات‌های تهدید NSA/CSS و مرکز جرایم سایبری وزارت دفاع ایالات متحده

---

۱ Virtual Environment

۲ Information Sharing and Analysis Center (ISAC)

۳ Common Operating Picture (COP) Exercise

آمریکا برگزار می‌شود. هدف از برگزاری این آزمون، تست توانایی دولت فدرال، برای توسعه‌ی یک مواجهه‌ی متناسب با تصویر عملکرد مشترک، برای دستگاه‌های تابعه‌ی کاخ سفید است.

آزمون آموزش میدان[۱] (FTX)

آزمون آموزش میدان (FTX) به صورت سالیانه توسط فرماندهی راهبردی ایالات متحده[۲] و با پشتیبانی فنی مرکز عملیات‌های مشترک[۳] (JOC) فرماندهی سایبری این کشور، برگزار می‌شود. هدایت، تنظیم مجدد، تحلیل، گزارش‌دهی و پاسخ به وقایع ناشی از این آزمون، بر عهده‌ی مرکز عملیات‌های مشترک فرماندهی سایبری است.

آزمون وزارت دفاع

این آزمون برای تشخیص آمادگی فرماندهان ارشد وزارت دفاع برای مواجهه با یک حمله‌ی گسترده‌ی سایبری به شبکه‌های حیاتی آمریکا، برگزار می‌شود. بر این اساس، پشتیبانی فنی برگزاری این آزمون، توسط فرماندهی سایبری آمریکا انجام می‌گیرد.

آزمون دفاع سایبری[۴] (CDX)

آزمون دفاع سایبری با حمایت آژانس امنیت ملّی آمریکا و توسط مرکز تحقیقات فضای سایبرِ آکادمی نیروی هوایی ارتش آمریکا برگزار می‌شود. تیم‌های شرکت‌کننده در این آزمون، تلاش می‌کنند تا شبکه‌های کامپیوتری امن، با قابلیت ارائه انواع سرویس‌ها، اعم از سرویس وب، پست الکترونیکی، VoIP، پیام‌رسانی آنی (IM) ، اشتراک‌گذاری فایل و ... را طراحی و اجرا نمایند و در ادامه، تیم‌های قرمز آژانس امنیت ملّی، اقدام به انجام حملات سایبری، علیه شبکه‌های مذکور می‌نمایند.

مسابقه‌ی CANVAS

این مسابقه‌ی یک‌روزه، از سال ۲۰۰۶ تا کنون در مرکز تحقیقات فضای سایبرِ آکادمی نیروی هوایی ارتش آمریکا برگزار می‌شود. در سال ۲۰۱۰، تعداد ۷۰ دانشجو در قالب ۱۲ تیم، شرکت نمودند. در این مسابقه، فرصتی برای بهره‌برداری از ابزارهای تهاجمی سایبری، به منظور کشف و گزارش‌نمودن آسیب‌پذیری‌های موجود در یک سامانه‌ی شبیه‌سازی شده در اختیار دانشجویان این آکادمی فراهم می‌گردد. در این مسابقه، دانشجویان در قالب تیم‌های ۳ یا ۴ نفره، با استفاده از ابزارهای شناسایی و تهاجمی، سعی می‌کنند آسیب‌پذیری‌های موجود در یک سامانه‌ی هوشمند و شبیه‌سازی شده را کشف نمایند و نتایج حاصل را به همراه توصیه‌هایی برای Fix نمودن آسیب‌پذیری موردنظر، در قالب یک گزارش، تنظیم و ارائه نمایند.

---

۱ Field Training Exercise (FTX)
۲ United State Strategic Command (USSTRATCOM)
۳ Joint Operation Center (JOC)
۴ Cyber Defense Exercise (CDX)

تمرین‌های سایبری فرماندهی سایبری نیروی زمینی

نظام تمرین‌ها و آزمون‌های دفاع سایبری ایالات متحده آمریکا، مطابق جدول (۶-۲)، قابل جمع‌بندی است. این نظام، متشکل از سه آزمون اصلی در سطح ملی با عناوین طوفان سایبری، حفاظ سایبری و پرچم سایبری است که به‌صورت سالیانه و دوسالانه برگزار می‌شوند. مدت برگزاری این آزمون‌ها، ۵ تا ۱۲ روز است. آزمون‌های حفاظ سایبری و پرچم سایبری، بخشی از نظام دفاع سایبری آمریکا است که توسط فرماندهی سایبری این کشور برگزار می‌شود و آزمون طوفان سایبری، بخشی از نظام امنیت سایبری آمریکا است که توسط وزارت امنیت داخلی این کشور برگزار می‌شود.

جدول (۶-۲) : دسته‌بندی تمرین‌ها و آزمون‌های دفاع سایبری ایالات متحده آمریکا

سطح	دوره زمانی برگزاری	متولی	مدت برگزاری	عنوان
ملی	دو سالانه	بخش امنیت سایبری وزارت امنیت داخلی	۵ روز	طوفان سایبری[۱]
		فرماندهی سایبری	۷ روز	حفاظ سایبری[۲]
	سالیانه	فرماندهی سایبری	۱۲ روز	پرچم سایبری[۳]
دستگاهی	سالیانه	مرکز عملیات‌های مشترک فرماندهی سایبری	۱ روز	آزمون آموزش میدان[۴]
		مرکز تحقیقات سایبری آکادمی نیروی هوایی	۱ روز	مسابقه CANVAS
	دائمی	وزارت امنیت داخلی	۱ روز	آزمون امنیت سایبر سنا[۵]
		وزارت دفاع	۱ روز	آزمون وزارت دفاع
		فرماندهی سایبری نیروی هوایی	۱ روز	آزمون دفاع سایبری[۶]

۷-۶- آشنایی با شبیه‌سازهای تمرین سایبری

شبیه‌سازها برای انجام عملیات سایبری در تمرین‌ها و مانورهای سایبری، مورد استفاده قرار می‌گیرند. ویژگی‌های بعضی از شبیه‌سازهای در اختیار ارتش ایالات متحده آمریکا، عبارت است از :

جعبه‌ابزار شبیه‌سازی ارزیابی امنیتی[۷] (SAST) یک جعبه‌ابزار است که برای آموزش حرفه‌ای سربازان نیروی هوایی، مورد استفاده قرار می‌گیرد. SAST توسط آزمایشگاه ملی شرق‌غرب اقیانوسیه[۸] (PNNL) برای شبیه‌سازی محیط شبکه‌ای تمامی سازمان‌های تحت پشتیبانی وزارت دفاع توسعه یافته است. این شبیه‌ساز، محیطی امن برای تعلیم

۱ Cyber Storm
۲ Cyber Guard (CYBER GUARD)
۳ Cyber Flag (CYBER FLAG)
۴ Field Training Exercise (FTX)
۵ Senate Cybersecurity Exercise
۶ Cyber Defense Exercise (CDX)
۷ Security Assessment Simulation Toolkit (SAST)
۸ Pacific Northwest National Laboratory (PNNL)

شتاب‌یافته فراهم می‌کند. به این معنا که در قالب یک شبکه‌ی ایزوله، یک شبکه‌ی بزرگ تحت حمله را شبیه‌سازی می‌کند. این شبیه‌ساز، یک ابزار تعلیم چندکاربره است که به صورت واقعی، میلیون‌ها کاربر با فعالیت‌های نُرمال را شبیه‌سازی می‌کند تا ترافیک واقعی زمینه را تأمین کند. این شبیه‌ساز همچنین ابزار حمله‌ی هماهنگ‌شده است که مبتنی بر ابزارهای موجود در اختیار هکرها، امکان توانمندسازی تهدیدات را برای تهاجم، فراهم می‌آورد.

محیط تمرین StealthNet یک محیط تمرین سایبری است که با حمایت مالی نیروی زمینی ارتش آمریکا توسعه یافته است. این محیط تمرین، یک چارچوب مجازی زنده برای تست، ارزیابی و تعلیم عملیات سایبری است. StealthNet خروجی یک پروژه‌ی ۳ ساله است که در سال ۲۰۱۰ آغاز شده است. با توجه به توسعه‌ی بهره‌گیری نیروی زمینی ارتش آمریکا از ارتباطات موبایل در عملیات‌های تاکتیکی، تمرکز این سامانه، روی پیامدهای Jaming و حملات ممانعت از سرویس توزیع‌شده (DDoS) است. این محیط، همچنین ایستگاه‌های رایانه‌ای را شبیه‌سازی می‌کند که از آسیب‌پذیری‌های سیستم عامل و مرورگر اینترنت برخوردار می‌باشند. یکی از اهداف این سامانه، ارزیابی ضربه ناشی از حملات سایبری روی شبکه‌های تاکتیکی و سامانه‌های شبکه‌محور متصل به آنها است. به این ترتیب که تجهیزات واقعی به این شبکه مجازی متصل می‌شوند و حس‌گرهای واقعی از طریق آنها اقدام به ارسال اطلاعات می‌نمایند. به این ترتیب، این بستر تست، قادر خواهد بود ضربه ناشی از حملات علیه سیستم عامل‌ها و مأموریت‌های شبکه را مورد ارزیابی قرار دهد.

شبیه‌ساز تعلیم تمرین شبکه[۱] (SIMTEX) ابزار شبیه‌سازی مورد استفاده در آزمون پرچم سایبری است. نیروی هوایی ارتش آمریکا، از سال ۲۰۰۸ که آزمون پرچم سایبری را آغاز نمود، به دنبال یک ابزار سایبری، برای شبیه‌سازی این تمرین نظامی برآمد. نهایتاً نیروی هوایی آمریکا، از میان پیشنهادات دریافتی، شبیه‌ساز تعلیم تمرین شبکه (SIMTEX) را برای استفاده در تمرین پرچم سایبری، انتخاب نمود. این شبیه‌ساز، برای استفاده‌ی نیروی هوایی و با توجه به نیازمندی‌های تمرین سایبری این نیرو، طراحی و پیاده‌سازی شده است. یکی از ویژگی‌های این شبیه‌ساز، شبکه‌ی امنی است که برای عملیات سایبری ایجاد می‌کند. شبیه‌ساز SIMTEX ، در تمرین پرچم سایبری سال ۲۰۱۱، برای ۲۰۰ شرکت‌کننده در قالب تیم قرمز، امکان حمله به تیم‌های آبی را فراهم نمود. SIMTEX حملات شبکه‌ای را در داخل شبکه‌ای با معماری مشابه شبکه نیروی هوایی ارتش آمریکا، شبیه‌سازی می‌کند. این شبیه‌ساز همچنین یک شبیه‌ساز اینترنت را در خود جای داده است و قادر به اجرای سناریوهای حمله خودکارسازی شده و قابل اجرا در کم‌تر از ۱۰ دقیقه می‌باشد. همچنین برای چندین موقعیت، امکان اتصال از راه دور به شبکه SIMTEX فراهم شده است تا این شبیه‌ساز، قابلیت استفاده برای اهداف آموزشی و آزمون را داشته باشد. علاوه بر این، امکان اتصال رایانه‌های واقعی به این شبیه‌ساز برای اجرای حمله توسط این رایانه‌ها نیز در داخل یک شبکه آموزشی مجرّد، فراهم شده است.

---

[۱] Simulator Training Exercise Network (SIMTEX)

سامانه CAAJED محصول پروژه‌ای با عنوان CAAJED در نیروی هوایی ارتش آمریکا است که از یکپارچه‌سازی شبیه‌ساز بازی جنگ تجاری با نام قدرت هوایی مدرن (MAP) با یک مدل واسط سایبری/جنبشی با نام اینترپرایز حاصل شده است. این سامانه که برای آموزش عملیات‌های سایبری (SECOT) مورد استفاده قرار می‌گیرد، روی شبیه‌سازی پیامدهای سطح بالای حملات سایبری در یک سناریوی جنگ، متمرکز می‌شود. این شبیه‌ساز، در تمرین دفاع سایبری (CDX) مورد استفاده قرار می‌گیرد. در این شبیه‌ساز، مجموعه‌ای از سرمایه‌های دفاعی شبیه‌سازی شده و اهداف تهاجمی وجود دارند و بازیگران، مأموریت خود را با واردنمودن ضربه‌ی جنبشی به اهداف موردنظر، انجام می‌دهند.

۶-۸- آشنایی با سامانه‌ی محیط تحقیقاتی عملیات سایبری[۱] (CORE)

وزارت دفاع ایالات متحده آمریکا، در گزارش خود به کنگره این کشور، در خصوص استفاده از شبیه‌سازی و مدل‌سازی سایبری توسط وزارت دفاع، از محیط تحقیقاتی عملیات سایبری (CORE) به عنوان یکی از امکانات ویژه‌ی شبیه‌سازی و مدل‌سازی در اختیار وزارت دفاع نام برده شده است.

این محیط تحقیقاتی، شرایط و اطلاعات موردنیاز، برای تحلیلِ پیش‌گیرانه روی پیامدهای تهدیدات سایبری بالقوه را فراهم می‌آورد و با استفاده از اطلاعاتِ حاصل، امکان ارتقاء سطح امنیت سامانه‌ها و شبکه‌ها، جهت اجرای مأموریت‌های دفاعی را فراهم می‌کند.

۶-۹- آشنایی با میدان تمرین سایبری ملی[۲] (NCR)

وزارت دفاع ایالات متحده آمریکا، مدعی است در پی اتخاذ یک رویکرد انقلابی در حوزه‌ی شبیه‌سازی و مدل‌سازی، پروژه‌ی توسعه میدان تمرین سایبری را اجرا نموده و در نتیجه اجرای این پروژه، میدان تمرین سایبری ملّی (NCR) تحقق یافته است. میدان تمرین سایبری ملّی، یک قابلیت ویژه برای آزمون سایبری در ابعاد گسترده را فراهم می‌آورد. NCR، توانایی ارزیابی فناوری‌ها، خط‌مشی‌ها و رویه‌های سایبری را دارد و یک سرمایه‌ی حیاتی، برای توسعه‌ی عملیات‌های سایبری آینده محسوب می‌شود. با قابلیت تست و تحلیل تمرین سایبری که NCR در شرایط واقعی فراهم می‌آورد، وزارت دفاع توانایی اصلاح، تحقیق و توسعه قابلیت‌هایی که موجب تقویت دفاع سایبری و ایجاد تغییرات اساسی در حوزه‌ی امنیت سایبری می‌شوند را یافته است.

۶-۱۰- آشنایی با بازی جنگ سایبری

---

۱ Cyber Operations Research Environment (CORE)
۲ National Cyber Range (NCR)

بازی جنگ، ابزار اجرای مجدد نمونه‌هایی از حملات سایبری است که قبلاً در فضای سایبر به مورد اجرا گذاشته شده‌اند و بر اساس ویژگی‌هایشان، در زمره جنگ‌های سایبری ثبت شده‌اند. اجرای مجدد این جنگ‌های سایبری، در محیط شبیه‌سازی شده انجام می‌گیرد و هدف از آن، تجربه‌آموزی بر اساس نمونه‌های واقعی جنگ سایبری است.

بازی جنگ اداره‌ی شناسایی ملّی [۱] (NRO)، نمونه‌ای از بازی جنگ فضایی و سایبری است که توسط فرماندهی سایبری ایالات متحده پشتیبانی می‌شود. هدف از این بازی جنگ، آشنایی و درک قابلیت‌های سرمایه‌های فضایی حیاتی و آسیب‌پذیری آنها در مقابل حملات سایبری است. این بازی جنگ، همچنین ارتباط بین امنیت فضای سایبر و امنیت فضایی را به شکل مناسبی، نشان می‌دهد.

کلوپ جنگ سایبری [۲] (CWC)، یک کلوپ دانشجویی است که در مرکز تحقیقات فضای سایبرِ آکادمی نیروی هوایی ارتش آمریکا و با هدف آموزش و درهم‌آمیختن دانش و تجربه در حوزه‌ی سایبری برای فرماندهان آینده‌ی نیروی هوایی، ایجاد شده است. این کلوپ، متشکل از شبکه‌ی Sandbox است که دانشجویان می‌توانند تکنیک‌های حمله، بهره‌برداری و دفاع سایبری را در آن تمرین کنند. دانشجویان در این کلوپ، در کنار متخصصین خبره و مجرب قرار می‌گیرند و با این تکنیک‌ها، آشنا می‌شوند.

بازی جنگ سطح بالا [۳] نیز یک بازی جنگ سایبری محسوب می‌شود. این شبیه‌ساز می‌تواند برای تست آمادگی سایبری سازمان‌ها مورد استفاده قرار گیرد. شبیه‌سازی تمرین‌های توفان سایبری شماره (۱)، (۲) و (۳) که در سال‌های ۲۰۰۶، ۲۰۰۸ و ۲۰۱۰ اجرا شدند، در این بازی جنگ سایبری وجود دارند. برای این تمرین‌ها، سنجش میزان مکانیزم‌های آمادگی، پاسخ، هماهنگی و بازیابی، در قالب یک واقعه‌ی سایبری شبیه‌سازی شده است. حملات سایبری در طول ۴ روز، ادامه می‌یابند و سازمان، باید راهبردهای پاسخ به این حملات را توسعه دهد. این شبیه‌ساز، به دنبال تست توانایی تاکتیکی سازمان نیست، بلکه به دنبال سنجش سیاست‌های پاسخ سازمان است.

ارتش فرانسه نوع مشابهی از بازی جنگ، با نام France's Piranet و ارتش هند نیز نوع مشابهی با نام India's Divine Matrix در اختیار دارند. همچنین نیروی هوایی ارتش آمریکا، نوعی بازی جنگ سطح بالا در اختیار دارد که راهبردهای اتخاذ شده توسط سازمان را مورد سنجش قرار می‌دهد.

۱۱-۶- آشنایی با آزمون سایبری سپر قفل‌شده [۴] ناتو

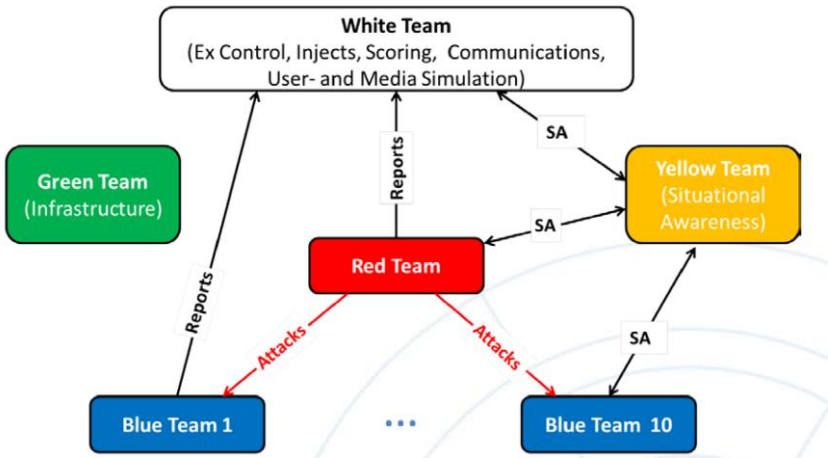
---

۱ National Reconnaissance Office (NRO)
۲ Cyber Warfare Clube (CWC)
۳ High-level wargaming
۴ Locked Shield

مرکز مشارکتی نخبگان دفاع سایبری ناتو، اولین مرتبه در سال ۲۰۱۰ با همکاری مراکز دفاع سایبری کشورهای عضو ناتو، یک آزمون دفاع سایبری[۱] (CDX) یک روزه با عنوان سپر سایبری بالتیک[۲] (BSC) اجر نمود. این مرکز آزمون‌های دفاع سایبری بعدی خود را از سال ۲۰۱۲، به صورت سالیانه و با عنوان سپر قفل‌شده[۳] (LS) برگزار نموده است. آخرین آزمون سپر قفل‌شده، در تاریخ ۲۷ آوریل ۲۰۱۸ برگزار شد.

آزمون سپر قفل‌شده، بزرگ‌ترین آزمون دفاع سایبری رقابتی و آتش–زنده جهان محسوب می‌شود. در آزمون سپر قفل‌شده سال ۲۰۱۷ (LS۱۷)، بیش از ۲۵۰۰ حمله سایبری انجام شد و بیش از ۳۰۰۰ سامانه مجازی‌شده مستقر شدند. در این آزمون، نزدیک به ۹۰۰ نفر از ۲۵ کشور عضو ناتو، شرکت نموده و به رقابت پرداختند.

ساختار اجرای آزمون آزمون سپر قفل‌شده، مطابق شکل (۶–۳) است.



شکل (۶–۳) : ساختار اجرای آزمون سپر قفل‌شده (LS)

قبل از شروع آزمون، تیم سبز[۴] (GT) اقدام به «طراحی، تنظیم و پیکربندی زیرساخت‌های موردنیاز برای برگزاری آزمون، اعم از تجهیزات فیزیکی، سکوی مجازی‌سازی، فضای ذخیره‌سازی، شبکه‌سازی، دسترسی از راه دور، ثبت ترافیک، مسیریاب‌های شبکه خصوصی مجازی برای تیم‌های آبی و حساب‌های کاربری»، «طراحی و ایجاد شبکه بازی و شبکه‌های تیم‌های آبی»، «برنامه‌ریزی شبکه بات و عامل‌های امتیازدهی خودکار به شرکت‌کنندگان در آزمون»، «توسعه

۱ Cyber Defense Exercise (CDX)
۲ Baltic Cyber Shield (BSC)
۳ Locked Shield (LS)
۴ Green Team (GT)

راه‌حل‌هایی برای تولید ترافیک» و «تنظیم راه‌حل مناسب برای پایش زیرساخت آزمون»، می‌نماید. در طول اجرای آزمون نیز، پشتیبانی از تیم‌های مشارکت‌کننده بر عهده این تیم قرار دارد.

در این آزمون، مخاطبان آموزش، متخصصان پاسخ اضطراری رایانه‌ای کشورها هستند که در قالب تعدادی تیم آبی[۱] (BT) ملی سازمان‌دهی می‌شوند. این تیم‌ها، نقش تیم‌های واکنش سریع کشورها را ایفا می‌کنند. تمرکز اصلی این تیم‌ها بر دفاع است. تیم‌های آبی وظیفه دارند از شبکه‌های مجازی‌شده‌ی مشابه سازمان‌های واقعی، در مقابل حملات تیم قرمز[۲] (RT) محافظت و نگهداری کنند. به عنوان بخشی از آزمون، لازم است تیم آبی اقدام به رسیدگی به حوادث نموده و به‌صورت پیوسته، یافته‌های خود را با مرکز فرماندهی خود مبادله نماید تا دستورات مناسب جهت اقدام را دریافت نماید. تیم‌های ابی را می‌توان به عنوان چند رشته‌ای توصیف نمود. در آزمون سال ۲۰۱۷، هر تیم آبی، به‌طور متوسط از ۳۰ عضو (بین ۱۵ تا ۵۶ عضو) تشکیل شد. یادگیری انفرادی، حیاتی است. اما بخش مهم، این است که چگونه تیم‌ها بر روی نقاط ضعف شخصی در مهارت‌ها و دانش غلبه می‌کنند و بهترین نتیجه را به عنوان یک تیم به دست می‌آورند.

تیم سفید[۳] (WT) مسئولیت آماده‌سازی آزمون و کنترل آن را در زمان برگزاری بر عهده دارد. آین تیم، اهداف آموزش، سناریو و اهداف سطح بالا برای تیم قرمز را تعیین می‌کند، قوانین را نوشته و رسانه‌ها، سناریوها و تزریق‌های قانونی و برنامه ارتباطی را تهیه می‌کند. در طی اجرای آزمون، تیم سفید به عنوان سلول کنترل‌کننده آزمون، مسئولیت تصمیم‌گیری برای شروع هر مرحله از آزمون، کنترل کمپین تیم قرمز و اتخاذ تصمیم در مورد امتیازدهی را بر عهده دارد. همچنین مدیریت آزمون و شبیه‌سازی کاربر و محیط، از وظایف این تیم است.

ماموریت تیم سرخ (RT) نیز به خطر انداختن یا تضعیف عملکرد سامانه‌های تیم آبی است. آنها در هر مرحله، تعدادی هدف از پیش تعیین شده دارند که مجاز به تکرار برخی از این اهداف، در مراحل بعدی نیز هستند.

تمرکز آزمون سپر قفل‌شده، بر آموزش تیم‌های آبی است. بنابراین، اعضای تیم قرمز به طور عمده به عنوان نیروی کار برای مبارزه با تیم‌های آبی به حساب می‌آیند. در اصل تیم قرمز از رویکرد جعبه سفید استفاده می‌کند. مشخصات فنی تنظیم اولیه سامانه‌های تیم‌های آبی، از قبل برای تیم قرمز در دسترس است.

نقش تیم زرد[۴] (YT)، آن است که به صورت مداوم، در مورد آخرین وضعیت آزمون، آگاهی موقعیتی بدهد. این آگاهی، در درجه اول به تیم سفید ارائه می‌شود تا بر اساس آن، اقدام به امتیازدهی نماید و همچنین به سایر شرکت‌کنندگان در آزمون نیز ارائه می‌شود. منابع اصلی داده‌ها برای تیم زرد، گزارش‌های دریافتی از تیم‌های آبی، گزارش‌های وضعیت حمله دریافت شده از تیم‌های قرمز و نتایج به دست آمده از امتیازات خودکار و دستی است. تحلیل‌گر تیم زرد، کلیه رابطهای موردنیاز برای بررسی همه گزارش‌های دریافتی و برچسب‌زنی آن‌ها بر اساس محتوای گزارش را در اختیار دارد.

---

۱ Blue Team (BT)
۲ Red Team (RT)
۳ White Team (WT)
۴ Yellow Team (YT)

به روز رسانی‌های منظم، برای رهبر تیم سفید و تیم‌های آبی، تأمین می‌شود. تیم زرد بر اساس این داده‌ها، آخرین وضعیت آزمون را از دیدگاه‌های مختلف، تهیه نموده و به‌صورت بصری‌شده، در اختیار مخاطبین قرار می‌دهد.

به این ترتیب، به عنوان بخشی از آزمون، لازم است تیم‌های قرمز و تیم‌های آبی، در کنار انجام اقدامات تهاجمی و دفاعی خود، آخرین یافته‌های خود را به صورت مداوم، علاوه بر سایر تیم‌های متناظر خود، با تیم زرد و تیم سفید نیز به اشتراک بگذارند تا از یک‌سو انجام اقدامات تهاجمی و تدافعی به‌صورت هماهنگ انجام شود و از سوی دیگر، تیم زرد در تأمین آگاهی موقعیتی و تیم سفید در داوری و امتیازدهی، کمک شوند.

نکته بسیار مهم، این‌که در آزمون سپر قفل‌شده، از یک رویکرد مبتنی بر بازی استفاده می‌شود، به این معنی که شرکت‌کنندگان در نقش واقعی زندگی خود بازی نمی‌کنند و فعالیت‌ها در یک محیط آزمایشگاهی انجام می‌شود. این آزمون بر روی یک شبکه بازی مجازی‌شده جداگانه اجرا می‌شود که تیم‌ها از راه دور و از طریق شبکه خصوصی مجازی (VPN)، به آن دسترسی دارند.

۱۲-۶- توصیه‌های ضروری

به‌منظور تحقق اهداف آموزشی پیش‌بینی شده برای دوره‌های آموزشی عرضی پدافند سایبری کشور و تبدیل قابلیت‌های تیم‌های پدافند سایبری به توانایی، آمادگی، کارآمدی و اقربخشی، لازم است اقدام‌های زیر، انجام پذیرند :

۱. هر دستگاه دولتی، حداقل باید یک نوع تمرین پدافند سایبری برای تیم پدافند سایبری خود طراحی و اجرا نماید. این تمرین پدافند سایبری، باید در حوزه تخصصی دستگاه مربوطه طراحی شود و در فضای آموزشی و شبیه‌سازی شده، مشابه با زیرساخت حیاتی، حساس یا مهمی که دستگاه مربوطه متولی آن است، اجرا شود.

۲. برای تمرین پدافند سایبری دستگاه خود، عنوان مناسب و اهداف آموزشی مشخص و قابل حصول، تعیین نمائید. هدف اصلی برگزاری تمرین پدافند سایبری، باید یادگیری انجام مأموریت‌های پدافند سایبری، با بهره‌گیری از ابزارهای آموزشی باشد. در کنار این هدف، تقویت کار تیمی و اقدام هماهنگ اعضای تیم پدافند سایبری در مواجهه با حملات سایبری نیز باید هدف‌گذاری شود.

۳. برای دست‌یابی به اهداف آموزشی پیش‌بینی شده، سناریوی تمرین پدافند سایبری مناسب طراحی کنید. توجه داشته باشید که تمرین سایبری، به‌منظور ارتقاء مهارت‌های تیم پدافند سایبری و تبدیل توانایی‌های این تیم به آمادگی اجرا می‌شود. بر این اساس، کافی است در سناریوی تمرین سایبری، یک یا چند کارشناس پدافند سایبری، در محیط آزمایشگاهی، برای مدت چند دقیقه تا چند ساعت، استفاده از ابزارهای پدافند سایبری، برای مقابله با تهاجم‌های سایبری را آموزش ببینند. در این سناریو، بهتر است انجام حملات سایبری، توسط سامانه‌های شبیه‌سازی حمله انجام شود و نوع حمله توسط افراد تحت آموزش، انتخاب شود تا از قبل، آمادگی ذهنی برای دفاع در مقابل آن، وجود داشته باشد.

٤. به‌منظور تحقق اهداف آموزشی تمرین پدافند سایبری، بهتر است ترکیبی از ابزارهای متن‌باز و ابزارهای پدافند سایبری بومی و دارای گواهی از مرکز پدافند سایبری کشور، مورد استفاده قرار گیرند. یک ابزار کلیدی در تمرین‌های سایبری، سامانه تولید ترافیک حمله یا سامانه اجرای تهاجم سایبری است. توجه داشته باشید، استفاده از این سامانه‌ها، باید حتماً در شبکه‌ای آزمایشگاهی و مستقل از شبکه سازمانی و مستقل از شبکه اینترنت انجام گیرد. این امر، از یک‌سو با هدف جلوگیری از وارد شدن صدمات پیش‌بینی نشده به شبکه سازمانی یا کاربران شبکه اینترنت و از سوی دیگر، با هدف پیش‌گیری از شناسایی فعالیت‌های در حال انجام و سوء استفاده از امکانات تمرینی برای اهداف مخرّب، انجام می‌گیرد.

٥. هر زیرساخت حیاتی، حداقل باید یک نوع آزمون پدافند سایبری برای تیم‌های پدافند سایبری دستگاه‌های تابعه خود، طراحی و اجرا نماید. این آزمون پدافند سایبری، باید در حوزه تخصصی زیرساخت مربوطه طراحی شود و در فضای آموزشی و شبیه‌سازی شده، مشابه با زیرساخت حیاتی، حساس یا مهم مربوطه، به مورد اجرا گذاشته شود.

٦. برای آزمون پدافند سایبری زیرساخت خود نیز عنوان مناسب و اهداف آموزشی مشخص و قابل حصول، تعیین نمائید. هدف اصلی برگزاری آزمون پدافند سایبری، باید انجام صحیح و دقیق مأموریت‌های پدافند سایبری، با بهره‌گیری از ابزارهای آموزشی باشد. در کنار این هدف، صحت و دقت کار تیمی یا به عبارت دیگر، هماهنگی صحیح و دقیق اعضای تیم پدافند سایبری در مواجهه با حملات سایبری نیز باید هدف‌گذاری شود.

٧. برای دست‌یابی به اهداف آموزشی پیش‌بینی شده، سناریوی آزمون پدافند سایبری مناسب طراحی کنید. توجه داشته باشید که آزمون پدافند سایبری، به‌منظور تبدیل آمادگی تیم پدافند سایبری زیرساخت مربوطه به کارآمدی اجرا می‌شود. بر این اساس، کافی است در سناریوی آزمون سایبری، تیم‌های پدافند سایبری دستگاه‌های تابعه، در محیط آزمایشگاهی، برای مدت چند ساعت، اجرای صحیح و دقیق مأموریت‌های پدافند سایبری خود را با استفاده از ابزارهای پدافند سایبری، به معرض رقابت بگذارند. در این سناریو، بهتر است انجام حملات سایبری، توسط سامانه‌های شبیه‌سازی حمله یا یک تیم مهاجم انجام شود و نوع حمله، از قبل برای تیم‌های شرکت‌کننده، مشخص باشد تا از قبل، آمادگی ذهنی برای دفاع در مقابل آن، وجود داشته باشد.

٨. به‌منظور تحقق اهداف آموزشی آزمون پدافند سایبری، بهتر است ترکیبی متنوع از ابزارهای متن‌باز و ابزارهای پدافند سایبری بومی و دارای گواهی از مرکز پدافند سایبری کشور، در اختیار تیم‌های شرکت‌کننده قرار گیرد. لیست این ابزارهای پدافندی باید از قبل مشخص باشد و به اطلاع تیم‌های شرکت‌کننده رسانده شود. از آن‌جا که تیم هر دستگاه، با ابزارهای موجود در دستگاه خود آشنایی دارد، ابزارهایی که در آزمون، در اختیار تیم‌های شرکت‌کننده قرار می‌گیرند، باید تجمیعی از ابزارهای مورد استفاده در دستگاه‌های تابعه باشند. یک ابزار کلیدی در آزمون‌های سایبری، سامانه تولید ترافیک حمله یا سامانه اجرای تهاجم سایبری است. توجه داشته باشید، استفاده از این سامانه‌ها، باید حتماً در شبکه‌ای آزمایشگاهی و مستقل از شبکه سازمانی، مستقل از زیرساخت مربوطه و

مستقل از شبکه اینترنت انجام گیرد. این امر، از یک‌سو با هدف جلوگیری از وارد شدن صدمات پیش‌بینی نشده به شبکه سازمانی، شبکه زیرساخت مربوطه یا کاربران شبکه اینترنت و از سوی دیگر، با هدف پیش‌گیری از شناسایی فعالیت‌های در حال انجام و سوء استفاده از امکانات آزمون برای اهداف مخرّب، انجام می‌گیرد.

۹. هر زیرساخت حیاتی، باید یک مانور پدافند سایبری سالیانه، برای تیم‌های پدافند سایبری دستگاه‌های تابعه خود، طراحی و اجرا نماید. این مانور پدافند سایبری، باید در حوزه تخصصی زیرساخت مربوطه طراحی شود و در فضای واقعی زیرساخت حیاتی، حساس یا مهم مربوطه، به مورد اجرا گذاشته شود.

۱۰. برای مانور پدافند سایبری زیرساخت خود نیز عنوان مناسب و اهداف مشخص و قابل حصول، تعیین نمائید. هدف اصلی برگزاری مانور پدافند سایبری، باید بازنمایی موفقیّت مأموریت‌های پدافند سایبری، در مواجهه با هرگونه تهاجم سایبری باشد. در کنار این هدف، صحت و دقت کار تیمی یا به عبارت دیگر، هماهنگی صحیح و دقیق اعضای تیم پدافند سایبری در مواجهه با حملات سایبری در فضای واقعی نیز باید هدف‌گذاری شود.

۱۱. برای دست‌یابی به اهداف آموزشی پیش‌بینی شده، سناریوی مناسب برای مانور پدافند سایبری، طراحی کنید. توجه داشته باشید که مانور پدافند سایبری، به‌منظور تبدیل کارآمدی تیم پدافند سایبری زیرساخت مربوطه به اثربخشی اجرا می‌شود. بر این اساس، لازم است در سناریوی مانور سایبری، تیم‌های پدافند سایبری دستگاه‌های تابعه، در محیط واقعی، حداقل برای مدت چند ساعت و حداکثر برای مدت ۲ روز، اجرای مؤثر مأموریت‌های پدافند سایبری خود را با استفاده از ابزارهای پدافند سایبری، به نمایش بگذارند. در این سناریو، بهتر است انجام حملات سایبری، توسط تیم‌های تهاجمی که خود، بخشی از مانور می‌باشند، انجام شود و نوع حمله یا حملات قابل انتخاب توسط تیم‌های مهاجم، از قبل برای تیم‌های شرکت‌کننده، مشخص باشد تا از بروز حوادث پیش‌بینی نشده در زیرساخت مربوطه، جلوگیری شود.

۱۲. در سناریوی برگزاری مانور پدافند سایبری، علاوه بر تیم‌های مهاجم و مدافع، حتماً یک تیم پشتیبانی فنی، یک تیم ناظر و یک تیم با اختیارات فرماندهی میدان نیز پیش‌بینی شوند. وظایف و اختیارات این تیم، به عنوان بخشی از سناریوی برگزاری مانور، طراحی شوند.

۱۳. به‌منظور تحقق اهداف آموزشی مانور پدافند سایبری، بهتر است ترکیبی متنوع از ابزارهای متن‌باز و ابزارهای تهاجمی و ابزارهای پدافند سایبری بومی و دارای گواهی از مرکز پدافند سایبری کشور، در اختیار تیم‌های شرکت‌کننده قرار گیرد. لیست این ابزارهای پدافندی باید از قبل مشخص باشد و به اطلاع تیم‌های شرکت‌کننده رسانده شود.

مراجع

[۱] ISO/IEC JTC۱, “Information technology-Security techniques-Information security management systems-Overview and vocabulary”, ISO/IEC, Geneva, Switzerland, ISO/IEC ۲۷۰۰۰, Jan. ۲۰۱٤.

[۲] ISO/IEC JTC۱, “Information technology-Security techniques-Guidelines for cybersecurity”, ISO/IEC, Geneva, Switzerland, ISO/IEC ۲۷۰۳۲, Jul. ۲۰۱۲.

[۳] ISO/IEC JTC۱, “Information technology-Security techniques-Information security risk management”, ISO/IEC, Geneva, Switzerland, ISO/IEC ۲۷۰۰٥, June. ۲۰۱۱.

[٤] NIST, “Official Common Platform Enumeration (CPE) Dictionary”, Available: https://nvd.nist.gov/cpe.cfm, June ۱٥, ۲۰۱٦.

[٥] Mitre, “CPE Specifications”, Available: https://cpe.mitre.org/specification, June ۱٥, ۲۰۱٦.

[٦] NIST, “Asset Identification ۱,۱ Schema”, Available: https://scap.nist.gov/schema/asset-identification/۱,۱/asset-identification_۱,۱,۰.xsd, June ۱٥, ۲۰۱٦.

[۷] Mitre, “Common Vulnerabilities and Exposures”, Mitre, Available: https://cve.mitre.org, January, ۲۰۱۹.

[۸] NIST, “National Vulnerability Database”, NIST, Available: https://nvd.nist.gov, January, ۲۰۱۹.

[۹] FIRST, “Common Vulnerability Scoring System V۳,۰: Specification Document”, FIRST, North Carolina, USA, https://www.first.org/cvss/specification-document, ۲۰۱٥.

[۱۰]C. Team, “Terminology.” [Online]. Available: https://cve.mitre.org/about/terminology.html.

[۱۱]C. Joshi, U. K. Singh, and K. Tarey, “A review on taxonomies of attacks and vulnerability in computer and network system,” Int. J. advbaced researcg ub Comput. Sci. Softw. Eng., vol. ۳, no. ٥, pp. ۷٤۲–۷٤۷, ۲۰۱٥.

[۱۲]F. Piessens, “A taxonomy of causes of software vulnerabilities in Internet software,” Suppl. Proc. ۱۳th Int. Symp. Softw. Reliab. Eng., pp. ٤۷–٥۲, ۲۰۰۲.

[۱۳]P. K. Singh, A. K. Vatsa, R. Sharma, and P. Tyagi, “Taxonomy Based Intrusion Attacks and Detection Management Scheme in Peer-to-Peer Network,” Int. J. Netw. Secur. Its Appl., vol. ٤, no. ٥, pp. ۱٦۷–۱۷۹, ۲۰۱۲.

[۱٤] R.P. Lippmann, J.F. Riordan, T.H. Yu, K.K. Watson, “Continuous Security Metrics for Prevalent Network Threats: Introduction and First Four Metrics”, Lincoln Laboratory, Massachusetts Institute of Technology, Massachusetts, USA, Project Report IA-۳, May. ۲۰۱۲.

[۱٥] ITU-T, “Security architecture for systems providing end-to-end communications”, ITU, Geneva, Switzerland, ITU-T Recommendation X.۸۰٥, October ۲۰۰۳.

[۱٦] Joint Task Force Transformation Initiative, “Guide for Conducting Risk Assessments”, NIST, Maryland, USA, NIST SP ۸۰۰-۳۰, Sep. ۲۰۱۲.

[۱۷]S. Hansman, “A taxonomy of network and computer attack methodologies,” Engineering, pp. ۱–٤۸, ۲۰۰۳.

[۱۸]C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi, “A taxonomy of computer program security flaws”, ACM Comput. Surv., vol. ۲٦, no. ۳, pp. ۲۱۱–۲٥٤, ۱۹۹٤.

[۱۹]G. Álvarez and S. Petrović, “A new taxonomy of web attacks suitable for efficient encoding”, Comput. Secur., vol. ۲۲, no. ٥, pp. ٤۳٥–٤٤۹, ۲۰۰۳.

[۲۰]A. D. Wood and J. A. Stankovic, “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks”, Handb. Sens. Networks Compact Wirel. Wired Sens. Syst., pp. ۷۳۹–۷٦۳, ۲۰۰٤.

[۲۱]A. N. Herold, “Attack Taxonomies and Ontologies”, no. March, pp. ۱–۱۰, ۲۰۱٥.

[۲۲]A. . Fallis, “Classifying network attack scenarios using an Ontology”, J. Chem. Inf. Model., vol. ٥۳, no. ۹, pp. ۱٦۸۹–۱٦۹۹, ۲۰۱۲.

[۲۳] Ali A.Ghorbani et al, “Network Intrusion Detection and Prevention”, July ۲۰۰۹.
[۲٤] Karen Scarfone, Peter Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, Feb ۲۰۰۷
[۲٥] D. E. Denning, “An Intrusion-Detection Model”, Feb ۱۹۸۷.
[۲٦] Varun Chandola, Arindam Banerjee, and Vipin Kumar, “Anomaly Detection: A Survey”, ۲۰۰۹.
[۲۷] P.Garcia-Teodoroa, J.Diaz-Verdejoa, G.Macia-Fernandez, E. Vazquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges”, ۲۰۰۹.
[۲۸] Critical Infrastructure Threat Information Sharing Framework; https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-٥٠٨.pdf
[۲۹] Australian Department of Defence, “A Survey of Cyber Ranges and Test beds”, October ۲۰۱۳
[۳۰] Defense Information Systems Agency, “Operationally Focused Cyber Training Framework”, May ۲۰۱۲
[۳۱] National Institute of Standards and Technology, “A Role-Based Model for Federal Information Technology Cybersecurity Training”, March ۲۰۱٤
[۳۲] Combat Support Agency-Joint Training Working Group, “Combat Command (CCMD) Training”, September ۲۰۱۲
[۳۳] Department of Homeland Security, “Cyber Storm III Final Report”, July ۲۰۱۱

[۳۴] وزارت ارتباطات و فناوری اطلاعات، ”سایت اطلاع‌رسانی مرکز ماهر“ ، سازمان فناوری اطلاعات ایران، تهران، ایران، ۱۳۹۷.

اختصارات

ADSL	Asymmetric Digital Subscriber Line
ALS	Applicability Language Specification
ALS	Applicability Language Statements
APT	Advanced Persistent Threats
BID	Bugtraq ID
BS	Base Score
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria
CCDC	Collegiate Cyber Defense Competition
CCD-COE	Cooperative Cyber Defence Centre of Excellence
CDX	Cyber Defense Exercise
CERT	Cyber Emergency Response Team
CIS	Center fo Internet Security
CNA	CVE Numbering Authorities
COP	Common Operating Picture
CORE	Cyber Operations Research Environment
CPE	Common Platform Enumeration
CTF	Capture the Flag
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWC	Cyber Warfare Clube
DoS	Denial of Service
ENISA	European Network and Information Security Agency
FTX	Field Training Exercise
HIDS	Host Based Intrusion Detection System
HIPS	Host Based Intrusion Prevention System
ICT	Information & Communication Tecnology
ICS	Industrial Control System
ICS-CERT	Industrial Control System- Cyber Emergency Response Team
IDI	ICT Development Index
IDPS	Intrusion Detection and Prevention System
ISAC	Information Sharing and Analysis Center
ISAS	Information Sharing and Alert System
JOC	Joint Operation Center
MBSA	Microsoft Baseline Security Analyser
MSSP	Managed Security Service Provider
NATO	North Atlantic Treaty Organization
NCR	National Cyber Range

NIDS	Network Based Intrusion Detection System
NIPS	Network Based Intrusion Prevention System
NRO	National Reconnaissance Office
NVD	National Vulnerability Database
OSVDB	Open Source Vulnerabilities Database
PNNL	Pacific Northwest National Laboratory
PDA	Personal Digital Assistant
PSTN	Public Switching Telephone Network
R&TO	Research and Technology Organization of NATO
SAST	Security Assessment Simulation Toolkit
SCAP	Security Content Automation Protocol
SDLC	System Development Life Cycle
SIMTEX	Simulator Training Exercise Network
SOC	Security Operation System
STIX	Structured Threat Information eXpression
TA	Type Approval
USSTRATCOM	United State Strategic Command
WAF	Web Application Firewall
WFN	Well-Formed CPE Name

واژه‌نامه انگلیسی به فارسی

واژه انکلیسی	معادل فارسی
Access Control	کنترل دسترسی
Accounting	پاسخ‌گویی
Action	اقدام
Activity	فعالیت
Advanced	پیشرفته
Agency	آژانس، مؤسسه
Alert	هشدار
Analysis	تحلیل
Analyzer	تحلیل‌گر
Applicability	کاربردپذیر
Application	کاربرد
Approval	نمونه
Assessment	ارزیابی
Asset	سرمایه
Asset-Oriented	سرمایه‌محور
Assistant	دستیار
Assurance	اعتماد، اطمینان
Attack	حمله
Authentication	احراز هویت، تصدیق هویت
Authority	اختیار
Authorization	اختیاردهی
Automation	اتوماسیون، خودکارسازی
Availability	دسترس‌پذیری
Backup	نسخه پشتیبان
Base	پایه
Baseline	خط مبنا

Board	هیأت‌مدیره
Cause	انگیزه
Center	مرکز
Centre of Excellence	مرکز نخبگان
Classification	طبقه‌بندی
Clube	باشگاه
Coalition	ائتلاف
Common	مشترک
Communication	ارتباطات
Competition	مسابقه، رقابت
Confidentiality	محرمانگی
Content	محتوا
Context	بافتار، زمینه
Cooperative	مشارکتی
Crime	جرم
Criminal	مجرم
Criteria	معیار
Cyber	فضای سایبر
Cycle	چرخه
Database	پایگاه داده
Decision	تصمیم
Decision Maker	تصمیم‌ساز
Defence	دفاع
Degree	درجه
Detection	تشخیص
Development	توسعه
Dictionary	لغت‌نامه، واژه‌نامه
Effectiveness	اثربخشی
Enumeration	سرشماری
Environment	محیط
Espionage	جاسوسی

Estimate	تخمین
European Union	اتحادیه اروپایی
Excellence	نخبگان
Exercise	آزمون
Exploit	بهره‌برداری
Exploit Code	کد بهره‌برداری
Exposure	نمایش، در معرض گذاری
Field	میدان
Financial	مالی
FireWall	دیوار آتش
Flag	پرچم
Formatted	فرمت‌شده
Framework	چارچوب
Group	گروه
Guard	سپر
Hacker	نفوذگر
Hacktivist	نفوذگر دارای انگیزه سیاسی
Health	سلامت
Host	میزبان
Hostile	دشمن، متخاصم
Identification	شناسایی
Identifier	شناسایی‌کننده هویت
Impact	ضربه
Information	اطلاعات
Insider	مهاجم خودی، مهاجم داخلی
Integrity	صحت، یکپارچگی
Intrusion	نفوذ، حمله
Joint	مشترک
Laboratory	آزمایشگاه
Language	زبان
Life	زندگی

Likelihood	احتمال
Location	موقعیت
Locked	قفل‌شده
Log	ثبت وقایع
Logical	منطقی
Managed	مدیریت شده
Manager	مدیر
Matching	تطبیق
Mercenary	مزدور
Naming	نام‌گذاری
NATO	سازمان پیمان آتلانتیک شمالی (ناتو)
Nation-state	دولت
National	ملی
Non Repudiation	عدم انکار
Numbering	شماره‌گذاری
Office	اداره
Open Source	متن‌باز
Operation	عملیات
Oriented	جهت‌دار، متمایل به
Organization	سازمان
Organized Cyber Criminal	مجرم سایبری سازمان‌یافته
Pattern	الگو
Penetration	نفوذ
Persistent	مانا، ماندگار
Picture	تصویر
Platform	سکو
Predisposing	مهیّا، ازپیش فراهم‌شده
Prevention	پیش‌گیری
Privacy	حریم خصوصی
Protocol	مقاوله‌نامه
Provider	تأمین‌کننده، عرضه‌کننده

Range	میدان تمرین
Reconnaissance	شناسایی
Repudiation	انکار
Required	موردنیاز
Requirements	نیازمندی‌ها
Research	پژوهش، تحقیق
Resource	منابع
Rights	حقوق
Risk	مخاطره
Scan	پویش
Scanner	پویش‌گر
Scenario	سناریو
Score	امتیاز
Scoring	امتیازدهی
Sector	بخش
Security	امنیت
Sequence	دنباله
Service	خدمت
Severity	شدّت
Sharing	اشتراک‌گذاری
Shield	سپر
Signature	امضاء
Simulation	شبیه‌سازی
Simulator	شبیه‌ساز
Specification	مشخصات
Sponsored	حمایت شده
State	دولت
Stateful	حالت کامل
State sponsored	تحت حمایت دولت
Storm	طوفان
Strategic	راهبردی

String	رشته
Success	موفقیت
System	سامانه
Technology-Oriented	فناوری‌محور
Termination	خاتمه، پایان، انتها
Terrorist	تروریست
Test	آزمون
Threat	تهدید
Threat Event	واقعه‌ی تهدید
Threat-Oriented	تهدیدمحور
TIER	رده
Toolkit	جعبه‌ابزار
Training	آموزش
Trieaty	پیمان
Type	نمونه، نوع
Uniform	متحدالشکل، یک‌شکل
Virtual	مجازی
Vulnerability	آسیب‌پذیری
Vulnerability-Oriented	آسیب‌پذیری‌محور
Warfare	جنگ
Wargaming	بازی جنگ
Well-Formed	خوش‌تعریف
Workstation	ایستگاه‌کاری
Zone	ناحیه

واژه‌نامه فارسی به انگلیسی

واژه فارسی	معادل انکلیسی
آزمایشگاه	Laboratory
آزمون	Exercise
آزمون	Test
آژانس، مؤسسه	Agency
آسیب‌پذیری	Vulnerability
آسیب‌پذیری‌محور	Vulnerability-Oriented
آموزش	Training
اتحادیه اروپایی	European Union
اتوماسیون	Automation
اثربخشی	Effectiveness
احتمال	Likelihood
احراز هویت	Authentication
اختیار	Authority
اختیاردهی	Authorization
اداره	Office
ارتباطات	Communication
ارزیابی	Assessment
اشتراک‌گذاری	Sharing
اطلاعات	Information
اعتماد	Assurance
اقدام	Action
الگو	Pattern
امتیاز	Score
امتیازدهی	Scoring
امضاء	Signature
امنیت	Security

Repudiation	انکار
Cause	انگیزه
Workstation	ایستگاه‌کاری
Coalition	ائتلاف
Wargaming	بازی جنگ
Clube	باشگاه
Context	بافتار
Sector	بخش
Exploit	بهره‌برداری
Accounting	پاسخ‌گویی
Database	پایگاه داده
Base	پایه
Flag	پرچم
Research	پژوهش
Scan	پویش
Scanner	پویش‌گر
Advanced	پیشرفته
Prevention	پیش‌گیری
Trieaty	پیمان
Provider	تأمین‌کننده
State sponsored	تحت حمایت دولت
Analysis	تحلیل
Analyzer	تحلیل‌گر
Estimate	تخمین
Terrorist	تروریست
Detection	تشخیص
Decision	تصمیم
Decision Maker	تصمیم‌ساز
Picture	تصویر
Matching	تطبیق
Development	توسعه

Threat	تهدید
Threat-Oriented	تهدیدمحور
Log	ثبت وقایع
Espionage	جاسوسی
Crime	جرم
Toolkit	جعبه‌ابزار
Warfare	جنگ
Oriented	جهت‌دار
Framework	چارچوب
Cycle	چرخه
Stateful	حالت کامل
Privacy	حریم خصوصی
Rights	حقوق
Sponsored	حمایت شده
Attack	حمله
Termination	خاتمه
Service	خدمت
Baseline	خط مبنا
Well-Formed	خوش‌تعریف
Degree	درجه
Availability	دسترس‌پذیری
Assistant	دستیار
Hostile	دشمن
Defence	دفاع
Sequence	دنباله
Nation-state	دولت
State	دولت
FireWall	دیوار آتش
Strategic	راهبردی
TIER	رده
String	رشته

Language	زبان
Life	زندگی
Organization	سازمان
NATO	سازمان پیمان آتلانتیک شمالی (ناتو)
System	سامانه
Guard	سپر
Shield	سپر
Enumeration	سرشماری
Asset	سرمایه
Asset-Oriented	سرمایه‌محور
Platform	سکو
Health	سلامت
Scenario	سناریو
Simulator	شبیه‌ساز
Simulation	شبیه‌سازی
Severity	شدّت
Numbering	شماره‌گذاری
Identification	شناسایی
Reconnaissance	شناسایی
Identifier	شناسایی‌کننده هویت
Application	کاربرد
Applicability	کاربردپذیر
Exploit Code	کد بهره‌برداری
Access Control	کنترل دسترسی
Integrity	صحت، یکپارچگی
Impact	ضربه
Classification	طبقه‌بندی
Storm	طوفان
Non Repudiation	عدم انکار
Operation	عملیات
Formatted	فرمت‌شده

Cyber	فضای سایبر
Activity	فعالیت
Technology-Oriented	فناوری‌محور
Locked	قفل‌شده
Group	گروه
Dictionary	لغت‌نامه
Financial	مالی
Persistent	مانا، ماندگار
Uniform	متحدالشکل
Open Source	متن‌باز
Virtual	مجازی
Criminal	مجرم
Organized Cyber Criminal	مجرم سایبری سازمان‌یافته
Content	محتوا
Confidentiality	محرمانگی
Environment	محیط
Risk	مخاطره
Manager	مدیر
Managed	مدیریت شده
Center	مرکز
Centre of Excellence	مرکز نخبگان
Mercenary	مزدور
Competition	مسابقه
Cooperative	مشارکتی
Common	مشترک
Joint	مشترک
Specification	مشخصات
Criteria	معیار
Protocol	مقاوله‌نامه
National	ملی
Resource	منابع

Logical	منطقی
Required	موردنیاز
Success	موفقیت
Location	موقعیت
Insider	مهاجم خودی، مهاجم داخلی
Predisposing	مهیّا
Field	میدان
Range	میدان تمرین
Host	میزبان
Zone	ناحیه
Naming	نام‌گذاری
Excellence	نخبگان
Backup	نسخه پشتیبان
Intrusion	نفوذ
Penetration	نفوذ
Hacker	نفوذگر
Hacktivist	نفوذگر دارای انگیزه سیاسی
Exposure	نمایش
Approval	نمونه
Type	نمونه
Requirements	نیازمندی‌ها
Threat Event	واقعه‌ی تهدید
Alert	هشدار
Board	هیأت‌مدیره