راهنمای معماری امنیت سایبری

نویسنده
لستر نیکولز

ترجمه و تالیف
دکتر امیرحسین رحیمیان-وحید علمی
شاهین شاپوری-هادی پاکدامن

سرشناسه	:	رحیمیان، امیرحسین، ۱۳۵۳
عنوان و نام پدیدآور	:	راهنمای معماری امنیت سایبری، دکتر امیرحسین رحیمیان-وحید علمی- شاهین شاپوری-هادی پاکدامن
مشخصات نشر	:	تهران: فناوران لیان وابسته به شرکت مهرنا رایانه لیان،۱۴۰۳
مشخصات ظاهری	:	۵۷۶ ص.
شابک	:	۹۷۸-۶۲۲-۹۱۱۴۳-۱-۵
وضعیت فهرست‌نویسی	:	فیپا
موضوع	:	معماری امنیت سایبری
موضوع	:	امنیت سایبری
موضوع	:	جلوگیری از هک و نفوذ سایبری
موضوع	:	امنیت فاوا
موضوع	:	امنیت تبادل اطلاعات سازمان
موضوع	:	cybersecurity
شناسه افزوده	:	شرکت مهرنا رایانه لیان
رده‌بندی کنگره	:	
رده‌بندی دیویی	:	
شماره کتابشناسی ملی	:	

عنوان کتاب:	راهنمای معماری امنیت سایبری
ترجمه و تالیف:	دکتر امیرحسین رحیمیان- وحید علمی- شاهین شاپوری- هادی پاکدامن
نویسنده:	لستر نیکولز
ناظر فنی چاپ و تولید:	
ناشر:	انتشارات فناوران لیان وابسته به شرکت مهرنا رایانه لیان
ویراستار:	دکتر امیرحسین رحیمیان- وحید علمی- هادی پاکدامن
صفحه‌آرایی و طراحی جلد:	بهمن پازوکی
نوبت چاپ:	چاپ اول
شمارگان:	۱۰۰ نسخه
شابک:	۹۷۸-۶۲۲-۹۱۱۴۳-۱-۵
قیمت:	۶۹۰۰۰۰۰ ریال
تلفن مرکز پخش:	۰۲۱۹۱۰۰۴۱۵۱
پایگاه اینترنتی:	www.liangroup.net/home/pub
پست الکترونیکی:	pub@liangroup.net

فناوران لیان
وابسته به شرکت مهرنا رایانه لیان

انتشارات فناوران لیان وابسته به شرکت مهرنا رایانه لیان
تهران، خیابان خوش جنوبی، خیابان شاد، پلاک ۳

ISBN : 978-622-91143-1-5

9 786229 114315

در دنیای پیچیده و متصل به هم امروز، امنیت سایبری به یک چالش اساسی برای سازمان‌ها تبدیل شده است. با افزایش وابستگی به فناوری‌های اطلاعاتی و عملیاتی، تهدیدات سایبری نیز پیچیده‌تر و متنوع‌تر شده‌اند. در این میان، معماری امنیت سایبری به عنوان یک رویکرد جامع و ساخت‌یافته برای محافظت از دارایی‌های سازمان‌ها، از اهمیت ویژه‌ای برخوردار است.

کتاب «راهنمای معماری امنیت سایبری» نوشته Lester Nichols، یکی از منابع ارزشمند در این حوزه است که به صورت جامع و کاربردی به مباحث مختلف معماری امنیت سایبری می‌پردازد. این کتاب با زبانی ساده و روان، مفاهیم پیچیده امنیت سایبری را برای طیف گسترده‌ای از مخاطبان، از جمله متخصصان امنیت، مدیران فناوری اطلاعات و دانشجویان این حوزه، قابل فهم می‌سازد.

چرا این کتاب را ترجمه کردیم؟

نیاز روزافزون به منابع فارسی: با توجه به رشد روزافزون تهدیدات سایبری در کشورمان و اهمیت امنیت اطلاعات، نیاز به منابع آموزشی و مرجع به زبان فارسی بیش از پیش احساس می‌شود.

جامعیت و کاربردی بودن کتاب: کتاب حاضر به عنوان یک مرجع جامع، تمامی جنبه‌های معماری امنیت سایبری را پوشش می‌دهد و به خواننده کمک می‌کند تا یک درک عمیق از این حوزه کسب کند.

رویکرد عملیاتی کتاب: نویسنده در این کتاب، با ارائه مثال‌های عملی و مطالعات موردی، به خواننده کمک می‌کند تا مفاهیم تئوری را در دنیای واقعی پیاده‌سازی کند.

آشنایی نویسنده با حوزه: Lester Nichols یکی از متخصصان برجسته در حوزه امنیت سایبری است و تجربیات ارزشمندی در این زمینه دارد.

اهداف ترجمه

هدف اصلی از ترجمه این کتاب، انتقال دانش و تجربیات نویسنده به مخاطبان فارسی‌زبان و کمک به ارتقای سطح دانش و آگاهی آن‌ها در حوزه امنیت سایبری است. با مطالعه این کتاب، خوانندگان قادر خواهند بود:

مفاهیم پایه امنیت سایبری: مفاهیمی مانند تهدیدات سایبری، آسیب‌پذیری‌ها، ریسک، و کنترل‌های امنیتی را به طور کامل درک کنند.

اصول طراحی معماری امنیت سایبری: با اصول طراحی یک معماری امنیت سایبری قوی آشنا شوند و بتوانند یک معماری مناسب برای سازمان خود طراحی کنند.

بهترین روش‌ها: از جدیدترین روش‌ها و فناوری‌های مورد استفاده در امنیت سایبری آگاه شوند.

مقابله با تهدیدات نوظهور: با تهدیدات سایبری نوظهور آشنا شوند و روش‌های مقابله با آن‌ها را بیاموزند.

مخاطبان کتاب

مدیران فناوری اطلاعات: برای تدوین استراتژی‌های امنیتی و تصمیم‌گیری‌های کلیدی در حوزه امنیت سایبری.

متخصصان امنیت اطلاعات: برای ارتقای دانش فنی خود و آشنایی با آخرین روش‌ها و فناوری‌ها.

دانشجویان رشته‌های مرتبط: برای درک عمیق‌تر مفاهیم امنیت سایبری و آمادگی برای ورود به بازار کار.

کارآفرینان و صاحبان کسب‌وکار: برای محافظت از دارایی‌های دیجیتال کسب‌وکار خود.

در پایان، امیدواریم که ترجمه این کتاب بتواند گامی موثر در جهت ارتقای سطح امنیت سایبری در کشورمان بردارد.

مقدمه

در دنیای پیچیده و متصل به هم امروز، امنیت سایبری به یک چالش اساسی برای سازمان‌ها تبدیل شده است. با افزایش وابستگی به فناوری‌های اطلاعاتی و عملیاتی، تهدیدات سایبری نیز پیچیده‌تر و متنوع‌تر شده‌اند. در این میان، معماری امنیت سایبری به عنوان یک رویکرد جامع، کلان‌نگر و ساختاریافته برای محافظت از دارایی‌های سازمان‌ها، از اهمیت ویژه‌ای برخوردار است. کتاب "راهنمای معماری امنیت سایبری" نوشته Lester Nichols، یکی از منابع ارزشمند در این حوزه است که به صورت جامع و کاربردی به مباحث مختلف معماری امنیت سایبری می‌پردازد. این کتاب با زبانی ساده و روان، مفاهیم پیچیده امنیت سایبری را برای طیف گسترده‌ای از مخاطبان، از جمله متخصصان امنیت، مدیران فناوری اطلاعات و دانشجویان این حوزه، قابل فهم می‌سازد.

چرا این کتاب را ترجمه و تالیف کردیم؟

• نیاز روزافزون به منابع فارسی: با توجه به رشد روزافزون تهدیدات سایبری در کشورمان و اهمیت امنیت اطلاعات، نیاز به منابع آموزشی و مرجع به زبان فارسی بیش از پیش احساس می‌شود.

•جامعیت و کاربردی بودن کتاب: کتاب حاضر به عنوان یک مرجع جامع، تمامی جنبه‌های معماری امنیت سایبری را پوشش می‌دهد و به خواننده کمک می‌کند تا یک درک عمیق از این حوزه کسب کند و مسیر راه رشد و تعالی خود را پیدا کند.

•رویکرد عملیاتی کتاب: نویسنده در این کتاب، با ارائه مثال‌های عملی و مطالعات موردی، به خواننده کمک می‌کند تا مفاهیم تئوری را در دنیای واقعی پیاده‌سازی کند.

•آشنایی نویسنده با حوزه: Lester Nichols یکی از متخصصان برجسته در حوزه امنیت سایبری است و تجربیات ارزشمندی در این زمینه دارد و کتاب فوق در بسیاری از مراکز علمی دنیا به عنوان کتاب مرجع معماری امنیت سایبری استفاده می شود.

اهداف ترجمه

هدف اصلی از ترجمه و تالیف این کتاب، انتقال دانش و تجربیات نویسنده به مخاطبان فارسی‌زبان و کمک به ارتقای سطح دانش و آگاهی آن‌ها در حوزه امنیت سایبری است. همچنین مترجمان کتاب که از متخصصان و صاحب نظران حوزه آموزش و خدمات امنیت سایبری هستند، تجارب و دانش عملی خود را که طی سالیان دراز فعالیت تحت عنوان گروه لیان (مهرنا رایانه لیان) اندوخته‌اند، در اختیار مخاطب کتاب قرار می‌دهند. با مطالعه این کتاب، خوانندگان قادر خواهند بود:

• مفاهیم پایه امنیت سایبری: مفاهیمی مانند تهدیدات سایبری، آسیب‌پذیری‌ها، ریسک، و

کنترل‌های امنیتی را به طور کامل درک کنند.

• اصول طراحی معماری امنیت سایبری: با اصول طراحی یک معماری امنیت سایبری قوی آشنا شوند و بتوانند یک معماری مناسب برای سازمان خود طراحی کنند.

• به‌روش‌ها: از جدیدترین روش‌ها و فناوری‌های مورد استفاده در امنیت سایبری آگاه شوند.

• با تهدیدات نوظهور: با تهدیدات سایبری نوظهور آشنا شوند و روش‌های مقابله با آن‌ها را بیاموزند.

• راه رشد و تعالی به سمت معمار امنیت سایبری سازمانی را طی کنند.

• طراحی معماری امنیت سایبری سازمانی را تدریس کنند.

مخاطبان کتاب

•مدیران ارشد و میانی فناوری اطلاعات: برای تدوین استراتژی‌های کوتاه‌مدت، میان‌مدت و بلندمدت امنیتی و تصمیم‌گیری‌های کلیدی و زیرساختی در حوزه امنیت سایبری سازمان.

• متخصصان امنیت اطلاعات: برای ارتقای دانش فنی خود و آشنایی با آخرین روش‌ها و فناوری‌ها و حرکت به سوی سطوح عالی معماری امنیت سایبری سازمانی.

• دانشجویان رشته‌های مرتبط: برای درک عمیق‌تر مفاهیم امنیت سایبری و آمادگی برای ورود به بازار کار.

• کارآفرینان و صاحبان کسب‌وکار: برای محافظت از دارایی‌های دیجیتال کسب‌وکار خود.

•محققان و دانش‌پژوهان و پژوهشکده‌های امنیت سایبری جهت استفاده در مقالات و تحقیقات و کتب علمی مرتبط و تدوین استراتژی‌های دفاع سایبری کلان و تدوین مدل‌های بلوغ سایبری سازمان.

در پایان، امیدواریم که ترجمه و تالیف این کتاب بتواند مورد توجه مخاطبان قرار گرفته و گامی موثر در جهت انتقال دانش، ارتقای سطح امنیت سایبری و تقویت زیرساخت دفاع سایبری در کشورمان بردارد.

ازمخاطبان و همراهان گرامی درخواست می شود ما را از نظرات و رهنمودهای ارزشمندشان بهرمند سازند تا کاستی‌های کتاب در نسخه های آتی برطرف گردد.

گروه لیان

از ابتدای تاسیس تا کنون، در کنار فعالیت‌های آموزشی تولید محتوای ناب و انتشار رسانه‌های مکتوب و دیجیتال چه در قالب تدوین و تالیف و ترجمه و تحقیق و چه در قالب محتوای دیجیتال، از جمله اهداف بنیادین شرکت مهرنا رایانه لیان بوده و از جمله معدود شرکت‌هایی است که به طور تخصصی در این حوزه سرمایه‌گذاری و تولید محتوا کرده است. با توجه به کمبود محتوای ناب در حوزه امنیت سایبری این شرکت در سال ۱۴۰۲ اقدام به اخذ مجوز انتشارات به نام فناوران لیان نمود و به‌طور تخصصی به چاپ و نشر کتاب و مقالات و منابع علمی در حوزه فناوری اطلاعات خصوصا امنیت سایبری می‌پردازد.

همچنین به موازات فعالیت در بخش تولید محتوا و نشر کتب تخصصی، این شرکت با اخذ مجوز آموزشگاه تخصصی امنیت سایبری از سازمان فنی و حرفه‌ای استان تهران، دوره‌های تخصصی امنیت فناوری اطلاعات (امنیت سایبری) را نیز تحت عنوان آموزشگاه مهرنا رایانه لیان برگزار کرده و مجموعه کاملی از دوره‌های عمومی و تخصصی در حوزه امنیت سایبری را ارایه می‌کند.

رویکرد آموزشی مدرن بر بستر کلاس‌های مجازی، حضوری و ترکیبی و استفاده از اساتید مجرب و کارآزموده و انتقال تجربه کاری در کنار تدریس مباحث نظری و برگزاری کارگاه‌های عملی و همچنین طراحی و ارایه دوره‌های تخصصی و متناسب با نیاز بازار کار، ایجاد پل ارتباطی بین دانشجویان و کارفرمایان، مشاوره و منتورینگ تا زمان موفقیت و هدایت به بازار کار از جمله مزیت‌های کلیدی این مجموعه بحساب می‌آید. بدین‌وسیله از مترجمان، محققان، نویسندگان و علاقه‌مندان به تولید محتوای ناب و همچنین از اساتید و متخصصان گرامی جهت همکاری در بخش انتشارات و تدریس در آموزشگاه لیان دعوت به همکاری می‌گردد.

فهرست:

فصل ۵:

فصل ۶:

فصل ۹

فصل ۱۰

فصل ۱۱

فصل ۱۳

فصل ۱۴

مقدمه و پیشگفتار:

راهنمای معماری امنیت سایبری

در دنیایی که وابستگی سازمان‌ها به فناوری‌های به‌هم‌پیوسته به‌طور مداوم در حال افزایش است، تهدیدات سایبری منشأ خطرات بسیاری است، بااین‌حال اقدامات امنیتی اغلب از این تهدیدات عقب می‌مانند. این کتاب به‌گونه‌ای طراحی شده است تا شما را برای پاسخ به این نیاز آماده کند.

این کتاب، راهنمای جامع و کاربردی برای متخصصان فناوری اطلاعات و امنیت است تا آنان را به معماران حرفه‌ای امنیت سایبری تبدیل کند. معماران امنیت سایبری قادرند تدابیر دفاعی استراتژیک متناسب با محیط‌ها و نیازهای خاص را طراحی و توسعه دهند.

این کتاب با پرداختن به مباحث بنیادین، مسیرهای شغلی و پیشرفت‌های حوزه امنیت سایبری، اصول امنیت سایبری را در کنار پیاده‌سازی آن در دنیای واقعی به‌طور عمیق تشریح می‌کند.

فصل‌های ابتدایی دانش پایه‌ای حیاتی در مورد مفاهیم کلیدی مانند محرمانگی، شبکه‌سازی، مدیریت ریسک و انطباق را پوشش می‌دهد. سپس مباحث به سمت هدایت مسیر شغلی به‌عنوان یک معمار امنیت سایبری پیش می‌رود و مهارت‌های اساسی مانند مستندسازی، مدیریت فروشندگان و همکاری تیمی توضیح داده می‌شود.

در ادامه، فرایندهای انتخاب و پیاده‌سازی کنترل‌ها، همسو کردن امنیت با اهداف تجاری و پرورش انطباق‌پذیری شخصی در میان تغییرات مداوم تشریح می‌شود.

در سراسر کتاب، تأکید بر جنبه‌های عملی و قابل‌اجراست و نظریه‌ها با استفاده از مثال‌های ملموس از محیط‌های سازمانی مختلف جان می‌گیرند. آزمایشگاه‌ها، نمودارها و تمرین‌ها شما را با به‌کارگیری مستقیم مفاهیم درگیر می‌کنند. افراد تازه‌وارد به امنیت سایبری جهت‌گیری ضروری را به دست می‌آورند، درحالی‌که متخصصان فعلی با دیدگاه‌های جدیدی آشنا می‌شوند.

مخاطب این کتاب چه کسانی هستند؟

این کتاب برای افراد زیر توصیه می‌شود:

• **مدیران فناوری اطلاعات:** کسانی که مسئولیت مدیریت سیستم‌های فناوری اطلاعات یک سازمان را بر عهده دارند، می‌توانند از این کتاب برای بهبود امنیت زیرساخت‌های خود استفاده کنند.

• **تحلیلگران امنیت:** این کتاب به تحلیل‌گران امنیت کمک می‌کند تا دانش خود را در مورد طراحی و پیاده‌سازی معماری امنیت سایبری گسترش دهند.

• **توسعه‌دهندگان:** توسعه‌دهندگان می‌توانند بامطالعه این کتاب، ملاحظات امنیتی را در فرایند توسعه نرم‌افزار یکپارچه‌سازی کنند.

• **مدیرانی که به دنبال ترقی به سطح معمار امنیت سایبری هستند:** این کتاب مسیر شغلی برای تبدیل‌شدن به یک معمار امنیت سایبری را ترسیم می‌کند.

بااین‌حال، هر متخصص فناوری که به دنبال طراحی ساختار دفاع سایبری جامع است، این کتاب را شفابخش خواهد یافت. این کتاب با تجهیز معماران به راه‌حل‌های استراتژیک متناسب با چشم‌اندازهای منحصربه‌فرد ریسک، به خوانندگان تازه‌کار و باتجربه این امکان را می‌دهد تا معماری‌های خود را برای ایمن‌سازی در دنیایی که به‌شدت به سمت دیجیتالی‌شدن حرکت می‌کند، آماده کنند.

گروه مخاطبان اصلی به شرح زیر هستند:

سه گروه اصلی مخاطب این کتاب است که در ادامه به آن‌ها اشاره می‌شود (مدیران فناوری اطلاعات، تحلیل‌گران امنیت، توسعه‌دهندگان) اما این کتاب برای هر فردی که در حوزه فناوری فعالیت می‌کند و به دنبال طراحی حفاظت‌های جامع است نیز مفید خواهد بود.

برای افراد مبتدی در حوزه امنیت سایبری یا فناوری اطلاعات

این کتاب به‌ویژه برای کسانی که تازه‌وارد به امنیت سایبری یا فناوری اطلاعات هستند و به دنبال ترسیم مسیر شغلی یا بهبود مسیر فعلی خود به سمت امنیت سایبری هستند، مناسب است. اگر در ابتدای ورود به دنیای فناوری یا امنیت سایبری هستید، این کتاب جهت‌گیری مهمی را برای شما فراهم می‌کند. فرقی نمی‌کند که از زمینه‌ای غیرفنی وارد این حوزه شده باشید یا به‌تازگی مسیر شغلی خود را در این زمینه آغاز کرده باشید، این کتاب نقشه راهی را برای تبدیل‌شدن به یک معمار امنیت سایبری حرفه‌ای پیش‌روی شما ترسیم می‌کند.

متخصصان فناوری اطلاعات که به دنبال تغییر مسیر به معمار امنیت سایبری هستند

این کتاب برای متخصصان فناوری اطلاعات فعلی در هر سطحی که به دنبال انتقال به سمت امنیت سایبری و به‌طور خاص به سمت معماری امنیت سایبری هستند، ایده‌آل است. برای متخصصان باتجربه فناوری اطلاعات مانند مدیران سیستم، مهندسان شبکه یا توسعه‌دهندگان نرم‌افزار که به دنبال انتقال به امنیت سایبری هستند، این کتاب مفاهیم آشنا و معماری متمرکز بر امنیت را به هم پیوند می‌دهد.

متخصصان فعلی در حوزه امنیت سایبری

این کتاب برای افراد حرفه‌ای فعلی در امنیت سایبری یا معماران امنیت سایبری سطح ابتدایی که به دنبال ارتقا و رشد در این زمینه و شغل خود هستند نیز مفید است. برای متخصصان امنیت سایبری که در ابتدای مسیر هستند، مانند تحلیل‌گران یا معماران سطح پایین، این کتاب مسیرهایی را برای دستیابی به مسئولیت‌های بیشتر و رهبری و رسیدن به مناصب عالی ارائه می‌دهد.

این کتاب چه موضوعاتی را پوشش می‌دهد

فصل‌هایی که در این کتاب مطرح می‌شود:

- **فصل ۱: مقدمه‌ای بر امنیت سایبری:**

مفاهیم اولیه و پایه امنیت سایبری را ارائه می‌دهد و نحوه ارتباط آن با نقش معمار امنیت سایبری را توضیح می‌دهد. این فصل هم برای افراد مبتدی در حوزه امنیت سایبری و هم برای کسانی که تا حدودی در این حوزه یا فناوری اطلاعات تجربه دارند، مفید است.

- **فصل ۲: مبانی امنیت سایبری:**

باتکیه‌بر مقدمه، به جزئیات بیشتری در سطح پایه می‌پردازد. این فصل برخی از حوزه‌های اصلی را که یک معمار امنیت سایبری باید در ارتباط با تیم‌های تجاری و عملیاتی دیگر درک کند، موردبحث قرار می‌دهد. این مبحث به‌طور خلاصه ارائه می‌شود، اما جنبه‌های اساسی برای پیشرفت به سمت بحث در مورد مسیر شغلی امنیت سایبری و گزینه‌های موجود برای معماران بالقوه امنیت سایبری جهت تخصص در یک حوزه خاص را فراهم می‌کند.

- **فصل ۳: معمار امنیت سایبری کیست و مسئولیت‌های او چیست؟**

این فصل با این فرضیه آغاز می‌شود که شما درک کافی از امنیت سایبری برای بحث در مورد

نقش معمار امنیت سایبری و چگونگی تکیه بر سایر نقش‌های فناوری دارید. چه این نقش در حوزه معماری سازمانی، برنامه کاربردی و یا شبکه یا پلتفرم باشد، این حوزه‌ها تمرکزهای متفاوتی دارند که همه چیز را از یک کل به یک زیرمجموعه خاص توسعه می‌دهند. پس از تعریف چارچوب معمار، مسئولیت‌ها باتوجه‌به حوزه خاص تمرکز یا سازمان آشکارتر می‌شوند.

- **فصل ۴: اصول، طراحی و تحلیل معماری امنیت سایبری:**

مفاهیم اساسی برای معماری امنیت سایبری، ازجمله اصول، طراحی و تحلیل را ارائه می‌دهد. این فصل بر استفاده از اصطلاحات واضح و ترسیم اهداف سازمان و تحمل ریسک به‌عنوان ورودی‌های کلیدی برای شکل‌دهی معماری تأکید می‌کند.

- **فصل ۵: ملاحظات تهدید، ریسک و حاکمیت به‌عنوان یک معمار:**

توضیح می‌دهد که تهدید، ریسک و حاکمیت چگونه بر تصمیمات مربوط به معماری تأثیر می‌گذارند. این فصل رویکردهای مختلف برای طراحی و تحلیل راه‌حل‌ها یا کنترل‌های امنیتی را موردبحث قرار می‌دهد و در انتخاب کنترل‌های مناسب بر اساس موقعیت، راهنمایی ارائه می‌کند.

- **فصل ۶: مستندسازی به‌عنوان یک معمار امنیت سایبری:**

این فصل کمی از مباحث عمیق‌تر فاصله می‌گیرد و به اهمیت مستندسازی مناسب در نقش معمار امنیت سایبری می‌پردازد. در این فصل به‌ضرورت جزئی‌نگری و رویکرد دقیق به مستندسازی از طریق ابزارهایی مانند Microsoft Visio یا Draw.io و سایر ابزارهای مشابه پرداخته می‌شود. همچنین نحوه مستندسازی و/یا ایجاد یادداشت‌ها با استفاده از ابزارهایی مانند CherryTree موردبحث قرار خواهد گرفت. هدف از همه این موارد کمک به ارتقای شفافیت راه‌حل‌ها و طراحی معماری نه‌تنها در داخل سازمان، بلکه برای الزامات نظارتی و انطباقی است.

- **فصل ۷: نقشه راه برای رسیدن به سطح معمار:**

این فصل مسیر رسیدن به جایگاه عالی‌رتبه یک معمار امنیت سایبری را شرح می‌دهد. بدیهی است که برخی مسیرهای شغلی برای رسیدن به جایگاه معمار امنیت سایبری مستقیم‌تر از سایر مسیرها هستند. همان‌طور که در اکثر حوزه‌های فناوری صادق است، پاسخ رایج می‌تواند «بستگی دارد» باشد. این فصل رویکردهای مختلفی را برای کسب تجربه یا مهارت لازم برای تبدیل‌شدن به یک معمار امنیت سایبری ارائه می‌دهد. چه شروع به‌عنوان تکنسین فناوری اطلاعات باشد و

چه انتقال از یک توسعه‌دهنده، مهارت‌های مشترکی وجود دارد که باید برای شکل‌دهی مسیر این حرفه به‌دست‌آمده یا به کار گرفته شود.

• فصل ۸: معضل صدور گواهینامه:

این فصل تعدادی از گواهینامه‌های مربوط به معماری امنیت، و همچنین سایر گواهینامه‌هایی را که برای تمایز خود از سایر افرادی که برای همان موقعیت رقابت می‌کنند نیاز دارید، موردبحث قرار می‌دهد. همچنین به جنبه‌های خوب، بد و زشت فرایند صدور گواهینامه و نحوه انتخاب‌هایی که بهترین تطابق را با برنامه و جهت کلی شغلی شما داشته باشند، می‌پردازد.

• فصل ۹: مرتب‌سازی جعبه‌ابزار - بخش ۱:

استراتژی‌هایی را برای معماران امنیت سایبری جهت مونتاژ هوشمندانه جعبه‌ابزار امنیتی خود با ارزیابی راه‌حل‌ها برای یافتن تناسب بهینه با چشم‌انداز تهدید خاص سازمان، نیازهای تجاری و محدودیت‌های عملیاتی آن‌ها بررسی می‌کند. این فصل بررسی اجمالی از دسته‌های اصلی ابزارهای امنیتی مانند مدل‌سازی تهدید، نظارت شبکه، محافظت از نقاط انتهایی، مدیریت دسترسی به هویت، رمزگذاری داده‌ها، مدیریت آسیب‌پذیری و موارد دیگر ارائه می‌دهد. این فصل بر تطبیق اقدامات دفاعی با آسیب‌پذیری‌ها و ریسک‌های خاص سازمان به‌جای رویکرد یکسان برای همه تأکید می‌کند.

• فصل ۱۰: مرتب‌سازی جعبه‌ابزار - بخش ۲:

بر اهمیت انتخاب هوشمندانه ابزارهای امنیت سایبری متناسب با آسیب‌پذیری‌ها، زیرساخت و اهداف استراتژیک منحصربه‌فرد یک سازمان تأکید می‌کند. این فصل توصیه می‌کند قبل از ارزیابی ابزارها، رویکردی منظم برای شناسایی شکاف‌های امنیتی و الزامات خاص در پیش گرفته شود. هم‌راستا بودن با چارچوب‌هایی مانند NIST CSF، اجرای دفاع‌های لایه‌بندی‌شده، سنجش عوامل تجاری مانند هزینه و قابلیت استفاده، و آینده‌نگری در انتخاب‌ها، به‌عنوان عوامل حیاتی برای ساخت یک جعبه‌ابزار بهینه، برجسته می‌شوند.

• فصل ۱۱: به‌روش‌ها:

به جزئیات به‌روش‌ها در ارتباط با امنیت سایبری می‌پردازد و توضیح می‌دهد که چرا بهترین کار این است که راه‌حل‌ها را با استفاده از به‌روش‌ها اجرا کرد. این موضوع شامل استفاده از استانداردها یا به‌روش‌های خاص فناوری است. این فصل همچنین در مورد شرایطی که ممکن است یک شیوه بر

دیگری ارجحیت داشته باشد و چرا ممکن است با چنین سناریویی مواجه شوید، بحث خواهد کرد.

• فصل ۱۲: انعطاف‌پذیری به‌عنوان یک معمار امنیت سایبری:

این فصل به بررسی چگونگی پرورش انعطاف‌پذیری شخصی و حرفه‌ای معماران برای پیاده‌سازی راه‌حل‌های عملیاتی متناسب با محیط‌های کسب‌وکار و اهداف منحصربه‌فرد می‌پردازد. این فصل باتکیه‌بر مفاهیم پیشین، بر این نکته تأکید می‌کند که پایبندی خشک به امنیت «ایده‌آل» اغلب با شکست مواجه می‌شود، درحالی‌که رویکردهای قابل‌تنظیم به موفقیت می‌رسند. موضوعات این فصل شامل پرورش طرز فکر و استراتژی‌هایی برای طراحی محافظت در راستای گردش کار، مدیریت محتاطانه ریسک و برقراری تعادل برای تسهیل بهره‌وری و نوآوری است. معماران یاد می‌گیرند که چگونه با انعطاف‌پذیری و جامع‌نگری بیشتر، رشد حرفه‌ای خود را تسریع بخشند و درعین‌حال نوآوری جسورانه را از طریق امنیتی که با نیازهای در حال تحول سازگار می‌شود، تقویت نمایند.

• فصل ۱۳: ملاحظات معماری – طراحی، توسعه و سایر استراتژی‌های امنیتی – بخش ۱:

بر رشته‌های اصلی که معماران امنیت سایبری را قادر می‌سازد تا نیازهای سازمانی را به راه‌حل‌های فنی سفارشی‌شده ترجمه کنند، تمرکز می‌کند. این فصل بر هم‌راستا کردن امنیت با اهداف کسب‌وکار در مراحل اولیه مفهوم‌سازی و طراحی تأکید می‌کند.

• فصل ۱۴: ملاحظات معماری – طراحی، توسعه و سایر استراتژی‌های امنیتی – بخش ۲:

به‌عنوان یک جمع‌بندی کلی، مفاهیم مختلف معماری امنیت سایبری را که در کتاب پوشش داده شده است، به هم پیوند می‌دهد. این فصل بر این نکته تأکید می‌کند که معماران علاوه بر تخصص فنی، باید انعطاف‌پذیری لازم برای پذیرش چارچوب‌های امنیتی در میان تغییرات مداوم را نیز داشته باشند.

برای بهره‌مندی بیشتر از این کتاب استفاده از موارد زیر توصیه می‌شود:

Software/hardware covered in the book	Operating system requirements
Kali Linux	Windows, macOS, or Linux
Snort	Processor: Minimum 4 cores/Best results with 8+ cores
OPNsense	Memory: Minimum 16 GB/recommended 32+ GB
Ansible	Storage: Minimum 500 GB/recommended 1 TB
Graylog	Hypervisor: VMware Workstation/Fusion/Oracle VirtualBox/Qemu/Proxmox
Veracrypt	
OpenVAS/Greenbone	
AWS	
StackStorm	
SecurityOnion	
ClamAV	
OWASP ZAP and Threat Dragon	
Microsoft Threat Modeling Tool	

قسمت اول:
مبانی

معماری امنیت سایبری نیازمند تلفیقی از دیدگاه عمیق استراتژیک و جزئیات فنی است. پیش از پرداختن به جزئیات پیاده‌سازی، ترسیم یک بنیان فکری مستحکم ضروری است. بخش ابتدایی این کتاب بر آشنایی شما با مفاهیم، اصول و حوزه‌های اساسی که زیربنای معماری مؤثر امنیت سایبری هستند، تمرکز دارد.

• فصل ۱: این فصل مروری کلی است بر اصول کلیدی امنیت سایبری و تشریح این موضوع که چرا امنیت در چشم‌انداز فناوری‌های درهم‌تنیده روزافزون اهمیت دارد.

• فصل ۲: این فصل به حوزه‌های بنیادی شامل کنترل دسترسی، امنیت شبکه، رمزنگاری و مدیریت ریسک می‌پردازد. مثال‌های عملی نشان می‌دهند که چگونه هر یک از این موارد به حفاظت چندلایه کمک می‌کند.

• فصل ۳: با قرار دادن بلوک‌های اصلی در جای خود، این فصل وظایف و نقش‌هایی که یک معمار امنیت سایبری ایفا می‌کند را مشخص می‌کند. این فصل همچنین هم‌افزایی‌ها و چالش‌های موجود بین استراتژی‌های امنیتی و اهداف تجاری را که معماران باید نقطه تعادل آن‌ها را پیدا کنند، بررسی می‌کند.

در این فصل‌ها شما به دانش اولیه امنیت مجهز می‌شوید و نقش معمار در ذهن شما به تصویر کشیده می‌شود. با پایه‌گذاری مباحث بنیادین در بستر محیط سایبری، این بخش شما را در راستای کشف مسیرهایی برای توسعه استراتژیک معماری امنیت سایبری مطابق با نیازهای خاص سازمانی آماده می‌کند. حتی کسانی که قبلاً با این مفاهیم آشنا هستند، از مرور مفاهیم اساسی و بنیادین آخرین چارچوب‌ها، کنترل‌ها و به‌روش‌های ارائه شده، بهره‌مند خواهند شد.

فصل‌های این بخش:

- **فصل ۱:** مقدمه‌ای بر امنیت سایبری
- **فصل ۲:** مبانی امنیت سایبری
- **فصل ۳:** معمار امنیت سایبری کیست و مسئولیت‌های او چیست؟

فصل ۱
مقدمه‌ای بر امنیت سایبری

در دنیای درهم‌تنیده امروز، به‌سختی می‌توان روزی را به شب رساند و خبری در مورد امنیت سایبری نشنید یا ناخواسته کاری مرتبط با آن انجام نداد. چه مربوط به تنظیم مجدد اجباری رمز عبور حساب کاربری شما در محل کار باشد، چه اطلاعیه‌ای مرتبط با نقض و انتشار داده‌ها، افراد در تمام سطوح مجبور به کلنجار با مفاهیم امنیت سایبری هستند. به همین دلیل است، و جای تعجب ندارد که امنیت سایبری به یک انتخاب محبوب شغلی و با تقاضای روبه‌رشد تبدیل شده است که بازار با کمبود شدید آن مواجه است.

بر اساس آمار اداره کار ایالات‌متحده، انتظار می‌رود بین سال‌های ۲۰۲۱ تا ۲۰۲۳ رشد ۳۵ درصدی در مشاغل امنیت سایبری وجود داشته باشد. طبق گزارش Cybersecurity Ventures[1] به‌طور بالقوه ۳.۵ میلیون کمبود نیروی متخصص امنیت سایبری در سراسر جهان وجود دارد.

این به چه معناست؟ این بدان معناست که نه‌تنها صنعت امنیت سایبری از بین نخواهد رفت؛ بلکه فرصت‌های شغلی موجود و رقابت برای آن مشاغل افزایش شدیدی خواهد یافت. به‌عبارت‌دیگر افراد، و به‌طور خاص افرادی که این کتاب را می‌خوانند، فقط به دنبال یک شغل نخواهند بود، بلکه به دنبال حرفه‌ای در حوزه‌ای هستند که می‌تواند فرصت‌های رشد و توسعه فردی و سازمانی زیادی را پیش پای آنان فراهم کند.

بالاترین سطح یک حرفه فنی امنیت سایبری، معمار امنیت سایبری (CSA)[2] است. او نقشی دارد که به شکل‌دهی، طراحی و برنامه‌ریزی جنبه‌های فنی رویکرد امنیتی یک سازمان در تمام

1. Cybersecurity Ventures (www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report)
2. Cyber security Architect (CSA)

سطوح کمک می‌کند. این فصل مفاهیم و اصول اولیه را برای درک مفاهیم امنیت سایبری و درنهایت نحوه ارتباط آن با نقش معمار امنیت سایبری ارائه می‌دهد. این کار مسیری در سطح مقدماتی را برای کسانی که تازه‌وارد امنیت سایبری شده‌اند، فراهم می‌کند و همچنین یک تصویر کلی بنیادین را برای کسانی که مدتی است در حوزه امنیت سایبری یا فاوا کار می‌کنند، ارائه می‌دهد.

در این فصل، ما در مورد موضوعات اصلی زیر صحبت خواهیم کرد:

- امنیت سایبری چیست؟
- محرمانگی/یکپارچگی/دسترس‌پذیری
- شبکه و سیستم‌عامل‌ها
- برنامه‌های کاربردی
- حاکمیت، مقررات و انطباق[۳]

در دنیای واقعی، برای درک کامل اصول اولیه امنیت سایبری، به متنی طولانی‌تر و با جزئیات بیشتری نسبت به آنچه در این فصل خواهید یافت، نیاز است. بااین‌حال، منابع اضافی (کتاب‌ها و منابع آنلاین) وجود دارند که می‌توانند درک عمیق‌تری از مفاهیمی که در این فصل به آن‌ها اشاره شده است، ارائه دهند. این منابع را در بخش «مطالعه بیشتر» در انتهای این فصل خواهید یافت.

علاوه بر این، درحالی‌که بخش ۱ (فصل‌های ۱ تا ۳) ممکن است برای برخی تکراری باشد، اما برای هر خواننده، چه مبتدی و چه حرفه‌ای باتجربه، ضروری است که سنگ بنایی مستحکم برای بحث در مورد معمار امنیت سایبری ایجاد شود. به همین دلیل، کسانی که با مطالب مقدماتی آشنا هستند می‌توانند به بخش ۲ بروند.

امنیت سایبری چیست؟

کتاب‌های زیادی در مورد امنیت سایبری نوشته شده است. این بخش قرار نیست یک رسالهٔ دکتری در مورد امنیت سایبری باشد، بلکه بیشتر یک بررسی اجمالی برای ارائه اطلاعات بنیادین در مورد موضوعات آتی کتاب است. درنتیجه، ما به‌طور دوره‌ای به سایر مطالب یا کتاب‌ها اشاره می‌کنیم تا به شما امکان دهیم در مورد موضوعات خاص، برای جلوگیری از تبدیل‌شدن این کتابچه راهنما به یک کتاب قطور، عمیق‌تر مطالعه کنید.

باید بپذیریم که بسته به اینکه از چه کسی بپرسید، تعاریف مختلفی از امنیت سایبری به دست خواهید آورد. این تعاریف می‌تواند از محافظت از سیستم‌ها، شبکه‌ها و برنامه‌ها در برابر حملات

3. Governance, regulations, and compliance (GRC)

سایبری تا کاهش سطح ریسک یک سازمان یا حتی نام‌گذاری امنیت سایبری با نام دیگری مانند تضمین اطلاعات و موارد دیگر متغیر باشد.

دلیل وجود تعاریف یا مترادف‌های مختلف به دیدگاه فرد یا سازمانی برمی‌گردد که تعریف یا نقطه تمرکز بحث را ارائه می‌دهد. همچنین به این معنا نیست که همه تعاریف مختلف نادرست هستند (زیرا درواقع اکثر آن‌ها نادرست نیستند) اما بر تمرکز و اولویت‌های متفاوت دررابطه‌با امنیت سایبری تأکید می‌کند.

طبق تعریف آژانس امنیت سایبری و زیرساخت امنیت سایبری ایالات‌متحده (CISA)[۴]، امنیت سایبری به‌عنوان «هنر محافظت از شبکه‌ها، دستگاه‌ها و داده‌ها در برابر دسترسی غیرمجاز یا استفاده مجرمانه و حصول اطمینان از محرمانگی، صحت و دردسترس‌بودن اطلاعات» تعریف می‌شود.

در عمل، این بدان معناست که شما به‌عنوان یک فرد یا کسب‌وکار، در حال تلاش برای انجام هر کاری یا کسب‌وکاری به امن‌ترین و کارآمدترین شکل ممکن هستید بدون اینکه در هزینه‌های مربوط به امنیت زیاده‌روی کنید.

رشد رایانه‌ها، برنامه‌های کاربردی مبتنی بر وب و فناوری اطلاعات انفجاری بوده است. انتشار اطلاعات در سراسر جهان هرگز به‌سرعت و آسانی امروز در دسترس نوک انگشتان افراد نبوده است و این روند همچنان سریع‌تر خواهد شد. فناوری مزایای فراوانی برای تمام جنبه‌های جامعه به ارمغان آورده است، اما متأسفانه فناوری روی تاریکی نیز دارد.

این روی تاریک به شکل سرقت داده‌ها، مجرمین سایبری، باج‌گیری، سرقت هویت و موارد بسیار دیگری خود را نشان می‌دهد. امنیت سایبری با ایمن‌سازی ارتباطات، برنامه‌های کاربردی، دسترسی فیزیکی و غیره سعی دارد جلوی این روی تاریک فناوری را بگیرد یا از آن جلوگیری کند.

واقعیت این است که تنها سیستم رایانه‌ای که واقعاً ایمن است، سیستمی است که هرگز روشن یا استفاده نمی‌شود. به‌محض اینکه آیفون جدید خود را فعال کنیم، تبلت یا رایانه جدید را راه‌اندازی کنیم یا به اینترنت متصل شویم، در حال شمارش معکوس برای افزایش ریسک‌ها و کاهش امنیت دستگاه یا برنامه هستیم.

می‌توانستیم یک ساختمان یا قلعه تقریباً نفوذناپذیر با خندق بسازیم، اما این کار زندگی یا تجارت را آسان‌تر نمی‌کند و از آسیب‌پذیری‌ها یا ریسک‌های مرتبط با برنامه‌ها یا سیستم‌هایی که استفاده می‌کنیم، جلوگیری نمی‌کند.

پیش‌ازاین، می‌توانستیم اقدامات دفاعی را در محدوده فناوری سنتی به‌طور افراطی انجام

4. Cybersecurity & Infrastructure Security Agency (CISA)

دهیم. اما امروزه و در آینده قابل‌پیش‌بینی، سیاست‌هایی مانند دورکاری و استفاده از دستگاه شخصی مرزهایی را که به‌طور سنتی تحت کنترل سازمان بود، مخدوش کرده‌اند و هدف بسیار گسترده‌تری را برای هکرها و بازیگران مخرب برای نفوذ یا کسب جای پا فراهم می‌کنند.

در عوض، باید راه‌حلی میانه پیدا کنیم که بیشترین امنیت را فراهم کند. این به امنیت داده‌هایی که ما به‌عنوان یک فرد، کسب‌وکار یا ترکیبی از هر دو ایجاد یا تغییر می‌دهیم، مربوط می‌شود. امنیت سایبری به دنبال برقراری تعادل قابل‌قبولی بین امنیت و ریسک‌هایی است که با آن‌ها مواجه هستیم.

با درنظرگرفتن این نکات، اکثر نهادهای صدور گواهینامه، انجمن‌ها و سازمان‌های دولتی مانند کنسرسیوم بین‌المللی صدور گواهینامه امنیت سیستم‌های اطلاعات [۵]، مرکز امنیت اینترنت [۶]، مؤسسه ملی فناوری و استانداردها [۷]، آژانس امنیت سایبری و زیرساخت امنیت سایبری و سایر سازمان‌ها، حوزه‌های مختلف یا گروه‌های موضوعی امنیت سایبری را به ترکیبی از موارد زیر تقسیم می‌کنند:

- **کنترل دسترسی:** مدیریت مجوزها و دسترسی کاربران به سیستم‌ها و داده‌ها.
- **توسعه امن نرم‌افزار:** ایجاد و نگهداری نرم‌افزار با درنظرگرفتن امنیت در کل فرایند توسعه.
- **برنامه‌ریزی تداوم کسب‌وکار/بازیابی فاجعه**[۸]: ایجاد استراتژی‌ها و روش‌هایی برای اطمینان از اینکه یک سازمان می‌تواند پس از یک حادثه به‌طور مؤثر به عملیات خود بازگردد.
- **رمزنگاری:** تبدیل اطلاعات به فرمی غیرقابل‌خواندن برای افراد غیرمجاز.
- **حاکمیت امنیت اطلاعات/مدیریت ریسک:** ایجاد و اجرای رویه‌هایی برای شناسایی، ارزیابی و مدیریت ریسک‌های امنیت اطلاعات.
- **حقوقی/تنظیم‌گری/انطباق و تحقیقات:** اطمینان از اینکه یک سازمان با قوانین و مقررات مربوط به امنیت اطلاعات مطابقت دارد و می‌تواند به حوادث امنیت اطلاعات به‌طور مؤثر رسیدگی کند.
- **عملیات امنیتی:** نظارت بر سیستم‌ها و شبکه‌ها برای شناسایی و مقابله با تهدیدات امنیتی.
- **امنیت فیزیکی و محیطی:** محافظت از سخت‌افزار، داده‌ها و کارکنان در برابر تهدیدات فیزیکی.
- **معماری امنیت:** طراحی و پیاده‌سازی سیستم‌های امنیتی و کنترل‌ها برای برآورده‌کردن نیازهای یک سازمان.

5. International Information Systems Security Certification Consortium (ISC2)
6. Center for Internet Security (CIS)
7. National Institute of Standards and Technology (NIST)
8. Business continuity planning/Disaster recovery (BCP/DR)

• **امنیت مخابرات/شبکه:** محافظت از شبکه‌های ارتباطی در برابر دسترسی غیرمجاز.

فهرست بالا تقسیم‌بندی‌ای است که معمولاً توسط کنسرسیوم بین‌المللی صدور گواهینامه امنیت سیستم‌های اطلاعات در مجموعه دانش خود برای صدور گواهینامه حرفه‌ای امنیت سیستم‌های اطلاعات (CISSP)[9] انجام می‌شود. ما در فصل ۸، "معضل صدور گواهینامه»، با جزئیات بیشتر در مورد صدور گواهینامه‌ها صحبت خواهیم کرد.

امنیت سایبری به دلیل وسعت زیاد حوزه‌ی کلی آن، به حوزه‌های موضوعی زیر تقسیم می‌شود. با تفکیک آن، گروه‌بندی محتوا برای مطالعه و تحلیل بیشتر آسان‌تر می‌شود. علاوه بر این، بسیاری از افرادی که وارد حوزه امنیت سایبری می‌شوند، تمایل دارند روی یک حوزه خاص تمرکز یا تخصص پیدا کنند؛ بنابراین، برای درک اینکه چرا یک نفر روی یک حوزه نسبت به حوزه دیگر تمرکز می‌کند، بیایید این حوزه‌ها را تعریف کنیم.

کنترل دسترسی: کنترل دسترسی شامل روشی است که تنها به افراد، برنامه‌ها یا سایر سیستم‌های رایانه‌ای مجاز اجازه می‌دهد تا منابع یک سیستم رایانه‌ای را مشاهده، تغییر یا کنترل کنند. علاوه بر این، به‌عنوان مکانیزمی برای محدودکردن استفاده از منابع خاص فقط برای کاربرانی که مجوز دریافت کرده‌اند، عمل می‌کند.

توسعه امن نرم‌افزار: توسعه امن نرم‌افزار شامل مجموعه‌ای از رویه‌ها و وظایفی است که با برنامه‌ریزی استراتژیک، کدگذاری و مدیریت نرم‌افزار و سیستم‌ها مرتبط است. علاوه بر این، شامل اجرای اقدامات حفاظتی در آن سیستم‌ها برای تضمین محرمانگی، یکپارچگی و دردسترس‌بودن نرم‌افزار و داده‌هایی است که پردازش می‌کند.

برنامه‌ریزی تداوم کسب‌وکار/بازیابی فاجعه: شامل اقدامات، رویه‌ها و استراتژی‌های ضروری برای حفظ عملیات بدون وقفه کسب‌وکار در مواجهه با اختلالات قابل‌توجه است. این موضوع شامل شناسایی، انتخاب، اجرا، آزمایش و نگهداری فرایندها و اقدامات خاصی است که برای محافظت از زیرساخت و عملیات حیاتی کسب‌وکار در برابر اختلالات سیستم و شبکه طراحی شده‌اند. هدف نهایی، بازگرداندن سریع خدمات ضروری و فعالیت‌های تجاری به حالت عادی عملکرد آن‌ها است.

رمزنگاری: رمزنگاری، علم و حتی برخی می‌گویند هنر استفاده از فریب و ریاضیات برای مخفی‌کردن داده‌ها در برابر دسترسی‌های ناخواسته است. رمزنگاری قرن‌هاست که مورداستفاده قرار می‌گیرد. این علم به اصول، ابزار و روش‌های تبدیل متن ساده به متن رمز و بالعکس برای اطمینان از محرمانگی، صحت و اصالت یا عدم انکار داده‌ها می‌پردازد.

9. Certified Information System Security Professional (CISSP)

حکمرانی امنیت اطلاعات و مدیریت ریسک

حکمرانی امنیت اطلاعات و مدیریت ریسک، استراتژی‌های چندوجهی سازمان‌ها برای حفاظت از دارایی‌ها و سیستم‌های اطلاعاتی حیاتی را در برمی‌گیرد. این حوزه به دنبال ایجاد معیارهای جامع برای حفاظت از طریق یکپارچه‌سازی چارچوب‌ها، سیاست‌ها، فرهنگ‌سازمانی و استانداردها است.

برای حکمرانی اثربخش، فراتر رفتن از فناوری به‌تنهایی و توجه به رفتار انسان ضروری است. ایجاد آگاهی امنیتی، پایبندی به به‌روش‌ها و پرورش فرهنگ مسئولیت‌پذیری به همان اندازه مهم است. چارچوب‌های حکمرانی پیشرو، مدل‌های راهنما مختلفی را ارائه می‌دهند. ITIL فرآیندهای مدیریت خدمات فناوری اطلاعات را ترسیم می‌کند. COBIT بر حکمرانی و کنترل فناوری اطلاعات تمرکز دارد. خانواده استانداردهای ایزو ۲۷۰۰۰ سیستم‌های مدیریت امنیت اطلاعات را پوشش می‌دهد. چارچوب امنیت سایبری NIST استانداردهای صنعتی را برای برنامه‌های امنیتی تعریف می‌کند.

سازمان‌ها با بهره‌گیری از اصول حکمرانی، می‌توانند رویکردی استراتژیک برای مدیریت ریسک‌های سایبری در پیش بگیرند که به معنای ارزیابی مداوم قابلیت‌های افراد، فرآیندها و فناوری آن‌ها در برابر استانداردها و سپس شناسایی و اولویت‌بندی زمینه‌های بهبود است. حکمرانی امنیتی بالغ، جامع و درعین‌حال تطبیق‌پذیر است. در این رویکرد، چارچوب‌های آزمایش‌شده، شیوه تعامل مدیران، آموزش کاربر، سیاست‌های چابک و کنترل‌های قوی برای حفاظت جامع از سیستم‌ها و اطلاعات ترکیب شده است. سازمان‌ها باید با هوشیاری بر حکمرانی نظارت کنند تا آن را تکامل دهند و انعطاف‌پذیر باقی بمانند.

حقوقی/تنظیم‌گری/انطباق و تحقیقات

رویه‌های حقوقی، تنظیم‌گری، انطباق و تحقیقات شامل سیاست‌ها، قوانین و فرایندهایی است که سازمان‌ها برای رسیدگی به جرائم رایانه‌ای و حوادث امنیتی به کار می‌گیرند. این حوزه موارد زیر را در برمی‌گیرد:

- **قوانین جرائم رایانه‌ای:** قوانینی که دسترسی غیرمجاز، هک‌کردن، توزیع بدافزار و سایر جرائم سایبری را ممنوع می‌کند.
- **مقررات مرتبط:** الزامات مربوط به حریم خصوصی داده‌ها، افشای نقض، الزامات خاص هر بخش و استانداردهای امنیت سایبری.
- **اقدامات تحقیقاتی:** تکنیک‌هایی برای شناسایی حوادث امنیتی از طریق نظارت،

تجزیه‌وتحلیل لاگ و پزشکی قانونی.

• **روش‌های جمع‌آوری و مدیریت شواهد:** رویه‌هایی برای جمع‌آوری، تجزیه‌وتحلیل، مستندسازی و نگهداری ایمن شواهد برای تحقیقات.

• **پروتکل‌های گزارش‌دهی:** دستورالعمل‌هایی برای گزارش حوادث به مقامات و طرف‌های آسیب‌دیده.

رعایت الزامات قانونی و مقرراتی، زیربنای امنیت است. نقض این الزامات می‌تواند منجر به جریمه، دادخواست و خدشه‌دار شدن شهرت شود. برنامه‌ریزی پیشگیرانه برای واکنش به حوادث اطمینان می‌دهد که سازمان‌ها در صورت نقض امنیتی بتوانند سریع و برنامه‌ریزی‌شده عمل کنند. پیروی از رویه‌های از پیش تعیین شده برای رسیدگی به شواهد برای تحقیقات دقیق جرم‌شناسی قانونی حیاتی است. با یکپارچه‌سازی انطباق قانونی در مدل‌های حاکمیتی خود و آماده‌سازی پروتکل‌های تحقیقاتی اصولی، سازمان‌ها تاب‌آوری و پاسخ‌گویی خود را تقویت می‌کنند. این امر با احترام به حقوق، امنیت سایبری را ارتقا می‌دهد.

عملیات امنیتی

عملیات امنیتی فرایندها و کنترل‌های مداومی است که برای ایمن‌سازی سیستم‌های اطلاعاتی و داده‌های یک سازمان اجرا می‌شود. این حوزه بر اجرای مداوم روش‌های امنیتی در محیط‌های فناوری متمرکز و توزیع‌شده، تمرکز دارد. مسئولیت‌های کلیدی شامل موارد زیر است:

• **محافظت از دارایی:** اطمینان از محرمانگی و درستی سخت‌افزار، برنامه‌های کاربردی، سرویس‌ها و داده‌ها از طریق کنترل دسترسی، رمزنگاری و اقدامات تاب‌آوری.

• **نظارت و کشف:** به‌کارگیری ابزارهایی مانند SIEM و IDS برای نظارت مداوم بر سیستم‌ها، شبکه‌ها و فعالیت‌های کاربران برای شناسایی سریع حوادث احتمالی.

• **پاسخ به حادثه:** بررسی رویدادهای مشکوک یا تأییدشده، محدودکردن تأثیرات، ریشه‌کن‌کردن تهدیدات، بازیابی سیستم‌ها و بهبود قابلیت‌های پاسخگویی در آینده.

• **نگهداری مستمر:** حفظ عملکرد قابل‌اعتماد ابزارها و سرویس‌های امنیتی مانند فایروال‌ها، آنتی‌ویروس و مدیریت لاگ از طریق وصله‌ها، ارتقا و افزونگی.

• **یکپارچه‌سازی فرایند:** یکپارچه‌سازی فرایندهای امنیتی در عملیات فناوری اطلاعات و گردش کار کسب‌وکار برای نهادینه‌کردن محافظت امنیتی خوب.

هدف نهایی، توسعه قابلیت‌های بالغ برای پیش‌بینی، پیشگیری، کشف و پاسخ به تهدیدات از طریق فناوری، فرایندها و تخصص انسانی است که با یکپارچه‌سازی روان عملیات امنیتی در

عملکردهای روزانه، یک سیستم ایمنی بنیانی مقاوم در برابر حملات سایبری ایجاد می‌کند.

امنیت فیزیکی و محیطی

امنیت فیزیکی و محیطی شامل محافظت از تأسیسات که سیستم‌های اطلاعاتی حیاتی را در خود جای داده‌اند، در برابر دسترسی غیرمجاز و خطرات محیطی است. این حوزه موارد زیر را در برمی‌گیرد:

- **بررسی‌های امنیتی:** ارزیابی منظم کنترل‌های دسترسی فیزیکی، سیستم‌های نظارت و آسیب‌پذیری تأسیسات در برابر تهدیداتی مانند آتش‌سوزی یا سیل.
- **ارزیابی ریسک و آسیب‌پذیری:** شناسایی زیرساخت‌های فیزیکی و ضعف‌های رویه‌ای که ممکن است منجر به نقض داده‌ها یا آسیب به سیستم شود.
- **برنامه‌ریزی و طراحی سایت:** یکپارچه‌سازی امنیت در چیدمان تأسیسات از طریق اقداماتی مانند مناطق کنترل دسترسی، دوربین‌ها، آژیرها و اتاق‌های ایمن تجهیزات.
- **سیستم‌های کنترل دسترسی:** مدیریت دسترسی فیزیکی به تأسیسات و اجزای سیستم‌های حیاتی از طریق روش‌هایی مانند کارت شناسایی، اعتبارسنجی بیومتریک و احراز هویت چندعاملی.
- **کنترل‌های محیطی:** حفظ دمای ایده‌آل، رطوبت، تأمین برق، اطفای حریق و سایر شرایط محیطی برای محافظت از سیستم‌ها.
- **رویه‌های امنیتی:** تعیین سیاست‌هایی برای همراهی بازدیدکنندگان، گزارش حوادث، انجام تعمیر و نگهداری تجهیزات و پاسخگویی به رویدادهای محیطی.

سازمان‌ها می‌توانند با پرداختن جامع به عوامل فیزیکی در کنار دفاع سایبری، سطوح حمله را کاهش دهند، تهدیدات را به‌سرعت شناسایی کنند و سرعت پاسخ به حوادث را بهبود بخشند. استفاده ترکیبی از سیاست‌های امنیت فیزیکی و دیجیتال، لایه‌های دفاعی مستحکمی ایجاد خواهد کرد.

معماری امنیت

معماری امنیت شامل ترجمه الزامات سازمانی به طرح‌های جامع امنیت سایبری است که افراد، فرایندها و کنترل‌های فناوری را در برمی‌گیرد. این حوزه بر موارد زیر تمرکز دارد:

- **اصول و چارچوب‌های امنیتی:** به‌کارگیری مدل‌هایی مانند «Zero Trust» و کنترل‌های CIS برای هدایت امنیت.

• **ترجمه کنترل:** تطبیق الزامات امنیتی با حفاظت‌های فنی و سیاست‌هایی که تعادل بین قابلیت استفاده و محافظت را برقرار می‌سازند.

• **طراحی محیط:** طراحی دفاع‌های لایه‌بندی‌شده متناسب با زیرساخت، محیط‌های ابری، برنامه‌های کاربردی، جریان داده‌ها و سناریوهای دسترسی متنوع.

• **یکپارچه‌سازی نظارت:** یکپارچه‌سازی کنترل‌ها و سیستم‌هایی برای ارائه قابلیت‌های ثبت دقیق وقایع، دیده‌پذیری، تجزیه‌وتحلیل و پاسخگویی قوی.

• **تطابق با الزامات:** تطبیق بخش امنیت برای رعایت مقررات، الزامات قانونی و استانداردهای امنیت سایبری بخش صنعت.

• **سازگاری مداوم:** تکامل‌بخش امنیت برای رسیدگی به تهدیدات جدید، نیازهای تجاری و پیشرفت‌های فناوری.

معماری امنیت به‌عنوان یک نقشه راه سطح بالا عمل می‌کند که چگونگی تطابق امنیت با اهداف تجاری را تدوین می‌نماید. این بستر، پیاده‌سازی یکپارچه دفاع‌های سایبری افراد، فرایندها و فناوری در سراسر سازمان را تسهیل می‌کند. دستیابی به یک معماری امنیتی مؤثر، مستلزم شناسایی و تلفیق نیازهای سازمانی با تخصص عمیق امنیت سایبری است.

امنیت مخابرات/شبکه

امنیت مخابرات و شبکه شامل انواع فناوری‌ها، روش‌های انتقال، چارچوب‌ها، قالب‌های داده و اقدامات حفاظتی می‌شود. هدف نهایی آن‌ها اطمینان از محرمانگی، یکپارچگی و دسترس بودن[10] داده‌هایی است که از طریق شبکه‌های خصوصی و عمومی روی انواع رسانه‌ها منتقل می‌شوند.

امنیت شبکه اغلب به‌عنوان یکی از ارکان اصلی امنیت فناوری اطلاعات شناخته می‌شود، چون شبکه در بسیاری از محیط‌ها دارایی مرکزی و حیاتی به شمار می‌رود. ازکارافتادن شبکه در اغلب موارد به معنای اختلال در کسب‌وکار و خدمات است.

همان‌طور که در حوزه‌های مختلف دیده می‌شود، امنیت مخابرات و شبکه نه‌تنها به هم مرتبط هستند؛ بلکه هر دو با مدیریت ریسک و کاهش آن سروکار دارند. ریسک همان‌طور که قبلاً گفته شد، احتمال وقوع یک رویداد ناخوشایند است. این رویداد می‌تواند یک بلایای طبیعی، خرابی هارددیسک یا حمله سایبری باشد. با درنظرگرفتن این موضوع، می‌توان گفت امنیت سایبری کاهش ریسک برای حفظ محرمانگی، یکپارچگی و دردسترس‌بودن (CIA) داده‌ها و سیستم‌ها است.

10. Confidentiality, Integrity, and Availability (CIA)

سه‌گانه‌های بنیادین در امنیت سایبری

سه‌گانه CIA مبنای امنیت سایبری را تشکیل می‌دهد.

• **محرمانگی:** اطمینان از اینکه اطلاعات فقط برای افراد یا سیستم‌های مجاز قابل‌دسترسی است.

• **یکپارچگی:** اطمینان از اینکه اطلاعات دقیق، کامل و به‌روز هستند.

• **دسترس‌پذیری:** اطمینان از اینکه اطلاعات و سیستم‌ها برای کاربران مجاز در زمان موردنیاز قابل‌دسترسی هستند.

سازمان‌ها برای حفظ امنیت سایبری خود باید اقداماتی را برای محافظت از داده‌ها و سیستم‌های خود در برابر تهدیدات داخلی و خارجی انجام دهند. این اقدامات می‌تواند شامل موارد زیر باشد:

• **کنترل‌های دسترسی:** محدودکردن دسترسی به داده‌ها و سیستم‌ها به افراد یا سیستم‌های مجاز.

• **محافظت از داده‌ها:** جلوگیری از افشا یا دست‌کاری غیرمجاز داده‌ها.

• **امنیت شبکه:** محافظت از شبکه در برابر دسترسی غیرمجاز، بدافزار و سایر تهدیدات.

• **آگاهی از امنیت:** آموزش کارکنان در مورد خطرات امنیت سایبری و نحوه محافظت از اطلاعات.

• **برنامه پاسخ به حادثه:** داشتن برنامه‌ای برای پاسخ‌گویی به نقض‌های امنیتی.

امنیت سایبری یک فرایند مداوم است و سازمان‌ها باید به‌طور مداوم اقدامات امنیتی خود را ارزیابی و به‌روزرسانی کنند تا با تهدیدات جدید مقابله کنند.

تصویر ۱.۱ – مثلث CIA

در حوزه امنیت سایبری، حفظ محرمانگی، یکپارچگی و دسترسی‌پذیری داده‌ها از اهمیت ویژه‌ای برخوردار است. علاوه بر این، مفهوم «عدم انکار»[11] متضمن آن است که افراد نتوانند انجام اقدامات و تراکنش‌های خود را انکار کنند. برای درک بهتر جنبه‌های مختلف و مفاهیم کلیدی و همچنین تبیین اهمیت امنیت سایبری، در ادامه اجزای اصلی سه‌گانه CIA شرح داده شده است.

محرمانگی

محرمانگی به معنای حفاظت از اطلاعات حساس در برابر دسترسی یا افشای غیرمجاز است و اطمینان می‌دهد که فقط افراد مجاز امکان دسترسی و مشاهدهٔ چنین داده‌هایی را داشته باشند. این اصل بر روی محافظت از اطلاعات حساس تمرکز دارد و از افتادن آن‌ها به دست افراد غیرمجاز جلوگیری می‌کند و کنترل دقیقی بر اینکه چه کسی می‌تواند به این اطلاعات دست یابد و آن‌ها را مشاهده کند، برقرار می‌سازد. در ادامه به برخی جنبه‌های کلیدی مرتبط با محرمانگی اشاره می‌کنیم:

- **رمزنگاری داده‌ها:** رمزنگاری فرایندی است که داده‌های متنی (plaintext) را به شکل کدگذاری شده تبدیل می‌کند که بدون کلید رمزگشایی مناسب، قابل خواندن نیست. این کار از درک محتوای داده‌ها توسط افراد غیرمجاز حتی در صورت دسترسی به آن‌ها جلوگیری می‌کند.
- **کنترل دسترسی:** کنترل دسترسی شامل اجرای مکانیزم‌هایی برای محدودکردن دسترسی به اطلاعات حساس براساس نقش کاربر، مجوزها و عوامل احراز هویت است. این کار از دسترسی افراد غیرمجاز به داده‌های محرمانه جلوگیری می‌کند.
- **طبقه‌بندی داده‌ها:** طبقه‌بندی داده‌ها شامل دسته‌بندی داده‌ها بر اساس سطح حساسیت آن‌ها است. این کار به سازمان‌ها اجازه می‌دهد تا اولویت را بر محافظت از اطلاعات بسیار حساس قرار دهند و کنترل‌های امنیتی مناسب را براساس طبقه‌بندی اعمال کنند.

یکپارچگی

یکپارچگی تضمین می‌کند که داده‌ها در طول چرخه حیات خود دقیق، بدون تغییر و قابل‌اعتماد باقی می‌مانند. حفظ یکپارچگی داده‌ها برای جلوگیری از تغییرات غیرمجاز، فساد یا دست‌کاری آن‌ها ضروری است. در ادامه به برخی جنبه‌های کلیدی مرتبط با یکپارچگی اشاره می‌کنیم:

- **اعتبارسنجی داده‌ها**[12]: اعتبارسنجی داده‌ها شامل تأیید صحت و سازگاری داده‌ها است. این کار اطمینان می‌دهد که داده‌ها مطابق با معیارهای از پیش تعریف‌شده خاص هستند و عاری

11. Non-repudiation
12. Data validation

از هرگونه خطا، نقص یا تغییر مخرب هستند.

• **توابع درهم‌سازی**[۱۳]: توابع درهم‌سازی الگوریتم‌های ریاضی هستند که برای یک مجموعه‌دادهٔ مشخص، رشته‌ای منحصربه‌فرد از کاراکترها (مقدار درهم‌سازی) ایجاد می‌کنند. با مقایسه مقدار درهم‌سازی قبل و بعد از انتقال یا ذخیره‌سازی داده‌ها، در صورت عدم تطابق مقادیر درهم‌سازی، می‌توان نقض را تشخیص داد.

در ادامه بحث در مورد امنیت سایبری، به بررسی دو مفهوم کلیدی دیگر و یک جنبه مهم از دسترسی‌پذیری می‌پردازیم.

• امضای دیجیتال: [۱۴]

امضای دیجیتال با استفاده از تکنیک‌های رمزنگاری، مکانیزمی را برای تأیید صحت و درستی اسناد یا پیام‌های الکترونیکی ارائه می‌دهد. امضای دیجیتال تضمین می‌کند که فرستنده نمی‌تواند ارسال پیام را انکار کند و محتوای پیام بدون تغییر باقی می‌ماند.

امضای دیجیتال شبیه امضای سنتی عمل می‌کند، اما به‌صورت الکترونیکی انجام می‌شود. امضای دیجیتال از یک کلید خصوصی برای رمزنگاری یک سند یا پیام استفاده می‌کند. هرکسی با کلید عمومی مربوطه می‌تواند امضا را تأیید کند و بدین ترتیب، هم صحت فرستنده و هم اینکه پیام دست‌کاری نشده است، قابل‌اثبات است.

دسترس‌پذیری

قبلاً اشاره کردیم که دسترس‌پذیری به معنای اطمینان از قابل‌دسترس بودن و استفاده از سیستم‌ها، شبکه‌ها و داده‌ها در زمان نیاز است. در ادامه به برخی جنبه‌های کلیدی مرتبط با دسترس‌پذیری می‌پردازیم:

• **افزونگی و تحمل خطا**[۱۵]: ایجاد سیستم‌های افزونگی و مقاوم در برابر خطا اطمینان می‌دهد که سیستم‌ها و داده‌های حیاتی دارای اجزای پشتیبان یا مسیرهای جایگزین هستند و تأثیر خرابی‌های سخت‌افزاری، بلایای طبیعی یا سایر اختلالات را به حداقل می‌رساند.

• **برنامه‌ریزی بازیابی فاجعه**[۱۶]: برنامه‌ریزی بازیابی فاجعه شامل ایجاد استراتژی‌ها و فرایندهایی برای بازیابی سیستم‌ها و داده‌های حیاتی پس از یک رویداد مخرب است. این

13. Hash functions
14 . Digital signatures
15. Redundancy and fault tolerance
16. Disaster recovery planning

برنامه‌ریزی شامل پشتیبان‌گیری منظم، ذخیره‌سازی خارج از سایت و رویه‌های مستند برای بازیابی سیستم می‌شود.

• **کاهش حمله توزیع‌شده منع سرویس**[۱۷]: حملات توزیع‌شده منع سرویس (DoS) باهدف تحت‌الشعاع قراردادن سیستم‌ها یا شبکه‌ها و ایجاد عدم دسترسی به سرویس انجام می‌شوند. اجرای راهکارهای کاهش اثرات DoS، مانند فیلترکردن ترافیک یا شبکه‌های توزیع محتوا (CDN)، به محافظت در برابر چنین حملاتی و اطمینان از دسترسی بدون وقفه به سرویس‌ها کمک می‌کند.

با درنظرگرفتن محرمانگی، یکپارچگی، دسترسی‌پذیری، عدم انکار و سایر اقدامات امنیتی مناسب، سازمان‌ها می‌توانند از دارایی‌های اطلاعاتی خود در برابر تهدیدات سایبری محافظت کرده و اطمینان حاصل کنند که اطلاعات و سیستم‌های‌شان قابل‌اعتماد، در دسترس و ایمن هستند.

عدم انکار

همان‌طور که اشاره شد، عدم انکار به این معناست که افراد نمی‌توانند انجام اقدامات و تراکنش‌های خود را انکار کنند. این مفهوم اطمینان می‌دهد که شواهدی برای اثبات وقوع یک اقدام خاص توسط یک نهاد (فرد یا سازمان) وجود دارد. عدم انکار برای بسیاری از فعالیت‌های دیجیتالی، ازجمله تجارت الکترونیک، امضای قراردادهای الکترونیکی و رأی‌گیری الکترونیکی، بسیار مهم است.

در دنیای دیجیتال، اثبات وقوع یک رویداد و اینکه چه کسی مسئول آن بوده است، می‌تواند چالش‌برانگیز باشد. امضای دیجیتال، همان‌طور که قبلاً ذکر شد، یکی از راه‌های دستیابی به عدم انکار است.

گواهینامه‌های دیجیتال [۱۸]

یکی دیگر از جنبه‌های کلیدی عدم انکار، گواهینامه‌های دیجیتال است. گواهینامه‌های دیجیتال اسناد الکترونیکی هستند که هویت افراد یا نهادها را در تراکنش‌های الکترونیکی تأیید می‌کنند. این گواهینامه‌ها توسط سازمان‌های ثالث مورداعتماد (مرجع صدور گواهینامه)[۱۹] صادر می‌شوند و تضمینی برای صحت اعتبار و عدم انکار ارائه می‌دهند.

گواهینامه‌های دیجیتال شبیه گواهینامه‌های رانندگی یا شناسنامه در دنیای واقعی عمل می‌کنند، با این تفاوت که به‌صورت الکترونیکی صادر و تأیید می‌شوند. گواهینامه دیجیتال حاوی

17. Distributed Denial of Service mitigation
18. Digital certificates
19. Certificate Authorities

اطلاعاتی در مورد دارنده آن، مانند نام، کلید عمومی و یک امضای دیجیتال از مرجع صدور گواهینامه است.

هنگام برقراری ارتباط امن در اینترنت، مانند اتصال به یک وب‌سایت با پروتکل HTTPS، از گواهینامه‌های دیجیتال برای تأیید هویت وب‌سایت و برقراری یک اتصال رمزگذاری‌شدن استفاده می‌شود. این امر اطمینان می‌دهد که شما با وب‌سایت موردنظر ارتباط برقرار می‌کنید و داده‌های شما در طول انتقال رمزگذاری شده‌اند.

با ترکیب امضای دیجیتال و گواهینامه‌های دیجیتال، سازمان‌ها می‌توانند سطح بالایی از عدم انکار را در تراکنش‌های الکترونیکی به دست آورند. این امر اعتماد و امنیت را در تعاملات دیجیتالی افزایش می‌دهد.

سوابق ممیزی

سوابق ممیزی، سوابقی هستند که فعالیت‌ها و رویدادهای داخل یک سیستم یا شبکه را ضبط و مستند می‌کنند. این سوابق به‌عنوان مدرکی از اقدامات انجام شده عمل می‌کنند و می‌توان از آن‌ها برای اثبات وقوع رویدادها یا تراکنش‌های خاص استفاده کرد.

انطباق با قوانین و مقررات

در بسیاری از صنایع عدم انکار پیامدهای قانونی و نظارتی دارد. انطباق با قوانین و الزامات خاص هر صنعت، به ایجاد پاسخ‌گویی و جلوگیری از انکار اقدامات یا تراکنش‌ها کمک می‌کند.

هر حمله سایبری یا تلاش نفوذ، سعی در نقض حداقل یکی از ویژگی‌های سه‌گانه CIA دارد. گروه‌بندی این سه مفهوم در یک سه‌گانه، به متخصصان امنیت سایبری این امکان را می‌دهد که وابستگی‌های متقابل، همپوشانی‌ها و تضادهای بین آن‌ها را درک کنند. این سه‌گانه چارچوبی را برای بررسی روابط بین محرمانگی، یکپارچگی و دسترسی‌پذیری فراهم می‌کند و متخصصان را قادر می‌سازد تا نحوهٔ تعامل و پتانسیل تضاد این اصول با یکدیگر را تجزیه‌وتحلیل کنند.

این سه‌گانه را می‌توان به یک صندلی سه‌پایه تشبیه کرد. هر پایه به‌تنهایی و تحت‌فشار، ثبات قابل‌توجهی را برای کل سکو فراهم می‌کند. اما اگر هر یک از این پایه‌ها به خطر بیفتد، ثبات و عملکرد کل سکو غیرقابل‌دوام می‌شود.

متخصصان امنیتی با بررسی تنش ذاتی بین اجزای این سه‌گانه، می‌توانند اولویت‌ها را به‌طور مؤثر تعیین کرده و فرایندهای لازم را اجرا کنند. این کار می‌تواند در یک برنامه یا سیستم واحد یا به‌طورکلی در کل مجموعه فناوری انجام شود.