تعریف سیسکو سیف (Cisco SAFE) به زبانی ساده

پیچیدگی امنیت در فناوری

پیچیدگی یکی از چالش‌های اصلی پیش روی متخصصان امنیت است. فناوری به طور مداوم به کاربردهای جدید تقسیم می‌شود و سازمان‌ها از ده‌ها محصول استفاده می‌کنند که به طور یکپارچه با یکدیگر عمل **نمی‌کنند**. این امر سطح‌های حمله را چند برابر می‌کند که به نوبه خود دفاع‌ها را پیچیده‌تر می‌سازد. کلاهبرداران از این ضعف سوءاستفاده می‌کنند تا تهدیدات پیشرفته‌ای را برای طرح‌های سودآورتر توسعه دهند.

نیاز به یک منبع جامع

صنعت به شدت به یک منبع نیاز دارد که مشکل را ساده کند. راه‌حل باید جامع، معتبر و بیش از فقط محصولات باشد؛ باید بر تهدیدات کسب‌وکار شما تمرکز کند.

Cisco SAFE چیست؟

Secure Architecture for Everyone (SAFE) Cisco یک مدل و روش امنیتی است که برای تامین امنیت کسب‌وکارها استفاده می‌شود. این مدل بر تهدیدات تمرکز دارد و بهترین روش‌ها برای دفاع در برابر آنها را ارائه می‌دهد Cisco SAFE چالش‌های کسب‌وکار امروز را به زبانی که نحوه تفکر ما درباره امنیت را تغییر می‌دهد، بیان می‌کند. این مدل با استفاده از مفاهیم ساده بر پیچیدگی‌های امروز تمرکز دارد، تا ما را برای چالش‌های فردا آماده کند.

مدل مرجع امنیتی Cisco SAFE

با استفاده از مدل مرجع امنیتی، چالش‌های تامین امنیت عملکردهای کسب‌وکار امروزی به رویکردی بلوکی ساده می‌شوند. این مدل بهترین روش‌های امنیتی امروزی، بحث‌های معماری، و طراحی‌های آزمایشگاهی را شامل می‌شود که توسط کارشناسان امنیتی برتر Cisco، مشتریان و شرکای آن تدوین شده‌اند. طراحی‌های تایید شده Cisco SAFE به موضوعات مهم امنیتی می‌پردازند و مستندسازی "چگونه انجام دادن" آنها را ارائه می‌دهند.

SAFE شامل موارد زیر است:

۱. سناریوهای کاربردی کسب‌وکار که سطح حمله‌ای که کلاهبرداران می‌توانند هدف قرار دهند را نشان می‌دهد
۲. قابلیت‌های امنیتی مرتبط با تهدیدات مشترک در سناریوهای کاربردی کسب‌وکار
۳. معماری‌های مرجعی که قابلیت‌های امنیتی را به صورت منطقی در نقشه‌های آبی قرار می‌دهند

۴. طراحی‌هایی که از معماری‌های مرجع برای سناریوهای رایج پیاده‌سازی و راه‌حل‌ها استفاده می‌کنند، که به عنوان طراحی‌های تایید شده Cisco (CVDs) ارائه می‌شوند

روش Cisco SAFE

روش SAFE مدل را برای شرکت‌های فردی سفارشی می‌کند. با استفاده از ابزارها و مطالب SAFE، شرکت‌ها می‌توانند تهدیدات و ریسک‌های کسب‌وکار خود را تحلیل کنند. این کارگاه می‌تواند مفید باشد زیرا بخش‌های مختلف شرکت را که ممکن است معمولاً با هم تعامل نداشته باشند، گرد هم می‌آورد. نتیجه این کارگاه، معماری امنیتی متناسب با کسب‌وکار شما خواهد بود.

نحوه استفاده از Cisco SAFE

SAFE یک پاسخ واحد نیست. این مدل به عنوان مرجعی برای تهدیدات، ریسک‌ها و سیاست‌های مشترک در کسب‌وکار یک شرکت عمل می‌کند. این به معنای این نیست که همه شرکت‌ها یکسان هستند. با این حال، وقتی چالش‌های امنیتی را به طور کلی بررسی می‌کنیم، الگوهایی شروع به ظهور می‌کنند. صرف‌نظر از صنعت، روش‌های کسب‌وکار معینی احتمالاً به کار گرفته می‌شوند و در نتیجه، مورد بهره‌برداری قرار می‌گیرند.

قابلیت‌های بنیادی و کنترل‌های عملکردی برای دفاع از سطح حمله ضروری هستند. به عنوان مثال، دسترسی به شبکه، استفاده از برنامه‌های کاربردی کسب‌وکار، و ارتباطات از طریق ایمیل در همه شرکت‌ها مشترک است. اتصال به اینترنت برای مرور وب و دسترسی به خدمات ارائه‌شده از طریق ابر نگرانی‌های امنیتی کسب‌وکار اضافی را ایجاد می‌کند SAFE راهنمایی‌هایی برای عملکردهای کسب‌وکار مشترک که به قابلیت‌های امنیتی نیاز دارند، ارائه می‌دهد و به عنوان مرجعی برای امنیت جامع عمل می‌کند.

روش SAFE بهترین شیوه‌های مدل مرجع را برای شرکت‌های فردی سفارشی می‌کند و اطمینان حاصل می‌کند که اهداف کسب‌وکار بر اساس سیاست امنیتی و ریسک‌پذیری هر شرکت، به صورت قابل اندازه‌گیری امن می‌شوند. مراحل این روش عبارتند از:

۱. شناسایی اهداف کسب‌وکار

۲. تجزیه شبکه به قطعات قابل مدیریت

۳. ایجاد معیارهایی برای موفقیت کسب‌وکار

۴. دسته‌بندی ریسک‌ها، تهدیدات و سیاست‌ها

۵. ساخت راه‌حل امنیتی

سه مرحله SAFE

۱. مرحله قابلیت‌ها

در این مرحله، جریان‌های کسب‌وکار یا موارد کاربرد تعریف می‌شوند. بر اساس این موارد، قابلیت‌های امنیتی برای مقابله با تهدیدات، ریسک‌ها و سیاست‌ها تعیین می‌شوند

۲. مرحله معماری

در این مرحله، یک معماری امنیتی منطقی با استفاده از قابلیت‌های امنیتی شناسایی‌شده در جریان‌های کسب‌وکار تعریف می‌شود

۳. مرحله طراحی

در این مرحله، یک طراحی مشخص برای پیاده‌سازی قابلیت‌های امنیتی ایجاد می‌شود که شامل لیست محصولات، پیکربندی، خدمات و هزینه‌هاست

ابزارها و مطالب SAFE

SAFE ابزارها و منابعی ارائه می‌دهد که بحث بین مخاطبان کسب‌وکار و فنی را ساده‌تر می‌کند. این ابزارها شامل:

۱. آیکون‌های قابلیت‌ها برای نمایش جریان‌های کسب‌وکار و کنترل‌های امنیتی مناسب

۲. راهنماهای معماری برای مرجع لایه‌های امنیتی مناسب و توجیهات آنها

۳. راهنماهای طراحی که راه‌حل‌ها با دستورالعمل‌های مرحله‌به‌مرحله را بر اساس آزمایش‌های تایید شده Cisco ارائه می‌دهند

سطح حمله

سطح حمله شامل هر انسانی، با هر دستگاهی، در هر شبکه‌ای است که به هر برنامه‌ای دسترسی دارد و می‌تواند هدف قرار گیرد.

انسان: شناسایی افرادی که در شبکه شما هستند.

دستگاه: اطمینان از عدم آلوده بودن دستگاه‌ها.

شبکه: شبکه‌ها می‌توانند به خطر بیفتند.

برنامه‌ها: خدمات می‌توانند مورد سوءاستفاده قرار گیرند.

تامین امنیت سطح حمله

سطح حمله باید با قابلیت‌های مناسب تأمین امنیت شود. هر هدف ممکن است بخشی از یک حمله کلی‌تر باشد. با شناسایی جریان‌های کسب‌وکار شرکت که سطح حمله شرکت را نشان می‌دهد، قابلیت‌های امنیتی مناسبی می‌توانند اعمال شوند (شکل ۷).

جریان‌های کسب‌وکار

سه دسته از کاربران در شبکه شما نقش دارند:

داخلی: فعالیت‌های کارکنان در شبکه شرکت.

شخص ثالث: دسترسی مهمانان، فروشندگان، ارائه‌دهندگان خدمات یا شرکا به شبکه شرکت.

مشتریان: دسترسی مشتریان به خدمات مختلف مانند پورتال‌های وب و اطلاعات مشتریان.
سیاست‌ها، ریسک‌ها و تهدیدات هر یک از آنها را تحت تأثیر قرار می‌دهد و به قابلیت‌های امنیتی نیاز دارند.
جریان‌های کسب‌وکار کدگذاری شده با رنگ SAFE نشان می‌دهد که هر نقش چه امنیتی نیاز دارد

کنترل‌های عملکردی

کنترل‌های عملکردی ملاحظات امنیتی مشترکی هستند که از جنبه‌های فنی جریان‌های کسب‌وکار استخراج می‌شوند:

برنامه‌های امن: برنامه‌ها به کنترل‌های امنیتی کافی نیاز دارند.

ترافیک داخلی و خارجی امن: داده‌هایی که به طور امن بین منابع داخلی و خارجی جابجا می‌شوند.

دسترسی امن: دسترسی امن کارکنان، اشخاص ثالث، مشتریان و دستگاه‌ها به شبکه.

دسترسی راه دور امن: دسترسی راه دور امن برای کارکنان و شرکای شخص ثالث که خارج از شبکه شرکت هستند.

ارتباطات امن: ایمیل، صدا و ارتباطات ویدئویی باید امن شوند.

دسترسی وب امن: کنترل‌های دسترسی به وب سیاست استفاده را اعمال می‌کنند و از آلودگی شبکه جلوگیری می‌کنند.