بسمه‌تعالی

امن‌سازی پایه زیرساخت شبکه

بخش اول: مقدمه

برای دستیابی به امنیت شبکه کارا و مؤثر باید روش دفاع در عمق به صورت یکپارچه پیاده‌سازی شود. اولین لایه از روش دفاع در عمق، رعایت اصول و مبانی پایه امنیت شبکه می‌باشد. مبانی پایه امنیت شبکه، یک خط مشی امنیتی است که ستون اصلی امنیت محسوب شده و سایر تمهیدات امنیتی بر روی آن سوار می‌شوند. از این‌رو تهیه مبانی پایه امنیت شبکه از اهمیت بالایی برخوردار بوده و بسیار چالش‌برانگیز است. بخش اعظم این مبانی مربوط به امنیت زیرساخت شبکه است. در این سلسله از گزارش‌ها سعی شده است تا به‌گوشه‌ای از نیازمندی‌های پایه امنیت زیرساخت شبکه اشاره شود و چگونگی پیاده‌سازی آن‌ها توسط تجهیزات سیسکو ارائه گردد.

مروری بر نیازمندی‌های پایه امنیت زیرساخت شبکه

نیازمندی‌های پایه امنیت شبکه ش امل موارد مهم و اساسی امنیتی می‌باشند که در ایجاد و توسعه یک ساختار امنیتی قوی مورد استفاده قرار می‌گیرند. تمرکز اصلی بر روی امن‌سازی زیرساخت خود شبکه می‌باشد، همچنان‌که امن‌سازی سرویس‌های شبکه و موارد زیر نیز به عنوان محدوده‌های مهم در بحث امنیت شبکه باید مورد توجه قرار گیرند:

- دسترسی به تجهیزات زیرساخت
- زیرساخت مسیریابی
- انعطاف‌پذیری و استحکام نرم‌افزاری تجهیزات
- دسترسی از راه دور به شبکه
- اجرای سیاست‌های شبکه
- زیرساخت سویچینگ

به جز موارد پایه امنیتی که در بالا بدان اشاره شد، معمولاً ویژگی‌ها و تکنولوژی‌های امنیتی اضافه بر آن‌ها مورد توجه قرار نمی‌گیرند. برای مثال، اگر یک حساب کاربری با گذرواژه و رمز عبور پیش‌فرض بر روی یک دستگاه زیرساخت فعال باشد، نیازی به برنامه‌ریزی و انجام یک حمله پیچیده برای نفوذ به دستگاه نمی‌باشد،

بلکه حمله‌کننده می‌تواند به راحتی با اطلاعات پیش‌فرض که تغییر پیدا نکرده‌اند به دستگاه وارد شده و برنامه‌های مخرب خود را پیش ببرد.

یک راه‌کار قابل قبول و مطمئن، استفاده از چارچوب امنیتی سیسکو (CSF) است. این چارچوب روش‌های مختلف تشخیص و اعتبارسنجی نیازمندی‌های امنیتی یک سیستم را فراهم می‌کند. معمولاً از CSF در ایجاد مباحث پایه امنیت برای حصول اطمینان از به کارگیری نیازهای امنیتی مربوط به بخش‌های مختلف شبکه استفاده می‌شود.

تمام تنظیمات نمونه که در این سلسله از گزارش‌ها ذکر شده‌اند، بر اساس پلتفرم IOS سیسکو و ویژگی‌های آن آورده شده است. البته رئوس کلی مطالب در هر بخش قابل تعمیم به دیگر پلتفرم‌ها نیز هستند.

ارزیابی مقدماتی طراحی شبکه

نیازمندی‌های پایه امنیت شبکه شامل برخی تکنیک‌های مرتبط با فیلترکردن ترافیک‌های مبتنی بر آدرس IP است. برای انجام این کار از ACL استفاده می‌شود تا بتوان سیاست‌های امنیتی برای دستگاه‌های مدیریت دسترسی، قابلیت کنترل توزیع مسیر و uRPF را اجرا کرد. تکنیک‌های پیشرفته‌تر امنیتی که می‌توانند به عنوان لایه‌های افزوده امنیتی اضافه گردند (مانند فایروال) نیز با مکانیزم مشابه فیلترکردن ترافیک بر اساس آدرس IP عمل می‌کنند.

یک طرح توزیع آدرس IP که منطقی، خلاصه، یا تفکیک‌شده و مجزا باشد (همان‌طور که در RFC1918 توضیح داده شده است)، می‌تواند پیاده‌سازی تکنیک فیلترکردن ترافیک مبتنی بر آدرس IP را ساده‌تر و کنترل‌پذیرتر کند.

در مرحله آماده‌سازی به منظور توسعه مبانی پایه امنیت، توصیه می‌شود که یک ارزیابی مقدماتی از طرح شبکه با هدف تسهیل در پیاده‌سازی آن انجام گیرد. نکته کلیدی در این ارزیابی، بررسی کامل طرح تخصیص آدرس IP با تکیه بر دو مورد زیر است:

- آیا طرح تخصیص آدرس IP به خوبی انجام شده است و آیا خلاصه‌سازی یا تفکیک این آدرس‌ها به سادگی قابل انجام است؟

- آیا RFC1918 در مورد تخصیص آدرس IP به طور مناسب پیاده شده است؟

ممکن است ارزیابی طرح تخصیص آدرس IP منجر به تغییر محدوده‌هایی از این طرح قبل از پیاده‌سازی مبانی امنیت شود. توجه به این موضوع اگرچه تغییراتی در شبکه به‌وجود می‌آورد ولی به طور کلی موجب کنترل‌پذیری و قابلیت اجرای بهتر سیاست‌های امنیتی می‌شود.

مروری بر چارچوب امنیتی سیسکو

چارچوب امنیتی سیسکو یک فرایند عملیاتی امنیتی است که با هدف اطمینان از عملکرد شبکه و سرویس‌ها، در دسترس بودن و تداوم کسب و کار سیستم استفاده می‌شود. تهدیدات امنیتی همیشه در حال رشد می‌باشند، CSF نیز به منظور تشخیص تهدیدات جاری و همچنین دنبال کردن تهدیدات جدید و در حال گسترش، با استفاده از راه‌حل‌های جامع و عملی استفاده می‌شود.

CSF بر اساس دو هدف بنا شده است، با این فرض که تا زمانی که بر روی چیزی نظارت نباشد و نتوان آن را دید یا اندازه گرفت، نمی‌توان آن را کنترل کرد:

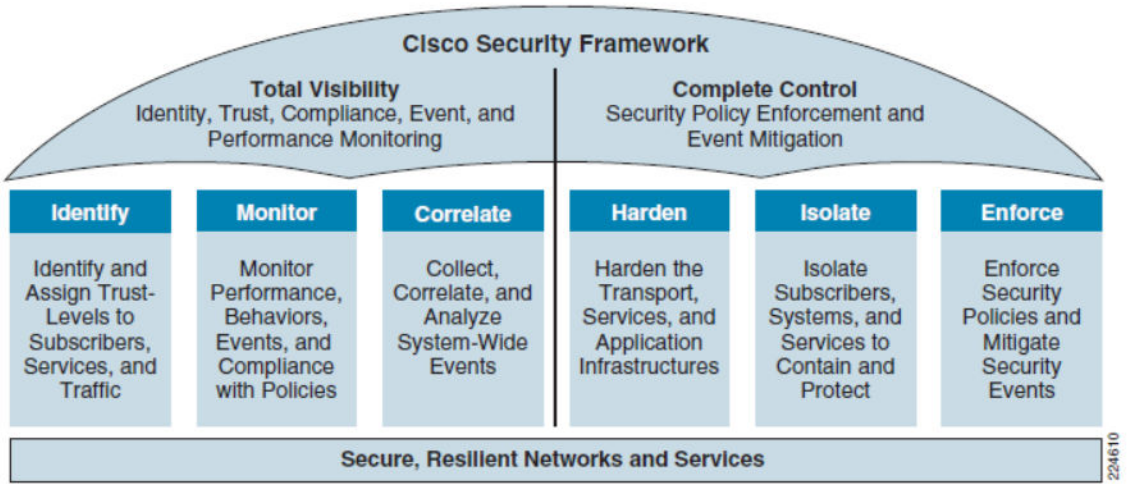
- تحصیل نظارت کامل
- تشخیص، پایش و همبسته‌سازی رخدادهای سیستم
- حصول اطمینان از کنترل کامل

در زیرساخت‌های بزرگ و پیچیده شبکه، ابتدا سیستم‌ها و سرویس‌ها را ایزوله کرده و پس از انجام آن سیاست‌های امنیتی را به منظور رسیدن به نظارت و کنترل کامل اجرا می‌کنند. تکنولوژی‌ها و قابلیت‌های گوناگونی در طول شبکه برای نظارت کامل بر فعالیت‌های شبکه، اجرای سیاست‌های امنیتی و تعیین ترافیک‌های غیرعادی استفاده می‌شود. اجزای زیرساخت شبکه مانند روتر و سوئیچ‌ها به عنوان اجزای فراگیر برای پایش مداوم سیاست‌ها و اجرای آن‌ها مورد استفاده قرار می‌گیرند.

همانگونه که در شکل ۱ مشاهده می‌شود، CSF بر روی شش مرحله کلیدی تمرکز می‌کند:

- شناسایی

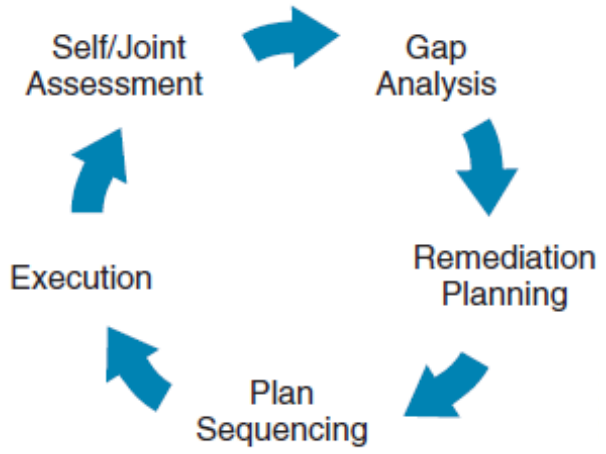
- پایش
- همبسته‌سازی
- استحکام بخشیدن
- جداسازی
- اجرا



شکل ۱- چارچوب امنیتی cisco

به کارگیری CSF برای شبکه نتایجی همچون شناخت تکنولوژی‌ها و بهترین روش برای برآوردن هریک از این شش راه حل عملیاتی را در بر خواهد داشت. با این حال CSF یک فرایند در حال توسعه، پویا و ساختار در حال بهبود محسوب می‌گردد که با تغییرات سیاست‌های امنیتی و نیازمندی‌های تجاری سازمان به روزرسانی می‌شود.

در شکل ۲ چرخه‌ی ارزیابی برای CSF نشان داده شده است:



شکل ۲- چرخه ارزیابی CSF

چرخه با ارزیابی اولیه آغاز می‌شود که هدف آن مشخص‌کردن ظرفیت و وضعیت فعلی امنیت می‌باشد. در ادامه در فاز تحلیل، نقاط ضعف و قوت معماری کنونی آشکار می‌گردد.

مباحث پایه امنیت به عنوان یک مدل مرجع در طول ارزیابی اولیه و فاز تحلیل مورد استفاده قرار می‌گیرد. این مدل حداقل نیازمندی‌های لازم برای کنترل و مدیریت پشتیبانی را فراهم می‌کند. نقاط ضعف و قوت شبکه‌های واقعی با مقایسه با این مدل مرجع می‌تواند مشخص شود.

پس از ارزیابی اولیه و اجرای فاز تحلیل، چرخه با برنامه بازسازی با هدف تامین نیازمندی‌های آینده به‌وسیله به‌روزرسانی معماری کل شبکه ادامه پیدا می‌کند. در ادامه، مرحله تعیین توالی طرح‌ها برای ایجاد نقشه پیاده-سازی برای مؤلفه‌های گوناگون برای معماری مورد نظر فراهم می‌گردد. سپس فازهای مختلف اجرا می‌شوند و نتایج به‌دست‌آمده مجدداً مورد ارزیابی قرار می‌گیرند.

همانطور که در شکل ۲ مشاهده می‌شود، این فرایند یک فرایند تکراری است و نتیجه هر تکرار، بهبود طراحی ساختار مورد نظر برای تامین سیاست‌های امنیتی و تجاری می‌باشد.

مستند امنیت پایه شبکه، بر مبنای چارچوب CSF توسعه یافته و ارائه شده است. بر این اساس در هـر بخـش مشخصات امنیتی پیشنهادی و نیز بهترین راه‌کار اجرایی برای پیاده‌سازی آن ارائه می‌گردد.