ایمن‌سازی بستر تبادل اطلاعات

امنیت شبکه چیست؟

آیا تاکنون به این موضوع فکر کرده‌اید که امنیت شبکه چه تعریفی دارد؟ موسسات آموزشی در آگهی‌های جذب دانشجو و شرکت‌ها در آگهی‌های سازمانی به واژه امنیت شبکه اشاره دارند؛ اما چه تعداد از این آگهی‌ها اصطلاح امنیت شبکه را برای شما به درستی تشریح کرده‌اند؟ امنیت شبکه اصطلاح کلی است که بسیاری از فناوری‌ها، دستگاه‌ها و فرآیندها را شامل می‌شود. در ساده‌ترین تعریف، امنیت شبکه مجموعه قوانین و پیکربندی‌هایی است که برای محافظت از یکپارچگی، محرمانگی و دسترسی به شبکه‌های کامپیوتری و داده‌ها در زمان استفاده از نرم‌افزار و سخت‌افزار تدوین می‌شود. هر سازمانی، صرف‌نظر از وسعت، حیطه کاری یا زیرساختی که بر پایه آن استوار است، نیاز دارد در نخستین گام به فکر پیاده‌سازی راه‌حل‌های امنیتی برای حفاظت از شبکه در برابر تهدیدات روبه رشد هکری باشد.

امنیت شبکه به چه معنا است؟

امنیت شبکه یک استراتژی سازمانی است و از دارایی‌های شبکه و ترافیک شبکه محافظت می‌کند. این حفاظت هر دو مؤلفه نرم‌افزار و سخت‌افزار را شامل می‌شود. یک سازمان هوشمند به‌خوبی می‌داند که دسترسی به شبکه باید بر مبنای بهترین استراتژی امنیتی استوار شده باشد. یک استراتژی راهبردی دقیق و درست باید طیف گسترده‌ای از تهدیدات را مدنظر قرار داده و برای رخدادها و موارد غیرمترقبه همچون یک حمله هکری پیش‌بینی‌های لازم را انجام داده باشد.

شبکه‌هایی که روزبه‌روز پیچیده‌تر می‌شوند

معماری شبکه‌های امروزی به‌مراتب پیچیده‌تر از سال‌های قبل شده است. جای تعجب نیست که مشاهده کنیم، چنین محیط پیچیده‌ای مملو از سخت‌افزارها و نرم‌افزارهای مختلفی است که هر یک ممکن است آسیب‌پذیری جدی درون خود جای داده باشند. هکرها همواره مترصد فرصتی هستند تا آسیب‌پذیری‌های کشف نشده را شناسایی کرده و از این آسیب‌پذیری‌ها برای نفوذ به شبکه استفاده کنند. این آسیب‌پذیری‌ها در بخش‌های مختلف شبکه از جمله دستگاه‌ها، داده‌ها، برنامه‌ها و عملکردهای کاربران مستتر هستند. مدیران شبکه از ابزارهای متنوعی که برای مدیریت امنیت شبکه و برنامه‌های کاربردی عرضه شده، استفاده می‌کنند تا تهدیدات سایبری و سوءاستفاده‌های احتمالی کارمندان از شبکه را به حداقل رسانده و اطمینان حاصل کنند که خط‌مشی‌های تعیین شده از سوی همه کارمندان رعایت می‌شود. دقت کنید تنها چند دقیقه خرابی یا اختلال در زیرساخت شبکه یک سازمان بزرگ می‌تواند باعث اختلالات گسترده‌ای شده که نه تنها ضرر و زیان‌های مالی سنگینی را به بار می‌آورد، بلکه به اعتبار و شهرت یک سازمان نیز خدشه وارد می‌کند. به‌طورکلی، امنیت شبکه یک دفاع یکپارچه و چند لایه‌ای است که از زیرساخت‌های ارتباطی یک سازمان محافظت می‌کند. این دفاع مستحکم در قالب خط‌مشی‌ها و کنترل‌هایی که درون هر لایه امنیتی پیاده‌سازی می‌شوند، در قالب چشم‌انداز امنیتی سازمان ترسیم می‌شوند. در چنین شرایطی دسترسی به شبکه و منابع آن فقط

برای کاربران احراز هویت شده مقدور بوده و مجرمان سایبری به‌راحتی موفق نخواهند شد به منابع شبکه دسترسی داشته باشند، زیرا در هر لایه امنیتی با مکانیزم‌های دفاعی مختلفی روبه‌رو می‌شوند.

سه رکن اصلی در برقراری امنیت شبکه

زمانی‌که درباره حفظ امنیت یک شبکه سازمانی صحبت می‌کنیم، باید توجه ویژه‌ای به لایه‌های مختلف داشته باشیم. هر یک از لایه‌های مدل مرجع OSI یا TCP/IP ممکن است هدف حمله هکرها قرار گیرند، بنابراین ضروری است، مقوله امنیت در ارتباط با سخت‌افزارها و نرم‌افزارها به‌دقت مورد توجه قرار گرفته و مهم‌تر از آن خط‌مشی‌های امنیتی شبکه برای هر بخش به‌درستی تدوین‌شده باشد. امنیت شبکه روی سه رویکرد کنترل فیزیکی، فنی و مدیریتی متمرکز است.

امنیت فیزیکی شبکه

کنترل‌های امنیت فیزیکی مانع از آن می‌شوند تا هر فرد غیرمجازی بتواند به منابع شبکه همچون روترها، اتاق داده، مراکز داده و سایر بخش‌های حساس مرتبط با شبکه دسترسی داشته باشد. دسترسی کنترل شده به معنای به‌کارگیری فناوری‌هایی همچون قفل‌ها، مکانیزم‌های احراز هویت زیستی و سایر فناوری‌های مشابه است که سعی می‌کنند یک ورود کنترل شده را به بخش‌های مختلف یک سازمان امکان‌پذیر کنند. ورود کنترل شده به معنای آن است که ورود و خروج هر کارمندی به مراکز حساس یک سازمان باید به‌دقت ثبت شود. البته این ثبت اطلاعات باید به شکل خودکار و از طریق سامانه‌های هوشمند انجام شود.

مطلب پیشنهادی

طراحی یک سامانه ضدنفوذ
رمزنگاری کوانتومی چالش نفوذ داده‌ای را درهم می‌شکند

امنیت فنی شبکه

کنترل‌های امنیتی فنی از داده‌هایی که در شبکه ذخیره می‌شوند یا به داخل یا خارج از شبکه انتقال پیدا کرده، محافظت می‌کنند. در بحث امنیت فنی باید به دو اصل مهمی که بسیاری از سازمان‌ها آن را نادیده می‌گیرند، توجه داشته باشیم: اول محافظت از داده‌ها و سیستم‌ها در مقابل افرادی که هنوز احراز هویت نشده‌اند، اما قصد دارند به منابع شبکه دسترسی داشته باشند (کارمندان تازه وارد به یک سازمان) و دیگری محافظت از منابع شبکه در برابر کارمندانی که قصد انجام فعالیت‌های مخرب را دارند.

خط‌مشی‌های مدیریتی

کنترل‌های امنیت اداری شامل خط‌مشی‌های امنیتی و فرآیندهایی است که رفتار کاربران را کنترل می‌کنند که از آن جمله می‌توان به چگونگی تأیید هویت کاربران، سطح دسترسی آن‌ها و چگونگی اعمال تغییرات از سوی کارمندان بخش فناوری‌اطلاعات اشاره کرد. در بحث خط‌مشی‌های مدیریتی ضروری است که سطوح مختلفی از دسترسی برای مدیران تعریف شود. همه مدیران یک سازمان یا حتی یک موسسه نباید به یک شکل به منابع و کل شبکه دسترسی داشته باشند.

رویکردهای مختلف امنیتی

درباره انواع مختلف کنترل‌های امنیتی شبکه توضیح داده شد. اکنون اجازه دهید اشاره‌ای داشته باشیم به برخی از روش‌های مختلفی که می‌توانید با استفاده از آن‌ها شبکه خود را امن کنید.

کنترل دسترسی به شبکه

برای اطمینان از این‌که مهاجمان نمی‌توانند به شبکه‌ای نفوذ کنند، خط‌مشی‌های جامع کنترل دسترسی باید برای هر

دو نهاد شبکه یعنی کاربران و دستگاه‌ها به‌درستی تدوین شود. کنترل دسترسی به شبکه (NAC) را می‌توان با جزئیات دقیقی ترسیم کرد. برای مثال، یک مدیر شبکه می‌تواند به مدیران اجرایی دسترسی کامل به شبکه را تخصیص دهد، اما دسترسی به پوشه‌های محرمانه و خاص را ممنوع کرده یا مانع از آن شود تا افراد دستگاه‌های شخصی خود را به شبکه متصل کنند.

انواع راهکارهای قابل استفاده در بحث امنیت شبکه

محافظت از یک شبکه سازمانی با یک شبکه خانگی کاملا متفاوت است. یک شبکه خانگی متشکل از یک روتر و چند دستگاه کلاینتی است که برای برقراری ارتباط با یکدیگر و اتصال به شبکه از آن‌ها استفاده می‌شود. البته برخی از کاربران خانگی از یک سوییچ برای مدیریت بهتر تجهیزات استفاده می‌کنند. اما در مقیاس کلان و سازمانی با تجهیزات، نرم‌افزارها و افراد مختلفی سروکار دارید که هر یک ممکن است خواسته یا ناخواسته باعث بروز مشکل شوند. به همین دلیل است که سازمان‌ها برای محافظت از زیرساخت‌ها و حفظ امنیت شبکه‌شان از راهکارها و فناوری‌های زیر استفاده می‌کنند: Antivirus and Antimalware Software؛ نرم‌افزار ضدویروس و ضدباج‌افزارApplication Security؛امنیت برنامه‌های کاربردی Behavioral Analytics؛ ابزارهای تجزیه‌وتحلیل الگوهای رفتاری که عمدتاً بر پایه یادگیری ماشین کار می‌کنند.
DLP (سرنام Data Loss Prevention)؛ پیشگیری از نشت (از دست رفتن) اطلاعاتEmail Security؛ امنیت ایمیلFirewalls؛ دیواره‌های آتشMobile Device Security؛ امنیت دستگاه‌های همراه Network Segmentation؛ تقسیم کردن شبکه به بخش‌های مختلف، رویکردی که شبکه به زیر شبکه‌هایی تقسیم می‌شود که فرآیند مدیریت آن‌ها ساده‌تر می‌شود. SIEM (سرنام Security Information and Event Management)؛ مدیریت امنیت اطلاعات و رخدادها VPN(سرنام Virtual Private Network)؛ شبکه خصوصی مجازیWeb Security؛ امنیت وبWireless Security؛ امنیت بی‌سیمEndpoint Security؛ امنیت نقطه پایانی NAC(سرنام Network Access Control)؛ کنترل دسترسی به شبکه

مطلب پیشنهادی

دفاع در برابر سوء استفاده
چگونه از کامپیوترمان در برابر دزد کدها و ماینرها محافظت کنیم؟

نرم‌افزارهای ضدویروسی و ضدبدافزاری

نرم‌افزارهای ضدویروس و ضدبدافزار از یک سازمان در برابر طیف گسترده‌ای از نرم‌افزارهای مخرب همچون ویروس‌ها، باج‌افزارها، کرم‌ها و تروجان‌ها محافظت می‌کنند. یک نرم‌افزار امنیتی خوب نه تنها فایل‌ها را پس از ورود به شبکه پویش می‌کند، بلکه به‌طور پیوسته فرآیند پویش را انجام داده و هرگونه تغییری را روی فایل‌ها به‌دقت زیر نظر می‌گیرد.

امنیت برنامه‌های کاربردی

مهم است که مقوله امنیت برنامه‌های کاربردی جدی قلمداد شود، زیرا هیچ برنامه‌ای کامل نیست. هر برنامه‌ای ممکن است شامل آسیب‌پذیری‌ها یا رخنه‌هایی باشد که توسط مهاجمان برای ورود به شبکه استفاده می‌شود. بنابراین، در بحث امنیت برنامه‌های کاربردی پیشنهاد می‌شود پیش از استقرار، ابتدا برنامه‌ها برای مدتی در یک محیط ایزوله شده اجرا شوند تا موارد مشکوک آن‌ها شناسایی شود.

تجزیه‌وتحلیل رفتاری

برای شناسایی رفتارهای غیرمعمول در شبکه ارزیابی رفتاری انجام می‌شود. یک مدیر شبکه یا امنیت باید درک درستی از رفتارهای طبیعی و غیرطبیعی داشته باشد. ابزارهای تجزیه‌وتحلیل رفتاری به‌طور خودکار فعالیت‌های خارج از عرف را شناسایی می‌کنند. تحلیل‌های ارائه شده از سوی این ابزارها به تیم امنیتی کمک می‌کند، فاکتورهایی را که زمینه‌ساز یک مشکل بالقوه می‌شوند، شناسایی کرده و تهدیدات را به‌سرعت برطرف می‌کنند. توجه داشته باشید،

تحلیل الگوهای رفتاری مختص به ارزیابی نرم‌افزارها نیست و رفتارهای کاربران را شامل می‌شود. شرکت F-Secure یکی از پیشگامان ارائه ابزارهای هوشمندی است که چنین سرویسی را ارائه می‌کند.

پیشگیری از نشت اطلاعات (DLP)

سازمان‌ها به‌ویژه آن‌هایی که سروکارشان با اطلاعات حساس است باید در اساسنامه خود به‌وضوح به این مسئله اذعان کرده باشند که کارمندانشان اطلاعات حساس را به خارج از شبکه ارسال نخواهند کرد. چنین سازمان‌هایی باید از فناوری DLP و سنجه‌های امنیتی استفاده کنند تا مانع از آن شوند که اطلاعات به شکل غیر ایمن آپلود شده، ارسال‌شده یا حتی چاپ شود.

امنیت ایمیل

در بحث نقض‌های امنیتی و رخنه‌ها، برای هر سازمانی ایمیل تهدید شماره یک است. مهاجمان از تاکتیک‌های مهندسی اجتماعی و اطلاعات شخصی استفاده می‌کنند تا کمپین‌های فیشینگ دقیق و درست را برای فریب قربانیان پیاده‌سازی کرده و آن‌ها را به بازدید از سایت‌هایی ترغیب کنند که نرم‌افزارهای مخرب یا اسکریپت‌های مخرب روی آن‌ها میزبانی شده است. یک برنامه امنیتی ایمیل می‌تواند این حملات ورودی را تشخیص داده و بر روند ارسال پیام‌های خروجی مدیریت دقیقی را اعمال کند تا اطلاعات حساس به خارج از سازمان نشت پیدا نکنند.

حفاظت از طریق پیاده‌سازی یک دیوارآتش

دیوارهای آتش، همان‌گونه که از نامشان مشهود است میان یک شبکه خارجی غیرقابل اعتماد و شبکه داخلی یک سازمان، دیواری ترسیم می‌کنند. به‌طورمعمول، مدیران شبکه یک دیوارآتش را بر مبنای مجموعه‌ای از قواعد منطبق با استراتژی‌های سازمانی پیکربندی می‌کنند که این قواعد مانع از آن می‌شوند تا ترافیک مشکوک به درون شبکه‌ای وارد شده یا برعکس از آن خارج شوند. به‌عنوان‌مثال، دیوارهای آتش نسل بعد NGFW (سرنام Next Generation Firewall) یک کنترل یکپارچه و متمرکز را روی ترافیک شبکه اعمال می‌کنند. در کنار دیوارآتش، سامانه‌های پیشگیری از نفوذ (IPS) نیز برای تامین امنیت شبکه استفاده می‌شوند. این ابزارها می‌توانند ترافیک شبکه را به‌منظور مسدود کردن یک حمله فعال پویش کنند.

امنیت دستگاه‌های همراه

دستگاه‌ها و برنامه‌های همراه به‌طور فزاینده‌ای مورد توجه هکرها هستند، زیرا سازمان‌ها به‌تدریج رویکرد BYOD یا همان استفاده از دستگاه‌های همراه کارکنان را به رسمیت می‌شناسند.[1]
انتظار می‌رود در آینده نزدیک بیش از 90% از سازمان‌های فناوری‌اطلاعات از این رویکرد به‌طور رسمی پشتیبانی کنند. به همین دلیل باید یک مدیر شبکه کنترل کند که چه دستگاه‌هایی می‌توانند به شبکه دسترسی پیدا کنند. همچنین لازم است برای محافظت از ترافیک شبکه ارتباطات این دستگاه‌ها به‌درستی پیکربندی شود.

تقسیم کردن/بخش‌بندی شبکه

یکی از مهم‌ترین و در عین حال پیچیده‌ترین فازهای طراحی شبکه، بخش‌بندی شبکه است. بخش‌بندی نرم‌افزار ـ محور تعیین می‌کند که ترافیک شبکه باید به طبقه‌بندی‌های متنوعی تقسیم شود تا خط‌مشی‌های امنیتی به شکل ساده‌ای قابل اجرا و پیگیری باشند. این طبقه‌بندی ترافیک بر پایه شناسه، هویت نقطه پایانی و آدرس‌های آی‌پی انجام می‌شود. در این میان مجوزها می‌توانند بر مبنای نقش‌ها، موقعیت مکانی و صلاحیت افراد تخصیص داده شده و دسترسی هرگونه دستگاه مشکوکی به شبکه تا روشن شدن وضعیت آن به حالت تعلیق درآمده یا کاملا محدود شود.

مدیریت امنیت اطلاعات و رخدادها (SIEM)

محصولات SIEM هرگونه اطلاعاتی را که یک کارمند امنیتی برای شناسایی و واکنش به تهدیدات به آن نیاز دارد، جمع‌آوری کرده و در اختیارش قرار می‌دهد. این محصولات در قالب‌های مختلف، از جمله تجهیزات مجازی، فیزیکی و نرم‌افزارهای سرور در دسترس هستند.

امنیت وب

یک راهکار کامل امنیتی وب بر روند دسترسی کارمندان به وب‌سایت‌هایی که بازدید می‌کنند، کمک می‌کند. پس بهتر است کنترل کامل‌تری داشته باشید و مانع از آن شوید که افراد به وب‌سایت‌های مخرب یا مسدود شده دسترسی پیدا کنند.

امنیت بی‌سیم

جنبش تجهیزات همراه در تعامل با شبکه‌های بی‌سیم و اکسس‌پوینت‌ها فراگیر شده است. با این‌حال، شبکه‌های بی‌سیم به‌اندازه شبکه‌های سیمی ایمن نیستند و این پتانسیل را دارند تا راه ورود هکرها به شبکه سازمان را هموار کنند. به همین دلیل، شبکه‌های بی‌سیم باید در امنیت بسیار بالایی پیاده‌سازی شده و به کار گرفته شوند. بدون توجه به تمهیدات امنیتی دقیق پیاده‌سازی و به‌کارگیری یک شبکه بی‌سیم می‌تواند شبیه به حالتی باشد که شما پورت‌های اترنت را در هر مکانی از ساختمان قرار داده‌اید. محصولاتی که به‌طور خاص برای حفاظت از یک شبکه بی‌سیم طراحی شده‌اند به میزان قابل‌توجهی مانع از بروز حملات رایج می‌شوند.

مطلب پیشنهادی

بایدها و نبایدهای مکانیسم احراز هویت دوعاملی
مکانیسم احراز هویت دوعاملی چیست و چرا سازمان‌ها از آن استفاده می‌کنند؟

امنیت نقطه پایانی

امنیت نقطه پایانی که به نام‌های حفاظت نقطه پایانی یا امنیت شبکه از آن یاد می‌شود، یک روش شناخته‌شده برای محافظت از شبکه‌های سازمانی در مواقعی است که دستگاه‌های راه دور مانند لپ‌تاپ‌ها یا سایر دستگاه‌های بی‌سیم و همراه قصد اتصال به شبکه را دارند. به‌عنوان‌مثال، محصول
Comodo Advanced Endpoint Protection Software یک مکانیزم دفاعی هفت لایه است که شامل File Reputation، Viruscope، جعبه شن خودکار، پیشگیری از نفوذ به میزبان، فیلترسازی آدرس‌های وب، دیوارآتش و ضدویروس است. همه این مولفه‌ها در قالب یک محصول واحد برای مقابله با تهدیدات شناخته و ناشناخته برای محافظت از یک شبکه استفاده می‌شوند.

کنترل دسترسی به شبکه

فرآیند برقراری امنیت شبکه به شما کمک می‌کند تا کنترل کنید که چه کسی می‌تواند به شبکه دسترسی پیدا کند. ضروری است پیش از آن‌که به هر دستگاه یا کاربری اجازه دسترسی به شبکه را بدهید، ابتدا او را شناسایی کنید تا خطر دسترسی یک هکر به شبکه را به حداقل برسانید. این استراتژی کمک می‌کند تا خط‌مشی‌های امنیتی را به‌درستی اجرا کنید. بهتر است دسترسی دستگاه‌های ناسازگار با شبکه محدود یا کاملا قطع شود.

شبکه خصوصی مجازی

شبکه‌های خصوصی مجازی می‌توانند میان دو نقطه پایانی درون یک شبکه ارتباط ایمنی را ایجاد کنند. به‌عنوان‌مثال، کاربران می‌توانند از درون خانه خود به شبکه خصوصی سازمان متصل شده و کارهایشان را انجام دهند. بر مبنای این رویکرد، فرآیند انتقال داده‌ها میان دو نقطه به شکل رمزگذاری شده انجام شده و کاربر برای برقراری ارتباط با شبکه سازمان و برقراری ارتباط با دستگاه‌های مختلف احراز هویت می‌شود

پی‌نوشت:
1. برای آشنایی با BYOD می‌توانید به مطلب زیر در سایت شبکه مراجعه کنید:
http://bit.ly/2RHkqyg

منبع:

comodo
forcepoint
تاریخ انتشار:
16 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16007/%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87-%DA%86%DB%8C%D8%B3%D8%AA%D8%9F