آموزش امنیت شبکه؛ محافظت از شبکه در برابر حملات سایبری

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

هر روز چندین مورد نقص امنیت شبکه در سراسر جهان رخ می‌دهد. برخی از آن‌ها بسیار جزئی هستند و شامل از دست دادن اطلاعات یا سرمایه می‌شوند، اما بسیاری از آن‌ها بسیار بزرگ و فاجعه بارند. هکرها دائما به دنبال نقاط آسیب پذیر در شرکت‌ها و سازمان‌ها هستند. وقتی شبکه‌ها ایمن نباشند، اطلاعات مربوط به سازمان‌ها، افراد و حتی دولت‌ها در معرض خطر قرار می‌گیرد. سازمان‌ها برای محافظت از شبکه‌های کامپیوتری خود اقدامات امنیتی را اجرا می‌کنند و با افزایش تعداد حملات سایبری، دانش و تخصص آن‌ها در این راه بسیار اهمیت میابد. اگر در حوزه فناوری اطلاعات فعالیت می‌کنید، مهم است که با آموزش امنیت شبکه آشنا باشید تا از سازمان خود در برابر حملات سایبری محافظت کنید. در این مقاله با آموزش امنیت شبکه همراه ما باشید.

امنیت شبکه چیست؟

امنیت شبکه به اقدامات پیشگیرانه‌ای گفته می‌شود که از زیرساخت شبکه در برابر دسترسی غیرمجاز و افشای اطلاعات محافظت می‌کند. اجرای این اقدامات به کامپیوترها، کاربران و برنامه‌ها اجازه می‌دهد تا وظایف خود را در یک محیط امن انجام دهند. ایمن سازی شبکه به ترکیبی پیچیده از دستگاه‌های سخت افزاری مانند روترها، فایروال‌ها و برنامه‌های نرم افزاری نیاز دارد. کارشناسان امنیت اطلاعات اقدامات لازم را جهت اجرای برنامه‌های امنیتی و نظارت بر اثربخشی آن‌ها انجام می‌دهند.

چرا امنیت شبکه مهم است؟

امنیت شبکه در شبکه‌های خانگی و همچنین در دنیای تجارت اهمیت ویژه‌ای دارد. اینترنت پرسرعت با یک یا چند روتر بی‌سیم در بیشتر خانه‌ها وجود دارد که در صورت عدم ایمنی مناسب، مورد سوء استفاده قرار می‌گیرند. سیستم امنیتی شبکه به کاهش خطر از دست دادن داده و سرقت اطلاعات کمک می‌کند. آموزش امنیت شبکه سازمان را قادر می‌سازد تا محصولات و خدمات را به صورت ایمن ارائه دهد و این نوع حفاظت اولین خط دفاعی در برابر تمام تهدیدات سایبری است:

حملات DDoS: این حملات با دستکاری ترافیک شبکه، در فرایند پردازش سرویس‌ها اختلال ایجاد می‌کند.

بدافزار: آلودگی‌های بدافزار شامل انواع مختلف باج‌افزار و جاسوس‌افزارها می‌شود.

حملات داخلی: تهدیدات داخلی زمانی اتفاق می‌افتند که کارمندان به طور تصادفی یا عمدی به شبکه آسیب می‌زنند یا داده‌ها را افشا می‌کنند.

تهدیدات پایدار پیشرفته (APT): حمله APT یک تهدید سایبری خطرناک است که معمولا در شبکه‌های آسیب پذیر صورت می‌گیرد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

نقاط آسیب پذیر: مهاجمان نقاط ضعف را در ورودی برنامه‌ها یا دستگاه‌ها هدف قرار می‌دهند تا به داخل شبکه نفوذ کنند.

آموزش امنیت شبکه یک ضرورت برای کسب و کارهاست

نقشه برداری منظم

مدیر شبکه باید درک روشنی از زیرساخت شبکه داشته باشد تا سیستم دفاعی مناسب را تنظیم کند. بهتر است اطلاعاتی را درباره مدل‌ها و پیکربندی‌های زیر داشته باشید:

- فایروال‌ها
- روترها
- سوئیچ‌ها
- کابل کشی
- پورت‌ها
- نقاط دسترسی

همچنین، مدیر باید تمام دستگاه‌های متصل (سرورها، رایانه‌ها، چاپگرها و غیره) و مسیر اتصال آن‌ها را از طریق شبکه بداند. نقشه برداری شبکه به شناسایی نقاط ضعف بالقوه و راه‌های بهبود ایمنی، عملکرد و قابلیت اطمینان شبکه کمک می‌کند. با این روش تجزیه و تحلیل دقیقی از روش‌های دفاعی خود خواهید داشت.

بخش بندی شبکه

تقسیم بندی شبکه را به زیر مجموعه‌های کوچک‌تر تقسیم می‌کند. هر زیرشبکه به عنوان یک سیستم مستقل با ویژگی‌های امنیتی و قوانین دسترسی مخصوص به خود عمل می‌کند. این اقدام مانع از حرکت آزادانه ویروس و مهاجم در سیستم می‌شود. اگر هکر بخشی از یک شبکه را مورد هدف قرار دهد، سایر بخش‌ها در خطر نخواهند بود.

از رمزهای عبور قوی استفاده کنید

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

انتخاب نامناسب رمز عبور شکاف‌های امنیتی خطرناکی ایجاد می‌کند. گذرواژه‌های ضعیف انجام حملات را آسان‌تر می‌کنند، تهدیدهای داخلی مخرب را افزایش می‌دهند و مهاجم را قادر می‌سازند تا راحت به شبکه دسترسی پیدا کند.

کارمندان باید از رمزهای عبور پیچیده و منحصر به فرد استفاده کنند و هر چند هفته یک‌بار آن را تغییر دهند. همچنین، در مورد به اشتراک گذاشتن رمز عبور به کارمندان هشدار دهید. برای ساده کردن این فرایند، استفاده از یک برنامه مدیریت رمز عبور سازمانی را در نظر بگیرید.

ایجاد آگاهی

کارمندان باید نقش و مسئولیت خود را در حفظ امنیت شبکه بدانند؛ چرا که آن‌ها همان خط دفاعی را در سازمان تشکیل می‌دهند، بنابراین به آن‌ها آموزش دهید تا:

- برای جلوگیری از حملات فیشینگ، روی لینک‌ها و ایمیل‌های ناشناس کلیک نکنید.
- فقط به شبکه‌های Wi-Fi ایمن متصل شوید.
- هرگز فایروال‌ها و نرم افزارهای آنتی ویروس را غیرفعال نکنید.
- حساب‌های قدیمی و غیرقابل استفاده را حذف کنید.
- به مقررات امنیتی شبکه احترام بگذارید.
- اگر مشکلی پیش آمد سریعا با تیم امنیتی مشورت کنید.
- اطمینان حاصل کنید که کارمندان از سیاست‌های امنیتی مطلع هستند و به آن‌ها دسترسی دارند.

نرم افزار را به روز نگه دارید

تمام نرم افزارهای شبکه باید آپدیت باشند تا در برابر آخرین تهدیدات به خوبی از خود دفاع کنند. بهتر است روی یک یک سیستم مدیریتی سرمایه گذاری کنید تا تمام نرم افزارهای شبکه را همیشه به روز نگه دارد.

امنیت Zero Trust

از این قابلیت برای محدود کردن دسترسی کاربر به داده‌های مهم استفاده کنید. کاربران باید فقط به داده‌هایی که برای انجام کارهای خود نیاز دارند، دسترسی داشته باشند. Zero Trust از شبکه و داده‌های آن در برابر خطرات

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

بیرونی و داخلی محافظت می‌کند. این پلتفرم به شرکت‌ها کمک می‌کند تا قوانین حفظ حریم خصوصی و امنیت داده‌ها را رعایت کنند.

امنیت شبکه برای کسب و کارها

هر سازمانی که با شبکه و برنامه سروکار دارد باید امنیت شبکه را در اولویت قرار دهد. امنیت شبکه نه تنها می‌تواند از یکپارچگی اطلاعات در برابر فعالیت‌های مخرب محافظت کند، بلکه ترافیک شبکه را به بهترین نحو تنظیم می‌کند، سرعت شبکه را بهبود می‌بخشد و تبادل امن داده‌ها را امکان پذیر می‌کند. ابزارها و برنامه‌های مختلفی از شبکه در برابر این حملات مخرب محافظت می‌کنند. رهاکو مجموعه‌ای از راهکارهای امنیت شبکه را ارائه می‌دهد که عملیات پیچیده را متمرکز و ساده کرده و در عین حال از شبکه در سراسر سازمان محافظت می‌کند.

مزایای امنیت شبکه

فرآیند محافظت از شبکه مستلزم حذف هرگونه سوء استفاده یا دسترسی غیرقانونی به شبکه یا اجزای آن است. در ادامه چند مورد از مزایای امنیت شبکه را بررسی می‌کنیم.

محافظت در برابر حملات سایبری

اینترنت منبع بیشتر حملات شبکه است. انواع مختلفی از حملات باج افزار و بدافزار وجود دارند و در صورت سهل انگاری شبکه با مشکلات جدیدی مواجه خواهند شد. با آموزش امنیت شبکه می‌توان در زمان درست از این حملات جلوگیری کرد.

سطوح دسترسی

کاربران مختلف سطوح دسترسی متفاوتی به نرم افزار امنیتی دارند. پس از احراز هویت، تعیین می‌شود که آیا کاربر می‌تواند به منابع خاصی دسترسی داشته باشد یا خیر. این برنامه به وضوح مشخص می‌کند که چه کسی به چه چیزی دسترسی دارد.

ایمن نگه داشتن داده‌ها

همانطور که قبلا گفته شد، امنیت شبکه از دسترسی غیرقانونی جلوگیری می‌کند. یک شبکه حاوی مقدار زیادی اطلاعات حساس مانند اطلاعات مشتری است. هر کسی که به شبکه دسترسی پیدا کند ممکن است این داده‌های حساس را به خطر بیندازد. در نتیجه، قابلیت‌های امنیت شبکه باید از آن‌ها محافظت کند.

به روز رسانی متمرکز

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

به روز نگه داشتن نرم افزار آنتی ویروس بسیار مهم است. نسخه قدیمی به اندازه کافی در برابر مهاجمان از شبکه محافظت نمی‌کند. یک سیستم امنیتی شبکه متمرکز مزایایی مانند به روزرسانی به موقع را نیز ارائه می‌دهد.

نتیجه گیری

تقریبا تمام شرکت‌ها در سراسر جهان از اینترنت و شبکه‌های کامپیوتری استفاده می‌کنند. حملات سایبری به سرعت در حال افزایش هستند و گاهی غیرقابل کنترل می‌شوند. بنابراین، سازمان‌ها از امنیت شبکه برای محافظت از داده‌های حساس و محرمانه استفاده می‌کنند. از دست دادن چنین داده‌هایی برای شرکت بسیار هزینه بر خواهد بود، از این رو، همه سازمان‌ها باید یک سیستم امنیت شبکه خوب داشته باشند. آموزش امنیت شبکه برای شما مفید خواهد بود. این آموزش اطلاعات شما را به عنوان یک تحلیلگر امنیت شبکه غنی می‌کند و در آینده شغلی بسیار موثر است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net