انواع امنیت شبکه؛ حفاظت از داده‌های ارزشمند شما در مقابل تهدیدات داخلی و خارجی

مجموعه شرکت‌های دانش بنیان رها

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

فهرست

حتما تا به حال اخبار بسیاری در مورد حملات سایبری شنیده‌اید و اینکه چگونه این مشکلات می‌توانند منجر به زیان مالی یا آسیب به اعتبار یک سازمان شوند. تنها راه محافظت از اطلاعات و منابع مهم، محدودسازی دسترسی به فایل‌ها، شبکه‌ها و سایر منابع محرمانه است؛ اینجاست که مفهوم امنیت شبکه مطرح می‌شود.

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

امنیت شبکه در حال حاضر بیش از هر زمان دیگری اهمیت دارد و انواع رایج آن عبارتند از: کنترل دسترسی به شبکه، سیاست‌های امنیتی فناوری اطلاعات، امنیت برنامه، شناسایی نقطه پایان (EDR)، امنیت ایمیل، تقسیم بندی شبکه، SIEM و امنیت وب. اما چگونه می‌توان شروع کرد؟ در سال 2022 سریع‌ترین و مقرون به صرفه‌ترین راه برای ایجاد یک شبکه امن چیست؟

در این مقاله، توضیح می‌دهیم که امنیت شبکه چیست و انواع مختلف آن کدام است؟ هم‌چنین، مؤلفه‌های مورد نیاز سازمان‌ها جهت پیاده سازی یک برنامه امنیتی موثر را بررسی خواهیم کرد.

چرا امنیت شبکه مهم است؟

سال 2020 سالی پر از خبرها و اتفاقات غیرمنتظره در سراسر جهان بود. شیوع بیماری کووید-19 به معنای واقعی کلمه نحوه عملکرد کسب و کارها را تغییر داد. کارمندانی که زمانی در اتاق‌ها یا پشت میزها مشغول به کار بودند، برای یک دوره زمانی نامشخص مجبور به دورکاری شدند.

در این میان، برخی مشاغل با استفاده از مجازی سازی به خوبی با این شرایط سازگار شده‌اند. با این حال، حملات سایبری همچنان ادامه داشت؛ در واقع فرصت دیگری برای این حملات در این شرایط فراهم شد. بخاطر این مشکلات بود که امنیت شبکه در دنیای تجارت جایگاه ویژه‌ای پیدا کرد. سیستم امنیتی شبکه به خطر از دست رفتن و سرقت داده ها را به حداقل می‌رساند.

حفاظت از داده‌های ارزشمند یک اصل اساسی برای کسب‌وکارهاست و امنیت شبکه این امکان را برای کارمندان فراهم کرده است تا حتی بدون حضور در محل کار، از راه دور به داده‌ها و برنامه‌ها دسترسی داشته باشند و نگران از دست رفتن اطلاعات مهم نباشند.

انواع امنیت شبکه را بشناسید

انواع مختلف امنیت شبکه عبارتند از:

- کنترل دسترسی شبکه (NAC)
- امنیت برنامه
- سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS)
- سیستم تشخیص نفوذ شبکه
- پیشگیری از دست رفتن داده ها (DLP)
- نرم افزار آنتی ویروس
- تشخیص و پاسخ نقطه پایانی (EDR)

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

- امنیت ایمیل
- فایروال
- امنیت بی سیم
- IDS/IPS
- تقسیم شبکه
- SIEM
- امنیت وب
- احراز هویت چند عاملی (MFA)
- شبکه خصوصی مجازی (VPN)

نرم افزار آنتی ویروس و ضد بدافزار:

نرم افزاری که از سیستم‌ها در برابر ویروس، حملات تروجان و غیره محافظت می‌کند، یک آنتی ویروس است. هر بار که فایل جدیدی در سیستم نصب می‌شود این نرم افزار آن را اسکن می‌کند. هم‌چنین، در صورت مشاهده هرگونه برنامه یا داده ویروسی، مشکل مربوطه را شناسایی و برطرف می‌نماید.

پیشگیری از دست رفتن داده:

سازمان‌های بزرگ، داده‌های محرمانه و اطلاعات داخلی خود را به نحوی حفظ می‌کنند که توسط هیچ یک از کارکنان به خارج درز نکند. این کار با فناوری DLP انجام می‌شود که در آن مدیر شبکه دسترسی کارمندان به اطلاعات را محدود می‌کند تا هیچکس امکان ارسال، آپلود یا حتی چاپ اطلاعات را نداشته باشد.

امنیت ایمیل:

مهاجمان می‌توانند با ارسال یک ایمیل، ویروس یا بدافزار را به شبکه شما وارد کنند. یک نرم افزار امنیت ایمیل پیام‌های دریافتی را اسکن کرده و داده‌های مشکوک را فیلتر می‌کند. هم‌چنین، وظیفه کنترل خروجی پیام‌ها را برعهده دارد.

فایروال‌ها:

فایروال‌ها بخش جدایی ناپذیر سیستم شبکه هستند و به عنوان یک دیوار میان دو شبکه یا دو دستگاه عمل می‌کند. درواقع، مجموعه‌ای از قوانین از پیش تعریف شده‌اند که برای جلوگیری از هرگونه دسترسی غیرمجاز به شبکه مورد استفاده قرار می‌گیرند.

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

فایروال‌ها دو نوع هستند: سخت افزار و نرم افزار. نرم افزار فایروال در سیستم نصب می‌شود تا از آن در برابر تهدیدات محافظت کند. فایروال سخت افزاری به عنوان دروازه‌ای بین دو سیستم عمل می‌کند به طوری که تنها یک کاربر به شبکه و منابع آن دسترسی دارد.

سیستم تشخیص نفوذ شبکه (IPS):

این سیستم امنیتی شامل مجموعه‌ای از قوانین است که با رعایت آن‌ها به راحتی می‌توانید تهدیدات را شناسایی کرده و دسترسی آن‌ها را بلاک نمایید.

امنیت موبایل:

مجرمان سایبری به راحتی می‌توانند لینک‌های ناامن را به گوشی‌های تلفن همراه ارسال کنند. از این رو لازم است یک آنتی ویروس بر روی موبایل نصب شود. علاوه بر این، افراد باید داده‌ها را فقط از منابع معتبر و وب‌سایت‌های امن دانلود کنند.

تقسیم شبکه:

از نظر امنیتی، یک سازمان داده‌های مهم خود را به دو یا سه قسمت تقسیم و در منابع مختلف نگهداری می‌کند. اگر در بدترین حالت، داده‌ها توسط یک حمله ویروسی خراب یا حذف شوند، می‌توان دوباره آن را از منبع پشتیبان بازیابی کرد.

امنیت وب:

امنیت وب یعنی محدود سازی وب‌سایت‌هایی که در برابر ویروس‌ها و هکرها آسیب پذیرتر هستند. بنابراین، این نوع از امنیت شبکه اساسا به کنترل تهدیدهای مبتنی بر وب می‌پردازد.

امنیت نقطه پایانی:

امنیت نقطه پایانی از دستگاه‌هایی مانند رایانه، لپ‌تاپ، تلفن‌های همراه و تبلت‌ها در برابر تهدیدات مخرب و حملات سایبری محافظت می‌کند. نرم‌افزار امنیتی Endpoint نیز برای همین منظور استفاده می‌شوند و از دستگاه‌ها در شبکه یا فضای ابری محافظت می‌کنند.

کنترل دسترسی:

شبکه باید به گونه‌ای طراحی شود که افراد نتوانند به منابع دسترسی داشته باشند. این کار با رمز عبور، نام کاربری اختصاصی و فرآیند احراز هویت انجام می‌شود و با اجرای آن می‌توان دسترسی‌های مختلف به شبکه را کنترل کرد.

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

شبکه خصوصی مجازی (VPN):

اتصال VPN یک ارتباط امن بین شما و اینترنت برقرار می‌کند. ترافیک داده‌های شما از طریق یک تونل مجازی رمزگذاری شده هدایت می‌شود. با این روش نشانی IP شما هنگام استفاده از اینترنت پنهان می‌شود و موقعیت قابل تشخیص نخواهد بود. VPN در برابر حملات خارجی بسیار ایمن است و یکی از ابزارهای قدرتمند امنیت شبکه محسوب می‌شود.

:UTM

واژه UTM به معنای سامانه مدیریت یکپارچه تهدیدات است. UTM در دسته فایروال‌های نسل ۳ که اصطلاحا به آن‌ها فایروال‌های نسل بعد گفته می‌شود، جای می‌گیرد. در این سامانه انواع سیستم‌های نظارتی و امنیتی نیز قرار دارند. با استفاده از UTM، شبکه شما با چندین ابزار مختلف از جمله آنتی ویروس، فیلتر محتوا، فیلتر ایمیل، آنتی اسپم و غیره محافظت می‌شوند.

نتیجه گیری

تمام سازمان‌ها باید برنامه‌هایی برای امنیت شبکه به منظور ایمن سازی و جلوگیری از حملات سایبری داشته باشند. بیش از هر زمان دیگری، فرصتی برای تیم‌های امنیتی فراهم شد تا در رویکرد خود برای ایمن سازی شبکه‌ها نوآورانه عمل کنند.

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