# امنیت شبکه چیست؟

امنیت شبکه چیست؟ امنیت شبکه یک اصطلاح گسترده است که شامل بسیاری از فناوری‌ها، دستگاه‌ها و فرایندها می‌شود. در ساده‌ترین حالت، مجموعه‌ای از قوانین و تنظیمات است که برای محافظت از یکپارچگی، محرمانه بودن و دسترسی شبکه‌ها و داده‌های رایانه‌ای با استفاده از فناوری‌های نرم افزاری و سخت افزاری طراحی شده است. هر سازمانی، صرف نظر از اندازه، صنعت یا زیرساخت‌ها، به درجه ای از راه‌حل‌های امنیت شبکه نیاز دارد تا از چشم انداز روزافزون تهدیدهای سایبری امروزه در طبیعت محافظت کند.

معماری شبکه امروزی پیچیده است و با محیطی تهدیدآمیز که همیشه در حال تغییر است و مهاجمانی که همیشه در تلاش برای یافتن و بهره برداری از آسیب پذیری‌ها هستند، روبرو می‌باشد. این آسیب پذیری‌ها می‌توانند در تعداد زیادی از مناطق از جمله دستگاه‌ها ، داده‌ها، برنامه‌ها، کاربران و مکان‌ها وجود داشته باشند. به همین دلیل، امروزه بسیاری از ابزارها و برنامه‌های مدیریت امنیت شبکه مورد استفاده قرار می‌گیرند که تهدیدها و سوء استفاده‌های فردی و همچنین عدم رعایت مقررات را برطرف می‌کند. هنگامی که فقط چند دقیقه تعطیلی می‌تواند باعث اختلال گسترده و خسارت گسترده به نتیجه و شهرت یک سازمان شود، ضروری است که این اقدامات حفاظتی انجام شود.

## امنیت شبکه چگونه کار می‌کند؟

در زمان انجام عملیات جهت امنیت شبکه لایه‌های زیادی در سراسر سازمان، باید در نظر گرفته شود. حملات ممکن است در هر لایه‌ای در مدل لایه‌های امنیتی شبکه اتفاق بیفتد، بنابراین سخت افزار، نرم افزار و خط مشی‌های امنیتی شبکه شما باید طوری طراحی شود که به هر منطقه پاسخ دهد.

امنیت شبکه معمولاً شامل سه کنترل مختلف است: فیزیکی، فنی و اداری. در اینجا شرح مختصری از انواع مختلف امنیت شبکه و نحوه عملکرد هر یک به اختصار توضیح داده شده است.

- **امنیت شبکه فیزیکی**

کنترل‌های امنیتی فیزیکی برای جلوگیری از دسترسی افراد غیر مجاز به اجزای شبکه مانند روترها، کابینت کابل و غیره طراحی شده است. دسترسی کنترل شده مانند قفل‌ها، احراز هویت بیومتریک و سایر دستگاه‌ها در هر سازمانی ضروری است.

- **امنیت شبکه فنی**

کنترل‌های فنی از داده‌هایی که در شبکه ذخیره می‌شوند یا در حال انتقال به داخل، یا خارج از شبکه هستند محافظت می‌کند. حفاظت دوگانه است؛ باید از داده‌ها و سیستم‌ها در برابر پرسنل غیر مجاز محافظت کند و همچنین باید در برابر فعالیت‌های مخرب کارکنان محافظت کند.

- **امنیت شبکه اداری**

کنترل‌های امنیتی اداری شامل سیاست‌ها و فرایندهای امنیتی است که رفتار کاربران را کنترل می‌کند، از جمله نحوه احراز هویت کاربران، سطح دسترسی آن‌ها و همچنین نحوه اعمال تغییرات کارکنان فناوری اطلاعات در زیرساخت‌ها.

## انواع امنیت شبکه

ما در مورد انواع مختلف کنترل‌های امنیتی شبکه صحبت کرده‌ایم. حالا بیایید نگاهی به چند روش مختلف برای ایمن سازی شبکه خود بیندازیم.

- **کنترل دسترسی به شبکه**

برای اطمینان از اینکه مهاجمان احتمالی نمی‌توانند به شبکه شما نفوذ کنند، باید سیاست‌های کنترل دسترسی جامع برای کاربران و دستگاه‌ها در نظر گرفته شود. کنترل دسترسی به شبکه (NAC) را می‌توان در دقیق‌ترین سطح تنظیم کرد. به عنوان مثال، می‌توانید به مدیران دسترسی کامل به شبکه را بدهید اما دسترسی به پوشه‌های محرمانه خاص را ممنوع کرده یا از پیوستن دستگاه‌های شخصی آن‌ها به شبکه جلوگیری کنید.

- **نرم افزار آنتی ویروس و ضد ویروس**

نرم افزارهای آنتی ویروس و ضد ویروس از سازمان در برابر طیف وسیعی از نرم افزارهای مخرب از جمله ویروس‌ها، باج افزارها، کرم‌ها و تروجان‌ها محافظت می‌کنند. بهترین نرم افزار نه تنها فایل‌ها را هنگام ورود به شبکه اسکن می‌کند بلکه به طور مداوم فایل‌ها را اسکن و ردیابی می‌کند.

- **حفاظت فایروال**

همانطور که از نام آن‌ها مشخص است، فایروال مانند یک مانع بین شبکه‌های خارجی نامعتبر و شبکه داخلی مورد اعتماد شما عمل می‌کنند. مدیران معمولاً مجموعه ای از قوانین تعریف شده را تنظیم می‌کنند که تردد به شبکه را مسدود یا اجازه می‌دهد. به عنوان مثال، فایروال نسل بعدی Forcepoint (NGFW) کنترل یکپارچه و مدیریت شده ترافیک شبکه را اعم از فیزیکی، مجازی یا ابر ارائه می‌دهد.

- **شبکه‌های خصوصی مجازی**

شبکه‌های خصوصی مجازی (VPN) از نقطه پایانی یا سایت دیگری اتصال به شبکه ایجاد می‌کنند. به عنوان مثال، کاربرانی که از خانه کار می‌کنند معمولاً از طریق VPN به شبکه سازمان متصل می‌شوند. داده‌های بین دو نقطه رمزگذاری شده است و کاربر باید احراز هویت کند تا بتواند بین دستگاه خود و شبکه ارتباط برقرار کند Secure . Enterprise SD-WAN Forcepointبه سازمان‌ها اجازه می‌دهد تا با استفاده از کشیدن و رها کردن سریع VPN ایجاد کرده و با راه‌حل فایروال نسل بعدی ما از همه مکان‌ها محافظت کنند.

**منبع forcepoint**

**انتخاب آنتی ویروس مناسب** خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های اجتماعی خودتان به اشتراک بگذارید.**