امنیت شبکه :

امنیت شبکه به مجموعه‌ای از شیوه‌ها و فناوری‌ها اطلاق می‌شود که از شبکه‌های داخلی در برابر حملات و نقض داده‌ها محافظت می‌کنند. این شیوه های نرم‌افزاری و سخت‌افزاری شامل کنترل دسترسی، پیشگیری از حملات سایبری، تشخیص بدافزار و سایر اقدامات امنیتی می‌شوند.

قوانین پایه‌ای برای امنیت شبکه وجود دارند که باید در تمام شبکه‌های کامپیوتری اجرا شوند. اما با توجه به نوع و اندازه شبکه برای امنیت هر کدام از آنها راهکارهای اختصاصی نیز وجود دارد.

خطرات رایج امنیت شبکه

شبکه‌های کامپیوتری نیز مانند هر دارایی تجاری دیگری به روش‌های مختلفی در معرض خطر قرار دارند. تهدیدهایی که شبکه‌ها به طور معمول باید برای آن آماده شوند عبارتند از:

دسترسی غیرمجاز

اگر یک کاربر غیرمجاز به یک شبکه دسترسی پیدا کند، می‌تواند اطلاعات محرمانه‌ای را که در غیر این صورت به صورت خصوصی باقی می‌ماند، مشاهده کند. با دسترسی غیرمجاز به شبکه‌های کامپیوتری می‌توانند داده‌های محرمانه را افشا کنند یا سیستم‌های داخلی را به خطر بیندازند.

حملاتDDoS

حملات DDoS با ارسال ترافیک ناخواسته به مقدار زیاد باعث کندی یا از دسترس خارج شدن سرویس برای کاربران مجاز می‌شود.

سوء استفاده از آسیب‌پذیری

مهاجمان می‌توانند از آسیب‌پذیری شبکه در پرتال‌های ورود، برنامه‌ها، سخت‌افزار یا سایر مناطق برای نفوذ به شبکه برای اهداف مخرب مختلف استفاده کنند.

آلودگی‌های بدافزار(Malware infections)

از آلودگی‌های رایج بدافزاری می‌توان به باج‌افزارها (Ransomware) اشاره کرد که داده‌ها را رمزگذاری یا از بین می‌برند و با این عمل دسترسی کاربران به شبکه را محدود می‌کنند. کرم‌ها (worms)بدافزارهایی هستند که می‌توانند به سرعت در سراسر شبکه تکثیر شوند.

نرم‌افزارهای جاسوسی (spyware) که به مهاجمان اجازه می‌دهند تا اقدامات کاربر را ردیابی کنند نیز از انواع دیگر بدافزار هستند.

بدافزار می‌تواند از منابع مختلفی از جمله وب‌سایت‌های ناامن، دستگاه‌های آلوده کارمندان یا حملات خارجی هدفمند وارد شبکه شود.

تهدیدات داخلی

کارمندان یا پیمانکاران داخلی می‌توانند به طور ناخواسته امنیت شبکه را تضعیف کنند یا در صورت عدم آگاهی از شیوه‌های امنیتی، داده‌ها را افشا کنند. در موارد دیگر، کاربران ممکن است عمدا یک شبکه را به خطر بیندازند یا با توجه به دلایل شخصی خود باعث افشای اطلاعات شوند.

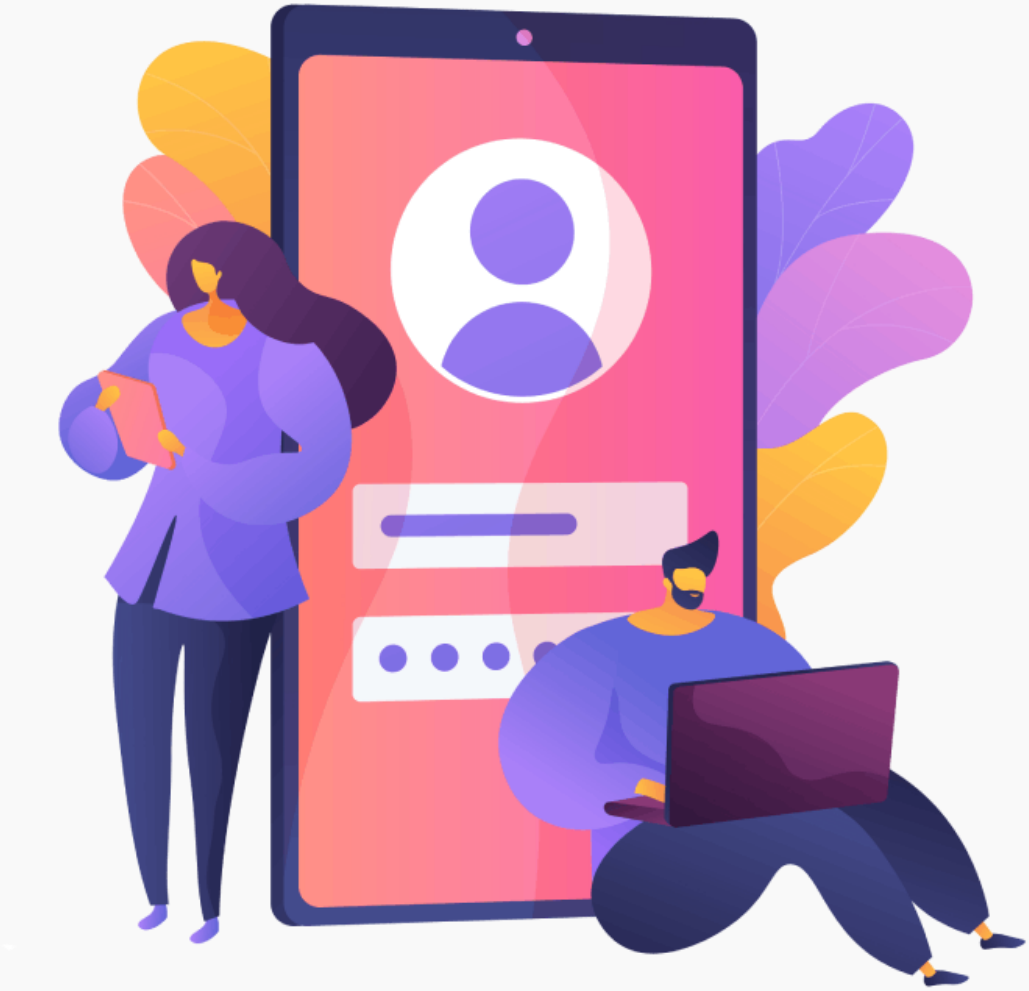
فناوری‌های مهم در امنیت شبکه کدامند؟

امنیت شبکه یک حوزه گسترده است که با توجه به اندازه شبکه و میزان حساسیت‌های امنیتی باید اقدامات متفاوتی را برای آن انجام داد. در ادامه تعدادی از اقداماتی که یک سازمان می‌تواند برای محافظت از شبکه خود استفاده کند، توضیح داده شده است. به منظور کاهش پیچیدگی، اکثر سازمان‌ها سعی می‌کنند تا حد امکان به فروشندگان کمتری برای امنیت شبکه تکیه کنند. بسیاری از شرکت‌ها به دنبال ارائه‌دهندگانی هستند که چندین مورد از این فناوری‌ها را با هم ارائه دهند.

کنترل دسترسی(Access control)

در بخش کنترل دسترسی، دسترسی به داده‌ها و نرم‌افزارهای مورد استفاده را برای جلوگیری از دستکاری آن داده‌ها محدود می‌کنند. کنترل دسترسی برای جلوگیری از دسترسی غیرمجاز و کاهش خطر تهدیدات داخلی بسیار مهم است. راه‌حل‌های مدیریت هویت و دسترسی (Identity and Access Management- IAM)می‌تواند در این زمینه به شما کمک کند. بسیاری از شرکت‌ها از شبکه‌های خصوصی مجازی (VPN) برای کنترل دسترسی استفاده می‌کنند. با این حال، امروزه جایگزین‌هایی برایVPN ها وجود دارد. این محدودیت‌ها می‌توانند با توجه به IP و Mac Address انجام شوند. برای کنترل دسترسی بهتر است پورت‌ها و سرویس‌هایی که استفاده نمی‌شوند را مسدود کنید.

احراز هویت کاربر(User authentication)



احراز هویت یا تایید هویت کاربر، یک جز حیاتی در کنترل دسترسی کاربران است. استفاده از احراز هویت دو مرحله‌ای (۲factor authentication) به جای رمزهای عبور ساده گام مهمی در جهت ایمن‌سازی شبکه هاست.

فایروال‌ها

فایروال‌ها تهدیدات بالقوه ترافیک شبکه را فیلتر می‌کنند. آنها می‌توانند حملات بدافزار، سوء استفاده از آسیب‌پذیری، حملات ربات‌ها و سایر تهدیدها را مسدود کنند. فایروال‌های سنتی با استفاده از یک دستگاه سخت‌افزاری در محل فیزیکی یک کسب و کار اجرا می‌شوند. امروزه بسیاری از فایروال‌ها می‌توانند به صورت نرم‌افزاری یا در فضای ابری اجرا شوند و نیاز به سخت‌افزار فایروال را از بین ببرند.

حفاظت ازDDoS

وب‌سایت‌ها و زیرساخت‌های شبکه هر دو باید در برابر حملات DDoS محافظت شوند تا عملیاتی باقی بمانند. به طور خاص، برای امنیت زیرساخت شبکه به جای لایه برنامه، به راهکارهای کاهش DDoS در لایه شبکه نیاز است.

پیشگیری از نشت داده‌ها(Data loss prevention- DLP)

در حالی که فایروال‌ها و حفاظت DDoS از ورود حملات خارجی به شبکه جلوگیری می‌کنند، پیشگیری از نشت داده‌ها (DLP) مانع از انتقال داده‌های داخلی به خارج از شبکه می‌شود.

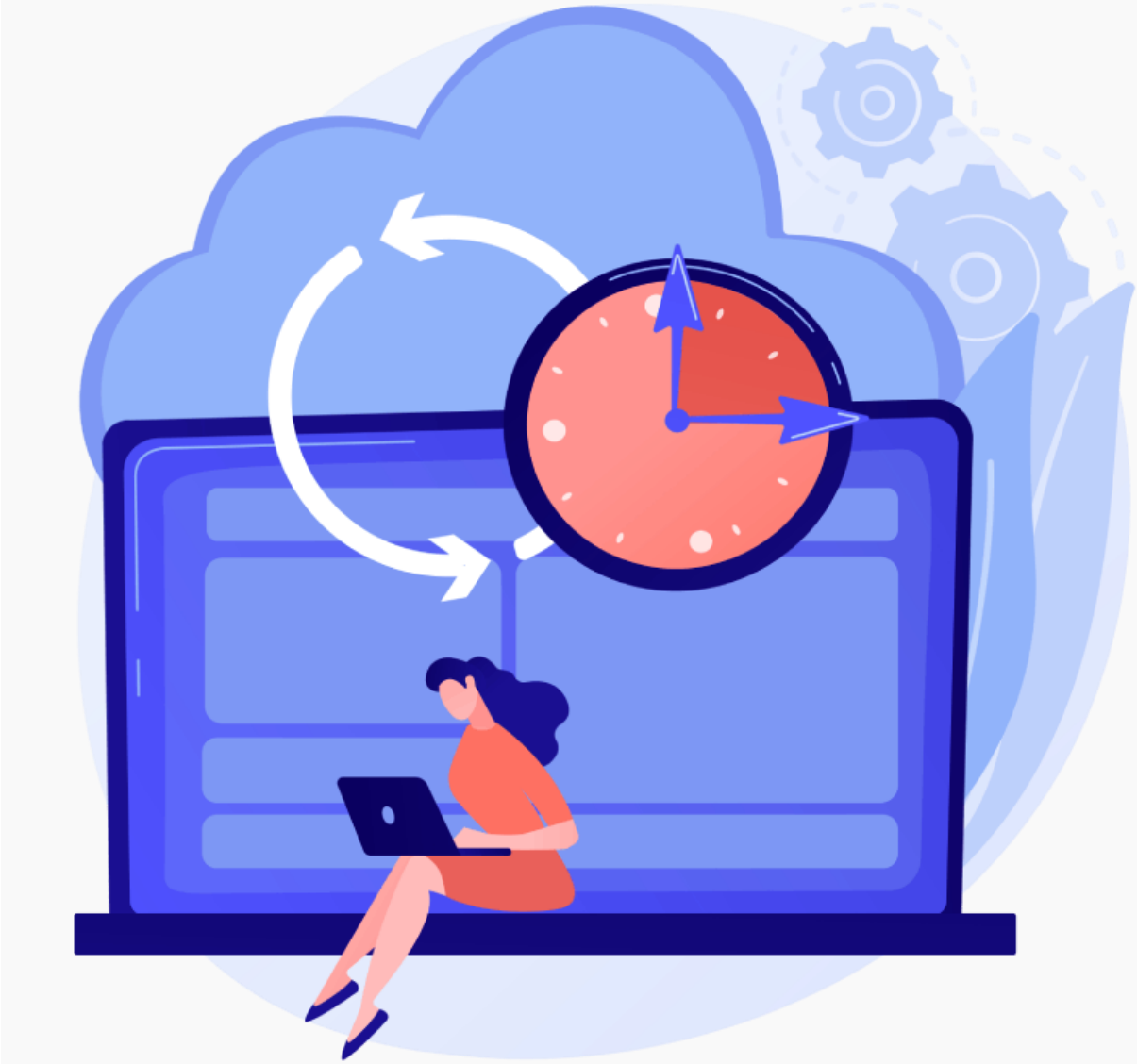
جداسازی مرورگر(Browser isolation)

دسترسی به اینترنت از طریق یک شبکه باعث ایجاد خطر برای شبکه می‌شود. زیرا مرورگر وب شامل اجرای کد از منابع غیرقابل اعتماد خارجی (مانند سرورهای وب‌سایت‌های مختلف) در دستگاه‌های کاربر است. جداسازی مرورگر این خطر را با اجرای کد از خارج از شبکه داخلی سازمان، اغلب روی یک سرور ابری، از بین می‌برد.

شرکت‌ها برای امنیت شبکه‌های خود باید چه اقدامات دیگری انجام دهند؟

در حالی که نمی‌توان به طور کامل در برابر حملات ایمن بود، این مراحل می‌توانند احتمال خطر را تا حد زیادی کاهش دهند:

پشتیبان‌گیری از داده‌ها و ذخیره چند فایل پشتیبان



حتی شبکه‌ای که به خوبی از آن دفاع می‌شود نیز ممکن است در معرض حمله قرار گیرد. از دست دادن دسترسی جزئی یا کامل به داده‌ها و سیستم‌های داخلی می‌تواند برای یک کسب و کار مخرب باشد. نگه داشتن نسخه‌های پشتیبان از داده‌ها به کاهش تاثیر چنین حمله‌ای کمک می‌کند.

آموزش کاربر

بسیاری از مشکلات داده‌ها و آلودگی‌های بدافزاری به این دلیل اتفاق می‌افتند که کاربر به سادگی مرتکب اشتباه شده است. این اشتباه می‌تواند با باز کردن تصادفی پیوست ایمیل ناامن، ارائه اعتبار ورود به سیستم خود در نتیجه حمله فیشینگ(phishing) ، یا اجازه دسترسی خارجی به روشی دیگر توسط کاربر اتفاق بیفتد. کارکنان داخلی و پیمانکاران باید از نحوه ایمن ماندن و محافظت از شبکه آگاه شوند.

به کارگیری فلسفه اعتماد صفر(zero trust)

چارچوب اعتماد صفر مجموعه‌ای از عوامل امنیتی است که همه کاربران داخلی و خارجی را قبل از ورود به سیستم احراز هویت می‌کند. در پروتکل اعتماد صفر به هیچ کاربر یا دستگاهی به طور پیش‌فرض نباید اعتماد کرد

پروتکل‌های امنیتی شبکه

پروتکل‌های امنیت شبکه مجموعه پروتکل‌هایی است که برای حفاظت از اطلاعاتی که در یک شبکه جریان دارد استفاده می‌شود.

پروتکلIPSec

پروتکل (IPSec (IP Security احراز هویت داده‌ها، یکپارچگی و همچنین حریم خصوصی بین دو موجودیت را ارائه می‌دهد.

SSL (Secure Sockets Layer)

لایه سوکت ایمن یک مکانیسم امنیتی استاندارد است که برای حفظ یک اتصال اینترنتی امن بین سرویس‌گیرنده و سرویس‌دهنده استفاده می‌شود. در این پروتکل امنیتی با استفاده از رمزنگاری از تغییر داده‌های شخصی، بسته‌ها و جزئیات در حین ارسال و هم چنین خواندن آنها توسط مجرمان جلوگیری می‌شود.

SSH (Secure Shell)

یک پروتکل امنیتی شبکه است که ارتباطات و داده‌های شبکه را رمزنگاری می‌کند. با استفاده از این پروتکل به خط فرمان اجازه می‌دهد تا از راه دور وارد سیستم شود و وظایف خاصی را از راه دور انجام دهد. عملکردهای مختلف FTP در SSH گنجانده شده است SSH-1 .وSSH-2جدیدترین در نوع خود هستند.

HTTPS (HyperText Transfer Protocol Secure)

HTTPSیک پروتکل امنیت شبکه است که برای ایمن‌سازی ارتباطات داده بین دو یا چند سیستم استفاده می‌شود. از آنجایی که داده‌های منتقل شده از طریق HTTPS رمزگذاری می‌شوند، مجرمان سایبری قادر به تغییر داده‌ها در طول انتقال از مرورگر به وب‌سرور نیستند. حتی زمانی که مجرمان سایبری به بسته‌های داده دسترسی پیدا می‌کنند، به دلیل رمزگذاری قوی بسته‌ها قادر به خواندن و تفسیر آنها نخواهند بود.

امنیت شبکه چیست؟

امنیت شبکه و آشنایی با مفهوم آن برای هر کسی که به هر طریقی با کامپیوتر و جمع‌آوری و نگه‌داری داده‌ها سروکار دارد، ضروری است. امنیت در شبکه با وجود وابستگی بسیار زیاد اغلب کسب‌وکارها به فناوری دیجیتال و متعاقباً افزایش روزافزون حمله‌های سایبری، به امری مهم تبدیل شده است.

تهدیدهای سایبری با سرعت بسیار بیشتری از رشد فناوری در کسب‌وکارها پیشرفت می‌کنند؛ به‌همین‌دلیل، به‌عنوان فردی که کسب‌وکارتان را در حوزه فناوری کامپیوتر گسترش داده‌اید، باید به‌خوبی با مفهوم امنیت شبکه آشنا باشید.

امنیت شبکه Network Security مجموع تمام مراحل و اقداماتی است که برای محافظت از یکپارچگی شبکه کامپیوتری و داده‌های درون آن انجام می‌شود. بیایید به کمی قبل‌تر برگردیم و مفهوم «شبکه» را مرور کنیم. شبکه از مجموعه‌ای از دستگاه‌های مرتبط به‌هم مانند کامپیوترها و سرورها و شبکه‌های بی‌سیم تشکیل شده است. معمولاً این دستگاه‌ها دربرابر مهاجم‌ها (هکرها) بسیار آسیب‌پذیرند. تأمین امنیت در شبکه های کامپیوتری از آن‌جایی اهمیت پیدا می‌کند که روزبه‌روز پیچیده‌تر می‌شوند و شرکت‌ها بیش‌ازپیش کسب‌وکارشان را به شبکه و داده‌ها متکی می‌کنند. روش‌های امنیتی باید با روی‌کارآمدن روش‌های جدید حمله‌های سایبری تغییر کنند. دلیل اصلی اهمیت امنیت شبکه آن است که داده‌های حساس را دربرابر حمله‌های سایبری ایمن نگه می‌دارد و به شما اطمینان می‌دهد که شبکه امن است. استراتژی‌های موفق امنیت در شبکه از

راه‌حل‌های امنیتی متفاوتی برای محافظت از کاربرها و سازمان‌ها در مقابل بدافزارها و حمله‌های سایبری استفاده می‌کنند.

چرا امنیت شبکه این‌قدر اهمیت دارد؟

است که حفظ امنیت شبکه به‌دلیل جلوگیری از دسترسی مجرمان سایبری به داده‌های ارزشمند و حساس اهمیت دارد.

درادامه، چهار دلیل برای اهمیت حفاظت از شبکه‌ها و داده‌ها را بیان می‌کنیم :

۱. ریسک‌های عملیاتی

زمانی‌که سازمان از امنیت شبکه کافی برخوردار نباشد، درمعرض خطر اختلال در سیستم عملیاتی و عملکردی قرار می‌گیرد. چه کسب‌وکارهای بزرگ‌تر و چه شبکه‌های شخصی، به دستگاه‌ها و نرم‌افزارهایی وابسته هستند که در مواقع آلوده‌شدن به ویروس‌ها و بدافزارها و حمله‌های سایبری، نمی‌توانند به‌طورمؤثر عمل کنند.

۲. ریسک‌های مالی برای اطلاعات شخصی در خطر

سازمان‌هایی که مسئولیت مدیریت اطلاعات شخصی مانند شماره‌تلفن و اطلاعات حساب بانکی و گذرواژه‌ها را برعهده دارند، باید امنیت آن را تأمین کنند. هرگونه سوءاستفاده از این داده‌ها ممکن است برای آن سازمان پرداخت جریمه، بازگرداندن خسارات، برطرف‌کردن آسیب‌ها و... را به‌دنبال داشته باشد. این دلیل را شاید بتوان مهم‌ترین دلیل برای اهمیت امنیت دانست.

۳. ریسک مالی برای مالکیت معنوی در معرض خطر

علاوه‌بر داده‌ها و مالکیت مادی، ممکن است مالکیت معنوی سازمان نیز در خطر قرار بگیرد. گاهی هکرها مستقیماً به ایده‌ها، اختراع‌ها، ابداع‌ها و محصول‌های شرکت‌ها را حمله و از آن‌ها سرقت می‌کنند. این مسئله ممکن است به ازدست‌دادن کسب‌وکار و مزیت‌های رقابتی منجر شود.

۴. مسائل نظارتی

علاوه‌بر مقررات خودِ سازمان‌ها، بسیاری از دولت‌ها از کسب‌وکارها می‌خواهند تا آن دسته از مقررات امنیت داده‌ها را رعایت کنند که جنبه‌های امنیت شبکه را پوشش می‌دهد. نقض این مقررات ممکن است جریمه نقدی و ممنوعیت کار و حتی زندان را به‌دنبال داشته باشد.

آشنایی با نحوه کار امنیت شبکه

به‌طورکلی، امنیت شبکه به‌کمک ترکیبی از ابزارهای سخت‌افزاری و نرم‌افزاری برقرار می‌شود. با بررسی مفاهیم امنیت شبکه در مطالب ذکرشده، می‌دانیم که هدف اصلی آن جلوگیری از دسترسی غیرمجاز به بخش‌های مختلف شبکه است.

مسئول یا تیم امنیتی استراتژی‌ها و سیاست‌هایی را تعیین می‌کند که امنیت شبکه سازمان را تأمین و به آن کمک می‌کند تا با استانداردها و مقررات امنیتی مطابقت داشته باشد. پس از تعیین و ابلاغ این سیاست‌های امنیتی، همه افراد در شبکه باید از آن پیروی کنند. این قوانین شامل تمام افرادی است که به داده‌ها دسترسی دارند یا در بخشی کار می‌کنند که ممکن است عاملی مخرب داده‌ها را ازطریق بی‌احتیاطی یا اشتباه کاربر درمعرض خطر دهند.

چهار مزیت اصلی برقراری امنیت شبکه

در هر محیط محاسباتی، برای محافظت از اطلاعات دربرابر کاربران غیرمجاز، از امنیت شبکه استفاده می‌شود. در مفاهیم امنیت شبکه باید سه جزء اصلی وجود داشته باشد:

۱. محرمانگی؛

۲. یکپارچگی؛

۳. دردسترس‌بودن.

ویژگی محرمانگی امنیت شبکه رهگیری‌نشدن داده‌ها به‌وسیله هکرها را به‌هنگام انتقال درون شبکه تضمین می‌کند. همچنین، ویژگی یکپارچگی تغییر نکردن داده‌ها در طول انتقال از طریق شبکه را تضمین و از آسیب یا دست‌کاری آن جلوگیری می‌کند.

در نهایت، ویژگی دردسترس‌بودن امنیت شبکه به شما اطمینان می‌دهد تا سیستم‌ها و دستگاه‌ها فقط برای استفاده افراد مجاز دردسترس هستند.

مزایای امنیت شبکه چیست؟

- اجرای رویکردهای امنیت شبکه و عملکرد عالی و مداوم شبکه‌ها بین کسب‌وکارها و کاربرها را تضمین می‌کند.
- با اجرای امنیت شبکه، به حفظ امنیت داده‌ها و حریم خصوصی کاربران و کارکنان می‌توانید کمک کنید.
- با محافظت از شبکه در سازمان خود، مالکیت معنوی ایده‌ها، محصولات، خدمات، استراتژی‌های تجاری و... را می‌توانید حفظ کنید.
- با اجرای خط‌مشی‌های امنیت شبکه، از قوانین تعیین‌شده برای حفاظت از داده‌ها در کشور محل کارتان پیروی می‌کنید.

انواع نرم‌افزارها و ابزارهای تأمین امنیت شبکه

سیاست‌ها و ابزارهایی که برای حفظ امنیت شبکه وجود دارند، از شبکه‌ای به شبکه دیگر متفاوت‌اند و حتی در طول زمان باید تغییر کنند. معمولاً سیاست امنیتی قوی شامل رویکردهای متعددی است که با عنوان امنیت لایه‌ای (Layered Security) شناخته می‌شود و حداکثر کنترل‌های امنیتی را به سازمان می‌دهد.

۱. کنترل دسترسی (Access Control)

این یکی از رویکردهای ابتدایی حفظ امنیت شبکه است که دسترسی به برنامه‌ها و سیستم‌های شبکه را تنها برای گروه خاصی از کاربرها و دستگاه‌ها مجاز می‌کند؛ یعنی در این سیستم، امکان دسترسی برای کاربرها و دستگاه‌های ازقبل‌تعیین‌نشده وجود ندارد.

۲. دسترسی ZTNA (Zero-Trust Network Access)

این روش نیز تا حدی مشابه کنترل دسترسی به شبکه است. در روش ZTNA که از انواع امنیت شبکه است، تنها به کاربران اجازه داده می‌شود تا کارهایشان را انجام دهند و تمام مجوزهای دسترسی به بخش‌های دیگر مسدود می‌شود.

۳. آنتی‌ویروس (Antivirus) و ضدبدافزار (Antimalware)

همه ما با آنتی‌ویروس‌ها و ضدبدافزارها که یکی از ابزارهای حفظ امنیت در شبکه است، آشنا هستیم. این نرم‌افزارها برای شناسایی یا حذف یا جلوگیری از آلوده‌کردن کامپیوتر و درنتیجه شبکه طراحی شده‌اند و با ویروس‌ها و بدافزارهایی مانند اسب تروجان (Trojan horse) و باج‌افزارها و جاسوس‌افزارها مقابله می‌کنند.

۴. امنیت برنامه (Application Security)

سازمان‌ها برای اجرای عملکردهای مختلف در کسب‌وکار خود از برنامه‌هایی استفاده می‌کنند که نظارت و محافظت از آن‌ها بسیار مهم است.

چه سازمان‌هایی که این برنامه‌ها را طراحی کرده‌اند و چه سازمان‌هایی که از آن‌ها استفاده می‌کنند، باید به امنیت این برنامه‌ها توجه کنند؛ زیرا تهدیدهای مدرن بدافزارها اغلب کدهای منبع‌باز و بخش‌هایی را هدف قرار می‌دهد که سازمان‌ها از آن‌ها برای ساختن نرم‌افزار و اپلیکیشن‌ها استفاده می‌کنند. پس امنیت برنامه‌ها، بخشی از تأمین امنیت شبکه سازمان است.

۵. تجزیه‌وتحلیل رفتاری (Behavioral Analytics)

آنالیز رفتاری، یکی از انواع امنیت شبکه است. در این روش، رفتار شبکه تجزیه‌وتحلیل می‌شود و سازمان‌ها را به‌طورخودکار از هرگونه فعالیت‌های غیرعادی آگاه می‌کند.

۶. امنیت ابری (Cloud Security)

اگر از سیستم‌ها و ابزارهای مبتنی‌بر فضای ابری استفاده کرده باشید، می‌دانید که ارائه‌دهندگان آن‌ها اغلب ابزارهای امنیتی مجزا را دراختیار شما قرار می‌دهند که قابلیت‌های امنیتی در فضای ابری را فراهم می‌کند. امنیت فضاها و سیستم‌های ابری، بخشی از تأمین امنیت در شبکه است. این ارائه‌دهندگان روی امنیت زیرساخت‌های کلی خود نظارت می‌کنند و ابزارهایی را ارائه می‌دهند که از این زیرساخت‌ها محافظت می‌کند.

برای مثال، می‌توان به خدمات امنیت شبکه وب آمازون اشاره کرد که گروه‌هایی امنیتی را سازمان‌دهی می‌کند تا ترافیک ورودی‌وخروجی مرتبط با برنامه یا منبع را کنترل کنند.

۷. روش پیشگیری ازدست‌دادن داده‌ها (DLP)

در این روش، پس از شناسایی داده‌های در حال استفاده یا در حال گردش یا حتی در حال استراحت، روی جلوگیری از نقض آن‌ها نظارت می‌شود. معمولاً در روش DLP (Data Loss Prevention)، مهم‌ترین داده‌های درمعرض خطر طبقه‌بندی می‌شوند و به کارکنان آموزش می‌دهند تا به بهترین شیوه‌های ممکن از آن‌ها محافظت کنند. این یکی از مراحل یادگیری امنیت شبکه است که کارکنان باید آموزش ببینند. برای مثال، یکی از روش‌های ساده و مهم این است که فایل‌های مهم را در ایمیل و به‌صورت پیوست ارسال نکنند.

۸. امنیت ایمیل (Email Security)

معمولاً ایمیل را به‌عنوان یکی از نقاط آسیب‌پذیر در شبکه در نظر می‌گیرند. در اغلب مواقع، کارمندان سازمان با کلیک روی پیوست‌های ایمیل که حاوی بدافزارها و نرم‌افزارهای مخرب هستند، آن‌ها را بدون اطلاع از محتویات پیوست دانلود و کل سازمان را قربانی حمله‌های فیشینگ و بدافزاری می‌کنند. پس در مراحل یادگیری امنیت شبکه برای کارکنان، باید به امنیت ایمیل‌ها هم اشاره کرد.

لازم است بدانید که ایمیل روشی ناامن برای ارسال فایل‌ها و داده‌های حساس است و کارمندان در تمام بخش‌ها باید با این موضوع آشنا باشند. این یکی از مفاهیم اصلی امنیت شبکه است که باید به کارکنان سازمان آموزش داده شود.

۹. فایروال (Firewall)

فایروال نرم‌افزار یا سیستم‌عاملی است که ترافیک ورودی‌وخروجی را برای جلوگیری از دسترسی‌های غیرمجاز به شبکه بررسی می‌کند. فایروال‌ها را می‌توان یکی از ابزارهای پرکاربرد امنیت در شبکه های کامپیوتری در نظر گرفت که در مناطق مختلفی از شبکه قرار می‌گیرند. نسل‌های بعدی فایروال‌ها محافظت بیشتری دربرابر حمله‌های لایه برنامه ارائه می‌دهند و با بررسی بسته‌های درون‌خطی، دربرابر بدافزارها بهتر مقاومت می‌کنند.

۱۰. سیستم تشخیص نفوذ (IDS)

سیستم IDS(Intrusion Detection System) یکی دیگر از انواع امنیت شبکه است. این سیستم تلاش‌های غیرمجاز برای دسترسی به داده‌ها یا شبکه را شناسایی و آن‌ها را به‌عنوان خطرهای بالقوه علامت‌گذاری می‌کند؛ اما هیچ‌یک را حذف نمی‌کند. معمولاً از IDS و سیستم پیشگیری از نفوذ (IPS) درکنار فایروال‌ها استفاده می‌شود. این سیستم بخشی از انواع امنیت شبکه است.

۱۱. سیستم پیشگیری از نفوذ (IPS)

سیستم IPS(Intrusion Prevention System) برای جلوگیری از نفوذ به شبکه طراحی شده است. این کار با شناسایی و مسدود کردن تلاش‌های غیرمجاز برای دسترسی به شبکه انجام می‌شود. جلوگیری از نفوذ، یک کاربرد امنیت شبکه بسیار مهم و اساسی است.

۱۲. امنیت دستگاه‌های موبایل (Mobile Device Security)

اپلیکیشن‌های متعددی که برای گوشی‌های هوشمند و سایر دستگاه‌های تلفن‌همراه طراحی شده‌اند، آن‌ها را به یکی از بخش‌های مهم در حوزه امنیت شبکه تبدیل کرده است. نظارت و کنترل برنامه‌هایی که به شبکه‌های همراه دسترسی دارند، برای امنیت در شبکه مدرن بسیار مهم است.

۱۳. احراز هویت چندعاملی (MFA)

سیستم احراز هویت چندمرحله‌ای یا MFA (Multifactor Authentication) روش امنیتی ساده‌ای است که در بین کاربران به‌شدت در حال محبوب‌شدن است. در این روش، احراز هویت کاربر نیازمند تأیید دو یا چند فاکتور مختلف است تا مطمئن شود که تنها کاربر اصلی در حال تلاش برای ورود به شبکه مدنظر است. یکی از انواع امنیت شبکه در این سیستم احراز هویت، سیستم Google Authenticator نام دارد که درواقع برنامه‌ای است که کدهای امنیتی منحصربه‌فردی تولید می‌کند تا کاربر درکنار رمزعبور خود وارد و هویتش را تأیید کند.

۱۴. تقسیم‌بندی شبکه (Network Segmentation)

یکی دیگر از ابزارهایی که در انواع خدمات امنیت شبکه می‌توان بررسی کرد، روش تقسیم شبکه است. معمولاً سازمان‌هایی که شبکه‌های بزرگ و با ترافیک فراوان دارند، از این روش برای تقسیم‌کردن شبکه به بخش‌های کوچک‌تر و مدیریت راحت‌تر آن‌ها استفاده می‌کنند. این رویکرد امکان کنترل بیشتر داده و دسترسی بیشتری درمقایسه‌با جریان ترافیک را برای سازمان‌ها فراهم می‌کند.

۱۵. سندباکسینگ (Sandboxing)

این روش نوعی ایزوله‌سازی است که به سازمان اجازه می‌دهد تا فایل را قبل از دسترسی به شبکه در محیطی ایزوله اسکن کنند. بعد از اسکن و باز کردن فایل در محیطی امن، سازمان می‌تواند بررسی کند که آیا این فایل به روشی مخرب عمل می‌کند یا نشانه‌هایی از بدافزارها را نشان می‌دهد.

۱۶. رویکرد اطلاعات امنیتی و مدیریت رویداد (SIEM)

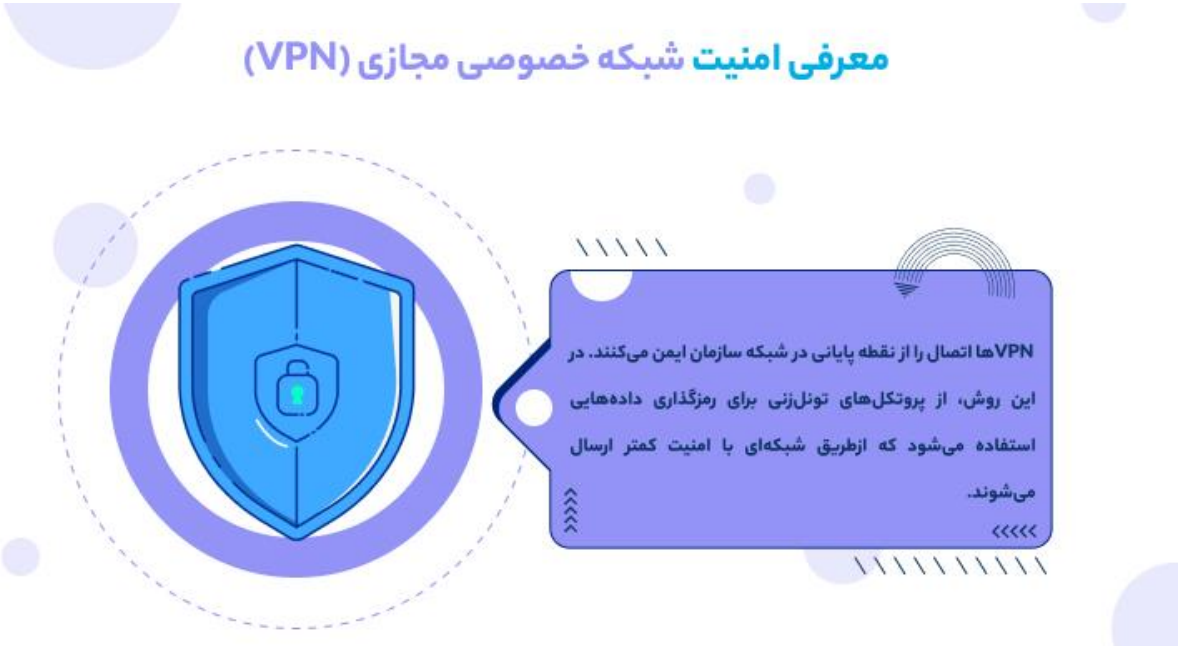
در روش SEIM (Security Information and Event Management)، امنیت داده‌های مدیریت‌شده از برنامه‌ها و سخت‌افزارهای شبکه ثبت‌شده و رفتارهای مشکوک نظارت می‌شود. زمانی‌که هرگونه رفتار مشکوک یا ناهنجاری شناسایی شود، سیستم امنیت شبکه SEIM به سازمان هشدار می‌دهد و اقدامات مناسب برای رفع آن انجام می‌شود.

۱۷. محیط نرم‌افزاری تعریف‌شده (SDP)

روش SDP (Software-Defined Perimeter) یکی دیگر از شیوه‌های تأمین امنیت شبکه است که از شبکه محافظت و آن را از دید مهاجمان و کاربران غیرمجاز به دسترسی پنهان می‌کند. درحقیقت، این رویکرد از معیارهای هویتی برای محدودکردن دسترسی به منابع و فایل‌ها استفاده و مرزبندی مجازی‌ای در اطراف آن ایجاد می‌کند که نفوذ عوامل خطرزا را غیرممکن می‌کند.

۱۸. شبکه خصوصی مجازی (VPN)

احتمالاً همه شما با VPN(Virtual Private Network) آشنا هستید؛ اما تابه‌حال به نحوه کار و نقش آن برای امنیت در شبکه های کامپیوتری فکر نکرده‌اید. VPNها اتصال را از نقطه پایانی در شبکه سازمان ایمن می‌کنند. در این روش، از پروتکل‌های تونل‌زنی برای رمزگذاری داده‌هایی استفاده می‌شود که ازطریق شبکه‌ای با امنیت کمتر ارسال می‌شوند.



۱۹. امنیت وب (Web Security)

در این روش، درکنار حفظ یکپارچگی وب‌سایت‌های سازمان، استفاده کارمندان از وب در دستگاه‌ها و شبکه‌های سازمان کنترل می‌شود. این کار ازطریق کنترل مسدودکردن برخی تهدیدها و وب‌سایت‌ها انجام می‌شود. شما می‌توانید در کنار روش‌ها و مراحل یادگیری امنیت شبکه برای کارکنان، از این روش‌ها برای کنترل عملکرد آن‌ها در حفظ امنیت بیشتر شبکه، استفاده کنید.

۲۰. امنیت وایرلس (Wireless Security)

یکی از بخش‌های پرخطر هر شبکه را می‌توان شبکه‌های بی‌سیم دانست که به حفاظت و نظارت بسیار دقیق‌تر نیاز دارند. در این سیستم‌ها، شیوه‌های امنیت وایرلس ازجمله تقسیم‌بندی کاربران Wi-Fi براساس شناسه‌های مجموعه سرویس یا SSIDها و احراز هویت X۸۰۲.۱ بسیار اهمیت دارد. همچنین، برای اطمینان از امنیت شبکه وایرلس یا بی‌سیم، به ابزارهای نظارت و ممیزی مناسب احتیاج است.

۲۱. امنیت حجم کار (Workload security)

در این روش، سازمان حجم کار مدنظر را بین دستگاه‌های مختلف در محیط‌های ابری و ترکیبی به‌طورمتعادل تقسیم می‌کند. با این کار سطوحی که حمله‌های سایبری و تهدیدها را دریافت می‌کنند، افزایش پیدا می‌کند. استفاده از اقدامات امنیتی به‌منظور نظارت روی بار کاری و متعادل‌کننده‌های بار امن، برای محافظت از داده‌ها و امنیت در شبکه مهم است.

چه چیزهایی امنیت شبکه را به‌خطر می‌اندازد؟

۱. تکامل روش‌های حمله به شبکه

یکی از مشکلات بزرگ پیش‌روی امنیت شبکه به سرعت تکامل حمله‌های سایبری مربوط است. هم عواملی که شبکه را تهدید می‌کنند و هم روش‌هایی که این عوامل را به‌کار می‌گیرند، همگی با تغییر تکنولوژی تغییر می‌کنند. به‌عنوان مثال، فناوری جدیدی مانند بلاک‌چین به انواع جدیدی از حمله‌های بدافزار مانند Crypto jacking منجر شده است؛ به‌همین‌دلیل، استراتژی‌های دفاعی و انواع امنیت شبکه باید با این تهدیدهای جدید سازگار شوند.

۲. پایبندی کاربر به قوانین

تأمین امنیت شبکه برعهده تمام کاربران حاضر در شبکه است؛ به‌همین‌دلیل، معمولاً برای سازمان‌ها دشوار می‌شود که از پایبندی تمام اعضا به قوانین و استراتژی‌های امنیت شبکه مطمئن شوند.

۳. دسترسی از راه دور و ازطریق موبایل

با گسترش کسب‌وکار، افراد و شرکت‌های بیشتری از سیاست‌های سازمان برای امنیت شبکه استفاده می‌کنند که به شبکه گسترده‌تر و پیچیده‌تری منجر می‌شود. همچنین، بسیاری از افراد مرتبط با سازمان ممکن است فعالیت از راه دور را انتخاب کرده باشند. این مسئله حفظ امنیت در

شبکه های کامپیوتری را با مسائلی روبه‌رو می‌کند که اغلب به سخت‌ترشدن حفظ امنیت منجر می‌شود.

۴. همکاران شخص ثالث

شرکت‌ها و افرادی ازجمله ارائه‌دهندگان خدمات ابری و خدمات امنیتی مدیریت‌شده و فروشندگان محصولات امنیت شبکه اغلب به شبکه اصلی سازمانتان دسترسی پیدا می‌کنند. این مسئله باعث می‌شود تا کل سیستم با مشکلات بیشتری ازنظر آسیب‌پذیری مواجه شود.

اقدامات مهم امنیت شبکه

سازمان برای جلوگیری از حمله به شبکه داده‌ها و اطلاعات مهمش، باید این اقدامات را انجام دهد:

۱. ایجاد خط‌مشی امنیت شبکه

برای ایجاد خط‌مشی امنیت شبکه سندی مکتوب تنظیم می‌شود که میزان دسترسی و محدودیت‌های کاربران مجاز در سازمان را تعیین می‌کند. همچنین، در این خط‌مشی اقدامات امنیتی‌ای بررسی می‌شود که باید به‌صورت دوره‌ای انجام شود. برای مثال، نحوه انجام آزمایش‌های ارزیابی میزان ریسک داده‌ها یا طرح‌های بازیابی اطلاعات بررسی می‌شوند.

۲. خط‌مشی رمزعبور

سیاست‌های مربوط به رمزعبور تعیین می‌کند که رمزهای عبور سیستم‌های دراختیار کاربران نباید خیلی ساده باشد یا اعداد و حروفی را شامل شود که به‌راحتی بتوان آن‌ها را حدس زد. این بخشی از مراحل یادگیری امنیت شبکه است.

برای مثال، برای رمزعبور از تاریخ‌های شخصی که ممکن است به‌سادگی پیدا شود، نباید استفاده کرد. رمزهای عبور باید به‌قدری قوی باشند که حمله‌هایی ازجمله حمله‌های Dictionary یا Rainbow Tables یا Brute-force را خنثی کنند. همچنین، کارکنان برای حفظ امنیت در شبکه باید رمزهای عبور را به‌صورت دوره‌ای تغییر دهند.

۳. استفاده از سیستم امنیتی چندلایه

یکی از انواع امنیت شبکه با عنوان امنیت چندلایه شناخته می‌شود. این روش از ترکیب چندین ابزار امنیتی مانند آنتی‌ویروس و فایروال و سیستم تشخیص نفوذ همزمان استفاده می‌کند.

۴. استقرار SIEM

پیش‌ازاین، به روش SIEM در میان انواع امنیت شبکه اشاره کردیم. روش SIEM به سازمان‌ها کمک می‌کند تا شبکه داده‌ها را امن کنند و با هشدار به تحلیلگران سیستم، از نفوذ عوامل تهدید مانع شوند.

۵. به‌روز نگه‌داشتن شبکه

عوامل تهدید و آسیب‌زننده اغلب به‌راحتی می‌توانند در نسخه‌های قدیمی‌تر سیستم‌عامل، نرم‌افزارها، درایورهای دستگاه و ... نفوذ کنند. برای جلوگیری از این مسئله، سازمان باید به‌موقع سیستم را به‌روزرسانی کند تا جدیدترین خط‌مشی‌های امنیتی در آن اِعمال شود. بروز نگه‌داشتن شبکه، یکی از خدمات امنیت شبکه اساسی است.

۶. ارائه آموزش به کارکنان

به‌عقیده بسیاری از متخصصان حوزه امنیت شبکه انسان ضعیف‌ترین حلقه در هر شبکه است. به‌همین‌دلیل، هر سازمان و کسب‌وکاری باید آموزش‌های لازم را به کارکنان خود ارائه دهد تا بتوانند دربرابر تهدیدهای بالقوه اقدامات لازم را انجام دهند و از آسیب به کل شبکه جلوگیری کنند.

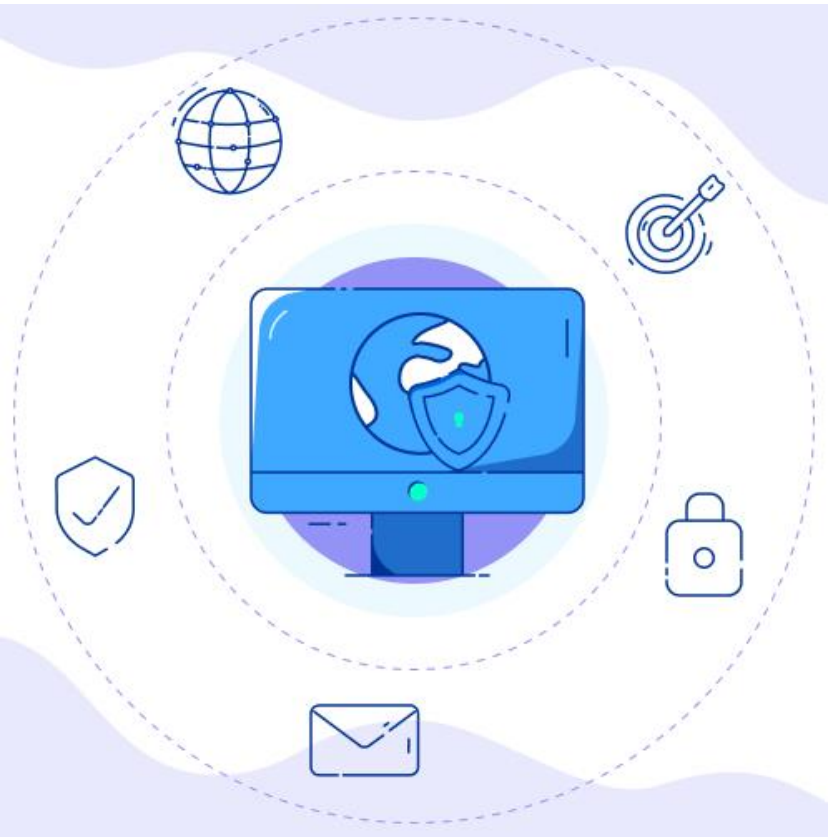
مراحل یادگیری امنیت شبکه متفاوت بوده و آموزش‌ها به میزان دسترسی کارکنان بستگی دارد. برای مثال، کاربران باید بدانند که در زمان اداری حق ندارند از شبکه‌های اجتماعی، دانلودهای بیهوده و... استفاده کنند.

۷. اقدامات پیشگیرانه فیزیکی

علاوه‌بر تمام راهکارهای نرم‌افزاری و سیستمی، اطمینان از امنیت فیزیکی در زیرساخت‌های امنیت در شبکه ضرورت دارد. برای مثال، سرور DNS، سرور داده، و سایر سیستم‌های حیاتی و دستگاه‌های شبکه باید در مرکزی امن نگه‌داری و برای امنیت آن از کنترل‌های فیزیکی و قفل‌های بیومتریک استفاده شود.

۸. رمزنگاری و امنیت Wi-Fi

علاوه‌بر داده‌ها که باید قبل از ارسال به مقاصد دیگر ازطریق شبکه رمزگذاری ایمن شوند، امنیت شبکه Wi-Fi لازم است ازطریق گواهی‌های دیجیتال تأمین شود.



سیستم امنیت شبکه قوی دربرابر چه حمله‌هایی مقاومت می‌کند؟

تهدیدهای مهمی که سیستم امنیت در شبکه‌های کامپیوتری با آن‌ها مقابله می‌کند، عبارت‌اند از:

۱. ویروس‌ها

ویروس‌ها فایل‌های مخرب و دانلودشدنی هستند که می‌توانند غیرفعال باشند و با تغییر سایر برنامه‌های کامپیوتری تکثیر شوند. فایل‌های آلوده می‌توانند از کامپیوتری به کامپیوتر دیگر منتقل شوند و داده‌ها یا کل شبکه را از بین ببرند. پس شناسایی و مقابله با ویروس، بخشی از امنیت شبکه است.

۲. کرم‌های (Worm) کامپیوتری

کرم‌های کامپیوتری با مصرف پهنای باند و کاهش کارایی کامپیوتر، پردازش داده‌ها را کُند می‌کنند. برخلاف ویروس که به برنامه میزبان نیاز دارد، کرم بدافزاری مستقل است. در خط‌مشی امنیت در شبکه های کامپیوتری باید به این نوع حملات توجه کرد.

۳. تروجان (Trojan)

تروجان با استفاده از برنامه‌ای که شبیه به برنامه‌ای واقعی به‌نظر می‌رسد، راه ورود به سیستم را پیدا می‌کند و ممکن است به حذف فایل‌ها و فعال‌کردن بدافزارهای مخفی یا سرقت داده‌های باارزش منجر شود تا در نهایت، امنیت در شبکه را به خطر بیاندازد.

۴. جاسوس‌افزارها

جاسوس‌افزار نوعی ویروس کامپیوتری است که به اطلاعات شخص یا سازمان دسترسی می‌تواند پیدا کند.

۵. Adware

آگهی‌افزارها یا Adware حین جست‌وجو در وب ممکن است کاربر را به وب‌سایت‌های تبلیغاتی غیرمفید هدایت کند. با این کار اطلاعات بازاریابی درباره شما جمع‌آوری و پس‌ازآن، تبلیغات سفارشی براساس سوابق جست‌وجو را به شما نشان می‌دهد. در مراحل یادگیری امنیت شبکه باید به کارکنان آموزش داده شود که در برخورد با آگهی‌افزارها باید چطور برخورد کنند.

۶. باج‌افزارها

باج‌افزار درواقع نوعی تروجان سایبری است که برای به‌دست‌آوردن پول از کامپیوتر شخص یا سازمان به‌کمک رمزگذاری داده‌ها طراحی شده است. این بدافزارها می‌توانند دسترسی به سیستم کاربر را مسدود کنند و امنیت شبکه را به خطر بیاندازند.

انواع راهکارها در مباحث امنیت شبکه

موارد زیر جزو اساسی ترین مباحث و راهکارهای کنترل امنیت در انواع مقیاس ها است. البته برخی موارد در مقیاس های کوچکتر قابل حذف هستند اما اگر امنیت اهمیت بالایی دارد بهتر است بر روی تمامی موارد زیر کار شود:

- Access controlبه معنی کنترل دسترسی
- Antivirus and antimalware softwareبه معنی نرم افزارهای مقابله با ویروس و بدافزار
- Application securityبه معنی امنیت نرم افزار
- Behavioral analyticsبه معنی تحلیل عملکرد و تعیین معیارها
- Data loss preventionبه معنی جلوگیری از دست رفتن اطلاعات
- Email securityبه معنی امنیت ایمیل
- Firewallsبه معنی دیوار آتش (نرم افزاری و سخت افزاری)
- Mobile device securityبه معنی امنیت دستگاه تلفن همراه
- Network segmentationبه معنی تقسیم بندی شبکه
- Security information and event managementبه معنی اطلاعات امنیتی و مدیریت رویداد

- VPNمخفف Virtual private network به معنی شبکه خصوصی مجازی
- Web securityبه معنی امنیت وب
- Wireless securityبه معنی امنیت شبکه بی سیم

کنترل دسترسی ها :در هر شبکه کوچک یا بزرگ، عمومی یا خصوصی بهتر است دسترسی ها کنترل و محدود شده باشند. اینکار یک قدم بسیار موثر و بزرگ در جلوگیری از بروز مشکلات امنیتی است. زیرا با اینکار دسترسی عموم به شبکه محدود شده و تنها افراد و دستگاه های مجاز می توانند به شبکه متصل شوند. تعیین محدویت برای اتصال اولیه به شبکه با مواردی مانند IP, Mac Addressانجام شده و در بستر شبکه با تعیین دسترسی ها قابل انجام است. یکی از بهترین راهکارهای تکمیلی در این موضوع غیرفعالسازی سرویس ها و پورت هایی می باشد که از آنها استفاده نمی شود.

نرم افزارهای مقابله با ویروس و بدافزار :استفاده از ابزارهایی مانند آنتی ویروس و ضد بدافزار بدون شک در شبکه ضروری است. رول هایی متعددی که در بطن این ابزارها وجود دارد و همواره در حال بروزرسانی و تقویت است موجب دفع و جلوگیری از مشکلات متعدد امنیتی در سطح شبکه می شود. در برخی مواقع بدافزارها و ویروس ها بصورت پنهان وارد عمل شده و ممکن است کل موجودیت شبکه را با مشکل اساسی مواجه نماید. خوشبختانه چنین ابزارهایی به صورت راهکارهای سازمانی و شرکتی برای انواع شبکه های کامپیوتری عرضه شده و می توان از آنها بهره برد.

امنیت نرم افزار :نرم افزارها در ساختار های متعددی وجود دارند. نرم افزارهای تحت وب و نرم افزارهای کامپیوتری در ارتباط با شبکه می بایست طبق اصول امنیتی نوشته شده و مورد استفاده قرار بگیرند. معمولا مشکلات امنیتی نرم افزار بصورت باگ مشخص و راهکار مناسب برای حل آن در نظر گرفته می شود. نمی توان ادعا کرد که امنیت یک نرم افزار مشکلی ندارد چون امنیت نرم افزار علاوه بر ساختار به عوامل متعددی مانند سرویس ها و فریم ورک ها وابسته است.

تحلیل عملکرد و تعیین معیارها :با مشخص شدن رفتارهای طبیعی و مجاز در سطح شبکه می توان معیارهای متناسب برای کنترل عملکردهای غیر طبیعی و مشکوک را تدوین کرد. پس از اینکار، مانیتورینگ شبکه بصورت مداوم ضرور است.

جلوگیری از درز و انتشار اطلاعات :این موضوع ابعاد بسیار گسترده ای دارد که با استاندارد DLP مشهور است. مبحثی که در این بخش بر روی آن می بایست تمرکز کرد Data loss prevention است. با راهکارهای موجود می بایست این اطمینان برای تیم امنیتی شبکه حاصل شود که اطلاعات محرمانه توسط افراد مجموعه یا سازمان و یا افراد دیگر به بیرون از شبکه درز نشده و امنیت اطلاعات (بخصوص اطلاعات محرمانه) تامین می شود.

امنیت ایمیل :ایمیل به عنوان یکی از روشهای ارتباطی که می تواند راه مناسبی برای نفوذ هکرها باشد می بایست بصورت مناسبی از لحاظ امنیتی پوشش داده شود. با توجه به اینکه امکان حملاتی نظیر فیشینگ، تزریق بدافزار و ویروس بر روی شبکه با ایمیل وجود دارد می بایست راهکار مناسبی جهت تشخیص و مقابله با این موضوع بکار برد.

استفاده از فایروال :یکی از موثرترین ابزارهای برای کنترل ترافیک و درخواست ها در بستر شبکه، فایروال است. این ابزار بصورت سخت افزاری و نرم افزاری و یا ترکیبی از این دو موجود است. البته می بایست توجه داشت که کارکرد مناسب فایروال ها برای بررسی صحیح درخواست ها، تعریف و تعیین رول های کاربردی و بروز است. از جمله مواردی که فایروال در برابر آنها می تواند عملکرد قابل قبولی از خود به نمایش بگذارد مسدودسازی درخواست های مغایر با قوانین و معیارهای سطح دسترسی ها و مقابله با حملات تکذیب سرویس (DDoS) است.

امنیت دستگاه تلفن همراه :یکی از مواردی که با گذشت زمان اهمیت بیشتری پیدا کرده است دستگاه های موبایل است. به این دلیل که بیشتر پلتفرم ها بر روی گوشی های هوشمند قابل اجراست و چون موبایل یک وسیله شخصی بوده و امکان نفوذ از این طریق برای هکرها نسبت به سطح شبکه آسانتر است عوامل و تیم امنیتی شبکه می بایست راهکاری مطمئن برای جلوگیری از بروز مشکلات امنیتی را بکار بگیرند.

تقسیم بندی شبکه :این موضوع می تواند آسیب های احتمالی از مشکلات امنیتی را کنترل و یا تعدیل کند. به اینصورت که با تقسیم بندی شبکه، چنانچه یک بخش از شبکه مشکل امنیتی پیدا کرد کل شبکه تحت تاثیر آن قرار نمی گیرد.

اطلاعات امنیتی و مدیریت رویداد :سرویس ها و ابزارهایی وجود دارند که اطلاعات لازم برای شناسایی و پاسخ به تهدیدات را برای عوامل تامین امنیت شبکه های کامپیوتری فراهم می کنند. این سرویس ها و ابزارها معمولا توسط شرکتهای فعال در زمینه راهکارهای امنیتی سازمانی و شرکتی ارائه می شوند.

شبکه خصوصی مجازی :استفاده از شبکه خصوصی مجازی با ساختار امن در صورت بهره گیری از قابلیت رمزنگاری اطلاعات و تراکنشهای انجام شده در بستر شبکه می تواند راهکاری مناسب برای تامین امنیت شبکه باشد.

امنیت وب :این راهکار بصورت شناسایی وب سایت های مخرب و مسدودسازی آنها و همچنین تامین امنیت وبسایت به کار گرفته می شود. لازم به ذکر است تامین امنیت وب می بایست بصورت ویژه ای در دستور کار قرار بگیرد.

امنیت شبکه بی سیم :همانطور که می دانید شبکه های بی سیم از محافظتی مانند شبکه سیمی برخوردار نیستند. به همین جهت می بایست نهایت محدودیت و کنترل را در شبکه های بی سیم اعمال کرد.