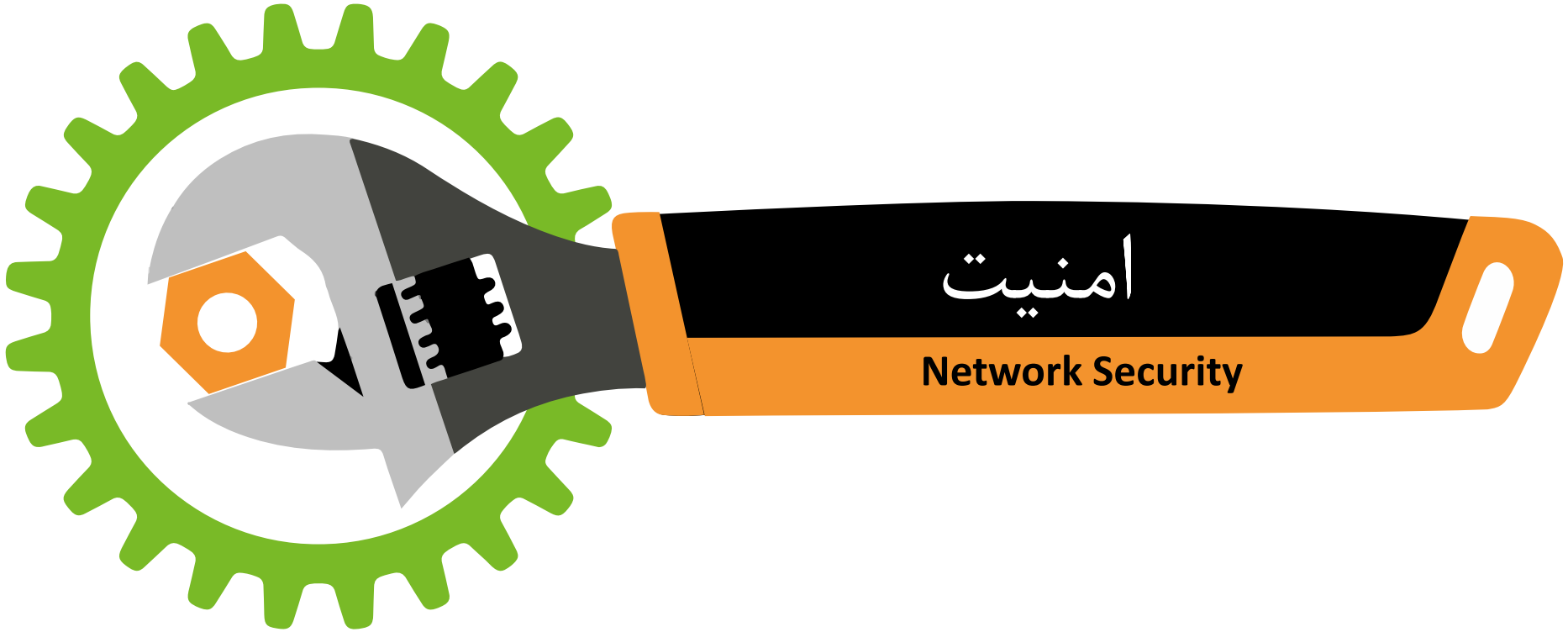

امنیت
Network Security

Network Security

عناوینی که مورد بررسی قرار میگیرد

۰۱ امنیت شبکه

تعریف امنیت شبکه

۰۲ اهداف امنیت شبکه

سه هدف اصلی اهداف اهمنیت شبکه ارایه می شود

۰۳ انواع امنیت

انواع امنیت شبکه از نظر تکنولوژی

۰۴ مزایا

مزایای امنیت شبکه ارایه می شود

Network Security

عناوینی که مورد بررسی قرار میگیرد

۰۵ عملکرد
نحوه عملکرد و معماری آن ارایه می شود

۰۶ چالش
خطرات و چالش های امنیت شبکه بررسی می شود

۰۷ تامین امنیت
راه های تامین امنیت شبکه بیان می شود

۰۸ پروتکل
پروتکل های امنیت شبکه ارایه می شود

امنیت شبکه

امنیت یک کلید واژه نسبی است که با مدیریت ریسک همراه است

امنیت شبکه مجموعه‌ای از روش ها و فناوری‌ها است که از زیرساخت شبکه در برابر حملات، دسترسی غیرمجاز و نقض داده‌ها محافظت می‌کند. امنیت شبکه را می‌توانیم به‌عنوان حوزه‌ای از امنیت سایبری مطرح کنیم که بر حفاظت از شبکه‌های کامپیوتری در برابر تهدیدهای سایبری متمرکز است.این شامل انواع اقدامات ,فناوری و شیوه های طراحی شده برای حفاظت از یکپارچگی شبکه و اطمینان از محرمانه بودن ودسترسی به داده ها است.

امنیت شبکه شامل تمام مراحلی

است که برای محافظت از یکپارچگی

یک شبکه کامپیوتری و داده های

درون آن انجام می شود.امنیت شبکه مهم است زیرا داده های حساس را از حملات سایبری ایمن نگه می دارد و

اطمینان می دهد که شبکه قابل

اطمینان و قابل استفاده است.

استراتژی های امنیت شبکه موفق از چندین راه حل امنیتی برای محافظت از کاربران و سازمان ها در برابر بدافزا رها و حملات سایبری مانند انکار سر ویس توزیع شده استفاده می کند

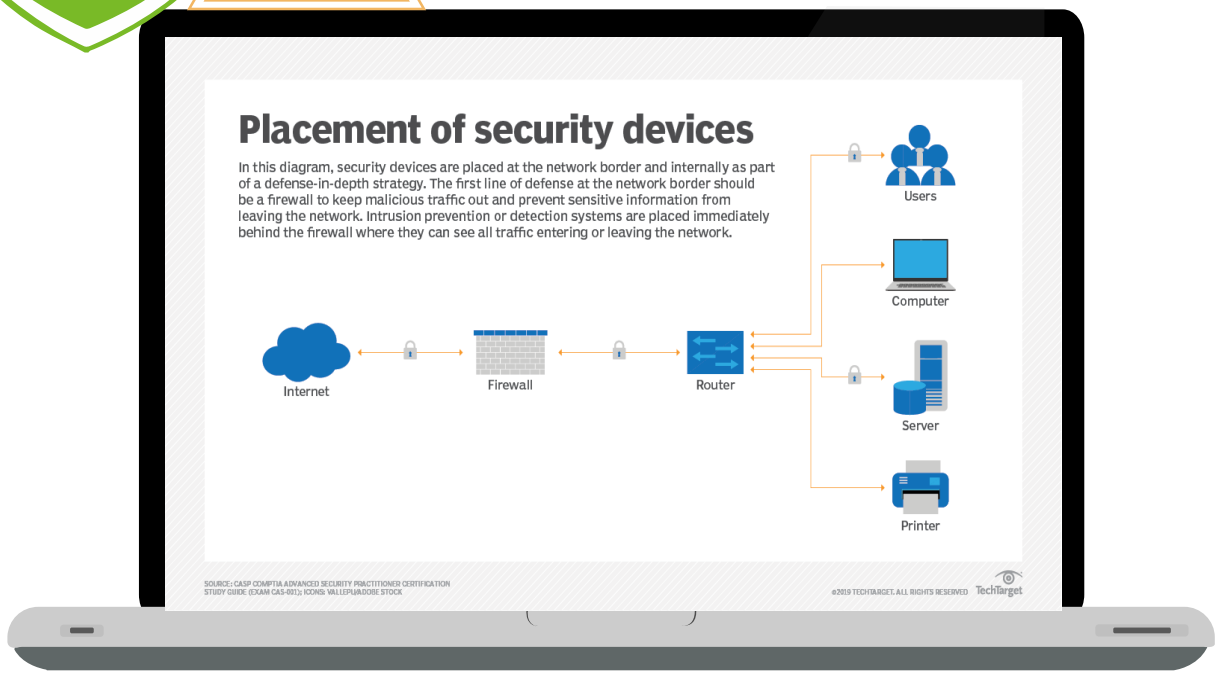
همون طور که همه میدونیم شبکه از دستگاه های متصل به هم مانند کام پیوتر ,سرور, و شبکه های بی سیم تشکیل شده است.بسیاری از این د ستگاه ها در برار مهاجمان بالقوه مس تعد هستند.

امنیت شبکه شامل استفاده از انو اع نرم افزار ها و ابزارهای سخت ا فزاری در شبکه یا به عنوان نرم ا فزار به عنوان سرویس است.

امنیت وقتی اهمیت خودش رو ب یشتر نشون می ده و نمود پیدا م یکند که شرکت ها جهت تجارت بیشتر به شبکه و داده های خود متکی هستند.جهت تهدید های جدیدی که در شبکه بوجود می آ ید باید متد و روش های جدیدی برای امنیت شبکه پیدا کرد.

روش های امنیتی باید با ایجاد رو ش های حمله جدید در این شب که های پیچیده تر متحول شوند.

نـمـا ی شمـا تـیـک



نمودار وسایل امنیتی

در این شکل وسایل امنیتی در مرز شبکه و به صورت داخلی به عنوان بخشی از استراتژی دفاعی عمیق قرار می گیرند.اولین خط دفاعی در مرز شبکه باید یک فایروال باشد تا از ترافیک مخرب جلوگیری کند و از خروج اطلاعات حساس از شبکه جلوگیری نماید.سیستم های تشخیص یا پیشگیری از نفوذ بلافاصله در پشت فایروال قرار می گیرند و می توانند تمام ترافیک ورودی یا خروجی از شبکه را ببینند.

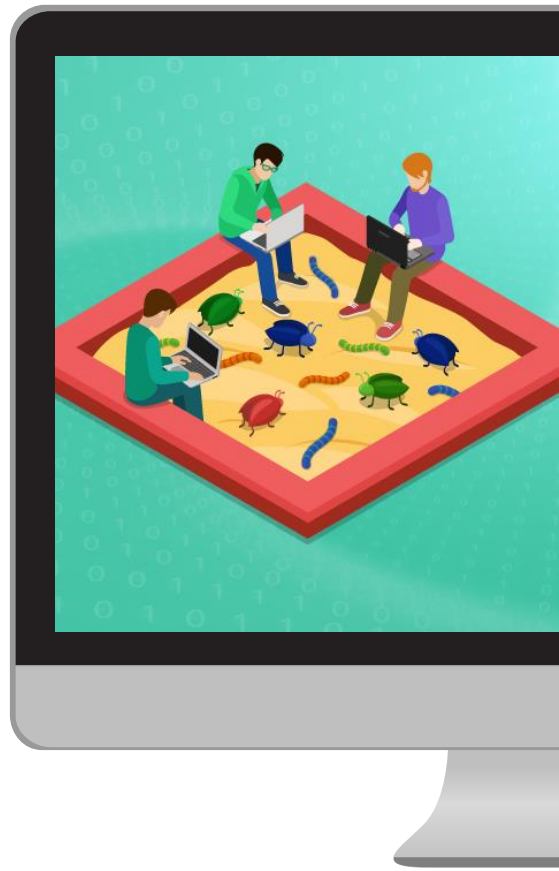
خط دفاعی

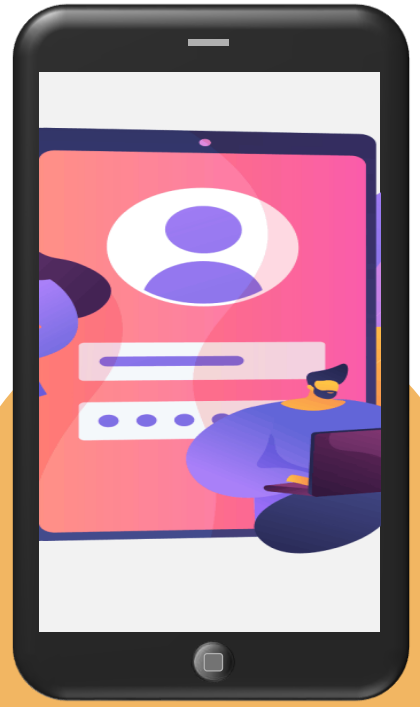
- آموزش کاربران
- فایروال (سخت افزاری یا نرم افزاری)
- تجهیزات امنیتی
- سامانه تشخیص نفوذ

اهداف امنیت شبکه

- جلوگیری از دسترسی غیرمجاز به منابع شبکه
- شناسایی و متوقف کردن حملات سایبری
- اطمینان از دسترسی ایمن کاربران مجاز به منابع شبکه مورد نیازشان
- جلوگیری از نقض داده

امنیت شبکه چگونه کار می کند؟





امنیت شبکه

معماری امنیت شبکه از ابزارهایی تشکیل شده است که از خود شبکه و اپلیکیشن‌هایی که روی آن اجرا می‌شوند، محافظت می‌کند. استراتژی‌های موثر امنیت شبکه از چندین خط دفاعی استفاده می‌کنند که مقیاس‌پذیر و خودکار هستند. هر لایه دفاعی مجموعه‌ای از سیاست‌های امنیتی تعیین‌شده توسط مدیر را اعمال می‌کند. امنیت شبکه با محافظت از یکپارچگی زیرساخت شبکه، منابع و ترافیک حملات سایبری را خنثی می‌کند و تاثیر مالی و عملیاتی آن‌ها را به حداقل می‌رساند.

امنیت شبکه

یک مقام یا تیم امنیتی استراتژی ها و سیاست هایی را تعیین می کند تا شبکه را ایمن نگه می دارد و به آن کمک میکند تا با استاندارد ها و مقررات امنیتی مطابقت داشته باشد.همه افراد در شبکه باید از این سیاست های امنیتی پیروی کنند.هر نقطه در شبکه که یک کاربر دسترسی دارد در واقع محلی است جهت تهدی توسط یک عامل خارجی یا مخرب که معمولا از طریق بی احتیاطی و یا اشتباه کاربر رخ می دهد.

عناصر امنیت شبکه

Network access control

بهترین راهکار ایجاد امنیت در لایه شبکه است که با راهکاری مطمئن برای اعطا دسترسی به افراد عمل میکند

SD-WAN security

رویکردی نرم فزاری در شبکه گسترده است به منظور ارتباطی ایمن و هوشمند میان سرویس های مختلف است

Network behavior anomaly detection

تشخیص ناهنجارهای رفتار شبکه با تحلیل الگوهای معمول ترافیک شبکه هر گونه انحراف از رفتارهای معمول و نرمال را شناسایی کرده و میتواند تهدیدات ناشناخته و پیچیده را شناسایی کند

Network firewalls

فایروال نرم‌افزار یا سخت‌افزاری است که از ورود یا خروج ترافیک مشکوک یک شبکه جلوگیری می‌کند و درعین‌حال به ترافیک قانونی اجازه عبور می‌دهد. به عبارت دیگر، فایروال‌ها تهدیدهای بالقوه ترافیک شبکه را فیلتر کرده و حملات بدافزار، سوءاستفاده از آسیب‌پذیری، حملات ربات‌ها و سایر تهدیدها را مسدود می‌کنند.فایروال‌های سنتی با استفاده از یک دستگاه سخت‌افزاری در محل فیزیکی یک کسب‌وکار اجرا می‌شوند. امروزه بسیاری از فایروال‌ها می‌توانند به‌صورت نرم‌افزاری یا در فضای ابری اجرا شوند و نیاز به سخت‌افزار فایروال را از بین می‌برند. به‌علاوه، فایروال‌ها را می‌توان در لبه‌های یک شبکه مستقر کرد یا به‌صورت داخلی برای تقسیم یک شبکه بزرگ‌تر به زیرشبکه‌های کوچک‌تر مورد استفاده قرار داد. به‌این‌ترتیب اگر بخشی از شبکه در معرض خطر باشد، هکرها از سایر بخش‌ها جدا خواهند بود.

Cloud access security brokes

یک خط مشی امنیتی است یا توافقنامه ایی که بین ازایه دهندگان خدمات ابر و کاربران آن است و اطمینان را می دهد سیاست های امنیتی مورد تطبیق قرار میگیرد.

Intrusion prevention systems

یه خطی اینجا کشیده شده است تحت عنوان intrusion است.این خط intrusion یا نفوذ فاصله بین این سمت که بهش گفته می شود event و incedent و دنیای public این طرف.تا زمانی که intro اتفاق نیفته هر چیزی را که بررسی کنیم event است . به محض اینکه intro اتفاق افتاد حادثه شکل میگیرد.

Advanced network threat prevention

به راهکار امنیتی اشاره دارد که از سازمان ها در برابر حملات سایبری پیشرفته و تهیدات بدافزاری که هدف آنها استخراج دیتا و یا ایجاد اختلال است محافظت میکند,

Unified threat management

مدیریت یکپارچه تهدیدات یک رویکرد راه حل برای امنیت است که به جای داشتن یک راه حل برای هر نوع تهدید ,عملکردهای امنیتی متعددی را ارایه می دهد

DDoS mitigation

تلاش هکرها برای از دسترس خارج DDoSحمله کردن وب سایت یا سرور با ارسال سیل ترافیک به آن است/

انواع امنیت شبکه از نظر تکنولوژی

سیستم‌های امنیتی شبکه در دو سطح کار می‌کنند؛ در محیط و در منابع داخلی شبکه. کنترل‌های امنیتی در محیط تلاش می‌کنند تا از ورود تهدیدهای سایبری به شبکه جلوگیری کنند. اما گاهی اوقات مهاجمان شبکه موفق به نفوذ می‌شوند؛ بنابراین تیم‌های امنیت IT باید کنترل‌هایی را در اطراف منابع داخل شبکه مانند لپ‌تاپ‌ها یا داده‌ها نیز اعمال کنند. این استراتژی یعنی لایه‌بندی کنترل‌های چندگانه بین هکرها و آسیب‌پذیری‌های احتمالی را Defense in depthمی‌نامند

کنترل دسترسی به شبکه :NAC (Network Access Control)

راه‌حل‌های کنترل دسترسی به شبکه (NAC)مانند دروازه‌بان عمل‌کنند و مشخص می‌کنند که چه کسانی اجازه ورود به شبکه دارند و چه کارهایی می‌توانند انجام دهند. احراز هویت (Authentication)و مجوز (Authorization) دو نکته مهم در این کنترل دسترسی به شبکه است و یک راه حل امنیتی شبکه با کاربرد آسان و به طور فزاینده ایی محبوب است که برای تایید هویت کاربر به عواملی نیاز دارد

آنتی ویروس و ضد بدافزار:

آنتی ویروس و ضد بدافزار نرم افزارهایی هستند که برای شناسایی ,حذف یا جلوگیری از آلوده کردن رایانه و شبکه.ویروس هاو بدافزارها مانند اسب های تروجان,باج افزارها و جاسوس افرازها طراحی شده اند.

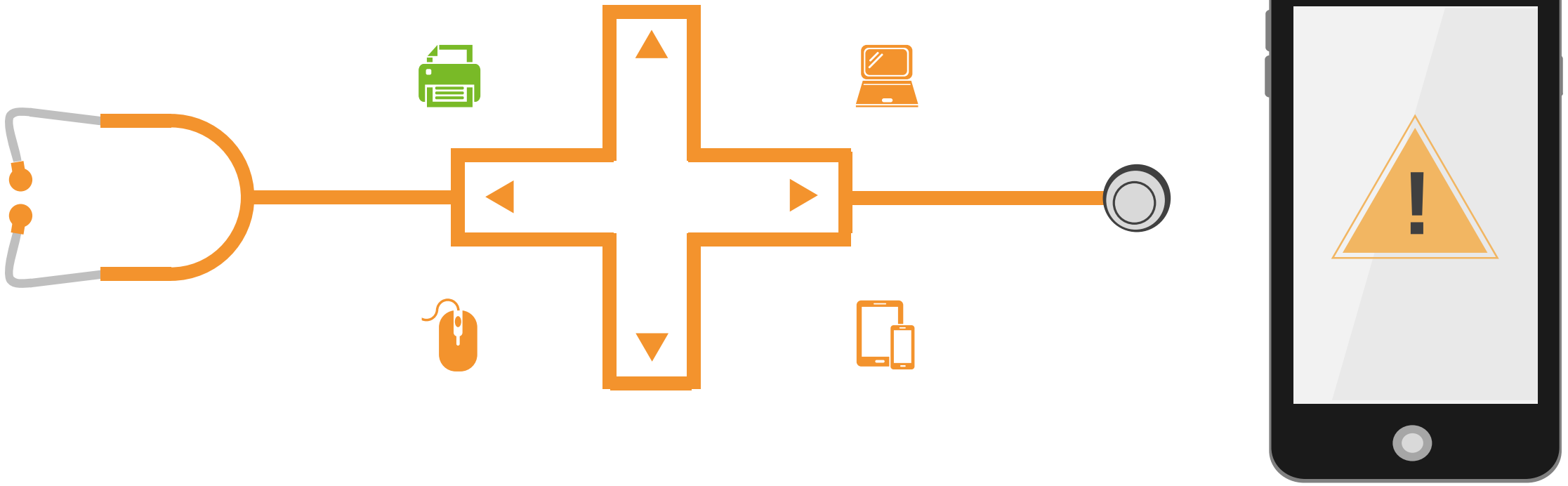
تقسیم بندی شبکه

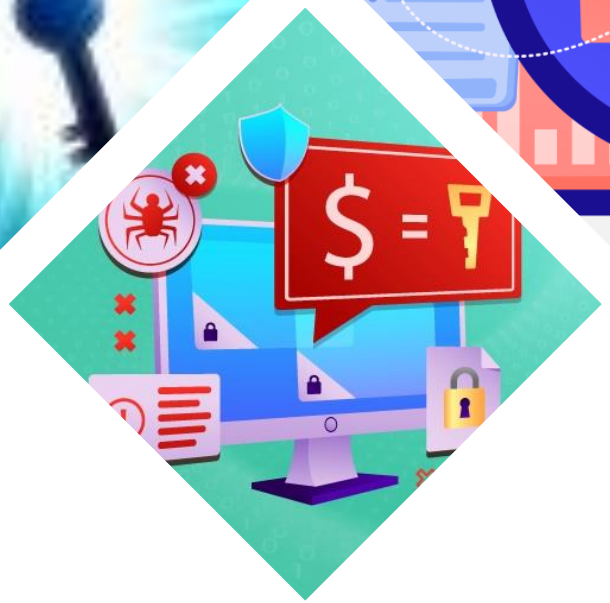
سازمان هایی با شبکه های بزرگ و ترافیک شبکه اغلب از تقسیم بندی شبکه به بخش های کوچکتر و مدیریت آسان تراستفاده می کنند.این رویکرد به سازمان ها کنترل بیشتر و دید بیشتری نسبت به جریان ترافیک می دهد.

امنیت دستگاه موبایل

برنامه های کاربردی تجاری برای گوشی های هوشمند و سایر دستگاه های تلفن همراه ,این دستگاه ها را به بخش مهمی از امنیت شبکه تبدیل کرده است.نظارت و کنترل اینکه کدام دستگاه های تلفن همراه به شبکه دسترسی دارند و کارهایی که پس از اتصال به شبکه انجام می دهند برای امنیت شبکه مدرن بسیار مهم است

انواع امنیت شبکه از نظر تکنولوژی





امنیت وب

این روش استفاده از وب کارمندان رادر شبکه و دستگاه های سازمان از جمله مسدئود کردن برخی تهدیدات و وب سایت ها کنترل می کند در حالی که از یکپارچگی خود وب سایت های سازمان نیز محافظت میکند.

امنیت بی سیم

شبکه های بی سیم یکی از پرخطر ترین بخش های یک شبکه هستند و نیاز به حفاظت و نظارت دقیق دارند.پیروی از بهترین شیوه های امنیت بی سیم مانند تقسیم بندی کاربران Wi-Fi بر اساس شناسه های مجموعه سرویس یا SSID و استفاده از احراز هویت ۸۰۲,۱ بسیار مهم است

تجزیه و تحلیل رفتاری

در این روش رفتار شبکه مورد بررسی قرار میگیرد و به طور خودکار سازمان را از فعالیت های غیر عادی مطلع نموده و هشدارهای لازم را صادر میکند

- **SIEM: Security information and event managemen**

این تکینک مدیریت امنیت داده ها را از برنامه ها و سخت افزار شبکه ثبت میکند و رفتارهای مشکوک را نظارت میکند.هنگامی که یک ناهنجاری شناسایی شودسیستم SIEM به سازمان هشدار می دهد و اقدامات مناسب دیگری را انجام میدهد.

انواع امنیت شبکه از نظر تکنولوژی

• محیط دفاع نرم افزاری SDP:Software defined perimeter

یک روش امنیتی است که در بالای شبکه ایی که از آن محافظت می کندقرار میگیردو آن را از مهاجمان و کاربران غیر مجاز پنهان می کند.از معیارهای هویت برای محدود کرددسترسی به منابع استفاده می کند و یک مرز مجازی در اطراف منابع شبکه تشکیل می دهد.

شبکه های خصوصی مجازی (VPN)

یک شبکه خصوصی مجازی (VPN)با رمزگذاری داده‌های کاربران و پوشاندن آدرس IP و مکان آن‌ها از هویتشان محافظت می‌کند. در صورت استفاده از VPN، کاربران به‌طور مستقیم به اینترنت متصل نمی‌شوند، بلکه به یک سرور امن که به اینترنت متصل است، وصل می‌شوند.VPNها به کارکنان از راه دور کمک می‌کنند تا حتی از طریق اتصالات Wifi عمومی ناامن به‌طور ایمن به شبکه‌های شرکت دسترسی پیدا کنند. شبکه‌های خصوصی مجازی ترافیک کاربر را رمزگذاری می‌کنند و آن را از هکرهایی که به‌دنبال رهگیری ارتباطات آن‌ها هستند، در امان نگه می‌دارند.

امنیت اپلیکیشن (Application security)

محافظت از برنامه های حیاتی یک سازمان است که جهت محافظت از کسب و کار او مجموعه می باشد.امنیت اپلیکیشن به مراحلی گفته می‌شود که تیم‌های امنیتی برای محافظت از اپلیکیشن‌ها و APIها در برابر مهاجمان شبکه انجام می‌دهند. ازآنجایی‌که بسیاری از کمپانی‌های امروزی از اپلیکیشن‌ها برای انجام توابع (Functions)کلیدی کسب‌وکار یا پردازش داده‌های حساس استفاده می‌کنند، اپلیکیشن‌ها یک هدف رایج برای مجرمان سایبری هستند. بسیاری از اپلیکیشن‌های کسب‌وکاری روی ابر عمومی میزبانی می‌شوند؛ ازهمین‌رو هکرها می‌توانند از آسیب‌پذیری‌های آن‌ها برای نفوذ به شبکه‌های خصوصی شرکت سوءاستفاده کنند.اقدامات امنیت اپلیکیشن از اپلیکیشن‌ها در برابر عوامل مخرب محافظت می‌کند. ابزارهای رایج امنیت اپلیکیشن شامل فایروال‌های وب اپلیکیشن (WAF)، خودمحافظتی اپلیکیشن در زمان اجرا (RASP)، تست امنیت اپلیکیشن استاتیک (SAST) و تست امنیت اپلیکیشن پویا (DAST) می‌شود.

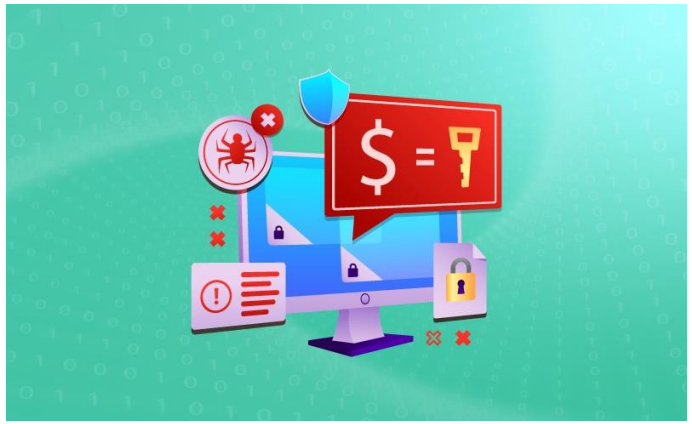
امنیت ایمیل (Email security)

درگاه‌های ایمیل اولین عامل تهدید برای نقض امنیت هستند. مهاجمان از اطلاعات شخصی و تاکتیک‌های مهندسی اجتماعی برای ایجاد کمپین‌های فیشینگ پیچیده برای فریب دادن گیرنده‌ها و ارسال آن‌ها به سایت‌هایی که بدافزار دارند، استفاده می‌کنند. ابزارهای امنیتی ایمیل می‌توانند به خنثی کردن حملات فیشینگ و سایر تلاش‌ها برای به خطر انداختن حساب‌های ایمیل کاربران کمک کنند. بیشتر سرویس‌های ایمیل ابزارهای امنیتی داخلی مانند فیلترهای اسپم و رمزگذاری پیام دارند. یک اپلیکیشن امنیت ایمیل حمله‌های ورودی را مسدود کرده و پیام‌های خروجی را کنترل می‌کند تا جلوی از دست رفتن داده‌های حساس را بگیرد.

انواع امنیت شبکه از نظر تکنولوژی

Sandbox

این رویکرد به سازمان ها اجازه می دهد تا با باز کردن یک فایل در یک محیط ایزوله قبل از دسترسی به شبکه بدافزار را اسکن کند.یک **Sandbox** به **IDS/IPS** شباهت دارد، با این تفاوت که **Sandbox** به امضاها وابسته نیست. یک **Sandbox** می‌تواند یک محیط سیستم نهایی (**End-system**) را شبیه‌سازی کرده و مشخص کند که آیا یک شی بدافزار در حال تلاش برای انجام کاری مانند اسکن پورت است یا خیر.



NTA/ NDR

- **NTA/NDR** به‌طور مستقیم به ترافیک یا رکوردهای ترافیک مانند **NetFlow** نگاه می‌کند و از الگوریتم‌های یادگیری ماشین و تکنیک‌های آماری برای ارزیابی ناهنجاری‌ها و تشخیص وجود یک تهدید بهره می‌برد. **NTA/NDR** ابتدا تلاش می‌کند تا یک خط مبنا (**Baseline**) تعیین کند؛ سپس با وجود یک خط مبنا ناهنجاری‌هایی مانند ارتباطات متناوب را شناسایی می‌کند.

DLP

پیشگیری از نشت داده ها – 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. **DLP** به ابزارها و استراتژی‌های امنیت اطلاعات اشاره دارد که تضمین می‌کنند داده‌های حساس نه به سرقت رفته‌اند و نه به‌طور تصادفی فاش شده‌اند. **DLP** شامل سیاست‌های امنیت داده‌ها و تکنولوژی‌های هدفمند است که جریان‌های داده‌ای را ردیابی کرده، اطلاعات حساس را رمزگذاری می‌کند و درصورت شناسایی فعالیت مشکوک، هشدار می‌دهد.

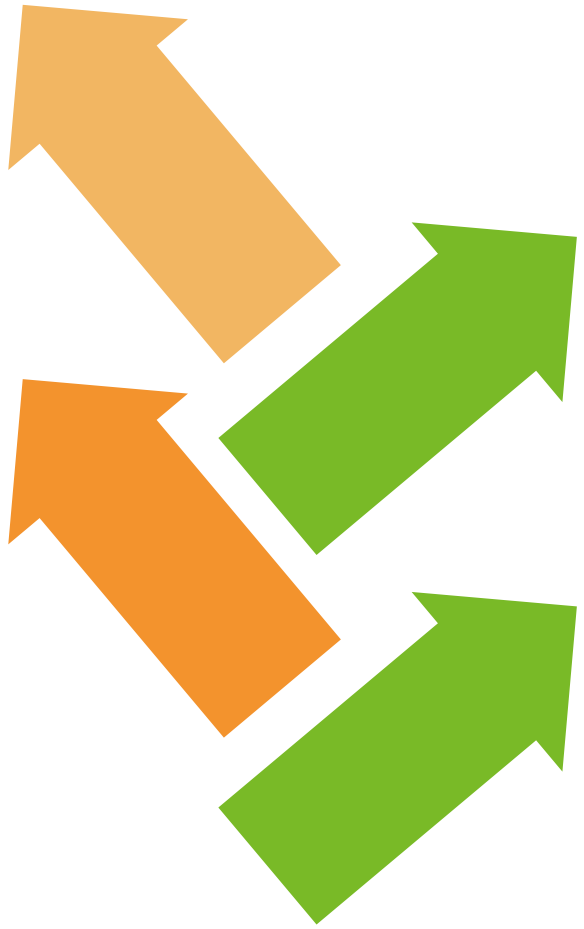
مزایای امنیت شبکه

از فروشگاه‌های آنلاین گرفته تا اپلیکیشن‌های سازمانی و دسکتاپ‌های از راه دور

امنیت شبکه کلید توانایی سازمان در ارائه محصولات و سرویس‌ها به مشتریان و کارکنان است

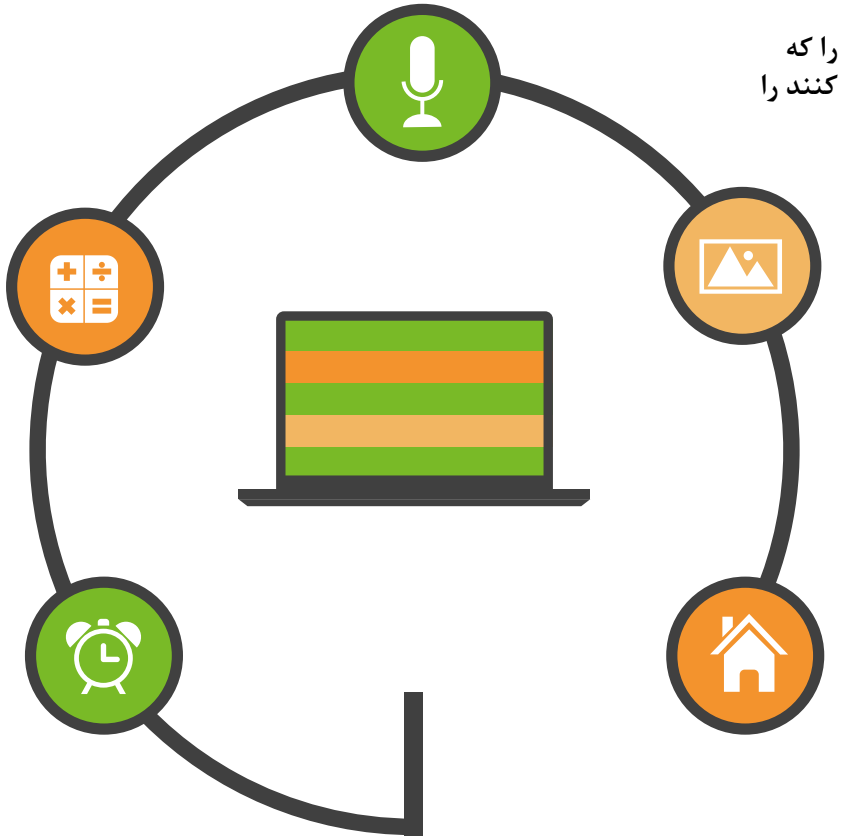
محافظت از اپلیکیشن‌ها و داده‌های روی شبکه برای پیشرفت و ترقی کسب‌وکار و همچنین اعتبار یک سازمان ضروری است

امنیت شبکه موثر از خارج شدن زیرساخت از دسترس جلوگیری کرده و در نتیجه عملکرد شبکه را بهبود می‌بخشد



مزایای امنیت شبکه

کارکرد :
امنیت شبکه عملکرد بالای مداوم شبکه هایی را که کسب و کارها و کاربران فردی به آن تکیه می کنند را تضمین می کنند



حریم خصوصی و امنیت
محرمانه بودن و در دسترس بودن و یکپارچگی که به عنوان سه گانه **CIA** شناخته می شود و اعتبار یک کسب و کار را تضمین میکند

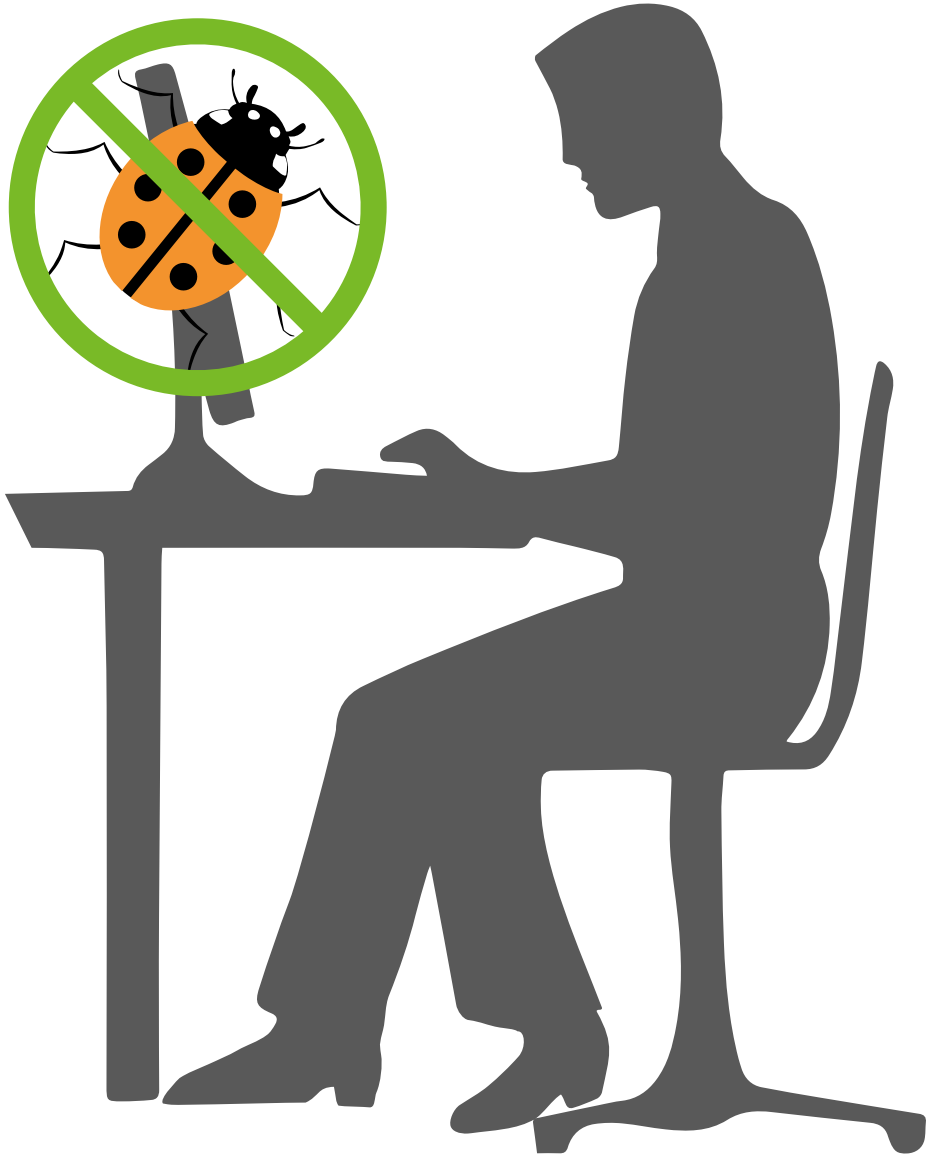
حفاظت از مالکیت معنوی
کلید توانایی شرکت ها برای رقابت و بوجود آمدن مزیت رقابتی است

انطباق
رعایت مقررات امنیت داده و حفظ حریم خصوصی

نحوه عملکرد امنیت شبکه

امنیت شبکه چندین لایه دفاعی را در لبه و شبکه ترکیب می‌کند، به‌طوری‌که هر لایه امنیتی شبکه سیاست‌ها و کنترل‌ها را پیاده‌سازی می‌کند. عناصر معماری امنیتی کامل و چند لایه که امنیت شبکه را در سراسر یک سازمان پیاده‌سازی می‌کند، به دو دسته کلی تقسیم می‌شوند؛ کنترل دسترسی و کنترل تهدید که در ادامه به بررسی آن‌ها می‌پردازیم

- **کنترل دسترسی (Access Control)**
- **کنترل تهدید (Threat Control)**

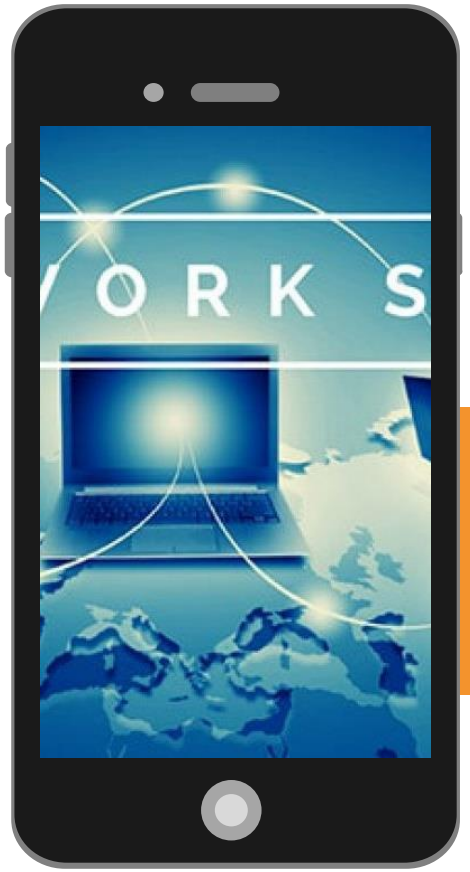


نحوه عملکرد امنیت شبکه

کنترل دسترسی Access Contr

(ol)

امنیت شبکه با کنترل دسترسی شروع می‌شود. در بخش کنتر
ل دسترسی، دسترسی به داده‌ها و نرم‌افزارهای مورد استفاده برا
ی جلوگیری از دستکاری آن داده‌ها محدود می‌شود. کنترل د
سترسی برای جلوگیری از دسترسی غیرمجاز و کاهش خطر ته
دیدهای داخلی بسیار مهم است. اگر عوامل مخرب به یک شب
که دسترسی پیدا کنند، می‌توانند با نظارت بر ترافیک و نقشه‌بر
داری از زیرساخت، اقدام به حمله DDoS کرده یا بدافزار وارد
کنند. راه‌حل‌های مدیریت هویت و دسترسی (Identity and
Access Management- IAM)می‌تواند در این زمینه به
شما کمک کند. بسیاری از شرکت‌ها از شبکه‌های خصوصی مجا
زی ((VPNبرای کنترل دسترسی استفاده می‌کنند. بااین‌حال،
امروزه جایگزین‌هایی برای VPNها 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.



کنترل تهدید Threat Co

(ntrol)

حتی با وجود کنترل دسترسی نیز ممکن است مشکلاتی ایجاد شود.
به‌عنوان مثال، یک عامل بد ممکن است از اعتبار یک کارمند برای و
رود به شبکه استفاده کند. بنابراین نیاز به کنترل تهدید Threat C
(ontrol کاملا احساس می‌شود که در ترافیکی که قبلا مجاز اعلام
شده است عمل کند. کنترل تهدید از اقدامات عوامل مخرب برای آ
سیب رساندن به شبکه جلوگیری می‌کند.فناوری‌های کنترل تهدید
با فایروال و لود بالانسر (Load balancer)شروع می‌شود. این دس
تگاه‌ها از شبکه در برابر حملات DoS و DDoS محافظت می‌کنند.
در مرحله بعد، IDS/IPS با حملات شناخته‌شده که از طریق شبکه ا
نجام می‌شود، مقابله می‌کند. در نهایت اشیای بدافزار ناشناخته‌ای که
در شبکه حرکت می‌کنند، با فناوری‌های Sandbox گرفته می‌شوند
؛ درحالی‌که ناهنجاری‌ها در ترافیک شبکه که ممکن است نشانه‌های
ی از یک تهدید باشند، با NTA/NDR شناسایی می‌شوند.

خطرات رایج امنیت شبکه

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

کنترل دسترسی از راه دور

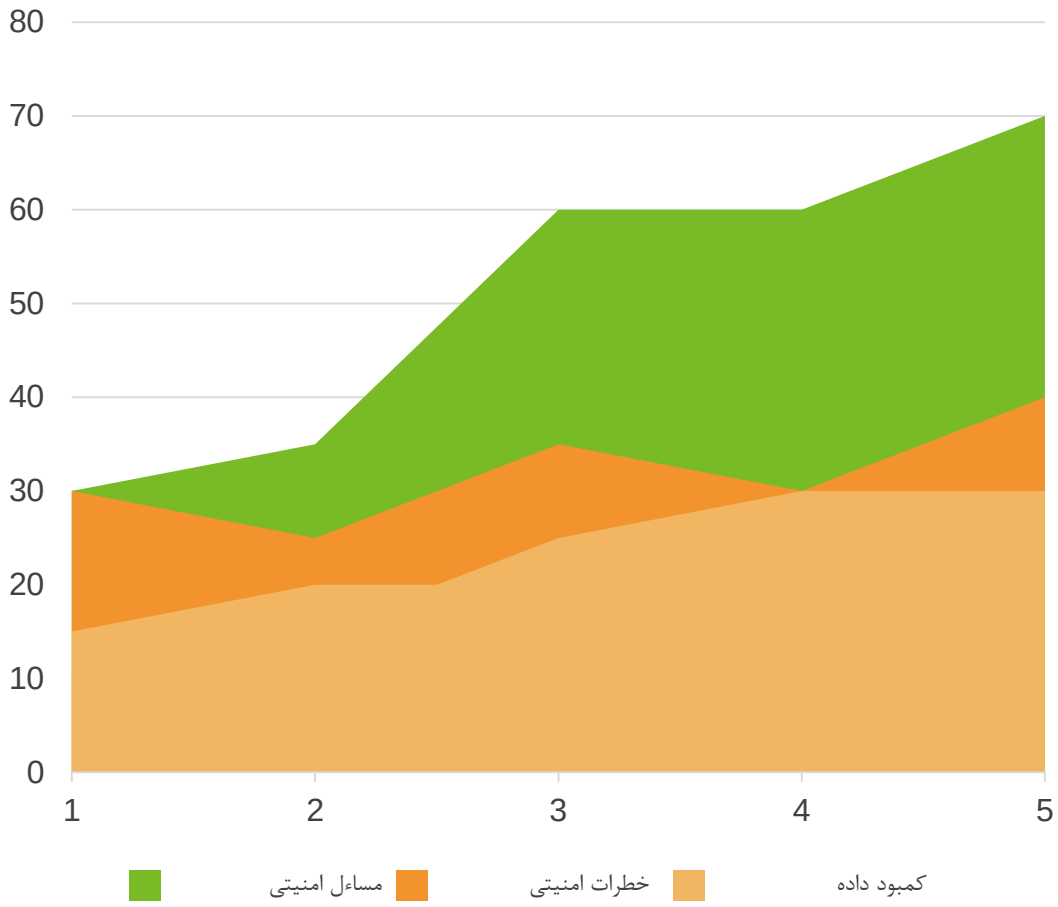
از آلودگی‌های رایج بدافزاری می‌توان به باج‌افزارها (Ransomware) اشاره کرد که داده‌ها را رمزگذاری می‌کنند یا از بین می‌برند و با این عمل دسترسی کاربران به شبکه را محدود می‌کنند. کرم‌ها (worms) بدافزارهایی هستند که می‌توانند به‌سرعت در سراسر شبکه تکثیر شوند. نرم‌افزارهای جاسوسی (spyware) که به مهاجمان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

اگر یک کاربر غیرمجاز به یک شبکه دسترسی پیدا کند، می‌تواند اطلاعات محرمانه آن شبکه را مشاهده کند. عوامل مخرب با دسترسی غیرمجاز به شبکه‌های کامپیوتری می‌توانند داده‌های محرمانه را افشا کنند یا سیستم‌های داخلی را به خطر بیندازند.

کارمندان یا پیمانکاران داخلی می‌توانند به‌طور ناخواسته امنیت شبکه را تضعیف کنند یا در صورت ناآگاهی 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.

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.

بزرگترین چالشهایی که تیم های شبکه در هنگام رسیدگی به مسایل امنیتی با آن مواجه هستند



گزینه A

%۴۹

ارتباط مسایل امنیتی با عملکرد شبکه

گزینه B

%۴۵

تایید خطرات امنیتی موجود

گزینهC

%۴۴

کمبود داده برای شناسایی حوادث امنیتی بالقوه

%۴۱

تلاش برای به دست آوردن داده های بیشتر

%۳۸

تلاش برای شناسایی نقطه ورود و دامنه نفوذ

راه‌های تامین امنیت شبکه‌های کامپیوتری

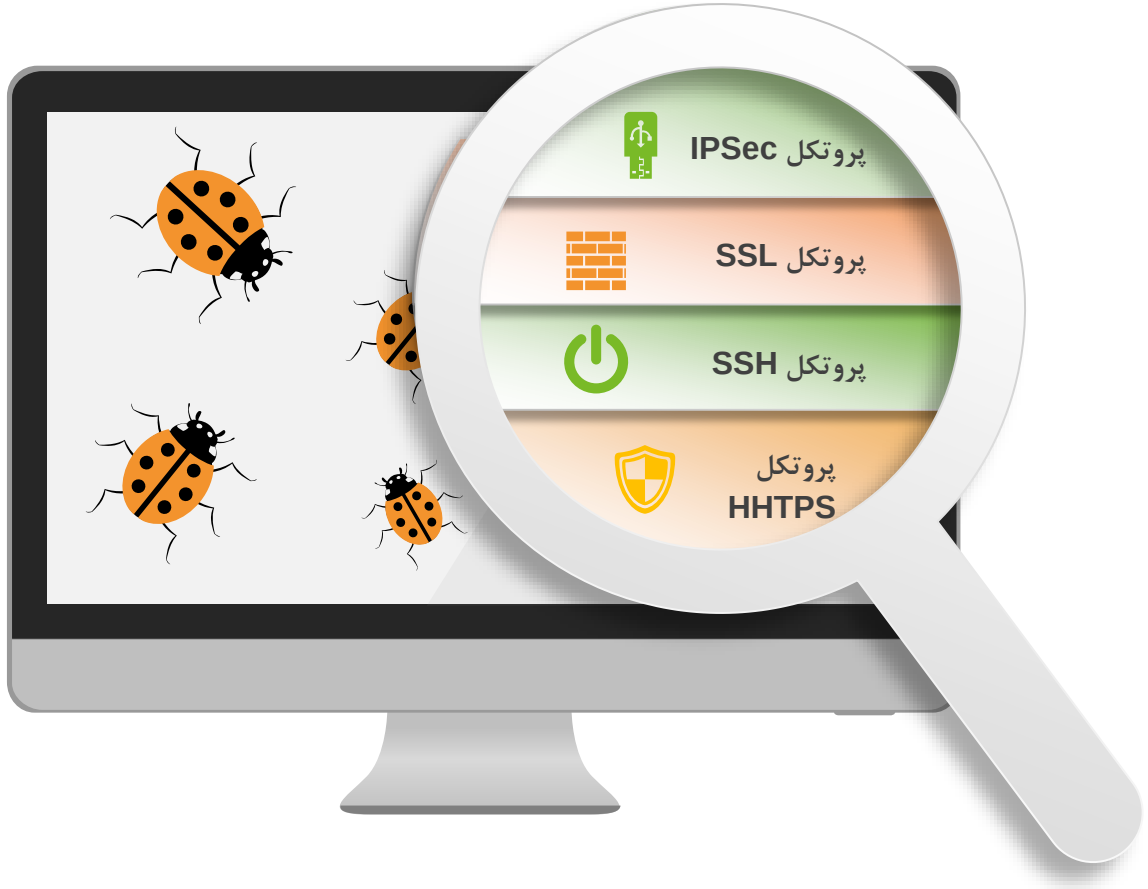
پشتیبان‌گیری از داده‌ها و ذخیره چند فایل پشتیبان

حتی شبکه‌ای که امنیت بسیار بالایی دارد نیز ممکن است در معرض حمله قرار گیرد. از دست دادن دسترسی جزئی یا کامل به داده‌ها و سیستم‌های داخلی می‌تواند برای یک کسب‌وکار 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.

پروتکل‌های امنیتی شبکه :



A

پـروتـکل IPSec

احراز هویت داده‌ها، یکپارچگی و همچنین حریم خصوصی بین دو موجودیت را ارائه می‌دهد

B

پـروتـکل SSL

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 همچنین خواندن آن‌ها توسط مجرمان جلوگیری می‌شود.

C

پروتکل SSH

پروتکل **SSH**یک پروتکل امنیتی شبکه است که ارتباطات و داده‌های شبکه را رمزنگاری می‌کند. این پروتکل به خط فرمان اجازه می‌دهد تا از راه دور وارد سیستم شود و وظایف خاصی را از راه دور انجام دهد

D

پروتکلHHTPS

پروتکل HTTPSیک پروتکل امنیت شبکه است که برای ایمن‌سازی ارتباطات داده بین دو یا چند سیستم استفاده می‌شود