" مفاهیم امنیت شبکه "

امنیت شبکه یا Network Security پروسه‌ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. متخصصین امنیت شبکه مراحل ذیل را برای ایجاد امنیت پیشنهاد و تایید نموده‌اند:

۱. شناسایی بخشی که باید تحت محافظت قرار گیرد.
۲. تصمیم گیری درباره مواردی که باید در مقابل آنها از بخش مورد نظر محافظت کرد.
۳. تصمیم گیری درباره چگونگی تهدیدات
۴. پیاده سازی امکاناتی که بتوانند از دارایی های شما به شیوه‌ای محافظت کنند که از نظر هزینه به صرفه باشد.
۵. مرور مجدد و مداوم پروسه و تقویت آن درصورت یاقتن نقطه ضعف

مفاهیم امنیت شبکه:

برای درک بهتر مباحث مطرح شده در این بخش ابتدا به طرح بعضی مفاهیم در امنیت شبکه می پردازیم.

۱. منابع شبکه :

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبکه را معرفی می کند که باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

۱. تجهیزات شبکه مانند Router , Switches , Firewall .
۲. اطلاعات عملیات شبکه مانند : Routing Table و Configuration و Access List که بر روی Router ذخیره شده اند.
۳. منابع نامحسوس شبکه مانند: Bandwidth و Traffic.
۴. اطلاعات و منابع اطلاعاتی متصل به شبکه مانند Database و Application Server .
۵. ترمینالهایی که برای استفاده از منابع مختلف به شبکه متصل می شوند.
۶. اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان .
۷. خصوصی نگهداشتن عملیات کاربران و استفاده آنها از منابع شبکه جهت جلوگیری از شناسایی کاربران.

مجموعه فوق به عنوان دارایی ها یا منابع یک شبکه قلمداد می شود .

۲. حمله :

اکنون به تعریف حمله می پردازیم تا بدانیم که از شبکه در مقابل چه چیزی باید محافظت کنیم. حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرارگیرد که مورد نظر نبوده است.متخصصین امنیت شبکه ، حملات شبکه را به سه دسته عمومی تقسیم کنیم:

۱. دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه .
۲. دستکاری غیرمجاز اطلاعات بر روی یک شبکه.
۳. حملاتی که منجر به اختلال در ارائه سرویس می شوند و اصطلاحاً Denial of Service نام دارند.

کلمه کلیدی در دو دسته اول انجام اعمال به صورت غیرمجاز است. تعریف یک عمل مجاز یا غیرمجاز به‌عهده سیاست امنیتی شبکه است، اما به عبارت کلی می توان دسترسی غیرمجاز را تلاش یک کاربر جهت دیدن یا تغییر اطلاعاتی که برای وی در نظر گرفته نشده است، تعریف نمود.اطلاعات روی یک شبکه نیز شامل اطلاعات موجود برروی رایانه های متصل به شبکه مانند Database Server و Web Server ، اطلاعات در حال تبادل بر روی شبکه و اطلاعات مختص اجزاء شبکه جهت انجام کارها مانند Router Routing Table است. منابع شبکه را نیز می‌توان تجهیزات انتهایی مانند Router و Firewall یا مکانیزمهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبکه ، حفاظت از شبکه در مقابل حملات فوق است، لذا می توان اهداف را نیز در سه دسته ارائه کرد:

۱. ثابت کردن محرمانگی داده
۲. نگهداری جامعیت داده
۳ . نگهداری در دسترس بودن داده

۳. تحلیل خطر :

پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها ، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطر محافظت کرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از :

۱. احتمال انجام حمله
۲. خسارت وارده به شبکه درصورت انجام حمله موفق

۴. سیاست امنیتی :

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات نپردازد. جزئیات می توانند طی

مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست های آن را تشکیل می دهند ثابت باقی می‌مانند. در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

۱. چه و چرا باید محافظت شود.
۲. چه کسی باید مسئولیت حفاظت را به عهده بگیرد .
۳. زمینه ای را بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

سیاستهای امنیتی را می توان به طور کلی به دو دسته تقسیم کرد:

۱. مجاز (Permissive) : هر آنچه بطور مشخص ممنوع نشده است ، مجاز است.
۲. غیر مجاز (Restrictive) : هر آنچه بطور مشخص مجاز نشده است ، ممنوع است.

معمولا ایده استفاده از سیاستهای امنیتی محدودکننده بهتر و مناسبتر است چون سیاستهای مجاز دارای مشکلات امنیتی هستند و نمی توان تمامی موارد غیرمجاز را برشمرد. المانهای دخیل در سیاست امنیتی در RFC2196 لیست و ارائه شده اند.

۵. طرح امنیت شبکه :

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یک طرح امنیت شبکه می رسیم. المانهای تشکیل دهنده یک طرح امنیت شبکه عبارتند از:

۱. ویژگیهای امنیتی هر دستگاه مانند کلمه عبور مدیریتی و یا بکارگیری SSH .
۲. Firewalls
۳. مجتمع کننده های VPN برای دسترسی از دور
۴. Intrusion Detection (تشخیص نفوذ)
۵. سرویس دهنده های امنیتی AAA (Authentication , Authorization & Accounting) و سایر خدمات AAA جهت شبکه .
۶. مکانیزمهای کنترل دسترسی و محدودکننده دسترسی برای دستگاههای مختلف شبکه.

۶. نواحی امنیتی :

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می‌کند. در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه ، طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر توپولوژی است و یکی از مهمترین ایده های مورد استفاده در شبکه های امن مدرن ، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

نواحی امنیتی بنابر استراتژی های اصلی ذیل تعریف می شوند.

تجهیزات و دستگاههایی که بیشترین نیاز امنیتی را دارند (شبکه خصوصی) در امن ترین منطقه قرار می‌گیرند. معمولا اجازه دسترسی عمومی یا از شبکه های دیگر به این منطقه داده نمی شود. دسترسی با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از دور امن (Secure Remote Access) کنترل می شود. کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه به شدت انجام می شود .

سرویس دهندهایی که فقط باید از سوی کاربران داخلی در دسترس باشند در منطقه ای امن ، خصوصی و مجزا قرار می گیرند. کنترل دسترسی به این تجهیزات با کمک فایروال انجام می شود و دسترسی ها کاملا نظارت و ثبت می شوند .

سرورهایی که باید از شبکه عمومی مورد دسترسی قرار گیرند در منطقه ای جدا و بدون امکان دسترسی به مناطق امن تر شبکه قرار می گیرند. درصورت امکان بهتر است هر یک از این سرورها را در منطقه ای مجزا قرار داد تا درصورت مورد حمله قرار گرفتن یکی ، سایرین مورد تهدید قرار نگیرند. به این مناطق DMZ یا Demilitarized Zone می گویند.

استفاده از فایروالها به شکل لایه ای و به کارگیری فایروالهای مختلف سبب می شود تا درصورت وجود یک اشکال امنیتی در یک فایروال ، کل شبکه به مخاطره نیفتد و امکان استفاده از Backdoor نیز کم شود.