" امنیت تجهیزات شبکه "

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیر ترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون: Router , Switch , Firewall .

امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد :

۱. عدم وجود امنیت تجهیزات در شبکه به نفوذگران به شبکه اجازه می‌دهد که با دستیابی به تجهیزات ،امکان پیکربندی آنها را به گونه‌ای که تمایل دارند آن سخت‌افزارها عمل کنند، داشته باشند. از این طریق هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه، توسط نفوذگر، امکان‌پذیر خواهد شد.

۲. برای جلوگیری از خطرهای DoS (Denial of Service) تأمین امنیت تجهزات بر روی شبکه الزامی است. توسط این حمله‌ها نفوذگران می‌توانند سرویس‌هایی را در شبکه از کار بیاندازند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای AAA فراهم می‌شود.

در این بخش اصول اولیه امنیت تجهیزات مورد بررسی اجمالی قرار می‌گیرد. عناوین برخی از این موضوعات به شرح زیر هستند :

۱. امنیت فیزیکی و تأثیر آن بر امنیت کلی شبکه
۲. امنیت تجهیزات شبکه در سطوح منطقی
۳. بالا بردن امنیت تجهیزات توسط افزونگی در سرویس‌ها و سخت‌افزارها

موضوعات فوق در قالب دو جنبه اصلی امنیت تجهیزات مورد بررسی قرار می‌گیرند :

۱. امنیت فیزیکی
۲. امنیت منطقی

امنیت فیزیکی:

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمله‌اند. با استفاده از افزونگی، اطمینان از صحت عملکرد سیستم در صورت ایجاد و رخداد نقص در یکی از تجهیزات (که توسط عملکرد مشابه سخت‌افزار و یا سرویس‌دهنده مشابه جایگزین می‌شود) بدست می‌آید.

در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطرهایی که از این طریق تجهزات شبکه را تهدید می‌کنند نگاهی داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله‌ها می‌توان به راه‌حل‌ها و ترفندهای دفاعی دربرابر این‌گونه حملات پرداخت.

۱. افزونگی در محل استقرار شبکه :

یکی از راه‌کارها در قالب ایجاد افزونگی در شبکه‌های کامپیوتری، ایجاد سیستمی کامل، مشابه شبکه‌ی اولیه‌ی در حال کار است. در این راستا، شبکه‌ی ثانویه‌ی، کاملاً مشابه شبکه‌ی اولیه، چه از بعد تجهیزات و چه از بعد کارکرد، در محلی که می‌تواند از نظر جغرافیایی با شبکه‌ی اول فاصله‌ای نه چندان کوتاه نیز داشته باشد برقرار می‌شود. بااستفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به‌طور کامل مختل می‌کند (مانند زلزله) می‌توان از شبکه‌ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده‌های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه‌ی مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه‌های معمول که حجم چندانی ندارند، به دلیل هزینه‌های تحمیلی بالا، امکان‌پذیر و اقتصادی به نظر نمی‌رسد، ولی در شبکه‌های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب می‌آیند از الزامات است.

۲. توپولوژی شبکه :

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند.

در این مقوله، سه طراحی که معمول هستند مورد بررسی قرار می‌گیرند :

۱. طراحی سری : در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

۲. طراحی ستاره‌ای : در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از سرویس دهنده اصلی، سرویس‌دهی به دیگر نقاط دچار اختلال نمی‌گردد. با این وجود از آنجاییکه سرویس دهنده اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که می‌تواند بر اثر حمله فیزیکی به آن رخ‌دهد، ارتباط کل شبکه دچار اختلال می‌شود، هرچند که با در نظر گرفتن افزونگی برای سرویس دهنده اصلی از احتمال چنین حالتی کاسته می‌شود.

۳. طراحی مش : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

۴. محلهای امن برای تجهیزات :

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می‌گیرد :

- ✓ یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه‌ای که هرگونه نفوذ در محل آشکار باشد.
- ✓ در نظر داشتن محلی که در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه‌ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان‌های بلا استفاده سود برده است (که باعث ایجاد خطرهای امنیتی می‌گردد)، می‌توان اعتدالی منطقی را در نظر داشت.

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت :

- ✓ محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.
- ✓ استفاده از دوربین‌های پایش در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات ومراکز پایگاه‌های داده.
- ✓ اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

۵. انتخاب لایه کانال ارتباطی امن :

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از سرویس دهنده‌ها و سرویس‌دهنده‌های مورد اطمینان شبکه معطوف شده است، ولی گونه‌ای از حمله‌ی فیزیکی کماکان دارای خطری بحرانی است.

عمل شنود بر روی سیم‌های مسی، چه در انواع Coaxial و چه در Twisted Pairs ، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به‌گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

۶. منابع تغذیه :

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- ✓ طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه. این طراحی باید به‌گونه‌ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی تامین فشار بیش‌اندازه‌ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند.
- ✓ وجود منبع یا منابع تغذیه پشتیبان به گونه‌ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه‌تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند

۷. عوامل محیطی :

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برابر عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی که در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید در نظر گرفت می‌توان به دو عامل زیر اشاره کرد:

- ✓ احتمال حریق (که عموماً غیر طبیعی است و منشأ انسانی دارد)
- ✓ زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که می‌توان از عدم اختلال در شبکه در صورت بروز چنین وقایعی اطمینان حاصل کرد.

امنیت منطقی :

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به Routerهاو Switch های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند. در این بخش به عوامل و مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

۱. امنیت Router ها :

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند Switches، را می‌توان به سه دسته‌ی اصلی تقسیم نمود :

- ✓ حمله برای غیرفعال سازی کامل
- ✓ حمله به قصد دستیابی به سطح کنترل
- ✓ حمله برای ایجاد نقص در سرویس‌دهی

طبیعی است که راه‌ها و نکاتی که در این زمینه ذکر می‌شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای مرتبط با این تجهیزات جدا هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تأمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنبه‌ی آنرا تشکیل می‌دهد.

۲. مدیریت Configuration :

یکی از مهمترین نکات در امنیت تجهیزات، نگهداری نسخه های پشتیبان از پرونده‌های مختص پیکربندی است. از این پرونده‌ها که در حافظه‌های گوناگون این تجهیزات نگاهداری می‌شوند، می‌توان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می‌یابند، نسخه پشتیبان تهیه کرد.

با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را به آخرین حالت بی‌نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت‌افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم‌افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه نسخ پشتیبان را فاصله‌های زمانی متغیر دارا می‌باشند. با استفاده از این نرم‌افزارها احتمال حملاتی که به سبب تأخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید می‌آید به کمترین حد ممکن می‌رسد.

۳. کنترل دسترسی به تجهیزات :

دو راه اصلی برای کنترل تجهزات فعال وجود دارد :

- ✓ کنترل از راه دور
- ✓ کنترل از طریق درگاه کنسول

در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استاندارد ها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در مورد روش دوم، با وجود آنکه به نظر می‌رسد استفاده از چنین درگاهی نیاز به دسترسی فیزیکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد.

لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تأمین نمی‌کند.

برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه کنسول به هریک از تجهیزات داخلی Router، که امکان دسترسی از راه‌دور دارند، اطمینان حاصل نمود.

۴. امن سازی دسترسی :

علاوه بر پیکربندی تجهیزات برای استفاده از Authentication، یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش SSH(Secure Shell) است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPSec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است، به گونه‌ای که اغلب تولیدکنندگان تجهیزات فعال شبکه، خصوصاً تولید کنندگان مسیریاب‌ها، این روش را مرجح می‌دانند.

۵. مدیریت Password ها :

مناسب‌ترین محل برای ذخیره Password های عبور بر روی Server Authentication است. هرچند که در بسیاری از موارد لازم است که بسیاری از این رمزها بر روی خود سخت‌افزار نگاه داری شوند. در این صورت مهم‌ترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رمزها بر روی Router یا دیگر سخت‌افزارهای مشابه است.

ملزومات و مشکلات امنیتی ارائه دهندگان خدمات :

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه می‌دهند. به عبارت دیگر این شبکه‌های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه‌ی جهانی اینترنت کنونی را شکل می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

۱. قابلیت های امنیتی :

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود :

- ✓ قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

- ✓ وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند. از آنجاییکه شبکه‌های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، با استفاده از سیستم‌های IDS بر روی آنها، می‌توان به بالاترین بخت برای تشخیص حملات دست یافت.
- ✓ قابلیت تشخیص منبع حملات. با وجود آنکه راه‌هایی از قبیل سرقت آدرس و استفاده از سیستم‌های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار می‌نمایند، ولی استفاده از سیستم‌های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه‌ی مشکوک به وجود منبع اصلی می‌نماید. بیشترین تأثیر این مکانیزم زمانی است که حملاتی از نوع DoS از سوی نفوذگران انجام می‌گردد.

۲. مشکلات اعمال ملزومات امنیتی :

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست.

یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS است. خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو جریان از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و بسته‌های اطلاعاتی خواهد کاست. برای جبران این کاهش سرعت تنها می‌توان متوسل به تجهیزات گران‌تر و اعمال سیاست‌های امنیتی پیچیده‌تر شد.

با این وجود، با هرچه بیشتر حساس شدن ترافیک و جریان‌های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبکه‌های کوچکی که خود به شبکه‌های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه‌ها می‌توان داشت.