امنیت شبکه های کامپیوتری

امنیت شبکه های کامپیوتری از مهمترین مسائل مبتلا به شبکه های کامپیوتری است. مهمترین رکن برپائی یک شبکه پس از پیکربندی صحیح سخت افزاری مساله تضمین امنیت شبکه است. این مساله در محورهای زیر بررسی شده است:

کلیات امنیت شبکه کامپیوتری

امنیت شبکه های بدون سیم

آشنائی باFireWall

کلیات امنیت شبکه کامپیوتری

حفاظت، پشتیبانی و نگهداری از داده‌های رایانه‌ای، اطلاعات مهم، برنامه‌های حساس، نرم‌افزارهای مورد نیاز و یا هر آنچه که در حافظه جانبی رایانه مورد توجه بوده و با اهمیت می‌باشد، امنیت رایانه‌ای نامیده می‌شود. تفکر امنیت در شبکه برای دستیابی به سه عامل مهم است که با یک دیگر مثلث امنیتی را تشکیل می دهند. این عوامل عبارتند از راز داری و امانت داری (Confidentiality)، یکپارچگی (Integrity) و در نهایت در دسترس بودن همیشگی .(Availability) این سه عامل (CIA)اصول اساسی امنیت اطلاعات - در شبکه و یا بیرون آن - را تشکیل می دهند بگونه ای که تمامی تمهیدات لازمی که برای امنیت شبکه اتخاذ میشود و یا تجهیزاتی که ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است.

Confidentiality

به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گیرد که به آن نیاز دارند و اینگونه تعریف شده است. بعنوان مثال از دست دادن این خصیصه امنیتی معادل است با بیرون رفتن قسمتی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات.

Integrity

بیشتر مفهومی است که به علوم سیستمی باز می گردد و بطور خلاصه می توان آنرا اینگونه تعریف کرد:
-تغییرات در اطلاعات فقط باید توسط افراد یا پروسه های مشخص و مجاز انجام گیرد.
-تغییرات بدون اجازه و بدون دلیل حتی توسط افراد یا پروسه های مجاز نباید صورت بگیرد .
-یکپارچگی اطلاعات باید در درون و بیرون سیستم حفظ شود. به این معنی که یک داده مشخص چه در درون سیستم و چه در خارج آن باید یکسان باشد و اگر تغییر می کند باید همزمان درون و برون سیستم از آن آگاه شوند.

Availability

این پارامتر ضمانت می کند که یک سیستم - مثلا اطلاعاتی - همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مد نظر باشد اما عواملی باعث خوابیدن سیستم شوند - مانند قطع برق - از نظر یک سیستم امنیتی این سیستم ایمن نیست.

اما جدای از مسائل بالا مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می شوند برای خود شخصیت جداگانه ای پیدا کرده اند. در این میان می توان به مفاهیمی نظیر Identification به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authenticationبه معنی مشخص کردن هویت کاربر، Authorizationبه معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountabilityبه معنی قابلیت حسابرسی از عملکرد سیستم و ... اشاره کرد.

امنیت در یک شبکه به ۲ روش صورت می پذیرد. ۱- برنامه های نرم‌افزاری ۲- قطعه‌های سخت‌افزاری. در بهترین حالت از برنامه های نرم افزاری و قطعات سخت افزاری بطور همزمان استفاده می گردد. عموماً برنامه‌های نرم‌افزاری شامل برنامه‌های ضدمخرب (مخرب‌ها شامل ویروس، کرم‌های مهاجم، اسب‌های تراوا، مخفی‌شده‌ها و ....) و دیوار آتش می‌باشد. قطعات سخت‌افزاری نیز عموماً شامل دیوار آتش می‌شود. این قطعه‌ها موجب کنترل درگاه‌های ورودی و خروجی به رایانه و شناخت کامل از حمله‌کننده‌ها بخصوص نشانه‌های خاص مهاجم را ایجاد می نماید.

فراموش نکنیم که شرکت مایکروسافت به عنوان عرضه‌کننده سیستم های عامل نسل) Windows که در حال حاضر پرمصرف ترین گروه سیستم‌های عامل را تشکیل می دهد)، به یک برنامه نرم افزاری دیوار آتش بصورت پیش فرض مجهز می باشد، که می‌تواند تا امنیت را هر چند کم، برای کاربران سیستم‌های عامل خود فراهم نماید اما قطعاً این نرم افزار به تنهایی کفایت امن سازی رایانه را تأمین نمی نماید. اما در اولین مرحله امن سازی یک شبکه ابتدا باید سازمان را به یک برنامه ضدمخرب قوی مانندَ Antivir, Symantec, Kaspersky, Nod32, BitDefender, Norton, Panda، Macبا قابلیت بروزآوری مجهز نمود، تا بتواند در مقابل حمله برنامه های مخرب واکنش مناسبی ارائه نماید. برنامه Antivir می تواند یک انتخاب مناسب در این زمینه باشد. چرا که این برنامه قابلیت بروزآوری را بطور مداوم دارا می‌باشد و خود برنامه نیز هر ۶ ماه یکبار ویرایش می‌گردد تا از موتور جستجوگر قوی تر و بهینه‌تری برای یافتن برنامه های مخرب بهره گیرد. خرید نسخه اصلی این نرم‌افزار توصیه می‌گردد، چرا که در صورت بروز مشکل شرکت اصلی نسبت به پشتیبانی از رایانه‌های شما اقدام لازم را در اسرع وقت به انجام می‌رساند.

در مرحله دوم امن سازی یک شبکه باید از دستگاه تقسیم‌کننده استفاده نمود. دستگاه های فوق خود بر دومدل قابل تنظیم و پیکربندی و غیرقابل تنظیم و غیر قابل پیکربندی تقسیم می شوند. ممکن است در گروه اول نیز قطعاتی یافت شود که تنظیمات جزئی پیکربندی را انجام دهند اما بطور کامل و با تمامی امکاناتی که در گروه دوم قطعات دیده می شوند، مجهز نمی‌باشند. عموماً این دستگاه تقسیم کننده از مدل Core و برای ارتباط سرویس‌دهنده‌های مرکزی به یکدیگر و انجام خدمات به شبکه داخلی یا دنیای اینترنت تهیه می‌شود و در لایه اصلی تقسیم ارتباط شبکه، از طرف سرویس‌دهنده‌های مرکزی به سرویس گیرنده های داخلی و بالعکس قرار گیرد. این قطعه می تواند از تکثیر یک برنامه ضدمخرب و همچنین ورود و خروج مهاجمان پنهان، در درون شبکه داخلی از یک رایانه به رایانه دیگر تا حد بسیار زیادی جلوگیری نماید. اما اگر تعداد کاربران و سرویس‌گیرنده‌های یک سازمان بیش از تعداد درگاههای خروجی یک تقسیم‌کننده مرکزی Core Switch باشد، در این صورت از تقسیم کننده های دیگری که قابلیت پیکربندی را دارا بوده و مقرون به صرفه نیز می‌باشند، می‌توان استفاده نمود، تا کنترل ورودی و خروجی های هر طبقه یا واحد را بیمه نماییم. در مورد قطعات سخت افزاری تقسیم کننده Cisco Switch گزینه مناسبی می باشد که برترین نام جهانی را در این زمینه به خود اختصاص داده و با بروزآوری قطعات خود و همچنین آموزش متخصصان خود سهم بزرگی در این بحث ایفا می نماید.

در مرحله سوم امن سازی، نیاز به خرید برنامه نرم افزاری و یا قطعه سخت افزاری دیوار آتش احساس می شود. بیشترین تأکید بر روی قطعه سخت افزاری استوار است زیرا که از ثبات، قدرت بیشتر و ایرادات کمتری نسبت به نرم افزارهای مشابه خود برخوردار است. قطعه سخت‌افزاری دژ ایمن می بایست در مسیر ورودی اینترنت به یک سازمان قرار گیرد. دقیقاً همانجایی که اینترنت غیرامن به یک سازمان تزریق می گردد. پیشنهاد ما، قطعه سخت‌افزاری Cisco ASAو یا Astaro Firewall می باشد. فراموش نشود استفاده از دو دستگاه همزمان موازی قطعاً نیاز ارجح هر سازمان می باشد چرا که با ایست، و توقف سرویس‌دهی یکی از قطعه‌ها، دستگاه دیگر کنترل ورودی ها و خروجی ها را بدست می‌گیرد. اما در برنامه نرم‌افزاری نیاز به نصب نرم‌افزار بر روی یک سرویس‌دهنده مرکزی دیوار آتش بوده که ورود اینترنت ناامن تنها از مسیر این سرویس‌دهنده مرکزی انجام پذیرد. باید توجه داشت در صورت تهیه قطعه‌های سخت‌افزاری خاصی استفاده نمود تا در قبل و بعد از قطعه مسیریاب‌ها قرار گیرد که در این صورت بهتر است تا از قطعه های Cisco ASA در دیواره داخلی و بعد از قطعه مسیرباب‌ها استفاده نمود.

در مرحله چهارم امن سازی نیاز به وجود قطعه سخت‌افزاری دیگری به نام مسیریاب برای شبکه داخلی می‌باشد که ضمن قابلیت پیکربندی، برای نشان دادن مسیر ورودی ها و خروجی ها، اشتراک اینترنت، تنظیم ورودی ها و خروجی های دیوار آتشین، و همچنین خروج اطلاعات به شکل اینترنتی از سازمان به رایانه های شهری و یا بین شهری از طریق خطوط تلفن و ... استفاده نمود. پیشنهاد ما نیز محصولات شرکت معتبر Cisco میباشد.

در مرحله بعدی امن سازی یک سازمان نیاز به وجود دستگاه های تنظیم جریان برق و دستگاه های پشتیبان جریان برق اضطراری برای ارائه خدمات به صورت تمام وقت، بدون قطعی و تنظیم جریان برق، تمامی قطعه‌های سخت افزاری راهبر یک شبکه شامل تقسیم‌کننده‌ها، مسیریاب ها ، سرویس‌دهنده‌هامی باشد. این سیستم به دلیل ایجاد خطرات احتمالی ناشی از قطع جریان برق نظیر از بین رفتن اطلاعات در حال ثبت بر روی سرویس‌دهنده ها، تقسیم کننده ها، مسیریاب ها می‌باشد.

به عنوان آخرین مرحله امن سازی، تهیه از اطلاعات و فایلهای مورد نیاز به صورت پشتیبان از برنامه‌های اصلی نرم‌افزاری بر روی یک سرویس‌دهنده پشتیبان ، آخرین لایه امن سازی درون سازمانی را تکمیل می نماید.

راه کارهای افزایش امنیت سیستمها

-بررسی میزان امنیت مورد نیاز کامپیوترها با توجه به اطلاعات ذخیره شده روی آنها، محیطی که در آن قرار گرفته اند، موارد و روشهای استفاده از آنها

-بررسی تنظیمات موجود روی کامپیوترها و تشخیص آسیب پذیریها و سوراخهای امنیتی با استفاده از برنامه های جدید و حرفه ای

-انجام تنظیمات و نصب برنامه های لازم جهت ارتقای امنیت منطقی کامپیوترها پیاده سازی امنیت برای فایلها

-کنترل میزان دسترسی کاربران به فایلها بر اساس موارد زیر: الف- فقط خواندن ب- خواندن و ویرایش ج- خواندن، ویرایش و حذف د- خواندن، ویرایش، حذف و کنترل دسترسی دیگران

-ثبت دسترسی کاربران مورد نظر به فایلهای تعیین شده (برای مثال جهت تشخیص کاربری که فایلهای خاصی را ویرایش می کند) - پیاده سازی رمزگذاری فایلها (Encrypting File System) جهت جلوگیری از دسترسی کاربران دیگر (حتی مدیر شبکه) به آنها

دیواره آتشFirewall

دیواره آتش برای جدا کردن شبکه ها از همدیگر به کار می رود با استفاده از یک Firewall مناسب اهداف زیر محقق می گردد.

-1می توان سیاستها و سرویسهای ارائه شده در شبکه ها را از همدیگر بصورت مجرا نگهداری ، مدیریت و کنترل نمود.

-2انتخاب سرویس های داخلی ارائه شوند به بیرون از شبکه و یا بالعکس

- 3کنترل امنیت و مدیریت دسترسی های کاربران

-4حفاظت از اطلاعات در ماقبل کسانی که قصد نفوذ به شبکه داخلی را دارند.

دیوار آتش سیستمی است که در بین کاربران یک شبکه محلی و شبکه جهانی قرار می‌گیرد و ضمن نظارت بردسترسی‌ها در تمام سطوح ورود و خروج اطلاعات راتحت نظر دارد. در این ساختار هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات را کنترل‌کند موظف است تمام ارتباطات مستقیم شبکه داخلی خود را با دنیای خارج قطع کرده و هرگونه ارتباط خارجی از طریق یک دروازه که دیوارآتش یا فیلتر نام دارد انجام‌شود. بسته‌های TCP و IPقبل از ورود به شبکه یا خروج ازآن ابتدا وارد دیواره آتش می‌شوند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند.

منابع

http://www.icrc.ac.ir/content/view/185/201
http://www.ipnetsecurity.com/archives/000019.html
http://www.ircert.com/articles/Firewall.htm
Ict.bzmed.ac.ir