راهکارهای امنیت شبکه

سارا رئیسی وانانی
دانشجوی کارشناسی گروه مهندسی کامپیوتر (نرم افزار) دانشگاه پیام نور
sara1983_r@yahoo.com
اسماعیل رئیسی وانانی
کارشناس مدیریت بازرگانی دانشکده شهید علی فارسی، دانشگاه اصفهان

چکیده:

امروزه بحث امنیت شبکه یکی از موضوعات اساسی در دنیای امروز است و مورد توجه بسیاری از افرادی که در زمینه شبکه و رایانه فعالیت می کنند واقع شده است. هرروز که سپری می شود به تعداد کاربران شبکه افزوده می شود و همین امر ما را ملزم به یادگیری و اموزش در زمینه امنیت می کند.

در این مقاله پس از معرفی اجمالی امنیت شبکه و بررسی عوامل تهدید کننده علیه آن به ارائه راهکارهایی می پردازیم که تا حد قابل قبولی امنیت را برای ما فراهم کند هرچند که هیچ شبکه ای صددرصد امن نخواهد بود.

واژگان کلیدی: بدافزار، امنیت، تهدید، حمله

مقدمه

آلوده شدن سیستم های رایانه ای به بدافزارهایی همچون ویروس و کرم از جمله مسائلی است که تقریباً همه اقشار جامعه با آن آشنا هستند. اما آیا همه ما با پیامدهای آن ها آشنا هستیم؟

امروزه به علت گستردگی شبکه های رایانه ای، امنیت سیستم ها به شدت کاهش یافته است. ویروس هایی که هرروز و شاید هر ثانیه در حال ورود به شبکه گسترده اینترنت هستند و سیستم های کل جهان را با مخاطرات جبران ناپذیری تهدید می کنند.

با نگاهی منطقی می توان ادعا کرد که ویروس ها هرچند از وسعت انتشار و قدرت تخریب قابل توجهی برخوردار هستند، اما به هیچ وجه غیرقابل ردیابی و غیرقابل کنترل نخواهند بود. کافی است سیستم ها به نرم افزارهای امنیتی به روز و قدرتمند مجهز شوند.

البته در برخی از موارد علی رغم استفاده از نرم افزارهای امنیتی مجهز و به روز، ویروس ها بازهم راه نفوذی به درون شبکه ها پیدا می کنند به این دلیل که متأسفانه در بسیاری از شبکه های گسترده، همیشه یک

یا چند رایانه و یا تعدادی از سیستم های پردازش اطلاعات، به نحوی و به علتی خارج از شبکه محلی قرار می گیرند و از سیاست های امنیتی اعمال شده و محدودیت حفاظتی تعریف شده عبور می کنند.

مدل های متنوعی از شبکه توسط سازمان های گوناگون به دنیا عرضه شده اند که از آن جمله مدل OSI است که به مرور زمان به دلیل پیچیدگی های بیش از حد و حجیم و سنگین بودن و از همه مهمتر کند بودن آن جای خود را به مدل TCP/IP واگذار کرد که طرفداران بسیاری یافت. این مدل علیرغم محبوبیت دارای مشکلات بسیاری در زمینه امنیت می باشد که باید راهکارهایی برای جبران این ناامنی ارائه گردد.

۱. امنیت شبکه چیست؟[۴]

همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی)، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است.

امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله این مؤلفه ها بوده که نمی توان آن را مختص یک فرد و یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن

سازی شبکه های کامپیوتری بوده و می بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد.

یکی از مشکلات مدیران شبکه، زیان های مالی ناشی از عدم رعایت امنیت در شبکه ها به همراه حملات و تهدیدهای اینترنتی بوده است. براساس تحقیقات انجام شده خسارت های ناشی از نادیده گرفتن امنیت شبکه در سال ۲۰۰۹ تنها در آمریکا، ده ها میلیارد دلار تخمین زده شده است.

۲. اهمیت امنیت شبکه [۳]

برای کشور ما که بسیاری از نرم افزارهای پایه از قبیل سیستم عامل و نرم افزارهای کاربردی و اینترنتی، از طریق واسطه ها و شرکت های خارجی تهیه می شود، بیم نفوذ از طریق راه های مخفی وجود دارد. در آینده که بانک هاو بسیاری از نهادها و دستگاه های دیگر از طریق شبکه به فعالیت می پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه به صورت مسئله ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران ناپذیر خواهد بود.

نکته جالب اینکه بزرگترین شرکت تولید نرم افزارهای امنیت شبکه، شرکت چک پوینت است که شعبه اصلی آن در اسرائیل می باشد. مسأله امنیت شبکه برای کشورها، مسئله ای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژی های امنیت شبکه مجهز شود و از آنجایی که این تکنولوژی ها به صورت محصولات نرم افزاری قابل خریداری نیستند، پس می بایست محققین کشور این مهم را به دست بگیرند و در آن فعالیت نمایند.

۳. انواع امنیت [۲]

۱. امنیت فیزیکی: با توجه به اینکه هر گونه طرح امنیتی با وجود دسترسی فیزیکی، قابل شکستن است، درحوزه های زیر بررسی های کارشناسی لازم صورت گرفته و گزارشی برای برطرف نمودن آنها به مدیر شبکه ارائه می گردد:

- امنیت فیزیکی سرورها، سوئیچ ها، روترها و فایروال ها
- امنیت فیزیکی ایستگاه های کاری
- امنیت فیزیکی ارتباطات سیمی و بی سیم

۲. امنیت سرورها: در هر سازمان، سرور یا سرورهایی به منظور ارائه سرویس های مختلف به کاربران وجود دارد .بدین جهت باید با در نظر گرفتن تنظیمات امنیتی خاص مانع از ایجاد اخلال در فعالیت های مهم آنها شویم.

۳. امنیت ایستگاه های کاری: یکی از مهمترین دلایل بروز مشکلات امنیتی، کامپیوترهای کاربرانی است که بدون تنظیمات امنیتی لازم در شبکه مشغول به کار هستند، در نتیجه باید بر روی تمام ایستگاه های کاری تنظیمات امنیتی خاص اعمال شود و علاوه بر آن تنظیمات امنیتی نیز از طریق سرور بر روی این ایستگاه های کاری به صورت خودکار انجام گیرد.

۴. امنیت ارتباطات: نشت اطلاعات سازمانی از مهم ترین تهدیدات امنیتی است. در نتیجه باید با پیکربندی مناسب، تمام ارتباطات از جمله ارتباطات بی سیم سازمان امن شود و ارتباطاتی که بستر آن شبکه های نا امنی مانند اینترنت است، به صورت رمزنگاری با استفاده از پروتکل های امنیتی مانند IPSec ایمن سازی گردند .

۵. امنیت ساختار شبکه: در صورت اصلاح نشدن ساختار شبکه، همیشه مشکل ناامنی باقی می ماند. در نتیجه باید با ناحیه بندی مناسب، جداسازی نواحی مختلف مانند شبکه اینترنت، سرورها، ایستگاه های کاری و ... انجام پذیرد. برای جلوگیری از حملات و دسترسی های غیر مجاز، باید ترافیک عبوری بین این نواحی توسط فایروال ها کنترل گردد.

۶. مستندسازی خط مشی ها و دستورالعمل های امنیتی : مهمتر از ایجاد امنیت در شبکه سازمان، حفظ و تداوم امنیت می باشد. از این رو اطلاعاتی مانند نقشه های منطقی و فیزیکی شبکه، کابلکشی، پیکربندی تجهیزات و سیستم عامل ها، مستند خواهد شد. همچنین باید دستورالعمل هایی برای نگهداری و بازبینی تجهیزات و سرویسها و فعالیت های مرتبط با شبکه سازمان مانند پشتیبان گیری ارائه گردد.

۷.نظارت امنیتی. برای اطمینان از عملکرد صحیح سیستم، باید ابزار و آموزش لازم برای مدیر شبکه سازمان جهت اسکن و کنترل شبکه و بررسی و تحلیل log ها ارائه شود.

۸. آموزش و فرهنگ سازی: با توجه به نقش مهم پرسنل سازمان در حفظ امنیت شبکه و اطلاعات سازمان، آموزش های لازم برای ارتقاء سطح دانش فنی در مورد مسائل امنیتی، با برگزاری دوره های آموزشی در دوسطح راهبران و کاربران در سازمان انجام می گردد.

۴. تهدیدات امنیتی شبکه: [۷]

حملات به چهار دسته عمده تقسیم می شوند: فعال، غیرفعال، مخرب و غیر مخرب. رایج ترین حملات در شبکه در جدول زیر آورده شده اند

جدول ۱- انواع حملات

نام حمله	نوع حمله	محدوده استفاده	شرح حمله
جلوگیری از سرویس (DOS)	فعال	توسط کاربر داخلی و یا خارجی	کاربر نمی تواند از منابع و اطلاعات و ارتباطات استفاده کند
استراق سمع	غیرفعال	توسط کاربر داخلی و یا خارجی	مهاجم بدون اطلاع طرفین تبادل داده، به شنود پیام ها و اطلاعات می پردازد
تحلیل ترافیک	غیرفعال	اکثراً توسط کاربران خارجی	مهاجم ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب می کند
دستکاری پیام ها و داده ها	فعال	معمولاً توسط کاربران خارجی	مهاجم جامعیت و صحت اطلاعات را با تغییرات غیرمجاز بهم می زند
جعل هویت	فعال	توسط کاربران خارجی	مهاجم هویت یک فرد مجاز در شبکه را جعل می کند

۵. راهکارها امنیتی ارائه شده:

۵-۱ سرویس های امنیتی عبارتند از: [۲]

می توانیم بگوییم که، برقراری امنیت در حفظ و بقاء پنج اصل می باشد:

- ♣ محرمانگی: اطلاعات فقط و فقط بایستی توسط افراد مجاز قابل دسترس باشد.
- ♣ تمامیت: داده ها به درستی در مقصد دریافت شوند.
- ♣ احراز هویت: گیرنده از هویت فرستنده اگاه شود .
- ♣ دسترس پذیری: اطلاعات بایستی به هنگام نیاز، توسط افراد مجاز قابل دسترس باشد.
- ♣ عدم انکار: به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن را انکار کند.

۵-۲ مکانیزم های امنیتی [۲]

- رمزنگاری که در آن با استفاده از کلید خصوصی یا عمومی و با استفاده از الگوریتم های پیچیده، پیام به صورت رمز در آمده و در مقصد رمزگشایی می شود .
- امضای دیجیتال که برای احراز هویت به کار می رود .

5-۳ تجهیزات امنیتی شبکه: [۶]

- پیاده سازی امنیت در لایه های مختلف
- پیاده سازی راه حل های AntiVirus، AntI-Spam و Anti-Spyware
- پیاده سازی VPN در لایه های مختلف (IPSec VPN ، SSL VPN) (VPN ها برای اتصال دو شبکه یا شرکت های تجاری است که باید در برقراری ارتباط شبکه های ناامن مثل اینترنت عمومی، از طریق ایجاد یک لینک امن، به طور معمول بین دیوار آتش، با استفاده از یک نسخه پروتکل امنیتی IPSec استفاده خواهد شد. VPN ها برای استفاده در دسترسی از راه درو توصیه می شوند.)
- فایروال: در صورت دستیابی سایرین به سیستم شما، کامپیوتر شما دارای استعداد بمراتب بیشتری در مقابل انواع تهاجمات می باشد. شما می توانید با استفاده و نصب یک فایروال، محدودیت لازم در خصوص دستیابی به کامپیوتر و اطلاعات را فراهم نمائید.

فایروال ها حفاظت لازم در مقابل مهاجمان خارجی را ایجاد و یک لایه و یا پوسته حفاظتی پیرامون کامپیوتر و یا شبکه را در مقابل کدهای مخرب و یا ترافیک غیرضروری اینترنت، ارائه می نمایند. با بکارگیری فایروال ها، امکان بلاک نمودن داده از مکانی خاص فراهم می گردد. امکانات ارائه شده توسط یک فایروال برای کاربرانی که همواره به اینترنت متصل و از امکاناتی نظیر DSL و یا مودم های کابلی استفاده می نمایند، بسیار حیاتی و مهم می باشد.

فایروال ها به دو شکل سخت افزاری (خارجی) و نرم افزاری (داخلی)، ارائه می شوند

فایروال های سخت افزاری: این نوع از فایروال ها که به آنان فایروال های شبکه نیز گفته می شود، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط DSL قرار خواهند گرفت.

فایروال های نرم افزاری: برخی از سیستم های عامل دارای یک فایروال تعبیه شده درون خود می باشند. در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می باشد، پیشنهاد می گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن سازی کامپیوتر و اطلاعات، ایجاد گردد. (حتی اگر از یک فایروال خارجی یا سخت افزاری استفاده می نمائید). در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی باشد، می توان اقدام به تهیه یک فایروال نرم افزاری کرد.

- Web Filtering
- IDSها (سیستم تشخیص نفوذ) و IPSها (سیست های جلوگیری از نفوذ) مشابه سیستم های انتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS، مسئولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و به صورت خودکار ترافیک آسیب رسان را مسدود می کنند.
- پشتیبانی از کلیه پروتکل ها و فناوری های رایج
- مدیریت پهنای باند
- Vulnerability Scan : امکانات نرم افزاری است برای تشخیص آسیب پذیری شبکه
- Logserver & Analysis: امکاناتی است برای ثبت و کنترل رویدادها مورد استفاده قرار می گیرد.
- سرورهای AAA: برای احراز هویت، کنترل و نظارت بر دسترسی کاربران داخلی و خارجی استفاده می شوند.

۶. تست امنیت شبکه [۴]

روشی است جهت ارزیابی امنیت شبکه به کمک شبیه‌سازی حملاتی که توسط هکرها انجام میگیرد. که به یکی از دو روش زیر انجام می‌شود:

BlackBox: کارشناس از مکانی خارج از سازمان سعی در یافتن نقاط آسیب‌پذیر موجود در سازمان دارد.

WhiteBox: کارشناس با استفاده از شبکه سازمان و زیرساخت‌های آن و بازبینی کدها سعی در یافتن نقاط آسیب‌پذیر موجود در سازمان دارد.

انجام تست نفوذ شامل مراحل زیر می‌باشد:

- ✓ جمع آوری اطلاعات
- ✓ Finger printingو Foot printing
- ✓ ارزیابی شبکه
- ✓ پویش پورت‌ها و شناسایی سرویس‌ها
- ✓ جستجوی دستی و خودکار برای آسیب‌پذیری‌ها
- ✓ استفاده از آسیب‌پذیری‌ها
- ✓ دسترسی به سرویس‌ها و سیستم‌ها و ارتقاع دسترسی
- ✓ تهیه و تنظیم گزارش نهایی و ارایه آن

مدیران شبکه های کامپیوتری می بایست، به صورت ادواری اقدام به تست امنیتی تمام کامپیوترهای موجود در شبکه (سرویس گیرندگان ، سرویس دهندگان، سوئیچ ها، روتر ها، فایروال ها و سیستم های تشخیص مزاحمین) نمایند. تست امنیت شبکه، پس از اعمال هرگونه تغییر اساسی در پیکربندی شبکه ، نیز می بایست انجام شود

۷. الگوی امنیتی[۵]

۷-۱ معماری امنیتی

با توجه به ساختار هر شبکه، معماری امنیتی شبکه به صورت نهفته در لایه های شبکه در نظر گرفته می شود و لایه بندی با توجه به محدوده های داخلی، خارجی، ارتباط از راه دور و ... به صورت یک معماری امنیتی چهار لایه تعیین می گردد که عبارتند از:

۱- امنیت زیرساخت که شامل پیکربندی دقیق تجهیزات شبکه است.
۲- امنیت ارتباطات که در آن با استفاده از فایروال ها، سیستم های IPS ، IDS، ضد ویروس ها، سرورهای AAA، نرم افزارهای مانیتورینگ، ثبت و تحلیل رویدادها می توان به تشخیص هویت و کنترل کاربران پرداخت.
۳- امنیت سیستم ها که در آن با بهره گیری از پویشگرهای امنیتی، آنتی ویروس ها، IDS و IPS به ثبت و کنترل دسترسی کاربران به منابع پرداخته می شود.
۴- امنیت کاربردها که با بهره گیری از سیستم های IDS، آنتی ویروس، پویشگر امنیتی و فیلترهای محتوا بر دسترسی کاربران نظارت می شود.

7-۲ الگوریتم جهت تهیه الگوی امنیتی شبکه

با توجه به تنوع شبکه ها، استفاده از الگوریتم زیر در طرح الگوی امنیتی شبکه مفید است:

۱- شروع
۲- در صورتی که شبکه موجود است به مرحله ۱۰ بروید.
۳- نیازمندی های امنیتی را تعیین کنید.
۴- منابع را شناسایی کنید.
۵- مخاطرات مربوط به شبکه را تحلیل کنید.
۶- راهکارهای مقابله با مخاطرات را ارائه کنید.
۷- تجهیزات و امکانات امنیتی مناسب را تعیین نمایید.
۸- سیاست ها و رویه های امنیتی را تدوین کنید.
۹- سیاست ها و رویه های امنیتی را اجرا کنید.
۱۰- وضعیت موجود را بررسی کنید.
۱۱- در صورتی که نیازمندی های سازمان تأمین نشده است ، به مرحله ۳ بروید .

۱۲- در صورتی که نیازمندی های امنیتی شبکه تأمین نشده است به مرحله ۴ بروید.
۱۳- به مرحله ۱۰ بروید.

این الگوریتم پایان نمی یابد چراکه همیشه باید شبکه را از نظر امنیتی بررسی و کنترل کرد.

نتیجه گیری

موضوع امنیت در شبکه ها آن قدر مهم است که لازم باشد ضمن تأکید مداوم بر آن، هراز گاهی نگاهی دوباره به آن انداخت و با توجه به تحولاتی که در این حوزه روی می دهد، موضوع جدیدی درباره آن نوشت یا موضوعات قبلی را با رویکردهای جدید بازخوانی کرد.

از یک شبکه کامپیوتری، عوامل مهمی مانند نوع سیستم عامل، موجودیتها، منابع، برنامه های کاربردی، نوع خدمات و کاربران نقش مهم ومستقیمی در امنیت شبکه دارند. برقراری امنیت بصورت ۱۰۰٪ امکان پذیر نیست چرا که بعضی از عوامل از حیطه قوانین سیستمی خارج هستند، بعنوان نمونه کانالهای مخابراتی هدایت ناپذیر (مثل امواج مخابراتی و ارتباط ماهواره ای) یا کاربران شبکه (که همیشه از آموزشهای امنیتی داده شده استفاده نمی کنند.).

بنابراین الگوی امنیتی شبکه یک طرح امنیتی چند لایه و توزیع شده را پیشنهاد می کند، به نحوی که کلیه بخشهای شبکه اعم از تجهیزات، ارتباطات، اطلاعات و کاربران را در برمی گیرد. در الگوی امنیتی ضمن مشخص کردن سیاست امنیتی شبکه که در اصل در مورد اهداف امنیتی بحث می کند، راهکارهای مهندسی و پیاده سازی امنیت نیز ارئه می گردد و با آموزشهای مختلف امنیتی و نظارت مداوم ، امنیت شبکه بطور مداوم ارزیابی می گردد.

هکرها به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی امنیت – یعنی یک فایروال در ترکیب با یک آنتی ویروس – در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است. اما شما می توانید با برقرای امنیت شبکه با استفاده از رویکرد لایه بندی شده، دفاع مستحکمی ایجاد کنید. با نصب ابزارهای امنیتی در پنج سطح موجود در شبکه تان می توانید از داده های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید.

اما فراموش نکنید هیچ سیستمی صد در صد امن نخواهد بود.

اکنون نوبت آن رسیده که سطح اطلاعات خود را در مورد شبکه و امنیت آن بالا ببریم چراکه زندگی امروز وابسته به شبکه است. برای بالا بردن امنیت همه راه ها را در نظر داشته باشیم و از افراد خبره در این زمینه یاری جوییم. در محیط های مجازی به هیچ چیز اعتماد صد در صد نداشته باشیم.

اگر امنیت در شبکه ها نباشد دیگر کسی شهامت استفاده از اینترنت را نخواهد داشت و به مرور زمان این فناوری رو به نابودی خواهد رفت. پس باید تلاش کنیم امنیت را گسترش دهیم تا بتوانیم به راحتی و با خیالی آسوده با تمام نقاط جهان در ارتباط باشیم و از اخبار به روز سراسر دنیا مطلع شویم.

اگر استفاده از اینترنت در سطح جهانی فرهنگ سازی شود و به صورت بهینه بتوان از آن بهره گرفت شاید روزی فرا برسد که همه ما به این باور برسیم که همانگونه که تجاوز به منازل اشخاص کاری بس ناپسند است، تجاوز به اطلاعات شخصی افراد و تباه کردن آن ها نیز به همان میزان از اخلاق انسانی به دور است.

در ایران افراد نخبه و با استعداد فراوانی وجود دارد که شاید به علت کمبود امکانات در کشور و نداشتن پشتیبان و به امید پیشرفت مجبور به خروج از کشور می شوند و همین مسئله منجر به عقب افتادن ایران در رقابت علم در جهان شده است.

همانگونه که همه ما می دانیم ایران از نظر نرم افزارهای امنیتی به کشورهای بیگانه وابستگی زیادی دارد و اکنون که ما در تحریم به سر می بریم چگونه می توان امنیت شبکه های ایران را تأمین کرد؟ آیا اگر ایران مقداری از سرمایه خود را وقف نخبگان کند وضع به همین منوال باقی می ماند یا اینکه این کشور می تواند گوی سبقت را از رقبای خود بگیرد؟

اگر از متخصصان داخلی حمایت شود بسیاری از نرم افزارها در داخل به تولید خواهند رسید و نه تنها وابستگی ایران به اجانب از بین خواهد رفت بلکه امنیت بالاتری خواهیم داشت.

به امید روزی که ایرانی مستقل و آباد داشته باشیم.

قدردانی

با سپاس از استاد عزیز سرکار خانم زهرا جعفری که مارا در تهیه این مقاله یاری نمودند .

مراجع:

[1]روزگار، احمدرضا، سیستم های نظام بانکی و نوع پروتکل های ارتباطی

[2] میوالد،اریک، امنیت شبکه

[3] خرم آبادی، بدالصمد، کلاهبرداری رایانه ای از دیدگاه بین المللی

[4] اخوان پور، لی رضا، امنیت شبکه

[5] خالقی، محمود، سیستم های مدیریت امنیت اطلاعات

[6]Mastering Network Security, Chris Brenton

[7]Network Security fundamentals, Peter Norto