مطالعات علوم کاربردی در مهندسی
Online ISSN: ٢٤٧٦-٤٥٠٧
دوره ۳، شماره ۲، تابستان ۱۳۹۶
Print ISSN: ٢٥٣٨-٢٠٥٥
صفحات ۱۷۴- ۱۶۳
www.irijournals.com

مدیریت ریسک امنیتی در تجهیزات سخت افزاری

نجمی سالمی

دانشجوی دکتری، گروه کامپیوتر، دانشگاه آراد اسلامی واحد علوم و تحقیقات، تهران، ایران

چکیده

دنیای شگفت انگیز تکنولوژی در عصر فعلی فواید و تهدیدات خاص مربوط به خود را دارا است. تلاش متخصصین در عرصه آی تی بهره وری مفید توام با تهدیدات مستقیم و غیر مستقیم می باشد. سعی آنها در امان ماندن از تهدیدات موجود و بالا بردن ضریت امنیتی در سیستم ها است. آنها می دانند علاوه بر تمهیدات امنیتی در زمینه های نرم افزاری و سخت افزاری نقش عوامل انسانی نیز نقش بسزائی در حفظ اطلاعات و صحت آنها داراست. برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا فایروال و ...، با توجه به اینکه تجهیزات سخت افزاری متنوع می باشد. در این مقاله سعی بر آشنایی با یکسری از سیستم ها و ماژول های سخت افزاری و انواع ریسک ها در آنها و نحوه برخورد با این ریسک ها است. در این مقاله ما تنها به بررسی ماژول امنیتی سخت افزار[1]، دستگاه خودپرداز[2]، محدوده امنیتی[3] و مدیریت یکپارچه تهدید[4] خواهیم پرداخت.

واژه‌های کلیدی: ریسک، فایروال، دستکاری،HSM، ATM، DMZ، UTM .

[1] Hardwear security module
[2] Automated Teller Machine
[3] Demilitarized Zone
[4] Unified threat management

۱- مقدمه

با گسترش استفاده از شبکه و اینترنت در سازمانها و موسسات کوچک و بزرگ، تهدیدهای امنیتی نیز مسئله جدی شده و خطراتی را برای اطلاعات ذخیره شده یا انتقال آنها بوجود آورده است. با توجه به اینکه در سازمان های بزرگ سعی در رعایت اصول امنیتی شده به دلیل عدم آگاهی ها و دانش لازم در خصوص امنیت (دانش عمومی امنیت)، کاربران شبکه و استفاده کنندگان اطلاعات داده های حساس و مهم را همیشه بعنوان مهمترین تهدید امنیتی مطرح کرده اند. بسیاری از اطلاعات ارزشمند امروزه در دیسک های کامپیوتری و یا قابل حمل ذخیره و جابجا می شوند و مابقی آنها نیز بر روی شبکه انتقال پیدا می کنند. حال چگونه باید از این اطلاعات مهم نگهداری کرد. عوامل موثر در امنیت آنها چه چیزهائی هستند.

در یک سیستم کامپیوتری چهار عنصر نقش بسزائی دارند که عبارتند از:

- سخت افزارها که شامل حافظه های داخلی و خارجی، دستگاه های ورودی و خروجی و پردازشگر می باشد.

– نرم افزارها یا برنامه های کاربردی که شامل نرم افزارهای تجاری، بازرگانی، گرافیکی، بازیها و نرم افزارهای بانک اطلاعاتی و... می باشد که برنامه های فوق با استفاده از سخت افزار بکار گرفته می شوند و از منابع آن استفاده می کنند.

– کاربران که شامل انسان و یا دیگر سیستم ها به منظور انجام امور و رفع احتیاجاتی مانند محاسبات می باشند که در نهایت با بکارگیری نرم افزار و سخت افزار به این هدف دست می یابند.

– سیستم عامل که رابط بین نرم افزارو سخت افزار می باشد و نحوه بکارگیری منابع سخت افزاری برای نرم افزارها، کنترل و هدایت می نماید.

اهمیت امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد:

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

ب – برای جلوگیری از خطرهای DoS[1] 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.

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند.

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها 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 است.

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

در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطرهایی که از این طریق، تجهزات شبکه را تهدید می‌کنند توجه داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله‌ها می‌توان به راه حل‌ها و ترفندهای دفاعی در برار این‌گونه حملات پرداخت (الن[2]، ۲۰۰۱). از جمله، ازمحل‌های امن برای تجهیزات، انتخاب لایه کانال ارتباطی امن می توان استفاده کرد.

[1] Denial of Service

[2] Allen

دو راه اصلی برای کنترل تجهزات فعال وجود دارد: ۱ -کنترل از راه دور،۲ -کنترل از طریق درگاه کنسول در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استانداردها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در این مقاله ما در بخش ۲ به بررسی ماژول امنیت سخت افزار (HSM) خواهیم پرداخت. در بخش ۳ در رابطه با دستگاه خود پرداز (ATM)، در بخش ۴ به بررسی DMZپیاده سازی و نحوه عملکرد آن خواهیم پرداخت. در بخش ۵ UTM ها را مورد بررسی قرار می دهیم و در انتها در بخش ۶ به مقایسه و نتیجه گیری سیستم های مورد بررسی خواهیم پرداخت.

۲- ماژول امنیت سخت‌افزار (HSM)

با افزایش نیاز به امنیت در کاربردهای حساس، استفاده از سخت‌افزار امنیتی (HSM) جایگزین راه کارهای سنتی نرم‌افزاری برای امنیت می‌گردد .دستگاه امنی که قابلیت‌های رمزنگاری لازم برای امن‌کردن تراکنش‌ها در کاربردهای مالی را فراهم می‌آورد. کاربردهای اصلی این دستگاه در ساختن کلید و ذخیره امن، پردازش گواهی‌های امنیتی و مدیریت کلیدهای رمزنگاری PKIاست.

HSM می تواند تعدادی از توابع مهم مربوط به امنیت را انجام دهد. سرعت عملیات رمزنگاری مانند رمزنگاری، امضاهای دیجیتال، هش کردن و تایید کدهای پیام را فراهم می کند. پیام تایید کد (یا MAC) یک الگوریتم که ترکیب ریاضی یک کلید با یک رشته هش به ارائه یک "کد" که می توان به عنوان یک تکه از داده برای اطمینان از درستی آن اضافه کرد.

۲-۱ پیاده سازی های معمول برای یک HSM

استفاده های مختلف HSM از نظرعملکرد و امنیت، قیمت متفاوت دارند. به طور کلی HSMs برای استفاده های زیر اجرا می شود:

- ژنراتور کلیدی و تاسیسات ذخیره سازی کلید امن برای یک مرجع گواهی (بوند و کلایتن[1]، ۲۰۰۱).
- ابزار برای کمک به احراز هویت با تایید امضای دیجیتال
- یک شتاب دهنده برای ارتباطات SSL
- ابزار برای رمزنگاری ایمن اطلاعات حساس برای ذخیره سازی در یک محل نسبتا نا امن مانند یک پایگاه داده
- ابزار برای بررسی یکپارچگی داده های ذخیره شده در یک پایگاه داده
- ژنراتور کلید امن برای تولید کارت هوشمند

۲-۲ اهداف خدمات HSMs

در هسته یک زیرساخت امنیت داده ها مبتنی بر سخت افزار رمزگذاری است: فرایند که در آن داده های حساس ارائه می شود. کشف، از طریق استفاده از کلید های مخفی، به همه به جز دریافت کنندگان مجاز است. به همین ترتیب، رمزگشایی باید در داخل مرز HSM به منظور اطمینان از محرمانه بودن پیام و اصالت باشد. رمزگشایی فرایند تبدیل داده های رمزگذاری شده (متن رمزی) به متن قابل خواندن است.

کلیدهای سری نقش حیاتی در رمزنگاری و رمزگشایی داده ها بازی می کنند. ارزش آنها به طور تصادفی تولید واجازه می دهد که اطلاعات را به رمزگذاری و رمزگشایی شوند. در نتیجه، نگه داشتن کلید خصوصی برای امنیت شبکه ضروری می باشد.

[1] Bond & Clayton

دوره ۳، شماره ۲، تابستان ۱۳۹۶، صفحات ۱۷۴-۱۶۳

ماژول های امنیتی سخت افزار، تولید و ذخیره سازی کلید های مورد استفاده برای ارتباطات رمز شده بین دستگاه در یک دستگاه رمزنگاری امن (SCD) است. هنگامی که اطلاعات به HSM از طریق اتصال فرستاده میشوند، تراشه مخصوص HSM رمزگذاری یا رمزگشایی سریع آن اطلاعات با استفاده از کلید مناسب اجازه می دهد.

موارد استفاده از کسب و کار برای ماژول های امنیتی سخت افزار:

- آماده سازی داده ها EMV و کارت شخصی
- تحقق انطباق PCI و TR-39
- بارگذاری کلیدی از راه دور برای شبکه های ATM
- رمزگذاری نقطه به نقطه (P۲P) از اطلاعات دارنده کارت
- پیشگیری از تقلب اعتباری، بدهی و کارت پیش پرداخت
- محاسبه MAC برای اطمینان از یکپارچگی داده ها در حمل و نقل
- تبادل کلید پویا برای نقطه ای از فروش و ATM
- ترجمه و تاییدPIN
- هر لحظه تولید رمز عبور برای امنیت آنلاین

HSMبه طور کلی بخش ارزشمندی از راه حل های امنیتی باشد. با این حال، به تنهایی بی ارزش و بدون توجه به پایه های فرآیند امنیتی مناسب، مانند تجزیه و تحلیل دقیق خطر، طراحی، پیاده سازی، تست امنیت، آموزش کاربران، سیاست امنیتی، نصب و راه اندازی دقیق و مدیریت محصول می باشد.

مزایای کلی که HSM می تواند به عنوان راه حل امنیتی به ارمغان بیاورد افزایش امنیت برای ایجاد، ذخیره سازی و استفاده از کلید های رمزنگاری، سرعت عملکرد رمزنگاری و صنعت استاندارد پلت فرم سخت افزار که برای معماری یک راه حل امنیتی مناسب برای سازمان است. در جدول ۱ ریسک های بوجود آمده در امنیت سخت افزار HSM و اقدامات کاهشی در رابطه با این ریسک ها را می توان مشاهده کرد.

جدول ۱: ریسک ها بوجود آمده در امنیت سخت افزار HSM و اقدامات کاهشی در رابطه با این ریسک ها

اقدامات امنیتی کاهش ریسک HSM	توضیحات	نوع ریسک
-قابلیت‌های رمزنگاری - ساختن کلید و ذخیره امن -پردازش گواهی‌های امنیتی -مدیریت کلیدهای رمزنگاریPKI -پشتیبان گیری کلیدی		-سرقت
-فعالیت الکتریکی غیر عادی برای جلوگیری از فرد غیر مجاز	-"zerosize"ا (پاک کردن تمام داده های حساس)	-دستکاری
- یک ماژول نرم افزار رمز نگاری جدید جایگزین	-باید HSM قابلیت ارتقا را داشته باشد	-ضعف در معرض یک الگوریتم رمزنگاری

دوره ۳، شماره ۲، تابستان ۱۳۹۶، صفحات ۱۷۴-۱۶۳

۳- دستگاه ATM

اولین دستگاه مکانیکی پرداخت وجه نقد توسط لوتر جورج سیم جیان[1] ساخته و در سال ۱۹۳۹ در نیویورک توسط بانک نیویورک نصب گردید؛ اما پس از گذشت ۶ ماه به دلیل عدم استقبال مشتریان برداشته شد. از آن پس تاریخچه دستگاه خودپرداز به مدت ۲۵ سال متوقف شد تا زمانی که "دلارو" اولین دستگاه خودپرداز الکترونیکی را ساخت.

سیستم مدیریت ATM یک سیستم مرکزی که برنامه ریزی و اجرا به منظور مدیریت، نظارت و ثبت دستگاه های خودپرداز است. مسئولیت نظارت از دستگاه، تشخیص و حذف اشتباهات در کوتاه ترین زمان و کمترین قیمت به منظور افزایش کیفیت خدمات مالی از بانک ها و موسسات مالی و اعتباری واستفاده مناسب از دستگاه به طوری که آنها می توانند در هرساعتی فعال و به مشتریان پاسخگو باشند.

شبکه های ATM از بسیاری تهدیدات رنج می برند. آنهایی که معمول هستند استراق سمع، دستکاری، خدمات انکار، سرقت کانال مجازی و تجزیه و تحلیل ترافیک و غیره. توجه داشته باشید که سرقت و تجزیه و تحلیل ترافیک کانال مجازی تنها درشبکه های ATM رخ می دهد.

۳-۱ چارچوب امنیتی ATM

بر اساس تجزیه و تحلیل اهداف از طرف مشتری، سمت اپراتور و سمت جامعه عمومی، پیش نویس شناسایی اهداف امنیتی برای امنیت خودپرداز:

- محرمانگی
- یکپارچگی داده
- پاسخگویی
- در دسترس بودن

محرمانه بودن و یکپارچگی داده ها آشکار است. پاسخگویی به این معنی که تمام فراخوانی خدمات شبکه دستگاه خودپرداز و فعالیت های مدیریت شبکه پاسخگو باشد. هر نهاد باید پاسخگو اعمال آن باشد. پاسخگویی شامل هر دو احراز هویت و عدم انکار است. در دسترس بودن به معنی تمام نهادهای مشروع باید قادر به دسترسی به امکانات دستگاه خودپرداز درست باشد، هیچ انکار سرویس نباید اتفاق بیافتد. برای عملیات های تضمین کیفیت سرویس مهم است.

با توجه به این اهداف اصلی، پیشنهاد پیش نویس توابع اصلی که یک سیستم امنیتی دستگاه خودپرداز باید ارائه دهد:

- تأیید هویت: سیستم امنیتی باید قادر به ایجاد و تایید هویت ادعا از هر کاربردر شبکه دستگاه خودپرداز باشد.
- کنترل دسترسی و مجوز: کاربران نباید قادر به دسترسی به اطلاعات یا منابع اگر آن مجاز نیست.
- حفاظت از محرمانگی: ذخیره و برقراری ارتباط داده باید محرمانه باشد.
- حفاظت از یکپارچگی داده ها: سیستم های امنیتی باید یکپارچگی داده های ذخیره شده و برقراری ارتباط داده را تضمین کند.
- پاسخگویی قوی: یک موسسه نمی تواند مسئولیت اقدامات انجام و همچنین اثرات آنها را انکار کند.
- ورود به سیستم فعالیت: سیستم های امنیتی باید قابلیت بازیابی اطلاعات در مورد فعالیت های امنیتی در عناصر شبکه با امکان ردیابی این اطلاعات به افراد و یا اشخاص را حمایت کنند.
- گزارش هشدار: سیستم های امنیتی باید قادر به تولید اطلاع رسانی هشدار در مورد برخی از وقایع مربوط به امنیت قابل تنظیم و انتخابی باشند.
- حسابرسی: هنگامی که نقض امنیتی اتفاق می افتد، سیستم باید قادر به تجزیه و تحلیل داده های مربوط به امنیت سیستم وارد شود.

[1] Luther George Simjian

• بازیابی امنیتی: سیستم های امنیتی باید قادر بهبود یافتن از نقض یا اقدام به امنیت باشد.
• مدیریت امنیت: سیستم های امنیتی باید قادر به مدیریت سرویس های امنیتی به دست آمده از شرایط فوق باشد.

۳-۲ محدوده امنیت ATM

اصولا معماری دستگاه خودپرداز شامل سه سطح:

• سطح کاربر
• سطح کنترل
• سطح مدیریت

در نگاه اول، امنیت دستگاه خودپرداز نباید بیش از حد دشوار به پیاده سازی یک شیوه امنیتی در زمینه های دیگر باشد؛ اما، امنیت دستگاه خودپرداز با پیاده سازی بسیار دشوار است. سوئیچ دستگاه خودپرداز یک سلول مالتی پلکسر سرعت بالا و شبکه دستگاه خودپرداز یک شبکه اتصال گرا است. این خواص از مشکلات منحصر به فرد، تازمانی که ما سعی برای حفظ ارتباط دستگاه خودپرداز داریم.

اولین چالش در تامین امنیت شبکه های دستگاه خودپرداز پیدا کردن یک مکانیسم رمزنگاری برای مطابقت با سرعت بالا ارتباطات از یک سوئیچ است. رمزنگاری برای ارائه محرمانگی، احراز هویت و خدمات یکپارچگی برای سیستم های امنیتی استفاده می شود.

با این حال، یک مشکل برای اجرای این طرح در دستگاه خودپرداز که نیازمند رمزگذاری توانمند برای دسترسی به طیف وسیعی از اطلاعات کلیدی با سرعت بالا دارد (ریچارد[1]، ۱۹۹۵). همچنین رمزگذاری می تواند از کلید جلسه به صورت پویا و اعمال به سلول بعدی به سرعت انجام شود. این نیاز، به نام مهارت کلیدی، غیر بدیهی است. همانطور که ذکر شد، برخی الگوریتم رمزنگاری نیازمند زمان طولانی برای رمزگذاری تغییرات کلیدی است. حتی، با توجه به تعداد زیادی از کانال های مجازی بالقوه، دنبال کلید در جدول کلید بزرگ سربار زمان که می تواند در مسیر بحرانی شود بنابراین می تواند تنگنا از سیستم معرفی کرد.

از جمله مشکلات دستگاهای ATM، دستکاری[2] است. دستکاری ATM به شدت رشد کرده و سارقان باعث بهبود تکنیک دستکاری هستند. درواقع با ارزش ترین دارایی های موسسات مالی مشتری ها هستند. دستکاری اعتماد مشتری را که جنبه های سود آور از کسب و کار دستگاه خودپرداز از بین می برد. در نهایت دستکاری باعث ضعیف شدن مارک ها و بی اعتباری شهرت می شود. اسکیمینگ روش مورد استفاده توسط جنایتکاران برای کپی کردن اطلاعات شخصی از نوار مغناطیسی بر روی یک کارت دستگاه خودپرداز است.

جنایتکاربا نصب یک دستگاه دستکاری شده در بالای اسلات کارت حافظه از دستگاه خودپرداز، به عنوان مثال پوشش کارت خوان، جلو یا قبل از آن است. هنگامی که کاربر کارت خود را وارد کارت خوان، دستگاه دستکاری جزئیات کارت را از نوار مغناطیسی بر روی کارت خوانده و آنها را به یک گیرنده با سیم یا بی سیم متصل انتقال خواهد داد.

راه حل:

راه حل های ضد دستکاری دستگاه ATM:

- مکانیسم ضد دستکاری مکانیکی[3]: شامل قطعات پلاستیکی که در شکاف کارت خوان نصب شده است. با اشکال خاص طراحی شده، برای جلوگیری از دستکاری از طریق مکانیسم های دستکاری است. مکانیسم ضد دستکاری با تکنولوژی های امنیتی دستگاه از خدمات درج شده یا نابودی دستگاه توسط نیروی مجهز حذف می کند.

[1] Richard
[2] Skimming
[3] **The** mechanical **anti-skimming mechanism**

- دستگاه ضد دستکاری هوشمند[1]:نظارت بر محیط کل اسلات کارت حافظه برای مکانیسم نفوذ غیر قانونی نصب شده است. این ماژول امنیتی در دستگاه خودپرداز نصب شده و از خارج قابل رویت نیست. دستگاه قادربه تشخیص مزاحم آنالوگ و حملات دستکاری دیجیتال است.

برخی از محصولات امنیت دستگاه خودپرداز در حال حاضر وجود دارد. بسیاری از آنها در مورد رمز نگاری می باشد. به عنوان مثال، GTE یک محصول به نام InfoGuard ۱۰۰ فراهم می کند که تحویل امن از سلول های دستگاه خودپرداز بیش از شبکه های دستگاه خودپرداز محلی و گسترده معرفی می کند. یک محصول از GATE که به نام رمزگذاری از Fastlane که ادعا به ارائه سرعت بالا، شفاف، تاخیر کم سرویس های امنیتی برای برنامه های کاربردی چند رسانه ای در سراسر هر دو شبکه های دستگاه خود پرداز محلی و گسترده است. فن آوری های شبکه با ارائه سیستم رمزگذاری کلیدی به نام CellCase که می تواند حداقل ۳۵ تماس در هر ثانیه را اداره کند. سیستم شبکه پیاده سازی یک سیستم فایروال دستگاه خودپرداز را ادعا می کند. اگر چه این پیاده سازی بسیار کوچک در مقایسه با تصویر بزرگ از امنیت دستگاه های خودپرداز است. تجربه برای پیاده سازی امنیت در شبکه های دستگاه خودپرداز را فراهم می کند.

جدول ۲ : ریسک ها بوجود آمده در امنیت سخت افزار ATM و اقدامات کاهشی در رابطه با این ریسک ها

نوع ریسک	توضیحات	اقدامات امنیتی کاهش ریسک ATM
سرقت	-تشخیص حملات -تغییرات سلول های سوئیچ	-کنترل دسترسی -مکانیسم ضد دستکاری -بوجود آوردن چند سطح امنیتی ATM
استراق سمع	فناوری ارتباطات و پروتکل های مربوطه عامل در نقطه ضربه زدن	-فناوری به روز تر
سرقت از کانال مجازی	تغییرات سلول های سوئیچ-	-سیاست های کنترل دسترسی
دستکاری	-دستگاه قادر به تشخیص حملات دستکاری -هشدار از طریق آلارم	-مکانیسم ضد دستکاری مکانیکی -دستگاه ضد دستکاری هوشمند

۴- محدوده امنیتی (DMZ)

اصطلاح علم DMZ توسط همکاران در وزارت ESnet در سال ۲۰۱۰ ابداع شد (دارت و همکاران[2]، ۲۰۱۱). تعدادی از دانشگاهها و آزمایشگاههای در حال گسترش علوم DMZ مستقر کرده اند. در سال ۲۰۱۲ بنیاد ملی علوم با ایجاد بهبود علوم DMZs در چند دانشگاه در ایالات متحده تامین شد.

مفهوم DMZ به عنوان یک منطقه محافظت شده فایروال غالبا شرکت دربخش جوامع کاربران به دلایل امنیتی استفاده می شود. در امنیت کامپیوتر، DMZ یا منطقه غیرنظامی (گاهی اوقات به عنوان یک محیط شبکه نامیده می شود) زیرشبکه فیزیکی یا منطقی در معرض خدمات خارجی یک سازمان به یک شبکه بزرگتر و غیر قابل اطمینان، معمولا اینترنت است. هدف از DMZ برای اضافه کردن یک لایه اضافی امنیتی به شبکه محلی سازمان (LAN) است. گره های خارجی شبکه فقط دسترسی مستقیم به تجهیزات در DMZ، به جای هر بخش دیگری از شبکه می باشد.

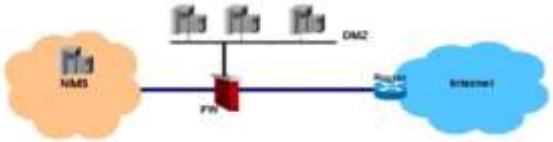
[1] **The** intelligent **anti-skimming device**

[2] Dart et al.

دوره ۳، شماره ۲، تابستان ۱۳۹۶، صفحات ۱۷۴-۱۶۳

۴-۱ طراحی یک DMZ

یک DMZ امنیت شبکه را تا حد زیادی افزایش می دهد. هر شبکه با سرور وب و حتی یک دستگاه دیگر می تواند از یک DMZ بهره مند شود. یک DMZ برای یک سیستم که حاوی اطلاعات ارزشمندی یا خصوصی مفید است. با اضافه کردن یک لایه اضافی از حفاظت به یک ماشین که می توان از یک DMZ بهره مند شد. DMZ، با پیکربندی درست به سرعت امنیت هر شبکه را افزایش می دهد. یک نمونه از DMZ در شکل ۲ نشان داده شده است.



شکل ۱: مثالی از طراحی یک DMZ در یک شبکه

شما می توانید یک فایروال یا دو تا فایروال را در یک DMZ استفاده کنید. این فقط یک نمونه برای نشان دادن این نکته که با استفاده از دو فایروال پیکربندی امن تر است. دو فایروال، شبکه های خارجی و داخلی از هم جدا است. با استفاده از دو فایروال، شما نیاز به یکی در مقابل و یکی در پشت DMZ دارید. یکی مقابل DMZ، باید بین شبکه های خارجی (اینترنت) و DMZ باشد. فایروالدیگر باید بین DMZ و شبکه داخلی به عنوان نمودار نشان می دهد.

شکل ۲ :چگونگی فایروال ها در طراحی

بعضی از چیزهایی که به نظر در هنگام تصمیم گیری یک DMZ برای شما مناسب عبارتند از:

- قیمت سخت افزار و نرم افزار از دستگاه اضافی مورد نیاز برای پیاده سازی یک DMZ
- کاهش اندکی در عملکرد
- هزینه برای زمان اجرای DMZ
- هزینه از کار افتادگی سیستم از اضافه کردن در DMZ
- سطح کاهش دسترسی به یک مهاجم

قیمت نرم افزار و سخت افزار اضافی برای اجرای یک DMZ کمتر، در مقایسه با هزینه اگر شبکه داخلی موفق به خطر افتاده است. یک DMZ امنیت شبکه را تا حد زیادی افزایش می دهد.

جدول ۳: ریسک ها بوجود آمده در امنیت سخت افزار DMZ و اقدامات کاهشی در رابطه با این ریسک ها

اقدامات امنیتی کاهش ریسک DMZ	توضیحات	نوع ریسک
-ایجاد لایه امنیتی بیشتراز طریق DMZ	-از طریق استانداردهای امنیتی	-جاسوسی شرکت های بزرگ
-فایروال	-از طریق استانداردهای امنیتی	-هک کامپیوتر

۵- مدیریت یکپارچه تهدید (UTM)

امنیت داده ها و دسترسی های غیر مجاز نگرانی های کسب و کاربرای شرکت های امروز تبدیل شده اند. به این دلیل که سوء قصد و از دست دادن اطلاعات محرمانه می تواند به زیان های مالی بزرگ و نیزبدهی های قانونی مربوطه منجر شود. لازم به ذکر در حال حاضربه رسمیت شناختن این واقعیت که جهل کاربرمنجرمی شود امنیت خارج از شبکه داخلی خود را به خطر بیافتد (الن، ۲۰۰۱).

مدیریت یکپارچه تهدید (UTM)[1] یا مدیریت امنیت یکپارچه (UTM)، یک راه حل در صنعت امنیت شبکه، از سال ۲۰۰۴ به عنوان یک راه حل دفاع دروازه شبکه اولیه برای سازمان بود. یک تئوری، UTM تکامل فایروال سنتی به یک محصول امنیتی فراگیر که قادر به انجام وظایف امنیتی متعدد در داخل یک سیستم واحد: فایروال شبکه، پیشگیری از نفوذ شبکه و آنتی ویروس دروازه (AV)، دروازه آنتی اسپم، VPN، فیلترینگ محتوا، تعادل بار، جلوگیری از نشت داده ها بر روی دستگاه است. مدیریت یکپارچه تهدید (UTM) یک رویکرد برای مدیریت امنیت که اجازه می دهد تا یک مدیر برای نظارت و مدیریت طیف گسترده ای از برنامه های کاربردی مربوط به امنیت و اجزای زیرساخت از طریق یک کنسول مدیریت واحد است.

جنبه های مهم انتخاب یک دستگاه UTM به حداقل رساندن خطرات در داخل سازمان را پوشش خواهد داد:

- ویژگی های بحرانی: طیف گسترده ای از ویژگی های ممکن، شما می توانید با انتخاب ویژگی های مورد نیاز به آدرس و پیدا کردن هر دستگاه که گم شده است.

- معیارهای انتخاب: مشخصات فنی می تواند بسیاری از مشکلات را حل کند. این معیارها به انتخاب راحت ترین دستگاه UTM برای نیازهای شما کمک خواهد کرد.

- طرح آزمون: ویژگی های مورد نیاز توسط شرکت باید تست شود و ثابت کند در صورتی که دستگاه واقعا قادر به برآوردن نیازهای شرکت می باشد.

- از جمله ویژگی های مهم برای یک دستگاه UTM: ظرفیت مناسب شبکه، به روز رسانی مکرر، سطح پشتیبانی، افزونگی قدرت، در دسترس بودن بالا، حالت شکست IPS، هشدار / شواهد قانونی، ادغام با معماری شبکه، قابلیت بازرسی، مدل تشخیص IPS، ویژگی های منحصر به فرد، امضا اشاره کرد.

از مزایای کلیدی UTM، کاهش پیچیدگی، سادگی: اجتناب از نصب نرم افزار های متعدد و نگهداری، مدیریت آسان: رابط کاربری گرافیکی مبتنی بر وب برای مدیریت آسان، کاهش نیاز به آموزش های فنی، پیروی از مقررات است.

از معایب کلیدی UTM، تنها نقطه شکست برای ترافیک شبکه، مگر اینکه HA[2] استفاده می شود، تنها نقطه سازش اگر UTM دارای آسیب پذیری، تاثیر بالقوه بر زمان نهفتگی و پهنای باند زمانی که UTM نمی تواند با ترافیک نگه دارید

جدول ۴:ریسک ها بوجود آمده در امنیت سخت افزار UTM و اقدامات کاهشی در رابطه با این ریسک ها

اقدامات امنیتی کاهش ریسک UTM	توضیحات	نوع ریسک
-استفاده از دستگاه یکپارچه امنیتی UTM	-با استفاده از فایروال شبکه، پیشگیری از نفوذ شبکه و آنتی ویروس دروازه (AV)، دروازه آنتی اسپم، VPN، فیلترینگ محتوا،	از دست دادن اطلاعات در شبکه
-استفاده از دستگاه یکپارچه امنیتی UTM		

[1] Unified threat management

[2] High availability

۶- نتیجه گیری

در مسائل مختلف امنیت نقش موثری را ایفاء می کند. هر تکنولوژی دارای یک سری ریسک ها وچالش هاست. هیچ تکنولوژی تضمینی برای از بین بردن این ریسک ها وجود ندارد. ولی می توان اقداماتی را برای کاهش این ریسک ها انجام داد. با توجه به بررسی های انجام شده به مقایسه و نتیجه گیری کلی سیستم ها و ماژول ها می پردازیم.

HSM به طور کلی بخش ارزشمند از راه حل های امنیتی است. با این حال، به تنهایی بی ارزش و توجه مناسب به پایه های فرآیند امنیتی مناسب، مانند تجزیه و تحلیل دقیق خطر، طراحی، پیاده سازی، تست امنیت، آموزش کاربران، سیاست امنیتی، نصب و راه اندازی دقیق و مدیریت محصول می باشد. HSM یک راه حل افزایش امنیت، ذخیره سازی و استفاده از کلید های رمزنگاری، سرعت عملکرد رمزنگاری و یک صنعت استاندارد سخت افزار برای معماری امنیت مناسب برای سازمان شما است.

فن آوری ATM شاید پیچیده ترین تکنولوژی شبکه تا کنون است. در حال حاضر مردم فقط شروع به بحث در مورد برخی مسائل مربوط به امنیت ATM می کنند. چرا که هدف از دستگاه خودپرداز ارائه یکپارچه شبکه و زیرساخت های ارتباطی، امنیت دستگاه خودپرداز، به عنوان بخشی از این زیرساخت ها، باید انعطاف پذیر و سازگار با فن آوری های دیگر باشد؛ که امنیت ATM سخت تر خواهد شد.

یک DMZ امنیت شبکه را تا حد زیادی افزایش می دهد. هر شبکه با وب سرور و حتی یک دستگاه دیگرمی تواند از یک DMZ بهره مند شوند. یک DMZ نه تنها برای یک سیستم که حاوی اطلاعات ارزشمندی یا خصوصی مفید است. بلکه با اضافه کردن یک لایه اضافی از حفاظت به یک دستگاه می توانید از یک DMZ بهره مند شوید. DMZ، اگر به درستی پیکربندی شود به سرعت باعث افزایش امنیت هر شبکه می شود. برای یک مهاجم رسیدن به مصالحه ازهر چیز با ارزش است. این تا حد زیادی مهارت های مورد نیاز یک هکر خارجی به سازش شبکه داخلی را افزایش می دهد و در نتیجه باعث کاهش خطر در شبکه داخلی می شود. البته، اصل دفاع در عمق، یادگیری و تمرین، اما یک DMZ افزایش قابل توجهی در امنیت را فراهم می کند.

با توجه به توضیحات داده شده در رابطه با فایروال ها و DMZ وتوضیحاتی که در رابطه با دستگاه UTM داده شده است اگر بتوانیم ترکیب DMZو UTM را با هم داشته باشیم امنیت بیشتری را می توانیم فراهم کنیم. در کل نمی توان گفت کدام سخت افزار امنیتی از تولیدات شرکت های موجود بهتر است بلکه در وهله اول باید سیستم و شرایط موجود را سنجید و نهایتا تمهیدات لازم برای سخت افزار امنیتی را فراهم کرد.

منابع

1. Eli Dart, Brian Tierney, Eric Pouyoul, Joe Breen (January 2012). "Achieving the Science DMZ". Retrieved 2015-12-31.
2. Dan Goodin (June 26, 2012). "Scientists experience life outside the firewall with "Science DMZs."". Retrieved 2013-05-12.
3. pmoyer (Dec 13, 2012). "Research & Education Network (REN) Architecture: Science-DMZ". Retrieved 2013-05-12.
4. Young, Scott, "Designing a DMZ". SANS Institute. p. 2. Retrieved 11 December 2015.
5. Allen, Julia. “The CERT Guide to System and Network Security Practices” Addison Wesley. 2001
6. Bond, M., Clayton, R.; “Extracting a 3DES key from an IBM 4758”; November 2001; University of Cambridge Computer Laboratory web site URL: http://www.cl.cam.ac.uk/~rnc1/descrack/index.html
7. Dart, Eli; Metzger, Joe (June 13, 2011). "The Science DMZ". CERN LHCOPN/LHCONE workshop. Retrieved 2013-05-26.

8. J. Kimmins and B. Booth: "Security for ATM networks"; Computer Security Journal; XII(1):21-29; 1996
9. L. Hanson, "The Impact of ATM on Security in Data Network", Proc. of Compsec International 1995, Conf. 12, pp 318-324.
10. Maryline Laurent, Olivier Paul, Pierre Rolin," Securing communications over ATM networks", IFIPSEC'97, Copenhagen, Denmark, May 1997
11. R. Deng et al: "Securing Data Transfer in Asynchronous Transfer Mode Networks"; Proceedings of GLOBECOM'95, Singapore, November 13-17, 1995, pp. 1198-1202
12. Richard Taylor, Greg Findlow, Asynchronous Transfer Mode: Security Issues, Proc. Aus tralian Telecommunication Networks and Applications Conference;pp. 161-166, 5-7 Dec. 1995; pp. 161-166 .
13. Shaw-Cheng Chuang: "Securing {ATM} Networks",3rd {ACM} Conference on Computer and Communications Security, New Delhi, India, 1996, pp.19-30 .

مطالعات علوم کاربردی در مهندسی

دوره ۳، شماره ۲، تابستان ۱۳۹۶، صفحات ۱۷۴-۱۶۳

Security Risks Management in Hardware

Najmi Salemi

Ph.D. Student, Computer Faculty, Islamic Azad University, Science and Research Branch, Tehran, Iran

Abstract

The amazing world of technology in the present age has its own specific benefits and threats. Experts' efforts in the field of IT are a useful tool for dealing with direct and indirect threats. They try to stay safe from existing threats and increase security in systems. They know that in addition to security measures in hardware and software, the role of human factors is also crucial in maintaining information and accuracy. To ensure security on a network, one of the most critical steps is to provide security of access and control of network equipment. Equipment such as routers, switches or firewalls, etc., due to the variety of hardware equipment. In this study, we will try to introduce a number of hardware systems and modules and types of risks in them and how to deal with these risks. In this study, we will only address Hardware security module, Automated Teller Machine, Demilitarized Zone and Unified threat management.

Keywords: Risk, Firewall, Manipulation, HSM, ATM, DMZ, UTM