به نام یگانه خالق بی همتا

موضوع سمینار : بررسی راهکارهای پیاده‌سازی امنیت در شبکه‌های کامپیوتری

ارائه دهنده : علیرضا اهری لاحق

کارشناس اداره کل مهندسی ارتباطات شرکت داده پردازی ایران
استاد دانشگاه علمی کاربردی داده پردازی ایران
سرپرست بخش شبکه انجمن انفورماتیک ایران

رئوس مطالب :

۱- استراتژی های طراحی و پیاده سازی امنیت

۲- انواع حملات و نفوذها و تهدیدهای امنیتی شبکه

۳- اصول طراحی امنیتی شبکه

۴- سیاستهای کلی جهت پیاده سازی امنیت اطلاعات

۵- نتیجه گیری کلی و پرسش و پاسخ

۱- استراتژی های طراحی و پیاده سازی امنیت :

- امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری در سطح کلان و از دیدگاه منافع ملی و استراتژیک

- پرداختن به موضوعات امنیتی ، در تمام سطوح سازمانی

- وجود زیرساختهای قوی اطلاعاتی و ایجاد اعتماد و اطمینان در تراکنشهای اطلاعاتی با در نظر گرفتن ساختار و مکانیزمهای امنیتی در شبکه های کامپیوتری .

- استفاده از استانداردهای موجود ملی و بین المللی به عنوان استانداردهای سیستم مدیریت امنیت اطلاعات (ISMS)، به طور مثال استاندارد ISO 17799 ، ISO 27002 و BS (British Standard)7799

- در نظر گرفتن فاکتورهای امنیتی شامل : محرمانگی (Confidentiality) ، یکپارچگی (Integrity) و در دسترس بودن (Availability)

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.

1- تجهیزات شبکه مانند روترها، سوئیچ ها و فایروالها

2- اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره شده اند.

3- منابع نامحسوس شبکه مانند پهنای باند و سرعت

4- اطلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه های داده و سرورهای اطلاعاتی

5- ترمینالهایی که برای استفاده از منابع مختلف به شبکه متصل می شوند.

6- اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

7- خصوصی نگهداشتن عملیات کاربران و استفاده آنها از منابع شبکه جهت جلوگیری از شناسایی کاربران.

مجموعه فوق به عنوان دارایی های یک شبکه قلمداد می شود.

۲- انواع حملات و نفوذها و تهدیدهای امنیتی شبکه

حمله تلاشی خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرار گیرد که مورد نظر نبوده است.

حملات شبکه را به چهار دسته عمومی تقسیم کنیم :

۱- دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه (Access Attacks)

۲- دستکاری غیرمجاز اطلاعات بر روی یک شبکه (Modification Attacks)

۳- حملاتی که منجر به اختلال در ارائه سرویس Denial of Service (DOS)

۴- حمله به منظور انکار و جعل هویت (Repudiation Attacks)

همچنین سایر تهدیدهای شبکه را میتوان در حالتهای مختلف زیر بیان کرد .

ویروس‌ها :

- ویروس‌ها، برنامه‌های کامپیوتری که توسط برنامه نویسان گمراه و در عین حال ماهر طراحی شده اند.
- ماکرو ویروس ، ویروسهایی که خود را به فایل‌هائی شامل دستورالعمل‌های ماکرو ملحق نموده و در ادامه، همزمان با فعال شدن ماکرو، شرایط لازم به منظور اجرای آنان نیز فراهم می‌گردد.
- برخی از ویروس‌ها بی‌آزار بوده و صرفا" باعث بروز اختلالات موقت در روند انجام عملیات در کامپیوتر می شوند (نظیر نمایش یک پیام مضحک بر روی صفحه نمایشگر همزمان با فشردن یک کلید خاص توسط کاربر).
- برخی دیگر از ویروس ها دارای عملکردی مخرب تر بوده و می توانند مسائل و مشکلات بیشتری نظیر حذف فایل ها و یا کاهش سرعت سیستم را به دنبال داشته باشند.

برنامه های اسب تروا (دشمنانی در لباس دوست) :

- برنامه‌های اسب تروا و یا Trojans ، به منزله ابزارهائی برای توزیع کدهای مخرب می باشند.

- تروجان ها ، قادر به حذف فایل‌ها، ارسال یک نسخه از خود به لیست آدرس‌های پست الکترونیکی، می باشند.

- این نوع از برنامه ها صرفا" می توانند از طریق تکثیر برنامه های اسب تروا به یک کامپیوتر، دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی، اقدام به آلودگی یک سیستم نمایند.

کرم های شبکه (Worms)

- نوعی از نرم افزارها که در اتصالات شبکه - مثلا" کامپیوتر - مستقر شده و می تواند علاوه بر زندگی و آسیب رساندن به آن اتصال، نسخه دیگری از خود را از طریق شبکه به سایر گره ها منتقل کنند .

- سرعت تولید مثل و انتشار یک کرم در شبکه بزرگ بسیار زیان بار میباشد و ترافیک زائد در سطح شبکه برقرار میسازد .

- در سطح شبکه های WAN این ترافیک زائد بسیار دردسر سازتر نسبت به شبکه های LAN میباشد .

جاسوسها (Spy Ware) :

- نرم افزاری که اقدام به جمع آوری اطلاعات شخصی بدون آگاهی و یا اجازه کاربران

- اطلاعات جمع آوری شده شامل لیست سایت های مشاهده شده توسط کاربر و یا اطلاعات به مراتب حساس تری نظیر نام و رمز عبور

- به این نوع برنامه ها ad ware نیز گفته می شود. نرم افزارهای فوق پس از نصب بر روی کامپیوتر، قادر به ارسال آگهی های تجاری pop-up، هدایت مرورگر به وب سایت هایی خاص، ارسال لیست سایت های مشاهده شده توسط کاربر و یا مانیتورینگ عملکرد کاربران در زمان اتصال به اینترنت می باشند .

۳- اصول طراحی امنیتی شبکه :

- بر اساس نیاز سنجی که در هر پروژه بر اساس هزینه ها ، تعداد کاربران ، پهنای باند و سرعت شبکه ، دسترسی کاربران به قسمتهای مختلف شبکه و ارتباط با اینترنت در نظر گرفته میشود .

فازهای اجرای کار به صورت زیر است :

۱- فاز شناسایی نیازمندیها

۲- فاز طراحی

۳- فاز آزمایش

۴- فاز اجرا و پیاده سازی

۵- فاز بررسی نتایج و عملکرد

۴ - سیاستهای امنیتی اطلاعات :

- سیاستهایی که توسط مدیران شبکه جهت بالا بردن ضریب امنیتی سازمان اتخاذ میشود .
- تفاوتهای ساختاری در پیاده سازی سیاستهای امنیتی در سازمانهای مختلف
- تناسب سیاستهای امنیتی اطلاعات سازمان با سایر سیاستهای امنیتی سازمانی
- استفاده از متخصصین در امر طراحی و پیاده سازی سیاستهای امنیتی اطلاعات
- عدم پیچیده کردن بیش از حد سیاستهای امنیتی اطلاعات در سازمان
- استفاده از استانداردهای موجود در امر طراحی و پیاده سازی سیاستهای امنیتی اطلاعات

مرکز عملیات امنیت (SOC (Security Operation Center :

مرکز عملیات امنیت شبکه، (SOC) مکاني جهت مانیتورینگ و کنترل ٢٤ ساعته ورود و خروج اطلاعات در شبکه مي باشد. به طور کلي هر مرکز SOC به سه سطح عمده تقسیم مي شود که هر يك وظایف خاصي را بر عهده دارند. این سطوح عبارتند از:

سطح یکم، نقطه تماس Clientها و مسئول پاسخ گویي به اخطارهاي دریافتي ازClient هاست. در این سطح به کلیه اخطارهایي که از پیچیدگي پایین‌تري برخوردارند، پاسخ داده مي‌شود.

سطح دوم، در حقیقت مکمل سطح یکم است و مسئول پاسخ‌گویي به مشکلات پیچیده تر در سیستم‌هاي امنیتي شبکه مي‌باشد. براي اخطارهایي که از اهمیت بالایي برخوردارند، سیستم هاي سطح دوم به طور کامل درگیر مي‌شوند.

سطح سوم، در این سطح کارشناسان ارشد و مشاوران امنیتي شبکه قرار دارند. این سطح در حقیقت پشتیبان دو سطح پایین‌تر است. در صورتي که به اشکالات امنیتي در دو سطح پایین پاسخ داده نشود، کارشناسان و سیستم‌هاي این سطح، درگیر مي‌شوند. کلیه تدابیر امنیتي و مدیریت امنیت شبکه، در این سطح اندیشیده مي‌شود.

۴-۱ کنترل دسترسی (Access Control):

از جمله سیاستهای امنیتی اطلاعات ، استانداردهایی است که برای کنترل دسترسی به فایلها مورد نیاز است. لازم است این مکانیزم به همراه مکانیزم اعتبار سنجی کار کند تا فقط کاربران مجاز قادر به دسترسی به فایلهای خاص میباشند . در این صورت هر کاربر از نظر مکانیزم خواندن و یا نوشتن و اجرا کردن فایل خاصی ، بر اساس ID خاصی که دارد اقدام میشود .

۴ ـ ۲ گزارش گیری (Audit) :

در این قسمت موار زیر باید لحاظ شود :

۱- ورود یا Login موفق و یا غیر موفق

۲- خروج یا Logout

۳- دسترسی نادرست به فایل یا سیستم

۴- دسترسی از راه دور (Remote Access) موفق و یا غیر موفق

۵- اعتبار سنجی (Privilege)

6- گزارش اتفاقات (Event Log) ائم از نصب نرم افزار یا خاموش و روشن کردن سیستم توسط مدیران

لازم است هر Event Log شامل موارد زیر باشد :

۱ - شناسه کاربر (User ID)

۲- تاریخ و زمان (Date & Time)

3- IP Address مربوطه

۴- فعالیتهای انجام شده

۵- موفقیت و یا عدم موفقیت واقعه

۴ ـ ۳ نحوه اتصال به شبکه (Network Connection):

برای هر نوع اتصال به شبکه لازم است قوانین مربوط به این اتصال و مکانیزمهای محافظتی توسط سیاست امنیتی تعیین گردد.

برای اتصال به شبکه محلی اگر هر کاربری به راحتی بتواند کامپیوتر غیر مجاز را به شبکه محلی متصل کند ، ضریب نفوذ و اختلال در سیستمهای شبکه افزایش خواهد یافت . بنابراین به عنوان مثال با استفاده از استاندارد IEEE 802.1X میتوان عملیات AAA را برای کاربران در حین اتصال به شبکه محلی را ایجاد کرد. همچنین میتوان با استفاده از جدول MAC Address Table در سوییچهای شبکه ، به صورت Static ویا Dynamic ، اتصال کامپیوترها و یا IP Phone ها به شبکه را کاملا کنترل کرد .

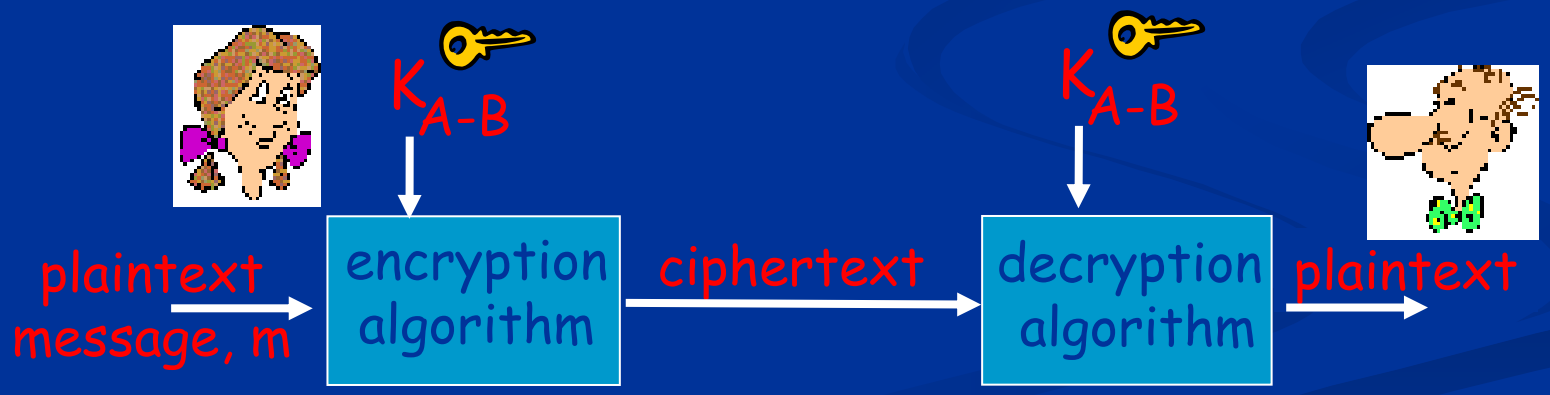
به این صورت که میتوان یک MAC Address خاص را به پرت خاصی و یا رنجی از پرتهای خاص اختصاص داد همچنین با استفاده از تکنولوژی Dynamic Vlaning میتوان محدودیتهای در نظر گرفته شده برای هر User را در هنگام اتصال به شبکه و پس از انجام عملیات AAA ، برای عضویت در VLAN مشخص در نظر گرفت و هرگونه محدودیتها و متغیر ها را به VLAN مشخص اعمال کرد .

۴ – ۴ دسترسی از راه دور به سیستمهای داخل سازمان (Remote Access) :

ارتباط از راه دور به این معناست که کاربران از طریق ارتباطات تلفنی و یا ارتباط VPN با مرکز در ارتباط باشند .

در این حالت بهتر است تمام ارتباط با استفاده از الگوریتمهای رمزنگاری محافظت شود . و همچنین عملیات IPSec روی ارتباطات برقرار شود . در این صورت استفاده از مکانیزمهای اعتبار سنجی AAA حتما لازم است .

همچنین در مکانیزم رمز نگاری ، پروسه مدیریت کلید (Key Management) بسیار مهم میباشد چراکه با استفاده از این تکنولوژی و تبدیل بالعکس اطلاعات رمزنگاری شده (Encryption) به حالت Clear Text ، یا (Decryption) ، باید به درستی انجام شود و اگر در سرویس مدیریت کلید (Key Management) خللی ایجاد شود کل اطلاعات رمزنگاری شده از دست میرود .



۴- ۵ - مانیتورینگ منظم :

هر سازمان باید پروسه ای داشته باشد که کنترل و مانیتورینگ شبکه را مستند نماید. برخی از سازمانها این نوع کنترل را به صورت پیوسته انجام میدهند و برخی دیگر از سازمانها به طور تصادفی انجام میدهند .

نرم افزارهایی از قبیل MRTG و Sniffer و Whats Up Gold و Network Analyzer و ... نرم افزارهایی هستند که با قابلیتهای متفاوت و عملکرد متفاوت هر کدام به نوبه ای شبکه را مانیتور میکنند .

حتی تجهیزات سخت افزاری از قبیل Fluke Network Analyzer این کار را انجام میدهند .

همچنین باید بسیار مراقب بود که خروجی (Output) این تجهیزات و نرم افزارها در اختیار نفوذ کنندگان و یا افراد غیر مجاز قرار نگیرد چراکه درغیراین صورت ، امنیت شبکه کاملا به خطر می افتد

۶-۴ غلبه بر خطا (Fail Over) :

- بر خلاف پشتیبان که به صورت Offline میباشد ، در این روش بروز خطا به صورت اتوماتیک تشخیص داده میشود و قابلیتهای آن سیستم مجددا برقرار میشود .

- به عنوان مثال Fail Over بر روی Domain Controller ها میتواند به صورت PDC (Primary Domain Controller) و BDC (Backup Domain Controller)

- و یا پیاده سازی مکانیزم Clustering روی سیستمهایی که سرویس مشابه ارائه میدهند .هم ارائه مکانیزم Fail Over و هم Load Balancing

۴-۷ مجوز سنجی (AAA (Authentication , Authorization , Accounting

- سرویس مجوز سنجی به خودی خود قادر به محافظت در برابر حملات نمیباشد بلکه باید به همراه سرویس های دیگری استفاده شوند تا آن سرویس به طور موثر تر به فعالیت خود ادامه دهد .

- این سرویس به عنوان یکی از مطمئن ترین و مهمترین بخش امنیتی مطرح میشود که هر کاربر با ID (Identifier) مربوط به خودش به شبکه متصل میشود و قدرت نفوذ هر سیستم در شبکه بر اساس ID و سطح دسترسی و نوع مجوز آن مطرح میباشد .

مدل امنیت لایه بندی شده :

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند.

ردیف	سطح امنیتی	ابزار و سیستم های امنیتی قابل استفاده
۱	پیرامون	•فایروال آنتی ویروس در سطح شبکه رمزنگاری شبکه خصوصی مجازی
۲	شبکه	•سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS) سیستم مدیریت آسیب پذیری تبعیت امنیتی کاربر انتهایی کنترل دسترسی/ تایید هویت کاربر
۳	میزبان	•سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان تبعیت امنیتی کاربر انتهایی آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
۴	برنامه کاربردی	•سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
۵	داده	•رمزنگاری کنترل دسترسی/ تایید هویت کاربر

جدول ۵. مقايسه تجهيزات امنيتي در لايه هاي چهارگانه TCP/IP

لايه تجهيزات امنيتي	Host to Network	IP	TCP	Application
حفاظت فيزيكي	√			
رمزنگاري	√	√	√	√
IP Sec		√		
SSL			√	
Firewall		√	√	√
AntiVirus				√
AAA Server	√	√	√	√
VPN	√	√	√	√
PGP				√
IDS/IPS		√	√	√

Pretty Good Privacy (PGP)

۵- نتیجه کلی در طراحی و پیاده سازی مکانیزم امنیت :

- اساس و پایه امنیت شبکه مبتنی بر ریسک و کنترل و نظارت بر روی تمام سطوح مکانیزمهای ارتباطی میباشد .
- آگاهی داشتن در مورد انواع حملات و نفوذهای شبکه و تاثیراتی که هر کدام به نوعی در شبکه خواهند گذاشت .
- پیاده سازی مکانیزم درست و صحیح محافظت از شبکه بر اساس نیازهای موجود و خطرات احتمالی در شبکه
- برآورد صحیح از نیازها و امکانات بالقوه و بالفعل سازمان بر اساس محدودیتهای موجود از قبیل محدودیتهای مالی و ....
- تست و پیاده سازی در محیط آزمایشگاهی قبل از پیاده سازی در محیط اصلی و واقعی .
- مد نظر داشتن این نکته که هیچ راه حل امنیتی وجود ندارد که 100 % تامین کننده تمام نیاز ها و انتظارات ما باشد و برای محافظت از داده ها و نقل و انتقالات در شبکه باید در حد توان تمام مسایل امنیتی به صورت فیزیکی و منطقی در نظر گرفته شود .
- آشنایی و آموزش تمام پرسنل مربوطه با تمهیدات امنیتی به کار گرفته شده در سازمانها و کمک گرفتن از خود پرسنل جهت نیل به اهداف امنیتی سازمان .

مراجع :

www.securityfocus.org

www.governmentsecurity.org

www.antionline.com

www.packetstormsecurity.org

www.watchfire.com

Cisco Security, by: Cisco Press(2006)

Mastering Network Security ,by: Chris Brenton (Sybex)2006

با تشکر و قدردانی از توجه شما عزیزان