10 راهکار برای ارتقاء امنیت شبکه

سید حمید کشفی

HAMID@OISSG.ORG

بهمن 1388

فهرست مطالب

- بخش اول (آشنایی با انواع محصولات و راهکارهای امنیتی)
  - معرفی موضوع سمینار
  - تعریفی کلی از آنچه امنیت نامیده می شود
  - آشنایی با منشأ و انواع تهدیدات رایج
  - مرور مشکلات رایج در شبکه های بزرگ و کوچک
  - معرفی انواع رایج محصولات و راهکارهای امنیتی
  - معرفی انواع سرویس های امنیتی
  - دسته بندی راهکارهای امنیتی متناسب با نوع سازمان
- بخش دوم
  - معرفی و مرور چند روش عملی و کاربردی برای بهبود و ارتقاع سطح امنیت در شبکه
  - پرسش و پاسخ

تعریف آنچه "امنیت" در شبکه خوانده می شود

- سه اصل مهم در هر سیستم:
  - حفظ (Confidentiality)
  - حفظ (Integrity)
  - حفظ (Availability)
- در هر شبکه به خطر افتادن یک یا تمامی این موارد، بصورت مستقیم و یا غیر مستقیم منجر به اختلال در سیستم یا چرخه کاری سیستم خواهد شد
- هدف از برقراری امنیت، محافظت از این سه اصل و در نتیجه تضمین پایداری سیستم و چرخه های کاریست.

آشنایی با تهدیدات امنیتی رایج

- تقسیم بندی از نظر منشاء حمله
  - حملات و تهدیدات از داخل شبکه
    - پرسنل ناراضی،کنجکاو، ناآگاه،...
    - پیمانکاران وارد شده به مجموعه،...
    - افراد ناشناس وارد شده به مجموعه که به شبکه دسترسی دارند
    - تروجان ها، ویروس ها و کرم های رایانه ایی
  - حملات و تهدیدات از خارج شبکه سازمان
    - ویروس ها و کرم های رایانه ایی
    - پرسنل یا مدیران شبکه خارج شده از مجموعه
    - رقبای تجاری و کاری
    - نفوذگران بدون هدف مشخص؛ افرادی که از سر تفنن اقدام به تلاش برای نفوذ می کنند
    - نفوذگران دارای هدف مشخص؛ افرادی که به دنبال اطلاعات خاصی از (شبکه) مجموعه شما هستند

آشنایی با تهدیدات امنیتی رایج (2)

- تقسیم بندی از نظر هدف حمله
  - از کار انداختن سرویس ها و ایجاد اختلال عمدی
  - دسترسی به اطلاعات و داده های ارزشمند
  - تخریب وجهه اجتماعی، سیاسی، ...
  - سایر موارد (ویروس های مزاحم و بدون هدف خاص)
- تقسیم بندی از نظر نحوه گسترش حملات
  - خودکار و گسترده (ویروسها، کرم های اینترنتی، ...)
  - غیر خودکار و موردی (اقدام به نفوذ توسط هکرها،...)
- برخی از مهم ترین علت های بروز تهدیدات امنیتی
  - بروز نبودن سیستم ها و نرم افزارها (عدم نصب اصلاحیه های امنیتی)
  - تنظیمات اشتباه یا نا امن پیاده سازی شده در سیستم ها و نرم افزارها
  - کلمات عبور ضعیف و قابل حدس
  - وجود اعتماد (Trust) بی جا و غیر ضروری بین سیستم ها و کاربران مختلف
  - عدم استفاده از نرم افزارهای آنتی ویروس، بروز نبودن آنها و یا نا کارآمد بودن نرم افزار
  - ورود و خروج کنترل نشده اطلاعات و نرم افزارها در شبکه و سیستم ها

مشکلات رایج در شبکه های بزرگ و گسترده

- گستردگی شبکه و تنوع سرویس ها سبب می شود که استفاده از نرم افزارهای جانبی و سرویس های فعال در شبکه از کنترل خارج گردد و نظارتی بر آنها وجود نداشته باشد
- شبکه عملاً توسط پیمانکارانی که نرم افزارها و سخت افزارهای آنها در شبکه پیاده سازی شده، هدایت می گردد.
- دغدغه اصلی و اولیه مدیران شبکه، کارکرد صحیح سیستم ها و راضی نگه داشتن پرسنل می باشد
- در اغلب موارد از نرم افزارهای قفل شکسته و بدون لایسنس استفاده می گردد = عدم بروز رسانی
- مدیران شبکه عموماً با مشکلات زیادی در دریافت بودجه برای مصارف امنیتی مواجه هستند
- امنیت سیستم ها و سرویس ها تا زمانی جدی گرفته می شود که بار مسئولیت و مدیریتی ایجاد نکرده و اختلال و سختی در کارها ایجاد نکند!
- در بسیاری از موارد تنها نام یکل محصول امنیتی در بستر شبکه به چشم می خورد، اما درعمل همه کارایی و قابلیت های آن مورد استفاده قرار نمی گیرد
- بدلیل عدم استفاده از تنظیمات بهینه، حجم اخطارها و پیغام های تولید شده توسط راهکارهای امنیتی آنقدر زیاد است که نادیده گرفته می شود
- حتی در صورت بهینه بودن تنظیمات، نیروی متخصص برای تحلیل رویداد های ثبت شده وجود ندارد
- روال پیچیده اداری در بسیاری از سازمانها، پیاده سازی امنیت در سطح گسترده را بسیار زمانبر و مشکل می کند

مشکلات رایج در شبکه های متوسط و کوچک

- مجموعه ایی کوچک از سیستمها در حد بانجام رسیدن کارهای مجموعه به هم متصل شده اند
- (سیستم های) پرسنل بدلیل نوع محیط دارای اعتمادی کاذب به یکدیگر هستند
- کسی بصورت مجزا و اختصاصی به امنیت سیستم ها فکر نمی کند
- معمولآ مدیریت یکپارچه در شبکه و جود ندارد و سیستم ها بصورت جزیره ایی کنترل می شوند
- راهکارها و روش های امنیتی بصورت سلیقه ایی مورد استفاده قرار می گیرند
- بدلیل کوچک بودن مجموعه ، خرید راهکارهای امنیتی پیشرفته ممکن است مقرون به صرفه نباشند (حتی در صورتی که به آنها نیاز باشد)
- حتی در صورت خرید این قبیل تجهیزات، نیرویی فنی برای استفاده صحیح از آنها وجود ندارد
- در اغلب موارد از نرم افزارهای قفل شکسته و بدون لایسنس استفاده می گردد = عدم بروز رسانی
- بدلیل عدم دسترسی به اینترنت با سرعت بالا و مناسب، کاربر عمومآ تمایلی به بروز رسانی نرم افزارها یا سیستم عامل ندارد

معرفی انواع رایج راهکارهای های امنیتی

- برخی از راهکارهای امنیتی که بیشتر شناخته شده اند
  - نرم افزارهای آنتی ویروس
  - سیستم های سخت افزاری یا نرم افزاری Firewall
  - سیستم های تشخیص/مقابله با نفوذ (IDP)
  - راهکارهای مدیریت اصلاحیه های امنیتی
  - راهکارهای جمع آوری، ثبت و مدیریت رویداد ها
  - راهکارهای ارتباطی امن (VPN)
  - ...
- در تمامی این موارد، تکیه برا استفاده از ابزار یا نرم افزاری خاص وجود دارد
- موارد ذکر شده تنها راهکارهای موجود و قابل استفاده نیستند.
- از دیدگاه ها و روش های دیگری نیز می توان امنیت را بهبود داد

آنچه شما با خرید نرم افزار یا سخت افزار به آنها نخواهید رسید

- راهکاری برای ایجاد و اعمال روال های امنیتی
- راهکاری برای امن سازی "تنظیمات" سیستم های موجود
- راهکاری برای استفاده بهینه از نرم افزارها و سخت افزارهای امنیتی
- راهکاری برای محکم سازی (Hardening) سرویس ها و نرم افزارهای موجود
- راهکاری که متناسب با شرایط، امکانات و بودجه شما برنامه ایی را برای پیاده سازی امنیت ارائه کند
- و در نهایت هرآنچه برای دستیابی به آن تجربه و تخصص فردی نیاز است

معرفی انواع سرویس های امنیتی

- تعریف "سرویس" امنیتی و تفاوت آن با محصولات نرم افزاری/سخت افزاری امنیتی
- فروشندگان محصولات لزوماً ارائه دهندگان "سرویس" های امنیتی نیستند
- برخی از فروشندگان محصولات امنیتی از ادعاهایی خلاف واقع برای تبلیغ محصولات خود استفاده می کنند
- انواع سرویس های امنیتی
  - بازبینی و طراحی ساختار شبکه بصورت امن
  - بازبینی تنظیمات و اعمال تنظیمات امن (Hardening)
  - ارزیابی امنیتی شبکه و سیستمها(Vulnerability Assessment)
  - تست نفوذ پذیری (Penetration Test)
  - ارزیابی امنیتی تنظیمات پیاده سازی شده (Security Audit)
  - مدیریت امنیت سیستم های فعال (Managed Security)
  - بازیابی از رخدادهای امنیتی (Incident Response)
  - طراحی و پیاده سازی روال ها و قوانین امنیتی
  - آموزش و فرهنگ سازی امنیت

معرفی انواع سرویس های امنیتی

- بازبینی و طراحی ساختار شبکه بصورت امن
  - شرایط موجود
    - در زمان طراحی بسیاری از شبکه ها، نکات امنیتی مد نظر قرار نگرفته است
    - از دید بسیاری از مسئولین و مدیران شبکه، همین اندازه که شبکه به خوبی کار کند کافیست!
    - برقراری امنیت در شبکه ایی با بستر و طراحی نا امن، همانند طراحی یک ساختمان بر روی شالوده ایی ناپایدار و سست است
    - بسیاری از راهکارهای امنیتی در سطح شبکه، اولین لایه مقابله با تهدیدات امنیتی بشمار می روند
  - راهکارهایی که این سرویس ارائه می کند
    - استفاده از تنظیمات استاندارد و معتبر که کارایی آنها به در شرایط واقعی به اثبات رسیده
    - بازبینی امنیتی و پیکره بندی مجدد زیر ساخت شبکه
      - طراحی Zone ها ، پیاده سازی VLAN ، پیکره بندی امن روتر ها و سویچ ها
    - بررسی ساختار و سرویس ها و انتخاب صحیح محصولات امنیتی
      - انتخاب و پیاده سازی صحیح فایروال ها، سیستم های تشخیص نفوذ، مانیتورینگ و ...

معرفی انواع سرویس های امنیتی

- بازبینی تنظیمات و اعمال تنظیمات امن (Hardening) سیستم عامل ها و سرویسها
  - شرایط موجود :
    - بخش بسیار زیادی از سیستم های فعال در شبکه های ما مبتنی بر سیستم عامل ویندوز می باشد
    - سازمان های محدودی برای سرورهای خود لایسنس خریداری کرده اند
    - تقریباً هیچ ارگان و سازمان ایرانی برای ایستگاه های کاری خود از ویندوزهای لایسنس شده استفاده نمی کند = مشکل در بروز رسانی اصلاحیه های امنیتی
    - علی رغم وجود دانش فنی مدیریت، به دلایلی که پیش از این ذکر شد، در بسیاری از موارد از تنظیمات پیش فرض سیستم عامل و سرویس های آن استفاده می شود
    - مدیران شبکه به ندرت اقدام به بهینه سازی تنظیمان امنیتی سرویس ها بصورت مجزا می کنند.
    - تنظیمات پیش فرض شاید در شرایط ایده آل مشکل و تهدیدی ایجاد نکنند، اما با بروز کوچکترین رویداد امنیتی نقطه ضعف خود را نشان خواهند داد
  - راهکارهایی که این سرویس ارائه می کند
    - تنظیم مجدد کلیه سرویس ها و تنظیمات سیستم عامل، با دید ارتقاع امنیت
    - حذف و غیر فعال کردن سرویس ها و قابلیت های بلا استفاده در سیستم ها، نرم افزارها و شبکه
    - استفاده از تنظیمات استاندارد و معتبر که کارایی آنها به در شرایط واقعی به اثبات رسیده
    - این بسته پیش نیاز و پایه بسیاری از سرویس ها و راهکارهای امنیتی دیگر است
    - تغییرات ناشی از این بسته، نا محسوس اما بسیار موثر می باشد

معرفی انواع سرویس های امنیتی

- بازبینی تنظیمات و اعمال تنظیمات امن (Hardening) بانک های اطلاعاتی
  - شرایط موجود :
    - تقریبا در هر مجموعه ایی بخش زیادی از اطلاعات مهم بر روی بانکهای اطلاعاتی ذخیره می شوند
    - سیستم تمامی نرم افزارهای حسابداری و اتوماسیون اداری با بانک های اطلاعاتی گره خورده است
    - آمار استفاده از انواع بانک های اطلاعاتی در ایران(1388):
      - Microsoft SQL Server %51.3
      - MySQL %39.9
      - Oracle %4.2
      - %4.6 سایر بانک های اطلاعاتی
    - تجربه نشان داده است که در کمتر سازمانی بصورت اختصاصی به امنیت بانک اطلاعاتی پرداخته شده است
    - بانک های اطلاعاتی در شرایط استفاده از تنظیمات پیش فرض خود بسیار نا امن هستند !
      - اوراکل در شرایط وتنظیمات پیش فرض خود، مشابه یک Backdoor است ! بیش از 200 کاربر پیش فرض...
      - مشکل نصب اصلاحیه های امنیتی بر روی بانک های اطلاعاتی
      - MS-SQL یکی از اولین انتخاب های هکرها برای نفوذ در شبکه های داخلی است
  - راهکارهایی که این سرویس ارائه می کند
    - بازبینی امنیتی و پیکره بندی امنیتی بانک های اطلاعاتی (MS-SQL, Oracle, MySQL)
    - استفاده از تنظیمات استاندارد و معتبر که کارایی آنها به در شرایط واقعی به اثبات رسیده
    - غیر فعال کردن بسیاری از قابلیت ها و دسترسی های پیش فرض که خطرساز می باشند
    - نظارت بر سیستم پس از اعمال تغییرات، بمنظور شناسایی مشکلات و تداخلات احتمالی، و رفع آنها

معرفی انواع سرویس های امنیتی

- ارزیابی امنیتی شبکه و سیستم ها (Vulnerability Assessment)
  - شرایط موجود :
    - چند درصد از شما پیش از این با مشکلات امنیتی در شبکه خود مواجه بوده اید؟
    - چند درصد از شما واقعآ از وضعیت امنیتی شبکه خود (بصورت فنی) آگاه هستید؟
    - چند درصد از شما بصورت منظم امنیت سیستم های خود را (به هر شکل) ارزیابی می کنید؟
    - چند درصد از شما بعد از ارزیابی امنیتی، استفاده موثری از خروجی آن داشته اید؟
    - تحلیل خروجی روال ها و ابزارهای ارزیابی امنیتی نیازمند آگاهی کامل و شناخت دقیق انواع تهدیدات امنیتی و مشکلات فنی است. چیزی که کمتر مدیر شبکه ایی فرصت درگیر شدن با آن را دارد
  - راهکارهایی که در این سرویس ارائه می شود
    - استفاده از متدودولوژی ها و ابزارهای بروز، کامل و استاندارد، برای ارزیابی وضعیت امنیت شبکه
    - بررسی سیستم ها از زوایای مختلف، برای آگاهی و بررسی دقیق تر شرایط موجود
    - شناسایی نقاط ضعف امنیتی موجود در تنظیمات و نسخ نرم افزارها و سرویس های مختلف شبکه
    - تهیه گزارشی دقیق و جامع از مشکلات امنیتی، که مشخص کننده اولویت ها و نیازهای شما از میان راهکارها و سرویس های امنیتی است

معرفی انواع سرویس های امنیتی

- تست نفوذ پذیری (Penetration Test)
  - شرایط موجود
    - مستندات امنیتی شبکه ها (در صورت وجود!) معمولآ دارای تفاوت زیادی با آنچه واقعآ وجود دارد هستند
    - حتی در صورت استفاده از راهکارهای امنیتی،ارزیابی امنیتی و پس از آن محکم سازی، نمی توان مطمئن بود که همه چیز طبق میل ما پیاده سازی شده است
    - تنها راه اطمینان از این مورد، به چالش کشیدن امنیت سیستم ها و شبکه است
    - به چالش کشیدن امنیت، نیازمند تخصص و تجربه و مهارت می باشد. چند درصد از مدیران حرفه ایی شبکه در این خصوص اطلاعاتی دارند ؟!
    - Pen.Test در واقع یک شبیه سازی استاندارد و کامل است از آنچه هکرها انجام می دهند تا به سیستم های شما نفوذ کنند
    - نفوذ توسط هکرهای کلاه سیاه (Blackhats, Crackers) صورت میگیرد اما P.T توسط هکرهای کلاه سفید (White Hats, Ethical Hackers)
    - حتی امن ترین شبکه ها و سیستم ها نیز در خلال این تست نقاط ضعفی را هرچند جزئی نمایان خواهند کرد!
    - شما نمی توانید به هکرها اطمینان کنید، یا از آنها انتظار کمک داشته باشید!
  - راهکارهایی که در این سرویس ارائه می شود
    - قبل از اینکه دیگران به سیستم های شما نفوذ کنند، خود به آنها نفوذ می کنید!
    - پیاده سازی حملات واقعی به شبکه و سیستم ها، توسط متخصصین با تجربه و قابل اطمینان
    - تست و بررسی کلیه اجزای سیستم ها و شبکه بر اساس متدولوژی های استاندارد و کامل
    - مستند سازی نقاط ضعف شناسایی شده و کشف روش های ممکن برای نفوذ به شبکه ها و سیستم های شما
    - آگاهی از اینکه راهکارهای امنیتی مورد استفاده در شرایط واقعی تا چه میزان کارآمد هستند

دسته بندی راهکارهای امنیتی متناظر با نوع سازمان

- اولویت های سازمان ها و ارگان های بزرگ
  - سرویس های زود بازده
    - ارزیابی امنیتی (Vulnerability Assessment)
    - محکم سازی سیستم ها و سرویس ها (Hardening)
    - تست نفوذ پذیری (Penetration Test)
  - محصولات زود بازده
    - سیستم های آنتی ویروس با مدیریت متمرکز
    - سیستم های مدیریت اصلاحیه های امنیتی (Patch Management)
    - فایروال ها
    - سیستم های تشخیص و مقابله با نفوذ (IDP)
  - سرویس و راهکارهای بلند مدت
    - بازبینی و طراحی امن ساختار شبکه
    - مدیریت امنیت سیستم های فعال (Managed Security)
    - پیاده سازی رویه های مدیریت امنیت اطلاعات
    - آموزش نکات و موارد امنیتی به پرسنل

دسته بندی راهکارهای امنیتی متناظر با نوع سازمان

- اولویت های سازمان ها و شرکت های متوسط و کوچک
  - سرویس های زود بازده
    - محکم سازی سیستم ها و سرویس ها (Hardening)
    - ارزیابی امنیتی (Vulnerability Assessment)
  - محصولات زود بازده
    - سیستم های آنتی ویروس با مدیریت متمرکز
    - سیستم های مدیریت اصلاحیه های امنیتی (Patch Management)
    - سیستم های یکپارچه مقابله با تهدیدات (UTM)
  - سرویس و راهکارهای بلند مدت
    - آموزش نکات و موارد امنیتی به پرسنل

بخش دوم

معرفی و مرور چند روش عملی و کاربردی
برای بهبود و ارتقاع سطح امنیت در شبکه

قدم اول: سازماندهی و یکپارچه سازی ساختار شبکه

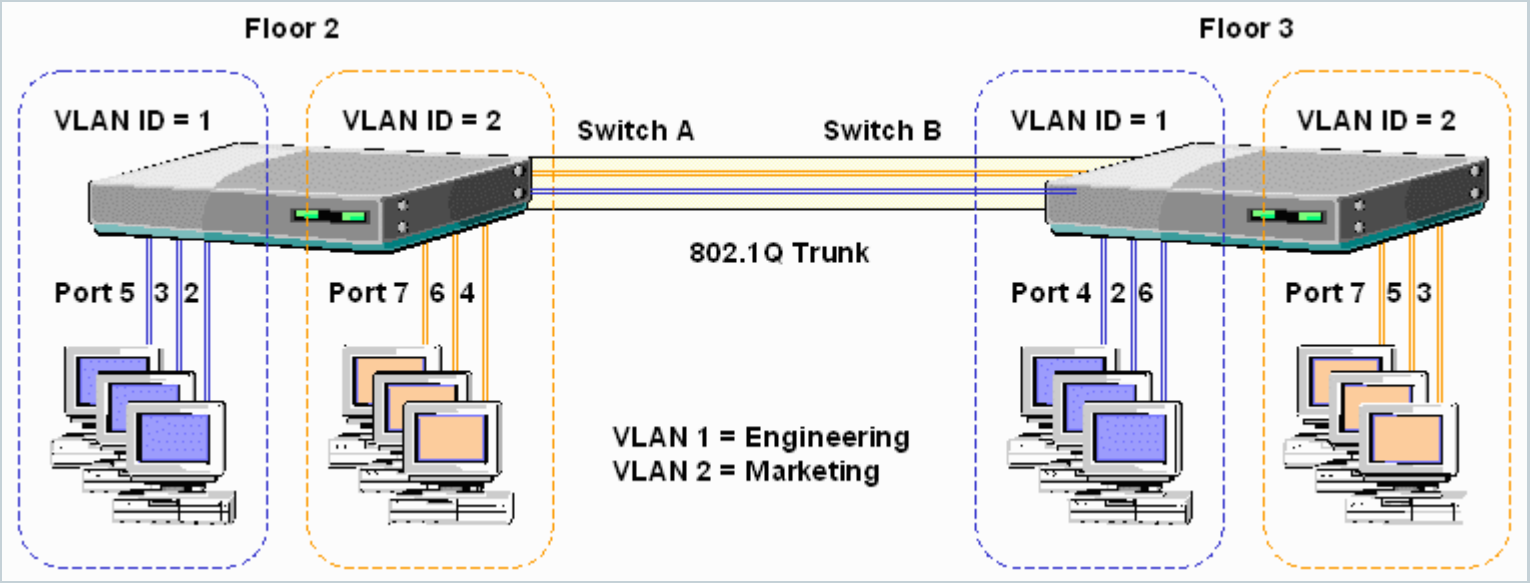
- پیش از برقراری امنیت، برقراری نظم در شبکه الزامی می باشد
- بسیاری از راهکارهای امنیتی برای کارکرد و عملکرد صحیح و کامل نیازمند شبکه ایی ساخت یافته و مدیریت شده می باشند
  - مدیریت مرکزی آنتی ویروس ها
  - مدیریت مرکزی اصلاحیه های امنیتی
  - مدیریت و مانیتورینگ سیستم های کاربران
  - ...
- برای شبکه و کلیه سیستم های فعال در آن شناسنامه تهیه کنید
- کلیه اجرای شبکه از طریق یکی یا چند مشخصه فنی آنها می بایست قابل شناسایی باشند
- پیاده سازی دامنه (Domain) یکی از بهترین و آسان ترین روش های سازمان دهی و یکپارچه سازی سیستم ها در شبکه می باشد
- مزایای راه اندازی دامنه در شبکه:
  - امکان دسترسی یکپارچه و مدیریت شده به کلیه منابع در شبکه
  - امکان پیاده سازی طیف وسیعی از تنظیمات و راهکارهای جانبی از طریق اکتیو دایرکتوری
  - امکان اعمال آسان انواع محدودیت ها بر روی کاربران، بصورت متمرکز و یکپارچه
  - فراهم سازی بستر و امکان تلفیق بسیاری از راهکارهای امنیتی پیشرفته که در آینده ممکن است استفاده شود

قدم دوم: کنترل و اعمال محدودیت برای کاربران

- تا زمانی که کاربران امکان مدیریت و تسلط کامل بر روی سیستم خود را داشته باشند، احتمال بروز مشکلات فنی و امنیتی بسیار بالاست
- کاربران دارای سطح دسترسی مدیر، براحتی امکان دور زدن و غیر فعال کردن بسیاری از راهکارهای امنیتی را (حتی در سیستم های عضو دامین) دارند.
- ذهنیت اشتباه: محدود کردن سطح دسترسی کاربران به معنی ایجاد اختلال در کار آنها ست
- به هر کاربر در شبکه باید حداقل دسترسی ممکن داده شود (قانون Least Privileges)
- برخی از محدودیت هایی که بهتر است اعمال شوند:
  - محدود کردن کاربر در غیرفعال کردن راهکارهای امنیتی
  - محدود کردن کاربر در نصب نرم افزارها و ابزارهای جانبی غیر ضروری
  - محدود کردن کاربر در نصب تجهیزات و استفاده از سخت افزارهای جانبی
  - محدود کردن کاربر در انتخاب (اشتباه) تنظیمات خاص یا امنیتی سیستم عامل
  - محدود کردن کاربر در امکان به اشتراک گذاشتن منابع سیستم بصورت آزادانه
  - محدود کردن کاربر در انتخاب (اشتباه) تنظیمات مرورگر وب
- همه موارد فوق از جمله امکاناتی هستند که اکتیو دایرکتوری از طریق اعمال Domain Policy ها در اختیار مدیر شبکه قرار می دهد
- پیاده سازی محدودیت ها از طریق Domain Policy می بایست کاملاً تست شده و عاری از محدودیت های بی مورد یا مشکل ساز باشد
- می توان برای هر گروه از کاربران، Policy های محتلفی را تنظیم و اعمال کرد

قدم سوم: پیاده سازی یک ساختار مشخص در سطح شبکه

- بسیاری از شبکه های موجود Flat هستند، یعنی هر عضو شبکه امکان برقراری ارتباط و دسترسی به کلیه اعضای دیگر شبکه را دارد
- در بسیاری از موارد، دسترسی به منابع غیر مجاز به معنی به خطر افتادن اطلاعات سازمانی و زیر سوال رفتن امنیت بطور جدی می باشد
- با تقسیم بندی شبکه بصورت فیزیکی و منطقی (Logical) پیاده سازی این اصل ساده ولی مهم امکان پذیر می باشد
- پیاده سازی تقسیم بندی عموماً از طریق استفاده از VLAN انجام می شود
- برخی از مزایای پیاده سازی VLAN در سطح شبکه
  - امکان کنترل و اعمال محدودیت دسترسی بخش های مختلف شبکه به یکدیگر
  - جلوگیری از گسترش سریع و غیرقابل کنترل کرم ها و ویروس های رایانه ایی
  - امکان تعریف قوانین دسترسی بین VLAN ها بر اساس نوع سرویس یا پروتکل
  - امکان مدیریت و نظارت و مانیتورینگ بخش های مختلف شبکه بصورت تفکیک شده


Floor 2
Floor 3
VLAN ID = 1
VLAN ID = 2
Switch A
Switch B
VLAN ID = 1
VLAN ID = 2
802.1Q Trunk
Port 5 3 2
Port 7 6 4
Port 4 2 6
Port 7 5 3
VLAN 1 = Engineering
VLAN 2 = Marketing

قدم سوم: پیاده سازی یک ساختار مشخص در سطح شبکه (2)

- دسترسی به شبکه را محدود و مستلزم اعتبارسنجی کنید
  - پیاده سازی راهکار امنیتی 802.1x به شما امکان اعتبارسنجی سیستم ها در لایه 2 را در زمان اتصال آنها به شبکه می دهد
  - بکمک 1x. تا زمانی که کاربر اعتبارسنجی نشود، سویچ شبکه اجازه اتصال وی به شبکه و استفاده از منابع را نخواهد داد
  - تکنولوژی 1x. قابلیت ترکیب شدن با اکتیو دایرکتوری را برای اعتبارسنجی داراست
- پورت های بلا استفاده سویچ های شبکه را غیر فعال کنید
- تفکیک فیزیکی بخش های مختلف شبکه سازمان
  - در برخی موارد حتی امنیت ارائه شده توسط VLAN قابل اطمینان نیست
  - علی رغم ایجاد بار مدیریتی و هزینه، در برخی شرایط بخش های مختلف شبکه بنا به مسایل امنیتی می بایست الزاماً بصورت فیزیکی جدا از شبکه اصلی باشند
- در صورتی که اطلاعات داخلی سازمان حساس و محرمانه می باشند ، تفکیک شبکه و سیستم های متصل به اینترنت از شبکه و سیستم های حاوی اطلاعات حساس الزامیست !

قدم چهارم: پیاده سازی تنظیمات امن (Hardening)

- هرگز به تنظیمات پیش فرض سیستم ها و نرم افزارها اطمینان نکرده و آنرا را مرور کنید
- با استفاده از چک لیست های امنیتی استاندارد، تنظیمات سیستم عامل ها و سرویس ها را در شبکه خود کنترل کرده و آنها را بهینه کنید
- Best Practice های ارائه شده توسط تولید کنندگان سیستم عامل و نرم افزار بهترین منبع و نقطه برای شروع می باشند
  - http://technet.microsoft.com/en-us/library/dd277328.aspx
  - http://technet.microsoft.com/en-us/library/dd366061.aspx
- گروه های مستقل نیز اقدام به ارائه چک لیست ها و استاندارد های Hardening می نمایند
  - http://www.cisecurity.org
- با کمی جستجو در اینترنت، می توان منابع بسیار زیادی را در این مورد یافت
  - http://www.google.se/search?q=hardening+checklist
- همه آیتم های آورده شده در چک لیست ها لزوماً متناسب با سیستم ها شما نیستند! اثر و کارایی آنها می بایست قبل از اعمال، در محیط آزمایشی تست و بررسی شود

قدم پنجم: سیستم ها و نرم افزارهای خود را بروز کنید

- هر روز چندین گزارش جدید در مورد ضعف های امنیتی سیستم عامل ها و نرم افزارها منتشر میشود و در پی آن اصلاحیه های امنیتی توسط تولید کنندگان نرم افزارها در اختیار قرار می گیرد
- بروز نگه داشتن سیستم ها و نرم افزارها و نصب اصلاحیه های امنیتی امری ضروری و غیر قابل چشم پوشی است
- در شبکه های کوچک انجام این کارآسان است، اما مدیریت اصلاحیه های امنیتی و نصب آنها در سطح گسترده و بصورت منظم بروش دستی عملاً غیر ممکن و یا بسیار مشکل است.
- با صرف هزینه کم و یا حتی بدون صرف هزینه می توان این مورد را پوشش داد:
  - استفاده از راهکار نرم افزاری مجانی WSUS ارائه شده توسط مایکروسافت
  - استفاده از نرم افزارها و راهکارهای جانبی تجاری مانند GFI LanGuard

قدم پنجم: سیستم ها و نرم افزارهای خود را بروز کنید (2)

- برخی از مزایای استفاده از WSUS
  - عدم نیاز به پرداخت هزینه یا تهیه لایسنس برا استفاده از آن
  - تلفیق آسان با اکتیو دایرکتوری و امکان پوشش کلیه سیستم های عضو دامین از طریق Policy
  - پوشش کلیه محصولات مایکروسافت
  - http://technet.microsoft.com/en-us/wsus/default.aspx
- برخی از مزایای استفاده از GFI LanGuard
  - قابلیت استفاده بصورت موردی برای اعمال اصلاحیه های امنیتی
  - قابلیت انتقال آسان اصلاحیه های دانلود شده و استفاده از آنها در شبکه های بدون اینترنت
  - قابلیت نصب نرم افزارهای جانبی و متفرقه از راه دور (بروز رسانی نرم افزارهای جانبی)
- سیستم عامل ها تنها مواردی نیستند که می بایست بروز نگه داشته شوند!
- بسیاری از نرم افزارهای جانبی و مورد استفاده کاربران شبکه نیز دارای ضعف های امنیتی بسیار جدی می باشند و باید دائماً بروز رسانی شوند
- یکی از راهکارهای توزیع نسخ بروز نرم افزارهای جانبی در شبکه، استفاده از بسته های MSI نرم افزار و توزیع آن از طریق Policy های تعریف شده در دامین می باشد
  - http://www.advancedinstaller.com/user-guide/tutorial-gpo.html
  - به کاربران خود فقط اجازه نصب نرم افزارهایی را بدهید که مجاز بوده و کنترل و بروز رسانی شده اند

قدم ششم: استفاده از سیستم های مدیریت متمرکز آنتی ویروس

- استفاده از نرم افزارهای آنتی ویروس بصورت متفرقه و مدیریت نشده در شبکه، آنطور که باید موثر ومفید نیست
- مدیر شبکه می بایست بتواند منشآ الودگی ها را در شبکه تشخیص داده و کنترل کند
- بروز نگه داشتن آنتی ویروس ها بر روی همه ایستگاه های کاری، همواره یکی از مشکلات مهم بشمار می رود
- کنترل فعال بودن و عملکرد صحیح آنتی ویروس ها بصورت دستی در شبکه امکانپذیر نیست
- سیستم های مدیریت متمرکز آنتی ویروس علاوه بر پوشش این مشکلات، امکانات مدیریتی متنوعی را نیز در اختیار می گذارند
- اغلب شرکت های تولید کننده آنتی ویروس، بسته های مدیریتی برای مدیریت متمرکز محصولات خود ارئه کرده اند اما قابلیت ها و امکانات جانبی آنها متفاوت است
- McAfee Protection Pilot و McAfee E-Policy یکی از کامل ترین نمونه های این قبیل سیستم ها می باشند.
- راه اندازی این راهکار، در صورت تلفیق با رهکار اکتیو دایرکتوری عملکرد بسیار بهتری را خواهد داشت.
- در صورت ارتباط با اینترنت، کنترل فایل های دریافتی از اینترنت توسط کاربران نیز الزامی می باشد
- اغلب شرکت های آنتی ویروس، راهکارهایی را برای مانیتور کردن ترافیک اینترنت نیز دارند

قدم هفتم: امنیت سیستم های خود را ارزیابی کنید

- اگرچه انجام Vulnerability Assessment بصورت کامل و دقیق نیاز به تخصص دارد اما یک مدیر شبکه نیز می تواند بکمک برخی از نرم افزارهای موجود، تا حدی این مرحله را انجام دهد
- برخی از نرم افزارهای قابل استفاده برای این منظور
  - Nessus : (http://nessus.org/nessus)
  - MBSA : (http://technet.microsoft.com/en-us/security/cc184923.aspx)
  - Retina : (http://www.eeye.com/Products/Retina.aspx)
  - GFI Languad Sec. Scanner : (http://www.gfi.com/lannetscan)
  - Secunia Scan : (http://secunia.com/vulnerability_scanning)
  - علی رغم تجاری بودن همه موارد، قیمت های این نرم افزارها قابل قبول می باشد
- انجام V.A به تنهایی کافی نیست! نتایج بدست آمده از خروجی این ابزارها نیز می بایست مورد استفاده قرار گرفته و ضعف های شناسایی شده رفع گردند
- V.A می بایست حتماً بصورت دوره ایی و در بازه های زمانی مشخص تکرار گردد
- در صورت امکان V.A هم بصورت Authenticated و هم بصورت معمولی می بایست بصورت موازی انجام شود

قدم هفتم: امنیت سیستم های خود را ارزیابی کنید (2)

- کلمات عبور مورد استفاده کاربران را ارزیابی و کنترل کنید
  - بیش از 60% از کاربران شبکه ها در ایران، از کلمات عبور نا امن و قابل حدس استفاده می کنند!
  - با استفاده از ابزارهای جانبی، مدیران شبکه می بایست این مورد را کنترل کرده و سیاست هایی را در مورد آن اعمال کنند
  - یک نمونه تجاری ابزار ارزیابی کلمات عبور L0pht Crack: http://www.l0phtcrack.com
  - نمونه مشابه و غیر تجاری LCP : http://www.lcpsoft.com/english/download.htm
- کاربران را مجبور به انتخاب کلمات عبور پیچیده و غیر قابل حدس کنید
  - پیاده سازی و اعمال Password Complexity در اکتیو دایرکتوری
- در هر سرویس، دستگاه و یا نرم افزار جدید که مورد استفاده قرار می گیرد، کلمات عبور پیش فرض را تغییر دهید یا کاربران پیش فرض را غیر فعال کنید
  - بانک های اطلاعاتی (ORACLE, MySQL, MS-SQL,...)
  - دستگاه های جانبی (پرینتر های تحت شبکه، دوربین های IP Base و ...)
  - روتر ها، سوئیچ ها ، اکسس پوینت های وایرلس و ...

قدم هشتم: ورود وخروج اطلاعات در شبکه را کنترل کنید

- در برخی از سازمانها، کنترل ورود و خروج اطلاعات و پیشگیری از نشر و نشت آنها دارای اهمیت بالایی می باشد
- با وجود سیستم های رایانه ایی و قابلیت های آنها، کنترل این مورد بسیار پیچیده و مشکل می باشد، اما غیر ممکن نیست!
- اولین قدم در این راه، محدود کردن روش های انتقال اطلاعات از رایانه هاست
  - محدود کردن دسترسی به CD-Drive
  - محدود کردن دسترسی به پورت های USB
  - محدود کردن دسترسی به چاپگرها و اسکنرها
  - محدود کردن دسترسی به سخت افزار و نصب سخت افزارهای جانبی غیر مجاز
  - مانیتور کردن و رویداد نگاری از داده های منتقل شده توسط کاربر
- برخی از این محدودیت ها توسط Policy های اکتیو دایرکتوری قابل اعمال است
- در صورت اهمیت این موضوع می بایست از نرم افزارهای جانبی ویژه این کار استفاده نمود
  - یک نمونه : GFI Endpoint Security (http://www.gfi.com/endpointsecurity)
  - نرم افرارهای دیگری نیز با قابلیت ها و امکانات مشابه وجود دارند

قدم نهم: کاربران شبکه را آموزش دهید

- بسیاری از مشکلات امنیتی پدید آمده، ناشی از عدم آگاهی کاربران شبکه از انواع تهدیدات امنیتی و میزان خطرات آنهاست
- آگاه کردن کاربران از روش های حمله مورد استفاده نفوذگران و معرفی تکنیک های مورد استفاده توسط ویروس ها و کرم های اینترنتی، اثر زیادی در کاهش تهدیدات ممکن علیه سیستم ها و اطلاعات دارد
- برخی از مواردی که می بایست به کاربران آموزش داد
  - نحوه استفاده صحیح از ابزارها و راهکارهای امنیتی
  - عدم استفاده از نرم افزارهای ناشناخته و غیر مطمئن
  - نحوه استفاده صحیح از منابع اینترنتی برای جستجوی نیازمندی ها و پیشگیری از هدایت شدن کاربران بسمت سایت های مخرب
  - آشنا کردن کاربران با انواع تهدیدات امنیتی و روش های حمله نفوذگران
  - ...

قدم دهم: اطلاعات (امنیتی)خود را بروز نگه دارید

- هر روز گزارشات بسیار زیادی از روش های حمله، و ضعف های امنیتی جدید سیستم ها در اینترنت منتشر می شود
- آگاهی از این موارد به مدیر شبکه برای فراهم کردن راهکارهای مقابله و ایمن سازی سیستم ها کمک زیادی می کند
- تا زمانی که شما از یک تهدید جدید یا مشکل امنیتی جدید خبر نداشته باشید، برای آن راهکاری نخواهید داشت!
- برخی از وب سایت هایی که مطالعه روزمره یا هفتگی آنها توصیه می شود:
  - http://www.securityfocus.com
  - http://secunia.com/advisories
  - http://www.microsoft.com/Security
  - http://www.viruslist.com
  - http://isc.sans.org
  - http://osvdb.org

پرسش و پاسخ