گزارش کار آموزی

دانشگاه آزاد اسلامی واحد خوی

مکان: شهرداری شهرستان خوی

موضوع: امنیت شبکه و کارایی آن

استاد کار آموزی:

جناب آقای دکتر مصطفایی

تهیه کننده:

کاظم نجفی

سال:۱۳۹۱

تشکر و قدر دانی

«سپاس خدایي را که باز فرصتي عطا فرمود»

سپاس خدایی را که باز فرصتی عطا فرمود تا دوباره در عرصه علم و دانش قدم بگذارم و بر علم و دانش خود بیفزایم و با سپاس از استاد گرامی جناب آقای دکتر مصطفائی که با زحمات زیاد ما در راه کسب علم و دانش یاری فرمودند. و با تشکر از سرپرست کار آموزی جناب آقای مهندس قندچی که در آموختن هرچه بیشتر استفاده کامپیوتر در امورات اداری و سازمانی ما را همراهی کردند و با سپاس از پدر و مادرم که شرایط کسب علم و دانش را فراهم کردند.

فصل اول

آشنایی کلی با مکان کارآموزی

تاریخچه شهرداری

پیدایش فکر تاسیس شهرداری مانند بسیاری از سازمان ها و وزارتخانه های دیگر بعد از انقلاب مشروطه در ایران در سال ۱۳۲۵ق . م صورت گرفت

قانون تاسیس بلدیه گرچه در دوره اول مجلس سال ۱۲۸۶ به تصویب رسید ولی اجراء آن تا سال ۱۲۸۸ به طول انجامید .سپس به تدریج در شهرهای بزرگ ایران تعداد قلیلی بلدیه تا پایان سلسله قاجار آغاز به کار کرد و از آن به بعد به مرور همه شهرها دارای شهرداری شدند . قانون فوق تا سال ۱۳۰۹ به قوت خود باقی بود . در این سال دومین قانون اصلاحی از تصویب گذشت ، سومین قانون در سال ۱۳۲۸ به تصویب رسید و در سال ۱۳۳۱ تغییراتی در آن صورت گرفت و بالاخره در سال ۱۳۲۸ با تغییرات دیگری از تصویب کمیسیون مجلسین وقت گذشت . مجددا به موجب اصلاحیه بهمن ماه ۱۳۴۵ پاره ای از مواد قانون مذکور اصلاح و مواد جدیدی به ان اضافه گردید

یکی از سازمان های مهم محلی شهرداری است که به منظور تامین وسائل و رفاه مردم از طریق ایجاد تاسیسات شهری و عمران و آباد در محدوده معین ایجاد می شود . شهرداری موسسه مستقلی است و دارای استقلال اداری و مالی و شخصیت حقوقی مجزا از دولت می باشد . امور استخدامی آن تابع مقررات خاص شهرداری است

در اکثر کشورها شهردار به وسیله آراء مردم شهر و از بین افرادبا لیاقت ، شایسته ، متخصص ، امانت دار و ... که به طور کلی صلاحیت اخلاقی و کاری را داشته باشد انتخاب می شود ولی در ایران علیرغم وجود قانون از گذشته تا حالا این مسئله عمل نشده است و شهردار از طرف استاندار به عنوان قائم مقام شورای شهر انتخاب و معرفی می گردد . اخیرا لایحه تشکیلات شوراهای شهر و روستا از جانب دولت (در تاریخ (۳۰/۱۰/۷۱تصویب و تقدیم مجلس شورای اسلامی گردیده است . لایحه مذکور در دو فصل با ۷۵ماده تنظیم و تدوین و به تصویب هیئت وزیران رسیده است.

مطابق با این لایحه شهرداران سراسر کشور با آراء مستقیم مردم انتخاب می شوند لایحه مذکور دخالت مستقیم احاد مردم در سرنوشت خویش را از طریق مشارکت گسترده و نظارت در امور مربوط به توسعه اقتصادی و سیاسی جامعه اسلامی و نیز محقق ساختن آنان و خواسته های ملی و منطقه ای به عنوان هدف دنبال می کند

در این لایحه چگونگی شکل گیری شوراهای اسلامی در سطح روستا –دهستان و شهر نیز ارائه شده است . بر اساس لایحه داده شده اعضای شورای روستا با رای مستقیم روستائیان انتخاب می شوند و اعضای شورای دهستان را اعضای شورای روستاها انتخاب می کنند

دهدار نیز با اخذ رای اعضای شورای دهستان انتخاب می شوند .اما در شهر اعضای شورای شهر ونیز شهرداران با آراء مستقیم مردم انتخاب می شوند

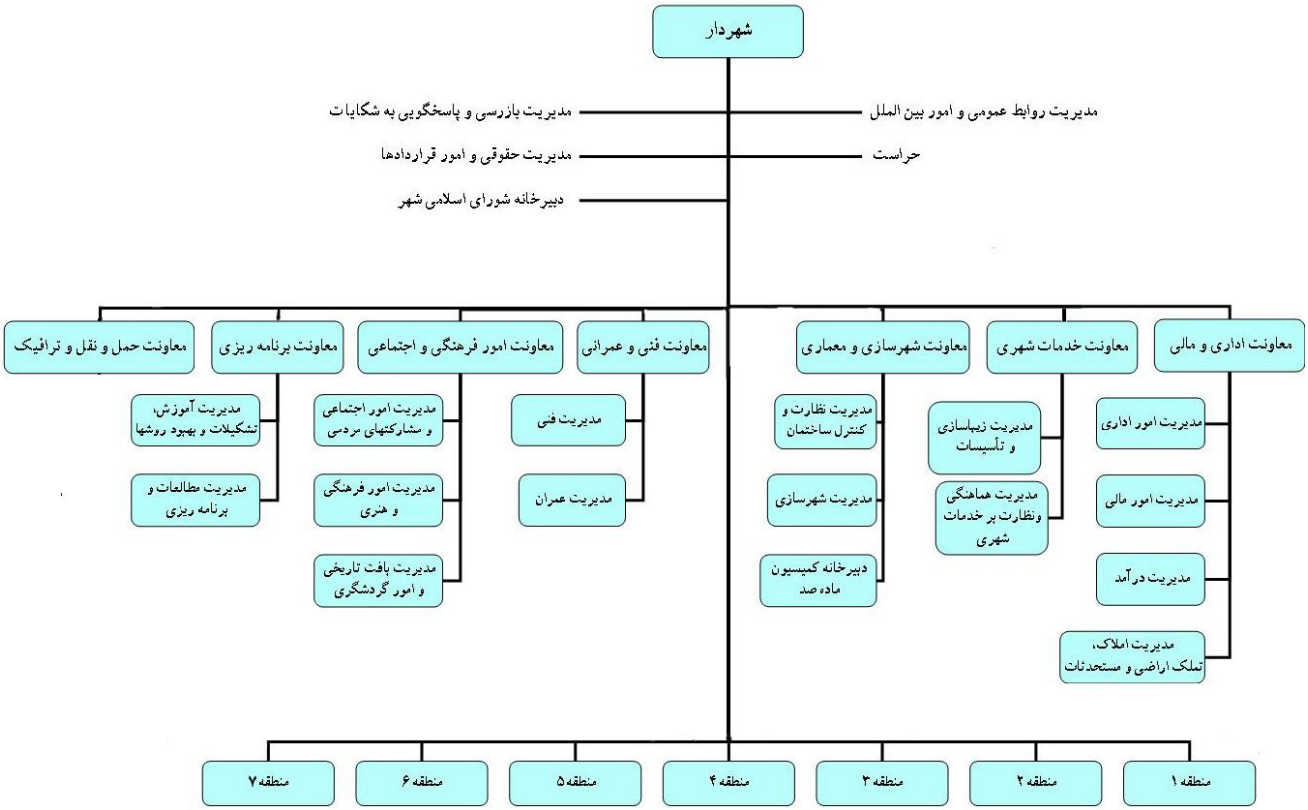
در این لایحه وظایفی نظیر سازمان دادن به فعالیت های مردمی برای برطرف کردن مشکلات ، بهبود وضع مناطق و همکاری و نظارت در امور عمرانی ، امدادی و فرهنگی برای شوراها پیش بینی شده است.

دهداران و شهرداران منتخب مردم بر اساس لایحه مذکور علاوه بر وظایف قانونی خود مصوبه های شورا ها را در حدود قانون اجرا می کنند.

تاریخچه شهرداری خوی

شهرداری خوی در سال ۱۳۰۷ هجری شمسی به دست استاد علی اکبر توانا (معمار مشهور خویی) در محل ساختمان قدیم شهرداری واقع در خیابان شهید صمد زاده (فعلی) تاسیس گردید. ملک شهرداری فعلی بصورت مشاعی (مشترک بین ملک مسجد و شهرداری) در اختیار شهرداری فعلی است .در ملک فعلی شهرداری در بیشه زار صدها درخت اصله تبریزی تنومند در محل قدیم شهرداری وجود داشت . به شهردار قدیم رئیس بلدیه شهر میگفتند . شهرداری در زمان ، ۵ الی ۶ نفر کارگر روز مزد داشت . و این کارگران (عمله) سپور بودند و کوچه ها را آب پاشی میکردند و جاروب میکردند . کوچه های شهر اکثراً خاکی بودند .در سال ۱۳۱۲ خیابان های اصلی شهر احداث شد (خیابان طالقانی و خیابان شریعتی)در سال ۱۳۱۶تنها در چند محل از شهر آسفالت وجود داشت از ۱۳۳۰ سر آغاز آسفالت خیابانهای شهر بوده است . وظایف شهرداری در بدو تشکیل بیشتر نظافت و رفت روب شهر بوده است . شهرداری در سال ۱۳۳۰ ، ۳۵ نفر کارمند و ۲۰ نفر کارگر داشته است . بیشتر منابع درآمدی شهرداری ، از وضع عوارض بوده است شهرداری بر امر آب ، برق ، نان ، گوشت ، بهداشت شهر با نظافت ، رفت و روب (خدمات شهری) نیز نظارت داشته است . در سال ۱۳۰۷ شهر خوی دارای پنج دروازه ورودی بوده و در هر کدام از این دروازه ها از ورود و خروج به شهر عوارض دریافت میگردید . از کالاهای وارداتی ، اجناس فروشی در میادین گندم ، نمک ، دواب عوارض دریافت میگردید . بعداً وظایف شهرداری توسعه یافته و به پروانه های ساختمانی و مغازه ها و سایر مجوزها از مردم عوارض دریافت میگردید . شهرداری از قدیم زیر نظر انجمن شهر فعالیت میکرد . فرمانداری مستاجر ۵ ساله در شهرداری خوی بوده است بصورت رایگان و در ساختمان قدیم شهرداری ادای وظیفه می نمود . تا سال ۱۳۳۰ بیشتر شعبات شهرداری در ساختمان قدیم اداری وظیفه می نمودند ع به تدریج در محوطه حیات قدیم ، ساختمان جدید مدن اضافه گردید . اختیارت شهرداری جامع بود.

چارت سازمانی



فصل دوم

ارزیابی بخش های مختلف

با رشته کارآموز

مقدمه :

امروزه گذران دوران تحصیل جز فرا گرفتن مطالب جزئی و پایه های مبتدی کار چیز دیگر نمی باشد و نخواهــد بود ؛ از این رو گذران ۲۴۰ ساعت کارآموزی نقطه قوتی بر جذب دانشجو در بازار کار و رسیدن به آرزو بزرگ میباشد.

در همین راستا اینجانب با گذران کارآموزی در قسمت شبکه و سایت شهرداری خوی سعی در فراگیری زیرساخت های کاری رشته را داشته ام اما با موانع و مشکلاتی روبرو گشته ام که ادامه مسیر را باریم سخت و نا بسامان کرد و امید است این روند تنها برای اینجانب بوده و دانشجویان دیگر مملکت عزیزمان از فرصت های مناسب کارآموزی کمال استفاده را داشته باشند.

متاسفانه در کشور ما از کار آموزی تعریف نامناسبی شده است ، چرا که من در پس ورود به دفتر کارآموزی شهرداری با سوالی مواجه گشته که موجب تعجباتم شده و روشن کردن این قضیه برای شما استادیار محترم حاکی از مشکلات کارآموز با کار کردن میباشد.

در محض ورود اینجانب از من سابقه کاری و تجربه کار در جامعه پرسیده شد تا به این طریق بتوانند از توان کاریم برای اهداف خود استفاده کنند و این بلعکس تصورات من از دوران کار آموزی بوده است.

حال به نظر شما از فردی مثل من که تجربه کاری ۳ ساله در اداره کافی نت و خدمات کامپیوتری را داشته چه توقعی خواهند داشت؟ جواب این سوال برای من سخت و عذاب آور بوده است ، چرا که بند ه تنها مسئول بررسی شبکه سایت های شهرداری ؛ جمع آوری اطلاعات و کتاب های الکترونیکی برای سایت جدید آنها شده ام و از خوشحالی این موقعیت مناسب در پوست خود نمیگنجم.

شاید این حالت برای یک کارآموز رشته کامپیوتر –نرم افزار عالی و فراتر از تصور بوده است چرا که بجای فرا گرفتن زیرساخت های شبکه با امکانات جالب برای سایت آشنا شده و بنده نیز تمام آنهارا در یک عدد لوح فشرده ضمینه این گزارش کرده ام.

اما اگر به همین موضوع بسنده میکردم جزء عذاب وجدان چیزی نسیبم نمیشود از این رو با سوالات مکرر از مسئولین شبکه سعی در فراگیری اتصالات شبکه و امنیت در فضای مجازی شده ام که با یک عدد وورد مواجه گشته و این تمام فرا گیری من از کارآموزی بودهاست که در ادامه مقدمه بر آن اشاره خواهم کرد.

با توجه به رشته کارآموزی در سازمان شهرداری ، کامپیوتر از الویت بالایی در انجام کارها از قبیل نقشه کشی و ثبت املاک و املاک واگذار شده به اشخاص دیگر و تایپ نامه های رسمی و اداری و ساماندهی پرونده های حقوقی شهرداری و... بر خوردار است کامپیوتر در سازمان باعث ایجاد نظم و هماهنگی و صرفه جویی در وقت شده است.

بررسی شرح وظایف رشته کارآموز در واحد صنعتی

وظایف رشته کارآموز در واحد صنعتی به شرح ذیل بوده است:

۱-شناسایی محل کار آموزی و آشنایی با واحد کار آموزی

۲-ثبت کامپیوتری املاک شهرداری

۳-ثبت کامپیوتری املا ک واگذار شده به اشخاص دیگر

۴- جمع بندی و ساماندهی نسبی پرونده های حقوقی شهرداری

۵-بررسی و تحلیل موضوع کار آموزی و موارد خواسته شده

امور جاری در دست اقدام

در حال حاضر تمام خیابانهایی که نیاز به جدول کثر داشته انجام گردیده و در برخی خیابانها که نیاز به مسیر گشایی وجود دارد شهرداری با تمام توان وارد عرصه شده و به میزان قابل توجهی از املاک واقع در مسیر را مصالحه و تا پایان سال نیز باقیمانده قطعات خریداری و مسیر گشایی انجام خواهد شد.

در موضوع خدمات شهری ، شهرداری نسبت به خرید چند دستگاه خودرو حمل زباله و یک دستگاه جاروب خیابانی اقدام نموده که این دستگاهها هنوز از این طریق مراجع به شهرداری تحویل نشده است که در صورت تحویل آن به شهرداری قسمت اعظم خیابانها به صورت مکانیزه رفت و روب خواهد شد .

افزایش فضای سبز و سرانه آن در سطح شهر در دوسال اخیر اقدامات قابل توجهی انجام شده است که نمونه آن را میتوان راه اندازی پارک چمران ، فضاهای سبز ورودی شهر از طرف ارومیه و خوی و... اشاره نمود.

خرید خودروی آتش نشانی ، احداث ایستگاه آتش نشانی ، خرید یک دستگاه کشنده چند منظوره، احداث چند دهنه پل، تکمیل کارخانه آسفالت ۱۶۰ تنی و نصب دستگاههای جانبی و خرید زمین جهت توسعه آتی آن و دهها پروژه دیگر ازجمله برنامه های اجرا شده و در دست اجرای شهرداری باشد.

برنامه های آینده

برنامه هایی نیز جهت بهره مندی شهروندان از امکانات شهری در دست مطالعه دارد که از جمله:

۱-جداسازی آب شرب از آب فضای سبز

۲-مطالعه ترافیک و حمل و نقل شهری و مکان یابی پارکینگ

۳-مطالعه مدیریت پسماند و زباله شهری و جمع آوری اصولی

۴-مطالعه اجرای فاز ۲ پارک دیلمان باغی

۵-مطالعه احداث مجتمع چند منظوره

تکنیک هایی که توسط رشته مورد نظر در واحد صنعتی به کار میرود

کامپیوتری کردن صدور پروانه با کمترین هزینه و بدون استفاده از پرینترهای حرارتی . در صورتی که در موارد مشابه احتیاج به نرم افزار مخصوص که بایستی با قیمت گزاف تهیه ، و با پرینترهای حرارتی با قیمت بالای ۲۰ میلیون ریال چاپ می شد .

تنظیم محاسبات برای صدور عوارض روزانه ساختمانی در محیط اکسل و استفاده بسیار ساده از برنامه مذکور بدون نیاز به نرم افزار مخصوص با قیمت بالا و مشکلات مربوط به یادگیری و استفاده از آن که در این زمینه آموزشهای لازم نیز به کاربران مربوطه داده شده است.

ثبت کلیه اطلاعات مربوط به صدور پروانه و پروانه های صادر شده بصورت فایل بر روی کامپیوتر و ارائه آمار ماهانه بصورت کامپیوتری و ایجاد بانک اطلاعاتی از پروانه های ساختمانی.

سایر مواردی که توسط کارآموزی به بررسی موارد فوق اختصاص یافته است

۱. ثبت املاک شهرداری و کلیه مصالحه ها و واگذاری های شهرداری در سنوات گذشته بر روی طرح تفصیلی و ثبت همزمان در دفتری جداگانه با شماره گذاری بر روی املاک که جزو ضروریات در حوزه املاک از دیر باز محسوب می شد ، که مورد نمونه به پیوست می باشد .

۲. تهیه نقشه بلوک بندی شهر بر روی طرح تفصیلی درخصوص ارزش منطقه ای که به عنوان نقشه مرجع در سطح سلماس شناخته شده و در تمامی ادارات شهر علاوه بر شهرداری مورد استفاده قرار می گیرد .

تطبیق طرح تفصیلی قدیم بر روی طرح تفصیلی جدید با اسکن کردن نقشه های طرح قدیم و جاگذاری برروی طرح جدید .(موارد مشابهی که در کمیته فنی کمیسیون ماده ۵ مورد استفاده قرار می گیرد.)

۳. بر آورد متراژ کلیه خیابانها و گذرها و معابر سطح شهر سلماس در اجرای دستور اداری درخصوص عوارض حق الارض.

فصل سوم

آزمون آموخته ها و نتایج

مراحل اولیه ایجاد امنیت در شبکه

شبکه های کامپیوتری زیر ساخت لازم برای عرضه اطلاعات در یک سازمان را فراهم می نمایند . بموازات رشد و گسترش تکنولوژی اطلاعات، مقوله امنیت در شبکه های کامپیوتری ، بطور چشمگیری مورد توجه قرار گرفته و همه روزه بر تعداد افرادی که علاقه مند به آشنائی با اصول سیستم های امنیتی در این زمینه می باشند ، افزوده می گردد . در این مقاله ، پیشنهاداتی در رابطه با ایجاد یک محیط ایمن در شبکه ، ارائه می گردد .

سیاست امنیتی

یک سیاست امنیتی، اعلامیه ای رسمی مشتمل بر مجموعه ای از قوانین است که می بایست توسط افرادیکه به یک تکنولوژی سازمان و یا سرمایه های اطلاعاتی دستیابی دارند، رعایت و به آن پایبند باشند . بمنظور تحقق اهداف امنیتی ، می بایست سیاست های تدوین شده در رابطه با تمام کاربران ، مدیران شبکه و مدیران عملیاتی سازمان، اعمال گردد . اهداف مورد نظر عموما با تاکید بر گزینه های اساسی زیر مشخص می گردند .

" سرویس های عرضه شده در مقابل امنیت ارائه شده ، استفاده ساده در مقابل امنیت و هزینه ایمن سازی در مقابل ریسک از دست دادن اطلاعات "

مهمترین هدف یک سیاست امنیتی ، دادن آگاهی لازم به کاربران، مدیران شبکه و مدیران عملیاتی یک سازمان در رابطه با امکانات و تجهیزات لازم ، بمنظور حفظ و صیانت از تکنولوژی و سرمایه های اطلاعاتی است . سیاست امنیتی ، می بایست مکانیزم و راهکارهای مربوطه را با تاکید بر امکانات موجود تبین نماید . از دیگر اهداف یک سیاست امنیتی ، ارائه یک خط اصولی برای پیکربندی و ممیزی سیستم های کامپیوتری و شبکه ها ، بمنظور تبعیت از سیاست ها است . یک سیاست امنیتی مناسب و موثر ، می بایست رضایت و حمایت تمام پرسنل موجود در یک سازمان را بدنبال داشته باشد .

یک سیاست امنیتی خوب دارای ویژگی های زیر است :

- امکان پیاده سازی عملی آن بکمک روش های متعددی نظیر رویه های مدیریتی، وجود داشته باشد .
- امکان تقویت آن توسط ابزارهای امنیتی ویا دستورات مدیریتی در مواردیکه پیشگیری واقعی از لحاظ فنی امکان پذیر نیست ، وجود داشته باشد .
- محدوده مسئولیت کاربران ، مدیران شبکه و مدیران عملیاتی بصورت شفاف مشخص گردد .
- پس از استقرار، قابلیت برقرای ارتباط با منابع متفاوت انسانی را دارا باشد . (یک بار گفتن و همواره در گوش داشتن)
- دارای انعطاف لازم بمنظور برخورد با تغییرات درشبکه باشد .(سیاست های تدوین شده ، نمونه ای بارز از مستندات زنده تلقی می گردنند .)

سیستم های عامل و برنامه های کاربردی : نسخه ها و بهنگام سازی در صورت امکان، می بایست از آخرین نسخه سیستم های عامل و برنامه های کاربردی بر روی تمامی کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده ، سوئیچ، روتر، فایروال و سیستم های تشخیص مزاحمین) استفاده شود . سیستم های عامل و برنامه های کاربردی می بایست بهنگام بوده و همواره از آخرین امکانات موجود بهنگام سازی (hotfixes , service pack , patches) استفاده گردد . در این راستا می بایست حساسیت بیشتری نسبت به برنامه های آسیب پذیر که زمینه لازم برای متجاوزان اطلاعاتی را فراهم می نمایند ، وجود داشته باشد .

برنامه های : BIND , Internet Explorer ,OutLook, IIS و sendmail بدلیل وجود نقاط آسیب پذیر می بایست مورد توجه جدی قرار گیرند . متجاوزان اطلاعاتی ، بدفعات از نقاط آسیب پذیر برنامه های فوق برای خواسته های خود استفاده کرده اند .

شناخت شبکه موجود

بمنظور پیاده سازی و پشتیبانی سیستم امنیتی ، لازم است لیستی از تمام دستگاههای سخت افزاری و برنامه های نصب شده ، تهیه گردد . آگاهی از برنامه هائی که بصورت پیش فرض نصب شده اند، نیز دارای اهمیت خاص خود است (مثلا" برنامه IIS بصورت پیش فرض توسط SMS و یا سرویس دهنده SQL در شبکه های مبتنی بر ویندوز نصب می گردد) . فهرست برداری از سرویس هائی که بر روی شبکه در حا ل اجراء می باشند، زمینه را برای پیمایش و تشخیص مسائل مربوطه ، هموار خواهد کرد .

سرویس دهندگان TCP/UDP و سرویس های موجود در شبکه تمامی سرویس دهندگان TCP/UDP در شبکه بهمراه سرویس های موجود بر روی هر کامپیوتر در شبکه ، می بایست شناسائی و مستند گردند . در صورت امکان، سرویس دهندگان و سرویس های غیر ضروری، غیر فعال گردند . برای سرویس دهندگانی که وجود آنان ضروری تشخیص داده می شود، دستیابی به آنان محدود به کامپیوترهائی گردد که به خدمات آنان نیازمند می باشند . امکانات عملیاتی را که بندرت از آنان استفاده و دارای آسیب پذیری بیشتری می باشند ، غیر فعال تا زمینه بهره برداری آنان توسط متجاوزان اطلاعاتی سلب گردد. توصیه می گردد ، برنامه های نمونه (Sample) تحت هیچ شرایطی بر روی سیستم های تولیدی (سیستم هائی که محیط لازم برای تولید نرم افزار بر روی آنها ایجاد و با استفاده از آنان محصولات نرم افزاری تولید می گردند) نصب نگردند .

رمزعبور

انتخاب رمزعبور ضعیف ، همواره یکی از مسائل اصلی در رابطه با هر نوع سیستم امنیتی است . کاربران، می بایست متعهد و مجبور به تغییر رمز عبور خود بصورت ادواری گردند . تنظیم مشخصه های رمز عبور در سیستم های مبتنی بر ویندوز، بکمک Account Policy صورت می پذیرد . مدیران شبکه، می بایست برنامه های مربوط به تشخیص رمز عبور را تهیه و آنها را اجراء تا آسیب پذیری سیستم در بوته نقد و آزمایش قرار گیرد .

برنامه های john the Ripper ، LOphtcrack و Crack ، نمونه هائی در این زمینه می باشند . به کاربرانی که رمز عبور آنان ضعیف تعریف شده است ، مراتب اعلام و در صورت تکرار اخطار داده شود (عملیات فوق، می بایست بصورت متناوب انجام گیرد) . با توجه به اینکه برنامه های تشخیص رمزعبور،زمان زیادی از پردازنده را بخود اختصاص خواهند داد، توصیه می گردد، رمز عبورهای کد شده (لیست SAM بانک اطلاعاتی در ویندوز) را بر روی سیستمی دیگر که در شبکه نمی باشد، منتقل تا زمینه بررسی رمزهای عبور ضعیف ، فراهم گردد . با انجام عملیات فوق برروی یک کامپیوتر غیر شبکه ای ، نتایج بدست آمده برای هیچکس قابل استفاده نخواهد بود(مگراینکه افراد بصورت فیزیکی به سیستم دستیابی پیدا نمایند) . برای تعریف رمز عبور، موارد زیر پیشنهاد می گردد :

- حداقل طول رمز عبور، دوازده و یا بیشتر باشد .
- دررمز عبور از حروف کوچک، اعداد، کاراکترهای خاص و Underline استفاده شود .
- از کلمات موجود در دیکشنری استفاده نگردد .
- رمز های عبور ، در فواصل زمانی مشخصی (سی و یا نود روز) بصورت ادواری تغییر داده شوند .
- کاربرانی که رمزهای عبور ساده و قابل حدسی را برای خود تعریف نموده اند، تشخیص و به آنها تذکر داده شود .(عملیات فوق بصورت متناوب و در فواصل زمانی یک ماه انجام گردد).

عدم اجرای برنامه ها ئی که منابع آنها تایید نشده است .

در اغلب حالات ، برنامه های کامپیوتری در یک چارچوب امنیتی خاص مربوط به کاربری که آنها را فعال می نماید ، اجراء می گردند.دراین زمینه ممکن است، هیچگونه توجه ای به ماهیت منبع ارائه دهنده برنامه توسط کاربران انجام نگردد . وجود یک زیر ساخت PKI (Public key infrastructure) ، در این زمینه می تواند مفید باشد . در صورت عدم وجود زیرساخت امنیتی فوق ،می بایست مراقبت های لازم در رابطه با طرفندهای استفاده شده توسط برخی از متجاوران اطلاعاتی را انجام داد. مثلا" ممکن است برخی آسیب ها در ظاهری کاملا" موجه از

طریق یک پیام الکترونیکی جلوه نمایند . هرگز یک ضمیمه پیام الکترونیکی و یا برنامه ای را که از منبع ارسال کننده آن مطمئن نشده اید ، فعال و یا اجراء ننمائید .

همواره از برنامه ای نظیر Outlook بمنظور دریافت پیام های الکترونیکی استفاده گردد . برنامه فوق در یک ناحیه محدوده شده اجراء و می بایست امکان اجرای تمام اسکریپت ها و محتویات فعال برای ناحیه فوق ، غیر فعال گردد .

ایجاد محدودیت در برخی از ضمائم پست الکترونیکی ضرورت توزیع و عرضه تعداد زیادی از انواع فایل های ضمیمه ، بصورت روزمره در یک سازمان وجود ندارد .بمنظور پیشگیری از اجرای کدهای مخرب ، پیشنهاد می گردد این نوع فایل ها ،غیر فعال گردند . سازمان هائی که از Outlook استفاده می نمایند، می توانند با استفاده از نسخه ۲۰۰۲ اقدام به بلاک نمودن آنها نمایند . (برای سایر نسخه های Outlook می توان از Patch امنیتی مربوطه استفاده کرد) .
فایل های زیر را می توان بلاک کرد :

نوع فایل هائی که می توان آنها را بلاک نمود .
.bas .hta .msp .url .bat .inf .mst .vb .chm .ins .pif .vbe .cmd .isp .pl .vbs .com .js .reg .ws .cpl .jse .scr .wsc .crt .lnk .sct .wsf .exe .msi .shs .wsh

در صورت ضرورت می توان ، به لیست فوق برخی از فایل ها را اضافه و یا حذف کرد. مثلا" با توجه به وجود عناصر اجرائی در برنامه های آفیس ، میتوان امکان اجرای برنامه ها را در آنان بلاک نمود . مهمترین نکته در این راستا به برنامه Access بر می گردد که برخلاف سایر اعضاء خانواده آفیس ، دارای امکانات حفاظتی ذاتی در مقابل ماکروهای آسیب رسان نمی باشد .

پایبندی به مفهوم کمترین امتیاز

اختصاص حداقل امتیاز به کاربران، محور اساسی درپیاده سازی یک سیتم امنیتی است. رویکرد فوق بر این اصل مهم استوار است که کاربران می بایست صرفا" دارای حقوق و امتیازات لازم

بمنظور انجام کارهای مربوطه باشند (بذل و بخشش امتیازات در این زمینه شایسته نمی باشد!) . رخنه در سیستم امنیتی از طریق کدهای مخربی که توسط کاربران اجراء می گردند، تحقق می یابد . در صورتیکه کاربر، دارای حقوق و امتیازات بیشتری باشد ، آسیب پذیری اطلاعات در اثر اجرای کدها ی مخرب ، بیشتر خواهد شد . موارد زیر برای اختصاص حقوق کاربران ، پیشنهاد می گردد :

- تعداد account مربوط به مدیران شبکه، می بایست حداقل باشد .
- مدیران شبکه ، می بایست بمنظور انجام فعالیت های روزمره نظیر خواندن پیام های پست الکترونیکی ، از یک account روزمره در مقابل ورود به شبکه بعنوان dministrator ،استفاده نمایند .
- مجوزهای لازم برای منابع بدرستی تنظیم و پیکربندی گردد . در این راستا می بایست حساسیت بیشتری نسبت به برخی از برنامه ها که همواره مورد استفاده متجاوزان اطلاعاتی است ، وجود داشته باشد . این نوع برنامه ها ، شرایط مناسبی برای متجاوزان اطلاعاتی را فراهم می نمایند. جدول زیر برخی از این نوع برنامه ها را نشان می دهد .

برنامه های مورد توجه متجاوزان اطلاعاتی
explorer.exe, regedit.exe, poledit.exe, taskman.exe, at.exe, cacls.exe,cmd.exe, finger.exe, ftp.exe, nbstat.exe, net.exe, net۱.exe,netsh.exe, rcp.exe, regedt۳۲.exe, regini.exe, regsvr۳۲.exe,rexec.exe, rsh.exe, runas.exe, runonce.exe, svrmgr.exe,sysedit.exe, telnet.exe, tftp.exe, tracert.exe, usrmgr.exe,wscript.exe,xcopy.exe

- رویکرد حداقل امتیاز ، می تواند به برنامه های سرویس دهنده نیز تعمیم یابد . در این راستا می بایست حتی المقدور، سرویس ها و برنامه ها توسط یک account که حداقل امتیاز را دارد ،اجراء گردند .

ممیزی برنامه ها

اغلب برنامه های سرویس دهنده ، دارای قابلیت های ممیزی گسترده ای می باشند . ممیزی می تواند شامل دنبال نمودن حرکات مشکوک و یا برخورد با آسیب های واقعی باشد . با فعال نمودن ممیزی برای برنامه های سرویس دهنده و کنترل دستیابی به برنامه های کلیدی نظیر برنامه هائی که لیست آنها در جدول قبل ارائه گردید، شرایط مناسبی بمنظور حفاظت از اطلاعات فراهم می گردد .

چاپگر شبکه

امروزه اغلب چاپگرهای شبکه دارای قابلیت های از قبل ساخته شده برای سرویس های FTP,WEB و Telnet بعنوان بخشی از سیستم عامل مربوطه ، می باشند . منابع فوق پس از فعال شدن ، مورد استفاده قرار خواهند گرفت . امکان استفاده از چاپگرهای شبکه بصورت Bound servers FTP ، Telnet و یا سرویس های مدیریتی وب ، وجود خواهد داشت . رمز عبور پیش فرض را به یک رمز عبور پیچیده تغییر و با صراحت پورت های چاپگر را در محدوده روتر / فایروال بلاک نموده و در صورت عدم نیاز به سرویس های فوق ، آنها را غیر فعال نمائید .

پروتکل (SNMP Simple Network Management Protocol)

پروتکل SNMP ، در مقیاس گسترده ای توسط مدیران شبکه بمنظور مشاهده و مدیریت تمام کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده، سوئیچ ، روتر، فایروال) استفاده می گردد .SNMP ، بمنظور تایید اعتبار کاربران ، از روشی غیر رمز شده استفاده می نماید . متجاوزان اطلاعاتی ، می توانند از نفطه ضعف فوق در جهت اهداف سوء خود استفاده نمایند . در چنین حالتی، آنان قادر به اخذ اطلاعات متنوعی در رابطه با عناصر موجود در شبکه

بوده و حتی امکان غیر فعال نمودن یک سیستم از راه دور و یا تغییر پیکربندی سیستم ها وجود خواهد داشت . در صورتیکه یک متجاوز اطلاعاتی قادر به جمع آوری ترافیک SNMP دریک شبکه گردد، از اطلاعات مربوط به ساختار شبکه موجود بهمراه سیستم ها و دستگاههای متصل شده به آن ، نیز آگاهی خواهد یافت . سرویس دهندگان SNMP موجود بر روی هر کامپیوتری را که ضرورتی به وجود آنان نمی باشد ، غیر فعال نمائید . در صورتیکه بهر دلیلی استفاده از SNMP ضروری باشد ، می بایست امکان دستیابی بصورت فقط خواندنی در نظر گرفته شود . در صورت امکان، صرفا" به تعداد اندکی از کامپیوترها امتیاز استفاده از سرویس دهنده SNMP اعطاء گردد .

تست امنیت شبکه

مدیران شبکه های کامپیوترهای می بایست، بصورت ادواری اقدام به تست امنیتی تمام کامپیوترهای موجود در شبکه (سرویس گیرندگان، سرویس دهندگان، سوئیچ ها ، روترها ، فایروال ها و سیتستم های تشخیص مزاحمین) نمایند. تست امنیت شبکه ، پس از اعمال هر گونه تغییر اساسی در پیکربندی شبکه ، نیز می بایست انجام شود .

مقدمه‌ای بر موضوعات اصلی امنیت در رابطه با تجارت الکترونیکی :

پس از ظهور اینترنت عمومی و تجارت الکترونیکی ، اگر کامپیوترهای خصوصی و همچنین شبکه‌های کامپیوتری بصورت مناسب محافظت نشده و ایمن نباشند ، به طرز افزایشی در خطر حملات خسارت بار قرار خواهند گرفت. Hacker ها ، ویروس‌ها ، کارمندان کینه‌جو و حتی خطاهای انسانی همگی بیانگر خطرات موجود و آشکار بر شبکه‌ها می‌باشند. و همه کاربران کامپیوتر ، از اکثر کاربران ساده اینترنتی گرفته تا کاربران شرکت‌های بزرگ می‌توانند بر اثر رخنه‌های موجود در امنیت شبکه تحت تاثیر قرار گیرند. با این وجود رخنه‌هایی که در امنیت شبکه وجود دارند به سادگی قابل پیشگیری می‌باشند. چگونه؟ تحقیق زیر یک دید عمومی در رابطه با معمول‌ترین تهدیدهای امنیتی شبکه و گامهایی که یک سازمان می‌تواند در جهت محافظت خود از این حملات و اطمینان از اینکه داده‌ای که از شبکه شما می‌گذرد ایمن خواهد بود ، داشته باشد ، ارایه می‌دهد.

اهمیت امنیت :

بدون شک اینترنت بزرگترین شبکه عمومی داده است که ارتباطات خصوصی و همچنین ارتباطات تجاری را در سرتاسر جهان مقدور ساخته و آن را تسهیل می‌کند. حجم ترافیکی که از اینترنت و شبکه‌های شرکتی عبور می‌کند هر روزه بطور نمایی توسعه و بسط پیدا می‌کند. ارتباطات از طریق پست الکترونیکی روز به روز افزایش پیدا می‌کند. کارمندان متحرک ، کارمندانی که هر روز در سفر می‌باشند و شعبات ادارات از اینترنت برای برقراری ارتباط با شبکه‌های شرکتی خود بهره می‌گیرند و معاملات تجاری که از طریق اینترنت و مخصوصاً شبکه جهانی به انجام می‌رسند ، قسمت عمده‌ای از سود شرکت‌ها را در بر دارند.

در حالی که اینترنت روش انجام معاملات تجاری را تغییر داده و باعث پیشرفت در آن می‌شود ، در مقابل این شبکه وسیع و تکنولوژی‌های مربوط به آن باعث باز شدن دری می‌شوند که تعداد زیادی خطرات امنیتی می‌توانند از آن وارد شوند و شرکت‌ها باید خود را در مقابل این حملات و خطرات آن محفوظ نگاه دارند. اگرچه حملات شبکه احتمالاً هنگامی جدی‌تر هستند که تجارتی را که داده‌های حساسی مانند داروهای شخصی یا سابقه مالی را ذخیره می‌کند ، مورد حمله قرار می‌دهند با این وجود نتیجه این حملات چه در صورت خرابی جزیی و چه خرابی کامل ، از بین رفتن اطلاعات مهم ، به مخاطره افتادن خصوصی‌بودن و ساعت‌ها و یا حتی روزها از کار افتادن شبکه خواهد بود.

با وجود خطرات هزینه‌بر شکاف‌های امنیتی ، اینترنت می‌تواند یکی از ایمن‌ترین راه‌های بکار بردن تجارت الکترونیکی باشد. به عنوان مثال دادن اطلاعات کارت اعتباری به یک فروشنده راه دور از طریق تلفن و یا به یک پیشخدمت در یک رستوران می‌تواند بسیار خطرناک‌تر از وارد کردن اطلاعات از طریق یک وب سایت باشد ، زیرا معاملات تجارت الکترونیکی عموماً با استفاده از تکنولوژی امنیتی محافظت می‌شوند. یک فروشنده راه دور و یا یک پیشخدمت همیشه قابل اعتماد و یا قابل پیگیری نمی‌باشند . البته هنوز ترس مشکلات مربوط به امنیت همان قدر در رابطه با تجارت مضر است که برای خطرات امنیتی واقعی می‌باشد. ترس و تردید عمومی در رابطه با کامپیوترها هنوز وجود دارند که همین مسئله باعث بی‌اعتمادی به اینترنت می‌شود. این بی‌اعتمادی می‌تواند باعث محدود کردن فرصت‌های تجاری شرکت‌ها ، مخصوصاً شرکت‌هایی که اساس آنها بر پایه Web می‌باشد ، بشود. بنابراین شرکت‌ها باید قوانین و مقررات امنیتی وضع کرده و از محافظ‌های امنیتی که بسیار موثر می‌باشند استفاده کنند. سازمان‌ها باید قادر به برقراری ارتباط مناسب در رابطه با توضیح چگونگی طرح و نقشه خود برای محافظت از مشتریانشان باشند. علاوه بر حفاظت از مشتریان، سازمان‌ها باید کارمندان و شرکای اقتصادی خود را نیز از خطرات امنیتی محفوظ دارند. اینترنت ، اینترانت‌ها و اکسترانت‌ها ارتباط سریع و موثر بین کارمندان و شرکای اقتصادی را فراهم می‌کنند. با این وجود چنین ارتباط و تاثیری می‌تواند به دلیل تاثیرات حملات شبکه از بین برود. یک حمله می‌تواند باعث از کار افتادن کارمندان و همچنین شبکه به دلیل بازیابی اطلاعات و یا تعمیر خرابی شود. واضح است که از دست دادن زمان و همچنین اطلاعات ارزشمند می‌تواند تاثیر به سزایی در فعالیت مفید کارمندان داشته باشد.

وضع قوانین نیز یکی دیگر از دلایلی است که باعث نیاز به امنیت در شبکه می‌شود. دولت‌ها اهمیت اینترنت و همچنین این حقیقت را که سهام اساسی و عمده تولید اقتصاد جهانی به اینترنت وابسته است را تصدیق می‌کنند. با این وجود آنها همچنین باز گذاشتن زیربنای اقتصادی جهان ، به گونه‌ای که توسط افراد جنایتکار مورد سو استفاده قرار گیرد را دلیل خطر و زیان اقتصادی بزرگی می‌دانند. بنابراین دولت‌های ملی قوانینی را جهت منظم ساختن جریان عظیم و وسیع اطلاعات الکترونیکی وضع می‌کنند. از این گذشته جهت مطابقت با قوانینی که دولت‌ها وضع نموده‌اند ، صنعت کامپیوتر یک سری استانداردهای امنیتی برای کمک به ایمن نمودن اطلاعات و اینکه آنها ایمن می‌باشند را تدارک دیده است. تجارتی که سیاست‌های امنیتی قابل اثبات جهت محافظت اطلاعات خویش نداشته باشد در مقام نقض این استانداردها بوده و مطابق با آن جریمه خواهد شد.

امنیت نامناسب شبکه معمولاً از ضعف پیاده‌سازی سیاست‌های امنیتی و همچنین ضعف بکارگیری از ابزارهای امنیتی موجود ناشی می‌شود. کامل نمودن تشخیص خطرات و تدارک نقشه‌ها و زیربناهای امنیتی جامع که توسط مدیریت فوقانی و بصورت عمومی قابل کنترل هستند ، امری بسیار حیاتی خواهد بود.

تهدیدهایی که در رابطه با داده‌ها می‌باشند:

مانند هر نوع جرم و جنایتی ، تهدیدهایی که در رابطه با اطلاعات محرمانه و بی‌عیب بودن آنها وجود دارد از طریق مجموعه کوچکی از بدکاران (کسی که از روی حماقت یا بدجنسی عملی را انجام می‌دهد) ناشی می‌شود. با این وجود در حالی که یک سارق اتومبیل در آن واحد تنها قادر به دزدیدن یک اتومبیل است ، یک Hacker که از یک کامپیوتر پایه کار خود را انجام می‌دهد قادر به تولید آسیب‌ها و زیان‌هایی برای گروه کثیری از شبکه‌های کامپیوتری می‌باشد که باعث ایجاد خرابی در سرتاسر جهان می‌شوند. شاید تعداد زیاد مزاحم‌ها دلیل این تفکر باشد که خطرات می‌توانند از اشخاصی که آنها را می‌شناسیم ناشی شده باشد. در واقع اکثر متخصصان در امنیت شبکه بر این باورند که اکثریت حملات شبکه توسط کارمندانی انجام می‌شود که در داخل سازمان ، جایی که شکاف‌ها و روزنه‌ها واقع شده‌اند ، می‌باشند . کارمندان از روی اذیت یا شرارت ، بدجنسی و یا اشتباه اغلب باعث ایجاد خرابی در شبکه شرکت خود و از بین بردن داده‌ها و اطلاعات می‌شوند. از این گذشته با وجود فراگیر بودن تکنولوژی‌های ارتباطی از راه دور ، تجارت نیز توسعه یافته و یک شرکت شامل تعداد بیشتری کارمندان در حال سفر ، شعبات شرکت و شرکای تجاری خواهد بود. این کارمندان راه دور و شرکا همان خطراتی را دارند که ممکن است یک کارمند داخلی شرکت داشته باشد. همچنین در صورتی که سیستم شبکه‌بندی راه دور آنها بطور مناسب محافظت نشده و قابل پیگیری نباشد ، خطر شکاف‌های امنیتی می‌تواند وجود داشته باشد. هنگام محافظت از یک ماشین ، یک خانه ، یک کشور و یا یک شبکه کامپیوتری ، داشتن دانش عمومی در رابطه با دشمن‌های بالقوه و همچنین چگونگی عملکرد آنها امری غیر قابل انکار می‌باشد.

دشمن‌ها چه کسانی هستند؟

Hacker ها :

عمومی‌ترین و خیال‌انگیزترین اصطلاحی است که به مشتاقان کامپیوتری که از دستیابی به کامپیوترها یا شبکه‌های دیگران احساس لذت می‌کنند اطلاق می‌شود. اکثر Hackerها به یک ورود ساده به کامپیوتر و بر جای گذاشتن یک رد پا که می‌تواند برنامه‌ای سرگرم‌کننده و یا پیام‌هایی بر روی صفحه آنها باشد ، بسنده می‌کنند. دیگر Hacker ها که اغلب به آنها Cracker گفته می‌شود خطرناک‌تر هستند ، زیرا باعث خرابی کل سیستم کامپیوتری ، دزدیدن و یا خراب کردن اطلاعات محرمانه ، تغییر صفحات وب و در نهایت ایجاد خلل در تجارت می‌شوند. بعضی از این Hackerهای تازه‌کار صرفاً بصورت مرتبط ابزارهای Hacking را قرار می‌دهند و بدون اینکه از آنها و چگونگی تاثیرشان اطلاع کاملی داشته باشند از آنها استفاده می‌کنند.

کارمندان بی‌اطلاع :

از آنجایی که کارمندان بر وظایف اصلی خود تمرکز دارند ، اغلب قوانین و استانداردهایی که مربوط به امنیت در شبکه می‌باشد را نادیده می‌گیرند. به عنوان مثال ممکن است اسامی رمزی را که بخاطر سپردن آنها آسان باشد را انتخاب کنند تا به سادگی و سهولت وارد شبکه‌های خویش شوند. اما چنین اسامی رمزی بسادگی قابل حدس زدن بوده و یا با استفاده از یک حسگر متداول ساده و یا یک برنامه و نرم‌افزار Cracking قابل دسترس ، توسط Hacker ها قابل شناسایی باشند. کارمندان می‌توانند باعث شکاف‌های امنیتی دیگری مانند ادغام تصادفی و یا پخش ویروس‌ها شوند. از متداول‌ترین راه‌های انتقال ویروس انتقال از طریق دیسکت فلاپی و یا ذخیره کردن فایل‌هایی از اینترنت می‌باشد. کارمندانی که عمل انتقال اطلاعات را از طریق دیسکت‌های فلاپی انجام می‌دهند می‌توانند بطور ناآگاهانه شبکه‌های سازمان خود را به ویروس‌هایی که از کامپیوترهای مرکز کپی و یا کتابخانه‌ها آمده‌اند ، آلوده کنند. آنها حتی ممکن است از اینکه ویروسی در حافظه کامپیوترشان مقیم شده است نیز خبر نداشته باشند. سازمان‌ها همچنین در خطر آلوده شدن توسط فایل‌هایی که از اینترنت گرفته می‌شوند قرار دارند. مثالی از این فایل‌ها می‌تواند گزارشات مربوط به Power Point باشد. بطرز حیرت‌آوری شرکت‌ها می‌بایست مراقب خطاهای انسانی نیز باشند. کارمندان چه کارکنان جزیی و چه کارکنان جدی کامپیوتر می‌توانند توسط اشتباهاتی نظیر نصب کردن نادرست برنامه‌های محافظ ویروس یا چشم‌پوشی از اخطارهایی که در رابطه با خطرات امنیتی می‌باشند ، شبکه را با خطراتی جدی مواجه سازند. ۹۱ درصد از

خطاهایی که کشف شده‌اند مربوط به نادرست استفاده کردن کاربران از امتیازات دسترسی به اینترنت بوده است.

کارمندان بداخلاق یا شاکی

علاوه بر خطاهای کارمندانی که می‌توانند باعث خرابی و صدمه دیدن شبکه شود ، نیروی بالقوه یک کارمند کینه‌جو و یا عصبانی نیز می‌تواند باعث تحمیل شدن خطا شود. کارمندان عصبانی ، اغلب کسانی که توبیخ می‌شوند ، برافروخته هستند و یا اخراج می‌شوند ممکن است بصورت انتقامی شبکه‌های سازمان خود را به ویروس آلوده کرده و یا از قصد فایل‌های مهم را پاک کنند. این گروه مخصوصاً خطرناک می‌باشند زیرا معمولاً ارزش شبکه بسته به اطلاعاتی است که از آن شبکه می‌گذرد ، جایی که اطلاعاتی با اولویت بالا قرار دارند و محافظ‌هایی از آنها حفاظت می‌کنند.

جاسوس‌ها

چه خشنود و چه ناراضی ، بعضی از کارمندان ممکن است کنجکاو و یا بدجنس باشند. کارمندانی که به عنوان " Snoops " شناخته می‌شوند از شرکت جاسوسی می‌کنند تا به داده‌های محرمانه دستیابی غیرمجاز داشته و به عنوان رقیبی برای اطلاعات غیر قابل دسترسی به شمار بروند. دیگران تنها به کنجکاوی‌های شخصی از طریق دسترسی به اطلاعات خصوصی مانند اطلاعات مالی ، ارتباطات بین دو همکار از طریق یک پست الکترونیکی عاشقانه و یا حقوق یک همکار بسنده می‌کنند. بعضی از این فعالیت‌ها می‌توانند بطور نسبی بی‌ضرر باشند ولی بقیه مانند بازدید از امور مالی خصوصی ، امور پزشکی و یا داده‌های منابع انسانی بسیار مهم وجدی هستند زیرا می‌توانند باعث خدشه‌دار شدن شهرت یک شرکت و یا باعث بدهکاری مالی برای آن بشوند.

دشمنان چه کارهایی می‌توانند بکنند؟

ویروس‌ها شناخته‌شده‌ترین تهدیدات امنیتی به شمار می‌روند زیرا اغلب در پوشش وسیعی پخش می‌شوند. ویروس‌ها برنامه‌های کامپیوتری هستند که توسط برنامه‌نویسان گمراه نوشته می‌شوند و برای تکرار خود (تولید مثل) جهت آلوده کردن کامپیوترها هنگام وقوع یک اتفاق خاص طراحی شده‌اند. به عنوان مثال

ویروس‌هایی که به ویروس‌های macro مشهور هستند خود را به فایل‌هایی که شامل دستورالعمل‌های macro (روتین‌هایی که می‌توانند بصورت خودکار تکرار شوند مانند ترکیب کردن در پست الکترونیکی) هستند الصاق می‌کنند و هر گاه این ماکرو اجرا می‌شود ، فعال می‌شوند. اثر بعضی از ویروس‌ها بطور نسبی بی‌خطر می‌باشد و فقط باعث ایجاد قطعی در کار ، مانند نمایش دادن یک پیغام خنده‌دار هنگام فشردن یک کلید خاص بر روی صفحه کلید ، می‌شوند. بقیه ویروس‌ها مخرب بوده و می‌توانند مشکلاتی از قبیل پاک کردن فایل‌های یک دیسک سخت و یا کند کردن یک سیستم ، ایجاد کنند.

یک شبکه تنها زمانی به ویروس آلوده خواهد شد که این ویروس از یک منبع خارجی از قبیل یک دیسکت فلاپی آلوده و یا یک فایل برگرفته شده از اینترنت انتقال یافته باشد. زمانی که یکی از کامپیوترهای شبکه آلوده به ویروس شود ، بقیه کامپیوترها نیز مستعد دریافت این ویروس خواهند بود.

برنامه‌های اسب تروآ

برنامه‌های اسب تروآ یا تروجان‌ها وسیله انتقال جهت کدهای مخرب می‌باشند. تروجان‌ها در نگاه اولیه بی‌خطر و یا برنامه‌های نرم‌افزاری سودمندی مانند بازی‌های کامپیوتری به نظر می‌رسند ولی در واقع دشمن پنهانی می‌باشند. تروجان‌ها قادر به پاک کردن داده‌ها ، ارسال نسخه‌هایی از خود به لیست‌های آدرس پست الکترونیکی و باز نمودن کامپیوتر جهت حملات بعدی ، می‌باشند. تروجان‌ها تنها از طریق کپی کردن برنامه اسب تروآ به یک سیستم از طریق دیسک یا گرفتن یک فایل از طریق اینترنت یا باز نمودن ضمیمه یک پست الکترونیکی انتقال پیدا می‌کنند. هیچکدام از برنامه‌های ویروس و یا برنامه‌های اسب تروآ از طریق خود متن پست الکترونیکی انتقال پیدا نمی‌کنند بلکه این مسئله از طریق ضمیمه پست الکترونیکی صورت می‌گیرد.

خرابکارها

سایت‌های وب از طریق توسعه برنامه‌های نرم‌افزاری مانند ActiveX و Java Appllet ها ظهور پیدا کردند. این ابزارها باعث اجرای جالب‌تر و بهتر سایت‌های وب از طریق فراهم نمودن متحرک‌سازی و دیگر ابزارهای خاص شدند. با این وجود ، سادگی انتقال این برنامه‌ها از اینترنت و اجرای آنها وسیله جدیدی جهت تحمیل کردن ضررها و زیان‌ها به دست می‌دهد. یک خرابکار برنامه نرم‌افزاری یا applet ی است که باعث ایجاد

خرابی در درجات مختلف می‌گردد. یک خرابکار تنها قادر به نابود کردن یک فایل یا قسمت عمده سیستم کامپیوتر خواهد بود.

حملات

انواع بیشماری از حملات به شبکه ثبت و شناسایی گردیده‌اند که بطور معمول در سه گروه عمومی طبقه‌بندی می‌شوند. این سه گروه عبارتند از : حملات اکتشافی ، حملات دستیابی و حملات عدم پذیرش سرویس (DoS).

- حملات شناسایی اساساً به فعالیت‌های جمع‌آوری اطلاعات توسط Hacker ها جهت گردآوردن داده‌ها برای به مخاطره انداختن شبکه در زمانی دیگر ، گفته می‌شود. معمولاً ابزارهای نرم‌افزاری از قبیل sniffer ها و scanner ها جهت بدست آوردن منابع شبکه و استخراج ضعف‌های بالقوه در شبکه‌های مورد هدف ، میزبان‌ها و برنامه‌های کاربردی مورد استفاده قرار می‌گیرند. به عنوان مثال نرم‌افزاری وجود دارد که بطور اختصاصی برای بدست آوردن اسامی رمز استفاده می‌شود. چنین نرم‌افزارهایی برای مسئول شبکه طراحی شده‌اند تا به کمک آنها اسامی رمز کسانی که آن را فراموش کرده‌اند و یا اسامی رمز افرادی که بدون گفتن اسم رمز خود از شرکت رفته‌اند را بازیابی کرده و یا تغییر دهد. اگر این نرم‌افزار در دستان یک شخص نالایق قرار گیرد می‌تواند به یک اسلحه خطرناک تبدیل شود.
- حملات دستیابی جهت استخراج نقاط آسیب‌پذیر در نواحی شبکه مانند سرویس‌های تشخیص هویت یا پروتکل انتقال فایل (FTP) برای دسترسی به ورودی اعتبار پست الکترونیکی ، بانک‌های اطلاعاتی و دیگر اطلاعات محرمانه ، انجام می‌گیرند.
- حملات DoS باعث جلوگیری از دسترسی به یک یا تمام قسمت‌های یک سیستم کامپیوتری می‌شوند. آنها معمولاً از طریق ارسال حجم زیادی از اطلاعات درهم و برهم و یا کنترل نشده به سمت ماشینی که به شبکه یک سازمان یا اینترنت متصل می‌باشد باعث مسدود کردن عملیات ترافیکی عادی و معمولی می‌شوند. حالت بدتر DoS ، DoS توزیعی یا DDoS می‌باشد که در آن حمله‌کننده ، ماشین‌ها یا میزبان‌های متعددی را با خطر مواجه می‌سازد.

جلوگیری از اطلاعات

اطلاعاتی که از طریق هر نوع شبکه انتقال پیدا می‌کند می‌تواند تحت کنترل افراد یا بخش‌های نامعتبر جهت جلوگیری از به مقصد رسیدن داده‌ها قرار گیرد. این افراد ممکن است در حال استراق سمع ارتباطاتمان و یا تغییر دادن پاکت‌های داده در حال انتقال باشند. این افراد مقصر می‌توانند از روش‌های مختلفی جهت قطع ارتباط داده‌ای استفاده کنند. به عنوان مثال روش IP Spoofing ، در عمل انتقال با استفاده از آدرس پروتکل اینترنت (IP) یکی از دریافت‌کنندگان داده ، خود را به جای شخصی که معتبرسازی شده است جا می‌زند.

مهندسی اجتماعی

مهندسی اجتماعی یکی از متداول‌ترین روش‌های جمع‌آوری اطلاعات امنیتی محرمانه شبکه از طریق راه‌های غیر تکنیکی می‌باشد که روز به روز نیز در حال افزایش است. به عنوان مثال یک مهندس اجتماع ممکن است خود را به عنوان یک پشتیبان فنی جا زده و بر اساس تماس‌هایی که با کاربران می‌گیرد اطلاعات اسامی رمز آنها را جمع‌آوری کند. مثال‌های دیگری از مهندسی اجتماع می‌تواند رشوه دادن به یک کارمند جهت بدست آوردن دسترسی به سرور یا جستجوی اداره یک همکار جهت پیدا کردن اسم رمزی که در یک مکان مخفی نوشته شده است ، باشد.

Spam

Spam واژه متداول جهت پست الکترونیکی غیر درخواستی و یا عمل انتشار پیام آگاهی غیر درخواستی از طریق پست الکترونیکی می‌باشد. Spam معمولاً بی‌خطر می‌باشد ، ولی می‌تواند به دلیل هدر دادن زمان و فضای ذخیره‌سازی دریافت‌کننده ، مزاحم باشد.

ابزارهای امنیتی

پس از شناسایی منابع بالقوه تهدیدات و انواع زیان‌های ناشی از آنها ، انتخاب سیاست امنیتی مناسب و استفاده از محافظ‌ها در مکان مناسب آسانتر و ساده‌تر خواهد بود. سازمان‌ها طیف وسیعی از تکنولوژی‌ها را جهت محافظت تمامی نواحی یک شبکه در اختیار می‌گذارند. این تکنولوژی‌ها می‌توانند شامل بسته‌های نرم‌افزاری ضد ویروس یا سخت‌افزار اختصاصی جهت امنیت شبکه مانند دیوارهای آتش و سیستم‌های ردیابی ورود و خروج غیر مجاز باشند. پس از انتخاب چنین راه‌حل‌هایی ، می‌توانیم از ابزارهایی جهت تشخیص آسیب‌پذیری‌های امنیتی بصورت متناوب استفاده کنیم. بعلاوه می‌توانیم با استخدام کردن مشاوران حرفه‌ای در امر شبکه جهت کمک در طراحی راه‌حل امنیتی مناسب جهت شبکه و یا حصول اطمینان از ایمن و بروز بودن راه‌حل امنیتی موجود بهره بگیریم. با وجود انتخاب‌های موجود و قابل دسترس کنونی ، پیاده‌سازی یک زیرساختار امنیتی که محافظت کافی در اختیار می‌گذارد بدون در نظر گرفتن نیاز سریع به دسترسی به اطلاعات امکان‌پذیر می‌باشد. (یعنی دسترسی سریع نادیده گرفته نمی‌شود)

ده نکته مهم امنیتی

۱. تشویق کردن یا درخواست کردن از کارمندان جهت انتخاب اسم رمزی که مشخص و آشکار نباشد.
۲. درخواست از کارمندان جهت تعویض اسم رمز خود هر سه ماه یک بار.
۳. اطمینان از اینکه اشتراک محافظ ویروس در جریان می‌باشد.
۴. مطلع ساختن کارمندان از خطرات ضمیمه‌های پست الکترونیکی.
۵. پیاده‌سازی یک راه‌حل کامل و جامع در رابطه با امنیت شبکه.
۶. بررسی وضعیت امنیتی بصورت متناوب.
۷. پس از ترک کارمند از شرکت ، بلافاصله دسترسی او به شبکه را از بین ببریم.
۸. اگر به مردم اجازه کار از خانه را می‌دهیم بایستی از یک سرور ایمن با مدیریت مرکزی جهت ترافیک راه دور استفاده کنیم.
۹. بروزرسانی نرم‌افزار وب سرور بطور منظم.
۱۰. به هیچ وجه سرویس‌های شبکه غیر ضروری را اجرا نکنیم.

بسته‌های نرم‌افزارهای ضد ویروس

نرم‌افزار محافظت از ویروس همراه اکثر کامپیوترها موجود می‌باشد و می‌تواند اکثر تهدیدات ویروسی را در صورت بروز رسانی منظم و استفاده صحیح از بین ببرد. صنعت ضد ویروس بر شبکه‌ای از کاربران تکیه کرده تا اخطارهای اولیه در رابطه با ویروس‌های جدید را تدارک ببیند ، بنابراین پادزهرها براحتی قابل توزیع و گسترش خواهند بود. با تولید هزاران ویروس در هر ماه ، بروز نگهداری بانک اطلاعاتی امری بنیادی و اساسی خواهد بود. بانک اطلاعاتی ویروس پیشینه‌ای است که توسط بسته ضد ویروس جهت شناسایی ویروس‌های شناخته شده هنگام حمله مورد استفاده قرار می‌گیرد. فروشندگان مشهور و قابل اطمینان بسته‌های نرم‌افزاری ضد ویروس ، جدیدترین پادزهرها را در وب سایت خود قرار می‌دهند ، و نرم‌افزار مربوطه قادر به اعلان متناوب به کاربر جهت گردآوری اطلاعات جدید می‌باشد. سیاست امنیت شبکه باید تصریح کند که تمامی کامپیوترهای موجود در شبکه بروزرسانی می‌شوند و اگر همگی توسط یک بسته ضد ویروس محافظت شوند ایده‌آل خواهد بود زیرا هزینه نگهداری و بروزرسانی آنها حداقل می‌باشد. همچنین بروز نگهداری خود نرم‌افزار نیز امری اساسی است. ویروس‌نویسان اغلب اولویت اول خود را بر گذشتن از بسته‌های ضد ویروس قرار می‌دهند.

سیاست‌های امنیتی

هنگام برپایی یک شبکه ، چه یک شبکه داخلی (LAN) ، چه یک شبکه داخلی مجازی (VLAN) و چه یک شبکه گسترده (WAN) ، اهمیت برپایی سیاست‌های امنیتی پایه در ابتدا بسیار مهم می‌باشد. سیاست‌های امنیتی قوانینی هستند که بصورت الکترونیکی ، در داخل تجهیزات امنیتی جهت کنترل چنین مناطقی از نقطه نظر حق و امتیاز دسترسی ، برنامه‌ریزی و ذخیره‌سازی شده‌اند. البته سیاست‌های امنیتی همچنین قواعد مکتوب و یا شفاهی هستند که یک سازمان بر اساس آنها عمل خود را انجام می‌دهد. بعلاوه شرکت‌ها بایستی شخصی را جهت اجرا کردن و مدیریت این سیاست‌ها برگزینند و تصمیم بگیرند که کارمندان چگونه باید از قوانین مطلع شده و بر محافظ‌ها نظارت داشته باشند.

سیاست‌ها چه می‌باشند؟

سیاست‌هایی که پیاده‌سازی می‌شوند باید بر این مسئله که چه کسانی بر چه محیط‌هایی دسترسی دارند و اینکه چگونه باید از ورود کاربران نامعتبر به محیط‌های ممنوع جلوگیری به عمل آید ، کنترل داشته باشند. به عنوان مثال ، عموماً ، تنها اعضای بخش منابع انسانی به سابقه حقوقی کارمندان دسترسی دارند. معمولاً اسامی رمز در صورتی که خصوصی باقی بمانند ، از ورود کارمندان به محیط‌های ممنوعه جلوگیری به عمل می‌آورند. سیاست‌های مکتوب و همچنین اخطارهایی که در رابطه با ارسال اسامی رمز در محیط‌های کاری صورت می‌گیرند ، اغلب شکاف‌های امنیتی را می‌بندند. مشتریان یا کارپردازانی که به قسمت‌های مهم شبکه دسترسی دارند باید توسط این سیاست‌ها بطور مناسب کنترل و بازدید شوند.

چه کسی مسوول اجرا و مدیریت این سیاست‌ها می‌باشد؟

شخص یا گروهی از اشخاص که مسوول حفظ و نگهداری شبکه و امنیت آن می‌باشند باید به تمام مناطق شبکه دسترسی داشته باشند. بنابراین عملیات مدیریت سیاست امنیتی باید به دست افرادی که فوق‌العاده قابل اطمینان و دارای صلاحیت‌های تکنیکی لازم می‌باشند ، سپرده شود. همانطور که قبلاً نیز گفته شد اکثر روزنه‌ها و شکاف‌های امنیتی از داخل شبکه ایجاد می‌شوند ، بنابراین این فرد یا گروه نباید به عنوان یک تهدید به شمار آیند. مدیران شبکه باید از ابزارهای نرم‌افزاری جهت تعریف ، توزیع ، اجرا و رسیدگی به سیاست‌های امنیتی از طریق رابط‌های بر پایه مرورگر سود بجویند.

چگونه می‌توان با سیاست‌ها ارتباط برقرار نمود؟

اساساً سیاست‌ها هنگامی که طرف‌های درگیر آنها را نشناخته و درک نکنند ، بی‌فایده خواهند بود. داشتن مکانیزم‌های بجا و موثر جهت انتقال سیاست‌های موجود ، تغییر آنها و سیاست‌های جدیدتر و هشدارهای امنیتی در مورد ویروس‌ها و حملات تهدیدآمیز بسیار حیاتی می‌باشند.

هویت

به محض اتخاذ سیاست‌ها ، روش‌ها و فن‌آوری‌های هویتی باید به کار گرفته شوند تا به گونه‌ای مثبت هویت کاربران و امتیازهای دسترسی آنها را تایید کنند.

اسامی رمز

حصول اطمینان از اینکه برخی نواحی شبکه از لحاظ اسم رمز حفاظت شده‌اند و تنها برای کسانی که اسم رمز خاصی دارند قابل دسترسی می‌باشند ، یکی از ساده‌ترین و رایج‌ترین روش‌هایی است که این اطمینان را بوجود می‌آورد که تنها کسانی که مجوز دارند می‌توانند وارد بخش ویژه‌ای از یک شبکه شوند. در مقیاس فیزیکی امنیت ، اسامی رمز همانند کارت‌های دسترسی امضا شده و برجسته می‌باشند. اگر چه قویترین زیرساختارهای امنیتی شبکه نیز چنانچه افراد از اسامی رمز خود محافظت نکنند ، عملاً بی‌فایده خواهد بود. بسیاری از کاربران اعداد و یا کلماتی که به سادگی به یاد می‌آورند را به عنوان اسم رمز خود انتخاب می‌کنند برای مثال روز تولد ، شماره تلفن و اسامی حیوانات خانگی؛ برخی نیز هیچگاه اسم رمز خود را تغییر نمی‌دهند و اصلاً دقت نمی‌کنند که آنها را به صورت سر نگهداری کنند. قوانین یا تدابیر طلایی در رابطه با کلمات عبور عبارتند از :

- اسامی رمز خود را بصورت منظم تغییر دهید
- تا جاییکه امکان دارد کلمات رمز را بی‌معنی انتخاب کنید
- مادامیکه آن شرکت را ترک نکرده‌اید ، اسم رمز را افشا نکنید

در آینده احتمال دارد که Biometric ها جایگزین اسامی رمز شوند. یعنی بکارگیری فن‌آوری که کاربران را طبق خصوصیات فیزیکی آنها همچون اثر انگشت ، شکل چشم و یا صدا از یکدیگر متمایز می‌کند.

مدارک دیجیتالی

گواهی‌های دیجیتالی یا گواهی‌های کلید عمومی معادل‌های الکترونیکی برای گواهی‌نامه‌های رانندگی یا پاسپورت‌هایی است که بوسیله مسوولان اعطای گواهی‌نامه صادر می‌شوند. گواهی‌های دیجیتالی بیشتر اوقات جهت تعیین هویت به هنگام ایجاد تونل‌های امنیتی از طریق اینترنت مانند VPN به کار می‌روند.

کنترل دسترسی

قبل از امکان دسترسی کاربر به شبکه با اسم رمز خود ، شبکه باید اعتبار اسم رمز را ارزیابی کند. سرورهای کنترل دسترسی بر مبنای پرونده ذخیره شده کاربر اعتبار و هویت او را تعیین کرده و نواحی و اطلاعاتی که می‌تواند به آنها دسترسی داشته باشد را تعیین می‌کنند. در مقیاس فیزیکی امنیت ، سرورهای کنترل دسترسی معادل نگهبان دری می‌باشند که استفاده کارت‌های دسترسی را چک کرده و کنترل می‌کند.

دیوارهای آتش

یک دیوار آتش راه‌حل سخت‌افزاری یا نرم‌افزاری است که در زیرساختار یک شبکه تعبیه شده است تا سیاست‌های امنیتی سازمان را با محدود کردن دسترسی به منابع خاص شبکه به اجرا در آورد. در مقیاس فیزیکی امنیت ، یک دیوار آتش معادل قفلی است که بر روی در ورودی یا در اتاقی در داخل ساختمان که تنها کاربران مجاز همانند کسانی که کلید یا کارت دسترسی ورود دارند ، قرار دارد.

تکنولوژی دیوار آتش حتی در نسخه‌هایی برای استفاده در منازل نیز موجود می‌باشد. دیوارهای آتش لایه محافظی بین شبکه و دنیای خارج بوجود می‌آورند. در حقیقت دیوار آتش در نقطه ورودی شبکه را نسخه‌برداری می‌کند ، بطوریکه می‌تواند داده‌های مجاز را بدون تاخیر محسوس دریافت و انتقال دهد. با این وجود دیوار آتش دارای فیلترهای ساخته‌شده‌ای در داخل است که می‌توانند از ورود محتویات غیر مجاز و یا اساساً خطرناک به سیستم جلوگیری به عمل آورند. همچنین دیوار آتش تلاش‌های جهت ورود به سیستم را ثبت کرده و به مسئولین شبکه گزارش می‌دهد.

کدگذاری

تکنولوژی کدگذاری اطمینان می‌دهد که پیام‌ها نمی‌توانند بوسیله کسی غیر از دریافت‌کننده مجاز خوانده یا دزدیده شوند. معمولاً کدگذاری برای حفظ داده‌هایی که در یک شبکه عمومی انتقال پیدا می‌کنند ، به کار گرفته می‌شود و از الگوریتم‌های ریاضی پیشرفته جهت بهم ریختن پیام و ملحقات آن استفاده می‌کند. الگوریتم‌های کدگذاری متعددی وجود دارند که بعضی از آنها ایمن‌تر هستند. کدگذاری امنیت لازم برای پشتیبانی از فن‌آوری مشهور VPN را فراهم می‌کند. VPN ها ارتباط‌های خصوصی یا تونل‌هایی بر روی

شبکه‌های عمومی نظیر اینترنت می‌باشند. آنها جهت برقراری ارتباط بین کارکنان در حال سفر ، کارکنان متحرک ، شعبات ادارات و شرکای تجاری به کار گرفته می‌شوند. کلیه قطعات سخت‌افزاری و نرم‌افزاری VPN از فن‌آوری پیشرفته کدگذاری جهت انتقال داده‌ها در شدیدترین شرایط امنیتی ، حمایت به عمل می‌آورند.

تشخیص ورود و خروج بدون اجازه

سازمان‌ها بکارگیری دیوارهای آتش را به عنوان نگهبان‌های دروازه مرکزی ادامه می‌دهند تا از ورود کاربران غیر مجاز به شبکه‌ها خودداری به عمل آورند. اگر چه امنیت شبکه از بسیاری لحاظ شبیه امنیت فیزیکی است ، با این وجود هیچ تکنولوژی برای تمامی نیازها جوابگو نمی‌باشد – لیکن یک دفاع لایه‌ای بهترین نتیجه را خواهد داد. سازمان‌ها بطور فزاینده‌ای به فن‌آوری‌های امنیتی اضافی جهت کاهش خطر و آسیب‌پذیری که دیوارهای آتش به تنهایی نمی‌توانند فراهم کنند ، چشم دوخته‌اند. یک سیستم آشکارسازی ورود و خروج غیر مجاز بر اساس شبکه ، بر تمامی شبکه نظارت می‌کند. یک IDS جریان داده‌های پاکت در یک شبکه را بررسی می‌کند ، و فعالیت‌های غیرمجاز نظیر حملات Hacker ها را جستجو می‌کند و به کاربران این امکان را می‌دهد تا به ایجاد شکاف‌های امنیتی قبل از انجام توافقات با سیستم‌ها پاسخ دهند. زمانی که فعالیت غیر مجازی آشکار می‌شود ، IDS می‌تواند اخطارهایی را با جزییات فعالیت برای مسئولین شبکه ارسال کند و اغلب به سایر سیستم‌ها نظیر راهبرها فرمان دهد تا جلسات غیر مجاز را قطع کنند. در مقیاس فیزیکی امنیت ، یک IDS معادل یک دوربین ویدئویی و حس‌گر حرکت می‌باشد که فعالیت‌های غیر مجاز را آشکار ساخته و با سیستم‌های پاسخ‌دهی اتوماتیک همانند نگهبان‌ها جهت متوقف ساختن فعالیت غیرمجاز همکاری به عمل می آورد.

اسکنرهای شبکه

اسکنرهای شبکه تجزیه و تحلیل‌هایی را بر روی سیستم شبکه شده اعمال می‌کنند تا کشفیات الکترونیکی را گرد آورده و آسیب‌پذیری‌ها را آشکار سازند که این خود می‌تواند منجر به یک خطر امنیتی شود. این فن‌آوری به مسئولین و مدیران شبکه اجازه می‌دهد تا ضعف‌های امنیتی را قبل از آنکه متجاوزین از آنها بهره‌برداری کنند ، شناسایی کرده و درست کنند. در مقیاس فیزیکی امنیت ، اسکن کردن همانند قدم زدن در طی زمان‌های تعیین

شده در محوطه می‌باشد تا از قفل بودن درها و پنجره‌ها اطمینان حاصل کنیم. اسکن کردن کمک می‌کند تا خطر را ارزیابی و درک کنیم تا بتوانیم اقدامات تصحیحی را انجام دهیم.

نظریه فنی

در حالیکه ابزارهای اسکن الکترونیکی می‌توانند در آشکار ساختن ضعف‌های امنیتی شبکه بسیار مهم باشند ، یک ارزیابی امنیتی که توسط مشاورین امنیتی صورت می‌پذیرد می‌تواند مکمل خوبی برای آنها باشد. یک ارزیابی امنیتی یک تجزیه و تحلیل متمرکز از نگهبان امنیتی یک شبکه می‌باشد که ضعف‌ها و آسیب‌پذیری‌های امنیتی که می‌بایست درست شوند را پیدا می‌کند. ارزیابی‌های دوره‌ای در طول تغییرات مکرر در یک شبکه جهت اطمینان از اینکه نگهبان شبکه ضعیف نشده باشد ، مفید خواهند بود. در مقیاس فیزیکی امنیت ، ارزیابی امنیت دوره‌ای مانند اسکن کردن همانند نگهبانی است که بصورت دوره‌ای ناحیه ایمن را کنترل می‌کند ، قفل‌ها و پنجره‌ها را چک کرده و هرگونه مسئله غیر عادی که امکان وجودش باشد را گزارش می‌کند و برای تصحیح آنها راهنمایی را ارائه می‌دهد.

نتیجه

همانگونه که زمان پیش می‌رود ، فن‌آوری جدیدتری بوجود خواهد آمد که کارآیی تجارت و ارتباطات را بهبود خواهد بخشید. در همین حال دستاوردها در فن‌آوری حتی امنیت شبکه بیشتری را فراهم خواهند کرد. بنابراین اذهان بیشتری در محیط‌های تجارت الکترونیکی عمل خواهند کرد.