ثبت‌کنندگان چت و ایمیل

این ثبت‌کنندگان یک کپی متنی از تمام ایمیلهای واردشونده و خارج‌شونده و چتها تهیه می‌کنند. یک جاسوس خانگی به کرات از این روش استفاده می‌کند.

ثبت‌کنندگان کلید و کلمات عبور

هنگامی که شما مشغول کار با کامپیوتر هستید، یک نفر بالای سر شما ایستاده است و اعمال شما را نظارت می‌کند! ثبت‌کننده کلمه عبور این کار را می‌کند یعنی کلمات عبور تایپ‌شده را ردگیری می‌کند. اما ثبت‌کننده کلید تمام آنچه را که تایپ می‌شود، ثبت می‌کند.

حشرات وبی!

حشرات وبی بعنوان جاسوسان تبلیغ‌کننده یا نرم‌افزارهای تبلیغ شناخته می‌شوند. هنگامی که شما چنین نرم‌افزاری روی کامپیوتر خود دارید، بعد از انجام بعضی کارها، مانند تایپ کردن عباراتی در یک موتور جستجو، پنجره‌های بازشونده تبلیغاتی خاصی را مرتبط با عناوین مورد جستجو دریافت می‌کنید. این تبلیغات حتی گاهی می‌توانند زمانی که به اینترنت متصل نیستید، بر روی صفحه شما ظاهر شوند. اگر بطور پیوسته زیربار

صفحات تبلیغاتی قراردارید، احتمالا یک حشره وبی بر روی کامپیوتر شما نصب شده است.

مرورگر ربایان!

بعضی‌ها کامپیوتر شما را برای استفاده خودشان بخدمت می‌گیرند ـ کاربران نرم‌افزارهای جاسوسی می‌توانند اتصال شما را برای ارسال اسپم‌هایشان از طریق سرویس‌دهنده‌اینترنت شما، بربایند!!! به این معنی که یک اسپم‌ساز انگل می‌تواند هزاران ایمیل اسپمی را از طریق اتصال کامپیوترتان به اینترنت و آدرس ISP شما، ارسال کند. دسترسیهای با سرعت و حجم بالا به اینترنت معمولا هدف این نوع کاربران قرار می‌گیرند. اغلب قربانیان متوجه نمی‌شوند که از اعتبار آنها سوءاستفاده شده است، تا اینکه به خاطر شکایت علیه اسپم‌ها، سرویس‌دهنده‌اینترنت اتصالشان را قطع کند.

مودم ربایان!

اگر برای اتصال به اینترنت از یک مودم و خط تلفن استفاده می‌کنید، یک فرد بی‌مرام! ممکن است قادر باشد یک شماره‌گیر آنلاین برای برقراری یک اتصال جدید اینترنت بر روی کامپیوتر شما نصب کند. این اتصال ممکن است یک اتصال راه دور با هزینه بالا باشد. هنگامی که قبض تلفن بدستان میرسد، به شما شک وارد خواهد شد. این نرم‌افزارهای جاسوسی اغلب داخل اسپم و ایمیلهای مربوط به امور جنسی قرار دارند. بازکردن ایمیل میتواند بصورت سهوی باعث آغاز نصب شماره‌گیر شود. این افراد بدذات! که پی‌گیریشان کار آسانی نیست، روی این حقیقت حساب می‌کنند که شما قبض تلفن را قبل از اینکه فرصت پیگیری داشته باشید، پرداخت می‌کنید.

PC ربایان!

PCربایان میانبرهای(shortcuts) اینترنتی را در فولدر Favorites شما بدون خبردادن به خودتان قرار میدهند. این میانبرها باعث می‌شوند که بسیاری بطور اتفاقی از وب‌سایتشان دیدن کنید و به این ترتیب بصورت تصنعی آمار ترافیک سایت خود را بالا می‌برند. این اتفاق به آنها اجازه دریافت مبالغ بیشتری را بابت تبلیغات در سایتشان می‌دهد که هزینه پرداخت‌شده آن در واقع زمان و پهنای باندی است که از شما گرفته می‌شود. ممکن است بتوانید با تغییر انتخابهای اینترنت خود از دست این Fovorites کاذب رها شوید، اما گاهی تنها راه خلاص شدن از شر این لینکهای مزاحم پاک کردن آنها از داخل رجیستری است. بهرحال، ممکن است این نرم‌افزار جاسوسی طوری طراحی شده باشد که با هر بار راه‌اندازی مجدد کامپیوتر خودش را در داخل رجیستری قرار دهد. تنها راه حل پیش پای شما برای کشتن این نوع جاسوس متجاوز! فرمت کردن هارد کامپیوتر یا استفاده از یک برنامه ضدجاسوس بسیار قدرتمند است.

تروا‌ها و ویروس‌ها

مانند اسب چوبی تروا که یونانیان برای ورود به شهر تروا استفاده کردند، این نرم‌افزار برای سوءاستفاده از کامپیوتر شما، خود را به شکلی بی‌ضرر درمیاورد. دیتای شما ممکن است کپی، توزیع یا تخریب شود. ویروس نیز مشابه تروا است با این تفاوت که قدرت ایجاد شبیه خود را دارد تا باعث خسارت به کامپیوترهای بیشتری شود. بهرحال، هردوی این قطعات آسیب‌رسان می‌توانند تحت تعریف نرم‌افزار جاسوسی قرار بگیرند، زیرا کاربر از وجودشان بی‌اطلاع است و هدف واقعی آنان را نمی‌داند.

نرم‌افزارهای جاسوسی و مقابله با آنها (۳)

چگونگی قرارگرفتن نرم‌افزار جاسوسی روی کامپیوتر و روش مقابله به آن

تنها مساله در مورد نرم‌افزار جاسوسی این نیست که چه مدت روی کامپیوتر شما قرار داشته و چه قصدی دارد، بلکه فهمیدن اینکه چگونه و از کجا این برنامه وارد کامپیوتر شما شده است، در درجه اول قرار دارد.

در شماره‌های (۱) و (۲) با نرم‌افزارهای جاسوسی و انواع و عملکرد آنها آشنا شدیم. درست مانند علفهای هرز که بدون سروصدا هنگام قدم زدن در جنگل به جوراب شما می‌چسبند، هنگامی که مشغول گشت و گذار در اینترنت هستید، نرم‌افزار جاسوسی خودش را مانند یک مسافر قاچاقی به کامپیوتر شما می‌چسباند! اما قبل از اینکه هرچیزی بتواند روی کامپیوتر شما نصب گردد، معمولا باید روی چیزی کلیک یا برنامه‌ای را باز کنید. در زیر چند تا از معمولترین روشهای مورد استفاده برای فریب‌دادن کاربران برای نصب نرم‌افزارهای جاسوسی بیان شده است:

- بازکردن ایمیل اسپمی
- کلیک کردن روی پنجره‌های بازشونده فریبنده
- دانلود کردن رایگان برنامه‌ها، بازیها، ابزارها و غیره
- برنامه‌های اشتراک فایل

- مشاهده وب‌سایتهای ناجور!
- نرم‌افزارهای اجرای فایلهای صوتی و تصویری آنلاین

درحالیکه حجم فراوانی از محتوا روی اینترنت قرار دارد که برای تماشای اعمال شما بصورت پنهانی طراحی نشده است، بسیاری از نرم‌افزارهای رایگان یا از رده خارج وجود دارد که بی‌سروصدا همراه با نرم‌افزار جاسوسی وارد کامپیوتر شما می‌شود. نرم‌افزار جاسوسی نه تنها علائق شما را برای تبلیغ‌کنندگان آشکار می‌سازد، بلکه می‌تواند منجر به افشای اطلاعات شخصی نیز شود. ببینیم نرم‌افزار جاسوسی چگونه روی هارددیسک شما قرار میگیرد و شما برای جلوگیری از آن چه می‌توانید بکنید.

اولا، یکی از بزرگترین اشتباهاتی که کاربران انجام میدهند این است که قبل از شروع گشت و گذار در وب تنظیمات سطح امنیتی خود را بسیار پایین انتخاب می‌کنند. سطح امنیتی پایین به تمام کوکی‌ها و برنامه‌های جاسوسی به سادگی اجازه ذخیره شدن در حافظه کامپیوتر را میدهد. کارهایی که شما می‌توانید برای دور نگهداشتن نرم‌افزارهای جاسوسی از سیستم خود انجام دهید شامل موارد زیر است:

- تنظیم سطح امنیتی به سطح پیش‌گزیده یا بالاتر
- نظارت دقیق بر آنچه دانلود می‌کنید
- به روز نگهداشتن سیستم‌عامل کامپیوتر

- نصب یک برنامه ضدجاسوسی که جلوی آنچه را که از دست می‌دهید، بگیرد!

برنامه ضدجاسوسی محل برنامه‌های جاسوسی را که بدون اطلاع شما وارد شده‌اند، تعیین می‌کند، آنها را قرنطینه و سپس پاک می‌کند.

در مرحله بعدی، به احساس و غریزه خود رجوع کنید! اگر منبعی آشنا یا قابل اعتماد بنظر نمی‌رسد، ایمیل را باز نکنید، popup را کلیک نکنید و وب‌سایت را نبینید. برنامه‌های مورد نیاز خود را از منبع قابل اعتماد دریافت کنید. گاهی‌اوقات برنامه‌های مجانی ارزش دردسر بعدی را ندارند! هنگامی که به یک پیشنهاد فریبنده برخورد می‌کنید به انگیزه آن دقت کنید. چرا یک نفر می‌خواهد به شما به‌روزرسانیهای مرتب مجانی ارائه دهد؟! دنبالش نروید.

از تجربیات دیگران برای فهمیدن اینکه کدام نرم‌افزارها درون خود به برنامه‌های جاسوسی پناه داده‌اند، استفاده کنید. در عرض چند ثانیه می‌توانید جستجویی انجام دهید تا بفهمید دیگران در مورد نرم‌افزارهای توام با جاسوس، شامل برنامه‌های به اشتراک‌گذاری

فایلها (مانند Kazza و BearShare) و نرم‌افزارهای اجرای فایلهای صوتی‌تصویری آنلاین چه می‌گویند. در مورد دوم صداهای اعتراض! علیه نرم‌افزارهای جاسوسی تاثیرگذار خواهد بود. برای مثال، یک برنامه محاسبه مالیات معروف اخیرا یک برنامه جاسوسی را بمنظور جلوگیری از هر گونه کپی‌برداری از فایلهایش ـ حتی برای مقاصد قانونی مانند تهیه پشتیبان یا استفاده سایر اعضای همان خانواده ـ داخل محصول خود قرار داد. اما مشتریان از این مساله ناراضی بودند که این نرم‌افزار توانایی نظارت بر رفتارشان را دارد، و بهمین دلیل برعلیه سازنده با صدای بلند! اعتراض کردند. شرکت نرم‌افزاری به حرف آنها گوش کرد و سال بعد نرم‌افزار را بدون برنامه جاسوسی فضول! به فروش رساند.

از آنجا که شما به نرم‌افزارهای جاسوسی "نه" می‌گویید، نصب‌کنندگان برای دریافت اجازه مزاحمتان نمی‌شوند! ـ بسیاری اعتقادی به انجام بازی جوانمردانه ندارند!!! بعضی بازاریابان از حقه‌های عادی برای نصب جاسوس‌شان روی کامپیوتر شما استفاده می‌کنند. برای مثال، بخشی از یک نرم‌افزار به نام Gator وجود دارد که تلاش می‌کند شما را برای نصب محصولش از طریق یک popup تبلیغاتی فریب دهد. هنگامی که شما به پیشنهاد دانلود "نه" بگویید (پنجره را ببندید)، popup دوم ظاهر می‌شود و می‌پرسد که "آیا مطمئن هستید؟" این سوال آری/خیر مبهم باعث می‌شود که افراد با کلیک جواب دهند، که به این ترتیب بدون آگاهی کاربر، دانلود آغاز می‌شود.

روش دیگری که باعث پیاده‌شدن نرم‌افزار جاسوسی روی کامپیوتر شما می‌شود، drive-by download نامیده می‌شود. وقتی شما یک وب‌سایت معلوم‌الحال! را مشاهده می‌کنید، به یک popup برمی‌خورید که از شما اجازه برای دانلود می‌خواهد. لحن! پیام باعث می‌شود که شما باور کنید که برای دیدن صفحه وب بازشده به دانلود نیاز است، حتی اگر نیازی نباشد. اگر "بله" بگویید، برنامه جاسوس در کامپیوتر شما دانلود می‌شود. اما اگر پاسخ منفی بدهید، popupها در صفحات بعدی ظاهر می‌شوند تا بالاخره شما به کلیک کردن روی یکی از آنها فریفته شوید و به این ترتیب برنامه جاسوسی به صورت خاموش کار خود را آغاز می‌کند!

بعضی شرکتها از نرم‌افزارهای جاسوسی تبلیغاتی استفاده می‌کنند. وقتی این adwareها روی سیستم شما نصب شدند، شروع به بازکردن popupهای تبلیغاتی می‌کنند. به این ترتیب شما سیلقه‌های شخصی شما و منابع کامپیوتریتان (پهنای باند، اتصال اینترنت و زمان پردازش کامپیوتر) از اختیار شما خارج خواهد شد، اما در عوض هیچ‌چیز بدست نخواهید آورد بجز بمباران تبلیغاتی و اگر نرم‌افزار جاسوسی آدرس ایمیل شما را بدست آورد انبوهی از اسپم‌ها.

چون همواره روش‌های جدید آلوده کردن کامپیوتر شما توسط نرم‌افزارهای جاسوسی در حال ایجاد است، یک نرم‌افزار ضدجاسوسی نصب کنید. این نرم‌افزار به منظور کشف و بیرون‌کردن جاسوس‌ها قبل از اینکه شما را به‌زحمت بیندازند، طراحی شده است. اگر شما از برنامه ضدجاسوسی خود بعنوان سگ محافظ! استفاده کنید، شما را از دانلودهای بدون اجازه و بی‌خبر، آگاه خواهد کرد. نرم‌افزار جاسوسی مزاحمت ایجاد می‌کند و منجر به دردسرهای جدی می‌شود. اگر شما مراتب احتیاط را رعایت کنید، می‌توانید از دردسر احتمالی پرهیز کنید و کامپیوترتان را تمیز نگه دارید.

حملات مبتنی بر مهندسی اجتماعی

آیا شما از جمله افرادی می باشید که به ظاهر افراد و نحوه برخورد آنان بسیار اهمیت داده و با طرح صرفا" یک سوال از جانب آنان، هر آنچه را که در ارتباط با یک موضوع خاص می دانید در اختیار آنان قرار می دهید؟ رفتار فوق گرچه می تواند در موارد زیادی دستاوردهای مثبتی را برای شما بدنبال داشته باشد، ولی در برخی حالات نیز ممکن است چالش ها و یا مسائل خاصی را برای شما و یا سازمان شما، ایجاد نماید. آیا وجود اینگونه افراد در یک سازمان مدرن اطلاعاتی(خصوصا" سازمانی که با داده های حساس و مهم سروکار دارد) نمی تواند تهدیدی در مقابل امنیت آن سازمان محسوب گردد؟ به منظور ارائه اطلاعات حساس خود و یا سازمان خود از چه سیاست ها و رویه هائی استفاده می نمائید؟ آیا در چنین مواردی تابع مجموعه مقررات و سیاست های خاصی می باشید؟ صرفنظر از پاسخی که شما به هر یک از سوالات فوق خواهید داد، یک اصل مهم در این راستا وجود دارد که می بایست همواره به آن اعتقاد داشت: "هرگز اطلاعات حساس خود و یا سازمان خود را در اختیار دیگران قرار نداده مگر این که مطمئن شوید که آن فرد همان شخصی است که ادعا می نماید و می بایست به آن اطلاعات نیز دستیابی داشته باشد."

یک حمله مهندسی اجتماعی چیست ؟

به منظور تدارک و یا برنامه ریزی یک تهاجم از نوع حملات مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت های اجتماعی خاص(روابط عمومی مناسب، ظاهری آراسته و ...)، سعی می نماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند. یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد.

مثلا" وانمود نماید که یک کارمند جدید است، یک تعمیر کار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید. یک مهاجم، با طرح سؤالات متعدد و برقراری یک ارتباط منطقی بین آنان، می تواند به بخش هائی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه سازمان شما دستیابی پیدا نماید. در صورتی که یک مهاجم قادر به اخذ اطلاعات مورد نیاز خود از یک منبع نگردد، وی ممکن است با شخص دیگری از همان سازمان ارتباط برقرار نموده تا با کسب اطلاعات تکمیلی و تلفیق آنان با اطلاعات اخذ شده از منبع اول، توانمندی خود را افزایش دهد.(یک قربانی دیگر!).

یک حمله Phishing چیست ؟

این نوع از حملات شکل خاصی از حملات مهندسی اجتماعی بوده که با هدف کلاهبرداری و شیادی سازماندهی می شوند. در حملات فوق از آدرس های Email و یا وب سایت های مخرب به منظور جلب نظر کاربران و دریافت اطلاعات شخصی آنان نظیر اطلاعات مالی استفاده می گردد. مهاجمان ممکن است با ارسال یک Email با ظاهری قابل قبول و از یک شرکت معتبر کارت اعتباری و یا موسسات مالی، از شما درخواست اطلاعات مالی را نموده و اغلب عنوان نمایند که یک مشکل خاص ایجاد شده است و ما در صدد رفع آن می باشیم. پس از پاسخ کاربران به اطلاعات درخواستی، مهاجمان از اطلاعات اخذ شده به منظور دستیابی به سایر اطلاعات مالی و بانکی استفاده می نمایند.

نحوه پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

- به تلفن ها، نامه های الکترونیکی و ملاقات هائی که عموما" ناخواسته بوده و در آنان از شما درخواست اطلاعاتی خاص در مورد کارکنان و یا سایر اطلاعات شخصی می گردد، مشکوک بوده و با دیده سوء ظن به آنان نگاه کنید. در صورتی که یک فرد ناشناس ادعا می نماید که از یک سازمان معتبر است، سعی نمائید با سازمان مورد ادعای وی تماس گرفته و نسبت به هویت وی کسب تکلیف کنید.

-
- هرگز اطلاعات شخصی و یا اطلاعات مربوط به سازمان خود را (مثلا" ساختار و یا شبکه ها) در اختیار دیگران قرار ندهید، مگر این که اطمینان حاصل گردد که فرد متقاضی مجور لازم به منظور دستیابی به اطلاعات درخواستی را دارا می باشد.
- هرگز اطلاعات شخصی و یا مالی خود را در یک email افشاء نکرده و به نامه های الکترونیکی ناخواسته ای که درخواست این نوع اطلاعات را از شما می نمایند، پاسخ ندهید (به لینک های موجود در اینگونه نامه های الکترونیکی ناخواسته نیز توجهی نداشته باشید).
- هرگز اطلاعات حساس و مهم شخصی خود و یا سازمان خود را بر روی اینترنت ارسال ننمائید. قبل از ارسال اینگونه اطلاعات حساس، می بایست Privacy وب سایت مورد نظر به دقت مطالعه شده تا مشخص گردد که اهداف آنان از جمع آوری اطلاعات شخصی شما چیست و نحوه برخورد آنان با اطلاعات به چه صورت است؟
- دقت لازم در خصوص آدرس URL یک وب سایت را داشته باشید. وب سایت های مخرب ممکن است خود را مشابه یک وب سایت معتبر ارائه نموده که آدرس URL آنان دارای تفاوت اندکی با وب سایت های شناخته شده باشد. وجود تفاوت اندک در حروف استفاده شده برای نام سایت و یا تفاوت در domain ، نمونه هائی در این زمینه می باشند (مثلا" com در مقابل net).
- در صورت عدم اطمینان از معتبر بودن یک Email دریافتی، سعی نمائید با برقراری تماس مستقیم با شرکت مربوطه نسبت به هویت آن اطمینان حاصل نمائید. از اطلاعات موجود بر روی یک سایت مخرب به منظور تماس با آنان استفاده نمائید چراکه این اطلاعات می تواند شما را به مسیری دیگر هدایت نماید

- که صرفا" اهداف مهاجمان را تامین نماید. به منظور آگاهی از این نوع حملات که تاکنون بوقوع پیوسته است، می توانید به آدرس

http://www.antiphishing.org/phishing_archive.html

مراجعه نمائید.

- با نصب و نگهداری نرم افزارهای آنتی ویروس، فایروال ها و فیلترینگ نامه های الکترونیکی ناخواسته(spam)، سعی نمائید یک سطح حفاظتی مناسب به منظور کاهش این نوع حملات را ایجاد نمائید.

اقدامات لازم در صورت بروز تهاجم

- در صورتی که فکر می کنید به هر دلیلی اطلاعات حساس سازمان خود را در اختیار دیگران (افراد غیر مجاز) قرار داده اید، بلافاصله موضوع را به اطلاع افراد ذیربط شاغل در سازمان خود (مثلا" مدیران شبکه) برسانید. آنان می توانند در خصوص هرگونه فعالیت های غیرمعمول ویا مشکوک، هشدارهای لازم را در اسرع وقت در اختیار دیگران قرار دهند.
- در صورتی که فکر می کنید اطلاعات مالی شما ممکن است در معرض تهدید قرار گرفته شده باشد، بلافاصله با موسسه مالی خود تماس حاصل نموده و تمامی حساب های مالی در معرض تهدید را مسدود نمائید. در این رابطه لازم است دقت، حساسیت و کنترل لازم در خصوص هر گونه برداشت از حساب های بانکی خود را داشته باشید.
- گزارشی در خصوص نوع تهاجم را تهیه نموده و آن را در اختیار سازمان های ذیربط قانونی قرار دهید.

شناسایی مزاحم کامپیوتری

اگر کامپیوتر شما به اینترنت وصل است همواره در معرض انواع تهدیدات هستید. به عنوان رایج‌ترین مورد می‌توان به امکان آلودگی دستگاه به انواع ویروس‌ها و کرم‌هایی که از طریق اینترنت توزیع می‌شوند اشاره نمود. نرم‌افزارهای جاسوس نمونه دیگری از این دست برنامه‌ها هستند که بر روی دستگاه قرار گرفته، فعالیت‌های کاربر و همینطور اطلاعات شخصی مانند گذر واژه‌ها، اطلاعات مربوط به کارت‌های اعتباری و... را ثبت کرده و به منتشر کنندگان خود گزارش می‌دهند. نفوذ در سیستم‌های کاربران و انجام اعمال نامطلوب آنان از جمله موارد دیگری است که کامپیوترهای متصل به اینترنت را تهدید می‌نماید. نفوذ به روش‌های مختلفی انجام می‌شود و در بسیاری از مواقع کاربر متوجه این مسئله نمی‌شود. حتی بعضی از نفوذگران ردپای خود را هم پاک می‌کنند به نحوی که حمله به سیستم قابل آشکارسازی نیست.

با این وجود نفوذکنندگان به سیستم به صورت معمول ردپاهایی از خود باقی می‌گذارند. با وجودی که تشخیص بعضی از ردپاها دشوار است ولی با استفاده از گام‌هایی که در ادامه بیان می‌شوند می‌توان بسیاری از نفوذها را تشخیص داد.

به عنوان اولین گام باید سیستم‌عامل و نرم‌افزارهای موجود در محیطی آزمایشی (مشابه شرایط عملیاتی) توصیف شوند. توصیف به این معناست که عملکرد برنامه‌ها در حال اجرا بررسی شده و موارد مختلفی مانند سرعت، زمان پاسخ، نحوه عمل و غیره به صورت دقیق شناسایی شوند. بنابراین باید برنامه‌ها را اجرا نموده و آنها را در شرایطی مشابه حالت عملیاتی قرار داد، سپس رفتار آنها را به دقت بررسی نمود.

در گام بعدی، باید از نرم‌افزارهای توصیف استفاده نمود. یکی از رایج‌ترین ابزارها برای این کار نرم‌افزار TripWire محصول tripwiresecurity.com است. این نرم‌افزار نسخه‌هایی برای سیستم‌عامل‌های مختلف دارد و متن برنامه بعضی نسخه‌های آن به کاربران عرضه می‌شود. غیر از این نرم‌افزار ابزارهای دیگری نیز وجود دارند که همین عملکرد را نشان می‌دهند. این دسته نرم‌افزارها در رده ابزارهای تشخیص نفوذ host-based قرار می‌گیرند. با جستجو بر روی اینترنت می‌توان برنامه‌های دیگری نیز با عملکرد مشابه یافت.

در نهایت باید همه فایل‌ها، دایرکتوری‌ها، تجهیزات و پیکربندی سیستم شناسایی شده و تغییرات آنها در زمان مورد بررسی قرار گیرند. در محیط آزمایشی کنترل شده، شرایط طبیعی شناسایی می‌شود. به خاطر داشته باشید هرگاه سیستم وارد فاز عملیاتی شود،

شرایط طبیعی بهتر شناسایی می‌شوند، زیرا هرچقدر که سیستم‌های تست خوب و قوی طراحی شوند تنها نشان دهنده تخمینی از محیط عملیاتی هستند. باید مجموعه تغییرات جدید را درک کرده و آنها را در توصیف سیستم وارد نمود.

فایل‌ها، دایرکتوری‌ها، تجهیزات و پیکربندی تنها بخشی از توصیف کامل سیستم کامپیوتری هستند. سایر مواردی که باید بررسی شوند به شرح زیر می‌باشند:

- **برنامه‌های در حال اجرا**

منابعی که این برنامه‌ها مورد استفاده قرار می‌دهند و زمان اجرای آنها. به عنوان مثال اگر برنامه تهیه کننده نسخه‌های پشتیبان هر روزه در زمان مقرری اجرا می‌شود، آیا این فعالیت طبیعی قلمداد می‌شود؟ در مورد برنامه واژه‌پردازی که مدت زمان زیادی از وقت CPU را اشغال نموده است چطور؟

- **ترافیک شبکه**

آیا ایجاد ناگهانی تعداد زیادی اتصال HTTP توسط سرور email طبیعی است؟ افزایش ناگهانی بار سرور وب چگونه ارزیابی می‌شود؟

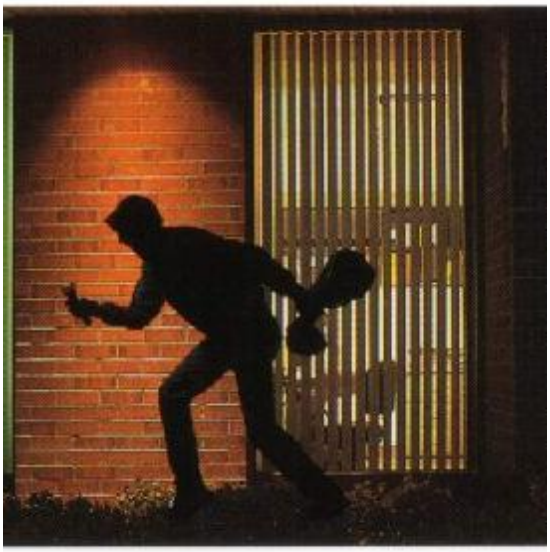
- **کارایی**

آیا سرعت وب سرور کاهش یافته است؟ سرور تراکنش، توان مدیریت چه تعداد تراکنش را دارد؟

- **سیستم عامل**

نفوذگذان در سیستم می‌توانند عملکرد سیستم عامل را به گونه‌ای عوض کنند که برنامه‌های کاربردی بدون اینکه تغییر کنند رفتاری متفاوت نشان دهند. تصور کنید

یک فراخوانی سیستم عامل که باید منجر به اجرای یک برنامه شود، برنامه دیگری را اجرا نماید.



متأسفانه ابزارهایی که برای بررسی این پارامترها وجود دارند به اندازه نرم‌افزارهایی که فایل‌ها، دایرکتوری‌ها، تجهیزات و پیکربندی را بررسی می‌کنند، رشد نداشته‌اند. با این وجود برای مدیریت هوشیارانه سیستم‌ها باید این پارامترها هم به صورت دقیق در توصیف سیستم قید شوند.

تنها در صورت انجام دقیق موارد فوق و نظارت بر تغییر مشخصات سیستم می‌توان به امن بودن کامپیوتر خود امیدوار بود.

ضمائم نامه های الکترونیکی

ارسال فایل و سایر مستندات به عنوان فایل ضمیمه همراه یک نامه الکترونیکی به امری متداول تبدیل شده است. علیرغم تمامی مزایای و پتانسل های ویژگی فوق، ضمائم نامه های الکترونیکی به یکی از منابع اصلی به منظور توزیع ویروس، تبدیل شده اند. استفاده کنندگان نامه های الکترونیکی، می بایست در زمان باز نمودن فایل های ضمیمه، دقت لازم را داشته باشند.(ولو اینکه این نوع ضمائم و نامه های الکترونیکی توسط افرادی ارسال می گردد که شما آنان را می شناسید).

چرا ضمائم نامه های الکترونیکی می توانند خطرناک باشند :

شاید این سوال برای شما مطرح شده باشد که چرا ضمائم نامه های الکترونیکی می توانند خطرناک بوده و تهدیدی در مقابل ایمن سازی اطلاعات باشند؟. در این رابطه به موارد زیر اشاره می گردد:

- چرخش آسان نامه های الکترونیکی: چرخش و حرکت نامه های الکترونیکی بسیار ساده بوده و ویروس ها می توانند در مدت زمان کوتاهی تعداد زیادی از ماشین ها را آلوده نمایند. اکثر ویروس ها حتی به این موضوع نیاز نخواهند داشت که کاربران نامه های الکترونیکی را فوروارد نمایند. ویروس ها، کامپیوتر کاربر را به منظور آگاهی از لیست آدرس نامه های الکترونیکی پویش نموده و به صورت اتوماتیک اقدام به ارسال پیام های آلوده برای هر یک از آدرس های موجود در دفترچه آدرس نامه های الکترونیکی، می نمایند. مهاجمان از این واقعیت ناگوار استفاده می نمایند که اکثر کاربران به نامه های ارسالی بهمراه ضمائم مربوطه از جانب هر شخص اعتماد می نمایند(سوء استفاده از حسن اعتماد کاربران).
- برنامه های پست الکترونیکی، سعی در تامین تمامی نیازهای کاربران می نمایند. تقریبا" هر نوع فایل می تواند به عنوان یک فایل ضمیمه در نظر گرفته شود.

-
- بنابراین مهاجمان دارای آزادی عمل زیادی در خصوص نوع ویروس ها، می باشند.
- برنامه های پست الکترونیکی دارای امکانات گسترده و متعددی در سطح لایه رابط کاربر می باشند. برخی از این نوع برنامه ها، امکان دریافت اتوماتیک ضمائم نامه های الکترونیکی را فراهم می نمایند. بدین ترتیب، امکان آلودگی سیستم بدلیل دریافت یک فایل ضمیمه آلوده افزایش خواهد یافت.

مراحل لازم به منظور حفاظت خود و سایر افراد موجود در لیست دفترچه آدرس

- **دقت لازم در خصوص ضمائم ناخواسته حتی در مواردی که از هویت فرد ارسال کننده، آگاهی لازم وجود داشته باشد.** صرف این که یک نامه الکترونیکی از طرف برادر، دوستان و یا همکاران ارسال شده باشد، به منزله ایمن بودن آنان نمی باشد. تعداد زیادی از ویروس ها قادر به "جعل" آدرس و نمایش آن به صورت یک پیام ارسالی توسط اشخاص دیگر می باشند. در صورت امکان و قبل از باز نمودن فایل ضمیمه، بررسی لازم در خصوص هویت فرد ارسال کننده فایل ضمیمه را انجام دهید. در برخی موارد این نوع نامه های الکترونیکی در ظاهری خیرخواهانه و اطلاع رسانی در خصوص ارائه یک محصول و یا Patch جدید، مخاطبان خود را شکار می نمایند. فراموش نکنیم که تولیدکنندگان نرم افزار، هرگز patch و یا محصول جدید خود را از طریق نامه الکترونیکی، ارسال نمی نمایند.

- **ذخیره و بررسی ضمائم قبل از باز نمودن آنان** : در صورتی که شما مجبور به باز نمودن یک فایل ضمیمه قبل از بررسی منبع ارسال کننده آن می باشید، پیشنهاد می گردد، مراحل زیر دنبال شود:

□ از بهنگام بودن نرم افزار آنتی ویروس خود مطمئن شوید.

□ فایل ضمیمه ارسال شده را بر روی کامپیوتر خود ذخیره نمائید.
□ با استفاده از نرم افزار آنتی ویروس، بررسی لازم در خصوص آلودگی فایل ذخیره شده را انجام دهید.
□ پس از انجام مراحل فوق و اطمینان از عدم آلودگی فایل ضمیمه، می توان آن را فعال نمود.

- **غیر فعال نمودن ویژگی دریافت اتوماتیک فایل های ضمیمه**. به منظور تسهیل در امر دریافت و مشاهده نامه های الکترونیکی، تعداد زیادی از برنامه های پست الکترونیکی، امکان دریافت اتوماتیک ضمائم نامه های الکترونیکی را در برنامه خود پیش بینی نموده اند. پیشنهاد می گردد بررسی لازم در خصوص تنظیمات موجود نرم افزار استفاده شده به منظور دریافت نامه های الکترونیکی انجام و در صورت وجود ویژگی فوق، آن را غیرفعال نمائید.

برنامه های IM و Chat

با این که برنامه های IM و Chat ، روشی مناسب به منظور ارتباط با سایر افراد می باشند، ابزارهای استفاده شده برای این نوع از مبادلات اطلاعاتی online می تواند خطرناک بوده و نتایج مخربی را به دنبال داشته باشد.

تفاوت ابزارهای استفاده شده برای مبادلات online

به منظور مبادله اطلاعاتی online بر روی اینترنت، از ابزارهای متعددی استفاده می گردد. بررسی ویژگی هر یک از این ابزارهای موجود بهمراه تمهیدات مربوطه، امکان استفاده ایمن و مطمئن از این نوع ابزارها را فراهم می نماید.

- **برنامه های IM (Instant messaging)** : از این نوع برنامه ها به منظور تفریح، سرگرمی، ارسال پیام، ارتباط صوتی و یا تصویری با سایر افراد استفاده می گردد. از برنامه های فوق در سازمان ها به منظور ارتباط بین کارکنان نیز استفاده می گردد. صرفنظر از نوع برنامه انتخابی IM ، این نوع برنامه ها بستر مناسبی به منظور ارتباط یک به یک را ایجاد می نماید.
- **اطاق های چت**: اطاق های چت صرفنظر از عمومی بودن و یا خصوصی بودن، تالارهائی برای گروههای خاص از مردم و به منظور ارتباط با یکدیگر می باشند. اکثر اطاق های چت مبتنی بر خصایص مشترکی می باشند: مثلا" اطلاق هائی مختص افرادی با سن خاص و یا علائق مشترک. با اینکه اکثر برنامه های سرویس گیرنده IM از چت، حمایت می کنند، برنامه های IM همچنان و بر اساس روش سنتی خود ابزاری برای ارتباطات یک به یک می باشند. در حالی که چت به صورت سنتی ابزاری برای ارتباط چند نفر به چند نفر می باشد. به منظور طراحی و پیاده سازی برنامه های فوق از فن آوری های متعددی نظیر:

Jabber استفاده می گردد. برخی از نرم افزارهای ارائه شده
با ترکیب چندین قابلیت توانسته اند پاسخگوی خواسته های متنوع کاربران باشند.

تهدیدات این نوع برنامه ها چیست ؟

- **وجود ابهام در خصوص هویت مخاطب**. در برخی موارد نه تنها شناسائی مخاطب و شخصی که در حال ارتباط با وی هستید مشکل می باشد بلکه ماهیت انسانی و رفتاری وی نیز قابل پیش بینی نخواهد بود. مردم ممکن است در رابطه با هویت خودشان، گزاف گفته، account ها ممکن است در معرض سوء ظن باشند و یا ممکن است کاربران عملیات logout را فراموش نمایند. در برخی موارد ممکن است یک account توسط چندین نفر و به صورت مشترک استفاده می گردد. تمامی موارد فوق، دلیلی است بر این ادعا که نمی توان بطور واقعی و حقیقی در رابطه با ماهیت شخصی که در حال گفتگو با وی هستید، قضاوت کرده و به یک سطح مطلوب از اطمینان دست پیدا کرد.
- **کاربران، مستعد انواع حملات می باشند**. سعی کنید به شخصی بقبولانید که برنامه ای را اجراء و یا بر روی یک لینک، کلیک نماید. اجرای یک برنامه به توصیه دیگران و یا کلیک بر روی یک لینک پیشنهادی توسط سایرین، یکی از روش های متداول به منظور انجام برخی تهاجمات می باشد. این موضوع در اطاق های چت و یا برنامه های IM امری متداول و مرسوم است. در محیطی که یک کاربر در این اندیشه است که در یک جو مطمئن و اعتمادپذیر در حال گفتگو با اشخاص است، یک کد مخرب و یا یک مهاجم می تواند شانس بیشتری برای رسیدن به اهداف خود و به دام انداختن سایر افراد را داشته باشد.
- **عدم وجود آگاهی لازم در خصوص سایر افراد درگیر و یا ناظر گفتگو**: مبادلات online بسادگی ذخیره می گردند و در صورتی که شما از یک سرویس اقتصادی رایگان استفاده می نمائید، ماحصل گفتگوی انجام شده می تواند بر روی

یک سرویس دهنده ذخیره شده (logs) و شما هیچگونه کنترلی

در خصوص این logs نخواهید داشت. شما نمی دانید که آیا اشخاص و افراد دیگر نظاره گر این گفتگو می باشند یا خیر؟ یک مهاجم می تواند بسادگی اقدام به شنود اطلاعات و ره گیری آنان از طریق مبادلات اطلاعاتی انجام شده در اطاق های چت نماید.

- **نرم افزاری که شما بدین منظور استفاده می نمائید ممکن است دارای نقاط آسیب پذیر خاص خود باشد.** همانند سایر نرم افزارها، نرم افزارهای چت، ممکن است دارای نقاط آسیب پذیری باشند که مهاجمان با استفاده از آنان می توانند به اهداف خود نائل گردند.
- **تنظیمات امنیتی پیش فرض انجام شده، ممکن است به درستی مقداردهی نشده باشند.** تنظیمات امنیتی در نرم افزارهای چت، با نگرشی خیرخواهانه و ساده در نظر گرفته شده تا بدینوسیله و به زعم خود پتانسیل های بیشتری را در اختیار متقاضیان قرار دهند. رویکرد فوق، کاربران و استفاده کنندگان از این نوع برنامه ها را مستعد انواع حملات توسط مهاجمان می نماید.

چگونه می توان از این ابزارها به صورت ایمن استفاده نمود ؟

- **بررسی و ارزیابی تنظیمات امنیتی**: در این رابطه لازم است تنظیمات پیش فرض در نرم افزار به منظور بهینه سازی امنیتی آنان بررسی گردد. مطمئن شوید که ویژگی دریافت اتوماتیک فایل (Download)، غیر فعال شده باشد. برخی از نرم افزارهای چت، امکان ارتباط محدود با افراد را ارائه می نماید. در صورتی که از این نوع برنامه ها استفاده می نمائید، پیشنهاد می گردد ویژگی فوق فعال گردد.
- **هشیاری و دقت لازم در خصوص افشای اطلاعات.** تا زمانی که نسبت به هویت طرف درگیر در ارتباط اطمینان لازم را کسب نکرده اید، از افشای اطلاعات شخصی و مهم خود جدا" اجتناب کنید. مبادله اطلاعات در اطاق های چت

می بایست با دقت و حساسیت بالا، انجام شود. هرگز اطلاعات تجاری و حساس مربوط به سازمان خود را در اطاق های چت و یا برنامه های عمومی IM افشاء و برملاء ننمائید.

- **شناسائی هویت افرادیکه در حال گفتگو با آنان هستید(حتی المقدور)**. در برخی موارد تشخیص هویت فردی که در حال گفتگو با وی می باشید، چندان حائز اهمیت نمی باشد. در صورتی که شما نیازمند سطح خاصی از اطمینان در خصوص شخص مورد نظر می باشید و یا قصد اشتراک اطلاعاتی خاص با وی را دارید، شناسائی هویت مخاطب بسیار حائز اهمیت است(مطمئن شوید شخصی که در حال گفتگو با وی هستید، همان شخص مورد نظر شما است).
- **عدم اعتماد و باور هر چیز**: اطلاعات و یا توصیه هائی که شما از طریق یک اطاق چت و یا برنامه های IM دریافت می نماید، ممکن است نادرست، غلط و حتی مخرب باشند. در اینگونه موارد می بایست در ابتدا بررسی لازم در خصوص صحت اطلاعات و یا دستورالعمل های ارائه شده، انجام و در ادامه از آنان استفاده گردد.
- **بهنگام نگه داشتن نرم افزارها**: فرآیند بهنگام سازی نرم افزارها شامل نرم افزار چت، مرورگر وب، سیستم عامل، برنامه سرویس گیرنده پست الکترونیکی و برنامه آنتی ویروس است. عدم بهنگام بودن هر یک از برنامه های فوق می تواند زمینه بروز تهاجمات توسط مهاجمان را فراهم نماید.

انتخاب و محافظت از کلمات عبور

کلمات عبور بخش مهمی از امنیت کامپیوتر هستند و در حقیقت در خط مقدم حفاظت از اکانت کاربران قرار می گیرند. یک کلمه عبور نامناسب ممکن است منجر به سوءاستفاده از کل شبکه شود. بهمین دلیل تمام کارمندان شامل پیمانکاران و فروشندگان که به سیستم شرکت دسترسی دارند مسوول انتخاب کلمه عبور مناسب و محافظت از آن هستند.

در این قسمت به نکاتی در مورد ایجاد کلمات عبور قوی و محافظت از آنها و زمان انقضاء و تغییر آنها اشاره می شود. در حقیقت مخاطب این مقاله تمام افرادی هستند که مسوول اکانت یا هر سیستمی هستند که از طریق آن به شبکه یا اطلاعات غیرعمومی دسترسی دارند.

سیاست کلی

- تمام کلمات عبور در سطح سیســـتم باید حداقل سه ماه یکبار عوض شونـــد.
- تمام کلمات عبور سطح کاربر(مانند ایمیل یا کامپیوتر) باید هر شش ماه تغییر کنند که البته تغییر چهار ماهه توصیه می شود.
- اکانتهای کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر اکانتهای آن کاربر متفاوت باشد.
- کلمات عبور نباید در ایمیلها یا سایر شکلهای ارتباطات الکترونیکی درج شوند.
- باید رهنمونهای زیر در تمام کلمات عبور سطح سیستم و سطح کاربر رعایت شود.

راهنماییها

راهنمایی کلی ساخت کلمه عبور

کلمات عبور برای اهداف گوناگونی در شرکتها استفاده می شوند. تعدادی از استفاده های معمول اینها هستند:

- اکانتهای سطح کاربر
- اکانتهای دسترسی به وب
- اکانتهای ایمیل
- حفاظت از مونیتور
- کلمه عبور صندوق پستی

. ورود به روتر محلی

چون سیستمهای بسیار کمی از نشانه های یکبارمصرف استفاده می کنند (مانند کلمات عبور دینامیک که فقط یکبار استفاده می شوند)، هرکسی باید از نحوه انتخاب کلمات عبور مناسب آگاه باشد.

کلمات عبور ضعیف معمولا مشخصات زیر را دارند:

- کلمه عبور شامل کمتر از هشت حرف است.
- کلمه عبور کلمه ای است که در یک فرهنگ لغت یافت می شود.
- کلمه عبور کلمه ای است که کاربردعمومی دارد مانند: نام خانوادگی، حیوانات اهلی، دوستان، همکاران، شخصیت های خیالی وغیره نامها و اصطلاحات کامپیوتری، فرمانها، سایتها، شرکتها، سخت افزار و نرم افزار.

نام شرکت یا کلمات مشتق شده از این نام.

. تاریخ های تولد و سایر اطلاعات شخصی مانند آدرس ها و شماره های تلفن.

. الگوهای کلمات یا شماره ها مانند aaabbb، qwerty،

zyxwvuts، 123321 و غیره.

. هرکدام از عبارات فوق بطور برعکس.

. هرکدام از عبارات فوق که تنها با یک رقم شروع یا به آن ختم می شود.

کلمات عبور مناسب مشخصات زیر را دارند:

- شامل هم حروف کوچک و هم بزرگ هستند (a-z و A-Z)
- علاوه بر حروف از ارقام و نشانه ها هم در آنها استفاده می شود مانند 0-9 و !@#$%^&*()_+|~='{}[];<>?./
- حداقل هشت حرف دارند.
- کلمه ای در هیچ زبان، گویش یا صنف خاص نیستند.
- برپایه اطلاعات شخصی، اسم یا فامیل نیستند.
- کلمات عبور هرگز نباید نوشته یا جایی ذخیره شوند. سعی کنید کلمات عبوری انتخاب کنید که بتوانید براحتی در ذهن داشته باشید. یک روش انجام این کار، ایجاد کلمه عبور بر پایه یک ترانه یا عبارت است.

برای مثال عبارت "This May Be One Way To Remember" و کلمه عبور می تواند "TmB1w2R!" یا "Tmb1W>r~" یا انواع دیگری از همین الگو باشد.

توجه: این مثالها را بعنوان کلمه عبور استفاده نکنید.

استانداردهای حفاظت از کلمه عبور

از کلمات عبور مشترک برای اکانتهای شرکت و دسترسی های شخصی استفاده نکنید. تا جایی ممکن است، از کلمه عبور مشترک برای نیازهای مختلف شرکت استفاده نکنید. برای مثال، برای سیستمهای مهندسی یک کلمه عبور انتخاب کنید و یک کلمه عبور دیگر برای سیستمهای IT . همچنین برای استفاده از اکانتهای NT و UNIX کلمات عبور متفاوت انتخاب کنید.

کلمات عبور شرکت با هیچ کس از جمله دستیاران و منشی ها در میان نگذارید. باید با تمام کلمات عبور بصورت اطلاعات حساس و محرمانه برخورد شوند.

در اینجا به لیستی از "انجام ندهید" ها اشاره می شود.

- کلمه عبور را از طریق تلفن به هیچ کس نگویید.
- کلمه عبور را از طریق ایمیل فاش نکنید.
- کلمه عبور را به رئیس نگویید.
- در مورد کلمه عبور در جلوی دیگران صحبت نکنید.
- به قالب کلمه عبور اشاره نکنید. (مثلا نام خانوادگی)
- کلمه عبور را روی فهرست سوالات یا فرمهای امنیتی درج نکنید.
- کلمه عبور را با اعضای خانواده در میان نگذارید.
- کلمه عبور را هنگامی که در مرخصی هستید به همکاران نگویید.

اگر کسی از شما کلمه عبور را پرسید، از ایشان بخواهید که این مطلب را مطالعه کند یا اینکه با کسی در قسمت امنیت اطلاعات تماس بگیرد.

از ویژگی "Remember Password" یا حفظ کلمه عبور در کامپیوتر استفاده نکنید.

مجدداً، کلمات عبور را در هیچ جای محل کار خود ننویسید و در فایل یا هر سیستم کامپیوتری ذخیره نکنید(شامل کامپیوترهای دستی) مگر با رمزکردن.

کلمات عبور را حداقل هر شش ماه عوض کنید(بجز کلمات عبور سطح سیستم که باید هر سه ماه تغییر کنند).

اگر هر اکانت یا کلمه عبور احتمال فاش و سوء استفاده از آن میرود، به بخش امنیت اطلاعات، اطلاع دهید و تمام کلمات عبور را تغییر دهید.

شکستن یا حدس زدن کلمه عبور ممکن است در یک زمان متناوب یا اتفاقی توسط بخش امنیت اطلاعات یا نمانیدگی های آن رخ دهد. اگر کلمه عبور در طول یکی از این پیمایش ها حدس زده یا شکسته شود، از کاربر خواسته خواهد شد که آن را تغییر دهد.

رعایت موارد مذکور، به حفاظت بیشتر از اطلاعات و قسمتهای شخصی افراد کمک خواهد کرد.

سیاست های امنیتی

در دنیایی که وجه مشخصه آن فناوری سطح بالا و ارتباطات گسترده می باشد، هر سازمانی نیاز به سیاست های امنیتی که مدبرانه تدوین شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان توسط هکرها، رقبا و یا کشورهای خارجی منافع سازمان را تهدید می کند. هدف سیاست های امنیتی تعریف روال ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می نماید. با اجرای دقیق سیاست های امنیتی، سازمان ها می توانند تهدیدات را کاهش دهند.

مفاهیم

سیاست امنیتی یک سازمان سندی است که برنامه های سازمان برای محافظت سرمایه های فیزیکی و مرتبط با فناوری ارتباطات را بیان می نماید. به سیاست امنیتی به عنوان یک سند زنده نگریسته می شود، بدین معنا که فرایند تکمیل و اصلاح آن هیچ گاه متوقف نشده، متناسب با تغییر فناوری و نیازهای کاربران به روز می شود. چنین سندی شامل شرایط استفاده مجاز کاربران، برنامه آموزش کاربران برای مقابله با خطرات، توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست های امنیتی و راه کار به روز رسانی آنها می باشد.

هر سیاست امنیتی مشخص کننده اهداف امنیتی و تجاری سازمان است ولی در مورد راه کارهای مهندسی و پیاده سازی این اهداف بحثی نمی کند. سند سیاست امنیتی سازمان باید قابل فهم، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر، از نظر عملی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن سطح حافظتی قابل قبولی را ارائه نماید.

تدوین سیاست

بهترین روش برای دستیابی به امنیت اطلاعات، فرموله نموده سیاست امنیتی است. مشخص نمودن سرمایه های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر اینکه چه افرادی به چه سرمایه هایی دسترسی دارند) در اولین گام باید انجام شود. هدف اصلی از سیاست امنیتی این است که کاربران بدانند مجاز به چه کارهایی هستند و از سوی دیگر مدیران سیستم و سازمان را در تصمیم گیری برای پیکربندی و استفاده از سیستم ها یاری رساند.

برای تدوین سیاست امنیتی پس از تحلیل ریسک های سازمان، می توان به روش هایی که دیگران برگزیده اند متوسل شد. معمولا تجارب مفیدی که قبلا در صنایع مشابه انجام شده و نتایج خوبی از آنها نتیجه شده است به صورت عمومی گزارش شده و در قالب مقالات تخصصی ارائه می گردند. استانداردهای شناخته شده ای نیز برای این کار وجود دارد که می توان از آنها هم بهره گرفت.

سازمان های بزرگ و متوسط برای تعریف سیاست امنیتی خود ناچار به پیروی روش بالا به پایین می باشند. ولی برای سازمان های کوچک انجام این کار به روش پایین به بالا نیز امکان پذیر است. در این حالت از قابلیت های ابزارهای موجود بهره گرفته می شود.

همانگونه که هرم سیاست فوق نشان می دهد، بهترین سیاست امنیتی در شرایطی تدوین می گردد که مدیریت سازمان سیاست کلی را ارائه نموده و یا دستور پیاده سازی اصول امنیتی را در سازمان صادر کند. تدوین کنندگان سیاست سازمان باید فعالیت خود را بر پایه اصول و استانداردهای صنعتی مانند ISO17799 و یا HIPAA انجام دهند. رویه ها، راهنماها و تجربیات پایه ای برای ایجاد و توسعه فناوری امنیتی در سازمان های مختلف هستند. محصولاتی مانند ESM سازگاری و انعطاف سیاست را با سیاست ها و روال های امنیتی سیستم عامل ها، پایگاه داده ها و برنامه های کاربردی ارزیابی می نمایند. این ابزارها ممکن است با محیط کامپیوتری و شبکه سازمان در تعامل باشند.

استانداردها و روال های امنیتی

سیاست های امنیتی دربردارنده کلیه انتظارات، برنامه ها و اهداف عملیاتی مدیریت سازمان می باشد. برای عملیاتی و قابل اجرا بودن، سیاست امنیتی باید با استفاده از استانداردها، راهنماها و رویه های شناخته شده تعریف شود که اطمینان از سازگاری کلیه عملیات اجرایی با سیاست های امنیتی حاصل گردد.

استاندارها، راهنما ها و روال ها تفسیر خاصی از سیاست را ارائه می کنند و کاربران، مشتریان و مدیران سازمان را برای پیاده سازی سیاست آماده می نمایند.

ساختار سیاست امنیتی

ساختار سیاست امنیتی مرکب از اجزاء زیر می باشد:

- عبارتی در رابطه با موضوع سیاست
- چگونگی اجرای سیاست در محیط سازمان
- نقش و مسئولیت افراد مختلف تاثیر گذار در سیاست
- سیاست به چه میزان انعطاف پذیر است؟
- اعمال، فعالیت ها و فرایندهای مجاز و غیر مجاز
- موارد سخت گیری و عدم انعطاف سیاست

سه محور اصلی در کنترل دسترسی در شبکه

AAA (Authentication, Authorization and Accounting)

AAA که مخفف Authentication, Authorization and Accounting است سه محور اصلی در کنترل دسترسی در شبکه هستند که در این بخش در مورد هریک از آنها به طور مجزا و مختصر صحبت می‌شود. ابتدا تعریفی از هریک از این مفاهیم ارائه می‌دهیم.

۱ – Authentication

۱-۱ – مفهوم Authentication

به معنای وارسی عناصر شناسایی ارائه شده از سوی کاربر، تجهیزات یا نرم‌افزارهایی است که تقاضای استفاده و دسترسی به منابع شبکه را دارند. عناصر شناسایی در ابتدایی‌ترین و معمول‌ترین حالت شامل نام کاربری و کلمه عبور می‌باشند. در صورت نیاز به بالاتر بودن پیچیدگی فرایند کنترل و وارسی هویت، می‌توان با اضافه نمودن عناصر شناسایی به این مهم دست یافت. بدیهی است که با اضافه نمودن فاکتورها و عناصر شناسایی، نوع خادم مورد استفاده، پایگاه‌های داده‌ای مورد نظر و در بسیاری از موارد پروتکل‌ها و استانداردها نیز باید مطابق با تغییرات اعمال شده در نظر گرفته شوند تا یکسانی در ارائه خدمات در کل شبکه حفظ شود.

پس از ارائه عناصر شناسایی از سوی متقاضی، سیستم کد کاربری و کلمه عبور را با بانک اطلاعاتی مختص کدهای شناسایی کاربری مقایسه کرده و پذیرش یا عدم پذیرش دسترسی به منابع را صادر می‌کند.

عمل Authentication، در طراحی شبکه‌هایی با حجم کم و متوسط عموماً توسط تجهیزات مسیریابی و یا دیوارهای آتش انجام می‌گیرد. علت استفاده از این روش مجتمع سازی و ساده سازی پیاده‌سازی عمل Authentication است. با استفاده از امکانات موجود نیاز به استقرار یک خادم مجزا برای صدور پذیرش هویت متقاضیان دسترسی مرتفع می‌گردد.

از سوی دیگر در شبکه‌های با حجم و پیچیدگی نسبتاً بالا، عموماً با توجه به پردازش بالای مختص عمل Authentication، خادمی بصورت مستقل و مجزا به این امر اختصاص می‌یابد. در این روش از استانداردها و پروتکل‌های مختلفی همچون TACACS+ و RADIUS استفاده می‌گردد.

۲-۱ - فعال نمودن Authentication

فعال نمودن Authentication بر روی تجهیزات مورد استفاده در شبکه عملی است که عموماً در چهار مرحله انجام می‌شود :

الف - فعال نمودن AAA بر روی سخت‌افزارهای مورد نظر

ب - ایجاد پایگاه داده‌ای از کدهای کاربری کاربران یا تجهیزات شبکه به همراه کلمه‌های عبور. همانگونه که ذکر شد، این پایگاه می‌تواند در داخل تجهیزات مورد استفاده در شبکه‌های با حجم کم پیاده‌سازی شود. در شبکه‌های با حجم نسبتاً بالا که در آنها نیاز به

استفاده از خادمی مختص عمل Authentication احساس می‌شود، تجهیزات فعال شبکه به گونه‌ای پیکربندی می‌شوند که عمل Authentication را با استفاده از پایگاه‌های داده‌ای مستقر بر روی خادم‌های مختص این فرایند، انجام دهند.

ج – ایجاد فهرست(های) روش انجام عمل Authentication. این فهرست‌ها به تعیین روش مورد نظر برای عمل Authentication اختصاص دارند.

د – اعمال فهرست(های) روش ساخته شده ار مرحله قبل.

در هر شبکه، در صورت نیاز به عمل Authentication، این چهار مرحله بر روی تمامی تجهیزاتی که در عمل AAA نقش دارند اجرا می‌شوند.

۲ – Authorization

۲-۱ – مفهوم Authorization

Authorization فرایندی است که طی آن به کاربران و یا تجهیزات متقاضی دسترسی به منابع، امکان استفاده از منبع یا منابع مستقر بر روی شبکه داده می‌شود. به بیان دیگر این عمل برای مدیران شبکه امکان تعیین نوع دسترسی به هریک از منابع شبکه، برای تک تک متقاضیان دسترسی و یا گروهی از آنها، را فراهم می‌کند.

از سوی دیگر، عمل امکان اختصاص آدرس‌های شناخته شده و از پیش تعیین شده به کاربران یا تجهیزات، همچون متقاضیانی که با استفاده از پروتکل PPP به شبکه متصل می‌شوند، را می‌دهد. این عمل متقاضی را ملزم به استفاده از نوع خاصی ار استانداردها یا پیکربندی‌های ارتباطی مورد نظر مدیر شبکه می‌کند.

زمانی که Authorization بر روی شبکه فعال شده باشد، خادم شبکه‌ای که مسئولیت Authorization را بر عهده دارد اطلاعات کاربر را از روی پایگاه داده کاربرها استخراج می‌کند. این پایگاه داده می‌تواند بر روی خادم محلی بوده و یا بر روی پایگاهی مجزا قرار داشته باشد.

پس از استخراج این اطلاعات، وضعیت دسترسی مورد قبول مدیریت با تقاضای کاربر قیاس گردیده و تایید یا عدم تایید اجازه استفاده از سرویس یا منبع مورد نظر متقاضی صادر می‌شود.

۲-۲ – برقراری Authorization

برقراری و فعال نمودن Authorization عملی مشابه فعال نمودن Authentication است. برای برقراری و فعال نمودن Authorization، Authentication باید فعال شده باشد. به عبارت دیگر کلیه مراحل را می‌توان به شکل زیرخلاصه نمود:

الف – فعال نمودن Authentication بر روی سخت‌افزارهای مورد نظر. همانگونه که ذکر شد اولین مرحله از چهار مرحله فعال‌سازی این فرایند، فعال سازی AAA بر روی تجهیزات است.

ب – ایجاد فهرست(های) روش انجام عمل Authorization. این فهرست‌ها علاوه بر تعیین روش مورد نظر برای عمل Authorization، مبین سرویس مورد نظر برای عمل Authorization نیز می‌باشند.

ج – اعمال فهرست(های) روش ساخته شده ار مرحله قبل.

۳ – Accounting

۳–۱ – مفهوم Accounting

Accounting آخرین بخش از فرایند جمعی AAA است. طی این فرایند، گزارشی از عملکرد کاربران یا سخت‌افزارهایی که هویت آنها طی اعمال Authentication و Authorization تایید شده است، توسط خادم AAA تهیه می‌شود. این عمل می‌تواند با استفاده از خادم های خارجی که اس پروتکل‌ها و استانداردهایی چون TACACS+ و RADIUS استفاده می‌کنند انجام گیرد.

به بیان دیگر، این عمل قدمی فراتر از دو مرحله پیشین برداشته، و پیگیری بعدی، پس از احراز هویت را انجام می‌دهد. پیام‌های Accounting به شکل رکورد، میان تجهیزاتی که از طریق آنها دسترسی متقاضی درخواست شده و پایگاه‌های داده‌ای از قبیل TACACS+ یا RADIUS، تبادل می‌گردد.

۳–۲ – فعال سازی Accounting

فرایند فعال سازی Accounting مشابه Authorization است که مهم‌ترین مراحل شامل ایجاد فهرست‌های روش Accounting و اعمال آنهاست

روشهای پنهان سازی سرورهای وب برای افزایای ایمنی

پوشش دادن یا پنهان کردن یک وب سرور شامل از بین بردن جزئیات هویتی ای است که هکرها می توانند برای کشف سیستم عامل و وب سرور نصب شده روی آن مورد استفاده قرار دهند. این اطلاعات در حالی که هیچ استفاده ای برای بهره برداران مشروع ندارد، اغلب نقطه شروعی برای هکرها می باشد.

دراین مقاله به بررسی برخی راهکارهایی که می توانیم با به کارگیری آنها خطر شناسایی را به حداقل برسانیم، می پردازد. بیشتر مثالها مربوط به IIS میکروسافت می باشد. زیرا بخاطر آسیب پذیری زیادش به طور وسیعی مورد توجه نفوذگران قرار گرفته است. همچنین یک سری از اقدامات پیشگیرانه شناسایی برای آپاچی سرور نیز ذکر خواهد شد. غیر قابل شناسایی کردن سرور وظیفه همه کسانی است که مسئولیت اجرایی وب سرور را بر عهده دارند.

نفوذگران از اینجا شروع می کنند ، چرا شما از این نقطه شروع نمی کنید ؟

بگذارید از نقطه نظر مهاجمین نگاه کنیم. آسیب پذیریهای امنیتی متکی بر نسخه (Version) و نوع نرم افزار دارند.

یک نفوذگر برای نفوذ به یک وب سرور باید بداند وب سرور از چه نوعی و دارای چه ورژنی می باشد. دانستن جزئیات یک وب سرور کارآمدی هرگونه تهاجمی را به مقدار زیاد افزایش می دهد.

Server Header ها همه چیز را می گویند:

بسیاری از وب سرورها خودشان و سیستم عاملی را که بر روی آن نصب هستند به هر کسی که بخواهد معرفی می نمایند.