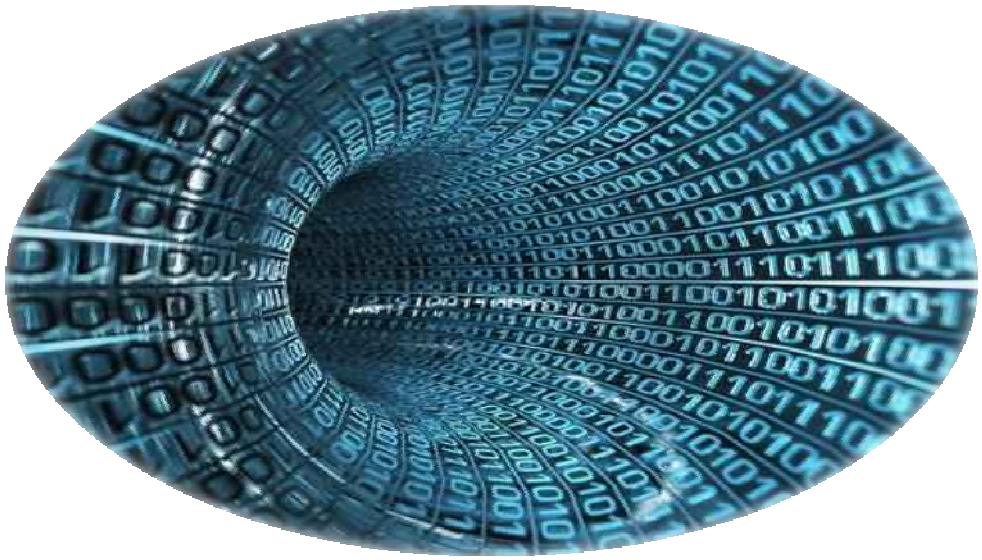
امنیت اطلاعات و شبکه



⇐ آشنایی با انواع تهدیدات امنیتی
⇐ رمزنگاری و امضای دیجیتال
⇐ نفوذگران و اهداف آنها
⇐ پنهان سازی اطلاعات

تدوین: مهندس توفان سماپور
(مدرس مرکز آموزش جامع علمی-کاربردی آستارا)

زینت انسان سه‌چیز است: علم، محبت، آزادی

افلاطون

فصل اول

انواع تهدیدات امنیتی و راهکارهای مقابله با آن

۱. مقدمه

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می‌باشیم. کافی است به اطراف خود نگاهی داشته باشیم تا به صحت گفته فوق بیشتر واقف شویم. همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه‌های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی)، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است. استفاده کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فن آوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می‌باشند. امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری از جمله این مولفه‌ها بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بوده و می‌بایست به این مقوله در سطح کلان و از بُعد منافع ملّی نگاه کرد. وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرفنظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می دهد.

در این فصل قصد داریم به بررسی مبانی و اصول اولیه امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری پرداخته و از این رهگذر با مراحل مورد نیاز به منظور حفاظت کامپیوترها در مقابل حملات، بیشتر آشنا شویم.

۲. اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها

تمامی کامپیوترها از کامپیوترهای موجود در منازل تا کامپیوترهای موجود در سازمان‌ها و موسسات بزرگ، در معرض آسیب و تهدیدات امنیتی می‌باشند. با انجام تدابیر لازم و استفاده از برخی روش‌های ساده می‌توان پیشگیری لازم و اولیهای را در خصوص ایمن‌سازی محیط کامپیوتری خود انجام داد. علیرغم تمامی مزایا و دستاوردهای اینترنت، این شبکه عظیم به همراه فن‌آوری های مربوطه، دریچهای را در مقابل تعداد زیادی از تهدیدات امنیتی برای تمامی استفاده‌کنندگان (افراد ، خانواده ها ، سازمان ها، موسسات و ...) گشوده است. با توجه به ماهیت حملات، می‌بایست در انتظار نتایج نامطلوب متفاوتی بود (از مشکلات و مزاحمت‌های اندک تا از کار انداختن سرویس ها و خدمات). در معرض آسیب قرار گرفتن داده‌ها و اطلاعات حساس، تجاوز به حریم خصوصی کاربران، استفاده از کامپیوتر کاربران برای تهاجم بر علیه سایر کامپیوترها، از جمله اهداف مهاجمانی است که با بهره گیری از آخرین فن‌آوری‌های موجود، حملات خود را سازماندهی و بالفعل می‌نمایند. بنابراین، می‌بایست به موضوع امنیت اطلاعات، ایمن‌سازی کامپیوترها و شبکه‌های کامپیوتری، توجه جدّی شده و از فرآیندهای متفاوتی در جهت مقاوم‌سازی آنان، استفاده گردد.

مدیران شبکه باید همواره آن را تحت کنترل داشته باشند و تمام سعی خود را دریافتن رخنه های جدید و بستن آنها بنماید. شبکه‌های دارای ویژگی‌های خاص بطور بالقوه می‌توانند مشکلات و خطراتی را داشته باشند. در اینجا لیست کلّی از خطرات احتمالی برای امنیت شبکه ارائه شده است که ما سعی می-کنیم در خلال این متن به بررسی جزئی‌تر هر یک از این خطرات بپردازیم:

- سهولت نسخه‌برداری از اطلاعات دیجیتال
- شبکه‌های کنترل نشده
- شبکه‌های متصل به اینترنت بدون firewall
- ویروسها
- تهاجم به واسطه TCP/IP
- روشهای همگانی
- کاربران ناآگاه
- کامپیوترهای ناامن
- اطلاعات نا امن (بدون Backup)
- تهاجم غیرعمدی
- تهاجم عمدی

۳. انواع تهدیدات شبکه

تقریباً هر نوع تهاجم، تهدیدی است در مقابل حریم خصوصی، پیوستگی، اعتبار و صحت داده ها. یک سارق اتومبیل می‌تواند در هر لحظه صرفاً یک اتومبیل را سرقت نماید، در صورتی که یک مهاجم با بکارگیری صرفاً یک دستگاه کامپیوتر، می‌تواند آسیب‌های فراوانی را متوجه تعداد زیادی از شبکه‌های کامپیوتری نموده و باعث بروز اشکالاتی متعدد در زیرساخت اطلاعاتی یک کشور گردد. آگاهی لازم در رابطه با تهدیدات امنیـتی و نحوه حفاظت خود در مقابل آنان، امکان حفاظت اطلاعات و داده های حساس را در یک شبکه کامپیوتری فراهم می‌نماید. در ادامه ما تهدیدات را به دسته‌بندی‌های زیر تقسیم نموده و در مورد هر دسته توضیحاتی را ارائه دادهایم.

۳ .۱. بد افزارها

بد افزار[1] اصطلاحی برای برنامه‌های کامپیوتری با اهداف بداندیشانه و مخرب مانند ویروسها، کرمها، و تروجانهاست. به عبارت دیگر بدافزارها برنامه‌های کامپیوتری نامطلوبی هستند که به صورت مخفیانه و یا بدون مجوز با فعالیت ناخواسته و یا با ناپایداری سیستم و یا با استفاده از منابع پردازنده و حافظه باعث می-شوند کامپیوتر قادر به عملکرد عادی خود نباشد.

بدافزارها گستره وسیعی از برنامه‌های مخرب را شامل می‌شوند. بدافزارها را می‌توان بر اساس عوامل مختلفی دسته‌بندی کرد؛ از جمله روشهای مورد استفاده برای حمله یا اجرا، هدف و کارکرد برنامه، شیوه

[1] Malware

تکثیر یا انتشار، سیستم‌های نرم‌افزاری مورد حمله و ... . فهرست زیر چند نوع معروف و رایج از بدافزارها را به اختصار تعریف می‌کند.

۱.۱.۳. ویروس‌ها [۲]

ویروس‌های کامپیوتری، متداولترین نوع تهدیدات امنیتی در سالیان اخیر بوده که تاکنون مشکلات گستردهای را ایجاد و همواره از خبرسازترین موضوعات در زمینه کامپیوتر و شبکه های کامپیوتری، بودهاند. ویروس برنامه نرم‌افزاری نامطلوبی است که خود را به صورت خودکار با آلوده‌سازی دیگر فایل‌های کامپیوتری منتشر می‌کند. ویروس احتیاج به فایل میزبان دارد تا خود را به آن بچسباند. مثلاً یک ویروس بوت، کد خود را در رکورد بوت یا رکورد بوت اصلی دیسک وارد می‌کند، سپس هنگام بوت شدن کامپیوتر از روی دیسک، کد ویروس اجرا می‌شود.

به عبارت دیگر ویروس‌ها، برنامه‌هایی کامپیوتری می‌باشند که توسط برنامه‌نویسان گمراه و در عین حال ماهر نوشته شده و بگونهای طراحی می‌گردند که قادر به تکثیر خود و آلودگی کامپیوترها بر اثر وقوع یک رویداد خاص، باشند. مثلاً ویروس‌هایی که از آنان با نام "*ماکرو ویروس*" یاد می‌شود، خود را به فایل‌هایی شامل دستورالعمل های ماکرو ملحق نموده و در ادامه، همزمان با فعال شدن ماکرو، شرایط لازم به منظور اجرای آنان نیز فراهم می گردد. برخی از ویروس‌ها بی‌آزار بوده و صرفاً باعث بروز اختلالات موقت در روند انجام عملیات در کامپیوتر می-شوند (نظیر نمایش یک پیام مضحک بر روی صفحه نمایشگر همزمان با فشردن یک کلید خاص توسط کاربر). برخی دیگر از ویروس‌ها دارای عملکردی مخرب‌تر بوده و می‌توانند مسائل و مشکلات بیشتری نظیر حذف فایل‌ها و یا کاهش سرعت سیستم را به دنبال داشته باشند. یک کامپیوتر صرفاً زمانی آلوده به یک ویروس می گردد که شرایط و امکان ورود ویروس از یک منبع خارجی (اغلب از طریق فایل ضمیمه یک نامه الکترونیکی و یا دریافت و نصب یک فایل و یا برنامه آلوده از اینترنت و انتقال فایل بواسطه حافظه‌های جیبی و قابل حمل)، برای آن فراهم گردد. زمانی که یک کامپیوتر در شبکهای آلوده گردید، سایر کامپیوترهای موجود در شبکه و یا سایر کامپیوترهای موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس، خواهند بود.

۲.۱.۳. کرم [۳]

کرم برنامهای است مشابه ویروس که به صورت خودکار از کامپیوتری به کامپیوتر دیگر منتشر می‌شود. کرم با ارسال خود از طریق ایمیل یا هر وسیله دیگری انتشار می‌یابد. کرمها برای انتشار نیاز به فایل میزبان ندارند. کرمها همانند ویروسها توانایی تکثیر خود را دارند و از کامپیوتری به کامپیوتر دیگر منتقل می شوند. اولین هدف کرمها و ویروسها انتشار است. عمده-ترین تفاوت بین کرمها و ویروسها این است که کرمها ممکن است خود را جایگزین فایلهای کامپیوتری کنند ولی کد خود را وارد فایلی نمی‌نمایند. در مقابل ویروس‌ها، کد خود را وارد فایلها می‌کنند و هرگز به صورت فایلهای جداگانهای ظاهر نمی‌شوند.

۳.۱.۳. تروجان [۴] (دشمنانی در لباس دوست)

[2] Viruses
[3] Worm
[4] Trojan

برنامه‌های اسب تروا، که نامشان یادآور داستان حمله به تروی و حیله مورد استفاده در آن حمله می‌باشد، به منزله ابزارهایی برای توزیع کدهای مخرب می‌باشند. تروجان‌ها، می‌توانند بی آزار بوده و یا حتی نرم‌افزار مفیدی نظیر بازی‌های کامپیوتری باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه می‌نمایند. تروجان‌ها، قادر به انجام عملیات متفاوتی نظیر حذف فایل‌ها، ارسال یک نسخه از خود به لیست آدرس‌های پست الکترونیکی، می‌باشند. این نوع از برنامه‌ها صرفاً می‌توانند از طریق تکثیر برنامه‌های اسب تروا به یک کامپیوتر، دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی، اقدام به آلودگی یک سیستم نمایند.

تروجان‌ها ابزارهایی هستند که به تناوب توسط مهاجمان به کار می رود. زمانی‌که تروجان اجرا می‌شود، مجموعه‌ای از کارها را انجام می‌دهد مانند حذف کردن فایل‌ها، اجرای برنامه‌های دیگر و یا نصب یک در پشتی برای دستیابی مهاجم به کامپیوتر آلوده.

۴.۱.۳. درپشتی[5]

درپشتی برنامه‌ای است که امکان دستیابی مهاجم به کامپیوتر آلوده را با دور زدن روال‌های اعتبار سنجی معمول فراهم می‌آورد. بر اساس نحوه عمل و انتشار، درهای پشتی به دو گروه عمده تقسیم می‌شوند. اولین گروه بسیار شبیه دیگر تروجان‌ها هستند، یعنی داخل برنامه‌های دیگری قرار می‌گیرند و با اجرای برنامه میزبان فعال می‌شوند. دومین گروه مشابه کرم‌ها عمل می‌کنند و به عنوان بخشی از پردازش بوت اجرا می‌شوند و معمولاً همراه کرم‌هایی که آنها را به عنوان بار هدف[6] همراه دارند، دیگر کامپیوترها را نیز آلوده می‌کنند.

۵.۱.۳. کیت ریشه [7]

کیت ریشه برنامه‌ای است که پس از دستیابی مهاجم به کامپیوتر مورد حمله بر روی آن نصب می‌شود. کیت‌های ریشه اغلب حاوی توابعی برای پنهان کردن ردپای حمله مانند پاک کردن یا تغییر فایلهای ثبت رویدادها[8] می‌باشند. کیت‌های ریشه ممکن است شامل درپشتی نیز باشند که به اندازه مهاجم اجازه دستیابی مجدد به کامپیوتر مورد حمله را می دهد؛ و یا حاوی برنامه‌های بهره‌بردار برای حمله به دیگر کامپیوترها باشد.

۲.۳. ویرانگران

در وب سایت های متعددی از نرم افزارهائی نظیر اکتیوایکس ها و یا اپلت‌های جاوا استفاده می‌گردد. این نوع برنامه‌ها به منظور ایجاد انیمیشن و سایر افکت‌های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می دهند. با توجه به دریافت و نصب آسان این نوع از برنامه ها توسط کاربران، برنامه‌های فوق به ابزاری مطمئن و آسان به منظور آسیب رسانی به سایر سیستم ها تبدیل شده اند . این نوع برنامه‌ها که به "ویرانگران" شهرت یافته اند، به شکل یک برنامه نرم افزاری و یا اپلت ارائه و

[5] Backdoor
[6] Payload
[7] Root kit
[8] Log files

در دسترس استفاده کنندگان قرار می‌گیرند. برنامه‌های فوق، قادر به ایجاد مشکلات متعددی برای کاربران می باشند(از بروز اشکال دریک فایل تا ایجاد اشکال در بخش اصلی یک سیستم کامپیوتری).

۳.۳. حملات

تاکنون حملات متعددی متوجه شبکه‌های کامپیوتری بوده است. این حملات را می‌توان بر اساس معیارهای گوناگونی نظیر شیوه‌ی کارکرد به دسته‌های مختلفی تقسیم‌بندی کرد.

۳.۳.۱. تقسیم‌بندی حملات براساس اهدافشان

الف) حملات شناسایی: در این نوع حملات، مهاجمان اقدام به جمع آوری و شناسائی اطلاعات با هدف تخریب و آسیب رساندن به آنان می نمایند. مهاجمان در این رابطه از نرم افزارهای خاصی نظیر Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب‌پذیر کامپیوترها، سرویس‌دهندگان وب و برنامه‌ها، استفاده می‌نمایند. در این رابطه برخی تولیدکنندگان، نرم‌افزارهائی را با اهداف خیرخواهانه طراحی و پیاده‌سازی نموده‌اند که متاسفانه از آنان در جهت اهداف مخرب نیز استفاده می شود. مثلاً به منظور تشخیص و شناسائی رمزهای عبور، نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است. نرم افزارهای فوق با هدف کمک به مدیران شبکه، افراد و کاربرانی که رمز عبور خود را فراموش کرده و یا آگاهی از رمز عبور افرادی که سازمان خود را بدون اعلام رمز عبور به مدیر شبکه، ترک نموده‌اند، استفاده می‌گردند. به هر حال وجود این نوع نرم-افزارها واقعیتی انکارناپذیر بوده که می تواند به منزله یک سلاح مخرب در اختیار مهاجمان قرار گیرد.

ب) حملات دستیابی: دراین نوع حملات، هدف اصلی مهاجمان، نفوذ در شبکه و دستیابی به آدرس‌های پست الکترونیکی، اطلاعات ذخیره شده در بانک های اطلاعاتی و سایر اطلاعات حساس، می باشد.

ج) حملات از کار انداختن سرویس ها[9]: در این نوع حملات، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به تمام و یا بخشی از امکانات موجود در شبکه برای کاربران مجاز می نمایند. حملات فوق به اشکال متفاوت و با بهره‌گیری از فن‌آوری‌های متعددی صورت می‌پذیرد. ارسال حجم بالایی از داده‌های غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه، نمونه‌هایی از این نوع حملات می‌باشند. برنامه های حمله DoS حملات را از یک کامپیوتر و با دستور مهاجم انجام می‌دهند. حملات DDoS[10] از تعداد زیادی کامپیوتر آلوده بدون اطلاع و موافقت کاربران آنها برای حمله به سرور مورد نظر خود استفاده می‌کند. مثالی از این نوع حمله در بیستم آگوست ۲۰۰۱ اتفاق افتاد که در آن کرم CodeRed حمله موفقی علیه وب-سایت ریاست جمهوری ایالات متحده به روش مذکور انجام داد.

۳.۳.۲. تقسیم‌بندی حملات براساس نوع عملکردشان

الف) حملات از نوع وقفه: بدین معنا که حمله‌کننده باعث شود شبکه مختل شده و مبادله اطلاعات امکان-پذیر نباشد.

ب) حملات از نوع استراق سمع: بر روی هر شبکه کامپیوتری روزانه اطلاعات متفاوتی جابجا می‌گردد و همین امر می تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حملات، مهاجمان اقدام به

[9] Denial of Service
[10] Distributed Denial of Service

استراق سمع و یا حتی تغییر بسته‌های اطلاعاتی در شبکه می‌نمایند. مهاجمان به منظور نیل به اهداف مخرب خود از روش‌های متعددی به منظور شنود اطلاعات، استفاده می‌نمایند.

ج) حملات از نوع دستکاری داده‌ها: یعنی حمله‌کننده توانسته به نحوی اطلاعاتی که روی شبکه مبادله می‌شوند را تغییر دهد. یعنی داده‌هایی که در مقصد دریافت می‌شود متفاوت با آن چیزی باشد که از مبدأ ارسال شده است.

د) حملات از نوع افزودن اطلاعات: در این نوع از حملات، مهاجم اطلاعاتی را که در حال تبادل روی شبکه است تغییر نمی‌دهد، بلکه اطلاعات دیگری را که می‌تواند مخرب یا بنیانگذار حملات بعدی باشد، به اطلاعات اضافه می‌نماید (مثل ویروسها).

فصل دوم

رمزنگاری و امضای دیجیتال

Cryptography & Digital Sign

۱. رمزنگاری

رمزنگاری اطلاعات، روشی مناسب به منظور حفاظت از اطلاعات حساس است. بدین ترتیب، صرفاً افراد مجاز قادر به دستیابی و استفاده از اطلاعات خواهند بود.

۱.۱. رمزنگاری چیست ؟

رمزنگاری، روشی به منظور ارسال یک پیام به صورت کد شده می‌باشد. پس از ارسال پیام، صرفاً افرادی که دارای کلید مناسب رمزگشائی می‌باشند، قادر به استفاده از پیام می‌باشند. افرادی که دارای کلید رمزگشائی نمی‌باشند، پیام را به صورت مجموعه‌ای از حروف، اعداد و کاراکترهای تصادفی مشاهده خواهند کرد. استفاده از رمزنگاری در مواردی که قصد ارسال اطلاعاتی حساس وجود داشته باشد و نمی‌بایست این اطلاعات توسط افراد غیرمجاز مشاهده و مطالعه گردد، اکیداً توصیه شده است.

با توجه به این که نامه‌های الکترونیکی بر روی اینترنت ارسال می‌گردند و امکان ره‌گیری و سوءاستفاده از آنان برای مهاجمان وجود دارد، می‌بایست یک لایه اضافه امنیتی در خصوص اطلاعات حساس را ایجاد نمود. پیام هایی که باید رمزنگاری شوند، **متن ساده** نام دارند و توسط تابعی تبدیل می‌شوند که پارامتر آن کلید است. خروجی فرآیند رمزنگاری را **متن رمزی** می‌نامند. هنر شکستن را **تحلیل رمز** و هنر ابداع آن را **رمزشناسی** می‌نامند.

قاعده مهم رمزنگاری این است که تحلیل‌گر رمز باید چگونگی رمزنگاری (E) و رمزگشایی (D) را بداند. کلید رمز متشکل از رشته‌ی نسبتاً کوتاهی است که یکی از چند روش رمزنگاری را انتخاب می‌کند. تلاش برای سرّی نگه‌داشتن الگوریتم رمز کارایی چندانی ندارد و فقط باید سعی شود تا کلیدها سرّی بمانند. چون بار اصلی رمزنگاری روی کلید است، طول آن موضوع مهم طراحی است. هرچه طول کلید بیشتر باشد عملیات رمزنگاری و رمزگشایی طولانی‌تر می‌شود، اما پنهان‌کاری و ضریب امنیت بسیار بالاتر می‌رود.

از دید تحلیل‌گر رمز، مسأله تحلیل رمز سه شکل مختلف دارد. وقتی مقداری از متن رمزی را بدون متن ساده ان در اختیار دارد، با مساله **متن رمزی محض** سر و کار دارد. رمز نگاری در بخش جدول روزنامه‌ها از این نوع است. وقتی متن رمزی را به همراه متن ساده آن در اختیار دارد، با مسأله **متن ساده‌ی مشخص** مواجه است. سرانجام وقتی تحلیل‌گر رمز، توانایی رمزگذاری قطعاتی از متن ساده انتخابی خود را دارد، با مسأله **متن ساده انتخابی** مواجه است.

روش‌های رمزنگاری از نظر تاریخی به دو دسته تقسیم می شوند: رمزهای جانشینی و رمزهای جابجایی.

- در رمز جانشینی هر حرف یا گروهی از حروف به جای حرف یا گروهی از حروف دیگر قرار می‌گیرد تا پنهان‌سازی صورت گیرد. یکی از قدیمی‌ترین رمزهای شناخته شده، رمز سزار نام دارد که به ژولیوس سزار نسبت داده می‌شود. در این روش a به D، b به E، c به F و ... و z به C تبدیل می‌شود. به عنوان مثال ، attack به DWWDFN تبدیل می‌شود. در مثال‌ها، متن ساده با حروف کوچک و متن رمزی با حروف بزرگ مشخص می‌شود.

۱.۲. نحوه عملکرد رمزنگاری

- دریافت کلید عمومی افرادی که قصد ارسال اطلاعات رمز شده برای آنان را داریم. در صورت انتخاب کلید عمومی از یک حلقه کلید عمومی، می‌بایست به منظور تایید اثرانگشت صاحب کلید با وی تماس گرفته شود.
- با استفاده از کلیدعمومی دریافت کننده پیام، می‌بایست اطلاعات را رمز نمود. اکثر برنامه‌های ارسال email دارای پتانسیل لازم به منظور انجام عملیات فوق می‌باشند.
- دریافت کننده یک پیام رمز شده با استفاده از کلید خصوصی خود اقدام به رمزگشایی پیام می-نماید.

۳.۱. کلیدها در رمزنگاری

با روشن شدن اهمیت وجود کلیدها در امنیت داده‌ها، اکنون باید به انواع کلیدهای موجود و مکان مناسب برای استفاده هر نوع کلید توجه کنیم.

۳.۱.۱. کلیدهای محرمانه (Secret keys)

الگوریتم‌های متقارن مانند DES از کلیدهای محرمانه استفاده می‌کنند؛ کلید باید توسط دو طرف تراکنش منتقل و ذخیره شود. چون فرض بر این است که الگوریتم شناخته شده و معلوم است، این قضیه اهمیت امن بودن انتقال و ذخیره کلید را مشخص می‌سازد. کارت‌های هوشمند معمولاً برای ذخیره کلیدهای محرمانه استفاده می‌شوند. در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است: باید همیشه فرض کنیم که یک کارت ممکن است با موفقیت توسط افراد غیرمجاز تحلیل گردد، و به این ترتیب کل سیستم نباید در مخاطره قرار گیرد.

۳.۱. ۲. کلیدهای عمومی و اختصاصی (Public and private keys)

امتیاز اصلی و مهم سیستم‌های کلید نامتقارن این است که آنها اجازه می‌دهند که یک کلید (کلید اختصاصی) با امنیت بسیار بالا توسط تولید کننده آن نگهداری شود در حالیکه کلید دیگر (کلید عمومی) می‌تواند منتشر شود. کلیدهای عمومی می‌توانند همراه پیام‌ها فرستاده شوند یا در فهرست‌ها لیست شوند (شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیام‌رسانی الکترونیکی ITU X.500 وجود دارد)، و از یک شخص به شخص بعدی داده شوند. مکانیسم توزیع کلیدهای عمومی می‌تواند رسمی (یک مرکز توزیع کلید) یا غیررسمی باشد.

محرمانگی کلید اختصاصی در چنین سیستمی مهمترین مساله است؛ باید توسط ابزار منطقی و فیزیکی در کامپیوتری که ذخیره شده، محافظت گردد. کلیدهای اختصاصی نباید هرگز بصورت رمزنشده در یک سیستم کامپیوتر معمولی یا بشکلی که توسط انسان قابل خواندن باشد، ذخیره شوند. در اینجا نیز کارت هوشمند برای ذخیره کلیدهای اختصاصی یک فرد قابل استفاده است، اما کلیدهای اختصاصی سازمان‌های بزرگ معمولاً نباید در یک کارت ذخیره شود.

۳.۱. ۳. کلیدهای اصلی و کلیدهای مشتق‌شده (Master keys and derived keys)

یک روش کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آنهاست هر زمانی که استفاده می‌شوند. در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق‌شده استفاده می‌شود که بعدا برای رمزنگاری استفاده می‌گردد. برای مثال، اگر یک صادرکننده با تعداد

زیادی کارت سروکار دارد، می‌تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق‌شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود.

شکل دیگری از کلیدهای مشتق‌شده با استفاده از tokenها که محاسبه‌گرهای الکترونیکی با عملکردهای بخصوص هستند، محاسبه می‌شوند. آنها ممکن است بعنوان ورودی از یک مقدار گرفته شده از سیستم مرکزی، یک PIN وارد شده توسط کاربر و تاریخ و زمان استفاده کنند. خود token شامل الگوریتم و یک کلید اصلی است. چنین tokenهایی اغلب برای دسترسی به سیستم‌های کامپیوتری امن استفاده می‌شوند.

۱.۳.۴. کلیدهای رمزکننده‌کلید (Key-encrypting keys)

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در یک سیستم بشمار می‌رود، رمزکردن کلیدها هنگام ارسال و ذخیره آنها بشکل رمزشده منطقی بنظر می‌رسد. کلیدهای رمزکننده کلید هرگز به خارج از یک سیستم کامپیوتری (یا کارت هوشمند) ارسال نمی‌شوند و بنابراین می‌توانند آسانتر محافظت شوند تا آنهایی که ارسال می‌شوند. اغلب الگوریتم متفاوتی برای تبادل کلیدها از آنچه که برای رمزکردن پیامها استفاده می‌شود، مورد استفاده قرار می‌گیرد.

از مفهوم دامنه کلید (Domain Key) برای محدود کردن میدان کلیدها و محافظت کردن کلیدها در دامنه‌شان استفاده می‌کنیم. معمولاً یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند بصورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده کلید محلی ذخیره می‌شوند. هنگامی که کلیدها می‌خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می‌شوند که اغلب بعنوان کلید کنترل ناحیه (Zone Control Key) شناخته می‌شوند. با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می‌شوند. بنابراین کلیدهایی که در دامنه‌های یک ناحیه قرار دارند از دامنه‌ای به دامنه دیگر بصورتی که بیان گردید منتقل می‌شوند.

۵- کلیدهای نشست (Session keys)

برای محدودکردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می‌شود. این کلید ممکن است یک عدد تصادفی تولید شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد باشد. اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می‌تواند با استفاده از کلید عمومی کارت رمز شود.

بخشی از تراکنش که در آن کلید منتقل می‌شود اغلب در مقایسه با بقیه تراکنش کوتاهتر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرفنظر است. چنانچه بقیه تراکنش بسبب استفاده از کلید متقارن با بالاسری کمتری رمز شود، زمان پردازش برای فاز تأیید هویت و انتقال کلید قابل پذیرش است. (توضیح اینکه روشهای رمز متقارن از نامتقارن به مراتب سریعتر هستند بنابراین می‌توان ابتدا یک کلید متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد.)

شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستم‌های پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می‌شود. بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می‌شود و این کلید برای تراکنش بعدی مورد استفاده قرار می‌گیرد.

۲. آشنایی با امضای دیجیتال

شاید تاکنون نامه‌های الکترونیکی متعددی را دریافت داشته اید که دارای مجموعه ای از حروف و اعداد در انتهای آنان می‌باشند. در اولین نگاه ممکن است اینگونه تصور گردد که اطلاعات فوق بی‌فایده بوده و شاید هم نشان‌دهنده بروز یک خطا در سیستم باشد! در حقیقت ما شاهد استفاده از امضای دیجیتال در یک نامه الکترونیکی می‌باشیم. به منظور ایجاد یک امضای دیجیتال از یک الگوریتم ریاضی به منظور ترکیب اطلاعات در یک کلید با اطلاعات پیام، استفاده می‌شود. ماحصل عملیات، تولید یک رشته مشتمل بر مجموعه‌ای از حروف و اعداد است. یک امضای دیجیتال صرفاً به شما نخواهد گفت که "این شخص یک پیام را نوشته است" بلکه در بردارنده این مفهوم مهم است که : "این شخص این پیام را نوشته است".

۲.۱. علّت استفاده از یک امضای دیجیتال

برای یافتن علّت استفاده ابتدا سوالاتی را مطرح می‌کنیم:

- برای تشخیص و تائید هویت فرد ارسال کننده یک نامه الکترونیکی از چه مکانیزم‌هایی استفاده می‌شود؟
- فرض کنید یک نامه الکترونیکی را از یکی از دوستان خود دریافت داشته‌اید که از شما درخواست خاصی را می‌نماید، پس از مطالعه پیام برای شما دو سوال متفاوت مطرح می‌گردد : **الف)** آیا این نامه را واقعاً وی ارسال نموده است؟ **ب)** آیا محتوای نامه ارسالی واقعی است و وی دقیقاً همین درخواست را داشته است؟
- آیا وجود هر نامه الکترونیکی در صندوق پستی، نشان‌دهنده صحت محتوا و تائید هویت فرد ارسال کننده آن است؟

با گسترش روزافزون کاربران اینترنت، سوءاستفاده از آدرس‌های Email برای مهاجمان و ویروس‌ها به امری متداول تبدیل شده است و با توجه به نحوه عملکرد آنان در برخی موارد شناسایی هویت فرد ارسال‌کننده یک پیام بسیار مشکل و گاهاً غیرممکن است. تشخیص غیرجعلی بودن نامه‌های الکترونیکی در فعالیت‌های تجاری و بازرگانی دارای اهمیت فراوانی است.

یک نامه الکترونیکی شامل یک امضای دیجیتال، نشاندهنده این موضوع است که محتوای پیام از زمان ارسال تا زمانی که به دست شما رسیده است، تغییر نکرده است. در صورت بروز هر گونه تغییر در محتوای نامه، امضای دیجیتال همراه آن از درجه اعتبار ساقط می‌شود.

۲.۲. نحوه عملکرد یک امضای دیجیتال

قبل از آشنائی با نحوه عملکرد یک امضای دیجیتال، لازم است در ابتدا با برخی اصطلاحات مرتبط با این موضوع بیشتر آشنا شویم :

- **کلیدها (Keys):** از کلیدها به منظور ایجاد امضاهای دیجیتال استفاده می‌گردد. برای هر امضای دیجیتال، یک کلید عمومی و یک کلید خصوصی وجود دارد: **کلید خصوصی،** بخشی از کلید است که که شما از آن به منظور امضای یک پیام استفاده می‌نمائید. کلید خصوصی یک رمزعبور حفاظت شده بوده و نمی‌بایست آن را در اختیار دیگران قرار داد. **کلید عمومی،** بخشی از کلید است که امکان استفاده از آن برای سایر افراد وجود دارد. زمانی که کلید فوق برای یک حلقه کلید عمومی (public key ring) و یا یک شخص خاص ارسال می‌گردد، آنان با استفاده از آن قادر به بررسی امضای شما خواهند بود.

- **حلقه کلید (Ring Key)**، شامل کلیدهای عمومی است. یک حلقه کلید از کلیدهای عمومی افرادی که برای شما کلید مربوط به خود را ارسال نموده و یا کلیدهائی که از طریق یک سرویس دهنده کلید عمومی دریافت نموده‌اید، تشکیل می‌گردد. یک سرویس‌دهنده کلید عمومی شامل کلید افرادی است که امکان ارسال کلید عمومی در اختیار آنان گذاشته شده است.
- **اثرانگشت**: زمانی که یک کلید تائید می‌گردد، در حقیقت منحصر بفرد بودن مجموعه‌ای از حروف و اعداد که اثر انگشت یک کلید را شامل می‌شوند، تائید می‌گردد.
- **گواهینامه‌های کلید**: در زمان انتخاب یک کلید از روی یک حلقه کلید، امکان مشاهده گواهینامه (مجوز) کلید وجود خواهد داشت. دراین رابطه می‌توان به اطلاعات متفاوتی نظیر صاحب کلید، تاریخ ایجاد و اعتبار کلید دست یافت.

۳.۲. مراحل ایجاد و استفاده از کلیدها:

الف) تولید یک کلید با استفاده از نرم افزارهایی نظیر PGP (اقتباس شده از کلمات Pretty Good Privacy) و یا GnuPG (اقتباس شده از کلمات GNU Privacy Guard)

ب) معرفی کلید تولید شده به سایر همکاران و افرادی که دارای کلید می‌باشند.

ج) ارسال کلید تولید شده به یک حلقه کلید عمومی تا سایر افراد قادر به بررسی و تائید امضای شما گردند.

د) استفاده از امضای دیجیتال در زمان ارسال نامه‌های الکترونیکی. اکثر برنامه‌های سرویس‌دهنده پست الکترونیکی دارای پتانسیلی به منظور امضاء یک پیام می‌باشند.

۳. تفاوت رمزنگاری با امضای دیجیتال

در رمزنگاری کلید عمومی همانند امضای دیجیتال از نرم افزاری نظیر PGP به منظور تبدیل اطلاعات با استفاده از الگوریتم‌های ریاضی استفاده می‌گردد. رمزنگاری کلید عمومی مبتنی بر کلیدهای خصوصی و عمومی است.

علیرغم وجود برخی شباهت‌ها بین فرآیندهای رمزنگاری و امضای دیجیتال، در این رابطه تفاوت‌هایی نیز وجود دارد:

- هدف رمزنگاری، محرمانگی است. با ترجمه محتوای پیام به یک کد، اطلاعات مخفی نگه داشته می‌شوند. هدف امضای دیجیتال، استحکام و واقعی بودن یک پیام است. بدین منظور بررسی لازم در خصوص فرستنده پیام و عدم تغییر محتوای آن، انجام می‌شود. با این که رمزنگاری و امضای دیجیتال می‌توانند مستقل از هم استفاده شوند، امکان امضای یک پیام رمز شده نیز وجود دارد.
- در زمان امضای یک پیام از کلید خصوصی استفاده می‌گردد و هر فردی که دارای کلید عمومی ارسال کننده پیام است، قادر به بررسی صحت و اعتبار امضای دیجیتال است. در زمان رمزنگاری

یک پیام از کلید عمومی فردی که اطلاعات برای وی ارسال می‌گردد، استفاده شده و وی با استفاده از کلید خصوصی خود قادر به رمزگشائی پیام است. با توجه به این که افراد کلید خصوصی را نزد خود محرمانه نگه داشته و از آن با استفاده از رمزهای عبور، حفاظت می‌نمایند، دریافت کننده یک پیام رمز شده، تنها شخصی است که قادر به رمزگشایی و مشاهده پیام خواهد بود.

فصل سوم

نفوذگر

Hacker

۱. مقدمه

امروزه نفوذگران با اهداف و روش‌های مختلف به چالشی عمده در دنیای کامپیوتر تبدیل شده‌اند. دیگر سارقان و تروریست‌ها تنها کسانی نیستند که با سلاح گرم یا سرد و بطور فیزیکی دست به اقدامات خرابکارانه بزنند. امروزه می‌توان برخی از نفوذگران به شبکه‌ها را با توجه به شدّت انجام عملیات خرابکارانه آنها و میزان خسارت‌های مادی و معنوی که به افراد، شرکت‌ها، سازمان‌ها و کشورهای مختلف وارد می-کنند، در زمره خطرناک‌ترین و برجسته‌ترین سارقان و تروریست‌ها به حساب آورد. با توجه به اهمیت موضوع، شناخت انواع مختلف این نفوذگران از لحاظ هدف و طرز کارشان یکی از مسائل مهم در رویارویی با تهدیدات امنیتی گوناگون است.

۲. نفوذگر کیست؟

هک در ساده‌ترین حالت می‌تواند ناشی از خطاهای برنامه‌نویسی و کاربرد باشد و یک جوان کنجکاو و کم اطلاع از دانش کامپیوتر می‌تواند یک هکر باشد. ابداع واژه نفوذگر به دهه‌ی شصت میلادی در دانشگاه MIT باز می‌گردد. در آن زمان "نفوذگر" یا هکر بدین‌گونه تعبیر می‌شد:

> "نفوذگر کسی است که از سرکشی کردن به جزئیات سیستم‌های قابل برنامه ریزی و نفوذ و رسوخ در آن لذت می‌برد و مصمم به شکست دادن توانایی محاسباتی ماشین در مقابل هوش و ذکاوت بشری خویش است. فردی که با سماجت و به گونه ای لجوجانه شیفته‌ی برنامه نویسی است. نفوذگر، بدخواه نیست و صدمه نمی زند."

در آن دوران این افراد نه تنها بدنام و مورد غضب و نفرت نبودند بلکه از آنها به نیکی و احترام یاد می‌شد. اکثر دانشجویان آنروز، اساتید، مدیران یا متخصصین حرف‌های امروز در سطح جهان هستند و رشد فن-آوری کامپیوتر وام دار تلاش و کوشش آنهاست.

در اواخر دهه هشتاد جنبش نفوذگری (Hacktivism) در شبکه به سوی فعالیتهای ضد امنیتی، ضد انسانی و مالیخولیایی گرایش پیدا کرد. در آن زمان وقتی در رسانه های خبری از واژه‌ی "نفوذگر" یاد می-شد، در ذهن مخاطبین، تصویر یک دزد کامپیوتری یا مخرّب نابکار تجسم می‌یافت؛ این ذهنیت با پیشینه و فرهنگ نفوذگری که در اصل به نخبگان رشته‌ی کامپیوتر تعلق داشت ناسازگار بود و یک اهانت بزرگ به این جمع متخصص محسوب می‌شد. این موضوع آنهایی را که قبلاً از لقب "نفوذگر یا هکر" به خود می بالیدند بشدت ناخشنود و دلگیر کرد، لذا آنان تلاش نمودند مجدداً به واژه هکر یا نفوذگر روحی مثبت و خوشایند بدمند. برخی از آنها سعی کردند نفوذگر را انسانی مثبت و نخبه بنامند که در جبهه مقابل Cracker قرار می‌گیرد. بدین ترتیب واژه Cracker نیز معنا یافت:

> " Cracker موجود بی ارزش و بیماری است که با فراگیری برخی از مهارتهای نفوذگری به کارهای بی‌ارزشی همانند دزدیدن شناسه کاربری و رمز عبور دیگران، مزاحمت و عملیات غیرقانونی و ضد اخلاقی می‌پردازد و با شکستن حریم امنیت یک سیستم اهداف غیر شرافتمندانه‌ی خود را دنبال می‌کند."

امروزه هکرها طیف وسیعی از کاربران را تشکیل می دهند که بعضی از آن‌ها حتی در مقام مدیر سیستم و مشاوره مشغول به فعالیت می‌باشند.

مفهوم هک همپای پیشرفت کامپیوتر همواره تغییر کرده است. در ابتدا مفهوم هک استفاده از ابزارهای الکترونیکی و ارتباطی نظیر تلفن جهت استفاده رایگان از آن‌ها بود که بعدها توسط کارشناسان نرم‌افزاری جهت بدست آوردن کد و اطّلاعات برنامه‌ها تغییر نمود و در حال حاضر هک به دستیابی غیرمجاز به اطلاعات یک کامپیوتر یا شبکه گفته می‌شود. با توجه به اینکه این کار غیرقانونی و گاهاً مخرب است، هکرها به عنوان کاربران خطرناک و حتّی پس از حملات ۱۱ سپتامبر بعنوان تروریست کامپیوتری مشهور شده‌اند.

در گذشته، تصور عمومی بر آن بود که هکرها بی آنکه قابل ردیابی باشند اطلاعات را به سرقت می-بردند، این در حالیست که اگر از کارشناسان امنیت کامپیوتر در این موارد استفاده شود، می‌توانند نحوه هک شدن و نیز حتی فرد هکر را نیز شناسایی کنند.
هک می‌تواند جنبه شخصی یا حرفه‌ای داشته باشد، به عبارت دیگر، هکرها می‌توانند کلمات عبور یا اطلاعات شخصی یا شرکتی را به سرقت ببرند و یا در سطح بالاتری برای امنیت ملی خطراتی ایجاد کنند، مانند دخالت در امور ارتباطی و مالی و ... . برخلاف تصوری که مردم از هکرها به عنوان افراد منزوی و ناراحت دارند، بسیاری از هکرها افراد باهوش و خلاق هستند و صرفاً بدلیل ارضاء حس کار گروهی یا احساس قدرت اقدام به این کار می‌نمایند.

۳. اهداف و مقاصد هکرها

جواب این سوال قطعی نیست از لحاظ جامعه‌شناسی نفوذگر در تمام ادوار تاریخ وجود داشته است اما در سیستم‌های شبکه نفوذ می‌تواند چند علّت اصلی داشته باشد.

۳ .۱. اعلام سواد و تسلط بر فن آوری اطلاعات

این نوع نفوذ کمتر با تخریب و تهدید نفوذگر همراه است فراموش نکنید برای نفوذ در سیستم های شبکه ؛ باید فرد دارای سواد پایه ای در حد کافی باشد. برخی از افراد برای به رخ کشیدن سواد و توانمندی خود در شبکه های نفوذ نموده و با به جا گذاشتن یک ردپایی خود برای اثبات نفوذ سعی می‌کنند که سواد خود را به همه اعلان کنند.

۳ .۲. اعلان ضعف امنیت شبکه کامپیوتری

این نوع نفوذ هم با تخریب و تهدید کم انجام می‌شود، بطوری‌که تنها نفوذگر سعی می‌کند نقاط ضعف امنیت شبکه را به مدیریت اعلان نماید و در برخی موارد هم به مدیریت اعلام می‌شود که نفوذگر حاضر به همکاری در رفع نقص و تقویت امنیت شبکه است.

۳.۳. انتقام شخصی یا گروهی

این نوع نفوذ به طور حتم بسیار خطرناک و دردسرساز است. در اینگونه حمله‌ها نفوذگر سعی می‌کند سیستم را تا حد امکان نابود و خسارات جبران ناپذیری را انجام دهد ؛ برخورد سخت با رقبا یکی از انگیزه‌های نفوذگران با نیت انتقام است در برخی موارد هم برخی از وبسایت‌ها و شبکه‌های منافع ملی، گروهی یا فردی افراد را به مخاطره می‌اندازد و در مقابل نفوذگر سعی در نابودی آن وبسایت را دارد.

۴.۳. بدون دلیل

بطور حتمی نباید هر کاری دلیل داشته باشد؛ برخی نیز برای خودنمایی یا سرگرمی و گاهی هم از سر بیکاری دست به نفوذ و تخریب شبکه می‌کنند. این نوع نفوذ به دلیل اینکه کور و بدون دلیل است ممکن است خطرآفرین باشد اما در مواردی بیشتر با یک شوخی تمام می‌شود.

۵.۳.دلایل شخصی

کمتر اتفاق می‌افتد که یک هکر انگیزه شخصی فراتر از انتقام داشته باشد ولی ممکن است این اتفاق بیافتد مانند اسید پاشی روی صورت معشوق و یا موارد دیگر البته این مورد کمتر اتفاق افتاده است.

۶.۳. دستیابی به اموال مجازی افراد یا شرکت‌ها

این امر ممکن است یکی از قویترین دلایل انجام هک باشد البته این نوع از نفوذ بیشتر از روش دزدی هویت یا فیشینگ صورت می‌گیرد. فرد نفوذگر سعی می‌کند با دستیابی به ID و شناسه کاربری قربانی و رمز عبور و پسورد وی، مدیریت بخشی از اموال مجازی فرد یا شرکت از قبیل وبلاگ، صندوق پست الکترونیکی، کارت اعتباری، عضویت باشگاه، عضویت وبسایت و یا هر مورد که می‌تواند وی را به اموال مجازی شخص قربانی نزدیک کند را در دست می‌گیرد. در ایران و در بین هکرهای تازه کار هدف‌هایی مانند انتقام، اعلام سواد، اعلان ضعف شبکه کمتر وجود دارد و هکر سعی می‌کند تنها توسط دستیابی به مدیریت یک وبلاگ یا صندوق پست الکترونیکی نفوذ را انجام دهد. این گونه نفوذهای ساده و با بهره‌گیری از ضعفهای امنیتی کاربران در ایران رایج است.

۴. انواع هکرها و نفوذگران کامپیوتر

هکرها را می‌توان بر اساس اهداف بیان شده، نوع فعالیت و دانش آن‌ها تقسیم‌بندی نمود. البته این تقسیم-بندی می‌تواند از دیدگاه و شرایط کاری خاصی انجام شود، اما در مجموع می‌توان هکرها را به پنج گروه طبقه بندی کرد:

۴ .۱. هکرهای کلاه سفید (Hacker)

که به آنها سامورایی یا هکرهای واقعی گفته می شود . هکرهای کلاه سفید متخصصان کامپیوتر و آشنا به فناوری اطلاعات می باشند و هدفشان از نفوذ به سیستم های کامپیوتری کشف عیوب امنیتی در سیستم و بر طرف نمودن آنها است ، نه سوء استفاده . به عبارت ساده تر ، کلاه سفید ها برای این کار باید مانند هکرهای کلاه سیاه عمل کنند تا بتوانند ضعف های سیستم را کشف کنند.

در حال حاضر بسیاری از شرکت‌ها و مؤسسات از هکرهای کلاه سفید برای کنترل و محافظت از سیستم‌های کامپیوتری خود استفاده می‌کنند، این موضوع پس از حملات گسترده سال گذشته به سایت‌های ایرانی و خسارت‌هایی که به این سایت‌ها و صاحبان آن‌ها و نیز خدمات دهندگان اینترنت وارد آمد، تا مدتی مورد توجه قرار گرفته و مطبوعات در آن موقع در مورد لزوم امنیت سیستم‌های کامپیوتری بررسی‌های کامل انجام دادند. ولی با گذشت زمان متأسفانه بسیاری از شرکت‌ها و مؤسسات با علم به ضعف امنیتی سیستم‌های خود حاضر به قبول مشاوره و نیز بر طرف نمودن این عیوب که بعضاً به سادگی قابل بر طرف شدن می‌باشد، نیستند.

۴ .۲. هکرهای کلاه سیاه - واکر (Wacker)

به آنها واکر هم گفته می‌شود و از نظر کاری هکرهای کلاه سیاه دقیقاً برعکس هکر کلاه سفید عمل می‌نماید. به این معنی که هدف آن‌ها نفوذ به سیستم‌ها و سوء استفاده از اطلاعات می‌باشد.

این گروه از هکرها بیشترین صدمات را به سیستم‌های کامپیوتری وارد می‌نمایند که بی‌سابقه‌ترین و بزرگترین حمله توسط این گروه از هکرها در تاریخ ۲۱ اکتبر سال ۲۰۰۲ ساعت ۴ بعد از ظهر به وقت آمریکا رخ داد. این حمله که از نوع (DDOS) بود بر روی ۱۳ سرور اصلی اینترنت صورت گرفت، در این حمله ۹ سرور به طور کامل از کار می افتد. اهمیت این واقعه آنقدر بود که حتی کاخ سفید و رئیس جمهور آمریکا وارد عمل می‌شوند و از آن بعنوان یک کار تروریستی مجازی اسم می‌برند، و اگر تلاش به موقع کارشناسان امنیتی نبود و هکرها موفق می شدند عملیات خود را تکمیل کنند، اکنون جهان درگیر یک فاجعه می‌شد.

۴ .۳. قفل بازکن یا کراکر (Cracker)

از نظر ماهیت کار این گروه از هکرها جزو گروه هکرهای کلاه سیاه می‌باشند. فعالیت این گروه از هکرها بیشتر در مورد نرم‌افزارها و سیستم‌های کامپیوتری می‌باشد که دارای قفل بوده و بصورت مجانی و یا اختصاصی مورد استفاده قرار می‌گیرد. فعالیت این گروه در حوزه نرم افزار بسیار فراگیر می‌باشد.

برخی از تولیدکنندگان نرم‌افزار بر این باورند که کراکرها به سراغ محصولات آنها نمی‌روند. با وجودی که متخصصان امنیت کامپیوتر به روش‌های گوناگون در این مورد تولیدکنندگان و کاربران این گونه محصولات هشدار می‌دهند ولی باز شاهد ضعف‌های این محصولات می‌باشیم. این ضعف‌ها می-تواند بصورت نقص در کد یا منطق برنامه و یا حتی عدم سازگاری محصول نرم‌افزاری با سایر محصولات موجود بر روی سیستم بروز نماید.

این امر در بین محصولات نرم افزار ایرانی گستردگی بیشتری نسبت به سایر نرم افزارها دارد، که جای تأمل و بررسی بیشتری دارد.

۴.۴. پراکر (Preaker)

از قدیمی‌ترین و در واقع هکرهای اولیه‌ای بودند که برای کارشان نیاز به کامپیوتر نداشتند و بیشتر کارشان نفوذ به خطوط تلفن برای تماس مجانی ، استراق سمع و ... بود.

۴.۵. هکرهای جوان (Script Kiddies)

این گروه از هکرها با سایر گروه‌های هک تفاوت دارند و هکرهای جوان بر خلاف سایر هکرها که ابزار و برنامه‌های مورد نیاز را خودشان می‌نویسند و برای هک از معلومات خود استفاده می‌کنند، با استفاده از برنامه‌های خدماتی ویژه هک که به وسیله دیگران نوشته شده است مانند (Sub 7) و به راحتی از طریق اینترنت و یا فروشگاه‌ها قابل تهیه می‌باشند، به سیستم‌های کامپیوتری خسارت وارد می‌نمایند.

این گروه از هکرها بیشتر با هدف سرگرمی و یا نمایش دانش خود به سایر دوستان و همکلاسی‌های خود اقدام به این کار می‌نمایند، ولی گاهی مشاهده شده است که از این کار برای اهداف دیگری بهره گرفته‌اند، بعنوان مثال می‌توان به هکی که توسط تعدادی دانش آموزان در یکی از مدارس آمریکا صورت گرفت اشاره نمود که در آن دانش‌آموزان با نفوذ به شبکه مدرسه نمرات امتحانی خود را تغییر داده‌اند.

بسیاری از کارشناسان معتقدند که ظهور رو به رشد هکرهای جوان، مهمترین تهدید برای امنیت سیستم‌های کامپیوتری شده است. زیرا با وجود ابزارهای موجود و در اختیار این گروه و نیز وقتی که این گروه از هکرها برای این کار صرف می‌کنند، از کار انداختن سایت های اینترنتی و یا نفوذ به یک شبکه، نیاز به داشتن اطلاعات کامل در مورد کامپیوتر ندارد.

۵. هکرها را کجا می توان پیدا کرد

هکرها در همه جا حضور دارند، اما شاید به اشتباه تصور کنید که سیستم شما به علت کوچک بودن و یا نداشتن اطلاعات مهم برای آن ها جالب توجه نیست، باید به یاد داشته باشیم که هکرها همیشه کامپیوترهای خاص را هدف قرار نمی‌دهند، آنها کامپیوترهای زیادی را کنترل می-کنند تا حفره‌های امنیتی را در آن‌ها پیدا کنند. یک هکر ممکن است یک کارمند شرکت باشد که برای انتقام گرفتن به سیستم‌های شرکت صدمه می زند و یا فردی باشد که از سیستم شما برای حمله به سیستم دیگر استفاده می‌کند.

بهترین راه مقابله با هکرها بالا بردن امنیت سیستم‌های کامپیوتری می‌باشد. این کار ممکن است با تهیه سیستم‌های نرم‌افزاری و سخت‌افزاری انجام شود. هیچ گاه به یک روش خاصی جهت حفظ امنیت اکتفا نکنید و نسخه جدید هر نرم افزار را تهیه کنید و دسترسی کاربران را به اطلاعات کنترل نمایید

یک توصیه

سعی کنید از هکرهای کلاه سفید بعنوان مشاوره امنیت سیستمهای کامپیوتری خود استفاده کنید و همیشه به خاطر داشته باشید که بر خلاف مدیران سیستم و شبکه که دارای وقت کمی برای جستجو و تحقیق و بررسی نقاط ضعف سیستم و بر طرف نمودن آنها می باشند، هکرها دارای وقت کافی و منابع اطلاعاتی مناسب برای صدمه زدن به سیستمهای شما می باشند.

فصل چهارم

اعتبار سنجی و تصدیق هویت

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 اعتبار سنجی(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 معمولی‌ترین حالت شامل نام کاربری و کلمه عبور می‌باشند. در صورت نیاز به بالاتر بودن پیچیدگی فرآیند 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 سرور 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. علّت استفاده از این روش مجتمع سازی و ساده‌سازی پیاده‌سازی عمل Authentication است. با استفاده از امکانات موجود نیاز به استقرار یک سرور 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.

به عبارت دیگر اعتبار سنجی تضمین می‌کند که اطلاعات از همان جایی ارسال شده است که ادعا می‌کند. بطور مثال اگر از طریق پست صورت‌حسابی برایتان ارسال گردد و در آن از شما خواسته شود که هزینه پرداختی را به یک نام و آدرس فرستنده متفاوتی ارسال کنید، در آن صورت متوجه خواهید شد که شخص می‌خواهد شما را فریب دهد. به همین ترتیب، فایروال‌هایی که در پشت مسیریاب‌ها اجرا می‌شوند

می‌توانند کنترل کنند که یک بسته اطلاعاتی از همان کامپیوتری ارسال شده است که خودش ادعا می‌کند. این فناوری، کامل و بی نقص نیست، اما به تدریج در حال توسعه است.

اگر محتویات یک بسته اطلاعاتی با آنچه که اعلام می‌کند مطابقت نداشته باشد، مسیریاب از هدایت آن امتناع نموده و یک پیام اخطار به مدیر شبکه می فرستد.

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

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

د – اعمال فهرست(های) روش ساخته شده از 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 فرآیندی 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.

زمانی‌که Authorization بر روی شبکه فعال شده باشد، سرور شبکه‌ای که مسئولیت Authorization را بر عهده دارد اطلاعات کاربر را از روی پایگاه داده کاربرها استخراج می‌کند. این پایگاه داده می‌تواند بر روی سرور 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 فرآیند جمعی AAA است. طی این فرآیند، گزارشی از عملکرد کاربران یا سخت‌افزارهایی که هویت آنها طی اعمال Authentication و Authorization تایید شده است، توسط

سرور AAA تهیه می‌شود. این عمل می‌تواند با استفاده از سرورهای خارجی که از 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.

۲.۳. فعال سازی Accounting

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

AAA Server .۴

افزایش تعداد سرورهای شبکه در پی راه اندازی سرویس‌های مختلف، پایگاه‌های داده‌ی مختلف، کاربران و سیاست‌های متنوع دسترسی افراد را به منابع مختلف ایجاد خواهد کرد، بطوریکه پس از مدتی جهت اضافه کردن کاربر جدید به سیستم، نیاز به تعریف آن در چندین سرور وجود خواهد داشت. این پراکندگی و لزوم اعمال سیاست های متمرکز، مدیران شبکه را ناچار به اتخاذ تدابیری مؤثرتر می‌کند. لذا تعریف و پیاده سازی AAA Server یکی از این تدبیرهاست که بر دسترسی کاربران به منابع شبکه ، مدیریت مستقیم و متمرکز نظارت خواهد داشت.

AAA Server یک برنامه نرم افزاری سرور است که امکان دسترسی کاربران را با منابع کامپیوتری شبکه برقرار می‌کند. این برنامه برای شبکه‌های Enterprise سرویس‌های Authentication، Authorization و Accounting را فراهم می آورد. در واقع AAA Server با دسترسی شبکه ، سرورهای Gateway، پایگاه‌های داده و جدول‌های اطلاعاتی کاربران در تعامل است. پروتکل استانداردی که اجازه ارتباط دستگاه-ها و نرم‌افزارهای مختلف را با AAA Server می‌دهد RADIUS می‌باشد (Remote Authentication Dial-In User Service).

Authentication، Authorization و Accounting اصطلاحاتی در یک چارچوب هستند که در کنترل هوشمند دسترسی کاربران نقش ایفا می کنند و پیشبرد سیاست گذاری، اصلاح کاربرد و تهیه اطلاعات مورد نیاز جهت راه اندازی سرویس ها از فایده های دیگر آن است. این پردازش های ترکیبی برای مدیریت شبکه و امنیت آن کاملا ضروری هستند.

منابع:

۱. "آشنایی با AAA Server"، کیانوش مرادیان، سایت تخصصی شبکه

۲. وب سایت گروه امداد امنیت کامپیوتری ایران http://ircert.com/

فصل پنجم

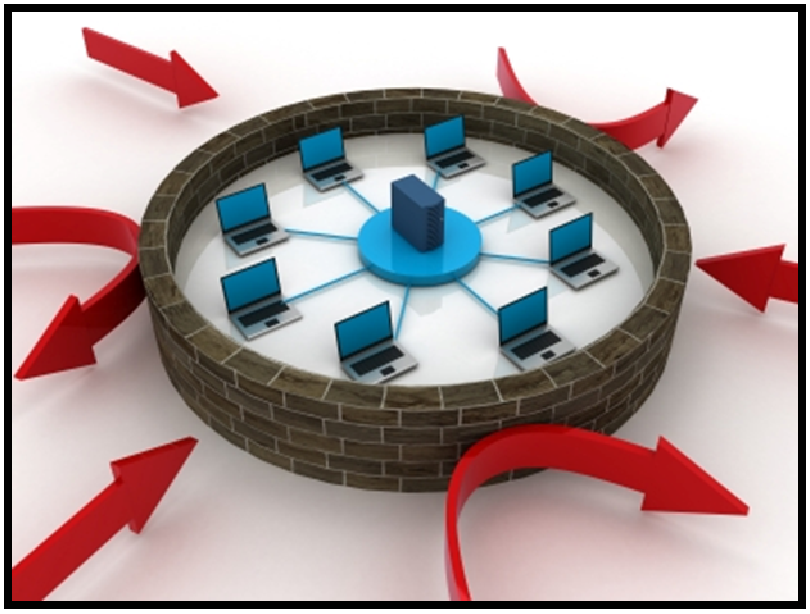
دیواره‌ی آتش

Firewall

۱. مقدمه

در صورت دستیابی سایرین به سیستم شما، کامپیوتر شما دارای استعداد بمراتب بیشتری در مقابل انواع تهاجمات می‌باشد. شما می‌توانید با استفاده و نصب یک فایروال[11] یا دیواره‌ی آتش، محدودیت لازم در خصوص دستیابی به کامپیوتر و اطلاعات را فراهم نمائید. به عبارت دیگر، فایروال وسیله‌ای است که کنترل دسترسی به یک کامپیوتر یا شبکه را بنابر سیاست امنیتی آن کامپیوتر یا شبکه تعریف می‌کند. علاوه بر آن از آنجایی که معمولاً یک فایروال بر سر راه ورودی یک شبکه می‌نشیند، لذا برای ترجمه آدرس شبکه نیز بکار گرفته می‌شود.

در بُعد اجرایی، فایروال‌ها حفاظت لازم در مقابل مهاجمان خارجی را ایجاد و یک لایه و یا پوسته حفاظتی پیرامون کامپیوتر و یا شبکه را در مقابل کدهای مخرب و یا ترافیک غیرضروری اینترنت، ارائه می‌نمایند (شکل ۱). با بکارگیری فایروال‌ها، امکان بلاک نمودن داده از مکانی خاص فراهم می‌گردد. امکانات ارائه شده توسط یک فایروال برای کاربرانی که همواره به اینترنت متصل و از امکاناتی نظیر DSL و یا مودم‌های کابلی استفاده می‌نمایند، بسیار حیاتی و مهم می‌باشد.



شکل۱ نمایش گرافیکی شیوه عمل فایروال در محافظت از شبکه

[11] Firewall

۲ . ویژگی‌های یک فایروال خوب

مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

۲ .۱. توانایی ثبت و اخطار

ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می‌رود و به مدیران شبکه این امکان را می دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می‌تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲ .۲. بازدید حجم بالایی از بسته های اطلاعات

یکی از تست‌های یک فایروال، توانایی آن در بازدید حجم بالایی از بسته‌های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده‌ای که یک فایروال می‌تواند کنترل کند برای شبکه‌های مختلف متفاوت است، اما یک فایروال قطعاً نباید به گلوگاه[۱۲] شبکه تحت حفاظتش تبدیل شود.

عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیت‌ها از طرف سرعت پردازنده و بهینه‌سازی کد نرم افزار بر کارایی فایروال تحمیل می‌شوند. عامل محدودکننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال نصب می‌شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۲ .۳. سادگی پیکربندی

سادگی پیکربندی[۱۳] شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه‌ها می‌شود به پیکربندی غلط فایروال بر می‌گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می‌کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزاری که بتواند سیاست‌های امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

۲ .۴. امنیت و افزونگی فایروال

امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعاً اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال، تأمین کننده امنیت فایروال و شبکه است:

[12] Bottleneck
[13] Configuration

الف- امنیت سیستم عامل فایروال: اگر نرم افزار فایروال بر روی سیستم عامل جداگانه‌ای کار می‌کند، نقاط ضعف امنیتی سیستم عامل، می‌تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی: یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روش‌ها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

۳. انواع فایروال‌ها

فایروال‌ها را بر حسب نوع فعالیت و روش انجام و ماهیت کارشان به دسته‌بندی مختلفی تقسیم می‌کنند. با اینکه هر یک از مدل‌های فوق دارای مزایا و معایب خاص خود می‌باشند، تصمیم در خصوص استفاده از یک فایروال به مراتب مهم‌تر از تصمیم در خصوص نوع فایروال است.

۳ .۱.دسته‌بندی اول

در این دسته‌بندی فایروال‌ها را برحسب ماهیت‌شان در دو قالب سخت‌افزاری (خارجی) و نرم‌افزاری (داخلی)، تقسیم می‌کنند.

۳ .۱. ۱. فایروال های سخت افزاری

این نوع از فایروال ها که به آنان فایروال‌های شبکه نیز گفته می‌شود، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط DSL قرار خواهند گرفت. تعداد زیادی از تولیدکنندگان و برخی از مراکز ISP دستگاههائی با نام "روتر" را ارائه می دهند که دارای یک فایروال نیز می‌باشند. فایروال‌های سخت‌افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می‌نمایند (امکان استفاده از آنان به منظور حفاظت یک دستگاه کامپیوتر نیز وجود خواهد داشت). در صورتی که شما صرفاً دارای یک کامپیوتر پشت فایروال می‌باشید و یا این اطمینان را دارید که سایر کامپیوترهای موجود بر روی شبکه نسبت به نصب تمامی patch ها، بهنگام بوده و عاری از ویروس‌ها و یا کرم‌ها می‌باشند، ضرورتی به استفاده از یک سطح اضافه حفاظتی (یک نرم افزار فایروال) نخواهید داشت. فایروال‌های سخت افزاری، دستگاه‌های سخت افزاری مجزائی می‌باشند که دارای سیستم عامل اختصاصی خود می‌باشد. بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می‌گردد.

۳ .۱. ۲. فایروال‌های نرم افزاری

برخی از سیستم‌های عامل دارای یک فایروال تعبیه شده درون خود می باشند. در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می باشد، پیشنهاد می‌گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن‌سازی کامپیوتر و اطلاعات، ایجاد گردد. (حتی اگر از یک فایروال خارجی یا سخت افزاری استفاده می نمائید). در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی‌باشد، می‌توان اقدام به تهیه یک فایروال نرم افزاری کرد. با توجه به عدم اطمینان لازم در خصوص دریافت نرم‌افزار از اینترنت با استفاده از یک کامپیوتر محافظت نشده، پیشنهاد می-گردد برای نصب فایروال از CD و یا DVD مربوطه استفاده گردد.

۳ .۲. دسته‌بندی دوم

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم، انجام می‌دهند، اما روش انجام کار توسط انواع مختلف، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می‌شود. بر این اساس در دسته‌بندی دیگری فایروال‌ها را به ۵ گروه تقسیم می‌کنند. همانطور که اشاره شد این دسته-بندی بر اساس روش کار فایروال‌ها انجام گرفته است و به شرح زیر است:

۳ .۲. ۱. فایروال‌های سطح مدار (Circuit-Level)

این فایروال‌ها به عنوان یک رله برای ارتباطات TCP عمل می‌کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می‌کنند و خود به جای آن رایانه به پاسخگویی اولیه می‌پردازند. تنها پس از برقراری ارتباط است که اجازه می-دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته‌های داده‌ای مرتبط اجازه عبور می‌دهند.

این نوع از فایروال‌ها هیچ داده‌ی درون بسته‌های اطلاعات را مورد بررسی قرار نمی‌دهند و لذا سرعت خوبی دارند. ضمناً امکان ایجاد محدودیت بر روی سایر پروتکل‌ها (غیر از TCP) را نیز نمی‌دهند.

۳ .۲. ۲. فایروالهای پروکسی سرور

فایروالهای پروکسی سرور به بررسی بسته‌های اطلاعات در لایه کاربرد می‌پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می‌کند و خود به جای آنها درخواست را ارسال می‌کند. نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه‌های کاربردی ارسال می‌کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می‌کند. از آنجایی که این فایروال‌ها پروتکل‌های سطح کاربرد را می‌شناسند، لذا می‌توانند بر مبنای این پروتکل‌ها محدودیت‌هایی را ایجاد کنند. همچنین آنها می‌توانند با بررسی محتوای بسته‌های داده‌ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می‌تواند به کندی این فایروال‌ها بیانجامد.

همچنین از آنجایی که این فایروال‌ها باید ترافیک ورودی و اطلاعات برنامه‌های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می‌یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتواند این فایروال‌ها را بکار گیرد. هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

۳ .۲. ۳. فیلترهای (Nosstateful packet)

این فیلترها روش کار ساده‌ای دارند. آنها بر مسیر یک شبکه می‌نشینند و با استفاده از مجموعه‌ای از قواعد، به بعضی بسته‌ها اجازه عبور می‌دهند و بعضی دیگر را بلوکه می‌کنند. این تصمیمات با توجه به اطلاعات آدرس‌دهی موجود در پروتکل‌های شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکل‌های لایه انتقال مانند سرآیندهای UDP و TCP اتخاذ می‌شود. این فیلترها زمانی می‌توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویس‌های مورد نیاز شبکه جهت محافظت داشته باشند.

همچنین این فیلترها می‌توانند سریع باشند چون همانند پروکسی‌ها عمل نمی‌کنند و اطلاعاتی درباره پروتکل‌های لایه کاربرد ندارند.

۳ .۲ .۴. فیلترهای (Stateful Packet)

این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آن‌ها تقریباً تمامی ترافیک ورودی را بلوکه می‌کنند، اما می‌توانند به ماشین‌های پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می‌کنند، انجام می‌دهند. این فیلترها، مکانیزم اصلی مورد استفاده جهت پیاده‌سازی فایروال در شبکه‌های مدرن هستند. این فیلترها می‌توانند رد پای اطلاعات مختلف را از طریق بسته‌هایی که در حال عبورند ثبت کنند.

برای مثال شماره پورت‌های TCP و UDP مبدأ و مقصد، شماره ترتیب TCP و پرچمهایTCP. بسیاری از فیلترهای جدید Stateful می‌توانند پروتکل‌های لایه کاربرد مانند HTTP و FTP را تشخیص دهند و لذا می-توانند اعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکل‌ها انجام دهند.

۳ .۲ .۵. فایروال‌های شخصی

فایروال‌های شخصی ، فایروال‌هایی هستند که بر روی رایانه‌های شخصی نصب می‌شوند. آنها برای مقابله با حملات شبکه‌ای طراحی شده‌اند. معمولاً از برنامه‌های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه‌ها اجازه می‌دهند که به کار بپردازند.

نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می‌دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می‌شوند، فایروال شبکه نمی‌تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولاً نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

۴. نحوه پیکربندی بهینه

اکثر محصولات فایروال تجاری (هم سخت افزاری و هم نرم افزاری) دارای امکانات متعددی بمنظور پیکربندی بهینه می باشند. با توجه به تنوع بسیار زیاد فایروال‌ها، می‌بایست به منظور پیکربندی بهینه آنان به مستندات ارائه شده مراجعه شود تا مشخص گردد که آیا تنظیمات پیش فرض فایروال نیاز شما را تأمین می‌نماید یا خیر. پس از پیکربندی یک فایروال یک سطح امنیتی و حفاظتی مناسب در خصوص ایمن‌سازی اطلاعات انجام شده است. لازم است به این موضوع مهم اشاره گردد که پس از پیکربندی یک فایروال نمی-بایست بر این باور باشیم که سیستم ما همواره ایمن خواهد بود. فایروال‌ها یک سطح مطلوب حفاظتی را ارائه می‌نمایند ولی هرگز عدم تهاجم به سیستم شما را تضمین نخواهند کرد. استفاده از فایروال به همراه سایر امکانات حفاظتی نظیر نرم افزارهای آنتی‌ویروس و رعایت توصیه‌های ایمنی می‌تواند یک سطح مطلوب حفاظتی را برای شما و شبکه شما به دنبال داشته باشد.

۵. موقعیت‌یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از:

- **موقعیت و محل نصب از لحاظ توپولوژیکی:** معمولاً مناسب بنظر می‌رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می‌کند.
- **قابلیت دسترسی و نواحی امنیتی:** اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی و تنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. درحالی که با استفاده از ناحیه DMZ سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.
- **مسیریابی نامتقارن:** بیشتر فایروال‌های مدرن سعی می‌کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می‌کنند تا تنها بسته‌های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.
- **فایروال‌های لایه‌ای:** در شبکه‌های با درجه امنیتی بالا بهتر است دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می‌دهد. معمولاً بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها، سایرین بتوانند امنیت شبکه را تامین کنند.

منابع:

۱. وب سایت امنیت اطلاعات (ایکس نت) به آدرس: http://www.xtak.net

فصل ششم

پنهان سازی اطلاعات

Information Hiding

۱. مقدمه

در رمزنگاری برای جلوگیری از دسترسی غیرمجاز به محتوای پیام از مخدوش نمودن آن استفاده می‌شود بطوریکه این پیام مخدوش و غیر قابل درک شده توسط شخص مجاز و با استفاده از یک کلید سرّی قابل بازسازی است و اطلاعات به راحتی استخراج می‌شود، لیکن همین امر برای شخص غیر مجازی که به اطلاعات رمز شده و الگوریتم رمزنگاری دسترسی دارد بدون داشتن کلید ناممکن است.

ارسال پیام رمز شده روی کانال عمومی صورت می پذیرد و همین امر موجب شکل گیری موج عظیمی از حملات مختلف روی این سیستم شده است بطوریکه می‌توان گفت جنگ سختی میان طراحان الگوریتم‌های رمزنگاری از یک طرف و تحلیل گران این الگوریتم‌ها ازطرف دیگر همواره وجود داشته و دارد. طراحان برای افزایش محافظت از محرمانگی وتمامیت پیام سعی در پیچیده‌تر کردن الگوریتم ها برای مقاومت در برابر تحلیل‌های مختلف را دارند، و تحلیل‌گران با نبوغ و استفاده از نقاط ضعف الگوریتم‌ها راههای نفوذ را جستجو می‌کنند.

اکنون بیایید از دیدگاه دیگری به این مسئله نگاه کنیم. آیا اگر ما بتوانیم بگونهای احتمال انجام شدن تحلیل روی الگوریتم را کاهش دهیم میزان محافظت از محرمانگی و تمامیت پیام افزایش نخواهد یافت؟ بدون شک اگر ما بتوانیم این احتمال را افزایش دهیم پاسخ پرسش فوق مثبت خواهد بود.

ایده استفاده از پنهان سازی اطلاعات راهی است در جهت نیل به هدف فوق که در۱۹۸۳ توسط سیمونز تحت عنوان مسئله زندانیان[۱۴] مطرح شد:

> آلیس و باب زندانی هستند و برای طرح نقشه فرار، آلیس می‌خواهد پیامی را برای باب ارسال کند. ارتباط آلیس و باب از طریق ارسال و دریافت نامه‌هایی با محتوای مجاز که توسط ویلی زندانبان چک می‌شود، ممکن است. بدیهی است در صورتیکه ویلی ارسال پیامی غیر مجاز را تشخیص دهد به سرپرست زندان اطلاع خواهد داد و این موجب قطع ارتباط آلیس و باب خواهد شد. بنابراین آلیس باید پیام خود را در قالب یک پیام عادی و پنهان شده در آن برای باب ارسال نماید طوریکه سوءظن ویلی برانگیخته نشود و باب هم قادر به فهم کامل پیام آلیس باشد.

۲. پنهان سازی اطلاعات در تاریخ

استفاده از پنهان سازی اطلاعات در گذشته دارای سابقه ای طولانی است سربازان یونانی برای انتقال پیام به جای آنکه طبق روال عادی آن زمان که روی موم کشیده شده بر لوح پیام نوشته می‌شد پیام را بنویسند روی خود لوح می نوشتند و سپس روی آن را با موم می‌پوشانید و اکنون از این لوح مثل یک لوح عادی استفاده می‌کردند و روی آن یک پیام عادی می‌نوشتند و یا اینکه برای ارسال پیام از میان نیروهای دشمن سر بردگان را می‌تراشیدند و روی پوست سر آنان نقشه یا پیام را خال‌کوبی می‌کردند، و مدتی بعد

[14] prisoner’s problem

که موی سر این بردگان بلند می‌شد و روی پیام را می‌گرفت آنها می‌توانستند به راحتی از میان سرزمین‌ها و اراضی مربوط به دشمن عبور کنند و در مقصد با تراشیدن مجدد موی سر آنان پیام استخراج می‌شد. همچنین استفاده از جوهرهای نامرئی از زمان‌های بسیار دور در نقاط مختلف دنیا مرسوم بوده است.

در طول دهه۱۹۸۰مارگارت تاچر که از نشت اطلاعات و اسناد کابینه‌اش بسیار ناراحت بود توانست با استفاده از یک پردازشگر کلمات مشخصات هر وزیر را در فاصله بین کلمات به نحوی ثبت کند و بنابراین وزرای خائن را از این طریق ردیابی نماید. در حال حاضر نیز تکنیکی مشابه در ردیابی انتشارات الکترونیکی مورد استفاده قرار می‌گیرد که به شماره سریال[۱۵] می توان اشاره کرد.

۳. روشهای پنهان سازی اطلاعات

۳ .۱. اصطلاحات پایه‌ای

- ✓ cover-medium

شیئی که پیام در قالب آن منتقل می شود و می‌تواند شامل تصویر، متن و... باشد که در این متن به آن میزبان گفته می‌شود.

- ✓ Embedded-message

همانطور که از اسمش پیداست، پیام توکار داده‌ای است که باید به صورت پنهانی منتقل شود که برای اینکار داخل میزبان جاسازی می‌گردد و در این متن به آن پیام گفته می‌شود.

- ✓ Stego-medium

حاصل ترکیب پیام در میزبان است که در این متن به آن شئ ترکیبی گفته می شود.

- ✓ Stego-key

اطلاعات سرّی است که مشترک بین فرستنده و گیرنده است و به منظور جاسازی و بازیابی اطلاعات از آن استفاده می‌شود.

- ✓ Embedder(E)

تابع جاسازی کننده پیام.

- ✓ extractor(E-1)

تابع بازسازی کننده پیام .

۳ .۲. مراحل انجام روشهای پنهان‌سازی

برای انجام هر روش پنهان‌سازی دو کار زیر باید صورت پذیرد:

الف) در آنچه به عنوان میزبان (مثلاً یک متن) بکار می‌رود این تحقیق باید انجام شود که چه تغییراتی را می توان روی آن اعمال نمود بدون اینکه تفاوت قابل درکی بین نمونه اصلی و نمونه ای که در آن تغییرات ایجاد شده بوجود آید. این تحقیق برای انجام عملیات فشرده

[15] serial number

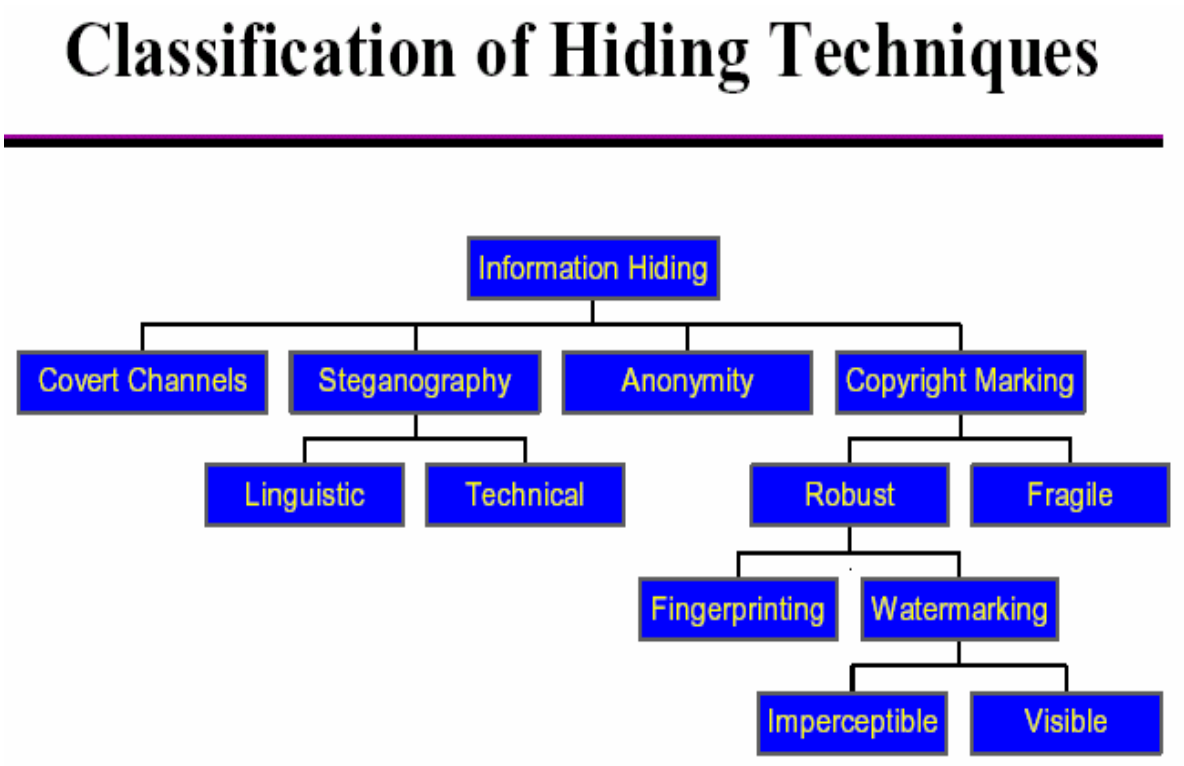
سازی نیز جهت حذف اجزاء زائدی که وجود یا عدم وجود آنها در کیفیت تاثیر چندانی ندارد انجام می شود.

ب) از مشخصه تحقیق شده در قسمت (الف) برای پنهان کردن اطلاعات استفاده شود.

اگرخواسته باشیم پنهان سازی اطلاعات رابه صورت فرمولی عنوان کنیم می توان گفت: برای قطعه ای اصلی از داده d که به عنوان میزبان مطرح است حد آستانه ای وجود دارد t که چنانچه زیر این حد آستانه، تغییراتی در d بوجود آوریم قابل تشخیص برای حسگرهای انسانی نیست. این حد آستانه از راه آزمایش بدست می آید و در افراد مختلف متفاوت است لیکن کمترین مقدار آن از لحاظ حس انسانی می‌تواند برای t در نظر گرفته شود. بنابراین ما همواره می توانیم تغییر c در d را زیر حد آستانه t بوجود آوریم طوری که قابل تشخیص بوسیله احساس نباشد $t>d+c$

۳.۳. انواع روشهای پنهان سازی

روشهای پنهان سازی اطلاعات رامی توان به صورت زیر دسته بندی کرد، بطوریکه بلوک دیاگرام و تعاریفی که در اولین کارگاه بین المللی پنهان سازی اطلاعات برای انجام این عمل عنوان شد به شرح زیر است



Ref: F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding - A Survey," in *Proc. Of the IEEE*, vol. 87, No. 7, July 1999, pg. 1063

۴.۳. موارد دیگر دارای اهمیت در طراحی یک روش پنهان سازی

- ✓ **شفافیت**[16]: شفافیت سیستم بیان می‌دارد که موضوع میزبان قبل و بعد از جاسازی در پیام نباید تفاوت محسوسی داشته باشد چرا که هدف غیر قابل حس کردن انتقال پیام است و در حقیقت امنیت یک سیستم پنهان‌سازی در همین مسئله شفافیت نهفته است و هر چقدر که شباهت موضوع میزبان پیام در هر دو حالت عاری و حاوی پیام بیشتر باشد امنیت این سیستم در سطح بالاتری قرار دارد.

- ✓ **مقاومت**[17]: مقاومت یک سیستم پنهان سازی به معنای این است که پیام پنهان شده درمقابل اعمال تغییرات ناخواسته و غیر عمدی که وجود نویز در طول مسیر انتقال بوجود می آورد و یا اعمال تغییرات عمدی که توسط حمله کننده فعال به منظور تغییر پیام یا از بین بردن آن انجام می گیرد مقاومت لازم را داشته باشد.

- ✓ **ظرفیت**[18] : در یک سیستم پنهان سازی هر چقدر بتوان پیام بیشتری را در یک میزبان مخفی نمود این سیستم مناسب تر خواهد بود حجم دادهای که می‌توان در یک میزبان ذخیره کرد دقیقا بستگی به ماهیت میزبان دارد و این که تا چه حدی می‌توان داده در آن پنهان کرد بدون اینکه در شفافیت آن تاثیری جدی بگذارد. سه ویژگی فوق بطور بسیار تنگاتنگی در ارتباط با یکدیگر هستند بدین معنی که باثابت فرض کردن ویژگی اول وافزایش ویژگی دوم ویژگی سوم حتما کاهش خواهد یافت

ثابت =مقاومت*ظرفیت

۵.۳. روش پوشیده نگاری [19]

بسیاری از شما نوشتن با آبلیمو و آب پیاز را در کودکی تجربه کرده‌اید و شاید هم برای دوستانتان این تردستی را اجرا کرده باشید که با گرم کردن کاغذ نوشته‌ها نمایان می‌شدند. از قلم‌های بی‌رنگ که استفاده کرده‌اید؟ قلم‌هایی که جوهر نامرئی دارند. نوشته‌های این قلم‌ها تنها با استفاده از نورهای مخصوص نمایش داده می‌شوند. برای نوشتن عبارات مخفی و سری بر روی کاغذ می‌توان از این روش استفاده کرد. و تنها کسانی می‌توانند نوشته‌ی روی آن را بخوانند که از شیوه کار آگاه بوده و چراغ مخصوص آن را داشته باشند. عبارت پوشیده نگاری متشکل از دو کلمه یونانی stego به معنی مخفی و graphos به معنای نوشته که روی هم معنی نوشته مخفی را تداعی می‌کنند. دراین متن از ترجمه پوشیده نگاری برای آن استفاده شده است.

در رمزنگاری دسترسی به محتوای پیام برای فرد غیر مجاز ناممکن می‌گردد، لیکن در پوشیده‌نگاری موجودیت پیام انکار می‌شود. هدف رمزنگاری حفظ محرمانگی و تمامیت پیام است که با رمزکردن آن حاصل می‌شود. پوشیده‌نگاری هم همین اهداف را با پنهان نمودن پیام دنبال می‌کند؛ بعلاوه در پوشیده-

[16] Transparency
[17] Resistance
[18] capacity
[19] steganography

نگاری انتخاب جا و ترتیب پنهان نمودن پیام نیز با بهره‌گیری از نوعی رمز در چینش بیت‌های پیام لابه-لای بیت‌های میزبان صورت می‌پذیرد. به عبارت دیگر برخلاف رمزنگاری که فایل حفاظت شده را کاملاً حساس جلوه می‌دهد و جلب توجه می‌کند، این روش از ناآگاهی افراد، برای جلوگیری از دستیابی آن‌ها به اطلاعات خاص بهره می‌برد. این کار شبیه پنهان‌کردن اشیای گرانبها در قوطی بیسکویت، داخل کابینت آشپزخانه است؛ جایی که معمولاً هیچ دزدی احتمالش را نمی‌دهد.

همچنین می‌توان پیام را قبل از جاسازی داخل میزبان با استفاده از الگوریتم‌های رمزنگاری به صورت رمز در آورد و سپس عمل پنهان‌سازی را انجام داد. بطوریکه می‌توان گفت با استفاده از پوشیده‌نگاری در حقیقت سه لایه حفاظتی بسیار محکم در دسترسی به پیام ایجاد خواهد شد: اول اینکه وجود ارتباط نامحسوس است و این هدف اصلی در پوشیده‌نگاری است و بنابراین گذشتن از اولین مانع کار چندان سادهای نخواهد بود. در صورتیکه وجود اطلاعات در یک میزبان مورد سوءظن واقع شود مرحله دوم پیدا کردن الگوریتم پنهان‌سازی است طوریکه باید جا و ترتیب پنهان شدن اطلاعات معلوم شود. لیکن در این مرحله نیز چون از یک کلید بنام stego_key برای جاسازی پیام استفاده شده، دانستن این کلید ضروری است و بنابراین گذشتن از این مرحله نیز با دشواری همراه خواهد بود و چنانچه دو مرحله قبلی با موفقیت پشت سر گذاشته شوند، اکنون به متن رمزی دسترسی پیدا شده است که تازه در این مرحله مسائل مربوط به رمزنگاری مطرح می‌گردند.

علاوه بر این استفاده از پنهان‌سازی اطلاعات در امور ارتباطات گاهاً گریز ناپذیر است. همان طور که در سناریوی مطرح شده در این مورد عنوان گردید آلیس مجبور به استفاده از این روش است.

در دنیای واقعی کنونی نیز استفاده از رمزنگاری قوی در ارتباطات شخصی توسط دولت‌ها محدود شده است که علّت این محدودیت سوء استفاده از این علم برای انجام فعالیت‌های جنایی و تروریستی و سایر امور مرتبط با این موضوعات می‌باشد و به شدت توسط ارگان‌های مربوطه کنترل می‌گردد، بطوریکه در صورت انجام تخلّف از فرستنده و گیرنده پیام رمزی توضیح خواسته می‌شود.

اساس کار روش‌های موجود در پوشیده‌نگاری را می‌توان به دو دسته کلّی زیر تقسیم کرد:

- روش هایی که بر پایه نقص در سیستم بینایی انسان[20] (hvs) استوار است.
- روش هایی که بر پایه نقص در سیستم شنوایی انسان[21] (hos) استوار است.

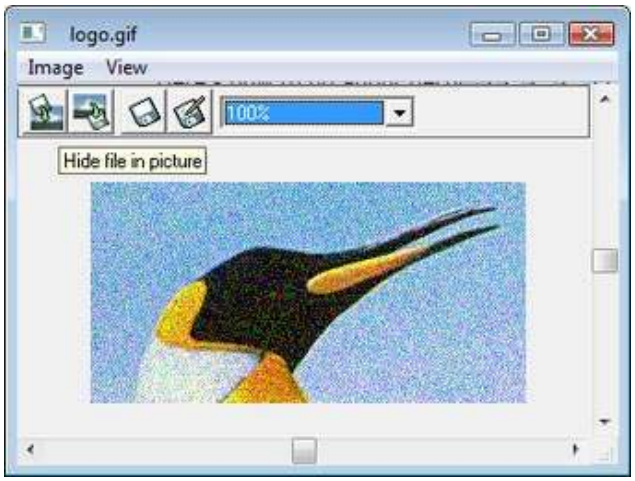
سیستم شنیداری انسان آنقدر دقیق نیست که تغییرات جزئی ایجاد شده در قطعات صوت را تشخیص دهد، بنابراین از همین نقطه ضعف می‌توان استفاده نمود و داده‌ای را لابه‌لای قطعات صوت جاسازی کرد. همچنین سیستم دیداری انسان دارای خصوصیاتی است که بر مبنای آنها روش‌های پنهان‌سازی متفاوتی در قالب تصاویر خصوصاّ تصاویر ثابت ابداع شده‌اند.

[20] human video system
[21] human audio system

۳ .۵ .۱. ابزارهای پوشیده‌نگاری و بازیابی

- **Hide in Picture**

این نرم‌افزار رایگان به شما اجازه می‌دهد که فایل‌ها را درون تصاویر GIF و BMP پنهان کنید. همچنین با استفاده از آن می‌توانید فایل‌های پنهان شده توسط دوستان‌تان را بازیابی کنید. علاوه بر آن برای افزایش ضریب امنیتی، امکان انتخاب رمزعبور برای داده‌های پنهان شده را خواهید داشت. در شکل زیر نمایی از این نرم‌افزار را مشاهده می‌کنید.



برای دانلود آن می‌توانید به http://sourceforge.net/projects/hide-in-picture/ مراجعه کنید.

نرم‌افزارهای ویندوزی دیگری هم وجود دارند، که امکان استفاده از انواع مختلف فایل را برای پوشش ظاهری اطلاعات فراهم می‌آورند. برای مثال wbStego می‌تواند اطلاعات شما را در فایل‌هایPDF، HTML و همچنین Bitmap پنهان کند.

همچنین برای پنهان‌سازی متن در فایل‌های MP3 می‌توان نرم‌افزار mp3stego را بکار برد، که هم به صورت گرافیکی و هم در محیط داس قابل استفاده است.

- **استفاده از Command line و ادغام فایل زیپ با گیف**

با استفاده از خط فرمان[۲۲] می‌توانید یک فایل ZIP را درون یک تصویر با فرمت GIF پنهان نمایید. فایل نهایی در این روش ظاهراً همان تصویر اولیه است، در حالیکه به وسیله برنامه‌های مربوط به هر دو پسوند(گیف و زیپ)، قابل اجرا است.

شیوه کار این تکنیک کاملاً وابسته به خصوصیات فایل های زیپ و گیف است. فایل‌های GIF اطلاعات را در قسمت ابتدایی خود نگهداری می‌کنند. در حالی که فایل ZIP اطلاعات را در قسمت انتهایی خود ذخیره می‌کنند. حال برنامه‌های ویرایش تصویر اطلاعات را از اول فایل نهایی می‌خوانند و تصویر را نشان می‌دهند. ولی برنامه‌های فشرده ساز، اطلاعات انتهای فایل نهایی را خوانده و بخش زیپ شده را برایتان باز می کنند.

[22] Command line

مشکلی که در این روش پیش می‌آید این است که فایل‌ها نهایی با همه‌ی نرم‌افزارهایی که قابلیت نمایش و استخراج فایل‌های ZIP را دارند، قابل بازیابی نیست. برای مثال نرم‌افزار ۷ zip-در بسیاری از موارد در استخراج داده‌ها از فایل نهایی ناتوان است. اما WinRAR به خوبی از پس این کار برمی‌آید.

برای استفاده از این روش باید ابتدا دو فایل مربوطه را در یک پوشه کپی کرده و سپس به صورت زیر عمل کنید (پوشه مربوطه را ترجیحاً در root یکی از درایوها ایجاد نمایید):

در ویندوز، منوی استارت را باز کنید و بر روی گزینه Run کلیک کنید. حال با تایپ دستور cmd درRun ، پنجره Command برای شما باز خواهد شد. در این پنجره با استفاده از دستور cd به پوشه‌ای که در بالا توضیح داده شد، مراجعه کنید.

```
Start> Run > cmd
```

سپس با استفاده از دستور زیر می‌توانید عمل پوشیده‌نگاری را انجام دهید:

```
copy /B filename.gif+filename.zip target.gif
```

توجه کنید که فایل نهایی که در اینجا با نام target.gif مشخص شده است، پس از انجام عملیات در پوشه مربوطه ایجاد می‌شود.

توجه کنید که برای امنیت هر چه بیشتر، می‌توانید قبل از انجام این فرآیند، هنگام آماده سازی فایل زیپ، آن را رمزگذاری کنید. آنگاه آن را با فایل گیف مورد نظرتان ادغام کنید. با این کار حتی اگر کسی اشتباهاً تصویر نهایی را با برنامه‌های فشرده ساز باز کند، چیزی عایدش نخواهد شد.

۲.۵.۳. برخی کاربردهای پوشیده‌نگاری:

- شما می‌توانید برای جلوگیری از پیگرد انتشار غیرقانونی محتوا و فایل‌های تولیدی تان از این روش استفاده کنید. فرض کنید که یک تصویر یا فایل PDF تولید کرده‌اید؛ با استفاده از این روش می‌توانید کپی رایت اثر خود را در فایل مربوطه پنهان کنید، تا در صورت لزوم بعداً بتوانید از حق خود دفاع کنید.
- تصور کنید که شما می‌خواهید رمزعبور یا یک فایل مهم اداری را توسط ایمیل برای همکارتان ارسال کنید، آیا استفاده از پوشیده‌نگاری راه خوبی برای این کار نیست؟ اگر ایمیل شما یا همکارتان هم توسط شخص دیگری (مثلاً سرویس دهنده اینترنت تان) هک و کنترل شود، کمتر کسی می‌داند که در یک تصویر معمولی چه اطلاعاتی ممکن است وجود داشته باشد!
- اگر بخواهید در یک تالار گفتگوی عمومی فایل یا اطلاعاتی خاصی را در اختیار برخی افراد قرار دهید، پوشیده‌نگاری بهترین راه حل است.
- شاید هم پوشیده‌نگاری جایگزین خوبی برای تردستی‌های آبلیمو و آب پیازتان باشد. حداقل دیگر به حرارت و آتش و کارهای خطرناک نیازی ندارید!

و نکته آخر اینکه، استفاده از Steganography یکی از بهترین روش‌ها برای مخفی کردن اطلاعات حساس شما است. پس با آگاهی از روشهای پوشیده‌نگاری می‌توانید اطلاعات خود باشید.

۶.۳. روش نشان حق تکثیر[۲۳]

در حقیقت نشان‌های حق‌تکثیر جنبه تجاری استفاده از پنهان‌سازی اطلاعات هستند که برای جلوگیری از استفاده‌های غیرمجاز تولیدات الکترونیکی اطلاعات به صورت نامحسوس و غیرقابل تفکیک از محصول داخل آن جاسازی می‌شود که در مواقع لزوم برای پیگیری استفاده غیرمجاز و اثبات حق مالکیت از طریق قانون می‌تواند به مالک واقعی محصول کمک کند. نشان حق تکثیر را می توان به دو دسته تقسیم کرد:

الف) نقش زمینه[۲۴]

نشان نقش زمینه اطلاعاتی هستند که داخل محصول الکترونیکی جا سازی می شوند و یا بهتر بگوئیم ترکیب می شوند طوری که از مقاومت بسیار بالایی برخوردار می‌باشند و معمولا این اطلاعات شامل آرم یا علامت مخصوص شرکت یا مالک است که به آن لوگو[۲۵] گفته می‌شود. فرقی که پوشیده نگاری با نقش زمینه دارد این است که در پوشیده نگاری آنچه مهم است پیامی است که داخل میزبان پنهان شده است و میزبان در حقیقت سدی است برای محافظت ازپیام لیکن درنقش زمینه آنچه که مهم است میزبان است و پیام برای محافظت از میزبان داخل آن جاسازی شده است. یکی از خصوصیات ضروری نقش زمینه داشتن مقاومت بسیار بالا است طوری که به هیچ وجه قابل تفکیک از میزبان نباشد و از بین بردن آن منجر به از بین رفتن میزبان شود.

ب) اثر انگشت[۲۶]

اثر انگشت اطلاعاتی است که برای محافظت در مقابل استفاده غیر مجاز از محصولات نرم افزاری داخل آن پنهان می شود طوری که استفاده کننده مجاز با وارد کردن آنها به صورت عدد شناسایی[۲۷] قادر به استفاده از آن خواهد بود. همچنین این عدد شناسایی برای پیگیری کپی‌های غیر مجاز از نرم افزار نیز می تواند مورد استفاده قرار گیرد.

۴. الگوریتم‌های پنهان‌سازی اطلاعات

تاکنون الگوریتم‌های گوناگونی برای پنهان‌سازی اطلاعات طراحی شده‌اند. پوشیده‌نگاری در دو حوزه زمان و تبدیل انجام می‌شود :

حوزه زمان شامل آن دسته از الگوریتم‌هایی می‌شود که بیت‌های پیام عیناً لابه‌لای بیت‌های میزبان گنجانیده می‌شوند. به عنوان مثال در حالتی‌که از تصویر به عنوان میزبان استفاده می‌شود در تکنیک LSB که یکی از ساده‌ترین آنها می‌باشد بیت‌های پیام در کم ارزش‌ترین بیت هر پیکسل گنجانیده می‌شوند .

---

[23] copyright marking
[24] watermarking
[25] logo
[26] fingerprinting
[27] ID Number

حوزه تبدیل شامل آن دسته از روش‌هایی است که اطلاعات بیت‌های پیام روی تمام یا قسمتی از بیت‌های میزبان پخش می‌گردد . در این روش‌ها از تبدیلاتی همچون DCT وDFT استفاده می‌شود. به عنوان مثال در همان حالت قبلی برای پنهان‌سازی در قالب تصویر ابتدا تصویر به بلوک‌های ۸ x 8 پیکسل تقسیم شده سپس روی این بلوک‌ها تک تک DCT گرفته می‌شود بیت‌های پیام با دستکاری ضرائب بدست آمده از این تبدیلات روی این ضرائب پیاده شده و در پایان DCT-1 گرفته می‌شود. و یا در تکنیک SS با شبیه‌سازی پیام به صورت نویز آن را روی طیف فرکانسی میزبان می‌گسترانند (گسترش باند باریک روی باند وسیع) .

دسته دیگری از تکنیک‌های پنهان‌سازی که تنها در پوشیده‌نگاری کاربر دارند به تکنیک‌های زبانی[۲۸] معروف هستند. در این روش‌ها پیام در قالب یک متن عادی پنهان می‌گردد. روش کار به این صورت است که با استفاده از یک دیکشنری که کلمات آن به دسته‌های مختلفی تقسیم می‌گردند و یک متن انتخابی، می‌توان بیت‌های پیام را به صورت یک متن کاملا عادی به عنوان مثال یک متن ادبی پنهان کرد. Nicetext یکی از الگوریتم‌هایی است که در این مورد پیاده سازی شده است.

۵. جمع بندی

در این قسمت به لحاظ اهمیتی که شاخه پنهان‌سازی اطلاعات در ارتباط با تجارت الکترونیک و مسائل مربوط به ایجاد امنیت و اطمینان برای عرضه محصولات نرم‌افزاری و الکترونیکی روی شبکه اینترنت دارد همچنین به لحاظ آشنایی با ارتباطات مخفی و پوشیدهای که به مدد این علم قابل حصول می‌باشند به معرفی و بررسی آن پرداخته شد لیکن به خاطر محدودیت حجم نوشتار توضیح جزئیات امکان پذیر نبود .

کاربرد این علم در امور تجاری بسیار زیاد است و در کشورهایی که متعهد به اجرای قانون حق تکثیر می‌باشند خدمات خوبی برای صاحبان تولیدات الکترونیکی روی شبکه اینترنت ارائه نموده است. در کشور ما در حال حاضر متأسفانه به دلیل عدم رعایت قانون ذکر شده شاید اهمیت کاربردی این علم زیاد مورد توجه نباشد، لیکن با پیشرفت صنعت IT در آیندهای نه چندان دور، توجه بیشتر به آن گریز ناپذیر خواهد بود.

همچنین به لحاظ ارتباط این علم با مسائل امنیتی در برقراری ارتباطات پوشیده توجه ارگان‌ها و نهادهای ذیربط و ذینفع را می‌طلبد و غفلت از آن زیان‌های جبران ناپذیری را متصور می‌سازد.

منبع:

نگهبان دات کام

[28] Linguistic

فصل هفتم

نقش عوامل انسانی در امنیت شبکه

Human’s Role in Network Security

۱. مقدمه

همانطور که می‌دانیم یک سیستم کامپیوتری از چهار عنصر سخت افزار، سیستم عامل، برنامه های کاربردی و کاربران، تشکیل می‌گردد. سخت افزار شامل حافظه، دستگاههای ورودی، خروجی و پردازشگر بوده که به عنوان منابع اصلی پردازش اطلاعات، استفاده می‌گردند. برنامه‌های کاربردی شامل کامپایلرها، سیستم‌های بانک اطلاعاتی، برنامه‌های تجاری و بازرگانی، بازی‌های کامپیوتری و موارد متنوع دیگری بوده که روش بخدمت گرفتن سخت افزار جهت نیل به اهداف از قبل تعریف شده را مشخص می نمایند. کاربران، شامل انسان، ماشین و دیگر کامپیوترها می‌باشد. هر یک از کاربران سعی در حل مشکلات تعریف شده خود از طریق بکارگیری نرم افزارهای کاربردی در محیط سخت افزار می‌نمایند. سیستم عامل، نحوه استفاده از سخت افزار را در ارتباط با برنامه‌های کاربردی متفاوتی که توسط کاربران گوناگون نوشته و اجرا می-گردند، کنترل و هدایت می‌نماید. بمنظور بررسی امنیت در یک سیستم کامپیوتری، می‌بایست به تشریح و تبیین جایگاه هر یک از عناصر موجود در یک سیستم کامپیوتری پرداخته گردد.

در این راستا، قصد داریم به بررسی نقش عوامل انسانی در رابطه با امنیت اطلاعات پرداخته و جایگاه هر یک از مولفه‌های موجود را تبیین و تشریح نمائیم. اگر ما بهترین سیستم سخت افزاری و یا سیستم عامل را به خدمت بگیریم ولی کاربران و یا عوامل انسانی درگیر در یک سیستم کامپیوتری، پارامترهای امنیتی را رعایت ننمایند، کاری را از پیش نخواهیم برد. وضعیت فوق مشابه این است که شما بهترین اتومبیل با درجه بالای امنیت را طراحی و یا تهیه نمائید ولی آن را در اختیار افرادی قرار دهید که نسبت به اصول اولیه رانندگی توجیه نباشند (عدم رعایت اصول ایمنی) .

ما می‌بایست به مقوله امنیت اطلاعات در عصر اطلاعات نه بصورت یک کالا و یا محصول بلکه بصورت یک فرآیند نگاه کرده و امنیت را در حد یک محصول خواه نرم‌افزاری و یا سخت‌افزاری تنزل ندهیم. هر یک از موارد فوق، جایگاه خاص خود را با وزن مشخص شدهای دارند و نباید به بهانه پرداختن به امنیت اطلاعات وزن یک پارامتر را بیش از آن‌چیزی که هست در نظر گرفت و پارامتر دیگری را نادیده گرفته و یا وزن غیر قابل قبولی برای آن مشخص نمائیم. بهرحال ظهور و عرضه شگفت انگیز تکنولوژی‌های نو در عصر حاضر، تهدیدات خاص خود را نیز بدنبال خواهد داشت. ما چه کار می‌بایست بکنیم که از تکنولوژی‌ها استفاده مفیدی را داشته و در عین حال از تهدیدات مستقیم و یا غیر مستقیم آنان نیز مصون بمانیم؟ قطعاً نقش عوامل انسانی که استقاده کنندگان مستقیم این نوع تکنولوژی‌ها می باشند، بسیار محسوس و مهم است.

با گسترش اینترنت و استفاده از آن در ابعاد متفاوت، سازمان‌ها و موسسات با مسائل جدیدی در رابطه با امنیت اطلاعات و تهاجم به شبکه‌های کامپیوتری مواجه می‌باشند. صرفنظر از موفقیت و یا عدم موفقیت مهاجمان و علیرغم آخرین اصلاحات انجام شده در رابطه با تکنولوژی‌های امنیتی، عدم وجود دانش و اطلاعات لازم (سواد عمومی ایمنی) کاربران شبکه های کامپیوتری و استفاده کنندگان اطلاعات حساس در

یک سازمان، همواره بعنوان مهمترین تهدید امنیتی مطرح و عدم پایبندی و رعایت اصول امنیتی تدوین شده، می تواند زمینه ایجاد پتانسیل‌هائی شود که توسط مهاجمین استفاده و باعث بروز مشکل در سازمان گردد. مهاجمان همواره بدنبال چنین فرصت‌هایی بوده تا با اتکاء به آنان به اهداف خود نایل گردند. در برخی حالات اشتباه ما زمینه موفقیت دیگران را فراهم می‌نماید. اگر سعی نمائیم بر اساس یک روش مناسب درصد بروز اشتباهات خود را کاهش دهیم به همان نسبت نیز شانس موفقیت مهاجمان کاهش پیدا خواهد کرد.

مدیران شبکه (سیستم)، مدیران سازمان و کاربران معمولی جملگی عوامل انسانی در یک سازمان می‌باشند که حرکت و یا حرکات اشتباه هر یک می تواند پیامدهای منفی در ارتباط با امنیت اطلاعات را بدنبال داشته باشد. در ادامه به بررسی اشتباهات متداولی خواهیم پرداخت که می تواند توسط سه گروه یاد شده انجام و زمینه بروز یک مشکل امنیتی در رابطه با اطلاعات حساس در یک سازمان را باعث گردد.

۲. اشتباهات متداول مدیران سیستم

مدیران سیستم، به افرادی اطلاق می‌گردد که مسئولیت نگهداری و نظارت بر عملکرد صحیح و عملیاتی سیستم‌ها و شبکه موجود در یک سازمان را برعهده دارند. در اغلب سازمانها افراد فوق، مسئولیت امنیت دستگاهها، ایمن‌سازی شبکه و تشخیص ضعف‌های امنیـتی موجود در رابطه با اطلاعات حساس را نیز برعهده دارند. بدیهی است واگذاری مسئولیت‌های متعدد به یک فرد، افزایش تعداد خطا و اشتباه را بدنبال خواهد داشت. فشار عصبی در زمان انجام کار مستمر بر روی چندین موضوع متفاوت و بصورت همزمان، قطعاً احتمال بروز اشتباهات فردی را افزایش خواهد داد. در ادامه با برخی از خطاهای متداولی که ممکن است توسط مدیران سیستم انجام و سازمان مربوطه را با تهدید امنیتی مواجه سازد، آشنا خواهیم شد.

۲ .۱. عدم وجود یک سیاست امنیتی شخصی

اکثر قریب به اتفاق مدیران سیستم دارای یک سیاست امنیتی شخصی بمنظور انجام فعالیت های مهمی نظیر امنیت فیزیکی سیستم‌ها، روش‌های بهنگام‌سازی یک نرم‌افزار و روشی بمنظور بکارگیری patchهای جدید در زمان مربوطه نمی‌باشند. حتی شرکت‌های بزرگ و شناخته شده به این موضوع اذعان دارند که برخی از سیستم‌های آنان با همان سرعت که یک باگ و یا اشکال تشخیص و شناسایی می‌گردد، توسط patch مربوطه اصلاح نشده است. در برخی حالات، مدیران سیستم حتی نسبت به آخرین نقاط آسیب‌پذیر تشخیص داده شده نیز آگاهی بهنگام شده‌ای را نداشته و قطعاً در چنین مواردی انتظار نصب patch مربوطه نیز توقعی بی‌مورد است. وجود نقاط آسیب‌پذیر در شبکه می‌تواند یک سازمان را در معرض تهدیدات جدی قرار دهد. امنیت فرآیندی است که می‌بایست بصورت مستمر به آن پرداخته شود و هرگز به اتمام نمی‌رسد. در این راستا لازم است، بصورت مستمر نسبت به آخرین حملات بهمراه تکنولوژی های

مربوطه، آگاهی لازم کسب و دانش خود را بهنگام نمائیم. اکثر مدیران سیستم، کارشناسان حرفهای و خبره امنیتی نمی‌باشند، در این رابطه لازم است، بمنظور افزایش حفاظت و ایمن سازی شبکه، اطلاعات و دانش مربوطه بصورت مستمر ارتقاء یابد. افرادیکه دارای گواهینامه‌های خاصی امنیتی و یا دانش و اطلاعات اضافه در رابطه با امنیت اطلاعات می‌باشند، همواره یک قدم از کسانی مهارت آنان صرفاً محدود به شبکه است، جلوتر می‌باشند. در ادامه، پیشنهاداتی بمنظور بهبود وضعیت امنیتی سازمان و افزایش و ارتقاء سطح معلومات مدیران سیستم، ارائه می‌گردد :

- بصورت فیزیکی محل کار و سیستم خود را ایمن سازید .زمینه استفاده از سیستم توسط افرادیکه در محدوده کاری شما فعالیت دارند ، می بایست کاملاً کنترل شده و تحت نظارت باشد .
- هر مرتبه که سیستم خود را ترک می کنید، عملیات logout را فراموش نکنید .در این رابطه می-توان یک زمان time out را تنظیم تا در صورت فراموش نمودن عملیات logout ، سیستم قادر به حفاظت خود گردد.
- خود را عضو خبرنامه‌های متفاوت امنیتی کرده تا شما را با آخرین نقاط آسیب پذیر آشنا نمایند. درحقیقت آنان چشم شما در این معرکه خواهند بود(استفاده مفید از تجارب دیگران).
- سعی گردد بصورت مستمر از سایت‌های مرتبط با مسائل امنیتی بازدید گردد تا در زمان مناسب با پیام‌های هشداردهنده امنیتی در رابطه با نرم افزارهای خارج از رده و یا نرم افزارهای غیر اصلاح شده (unpatched) آشنا گردید.
- مطالعه آخرین مقالات مرتبط با مسائل امنیتی یکی از مراحل ضروری و مهم در فرآیند خود آموزشی (فراگیری) مدیران شبکه است. بدین ترتیب این اطمینان بوجود خواهد آمد که مدیر مربوطه نسبت به آخرین اطلاعات و مسائل مربوطه امنیتی در کمیته های موجود، توجیه است .
- استفاده از یادداشت‌ها و مقالات در ارتباط با هر نوع اطلاعات حساس نظیر رمزهای عبور و هر چیزی که ممکن است زمینه ساز ایجاد یک پتانسیل آسیب‌پذیر و دستیابی به سیستم مطرح گردد را محدود نمائید. در صورتیکه از این نوع اطلاعات استفاده می‌شود، قبل از ترک محل کار، آنها را از بین ببرید. افرادیکه دارای سوء نیت بوده و در محدوده کاری شما می‌باشند، می‌توانند از مزایای ضعف‌های شناخته شده استفاده نمایند، بنابراین ضروری است استفاده از چنین یادداشت-هائی محدود و یا بصورت کامل حذف گردد.

۲.۲. اتصال سیستم های فاقد پیکربندی مناسب به اینترنت

همزمان با گسترش نیازهای سازمان، سیستم ها و سرویس دهندگان جدیدی بر اساس یک روال معمول به اینترنت متصل می‌گردند. قطعاً توسعه سیستم با هدف افزایش بهره‌وری در یک سازمان دنبال خواهد شد. اکثر اینچنین سیستمهائی بدون تنظیمات امنیتی خاص به اینترنت متصل شده و می تواند زمینه بروز آسیب و حملات اطلاعاتی توسط مهاجمان را باعث گردد (در بازه زمانی که سیستم از لحاظ امنیتی بدرستی ممیزی نشده باشد ، این امر امکان پذیر خواهد بود).

مدیران سیستم ممکن است به این موضوع استناد نمایند که سیستم جدید بوده و هنوز کسی آن را نمی شناسد و آدرس IP آن شناخته شده نیست ، بنابراین امکان شناسائی و حمله به آن وجود نخواهد داشت .طرز فکر فوق ، یک تهدید برای هر سازمان بشمار می رود . افراد و یا اسکریپت های پویش اتوماتیک در اینترنت ، بسرعت عملیات یافتن و تخریب این نوع سیستم های آسیب پذیر را دنبال می نمایند. در این راستا ، شرکت هائی خاصی وجود دارد که موضوع فعالیت آنان شبکه بوده و برای تست سیستم های تولیدی خود بدنبال سیستم های ضعیف و آسیب پذیر می گردند.(سیستم آسیب پذیر ما ابزار تست دیگران خواهد شد). بهرحال همواره ممکن است افرادی بصورت مخفیانه شبکه سازمان شما را پویش تا در صورت وجود یک نقطه آسیب پذیر، از آن برای اهداف خود استفاده نمایند. لازم است در این راستا تهدیدات و خطرات را جدی گرفته و پیگری لازم در این خصوص انجام شود. در این رابطه موارد زیر پیشنهاد می گردد :

- قبل از اتصال فیزیکی یک کامپیوتر به شبکه ، مجوز امنیتی لازم با توجه به سیاست های تدوین شده امنیتی برای آن صادر گردد (بررسی سیستم و صدور مجوز اتصال)
- کامپیوتر مورد نظر می بایست شامل آخرین نرم افزارهای امنیتی لازم بوده و از پیکربندی صحیح آنان می بایست مطمئن گردید.
- در صورتیکه لازم است بر روی سیستم مورد نظر تست های شبکه ای خاصی صورت پذیرد ، سعی گردد امکان دستیابی به سیستم فوق از طریق اینترنت در زمان تست ، بلاک گردد.
- سیستمی را که قصد اتصال آن به اینترنت وجود دارد ، نمی بایست شامل اطلاعات حساس سازمان باشد.
- سیستم مورد نظر را تحت برنامه های موسوم به Intrusion Detection System قرار داده تا نرم افزارهای فوق بسرعت نقاط آسیب پذیر و ضعف های امنیتی را شناسائی نمایند.

۳.۲. اعتماد بیش از اندازه به ابزارها

برنامه‌های پویش و بررسی نقاط آسیب پذیر،اغلب بمنظور اخذ اطلاعات در رابطه وضعیت جاری امنیتی شبکه استفاده می گردد. پویشگرهای تشخیص نقاط آسیب پذیر، اطلاعات مفیدی را در ارتباط با امنیت سیستم نظیر: مجوزهای فایل، سیاستهای رمز عبور و سایر مسائل موجود، ارائه می‌نمایند. بعبارت دیگر پویشگران نقاط آسیب پذیر شبکه، امکان نگرش از دید یک مهاجم را به مدیریت شبکه خواهند داد. پویشگرهای فوق، عموماً نیمی از مسائل امنیتی مرتبط را به سیستم واگذار نموده و نمی‌توان به تمامی نتایج بدست آمده توسط آنان بسنده و محور عملیات خود را بر اساس یافته‌های آنان قرار دهیم. در این رابطه لازم است متناسب با نوع سیستم عامل نصب شده بر روی سیستم‌ها از پویشگران متعدد و مختص سیستم عامل مربوطه استفاده گردد (اخذ نتایج مطلوبتر). بهرحال استفاده از این نوع نرم افزارها قطعاً باعث شناسائی سریع نقاط آسیب پذیر و صرفه جوئی زمان می‌گردد ولی نمی‌بایست این تصور وجود داشته باشد که استفاده از آنان بمنزله یک راه حل جامع امنیتی است. تاکید صرف بر نتایج بدست آمده توسط آنان، می‌تواند نتایج نامطلوب امنیتی را بدنبال داشته باشد. در برخی موارد ممکن است لازم باشد، بمنظور تشخیص نقاط آسیب پذیر یک سیستم، عملیات دستی انجام و یا حتی اسکریپت های خاصی در این رابطه نوشته گردد.

۲ .۴. عدم مشاهده لاگ‌ها (Logs)

مشاهده لاگ های سیستم، یکی از مراحل ضروری در تشخیص مستمر و یا قریب الوقوع تهدیدات است . لاگ ها، امکان شناسائی نقاط آسیب پذیر متداول و حملات مربوطه را فراهم می نمایند. بنابراین می توان تمامی سیستم را بررسی و آن را در مقابل حملات مشخص شده ، مجهز و ایمن نمود. در صورت بروز یک تهاجم ، با استفاده از لاگ های سیستم ، تسهیلات لازم بمنظور ردیابی مهاجمان فراهم می گردد.(البته بشرطی که آنان اصلاح نشده باشند) . لاگ ها را بصورت ادواری بررسی و آنها را در یک مکان ایمن ذخیره نمائید.

۲ .۵. اجرای سرویس ها و یا اسکریپت های اضافه و غیر ضروری

استفاده از منابع و شبکه سازمان، بعنوان یک زمین بازی شخصی برای تست اسکریپت‌ها و سرویس‌های متفاوت، یکی دیگر از اشتباهات متداولی است که توسط اکثریت قریب به اتفاق مدیران سیستم انجام می‌شود. داشتن اینچنین اسکریپت‌ها و سرویس‌های اضافه‌ای که بر روی سیستم اجرا می‌گردند ، باعث ایجاد مجموعه‌ای از پتانسیل‌ها و نقاط ورود جدید برای یک مهاجم می‌گردد (در صورتیکه سرویس‌های اضافه و یا اسکریپت‌ها بر روی سرویس‌دهنده اصلی نصب و تست گردند، مشکلات می‌تواند مضاعف گردد). در صورت نیاز به تست اسکریپت‌ها و یا اجرای سرویس‌های اضافه، می‌بایست عملیات مورد نظر خود را از طریق یک کامپیوتر ایزوله شده انجام داد (هرگز از کامپیوتری که به شبکه متصل است در این راستا استفاده نگردد) .

۳. اشتباهات متداول مدیران سازمان ها

مدیران سازمان، به افرادی اطلاق می گردد که مسئولیت مدیریت ، هدایت و توسعه سازمان را بر عهده داشته و با منابع متفاوت موجود در سازمان نظیر بودجه ، سروکار دارند. امروزه استفاده از اینترنت توسط سازمان‌ها و موسسات، مزایای متعددی را بدنبال دارد. واژه " تجارت الکترونیکی" بسیار متداول و استراتژی تجارت الکترونیکی، از جمله مواردی است که در هر برنامه‌ریزی تجاری به آن توجه خاص می‌گردد. در صورتیکه سازمان ها و موسسات دارای یک استراتژی امنیتی مشخص شده‌ای نباشند، اتصال به شبکه جهانی تهدیدی در ارتباط با اطلاعات حساس خواهد بود. در ادامه به برخی از اشتباهات متداول که از ناحیه مدیران سازمان بروز و تاثیر منفی در ارتباط با امنیت اطلاعات در سازمان را بدنبال خواهد داشت، اشاره می گردد:

۳ .۱. استخدام کارشناسان آموزش ندیده و غیرخبره

بدون تردید ، کارشناسان آموزش دیده و خبره ، یکی از منابع ارزشمند درهر سازمان محسوب می گردند. همواره می بایست از کارشناسان ورزیده در ارتباط با امنیت در یک سازمان استفاده گردد. فرصت سعی و خطاء نیست و ممکن است در این محدوده زمانی چیزی را که یک سازمان از دست می دهد بمراتب بیشتر از چیزی است که می خواهد بدست آورد. امنیت اطلاعات از جمله مقولاتی است که برای یک سازمان دارای جایگاهی است و همواره می بایست بهترین تصمیم دررابطه با استفاده از منابع انسانی ماهر ، اتخاذ

گردد. استفاده از یک کارشناس غیر ماهر در امور امنیت اطلاعات و شبکه در یک سازمان ، خود تهدیدی امنیتی است که بر سایر تهدیدات موجود اضافه خواهد شد . (ما نمی توانیم مسئولیت پیاده سازی استراتژی امنیتی در سازمان را به افرادی واگذار نمائیم که در این رابطه اطلاعات و دانش لازم را ندارند) .

۲.۳. فقدان آگاهی لازم در رابطه با تاثیر یک ضعف امنیتی بر عملکرد سازمان

بسیاری از مدیران سازمان بر این باور می باشند که " این مسئله برای ما اتفاق نخواهد افتاد " و بر همین اساس و طرز فکر به مقوله امنیت نگاه می نمایند . بدیهی است در صورت بروز مشکل در سازمان ، امکان عکس العمل مناسب در مقابل خطرات و تهدیدات احتمالی وجود نخواهد داشت . این مسئله می تواند بدلیل عدم آشنائی با ابعاد و اثرات یک ضعف امنیتی در سازمان باشد . در این رابطه لازم است به این نکته اشاره گردد که همواره مشکل برای دیگران بوجود نمی آید و ما نیز در معرض مشکلات فراوانی قرار خواهیم داشت .بنابراین لازم است همواره و بصورت مستمر مدیران سازمان نسبت به اثرات احتمالی یک ضعف امنیتی توجیه و دانش لازم در اختیار آنان قرار گیرد . در صورت بروز یک مشکل امنیتی در سازمان ، مسئله بوجود آمده محدود به خود سازمان نشده و می تواند اثرات منفی متعددی در ارتباط با ادامه فعالیت سازمان را بدنبال داشته باشد. در عصر اطلاعات و دنیای شدید رقابت ، کافی است سازمانی لحظاتی آنچیزی باشد که نمی بایست باشد ، همین امر کافی است که تلاش چندین ساله یک سازمان هرز و در برخی حالات فرصت جبران آن نیز وجود نخواهد داشت .

- تاثیر منفی بر سایر فعالیت های تجاری online سازمان
- عاملی برای توزیع اطلاعات غیر مفید و غیر قابل استفاده در یک چرخه تجاری
- عرضه اطلاعات حساس مشتریان به یک مهاجم و بمخاطره افتادن اطلاعات خصوصی مشتریان
- آسیب جدی وجهه سازمان و بدنبال آن از دست دادن مشتریان و همکاران تجاری

۳.۳. عدم تخصیص بودجه مناسب برای پرداختن به امنیت اطلاعات

مجاب نمودن یک مدیر سازمان مبنی بر اختصاص بودجه مناسب برای پرداختن به مقوله امنیت اطلاعات در سازمان از حمله مواردی است که چالش های خاص خود را خواهد داشت .مدیران، تمایل دارند بودجه را به حداقل مقدار خود برسانند، چراکه آنان یا اطلاعات محدودی در رابطه با تاثیر وجود ضعف های امنیتی در عملکرد سازمان را دارند و یا در برخی حالات بودجه ، آنان را برای اتخاذ تصمیم مناسب محدود می نماید.اینترنت یک شبکه جهانی است که فرصت های جذاب و نامحدود تجاری را برای هر بنگاه تجاری فراهم می نماید، با رعایت امنیت اطلاعات و حفا ظت مناسب از داده های حساس ،امکان استفاده از فرصت های تجاری بیشتری برای یک سازمان فراهم خواهد شد. با اختصاص یک بودجه مناسب برای پرداختن و بهاء دادن به مقوله امنیت اطلاعات در یک سازمان ، پیشگیری های لازم انجام ودر صورت بروز مسائل بحرانی ، امکان تشخیص سریع آنان و انجام واکنش های مناسب فراهم می گردد . بعبارت دیگر با در نظر گرفتن بودجه مناسب برای ایمن سازی سازمان ، بستر مناسب برای حفاظت سیستم ها و داده های حساس در یک سازمان فراهم خواهد شد . قطعا" تولید و عرضه سریع اطلاعات در سازمان های مدرن و مبتنی بر

اطلاعات ، یکی از مهمترین شاخص های رشد در عصر حاضر بوده و هر آنچیزی که می تواند خللی در فرآیند فوق ایجاد نماید ، باعث توقف و گاها" برگشت به عقب یک سازمان ، می گردد.

۳ .۴. اتکاء کامل به ابزارها و محصولات تجاری

اگر از یک سازمان سوال شود که چگونه خود را در مقابل حملات حفاظت نموده اید ؟ اغلب آنان در پاسخ خواهند گفت :" ما از یک فایروال شناخته شده و یک برنامه ویروس یاب بر روی سرویس دهنده استفاده می کنیم ، بنابراین ما در مقابل حملات ایمن خواهیم بود " . توجه داشته باشید که امنیت یک فرآیند است نه یک محصول که با خریداری آن خیال خود را در ارتباط با امنیت راحت نمائیم . مدیران سازمان لازم است شناخت مناسب و اولیه ای از پتانسل های عمومی یک فایروال و یا برنامه های ویروس یاب داشته باشند (قادر به انجام چه کاری می باشند و چه کاری را نمی توانند انجام دهند. مثلا" اگر ویروس جدیدی نوشته و در شبکه توزیع گردد ، برنامه های ویروس یاب موجود قادر به تشخیص و برخورد با آن نخواهند بود.این نوع برنامه ها صرفا" پس از مطرح شدن یک ویروس و آنالیز نحوه عملکرد آن می بایست بهنگام شده تا بتوانند در صورت بروز وضعیتی مشابه با آن برخورد نمایند) . ابزارهائی همچون فایروال و یا برنامه های ویروس یاب ، بخشی از فرآیند مربوط به ایمن سازی اطلاعات حساس در یک سازمان بوده و با بکارگیری آنان نمی توان این ادعا را داشت که آنان سازمان را بطور کامل در مقابل تهاجمات ، حفاظت خواهند نمود .

۳ .۵. یک مرتبه سرمایه گذاری در ارتباط با امنیت

امنیت مفهمومی فراگیر و گسترده بوده که نیازمند هماهنگی و سرمایه گذاری در دو بعد تکنولوژی و آموزش است. هر روز ما شاهد ظهور تکنولوژی های جدیدی می باشیم . ما نمی توانیم در مواجهه با یک تکنولوژی جدید بصورت انفعالی برخورد و یا عنوان نمائیم که ضرورتی به استفاده از این تکنولوژی خاص را نداریم . بکارگیری تکنولوژی عملا" صرفه جوئی در زمان و سرمایه مادی را بدنبال داشته و این امر باعث ارائه سرویس های مطلوبتر و ارزانتر به مشتریان خواهد شد. موضوع فوق هم از جنبه یک سازمان حائز اهمیت است و هم از نظر مشتریان ، چراکه ارائه سرویس مطلوب با قیمت تمام شده مناسب یکی از مهمترین اهداف هر بنگاه تجاری محسوب شده و مشتریان نیز همواره بدنبال استفاده از سرویس ها و خدمات با کیفیت و قیمت مناسب می باشند. استفاده از تکنولوژی های جدید و سرویس های مرتبط با آنان،همواره تهدیدات خاص خود را بدنبال خواهد داشت . بنابراین لازم است به این موضوع توجه شود که امنیت یک سرمایه گذاری پیوسته را طلب می نماید، چراکه با بخدمت گرفتن تکنولوژی ها ی نو بمنظور افزایش بهره وری در یک سازمان ، زمینه پرداختن به امنیت می بایست مجددا" و در ارتباط با تکنولوژی مربوطه بررسی و در صورت لزوم سرمایه گذاری لازم در ارتباط با آن صورت پذیرد . تفکر اینکه، امنیت یک نوع سرمایه گذاری یکبار مصرف است ، می تواند از یکطرف سازمان را در استفاده از تکنولوژی ها ی نو با تردید مواجه سازد و از طرف دیگر با توجه به نگرش به مقوله امنیت (یکبار مصرف) ، بهاء لازم به آن داده نشده و شروع مناسبی برای پیاده سازی یک سیستم امنیتی و حفاظتی مناسب را نداشته باشیم.

۴. اشتباهات متداول کاربران معمولی

کاربران ، به افرادی اطلاق می گردد که طی روز با داده ها ی حساس در یک سازمان سروکار داشته و تصمیمات و فعالیت های آنان، داده ها ی حساس و مقوله امنیت و حفاظت از اطلاعات را تحت تاثیر مستقیم قرار خواهد داد. در ادامه با برخی از اشتباهات متداولی که این نوع استفاده کنندگان از سیستم و شبکه مرتکب می شوند ، اشاره می گردد.

۴ .۱. تخطی از سیاست امنیتی سازمان

سیاست امنیتی سازمان، اعلامیه‌ای است که بصورت جامع، مسئولیت هر یک از پرسنل سازمان (افرادیکه به اطلاعات و سیستم‌های حساس در سازمان دستیابی دارند) در ارتباط با امنیت اطلاعات و شبکه را تعریف و مشخص می‌نماید. سند و یا اعلامیه مورد نظر، بعنوان بخش لاینفک در هر مدل امنیتی بکارگرفته شده در سازمان محسوب می‌گردد. هدف عمده اعلامیه فوق، ارائه روشی آسان بمنظور شناخت و درک ساده نحوه حفاظت سیستم‌های سازمان در زمان استفاده است. کاربران معمولی، عموماً تمایل به تخطی از سیاست‌های تدوین شده امنیتی در یک سازمان را داشته و این موضوع می تواند عاملی مهم برای تحت تاثیر قراردادن سیستم‌های حساس و اطلاعات مهم سازمان در مواجهه با یک تهدید باشد. پیامد این نوع عملیات، بروز اشکال و خرابی در رابطه با اطلاعات ارزشمند در یک سازمان خواهد بود. بهمین دلیل است که اکیداً توصیه می‌گردد که اطلاعات لازم در رابطه با نقش کاربران در تبعیت از سیاست‌های امنیتی در سازمان به آنان یادآوری و بر آن تاکید گردد.

۴ .۲. ارسال داده حساس بر روی کامپیوترهای منزل

یکی از خطرناکترین روش ها در رابطه با داده های حساس موجود در یک سازمان ، فعالیتی است که باعث غیر فعال شدن تمامی پیشگیری‌های امنیتی ایجادشده و درگیر شدن آنان در یک فرآیند غیرامنیتی می-گردد. پرسنل سازمان عادت دارند،اطلاعات حساس سازمان را بر روی کامپیوتر منزل خود فوروارد (ارسال) نمایند . در حقیقت کاربران تمایل به فوروارد نمودن یک پروژه ناتمام و یا برنامه‌ریزی تجاری به کامپیوتر منازل خود را داشته تا از این طریق امکان اتمام کار خود در منزل را پیدا نمایند. کاربران به این موضوع توجه نکرده اند که تغییر محیط ایمن سازمان با کامپیوتر منزل خود که دارای ایمنی بمراتب کمتری است ، بطور جدی اطلاعات را در معرض آسیب و تهاجم قرار خواهد داد . در صورتیکه ضروری است که اطلاعات را به کامپیوترهای منزل فوروارد نمود، یک سطح مناسب ایمنی می‌بایست وجود داشته باشد تا این اطمینان بوجود آید که نوت بوک ها و یا کامپیوترهای منازل در مقابل مهاجمین اطلاعاتی حفاظت شده و ایمن می باشند.

۴ .۳. یادداشت داده های حساس و ذخیره غیرایمن آنان

ایجاد و نگهداری رمزهای عبور قدرتمند، فرآیندی مستمر است که همواره می‌بایست مورد توجه قرار گیرد. کاربران همواره از این موضوع نفرت دارند که رمز عبورهائی را ایجاد نمایند که قادر به بخاطرآوردن آن

نمی‌باشند. سیاست امنیتی تدوین شده سازمان می‌بایست تعیین نماید که یک رمز عبور چگونه می‌بایست ایجاد و نگهداری گردد. بخاطر سپردن چنین رمزعبوری همواره مسائل خاص خود را خواهد داشت. بمنظور حل اینچنین مشکلی، کاربران تمایل دارند که یادداشت‌های مخفی را نوشته و آنها را زیر صفحه کلید، کیف جیبی و یا هر مکان دیگر در محل کار خود نگهداری نمایند. یادداشت‌های فوق، شامل اطلاعات حساس در ارتباط با داده‌های مربوط به رمزعبور و سایر موارد مرتبط است. استفاده از روشهای فوق برای نگهداری اطلاعات، یک تخطی امنیتی است. دراین راستا لازم است، کاربران توجیه و به آنان آگاهی لازم داده شود که با عدم رعایت موارد مشخص شده امنیتی، پتانسیل‌های لازم بمنظور بروز مشکل در سیستم افزایش خواهد یافت. لازم است به کاربران، روش‌ها و تکنیک‌های متفاوت بخاطر سپردن رمز عبور آموزش داده شود تا زمینه استفاده کاربران از یاداشت برای ثبت اینگونه اطلاعات حساس کاهش یابد. سناریوی‌های متفاوت برای آنان تشریح و گفته شود که یک مهاجم با استفاده از چه روش‌هایی ممکن است به اطلاعات ثبت شده در یادداشت ها دست پیدا نموده و زمینه بروز مشکل را فراهم نماید.

۴.۴. دریافت فایل از سایت های غیر مطمئن

یکی از سرویس های اینترنت امکان دریافت فایل توسط کاربران است. کاربران بمنظور دریافت فایل از اینترنت ، اغلب از امتیازات خود تعدی و حتی سیاست ها ی موجود در سازمان را در معرض مخاطره و آسیب قرار می دهند . دریافت فایل از وب سایت های گمنام و یا غیر مطمئن باعث کمک در توزیع برنامه های مهاجم در اینترنت می گردد. بدین ترتیب ما بعنوان ابزاری برای توزیع یک برنامه مخرب در اینترنت تبدیل خواهیم شد. فایل ها و برنامه های دریافتی پس از آلودگی به نوع خاصی از برنامه مخرب (ویروس ، کرم ، اسب تراوا) ، می تواند تاثیرات منفی فراوانی را در ارتباط با عملکرد یک سازمان بدنبال داشته باشد .کاربران می بایست بندرت فایل هائی را از اینترنت دریافت در مواردیکه ضرورت این کار حس و به برنامه ای خاص نیاز باشد ، اکیداً توصیه می گردد که موضوع با دپارتمان IT (یا سایر بخش های مسئول در سازمان) درمیان گذاشته شود تا آنان بر اساس تجربه و دانش خود ، اقدام به تهیه برنامه مورد نظر از منابع مطمئن نمایند .

۴.۵. عدم رعایت امنیت فیزیکی

میزان آگاهی و دانش کاربران در رابطه با رعایت مسائل ایمنی خصوصاً امنیت فیزیکی ، بطرز کاملاً محسوسی افزایش امنیت و حفاظت داده ها ی حساس در یک سازمان را بدنبال خواهد داشت . عموماً ، رفتار کاربران در زمان استفاده از ایستگاه های کاری سازمان سهل انگارانه و فاقد سوادعمومی ایمنی است. کاربران ، اغلب ایستگاههای کاری خود را بدون در نظر گرفتن امنیت فیزیکی رها و screensaver آنان، بندرت دارای رمز عبور بوده و می تواند باعث بروزمسائل متعددی گردد. به کاربران می‌بایست آموزش‌های لازم در رابطه با استراتژی های متفاوت بمنظور استفاده از سیستم‌های سازمان داده شود: مطمئن شوید آنها قادرند بدرستی با اطلاعات حساس در سازمان برخورد نمایند و همواره پیامدهای عدم رعایت امنیت فیزیکی به آنان یادآوری گردد.

خلاصه

در این مقاله به بررسی اهم اشتباهات متداول که ممکن است از جانب عوامل انسانی در یک سیستم کامپیوتری بروز نماید ، اشاره و گفتته شد که عدم رعایت مسائل مربوطه می تواند زمینه بروز مشکلات متعدد ایمنی در سازمان را بدنبال داشته باشد . مواردااعلام شده را جدی گرفته و در صورت ضرورت مدل امنیتی جاری را بازسازی نمائید . به کاربران ، مدیران شبکه و حتی مدیران سازمان آموزش های لازم داده شود تا سطح آگاهی و اطلاعات آنان دررابطه با امنیت افزایش یابد (جملگی می بایست دارای یک سطح مناسب از سواد عمومی در ارتباط با امنیت اطلاعات باشیم). تداوم عملیات یک سازمان در عصر حاضر ارتباط مستقیم به رعایت مسائل ایمنی توسط عوامل انسانی آن سازمان دارد.

فصل هشتم

امنیت شبکه

Network Security

امنیت شبکه فرآیندی است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می‌شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تایید شده اند:

۱. شناسایی بخشی که باید تحت محافظت قرار گیرد.

۲. تصمیم گیری درباره مواردی که باید در مقابل آنها از بخش مورد نظر محافظت کرد.

۳. تصمیم گیری درباره چگونگی تهدیدات

۴. پیاده‌سازی امکاناتی که بتوانند از دارایی‌های شما به شیوه‌ای محافظت کنند که از نظر هزینه به صرفه باشد.

۵. مرور مجدد و مداوم فرآیند و تقویت آن درصورت یافتن نقطه ضعف

در واقع وقتی از امنیت شبکه صحبت می‌کنیم، مباحث زیادی قابل طرح و بررسی هستند، موضوعاتی که هر کدام به تنهایی می‌توانند در عین حال جالب، پرمحتوا و قابل درک باشند. اما وقتی صحبت کار عملی به میان می‌آید، قضیه تا حدودی پیچیده می‌شود. ترکیب علم و عمل، احتیاج به تجربه دارد و نهایت هدف یک علم بعد کاربردی آن است.

در اینجا برای ورود به نکات کاربردی که باید در مبحث امنیت شبکه بکار گرفته شود، باید با برخی از مهمترین و کاربردی ترین مطالب و نکات مربوطه آشنا شویم.

برای امنیت شبکه، ممکن است این سوال برایتان مطرح شود که "حالا باید از کجا شروع کرد؟ اول کجا باید ایمن شود؟ چه استراتژی را در پیش گرفت و کجا کار را تمام کرد؟"، به این ترتیب انبوهی از این قبیل سوالات فکر شما را مشغول می‌کند. برای اینکه یک استراتژی علمی - کاربردی داشته باشیم، توجه به نکات زیر بسیار مهم و ضروری است.

همیشه در امنیت شبکه موضوع لایه‌های دفاعی، موضوع داغ و مهمی است. در این خصوص نیز نظرات مختلفی وجود دارد. عده‌ای فایروال را اولین لایه دفاعی می‌دانند، بعضی‌ها هم Access List را اولین لایه دفاعی می‌دانند، اما واقعیت این است که هیچکدام از این‌ها، اولین لایه دفاعی محسوب نمی‌شوند. به خاطر داشته باشید که اولین لایه دفاعی در امنیت شبکه و حتی امنیت فیزیکی وجود یک خط مشی و سیاست امنیتی مناسب است. بدون سیاست امنیتی، لیست کنترل، فایروال و هر لایه دیگر، بی معنی می‌شود و اگر بدون سیاست امنیتی شروع به ایمن سازی شبکه کنید، محصول وحشتناکی از کار در می‌آید.

با این مقدمه، و با این فرض که سیاست امنیتی مورد نظر برای شبکه بطور کامل مورد تجزیه و تحلیل قرار گرفته است و بایدها و نبایدها نیز مشخص شده است، کار شروع می‌شود. حال باید پنج مرحله پشت سر گذاشته شود تا کار تمام شود. این پنج مرحله عبارت اند از:

۱- Inspection (بازرسی)

۲- Protection (حفاظت)

۳- Detection (ردیابی)

۴- Reaction (واکنش)

۵- Reflection (بازتاب)

در طول مسیر ایمن سازی شبکه از این پنج مرحله عبور می کنیم، ضمن آن که این مسیر، احتیاج به یک تیم امنیتی دارد و یک نفر به تنهایی نمی تواند این پروسه را طی کند. در ادامه ۱۳ گامی که برای امن نمودن سیستم باید طی کرد را نام می‌بریم:

۱- اولین جایی که ایمن‌سازی را شروع می‌کنیم، ایمن کردن کلیه روش‌های اعتبارسنجی[۲۹] یا تصدیق هویت موجود است. معمولاً رایج‌ترین روش اعتبارسنجی، استفاده از شناسه کاربری و کلمه رمز است.

مهمترین قسمت هایی که باید اعتبارسنجی را ایمن و محکم کرد عبارتند از :

- کنترل کلمات عبور کاربران، به ویژه در مورد مدیران سیستم.
- کلمات عبور سوییچ و روترها (در این خصوص روی سوییچ تاکید بیشتری می شود، زیرا از آنجا که این ابزار به صورت plug and play کار می‌کند، اکثر مدیران شبکه از پیکربندی‌کردن آن غافل می‌شوند. در حالیکه توجه به این مهم می‌تواند امنیت شبکه را ارتقا دهد. لذا به مدیران امنیتی توصیه می‌شود که حتماً سوییچ و روترها رو کنترل کنند).
- کلمات عبور مربوط به SNMP.
- کلمات عبور مربوط به پرینت سرور.
- کلمات عبور مربوط به محافظ صفحه نمایش.

در حقیقت آنچه که در مبحث امنیت شبکه در مورد Account and Password Security وجود دارد، این جا به کار می رود.

۲- گام دوم نصب و به روز رسانی آنتی‌ویروس‌ها روی همه کامپیوترها، سرورها و میل سرورها است. ضمن اینکه آنتی‌ویروس‌های مربوط به کاربران باید به صورت خودکار به روز رسانی شود و آموزش‌های لازم در مورد فایل‌های ضمیمه ایمیل‌ها و راهنمایی لازم جهت اقدام صحیح در صورت مشاهده موارد مشکوک نیز باید به کاربران داده شود.

۳ - گام سوم شامل نصب آخرین وصله‌های امنیتی و به‌روز رسانی‌های امنیتی سیستم‌عامل و سرویس‌های موجود است. در این مرحله علاوه بر اقدامات ذکر شده، کلیه سرورها، سوییچ ها، روترها و دسک تاپ ها با ابزارهای شناسایی حفره‌های امنیتی بررسی می‌شوند تا علاوه بر شناسایی و رفع حفره‌های امنیتی، سرویس‌های غیر ضروری هم شناسایی و غیرفعال شوند.

[29] authentication

۴-در این مرحله نوبت گروه بندی کاربران و اعطای مجوزهای لازم به فایل‌ها و دایرکتوری‌ها است. ضمن اینکه اعتبارهای(account) قدیمی هم باید غیر فعال شوند. گروه بندی و اعطای مجوز بر اساس یکی از سه مدل استاندارد Control Techniques Access یعنی DAC , MAC یا RBAC انجام می شود. بعد از پایان این مرحله، یک بار دیگر امنیت سیستم عامل باید چک شود تا چیزی فراموش نشده باشد.

۵- حالا نوبت وسایل و ابزار سخت افزاری است که معمولاً شامل روتر، سوییچ و فایروال می‌شود. بر اساس سیاست امنیتی موجود و توپولوژی شبکه، این ابزارها باید پیکربندی شوند. تکنولوژی‌هایی مثل NAT, PAT و filtering و غیره در این مرحله مطرح می‌شود و به همین علّت این مرحله خیلی مهم است. حتی موضوع مهم IP Addressing که از وظایف مدیران شبکه هست نیز می‌تواند مورد توجه قرار گیرد تا اطمینان حاصل شود که از حداقل ممکن برای IP Assign به شبکه‌ها استفاده شده است.

۶- قدم بعد تعیین راهبرد تهیه نسخه پشتیبان[۳۰] است. نکته مهمی که وجود دارد این است که باید مطمئن شویم که سیستم تهیه نسخه پشتیبان و بازیابی به درستی کار کرده و در بهترین حالت ممکن قرار دارد.

۷- امنیت فیزیکی. در این خصوص اول از همه باید به سراغ UPSها رفت. باید چک کنیم که UPS ها قدرت لازم رو برای تامین نیروی الکتریکی لازم جهت کارکرد صحیح سخت افزارهای اتاق سرور در زمان اضطراری را داشته باشند. نکات بعدی شامل کنترل درجه حرارت و میزان رطوبت، ایمنی در برابر سرقت و آتش‌سوزی است. سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم‌های الکترونیکی آسیب وارد نکند. به طور کل آنچه که مربوط به امنیت فیزیکی می‌شود در این مرحله به کار می‌رود.

۸- امنیت وب سرور یکی از موضوعاتی است که باید وسواس خاصی در مورد آن داشت. به همین دلیل در این قسمت، مجدداً و با دقت بیشتر وب سرور ر چک و ایمن می‌کنیم. در حقیقت، امنیت وب نیز در این مرحله لحاظ می شود.

توجه:

"هیچ گاه اسکریپت های سمت سرویس دهنده را فراموش نکنید"

۹ - حالا نوبت بررسی، تنظیم و آزمایش سیستم‌های Auditing و Logging هست. این سیستم‌ها هم می تواند بر پایه host و هم بر پایه network باشد. سیستم‌های رد گیری و ثبت حملات هم در این مرحله نصب و تنظیم می‌شوند. باید مطمئن شوید که تمام اطلاعات لازم ثبت و به خوبی محافظت می‌شود. در ضمن ساعت و تاریخ سیستم‌ها درست باشد چرا که در غیر این صورت کلیه اقدامات قبلی از بین رفته و امکان پیگیری‌های قانونی در صورت لزوم نیز دیگر وجود نخواهد داشت.

۱۰- ایمن کردن Remote Access با پروتکل و تکنولوژی های ایمن و Secure گام بعدی محسوب می-شود. در این زمینه با توجه به شرایط و امکانات، ایمن ترین پروتکل و تکنولوژی‌ها را باید به خدمت گرفت.

[30] Backup

۱۱ - نصب فایروال‌های شخصی در سطح host ها، لایه امنیتی مضاعفی به شبکه شما می‌دهد. پس این مرحله را نباید فراموش کرد.

۱۲ - شرایط بازیابی در حالت‌های اضطراری را حتما چک و بهینه کنید. این حالت ها شامل خرابی قطعات کامپیوتری، خرابکاری کاربران، خرابی ناشی از مسایل طبیعی (زلزله - آتش سوزی – ضربه خوردن - سرقت - سیل) و خرابکاری ناشی از نفوذ هکرها، است. استاندارد های warm site و hot site را در صورت امکان رعایت کنید.

به خاطر داشته باشید که " *همیشه در دسترس بودن اطلاعات* "، جز، قوانین اصلی امنیتی هست.

۱۳- و قدم آخر این پروسه که در حقیقت شروع یک جریان همیشگی است، عضو شدن در سایت‌ها و بولتن های امنیتی و آگاهی ازآخرین اخبار امنیتی است.

توجه:

مدیران شبکه‌های کامپیوترهای می‌بایست، بصورت ادواری اقدام به تست امنیتی تمام کامپیوترهای موجود در شبکه (سرویس‌گیرندگان، سرویس‌دهندگان، سوئیچ‌ها، روترها، فایروال‌ها و سیستم‌های تشخیص مزاحمین) نمایند. تست امنیت شبکه، پس از اعمال هر-گونه تغییر اساسی در پیکربندی شبکه، نیز می‌بایست انجام شود.

نکات کاربردی تکمیلی

۱. استفاده از نرم افزارهای محافظتی (مانند ضد ویروسها)وبه روز نگه داشتن انها

از وجود ضد ویروس بر روی دستگاه خود اطمینان حاصل کنید این نرم افزارها برای محافظت از کامپیوتر در برابر ویروسهای شناخته شده به کار می‌روند و در صورت استفاده از آنها کاربر نیاز به نگرانی در مورد ویروسها نخواهد داشت . در شرایطی که هر روز ویروسهای جدید تولید شده وتوزیع میشوند .نرم افزارهای ضد ویروس برای تشخیصو از بین بردن انها باید به صورت منظم به روزشوند برای این کار می‌توان به سایت شرکت تولید کننده ضد ویروس مراجعه کرده و اطلاعات لازم در مورد نحوه به‌روز رسانی و نیز فایلهای جدید جدید را دریافت نمود. عموماً نرم افزارهای ضد ویروس ابزارهای به‌روز رسانی و زمان‌بندی این این فرآیند را در خود دارند. پیشنهاد می‌کنیم برای شناسایی و محافظت از سیستم خود در برابر ویروسها از آنتی ویروس NOD32 استفاده کنید.

۲. باز نکردن نامه های دریافتی از منابع ناشناس

این قانون ساده را پیروی کنید :اگر فرستنده نامه را نمیشناسید نسبت به نامه وپیوستهای ان بسیاربادقت

عمل نمایید .هر گاه یک نامه مشکوک دریافت کردید بهترین عمل حذف کل نامه با پیوستهای ان است. برای امنیت بیشتر حتی اگر فرستنده نامه اشنا باشد هم باید با احتیاط بود اگر عنوان نامه نا آشنا و عجیب باشد و بالاخص در صورتی که نامه حاوی لینک های غیر معمول باشد .باید با دقت عمل کرد ممکن است دوست شما به صورت تصادفی ویروسی را برای شما فرستاده باشد .ویروسI love you دقیقا به همین صورت میلیونها کامپیوتر را در سراسر دنیا الوده نمود.
تردید نکنید نامه های مشکوک را پاک کنید .

۳. استفاده از گذر واژه های مناسب

گذر واژه در صورتی دسترسی غریبه ها به منابع موجود را محدود میکند که حدس زدن ان به سادگی امکان پذیر نباشد.
گذر واژه‌های خود را در اختیار دیگران قرار ندهید و از یک گذر واژه در بیشتر از یک جا استفاده نکنید در این صورت اگر یکی از گذر واژه های شما لو برود همه منابع در اختیار شما در معرض خطر قرار خواهند گرفت.
گذر واژه باید حداقل شامل حرف بوده حتی الامکان کلمه های بی معنی باشد. در انتخاب این کلمه اگر از حروف کوچک بزرگ و اعداد استفاده شود ضریب امنیت بالاتر خواهد رفت. به صورت منظم گذر واژه های قبلی را عوض نمایید گذر واژه خود را در اختیار دیگران قرار ندهید.

۴. محافظت از کامپیوتر در برابر نفوذ با استفاده ازحفاظ (firewall)

حفاظ دیواری مجازی بین سیستم کامپیوتریو دنیای بیرون ایجاد میکند . این محصول به دو صورت نرم افزاری و سخت افزاری تولید میشود و برای حفاظت کامپیوتر های شخصی و نیزشبکه ها به کار میرود .حفاظ دادههای غیر مجاز یا داده هایی که به صورت بالقوه خطرناک می باشند را **** کرده و سایر اطلاعات را عبور می دهد علاوه بر این حفاظ در شرایطی که کامپیوتر به اینترنت وصل است مانع دسترسی افراد غیر مجاز به کامپیوتر میشود.
پیشنهاد میکنیم برای محافظت از سیستم های شخصی خود در برابر نفوذ هکرها از طریق نرم افزارهای مخرب از نرم افزارZoneAlarm استفاده کنید.

۵. خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه

سیستمهای عامل این امکان را برای کاربران خود فراهم می اورند که با هدف به اشتراک گذاری فایل دسترسی دیگران را از طریق شبکه ویا اینترنت به دیسک سخت محلی فراهم اورند .این قابلیت امکان انتقال ویروس از شبکه را فراهم میکند . از سوی دیگر در صورتی که کاربر دقت کافی را در به اشتراک

گذاشتن فایلها به عمل نیاورد امکان مشاهده فایلهای خود را به دیگرانی که مجاز نیستند ایجاد میکند .بنابراین در صورتی که نیازواقعی به این قابلیت راندارید به اشتراک گذاری فایل را متوقف کنید.

۶. قطع اتصال به اینترنت در مواقع عدم استفاده

به خاطر داشته باشید که بزرگراه دیجیتال یک مسیر دوطرفه است و اطلاعات ارسال و دریافت می شوند قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به ان نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین میبرد.

۷. تهیه پشتیبان از داده های موجود بر روی کامپیوتر

همواره برای از بین رفتن اطلاعات ذخیره شده برروی حافظه دستگاه خود امادگی داشته باشید.امروزه تجهیزات سخت افزاری و نرم افزاری متنو عی برای تهیه نسخه های پشتیبان توسعه یافته اند که با توجه به نوع داده و اهمیت ان میتوان از انها بهره گرفت . بسته به اهمیت داده باید سیاست گذاری های لازم انجام شود .در این فرایند تجهیزات مورد نیاز و زمانهای مناسب برای تهیه پشتیبان مشخص میشوند .علاوه بر این باید همواره دیسک هایStart up در دسترس داشته باشید تا در صورت وقوع اتفاقات نا مطلوب بتوانید در اسرع وقت سیستم را بازیابی نمایید.

۸. گرفتن وصله های امنیتی (patches)

بیشتر شرکتهای تولید کننده نرم افزار هر از چند گاهی نرم افزارهای به روز رسان و وصله های امنیتی جدیدی را برای محصولات خود ارائه می دهند
با گذر زمان اشکالات جدید در نرم افزارهای مختلف شناسایی میشوند که امکان سوء استفاده را برای هکرها)البته نه جوجه هکرها) بوجود می اورند
پس از شناسایی هر اشکالی شرکت تولید کننده محصول اقدام به نوشتن وصله های مناسب برای افزایش امنیت و از بین بردن راههای نفوذ به سیستم می کنند .این وصله ها بر روی سایت های وب شرکت ها عرضه میشوند و کاربران باید برای تامین امنیت سیستم خود همواره اخرین نسخه های وصله ها را گرفته و بر روی سیستم خود نصب کنند.
برای راحتی کاربران ابزارهایی توسعه داده شده اند که به صورت اتوماتیک به سایتهای شرکتهای تولید کننده محصولات وصل شده لیست اخرین وصله ها را دریافت می کنند. سپس با بررسی سیستم موجود نقاط ضعف ان را شناسایی و به کاربر اعلام می شود .به این ترتیب کاربر از وجود اخرین نسخه های به روز رسان آگاه می‌شود.

۹. بررسی منظم امنیت کامپیوتر

در بازه های زمانی مشخص وضعیت امنیتی سیستم کامپیوتری خود را مورد ارزیابی قرار دهید .انجام این کار حداقل دو بار در سال توصیه میشود.بررسی پیکر بندی امنیتی نرم افزارهای مختلف شامل مرور گرها و حصول اطمینان از مناسب بودن تنظیمات سطوح امنیتی در این فر ایند انجام می‌شود.

۱۰. حصول اطمینان از آگاهی اعضای خانواده و یا کارمندان از نحوه برخورد با کامپیوترهای آلوده

هر کسی که از کامپیوتر استفاده می‌کند باید اطلاعات کافی در مورد امنیت داشته باشد .چگونگی استفاده از ضد ویروس ها و به روز رسانی آنها، روش گرفتن وصله های امنیتی و نصب آنها و چگونگی انتخاب گذر واژه مناسب از جمله موارد ضروری می باشد.