

اگر دیسکی حاوی فایل‌های سیستمی هم نبوده باشد ولی به یک ویروس بوت سکتوری آلوده باشد وقتی اشتباهاً دیسکت را درون فلاپی درایو قرار دهید و کامپیوتر را دوباره راه‌اندازی کنید پیغام زیر مشاهده می‌شود. ولی به هر حال ویروس بوت سکتوری پیش از این اجرا شده و ممکن است کامپیوتر شما را نیز آلوده کرده باشد.

Non-system disk or disk error

Replace and press any key when ready

کامپیوترهای بر پایه Intel در برابر ویروس‌های Boot Sector و Partition Table آسیب پذیر هستند.

تا قبل از اینکه سیستم بالا بیاید و بتواند اجرا شود صرف‌نظر از نوع سیستم عامل می‌تواند هر کامپیوتری را آلوده سازد.

تروجان چیست؟ چگونه کار می‌کند؟

یک تروجان یک برنامه کامپیوتری می‌باشد که جاسوس کامپیوتری نیز نامیده می‌شود. یک تروجان وقتی در کامپیوتری اجرا می‌شود در آن کامپیوتر ماندگار می‌شود (مانند ویروس‌ها که در کامپیوتر می‌مانند). با نصب فایروال و آنتی ویروس‌ها می‌توانیم جلوی ورود بعضی از آنها را به سیستم خود بگیریم. البته همه تروجانها را آنتی ویروس‌ها نمیتوانند تشخیص دهند.

تروجانها اطلاعاتی از کامپیوتر را (کامپیوتری که فایل سرور در آن اجرا شده) به شخصی که (هکرها) آن تروجان را به کامپیوتر قربانی فرستاده، می‌فرستد. این اطلاعات میتواند پسوردهای کامپیوتر مانند پسورد Admin و یا پسوردهای اینترنتی مانند Yahoo Password و Internet Connection Password و یا آدرس IP باشد.

این اطلاعات می‌توانند در قالب یک ایمیل (E-Mail) به شخص هکر فرستاده شوند.

بعضی از تروجانها توانایی سرویس دهی برای هکرها را نیز دارند؛ یعنی اگر تروجانی در کامپیوتری اجرا شود فرستنده آن تروجان میتواند کامپیوتر قربانی را با استفاده از کامپیوتر خود و از راه دور کنترل کند و عملیاتی بر روی کامپیوتر (مانند: حذف فایل، مشاهده درایوها، فرمت کردن درایوها و...) انجام دهد. البته باید سرور (فایل اجرا شده در کامپیوتر قربانی) این سرویس دهی‌ها را دارا باشد.

ویروس‌های چند جزئی Multipartite virus

بعضی از ویروسها، ترکیبی از تکنیکها را برای انتشار استفاده کرده ، فایل‌های اجرایی، بوت سکتور و پارتیشن را آلوده می سازند. اینگونه ویروسها معمولاً تحت windows 98 یا Win.Nt انتشار نمی یابند.

چگونه ویروسها گسترش می یابند؟

زمانی که یک کد برنامه آلوده به ویروس را اجرا می کنید، کد ویروس هم پس از اجرا به همراه کد برنامه اصلی ، در وهله اول تلاش می کند برنامه های دیگر را آلوده کند. این برنامه ممکن است روی همان کامپیوتر میزان یا برنامه ای بر روی کامپیوتر دیگر واقع در یک شبکه باشد. حال برنامه تازه آلوده شده نیز پس از اجرا دقیقاً عملیات مشابه قبل را به اجرا درمی آورد. هنگامیکه بصورت اشتراکی یک کپی از فایل آلوده را در دسترس کاربران دیگر کامپیوترها قرار می دهید ، با اجرای فایل کامپیوترهای دیگر نیز آلوده خواهند شد. همچنین طبیعی است با اجرای هرچه بیشتر فایل‌های آلوده فایل‌های بیشتری آلوده خواهند شد.

اگر کامپیوتری آلوده به یک ویروس بوت سکتور باشد، ویروس تلاش می کند در فضاهای سیستمی فلاپی دیسکها و هارد دیسک از خود کپی هایی بجا بگذارد . سپس فلاپی آلوده می تواند کامپیوترهایی را که از روی آن بوت می شوند و نیز یک نسخه از ویروسی که قبلاً روی فضای بوت یک هارد دیسک نوشته شده نیز می تواند فلاپی های جدید دیگری را نیز آلوده نماید.

به ویروسهایی که هم قادر به آلوده کردن فایلها و هم آلوده نمودن فضاهای بوت می باشند اصطلاحاً ویروسهای چند جزئی (multipartite) می گویند.

فایل‌هایی که به توزیع ویروسها کمک می کنند حاوی یک نوع عامل بالقوه می باشند که می توانند هر نوع کد اجرایی را آلوده کنند. برای مثال بعضی ویروسها کدهای را آلوده می کنند که در بوت سکتور فلاپی دیسکها و فضای سیستمی هارد دیسکها وجود دارند.

نوع دیگر این ویروس ها که به ویروسهای ماکرو شناخته می شوند ، می توانند عملیات پردازش کلمه ای (word processing) یا صفحه های حاوی متن را که از این ماکروها استفاده می کنند ، آلوده می کنند. این امر برای صفحه هایی با فرمت HTML نیز صادق است.

از آنجائیکه یک کد ویروس باید حتماً قابل اجرا شدن باشد تا اثری از خود به جای بگذارد از اینرو فایل‌هایی که کامپیوتر به عنوان داده های خالص و تمیز با آنها سرو کار دارد امن هستند.

فایل‌های گرافیکی و صدا مانند فایل‌هایی با پسوند . gif , .jpg , .wav . . . هستند .

برای مثال زمانی که یک فایل با فرمت **picture** را تماشا می‌کنید کامپیوتر شما آلوده نخواهد شد.

یک کد ویروس مجبور است که در قالب یک فرم خاص مانند یک فایل برنامه‌ای **exe** یا یک فایل متنی **doc** که کامپیوتر واقعاً آن را اجرا می‌کند، قرار گیرد.

عملیات مخفیانه ویروس در کامپیوتر

همانطور که می‌دانید ویروسها برنامه‌های نرم افزاری هستند. آنها می‌توانند مشابه برنامه‌هایی باشند که به صورت عمومی در یک کامپیوتر اجرا می‌گردند.

اثر واقعی یک ویروس بستگی به نویسنده آن دارد. بعضی از ویروسها با هدف خاص ضربه زدن به فایلها طراحی می‌شوند و یا اینکه در عملیات مختلف کامپیوتر دخالت کرده و ایجاد مشکل می‌کنند.

ویروسها براحتی بدون آنکه متوجه شوید خود را تکثیر کرده، گسترش می‌یابند، در حین گسترش یافتن به فایلها صدمه رسانده و یا ممکن است باعث مشکلات دیگری شوند.

نکته: ویروسها قادر نیستند به سخت افزار کامپیوتر صدمه ای وارد کنند. مثلاً نمی‌توانند باعث ذوب شدن **CPU**، سوختن هارد دیسک و یا انفجار مانیتور و غیره شوند.

نکاتی برای جلوگیری از ورود کرمها به سیستم:

از آنجائیکه این نوع برنامه‌ها (**worms**) امروزه گسترش بیشتری یافته و باید بیشتر از سایر برنامه‌های مخرب از آنها دوری کنیم، از این رو به این نوع برنامه‌های مخرب بیشتر می‌پردازیم.

کرمها برنامه‌های کوچکی هستند که با رفتاری بسیار مودبانه به درون سیستم رسوخ کرده، بدون واسطه خود را تکثیر کرده و خیلی زود سراسر سیستم را فرا می‌گیرند. در زیر نکاتی برای جلوگیری از ورود کرمها آورده شده است.

(۱) بیشتر کرمهایی که از طریق **E-mail** گسترش پیدا می‌کنند از طریق نرم افزارهای **microsoft outlook** و یا **out look express** وارد سیستم می‌شوند. اگر شما از این نرم افزار استفاده می‌کنید پیشنهاد می‌شود همیشه آخرین نسخه **security patch** این نرم افزار را از سایت **microsoft** دریافت و به روز کنید.

همچنین بهتر است علاوه بر به روز کردن این قسمت از نرم افزار outlook سعی کنید سایر نرم افزارها و حتی سیستم عامل خود را نیز در صورت امکان همیشه به روز نگه دارید، و یا حداقل بعضی از تکه‌های آنها را که به صورت بروز درآمده قابل دسترسی است.

اگر از روی اینترنت بروز می‌کنید و یا از cd ها و بسته‌های نرم افزاری آماده در بازار، از اصل بودن آنها اطمینان حاصل کنید.

۲) تا جای ممکن در مورد e-mail attachment ها محتاط باشید. چه در دریافت e-mail و چه در ارسال آنها.

۳) همیشه ویندوز خود را در حالت show file extensions قرار دهید.

این گزینه در منوی Tools/folder option/view با عنوان “ Hide file extensions for known file Types” قرار دارد که به صورت پیش فرض این گزینه تیک خورده است، تیک آنرا بردارید.

۴) فایل‌های attach شده با پسوند های SHS و VBS و PIF را هرگز باز نکنید. این نوع فایلها در اکثر موارد نرمال نیستند و ممکن است حامل یک ویروس و یا کرم باشند.

۵) هرگز ضمايم دو پسوندی را باز نکنید.

email attachment هایی با پسوندهایی مانند Neme.BMP.EXE و یا Name.TxT.VBS و ...

۶) پوشه‌های موجود بر روی سیستم خود راجز در مواقع ضروری با دیگر کاربران به اشتراک نگذارید. اگر مجبور به این کار هستید، اطمینان حاصل کنید که کل درایو و یا شاخه ویندوز خود را به اشتراک نگذاشته اید.

۷) زمانی که از کامپیوتر استفاده نمی‌کنید کابل شبکه و یا مودم را جدا کرده و یا آنها را خاموش کنید.

۸) اگر از دوستی که به نظر می‌رسد ناشناس است ایمیلی دریافت کردید قبل از باز کردن ضمايم آن حتماً متن را چند بار خوانده و زمانی که مطمئن شدید از طرف یک دوست است، آنگاه سراغ ضمايم آن بروید.

۹) توصیه می‌شود فایل‌های ضمیمه شده به ایمیل‌های تبلیغاتی و یا احياناً weblink های موجود در آنها را حتی الامکان باز نکنید.

۱۰) از فایل‌های ضمیمه شده‌ای که به هر نحوی از طریق تصاویر و یا عناوین خاص، به تبلیغ مسائل جنسی و مانند آن می‌پردازند، دوری کنید. عناوینی مانند porno.exe و یا pamela-Nude.VBS که باعث گول خوردن کاربران می‌شود.

۱۱) به آیکون فایل‌های ضمیمه شده نیز به هیچ عنوان اعتماد نکنید. چرا که ممکن است کرم‌هایی در قالب فایل عکس و یا یک فایل متنی فرستاده شود ولی در حقیقت این فایل یک فایل اجرایی بوده و باعث فریب خوردن کاربر می‌شود.

۱۲) در messenger هایی مانند ICQ, IRC و یا AOL به هیچ عنوان فایل‌های ارسالی از جانب کاربران ناشناس در on-line chat system ها را قبول (accept) نکنید.

۱۳) از Download کردن فایل از گروه‌های خبری همگانی نیز پرهیز کنید. (usenet news) زیرا اغلب گروه‌های خبری خود یکی از علل پخش ویروس می‌باشند.

ویروس‌ها چگونه کار می‌کنند؟

ویروس‌های رایانه‌ای بسیار اسرار آمیز هستند و توجه بسیاری از برنامه‌ویسان مشاوران امنیتی شبکه‌های اینترنتی و حتی افراد عادی که از رایانه برای کارهای معمولی خود استفاده می‌کنند را به خود جلب کرده‌اند و سالانه هزینه هنگفتی برای جلوگیری از انتشار و بالا بردن امنیت شبکه‌ها و رایانه‌ها در مقابل ویروس‌ها صرف می‌شود. اگر بخواهیم از دید دیگری به ویروس‌ها نگاه کنیم نقاط آسیب‌پذیری و میزان آسیب‌پذیر بودن سیستم رایانه‌ای خود و یا اکثرت شبکه‌ای که ما در حال کار با آن هستیم به ما نشان می‌دهند که البته ممکن است این کار کمی برایمان گران تمام شود!

یک ویروس که از طراحی و زیر ساخت پیچیده و سازمان یافته‌ای بهره‌مند باشد می‌تواند تاثیرات شگفت‌انگیز و در بعضی موارد مخرب بر روی شبکه اینترنت بگذارد. اثراتی که این ویروس‌ها بر اینترنت می‌گذارند و تعداد رایانه‌هایی که آلوده می‌کنند خود گواه ارتباطات پیچیده و عظیم انسان‌ها و رایانه‌ها و شبکه‌های اطلاع‌رسانی در اینترنت می‌باشد.

برای مثال ویروس جدید مایدم (Mydoom worm) تخمین زده شده که در یک روز حدود ۲۵۵ هزار رایانه را آلوده کرده باشد. ویروس ملیسا (Melissa virus) در سال ۹۹ و من شما را دوست دارم I LOVE YOU در سال ۲۰۰۰ که ویروس‌های قدرتمندی که مایکروسافت و بسیاری از شرکت‌های ارائه‌دهنده سرویس ایمیل را مجبور کرد تا زمان پاک‌سازی و رفع مشکلات بوجود آمده توسط ویروس سرورهای خود را خاموش کنند. شاید وقتی کمی تحقیق کنید و عملکرد این ویروس‌ها را مورد مطالعه قرار دهید بسیار شگفت‌زده خواهید شد وقتی بفهمید که این ویروس‌ها بطرز بسیار ساده‌ای این کارها را انجام می‌دهند. اگر در زمینه برنامه‌نویسی اطلاعات مختصر و یا حتی زبان برنامه‌نویسی بلد باشید با دیدن کدهای برنامه این ویروس‌ها به ساده بودن و طرز کار ساده آن‌ها پی خواهید برد و از آن شگفت‌زده می‌شوید.

- کرم‌های اینترنتی مفید

خبرگزاری BBC در می ۲۰۰۱ خبر از ظهور و گسترش کرمی به نام کرم پنیر (Cheese worm) داد. محتوای خبر نشان از فعالیت این کرم علیه هکرها میداد، نه به نفع آنان!

«یک ویروس مفید در حال گشت در اینترنت است و شکاف امنیتی کامپیوترها را بررسی و در صورت یافتن، آنها را می‌بندد. هدف این کرم، کامپیوترهای با سیستم عامل لینوکس است که توسط یک برنامه مشابه اما زیان‌رسان قبلاً مورد حمله قرار گرفته‌اند.»

اما این کرم توسط شرکت‌های تولید آنتی‌ویروس تحویل گرفته نشد! چراکه آنان معتقد بودند هر نرم‌افزاری که تغییراتی را بدون اجازه در یک کامپیوتر ایجاد کند، بالقوه خطرناک است.

در مارس همین سال یک برنامه زیان‌رسان با عنوان Lion worm (کرم شیر) سرویس‌دهندگان تحت لینوکس بسیاری را آلوده و درهای پشتی روی آنها نصب کرده بود تا ایجادکنندگان آن بتوانند از سرورها بهره‌برداری کنند. کرم همچنین کلمات عبور را می‌دزدید و به هکرهایی که از این ابزار برای ورود غیرمجاز استفاده می‌کردند، می‌فرستاد. این درهای پشتی می‌توانستند برای حملات DoS نیز استفاده شوند.

کرم پنیر تلاش می‌کرد بعضی از خسارات وارده توسط کرم شیر را بازسازی کند. در حقیقت کرم پنیر شبکه‌هایی با آدرسهای مشخص را پیمایش می‌کرد تا آنکه درهای پشتی ایجاد شده توسط کرم شیر را بیابد، سپس برای بستن سوراخ، وصله آنرا بکار می‌گرفت و خود را در کامپیوتر ترمیم‌شده کپی می‌کرد تا برای پیمایش شبکه‌های دیگر با همان شکاف امنیتی از این کامپیوتر استفاده کند.

مدیران سیستمها که متوجه تلاشهای بسیاری برای پیمایش سیستمهایشان شده بودند، دنبال علت گشتند و کرم پنیر را مقصر شناختند. ارسال گزارشهای آنها به CERT باعث اعلام یک هشدار امنیتی گردید.

این برنامه با مقاصد بدخواهانه نوشته نشده بود و برای جلوگیری از فعالیتهای هکرهاي مزاحم ایجاد گشته بود. اما بهرحال یک «کرم» بود. چرا که یک شبکه را می‌پیماید و هر جا که میرفت خود را کپی می‌کرد.

زمانیکه بحث کرم پنیر مطرح شد، بعضی متخصصان امنیت شبکه‌های کامپیوتری احساس کردند که ممکن است راهی برای مبارزه با شکافهای امنیتی و هکرهاي آسیب‌رسان پیدا شده باشد. یکی از بزرگترین علت‌های وجود رخنه‌های امنیتی و حملات در اینترنت غفلت یا تنبلی بسیاری از مدیران سیستمهاست. بسیاری از مردم سیستمهای خود را با شکافهای امنیتی به امان خدا! رها می‌کنند و تعداد کمی زحمت نصب وصله‌های موجود را می‌دهند.

بسیاری از مدیران شبکه‌ها از ورود برنامه‌ها و بارگذاری وصله‌ها ابراز نارضایتی می‌کنند. این نکته‌ای صحیح است که یک وصله ممکن است با برنامه‌های موجود در کامپیوتر ناسازگار باشد. اما در مورد یک کرم مفید که وجود شکافهای امنیتی در سیستمها را اعلام می‌کند، چه؟ این روش مشکل مدیرانی را که نمی‌توانند تمام شکافهای امنیتی را ردیابی کنند، حل می‌کند. بعضی می‌گویند که برنامه‌های ناخواسته را روی سیستم خود نمی‌خواهند. در پاسخ به آنها گفته

می‌شود «اگر شکاف امنیتی در سیستم شما وجود نداشت که این برنامه‌ها نمی‌توانستند وارد شوند. یک برنامه را که سعی می‌کند به شما کمک کند، ترجیح می‌دهید یا آنهایی را که به سیستم شما آسیب می‌رسانند و ممکن است از سیستم شما برای حمله به سایرین استفاده کنند؟»

این آخری، یک نکته مهم است. رخنه‌های امنیتی کامپیوتر شما فقط مشکل شما نیستند؛ بلکه ممکن است برای سایر شبکه‌ها نیز مساله‌ساز شوند. ممکن است فردی نخواهد علیه بیماریه‌های مسری واکسینه شود، اما به‌رحال بخشی از جامعه‌ای است که در آن همزیستی وجود دارد.

آنچه که در این میان آزردهنده است این است که هر ساله برای امنیت اتفاقات بدی رخ میدهد، و هرچند تلاشهایی برای بهبود زیرساختهای امنیتی انجام می‌گیرد، اما برای هر گام به جلو، دو گام باید به عقب بازگشت. چرا که هرکرا باهوش‌تر و در نتیجه تهدیدها خطرناکتر شده‌اند. و شاید بدلیل تنبلی یا بار کاری زیاد مدیران شبکه باشد.

در بیشتر موارد، مشکلات بزرگ امنیتی که هر روزه درباره آنها می‌خوانید، بخاطر وجود حملاتی است که بر روی سیستمهایی صورت می‌گیرد که به علت عدم اعمال وصله‌ها، هنوز مشکلات قدیمی را در خود دارند.

بنابه عقیده بعضی، اکنون زمان استفاده از تدبیر براساس کرم! و ساختن کرمهای مفید برای ترمیم مشکلات است. درباره این روش قبلا در مجامع مربوط به امنیت بحث شده است و البته هنوز اعتراضات محکمی علیه استفاده از آنها وجود دارد. اما در مواجهه با شبکه های zombie (کامپیوترهای آلوده ای که برای حملات DoS گسترده، مورد استفاده قرار می‌گیرند) که تعداد آنها به دهه‌هازار کامپیوتر میرسد، می‌توانند یک شبه! توسط کرمهای مفید از کار انداخته شوند.

البته، یک کرم مفید هنوز یک کرم است و بحث دیگری که در اینجا مطرح می‌شود این است که کرمها ذاتا غیرقابل کنترل هستند، به این معنی که کرمهای مفید هم باعث بروز مشکلات ترافیک می‌شوند و بصورت غیرقابل کنترل گسترده می‌گردند. این مساله در مورد بیشتر کرمها صدق می‌کند، اما دلیل آن این است که تاکنون هیچ کس یک کرم قانونی! و بدرستی برنامه نویسی شده ایجاد نکرده است. می‌توان براحتی کنترلهای ساده ای همچون انقضای در زمان مناسب و مدیریت پهنای باند را که این تاثیرات ناخوشایند را محدود یا حذف کند، برای یک کرم مفید تصور کرد.

اشکال وارده به ایجاد یک کرم قانونی و مناسب این است که زمان زیادی می‌طلبد، بسیار بیشتر از زمانی که یک کرم گسترش پیدا می‌کند. در پاسخ می‌توان گفت بیشتر کرمها از مسائل تازه کشف شده بهره نمی‌برند. بیشتر آنها از شکافهای امنیتی استفاده می‌کنند که مدت‌هاست شناخته شده‌اند.

تعدادی پرسش وجود دارد که باید پاسخ داده شوند. چه کسی این کرمها را طراحی و مدیریت می‌کند؟ دولت، CERT، فروشندگان یا اینکه باید شکل‌هایی براه انداخت؟ برای ترمیم چه ایراداتی باید مورد استفاده قرار گیرند؟ روند اخطار برای سیستمهایی که توسط یک کرم مفید وصله شده‌اند، چیست؟ آیا پیامی برای مدیر شبکه بگذارند؟ که البته هیچ کدام موانع غیرقابل حلی نیستند.

بهرحال، بهترین کار مدیریت صحیح سیستم‌هایتان است، بنحوی که با آخرین ابزار و وصله های امنیتی بروز شده باشند. در این صورت دیگر چندان نگران وجود کرم‌ها در سیستم‌هایتان نخواهید بود.

آنچه که نمی توان در مورد آن با اطمینان صحبت کرد، امن و موثر بودن یک کرم مفید است، که این مطلب مطالعات و تحقیقات جدی را می طلبد. بعلاوه اینکه، اگر برنامه نوشته شده در دنیای بیرون متفاوت از آزمایشگاه رفتار کند، چه کسی مسوولیت آنرا می پذیرد؟ مساله بعدی اینست که تحت قانون جزایی بعضی کشورها، هک کردن یک سیستم و تغییر دیتای آن بدون اجازه زیان محسوب می شود و چنانچه این زیان به حد مشخصی مثلا ۵هزار دلار برسد، تبهکاری بحساب می آید، حتی اگر قانون جنایی حمایتی برای نویسندگان کرمهای مفید در نظر بگیرد. ایده اصلی در این بین، اجازه و اختیار برای دستیابی به کامپیوتر و تغییر دیتای آن یا انجام عملیاتی بر روی آن است. از منظر قانونی، این اجازه می تواند از طرقی اعطاء شود. بعلاوه اینکه سیستمهایی که امنیت در آنها رعایت نشود، اساسا به هر کس اجازه تغییر دیتا را می دهند.

خوشبختانه، روشهای محدودی برای اخذ اجازه وجود دارد. برای مثال، ISPها از پیش بواسطه شرایط خدمات رسانی به مشتریان اجازه تغییر دیتا را دارند. یک ISP معتبر ممکن است حتی سرویس بروز رسانی رایگان یک برنامه ضدویروس را نیز به مشتریان ارائه کند.

راه دیگر اخذ اجازه از طریق پروانه های دولتی است. مثلا در بعضی کشورها، افسران پلیس این قدرت را دارند که بتوانند تحت قوانین محدود و شرایط خاصی وارد فضای خصوصی افراد شوند. مثال دیگر در مورد سارس است. افراد می توانند بخاطر سلامت عمومی قرنطینه شوند، اما فقط توسط افرادی که اختیارات دولتی دارند.

در آخر توجه شما را به یک مساله جلب می کنیم: اجرای قوانین سلامت بیشتر بصورت محلی است، در حالیکه اینترنت ماهیت دیگری دارد. ممکن است بتوان در بعضی کشورها به سوالات مربوط در مورد نوشتن و گسترش کرمهای مفید جواب داد، اما کاربران کشورهای دیگر را شامل نمی شود.

انواع حملات در شبکه های کامپیوتری

حملات (Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری ، خصوصاً "اینترنت ، امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس دهندگان می باشیم . علت بروز چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد .

برای پیشگیری ، شناسائی ، برخورد سریع و توقف حملات ، می بایست در مرحله اول قادر به تشخیص و شناسائی زمان و موقعیت بروز یک تهاجم باشیم . به عبارت دیگر چگونه از بروز یک حمله و یا تهاجم در شبکه خود آگاه می شویم ؟ چگونه با آن برخورد نموده و در سریعترین زمان ممکن آن را متوقف نموده تا میزان صدمات و آسیب به منابع اطلاعاتی سازمان به حداقل مقدار خود برسد ؟ شناسائی نوع حملات و نحوه پیاده سازی یک سیستم حفاظتی مطمئن در مقابل آنان یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است . شناخت دشمن و آگاهی از روش های تهاجم وی ، احتمال موفقیت ما را در رویارویی با آنان افزایش خواهد داد . بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه های کامپیوتری شده است ، بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب تا در آینده بتوانیم به نحو مطلوب از آنان استفاده نمائیم . جدول زیر برخی از حملات متداول را نشان می دهد :

انواع حملات :

انواع حملات

Denial of Service (DoS) & Distributed
Denial of Service (DDoS)

Spoofing

Back Door

Replay

Man in the

Weak Keys	Middle TCP/IP Hijacking
Password Guessing	Mathematical
Dictionary	Brute Force
Software Exploitation	Birthday
Viruses	Malicious Code
Trojan Horses	Virus Hoaxes
Worms	Logic Bombs
Auditing	Social Engineering
	System Scanning

حملات از نوع DoS

هدف از حملات DoS، ایجاد اختلال در منابع و یا سرویس هائی است که کاربران قصد دستیابی و استفاده از آنان را دارند (از کار انداختن سرویس ها). مهمترین هدف این نوع از حملات، سلب دستیابی کاربران به یک منبع خاص است. در این نوع حملات، مهاجمان با بکارگیری روش های متعددی تلاش می نمایند که کاربران مجاز را به منظور دستیابی و استفاده از یک سرویس خاص، دچار مشکل نموده و بنوعی در مجموعه سرویس هائی که یک شبکه ارائه می نماید، اختلال ایجاد نمایند. تلاش در جهت ایجاد ترافیک کاذب در شبکه، اختلال در ارتباط بین دو ماشین، ممانعت کاربران مجاز به منظور دستیابی به یک سرویس، ایجاد اختلال در سرویس ها، نمونه هائی از سایر اهدافی است که مهاجمان دنبال می نمایند. در برخی موارد و به منظور انجام حملات گسترده از حملات DoS به عنوان نقطه شروع و یک عنصر جانبی استفاده شده تا بستر لازم برای تهاجم اصلی، فراهم گردد. استفاده صحیح و قانونی از برخی منابع نیز ممکن است، تهاجمی از نوع DoS را به دنبال داشته باشد. مثلاً "یک مهاجم می تواند از یک سایت FTP که مجوز دستیابی به آن به صورت anonymous می باشد، به منظور ذخیره نسخه هائی از نرم افزارهای غیرقانونی، استفاده از فضای ذخیره سازی دیسک و یا ایجاد ترافیک کاذب در شبکه استفاده نماید. این نوع از حملات می تواند غیرفعال شدن کامپیوتر و یا شبکه مورد نظر را به دنبال داشته باشد. حملات فوق با محوریت و

تاکید بر نقش و عملیات مربوط به هر یک از پروتکل های شبکه و بدون نیاز به اخذ تائیدیه و یا مجوزهای لازم ، صورت می پذیرد . برای انجام این نوع حملات از ابزارهای متعددی استفاده می شود که با کمی حوصله و جستجو در اینترنت می توان به آنان دستیابی پیدا کرد . مدیران شبکه های کامپیوتری می توانند از این نوع ابزارها ، به منظور تست ارتباط ایجاد شده و اشکال زدائی شبکه استفاده نمایند . حملات DoS تاکنون با اشکال متفاوتی ، محقق شده اند . در ادامه با برخی از آنان آشنا می شویم .

متداولترین پورت های استفاده شده در حملات DoS

یکی دیگر از حملات DoS ، نوع خاص و در عین حال ساده ای از یک حمله DoS می باشد که با نام (DDoS) Distributed DoS، شناخته می شود. در این رابطه می توان از نرم افزارهای متعددی به منظور انجام این نوع حملات و از درون یک شبکه ، استفاده بعمل آورد. کاربران ناراضی و یا افرادی که دارای سوء نیت می باشند، می توانند بدون هیچگونه تاثیری از دنیای خارج از شبکه سازمان خود ، اقدام به ازکارانداختن سرویس ها در شبکه نمایند. در چنین حملاتی ، مهاجمان نرم افزاری خاص و موسوم به **Zombie** را توزیع می نمایند . این نوع نرم افزارها به مهاجمان اجازه خواهد داد که تمام و یا بخشی از سیستم کامپیوتری آلوده را تحت کنترل خود درآورند. مهاجمان پس از آسیب اولیه به سیستم هدف با استفاده از نرم افزار نصب شده **Zombie** ، تهاجم نهائی خود را با بکارگیری مجموعه ای وسیع از میزبانان انجام خواهند داد. ماهیت و نحوه انجام این نوع از حملات ، مشابه یک تهاجم استاندارد DoS بوده ولی قدرت تخریب و آسیبی که مهاجمان متوجه سیستم های آلوده می نمایند ، متاثر از مجموع ماشین هائی (**Zombie**) است که تحت کنترل مهاجمان قرار گرفته شده است .

به منظور حفاظت شبکه ، می توان فیلترهائی را بر روی روترهای خارجی شبکه به منظور دورانداختن بسته های اطلاعاتی مشمول حملات DoS ، پیکربندی نمود . در چنین مواردی می بایست از فیلتری دیگر که امکان مشاهده ترافیک (مبداء از طریق اینترنت) و یک آدرس داخلی شبکه را فراهم می نماید ، نیز استفاده گردد .

حملات از نوع Back door

Back door، برنامه ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی ، فراهم می نماید . برنامه نویسان معمولاً "چنین پتانسیل هائی را در برنامه ها پیش بینی تا امکان اشکال زدائی و ویرایش کدهای نوشته شده در زمان تست بکارگیری نرم افزار ، فراهم گردد. با توجه به این که تعداد زیادی از امکانات فوق ، مستند نمی گردند ، پس از اتمام مرحله تست به همان وضعیت باقی مانده و تهدیدات امنیتی متعددی را به دنبال خواهند داشت .

برخی از متداولترین نرم افزارها ئی که از آنان به عنوان **back door** استفاده می گردد ، عبارتند از :

Back Orifice: برنامه فوق یک ابزار مدیریت از راه دور می باشد که به مدیران سیستم امکان کنترل یک کامپیوتر را از راه دور (مثلاً" از طریق اینترنت) ، خواهد داد. نرم افزار فوق ، ابزاری خطرناک است که توسط گروهی با نام **Cult of the Dead Cow Communications**، ایجاد شده است . این نرم افزار دارای دو بخش مجزا می باشد : یک بخش سرویس گیرنده و یک بخش سرویس دهنده . بخش سرویس گیرنده بر روی یک ماشین اجراء و زمینه مانیفور نمودن و کنترل یک ماشین دیگر که بر روی آن بخش سرویس دهنده اجراء شده است را فراهم می نماید .

NetBus: این برنامه نیز نظیر **Back Orifice** ، امکان دستیابی و کنترل از راه دور یک ماشین از طریق اینترنت را فراهم می نماید... برنامه فوق تحت سیستم عامل ویندوز (نسخه های متفاوت از NT تا ۹۵ و ۹۸) ، اجراء و از دو بخش جداگانه تشکیل شده است : بخش سرویس دهنده (بخشی که بر روی کامپیوتر قربانی مستقر خواهد شد) و بخش سرویس گیرنده (برنامه ای که مسولیت یافتن و کنترل سرویس دهنده را برعهده دارد) . برنامه فوق ، به حریم خصوصی کاربران در زمان اتصال به اینترنت ، تجاوز و تهدیدات امنیتی متعددی را به دنبال خواهد داشت .

SubSeven (Sub7)، این برنامه نیز تحت ویندوز اجراء شده و دارای عملکردی مشابه **Back Orifice** و **NetBus** می باشد . پس از فعال شدن برنامه فوق بر روی سیستم هدف و اتصال به اینترنت ، هر شخصی که دارای نرم افزار سرویس گیرنده باشد ، قادر به دستیابی نامحدود به سیستم خواهد بود .

نرم افزارهای **Back Orifice** ، **Sub7** ، **NetBus** دارای دو بخش ضروری سرویس دهنده و سرویس گیرنده، می باشند . سرویس دهنده بر روی ماشین آلوده مستقر شده و از بخش سرویس گیرنده به منظور کنترل از راه دور سرویس دهنده ، استفاده می گردد. به نرم افزارهای فوق ، " سرویس دهندگان غیرقانونی " گفته می شود .

برخی از نرم افزارها از اعتبار بالائی برخوردار بوده ولی ممکن است توسط کاربرانی که اهداف مخربی دارند ، مورد استفاده قرار گیرند:

VNC (Virtual Network Computing): نرم افزار فوق توسط آزمایشگاه **AT&T** و با هدف کنترل از راه دور یک سیستم ، ارائه شده است . با استفاده از برنامه فوق ، امکان مشاهده محیط **Desktop** از هر مکانی نظیر اینترنت ، فراهم می گردد . یکی از ویژگی های جالب این نرم افزار ، حمایت گسترده از معماری های متفاوت است .

PCAnywhere: نرم افزار فوق توسط شرکت **Symantec** ، با هدف کنترل از راه دور یک سیستم با لحاظ نمودن فن آوری رمزنگاری و تائید اعتبار ، ارائه شده است . با توجه به سهولت استفاده از نرم افزار فوق ، شرکت ها و موسسات فراوانی در حال حاضر از آن و به منظور دستیابی به یک سیستم از راه دور استفاده می نمایند .

Terminal Services: نرم افزار فوق توسط شرکت مایکروسافت و به همراه سیستم عامل ویندوز و به منظور کنترل از راه دور یک سیستم ، ارائه شده است .

همانند سایر نرم افزارهای کاربردی ، نرم افزارهای فوق را می توان هم در جهت اهداف مثبت و هم در جهت اهداف مخرب بکارگرفت .

بهترین روش به منظور پیشگیری از حملات **Back doors** ، آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم افزارهای موجود می باشد. به کاربران می بایست آموزش داده شود که صرفاً از منابع و سایت های مطمئن اقدام به دریافت و نصب نرم افزار بر روی سیستم خود نمایند . نصب و استفاده از برنامه های آنتی ویروس می تواند کمک قابل توجهی در بلاک نمودن عملکرد اینچنین نرم افزارهایی (نظیر **Back Orifice, NetBus, and Sub7**) را به دنبال داشته باشد . برنامه های آنتی ویروس می بایست به صورت مستمر بهنگام شده تا امکان شناسایی نرم افزارهای جدید ، فراهم گردد.

نمونه هایی از حملات اینترنتی توسط نامه های الکترونیکی

بمنظور بررسی نقاط آسیب پذیر و نحوه انتشار ویروس های کامپیوتری با استفاده از کدهای مخرب ، عملکرد سه ویروس را مورد بررسی قرار می دهیم . هدف از بررسی فوق استفاده از تجارب موجود و اتخاذ راهکارهای مناسب بمنظور پیشگیری از موارد مشابه است . آنالیز دقیق رفتار هر یک از ویروس ها و نحوه مقابله و یا آسیب زدائی آنان از حوصله این مقاله خارج بوده و هدف ، صرفاً نشان دادن تاثیر نقاط آسیب پذیر در یک تهاجم اطلاعاتی بمنظور تخریب اطلاعات و منابع موجود در یک شبکه کامپیوتری (اینترنت ، اینترنت) و نقش کاربران در این زمینه است .

بررسی عملکرد کرم ILOVEYOU

کرم فوق ، در یک اسکریپت ویژوال بیسیک و بصورت فایل ضمیمه در یک نامه الکترونیکی عرضه می گردد . همزمان با باز نمودن فایل ضمیمه توسط کاربران ، زمینه فعال شدن کرم فوق ، فراهم خواهد شد . عملکرد این کرم ، بصورت زیر است:

نسخه هائی از خود را در فولدر سیستم ویندوز با نام LOVE-LETTER-FOR- و MSKernel32.vbs
YOU.vbs تکثیر می نماید .

نسخه ای از خود را در فولدر ویندوز و با نام Win32DLL.vbs تکثیر می نماید.

اقدام به تغییر مقادیر دو کلید رجیستری زیر می نماید . کلیدهای فوق، باعث فعال نمودن (فراخوانی) کرم ، پس از هر بار راه اندازی سیستم می گردند .

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\Run\MSKernel32

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\RunService\Win32DLL

در ادامه، بررسی می گردد که آیا دایرکتوری سیستم شامل فایل WinFAT32.exe است؟ در صورت وجود فایل فوق (نشاندهنده ویندوز ۹۵ و ۹۸)، صفحه آغاز برنامه مرورگر اینترنت (IE)، به فایل WIN-BUGFIX.exe بر روی سایت www.skyinet.net تبدیل می گردد . فایل فوق از یکی از دایرکتوری های موجود در سایت فوق با نام angelcat , chu , koichi دریافت خواهد شد . پس از فعال شدن مرورگر اینترنت (در زمان آتی) ، صفحه آغاز ، آدرس فایل مورد نظر را از راه دور مشخص و بدین ترتیب فایل از سایت skyinet اخذ می گردد . کلید رجیستری صفحه آغاز، در آدرس زیر قرار می گیرد.

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

ما قادر به دستیابی به www.skyinet.net ، بمنظور اخذ یک نسخه از فایل فوق نمی باشیم . با پیگیری انجام شده بر روی اینترنت مشخص شده است که برنامه فوق ، ممکن است آژانسی بمنظور جمع آوری رمزهای عبور و ارسال آنها به یک سایت مرکزی از طریق پست الکترونیکی باشد .

ILOVEYOU در ادامه بررسی می نماید که آیا ماشین را آلوده کرده است؟ بدین منظور در دایرکتوری مربوط به اخذ فایل ها (Download directory) ، بدنبال فایل WIN-BUGFIX.exe می گردد . در صورتیکه فایل فوق پیدا گردد ، کدهای مخرب ، یک کلید RUN را بمنظور فراخوانی WIN-BUGFIX.exe از دایرکتوری مربوطه فعال می نمایند . نشانه گویای این کلید رجیستری، بصورت زیر است:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WINB
UGFIX

ILOVEYOU در ادامه ، یک فایل با نام LOVE-LETTER-FOR-YOU.HTM در دایرکتوری سیستم ایجاد می نماید .فایل Htm ، شامل منطق VBScript بوده که به نسخه مربوطه vbs ارتباط خواهد داشت .

کدهای مخرب در ادامه ، از طریق نامه الکترونیکی برای افرادی که در لیست دفترچه آدرس مربوط به کاربر می باشند، اشاعه و توزیع می شوند . برای هر شخص موجود در دفترچه آدرس، یک پیام الکترونیکی ایجاد و یک نسخه از فایل LOVE-LETTER-FOR-YOU.vbs قبل از ارسال به آن ضمیمه می گردد. پس از ارسال پیام برای تمام افراد موجود در لیست دفترچه آدرس، ILOVEYOU بر روی تمام درایوهای موجود در کامپیوتر ، عملیات خود را تکرار می نماید . در صورتیکه درایو یک درایو شناخته شده (نظیر هارد و یا (CDROM باشد ، در تمام زیرفهرست های موجود در درایو مربوطه ، عملیات جستجو برای یافتن فایل های با انشعاب , hta jpg , sct , vbe , vbs , jpeg انجام خواهد شد . تمامی فایل های با انشعابات فوق، توسط کدهای مخرب بازنویسی و یک نسخه از کدهای مخرب در آنها قرار خواهد گرفت.

در صورتیکه فایلی از نوع mp2 و یا mp3 پیدا گردد، یک نسخه از کدهای مخرب در فایلی با انشعاب vbs ایجاد و در دایرکتوری مربوطه مستقر می گردد . نام فایل به نام دایرکتوری بستگی داشته و دارای انشعاب vbs است .

در صورتیکه ILOVEYOU فایلی با نام mirc.ini , mlink.exe , micr32.exe و یا mirc.hlp را پیدا نماید، فرض را بر این خواهد گذاشت که فهرست مربوطه ، یک دایرکتوری شروع (Internet Relay Chat) IRC است و فایلی با نام Script.ini را ایجاد و در محل مربوطه قرار خواهد داد . اسکریپت فوق، زمانیکه برنامه سرویس گیرنده IRC اجرا گردد، شروع به فعالیت نموده و اقدام به ارسال کدهای مخرب برای تمام کامپیوترهایی که با میزبان آلوده یک ارتباط IRC ایجاد نموده اند ، خواهد کرد.

امنیت نامه های الکترونیکی

اینترنت چالش های جدیدی را در عرصه ارتباطات ایجاد کرده است. کاربران اینترنت با استفاده از روش های متفاوت ، امکان ارتباط با یکدیگر را بدست آورده اند .اینترنت زیر ساخت مناسب برای ارتباطات نوین را فراهم و زمینه ای مساعد و مطلوب بمنظور بهره برداری از سرویس های ارتباطی توسط کاربران فراهم شده است . بدون شک ، پست الکترونیکی در این زمینه دارای جایگاهی خاص است .

پست الکترونیکی، یکی از قدیمی ترین و پرکاربردترین سرویس موجود در اینترنت است . شهروندان اینترنت، روزانه میلیون ها نامه الکترونیکی را برای یکدیگر ارسال می دارند. ارسال و دریافت نامه الکترونیکی، روش های سنتی ارسال اطلاعات (نامه های دستی) را بشدت دستخوش تحول نموده و حتی در برخی از کشورها، اغلب مردم تمایل به

استفاده از نامه الکترونیکی در مقابل تماس تلفتی با همکاران و خویشاوندان خود دارند. در این مقاله قصد نداریم به بررسی مزایای سیستم پست الکترونیکی اشاره نمائیم. در صورتیکه بپذیریم که سیستم پست الکترونیکی عرصه جدیدی را در ارتباطات افراد ساکن در کره زمین ایجاد کرده است، می بایست بگونه ای حرکت نمائیم که از آسیب های احتمالی تکنولوژی فوق نیز در امان باشیم.

طی سالیان اخیر، بدفعات شنیده ایم که شبکه های کامپیوتری از طریق یک نامه الکترونیکی آلوده و دچار مشکل و تخریب اطلاعاتی شده اند. صرفنظر از وجود نواقص امنیتی در برخی از محصولات نرم افزاری که در جای خود تولید کنندگان این نوع نرم افزارها بمنظور استمرار حضور موفقیت آمیز خود در عرصه بازار رقابتی موجود، می بایست مشکلات و حفره های امنیتی محصولات خود را برطرف نمایند، ما نیز بعنوان استفاده کنندگان از این نوع نرم افزارها در سطوح متفاوت، لازم است با ایجاد یک سیستم موثر پیشگیرانه ضریب بروز و گسترش این نوع حوادث را به حداقل مقدار خود برسانیم. عدم وجود سیستمی مناسب جهت مقابله با این نوع حوادث، می تواند مسائلی بزرگ را در یک سازمان بدنال داشته که گرچه ممکن است تولیدکننده نرم افزار در این زمینه مقصر باشد ولی سهل انگاری و عدم توجه به ایجاد یک سیستم امنیتی مناسب، توسط استفاده کنندگان مزید بر علت خواهد بود (دقیقا" مشابه عدم بستن کمر بند ایمنی توسط سرنشین یک خودرو با نواقص امنیتی). در این مقاله، به بررسی روش های پیشگیری از تخریب اطلاعات در شبکه های کامپیوتری از طریق پست الکترونیکی پرداخته و با ارائه راهکارهای مناسب، یک سیستم حفاظتی مطلوب پیشنهاد می گردد. در این راستا، عمدتاً" بر روی برنامه سرویس گیرنده پست الکترونیکی ماکروسافت (Outlook) متمرکز خواهیم شد(بدلیل نقش بارز و مشهود این نوع از برنامه ها در جملات اینترنتی اخیر.)

سیل ناگهانی حملات اینترنتی مبتنی بر کدهای مخرب، با ظهور کرم ILOVEYOU، وارد عرصه جدیدی شده است. سیستم های مدرن پست الکترونیکی بمنظور مقابله با این نوع از تهدیدات، تدابیر لازم را در جهت ایجاد یک حفاظ امنیتی مناسب برای مقابله با عرضه و توزیع کدهای مخرب آغاز نموده اند. برنامه های سرویس گیرنده پست الکترونیکی متعلق به شرکت ماکروسافت، هدفی جذاب برای اغلب نویسندگان کدهای مخرب می باشند. شاید یکی از دلایل آن، گسترده گی و مدل برنامه نویسی خاص بکارگرفته شده در آنان باشد. تاکنون کدهای مخرب فراوانی، محصولات ماکروسافت را هدف قرار داده اند. عملکرد قدرتمند سه نوع ویروس (و یا کرم) در زمینه تخریب اطلاعات از طریق اینترنت، شرکت ماکروسافت را وادار به اتخاذ تصمیمات امنیتی خاص در اینگونه موارد نمود. این ویروس ها عبارتند از :

ویروس Melissa، هدف خود را بر اساس یک فایل ضمیمه Word مورد حمله ویرانگر قرار می دهد. بمحض باز نمودن فایل ضمیمه، کد مخرب بصورت اتوماتیک فعال می گردد.

ویروس BubbleBoy، همزمان با مشاهده (پیش نمایش) یک پیام، اجراء می گردد. در این رابطه ضرورتی به باز نمودن فایل ضمیمه بمنظور فعال شدن و اجرای کدهای مخرب وجود ندارد. در ویروس فوق، کدهای نوشته شده در بدنه نامه الکترونیکی قرار می گیرند. بدین ترتیب، بمحض نمایش پیام توسط برنامه مربوطه، زمینه اجرای کدهای مخرب فراهم می گردد.

کرم ILOVEYOU از لحاظ مفهومی شباهت زیادی با ویروس Mellisa داشته و بصورت یک فایل ضمیمه همراه یک نامه الکترونیکی جابجا می گردد. در این مورد خاص، فایل ضمیمه خود را بشکل یک سند Word تبدیل نکرده و در مقابل فایل ضمیمه از نوع یک اسکریپت ویژوال بیسیک (. vbs) بوده و بمحض فعال شدن، توسط میزبان اسکریپت ویندوز (Windows Scripting Host :WSH) تفسیر و اجراء می گردد.

کاربرد پراکسی در امنیت شبکه

پراکسی چیست؟

در دنیای امنیت شبکه، افراد از عبارت «پراکسی» برای خیلی چیزها استفاده می کنند. اما عموماً، پراکسی ابزار است که بسته های دیتای اینترنتی را در مسیر دریافت می کند، آن دیتا را می سنجد و عملیاتی برای سیستم مقصد آن دیتا انجام می دهد. در اینجا از پراکسی به معنی پروسه ای یاد می شود که در راه ترافیک شبکه ای قبل از اینکه به شبکه وارد یا از آن خارج شود، قرار می گیرد و آن را می سنجد تا ببیند با سیاست های امنیتی شما مطابقت دارد و سپس مشخص می کند که آیا به آن اجازه عبور از فایروال را بدهد یا خیر. بسته های مورد قبول به سرور مورد نظر ارسال و بسته های رد شده دور ریخته می شوند.

پراکسی چه چیزی نیست؟

پراکسی ها بعضی اوقات با دو نوع فایروال اشتباه می شوند «Packet filter» و «Stateful packet filter» که البته هر کدام از روش ها مزایا و معایبی دارد، زیرا همیشه یک مصالحه بین کارایی و امنیت وجود دارد.

پراکسی با Packet filter تفاوت دارد

ابتدایی ترین روش صدور اجازه عبور به ترافیک بر اساس TCP/IP این نوع فیلتر بود. این نوع فیلتر بین دو یا بیشتر رابط شبکه قرار می گیرد و اطلاعات آدرس را در IP header ترافیک دیتایی که بین آنها عبور می کند، پیمایش می کند.

اطلاعاتی که این نوع فیلتر ارزیابی می‌کند عموماً شامل آدرس و پورت منبع و مقصد می‌شود. این فیلتر بسته به پورت و منبع و مقصد دیتا و براساس قوانین ایجادشده توسط مدیر شبکه بسته را می‌پذیرد یا نمی‌پذیرد. مزیت اصلی این نوع فیلتر سریع بودن آن است چرا که header، تمام آن چیزی است که سنجیده می‌شود. و عیب اصلی آن این است که هرگز آنچه را که در بسته وجود دارد، نمی‌بیند و به محتوای آسیب‌شده اجازه عبور از فایروال را می‌دهد. بعلاوه، این نوع فیلتر با هر بسته بعنوان یک واحد مستقل رفتار می‌کند و وضعیت (State) ارتباط را دنبال نمی‌کند.

امنیت شبکه: چالشها و راهکارها

اینترنت یک شبکه عظیم اطلاع رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک تک افراد ممکن خواهد شد. کارشناسان ارتباطات، بهره‌گیری از این شبکه را یک ضرورت در عصر اطلاعات می‌دانند.

این شبکه که از هزاران شبکه کوچکتر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. طبق آخرین آمار بیش از شصت میلیون رایانه از تمام نقاط جهان در این شبکه گسترده به یکدیگر متصل شده‌اند که اطلاعات بی‌شماری را در تمامی زمینه‌ها از هر سنخ و نوعی به اشتراک گذاشته‌اند. گفته می‌شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است.

این اطلاعات با سرعت تمام در بزرگراههای اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود.

حمایت از جریان آزاد اطلاعات، گسترش روزافزون فناوری اطلاعات و بسترسازی برای اتصال به شبکه‌های اطلاع‌رسانی شعار دولتهاست. این در حالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. انتشار تصاویر مستهجن، ایجاد پایگاههایی با مضامین پورنوگرافی و سایتهای سوءاستفاده از کودکان و انواع قاچاق در کشورهای پیشرفته صنعتی بخصوص در خاستگاه این شبکه جهانی یعنی آمریکا، کارشناسان اجتماعی را بشدت نگران کرده، به گونه‌ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا نموده است. هشدار، جریمه و بازداشت برای برپاکندگانی پایگاههای مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده‌اند.

ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه‌ای چارچوبهای اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می‌تواند سلامت و امنیت جامعه را به خطر اندازد. علی‌الرغم وجود جنبه‌ای مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبرو

ساخته است. از این رو بکارگیری فیلترها و فایر وال‌های مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه اینترنت را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است.

۲. امنیت شبکه‌های اطلاعاتی و ارتباطی

اهمیت امنیت شبکه

چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه‌ها مشخص می‌گردد. اگر امنیت شبکه برقرار نگردد، مزیت‌های فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعات عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی هستند. همچنین دستکاری اطلاعات - به عنوان زیربنای فکری ملت‌ها توسط گروه‌های سازماندهی شده بین‌المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود.

برای کشور ما که بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکت‌های خارجی تهیه می‌شود، بیم نفوذ از طریق راه‌های مخفی وجود دارد. در آینده که بانکها و بسیاری از نهادها و دستگاه‌های دیگر از طریق شبکه به فعالیت می‌پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه بصورت مسئله‌ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایت‌های ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟

نکته جالب اینکه بزرگترین شرکت تولید نرم‌افزارهای امنیت شبکه، شرکت چک پوینت است که شعبه اصلی آن در اسرائیل می‌باشد. مسأله امنیت شبکه برای کشورها، مسأله‌ای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژیها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، پس می‌بایست محققین کشور این مهم را بدست بگیرند و در آن فعالیت نمایند.

امروزه اینترنت آنقدر قابل دسترس شده که هرکس بدون توجه به محل زندگی، ملیت، شغل و زمان میتواند به آن راه یابد و از آن بهره ببرد. همین سهولت دسترسی آن را در معرض خطراتی چون گم شدن، ربوده شدن، مخدوش شدن یا سوءاستفاده از اطلاعات موجود در آن قرار می‌دهد. اگر اطلاعات روی کاغذ چاپ شده بود و در قفسه‌ای از اتاقهای محفوظ اداره مربوطه نگهداری می‌شد، برای دسترسی به آنها افراد غیرمجاز می‌بایست از حصارهای مختلف عبور می‌کردند، اما اکنون چند اشاره به کلیدهای رایانه‌ای برای این منظور کافی است.

سابقه امنیت شبکه

اینترنت در سال ۱۹۶۹ بصورت شبکه‌های بنام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌های متصل به هم، شرایطی ایجاد شود که حتی اگر، بخشهای عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتند، کل شبکه بتواند به کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا، فکر ایجاد شبکه، برای جلوگیری از اثرات مخرب حملات اطلاعاتی بود.

در سال ۱۹۷۱ تعدادی از رایانه‌های دانشگاهها و مراکز دولتی به این شبکه متصل شدند و محققین از این طریق شروع به تبادل اطلاعات کردند.

با بروز رخدادهای غیرمنتظره در اطلاعات، توجه به مسأله امنیت بیش از پیش اوج گرفت. در سال ۱۹۸۸، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه، مواجه شد که بعداً، «کرم موریس» نام گرفت. رابرت موریس که یک دانشجو در نیویورک بود، برنامه‌هایی نوشت که می‌توانست به یک رایانه‌ای دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و بصورت هندسی تکثیر شود. آن زمان ۸۸۰۰۰ رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه در آمریکا از کار بیفتند.

به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی (IRST) شکل گرفت که در هماهنگی فعالیتهای مقابله با حملات ضد امنیتی، آموزش و تجهیز شبکه‌ها و روشهای پیشگیرانه نقش مؤثری داشت. با رایج‌تر شدن و استفاده عام از اینترنت، مسأله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث، اختلال در امنیت شبکه، WINK/OILS در سال ۱۹۸۹، Sniff packet در سال ۱۹۹۴ بود که مورد اخیر از طریق پست الکترونیک منتشر می‌شد و باعث افشای اطلاعات مربوط به اسامی شماره رمز کاربران می‌شد. از آن زمان حملات امنیتی - اطلاعاتی به شبکه‌ها و شبکه جهانی روزبه‌روز افزایش یافته است.

گرچه اینترنت در ابتدا، با هدف آموزشی و تحقیقاتی گسترش یافت، امروزه کاربردهای تجاری، پزشکی، ارتباطی و شخصی فراوانی پیدا کرده است که ضرورت افزایش ضریب اطمینان آن را بیش از پیش روشن نموده است.

جرایم رایانه‌ای و اینترنتی

ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک همچون انتقال صدای انسان، جای خود را، به مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسانها بلکه مابین انسانها و رایانه‌ها، و همچنین بین خود رایانه‌ها نیز وجود دارد. استفاده وسیع از پست الکترونیک، و دستیابی به اطلاعات از طریق وبسایتهای متعدد در اینترنت نمونه‌هایی از این پیشرفتهای می‌باشد که جامعه را بطور پیچیده‌ای دگرگون ساخته‌اند.

سهولت در دسترسی و جستجوی اطلاعات موجود در سیستمهای رایانه‌ای توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی، منجر به رشد سرسام‌آور مقدار اطلاعات موجود در آگاهی که می‌توان از آن بدست آورد، شده است.

این اطلاعات موجب افزایش تغییرات اجتماعی و اقتصادی پیش‌بینی نشده گردیده است. اما پیشرفتهای مذکور جنبه خطرناکی نیز دارد که پیدایش انواع جرایم و همچنین بهره‌برداری از فناوری جدید در ارتکاب جرایم بخشی از آن به شمار می‌رود. بعلاوه عواقب و پیامدهای رفتار مجرمانه می‌تواند خیلی بیشتر از قبل و دور از تصور باشد چون که محدودیتهای جغرافیایی یا مرزهای ملی آن را محدود نمی‌کنند. فناوری جدید مفاهیم قانونی موجود را دچار چالشهایی ساخته است. اطلاعات و ارتباطات راه دور به راحت‌ترین وجه در جهان جریان پیدا کرده و مرزها دیگر موانعی بر سر این جریان به شمار نمی‌روند. جنایتکاران غالباً در مکانهایی به غیر از جاههایی که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند.

سوءاستفاده گسترده مجرمین، به ویژه گروههای جنایتکار سازمان نیافته از فناوری اطلاعات سبب گشته است که سیاستگذاران جنایی اغلب کشورهای جهان با استفاده از ابزارهای سیاست جنایی درصدد مقابله با آنها برآیند. تصویب کنوانسیون جرایم رایانه‌ای در اواخر سال ۲۰۰۱ و امضای آن توسط ۳۰ کشور پیشرفته، تصویب قوانین مبارزه با این جرایم توسط قانون‌گذاران داخلی و تشکیل واحدهای مبارزه با آن در سازمان پلیس بیشتر کشورهای پیشرفته و تجهیز آنها به جدیدترین سخت‌افزارها و نرم‌افزارهای کشف این گونه جرایم و جذب و بکارگیری بهترین متخصصین در واحدهای مذکور، بخشی از اقدامات مقابله‌ای را تشکیل می‌دهد.

پیدایش جرایم رایانه‌ای

در مورد زمان دقیق پیدایش جرم رایانه‌ای نمی‌توان اظهار نظر قطعی کرد. این جرم زائیده تکنولوژی اطلاعاتی و انفورماتیکی است، بنابراین بطور منظم بعد از گذشت مدت کوتاهی از شیوع و کاربرد تکنولوژی اطلاعات، باب سوءاستفاده نیز قابل طرح است. شیوع استعمال این تکنولوژی و برابری کاربران آن حداقل در چند کشور مطرح جهان بصورت گسترده، امکان بررسی اولین مورد را دشوار می‌سازد. در نهایت آن چه مبرهن است اینکه در جامعه آمریکا رویس موجب شد برای اولین بار اذهان متوجه سوءاستفاده‌های رایانه‌ای شود.

قضیه رویس:

آلدون رویس حسابدار یک شرکت بود. چون به گمان وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای، قسمتی از پولهای شرکت را اختلاس کرد. انگیزه رویس در این کار انتقام‌گیری بود.

مکانیزم کار بدین گونه بود که شرکت محل کار وی یک عمده‌فروش میوه و سبزی بود. محصولات متنوعی را از کشاورزان می‌خرید و با استفاده از تجهیزات خود از قبیل کامیونها، انبار و بسته‌بندی و سرویس‌دهی به گروههای فروشندگان، آنها را عرضه می‌کرد. به دلیل وضعیت خاص این شغل، قیمتها در نوسان بود و ارزیابی امور تنها می‌توانست از عهده رایانه برآید تا کنترل محاسبات این شرکت عظیم را عهده‌دار شود.

کلیه امور حسابرسی و ممیزی اسناد و مدارک و صورت حسابها به صورت اطلاعات مضبوط در نوارهای الکترونیکی بود.

رویس در برنامه‌ها، دستورالعمل‌های اضافی را گنجانده بود و قیمت کالاها را با ظرافت خاصی تغییر می‌داد. با تنظیم درآمد اجناس وی مبلغی را کاهش می‌داد و مبالغ حاصله را به حسابهای مخصوص واریز می‌کرد. بعد در زمانهای خاص چکی به نام یکی از هفده شرکت جعلی و ساختگی خودش صادر و مقداری از مبالغ را برداشت می‌کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما او بر سر راه خودش مشکلی داشت و آن این بود که مکانیسمی برای توقف عملکرد سیستم نمی‌توانست بیندیشد. بنابراین در نهایت خود را به مراجع قضایی معرفی و به جرم خود اعتراض کرد و به مدت ده سال به زندان محکوم شد. از این جا بود که مبحث جدیدی به نام جرم رایانه‌ای ایجاد شد.

تعریف جرم رایانه‌ای

تاکنون تعریف‌های گوناگونی از جرم رایانه‌ای از سوی سازمانها، متخصصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم است.

جرم رایانه‌ای یا جرم در فضای مجازی (سایر جرایم) دارای دو معنی و مفهوم است. در تعریف مضیق، جرم رایانه‌ای صرفاً عبارت از جرایمی است که در فضای سایبر رخ می‌دهد. از این نظر جرایمی مثل هرزه‌نگاری، افتراء، آزار و اذیت سوءاستفاده از پست الکترونیک و سایر جرایمی که در آنها رایانه به عنوان ابزار و وسیله ارتکاب جرم بکار گرفته می‌شود، در زمره جرم رایانه‌ای قرار نمی‌گیرند.

در تعریف موسع از جرم رایانه‌ای هر فعل و ترک فعلی که در اینترنت یا از طریق آن یا با اینترنت یا از طریق اتصال به اینترنت، چه بطور مستقیم یا غیرمستقیم رخ می‌دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است جرم رایانه‌ای نامیده می‌شود. براین اساس اینگونه جرایم را می‌توان به سه دسته تقسیم نمود:

دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند. مانند سرقت، تخریب و غیره

دسته دوم: جرایمی هستند که در آنها رایانه به عنوان ابزار وسیله توسط مجرم برای ارتکاب جرم بکار گرفته می‌شود.

دسته سوم: جرایمی هستند که می‌توان آنها را جرایم رایانه‌ای محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می‌پیوندند اما آثار آنها در دنیای واقعی ظاهر می‌شود. مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای.

راهکارهای امنیتی شبکه

۱ - کنترل دولتی

علاوه بر بهره‌گیری از امکانات فنی، روشهای کنترل دیگری نیز برای مهار اینترنت پیشنهاد شده است. در این روش، سیاست کلی حاکم بر کشور اجازه دسترسی به پایگاههای مخرب و ضد اخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازه اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند.

۲ - کنترل سازمانی

روش دیگر کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرند، خود موظف به کنترل شبکه و نظارت بر استفاده صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی توأمآ انجام این وظیفه را تضمین کند.

۳ - کنترل فردی

کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل تمام تضمینهای اجرایی، درون فردی است و شخص با بهره‌گیری از وجدان فردی و مبانی اخلاقی و تعهد دینی، مراقبتهای لازم را در ارتباط با شبکه‌های جهانی به عمل آورد. این اعتقاد و فرهنگ در محدوده خانواده نیز اعمال می‌شود و چه بسا اطرافیان را نیز تحت تأثیر قرار دهد. البته شیوه اخیر در صورتی ممکن خواهد بود که واگذاری خط اشتراک IP پس از شناسایی کامل افراد و با ملاحظه خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند. آرزویی که نمی‌تواند بسیاری از تأثیرات سوء این شبکه را از بین ببرد و آن را بسوی شبکه سالم سوق دهد.

۴ - تقویت اینترنت‌ها

از سوی دیگر تقویت شبکه‌های داخلی که به اینترنت معروف است می‌تواند نقش بسزایی در کاهش آلودگیهای فرهنگی و اطلاعاتی اینترنت یاری کند. قرار دادن اطلاعات مفید اینترنت به صورت ناپیوسته و روی شبکه‌های داخلی یا اینترنتها، علاوه بر ارائه خدمات و اطلاع‌رسانی سالم، پس از چندی، بایگانی غنی و پرباری از انواع اطلاعات فراهم آمده از چهار گوشه جهان را در اختیار کاربران قرار می‌دهد که با افزایش اطلاعات داخلی و یا روزآمد کردن آن، به عنوان زیربنای اطلاعاتی کشور قابل طرح می‌باشد. به هر حال سرعت بالا و هزینه کم در استفاده از اینترنتها، دو عامل مورد توجه کاربران به شبکه‌های داخلی است که به نظر نمی‌رسد محمل مناسبی برای اطلاعات گزینش شده اینترنت باشد.

۵ - وجود یک نظام قانونمند اینترنتی

مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیبهای اینترنتی از قبیل تهاجم فرهنگی، اطلاعات نادرست و یا پیامدهای ضد اخلاقی نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که اداره آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسار گسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری نماید.

این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تأثیرپذیری از فرهنگهای بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد.

۶ - کار گسترده فرهنگی برای آگاهی کاربران

اما بهترین روش، کار گسترده فرهنگی، برای آگاهی کاربران است. کافی است که آنها آگاه شوند که گرایش و ارتباط با پایگاههای غیرمتعارف جز ضلالت و تباهی ثمره‌های ندارد. باید تقوای درونی و اعتقادات دینی کاربران را رشد داد و آنها را تقویت کرد. بنابراین بهترین بارو (فایروال) برای ممانعت از خطرات اینترنت و جلوگیری از تأثیر ابعاد منفی آن، وجدان درونی و ایمان هر نسل است که بخشی از این ایمان را علمای دین باید در وجود نسل جوان و انسانهای این عصر بارور سازند.

۷ - فایروالها

در حقیقت فایروال یا بارو شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها (هکرها) و وب سایت‌های نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و داراییهای شما را از دسترس نیروهای متخاصم دور نگاه می‌دارد.

بارو یک برنامه یا وسیله سخت‌افزاری است که اطلاعات ورودی به سیستم رایانه و شبکه‌های اختصاصی را تصفیه می‌کند. اگر یک بسته اطلاعاتی ورودی به وسیله فیلترها نشان‌دار شود، اجازه ورود به شبکه و رایانه کاربر را نخواهد داشت.

به عنوان مثال در یک شرکت بزرگ بیش از صد رایانه وجود دارد که با کارت شبکه به یکدیگر متصل هستند. این شبکه داخلی توسط یک یا چند خط ویژه به اینترنت متصل است. بدون استفاده از یک بارو تمام رایانه‌ها و اطلاعات موجود در این شبکه برای شخص خارج از شبکه قابل دسترسی است و اگر این شخص راه خود را بشناسد می‌تواند یک رایانه‌ها را بررسی و با آنها ارتباط هوشمند برقرار کند. در این حالت اگر یک کارمند خطایی را انجام دهد و یک حفره امنیتی ایجاد شود، رخنه‌گرها می‌توانند وارد سیستم شده و از این حفره سوء استفاده کنند.

اما با داشتن یک بارو همه چیز متفاوت خواهد بود. باروها روی خطوطی که ارتباط اینترنتی برقرار می‌کنند، نصب می‌شوند و از یک سری قانونهای امنیتی پیروی می‌کنند. به عنوان مثال یکی از قانونهای امنیتی شرکت می‌تواند به صورت زیر باشد:

از تمام پانصد رایانه موجود در شرکت فقط یکی اجازه دریافت صفحات ftp را دارد و بارو باید مانع از ارتباط دیگر رایانه‌ها از طریق ftp شود.

این شرکت می‌تواند برای وب سرورها و سرورهای هوشمند و غیره نیز چنین قوانینی در نظر بگیرد. علاوه بر این، شرکت می‌تواند نحوه اتصال کاربران- کارمندان به شبکه اینترنت را نیز کنترل کند به عنوان مثال اجازه ارسال فایل از شبکه به خارج را ندهد.

در حقیقت با استفاده از بارو یک شرکت می‌تواند نحوه استفاده از اینترنت را تعیین کند. باروها برای کنترل جریان عبوری در شبکه‌ها از سه روش استفاده می‌کنند:

Packet Filtering

یک بسته اطلاعاتی با توجه به فیلترهای تعیین شده مورد تحلیل و ارزیابی قرار می‌گیرند. بسته‌هایی که از تمام فیلترها عبور می‌کنند به سیستمهای موردنیاز فرستاده شده و بقیه بسته‌ها رد می‌شوند.

Proxy Services

اطلاعات موجود در اینترنت توسط بارو اصلاح می‌شود و سپس به سیستم فرستاده می‌شود و بالعکس.

Stateful Inspection

این روش جدید محتوای هر بسته با بسته‌های اطلاعاتی ویژه‌ای از اطلاعات مورد اطمینان مقایسه می‌شوند. اطلاعاتی که باید از درون بارو به بیرون فرستاده شوند، با اطلاعاتی که از بیرون به درون ارسال می‌شود، از لحاظ داشتن

خصوصیات ویژه مقایسه می‌شوند و در صورتی که با یکدیگر ارتباط منطقی داشتن اجازه عبور به آنها داده می‌شود و در غیر اینصورت امکان مبادله اطلاعات فراهم نمی‌شود.

کوکی (Cookie) چیست؟

تقریباً تمام سایت‌هایی که بازدید می‌کنید اطلاعاتی را در قالب یک فایل کوچک متنی (Text) بر روی کامپیوتر شما ذخیره می‌کنند به این فایل کوکی می‌گویند محل ذخیره شدن این فایل در فولدر Temporary Internet Files در اینترنت اکسپلورر و در نت اسکپ در فولدر Cashe است در اپرا و موزیلا و نسخه‌های قدیمی‌تر اینترنت اکسپلورر در فولدر جدایی به نام کوکی است.

انواع مختلفی از کوکی‌ها وجود دارد و شما در نسخه‌های جدیدتر وب‌بروسرها (Web Browsers) این امکان را دارید که انتخاب کنید کدام کوکی‌ها بر روی کامپیوتر شما ذخیره شوند در صورتی که کوکی‌ها را کاملاً غیر فعال کنید ممکن است بعضی سایت‌های اینترنتی را نتوانید ببیند و یا از بعضی امکانات مثل به یاد داشتن شناسه و رمز عبور شما در آن سایت محروم شوید و یا انتخاب‌هایی که داشتید مثل ساعت محلی و یا دمای هوای محلی و کلاً از تنظیمات شخصی‌ای که در آن وب‌سایت انجام داده‌اید نتوانید استفاده کنید.

کوکی‌ها چگونه مورد استفاده قرار می‌گیرند؟

همانطوری که گفتیم کوکی یک فایل است که توسط یک وب‌سایت برای حفظ اطلاعات بر روی کامپیوتر شما قرار می‌گیرد یک کوکی می‌تواند شامل اطلاعاتی باشد که شما در آن سایت وارد کرده‌اید مانند ای‌میل - آدرس - شماره تلفن و سایر اطلاعات شخصی - همچنین کوکی‌ها می‌توانند صفحات و یا کارهایی را که در آن وب‌سایت انجام داده‌اید مثل تعداد کلیک لینک‌های بازدید شده و مدت بازدید را نیز ضبط کنند. این به سایت کمک می‌کند تا دفعه بعد که به آن سایت بازگشتید اطلاعات شما را به خاطر داشته باشد و از وارد کردن تکراری اطلاعات خودداری کنید نمونه بارز این مطلب لاگ این ماندن شما در آن سایت است و یا پیغام‌های Welcome Back و یا حفظ تنظیماتی که در آن سایت انجام داده‌اید به عنوان مثال می‌توان به خصوصی کردن صفحه My MSN اشاره کرد. نکته‌ای را که باید به خاطر داشته باشید این است که هر وب‌سایت فقط می‌تواند از اطلاعاتی که شما وارد کرده‌اید استفاده کند نه بیشتر مثلاً اگر ای‌میل خود را در آن سایت وارد نکرده‌اید آن وب‌سایت نمی‌تواند ای‌میل شما را به دست آورد و یا به سایر اطلاعات کامپیوتر شما دست یابد.

مورد دیگر اینکه وب‌سایت‌ها فقط می‌توانند کوکی‌هایی را که خود ایجاد کرده‌اند بخوانند و نمی‌توانند از سایر کوکی‌های موجود استفاده کنند. وقتی که از یک وب‌سایت برای بار دوم بازدید می‌کنید آن وب‌سایت به دنبال کوکی مربوط به خود می‌گردد و در صورت وجود آن استفاده می‌کند. (البته باز هم با توجه به تنظیماتی که انجام داده‌اید)

و اما این مفاهیم در کوکی‌ها چه معنایی می‌دهند؟

First Party : کوکی هایی هستند که فقط اطلاعات آنها به سایت که توسط آنها ایجاد شده اند فرستاده می شود و کار آنها همانطور که اشاره شد یادآوری اطلاعات ماست.

Third Party : کوکی هایی هستند که اطلاعات را به چندین سایت مختلف غیر از آنچه بازدید می کنید می فرستند استفاده این کوکی ها معمولا تجاری است بدینگونه که شما از سایتی بازدید می کنید و آن سایت دارای برندهای تجاری و تبلیغات از سایت دیگری (**Third Party**) می باشد در اینجاست که کوکی **Third Party** وارد عمل شده و اطلاعات شما را ثبت می کند به عنوان مثال صاحب تبلیغ با استفاده از این امکان می تواند ببیند که شما چه نوع تبلیغ هایی را بازدید می کنید و در کدام سایت ها. این نوع کوکی هم می توانند از نوع دائمی و هم موقت باشند. اصولا این نوع کوکی ها استاندارد نیستند و توسط مرورگرهای جدید بلوک می شوند. همچنین این کوکی ها ممکن است به هکر ها کمک کنند تا اطلاعات شخصی شما را بدست بیاورند. (برای جلوگیری از آخرین پیچ های مرورگر خود استفاده کنید*) اصولا پیشنهاد می شود تا این کوکی ها را که هیچ استفاده مفیدی برای کاربر ندارند بلوک کنید.

آشنایی با دیواره آتش - Firewall

Firewall در فرهنگ کامپیوتر یعنی محافظت از شبکه های داخلی در مقابل شبکه های خطا کار . معمولا یک شبکه کامپیوتری با تمام دسترسی ها در طرف و در طرف دیگر شما شبکه تولیدات شرکت را دارید که باید در مقابل رفتارهای مخرب محافظت شود. چند سوال مطرح می شود که آیا واقعا نیاز به محافظت از یک شبکه داخلی داریم و سوال دیگر اینکه چگونه از طریق **Firewall** در فرهنگ کامپیوتر یعنی محافظت از شبکه های داخلی در مقابل شبکه های خطا کار .

معمولا یک شبکه کامپیوتری با تمام دسترسی ها در طرف و در طرف دیگر شما شبکه تولیدات شرکت را دارید که باید در مقابل رفتارهای مخرب محافظت شود. چند سوال مطرح می شود که آیا واقعا نیاز به محافظت از یک شبکه داخلی داریم و سوال دیگر اینکه چگونه از طریق یک شبکه عمومی مانند اینترنت به آن دسترسی داشته باشیم .

دلیل بسیار ساده ای دارد ؟ که آن نیاز به بقاء و رقابت است . اعتبار کمپانیها در اینترنت به تبلیغات تولیداتشان می باشد . اینترنت به صورت شگفت انگیزی در حال رشد است .

مانند یک فروشگاه بسیار بزرگ بیشتر مردم به طرف اینترنت می آیند و همانطوریکه در یک فروشگاه باید محصولات سالم باشند و بعد از فروش گارانتی بشوند اطلاعات و داده و انتقالات آنها نیز باید به صورت امن و گارانتی شده باشد .

حال باید مکانیزمهایی برای حفاظت از شبکه داخلی یا اینترنت شرکت در مقابل دسترسی های غیر مجاز ارائه دهیم

Firewall های مختلفی با ساختارهای مختلف وجود دارد ولی عقیده اصلی که پشت آنها خوابیده یکسان است . شما به شبکه ای نیاز دارید که به کاربرانان اجازه دسترسی به شبکه های عمومی مانند اینترنت را بدهد و برعکس .

مشکل زمانی پیش می آید که کمپانی شما بدون در نظر گرفتن معیارهای امنیت بخواهد به اینترنت وصل شود و شما در معرض دسترسی از طرف **Server** های دیگر در اینترنت هستید. نه تنها شبکه داخلی کمپانی در مقابل دسترسی های غیر مجاز آسیب پذیر است بلکه تمام **Server** های موجود در شبکه کمپانی در معرض خطر هستند .

بنابراین به فکر محافظت از شبکه می افتید و اینجاست که نیاز به یک **Firewall** احساس می شود .

به هر حال قبل از فکر کردن درباره **Firewall** باید سرویسها و اطلاعاتی که می خواهید روی اینترنت در دسترس عموم قرار دهید مشخص کنید .

آشکارست که در ابتدا شما می خواهید مطمئن شوید که سرور شما امن است شما می توانید مجوزهای دسترسی ، انتقال فایل و اجرای راه دور و همچنین منع مجوزهای ورود دوباره ، **Telnet , Ftp , SMTP** و دیگر سرویسها . اگر شما بخواهید از این سرویسها استفاده کنید نیاز به **Firewall** دارید

به هر حال **Firewall** چیست ؟ اساسا یک فایروال جداکننده شبکه های امن از ناامن در اینترنت است . **Firewall** تمام اتصالاتی که از اینترنت به شبکه های محافظت وارد می شوند را فیلتر می کند .

قبل از تعریف اینکه چه نوع از **Firewall** ها بهترین مجموعه برای نیازهای ماست ، ما باید توپولوژی شبکه را برای تعیین اجزای آن مانند **Hub** ها ، **Switch** ها ، **Router** ها و **Cabling** آنالیز کنیم تا بهترین **Firewall** که مخصوص این توپولوژی باشد را پیدا کنیم .

برای ایجاد امنیت در شبکه ما نیاز به بررسی شبکه داخلی از لحاظ مدل لایه بندی **ISO** آن داریم بطوریکه می دانید **Reapter** ها و **Hub** ها در لایه اول ، **Switch** ها و **Bridge** ها در لایه دوم و **Router** ها در لایه سوم ، یک **Firewall** در تمام لایه های شبکه می تواند عمل کند (از جمله در هر هفت لایه) لایه ها مسئول پاسخگویی به کنترل و ایجاد نشستها و بکارگیری آنها می باشند . بنابراین با یک **Firewall** ما می توانیم جریان اطلاعات را در طول ایجاد کنترل کنیم .

بالا بردن امنیت شبکه خانگی

از نظر بسیاری از کارشناسان امنیتی ، استفاده از یک کامپیوتر قدیمی برای ارتباط با یک شبکه خانگی بیشترین ضرر خود را متوجه امنیت شبکه ای و کامپیوتر شما خواهد کرد. اما یقیناً هر چیزی راه حلی دارد. در این ترفند قصد داریم تا روشی بسیاری کاربردی را به شما معرفی کنیم که با بهره گیری از آن میتوانید امنیت شبکه خانگی خود را بر روی کامپیوتر قدیمی به حد اکثر برسانید. آن هم با هزینه ای بسیار ناچیز اما توانمندی و کاربردی واقعاً بالا. این دیوار امنیتی قدرتمند بر روی شبکه خانگی SmoothWall نام دارد.

تعریف یک کامپیوتر قدیمی:

در اینجا ، هدف ما از نام بردن یک کامپیوتر قدیمی ، سیستمی است با حداقل توانایی داشتن پردازنده پنتیوم ، ۶۴ مگابایت رم ، یک هارد درایو و یک CD-ROM.

به چه چیزهایی نیاز خواهید داشت؟

شما حداقل به دو کارت Ethernet نیاز دارید: یکی برای اتصال به منبع اینترنت خود و دیگری برای اتصال به شبکه خانگی.

چه تعداد کامپیوتر مورد حفاظت قرار خواهند گرفت؟

شما در صورت داشتن یک Hub میتوانید شبکه خانگی خود را میان چندین کامپیوتر پخش کنید. در نتیجه با این روش محدودیتی نخواهید داشت. به عنوان مثال اگر ۵ کامپیوتر قدیمی داشته باشید که با هم شبکه شده اند به سادگی و با استفاده از این روش میتوانید امنیت کلیه این سیستم ها را بالا ببرید.

روش انجام کار:

ابتدا باید این حفاظ امنیتی یعنی SmoothWall Express را دانلود کنید. بدین منظور به آدرس اینترنتی <http://www.smoothwall.org/get> بروید. اکنون آخرین ورژن منتشر شده این بسته رایگان را بسته به نوع سیستم قدیمی خود دانلود کنید. دقت فراوان کنید ، فایلی که شما دانلود میکنید یک ISO CD Image است. معنی

این است که پس از دریافت این فایل شما میبایست فایل فوق را که یک Image است را بر روی یک CD خام ، رایت کنید. دقت کنید این فایل را توسط نرم افزارهای جانبی همانند Nero و توسط گزینه Burn image to disk رایت کنید نه به عنوان یک Data CD.

حال پس از رایت CD ، سیستم خود را از نو راه اندازی کنید. (ترفندستان) دقت کنید که حتماً تنظیمات BIOS به گونه ای تنظیم شده باشد که سیستم از روی CD بوت شود.

اکنون پس از بوت شدن سیستم توسط CD صفحه نصب SmoothWall Express برای شما نمایان خواهد شد. شما میبایست مراحل ساده نصب را طی کنید تا این دیوار امنیتی قدرتمند بر روی کامپیوتر و شبکه شما نصب گردد.

در پایان کافی است کابل شبکه خود را نصب کنید. در حال حاضر یک حافظ امنیتی کل شبکه خانگی و کامپیوتر قدیمی شما را احاطه کرده است.