نمی‌گردد. با این وجود از آنجاییکه خادم اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که می‌تواند بر اثر حمله فیزیکی به آن رخ دهد، ارتباط کل شبکه دچاراختلال می‌شود، هرچند که با درنظرگرفتن افزونگی برای خادم اصلی از احتمال چنین حالتی کاسته می‌شود.

ج – طراحی مش : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

۳-۱ – محل‌های امن برای تجهیزات

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می‌گیرد :

- یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه‌ای که هرگونه نفوذ در محل آشکار باشد.
- در نظر داشتن محلی که در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه‌ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان‌های بلااستفاده سود برده است (که باعث ایجاد خطرهای امنیتی می‌گردد)، می‌توان اعتدالی منطقی را در نظر داشت.

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت:

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.
- استفاده از دوربین‌های پایش در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه‌های داده.
- اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

۴-۱ – انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از خادم‌ها و سرویس‌دهنده‌های مورد اطمینان شبکه معطوف شده است، ولی گونه‌ای از حمله‌ی فیزیکی کماکان دارای خطری بحرانی است.

عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه در زوج‌های تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای

نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

۵-۱ – منابع تغذیه

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه. این طراحی باید به گونه‌ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی تامین فشار بیش‌اندازه‌ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند.
- وجود منبع یا منابع تغذیه پشتیبان به گونه‌ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

۶-۱ – عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برابر عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید در نظر گرفت می‌توان به دو عامل زیر اشاره کرد:

- احتمال حریق (که عموماً غیر طبیعی است و منشآ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که می‌توان از عدم اختلال در شبکه در صورت بروز چنین وقعایعی اطمینان حاصل کرد.

۲ – امنیت منطقی

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند. در این بخش به عوامل و مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

۲-۱ – امنیت مسیریاب‌ها

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود:

- حمله برای غیرفعال سازی کامل
- حمله به قصد دستیابی به سطح کنترل
- حمله برای ایجاد نقص در سرویس‌دهی

طبیعی است که راه‌ها و نکاتی که در این زمینه ذکر می‌شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای ولو مرتبط با این تجهیزات منفک هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تآمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنبه‌ی آنرا تشکیل می‌دهد.

۲-۲ – مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخ پشتیبان از پرونده‌ها مختص پیکربندی است. از این پرونده‌ها که در حافظه‌های گوناگون این تجهیزات نگاهداری می‌شوند، می‌توان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می‌یابند، نسخه پشتیبان تهیه کرد.

با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را

به آخرین حالت بی‌نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت‌افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه نسخه پشتیبان را فاصله‌های زمانی متغیر دارا می‌باشند. با استفاده از این نرم‌افزارها احتمال حملاتی که به سبب تآخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید می‌آید به کمترین حد ممکن می‌رسد.

۳-۲ – کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد:

- کنترل از راه دور
- کنترل از طریق درگاه کنسول

در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استاندارها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در مورد روش دوم، با وجود آنکه به نظر می‌رسد استفاده از چنین درگاهی نیاز به دسترسی فیزکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد. لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تآمین نمی‌کند.

برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه کنسول به هریک از تجهیزات داخلی مسیریاب، که امکان دسترسی از راه‌دور دارند، اطمینان حاصل نمود.

۲-۴ – امن سازی دسترسی

علاوه بر پیکربندی تجهیزات برای استفاده از Authentication، یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش SSH(Secur Shell) است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPsec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است، به گونه‌ای که اغلب تولیدکنندگان تجهیزات فعال شبکه، خصوصاً تولید کنندگان مسیریاب‌ها، این روش را مرجح می‌دانند.

۲-۵ – مدیریت رمزهای عبور

مناسب‌ترین محل برای ذخیره رمزهای عبور بر روی خادم Authentication است. هرچند که در بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخت‌افزار نگاه‌داری شوند. در این صورت مهمترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه است.

۳ – ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه

می‌دهند. به عبارت دیگر این شبکه‌های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه‌ی جهانی اینترنت کنونی را شکل می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

۱-۳ – قابلیت‌های امنیتی

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود:

۱ – قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

۲ – وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند. از آنجاییکه شبکه‌های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، با استفاده از سیستم‌های IDS بر روی آنها، می‌توان به بالاترین بخت برای تشخیص حملات دست یافت.

۳ – قابلیت تشخیص منبع حملات. با وجود آنکه راه‌هایی از قبیل سرقت آدرس و استفاده از سیستم‌های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار می‌نمایند، ولی استفاده از سیستم‌های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه‌ی مشکوک به وجود منبع اصلی می‌نماید. بیشترین تأثیر این مکانیزم زمانی است که حملاتی از نوع DoS از سوی نفوذگران انجام می‌گردد.

۲-۳ – مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست.

یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS است. خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو جریان از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و بسته‌های اطلاعاتی خواهد کاست. برای جبران این کاهش سرعت تنها می‌توان متوسل به تجهیزات گران‌تر و اعمال سیاست‌های امنیتی پیچیده‌تر شد.

با این وجود، با هرچه بیشتر حساس شدن ترافیک و جریان‌های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبکه‌های کوچکی که خود به شبکه‌های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه‌ها می‌توان داشت.

امنیت در اینترنت

قطعا" تاکنون اخبار متعددی را در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آنان، یکی از روش های مناسب دفاعی است.

اهمیت امنیت در اینترنت

بدون شک کامپیوتر و اینترنت در مدت زمان کوتاهی توانسته اند حضور مشهود خود را در تمامی عرصه های حیات بشری به اثبات برسانند. وجود تحولات عظیم در ارتباطات (نظیر Email و تلفن های سلولی)، تحولات گسترده در زمینه تجهیزات الکترونیکی و سرگرمی (کابل دیجیتال، mp3)، تحولات گسترده در صنعت حمل و نقل (سیستم هدایت اتوماتیک اتومبیل، ناوبری هوائی)، تغییرات اساسی در روش خرید و فروش کالا (فروشگاههای online، کارت های اعتباری)، پیشرفت های برجسته در عرصه پزشکی، صرفا" نمونه هائی اندک در این زمینه می باشد.

اجازه دهید به منظور آشنائی با جایگاه کامپیوتر در زندگی انسان عصر حاضر و اهمیت امنیت اطلاعات، این پرسش را مطرح نمائیم که در طی یک روز چه میزان با کامپیوتر درگیر هستید و چه حجمی از اطلاعات شخصی شما بر روی کامپیوتر خود و یا سایر کامپیوترهای دیگر، ذخیره شده است؟ پاسخ به سوال فوق، جایگاه کامپیوتر و اهمیت ایمن سازی اطلاعات در عصر اطلاعات را به خوبی مشخص خواهد کرد.

امنیت در اینترنت، حفاظت از اطلاعات با استناد به سه اصل اساسی زیر است:

- نحوه پیشگیری از بروز یک تهاجم
- نحوه تشخیص یک تهاجم

-
- نحوه برخورد با حملات

انواع تهدیدات

اینترنت، علیرغم تمامی جنبه های مثبت دارای مجموعه ای گسترده از خطرات و تهدیدات امنیتی است که برخی از آنان بسیار جدی و مهم بوده و برخی دیگر از اهمیت کمتری برخوردار می باشند:

- عملکرد ویروس های کامپیوتری که می تواند منجر به حذف اطلاعات موجود بر روی یک کامپیوتر شود.
- نفوذ افراد غیر مجاز به کامپیوتر شما و تغییر فایل ها
- استفاده از کامپیوتر شما برای تهاجم علیه دیگران
- سرقت اطلاعات حساس نظیر شماره کارت اعتباری و خرید غیر مجاز با استفاده از آن

با رعایت برخی نکات می توان احتمال بروز و یا موفقیت این نوع از حملات را به حداقل مقدار خود رساند.

نحوه حفاظت

اولین مرحله به منظور حفاظت و ایمن سازی اطلاعات ، شناخت تهدیدات و آگاهی لازم در خصوص برخی مفاهیم اولیه در خصوص ایمن سازی اطلاعات است.

- **Hacker، attacker و یا Inruder** . اسامی فوق به افرادی که همواره در صدد استفاده از نقاط ضعف و آسیب پذیر موجود در نرم افزارها می باشند، اطلاق می گردد. با این که در برخی حالات ممکن است افراد فوق اهداف غیر
- مخربی را نداشته و انگیزه آنان صرفا" کنجکاوی باشد، ماحصل عملیات آنان می تواند اثرات جانبی منفی را به دنبال داشته باشد.

- **کد مخرب** : این نوع کدها شامل ویروس ها، کرم ها و برنامه های تروجان (Trojan) بوده که هر یک از آنان دارای ویژگی های منحصر بفردی می باشند:

□ **ویروس ها** ، نوع خاصی از کدهای مخرب می باشند که شما را ملزم می نمایند به منظور آلودگی سیستم، عملیات خاصی را انجام دهید. این نوع از برنامه ها به منظور نیل به اهداف مخرب خود نیازمند یاری کاربران می باشند. باز نمودن یک فایل ضمیمه همراه Email و یا مشاهده یک صفحه وب خاص، نمونه هائی از همکاری کاربران در جهت گسترش این نوع از کدهای مخرب است.

□ **کرم ها** : این نوع از کدهای مخرب بدون نیاز به دخالت کاربر، توزیع و گسترش می یابند. کرم ها، عموما" با سوء استفاده از یک نقطه آسیب پذیر در نرم افزار فعالیت خود را آغاز نموده و سعی می نمایند که کامپیوتر هدف را آلوده نمایند . پس از آلودگی یک کامپیوتر، تلاش برای یافتن و آلودگی سایر کامپیوتر انجام خواهد شد. همانند ویروس های کامپیوتری، کرم ها نیز می توانند از طریق Email، وب سایت ها و یا نرم افزارهای مبتنی بر شبکه، توزیع و گسترش یابند. توزیع اتوماتیک کرم ها نسبت به ویروس ها یکی از تفاوت های محسوس بین این دو نوع کد مخرب، محسوب می گردد.

□ **برنامه های تروجان** : این نوع از کدهای مخرب، نرم افزارهائی می باشند که ادعای ارائه خدماتی را داشته ولی در عمل، اهداف خاص خود را دنبال می نمایند. (تفاوت در حرف و عمل). مثلا" برنامه ای که ادعای افزایش سرعت کامپیوتر شما را می نماید، ممکن است در عمل اطلاعات حساس موجود برروی کامپیوتر شما را برای یک مهاجم و یا سارق از راه دور، ارسال نماید.

محافظت در مقابل خطرات ایمیل (۱)

مقدمه

می خواهیم ببینیم چرا نرم افزار ضد ویروس به تنهایی برای محافظت سازمان شما در مقابل حمله ویروسهای کامپیوتری فعلی و آینده کافی نیست. علاوه بر اینها گاهی به ابزاری قوی برای بررسی محتوای ایمیلها برای حفاظت در مقابل حملات و ویروسهای ایمیل(منظور از ویروس ایمیل ویروسی است که ازطریق ایمیل گسترش می یابد) و جلوگیری از نشت اطلاعات نیاز است. اما در هر صورت رعایت بعضی نکات همیشه توسط کاربران الزامی است.

خطرات ویروسهای ایمیل و اسبهای تروا

استفاده گسترده از ایمیل راه ساده ای را برای گسترش محتویات مضر در شبکه ها پیش روی هکرها قرار داده است. هکرها براحتی می توانند از حصار ایجاد شده توسط یک فایروال از طریق نقب زدن از راه پروتکل ایمیل عبور کنند، زیرا فایروال محتویات ایمیل را بررسی نمی کند. CNN در ژانویه ۲۰۰۴ گزارش داد که ویروس MyDoom هزینه ای در حدود ۲۵۰ میلیون دلار را بدلیل آسیب های وارده و هزینه های پشتیبانی فنی بر شرکتها تحمیل کرده است، این در حالیست که NetworkWorld هزینه های مقابله با Blaster، SoBig.F، Wechia و سایر ویروسهای ایمیل تا سپتامبر ۲۰۰۳ را تنها برای شرکتهای ایالات متحده ۳/۵ میلیارد دلار ذکر کرد.(یعنی عدد ۳۵ با هشت تا صفر جلوش!!!)

بعلاوه، از ایمیل برای نصب اسبهای تروا استفاده می شود که مشخصاً سازمان شما را برای بدست آوردن اطلاعات محرمانه یا بدست گیری کنترل سرورتان، هدف می گیرند. این ویروسها که خبرگان امنیت از آنها بعنوان ویروسهای جاسوسی یاد می کنند، ابزار قدرتمندی در جاسوسی صنعتی بشمار میروند! یک مورد آن حمله ایمیلی به شبکه مایکروسافت در اکتبر۲۰۰۰ است که یک سخنگوی شرکت مایکروسافت از آن بعنوان "یک عمل جاسوسی ساده و تمیز" یاد کرد. برطبق گزارشها، شبکه مایکروسافت توسط یک تروای backdoor که به یک کاربر شبکه توسط ایمیل ارسال شده بود، هک شد.

خطر نشت و فاش شدن اطلاعات

سازمانها اغلب در آگاهی دادن به کارکنانشان نسبت به وجود مخاطرات دزدی داده های مهم شرکتهایشان، کوتاهی می کنند. مطالعات مختلف نشان داده است که چگونه کارمندان از ایمیل بمنظور فرستادن اطلاعات حقوقی محرمانه استفاده می کنند. گاهی آنها اینکار را از روی ناراحتی یا کینه توزی انجام می دهند. گاهی بدلیل عدم درک مناسب از ضربه مهلکی است که در اثر این عمل به سازمان وارد می شود.

گاهی کارمندان از ایمیل برای به اشتراک گذاری داده های حساسی استفاده می کنند که رسماً می بایست در داخل سازمان باقی می ماند.

بر طبق مطالعات و پرس وجوهای Hutton در انگلستان در سال ۲۰۰۳ نشان داده شد که صاحب منصبان دولتی و اعضاء هیات رئیسه BBC از ایمیل برای فاش ساختن اطلاعاتی که محرمانه بوده اند استفاده کرده اند. مقاله ای در مارس ۱۹۹۹ در PC Week به تحقیقی اشاره کرد که طی آن از میان ۸۰۰ پرسنل مورد مطالعه، ۲۱ تا ۳۱ درصد آنها به ارسال اطلاعات محرمانه ـ مانند اطلاعات مالی یا محصولات ـ به افراد خارج از شرکتشان اعتراف کرده اند.

خطر ایمیلهای دربردارنده محتویات بدخواهانه یا اهانت آور

ایمیلهای ارسالی توسط کارکنان که حاوی مطالب نژادپرستانه، امور جنسی یا سایر موضوعات ناخوشایند است، می تواند یک شرکت را از نقطه نظر قانونی آسیب پذیر نماید. در سپتامبر ۲۰۰۳ مشاوران شرکت مالی Holden Meehan مجبور به پرداخت ۱۰هزار پوند به یکی از کارکنان سابق بدلیل ناتوانی در محافظت وی در مقابل آزار ایمیلی! شدند. Chevron مجبور به پرداخت ۲/۲ میلیون دلار به چهار نفر از کارکنانش شد که به وضوح ایمیلهای آزاردهنده جنسی دریافت کرده بودند. تحت قانون انگلیس، کارفرمایان مسوول ایمیلهایی هستند که توسط کارکنانشان در مدت استخدامشان نوشته و ارسال می شود، خواه کارفرما راضی به آن ایمیل بوده باشد، خواه نباشد. مبلغی معادل ۴۵۰هزار دلار از شرکت بیمه Norwich Union طی یک توافق خارج از دادگاه بخاطر ارسال توضیحات مربوط به یک سری از مسابقات درخواست شد.

روشهای استفاده شده برای حمله به سیستم ایمیل

برای درک انواع تهدیدات ایمیلی که امروزه وجود دارد، نگاهی اجمالی به روشهای اصلی فعلی حملات ایمیلی می اندازیم:

ضمیمه هایی با محتوای آسیب رسان

Melissa و LoveLetter جزو اولین ویروسهایی بودند که مساله ضمیمه های (Attachments) ایمیل و اعتماد را نشان دادند. آنها از اعتمادی که بین دوستان و همکاران وجود داشت استفاده می کردند. تصور کنید یک ضمیمه از دوستی دریافت می کنید که از شما می خواهد آن را باز کنید. این همانی است که در Melissa، AnnaKournikova، SirCam و سایر ویروسهای ایمیلی مشابه اتفاق می افتاد. به محض اجرا شدن، چنین ویروسهایی معمولاً خودشان را به آدرسهای ایمیلی که از دفترچه آدرس شخص قربانی بدست میاورند و به ایمیلهایی که صفحات وب ذخیره می کنند، ارسال می کنند. ویروس نویسان تأکید زیادی روی اجرای ضمیمه ای که توسط قربانی دریافت می شود، دارند. بنابراین برای نام ضمیمه ها از عناوین متفاوت و جذاب مانند SexPic.cmd و me.pif استفاده می کنند.

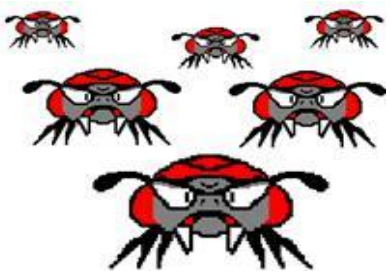
بسیاری از کاربران سعی می کنند که از سرایت ویروسهای ایمیل جلوگیری کنند و فقط روی فایلهایی با پسوندهای مشخص مانند JPG و MPG کلیک می کنند. به هرحال بعضی ویروسها، مانند کرم AnnaKournikova، از پسوند چندتایی بمنظور گول زدن کاربر برای اجرای آن استفاده می کند. ویروس AnnaKournikova از طریق ضمیمه

ایمیل و با عنوان 'AnnaKournikova.jpg.vbs' منتقل میشد که دریافت کننده را متقاعد می کرد که یک تصویر به فرمت JPG را از ستاره مشهور تنیس دریافت کرده است تا اینکه فایل ضمیمه یک اسکریپت ویژوال بیسیک حاوی کدهای آسیب رسان باشد.

بعلاوه، پسوند Class ID (CLSID) به هکرها این اجازه را می دهد که پسوند واقعی فایل را پنهان کنند و بدینوسیله این حقیقت که cleanfile.jpg یک برنامه HTML می باشد پنهان می ماند. این روش در حال حاضر نیز فیلترهای محتوای ایمیل را که از روشهای ساده بررسی فایل استفاده می کنند، فریب می دهد و به هکر امکان رسیدن به کاربر مقصد را به سادگی می دهد.

ایمیلهای راه اندازنده اکسپلویت های شناخته شده

اکسپلویت در حقیقت استفاده از شکافهای امنیتی موجود است. کرم Nimda اینترنت را با شگفتی مواجه کرد و با گول زدن بسیاری از ابزار امنیت ایمیل و نفوذ به سرورها و شبکه های بزرگ و سرایت کردن به کابران خانگی، اینترنت را فراگرفت. حقه بکارگرفته شده توسط Nimda این است که روی کامپیوترهایی که نسخه آسیب پذیری از IE یا Outlook Express را دارند، بطور خودکار اجرا می شود. Nimda از اولین ویروسهایی بود که از یکی از این شکافها بمنظور انتشار بهره برداری می کنند. برای مثال، انواعی از ویروس Bagle که در مارس ۲۰۰۴ ظهور کردند، از یکی از شکافهای اولیه Outlook برای انتشار بدون دخالت کاربر استفاده می کردند.



ایمیلهای با فرمت HTML دربردارنده اسکریپت

امروزه، تمام استفاده کنندگان ایمیل می توانند ایمیلهای HTML را ارسال و دریافت کنند. ایمیل با فرمت HTML می تواند اسکریپتها و محتویات فعالی را دربرگیرد که می توانند به برنامه یا کدها اجازه اجرا روی سیستم دریافت کننده را دهند. Outlook و محصولات دیگر از اجزا IE برای نمایش ایملهای HTML استفاده می کنند، به این معنی که اینها شکافهای امنیتی موجود در IE را به ارث می برند!

ویروسهای بر پایه اسکریپتهای HTML خطر مضاعف توانایی اجرای خودکار را، وقتی که ایمیل آسیب رسان باز می شود، دارند. آنها به ضمیمه ها متوسل نمی شوند؛ بنابراین فیلترهای ضمیمه که در نرم افزارهای ضدویروس وجود دارند در نبرد با ویروسهای اسکریپت HTML بلااستفاده هستند. برای مثال ویروس BadTrans.B از HTML برای اجرای خودکار در هنگام بازشدن استفاده می کند و از یک اکسپلویت ایمیل با فرمت HTML برای انتشار استفاده می کند. در قسمت بعدی به روشهای مقابله خواهیم پرداخت.

محافظت در مقابل خطرات ایمیل (۲)

آسانی تولید یک ویروس در سالهای اخیر

با داشتن اطلاعات مختصری مثلا در مورد ویژوال بیسیک، می توان با بهره گیری از شکافهای امنیتی، باعث آشفتگی در شبکه ها و سیستم های استفاده کنندگان ایمیل شد. مطالعه بعضی سایتها، شما را با بعضی از شکافهای موجود در Outlook و نحوه بهره گیری از آنها آشنا خواهد کرد. حتی بعضی از کدها نیز در دسترس شما خواهد بود و با تغییرات اندکی می توانید ویروسی تولید کنید که کدهای مورد نظر شما را اجرا کند.

برای مثال می توانید ویروسی تولید کنید که شخص قربانی بمحض باز کردن ایمیل حاوی آن در Outlook، کدهای مورد نظر شما اجرا شود. به این ترتیب تمام فایلهای HTML آلوده می شود و این ویروس به تمام آدرسهای موجود در دفترچه آدرس سیستم آلوده شده فرستاده می شود. در اصل، ویژگی کلیدی این ویروس اجرا شدن آن بمحض باز شدن ایمیل حاوی HTML آسیب رسان است.

آیا نرم افزار ضدویروس یا فایروال برای مقابله کافیست؟

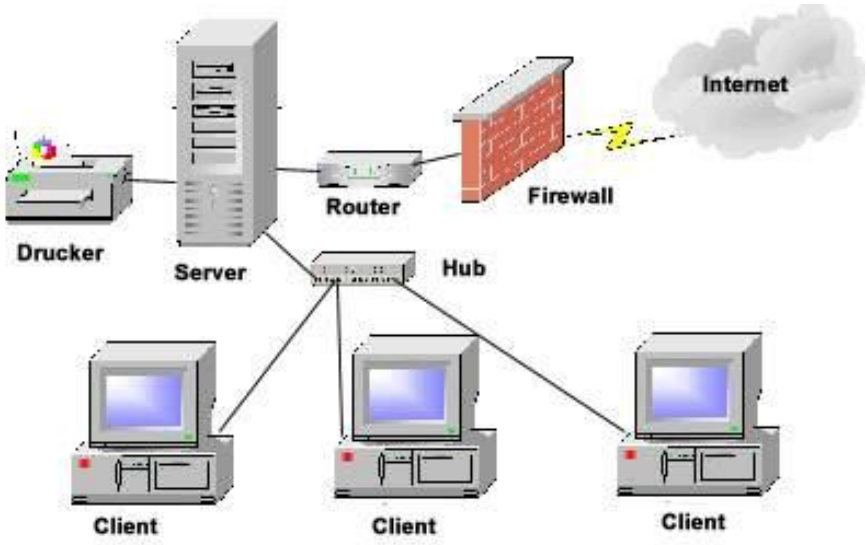
بعضی سازمانها با نصب کردن یک فایروال، خیال خود را از بابت امنیت آسوده می کنند. البته این یک گام ضروری برای محافظت از شبکه داخلیشان است اما کافی

نیست. فایروالها می توانند شبکه شما را از دسترس کاربران غیرمجاز مصون بدارند، اما محتوای ایمیلهایی را که توسط کاربران مجاز از طریق شبکه ارسال و دریافت می شود، بررسی نمی کنند. به این معنی که ویروسهای ایمیلی! می توانند از این سطح امنیتی عبور کنند.

در ضمن، نرم افزارهای ویروس یاب نیز نمی توانند سیستم ها را علیه تمام حمله ها و ویروسهای ایمیلی محافظت کنند.

تولیدکنندگان نرم افزارهای ضدویروس نمی توانند همواره برعلیه ویروسهای مهلکی که از طریق ایمیل در عرض چند ساعت در کل دنیا پراکنده می شوند(مانند کرمهای MyDoom ، NetSky.B و Beagle) مراقبت کامل کنند. بنابراین تکیه تنها بر موتور جستجوی ویروس نیز باعث مراقبت کامل نمی گردد.

برای مثال، یک مطالعه در سال ۲۰۰۴ توسط دولت بریتانیا نشان می دهد که اگرچه ٪۹۹ از شرکتهای بزرگ انگلیسی از ضدویروس استفاده می کنند، اما ٪۶۸ از آنها در طی سال ۲۰۰۳ به ویروسهای مختلف آلوده شده اند. یک تحقیق که در سال ۲۰۰۳ در آزمایشگاههای تحقیقاتی هیولت ـ پکارد در بریستول انجام شد، نشان داد که کرمها از نسخه های به روز ضدویروس ها بمراتب سریعتر گسترش پیدا می کنند.



راه حل: یک رویکرد پیشگیرانه

بنابراین چگونه می توان علیه این خطرات ایمیلی محافظت شد؟ در حقیقت به یک رویکرد پیشگیرانه نیاز است تا محتوای تمام ایمیلهایی وارد شونده و خارج شونده قبل از رسیدن به کاربران، در سطح سِرور بررسی شود. به این ترتیب، تمام محتوای مضر از ایمیل آلوده حذف می گردد و سپس به کاربر فرستاده می شود. سازمانها و شرکتها با نصب یک فیلتر جامع برای بررسی محتوای ایمیلها و یک دروازه (gateway) ضدویروس برروی سرویس دهنده ایمیل، می توانند در مقابله آسیب رسانیهای بالقوه و از بین رفتن زمان مفید کار توسط ویروسهای فعلی و آینده، خود را محافظت کنند.

در مقاله پیشین یعنی محافظت در مقابل خطرات ایمیل(۱) به نکاتی که توسط کاربران ایمیل باید رعایت شود، پرداخته شد و در اینجا به قابلیتهای یک فیلتر خوب برای نصب

در سرویس دهنده ایمیل برای جلوگیری از آلوده شدن توسط ویروسهای ایمیلی اشاره می شود.

- بررسی محتوای ایمیل
- کشف بهره برداریها از شکافهای امنیتی(اکسپلویتها)
- تحلیل خطرات
- راه حلهای ضدویروسی

موارد فوق برای ازبین بردن انواع خطراتی است که توسط ایمیلها منتقل می شود، قبل از اینکه بتوانند کاربران ایمیل را تحت تاثیر قرار دهند.

ویژگیهای زیر را نیز می توان به فیلتر مذکور اضافه کرد:

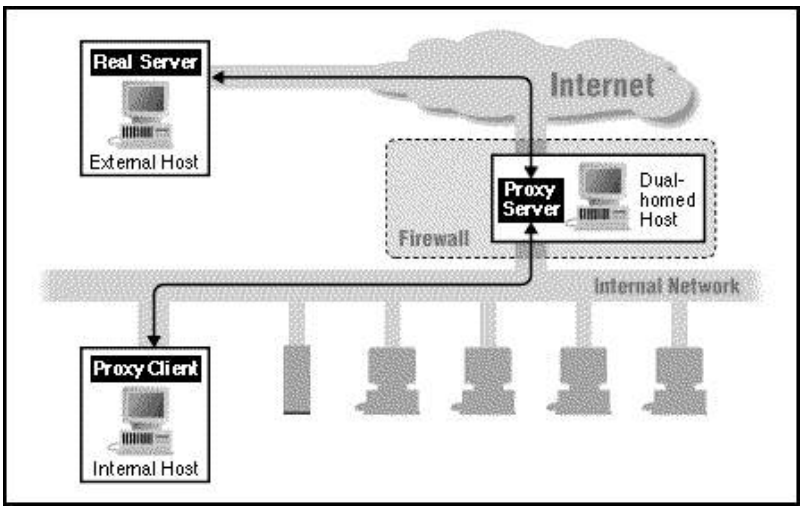
- دربرداشتن چندین موتور ویروس برای بالا بردن نرخ کشف ویروس و پاسخ سریعتر به ویروسهای جدید.
- بررسی پیوستـهای ایمیلها برای مصونـیت در مقابل ضمـیمه های خـــــطرناک
- یک سپر در مقابل اکسپلویتها برای محافظت در مقابل ویروسهای فعلی و آتی که برپایه اکسپلویتها ایجاد گشته اند.
- یک موتور بررسی خطرات HTML برای از کار انداختـــن اسکریپتهای HTML
- یک پویشگر برای ترواها و فایلهای اجرایی برای کشف فایـــــلهای اجرایی آسیب رسان و مهم ترین و آخرین نکته که تا کنون چندین بار به آن اشاره شده است این است که ایمیلهای ناشناخته را باز نکنید.

بخش : هشتم

Security Tools

پراکسی سرور

در یک تشکیلات که از اینترنت استفاده می‌کند، یک پراکسی سرور ترکیبی از سخت‌افزار و نرم‌افزار است که بعنوان یک واسطه بین کاربر داخلی و اینترنت عمل می‌کند به طوریکه امنیت، نظارت مدیریتی و سرویس‌های caching تامین می‌شود. یک سرور پراکسی دارای پروتکل مشخصی است، بنابراین برای هرنوع پروتکلی (HTTP، FTP، Gogher و غیره) باید تنظیم شود. پراکسی سرور بعنوان بخشی از یک سرور gateway (نقطه‌ای در یک شبکه که ورودی به شبکه‌ای دیگر است) رفتار می‌کند و می‌تواند برای انجام یک یا چند فانکشن که در بخش بعد به آن اشاره می‌شود، تنظیم شود.



عملکردهایی که پراکسی سرور می‌تواند داشته باشد

با تعریفی که از یک پراکسی ارائه شد، می‌توان از پراکسی برای بهبود عملکرد یک شبکه استفاده‌هایی کرد که در اینجا به چند مورد آن به اختصار اشاره می‌کنیم:

- **Firewall (دیواره آتش)**

برای سازمانی که فایروال دارد، پراکسی سرور تقاضاهای کاربران را به فایروال می‌دهد که با آنها اجازه ورود یا خروج به شبکه داخلی را می‌دهد.

- **Caching (ذخیره سازی)**

سرور پراکسی که عمل caching را انجام می‌دهد، منابعی مانند صفحات وب و فایل‌ها را ذخیره می‌کند. هنگامی که یک منبع مورد دسترسی قرار گرفت، در سرور دخیره می‌شود و تقاضاهای بعدی برای همین منبع مشخص با محتویات cache پاسخ داده می‌شود. این عمل، دسترسی به آن منبع را برای کاربرانی که از طریق پراکسی به اینترنت متصل هستند، سرعت می‌بخشد و از طرفی از ترافیک اینترنت می‌کاهد و اجازه استفاده بهتر از پهنای باند به کاربران داده می‌شود.

- **Filtering (فیلتر کردن)**

سرور پراکسی می‌تواند ترافیک وارد شونده و خارج شونده از شبکه را بررسی کند و به آنچه که با معیارهای امنیتی یا سیاست سازمان مغایرت دارد، اجازه عبور ندهد.

- **Authentication (تصدیق هویت)**

بسیاری منابع الکترونیکی سازمانی توسط ورود با کلمه رمز یا قرار داشتن در دامنه مشخصی از IP محدود شده‌اند. کاربران دور معمولاً از یک سرویس‌دهنده اینترنت ثالث استفاده می‌کنند که در این صورت این کاربر یا IP کامپیوتر آن برای سازمان معتبر تشخیص داده نمی‌شود. برای کاربرانی که بصورت فیزیکی به شبکه داخلی سازمان متصل نشده‌اند، پراکسی طوری عمل می‌کند که به کاربران دور اجازه ورود موقت داده شود یا به آنها بطور موقت یک IP سازمان تخصیص داده شود که بتوانند به منابع محدود شده دسترسی پیدا کنند.

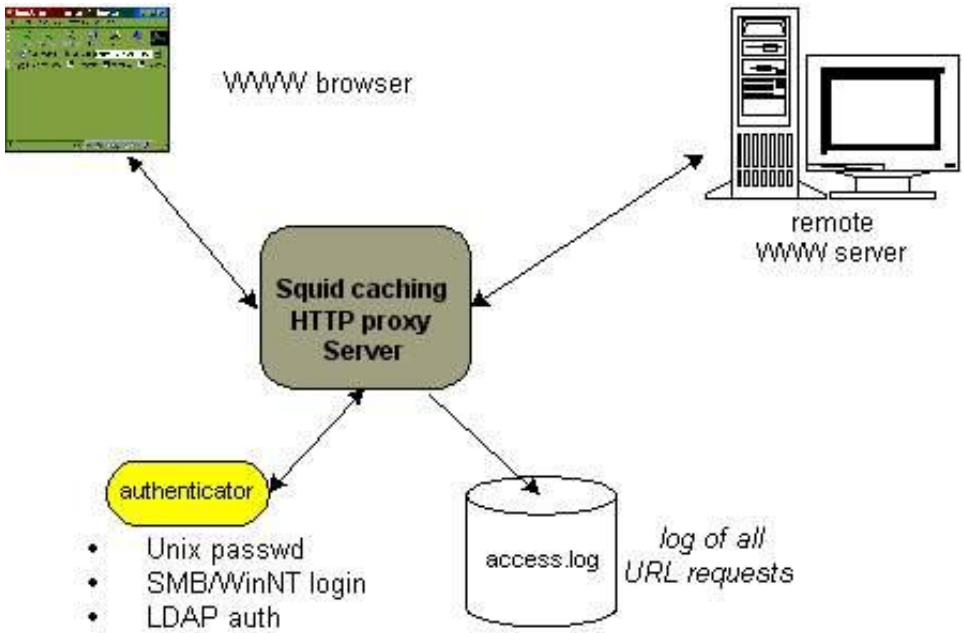
- **Anonymization (تغییر هویت)**

برای محافظت شبکه داخلی یک سازمان از کاربران موجود در اینترنت، سرور پراکسی می‌تواند هویت سیستم‌های متقاضی داخلی را تغییر دهد. اگر منبع (مثلاً صفحه وب یا فایل) تقاضا شده توسط کاربر داخلی سازمان، در cache موجود نباشد، سرور پراکسی برای آن کاربر، بعنوان کلاینت عمل می‌کند و از یکی از آدرس‌های IP خودش برای تقاضای آن منبع از سرور موجود در اینترنت استفاده می‌کند. این آدرس IP «موقت»، آدرسی نیست که واقعاً در شبکه داخلی سازمان استفاده گردد و در نتیجه از بعضی از حمله‌های نفوذگران جلوگیری می‌شود. هنگامی که صفحه تقاضا شده، از طرف سرور روی اینترنت به پراکسی سرور می‌رسد، پراکسی سرور آن را به تقاضای اولیه مرتبط

می‌کند و برای کاربر می‌فرستد. این پروسه تغییر دادن IP باعث می‌شود که تقاضا دهنده اولیه قابل ردیابی نباشد و همچنین معماری شبکه سازمان از دید بیرونی مخفی بماند.

- **Logging (ثبت کردن)**

پراکسی سرور می‌تواند تقاضاها را بهمراه اطلاعات لازم در جایی ثبت کند تا بعداً امکان پیگیری اعمال کاربران داخل سازمان فراهم شود.



پیکربندی مرورگر

- **تعامل کاربر:** کاربر باید از ابتدا مرورگر خود را پیکربندی کند که بدین ترتیب نیاز است که اطلاعات را از پشتیبانی فنی سازمان بدست آورد.

- **پیکربندی دستی:** در این پیکربندی کاربر باید سروری را که نرم‌افزار پراکسی را اجرا می‌کند، مشخص کند. کاربر باید استثنائات هر دامنه‌ای را که می‌تواند بطور مستقیم به آن

وصل شود، مشخص کند و به این ترتیب در اتصال به این دامنه‌های مشخص‌شده، پراکسی در مسیر قرار نمی‌گیرد.

- **پیکربندی خودکار**: یک فایل تنظیم پیکربندی توسط سازمان که منطق استفاده از پراکسی توسط مرورگر در آن قرار دارد. URL فایل باید در پیکربندی مرورگر وارد گردد. اینکه یک تقاضا از طریق پراکسی مسیریابی شود یا خیر، بستگی به شروط موجود در آن فایل دارد.

کاربرد پراکسی در امنیت شبکه (۱)

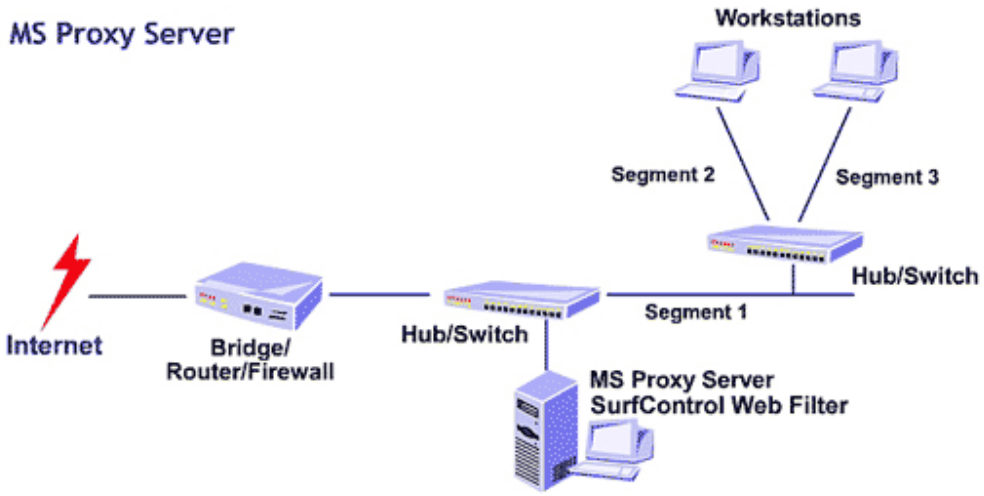
بعد از آشنایی با پراکسی «پراکسی سرور» در این قسمت به این مطلب می پردازیم که از دیدگاه امنیتی پراکسی چیست و چه چیزی نیست، از چه نوع حملاتی جلوگیری می کند و به مشخصات بعضی انواع پراکسی پرداخته می شود. البته قبل از پرداختن به پراکسی بعنوان ابزار امنیتی، بیشتر با فیلترها آشنا خواهیم شد.

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 میگیرد 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 ردشده دور ریخته می شوند.

پراکسی چه چیزی هست؟

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 می کند عموماً شامل آدرس و پورت منبع و مقصد می شود. این فیلتر بسته به پورت و منبع و مقصد دیتا و بر اساس قوانین ایجاد شده توسط مدیر شبکه بسته را می پذیرد یا نمی پذیرد. مزیت اصلی این نوع فیلتر سریع بودن آن است چرا که header، تمام آن چیزی است که سنجیده می شود. و عیب اصلی ان این است که هرگز آنچه را که در بسته وجود دارد نمی بیند و به محتوای آسیب رسان اجازه عبور از فایروال را می دهد. بعلاوه، این نوع فیلتر با هر بسته بعنوان یک واحد مستقل رفتار می کند و وضعیت (State) ارتباط را دنبال نمی کند.

پراکسی با Stateful packet filter تفاوت دارد

این فیلتر اعمال فیلتر نوع قبل را انجام می دهد، بعلاوه اینکه بررسی می کند کدام کامپیوتر در حال ارسال چه دیتایی است و چه نوع دیتایی باید بیاید. این اطلاعات بعنوان وضعیت (State) شناخته می شود.

پروتکل ارتباطی TCP/IP به ترتیبی از ارتباط برای برقراری یک مکالمه بین کامپیوترها نیاز دارد. در آغاز یک ارتباط TCP/IP عادی، کامپیوتر A سعی می کند با ارسال یک بسته SYN (synchronize) به کامپیوتر B ارتباط را برقرار کند. کامپیوتر B در جواب یک بسته SYN/ACK (Acknowledgement) برمی گرداند، و کامپیوتر A یک ACK به کامپیوتر B می فرستد و به این ترتیب ارتباط برقرار می شود. TCP اجازه وضعیتهای دیگر، مثلاً FIN (finish) برای نشان دادن آخرین بسته در یک ارتباط را نیز می دهد.

هکرها در مرحله آماده سازی برای حمله، به جمع آوری اطلاعات در مورد سیستم شما می پردازند. یک روش معمول ارسال یک بسته در یک وضعیت غلط به منظوری خاص است. برای مثال، یک بسته با عنوان پاسخ (Reply) به سیستمی که تقاضایی نکرده، می فرستند. معمولاً، کامپیوتر دریافت کننده بیاید پیامی بفرستد و بگوید "I don't understand". به این ترتیب، به هکر نشان می دهد که وجود دارد، و آمادگی برقراری ارتباط دارد. بعلاوه، قالب پاسخ می تواند سیستم عامل مورد استفاده را نیز مشخص کند، و برای یک هکر گامی به جلو باشد. یک فیلتر Stateful packet منطق یک ارتباط

TCP/IP را می فهمد و می تواند یک "Reply" را که پاسخ به یک تقاضا نیست، مسدود کند ـــ آنچه که یک فیلتر packet ردگیری نمی کند و نمی تواند انجام دهد. فیلترهای Stateful packet می توانند در همان لحظه قواعدی را مبنی بر اینکه بسته مورد انتظار در یک ارتباط عادی چگونه باید بنظر رسد، برای پذیرش یا رد بسته بعدی تعیین کنند. فایده این کار امنیت محکم تر است. این امنیت محکم تر، بهرحال، تا حدی باعث کاستن از کارایی می شود. نگاهداری لیست قواعد ارتباط بصورت پویا برای هر ارتباط و فیلترکردن دیتای بیشتر، حجم پردازشی بیشتری به این نوع فیلتر اضافه می کند.

پراکسی ها یا Application Gateways

Application Gateways که عموماً پراکسی نامیده می شود، پیشرفته ترین روش استفاده شده برای کنترل ترافیک عبوری از فایروال ها هستند. پراکسی بین کلاینت و سرور قرار می گیرد و تمام جوانب گفتگوی بین آنها را برای تایید تبعیت از قوانین برقرار شده، می سنجد. پراکسی بار واقعی تمام بسته های عبوری بین سرور و کلاینت را می سنجد، و میتواند چیزهایی را که سیاستهای امنیتی را نقض می کنند، تغییر دهد یا محروم کند. توجه کنید که فیلترهای بسته ها فقط headerها را می سنجند، در حالیکه پراکسی ها محتوای بسته را با مسدود کردن کدهای آسیب رسان همچون فایلهای اجرایی، اپلت های جاوا، ActiveX و ... غربال می کنند.

پراکسی ها همچنین محتوا را برای اطمینان از اینکه با استانداردهای پروتکل مطابقت دارند، می سنجند. برای مثال، بعضی اَشکال حمله کامپیوتری شامل ارسال متاکاراکترها برای فریفتن سیستم قربانی است؛ حمله های دیگر شامل تحت تاثیر قراردادن سیستم با دیتای بسیار زیاد است. پراکسی ها می توانند کاراکترهای غیرقانونی یا رشته های خیلی طولانی را مشخص و مسدود کنند. بعلاوه، پراکسی ها تمام اعمال فیلترهای ذکرشده را انجام می دهند. بدلیل تمام این مزیتها، پراکسی ها بعنوان یکی از امن ترین روشهای عبور ترافیک شناخته می شوند. آنها در پردازش ترافیک از فایروالها کندتر هستند زیرا کل بسته ها را پیمایش می کنند. بهرحال «کندتر» بودن یک عبارت نسبی است.

آیا واقعاً کند است؟ کارایی پراکسی بمراتب سریعتر از کارایی اتصال اینترنت کاربران خانگی و سازمانهاست. معمولاً خود اتصال اینترنت گلوگاه سرعت هر شبکه ای است. پراکسی ها باعث کندی سرعت ترافیک در تست های آزمایشگاهی می شوند اما باعث کندی سرعت دریافت کاربران نمی شوند.

در شماره بعد بیشتر به پراکسی خواهیم پرداخت.

کاربرد پراکسی در امنیت شبکه (۲)

در مقایسه فایروال‌ها، ما مفهومی از پراکسی ارائه می‌دهیم و پراکسی را از فیلترکننده بسته‌ها متمایز می‌کنیم. با پیش‌زمینه‌ای که از پراکسی در شماره قبل بیان کردیم، می‌توانیم در اینجا مزایای پراکسی‌ها بعنوان ابزاری برای امنیت را لیست کنیم:

- با مسدود کردن روش‌های معمول مورد استفاده در حمله‌ها، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با پنهان کردن جزئیات سرورهای شبکه شما از اینترنت عمومی، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با جلوگیری از ورود محتویات ناخواسته و نامناسب به شبکه شما، استفاده از پهنای باند شبکه را بهبود می‌بخشند.
- با ممانعت از یک هکر برای استفاده از شبکه شما بعنوان نقطه شروعی برای حمله دیگر، از میزان این نوع مشارکت می‌کاهند.
- با فراهم‌آوردن ابزار و پیش‌فرض‌هایی برای مدیر شبکه شما که می‌توانند بطور گسترده‌ای استفاده شوند، می‌توانند مدیریت شبکه شما را آسان سازند.

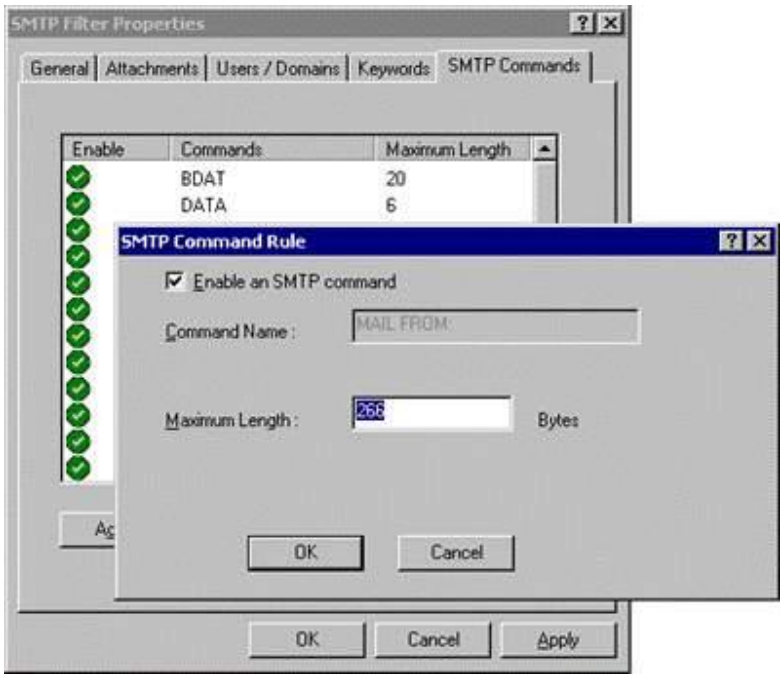
بطور مختصر می‌توان این مزایا را اینگونه بیان کرد؛ پراکسی‌ها به شما کمک می‌کنند که شبکه‌تان را با امنیت بیشتر، موثرتر و اقتصادی‌تر مورد استفاده قرار دهید. بهرحال در ارزیابی یک فایروال، این مزایا به فواید اساسی تبدیل می‌شوند که توجه جدی را می‌طلبند.

برخی انواع پراکسی

تا کنون به پراکسی بصورت یک کلاس عمومی تکنولوژی پرداختیم. در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. در بخش بعد به چند نوع آن اشاره می‌کنیم و شرح می‌دهیم که هرکدام در مقابل چه نوع حمله‌ای مقاومت می‌کند.

البته پراکسی‌ها تنظیمات و ویژگی‌های زیادی دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد. در ادامه به پراکسی‌های زیر اشاره خواهیم کرد:

- SMTP Proxy
- HTTP Proxy
- FTP Proxy
- DNS Proxy



SMTP Proxy

پراکسی SMTP (Simple Mail Transport Protocol) محتویات ایمیل‌های وارد شونده و خارج‌شونده را برای محافظت از شبکه شما در مقابل خطر بررسی می‌کند. بعضی از تواناییهای آن اینها هستند:

- **مشخص کردن بیشترین تعداد دریافت‌کنندگان پیام**: این اولین سطح دفاع علیه اسپم (هرزنامه) است که اغلب به صدها یا حتی هزاران دریافت‌کننده ارسال می‌شود.
- **مشخص کردن بزرگترین اندازه پیام**: این به سرور ایمیل کمک می‌کند تا از بار اضافی و حملات بمباران توسط ایمیل جلوگیری کند و با این ترتیب می‌توانید به درستی از پهنای باند و منابع سرور استفاده کنید.

- **اجازه دادن به کاراکترهای مشخص در آدرسهای ایمیل آنطور که در استانداردهای اینترنت پذیرفته شده است:** چنانچه قبلاً اشاره شد، بعضی حمله‌ها بستگی به ارسال کاراکترهای غیرقانونی در آدرسها دارد. پراکسی می‌تواند طوری تنظیم شود که بجز به کاراکترهای مناسب به بقیه اجازه عبور ندهد.

- **فیلترکردن محتوا برای جلوگیری از انواعی محتویات اجرایی:** معمول‌ترین روش ارسال ویروس، کرم و اسب تروا فرستادن آنها در پیوست‌های به ظاهر بی‌ضرر ایمیل است. پراکسی SMTP می‌تواند این حمله‌ها را در یک ایمیل از طریق نام و نوع، مشخص و جلوگیری کند، تا آنها هرگز به شبکه شما وارد نشوند.

- **فیلترکردن الگوهای آدرس برای ایمیل‌های مقبول\مردود:** هر ایمیل شامل آدرسی است که نشان‌دهنده منبع آن است. اگر یک آدرس مشخص شبکه شما را با تعداد بیشماری از ایمیل مورد حمله قرار دهد، پراکسی می‌تواند هر چیزی از آن آدرس اینترنتی را محدود کند. در بسیاری موارد، پراکسی می‌تواند تشخیص دهد چه موقع یک هکر آدرس خود را جعل کرده است. از آنجا که پنهان کردن آدرس بازگشت تنها دلایل خصمانه دارد، پراکسی می‌تواند طوری تنظیم شود که بطور خودکار ایمیل جعلی را مسدود کند.

- **فیلترکردن Headerهای ایمیل:** Headerها شامل دیتای انتقال مانند اینکه ایمیل از طرف کیست، برای کیست و غیره هستند. هکرها راه‌های زیادی برای دستکاری اطلاعات Header برای حمله به سرورهای ایمیل یافته‌اند. پراکسی

مطمئن می‌شود که Headerها با پروتکل‌های اینترنتی صحیح تناسب دارند و ایمیل‌های دربردارنده headerهای تغییرشکل‌داده را مردود می‌کنند. پراکسی با اعمال سختگیرانه استانداردهای ایمیل نرمال، می‌تواند برخی حمله‌های آتی را نیز مسدود کند.

- **تغییردادن یا پنهان‌کردن نامهای دامنه و IDهای پیام‌ها:** ایمیل‌هایی که شما می‌فرستید نیز مانند آنهایی که دریافت می‌کنید، دربردارنده دیتای header هستند. این دیتا بیش از آنچه شما می‌خواهید دیگران درباره امور داخلی شبکه شما بدانند، اطلاعات دربردارند. پراکسی SMTP می‌تواند بعضی از این اطلاعات را پنهان کند یا تغییر دهد تا شبکه شما اطلاعات کمی در اختیار هکرهایی قرار دهد که برای وارد شدن به شبکه شما دنبال سرنخ می‌گردند.

در شماره بعد بررسی انواع دیگر پراکسی را ادامه خواهیم داد.

کاربرد پراکسی در امنیت شبکه (۳)

در شماره های قبل به پراکسی سرور، مقایسه پراکسی و فایروال و پراکسی SMTP پرداختیم. به بررسی انواع دیگر پراکسی می پردازیم:

HTTP Proxy

این پراکسی بر ترافیک داخل شونده و خارج شونده از شبکه شما که توسط کاربرانتان برای دسترسی به World Wide Web ایجاد شده، نظارت می کند. این پراکسی برای مراقبت از کلاینت های وب شما و سایر برنامه ها که به دسترسی به وب از طریق اینترنت متکی هستند و نیز حملات برپایه HTML، محتوا را فیلتر می کند. بعضی از قابلیتهای آن اینها هستند:

- **برداشتن اطلاعات اتصال کلاینت:** این پراکسی می تواند آن قسمت از دیتای header را که نسخه سیستم عامل، نام و نسخه مرورگر، حتی آخرین صفحه وب دیده شده را فاش می کند، بردارد. در بعضی موارد، این اطلاعات حساس است، بنابراین چرا فاش شوند؟
- **تحمیل تابعیت کامل از استانداردهای مقررشده برای ترافیک وب:** در بسیاری از حمله ها، هکرها بسته های تغییرشکل داده شده را ارسال می کنند که باعث

دستکاری عناصر دیگر صفحه وب می شوند، یا بصورتی دیگر با استفاده از رویکردی که ایجادکنندگان مرورگر پیش بینی نمی کردند، وارد می شوند.

پراکسی HTTP این اطلاعات بی معنی را نمی پذیرد. ترافیک وب باید از استانداردهای وب رسمی پیروی کند، وگرنه پراکسی ارتباط را قطع می کند.

- **فیلترکردن محتوای از نوع MIME** : الگوهای MIME به مرورگر وب کمک می کنند تا بداند چگونه محتوا را تفسیر کند تا با یک تصویرگرافیکی بصورت یک گرافیک رفتار شود، یا **.wav** فایل بعنوان صوت پخش شود، متن نمایش داده شود و غیره. بسیاری حمله های وب بسته هایی هستند که در مورد الگوی MIME خود دروغ می گویند یا الگوی آن را مشخص نمی کنند. پراکسی HTTP این فعالیت مشکوک را تشخیص می دهد و چنین ترافیک دیتایی را متوقف می کند.
- **فیلترکردن کنترلهای Java و ActiveX**: برنامه نویسان از Java و ActiveX برای ایجاد برنامه های کوچک بهره می گیرند تا در درون یک مرورگر وب اجراء شوند (مثلاً اگر فردی یک صفحه وب مربوط به امور جنسی را مشاهده می کند، یک اسکریپت ActiveX روی آن صفحه می تواند بصورت خودکار آن صفحه را صفحه خانگی مرورگر آن فرد نماید). پراکسی می تواند این برنامه ها را مسدود کند و به این ترتیب جلوی بسیاری از حمله ها را بگیرد.
- **برداشتن کوکی ها:** پراکسی HTTP می تواند جلوی ورود تمام کوکی ها را بگیرد تا اطلاعات خصوصی شبکه شما را حفظ کند.