
Web Site: http://www.MixofTix.net
Document # 7856-292-EHR-01

# Material: Network & Security Overview


| موضوع | | صفحه |
|---|---|---|
| فهرست | ..... | 1 |
| مقدمه | ..... | 2 |
| امنیت شبکه‌های اطلاعاتی و ارتباطی | ..... | 3 |
| جرائم رایانه ای و اینترنتی | ..... | 5 |
| تعریف جرم رایانه‌ای | ..... | 6 |
| رایانه‌ای طبقه‌بندی جرایم | ..... | 7 |
| امنیتی شبکه راهکارهای | ..... | 11 |
| فایروالها | ..... | 14 |
| یک رویکرد امنیتی لایه بندی شده | ..... | 17 |
| امنیت پیرامون | ..... | 18 |
| امنیت شبکه | ..... | 23 |
| امنیت میزبان | ..... | 27 |
| امنیت برنامه کاربردی | ..... | 29 |
| امنیت دیتا | ..... | 31 |
| رویدادهای امنیتی و اقدامات لازم در برخورد با آنها | ..... | 32 |
| مثالی از واکنش به یک رویداد در یک سازمان بزرگ | ..... | 33 |
| کاربرد پراکسی در امنیت شبکه | ..... | 36 |
| پروتکل های انتقال فایل امن | ..... | 40 |
| تشخیص نفوذ | ..... | 44 |
| انواع حملات شبکه ای با توجه به حمله کننده | ..... | 46 |

# امنیت شبکه

موضوع امنیت شبکه این روزها به بحثی اساسی در میان سایت های اینترنتی و شبکه های ایرانی تبدیل شده است. نقش برخی از حملات اینترنتی اخیر و افزایش قابل ملاحظه کارکردهای سایت ها و شبکه های ایرانی در این رویکردی بی تاثیر نیست.

اینترنت یک شبکهٔ عظیم اطلاع‌رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک‌تک 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 شبکهٔ 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 فنآوری 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 شبکهٔ 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 برپاکنندگان 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 شبکهٔ اینترنت را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است .

## امنیت شبکه‌های اطلاعاتی و ارتباطی

### اهمیت امنیت شبکه

چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن دربافت 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، اطلاعاتی 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 .

به امینت شبکه باید به صورت یک بستر نگاه کنیم یعنی به صورت یک زیر ساخت ، برای این که امنیت یک شبکه را ایجاد کنیم باید در درجه اول به زیر ساخت آن توجه داشته باشیم دقیقا مثل نقشی که جاده ها در حمل و نقل دارند هر چه زیر ساخت یعنی جاده از نظر ایمنی امن تر باشد به طبع حمل و نقل و جابجای افراد نیز از نظر ایمنی بی خطر صورت می گیرد در مورد شبکه های کامپیوتری نیز دقیقا همین طور است اگر زیر ساخت امنیتی مناسب باشد عرضه و جابجای اطلاعات نیز به طبع راحت تر صـــــــــورت می گیرد شبکه را می توان با نگرش سخت افزاری یا نرم افزاری مطالعه کرد به هر حال بحث امنیت شبکه باید از هر دو قطب روی آن کار شود .

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 شبکهٔ 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 شعبهٔ اصلی آن در اسرائیل می‌باشد. مسأله امنیت شبکهٔ 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 1969 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 بیفتد، 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 1971 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 1988، 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 تصاعدی تکثیر شود. آن زمان 88000 رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه در آمریکا از کار بیفتد .

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 WORM در سال 1989، Sniff packet در سال 1994 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 .

## جرائم 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 پیشرفتها 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 جنبهٔ 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 2001 و امضای آن توسط 30 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 اظهارنظر 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. انگیزهٔ 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 عهدهٔ 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 6 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، افترا، 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 زمرهٔ جرم رایانه‌ای قرار نمی‌گیرند .

در تعریف جامع 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 نو ع 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 .

**طبقه‌بندی جرایم رایانه‌ای**

طبقه‌بندی‌های مختلفی از جرایم رایانه‌ای توسط مراجع مختلف انجام گرفته است.

طبقه‌بندی OECDB

در سال 1983 «او.ای.سی.دی.بی» مطالعه امکان پذیری اعمال بین‌المللی و هماهنگی قوانین کیفری را به منظور حل مسئله جرم یا سوءاستفاده‌های رایانه‌ای متعهد شد. این سازمان در سال 1986 گزارشی تحت عنوان جرم رایانه‌ای، تحلیل سیاستهای قانونی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. بدین گونه اولین تقسیم‌بندی از جرایم رایانه‌ای در سال 1983 ارائه شد و طی آن پنج دسته اعمال را مجرمانه تلقی کرد و پیشنهاد کرد در قوانین ماهوی ذکر شود. این پنج دسته عبارتند از :

الف: ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که بطور ارادی با قصد انتقال غیرقانونی وجوه یا هر چیز باارزش دیگر صورت گرفته باشد .

ب: ورود، تغییر، پاک کردن، و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که بصورت عمدی و به قصد ارتکاب جعل صورت گرفته باشند. یا هرگونه مداخله دیگر در سیستمهای رایانه‌ای که بصورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه‌ای و یا ارتباطات صورت گرفته باشد .

ج: ورود، تغییر، پاک کردن و متوقف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای .

د: تجاوز به حقوق انحصاری مالک یک برنامهٔ رایانه‌ای حفاظت شده با قصد بهره‌برداری تجاری از برنامه‌ها و ارائه آن به بازار .

ه- دستیابی یا شنود در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور یا تخطی از تدابیر امنیتی و چه با هدف غیر شرافتمندانه و یا موضوع صورت گرفته باشد .

طبقه‌بندی شورای اروپا :

کمیتهٔ منتخب جرایم رایانه‌ای شورای اروپا، پس از بررسی نظرات «او.ای.سی.دی.بی» و نیز بررسیهای حقوقی- فنی دو لیست تحت عناوین لیست حداقل و لیست اختیاری را به کمیته وزراء پیشنهاد داد و آنان نیز تصویب کردند. این لیستها بدین شرح هستند :

الف: کلاه‌برداری رایانه‌ای

ب :جعل رایانه‌ای

ج: خسارت زدن به داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای

د: دستیابی غیرمجاز

ه: ایجاد مجدد و غیرمجاز یک برنامهٔ رایانه‌ای حمایت شده

و: ایجاد مجدد غیرمجاز یک توپوگرافی .

ز: لیست اختیاری شامل:

- تغییر داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای
- جاسوسی رایانه‌ای
- استفاده غیرمجاز از رایانه
- استفاده غیرمجاز از برنامهٔ رایانه‌ای حمایت شده .

طبقه‌بندی اینترپول :

سالهاست که اینترپول در مبارزه با جرایم مرتبط با فناوری اطلاعات فعال می‌باشد. این سازمان با بهره‌گیری از کارشناسان و متخصصین کشورهای عضو اقدام به تشکیل گروههای کاری در این زمینه کرده است. رؤسای واحدهای مبارزه با جرایم رایانه‌ای کشورهای باتجربه عضو سازمان در این گروه کاری گردهم آمده‌اند .

گروههای کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا مشغول به کارند. و زیر نظر کمیتهٔ راهبردی جرایم فناوری اطلاعات، مستقر در دبیرخانهٔ کل اینترپول فعالیت می‌نمایند .

گروه کاری اروپایی اینترپول با حضور کارشناسان هلند، اسپانیا، بلژیک، فنلاند، فرانسه، آلمان، ایتالیا، سوئد و انگلیس در سال 1990 تشکیل شد. این گروهها هر سال سه بار تشکیل جلسه می‌دهند و در ژانویه سال 2001 سی‌امین گردهمایی آن در دبیرخانه کل تشکیل گردید .

تهیه کتابچهٔ راهنمای پی‌جویی جرایم رایانه‌ای، کتاب و سی‌دی راهنمای جرایم رایانه‌ای، تشکیل دوره‌های آموزشی برای نیروهای پلیس در

طول 5 سال گذشته، تشکیل سیستم اعلام خطر که مرکب از سیستمهای پاسخگوی شبانه‌روزی، نقاط تماس دائمی شبانه‌روزی، تبادل پیام بین‌المللی در قالب فرمهای استاندارد در زمینهٔ جرایم رایانه‌ای واقعه می‌باشد و انجام چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرایم رایانه‌ای از جمله اقدامات گروه کاری مذکور می‌باشد. گروه کار آمریکایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان و متخصصین کشورهای کانادا، ایالات متحده، آرژانتین، شیلی، کلمبیا، جامائیکا و باهاماست .

گروه کاری آفریقایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان آفریقای جنوبی، زیمبابوه، نامبیا، تانزانیا، اوگاندا، بوتسوانا، سوازیلند، زنگبار، لسوتو و رواندا در ژوئن سال 1998 تشکیل گردید. آنها کارشان را با برگزاری یک دوره آموزشی آغاز نمودند و دومین دوره آموزشی آنها با مساعدت مالی سفارتخانه‌های انگلیس برگزار شد .

گروه کاری جنوب اقیانوس آرام، و آسیا در نوامبر سال 2000 در هند تشکیل شد و کارشناسانی از کشورهای استرالیا، چین، هنگ کنگ، هند، ژاپن، نپال، و سریلانکا عضو آن هستند. این گروه کاری با الگو قرار دادن کمیته راهبردی جرایم مربوط به فناوری اطلاعات به منظور ایجاد و هماهنگی میان اقدامات گروههای کاری منطقه‌ای در محل دبیرخانه کل اینترپول تشکیل گردیده است .

سازمان پلیس جنایی بین‌المللی جرایم رایانه‌ای را به شرح زیر طبقه‌بندی کرده است :

- دستیابی غیرمجاز
  - نفوذغیرمجاز
  - شنود غیرمجاز
  - سرقت زمان رایانه
  - تغییر داده‌های رایانه‌ای
  - بمب منطقی
  - اسب تروا
  - ویروس رایانه‌ای
  - کرم رایانه‌ای

- کلاه‌برداری رایانه‌ای
  - صندوقهای پرداخت
  - جعل رایانه‌ای
  - ماشینهای بازی
  - دستکاریها در مرحله ورودی/ خروجی
  - ابزار پرداخت (نقطه فروش)
  - سوءاستفاده تلفنی
- تکثیر غیرمجاز
  - بازیهای رایانه‌ای
  - نرم‌افزارهای دیگر
  - توپوگرافی نیمه هادی
- سابوتاژ رایانه‌ای
  - سخت‌افزار
  - نرم‌افزار
- سایر جرائم رایانه‌ای
  - سیستمهای تابلوی اعلانات الکترونیک
  - سرقت اسرار تجاری
  - سایر موضوعات قابل تعقیب

**طبقه‌بندی در کنوانسیون جرایم سایبرنتیک**

این کنوانسیون در اواخر سال 2001 به امضای 30 کشور پیشرفته رسیده است و دارای وظایف زیر می‌باشد :هماهنگ کردن ارکان تشکیل دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسائل مربوطه در بخش جرایم سایبراسپیس .

الف: فراهم آوردن اختیارات لازم آیین دادرسی کیفری داخلی برای پی‌جویی و تعقیب چنین جرائمی علاوه بر جرایم دیگر که با استفاده از سیستمهای رایانه‌ای ارتکاب می‌یابند .

ب: تدوین سیستم سریع و مؤثر همکاری بین‌المللی

ج: کنوانسیون بین‌المللی جرایم رایانه‌ای بوداپست (2001) جرم را موارد زیر تعریف نموده است :

- نفوذ غیرمجاز به سیستمهای رایانه‌ای
- شنود غیرمجاز اطلاعات و ارتباطات رایانه‌ای
- اخلال در داده‌های رایانه‌ای
- اخلال در سیستمهای رایانه‌ای
- جعل رایانه‌ای
- کلاه‌برداری رایانه‌ای
- سوءاستفاده از ابزارهای رایانه‌ای
- هرزه‌نگاری کودکان
- تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای و نقض حقوق ادبی و هنری

**راهکارهای امنیتی شبکه**

امنیت شبکه در وهله اول باید در سطح شبکه های داخلی کنترل بشود یعنی هر سازمان تدابیر لازم امنیتی مورد نیاز را اتخاذ و در اصل یک استراتژیک امنیتی را تبیین کند و براساس آن یکسری سیاست های امنیتی پی ریزی شود سپس لازم است مجریان و کسانی که استراتژیک و سیاست ها را تعیین می کنند همه با هم به دانش روز آگاه باشند و اطلاعاتشان دائم به روز شود که بعدا این افراد بتوانند با توجه به سیاست های محلی هر سازمان یک پوسته حفاظتی مناسب را در سطح شبکه داخلی خودشان ایجاد کنند. در ضمن علاوه بر اینکه سازمان ها این پوسته حفاظتی را ایجاد می کنند باید مکان و سازمان به خصوصی وجود داشته باشد که آخرین اطلاعاتی که در زمنیه امنیت شبکه وجود

دارد و یا چالش های موجود در این زمنیه را تقسیم و آنالیزه کرده و این موارد را در سطح کل کشور و آن جای که مد نظر است ارایه دهد که همه بتوانند از آن استفاده کنند . در مجموع طبقه بندی زیر قابل ارائه میباشد:

**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 .

دولت از یک بعد و آن پورت های ورودی و خروجی و دستیابی به اینترنت می تواند سیاستی را پیاده کرده و بحث امنیت را از بالا نظارت کند اما در ابعاد دیگر نیز دولت می تواند از مجموعه و کسانی که درگیر این مسایل هستند حمایت کند دولت همچنین می تواند برای شکل گیری ساختار فیزیکی کمک کند یعنی در اصل هم می تواند حمایت لجستیکی و هم حمایت فنی و ساختاری داشته باشد هم اکنون از سوی دولت طرحی مثل تکفا یا طرح های دیگر ارایه شده اما اگر ما قصد مسافرت داریم باید قبل از اینکه به این فکر باشیم که در راه چه چیزی بخوریم بهتر است اول به فکر اتومبیل و جاده باشیم و ایمنی آن را در نظر بگیریم در مورد اینترنت که بستر آن بزرگراه نام دارد بهتر است قبل از حرکت روی مسئله امنیت آن توجه کنیم و دولت می تواند روی این مسئله نقش جدی داشته باشد و هم روی مسئله اصلی که ورودی و خروجی اینترنت است و هم در سطوح دیگر به عنوان نمونه در مورد حمایت از بخش خصوصی که اگر دولت این کارها را انجام ندهد در آینده حتما ضرر می کنیم چرا که شاید الان ما اطلاعات با ارزشی نداشته باشیم که نگران و نارحت از دست دادن آن هم نیستیم ولی اگر یک زمانی اطلاعات با ارزشی داشته باشیم که بخواهیم به صورت آن لاین در اختیار متقاضیان قرار بگیرد مطمئن باشید اگر آن سیستم تنها یک ساعت به دلیلی از کار بیفتد کل مسیر طی شده بر می گردد به نقطه شروع یعنی تمام مسیری که با زحمت به جلو سوق داده ایم در یک لحظه از دست می دهیم .

**کنترل سازمانی**

روش دیگر کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی 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 تواماً انجام این وظیفه را تضمین کند .

### 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 محدودهٔ خانواده نیز اعمال می‌شود و چه بسا اطرافیان را نیز تحت تأثیر قرار دهد .البته شیوهٔ اخیر در صورتی ممکن خواه بود که واگذاری خط اشتراک IPپس 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 .

### تقویت اینترانت‌ها

از سوی دیگر تقویت شبکه‌های داخلی که به اینترانت معرو ف 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 اینترانتها، علاوه بر ارائهٔ 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 اینترانتها، دو عامل مورد توجه کاربران به شبکه‌های داخلی است که به نظر نمی‌رسد محل مناسبی برای اطلاعات گزینش شده اینترنت باشد .

### 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 ادارهٔ 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 .

**کار گسترده فرهنگی برای آگاهی کاربران**

اما بهترین روش، کار گستردهٔ 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 .

اکنون به بررسی تخصصی از شبکه و اجزا آن جهت حفظ امنیت می پردازیم:

**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 دارایهای 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 وسیلهٔ 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 شبکهٔ 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 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 نحوهٔ 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 نحوهٔ 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 مبادلهٔ اطلاعات فراهم نمی‌شود .

برای امن کردن یک شبکه حداقل نیاز به سه ابزار زیر داریم :

Firewall

IDS (Intrusion Detection System)

Honey Pot

برای اینکه با وظایف این ابزارها آشنا شویم، آنها را با ابزارهای امنیتی ساختمان (برای جلوگیری از وقوع سرقت) مقایسه می‌کنیم .

محل های مختلف یک ساختمان (مثلا" یک شرکت یا سازمان) را از لحاظ امنیتی می‌توان به بخش‌های مختلفی تقسیم کرد .

- محل‌های غیرحساس: محل‌هایی که به امنیت کمتری نیاز دارند مثل حیاط، حیاط خلوت، پشت بام و ...
- محل‌های حساس: محل‌هایی که به امنیت بالا نیاز دارند، مانند محل قرار گرفتن گاوصندوق، بایگانی محرمانه، اطاقی که تجهیزات گران‌قیمت در آن قرار دارد و ...

شما برای ایمنی ساختمان‌تان چه می‌کنید؟

- موانع امنیتی ایجاد می‌کنید. تمام درهای ورودی خود را قفل می‌کنید. ممکن است روی دیوار حیاط و روی پنجره ها، حفاظ نصب کنید، علاوه بر در ورودی ساختمان، در ورودی آپارتمان‌ها و حتی اتاق‌ها را نیز قفل می‌کنید و .....
- در ساختمان دزدگیر و در هر کدام از محل‌های مستقل حساس یک حسگر (Sensor – Detector) نصب می‌کنید .
- هرچند خیلی معمول نیست، اما می‌توانید مقداری لوازم و وسایل که از نظر شما ارزشی ندارند در محل‌های غیرحساس قرار دهید تا سارق با دیدن آنها از خیر عبور از موانع امنیتی و ورود به محل‌های حساس بگذرد و به همان‌ها قناعت کند .

علاوه بر تمام تمهیدات بالا، شما به طور مستمر امنیت ساختمان‌تان را زیر ذره بین دارید. قفل‌ها را هر روز چک می‌کنید. اگر مطلع شوید یکی از قفل‌ها یا حسگرها، کارآیی لازم را ندارد و سارقان به راحتی آن‌را باز و یا از آن عبور می‌کنند، فوری آن را عوض خواهید کرد .

در یک شبکه کامپیوتری برای ایجاد موانع عبور، Firewall نصب می‌کنیم. برای آگاه شدن از وقوع نفوذ، IDS نصب می‌کنیم و برای منحرف کردن و شناسایی رفتار و روش نفوذگر، Honey Pot نصب می‌کنیم .

یکی از اصول امنیت، استفاده از الگوی دفاع لایه به لایه است. (استفاده از برج، دیوارهای بلند، دروازه های اصلی و فرعی، خندق و ... در قلعه های قدیمی)

کل شبکه (Internetwork) را می‌توان به دو بخش قابل اعتماد (Trusted) و غیرقابل اعتماد (Untrusted) تقسیم بندی کرد. شبکه داخلی را می‌توان شبکه قابل اعتماد و شبکه عمومی(اینترنت) را شبکه غیرقابل اعتماد دانست. در شبکه های کامپیوتری محلی را به نام DMZ (Demilitarized Zone) تعریف می‌کنیم. در واقع DMZ ناحیه‌ای بین شبکه داخلی شما (Trusted) و شبکه عمومی (Untrusted) است. سرورهایی را که باید از اینترنت قابل دسترسی باشند (مانندWeb Server ، Mail Server، FTP Serverو DNS Server) را در DMZ قرار می‌دهیم. این سیاست مطابق الگوی دفاع لایه به لایه است. به این ترتیب می‌توانیم راه برقراری ارتباط از اینترنت به داخل شبکه را به طور کامل مسدود کنیم .برای ایجاد لایه های بیشتر می‌توان بیش از یک DMZ در شبکه ایجاد کرد .

تعدادDevice های امنیت شبکه به تعدادDMZ ها و موارد دیگری بستگی دارد و با توجه به ساختار شبکه‌ی هر سازمان، میزان حساسیت و برخی پارامترهای دیگر تعیین می‌شود .

نقش Honey Pot را همواره سروری بازی می‌کند که سرویس‌های مختلفی روی آن فعال است. نظیرHTTP ، Mail، FTP، DNSو غیره و اطلاعات بدون ارزشی نیز روی آن قرار دارد. محل این سرور، در دسترس ترین مکان برای نفوذ انتخاب می‌شود (بین شبکه Public و اولین Firewall)، تا نفوذگر به محض اقدام به نفوذ به شبکه آن را ببیند و با آن مشغول شود. حسن Honey Pot ، علاوه بر منحرف کردن نفوذگر از سرورهای اصلی، شناسایی روش نفوذ او نیز هست. تا بتوانیم سیاست‌های بر ضد این روش را در Firewall خود پیاده سازی کنیم .با Deviceهای مورد نیاز برای امنیت شبکه آشنا شدیم .این Device ها را می‌توان در قالب‌های مختلف ارائه کرد .

برای ارائه Device های ذکر شده دو روش وجود دارد :

الف) از محصولات آماده شرکت‌های سازنده این Device ها مانند Cisco استفاده شود .

ب) به شکل نرم افزاری بر روی یک Intel Based Device (IBD) نصب و تنظیمات لازم اعمال شود. لازم به گفتن است که این دستگاه در واقع، مشابه یک PC است که براساس نوع نیاز مشتری و نوع استفاده از آن ساخته می‌شود. سیستم عامل نصب شده بر روی این دستگاه، می‌تواند از محصولات Open Source نظیر Linux و xBSD و یا Windows باشد .

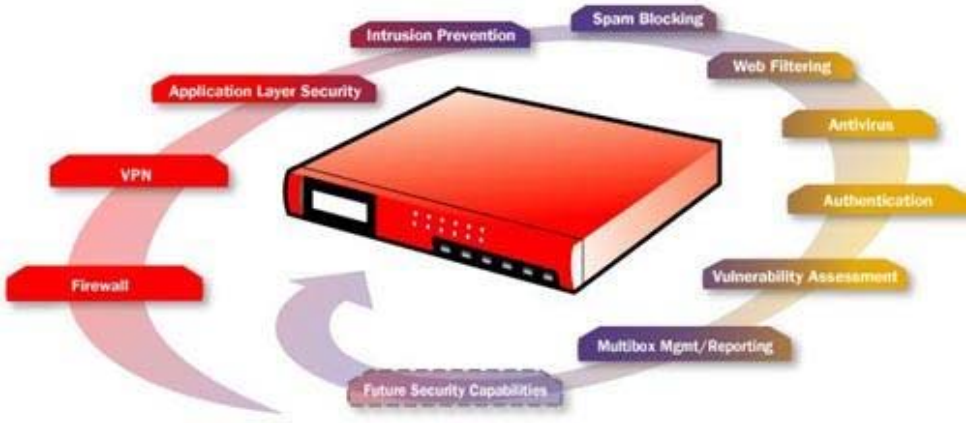
مطلب بسیار مهمی که قابل تاکید دوباره است، این است که سیستم امنیت شبکه، فقط تعریف سیاست‌های امنیتی و نصب و تنظیم تعدادی Deviceبراساس این سیاست‌ها نیست، بلکه امنیت شبکه (درست مانند امنیت یک ساختمان)، یک فرایند مستمر است. به این مفهوم که باید به صورت مرتب، اعمال زیر را انجام داد :

- تعریف سیاست‌های امنیتی جدید
- اعمال فیلترها برای مقابله با روش‌های نفوذ جدید (یاworm های جدید)
- پایش یا Monitoring مستمر شبکه و ارزیابی متناوب شبکه برای جلوگیری از ایجاد منافذ و نارسایی های جدید در شبکه
- ...

در ایران رخنه گرها ( هکرها ) هر کاری که بخواهند می توانند انجام دهند و این در حالی است که در کشورهای خارجی به اولین چیزی که توجه می شود امنیت شبکه ها است:

**یک رویکرد امنیتی لایه بندی شده**

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است.



رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد:

۱ - پیرامون

۲ - شبکه

۳ - میزبان

۴ - برنامه کاربردی

۵ - دیتا

محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید .

**افزودن به ضریب عملکرد هکرها**

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد (work factor) استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است. ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از سیستمها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که یک شبکه ضریب عملکرد بالایی دارد، که دارای رویکرد لایه بندی شده نیز هست، احتمالاً آن شبکه را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که از یک شبکه امن انتظار میرود .

تکنولوژی های بحث شده در این جا مجموعاً رویکرد عملی خوبی برای امن سازی دارایی های دیجیتالی یک شبکه را به نمایش می گذارند. در یک دنیای ایده آل، بودجه و منابع را برای پیاده سازی تمام ابزار و سیستم ها وجود خواهد داشت. اما متأسفانه در چنین دنیای حقیقی باید شبکه ها ارزیابی شوند و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی شود .

**مدل امنیت لایه بندی شده**

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند.

| سطح امنیتی | ابزار و سیستم های امنیتی قابل استفاده |
|---|---|
| پیرامون | فایروال<br>آنتی ویروس در سطح شبکه<br>رمزنگاری شبکه خصوصی مجازی |
| شبکه | سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS)<br>سیستم مدیریت آسیب پذیری<br>تبعیت امنیتی کاربر انتهایی<br>کنترل دسترسی/ تایید هویت کاربر |
| میزبان | سیستم تشخیص نفوذ میزبان<br>سیستم ارزیابی آسیب پذیری میزبان<br>تبعیت امنیتی کاربر انتهایی<br>آنتی ویروس<br>کنترل دسترسی/ تایید هویت کاربر |
| برنامه کاربردی | سیستم تشخیص نفوذ میزبان<br>سیستم ارزیابی آسیب پذیری میزبان<br>کنترل دسترسی/ تایید هویت کاربر<br>تعیین صحت ورودی |
| داده | رمزنگاری<br>کنترل دسترسی/ تایید هویت کاربر |

**سطح ۱: امنیت پیرامون**

منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان DMZ (demilitarized zone) شناخته می شود. معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرورها در DMZ می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد .

پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست .

تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند :

- فایروال ـ معمولاً یک فایروال روی سروری نصب می گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می دهد ۱- کنترل ترافیک ۲- تبدیل آدرس و ۳ -نقطه پایانی .VPN فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند .

- آنتی ویروس شبکه ـ این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود .

- یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند. اساساً VPN، یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایهVPN ، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد .برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود .

شبکه خصوصی مجازی یا Virtual Private Network که به اختصار VPN نامیده می شود، امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولا از VPN برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می شود.منظور از یک شبکه خصوصی شبکه ای است که بطور آزاد در اختیار و دسترس عموم نیست. VPN به این دلیل مجازی نامیده می شود که از نظر دو شبکه خصوصی ، ارتباط از طریق یک ارتباط و شبکه خصوصی بین آنها برقرار است اما در واقع شبکه عمومی این کار را انجام می دهد. پیاده سازی VPN معمولا اتصال دو یا چند شبکه خصوصی از طریق یک تونل رمزشده انجام می شود. در واقع به این وسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایر کاربران محفوظ می ماند. VPN را می توان بسته به شیوه پیاده سازی و اهداف پیاده سازی آن به انواع مختلفی تقسیم کرد.

دسته بندی VPN براساس رمزنگاری

VPN را می توان با توجه به استفاده یا عدم استفاده از رمزنگاری به دو گروه اصلی تقسیم کرد:

1- VPNرمزشده : VPN های رمز شده از انواع مکانیزمهای رمزنگاری برای انتقال امن اطلاعات بر روی شبکه عمومی استفاده می کنند. یک نمونه خوب از این VPN ها ، شبکه های خصوصی مجازی اجرا شده به کمک IPSec هستند.

2- VPN رمزنشده : این نوع از VPN برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع شبکه یکدیگر ایجاد می شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تامین می شود. یکی از این روشها تفکیک مسیریابی است. منظور از تفکیک مسیریابی آن است که تنها اطلاعات در حال تبادل بین دو شبکه خصوصی به هر یک از آنها مسیر دهی می شوند. (MPLS VPN) در این مواقع می توان در لایه های بالاتر از رمزنگاری مانند SSL استفاده کرد.

هر دو روش ذکر شده می توانند با توجه به سیاست امنیتی مورد نظر ، امنیت مناسبی را برای مجموعه به ارمغان بیاورند، اما معمولا VPN های رمز شده برای ایجاد VPN امن به کار می روند. سایر انواع VPN مانند MPLS VPN بستگی به امنیت و جامعیت عملیات مسیریابی دارند.

دسته بندی VPN براساس لایه پیاده سازی

VPN بر اساس لایه مدل OSI که در آن پیاده سازی شده اند نیز قابل دسته بندی هستند. این موضوع از اهمیت خاصی برخوردار است. برای مثال در VPN های رمز شده ، لایه ای که در آن رمزنگاری انجام می شود در حجم ترافیک رمز شده تاثیر دارد. همچنین سطح شفافیت VPN برای کاربران آن نیز با توجه به لایه پیاده سازی مطرح می شود.

1- VPN لایه پیوند داده : با استفاده از VPN های لایه پیوند داده می توان دو شبکه خصوصی را در لایه 2 مدل OSI با استفاده از پروتکلهایی مانند ATM یا Frame Relay به هم متصل کرد.با وجودی که این مکانیزم راه حل مناسبی به نظر می رسد اما معمولا روش

ارزانی نیست چون نیاز به یک مسیر اختصاصی لایه 2 دارد. پروتکلهای Frame Relay و ATM مکانیزمهای رمزنگاری را تامین نمی کنند. آنها فقط به ترافیک اجازه می دهند تا بسته به آن که به کدام اتصال لایه 2 تعلق دارد ، تفکیک شود. بنابراین اگر به امنیت بیشتری نیاز دارید باید مکانیزمهای رمزنگاری مناسبی را به کار بگیرید.

2- VPN لایه شبکه : این سری از VPN ها با استفاده از tunneling لایه 3 و/یا تکنیکهای رمزنگاری استفاده می کنند. برای مثال می توان به IPSec Tunneling و پروتکل رمزنگاری برای ایجاد VPN اشاره کرد.مثالهای دیگر پروتکلهای GRE و L2TP هستند. جالب است اشاره کنیم که L2TP در ترافیک لایه 2 تونل می زند اما از لایه 3 برای این کار استفاده می کند. بنابراین در VPN های لایه شبکه قرار می گیرد. این لایه برای انجام رمزنگاری نیز بسیار مناسب است.

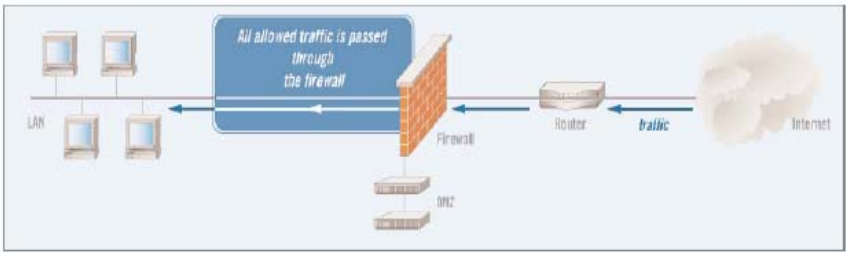
3- VPN لایه کاربرد : این VPN ها برای کار با برنامه های کاربردی خاص ایجاد شده اند. VPN های مبتنی بر SSL از مثالهای خوب برای این نوع از VPN هستند. SSL رمزنگاری را بین مرورگر وب و سروری که SSL را اجرا می کند، تامین می کند. SSH مثال دیگری برای این نوع از VPN ها است.SSH به عنوان یک مکانیزم امن و رمز شده برای login به اجزای مختلف شبکه شناخته می شود. مشکل VPNها در این لایه آن است که هرچه خدمات و برنامه های جدیدی اضافه می شوند ، پشتیبانی آنها در VPN نیز باید اضافه شود.

دسته بندی VPN براساس کارکرد تجاری:

VPN ها برای رسیدن به اهداف تجاری خاصی ایجاد می شوند. این اهداف تجاری تقسیم بندی جدیدی را برای VPN بنا می کنند .

1- VPN اینترانتی : این سری از VPN ها دو یا چند شبکه خصوصی را در درون یک سازمان به هم متصل می کنند. این نوع از VPN زمانی معنا می کند که می خواهیم شعب یا دفاتر یک سازمان در نقاط دوردست را به مرکز آن متصل کنیم و یک شبکه امن بین آنها برقرار کنیم.

VPN اکسترانتی : این سری از VPN ها برای اتصال دو یا چند شبکه خصوصی از دو یا چند سازمان به کار می روند. از این نوع VPN معمولا برای سناریوهای B2B که در آن دو شرکت می خواهند به ارتباطات تجاری با یکدیگر بپردازند، استفاده می شود



**مزایا**

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند. بعضی از فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند .

**معایب**

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور-زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان IT تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند .

**ملاحظات**

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند .

انواع ابزاری که در DMZ شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

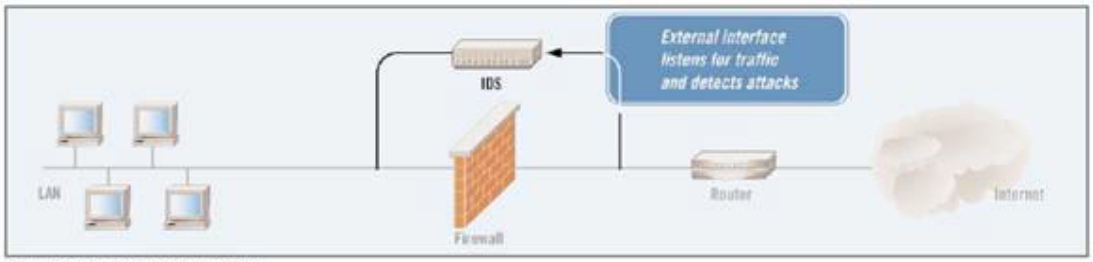
**سطح ۲ - امنیت شبکه**

سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند.

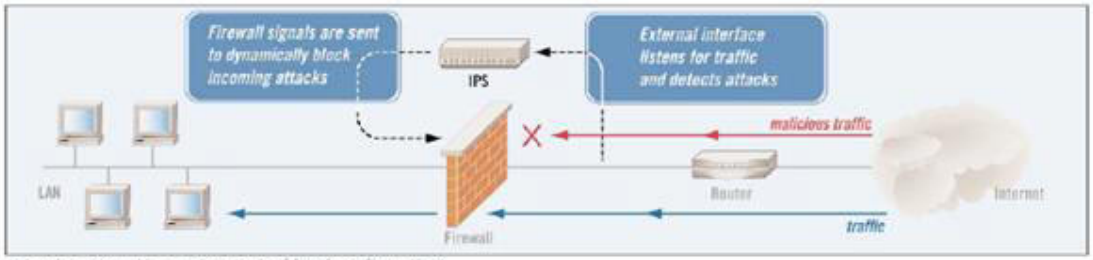
تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند :

IDS ·ها (سیستم های تشخیص نفوذ) وIPS ها (سیستم های جلوگیری از نفوذ (ـ تکنولوژیهای IDS و IPS ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته

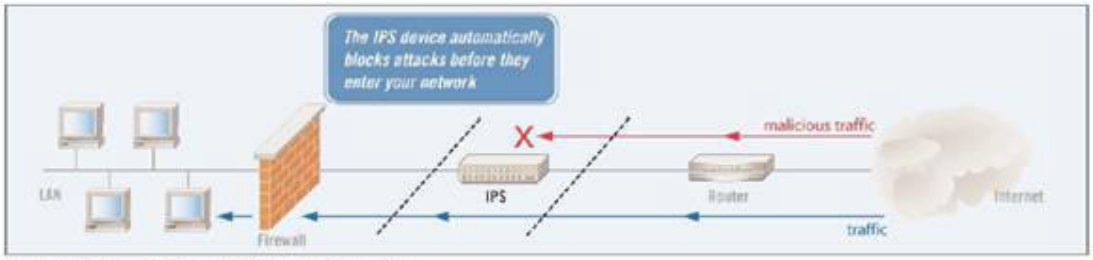
اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند .ابزارهای IDS مسؤولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و بصورت خودکار ترافیک آسیب رسان را مسدود می کنندIDS .ها وIPS ها مشخصات مشترک زیادی دارند. در حقیقت، بیشترIPS ها در هسته خود یک IDSدارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می شود. محصولات IDS تنها ترافیک آسیب رسان را تشخیص می دهند، در حالیکه محصولات IPS از ورود چنین ترافیکی به شبکه شما جلوگیری می کنند .



Intrusion detection system (IDS)



Intrusion prevention system (out-of-band configuration)



Intrusion prevention system (in-line configuration)

**مدیریت آسیب پذیری**: سیستم های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می کنند و (۲)روند مرمت آسیب پذیری یافته شده را مدیریت می کنند. در گذشته، این تکنولوژی( VA) تخمین آسیب پذیری نامیده می شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می دهند .

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری هایی که می توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می کنند. آنها معمولاً پایگاه داده ای از قوانینی را نگهداری می کنند که آسیب پذیری های شناخته شده برای گستره ای از ابزارها و برنامه های شبکه را مشخص می کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می آزماید .

همچنانکه از نامش برمی آید، سیستم مدیریت آسیب پذیری شامل ویژگیهایی است که روند بازسازی را مدیریت می کند. لازم به ذکر است که میزان و توانایی این ویژگی ها در میان محصولات مختلف، فرق می کند .

**تابعیت امنیتی کاربر انتهایی**: روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می کنند که تضمین می کنند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند، رعایت کرده اند. این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم های ناامن کارمندان و ابزارهای VPN و RAS می گیرد .

روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می دهند، اجازه دسترسی می دهند. هدف آنها از این تست ها معمولاً برای بررسی (۱) نرم افزار مورد نیاز، مانند سرویس پک ها، آنتی ویروس های به روز شده و غیره و (۲) کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است .

**کنترل دسترسی\تأیید هویت**: کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند. هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند .

میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می افتد. اما به خاطر داشته باشید که کنترل دسترسی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند .

**مزایا**

تکنولوژی هایIDS ، IPSو مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد، ابزار IPS و IDS تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد .

سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند. انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیرعملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید،

ارتقاءدادن نرم افزارها و وصله ها، و افزودن و کاستن از کاربران، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری های جدید پیمایش کنید .

روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است. هکرها بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، همچانکه پدیده های اخیر چونMydoom ، Sobig، و Sasser گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند .

**معایب**

IDSها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان false positives نیز شناخته می شوند. در حالیکه IDS ممکن است که یک حمله را کشف و به اطلاع شما برساند، این اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری بالا، یک IDSباید بصورت پیوسته بررسی شود و برای الگوهای مورد استفاده و آسیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند .

سطح خودکار بودن درIPS ها می تواند به میزان زیادی در میان محصولات، متفاوت باشد. بسیاری از آنها باید با دقت پیکربندی و مدیریت شوند تا مشخصات الگوهای ترافیک شبکه ای را که در آن نصب شده اند منعکس کنند. تأثیرات جانبی احتمالی در سیستمهایی که بهینه نشده اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می شود .

بسیاری، اما نه همه روش های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر نقطه انتهایی دارد. این عمل می تواند مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه کند .

تکنولوژی های کنترل دسترسی ممکن است محدودیت های فنی داشته باشند .برای مثال، بعضی ممکن است با تمام ابزار موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای ایجاد پوشش نیاز داشته باشید. همچنین، چندین فروشنده سیستم های کنترل دسترسی را به بازار عرضه می کنند، و عملکرد می تواند بین محصولات مختلف متفاوت باشد. پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد .چنین عمل وصله-پینه ای یعنی رویکرد چند محصولی ممکن است در واقع آسیب پذیری های بیشتری را در شبکه شما به وجود آورد .

**ملاحظات**

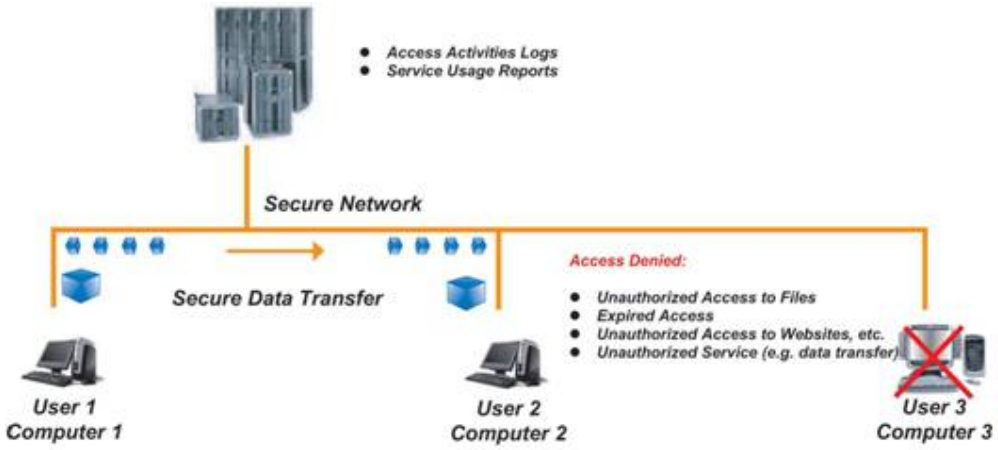
موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS/IPS ، مدیریت آسیب

پذیری و امنیت کاربر انتهایی ممکن است منابعی از شبکه ای را که از آن محافظت می کنند، مصرف کنند. سرعت های اتصالی بالاتر تأثیری را که این ابزارها بر کارایی شبکه دارند به حداقل خواهد رساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت بهبودیافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد .

وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد.

### سطح ۳- امنیت میزبان

سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها و غیره در شبکه است. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادرستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات رجیستری، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.




تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

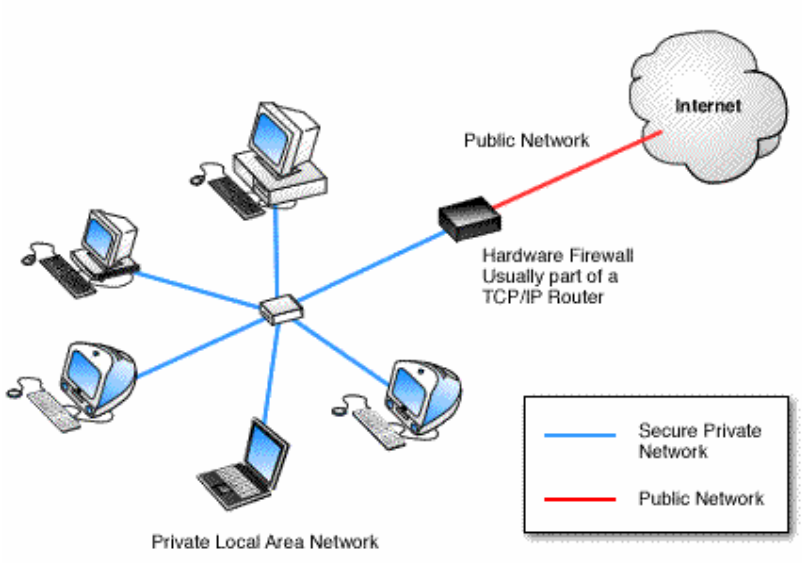
**IDS در سطح میزبان:** IDS های سطح میزبان عملیاتی مشابه IDS های شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDS های سطح میزبان برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.

**VA (تخمین آسیب پذیری) سطح میزبان:** ابزارهای VA سطح میزبان یک ابزار شبکه مجزا را برای آسیب پذیری های امنیتی پویش می کنند. دقت آنها نسبتا بالاست و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، درصورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.

**تابعیت امنیتی کاربر انتهایی:** روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیوسته میزبان را برای عملیات زیان رسان و آلودگی ها بررسی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.

**آنتی ویروس:** هنگامی که آنتی ویروس های مشخص شده برای ابزار در کنار آنتی ویروس های شبکه استفاده می شوند ، لایه اضافه ای برای محافظت فراهم می کنند.

**کنترل دسترسی\تصدیق هویت**: ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.




**مزایا**

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن مشخصات عملیاتی مخصوص یک ابزار پیکربندی می گردند. دقت و پاسخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت مشخص کنند کدام تنظیمات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.

**معایب**

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز رسانی مداوم دارند، اغلب ساعات زیادی برای مدیریت مناسب می طلبند. اغلب نصبشان مشکل است و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است. همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد.

**ملاحظات**

بدلیل هزینه ها و باراضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند. بعنوان یک اصل راهنما، بیشتر سازمان ها این ابزار را فقط روی سیستم های بسیار حساس شبکه نصب می کنند. استثناء این اصل یک راه حل تابعیت امنیتی کاربر انتهایی است، که اغلب برای پوشش دادن به هر ایستگاه کاری که تلاش می کند به شبکه دسترسی پیدا کند، بکار گرفته می شود

## سطح ۴- امنیت برنامه کاربردی


در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند. این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند. این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیات بد دارند، باشند. بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

**پوشش محافظ برنامه:** از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شفاف است و با درجه بالایی با سیستم یکپارچه می شود.

یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور پیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.

**کنترل دسترسی/تصدیق هویت**: مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.

**تعیین صحت ورودی**: ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در جای خود مورد استفاده قرار نگیرند، هر تراکنش بین افراد و واسط کاربر می تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود!

به عنوان مثال، یک فرم وبی با یک بخش zip code را در نظر بگیرید. تنها ورودی قابل پذیرش در این قسمت فقط پنج کاراکتر عددی است. تمام ورودی های دیگر باید مردود شوند و یک پیام خطا تولید شود. تعیین صحت ورودی باید در چندین سطح صورت گیرد. در این مثال، یک اسکریپت جاوا می تواند تعیین صحت را در سطح مرورگر در سیستم سرویس گیرنده انجام دهد، در حالیکه کنترل های بیشتر می تواند در سرور وب قرار گیرد. اصول بیشتر شامل موارد زیر می شوند:

- کلید واژه ها را فیلتر کنید. بیشتر عبارات مربوط به فرمانها مانند «insert»، باید بررسی و در صورت نیاز مسدود شوند.
- فقط دیتایی را بپذیرید که برای فلید معین انتظار می رود. برای مثال، یک اسم کوچک ۷۵ حرفی یک ورودی استاندارد نیست.

**مزایا**

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

**معایب**

پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با امنیت سطح برنامه می تواند عملی ترسناک! و غیرعملی باشد. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

**ملاحظات**

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی بلندمدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند.

## سطح ۵ - امنیت دیتا

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان روشی بسیار مناسب توصیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند. امنیت دیتا تا حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد که سیاست های دسترسی و ابزار امنیتی مناسبی را که باید بکار گرفته شوند، مشخص کنید.

تکنولوژی های زیر امنیت در سطح دیتا را فراهم می کنند:

**رمزنگاری:** طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/رمزگشایی هستند که تمام افرادی که به دیتا دسترسی دارند، باید داشته باشند. استراتژی های رمزنگاری معمول شامل PKI، PGP و RSA هستند.

**کنترل دسترسی / تصدیق هویت** : مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.

**مزایا**

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می کند.

**معایب**

بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

**ملاحظات**

رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری باید برای تمام ابزارها و برنامه های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است.

## رویدادهای امنیتی و اقدامات لازم در برخورد با آنها (Incident Handling)

هر رویداد مضر مشخص یا مشکوکی که به امنیت سیستم ها یا شبکه های کامپیوتری مربوط باشد.

یا

عمل نقض کردن آشکار یا ضمنی سیاست امنیتی.

فعالیت هایی زیر مثال هایی از یک رویداد امنیتی هستند:

- تلاشهایی (چه موفق و چه ناموفق) برای حصول دسترسی غیرمجاز به یک سیستم یا دیتای آن
- ازکار افتادن ناخواسته یا عدم پذیرش سرویس
- استفاده غیرمجاز از یک سیستم به هدف پردازش یا ذخیره سازی دیتا
- تغییراتی در مشخصات سخت افزار یا نرم افزار بدون آگاهی یا اجازه یا دخالت صاحب آن.

فعالیت شبکه یا میزبان که بالقوه امنیت کامپیوتر را تهدید می کند نیز می تواند بعنوان رویداد امنیتی کامپیوتری تعریف گردد.

**برخورد با رویداد**

منظور از این عبارت نحوه مقابله و اقداماتی است که در هنگام وقوع یک مسأله امنیتی انجام می گیرد. در حقیقت این اقدامات به سه بخش تقسیم می شود. گزارش رویداد، تحلیل رویداد و واکنش به رویداد.

اهمیت واکنش به رویدادهای امنیتی سیستم ها، کمتر از تشخیص آنها نیست. اقداماتی که شما بدنبال تشخیص یک رویداد انجام می دهید، نه تنها عملیات سازمان را تحت تأثیر قرار می دهد، بلکه ممکن است باعث تغییرات بسیاری در آینده چنین روندهایی و وضعیت امنیتی خودتان گردد.

**مثالی از واکنش به یک رویداد در یک سازمان بزرگ**

این مثال فقط برای نشان دادن تلاش های ممکن برای واکنش ارائه شده است و یک مدل کلی نیست.

هنگام مشاهده ثبت وقایع مربوط به نفوذ در ساعت ۲ بامداد، پرسنل ۲۴ ساعته مراقبت از شبکه کشف می کنند که حمله ای با موفقیت انجام شده است.

برای بسیاری از سازمان ها، واکنش فوری، قطع شبکه برای تأخیر یا قطع افشای اطلاعات بیشتر خواهد بود، اما ما سعی داریم که از چنین واکنشی پرهیز کنیم و پرسنل بخش مراقبت نیز از این قضیه مطلع هستند. درعوض، چک لیست هایی را که در اختیار دارند برای برخورد با این نوع رویداد به اجرا می گذارند.

قدم اول خبرکردن و ارائه گزارشی مختصر به رئیس بخش امنیت سیستمها (یا نماینده اش) است. تا این فرد از خواب بیدار گردد و از حمله مطلع گردد، چهار دقیقه از اطلاع دهی اولیه سپری شده است.

با اطلاعاتی که موجود است، نماینده امنیت shutdown کامل سیستم را نمی پذیرد، اما اجازه فراخوانی یک گروه امداد را می دهد. در حالیکه نماینده بخش امنیت به سمت محل حرکت می کند، پرسنل بخش مراقبت شروع به این فراخوانی می کند. نمایندگانی از بخشهایی چون عملیات شبکه، قانونی، مهندسی، اجرایی و مدیریت آگاه شده اند و به محل فراخوانده شده اند. مجری قانون محلی نیز خبر شده است و ثبت رویدادها به ترتیب وقوع آغاز می شود.

حالا از اخطار اولیه ۲۸ دقیقه گذشته است.

نماینده بخش امنیت که اولین فرد باخبر شده است، اولین کسی است که می رسد. این شخص تنظیم و آماده سازی مرکز امداد را آغاز می کند. کیف امداد باز است که در آن یک لپ تاپ، باتری اضافه، لامپ، ابزار، چک لیست ها و صفحات یادداشت برای تمام اعضای تیم امداد، و ابزار گوناگون دیگر وجود دارد. کپی هایی از اطلاعات موجود نیز برای توزیع بین اعضای تیم و مدیریت ارشد آن آماده شده است. ۵۷ دقیقه از زمان اخطار اولیه گذشته است.

سایر اعضای گروه به صورت پراکنده در طول این زمان وارد شده اند و پرسنل بخش مراقبت نیز تحقیق بیشتری در مورد نفوذ انجام داده است. بررسی اولیه آشکار می کند که نفوذگر به سیستم یک کاربر وارد شده است، اما هنوز به نقاط دیگر شبکه پیشروی نکرده است. حمله از طریق استفاده یک کاربر از یک اتصال dial-up که مورد تأیید نبوده صورت گرفته است. نفوذ واقعی هشت ساعت قبل از کشف اولیه صورت گرفته است.

کل گروه ۹۲ دقیقه بعد از اولین اخطار گرد هم می آیند. تمام اعضاء با سرعت در محل حاضر و شروع به فکر کردن و نقشه کشیدن و ارائه راه حل شده اند. مناظرات به موافقت هایی منجر می شود. سیستم مورد نفوذ از شبکه جدا خواهد شد و عملیات تعیین و تشخیص آغاز خواهد شد. خلاصه ای برای مدیر ارشد تهیه و مراحل اولیه کامل می شوند. ۱۰۸ دقیقه گذشته است.

نماینده عملیات شبکه، مسؤول قطع کردن سیستم مذکور می شود. نماینده اجرایی ثبت وقایع را روی لپ تاپ به روز و بررسی مجدد می کند. این فرد با ثبت لحظه به لحظه از تمام رویدادها، بعنوان نقطه مرکزی تمام فعالیت ها و ارتباطات گروه عمل می کند. نماینده قانونی با آگاه شدن از وضعیت موجود و راهنمایی هایی داده شده به وی، به خانه برمی گردد تا ابتدای صبح به محل برگردد. پرسنل بخش مهندسی و امنیت، اطلاعاتی را که تا کنون جمع آوری شده و شامل دیتای حاصل از سیستم تحت نفوذ قرار گرفته است، بررسی می کنند. این اطلاعات روی بستر یک شبکه مجزا بررسی و تحلیل می شود تا نفوذگر، ابزار حمله و روش هایی ممکن برای بستن آسیب پذیری در کل سازمان مشخص شود.

با سپری شدن ۱۴۱ دقیقه از آغاز، گروه برای مرور و به روز رسانی پیشرفت کار دوباره دور هم جمع می شوند. مشخص شده است که نفوذگر از یک IP بیگانه جعلی از طریق اتصال dial-up استفاده کرده است و فقط قادر به دستیابی به همان سیستم بوده است. بررسی کامل شبکه احتیاج به این دارد که سرورها از شبکه جدا شوند و این عملیات ۶ ساعت زمان نیاز دارد. گروه با مشورت و تصویب مدیریت ارشد، تصمیم به این بررسی می گیرد اما بعد از بسته شدن سازمان در انتهای روز کاری بعد.

هنگامی که روز کاری آغاز می شود، فعالیت ها به بیرون فاش می شود و فردی که سیستمش مورد نفوذ قرار گرفته مورد مصاحبه قرار می گیرد و سیستم مورد نفوذ پاکسازی می گردد و به افراد ارشد گزارشها بصورت خلاصه ارائه می شود. بهرحال، عملیات امداد به اوج خود می رسد و مرتفع سازی آغاز می شود. تا ساعت ۲۳ رویداد برطرف شده است و گزارش نهایی روز بعد آماده خواهد شد.

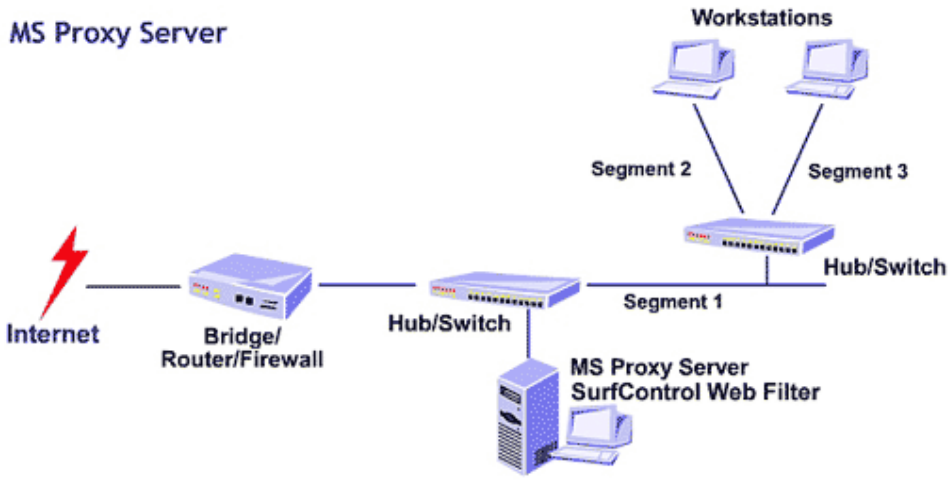
کسانی هستند که به فوریت مستندسازی تهدید بوجود آمده و عملیات آنی اصرار می ورزند که باید ۲ ساعت اضافه نیز برای آنها دید. برای سازمان شما، ممکن است چنین موردی رخ دهد، و شما بخواهید اولین گام بعد از تعیین رویداد، جداسازی یکطرفه و ناگهانی از شبکه و سیستم ها باشد. اما در این حالت خاص، مزیت انتخاب یک روند سیستماتیک، حفظ عملیات عادی برای یک روز کامل کاری بود، (بجای خاموش کردن کل سیستم سازمان برای یک روز کاری) که نتیجه آن نیم دوجین افراد خسته، چند ساعت کار جبرانی و اضافه کاری و خاموش بودن تنها یک سیستم در طول یک روز کاری بود.

**از نظر افراد درگیر این عملیات، هزینه ای که توسط این روش صرفه جویی شد، ارزش ریسک را داشت.**

## 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 ردشده 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 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 (Acknowledgement SYN/ACK) 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 می تواند چیزهایی را که سیاستهای امنیتی را نقض می کنند، تغییر دهد یا محروم کند. توجه کنید که فیلترهای بسته ها فقط header ها 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 مقایسه فایروال‌ها، ما مفهومی از پراکسی ارائه می‌دهیم و پراکسی را از فیلترکننده بسته‌ها متمایز می‌کنیم. با پیش‌زمینه‌ای که از پراکسی 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.

Client connects to the actual server, but the proxy server incercepts every message and can change it if neccessary.

**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

**پروتکل های انتقال فایل امن**

**AS2**

AS2 (Applicability Statement 2) گونه ای EDI (Electronic Date Exchange) یا تبادل دیتای الکترونیکی (اگرچه به قالبهای EDI محدود نشده) برای استفاده های تجاری با استفاده از HTTP است. AS2 در حقیقت بسط یافته نسخه قبلی یعنی AS1 است. AS2 چگونگی تبادل دیتای تجاری را بصورت امن و مطمئن با استفاده از HTTP بعنوان پروتکل انتقال توصیف می کند. دیتا با استفاده از انواع محتوایی MIME استاندارد که XML، EDI ، دیتای باینری و هر گونه دیتایی را که قابل توصیف در MIME باشد، پشتیبانی می کند، بسته بندی می شود. امنیت پیام (تایید هویت و محرمانگی) با استفاده از S/MIME پیاده سازی می شود. AS1 در عوض از SMTP استفاده می کند. با AS2 و استفاده از HTTPیا HTTP ) HTTP/S با(SSL برای انتقال، ارتباط بصورت زمان حقیقی ممکن می شود تا اینکه از طریق ایمیل انجام گیرد. امنیت، تایید هویت، جامعیت پیام، و خصوصی بودن با استفاده از رمزنگاری و امضاهای دیجیتال تضمین می شود، که برپایه S/MIME هستند و نه SSL. استفاده از HTTP/S بجای HTTP استاندارد بدلیل امنیت ایجادشده توسط S/MIME کاملاً انتخابی است. استفاده از S/MIME اساس ویژگی دیگری یعنی انکارناپذیری را شکل می دهد، که امکان انکار پیام های ایجادشده یا فرستاده شده توسط کاربران را مشکل می سازد، یعنی یک شخص نمی تواند منکر پیامی شود که خود فرستاده است.

AS2 مشخصاً برای درکنارهم قراردادن ویژگیهای امنیتی با انتقال فایل یعنی تایید هویت، رمزنگاری، انکارناپذیری توسط S/MIME و SSL انتخابی، طراحی شده است. از آنجا که AS2 یک پروتکل در حال ظهور است، سازمانها باید تولید کنندگان را به پشتیبانی سریع از آن تشویق کنند. قابلیت وجود انکارناپذیری در تراکنش های برپایه AS2 از اهمیت خاصی برای سازمانهایی برخوردار است که می خواهند پروسه های تجاری بسیار مهم را به سمت اینترنت سوق دهند. وجود قابلیت برای ثبت تراکنش پایدار و قابل اجراء برای پشتبانی از عملکردهای بسیار مهم مورد نیاز است. AS2 از MDN (Message Disposition Notification) بر پایه RFC 2298 استفاده می کند. MDN (که می تواند در اتصال به سایر پروتکل ها نیز استفاده شود) بر اساس محتوای MIME است که قابل خواندن توسط ماشین است و قابلیت آگاه سازی و اعلام وصول پیام را بوجود می آورد، که به این ترتیب اساس یک ردگیری نظارتی پایدار را فراهم می سازد.

**FTP**

FTP یا پروتکل انتقال فایل به منظور انتقال فایل از طریق شبکه ایجاد گشته است، اما هیچ نوع رمزنگاری را پشتیبانی نمی کند. FTP حتی کلمات عبور را نیز بصورت رمزنشده انتقال می دهد، و به این ترتیب اجازه سوءاستفاده آسان از سیستم را می دهد. بسیاری سرویس ها FTP بی نام را اجراء می کنند که حتی نیاز به کلمه عبور را نیز مرتفع می سازد (اگرچه در این صورت کلمات عبور نمی توانند شنیده یا دزدیده

شوند) FTP بعنوان یک روش امن مورد توجه نیست، مگر اینکه درون یک کانال امن مانند SSL یا IPSec قرار گیرد. گرایش زیادی به FTP امن یا FTP بر اساس SSL وجود دارد.

**SFTP**

SFTP به استفاده از FT بر روی یک کانال که با SSH امن شده، اشاره دارد، در حالیکه منظور از FTPS استفاده از FT بر روی SSL است. اگرچه SFTP دارای استفاده محدودی است، FTPS (که هر دو شکل FTP روی SSL و FTP روی TLS را بخود می گیرد) نوید کارایی بیشتری را می دهد. RFC 2228 ( (FTPS رمزنگاری کانالهای دیتا را که برای ارسال تمام دیتا و کلمات عبور استفاده شده اند، ممکن می سازد اما کانالهای فرمان را بدون رمزنگاری باقی می گذارد (بعنوان کانال فرمان شفاف شناخته می شود). مزیتی که دارد این است که به فایروالهای شبکه های مداخله کننده اجازه آگاهی یافتن از برقراری نشست ها و مذاکره پورتها را می دهد. این امر به فایروال امکان تخصیص پورت پویا را می دهد، بنابراین امکان ارتباطات رمزشده فراهم می شود بدون اینکه نیاز به این باشد که تعداد زیادی از شکاف های دائمی در فایروال پیکربندی شوند.

اگرچه معمول ترین کاربردهای FTP ( مخصوصاً بسته های نرم افزاری کلاینت) هنوز کاملاً FTPS (FTP روی (SSL را پشتیبانی نمی کنند و پشتیبانی مرورگر برای SSL، برای استفاده کامل از مجموعه کامل فانکشن های RFC 2228 FTPS کافی نیست، اما این امر در حال پیشرفت است. بسیاری از تولیدکنندگان برنامه های کاربردی در حال استفاده از SSL استاندارد در کنار FTP استاندارد هستند. بنابراین، گرچه در بعضی موارد مسائل تعامل همچنان وجود دارند، اما امیدواری برای پشتیبانی گسترده از FT امن در ترکیب با SSL وجود دارد. (و حتی امیدواری برای پذیرش گسترده مجموعه کامل فانکشن های RFC 2228 FTPS)

**رمزنگاری در پروتکل‌های انتقال**

تمرکز بیشتر روش‌های امنیت انتقال فایل بر اساس رمزنگاری دیتا در طول انتقال از طریق شبکه‌های عمومی مانند اینترنت است. دیتایی که در حال انتقال بین سازمانهاست بوضوح در معرض خطر ربوده شدن در هر کدام از محلها قرار دارد. – مثلا در شبکه‌های محلی برای هر یک از طرفین یا مرزهای Internet-LAN که سرویس‌دهندگان‌اینترنت از طریق آنها مسیر دیتا را تا مقصد نهایی مشخص می‌کنند. حساسیت دیتا ممکن است بسیار متغییر باشد، زیرا دیتای انتقالی ممکن است بهر شکلی از رکوردهای مالی بسته‌بندی شده تا تراکنش‌های مستقیم باشند. در بعضی موارد، ممکن است علاوه بر محافظت دیتا روی اینترنت، نیاز به محافظت دیتا روی LAN نیز باشد. مشخصاً، محافظت از دیتا در مقابل حملات LAN مستلزم رمزنگاری دیتای انتقالی روی خود LAN است. به این ترتیب، بهرحال، نیاز به بسط امنیت تا برنامه‌هایی است که خود

دیتا را تولید و مدیریت می‌کنند، و تنها اطمینان به راه‌حلهای محیطی کفایت نمی‌کند و به این ترتیب بر پیچیدگی مسأله امنیت افزوده می‌شود.

**پروتکل‌ها**

اگرچه ثابت‌شده است که رمزنگاری راه‌حل بدیهی مسائل محرمانگی است، اما سردرگمی در مورد دو نوع رمزنگاری (برنامه در مقابل شبکه) همچنان وجود دارد و بدلیل وجود پروتکلهای ارتباطی گوناگون است که نیازهای تعامل بیشتر آشکار می‌شود. (مانند IPSec ، S/MIME، SSL و TLS) اگرچه این پروتکلها قول تعامل را می‌دهند، اما تعامل کامل بدلیل مستقل بودن محصولات پروتکلها در حال حاضر وجود ندارد. آزمایشهایی در حال حاضر در حال انجام هستند که به حل شدن این مسائل کمک می‌کنند، اما کاربران باید مطمئن شوند که تعامل بین محصول انتخابیشان و محصولات سایر شرکای تجاری امری تثبیت شده است. پروتکل‌های ساده‌تر (SSL/TLS، IPSec و تا حدی پایین‌تر S/MIME ) عموماً مسائل کمتری از نظر تعامل دارند.

**پروتکل‌های رمزنگاری انتقال**

با ترکیب توانایی‌ها برای تایید هویت توسط رمزنگاری متقارن و نامتقارن برای ممکن ساختن ارتباطات تاییدشده و رمزشده، این پروتکلها پایه‌های امنیت را فراهم می‌کنند. تقریباً تمام پروتکلها نیازهای جامعیت را پشتیبانی می‌کنند به طوری که محتویات ارتباطات نمی‌توانند تغییر یابند، اما بیشتر آنها از Non-Repudiation پشتیبانی نمی‌کنند و به این ترتیب امکان ایجاد رکوردهای پایداری را که هویت منبع را به محتوای پیام پیوند می‌دهند، ندارند.

به این چند پروتکل به طور مختصر اشاره می‌شود:

**SSL**

تکنولوژی SSL (Secure Socket Layer) اساس World Wide Web امن را تشکیل می‌دهد. SSL که در مرورگرهای وب کاملاً جاافتاده است، توسط بسیاری از سازمانها برای رمزنگاری تراکنش‌های وبی خود و انتقال فایل استفاده می‌شود. بعلاوه SSL بصورت روزافزون بعنوان یک مکانیسم امنیت در تلاقی با پروتکلهای پرشمار دیگر استفاده می‌شود و بهمین ترتیب ابزاری برای ارتباط سروربه‌سرور امن است. SSL ارتباطات رمزشده و بشکل آغازین خود تایید هویت سرور از طریق استفاده از گواهی را (در حالت کلاینت‌به‌سرور) پشتیبانی می‌کند. کاربران اغلب برای استفاده از برنامه‌ها از طریق کلمه عبور تایید هویت می‌شوند، و با پیشرفت SSL استاندارد (مثلا SSL V.3.0) تایید هویت کلاینت از طریق گواهی به این پروتکل اضافه شده است.

**برای FT (انتقال فایل):** ابزار FT اغلب از SSL برای انتقال فایل در یکی از دو حالت استفاده می‌کنند. اولی، مد کلاینت‌به‌سرور است که کاربر را قادر می‌سازد، در حالیکه در حال استفاده از یک مرورگر وب استاندارد است مستندات را از یک سرور دریافت یا آنها را به سرور منتقل کند. که این قابلیت نیاز به نرم‌افزار مختص انتقال در کلاینت را برطرف می‌سازد و بسیار راحت است، اما اغلب فاقد بعضی ویژگیهای پیشرفته مانند نقاط آغاز مجدد و انتقالهای زمانبندی‌شده است که سازمانها نیاز دارند. SSL همچنین می‌تواند برای اتصالات سروربه‌سرور امن – برای مثال، در اتصال با FTP و سایر پروتکلها – مورد استفاده قرار گیرد.

**TLS**

TLS (Transport Layer Security)، جانشین SSL، برپایه SSL3.0 بنا شده است، اما به کاربران یک انتخاب کلید عمومی و الگوریتمهای Hashing می‌دهد. (الگوریتمهای Hashing فانکشن‌های یک‌طرفه‌ای برای حفظ جامعیت پیامها هستند و توسط بیشتر پروتکلها استفاده می‌شوند.) اگرچه TLS و SSL تعامل ندارند، اما چنانچه یکی از طرفین ارتباط TLSرا پشتیبانی نکند، ارتباط با پروتکل SSL3.0 برقرار خواهد شد. بیشتر مزایا و معایب SSL به TLS هم منتقل می‌شود، و معمولا وجه تمایز خاصی وجود ندارد، و از همه نسخه‌ها به عنوان SSL یاد می‌شود.

**S/MIME**

S/MIME (Secure Multipurpose Internet Mail Extention) که اختصاصاً برای پیام‌رسانی ذخیره-و-ارسال طراحی شده است، بعنوان استاندارد امنیت ایمیل برتر شناخته شده است. مانند بیشتر پروتکل‌های رمزنگاری (مثلا SSL ، TLS و IPSec)، S/MIME با رمزنگاری تنها سروکار ندارد. بهرحال، علاوه بر تصدیق هویت کاربران و ایمن‌سازی جامعیت پیامها (برای مثال مانند آنچه SSL انجام می‌دهد)، S/MIME توسط امضای دیجیتال، رکوردهای پایداری از صحت پیامها ایجاد می‌کند (ضمانت هویت فرستنده چنانچه به محتوای پیام مشخصی مرتبط شده). این عمل باعث می‌شود فرستنده پیام نتواند ارسال آن‌را انکار کند.

سیستم‌های ایمیل رمزشده (با استفاده از S/MIME) می‌توانند برای ارسال فایل‌های کوچک استفاده شوند (محدودیت حجم فایل بخاطر داشتن محدودیت حجم فایل در بیشتر سرورهای ایمیل است)، ولی S/MIME کلاً می‌تواند برای انتقال فایل‌های بزرگتر توسط پروتکلهای انتقال فایل استفاده شود.

**SSH**

SSH (Secure Shell) هم یک برنامه و یک پروتکل شبکه بمنظور وارد شدن و اجرای فرمانهایی در یک کامپیوتر دیگر است. به این منظور ایجاد شد تا یک جایگزین رمزشده امن برای دسترسی‌های ناامن به کامپیوترهای دیگر مثلا rlogin یا telnet باشد. نسخه بعدی این پروتکل تحت نام SSH2 با قابلیتهایی برای انتقال فایل رمزشده از طریق لینک‌های SSH منتشر شد.

SSH می تواند برای پشتیبانی انتقال فایل رمزشده (به شکل SFTP) استفاده شود اما طبیعت خط فرمان بودن آن به این معنی است که بیشتر توسط مدیران سیستمها برای ارسال درون سازمان استفاده می‌شود تا برای انتقال فایل تجاری. بعلاوه استفاده از SSH نیاز به نرم‌افزار یا سیستم عاملهای سازگار با SSH در دو طرف اتصال دارد، که به این ترتیب SSH برای سروربه‌سرور انجام می‌گیرد.

**تشخیص نفوذ (Intrusion Detection)**

تشخیص نفوذ عبارت است از پردازه تشخیص تلاشهایی که جهت دسترسی غیرمجاز به یک شبکه یا کاهش کارایی آن انجام می شوند.در تشخیص نفوذ باید ابتدا درک صحیحی از چگونگی انجام حملات پیدا کرد. سپس بنابر درک بدست آمده، روشی دو مرحله ای را برای متوقف کردن حملات برگزید. اول این که مطمئن شوید که الگوی عمومی فعالیتهای خطرناک تشخیص داده شده است. دوم این که اطمینان حاصل کنید که با حوادث مشخصی که در طبقه بندی مشترک حملات نمی گنجند، به سرعت رفتار می شود.به همین دلیل است که بیشتر سیستم های تشخیص نفوذ (IDS) بر مکانیزمهایی جهت بروزرسانی نرم افزارشان متکی هستند که جهت جلوگیری از تهدیدات شبکه به اندازه کافی سریع هستند. البته تشخیص نفوذ به تنهایی کافی نیست و باید مسیر حمله را تا هکر دنبال کرد تا بتوان به شیوه مناسبی با وی نیز برخورد کرد.

**انواع حملات شبکه ای با توجه به طریقه حمله**

یک نفوذ به شبکه معمولا یک حمله قلمداد می شود. حملات شبکه ای را می توان بسته به چگونگی انجام آن به دو گروه اصلی تقسیم کرد. یک حمله شبکه ای را می توان با هدف نفوذگر از حمله توصیف و مشخص کرد. این اهداف معمولا از کار انداختن سرویس (DoS یا Denial of Service) یا دسترسی غیرمجاز به منابع شبکه است.

### 1- حملات از کار انداختن سرویس

در این نوع حملات ، هکر استفاده از سرویس ارائه شده توسط ارائه کننده خدمات برای کاربرانش را مختل می کند. در این حملات حجم بالایی از درخواست ارائه خدمات به سرور فرستاده می شود تا امکان خدمات رسانی را از آن بگیرد. در واقع سرور به پاسخگویی به درخواستهای بی شمار هکر مشغول می شود و از پاسخگویی به کاربران واقعی باز می ماند.

### 2- حملات دسترسی به شبکه

در این نوع از حملات، نفوذگر امکان دسترسی غیرمجاز به منابع شبکه را پیدا می کند و از این امکان برای انجام فعالیتهای غیرمجاز و حتی غیرقانونی استفاده می کند. برای مثال از شبکه به عنوان مبدا حملات DOS خود استفاده می کند تا درصورت شناسایی مبدا، خود گرفتار نشود. دسترسی به شبکه را می توان به دو گروه تقسیم کرد.

الف– دسترسی به داده : در این نوع دسترسی ، نفوذگر به داده موجود بر روی اجزاء شبکه دسترسی غیرمجاز پیدا می کند. حمله کننده می تواند یک کاربر داخلی یا یک فرد خارج از مجموعه باشد. داده های ممتاز و مهم معمولا تنها در اختیار بعضی کاربران شبکه قرار می گیرد و سایرین حق دسترسی به آنها را ندارند. در واقع سایرین امتیاز کافی را جهت دسترسی به اطلاعات محرمانه ندارند، اما می توان با افزایش امتیاز به شکل غیر مجاز به اطلاعات محرمانه دسترسی پیدا کرد. این روش به تعدیل امتیاز یا Privilege Escalation مشهور است.

ب- دسترسی به سیستم : این نوع حمله خطرناکتر و بدتر است و طی آن حمله کننده به منابع سیستم و دستگاهها دسترسی پیدا می کند. این دسترسی می تواند شامل اجرای برنامه ها بر روی سیستم و به کار گیری منابع آن در جهت اجرای دستورات حمله کننده باشد. همچنین حمله کننده می تواند به تجهیزات شبکه مانند دوربینها ، پرینترها و وسایل ذخیره سازی دسترسی پیدا کند. حملات اسب تروا ها ، Brute Force و یا استفاده از ابزارهایی جهت تشخیص نقاط ضعف یک نرم افزار نصب شده بر روی سیستم از جمله نمونه های قابل ذکر از این نوع حملات هستند.

فعالیت مهمی که معمولا پیش از حملات DoS و دسترسی به شبکه انجام می شود، شناسایی یا reconnaissance است. یک حمله کننده از این فاز جهتی افتن حفره های امنیتی و نقاط ضعف شبکه استفاده می کند. این کار می تواند به کمک بعضی ابزارها آماده انجام پذیرد که به بررسی پورتهای رایانه های موجود بر روی شبکه می پردازند و آمادگی آنها را جهت انجام حملات مختلف بر روی آنها بررسی می کنند.

**انواع حملات شبکه ای با توجه به حمله کننده**

حملات شبکه ای را می توان با توجه به حمله کننده به چهار گروه تقسیم کرد :

1- حملات انجام شده توسط کاربر مورد اعتماد (داخلی) : این حمله یکی از مهمترین و خطرناکترین نوع حملات است، چون از یک طرف کاربر به منابع مختلف شبکه دسترسی دارد و از طرف دیگر سیاستهای امنیتی معمولا محدودیتهای کافی درباره این کاربران اعمال نمی کنند.

2- حملات انجام شده توسط افراد غیر معتمد (خارجی) : این معمولترین نوع حمله است که یک کاربر خارجی که مورد اعتماد نیست شبکه را مورد حمله قرار می دهد. این افراد معمولا سخت ترین راه را پیش رو دارند زیرا بیشتر سیاستهای امنیتی درباره این افراد تنظیم شده اند

3- حملات انجام شده توسط هکرهای بی تجربه : بسیاری از ابزارهای حمله و نفوذ بر روی اینترنت وجود دارند. در واقع بسیاری از افراد می توانند بدون تجربه خاصی و تنها با استفاده از ابزارهای آماده برای شبکه ایجاد مشکل کنند.

4- حملات انجام شده توسط کاربران مجرب : هکرهای با تجربه و حرفه ای در نوشتن انواع کدهای خطرناک متبحرند. آنها از شبکه و پروتکلهای آن و همچنین از انواع سیستم های عمل آگاهی کامل دارند. معمولا این افراد ابزارهایی تولید می کنند که توسط گروه اول به کار گرفته می شوند. آنها معمولا پیش از هر حمله ، آگاهی کافی درباره قربانی خود کسب می کنند.

**پردازه تشخیص نفوذ**

تا بحال با انواع حملات آشنا شدیم. حال باید چگونگی شناسایی حملات و جلوگیری از آنها را بشناسیم. امروزه دو روش اصلی برای تشخیص نفوذ به شبکه ها مورد استفاده قرار می گیرد:

1- IDS مبتنی بر خلاف قاعده آماری

2- IDS مبتنی بر امضا یا تطبیق الگو

روش اول مبتنی بر تعیین آستانه انواع فعالیتها بر روی شبکه است، مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان (host) اجرا می شود.لذا در صورت بروز یک نفوذ امکان تشخیص آن به علت خلاف معمول بودن آن وجود دارد. اما بسیاری از حملات به گونه ای هستند که نمی توان براحتی و با کمک این روش آنها را تشخیص داد.

در واقع روشی که در بیشتر سیستمهای موفق تشخیص نفوذ به کار گرفته می شود، IDS مبتنی بر امضا یا تطبیق الگو است.منظور از امضا مجموعه قواعدی است که یک حمله در حال انجام را تشخیص می دهد. دستگاهی که قرار است نفوذ را تشخیص دهد با مجموعه ای از قواعد بارگذاری می شود.هر امضا دارای اطلاعاتی است که نشان می دهد در داده های در حال عبور باید به دنبال چه فعالیتهایی گشت. هرگاه ترافیک در حال عبور با الگوی موجود در امضا تطبیق کند، پیغام اخطار تولید می شود و مدیر شبکه را از وقوع یک نفوذ آگاه می کند. در

بسیاری از موارد IDS علاوه بر آگاه کردن مدیر شبکه، اتصال با هکر را بازآغازی می کند و یا با کمک یک فایروال و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله می کند.

اما بهترین روش برای تشخیص نفوذ ، استفاده از ترکیبی از دو روش فوق است. در مجموع استفاده ترکیبی از نرم افزار و سخت افزار با توجه به اهمیت اطلاعات و هزینه های ایجاد امنیت، توصیه میگردد