

ویژگی ها و کارکردهای نگهبانان سیستم های اطلاعاتی رایانه ها

فایروال ها، نگهبانان محله

[وحدت نقشینه]

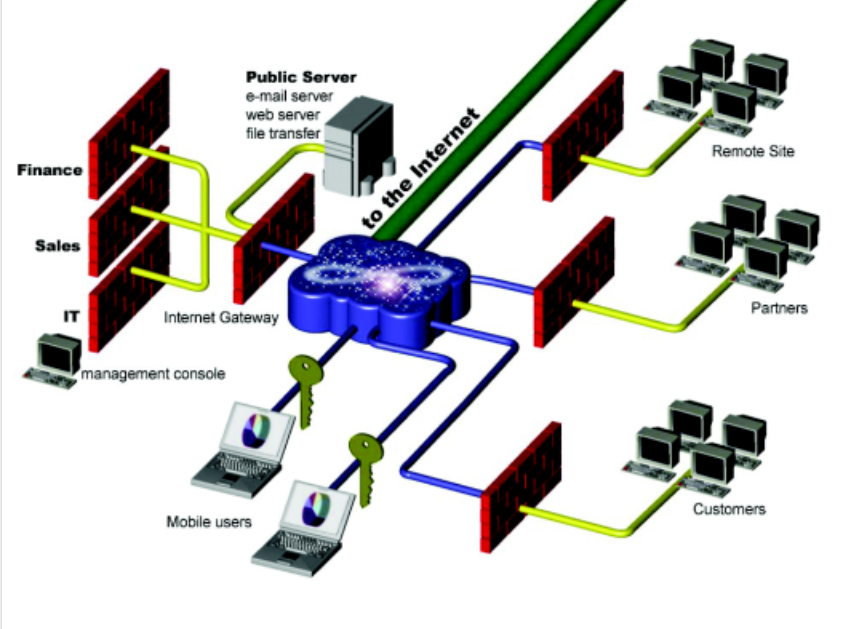
اگر قرار باشد از ساختمان و وسایل داخل آن محافظت به عمل آید نخستین کاری که به ذهن هر کسی خطور می کند، کنترل راه های ورود و خروج به ساختمان است و در این کنترل تنها به افراد خاصی که برای نگهبان شناخته شده هستند و افراد شناسایی قرار می گیرند اجازه ورود داده می شود به علاوه اگر فردی از ساختمان خارج شود بسته به کیفیت هایی که به همراه دارد مورد بازرسی قرار می گیرد تا از لوازم و تجهیزات ساختمان چیزی را به سرقت نبرد باشد. ملاک ورود و خروج افراد نیز چارچوب و مقررات عمومی و قابل سازماندهی از پیش تعیین شده است تا از ورود افراد ناشناس محافظت به عمل آید. همین مکانیزم های امنیتی را باید در شبکه های رایانه ای نیز کنترل کرد تا امیدا افراد و یا اطلاعاتی که آلوده هستند وارد سیستم و خصوصاً شبکه شده و امنیت اطلاعات قبلی را به خطر بیندازند. به همین منظور باید خود تماس دارد تحت نظر و کنترل درآورد و اجازه ورود بسته های مشکوک را صادر نکند. نگهبان این مرزها در سیستم های رایانه ای Fire wall می نامند که مسئولیت خطیر حفظ صحت و سلامت اطلاعات شما را بر عهده دارد البته در صورتی که Fire wall را فعال کرده و آن مدیریت کنید.

تاریخچه
هکرها و دزدان امنیت هر ساله خسارت بسیار سنگینی را به شرکت های تجاری و مالی و افراد وارد می کنند، امروزه هکرها می توانند بسیار خطرناک تر از یک تروریست به فعالیت خود ادامه دهند، همین اهمیت و نفوذهای مداوم هکرها به سیستم های رایانه ای موجب شد که بسیاری از شرکت های نرم افزاری که مشغول فعالیت در حوزه های امنیتی هستند، دست به تولید نرم افزارهای فایروال برای جلوگیری از نفوذ هکرها بزنند. این نرم افزارها و نرم افزارهای مشابه (Fire wall)، می نامند که در گردن این سد ها و عبور از آن برای زدن دنیای دیجیتال دربردارنده است. البته این نرم افزارها نیز همگی دارای درجه ای از ریسک هستند.

روش کار
Fire wall را می توان برنامته دانست - البته نوع سخت افزاری آن وجود دارد - که وظیفه اش فیلتر کردن بسته های اطلاعاتی ورودی به سیستم است که در صورت تشخیص مغایرت در اطلاعات و دردی به سیستم آنچه که در برنامه مشخص شده است اجازه ورود را صادر نکرده و بسته اطلاعاتی را در مبدأ روگردانی می دارد تا مجوز لازم برای وارد شدن آن وجود داشته باشد. دوره آتش (Fire wall) سیستمی است که بین کاربران شبکه های محلی و شبکه بیرونی قرار گرفته و ضمن نظارت بر دسترسی ها، کلیه مراحا را کنترل و خروج اطلاعات را تحت نظر قرار می دهد.

بسته های اطلاعاتی ارسال از سوی کاربران خارجی و پس از ورود به شبکه ابتدا وارد دیواره آتش می شوند و در این مکان منتظر هستند تا به طبق استاندارد ها و ملاک های امنیتی از پیش تعیین شده منقبذ گیری برای ورود و یا عدم ورود صادر شود. سه تان برای خروج اطلاعات از دیواره آتش نظر گرفته شده است:

- ۱- اجازه عبور داده نمی شود
- ۲- اجازه عبور داده نمی شود و همزمان پیام نیز از مبدأ
- ۳- اجازه عبور داده نمی شود و دریافتی در ارتباطات اینترنتی



۱- کنترل و نظارت بر شبکه های محلی
۲- ثبت همه فعالیت ها و ارائه گزارش های درخواستی مدیر شبکه
۳- شناسایی حملات انجام شده به شبکه
۴- حفاظت از شبکه در مقابل هکرها
۵- بسته نگاه داشتن پورت های بلااستفاده در شبکه برای جلوگیری از سوءاستفاده های احتمالی
۶- دیواره های آتش هوشمند
۷- امروزه حملات هکرها بسیار هوشمندانه صورت می گیرد به گونه ای که دیگر دیواره های آتش معمولی و شناخته شده توانایی مقابله با آنها را ندارند و لذا باید به سراغ دیواره های آتش و فیلترهای هوشمند رفت، باتوجه به این که دیواره های آتش را استفاده از حذف بسته ها و بستن پورت های حساس شبکه را محافظت می کند و به علاوه دیواره های آتش بخشی از ترافیک بسته ها را به داخل شبکه منتقل می نمایند، هکرها می توانند با

کنترل و نظارت بر شبکه های محلی
ثبت همه فعالیت ها و ارائه گزارش های درخواستی مدیر شبکه
شناسایی حملات انجام شده به شبکه
حفاظت از شبکه در مقابل هکرها
بسته نگاه داشتن پورت های بلااستفاده در شبکه برای جلوگیری از سوءاستفاده های احتمالی
دیواره های آتش هوشمند
امروزه حملات هکرها بسیار هوشمندانه صورت می گیرد به گونه ای که دیگر دیواره های آتش معمولی و شناخته شده توانایی مقابله با آنها را ندارند و لذا باید به سراغ دیواره های آتش و فیلترهای هوشمند رفت، باتوجه به این که دیواره های آتش را استفاده از حذف بسته ها و بستن پورت های حساس شبکه را محافظت می کند و به علاوه دیواره های آتش بخشی از ترافیک بسته ها را به داخل شبکه منتقل می نمایند، هکرها می توانند با

مینی برعد اجازه ورود صادر می شود.
دیواره آتش دقیقاً مانند ایستگاه ایست - بازرسی مستقر در جاده های عمل می کند و مانند همین ایستگاه ها وقت گیر و اعصاب خردکن نیز هست و همواره به عنوان گلوگاهی در شبکه های رایانه ای شناخته می شود و بسیار آفرایش ترافیک، تأخیر و ازدحام در شبکه رایانه ای خواهد شد. به علاوه با توجه به این که معماری شبکه به صورت لایه، لایه است، همه بسته ها باید از چهار لایه فیلترهای شبکه، انتقال و کاربردی عبور کنند و لذا باید همه لایه های شبکه مورد بررسی و سحت و چو قرار داد تا امیدا در لایه های زیرین بسته های بیخطر عبور کنند. در بین لایه های چهارگانه فوق پیشترین اهمیت در لایه های شبکه، انتقال و کاربرد یافته است.

ویژگی های دیواره آتش
۱- کنترل قابل های مشکوک
۲- کنترل بسته های ارسالی و دریافتی در ارتباطات اینترنتی

هکرها می توانند با ارسال بسته های مضموعی اما مجاز و قابل نفوذ پورت های باز شبکه را شناسایی کرده و راه نفوذ خود به شبکه را پیدا کنند

از ارتباط را برقرار می کند:
۱- ارتباط بین پروکسی و مقصد
۲- ارتباط بین پروکسی و مبدأ.
این دسته از دیواره های آتش نیاز به حافظه بالا و به cpu سرعیمی دارند، زیرا در صورت اختلال در Fire wall اختلال کلی شبکه را می توان شاهد بود.

● چند نمونه
به توجه به فراوانی و تنوع دیواره های آتش موجود در بازارهای جهانی و داخلی نمودار از بهترین دیواره های آتش را مورد بررسی قرار می دهیم:

۱- Mcafee internet security
شاید نام شرکت مک اف ای در یاد تمام افراد آفرزهای ضدویروس این شرکت بیندازد اما امروزه محصولات دیگری مانند فایروال ها، نرم افزارهای امنیت شبکه، نرم افزارهای حفاظتی شبکه های بیسیم و غیره در زمره تولیدات این شرکت قرار دارد. نرم افزار Mcafee internet security نسبت به دیواره های آتشی مانند Zone Alarm و pc-cillin سرعت پایینتری دارد اما در تست های که توسط DSL Reports انجام شده است این نرم افزار توانایی جلوگیری از برنامه های نفوذ به شبکه را به خوبی دارا می باشد. در نسخه های جدیدتر این نرم افزار با بهره گیری از بانک اطلاعاتی جامع ای ادیتور site که در آن آدرس سایت هایی که می تواند برای رایانه شما مشکل ساز شود جمع آوری شده است، امنیت بیشتری در اختیار شما قرار می گیرد و به علاوه plug in های جدیدی برای هر دو مرورگر Firefox و IE در آتش در آتش پیش بینی شده است.

۲- Microsoft window Firewall
این فایروال که محصول شرکت معروف مایکروسافت است بسیار محدودتر از سایر فایروال ها عمل می کند و در حقیقت تنها به عنوان یک Internet connection Firewall وارد عمل می شود و لذا چندان قدرتی در مقابله با کرمهای دیربخت و با هکرها ندارد. در سال های اخیر کرم های چون sasser و Microsoft windows firewall از این ضعف آفرزهای ضدویروس درون رایانه ها نفوذ پیدا کردند. با استفاده از تست هایی که توسط DSL Reports صورت گرفته است فایروال ویندوز در مورد تهدیدات بیرون از شبکه و آتش های حیوی از خود نشان می داد اما در مقابل تهدیدات داخلی شبکه فاقد عکس العمل های لازم بود. از توانمندی های دیگری که می توان در این فایروال مشاهده کرد توانایی تنظیم یکپسندی آن مطابق با شبکه های رایج است. اما باید این نکته توجه کرد که به دلیل محدودیت های زیادی که Microsoft windows firewall دارد در نباید انتظار عملکردی مشابه قبلی فایروال کامل را از آن انتظار داشت.

ارسال بسته های مضموعی اما مجاز و قابل نفوذ پورت های باز شناسایی کرده و راه نفوذ خود به شبکه را پیدا کنند. برای جلوگیری از بروز چنین مشکلاتی باید تنها به بسته های اجازه عبور داده شود که با درخواست قبلی ارسال شده باشد. دیواره های آتش هوشمند با توجه به هوشمند بودنشان توانایی این تشخیص و رهگیری را دارند و در صورتی که اطلاعات ارسالی با اطلاعات درخواستی یکسان نباشد، هیچ گونه اجازه ورود داده نمی شود.

۳- دیواره های آتش مبتنی بر پروکسی
این دیواره های آتش پس از ایجاد ارتباط با طرفین معامله فعالیت خود را آغاز می کند و به عنوان واسطه ای بین رایانه شبکه محلی و رایانه شبکه خارجی ارتباطی غیرمستقیم صورت می دهد و پس از مقیم شدن در لایه مورد وارد عمل می شود و لذا می تواند بر داده های ارسالی و دریافتی نظارت داشته باشد، این دیواره های آتش نوع

۳- کنترل بسته های ارسالی و دریافتی در ارتباطات اینترنتی

وب گرد

یک نوجوان ۱۸ ساله نیوزیلندی رهبر گروه بین المللی مجرمان اینترنتی بازداشت شد

این گروه به پیش از یک میلیون رایانه و کسب میلیون ها دلار از حساب های بانکی قربانیان خود متمم است.
این نوجوان ۱۸ ساله که نامش به دلیل قانونی فاش نشد در یکی از مبارزه پلیس آمریکا با مجرمان اینترنتی که بخشی های رایانه ای آلوده موسوم به بوت نت را اداره می کنند، بازداشت شد.
این نوجوان پس از بازجویی بدون داشتن اتهامی آزاد شد، اما پلیس نیوزیلند اعلام کرد که تحقیقات از وی همچنان ادامه خواهد داشت.
طبق گزارش پلیس آمریکا ۱/۳ میلیون رایانه تحت کنترل این نوجوان بوده و بیش از ۲۵ میلیون دلار به نظر غیرقانونی توسط وی سرقت شده است، جاسکر مجازات اتهاماتی که وی با آنها روبروست ۱۰ سال زندان است.
براساس گزارش، بوت نت برای بار اول ارتکاب جرائم مختلفی مانند سرقت اطلاعات شخصی از رزمندگان، زنده هرزنامه کلاهبرداری برای ارسال اطلاعات ریخته وی وب سایت ها به منظور از کار انداختن آنها مورد استفاده قرار می گیرد.

نیم میلیون مالکدو از نسخه پتای مورگر فایرفاکس ۳

بنیاد مؤسسه اطلاع راکر مورگر در صفحات و Beta1 Firefox در مدت دو هفته بیش از ۵۰۰ هزار بار دانلود شده است.
این گزارش اضافه می کند تا عزم نسخه نهایی فایرفاکس ۳ در سال آینده، دو نسخه پتای دیگر نیز در اختیار کاربران قرار خواهد گرفت. بدین ترتیب، نسخه پتای Beta2 Firefox که در پایان سال میلادی و نسخه ۲ تا نیز در اوایل سال ۲۰۰۸ عرضه خواهد شد.
با به گفته تیم توسعه فایرفاکس، تا امروز ۴۲۹ هزار همی از این نسخه پتای فایرفاکس ۳ دانلود شده است که معادل هزار بار از این فعالیت مالکدو مستخدم کاربرانی است که در تست این مرورگر مشارکت دارند. دو نسخه پتای دیگر فایرفاکس ۳ ویژگی های

براساس این گزارش برنامه های مسنجر دیگر موجود در بازار نیز برای گردآوری فهرست سیاه هرزنامه نویسان برنامه پیام رسانی عمومی به منظور مسدود کردن آنها از ابزارهای گزارش دهد استفاده می کنند. به گزارش منابع خبری تردیسک به مایکروسافت، این کمپانی قصد دارد دو طی هفته های آینده نسخه انتخابی اول (Release Candidate) از اسپیک وی ویندوز ویستا را جهت بررسی در اختیار تعداد اندکی از آزمایش کنندگان محصولات خود قرار دهد. این منابع خبری اضافه می کنند، پس از آن در گام بعدی و در دو سیمین هفته از ماه دسامبر، مایکروسافت با انتخاب یک شماره برجسته برای SP1 RC آن را در اختیار عموم کاربران علاقه مند قرار می دهد. هم اکنون این شرکت به صورت داخلی در حال آزمایش RC نسخه SP1 است.

مایکروسافت اعلام کرده است قصد دارد نگارش نهایی اسپیک وی نخست ویندوز ویستا را طی چهار ماه اول سال ۲۰۰۸ میلادی منتشر نماید. پیش از این یک نسخه پیش نمایشی از SP1 RC در اختیار بازار هزانه نظر از آزمایش کنندگان قرار گرفته بود.

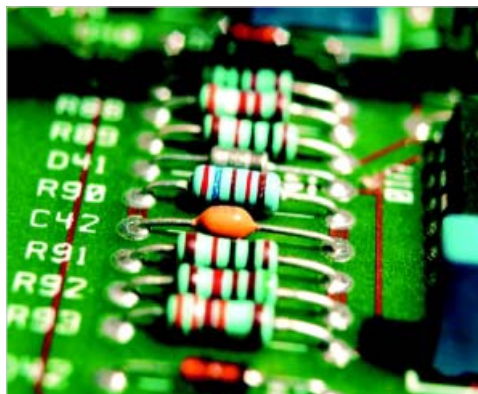
ثبت رکورد خرید اینترنتی ۷۳۳ میلیون دلاری در یک روز

خریداران آنلاین در آمریکا صرف ۷۳۳ میلیون دلاری برای خرید یک روز، رکورد بر جای گذاشتند. طبق اعلام شرکت آمازون تحقیقات اینترنتی کام اسکالر، این آمار با ۲۱ درصد افزایش نسبت به روز مشابه (دوشنبه سابق) در سال گذشته، بیشترین هزینه ای است که خریداران آمریکایی برای خرید از اینترنت صرف کرده اند. خریداران آنلاین آمریکایی از اول ماه دسامبر تاکنون برای نقل محصولات ۱۰/۷ میلیارد دلار صرف کرده اند که ۱۷ درصد نسبت به مدت مشابه در سال قبل بیشتر است.
دوشنبه سابق، اولین دوشنبه بعد از تعطیلات جشن خریدگرزای در آمریکا است که مردم به سر کارهای خود حاضر می شوند و به خرید آنلاین می پردازند.
براساس این گزارش فروشگاه های اینترنتی تلاش کردند در این روز با سخوی تقاضای خریداران باشند؛ هر چند به گفته تحلیلگران ۱۰ سایت از ۳۰ سایت فروشن بزرگ به کنده کلیه توجیه دچار شدند.

بین المللی دانشگاه های جهان است، دیجیتالی کردن ۱/۵ میلیون کتاب به صورت آنلاین تکمیل شد.
این پروژه با همکاری دانشگاه های کارنگی ملون در آمریکا، زی جانگ در چین، مؤسسه هنری علوم و هنر و کتابخانه اسکندریه در مصر انجام می گیرد.
براساس این گزارش از زمان آغاز این پروژه در سال ۲۰۰۲، برای نخستین بار است که تمام کتاب ها از طریق پورتال وب و واحد یونیورسالی لایبری به نشانی www.ulib.org در دسترس قرار می گیرند.
با وجودی که گوگل، مایکروسافت و شرکت اینترنت آرشو، همگی طرح های بزرگ دیجیتالی کردن کتاب را راه اندازی کرده، نزدیک به یک میلیون بوک، بزرگترین کتابخانه دیجیتالی دانشگاهی جهان است که کتاب های آن به صورت رایگان در دسترس قرار دارند. دست کم تیمی از کتاب های این کتابخانه فاقد کسی رایت بوده و یا با اجازه دارند کسی رایت، دیجیتالی شده اند. کتاب های دیجیتالی شده به بیست زبان دنیا هستند و مسئولان این پروژه برای توسعه آن به نام کشورها و زبان ها تلاش می کنند.

نسخه آزمایشی ویندوز لایو مسنجر مایکروسافت منتشر شد

نسخه جدید برنامه پیام رسانی فوری مایکروسافت (Windows Live Messenger) دارای ویژگی امنیتی جدید خواهد بود که به کاربران گزارش می کند چه کسی پیام های ناخواسته مصرف می کند. SPIM هرزنامه بر روی مسنجر را ارسال کرده است. این ویژگی امنیتی یکی از خصوصیات متعدد و جدید ویندوز لایو مسنجر ۹.۰ است که از هفته گذشته در اختیار آزمایش کنندگان خصوصی این نسخه قرار گرفت. براساس این گزارش SPIM علاوه بر آزار دهنده بودن، خطرناک است زیرا یک هکر ممکن است جزئیات کتاب مسنجر یک کاربر را به دست آورد. کارها را انجام دهند، وجود نداشته.
با کاربرد این نرم افزار یک بات ماهر با توانایی برداشتن شباهتی جدید که قبلاً برای برداشتن نرم برنامه ریزی نشده، می تواند برای انجام وظایف خانگی پیچیده مانند غذا دادن به حیوانات یا پر کردن ماشین ظرفشویی مفید باشد.
سختگیر پس از گردآوری فهرست تماس های ماسکر تراش می کند کاربرد برای کلیک بر روی لینک ها فریب دهند و کلیک بر روی این لینک ها، نصب ناخواسته جاسوس افزار را بر نرم افزارهای مغرب دیگر را از طریق اسپیک پدیری مرورگرها حفره های امنیتی دیگر آغاز می کند.



خطر مواجه شدن با محتوای خشنونت آمیز با غیر اخلاقی وب را جست و جو کند.
سایت www.fraginn.com مجموعه ای از بازی ها، اطلاعات و لینک های مربوط به سایت های مناسب و ویژه برای کودکان را عرضه می کند. صدراعظم اطلاع اظهار کرد: این سایت به کودکان اجازه می دهد با امنیت کامل وارد دنیای آنلاین شوند. براساس این گزارش دولت آلمان در حدود ۱/۵ میلیون بوک از بودجه این سایت تأمین کرده و این سایت را با همکاری مشترک شرکت های بزرگ مانند AOL، مایکروسافت، گوگل، لینکس، و دافون و داچ نتکار راه اندازی کرده است.
طراحی نرم افزاری که هوشمندی ربات ها را افزایش می دهد
محققان در دانشگاه استنفورد نرم افزاری را طراحی کرده که به ربات یاد می دهد چگونه شباهتی را که هرگز با آن رو به رو نشده، بردارد. نرم افزار ربات