نرم‌افزار Nessus، و نسخه‌ی تحت Windows آن یعنی NeWT، با توجه به بازه‌ی نستباً وسیعی از سرویس‌ها و جوانب امنیتی که مد نظر قرار داده است، یکی از قوی‌ترین نرم‌افزارها در میان ابزارهای مشابه است. از آن‌جاکه رایگان بودن و راحتی استفاده از آن، به همراه گزارش نسبتاً مفصل و جامع پس از پویش، به جذابیت‌های آن افزوده است، یکی از ابزارهای مناسب برای کاربران مبتدی، متوسط و حتی پیشرفته محسوب شده و استفاده از آن به همه توصیه می‌گردد.

Snort، نمونه‌ای از یک ابزار تشخیص نفوذ شبکه‌ای

یک نرم‌افزار تشخیص نفوذ به‌صورت کدباز است که بر روی محیط‌های Linux و Windows عرضه می‌گردد و با توجه به رایگان بودن آن، به یکی از متداول‌ترین سیستم‌های تشخیص نفوذ شبکه‌های رایانه‌یی مبدل شده است. از آن‌جاکه برای معرفی آن نیاز به معرفی کوتاه این دسته از ابزارها داریم، ابتدا به مفاهیمی اولیه درباره‌ی ابزارهای تشخیص نفوذ می‌پردازیم، به عبارت دیگر معرفی این نرم‌افزار بهانه‌یی است برای ذکر مقدمه‌یی در باب سیستم‌های تشخیص نفوذ.

Intrusion Detection System (IDS) یا سیستم تشخیص نفوذ به سخت‌افزار، نرم‌افزار یا تلفیقی از هر دو اطلاق می‌گردد که در یک سیستم رایانه‌یی که می‌تواند یک شبکه‌ی محلی یا گسترده باشد، وظیفه‌ی شناسایی تلاش‌هایی که برای حمله به شبکه صورت می‌گیرد و ایجاد اخطار احتمالی متعاقب حملات، را بر عهده دارد.

IDSها عملاً سه وظیفه‌ی کلی را برعهده دارند: پایش، تشخیص، واکنش. هرچند که واکنش در مورد IDSها عموماً به ایجاد اخطار، در قالب‌های مختلف، محدود می‌گردد. هرچند دسته‌یی مشابه از ابزارهای امنیتی به نام Intrusion Prevention System (IPS) وجود دارند که پس از پایش و تشخیص، بسته‌های حمله‌های احتمالی را حذف می‌کنند. نکته‌یی که در این میان باید متذکر شد، تفاوت و تقابل میان Firewallها و IDSها است. از آن‌جاکه ماهیت عمل‌کرد این دو ابزار با یکدیگر به کلی متفاوت است، هیچ‌یک از این دو ابزار وظیفه‌ی دیگری را به طور کامل برعهده نمی‌گیرد، لذا تلفیقی از استفاده از هردو ابزار می‌تواند امنیت کلی سیستم را بالا ببرد.

در حالت کلی IDSها را می‌توان به دو دسته‌ی کلی تقسیم‌بندی نمود :

- Network IDS (NIDS)
- Host IDS (HIDS)

HIDSها، اولین سیستم IDSی هستند که در یک سیستم رایانه‌ای باید پیاده‌سازی شود. معیار تشخیص حملات در این سیستم‌ها، اطلاعات جمع‌آوری شده بر روی خادم‌های مختلف شبکه است. برای مثال این سیستم با تحلیل صورت عملیات انجام شده، ذخیره شده در پرونده‌هایی خاص، سعی در تشخیص تلاش‌هایی که برای نفوذ به خادم مذکورد انجام شده است دارد. این تحلیل‌ها می‌تواند به صورت محلی بر روی خود خادم انجام گردد یا به سیستم تحلیل‌گر دیگری برای بررسی ارسال شود. یک **HIDS** می‌تواند تحلیل اطلاعات بیش از یک خادم را بر عهده بگیرد.

با این وجود، اگر نفوذگر جمع‌آوری صورت عملیات انجام‌شده بر روی هریک از خادم‌های مورد نظر را به نحوی متوقف کند، HIDS در تشخیص نفوذ ناموفق خواهد بود و این بزرگ‌ترین ضعف HIDS است.

NIDSها، به عنوان دومین نوع IDSها، در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته‌ها و پروتکل‌های ارتباطات فعال، به جستجوی تلاش‌هایی که برای حمله صورت می‌گیرد می‌پردازند. به عبارت دیگر معیار NIDSها، تنها بسته‌هایی است که بر روی شبکه‌ها رد و بدل می‌گردد. از آن‌جایی‌که NIDSها تشخیص را به یک سیستم منفرد محدود نمی‌کنند، عملاً گسترده‌گی بیش‌تری داشته و فرایند تشخیص را به صورت توزیع‌شده انجام می‌دهند. با این وجود این سیستم‌ها در رویایی با بسته‌های رمزشده و یا شبکه‌هایی با سرعت و ترافیک بالا کارایی خود را از دست می‌دهند.

با معرفی انجام شده در مورد دو نوع اصلی IDSها و ضعف‌های عنوان شده برای هریک، واضح است که برای رسیدن به یک سیستم تشخیص نفوذ کامل، بهترین راه استفاده‌ی همزمان از هر دو نوع این ابزارهاست.

Snort، در کامل‌ترین حالت نمونه‌یی از یک NIDS است. این نرم‌افزار در سه حالت قابل برنامه‌ریزی می‌باشد :

- حالت **Sniffer**

در این حالت، این نرم‌افزار تنها یک Sniffer ساده است و محتوای بسته‌های ردوبدل شده بر روی شبکه را بر روی کنسول نمایش می‌دهد.

- حالت ثبت‌کننده‌ی بسته‌ها

Snortدر این وضعیت، اطلاعات بسته‌های شبکه را در پرونده‌یی که مشخص می‌شود ذخیره می‌کند.

- سیستم تشخیص نفوذ

در این پیکربندی، بر اساس دو قابلیت پیشین و با استفاده از قابلیت تحلیل بسته‌ها و قوانینی که تعیین می‌گردد، Snort امکان پایش و تحلیل بسته و تشخیص نفوذ را یافته و در صورت نیاز واکنش تعیین شده را به‌روز می‌دهد.

حالت پیش‌فرض خروجی این ابزار فایلی متنی است که می‌تواند در آن ابتدای بسته‌ها را نیز درج کند. با این وجود در صورتی‌که این ابزار در حال فعالیت بر روی ارتباطات شبکه‌یی با سرعت بالا می‌باشد به‌ترین راه استفاده از خروجی خام باینری و استفاده از ابزاری ثانویه برای تحلیل و تبدیل اطلاعات خروجی است.

بُعد دیگر از پیکربندی Snort به عنوان یک سیستم تشخیص نفوذ، استفاده از قوانین برای ایجاد معیار نفوذ برای Snort است. برای مثال می‌توان با قانونی، Snort را مکلف

ساخت که نسبت به دسترسی‌های انجام شده مبتنی بر پروتکلی تعیین شده از/ به یک پورت خاص و از/ به یک مقصد معین با محتوایی شامل رشته‌یی خاص، اخطاری یا واکنشی ویژه را اعمال کند.

نکته‌یی که باید در نظر داشت این است که از آن‌جاکه Snort را می‌توان به گونه‌یی پیکربندی نمود که قابلیت تشخیص حمله توسط ابزارهای پویش پورت را نیز داشته باشد، لذا با وجود استفاده از Snort نیازی به استفاده از ابزاری ثانویه برای تشخیص پویش‌گرهای پورت وجود ندارد.

همان‌گونه که گفته شد، Snort با قابلیت‌های نسبتاً کاملی که در خود جای داده‌است، به همراه رایگان بودن آن و قابلیت نصب بر روی محیط‌ها و سیستم‌های عامل متدوال، به یکی از معمول‌ترین IDSهای کنونی مبدل شده است. برای دریافت این نرم‌افزار و همچنین اطلاعات جامعی در مورد آن می‌توانید به پایگاه اصلی آن، www.snort.org، مراجعه کنید.

Retina Network Security Scanner

این نرم‌افزار که محصولی از شرکت eEye Digital Security است، کاربردی مشابه Scanner LANGuard Security دارد. از آنجاکه در این پایگاه مقدمه‌یی از نرم‌افزار LANGuard، به عنوان آشنایی با نرم‌افزارهای پویش امنیت در شبکه قرار گرفته است، در این متن ضمن معرفی Retina به مقایسه مختصر و اجمالی میان این دو محصول، که تحت Windows رقبای یکدیگر محسوب می‌شوند، نیز پرداخته خواهد شد.

پویش‌گر امنیت شبکه‌ی Retina، یکی از قوی‌ترین نرم‌افزارها در این دسته از محصولات به شمار می‌آید. امکانات و قابلیت‌های متنوع، به همراه امکان پویش در شبکه‌هایی که از سیستم‌های عامل متنوعی، همچون Windows و خانوادهی Linux و Unix استفاده می‌کنند، و همچنین امکان نصب اصلاحیه‌های امنیتی ویژه ضعف‌های امنیتی یافت شده که به‌صورت خودکار توسط **Retina** انجام می‌گیرد، این نرم‌افزار را به محصولی خاص و قدرتمند تبدیل می‌کند، تا حدی که اغلب مجلات و منابعی که در زمینه‌ی بررسی چنین نرم‌افزارهایی از اعتباری بالا برخوردارند، آن‌را به عنوان محصولی برتر معرفی می‌کنند.

از امکانات ویژه و منحصربه‌فرد این نرم‌افزار، که در دیگر پویش‌گرهای امنیت شبکه‌ی مشابه یافت نمی‌شود، می توان به امکان Auditing آن اشاره کرد. توسط Auditing Tool این نرم‌افزار می‌توان در زمان پویش، دسته‌یی خاص از ضعف‌های امنیتی را برای تعدادی از ایستگاه‌های کاری یا خادم‌های تعیین شده اعمال کرد. همچنین در این ابزار امکان اضافه نمودن ضعفی جدید، به صورت دستی، توسط مدیر شبکه نیز وجود دارد. به عبارت دیگر، می‌توان گزارشی از وضعیت تعدادی رایانه‌ی خاص در برابر ضعف‌هایی معین، تهیه نمود و در صورت نیاز اقدام به نصب خودکار اصلاحیه‌های امنیتی نمود.

این پویش‌گر، با استفاده از بازه‌یی از آدرس‌های IP به پویش شبکه می‌پردازد و ضعف‌های امنیتی را بر اساس بحرانی‌بودن آن‌ها مرتب می‌کند. همان‌گونه که گفته شد می‌توان بررسی امنیتی شبکه را محدود به دسته‌ی خاصی از ضعف‌های، نرم‌افزارها و یا جنبه‌های امنیتی نمود. در این میان شاید تنها ایرادی، آن هم از بعد گزارش‌گیری و رابط کاربری، می‌توان به این نرم‌افزار وارد دانست، نبود امکان مرتب‌سازی ایستگاه‌های پویش‌شده بر اساس نوع سیستم‌عامل آن‌هاست.

در هنگام نصب، پویش‌گر، اقدام به اتصال به پایگاه داده‌ی اصلی شرکت سازنده کرده و به به‌روز سازی ضعف‌های امنیتی شناخته شده می‌پردازد. این اقدام با هدف کاهش احتمال نادیده انگاشتن ضعف‌های نوین امنیتی صورت می‌گیرد.

حفاظ شخصی Zone Alarm

استفاده از حفاظ‌های شخصی، در دنیای کنونی که اغلب حملات امنیتی و ویروس‌ها، کاربران عادی خانه‌گی را هدف قرار داده‌اند، اهمیتی ویژه یافته است.

شرکت ZoneLabs با ارایه‌ی این نرم‌افزار، عملاً خود را در بازار این دسته از نرم‌افزارها مبدل به حریفی بی‌رقیب نموده است. رقبای دیگر این نرم‌افزار محصولات مشابه دیگری از McAfee و Norton هستند.

مهم‌ترین امکانات و قابلیت‌های این نرم‌افزار را می‌توان به‌صورت زیر برشمرد:

- محدود ساختن دسترسی نرم‌افزارهای مختلف بر روی رایانه

این نرم‌افزار قابلیت بررسی وضعیت ارتباط نرم‌افزارهای نصب شده بر روی سیستم با شبکه را داراست. لذا در صورتی‌که نرم‌افزاری ناشناس سعی در تماس به شبکه داشته باشد، می‌توان این دسترسی را محدود ساخت.

- محدودیت بر روی آدرس‌ها، پورت‌ها و پروتکل‌ها

توسط این امکان می‌توان از دسترسی‌هایی که از بیرون از رایانه‌مان صورت می‌گیرد، در قالب آدرس IP، پورت و پروتکل مورد نظر آگاهی یافت و در

صورت نیاز این دسترسی را بست. از سوی دیگر می‌توان آدرس‌ها، پورت‌ها و پروتکل‌هایی که دسترسی از طریق آن‌ها به سیستم مانعی ندارد را مشخص نمود.

- **امکان حفاظت از اطلاعات شخصی**

توسط این امکان، و با پاک کردن Cacheهای مختلف پرونده‌ها، آدرس‌ها، Cookieها و دیگر اطلاعات شخصی حساس مشابه، می‌توان از درز کردن اطلاعات شخصی مهمی از این قبیل به شبکه جلوگیری نمود.

- **سیستم محافظت از سرویس پست الکترونیک**

توسط این امکان، نامه‌های ورودی به سیستم، که احتمال آلوده‌گی آن‌ها وجود دارد را مسدود ساخت. از سوی دیگر در صورت آلوده بودن سیستم به ویروس‌هایی که خود را از طریق ارسال نامه به دریافت‌کننده‌گانی که آدرس آنها در فهرست آدرس برنامه‌ی ارسال پست‌الکترونیک موجود است، منتشر می‌کنند، می‌توان جلو این انتشار را با مسدود ساختن نامه‌های ارسالی گرفت.

- **صدور اخطارهای امنیتی**

جدا از گزارش حملات احتمالی، درصورتی‌که قصد ارسال اطلاعات به شبکه را داشته باشیم، هشدارهای امنیتی از سوی این نرم‌افزار توجه استفاده کننده را به دقت بیشتر در این زمینه جلب می‌کند.

- **تغییر سطح امنیت به صورت خودکار**

در صورت بروز حملات متعدد امنیتی، نرم‌افزار به طور خودکار سطح حفاظت را بالاتر می‌برد. این امکان احتمال دفع حملات را بالا می‌برد.

آخرین نگارش این نرم‌افزار نسخه‌ی ۴ است که کماکان بیشترین اقبال را در میان این دسته از نرم‌افزارها به خود جلب کرده، و بیشترین محبوبیت و کارایی را در میان کاربران عادی یافته است.

مقدمه‌ای بر SSH

SSH که مخفف Secure Shell می‌باشد، به‌طور عمومی به برنامه‌یی اطلاق می‌گردد که برای دسترسی امن به رایانه‌یی از راه دور، برای اجرای فرامین یا انتقال پرونده‌ها، مورد استفاده قرار می‌گیرد. علت اهمیت چنین روش‌هایی، اقدامات معمول نفوذگران در قالب پویش شبکه برای آگاهی از محتوای بسته‌ها، استفاده از IPهای جعلی و سرقت آدرس‌های IP، تهدیدات سرویس‌های DNS و دیگر روش‌های حمله است. عملاً با رمزکردن کانال ارتباطی میان کاربر و خادم، احتمال هریک از این حملات در پی اقدامات نفوذگران به حداقل می‌رسد.

با وجود آن‌که SSH به برنامه‌یی که این وظیفه را بر عهده دارد اطلاق می‌گردد، ولی تمامی این برنامه‌ها از استاندارد واحدی تبعیت می‌کنند. در نگارش جدید آن به نام SSH2، نرم‌افزاری به نام sftp برای برعهده‌گرفتن وظیفه‌ی FTP Clientها نیز وجود دارد. طبق آمارهای تقریبی ارایه شده، قریب به ۲ میلیون کاربر از نسخه‌های مختلف برنامه‌های متنوع SSH تحت سیستم‌های عامل مختلف استفاده می‌کنند.

نکته‌یی که لازم به گفتن است، تفاوت میان پروتکل‌های استفاده شده در SSH1 و SSH2 است. به بیان دیگر این دو استاندارد با یکدیگر سازگاری ندارند. استانداردی که SSH1 بر مبنای آن است را می‌توان از آدرس
http://www.tigerlair.com/ssh/faq/ssh1-draft.txt به‌دست آورد و برای آگاهی از استاندارد SSH2 می‌توانید به آدرس

http://www.ietf.org/ids.by.wg/secsh.html مراجعه کنید. در حال حاضر، پشتیبان این استاندارد IETF است. با این وجود تعداد زیادی از شرکت‌ها نرم‌افزارهایی بر اساس این استاندارد تولید می‌کنند که برخی رایگان و برخی تجاری است.

برای استفاده از SSH، نیاز به سرویس و نرم‌افزاری داریم که در سوی خادم نصب می‌گردد. پس از آن نرم‌افزاری به عنوان مخدوم، کانال ارتباطی را ایجاد کرده و ارتباط امن برقرار می‌گردد. در حال حاضر سرویس‌ها و نرم‌افزارهای مخدوم برای سیستم‌های عامل مختلفی از جمله Windows، Macintosh، خانواده‌ی Unix، PalmOS، OS/2 و سیستم‌های عامل کم استفاده‌یی همچون VMS موجود است.

نکته‌یی که در این میان اهمیتی خاص دارد، مقایسه‌ی میان SSH1 و SSH2 است و اینکه باید از کدام یک از این استانداردها و نرم‌افزارهای مبتنی بر آن‌ها استفاده کرد؟ پاسخ به این سؤال چندان ساده نیست زیرا کماکان نرم‌افزارهای بسیاری وجود دارند که بر مبنای SSH1 هستند و عملاً این استاندارد SSH1 است که برای تمامی سیستم‌های عامل و محیط‌ها توسعه یافته و نرم‌افزارهایی بر مبنای آن تولید شده‌اند. با این وجود عملاً توسعه‌ی SSH1 متوقف شده است و تولیدکننده‌گان نرم‌افزار تنها بر روی SSH2 تمرکز کرده‌اند. از علل این تغییر می‌توان به ضعف‌های امنیتی موجود در ساختار SSH1، امکان حملات شناخته شده‌یی مانند نوع man-in-the-middle در مورد آن و احتمال رخداد حملات پیش‌بینی‌نشده، اشاره کرد.

Windows XP Service Pack 2

هدف اصلی SP2، بهبود امنیت کاربران ویندوز XP است که این کار را با ٤ رویکرد انجام می دهد:

- محافظت بهتر از شبکه
- بهبود حفاظت از حافظه
- ایمن سازی امور مربوط به E-Mail
- امنیت در مرور اینترنت (توسط Internet Explorer)

محافظت از شبکه با فایروال پیشرفت کرده ویندوز است (که قبلا تحت عنوان Internet Firewall Connection وجود داشت) که به صورت پیش فرض فعال می باشد. این فایروال در مراحل اولیه بوت شدن ویندوز، قبل از اینکه Network Stack فعال شود، شروع به کار می کند و نفوذ گر در مراحل اولیه بالا آمدن سیستم هم نمی تواند آن را مورد حمله قرار دهد. همچنین هنگام خاموش شدن سیستم نیز، این فایروال بسیار دیر خاموش می شود و بعد از اینکه لایه های شبکه غیر فعال شدند، این فایروال کار خود را پایان می دهد. این فایروال دارای واسط کاربری قابل قبولی برای مدیریت آن می باشد و قابل مدیریت و اعمال سیاست از سوی مدیر شبکه یا همان Domain Administrator می باشد. همچنین از IPv6 که در این نسخه از ویندوز ارائه شده است نیز پشتیبانی می کند.

RPC که در دو سال گذشته، هدف حملات اصلی کرم های اینترنتی بود نیز در این نسخه از ویندوز بهبود یافته است. آسیب پذیری کمتر، سطوح دسترسی بیشتر و همچنین

امکان استفاده از آن در شبکه های محدود و مدیریت آن برای جلوگیری از حملات خارج از شبکه از بهبودهایی است که در RPC صورت گرفته است.

مدیریت دسترسی بیشتر روی DCOM [3] برای پایین آوردن احتمال حمله از این طریق، از ویژگی های دیگر SP2 است. در این نسخه، تنها مدیران تایید هویت شده حق اتصال و فعال کردن از راه دور اجزا COM را دارند و تنها کاربران تأئید هویت شده می توانند به صورت از راه دور، COMها را صدا(Call) کنند.

ویژگی امنیتی قابل توجه دیگر در SP2، حمایت و پشتیبانی از پردازنده های با تکنولوژی NX است. در این مدل، ویندوز صفحه های حافظه که مربوط به Data هستند را برچسب غیر اجرایی (non-executable) می زند و بدین طریق، از بسیاری از حملات Buffer Overflow که با فرستادن Data به صورت خاص، ویندوز را وادار به اجرای آن می کردند، جلوگیری می شود. شایان ذکر است که در حال حاضر، تنها پردازنده هایی که NX را پشتیبانی می کنند، پردازنده های ٦٤ بیتی AMD K8 و Intel Itanium هستند که مایکروسافت امیدوار است سایر پردازنده های ٣٢ و ٦٤ بیتی به زودی از این تکنولوژی استفاده کنند و این امنیت سخت افزاری را برای کاربران فراهم آورند.

در زمینه جلوگیری از Buffer Overflow، علاوه بر پشتیبانی از NX، ویژگی دیگری موسوم به Sandboxing را نیز در ویندوز پیاده سازی کرده اند که طی آن، کلیه کدهای باینری قبل از اجرا، دوباره کامپایل می شوند و ویژگیهای امنیت بافر در آن فعال می شود تا runtime libraryهایی بتوانند در حال اجرا، حملات مبتنی بر Buffer overflow را تشخیص دهند و از آن جلوگیری کنند و Cookieهایی به heap افزوده می شود تا بتواند حملات heap buffer overflow رانیز محافظت کند.

با ارائه نسخه جدیدی از Outlook Express در SP2، از عکسها و کلیه محتوای خارجی جلوگیری می شود، در مورد سایر برنامه ها که قصد فرستادن E-Mail

را دارند، هشدار داده می شود و روی باز کردن و ذخیره کردن ضمیمه نامه ها(Email Attachments) نیز کنترل صورت می گیرد.

برای کنترل اجرای ضمیمه های آسیب رسان، از سرویس دیگری به نام Application New Execution Servic استفاده می شود. همچنین کاربران این امکان را دارند تا همه نامه ها را به صورت Plain Text یا متنی مشاهده کنند و بدین وسیله از حملاتی که بالقوه ممکن است در HTML صورت پذیرد، جلوگیری کنند. Windows Messenger و Messenger MSN نیز از بهبودهای Attachment استفاده می کنند. بهبود امنیت Internet Explorer از دغدغه های اصلی SP2 است. مدیریت add-onها و تشخیص توقف سیستم (Crash) مربوط به آنها، کنترل اینکه آیا اطلاعات باینری اجازه اجرا دارند یا خیر، به کار بردن محدودیت های امنیتی برای همه URL Objectها که قبلا تنها در مورد ActiveXها وجود داشت و کنترل روی اجرای همه نوع محتوا (Content) از ویژگی های SP2 هستند. SP2 IE به صورت جدی، امکانات Local Machine Zone را محدود کرده است تا از حملاتی که از این ناحیه امنیتی برای اجرای HTMLهای مخرب استفاده می کردند، جلوگیری کند. همچنین IE بر سازگاری اطلاعات همه انواع فایلها که از طرف سرورها فرستاده می شود، نظارت می کند که اطلاعاتی که برای یک نوع فایل خاص فرستاده می شود از همه نظر مطابق آنچه مورد انتظار است باشد؛ همچنین فایلها را sniff می کند تا کدهای مخرب را درون فایلهای ظاهرا بی خطر شناسایی کند.IE SP2 از دسترسی به cached scriptable object جلوگیری می کند، یعنی صفحه های HTML تنها به اشیاء مربوط به خود دسترسی دارند و بدین وسیله، از حملاتی که روی مدل cross-domain security model انجام می شوند تا حد زیادی جلوگیری می کند، به scriptها اجازه نمی دهد که به رخدادها

(events) و محتوای سایر فریم ها گوش دهند و مثلا از دزدیده شدن اطلاعات مربوط به Credit Card در یک فرم دیگر جلوگیری می کند. از ویژگی های دیگر IE، قابلیت جلوگیری از پنجره های pop-up ناخواسته است و کاربر می تواند به دلخواه خود، pop-upها را مدیریت کند. IE همچنین از اطلاعات امضا شده توسط منبع غیر مطمئن جلوگیری می کند، کد های امضا شده با امضای الکترونیکی غیر معتبر را به صورت پیش فرض مانع می شود. همچنین IE از کدهای مربوط به تغییر اندازه پنجره ها و تغییر status bar محافظت می کند.

در SP2، با استفاده از DirectX 9 و Windows Media Player 9، ویژگی های امنیتی، سرعت و کارایی آنها را افزایش داده است. با افزودن امکاناتی به سیستم Update ویندوز، به روز رسانی و نصب patchها را سریع، ساده، اتوماتیک و امن تر کرده است و حجم این Patchها از این پس، بسیار کمتر خواهد بود و بخش عمده کار به عهده Installer خواهد بود. با استفاده ازWindows Installer ۳،۰، امکانات زیادی در زمینه امنیت در نصب برنامه ها افزوده شده است و سیستم مدیریت patchها و حجم کمتر patchها را با استفاده از تکنولوژی Delta Compression فراهم کرده است و patch removal را نیز قابل اطمینان تر کرده است. وجود Windows Security Center از امکانات جدید ویندوز SP2 است که با فراهم کردن یک محیط user friendly و ثابت برای کاربر، امکان مدیریت امنیتی متمرکز ویندوز را برای کاربران فراهم می کند. مدیریت فایروال ویندوز، به روز رسانی ویندوز، گزینه های امنیتی اینترنت و محافظت در مقابل ویروسها از امکانات این محیط است. این امکان وجود دارد تا در این محیط از فایروال خود ویندوز استفاده شود و یا تولید کنندگان دیگر فایروال شخصی، محصولات خود را برای این محیط سازگار کنند. درمورد Anti-Virus این امکان در Security Center قرار داده شده تا سایر شرکتهای تولید کننده Anti-Virus خود را با این محیط مطابقت دهند و هنوز مایکروسافت راه حل مستقلی در این زمینه ندارد.

نرم افزارهای ضدویروس

با استفاده از نرم افزارهای ضد ویروس، امکان شناسائی و بلاک نمودن ویروس ها قبل از آسیب رساندن به سیستم شما، فراهم می گردد. با نصب این نوع نرم افزارها بر روی سیستم خود یک سطح حفاظتی مناسب در خصوص ایمن سازی کامپیوتر و اطلاعات موجود بر روی آن ایجاد خواهد شد. به منظور استمرار سطح حفاظتی ایجاد شده، می بایست نرم افزارهای ضدویروس بطور دائم بهنگام شده تا امکان شناسائی ویروس های جدید، وجود داشته باشد.

نرم افزارهای ضد ویروس، چه کار می کنند ؟

جزئیات عملکرد هر یک از برنامه های ضد ویروس با توجه به نوع هر یک از نرم افزارهای موجود، متفاوت است. اینگونه نرم افزارها فایل های موجود بر روی کامپیوتر و یا حافظه کامپیوتر شما را به منظور وجود الگوهائی خاص که می تواند باعث ایجاد آلودگی گردند را پویش می نمایند. برنامه های ضد ویروس بدنبال الگوهائی مبتنی بر علائم خاص، تعاریفی خاص و یا ویروس های شناخته شده، می گردند. نویسندگان ویروس های کامپیوتری همواره اقدام به نوشتن ویروس های جدید نموده و ویروس های نوشته شده قبلی خود را بهنگام می نمایند. بنابراین لازم است که همواره بانک اطلاعاتی شامل تعاریف و الگوهای ویروس های کامپیوتری مربوط به نرم افزار، بهنگام گردد. پس از نصب یک نرم افزار آنتی ویروس بر روی کامپیوتر خود، می توان عملیات پویش و بررسی سیستم به منظور آگاهی از وجود ویروس را در مقاطع زمانی مشخص و بصورت ادواری انجام داد. در این رابطه می توان از دو گزینه متفاوت استفاده نمود:

- **پویش اتوماتیک** : برخی از برنامه های ضد ویروس دارای پتانسلی به منظور پویش اتوماتیک فایل ها و یا فولدرهائی خاص و در یک محدوده زمانی مشخص شده ، می باشند.

- **پویش دستی** : پیشنهاد می گردد، پس از دریافت هرگونه فایلی از منابع خارجی و قبل از فعال نمودن و استفاده از آن، عملیات بررسی و پویش آن به منظور شناسائی ویروس صورت پذیرد. بدین منظور عملیات زیر توصیه می گردد:

– ذخیره و پویش ضمائم نامه های الکترونیکی و یا نرم افزارهائی که از طریق اینترنت Download می نمائید(هرگز ضمائم نامه های الکترونیکی را مستقیما" و بدون بررسی آن توسط یک برنامه ضد ویروس، فعال ننمائید).

– بررسی فلاپی دیسک ها، CD و یا DVD به منظور یافتن ویروس بر روی آنان قبل از باز نمودن هر گونه فایلی

نحوه برخورد نرم افزار ضدویروس با یک ویروس

نرم افزارهای ضد ویروس به منظور برخورد با یک ویروس از روش های متفاوتی استفاده می نمایند. روش استفاده شده می تواند با توجه به مکانیزم پویش (دستی و یا اتوماتیک) نیز متفاوت باشد. در برخی موارد ممکن است نرم افزار مربوطه با ارائه یک جعبه محاوره ای، یافتن یک ویروس را به اطلاع شما رسانده و به منظور برخورد با آن از شما کسب تکلیف نماید . در برخی حالات دیگر، نرم افزار ضدویروس ممکن است بدون اعلام به شما اقدام به حذف ویروس نماید. در زمان انتخاب یک نرم افزار ضد ویروس، لازم است به ویژگی های ارائه شده و میزان انطباق آنان با انتظارات موجود، بررسی کارشناسی صورت پذیرد.

از کدام نرم افزار می بایست استفاده نمود ؟

تولید کنندگان متعددی اقدام به طراحی و پیاده سازی نرم افزارهای آنتی ویروس می نمایند. عملکرد این نوع نرم افزارها مشابه یکدیگر می باشد. به منظور انتخاب یک نرم افزار ضد ویروس می توان پارامترهای متعددی نظیر ویژگی های ارائه شده توسط نرم افزار، قیمت و میزان انطباق آنان با خواسته های موجود را بررسی نمود.

نصب هر نوع نرم افزار ضد ویروس (صرفنظر از نرم افزاری انتخاب شده)، باعث افزایش حفاظت شما در مقابل ویروس ها می گردد. برخی از پیام های ارسالی که ادعا می نمایند شامل نرم افزارهای ضدویروس بوده و یا اینگونه نرم افزارها را به شما معرفی می نمایند، خود به منزله یک ویروس بوده و می بایست دقت لازم در خصوص بازنمودن آنان و ضمائم مربوطه را داشته باشیم.

چگونه می توان از آخرین اخبار و اطلاعات مربوط به ویروس ها، آگاهی یافت ؟

فرآیند بهنگام سازی در هر نرم افزار ضدویروس متفاوت بوده و می بایست در زمان انتخاب اینگونه نرم افزارها، پتانسیل آنان در خصوص بهنگام سازی بانک اطلاعاتی تعاریف الگوها، بررسی گردد. تعداد زیادی از نرم افزاری ضد ویروس دارای گزینه ای به منظور بهنگام سازی اتوماتیک، می باشند. استفاده از پتانسیل فوق با توجه ایجاد ویروس های جدید، امری لازم و اجتناب ناپذیر است. نصب یک نرم افزار ضد ویروس، یکی از ساده ترین و در عین حال موثرترین روش های حفاظت از کامپیوتر است. آیا صرفا" با یک نصب همه چیز تمام شده و ما همواره دارای ایمنی لازم و حفاظت مطلوب خواهیم بود؟ پاسخ به سوال فوق قطعا" منفی بوده و این نوع نرم افزارها دارای محدودیت های خاص خود نیز می باشند. نرم افزارهای ضد ویروس به منظور شناسائی و برخورد با ویروس ها از الگوهای شناخته شده، استفاده می نمایند. بنابراین طبیعی است که اینگونه نرم افزارها صرفا" قادر به شناسائی و برخورد با ویروس هائی می باشند که قبلا" الگوی آنان برای نرم افزار معرفی شده باشد. به منظور حفظ اقتدار نرم افزارهای ضد ویروس و کمک به آنان در جهت شناسائی و برخورد با ویروس های جدید، می بایست فرآیند بهنگام سازی آنان بطور مداوم و در محدوده های زمانی مشخص، تکرار گردد.

قابلیت‌های نرم‌افزارهای ضدویروس

قابلیت‌های نرم‌افزارهای ضدویروس وتفاوت بین نسخه‌های ضد ویروس

همه نرم‌افزارهای ضد ویروس عمل واحدی را انجام می‌دهند که همان اسکن فایل‌ها و پاک‌سازی موارد آلوده می‌باشد. بعضی از آنها حتی از موتورهای اسکن یکسانی برای شناسایی ویروس‌ها بهره می‌گیرند. تفاوت اصلی بین این محصولات در کیفیت واسط کاربر، سرعت و دقت محصول و قابلیت‌های خاص (مانند اسکنرهای e-mail، بروز رسانی‌های خودکار زمان بندی شده، اسکن‌های ابتکاری و ...) می‌باشد.

در حال حاضر با توجه به اتصال اکثر کامپیوترها به شبکه اینترنت و خطرات گسترده‌ای که از این طریق کاربران را تهدید می‌کند تامین امنیت در برابر ویروس‌هایی که از طریق اینترنت انتقال می‌یابند اهمیت زیادی دارد. از سوی دیگر اینترنت می‌تواند به عنوان ابزاری برای بروز نگه‌داری نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد.

حافظت e-mail

افزایش تعداد کرم‌هایی که از طریق e-mail توزیع می‌شوند نیاز همه افراد به محصولات ضد ویروسی که امنیت آنها را تامین کنند افزایش داده است. تعدادی از محصولات نرم‌افزاری نمی‌توانند امنیت مورد نیاز را برای همه کاربران تامین کنند.

از سوی دیگر تمایل زیاد کاربران به یکپارچه سازی نرم افزارهای e-mail با برنامه‌های اداری باعث شده، شکاف‌های امنیتی موجود در نرم‌افزارهای اداری توسط کرم‌هایی مانند ILOVEYOU و W32.Klez به سادگی مورد استفاده قرار گیرد. در چنین مواردی اگر وصله‌های امنیتی سیستم قدیمی باشند(که این مساله بسیار رایج است)، تنها مشاهده یک نامه آلوده کافی است که کرم به دستگاه نفوذ کند.

مشکل اصلی در رابطه با امنیت e-mail به نحوه کار برنامه‌ها برمی‌گردد. برنامه‌های e-mail پیام‌ها را دریافت کرده و آنها را در پایگاه‌داده‌های خاص خود ذخیره می‌نمایند. از سوی دیگر برنامه‌های ضد ویروس فقط فایل‌هایی را که در قالب فایل‌سیستم‌های شناخته شده مانند Fat16، Fat32، NTFS و ... هستند را اسکن می‌کنند، بنابراین لزوما نمی‌توانند ساختمان داده‌ای را که برنامه e-mail برای ذخیره سازی اطلاعات استفاده می‌کند شناخته و پیام‌های ذخیره شده و فایل‌های ضمیمه آن را اسکن کند. این بدان معناست که هرگاه یک e-mail آلوده بر روی دستگاهی که وصله‌های جدید بر روی آن نصب نشده بار شود، نه تنها کامپیوتر آلوده می‌شود بلکه پاک کردن دستگاه به سادگی امکان پذیر نیست و حتی ممکن است همه e-mailها از دست بروند. به عنوان مثال کرم W32.Klez که کامپیوترهای زیادی را آلوده نمود، در گام اول برنامه‌های ضد ویروس را مورد هجوم قرار می‌دهد و در نتیجه برنامه آلوده شده قادر به پاک کردن محتویات صندوق‌های پستی کاربران نیست.

دو راه حل برای این مشکل وجود دارد، یا باید با دقت همه وصله های جدید مرورگر وب و برنامه‌های e-mail را گرفته و بر روی دستگاه نصب نمود و یا از برنامه‌های ضدویروسی استفاده کرد که به مرورگر و برنامه mail متصل شده و آنها را به روز نگه‌می‌دارند.

برای اینکه سیستم e-mail کاملا حافظت شده باشد، باید عملیات اسکن قبل از اینکه e-mail در جایی از حافظه ذخیره شود صورت گیرد. به عبارت دیگر برنامه e-mail

داده را بعد از گرفتن از اینترنت به اسکنر ضدویروس ارسال می‌نماید تا عملیات لازم بر روی آن صورت گیرد.

همه نرم‌افزارهای e-mail قابلیت این نوع مجتمع شدن را ندارند. اما اسکنرهایی وجود دارند که به خوبی با بعضی از نسخه‌های Microsoft Outlook Express، Microsoft Outlook، Netscape Messenger، Netscape، Eudora Pro و Becky Internet Mail مجتمع می‌شوند. بعضی از اسکنرها ادعای مجتمع شدن با همه سرویس‌گیرنده‌های POP3 و MAPI را مطرح می‌کنند.

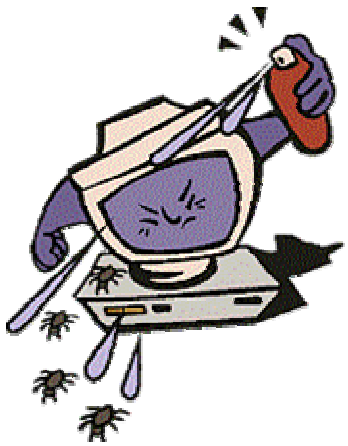
بروز رسانی نرم‌افزارهای ضدویروس

نصب برنامه ضد ویروس و رها کردن آن برای داشتن دستگاهی بدون ویروس و مقاوم در برابر حملات ویروس‌ها کافی نیست. هر روزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های جدید انتشار سریع کرم‌ها از طریق اینترنت نرخ ایجاد ویروس را افزایش داده است. این مساله در ترکیب با افزایش دانش عمومی در مورد مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل سرعت ایجاد ویروس‌های جدید را افزایش داده است. امروزه برای ایجاد یک ویروس نیاز به مهارت و تخصـــص زیاد نیست.

تولید کنندگان ویروس‌ها می توانند ویروس‌هایی با تفاوت‌های اندک نوشته و در دنیای مجازی انتشار دهند. بنابراین علاوه بر خرید و نصب نرم‌افزار ضدویروس دقت در بروز نگه‌داشتن آن هم از اهمیت خارق‌العاده‌ای برخوردار است. شرکت‌های تولید کننده نرم‌افزار برای مقابله با این مشکل قابلیت بروز رسانی خودکار را به محصولات جدید خود افزوده‌اند. بنابراین کاربران تنها با انتخاب گزینه مناسب از منوهای نرم‌افزار می‌توانند از بروز بودن نرم‌افزار خود مطمئن باشند.

طرز کار برنامه های ضد ویروس

ضد ویروس اصطلاحی است که به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند. مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن (Scanning engine) آن است. جزئیات عملکرد هر موتور متفاوت است ولی همه آنها وظیفه اصلی شناسایی فایل های آلوده به ویروس را با استفاده از فایل امضای ویروس ها بر عهده دارند. فایل امضای ویروس یک رشته بایت است که با استفاده از آن می توان ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسان ها می باشد. ضد ویروس متن فایل های موجود در کامپیوتر را با نشانه های ویروس های شناخته شده مقایسه می نماید. در بیشتر موارد در صورتی که فایل آلوده باشد برنامه ضدویروس قادر به پاکسازی آن و از بین بردن ویروس است. در مواردی که این عمل ممکن نیست مکانیزمی برای قرنطینه کردن فایل آلوده وجود دارد و حتی می توان تنظیمات ضدویروس ها را به گونه ای انجام داد که فایل آلوده حذف شود.



بعضی از برنامه های ضد ویروس برای شناسایی ویروس های جدیدی که هنوز فایل امضای آنها ارائه نشده از روش های جستجوی ابتکاری استفاده می کنند. به این ترتیب

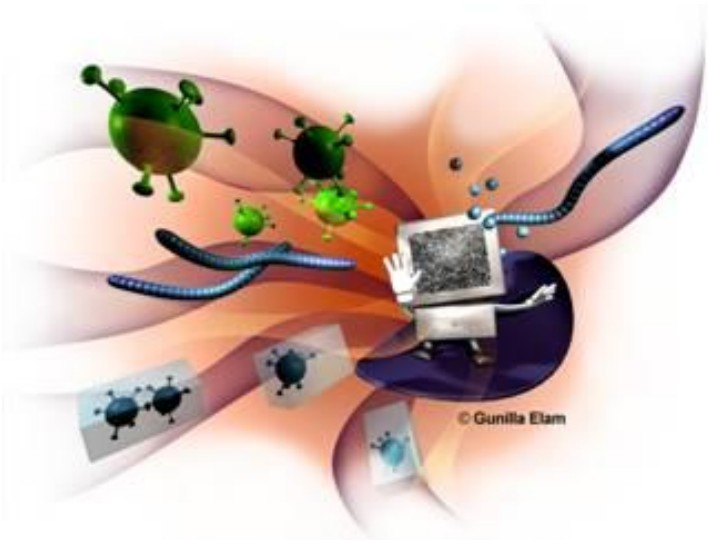
داده های مشکوک در فایل های موجود در سیستم و یا فعالیت های مشکوک مشابه رفتار ویروس ها (حتی در صورتی که تعریف ویروسی منطبق با آنچه که در فایل مشکوک یافت شده موجود نباشد) علامت گذاری می شوند. اگر ضد ویروس فعالیت مشکوکی را مشاهده نماید، برنامه ای که فعالیت مشکوک انجام داده را قرنطینه نموده و به کاربر در مورد آن اعلام خطر می کند (به عنوان مثال اعلام می شود که برنامه مشکوک مایل به تغییر Windows Registry می باشد). دقت این روش پایین است و در بسیاری از مواقع در شناخت فایل های مشکوک به ویروس اشتباهاتی رخ می دهد.

در چنین مواقعی فایل قرنطینه شده برای شرکت های سازنده ضد ویروس ها ارسال می شود که پس از تحقیق و آزمایش آن، در صورتی که واقعا فایل آلوده به ویروس باشد نام، امضاء و مشخصات آن مشخص شده و پادزهر آن ارائه می گردد. در این صورت کد مشکوک تبدیل به یک ویروس شناخته شده می شود.

قابلیت های نرم افزار های ضدویروس

سطح محافظت نرم افزار بسته به جدید و بروز بودن آن متغیر است. محصولات جدیدتر قابلیت های مانند بروز رسانی خودکار، اسکن های زمان بندی شده، محافظت از سیستم به صورت ماندگار در حافظه و همچنین امکان یکپارچه شدن با برنامه های

کاربردی اینترنتی مانند برنامه های e-mail و مرورگرهای وب را دارند. نسخه های قدیمی تر نرم افزارهای ضدویروس تنها یک اسکنر بودند که باید به صورت دستی راه اندازی می شدند. همه نرم افزار های ضدویروس در صورتی که به صورت منظم به روز رسانی شده و عملیات اسکن بر روی دیسک های سخت، تجهیزات قابل انتقال (مانند فلاپی و Zip disk) انجام شود می توانند دستگاه کامپیوتر را در برابر ویروس ها مقاوم کنند. در واقع نقطه برتری محصولات جدید ضد ویروس در قابلیت های آنها برای محافظت از سیستم در مواقعی است که کاربر دانش و یا دقت لازم برای به کارگیری آن را ندارد.



حداقل توقعی که از یک برنامه ضد ویروس خوب می توان داشت این است که در برابر ویروس های boot-sector، ماکرو، اسب های تروا و فایل های اجرایی آلوده به ویروس و کرم اقدامات محافظتی لازم را به عمل آورد. از محصولات جدیدتر می توان انتظار محافظت در برابر صفحات وب، اسکریپت ها، کنترل های ActiveX و اپلت های جاوای خطرناک، همچنین کرم های e-mail را داشت.

امنیت شبکه های کامپیوتری

www.teach.toghraee.ir

www.toghraee.ir

ایمیل

Toghraee_university@yahoo.com