ایمن سازی سیستم عامل Windows

چکیـــده

در این مقاله با توجه به پیام شرکت Microsoft مبنی بر انجام سه عمل در گرایش هـای مختلـف در جهـت ایمن سازی سیستم عامل ، در می یابیم که می توان به مقدار قابـل تـوجهی از امنیـت سیسـتم عامـل مطمـئن گردید.

با توجه به ذکر مهمترین خصوصیات نرم افزارهایی چون :

Microsoft Internet Security and Acceleration 2000
Software Update service
Norton Antivirus Corporate, edition

می توان دریافت که این نرم افزارها را میتوان با قابلیت های فوق العاده بالایشان به طرز کاملا مطلوبی در کنـار یکدیگر جهت هرچه بالاتر بردن امنیت سیستم عامل استفاده نمود.

مـقـدمـه

با توجه به اینکه امروزه بخش عظیمی از سیستم های عامل در دست (انحصار) شرکت Microsoft می باشد و با توجه به چالشهای امنیتی جدیدی که این شرکت در ماه های اخیر با آن مواجه گشته نگاهی می اندازیم بـه استراتژی امنیتی این شرکت و به بررسی مهمترین پیام امنیتی این شرکت در رابطه با حفظ امنیت می پردازیم.
همچنین در راستای عملی سازی این پیام به بررسی تکنیک ها و نـرم افزارهـای پیشـنهادی ایـن شـرکت مـی پردازیم.

واژگان کلیدی

Security, Hack, Firewall, Update, SUS, Antivirus, ISA Server , سیسـتم عامل, امنیت.

نگاهی اجمالی به واژه Hack و استراتژِی Hacking

امـــروزه تعریف مشخص و معینی از واژه Hack وجود ندارد و از دیدگاه های مختلف , تعاریف متعددی از ایـن واژه وجود دارد . اما در نگاه کلی منظور از Hack فعـالیتی اسـت کـه یـک شـخص (Hacker) ، از آن در

جهت دستیابی بدون مجوز به یک کامپیوتر ، شبکه یا برنامه استفاده می کند . هکرها را به تناسب گرایشی که دارند می توان در گروه های مختلفی دسته بندی کرد، برای مثال (Cracking) ، (Phreaking) و (Social Engineering)
در هر دسته مهمترین عاملی که به یک هکر اجازه فعالیت می دهد ، پیدا کردن نقاط ضعف و حفره های امنیتی موجود در برنامه ، کامپیوتر و یا شبکه از طریق پویش های متوالی می باشد .

با توجه به نکات ذکر شده و با توجه به اینکه موضوع مورد نظر ما در این مقاله امنیت سیستم عامل می باشد در منطقی ترین و ساده ترین روش برای حفظ امنیت می توان چنین نتیجه گرفت :
۱- مانع از دسترسی و پویش سیستم عامل توسط مهاجمان شویم.
۲- حفره های امنیتی ویندوز را از طریق نصب Patch ها برطرف سازیم.

نگاهی به پیام امنیتی شرکت Microsft

درست پس از شیوع ویروس Blaster و کمی بعد از به کنترل درآمدن اوضاع ، شرکت Microsoft پیامی مبنی برحفظ امنیت سیستم عامل به طریق اجرای ۳ مرحله در صفحه اصلی خود قرار داد . اهمیت این پیام به قدری می باشد که تقریبا در همه صفحه های اصلی سایت این پیام مشاهده می گردد .

بررسی پیام شرکت Microsoft

در نگاه اول ، پیام بالا را می توان سندی بر صدق گفته های بعضی از بزرگان شرکت مایکروسافت نظیر آقایان (Bob Muglia) از مدیران عالیرتبه این شرکت و (Steve Ballmer) مدیر ارشد اجرایی این شرکت ، در خصوص اینکه (امنیت مهمترین اولویت شرکت Microsoft می باشد) دانست .

1) Use an Internet firewall

با توجه به پیام این شرکت و با توجه به صحبتهای اخیر آقای Muglia در مصاحبه با سایت ZDnet.com می توان به راحتی دریافت روشی که Microsoft در جهت امنیت سیستم عامل در پیش گرفته یک سیستم کاملا پوششی (Shielded) می باشد و استراتژی امنیتی این شرکت ، تمایل بسیاری به سیستم دفاعی چند لایه دارد . به طوری که در اولین مرحله ، این شرکت کاربران را به استفاده از Firewall به جهت جلوگیری از دسترسی مهاجمان به سیستمهای عامل تشویق می کند . اهمیت این موضوع را می توان با نگاهی

دقیق تر به نحوه آسیب رسانی ویروس Blaster دریافت ، با توجه به اینکه تقریبا هیچ کاربر یا شبکه ای که از Firewall استفاده نموده به این ویروس دچار نشده است .

2) Get computer updates

در مرحله دوم ، شرکت Microsoft بر نصب Update های ویندوز تاکید بسیاری می کند و بـه روشـهای مختلف سعی بر تشویق کاربران به نصب اینگونه Patch ها دارد . همچنین این شرکت جهت هر چه آسان تـر کردن این فرآیند اعمال مختلفی صورت داده که از جمله می توان به نکات زیر اشاره کرد :

1- اولیـــن استـــفاده از پـــردازنده هـــای ۶۴ بـــیتی ایـــن شـــرکت در ســـــرورهای ســـایت Windowsupdate.com و ارتقاع چشمگیر کارایی این سایت .

2- استفاده از برنامه ای با نام (Automatic update client) که همـراه سـرویس پـک ۳ (SP3) روی سیـستم عـامل نصب می گردد و فرآیند نصب update ها را به صورت اتوماتیک در می آورد.

3) Use up-To-Date Antivirus Software

در مرحله سوم ، با توجه به اینکه بستر عملیاتی بیشتر ویروسها نقاط ضعف سیستم عامل می باشد و با توجه بـه اینکه در دو مرحله اول امکان استفاده از این نقاط ضعف به مقدار بسیاری کـاهش می یابد ، این شرکت کاربران را به استفاده از برنامه های ضد ویروس به روز، تشـویق می کند .
در نگاه کلی به نکات مطرح شده و بررسی آن می توان نتیجه گرفت که اعمال صورت گرفته می تواند به مقدار قابل توجهی ، نگرانیها را در مورد امنیت سیستم عامل برطرف سازد .

نحوه عملی سازی پیام Microsoft an Internet firewall Use

در این مقاله جهت Firewall به بررسی برنامه ISA Server می پردازیم . در این قسمت به طور خلاصه به ذکر مهمترین ویژگی های این Firewall می پردازیم .

Edition Comparison

برنامه ISA Server در دو نسخه Standard و Enterprise موجود می باشد که تفاوتهای اصلی این دو نسخه طبق جدول زیر می باشد :

Feature	ISA Server Standard Edition	ISA Server Enterprise edition
Server deployment	Standalone only	Multiserver with centralized management
Policy level support	Local only	Enterprise and array
Hardware scalability	4 CPUs only	No limit

ISA Server Roles :

قابلیت استفاده در دو Mode : (Firewall Server) and (Cache Server)

Windows 2000 Integration

برنامه ISA Server براساس تکنولوژی ویندوز ۲۰۰۰ ساخته شده و بسیاری از سرویسهای ویندوز ۲۰۰۰ بـه صورتی بسیار کارا با ISA Server جهت امنیت و کارایی و مدیریت بهتر ادغام می گردد .

Authentication	System Hardening
MMC Administration	Quality of Service
Web filters	Alerts
Active Directory Storage	Multiprocessor Support
Tiered-Policy Management	Client-Side Auto-Discovery

Integrated Virtual Private Networking	Administration Component Object Model (COM) objec

Scalability

کامپیوترهایی که از نسخه Enterprise برنامه ISA Server استفاده می کنند را می توان در گروه هایی به نام (Array) دسته بندی کرد .

Array گروهی است متشکل از چند ISA Server که فواید زیر را حاصل می کند .

Fault Tolerance	Load Balancing
Distributed Caching	Centralized Management

Filtering Methods

برنامه ISA Server ، امنیت را توسط روشهای فیلترینگ مختلفی افزایش می دهد از جمله :

Packet Filtering

Circuit – Level (protocol) filtering

Application filtering

Application Filters

پیچیده ترین سطح Filtering در این قسمت صورت می پذیرد . برای ISA Server می توان از Application filter های مختلفی استفاده نمود. برنامه ISA Server هنگام نصب دارای Application filter های زیر می باشد .

HTTP Redirector Filter	FTP Access Filter
Socks Filter	SMTP Filter

RPC Filter	H.323 Filter
Streaming media Filter	POP and DNS Intrusion Detection Filters

Integrated Virtual Private Networking

ISA Server را می توان به عنوان یک VPN SERVER نصب نمود که مـی توانـد در دو نقـش عمـل نماید.

Client – To – Gateway یا Gateway-to-Gateway.

Integrated Intrusion Detection

برنامه ISA Server دارای یک مکانیسم داخلی جهت رد یابی حملات می باشد. این سیستم دارای انعطـاف پذیری مطلوبی می باشد که مدیر شبکه را قادر می سازد رفتار ISA Server را هنگـام مواجـه بـا حمـلات تعین کند .

Packet Filter Intrusions

در سطح Packet Filter ، برنامه ISA Server می تواند حملات زیر را ردیابی کند :

o IP half Scan Attack	o All Ports Scan Attack
o Land Attack	o Enumerated Port Scan Attack
o UDP Bomb Attack	o UDP Bomb Attack
	o UDP Bomb Attack

computer update Get

دراین قسمت نگاهی می اندازیم به برنامه Software Update Service ، برنامه ای برا ی مدیریت و توزیع Patch های بحرانی ویندوز . از آنجائیکـه در زمینـه امنیـت سیسـتم عامـل ، نصـب Patch هـا از ضروریات می باشد ، برنامه SUS را می توان در جهت هر چه آسان تر شدن و ارتقاء مـدیریت نصـب Patch ها در مقیاسی وسیع در شبکه استفاده نمود .

در صورت وجود یک Domain ، می توان روند Update کامپیوترهای Client را بـه وسـیله تنظـیم Group policy های مربوط به صورت کاملا Automatic درآورد .
برنامه SUS از اجزاء زیر تشکیل می گردد :

Automatic update client	Software update service

برنامـه SUS بـه حجـم تقریبـی 33Mb از سـایت Microsoft قابـل دریافـت مـی باشـد و برنامـه Automatic update client را نیز می توان به روشهای زیر نصب نمود .

1- Install automatic update clients using MSI Install Package.
2- Install windows 2000 Service Pack 3 (SP3)
3- Install windows XP (SP1)
4- Install windows server 2003

مهمترین خصوصیات برنامه SUS

An administrator–controlled content synchronization service within the intranet:

سرویس synchronization یک بخش از برنامه SUS می باشد که عمل دریافت آخرین Patch هـا را از سایت Microsoft به صورت اتوماتیک انجام می دهد . این سرویس جهت انجام عمل همزمانی قابلیـت Schedule دارد .

An Intranet – hosted windows update server :

کامپیوتر SUS Server می تواند به عنوان سایت Windowsupdate داخلی عمل نماید ، ابزارهـای مدیریتی این سرور ، عمل Update را کاملا تحت کنترل درمی آورد .

Administrator control over updates :

به وسیله این سرویس می توان قبل از اجازه نصب هر Patch ، آنها را در محیط های دیگری تست نمـود و از عدم نا سازگاری آن با برنامه های شبکه مطمئن شد .

Update clients that haven't access to internet

به وسیله این سرویس ، نیازی به دسترسی به اینترنت برای Client ها نمی باشد .

Full compatible with active directory

به وسیله نصب Template های مناسب Group policy در Active Directory می توان پیکربندی Client ها را به صورت مرکزی انجام داد .

Up-To-Date Antivirus Software Use

در این بخش باید توجه داشت که نصب یک Antivirus سیستم ها را فقط در برابر ویروسهایی که قبلا شناسایی شده اند محافظت می کند و برای اطمینان از امن بودن ویندوز در برابر ویروسها نیاز است که آنتی ویروس همیشه به روز نگاه داشته شود..

یکی از پیشگامان و در حقیقت قویترین شرکت ها در زمینه Antivirus شرکت Symantec می باشد.

از سایت این شرکت می توان کلیه اطلاعات لازم نظیر نحوه آسیب رسانی ویروس, پراکندگی جغرافیایی ویروس , تغییراتی که ویروس در سیستم ایجاد می کند و نحوه از بین بردن ویروس را دریافت کرد.

همچنین ابزارهای مختلفی جهت ویروسهای خاصی که برنامه Antivirus قادر به پاک سازی آنها نمی باشد در این سایت یافت می گردد که بسیار کارآمد می باشد.

ضد ویروس نسخه (Norton Antivirus Corporate Edition) این شرکت, که از لحاظ استفاده در شبکه و مدیریت آسان بسیار مطلوب می باشد در شرکت های ایرانی نیز بسیار استفاده می شود.

این برنامه در دو نسخه Server و Client وجود دارد و از نظر مدیریت و پیکر بندی بسیار کاربر پسند می باشد.

سرویس Live Update برنامه مذکور آخرین Update های موجود را به صورت هفتگی و به صورت خودکار دریافت کرده و کلیه Client های شبکه را نیز به روز می کند.