امنیت نامه های الکترونیکی

« قسمت اول »

منبع : سایت www.SRCO.ir

اینترنت چالش های جدیدی را در عرصه ارتباطات ایجاد کرده است. کاربران اینترنت با استفاده از روش های متفاوت ،امکان ارتباط با یکدیگر را بدست آورده اند .اینترنت زیر ساخت مناسب برای ارتباطات نوین را فراهم و زمینه ای مساعد و مطلوب بمنظور بهره برداری از سرویس های ارتباطی توسط کاربران فراهم شده است . بدون شک ، پست الکترونیکی در این زمینه دارای جایگاهی خاص است .

پست الکترونیکی، یکی از قدیمی ترین و پرکاربردترین سرویس موجود در اینترنت است . شهروندان اینترنت، روزانه میلیون ها نامه الکترونیکی را برای یکدیگر ارسال می دارند. ارسال و دریافت نامه الکترونیکی، روش های سنتی ارسال اطلاعات (نامه های دستی) را بشدت دستخوش تحول نموده و حتی در برخی از کشورها ،اغلب مردم تمایل به استفاده از نامه الکترونیکی در مقابل تماس تلفنی با همکاران و خویشاوندان خود دارند . در این مقاله قصد نداریم به بررسی مزایای سیستم پست الکترونیکی اشاره نمائیم. در صورتیکه بپذیریم که سیستم پست الکترونیکی عرصه جدیدی را در ارتباطات افراد ساکن در کره زمین ایجاد کرده است، می بایست بگونه ای حرکت نمائیم که از آسیب های احتمالی تکنولوژی فوق نیز در امان باشیم .

طی سالیان اخیر، بدفعات شنیده ایم که شبکه های کامپیوتری از طریق یک نامه الکترونیکی آلوده و دچار مشکل و تخریب اطلاعاتی شده اند. صرفنظر از وجود نواقص امنیتی در برخی از محصولات نرم افزاری که در جای خود تولید کنندگان این نوع نرم افزارها بمنظور استمرار حضور موفقیت آمیز خود در عرصه بازار رقابتی موجود، می بایست مشکلات و حفره های امنیتی محصولات خود را برطرف نمایند ، ما نیز بعنوان استفاده کنندگان از این نوع نرم افزارها در سطوح متفاوت ، لازم است با ایجاد یک سیستم موثر پیشگیرانه ضریب بروز و گسترش این

نوع حوادث را به حداقل مقدار خود برسانیم . عدم وجود سیستمی مناسب جهت مقابله با این نوع حوادث ، می تواند مسائلی بزرگ را در یک سازمان بدنبال داشته که گرچه ممکن است تولیدکننده نرم افزار در این زمینه مقصر باشد ولی سهل انگاری و عدم توجه به ایجاد یک سیستم امنیتی مناسب ، توسط استفاده کنندگان مزید بر علت خواهد بود (دقیقا" مشابه عدم بستن کمربند ایمنی توسط سرنشین یک خودرو با نواقص امنیتی) . در این مقاله ، به بررسی روش های پیشگیری از تخریب اطلاعات در شبکه های کامپیوتری از طریق پست الکترونیکی پرداخته و با ارائه راهکارهای مناسب ، یک سیستم حفاظتی مطلوب پیشنهاد می گردد . در این راستا ، عمدتا" بر روی برنامه سرویس گیرنده پست الکترونیکی ماکروسافت (Outlook) متمرکز خواهیم شد(بدلیل نقش بارز و مشهود این نوع از برنامه ها در جملات اینترنتی اخیر) . سیل ناگهانی حملات اینترنتی مبتنی بر کدهای مخرب، با ظهور کرم ILOVEYOU ، وارد عرصه جدیدی شده است . سیتسم های مدرن پست الکترونیکی بمنظور مقابله با این نوع از تهدیدات ، تدابیر لازم را در جهت ایجاد یک حفاظ امنیتی مناسب برای مقابله با عرضه و توزیع کدهای مخرب آغاز نموده اند .برنامه های سرویس گیرنده پست الکترونیکی متعلق به شرکت ماکروسافت ، هدفی جذاب برای اغلب نویسندگان کدهای مخرب می باشند . شاید یکی از دلایل آن ، گستردگی و مدل برنامه نویسی خاص بکارگرفته شده در آنان باشد . تاکنون کدهای مخرب فراوانی ، محصولات ماکروسافت را هدف قرار داده اند . عملکرد قدرتمند سه نوع ویروس (و یا کرم) در زمینه تخریب اطلاعات از طریق اینترنت ، شرکت ماکروسافت را وادار به اتخاذ تصمیمات امنیتی خاص در اینگونه موارد نمود . این ویروس ها عبارتند از :

- ویروس Melissa ، هدف خود را بر اساس یک فایل ضمیمه Word مورد حمله ویرانگر قرار می دهد . بمحض باز نمودن فایل ضمیمه ، کد مخرب بصورت اتوماتیک فعال می گردد .
- ویروس BubbleBoy ، همزمان با مشاهده (پیش نمایش) یک پیام ، اجراء می گردد . در این رابطه ضرورتی به باز نمودن فایل ضمیمه بمنظور فعال شدن و اجرای کدهای مخرب وجود ندارد . در ویروس فوق ، کدهای نوشته شده در بدنه نامه الکترونیکی قرار می گیرند . بدین ترتیب، بمحض نمایش پیام توسط برنامه مربوطه ، زمینه اجرای کدهای مخرب فراهم می گردد .
- کرم ILOVEYOU از لحاظ مفهومی شباهت زیادی با ویروس Mellisa داشته و بصورت یک فایل ضمیمه همراه یک نامه الکترونیکی جابجا می گردد . در این مورد خاص، فایل ضمیمه خود را بشکل یک سند Word تبدیل نکرده و در مقابل فایل ضمیمه از نوع یک اسکریپت ویژوال بیسیک (vbs .) بوده و بمحض فعال شدن، توسط میزبان اسکریپت ویندوز (Windows Scripting Host :WSH) تفسیر و اجراء می گردد .

پیشگیری ها

در این بخش به ارائه پیشنهادات لازم در خصوص پیشگیری از حملات اطلاعاتی مبتنی بر سرویس گیرندگان پست الکترونیکی خواهیم پرداخت.رعایت مواردیکه در ادامه بیان می گردد، بمنزله حذف کامل تهاجمات اطلاعاتی از این نوع نبوده بلکه زمینه تحقق این نوع حوادث را کاهش خواهد داد .

پیشگیری اول : Patch های برنامه پست الکترونیکی ماکروسافت

بدنبال ظهور کرم ILOVEYOU و سایر وقایع امنیتی در رابطه با امنیت کامپیوترها در شبکه اینترنت، شرکت ماکروسافت یک Patch امنیتی برای برنامه های outlook 98 و outlook 2000 عرضه نموده است . Patch فوق، با ایجاد محدودیت در رابطه با برخی از انواع فایل های ضمیمه ، زمینه اجرای کدهای مخرب را حذف می نماید . با توجه به احتمال وجود کدهای مخرب در فایل های ضمیمه و میزان مخرب بودن آنان، تقسیمات خاصی توسط ماکروسافت انجام گرفته است .فایل های ضمیمه ای که دارای بیشترین احتمال تهدید برای سیستم های کامپیوتری می باشند ، **سطح یک** و فایل هائی با احتمال تخریب اطلاعاتی کمتر **سطح دو** ، نامیده شده اند. نحوه برخورد برنامه های سرویس گیرنده پست الکترونیکی با هر یک از سطوح فوق متفاوت است . این نوع برنامه ها ، امکان اجرای کدهای موجود در فایل های ضمیمه از نوع سطح یک را بلاک می نمایند. جدول زیر انواع فایل ها ی موجود در سطح یک را نشان می دهد .

شرح	انشعاب
Microsoft Access project extension	ade
Microsoft Access project	adp
Visual Basic class module	bas
Batch file	bat
Compiled HTML Help file	chm
Windows NT Command script	cmd
MS-DOS program	com
Control Panel extension	cpl
Security certificate	crt
Program	exe
Help file	hlp
HTML	hta
Setup Information	inf
Internet Naming Service	ins
Internet Communication settings	isp
JScript Script file	js
JScript Encoded Script file	jse
Shortcut	lnk
Microsoft Access program	mdb
Microsoft Access MDE database	mde
Microsoft Common Console document	msc
Windows Installer package	msi
Windows Installer patch	msp
Visual Test source files	mst
Photo CD image	pcd
Shortcut to MS-DOS program	pif
Registration entries	reg
Screen saver	scr
Windows Script Component	sct
Shell Scrap Object	shs
Internet shortcut	url
VBScript file	vb
VBScript encoded script file	vbe

Patch فوق، در رابطه با ضمائمی که با نام سطح دو(مثلا" فایل هائی از نوع zip) ، شناخته می شوند از رویکردی دیگر استفاده می نماید . این نوع ضمائم بلاک نمی گردند ولی لازم است که کاربر قبل از اجراء آنان را بر روی کامپیوتر خود ذخیره نماید . بدین ترتیب در روند اجراء یک توقف ناخواسته بوجود آمده و زمینه فعال شدن ناگهانی آنان بدلیل سهل انگاری ، حذف می گردد. در رابطه با این نوع از فایل ها ، پیامی مشابه زیر ارائه می گردد .

فایل هائی بصورت پیش فرض درسطح دو ، وجود نداشته و مدیرسیستم می تواند فایل هائی با نوع خاص را اضافه نماید (در رابطه با فایل های سطح یک نیز امکان حذف و یا افزودن فایل هائی وجود دارد) . در زمان تغییر نوع فایل های سطح یک و دو، می بایست به دو نکته مهم توجه گردد : عملیات فوق، صرفا" برای کاربرانی که به سرویس دهنده پست الکترونیکی Exchange متصل هستند امکان پذیر بوده و کاربرانی که از فایل ها ی pst . برای ذخیره سازی پیام های الکترونیکی خود استفاده می نمایند را شامل نمی شود. قابلیت تغییر تعاریف ارائه شده سطح یک و دو، می تواند بعنوان یک رویکرد مضاعف در رابطه با سیاست های امنیتی محلی، مورد استفاده قرار گیرد . مثلا" می توان با استفاده از ویژگی فوق، فایل های با انشعاب doc . (فایل های word) را به لیست فایل های سطح یک اضافه کرد. برای انجام تغییرات مورد نظر در نوع فایل ضمیمه تعریف شده در سطح یک ، می بایست مراحل زیر را دنبال نمود :

- برنامه Regedit.exe را اجراء نمائید .
- کلید

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Security

key را انتخاب نمائید . (در صورتیکه کلید فوق وجود ندارد می بایست آن را ایجاد کرد) .
- از طریق منوی Edit دستور New و در ادامه String Value انتخاب گردد .
- نام جدید را Level1AttachmentAdd منظور نمائید.

- گزینه new Level1AttachmentAdd value را انتخاب و دکمه Enter را فعال نمائید .
- یک رشته شامل انشعاب فایل های مورد نظر را که قصد اضافه کردن آنها را داریم ، وارد نمائید (هر یک از انشعاب فایل ها توسط ";" از یکدیگر تفکیک می گردند)

Example:
Name: Level1AttachmentAdd
Type: REG_SZ
Data: doc;xls

در زمان بازنمودن فایل های ضمیمه ای که از نوع سطح یک و یا دو نمی باشند(فایل های آفیس نظیر Word ,Powerpoint بجزء فایل های مربوط به Access) ، پیامی مطابق شکل زیر ارائه و کاربران دارای حق انتخاب بمنظور فعال نمودن (مشاهده) فایل ضمیمه و یا ذخیره آن بر روی کامپیوتر را دارند . پیشنهاد می گردد که در چنین مواردی فایل ذخیره و پس از اطمینان از عدم وجود کدهای مخرب ، فعال و مشاهده گردد . در این رابطه می توان از ابزارهای موجود استفاده کرد .

Patch فوق، همچنین امکان دستیابی به دفترچه آدرس Outlook را از طریق مدل شی گراء Outlook و Collaborative(CDO Data Objects) ، توسط کدهای برنامه نویسی کنترل می نماید .بدین ترتیب، پیشگیری لازم در مقابل کدهای مخربی که بصورت خودکار و تکراری اقدام به تکثیر نسخه هائی از خود برای لیست افراد موجود در دفترچه آدرس می نمایند ، انجام خواهد یافت . Patch فوق، صرفا" برای نسخه های Outlook 98 و outlook 2000 ارائه شده است (برای نسخه های قبلی و یا Outlook Express نسخه مشابهی ارائه نشده است) .

پیشگیری دوم : استفاده از نواحی امنیتی Explorer Internet

سرویس گیرندگان Outlook 98/2000 و Outlook Express ٥,٠/٤,٠ امکان استفاده از مزایای نواحی (Zones) امنیتی مرورگر IE را بمنظور حفاظت در مقابل کدهای مخرب (کنترل های ActiveX ، جاوا و یا اسکریپت ها) موجود در بدنه پیام ها ،خواهند داشت . مرورگر IE ، امکان اعمال محدودیت در اجرای کدها را بر اساس چهار ناحیه فراهم می نماید . قبل از پرداختن به نحوه استفاده از تنظیمات فوق توسط برنامه outlook ، لازم است که به کاربرد هر یک ازنواحی در مرورگر IE ، اشاره گردد :

- Local Intranet zone . ناحیه فوق، شامل آدرس هائی است که قبل از فایروال سازمان و یا سرویس دهنده Proxy قرار می گیرند . سطح امنیتی پیش فرض برای ناحیه فوق ، " low– medium" است .
- Trusted Sites zone . ناحیه فوق، شامل سایت هائی است که مورد اعتماد می باشند . (سایت هائی که شامل فایل هائی بمنظور تخریب اطلاعاتی نمی باشند) . سطح امنیتی پیش فرض برای ناحیه فوق، " low" است .
- Restricted Sites zone . ناحیه فوق، شامل لیست سایت هائی است که مورد اعتماد و تائید نمی باشند . (سایت هائی که ممکن است دارای محتویاتی باشند که در صورت دریافت و اجرای آنها ، تخریب اطلاعات را بدنبال داشته باشد) .سطح امنیتی پیش فرض برای ناحیه فوق ،" high" است .
- Internet zone . ناحیه فوق ، بصورت پیش فرض شامل هرچیزی که بر روی کامپیوتر و یا اینترانت موجود نمی باشد ، خواهد بود . سطح امنیتی پیش فرض برای ناحیه فوق، " medium " است .

برای هر یک از نواحی فوق، می توان یک سطح امنیتی بالاتر را نیز تعریف نمود. ماکروسافت در این راستا سیاست هائی با نام : low , medium-low , medium و high را تعریف کرده است . کاربران می توانند هر یک از پیش فرض های فوق را انتخاب و متناسب با نیاز خود آنان را تغییر نمایند .

برنامه outlook می تواند از نواحی فوق استفاده نماید . در این حالت کاربر قادر به انتخاب دو ناحیه (Internet zone و Restricted Zone) خواهد بود .

تنظیمات تعریف شده برای ناحیه انتخاب شده در رابطه با تمام پیام های outlook اعمال خواهد شد . پیشنهاد می گردد ناحیه restricted انتخاب گردد . بدین منظور گزینه Tools/Options و در ادامه گزینه Security را انتخاب نموده و از لیست مربوطه ناحیه Restricted sites را انتخاب نمائید. در ادامه و بمنظور انجام تنظیمات مورد نظر ، دکمه Zone Settings را فعال و گزینه Custom Level را انتخاب نمائید . تغییرات اعمال شده در زمان استفاده از برنامه مرورگر برای دستیابی به وب سایت ها نیز مورد توجه قرار خواهند گرفت . پیشنهادات ارائه شده مختص برنامه IE 5.5 بوده و در نسخه های ۵ و ۴ نیز از امکانات مشابه با اندکی تغییرات استفاده می گردد. در این رابطه تتظیمات زیر پیشنهاد می گردد :

گزینه	وضعیت
Download signed ActiveX controls	DISABLE
Download unsigned ActiveX controls	DISABLE
Initialize and script ActiveX controls not marked as safe	DISABLE
Run ActiveX controls and plug-ins	DISABLE
Script ActiveX controls marked safe for scripting	DISABLE
Allow per-session cookies (not stored)	DISABLE
File download	DISABLE
Font download	DISABLE
Java permissions	DISABLE JAVA
Access data sources across domains	DISABLE
Don’t prompt for client certificate selection when no certificates or only one certificate exists	DISABLE
Drag and drop or copy and paste files	DISABLE
Installation of desktop items	DISABLE
Launching programs within an IFRAME	DISABLE
Navigate sub-frames across different domains	DISABLE
Software channel permissions	HIGH SAFETY
Submit nonencrypted form data	DISABLE
Userdata persistence	DISABLE
Active scripting	DISABLE
Allow paste operations via script	DISABLE
Scripting of Java Applets	DISABLE
Logon	Anonymous logon

با غیر فعال نمودن گزینه های فوق، امکانات پیشرفته ای از کاربر سلب می گردد. امکانات فوق برای تعداد زیادی از کاربران پست الکترونیکی ، دارای کاربردی خاص نخواهند بود . اکثر نامه های الکترونیکی ، پیام های ساده متنی بهمراه ضمائم مربوطه می باشند. گزینه های فوق، عموما" به غیر فعال نمودن اسکریپت ها و کنترل های موجود در بدنه یک پیام الکترونیکی اشاره داشته و برای کاربران معمولی سیستم پست الکترونیکی دارای کاربردی خاص نمی باشند. تنظیمات فوق، بصورت مشترک توسط مرورگر IE نیز استفاده خواهند شد (صفحات وبی که از برخی از ویژگی های فوق استفاده می نمایند) . در این رابطه لازم است مجددا" به این موضوع اشاره گردد که ناحیه Restricted صرفا" شامل سایت هائی است که مورد اعتماد نبوده و مشکلی (عدم فعال بودن برخی از پتانسیل های مرورگر) را در رابطه با مشاهده صفحات وب از سایت های تائید شده ،نخواهیم داشت.مهمترین دستاورد تنظیمات فوق،پیشگیری از حملاتی است که سیاست تخریبی خود را بر اساس درج محتویات فعال در بدنه نامه های الکترونیکی، تبین نموده اند . (نظیر ویروس BubbleBoy) .