خبرنامه امنیت رایانه ای
کمیته امداد امام خمینی (ره)

سال اول، شماره نوزدهم نیمه دوم دی هشتاد و شش

دفتر آمار و فناوری اطلاعات

مطابق روند معمول در بحث امنیت رایانه ای و شبکه ای این خبرنامه تلاش شده است تا حد امکان مطالب به زبان ساده و قابل فهم برای همه و بر مبنای نرم افزارها و سخت افزارهایی به طور معمول در رایانه های فعلی موجودند بیان شود و با این وجود مطالب خبرنامه برای افراد با تجربه نیز حاوی نکات و مطالب جدیدی باشد.

شما نیز می توانید نیازهای خود را جهت طرح و پاسخ و یا مطالب و مقالات خود را جهت درج با نام خود در این خبرنامه با ارسال به دفتر آمار و فناوری اطلاعات مرکز با ما در میان بگذارید.

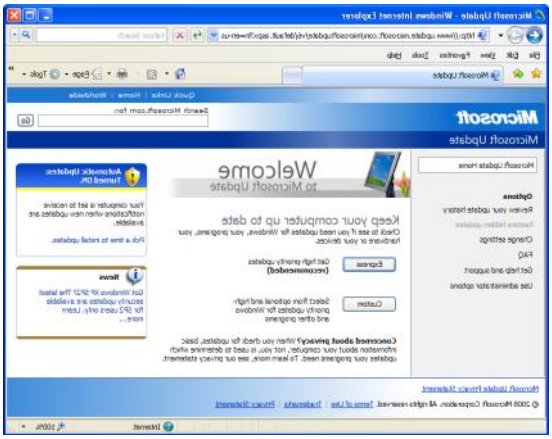
اهمیت به روز رسانی نرم افزارها

اگر چه سازندگان نرم افزارها اعم از سیستم عامل، نرم افزارهای اداری و نرم افزارهای کاربردی و حتی بازیها تلاش خود را در تولید محصولی بدون نقص به کار می گیرند، اغلب حداکثر چند ماه پس از ارائه محصول به بازار ناچار به ارائه به روز رسانی های (Update) متعدد برای آن می گردند. بخشی از این به روز رسانی ها جهت بهبود و افزایش کارآیی نرم افزار و بخش دیگر رفع عیوب و مشکلات آن است که بسیاری از این اشکالات از نوع اشکالات امنیتی هستند.

دسترسی با سرعت کم به شبکه جهانی اینترنت، استفاده از کپی های غیرمجاز و عدم احساس نیاز به نصب به روز رسانی ها در کشور ما دلایل رایجی هستند که نصب آنها را به تأخیر می اندازند یا گاهی اصولاً به روز رسانی انجام نمی شود که در این شماره می بینیم این امر چگونه ممکن است باعث مشکلات مهم در امنیت رایانه ها شود.

از دیدگاه امنیت رایانه، نصب به روز رسانی های ارائه شده از سوی شرکت تولیدکننده نرم افزار اهمیت بسیاری دارد. این اهمیت در به روز رسانی نرم افزار ضد ویروس شما مشخص است چرا که بدون Update کردن آن، رایانه شما در برابر حملات ویروسها آسیب پذیر خواهد شد. اما در مورد سایر نرم افزارها چطور؟

لزوم به روز رسانی از دیدگاه امنیت رایانه در سیستم عامل معمولاً مشخص است اما

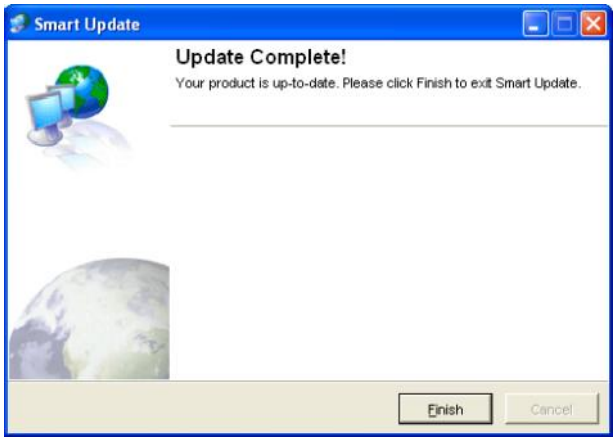


اهمیت به روز رسانی نرم افزارها

یادآوری آن خالی از فایده نیست. هر از چند گاهی یک ایراد مهم در سیستم عامل شما (خواه ویندوز، لینوکس یا هر سیستم عامل دیگری) یافت می شود که به طریقی به نفوذگران ابزاری جهت نفوذ به سیستم شما را ارائه می کند. نفوذگران برای رخنه به سیستم شما حتی از یک مشکل ساده هم می توانند استفاده کنند. مثلاً اگر بتوانند با ارائه ورودی خراب کاری کنند که بخشی از سیستم عامل شما به اصطلاح هنگ کند و از کار بیفتد ممکن است بتوانند از طریق آن کنترل تمام سیستم عامل شما را به دست بگیرند. خوشبختانه به روز رسانی های مهم (Critical Updates یا High Priority Update) بدون بررسی اصل بودن سیستم عامل شما نیز قابل نصب می باشند. به عنوان نمونه در سیستم عامل ویندوز با روشن کردن 'به روز رسانی خودکار' یا همان ' Automatic Updates ' ویندوز شما به صورت خودکار آخرین به روز رسانی های مهم و امنیتی را دریافت می کند. برای افراد ماهرتر تنظیم

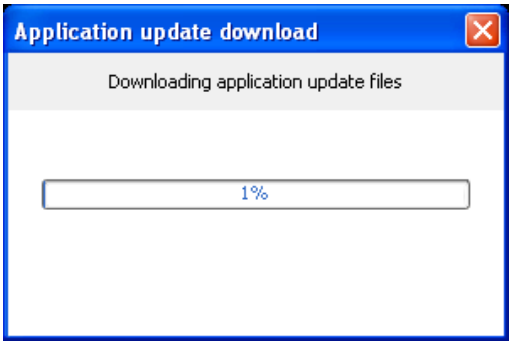
کردن بخش به روز رسانی خودکار به این صورت که پیش از نصب از او اجازه بگیرند توصیه می شود تا در صورت لزوم بتوانند به روز رسانی های خاصی (مانند آنهایی که به بررسی اصل بودن ویندوز می پردازند) را نصب نکنند.

به روز رسانی فقط به سیستم عامل منحصر نمی شود. در هر برنامه کاربردی ممکن است مشکلات امنیتی یافت شود که در نتیجه آنها راهی برای نفوذ به سیستم پیدا شود. درجه امنیت یک سیستم معمولاً برابر درجه امنیت ضعیفترین جزء آن است چرا که نفوذ از ضعیفترین بخش صورت خواهد گرفت. نرم افزارهای مشاهده و پخش فیلم، موسیقی، فایلهای اداری و علمی نیز از این قاعده مستثنی نیستند و در صورتی که به موقع به روز رسانی نشوند می توانند سیستم شما را آسیب پذیر سازند.



اهمیت به روز رسانی نرم افزارها

در شماره های قبل خواندیم که پسوندهای اجرایی شامل exe ، com ، bat ، Vbs ، scr ، pif و ... هستند که هر کدام به نوعی قابلیت اجرا دارند و در نتیجه برای ویروسها مکانی مناسب به شمار می روند. همچنین با فایلهای دارای دو پسوند و خطرات آنها آشنا شدیم. حال با آنچه در این شماره خواندیم می دانیم که یک فایل صوتی هم بالقوه می تواند ابزاری برای نفوذ به سیستم باشد. به بیان دیگر اگر چه فایلی که پسوند آن مربوط به فایلهای چند رسانه ای است قابلیت اجرای مستقیم را ندارد و گزینه مناسبی برای یک ویروس به شمار نمی رود، در صورتی که ضعف امنیتی در نرم افزار مورد استفاده شما جهت پخش فایل صوتی پیدا شده باشد ممکن است فرد



نفوذگر بر مبنای آن، فایل صوتی ساخته باشد که با استفاده از آن ضعف بتواند کنترل سیستم شما را به دست گیرد.

جالب است بدانید که حفره های امنیتی حتی در نرم افزارهای ضد ویروس هم مشاهده شده است به این معنا که نرم افزار ضد ویروس ایرادی داشته است که فرد نفوذگر می توانسته است از طریق آن به سیستم شما رخنه کند و کنترل آن را در دست بگیرد. این در حالی است که سازندگان نرم افزارهای ضد ویروس تمام تلاش خود را در کسب اطمینان از صحت آن به کار می برند. بدیهی است در زمان کوتاهی پس از کشف این حفره امنیتی به روز رسانی مناسب جهت رفع آن ارائه شده است.

به همین دلیل است که بر لزوم به روز رسانی در کلیه نرم افزارها تأکید داریم تا آسیب پذیری سیستم را کاهش دهیم. مسئله دیگر این است که اغلب بین کشف یک نقص امنیتی و ارائه راهکار برای آن فاصله زمانی وجود دارد یعنی مثلاً اگر امروز ایرادی در ویندوز پیدا شود، ممکن است چند روز طول بکشد تا مایکروسافت از ایراد با خبر شود، به روز رسانی آن را بسازد، تستهای لازم را انجام دهد و آن را برای عموم ارائه کند. پس شما حتی اگر بلافاصله پس از ارائه یک Update آن را نصب کنید باز هم به دلیل تأخیر یاد شده در روزهای پیش از نصب آن در معرض خطر هستید. به این قبیل مشکلات که تازه کشف شده اند اغلب Zero-day threats می گویند. برای حفاظت در برابر این مشکل توصیه های زیر را نیز علاوه بر نصب بلافاصله به روز رسانی ها به کار ببندید:

۱. نرم افزارهایی که نیاز ندارید را نصب نکنید و نرم افزارهایی را که دیگر از آنها استفاده نمی کنید حذف نمایید.

۲. فایلهایی که نمی دانید از کجا آمده اند

اهمیت به روز رسانی نرم افزارها

را اجرا نکنید. ضمایم و ایمیل هایی که مطمئن نیستید از طرف چه کسی و به چه دلیل برای شما ارسال شده اند را دریافت نکنید.

۳. از نرم افزارهای هوشمند ضد نفوذ مانند PC Tools Threat Fire که در شماره های گذشته معرفی شده است استفاده کنید.

در اغلب موارد سایتهای اینترنتی شرکتهای سازنده نرم افزار فایلهای اجرایی مربوط به به روز رسانی را برای دانلود عرضه می کنند که در این صورت برای صرفه جویی در پهنای باند اینترنت و افزایش سرعت و دقت می توان به روز رسانی را روی شبکه داخلی قرار داد و آن را برای تمام رایانه ها از روی شبکه داخلی نصب نمود.

یک نکته مهم دیگر که باید به آن دقت شود استفاده از CD های جدید تر در هنگام نصب نرم افزارهاست. اگر هنوز از CD ویندوزی که یک سال پیش خریده اید استفاده می کنید و این CD نیاز به نصب به روز رسانی های متعدد دارد، ممکن است بتوانید CD را پیدا کنید که جدیدتر باشد و لذا تنها نیاز به نصب به روز رسانی های یک ماه اخیر را داشته باشد. در مورد سایر نرم افزارها نیز در صورتی که امکانات سخت افزاری شما اجازه بدهد همیشه نصب آخرین نسخه ها بهترین گزینه است و کارآیی و امنیت بیشتری را ارائه می کند. در نقطه مقابل از نصب نرم افزارهایی که در مراحل آلفا و بتا یا آماده عرضه (Alpha, Beta or Replace Candidate (RC)) هستند خودداری کنید چرا که اگر چه این نرم افزارها بسیار جدید هستند، هنوز تستهای لازم را پشت سر نگذرانده اند و به احتمال قوی در آنها مشکلاتی وجود دارد که برای رفع آن به زودی نیاز به چندین به روز رسانی خواهند داشت.

پرسشهای خود را در هر زمینه مرتبط با IT و رایانه از طریق پست الکترونیک یا نامه به دفتر آمار و فناوری اطلاعات مرکز با ما در میان بگذارید تا پاسخ آنها را در همین خبرنامه دریافت کنید.

همچنین در صورتی که علاقمند به همکاری با این خبرنامه می باشید، می توانید مقالات و مطالب خود را اعم از تألیف یا ترجمه در قالب یک فایل Word به صورت پست الکترونیک یا بر روی CD به دفتر آمار و فناوری اطلاعات ارسال نمایید تا پس از بررسی با نام خود شما در این خبرنامه درج شود.

تهیه شده در دفتر آمار و فناوری اطلاعات
با همکاری شرکت گسترش فناوری اطلاعات و ارتباطات خاورمیانه
نگارش و مشاوره علمی: احسان ریاضی اصفهانی

آدرس اینترنتی
http://www.Emdad.ir/security

کمیته امداد امام خمینی (ره)
لجنه امداد الامام الخمینی (ره)
Imam Khomeini Relief Foundation