آیا Windows XP قابل اطمینان است؟

تهیه و تنظیم : شهرام انسان
shahramensan@yahoo.com

آخرین نسخه ارائه شده ویندوز، دارای امنیت داخلی بالایی است. با این وجود،بیشتر مدیران در صنعت IT نگران امنیت در محصول جدید مایکروسافت می‌باشند. در این مقاله، نگاهی کوتاه خواهیم داشت به مباحث مطرح شده در اخبار در زمینه امنیت در ویندوز XP.

ویندوز XP عرضه شده است. به زودی حملات آغاز خواهد شد. هزاران نفوذگر در سراسر جهان، در انتظار انتشار نقطه ضعف های ویندوز جدید به سر می برند و وعده حملات گسترده ای را بر پایه نقص های احتمالی ویندوز XP اعلام نموده اند.

با وجود چندین مورد آسیب پذیری در ویندوز XP که درچند ماه گذشته از سوی تحلیل گران امنیت و مدافعان حریم خصوصی اطلاعاتی افراد ارائه شده است، کاربران تست کننده نسخه بتا قادر به پیدا نمودن تهدید امنیتی جدی در ویندوز XP نشده اند. برعکس، بنا به اظهارات جان پسکاتور، مدیر امنیتی شرکت Gartner Inc. حداقل کاری که مایکروسافت در ویندوز XP انجام داده است، از بین بردن اشکالات موجود در نسخه های قدیمی است که این امر بیشتر از آن چیزی است که برای سایر سیستم عامل ها گفته می شود.

نه تنها آنالیست ها و تست کنندگان بتا، مایکروسافت را برای بر طرف نمودن اشتباهات امنیتی گذشته - که باعث نفوذپذیری ویندوزهای ۹x و NT شده بود - ستایش می کنند، بلکه احساس می کنند که لایه های امنیتی جاسازی شده در ویندوز XP، به خصوص قابلیت اعطای حق دسترسی متفاوت به کاربران مختلف و firewall داخلی، به خوبی کاربران و سیستم هایشان را از حملات محافظت می کند، و در مورد نسخه XP Professional همان قابلیت های امنیتی برای پیاده سازی قوانین محلی قابل

اجـرا می باشند.

با این وجود، برخی از متخصصین IT، در باره ارائه یک سیستم عامل مطمئن از سوی مایکروسافت، قانع نشده اند. آنها به امکان آسیب پذیری در تکنولوژی های نوپای Socket و قابلیت دسترسی از راه دور و پشتیبانی از تکنولوژی داخـلی سرویس مدیریت اطلاعات شخصی (Passport) اشاره می کنند.

مشکل، از وجود یک سیستم «back door» در ویندوز که بر اساس «raw sockets» بنا شده است، ناشی می گردد. row socket به معنای یک دسترسی ناقص به اینترنت است و ممکن است نفوذگران، از این طریق بتوانند به سیستم ها نفوذ نمایند. به علت استفاده از پروتکل قـدیمی TCP/IP نفوذگران می توانند از row socket برای ایجاد بسته های اطلاعاتی TCP استفاده کنند، و این در حـالی است که برای شبکه های دریافت کننده این بسته ها، تشخیص مخرب بودن یک بسته اطلاعاتی، غیر ممکن می نماید. روشی برای سد کردن راه این بسته ها وجود ندارد، زیرا در این صورت، مسیر کلیه بسته ها مسدود خواهد شد. البته row socket تکنولوژی جدیدی نیست، چندین نسخه متفاوت Unix، Linux و همچنین Windows ۲۰۰۰ از آن استفـاده می کنند. اما در این سیستم عامل ها، دسترسی به raw socket را در بالاترین سطح دسترسی ممکن قرار داده اند. برخلاف آنها، ویـندوز XP با حق دسترسی کامل نصب می شود که قابلیت دسترسی کامل به سیستم را - حتی به کاربران مبتدی - می دهد.

در پاسخ، متخصصین مایکروسافت معتقدند که حمله از یک ماشین XP بسیار دشوار است، زیرا نفوذگر می بایست برنامه نفوذ را روی ماشین اجرا کند، و این امر به علت وجود firewall داخلی XP دشوار می باشد. تنظیمات پیش فرض firewall به گونه ای است که هر چیزی را کنترل می کند و زمانی تاثیر خود را نشان می دهد که کاربر، چگونگی کنترل اجرای برنامه های exe را نمی داند.

نکته دیگری که در ویندوز XP در نظر گرفته شده است، حذف کلمه عبور پیش فرض کاربر administrator می باشد که در نسخه های گذشته ویندوز، باعث حملات بسیاری شده بود. Firewall ویندوز XP برای کاربران حرفه ای طراحی نشده است. طراحی آن به گونه ای است که کاربران خانگی با اتصال اینترنت با پهنای باند وسیع که از firewall استفـاده نمی کنند، محـافظت شوند.

اما در مورد قابلیت دسترسی از راه دور XP (دستیار ویندوز)، کنترل های بسیاری برای محافظت کاربر و سیستم در برابر حمـلات انجام می شود. کاربر می بایست برای اولین مرتبه دسترسی از راه دور، کد رمز دسترسی را از طریق E-mail رمز شده به سیستم بفرستد. اجازه دسترسی نیز در زمان های کوتاه ۲۴ ساعته (که حتی می تواند بنا به تنظیم کاربران، کوتاه تر نیز باشد) باطل می گردد و سیستم دستیار پس از هر ابطال، درخواست جدیدی از کاربر برای تمدید اجازه دسترسی انجام می دهد...

نکته قابل پیش بینی، این است که در ایام پس از ارائه ویـندوز XP چه نوع از تجاوزات و حمـلات را در پیش خواهیم داشت. در حال حاضر سیاست واضح مایکروسافت درارائه فنـاوری های پیشرفته در امنیت است. اما سوالی که مطرح می شود این است که مایکروسافت در چه زمان و به چه قیمتی تمرکز امنیتی را در محصولات خود خواهد فروخت؟!