پنج نکته مهم ابتدایی در مدیریت امنیتی ویندوز ۸ و ۸.۱

خرداد 8, 1393

با وجود آنکه اکنون ویندوز ۸.۱ به لحاظ امنیتی پیشرفت فراوانی نسبت به نسخه‌های پیشین خود داشته است، به هیچ وجه دلیلی بر آن نیست که شما به اقدامات مایکروسافت ۱۰۰ درصد اطمینان کنید. هنوز مسائل بسیاری وجود دارد که هر کاربر هشیاری باید برای امنیت، سلامت و صیانت از حریم شخصی خود صورت دهد.

نکته امنیتی روز: از Password به Passphrase

استفاده از گذر واژه‌های بلند و طولانی همواره مطمئن و مفید است؛ اما متأسفانه به یاد سپردن آن‌ها دشوار است. برای حل این مسأله می‌توانید از عبارات و جملات برای ایجاد یک گذرواژه استفاده کنید؛ برای نمونه، I Go To Work At ۸ را می‌توان یک Passphrase یا گذر عبارت به شمار آورد که هم امنیت بالایی دارد و هم یادآوری آن ساده است؛ اما بدانید که از جملات و عبارات مشهور و اسامی و لغات قابل حدس همچون نام خود در این Passphrase پرهیز کنید.

ویندوز ۸.۱ را به عنوان امن‌ترین نسخه‌ای که مایکروسافت تا کنون از سیستم عامل خود ارائه کرده است تلقی می‌کنند. در این نسخه از ویندوز مایکروسافت مبحث امنیت را کامل از نو پیاده‌سازی و لایه‌های امنیتی جدیدی را تعبیه کرده است. شاید این موضوع بیش از همه در راستای انتقاداتی بوده که در یک دهه گذشته به امنیت ویندوز وارد شده است.

اما در ورای همه این اقدامات مایکروسافت، چند نکته امنیتی ابتدایی وجود دارد که هر کاربر ویندوز ۸.۱ باید در راستای مدیریت مبحث امنیت مورد توجه جدی قرار دهد. در اینجا نگاهی سریع و خلاصه به این مباحث امنیتی می‌اندازیم.

بروزرسانی‌های ویندوز

کد نوشته شده پشت سیستم عامل ویندوز شامل خلل و فرج امنیتی نیز

می‌شود؛ به این معنا که به هیچ عنوان و تحت هیچ شرایطی نباید بروز رسانی ویندوز را دست کم گرفت؛ اما متأسفانه بخش بزرگی از کاربران این موضوع را جدی نگرفته و از نصب بروز رسانی‌های ویندوز خودداری می‌کنند. این موضوع به ویژه در میان کاربران ایرانی ـ که بیشتر از ویندوزهای غیر قانونی استفاده می‌کنند ـ شیوع بیشتری دارد، زیرا بروز رسانی در مواقعی منجر به از بین رفتن Activation غیر قانونی ویندوز می‌شود.

سه دلیل عمده و اصلی در بروزرسانی ویندوز می‌توان عنوان کرد؛ نخست اینکه با توجه به وجود روزنه‌های امنیتی شناخته نشده در ویندوز، در صورت عدم بروزرسانی، سیستم شما از احتمال بیشتری برای قربانی شدن حملات سایبری برخوردار است. دلیل دوم آنکه بروز رسانی ویندوز، منجر به بهبود عملکرد و ثبات سیستم عامل می‌شود و در نهایت اینکه بروز رسانی منجر به نصب و استفاده از امکانات جدید ویندوز خواهد شد.

نکته دیگر در خصوص بروز رسانی ویندوز این است که به سادگی و خودکار کار خود را انجام می‌دهد. اگر از آن دسته کاربران بی‌حوصله یا فراموش کارید که نمی‌توانید خود اقدام به نصب بروز رسانی‌ها کنید، می‌توانید کل ماجرا را به دست ویندوز بسپارید، یا در غیر این صورت خود اقدام به انتخاب و نصب بروزرسانی‌ها در ویندوز کنید.

برای این کار به Control Panel رفته و روی Windows Update کلیک کنید. سپس از پنل سمت چپ گزینه Change Settings را برگزیده و از لیست پایین افتادنی، گزینه مورد نظر خود را ـ نصب خودکار یا دستی بروز رسانی‌ها ـ انتخاب کنید.

حساب کاربری مایکروسافت

نکته‌های امنیتی بسیاری در استفاده از حساب کاربری مایکروسافت وجود دارد. از زمان انتشار نسخه ۸ ویندوز، همه تلاش مایکروسافت معطوف به کشاندن کاربران از حساب‌های کاربری Local به سمت حساب کاربری آنلاین مایکروسافت بوده که این امکان را فراهم می‌آورد همه تنظیمات و نرم افزارهای کاربر در هر جایی همگام‌سازی شود.

مانند همیشه در ایجاد حساب کاربری و استفاده از آن مهم‌ترین نکته انتخاب یک گذر واژه قوی است. این موضوع به ویژه زمانی اهمیت دارد که از حساب کاربری استفاده می‌کنید که قبلا ایجاد شده؛ اما اکنون در ویندوز مجبور به استفاده دوباره از آن هستید.

از سوی دیگر، اکنون مایکروسافت همچون بسیاری دیگر از رقبای خود از سیستم دو مرحله‌ای برای ورود به حساب کاربری استفاده می‌کند؛ به این معنا که کاربر نیازمند ورود گذر واژه به همراه کدی است که از طریق ایمیل یا SMS به وی فرستاده می‌شود. همچنین اکنون امکان دیدن فعالیت‌های صورت گرفته روی حساب کاربری نیز وجود دارد که کاربر را از فعالیت‌های مشکوک بر روی حساب کاربری خود آگاه سازد.

نکته دیگر در خصوص حساب کاربری مایکروسافت این است که چنانچه از یک حساب Local برای ورود به ویندوز استفاده کنید، قادر به دانلود نرم‌افزارها از Store مایکروسافت نخواهید بود.

به سیستم خود اعتماد کنید!

همان گونه که گفته شد، اکنون این قابلیت در ویندوز وجود دارد که کاربر اقدام به همگام‌سازی یا Sync کردن اطلاعات و داده‌ها روی چندین دستگاه کند؛ اما پیش از آن نیاز است که سیستم کاربر به اصطلاح مورد اعتماد قرار گرفته یا Trust شود.

برای این کار به Control Panel رفته و به بخش Action Center وارد شوید. در این بخش می‌توانید سیستم خود را به لیست دستگاه‌های مورد اطمینان یا Trusted اضافه کنید. پس از آنکه بر دکمه Trust This PC کلیک کردید، به یک وب‌سایت منتقل می‌شوید که از شما درخواست ورود کدی را می‌کند که به ایمیل شما فرستاده شده و یا از طریق SMS به دست شما رسیده است.

آنتی ویروس و حفاظت در برابر بدافزارها

نرم‌افزار Microsoft Security Essentials یا MSE آنتی ویروس رایگان مایکروسافت است. این آنتی ویروس در نسخه‌های XP تا ویندوز ۷ مأمور محافظت از سیستم در برابر بدافزارها را بر عهده داشت؛

اما در ویندوز ۸ به بعد در قالب Windows Defender ادغام شده است.

واقعیت این است که MSE هیچ گاه نتوانست به عنوان یک آنتی ویروس قوی خود را مطرح کند و به ویژه در سال‌های اخیر انتقادات شدیدی از مایکروسافت را سبب شد. از همین روی است که همواره پیشنهاد جایگزین کردن آن یک پیشنهاد عاقلانه است:

متأسفانه Windows Defender نیز چندان بهتر از MSE نیست. در اصل موتور هر دو یکی است و در نتیجه هنوز پیشنهاد این است که اقدام به نصب یک آنتی‌ویروس قوی و مطمئن روی سیستم خود کنید.

تنظیم فایروال در ویندوز

فایروال ذاتی ویندوز ۸ و ۸.۱ دقیقا مشابه نسخه قبلی ویندوز عمل می‌کند. ارتباطات ورودی یا Inbound به کلی Block می‌شوند، مگر آنکه در لیست سفید قرار داشته باشند. در حالی که ارتباطات خروجی یا Outbound در صورتی که از Rule تعریف شده‌ای برخوردار نباشند به شکل پیش فرض مجوز دارند.

در این فایروال کاربران از یک پروفایل ویژه برای مدیریت نرم‌افزارها به شبکه و نت برخوردار هستند و قابلیت تنظیم فایروال برای مدیریت دسترسی ورودی و خروجی نرم افزارها به شبکه و نت فراهم است:

همچنین این فایروال به کاربر اجازه آن را می‌دهد که موقتی همه ارتباطات اینترنتی را قطع کند که در مواقع خاص بسیار مناسب است. از سوی دیگر، در این فایروال بین پروفایل Public و Private تمایز گذاشته شده که کنترل کاربر بر ایجاد محدودیت بر به اشتراک‌گذاری فایل‌ها و دستگاه‌ها روی شبکه‌های عمومی و یا خانگی را فراهم می‌کند.

برای تنظیم فایروال می‌توانید پس از رفتن به Control Panel به بخش Windows Firewall بروید و از پنل سمت چپ گزینه‌هایی را که برای

تنظیم و تغییر عملکرد این ابزار امنیتی است، مرور کنید. هیچ ابایی از دست کاری و تغییر این تنظیمات نداشته باشید و تلاش کنید با آزمون و خطا مناسب‌ترین مقررات و اقدامات را در پیش گیرید. در صورتی که هر گونه مشکلی پیش آید، می‌توانید با فشردن دکمه Restore defaults به تنظیمات اصلی بازگردید.

این موارد از ابتدایی‌ترین کارهایی است که هر کاربر جدید در ویندوز ۸.۱ باید نسبت به آن‌ها هشیار باشد. بی‌گمان لایه‌های امنیتی تعبیه شده از سوی مایکروسافت در دل ویندوز ۸.۱ بسیار فراتر و وسیع‌تر از این‌هاست ـ برای نمونه Secure Boot و Dynamic Access ـ که با کمی کنکاش در دل ویندوز می‌توان آن‌ها را نیز در راستای تقویت خطوط امنیتی ویندوز به کار گرفت.