OUCH! فوریه 2023

ماهنامه آگاهی از امنیت اطلاعات برای شما

آیا من نیاز به برنامه امنیتی دارم؟

مقدمه

سال‌ها پیش زمانی که یک رایانه جدید خریداری می‌کردید، اغلب مجبور بودید نرم‌افزار امنیتی اضافی بر روی رایانه خود نصب کنید تا از ایمن بودن آن در برابر مهاجمان سایبری اطمینان حاصل کنید. با این حال، اکثر رایانه‌ها و دستگاه‌های امروزی دارای ویژگی‌های امنیتی متعددی هستند که به صورت پیش فرض داخل سیستم عامل قرارگرفته است، مانند به‌روزرسانی خودکار، فایروال‌ها، رمزگذاری دیسک و محافظت از فایل‌ها. علاوه بر این، مایکروسافت قابلیت امنیتی به نام Microsoft Defender را در رایانه های ویندوزی ارائه می دهد که شامل ویژگی های بیشتری مانند آنتی ویروس است. از بسیاری جهات، سیستم های امروزی به صورت پیش فرض بسیار امن تر هستند. در واقع، شما به احتمال زیاد اکنون بزرگترین نقطه ضعف هستید. به همین دلیل است که مهاجمان سایبری به طور مداوم افراد را مورد هدف قرار می دهند و سعی می کنند شما را فریب دهند تا کارهایی را انجام دهید که نباید انجام بدهید، مانند فاش کردن رمز عبور خود، کلیک کردن بر روی پیوندها یا باز کردن پیوست های ایمیلی که بدافزار را روی رایانه شما نصب می کنند یا به اشتراک گذاشتن اطلاعات کارت اعتباری خودتان.

کدام ابزارها را میبایست در نظر بگیرم؟

اگر می‌خواهید چند قدم اضافی برای ایمن کردن سیستم‌های خود بردارید، برنامه های امنیتی بیشتری نیز وجود دارند که میتوانید آنها را در نظر بگیرید.

مدیریت رمز عبور: رمزهای عبور می‌توانند پیچیده و طاقت‌فرسا باشند، مخصوصاً میبایست صدها رمز عبور مختلف را به خاطر بسپاریم. مدیر رمز عبور(Password Manager) یک انبار امن است که تمام رمزهای شما را ذخیره و از آنها محافظت میکند، بنابراین شما باید فقط یک رمز عبور اصلی را به خاطر بسپارید. علاوه بر این، آنها می توانند شما را وارد وب سایت ها کرده، رمز عبور برای شما ایجاد کنند و به اعتبارسنجی وب سایت های خاص کمک کنند.

شبکه خصوصی مجازی (VPN): VPN ها در درجه اول بر محافظت از حریم خصوصی شما با رمزگذاری اتصال شما به اینترنت و پنهان کردن مکان و مبدا شما تمرکز می کنند.

Security Suites: اینها بسته‌هایی از نرم‌افزار امنیتی هستند که مجموعه‌ای از ویژگی‌های امنیتی اضافی را بیشتر و فراتر از آنچه سیستم عامل شما قبلاً ارائه داده، فراهم می‌کنند. به عنوان مثال، فیلتر کردن وب سایت های خطرناک، کنترل های والدین و اغلب یک VPN نیز ارائه میکنند. هر بسته نرم افزاری دارای ویژگی‌های متفاوتی است، بنابراین در صورت نیاز به یکی از آنها برای یافتن موردی که میتواند بهترین گزینه برای شما باشد، تحقیق کنید.

انتخاب یک فروشنده محصولات امنیتی

اگر نیاز به خرید ابزار یا نرم افزار امنیتی اضافی دارید، فروشندگان مختلفی وجود دارد که می توانید از بین آنها انتخاب کنید. کدام یک را می بایست انتخاب کنید ؟ اغلب اوقات فروشندگان مختلف در ویژگی هایی که ارائه می دهند بیشتر شبیه هم میباشند و کمتر با هم تفاوت دارند. نکته کلیدی استفاده از راهکارهای یک فروشنده قابل اعتماد است. شما نمی خواهید به طور تصادفی چیزی را خریداری و نصب کنید که توسط مجرمان سایبری تهیه و ارائه شده و به بدافزارآلوده شده است.

ابزارها را فقط از فروشندگان معروفی که نام آنها را شنیده و به آنها اعتماد دارید خریداری کنید. هرگز از شرکتی که چیزی در مورد آن نمی دانید، یا کاملاً جدید و تازه تاسیس است، یا نظرات کاربران ندارد و یا نظرات منفی بسیاری دارد، ابزاری خریداری نکنید. شما می خواهید مطمئن باشید که راه حلی که خریداری می کنید کاملا قانونی بوده و به صورت فعال به روزرسانی شده و نگهداری می شود. حتی ممکن است بخواهید این موضوع را در نظر بگیرید که فروشنده در کدام کشور مستقر شده است. سایت‌های آنلاین متعددی وجود دارند که بررسی‌هایی از فروشندگان مورد اعتماد دارند که تفاوت‌ها در ویژگی‌ها و هزینه‌های نرم‌افزار امنیتی مختلف را نشان می‌دهند.

مراقب ابزارهای رایگان باشید. در حالی که ابزارهای امنیتی رایگان عالی وجود دارند، ممکن است نگرانی هایی وجود داشته باشد. این ابزارها ممکن است از نظر ویژگی‌ها محدود شده باشند، استفاده از آنها دشوار باشد، یا اغلب مواقع به روزرسانی نشوند. در برخی موارد، ابزارهای رایگان ممکن است توسط مهاجمان سایبری توسعه یافته و سپس به بدافزار آلوده شده باشند.

به یاد داشته باشید، در حالی که این ابزارهای امنیتی مفید هستند، ابتدا با ویژگی های امنیتی داخلی رایانه خود شروع کنید، که شامل فعال کردن به روز رسانی خودکار نیز می شود. سیستم عامل های امروزی به طور پیش فرض بسیار امن هستند. در انتها، شخص شما بهترین دفاع از خودتان خواهید بود. نسبت به هرگونه تماس تلفنی عجیب یا مشکوک، ایمیلها یا پیامکهای غیرعادی، محتاط باشید. هیچ نرم افزار امنیتی در جهان نمی تواند شما را در برابر کسی که سعی دارد شما را فریب دهد یا به کاری که نباید انجام دهید ترغیب کند، محافظت نماید.

سردبیر مهمان

Nico "Dutch_OsintGuy" Dekens یک مربی معتبر SANS و تحلیلگر اطلاعاتی دولتی سابق است که متخصص در اطلاعات منبع باز (OSINT) است.
اطلاعات بیشتر را در مورد Nico اینجا ببینید:https://www.sans.org/profiles/nico-dekens
و در اینجا https://www.dutchosintguy.com.

منابع

برنامه های مدیریت رمز عبور: https://www.sans.org/newsletters/ouch/password-managers
قدرت به روز رسانی: https://www.sans.org/newsletters/ouch/the-power-of-updating
شبکه های خصوصی مجازی: https://www.privacyguides.org/vpn
مهندسی اجتماعی: https://www.youtube.com/watch?v=lc7scxvKQOo
بررسی مجموعه ابزارهای امنیتی: https://www.pcmag.com/picks/the-best-security-suites

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو