Ouch! اکتبر 2023

SANS SECURITY AWARENESS

قدرت به روز رسانی (آپدیت)

مقدمه

مهاجمان سایبری به طور مداوم به دنبال و یافتن آسیب پذیری های جدید در نرم افزارهایی هستند که هر روز از آنها استفاده می کنید. آسیب پذیری یک اشتباه یا ضعف در نحوه توسعه نرم افزار است. این نرم‌افزار ممکن است لپ‌تاپ شما، برنامه‌های تلفن همراه روی گوشی هوشمند یا شاید حتی نرم‌افزار موجود در ترموستات شما را اجرا کند. مهاجمان سایبری از این آسیب‌پذیری‌های نرم‌افزاری سوء استفاده کرده تا بتوانند از راه دور به سیستم‌ها، از جمله سیستم‌هایی که شما استفاده می‌کنید، نفوذ کنند. در همان زمان، تولید کنندگانی که دستگاه‌ها و نرم‌افزارها را میسازند، دائماً در حال توسعه راههای جدید برای رفع این آسیب‌پذیری‌ها هستند و آنها را به‌عنوان به‌روزرسانی نرم‌افزار ارائه میدهند. یکی از بهترین راه‌هایی که می‌توانید از خود محافظت کنید این است که مطمئن شوید فناوری‌هایی که استفاده می‌کنید همیشه آخرین به‌روزرسانی‌ها را دارند. این به‌روزرسانی‌ها نه تنها آسیب‌پذیری‌های شناخته‌شده را برطرف می‌کنند، بلکه اغلب، ویژگی‌های امنیتی جدیدی را اضافه می‌کنند که هک کردن دستگاه‌های شما را برای مهاجمان سایبری سخت‌تر می‌کند.

به روز رسانی ها چگونه کار میکنند

هنگامی که یک آسیب‌پذیری نرم‌افزاری شناخته می‌شود، توسعه‌دهنده یا سازنده یک تعمیر نرم‌افزاری برای آسیب‌پذیری ایجاد می‌کند (به نام Patch) و به‌روزرسانی را برای عموم منتشر می‌کند. سپس سیستم شما این به‌روزرسانی را دانلود و نصب می‌کند و آسیب‌پذیری‌ها را برطرف می‌کند. نمونه هایی از نرم افزارهایی که باید به روز رسانی کنید عبارتند از:

- سیستم عامل هایی که لپ تاپ شما را اجرا می کنند (مانند Microsoft Windows یا Apple OSX) یا در تلفن هوشمند شما وجود دارند (مانند Android یا iOS)
- تجهیزات شبکه خانگی مانند روتر اینترنت یا اکسس پوسنت Wi-Fi یا دستگاه های هوشمند خانگی مانند ترموستات، زنگ در، لوازم خانگی یا دوربین های امنیتی
- برنامه هایی که روی دستگاه های شما اجرا می شوند، مانند مرورگر وب لپ تاپ یا برنامه های تلفن همراه شما

به همین دلیل است هر زمان که می‌خواهید یک دستگاه جدید بخرید یا یک برنامه رایانه یا برنامه تلفن همراه جدید نصب کنید، ابتدا بررسی کنید تا مطمئن شوید که فروشنده به طور فعال برنامه یا دستگاه را به‌روزرسانی می‌کند. هر چه نرم افزار مدت زمان بیشتری بدون به روز رسانی کار کند، احتمال آسیب پذیری آن بیشتر می شود و مهاجمان سایبری می توانند از آنها سوء استفاده کنند. به همین دلیل است که بسیاری از فروشندگان، مانند مایکروسافت، هر ماه به طور خودکار وصله های جدید را منتشر می کنند. علاوه بر این، اگر دیگر از یک برنامه کامپیوتری، نرم افزار یا برنامه موبایل خاص استفاده نمی کنید، آن را از سیستم خود حذف کنید. هرچه نرم افزارهای کمتری نصب کرده باشید، آسیب پذیری های احتمالی کمتری دارید و امنیت بیشتری خواهید داشت. در نهایت، اگر هر یک از دستگاه‌ها یا برنامه‌های شما قدیمی است و دیگر توسط فروشنده پشتیبانی نمی‌شود، توصیه می‌کنیم آن‌ها را با نسخه‌های جدیدتر که به صورت فعال به‌روزرسانی و پشتیبانی می‌شوند جایگزین کنید.

نحوه به روز رسانی

دو راه برای به روز رسانی سیستم شما وجود دارد.

1. به صورت دستی(راه سختتر): هنگامی که یک به روز رسانی در دسترس است، به صورت دستی به روز رسانی را دانلود و نصب می کنید. این به شما کنترل بیشتری میدهد که چه چیزی را در چه زمانی نصب کنید. عیب به‌روزرسانی‌های دستی این است که کار بسیار بیشتری میطلبد، زیرا نه تنها باید زمان به‌روزرسانی هر یک از دستگاه‌ها یا برنامه‌های خود را شناسایی کنید، بلکه باید آنها را به‌صورت دستی به‌روزرسانی کنید، که باعث می‌شود فراموش کردن به روز رسانی آنها آسانتر گردد.

2. اتوماتیک (راه آسان تر): شما به‌روزرسانی خودکار را در همه دستگاه‌های خود فعال می‌کنید، به این معنی که هر زمان یک پچ جدید منتشر شد، دستگاه شما به‌طور خودکار آن را دانلود و نصب می‌کند. مزیت به روز رسانی خودکار این است که بیشتر کار را خودکار برای شما انجام میدهد. نقطه ضعف به روز رسانی خودکار این است که برنامه به روز شده می تواند مشکل ایجاد کند و در نتیجه باعث عملکرد نادرست یا از بین رفتن داده ها شود. این برای دستگاه‌های شخصی نادر است، اما می‌تواند برای محیط‌های پیچیده‌تر، مانند شرکت‌های بزرگ اتفاق بیفتد. وقتی به‌روزرسانی‌های خودکار را فعال می‌کنید، حتماً سیستم خود را مرتباً بررسی کنید تا مطمئن شوید به‌روزرسانی‌ها انجام می‌شوند.

از بین دو رویکرد فوق، ما به شدت توصیه می کنیم که به روز رسانی خودکار را در تمام دستگاه های شخصی خود فعال کرده و از آن استفاده کنید. این تضمین می‌کند که تمام فناوری‌هایی که استفاده می‌کنید، از تلفن هوشمند و لپ‌تاپ گرفته تا مانیتور کودک و قفل درب، دارای جدیدترین نرم‌افزار هستند. دستگاه‌ها و نرم‌افزارهای به‌روزشده، هک کردن شما و سیستم‌هایتان را برای هر مهاجم سایبری بسیار سخت‌تر می‌کنند.

سردبیر مهمان

دکتر Janell Straach یکی از اعضای هیئت علمی دانشگاه رایس است که در آنجا امنیت سایبری و هوش مصنوعی را تدریس می کند. جانل رئیس هیئت زنان در امنیت سایبری (WiCyS) است. دکتر straachl را در janell@wicys.org دنبال کنید.

منابع

پاکسازی بهاری سایبر دیجیتال: https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps
آیا نیاز به نرم افزار امنیتی دارم؟: https://www.sans.org/newsletters/ouch/security-software
محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you

ترجمه شده برای عموم توسط: هومن خجاو، مجید هدایتی