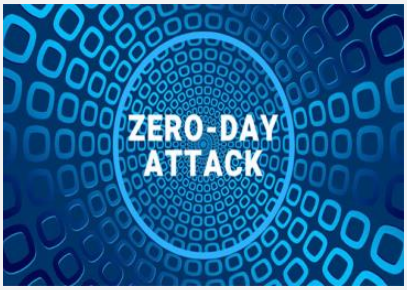

یکشنبه 26 بهمن 1399 - 13:33

امنیت به زبان ساده

امنیت به زبان ساده: آسیب‌پذیری روز صفر چیست و چطور کار می‌کند؟

آسیب پذیری روز صفر یک نقص امنیتی نرم افزاری است که سازنده نرم افزار از وجودش باخبر است اما هنوز به روزرسانی لازم برای برطرف سازی مشکل را منتشر نکرده. به این ترتیب، توسعه دهنده ای که از آن نرم افزار استفاده می کند از روز نخست با آسیب پذیری ای مواجه است که می تواند مورد سوء استفاده مجرمان سایبری قرار بگیرد.

در جهان امنیت سایبری، آسیب پذیری به معنای نواقص ناخواسته ای است که در سیستم عامل ها و نرم افزارها یافت می شود. آسیب پذیری ها چه می توانند نتیجه تنظیمات نامناسب امنیتی یا کامپیوتری باشند، چه اشتباهات توسعه دهنده در کدنویسی. و اگر از این نواقص چشم پوشی شود، حفره هایی به وجود می آید که هکرها به راحتی قادر به استفاده از آن خواهند بود.

چرا آسیب پذیری ها خطر امنیتی دارند؟

هکرها کدی را می نویسند که نواقص امنیتی را به صورت خاص هدف قرار می دهند. آن ها از نواقص درون یک پکیج بدافزاری استفاده می کنند که آسیب پذیری روز صفر نام می گیرد. این نرم افزار بدخواهانه می تواند از یک آسیب پذیری سوء استفاده کرده و یک سیستم کامپیوتری را به خطر بیندازد یا منجر به رفتارهای ناخواسته در آن شود. در اکثریت مواقع، توسعه دهنده اصلی نرم افزار می تواند با یک پچ، مشکل را رفع و رجوع کند.

چه می شود اگر کامپیوترتان آلوده شود؟ بدافزار شروع به سرقت اطلاعات خصوصی می کند و هکرها قادر خواهند بود که کنترل کامپیوتر را به دست بگیرند. خود نرم افزار نیز ممکن است به روش هایی مورد استفاده قرار گیرد که قرار نبوده قادر به انجام شان باشد. برای مثال ممکن است به نصب بدافزارهای دیگری کمک کند که فایل ها را آلوده می کنند یا منجر به ارسال پیام های خاص برای افراد حاضر در لیست مخاطبان می شوند. حتی می توان به نصب یک جاسوس افزار پرداخت و تمام اطلاعات حساس را استخراج کرد.

آسیب پذیری روز صفر دقیقا چیست؟

عبارت «روز صفر» به جدید بودن کشف آسیب پذیری نرم افزاری اشاره دارد. از آن جایی که توسعه دهنده تازه از وجود نقص باخبر شده، یعنی هنوز فرصتی برای انتشار به روزرسانی لازم نداشته و آسیب پذیری کماکان قابل سوء استفاده است. بنابراین «روز صفر» یعنی توسعه دهندگان به معنای واقعی کلمه «صفر روز» برای حل مشکل وقت داشته.

وقتی آسیب پذیری عمومی شود، توسعه دهنده اصلی باید تمام تلاش خود را به کار بگیرد تا در سریع ترین زمان ممکن، از کاربران محافظت کند. اما گاهی هم سازندگان نرم افزار در عرضه پچ پیش از دست به کار شدن هکرها شکست می خورند و شرایط وخیم تر می شود. به حملات هکرها در چنین حالتی، «حمله روز صفر» گفته می شود.

در برابر آسیب پذیری های روز صفر چه می توان کرد؟

آسیب پذیری های روز صفر خطرات امنیتی بسیار جدی با خود به همراه می آورند و می توانند خسارات فراوانی به کامپیوتر یا اطلاعات شخصی شما وارد کنند. بنابراین برای محافظت از این اطلاعات لازم است که تدابیر امنیتی لازم را به کار بسته باشید. نخستین خط دفاع شما، استفاده از آنتی ویروس های قدرتمند و معتبر است که از شما هم در برابر خطرات ناشناخته و هم شناخته شده محافظت کند.

دومین خط دفاعی هم نصب آخرین به روزرسانی های نرم افزار و سیستم عامل است. این به روزرسانی ها معمولا قابلیت های جدید اضافه می کنند، قابلیت های قدیمی را حفظ می کنند، منجر به به رزورسانی درایورها می شوند، باگ ها را از بین می برند و مهم تر از همه، حفره های امنیتی شناخته شده را ترمیم می کنند.

بنابراین برای حصول اطمینان از اینکه حملات روز صفر گریبان تان را نمی گیرند، باید تمام کارهای لیست شده در پایین را انجام دهید:

نرم افزارها و پچ های امنیتی را به روز نگه دارید و آخرین آپدیت ها را دانلود کنید. به این ترتیب به نصب پچ هایی امنیتی می پردازید که باگ هایی را رفع کرده اند که در ورژن های قبلی یا وجود نداشته اند یا از چشم دور مانده اند.

برای خود عادات تازه ای در زمینه محافظت از حریم شخصی در فضای آنلاین به وجود آورید.

تنظیمات امنیتی سیستم عامل، مرورگر اینترنت و نرم افزارهای امنیتی را بهبود ببخشید.

یک نرم افزار امنیتی معتبر و قدرتمند نصب کنید تا آسیب پذیری های ناشناخته و شناخته شده به راحتی مورد سوء استفاده قرار نگیرند.

یک مثال برجسته از حملات روز صفر

استاکس نت که یک جور آسیب پذیری روز صفر به حساب می آید یکی از نخستین تسلیحات دیجیتالی جهان به حساب می آید. استاکس نت یک کرم کامپیوتری بسیار شیوع پذیر است که با شبیه سازی مداوم خود، در کار تاسیسات هسته ای ایران اختلال ایجاد کرد. این کرم توانست کنترل کامپیوترها را به دست بگیرد، سرعت گردش سانتریفیوژ ها را دستکاری کند و عملا تاسیسات را از کار بیندازد.

اریک چین و لیام اومارچو دو محقق امنیتی هستند که به بررسی ابعاد مختلف این کرم کامپیوتری پرداختند. آن ها دریافتند که استاکس نت یک کرم کامپیوتری بسیار خوش ساخت است که تنها یک دولت قادر به ساخت آن برای کنترل تاسیسات صنعتی در ابعاد وسیع است. این دو به کمک یک تیم امنیت سایبری توانستند راه حلی برای مبارزه با این کرم بیابند.
نکاتی که باید راجع به آسیب پذیری های روز صفر در یاد داشت

نرم افزار را به روز نگه دارید تا از خودتان درباره آسیب پذیری روز صفر محافظت کنید.
بعد از اعلام وجود آسیب پذیری، پیگیر اخبار مربوط به راه حل مقابله با آن باشید. اکثر توسعه دهندگان به سرعت آسیب پذیری های امنیتی را پچ می کنند.
تهدید را دست کم نگیرید. مجرمان سایبری به طور یقین در پی سوء استفاده از حفره های امنیتی و دسترسی یافتن به دیوایس ها و اطلاعات شخصی شما خواهند بود. با اطلاعات استخراج شده، آن ها قادر به ارتکاب جرایمی نظیر مانند سرقت هویت، کلاه برداری بانکی یا باج گیری خواهند بود

https://dgto.ir/1wwz