اضافه شدن ده ها بدافزار به ضدویروس ایمن

در اردیبهشت ماه سال جاری تعداد ۲۳۶ بدافزار به پایگاه داده ضدویروس ایمن افزوده شده است. از جمله این نرم افزارهای مـوذی و مـزاحم می توان به گونه های مختلف دانلودرها، Poison، Onlinegames، Frauder و ... اشاره کرد. *(منبع: مهران رایانه)*

راهنمای آزمایش امنیت شبکه (قسمت چهل و ششم – مبانی عمومی امنیت اطلاعات)

به هنگام اصلاح نواقص و ناهنجاری های امنیتی، باید یکسری قواعد و اصول را رعایت نمود:

۱. سادگی[1]: مکانیسم های امنیتی (و به طور کلی سیستم های اطلاعاتی) باید تا سر حد امکان «ساده» طراحی شـود. اصولاً پیچدگی، خود می تواند به منشا بسیاری از معضلات امنیتی تبدیل گردد.

۲. خرابی ملایم[2]: به هنگام بروز اشکال و اخطار، سیستم باید «به صورتی ایمن» دچار خطـا شـود. بـه عبـارت دیگـر هنگامی که نقصی در عملکردها پیش می آید، امنیت باید همچون پابرجا باشد. مخدوش شدن عملکرد بسیار بهتـر از ضربه وارد شدن به امنیت است.

۳. واسطه کامل و فراگیر[3]: علاوه بر دسترسی مستقیم به اطلاعات، میانجی ها یا همان واسطه ها باید به برخی منابع دسترسی عمومی داشته باشند. مثال رایج آن عبارت است از وب پروکسی ها، mail gateway ها و files system permission ها.

۴. طراحی باز[4]: در طراحی یا اجرای مباحث امنیتیِ سیستم ها نباید بـه پنهـان کـاری روی آورد. "امنیـت در تـاریکی" سودی نخواهد داشت.

۵. تفکیک امتیازات[5]: حتی المقدور حقوق و اختیارات را از یکدیگر تفکیک کنید. این امر هم بـه سیـستم هـا مربـوط

---

[1] Simplicity
[2] Fail-Safe
[3] Complete Mediation
[4] Open Design
[5] Separation of Privilege

می‌شود و هم به اپراتورها و کاربران. به عنوان مثال اگر منابع به شما اجازه می دهد، دسترسی ها و قوانین مربوط به مدیران سیستم ها را به گونه ای متفاوت و مجزا از اختیارات مدیران امنیتی تعیین نمایید.

۶. پذیرفتگی‌های روانشناسانه[6]: کاربران باید اهمیت امنیت را درک کنند. این کار را می‌توان از طریق ارائه آموزش-های لازم به آنان صورت داد. علاوه بر این، مکانیسم های امنیتی مورد استفاده باید به گونه ای باشد که حس مهم بودن امنیت را به آنها القا کند. اگر کاربران ببینند که مکانیسم های امنیتی دست و پا گیر هستند و کار کردن با آنها دشوار است، آنها راه هایی برای دور زدن این مکانیسم ها خواهند یافت!

۷. دفاع چند لایه[7]: سازمان ها باید متوجه این نکته باشند که استفاده از یک متد امنیتی به تنهایی، معمولاً کارساز و کافی نخواهد بود. مکانیسم های امنیتی (دفاع) باید در چند لایه طراحی شوند تا نفوذ به آنها عملاً کار دشوار و طاقت فرسایی باشد. با جادو و جمبل نمی توان برای اطلاعات سیستم ها، امنیت فراهم کرد!

۸. ثبت موارد نفوذ[8]: وقتی سیستم ها یا شبکه ها مورد حمله و اخلال قرار می گیرند، رکوردها و لاگ های این حوادث باید ساخته و ذخیره شود. از این اطلاعات ذخیره شده می توان برای بهبود امنیت و نیز شناسایی شیوه های نفوذ هکرها استفاده کرد. در واقع با کنکاش این اطلاعات می توان راه هایی برای بالا بردن سطح امنیت شبکه یافت.

(منبع: مهران رایانه)

ترجیع بند مایکروسافت!

مایکروسافت از شناسایی یک حفره دیگر در مجموعه ای از محصولات خود خبر داده است. بر اساس این گزارش مایکروسافت ضمن اعلام وجود یک آسیب پذیری امنیتی خطرناک در Windows 2000، Windows XP و Windows Server 2003 به کاربران هشدار داده است که اگر این باگ، اصلاح نشده به حال خود رها گردد، این امکان وجود دارد که هکرها با استفاده از آن، کنترل رایانه قربانی را

[6] Psychological Acceptability
[7] Layered Defense
[8] Compromise Recording

تهیه کننده: شرکت مهندسی مهران رایانه – واحد پشتیبانی فنی | تلفن: ۲۲۰۵۰۷۸۰ – ۲۶۲۰۲۴۹۳
آدرس: تهران- انتهای بلوار آفریقا – خ شهید طاهری – ایثار۳ – ایثار۲ – شماره ۱۷ – ساختمان مهران | نمابر: ۲۲۰۵۳۹۲۷

به دست گیرند. بنا به اعلام وبلاگ Microsoft Security Response Center موسوم به MSRC، این مـشکل در Microsoft DirectX قـرار دارد و هکرها قادرند با بهره گیری از فایل های ویدئویی کوئیـک تـایم، از آن سو استفاده کنند. MSRC با بیـان اینکـه ایـن بـاگ در کوئیـک تـایم Apple وجود ندارد، گفته است که کد آسیب پذیر، از ویندوز ویـستا، وینـدوز ۷ و Windows Server 2008 حـذف شده است. *(خبر: MX Logic - تصویر: guy-sports.com)*

حمله یک بدافزار به ۳۰ هزار وب سایت

CyberInsecure در گزارش ۳۰ مـی (۹ خرداد) به نقل از The Register اعلام کرد که یک بدافزار قوی به ۳۰ هزار وب سایت اعـم از تجـاری، دولتـی و غیره حمله ور شده است. در ایـن تهـاجم، یـک جـاوا اسـکریپت مخرب در صفحه اول وب سایت ها جاسـازی مـی شـود کـه در نهایت، عملکرد آن به SQL injection منجر می گردد. این کد به گونـه ای طراحـی شـده کـه مـشابه بـا اسـکریپت Google Analytics (تحلیلگر گوگـل) از آب درآیـد. کـد مـذکور از جـاوا اسکریپت نامشخصی استفاده می کند و همین امر، مقابله با آن را مشکل می سازد. به نظر می رسد اسـتفاده از چنـین ترفند بزهکارانه ای، با رشدی صعودی همراه بوده است. *(منبع: Doğan ÇAKMAK)* ■

- *نظرات، انتقادات و پیشنهادهای شما برای ما ارزشمند است: support@MehranCo.com*
- *منابع اخبار و تصاویر در «پشتیبانی فنی شرکت مهندسی مهران رایانه» موجود است.*
- *وب سایت رسمی شرکت مهندسی مهران رایانه، www.MehranCo.com می باشد.*
- *استفاده از اخبار و مطالب خبرنامه «با ذکر منبع» بلامانع است.*