خشم کاربران Gmail از سیل هرزنامه ها

Gmail، سرویس ایمیل شرکت گوگل است که بدلایل مختلف مورد قبول کاربران واقع شده است. رایگان بودن، ارائه فضای بالا و کاربرپسند بودن از جمله این عوامل است. ولی امنیت چه؟ آیا می توان جیمیل را یک سرویس امن و با خطرپذیری اندک نامید؟ پاسخ به این سوال خود فضا و مجالی دیگر می طلبد ولی عجالتاً گزارش شده که کاربران Gmail به گونه ای دیوانه وار و خشمگین، از سیل هرزنامه هایی سخن می گویند که inbox آنها را درنوردیده است! این اعلام نظرها از هفته چهارم آوریل آغاز شده و تا انتهای ماه می ادامه داشته است. در برخی از این اظهار نظرها ادعا گردیده که فیلتر هرزنامه Gmail کارایی مخدوش و نامطلوبی داشته است.

به هر حال اکنون بیش از یک ماه است که از بروز این مشکل می گذرد و تعداد کاربرانی که با گله مندی از جیمیل، از افزایش سرسام آور spam ها در ایمیل خود سخن می گویند، سیر صعودی داشته است. XLogic در اول ژوئن به نقل از یکی از کاربران جیمیل گزارش داده که تعداد بسیار زیادی هرزنامه، با عبور از سد فیلترها، توانسته به inbox کاربران راه یابد. سخنگوی گوگل اعلام کرد که یک پیکره بندی نادرست در تعداد اندکی از serverهای گوگل، باعث فیلتر نشدن هرزنامه ها گشته است. وی همچنین خاطرنشان کرد که این مشکل، فقط گریبانگیر یک درصد از کاربران Gmail بوده است. سخنگوی گوگل ضمن اعلام عذرخواهی شرکت متبوع خود، از حل این مشکل خبر داد. *(منابع: SPAMfighter News و SpamDefy)*

آسیب‌پذیری‌های Symantec Altiris Deployment Solution

گزارش اخیر *secunia* از بروز چندین ضعف امنیتی در نرم افزار Altiris Deployment Solution سیمانتک خبر می دهد. این باگ ها می تواند برای ارتقا سطح دسترسی یا دستکاری برخی داده ها، مورد سو استفاده کاربران محلی قرار گیرد. اجرای حملات SQL injection و رخنه به سیستم های آسیب پذیر نیز از دیگر معضلات ناشی از این نواقص قلمداد شده است.

راهنمای آزمایش امنیت شبکه (قسمت چهل و هشتم – مقایسه تطبیقی ، بخش دوم)

در ادامه بحث مقایسه تطبیقی بین تکنیک های مختلف تست شبکه، مزایا و معایب «تست نفوذ» را مرور می کنیم:

۳. تست نفوذ (Penetration Testing)

مزایا:

- با استفاده از ابزارها و شیوه های خود هکرها، شبکه را تست می کند؛
- آسیب پذیری ها را درستی سنجی (verify) می کند؛
- به پشت حفره ها می رود و میزان خطرناک بودن آنها را تشخیص می دهد؛
- تعیین می کند که آیا این حفره ها تئوری هستند یا خیر؛
- می تواند منجر به جمع آوری اطلاعات و شواهدی شود که برای رفع حفره ها مفید است؛
- در آن می توان از مهندسی اجتماعی استفاده کرد.

ضعف ها:

- برای اجرا، به تجارب بالایی نیاز است؛
- برای اجرا، به کار طاقت فرسایی نیاز است؛
- کند است. ممکن است عملکرد میزبان های مقصد، ساعت ها یا روزها مخدوش گردد؛
- با توجه به زمانی که برای انجام این آزمون مورد نیاز است، در شبکه های متوسط یا بزرگ نمی توان تمام میزبان ها را تست کرد؛
- استفاده تست کننده های ناشی یا کم تجربه از آن، ممکن است می تواند خطرساز باشد؛
- ابزارها یا تکنیک های خاص مورد استفاده برای این امر (از قبیل network sniffers، password crackers و ...)، ممکن است در چارچوب قوانین دولتی، محذور یا ممنوع باشد؛
- گران است؛
- ممکن است ساختار عملیاتی سازمان را به هم بریزد. *(منبع: مهران رایانه)*

دانش آموز هکر دستگیر شد

پلیس ایالتی نیویورک در کلیفتن پارک، از دستگیری یک هکر دبیرستانی خبر داده است. وی که ۱۶ سال سن دارد و به نام Matthew Beighey معرفی شده، متهم است که با نفوذ به رایانه های دبیرستان، جلوی عملکرد صحیح آنها را گرفته است. بنا به گفته پلیس، این نفوذگر با استفاده از نام کاربری و کلمه عبور یک دانش آموز دیگر، به شبکه وارد شده است. *(منبع: Capital News 9)*

دو رقیـب بیـمار!

شناسایی چندین باگ دیگر در دو مرورگر مهم اینترنتی کـه اتفاقـاً بـا یکـدیگر رقیب می باشند، باز هم خبرساز شـده اسـت. بـر اسـاس گـزارش موجـود، بـاگ هـای خطرناکی که در ***فایرفاکس*** کشف شده، راه را برای تبهکـاری هـایی همچـون دور زدن تدابیر امنیتی، اسپوفینگ (Spoofing)، افشای داده های مهم و حساس، اجرای حملات DoS و ... باز می کند. باگ های جدید ***اینترنت اکسپلورر*** نیز که در نسخه های 5.01 و 6.x و 7.x و 8.x نـرم افـزار Microsoft Internet Explorer یافـت شـده، «خطرناک» بوده و امکان دسترسی به سیستم قربانی را برای هکرها به ارمغان می‌آورد.

گفتنی است باگ‌های فایرفاکس، نسخه Mozilla Firefox 3.x را تهدید می کند. *(منابع: secunia و SitePoint)*

هک شدن یک ISP، به خودکشی مدیر آن انجامید

شرکت VAserv کـه ارائـه کننـده سرویس های میزبانی برای سایت های اینترنتی است، مورد حمله ویروسی قرار گرفته و اطلاعـات حـدود ۱۰۰ هـزار سایت آن پاک شده است. نفوذگران با بهـره گیـری از بـاگ موجـود در نـرم افـزار مجـازی سـازی HyperVM، بـه serverهای شرکت رخنه نموده و تمام اطلاعات مندرج در آن را پاک کرده اند. به نظر می رسد هکرها به اطلاعـات کارت اعتباری مشتریان و دیگر داده های ثبت شده در server های شرکت دست یافته اند. گفتنی است HyperVM یک برنامه مجازی سازی است که توسط شرکت هندی LXLabs طراحی و تولید شده است. در ادامـه گـزارش آمـده است که K T Ligesh رئیس ۳۲ ساله LXLabs با حلق آویز کردن خود، دست به خودکشی زده اسـت. جـسد وی در خانه اش واقع در بنگ لر استان کارناتکای هند یافت شد. *(منبع: Techworld)* ■

- *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.*