باسمه تعالی

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co.

خبرنامه تخصصی - امنیتی مهران رایانه
(شـمـاره ۱۸٤)

خـبـرنـامـهٔ هفـتگی در حـوزهٔ **امـنـیـتِ**
اطلاعات رایانه ای، شبکه ها و اینترنت

برگزاری همایش آسیب پذیری و امنیت در خدمات اینترنتـی

مرکـز پدافنـد غیرعامل فاوای کشور در نظر دارد در چهاردهم مرداد ماه سال جاری با برگزاری همایشی بـا عنـوان «همـایش آسـیب پذیری و امنیت در خدمات اینترنتی»، با استفاده از تفکـرات و ایـده هـای اندیـشمندان و صاحبنظران این عرصه، ضمن توجه دادن جامعه به این مقوله مهم و حیاتی، در راسـتای تدوین الگوی مناسب برای بهره برداری از شـبکه اینترنـت گـام هـای اصـولی واولیـه را بردارد. بنا به گزارش سایت سازمان پدافند غیرعامل کشور، اهداف اصـلی ایـن همـایش عبارت است از ۱. تبیین تهدیدات و آسیب هـای گونـاگون در اسـتفاده ازسـرویس هـای اینترنتی و ۲. آشنائی با اقدامات امنیتی، پیشگیری و مقابله دفاعی در مقابل تهدیدات و آسیب ها. خاطرنشان مـی شـود شرکت مهندسی مهران رایانه به عنوان یکی از حامیان این همایش، در آن حضوری فعال خواهد داشت. *(منبع: مهران رایانه)*

پارکینگ ها هم هک شدند!

قانون شکنان حتی می توانند بلیط های هوشمند پارکبان های الکترونیکی را هم هک کنند و در این شلوغی و کمبود جایی که در کلان شهرها دیده می شود، تا هر وقت که دلـشان خواست خودروی خود را در محل پارک نگه دارند! این، حکایتی است که در برخی شهرهای بزرگ آمریکا رخ داده است. به گزارش CNN با دستکاری برنامه های این نوع پارکبان ها می توان به راحتـی آنهـا را هک کرد و یک محل پارک رایگان و البته نامحدود برای خود دسـت و پا کرد! گفتنی است در سال ۲۰۰۳، مقامات سان فرانسیـسکو مبلـغ ۳۵ میلیون دلار برای توسعه پروژه توسعه پارکبان های هوشمند هزنیه کرده اند. قبلاً خبر مشابهی منتشر شده بود مبنی بر هک شدن متروی ماساچوست توسط چند تن از دانشجویان MIT. شاید بتوان اینگونه نتیجه گرفت که وقتی پای پول و پول دادن در میان است، با کمی تفحص می توان از هکرها هم سراغی یافت! *(منبع: CNN)*

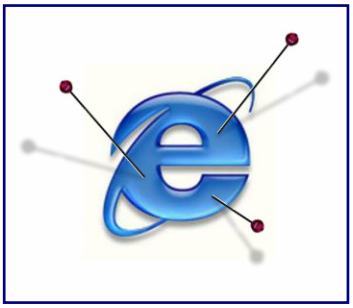
تهیه کننده: شرکت مهندسی مهران رایانه - واحد پشتیبانی فنی	تلفن: ۲۲۰۵۰۷۸۰ - ۲۶۲۰۲۴۹۳
آدرس: تهران- انتهای بلوار آفریقا - خ شهید طاهری - ایثار۳ - ایثار۲ - شماره ۱۷ - ساختمان مهران	نمابر: ۲۲۰۵۳۹۲۷

راهنمای آزمایش امنیت شبکه (قسمت پنجاه و پنجم – تعیین اولویت ها)

با استفاده از نتایج حاصل از بندهای ۱ تا ۳ (که در شماره های قبلی خبرنامه به آن پرداختیم) می توان به اولویت بندی سیستم ها جهت اجرای آزمایش امنیتی اقدام کرد. در واقع تجزیه و تحلیل این نتایج باید به ارائه فهرستی از سیستم ها منجر شود که بر اساس رده امنیتی، هزینه اجرای آزمایش و مزایای اجرای آزمایش، مرتب شده است. این فهرست همچنین منابع لازم (هزینه های) اجرای هر نوع آزمایش را برای هر سیستم شامل می گردد. منابع موجود برای اجرای آزمایش نفوذ باید مشخص شود و با منابع مورد نیاز برای انجام این کار مقایسه گردد. اگر فاصله بین این دو، آزمایش حداقلی که بر مهمترین سیستمها اجرا می شود را پوشش ندهد، باید منابع اضافی و کمکی لحاظ گردد. *(منبع: مهران رایانه)*

سه باگ دیگر در Internet Explorer

با کشف سه حفره امنیتی خطرناک در نسخه های 5.01 ، 6.x ، 7.x و 8.x نرم افزار وبگردی مایکروسافت، برگ دیگری بر پرونده ضعف های امنیتی این غول نرم افزاری افزوده شد. بروز یک خطا به هنگام دسترسی به آبجکت های حذف شده در حافظه می تواند حافظه را – با استفاده از بستر یک صفحه وب آلوده – مختل سازد. مایکروسافت وصله های اصلاحی این باگ ها را عرضه نموده است. یادآور می شود اینترنت اکسپلورر یا همان IE، نرم افزار گرافیکی مرور وب است که مایکروسافت آن را در سال ۱۹۹۵ عرضه نمود. هرچند در یک دوره زمانی، IE یکه تاز اینترنت بود و حتی بسیاری از کاربران، نخستین تجربه های وبگردی خود را از این برنامه آغاز کرده اند، ولی عوامل مختلفی از جمله کندی سرعت و برخوردار بودن از حجم عظیم حفره ها و ضعف های امنیتی – که نمونه آن تقدیم شما شد – نرخ استفاده از این مرورگر را کاهش داده است. هرچند در دنیای اینترنت مرورگرهای بسیاری وجود دارد ولی در یک برآورد کلی می توان موزیلا، اپرا و کروم را به عنوان رقبای قدر قدرت IE برشمرد.



(منابع: مهران رایانه ، Security and the Net و Wikipedia)

با بازی‌های آنلاین موافقید؟!

W32/Onlinegames.cae گونه کرم اینترنتـی جدیـدی است که اخیراً توسط آزمایشگاه تحقیقات ویروس‌های رایانه‌ای ایمن بررسی شده است. این کرم که ظاهراً خطر چندانی در بر ندارد، فایلی به نام waugafe.exe را بر رایانه های آسـیب دیـده ایجـاد مـی کنـد. اطلاعـات بیـشتر در نـشانی www.imenantivirus.com/encycf/W/W_00534.HTM آمده است: این فایل توسط ضد ویروس ایمن با نام W32/Trojan.zv شناسائی می گردد.

گوش مالی یک اسپمر هلندی

یک توسعه دهنده نرم افزار به نام Reinier Schenkhuizen به جرم ارسال بیش از ۲۱ میلیون ایمیل ناخواسته (اسپم)، به پرداخت ۲۵۰ هزار یورو محکوم شده است. بنـا بـه اعـلام OPTA سازمان تنظیم مقررات مخابراتی و رادیـویی هلنـد، ایـن شـخص کـه مالک شرکت Serinco Benelux است باید به ازای هر روزی که ایمیل‌های اسپم ارسال کرده، ۵۰۰۰ یـورو پرداخـت نمایـد. ایـن اسـپمر در مـصاحبه بـه خبرگزاری آلمان، ضمن رد ادعای ارسال ۲۱ میلیون هرزنامـه توسـط شـرکت متبوع وی، گفته که از این تصمیم دادگاه استیناف درخواست خواهد کرد. گفتنی است ماجرای اسپمرهایی که بعـضاً لـو می روند و از دادگاه و جریمه و مسائلی از این قبیل سر در می آورند، به جای خود خواندنی است. به عنوان مثال گاردین چندی پیش از جریمه ۲۳۰ میلیون دلاری اسپمر MySpace خبر داده بود. سایت The Register هم در ژانویه ۲۰۰۶ اعلام کرد که یک ISP در فلوریدا به دلیل ارتکاب همین بزهکاری، به پرداخت جریمه حیرت آور یـازده میلیـارد دلاری محکوم شده است. *(منابع: Spam Laws و Monsters and Critics)* ■

- *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.*