خبر

تعیین چارچوب پروانه اپراتور چهارم

به گفته وزیر ارتباطات و فناوری اطلاعات چارچوب پروانه اپراتور چهارم تعیین شده و طراحی کلانی نیز در این زمینه صورت گرفته است.

به گزارش مهر رضا تقی‌پور با بیان مطلب فوق افزود: «دولت باید برای تکمیل پروانه فعالیت این اپراتور مجوز صادر کند تا فرآیند انتخاب اپراتور طی شود.» وی ادامه داد: «پس از طی این فرآیند پروانه صادر شده و به اپراتور تحویل داده می‌شود.» به گفته وی برای تعیین اپراتور در این پروژه باید از دولت موافقت اصولی دریافت شود و پس از این مرحله، اپراتور از طریق مزایده یا ترک تشریفات انتخاب می‌شود. بنا بر اظهارات تقی‌پور فرآیند انتخاب شرکت برنده در اپراتور چهارم همانند فرآیندی است که برای تعیین برنده در اپراتورهای دوم و سوم تلفن همراه صورت گرفته است. از طرفی خارجی‌ها هم می‌توانند در این اپراتور حضور داشته باشند، به این معنی که خارجی‌ها با مشارکت شرکت‌های داخلی در این پروژه حضور یابند و بیش از ۴۹ درصد از سهام این اپراتور را در اختیار نگیرند.

برگزاری مناقصه دیتاسنتر ملی

سازمان تنظیم مقررات و ارتباطات رادیویی برای انتخاب اپراتورها و ارائه‌کنندگان خدمات مراکز داده اینترنتی- دیتا سنتر- مناقصه برگزار می‌کند. به گزارش «شرق»، بنا بر اعلام سازمان رگولاتوری برگزاری مناقصه انتخاب اپراتورهای دیتاسنتر (IDC) از سوی سازمان تنظیم مقررات و ارتباطات رادیویی برای تدوین و بازنگری شرایط و ضوابط نحوه فعالیت این اپراتورهاست. بر این اساس سازمان تنظیم مقررات و ارتباطات رادیویی در نظر دارد نسبت به تهیه درخواست برای ارائه پیشنهاد در مورد بازنگری شرایط و ضوابط نحوه فعالیت و انتخاب اپراتورها و ارائه‌کنندگان خدمات مراکز داده اینترنتی (IDC) از طریق مناقصه عمومی و انعقاد قرارداد از طریق اشخاص حقوقی اقدام کند. فروش اسناد این مناقصه از یازدهم آبان آغاز شده و تا پایان وقت اداری روز بیست و دوم این ماه نیز ادامه خواهد داشت.

ارائه خدمات صدور گواهی امضای دیجیتال

نایب رئیس هیات مدیره شرکت سازمان فناوری اطلاعات از افتتاح ارائه خدمات صدور گواهی امضای دیجیتال در نمایشگاه الکامپ امسال خبر داد. به گزارش «شرق» مهندس سعید مهدیون با اعلام این خبر گفت: «در عین حال در نمایشگاه امسال فعالیت‌ها و برنامه‌های انجام شده عرضه و اطلاعات لازم در خصوص مرکز ماهر و مدیریت آدرس‌های آی‌پی به اطلاع و آگاهی بازدیدکنندگان می‌رسد.» وی ادامه داد: «به خدمات در حوزه شهروند و خدمات الکترونیکی در نمایشگاه توجه ویژه شده، بنابراین بهترین فرصت هم برای شرکت‌کنندگان و هم بازدیدکنندگان فراهم شده است و به اعتقاد من نمایشگاه امسال با استقبال بازدیدکنندگان همراه خواهد بود.»

عرضه خدمات الکترونیکی جدید وزارت جهاد کشاورزی

مدیرکل دفتر آمار و فناوری اطلاعات وزارت جهاد کشاورزی از ارائه خدمات الکترونیکی وزارت جهادکشاورزی در نمایشگاه الکامپ خبر داد. به گزارش «شرق»، علی رادمهر با اعلام این خبر گفت: «اولین خدمت صدور مجوزهای الکترونیکی صنایع و تبدیلی بخش کشاورزی شامل صدور جواز تاسیس، پروانه بهره‌برداری و طرح و توسعه به متقاضیان از جمله این خدمات است.» وی ادامه داد: «صدور مجوزهای الکترونیکی دام و طیور شامل تمدید یا ابطال پروانه صدور جواز تاسیس و پروانه بهره‌برداری را می‌توان دومین خدمت جدید الکترونیکی برشمرد.» به گفته وی ارائه الکترونیکی درخواست زمین و تغییر کاربری در سطح وزارت جهاد کشاورزی به منظور یکپارچه‌سازی و سهولت کاربران و یکسان‌سازی پرونده‌ها از سوی متقاضیان و ایجاد انگیزه برای بخش خصوصی و در نهایت طرح تکریم ارباب رجوع، خدمات جدید و الکترونیکی دیگری است که ارائه می‌شود.

فروش ۱/۳ میلیارد دلار سهم مدیر عامل مایکروسافت

مدیرعامل مایکروسافت ۴۹/۳ میلیون از سهمش به ارزش حدود ۱/۳ میلیارد دلار را می‌فروشد. به گزارش ایسنا، استیو پالمر ۵۴ ساله در بیانیه‌ای تایید کرد که مقداری از سهمش در مایکروسافت را می‌فروشد تا تنوع مالی کسب کرده و به برنامه‌ریزی مالیاتی تا پیش از پایان سال کمک کند. مدیرعامل مایکروسافت تاکید کرد که اقدام مذکور نباید به عنوان نبود اعتماد به این غول نرم‌افزاری ملاحظه شود و وی کاملاً به این شرکت متعهد است. طبق اعلام مایکروسافت، پالمر در این شرکت پیش از جدیدترین فروش سهمش، حدود ۴۰۸ میلیون سهم داشت و قصد دارد ۷۵ میلیون سهم خود را تا پایان سال جاری بفروشد. سهام مایکروسافت در وال‌استریت تا روز جمعه ۲۶/۸۵ دلار بود.

تدوین پیش‌نویس آموزشی دوره‌های مجازی

به گفته رئیس دانشکده آزمون‌های الکترونیکی دانشگاه شیراز از سوی وزارت علوم پیش‌نویس آیین‌نامه آموزشی دوره‌های مجازی تهیه شده که امیدواریم به زودی آیین‌نامه آن ابلاغ می‌شود. به گزارش مهر، دانش‌منش با بیان مطلب فوق افزود: «استاندارد آموزشی ما نیاز به یک بازنگری دارد چرا که الگوی آموزشی‌ای که در کشور وجود دارد، ترکیبی از آموزش سنتی و مجازی است و الگوی خاصی در این زمینه نداریم.» وی ادامه داد: «فرآیند جهش برای رسیدن به سیستم کامل آموزش‌های الکترونیکی، فرآیندی زمانبر است.» به گفته وی زیرساخت‌ها برای برگزاری آزمون‌های آنلاین و ایجاد آزمایشگاه‌های مجازی در کشور وجود دارد اما هزینه‌های آنها سنگین است که به دنبال آن هزینه‌های آموزش‌های الکترونیکی را افزایش می‌دهد.

هدف‌گذاری ایجاد فضای امنیت اطلاعاتی در اینترنت از سوی وزارت اطلاعات

وزیر ارتباطات: ایران رتبه ششم امنیت فضای سایبر در منطقه است

حامد شفیعی

بنا بر اظهارات وزیر اطلاعات باید در اینترنت فضای امنیت اطلاعاتی به وجود آوریم. گرچه حیدر مصلحی از اشراف کامل مجموعه اطلاعاتی کشور بر شبکه اینترنت و فضای مجازی خبر داد اما سخنان عالی‌ترین مقام وزارت اطلاعات در راستای اتفاقات روی داده طی ماه‌های اخیر در فضای مجازی بوده که تازه‌ترین آنها انتشار ویروس استاکس‌نت است که طی مدت کوتاهی نزدیک به ۶۰ درصد اطلاعات صنعت کشور را به سرقت برد. البته مسوولان کشور هر کدام در حوزه‌های خود نسبت به این رویداد واکنش نشان داده و از اعلام آمادگی دستگاه‌ها برای مقابله با این ویروس خبر دادند. هرچند این واکنش‌ها پس از کمرنگ شدن بحث ویروس صورت گرفت در عین حال به تعویق افتادن راه‌اندازی نیروگاه بوشهر که برخی عامل اصلی آن را ویروس استاکس‌نت می‌دانستند مزید بر علت شد تا بلافاصله مسوولان اجرایی بیان کنند. این نیروگاه از تخریب و سرقت اطلاعات ویروس مصون بوده و هیچ آسیبی ندیده است. البته پس از آن وزیر ارتباطات و فناوری اطلاعات و همچنین وزیر اطلاعات از دستگیری عاملان انتشار این ویروس برای تخریب صنایع به ویژه نیروی هسته‌ای خبر دادند. انتشار این ویروس رایانه‌ای محک دقیقی برای عیارسنجی توان سیستم امنیت کشور به حساب می‌آید. از این رو رضا تقی‌پور وزیر ارتباطات و فناوری اطلاعات در تازه‌ترین اظهارات خود بر این عقیده است که در فضای سایبر ایران می‌تواند قطب امنیت در منطقه شود. به گفته کارشناسان اقدامات تخریبی در فضای سایبر علیه ایران، آغاز جنگ نرم بوده و در این راستا نیاز به آموزش نیروهای متخصص برای مقابله با تهدیدات رایانه‌ای است. به همین دلیل سپاه و بسیج آموزش هزاران بسیجی را در زمینه جنگ نرم در دستور کار خود قرار داده‌اند؛ آموزشی تحت عنوان «ارتش سایبری» که در آن روش‌های شناسایی، مقابله و حمله آموزش داده می‌شود. از طرفی به گفته وزیر اطلاعات تمامی اقدامات مخرب در فضای مجازی توسط سربازان گمنام به سرعت کشف و راهکارهای مقابله با آن طراحی و به اجرا گذاشته می‌شود. او بر این باور است که اشراف آنان بر شبکه‌های مجازی اجازه فعالیت در این زمینه را از دشمنان سلب کرده است. وزیر ارتباطات و فناوری اطلاعات نیز در این باره می‌گوید: اطمینان از نفوذناپذیری زیرساخت‌های فناوری اطلاعات حاصل جریانات و خطراتی است که کشور ما در حوزه سایبر به سلامت سپری کرد و این امر به گونه‌ای بود که ایران را در جایگاه ششم منطقه به لحاظ امنیت قرار داد. اقدامات دستگاه‌های امنیتی در حالی صورت می‌گیرد که قوانین جاری کشور در مورد ضدامنیت داخلی مواردی را بیان کرده که بر اساس آن با مجرمان برخورد کنند. همچنین برخی قوانین دایره حضور و محدوده فعالیت برای دستگاه‌ها را به منظور ایجاد فضای امنیتی مشخص کرده است. البته باید از سوی کارشناسان تحلیل‌های منطقی و مستدلی صورت گیرد تا از برخی کلمات و جملات به بهانه پیشگیری، تفسیرهای متعددی صورت نگیرد. فصل اول کتاب پنجم قانون مجازات اسلامی به جرائم ضدامنیت داخلی و خارجی کشور می‌پردازد که این فصل خود مشتمل بر ۱۵ ماده است که هر کدام به مساله‌ای در زمینه امنیت ملی اشاره دارد. همچنین در قانون جرائم رایانه‌ای نیز به موارد مسائل ضدامنیت داخلی پرداخته شده است. مبحث دوم فصل دوم جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی به تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی اشاره دارد که بر اساس تبصره یک ماده ۳ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند بنابراین طبق ماده ۳ هر کس به طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های معلوم در این قانون محکوم خواهد شد. با این حال خبر حمله‌های سایبری در ایران، معمولاً پنهان می‌ماند مگر آنکه صفحه نخست یک وب‌سایت طوری تغییر شکل دهد که کاربران متوجه آن شوند یا اینکه از طریق رسانه‌ها اعلام شود.

رویکردهای رویارویی با تهدیدات فضای سایبر

بنا بر اظهارات وزیر ارتباطات و فناوری اطلاعات با توجه به استراتژی‌های تعریف شده ایران می‌تواند بر اساس سند چشم‌انداز تبدیل به قطب امنیت در فضای سایبر و در فضای تبادل اطلاعات شود. به گفته رضا تقی‌پور تامین محیطی امن برای حفاظت از ارزش‌ها و هنجارها و برای حفظ دارایی‌های فضای اطلاعات بخشی از موارد مورد اهمیت امنیت در فضای سایبر است. در همین حال مصلحی وزیر اطلاعات نیز بیان می‌کند: امروز تمام حرکت‌های دشمن در فضای مجازی زیر ذره‌بین بوده و بدنه وزارت اطلاعات ایده‌های مختلفی برای مقابله با کارهای دشمن در اینترنت به ویژه شبکه‌های اجتماعی دارد. به گفته کارشناسان تهدیدات اینترنتی دو جنبه فنی - تخریب سایت‌ها، حمله به سرورها و سرویس‌دهندگان اینترنتی- و غیرفنی- تهدیدات علیه امنیت داخلی، سرقت اطلاعات محرمانه و... - دارد که ایران در هر دو زمینه بارها مورد حمله قرار گرفته است. رضا هاشمی کارشناس شبکه‌های کامپیوتری با اشاره به اظهارات وزیر اطلاعات و همچنین وزیر ارتباطات بیان می‌کند: سخنان وزیر اطلاعات در راستای تهدیدات امنیتی و سخنان وزیر ارتباطات بیشتر در زمینه تهدیدات فنی است هرچند هر کدام به نوبه خود دارای اهمیت است. رضا باقری‌اصل کارشناس مرکز پژوهش‌های مجلس نیز در این باره بیان می‌کند: سه رویکرد در رویارویی با تهدیدات فضای سایبر و اقدامات قابل سرزنش که امنیت و سلامت این فضا با آن روبه‌روست، موجود است که جرم‌انگاری با توسل جستن به قانون جرائم رایانه‌ای و بسیاری از قوانین مکمل دیگر یکی از رویکردهاست. از جمله رویکردهای دیگر ایجاد و در نظر گرفتن تدابیر حفاظتی و کنترلی در قالب پیشگیری وضعی و آموزش کاربران، توانمندسازی در مقابل و اجتناب از تهدیدات به همراه پیشگیری اجتماعی است اما بهترین روش بهره‌گیری همزمان از این سه رویکرد است.

چالش‌های امنیتی رودرروی ایران

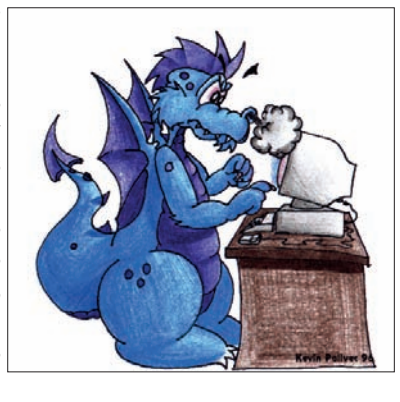
وزیر اطلاعات بر این باور است که بدنه اطلاعاتی کشور اشراف کاملی بر شبکه اینترنت داشته و از طرفی درصدد ایجاد فضای امنیت اطلاعاتی در شبکه‌های اجتماعی است. همچنین وزیر ارتباطات و فناوری اطلاعات نیز معتقد است ایران در حوزه دفاع و امنیت سایبری توانمندی‌های بالایی داشته و طبق رتبه‌بندی‌های جهانی ایران در جایگاه ششم امنیت فضای تبادل اطلاعات در دنیا قرار دارد که این عدد حداقل است. اما در مقابل کارشناسان شبکه‌های اینترنتی بیان می‌کنند ایران در بسیاری از موارد برای مقابله با تهدیدات دارای آسیب‌های جدی است. هاشمی معتقد است شرکت‌های توانمندی در حوزه سایبر وجود دارند اما آنها نه به دلیل صلاحیت و توانایی‌شان، بلکه به دلیل رانت و ارتباطات رشد کرده‌اند. به گفته او در ایران کارشناسان خوب و متبحری در حوزه امنیت فضای مجازی فعالیت می‌کنند اما متاسفانه نظام اعتبارسنجی درستی در این حوزه و همچنین صنف مشخصی وجود ندارد. اما در مقابل فرشاد اسماعیلیان کارشناس اینترنت و مدیر یکی از شرکت‌های ارائه‌دهنده خدمات میزبانی وب بیان می‌کند: در حال حاضر وضع بهتر از سال‌های گذشته شده است. به گفته او اگر از ابتدا به شکل استانداردی هزینه و برنامه‌ریزی شود امنیت مشکلی پیدا نمی‌کند. در این میان گروه‌های فعال در حوزه جنگ نرم دیدگاه‌های دیگری نسبت به این قضیه داشته و معتقدند ایران از سال گذشته با تهدیدات زیاد امنیتی در فضای مجازی روبه‌رو بوده است. از این رو نیازمند آموزش برای آشنایی و مقابله با این تهدیدات هستیم. روح‌الله سیفیان دبیر موقت شورای هماهنگی فعالان سایبری انقلاب اسلامی بیان می‌کند افرادی هستند که به صورت ناشناس مکان‌هایی را که به آنها از طرف دشمن از لحاظ فنی و در بعد امنیتی هجمه صورت می‌گیرد، شناسایی می‌کنند. هدف اصلی آنان تامین امنیت پایگاه‌های اینترنتی خودی از هجمه‌های دشمن است. در مواقعی هم که نیاز باشد، حمله می‌شود. محمدرضا موحدی‌صفت پژوهشگر امنیت در فضای سایبر بر این عقیده است‌که اگرچه امنیت مطلق در محیط‌های واقعی و مجازی امکان‌پذیر نیست اما ایجاد سطحی از امنیت به اندازه کافی و متناسب با نیازها و سرمایه‌گذاری‌های انجام شده تقریباً در همه شرایط محیطی امکان‌پذیر است. او در نهایت بیان می‌کند آنچه مسلم است این است که چالش امنیتی رودرروی کشور، عدم دسترسی به فناوری یا عدم وجود محصولات امنیتی نیست، بلکه سیاستگذاری، فرهنگ‌سازی، مدیریت مناسب منابع موجود و نیز سازگاری آنها به گونه‌ای است که نیاز منحصر به فرد شبکه و فضای دیجیتال کشور را تامین کند. از طرفی باید توجه کرد امنیت ملی در فضای سایبر بدون امنیت شبکه جهانی امکان‌پذیر نیست و هیچ کشوری نمی‌تواند نسبت به آنچه در سایر کشورهای حاضر در شبکه جهانی در حال وقوع است بی‌تفاوت باشد زیرا صدمات آن در صورت وقوع قابل انتقال به سایر کشورهاست. بنابراین لازم است بخش‌هایی از دولت به ویژه سرویس‌های اطلاعاتی- امنیتی به بازتعریف تقویت خویش در فضای سایبر بپردازند.

آنلاین

راه خلاصی از ویروس

شرق: ویروس‌های کامپیوتری به این دلیل ویروس نامیده می‌شوند چون دارای برخی وجوه مشترک با ویروس‌های زیست‌شناسی هستند چرا که یک ویروس کامپیوتری از کامپیوتر به کامپیوتر دیگر عبور کرده، دقیقاً مشابه ویروس‌های زیست‌شناسی که از شخصی به شخص دیگری منتقل می‌شود. ویروس‌های کامپیوتری از جمله موارد اسرارآمیز و مرموز در دنیای کامپیوتر بوده که توجه اغلب کاربران را به خود جلب می‌کند و به نوعی باید گفت ویروس‌های کامپیوتری به خوبی قدرت آسیب‌پذیری سیستم را به کاربر نشان می‌دهند. در مجموع باید گفت ویروس یک قطعه نرم‌افزار کوچک بوده که بر دوش یک برنامه حقیقی حمل می‌شود. مثلاً یک ویروس می‌تواند خود را به برنامه‌ای نظیر واژه‌پرداز متصل کند و هر مرتبه که برنامه واژه‌پرداز اجرا می‌شود، ویروس نیز اجرا شده و این شانس را پیدا کند که نسخه‌ای از خود را مجدداً تولید کند یا یک خرابی عظیم را باعث شود. یکسری دستورالعمل‌های ساده برای اجتناب از ویروس‌ها وجود دارد که با پیروی از آنها می‌توان تا حد بسیار زیادی از شر ویروس‌ها و بدافزارها در امان ماند. هیچ‌گاه پیوست‌های یک ای‌میل ناشناس را باز نکرده و روی هایپرلینک‌های موجود در آن کلیک نکنید. نویسندگان ویروس تمایل به فریب کاربران برای کلیک روی لینک‌هایی دارند که آنها را به وب‌سایت‌های خرابکار هدایت می‌کنند. به دوستان خود اطلاع دهید که هیچ‌گاه روی لینکی کلیک نکنند مگر اینکه توضیح کوتاهی در مورد آن در ای‌میل موجود باشد. در صورتی که سرویس ای‌میل شما دارای امکان باز کردن اتوماتیک لینک‌هاست، این امکان را غیرفعال سازید. در غیر این صورت ممکن است تنها با باز کردن ای‌میل، ویروسی را به صورت اتوماتیک فعال سازید. قضیه فوق در مورد دیگر پیغام‌ها، مانند پیغام‌هایی که در فیس‌بوک، اتاق‌های چت و غیره دریافت می‌کنید نیز صادق است. از آنجایی که گاهی اوقات این پیغام‌ها شما را به بدافزارها هدایت می‌کنند، به منبع پیغام توجه کافی داشته باشید. به برخی علامت‌های غیرعادی نیز توجه کنید. برای مثال املای غلط یک کلمه یا وجود اشتباهات دستوری در متن پیغام، به خصوص اگر فرستنده پیغام غالباً موارد فوق را رعایت می‌کند، می‌تواند مشکوک باشد، در صورتی که یک ای‌میل یا پیغام مشکوک را مشاهده کردید، به فرستنده آن اطلاع دهید زیرا ممکن است قربانی هکرها شده و اطلاعات رمز عبور وی به سرقت رفته باشد.

وب‌سایت‌های مشکوک را صرف نظر از اطلاعاتی که ارائه می‌دهند، به هیچ وجه مورد بازدید قرار ندهید. بسیاری از مرورگرهای فعلی به شما در مورد وب‌سایت‌های حاوی بدافزار هشدار می‌دهند. این هشدارها را جدی گرفته و از وب‌سایت‌های مذکور دوری کنید. به پنجره‌هایی که در زمان گشت و گذار در وب بالا می‌آیند، کاملاً دقت کرده و در صورتی که نشان‌دهنده نیاز به نصب یک درایور ویدئوی جدید برای دیدن فیلمی هستند، بسیار بااحتیاط عمل کنید زیرا این روش یکی از تاکتیک‌های اصلی انتشار بدافزار است.



دنیای نرم‌افزار

برنامه‌نویسی به زبان ساده

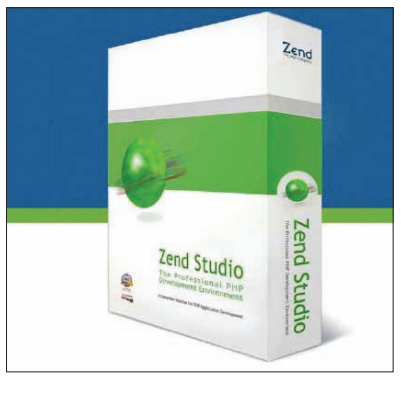
شرق: برنامه‌نویسی تحت وب برای طراحی وب‌سایت‌ها به کمک زبان‌های برنامه‌نویسی مختلف انجام می‌شود. از این زبان‌ها می‌توان به زبان‌هایی نظیر PHP , HTML ASP و... اشاره داشت. برنامه‌نویسان وب با توجه به اصولی که برای خود تعیین کرده‌اند و همچنین نیازهایی که برای برنامه‌نویسی وب وجود دارد اقدام به انتخاب یکی از این زبان‌ها برای برنامه‌نویسی حرفه‌ای و به عنوان زبان اصلی خود می‌کنند. کدنویسی برای تعدادی از این زبان‌ها نیاز به محیط برنامه‌نویسی خاصی دارد تا کدنویسی به صورت مرتب و منظم و بدون اشکال انجام شود. هر یک از این زبان‌ها برای کدنویسی نیازمند محیط خاصی است که شرکت‌های مختلف نرم‌افزاری با ساخت برنامه‌های مختلف طراحی این محیط را برای کاربران فراهم می‌کنند. در این مطلب شما را با نرم‌افزاری آشنا می‌کنیم که در محیط آن می‌توانید به راحتی اقدام به برنامه‌نویسی به زبان PHP کنید.

Zend Studio نام نرم‌افزاری نام‌آشنا برای برنامه‌نویسان زبان PHP است. این نرم‌افزار با فراهم کردن محیطی مناسب برای کدنویسی به زبان PHP و با قرار دادن ابزار و امکانات مختلف برای راحتی کاربران توانسته است جایگاه مناسبی را در میان برنامه‌نویسان PHP برای خود باز کند. این ویرایشگر زبان PHP دارای امکانات و قابلیت‌های متعددی است. ویرایش، خطایابی و آنالیز کدها و انتشار فایل‌ها از امکاناتی است که می‌توان از آنها در این نرم‌افزار نام برد. شما با کمک این نرم‌افزار و زبان برنامه‌نویسی PHP می‌توانید وب‌سایت‌های خود را به صورت پویا ساخته و با کمک ادغام آن با دیگر زبان‌های برنامه‌نویسی و پایگاه‌های داده وب‌سایتی کاملاً حرفه‌ای طراحی کنید. این ویرایشگر با تکنولوژی‌های جدید برنامه‌نویسی وب همانند تکنولوژی AJAX سازگاری داشته و شما می‌توانید از این فناوری نیز در ساخت وب‌سایت خود استفاده کنید.

این نرم‌افزار با خطایابی کدهای وب‌سایت در صورت بروز اشتباه‌های تایپی و گرامری و دستوری و نشان دادن آنها با رنگ‌های متفاوت به طراح در هرچه بهتر شدن وب‌سایت کمک می‌کند. همچنین در محیط ویرایشگر این نرم‌افزار شما می‌توانید از زبان‌های دیگری نظیر HTML,CSS , XML , JavaScript نیز برای برنامه‌نویسی وب استفاده کنید.

این نرم‌افزار دارای ویژگی‌های بسیاری است که از جمله آن می‌توان به این موارد اشاره داشت:

- مشخص کردن خطاهای گرامری در کدنویسی و رنگی کردن خطاها
- توانایی کلاس‌بندی فایل‌ها
- دارای نمودار درختی برای هرچه راحت کنترل کردن فایل‌های مرتبط
- با قابلیت آنالیز کردن کدهای نوشته شده و Debug کردن کدها.



به هرحال اگر شما جزء آن دسته از کاربرانی به حساب می‌آیید که به برنامه‌نویسی علاقه خاصی دارید به شما توصیه می‌کنیم حتماً سری به سایت p30world.com بزنید تا علاوه بر بارگذاری رایگان به اطلاعات جامعی در خصوص این نرم‌افزار دست پیدا کنید. گفتنی است نرم‌افزار قوی محصولی از Zend Technologies به شمار می‌آید.

جرائم رایانه‌ای

جرائم رایانه‌ای و فنون کشف آن

آرام حامدی

در این مقاله درباره زمینه‌هایی بحرانی از شرارت‌ها در صنعت فناوری اطلاعات صحبت می‌شود و خواهیم گفت که در دنیای امروز متخصصان امنیت فضای مجازی چگونه با آن مبارزه می‌کنند.

شرارت‌های رایانه‌ای چه هستند: شرارت‌های رایانه‌ای تخصص‌ها و علوم رایانه و آخرین دستاوردهای فناوری اطلاعات را به خدمت می‌گیرد تا از آنها برای جمع‌آوری اطلاعات و مدارکی برای سوءاستفاده و خلافکاری در فضای مجازی استفاده کند. از منظر قانونی یک مامور دولتی جرائم رایانه‌ای می‌تواند در سیستم‌های رایانه‌ای و شبکه‌ها به جست‌وجو بپردازد و با استفاده از یکسری روش‌های فنی در نهایت مدارک و سرنخ‌هایی خواهد یافت تا یک شرارت رایانه‌ای را کشف کند. یک جرم رایانه‌ای هر جرمی می‌تواند باشد. تنها تفاوت آن این است که این خلافکاری‌ها در فضای مجازی صورت می‌گیرد.

چرا جرائم رایانه‌ای: فنون رایانه‌ای راهی اصولی و مشخص برای جمع‌آوری اطلاعات در سیستم‌های کامپیوتری و شبکه‌ای فراهم می‌کند که این روش‌ها می‌تواند بسیار مرموز و مخفی باشد و تشخیص آنها بسیار مشکل باشد. و افراد عادی هم به سختی می‌توانند از این روش‌ها استفاده کنند. معمولاً کامپیوتری که از آن برای شرارت‌های رایانه‌ای استفاده می‌شود، از تکنیک‌هایی استفاده می‌کند که به کمک آن می‌تواند اطلاعات را مخفی کند یا رمزگذاری کند. در سیستم‌های رایانه‌ای و شبکه‌ها شرارت‌های رایانه‌ای به این صورت‌ها انجام می‌گیرد.

بوکشیدن بسته‌ها (packet sniffing): بوکشیدن به معنای احساس کردن چیزی و گوش دادن به آن است. اطلاعات در شبکه مانند اکسیژن در هواست. هنگام تنفس، بدن اکسیژن را جذب می‌کند. این همان اتفاقی است که هنگام packet sniffing می‌افتد. بسته‌های اطلاعاتی مشکوک به این روش از شبکه ربوده می‌شوند. این بسته‌های اطلاعاتی می‌توانند نام کاربری و رمز عبور هم داشته باشند.

ردیابی آدرس IP: ردیابی آدرس IP به معنای ردیابی آدرس واقعی کسی است که این آدرس IP را دارد. ردیابی آدرس IP از طریق جست‌وجوی معکوس IP است یعنی تعداد سرورهایی را که بین مقصد و منبع وجود دارد می‌شمارند. در این روش ابتدا آدرس ISP ردیابی می‌شود سپس با نفوذ به اطلاعات موجود در سرور آن ISP اطلاعات صاحب IP به دست می‌آید.

ردگیری آدرس email: بعضی مواقع اینکه بدانید ای‌میل دریافت‌شده از کجا آمده است بسیار مهم است. این کار با بررسی سربرگ (header) ای‌میل امکان‌پذیر است. سربرگ ای‌میل دربردارنده آدرس IP کامپیوتر مبدا است و به کمک این آدرس IP می‌توان آدرس واقعی را پیدا کرد یا به عبارت دیگر از روش ردیابی آدرس IP استفاده کرد. سربرگ ای‌میل همین طور می‌تواند حاوی اطلاعات مهمی مانند سرور واقعی ای‌میل یعنی جایی که ای‌میل به وجود آمده است و تاریخ و زمان آن باشد.

ساختار فایل: برای یک کامپیوتر ساختار فایل‌ها مورد بررسی قرار می‌گیرد تا فایل‌های مشکوک را در هر گوشه کامپیوتر پیدا کند. بعضی از این فایل‌ها ممکن است رمزگذاری شده باشند. چنین فایل‌هایی ابتدا مورد بررسی قرار می‌گیرند تا اگر اطلاعات باارزشی دارند آنها را به دست آورند. این کار به وسیله ابزارهای اتومات انجام می‌شود. مثلاً ممکن است نرم‌افزاری در کامپیوتر فرد مشکوک نصب شده باشد و او از آن بی‌خبر باشد و حتی هنگامی که در حال کار با کامپیوتر است اطلاعاتی را جمع‌آوری کند. خب برای این منظور باید کسی به کامپیوتر شما دسترسی داشته باشد.

ابزارهای ذخیره اطلاعات: این ابزارها می‌تواند یک سی‌دی، حافظه فلش و هارددیسک و مانند آن باشد. این دیسک‌ها ممکن است پاک (فرمت) شوند و بازیابی اطلاعات آن تقریباً غیرممکن شود هر چند بازیابی اطلاعات به کمک ابزارهایی ممکن است. اطلاعاتی که در هارددیسک ذخیره می‌شود حتی پس از پاک شدن هم قابل بازیابی است. این اطلاعات را حتی هنگام جابه‌جایی از کامپیوتری به کامپیوتر دیگر می‌توان بازیابی کرد.

مخفی‌نویسی: یکی از راه‌هایی که خلافکاران برای انتقال اطلاعات محرمانه خود از آن استفاده می‌کنند مخفی‌نویسی است. در این روش اطلاعاتی را در فایل‌های صوتی، تصویری و مانند آن ذخیره می‌کنند. بعضی مواقع قسمتی از اطلاعات را در یک فایل و بقیه را در فایل‌های دیگر مخفی می‌کنند، در این حالت تشخیص و رمزگشایی بسیار مشکل است.

پرینت‌ها: پرینت‌هایی که از پرینترها گرفته می‌شود می‌تواند حاوی اطلاعاتی باشد که با چشم معمولی قابل دیدن نیست و معمولاً با این روش اطلاعات زیادی از شرکت و سازمان‌ها سرقت می‌شود و در بیشتر اوقات کسی حتی به آن شک هم نمی‌کند چه برسد که بخواهد متوجه آن شود. بنابراین نباید به پرینت‌هایی که در شرکت شما گرفته می‌شود بی‌تفاوت باشید.

ابزار تجارت: بعضی از ابزارهایی که کارآگاهان رایانه‌ای از آنها سود می‌برند عبارتند از هگز ادیتورها، دیس اسمبلرها، دیسک آنالایزرها، رمزگشاها، پاکت اسنیفر، ابزارهای DNS.

شرارت‌های رایانه‌ای زمینه‌ای است که سود زیادی برای خلافکاران دارد و پیش‌بینی می‌شود این خلافکاری‌ها در دهه پیش رو افزایش چشمگیری داشته باشد.