بدافزارها و چالش های ایمنی در محیط سایبر

نوید علیزاده*[1]، زهرا انصاری[1]

چکیده

هم اکنون، عموم رشته ها به نوعی رایانه و اینترنت را بکار می برند، اما به امکانات و خطرهای آن آگاهی ندارند. در فضای سایبری کاربرانی هستند که طعمه نفوذگران هستند؛ نه تنها برای بکارگیری داده هایشان، بلکه برای استفاده از رایانه برای نفوذ و تاختن به مراکز مهم تر. کاربران می باید این را بدانند که کرم ها، کوکی ها و ویروس های اینترنتی به تندی در حال پخش شدن در شبکه هستند و از بین میلیون ها کاربر، دست کم یک کاربر می تواند آنها را به هدف خود برساند. بنابراین، پیشنهاد می شود پیش از بکارگیری رایانه و اینترنت با امکانات آن آشنا شوید. در این نوشتار، کوشش بر شناساندن انواع نا امنی ها در محیط سایبر و نحوه تشخیص نگهبانی های مناسب توسط کاربر و همچنین بررسی راهکار های بالا بردن نرم افزار های نگهبان پرداخته می شود.

واژگان کلیدی: نرم افزار ویران گر، ویروس الکترونیکی، کرم اینترنتی، اسب تروا، نرم افزار پاداش، نرم افزار ردیابی، درب های پنهان، ثبت کننده های کلید، امنیت داده ها، آنتی ویروس.

چاره جویی های ایمنی

هم اکنون، بسیاری از کاربران بر این گمانند که به علت ناشناس بودن در شبکه های رایانه ای به ویژه اینترنت، کسی نیت آزار رساندن و دسترسی به داده های ایشان را ندارد. گمان می شود که «کسی به من کاری نخواهد داشت، چون من با ایشان کاری ندارم»، یا این که «کسی چه می داند پشت این رایانه من نشسته ام که بخواهد به داده های من دسترسی داشته باشد؟»، یا مهم تر از همه این که «مگر داده های من به چه درد افراد دیگر می‌خورد». این طرز فکر نادرست منجر به عدم رعایت چاره جویی های ایمنی می شود[۲و۱].

در نخستین روزهای بکارگیری رایانه در سامانه های به اشتراک گذاشته شده، تنها نام کاربری برای شناسایی افراد بکارگرفته می شد و نیازی به وارد کردن رمز عبور نبود. ولی، پس از آن که کاربران بدخواه، آغاز به بکارگیری ناروا در این سامانه کردند، رمزهای عبور نیز به سامانه ها افزوده شد. هم اکنون، کاربران بیش از هر زمان دیگری باید به ایمنی بیشتر شبکه رایانه خود به پردازند. در ادامه، به سه مورد از دلایل اهمیت ایمنی اشاره می شود:

- امروزه، سرمایه گذاری روی تجهیزات سخت افزاری و نرم افزاری بسیار ارزش مندتر شده است. از این رو، اگر در یک یورش امنیتی، اجزای سخت افزاری و نرم افزاری آسیب ببینند، به جهت هزینه بسیار بالای نصب و تعمیر[1] تجهیزات و نیز افزایش زمان از کار افتادگی، بهره وری سامانه کاهش خواهد یافت.
- داده های سازمانی و فردی مانند فهرست مشتریان و ارتباط ها با آنها، طرح های مالی، داده های حسابداری و دارایی، رساله یا پایان نامه و غیره، همواره با ارزش بوده اند.
- تهدیدهای نفوذگران اینترنتی از قبیل بدست آوردن رمز کارت بانکی یا حتی تفریح با کاربران بی احتیاط و تلاش در به دام انداختن آنها افزایش

*. عهده دار مکاتبات، تلفن/ دورنگار:۶۶۴۶۹۲۰۲ (۹۸۲۱+) پست الکترونیکی: Nalizadeh@ut.ac.ir
۱. مرکز تحقیقات بیوشیمی و بیوفیزیک دانشگاه تهران.

1. Recovery

یافته است.[۵ و۳].

این روزها، رایانه ها در فضای مجازی[1] با انواع گوناگونی از بدافزارها و ویروس ها آلوده می شوند. به همین دلیل شرکت های آنتی ویروس پیوسته، در حال بالا بردن نرم افزارهای خود برای مبارزه با این تهدیدها می باشـــند. اما بااین حال، به دلایل زیر ســـامانه ها همچنان در معرض خطر هستند.[۷و۶]:

- سهل انگاری
- اولویت نداشتن صرف هزینه برای مسائل ایمنی
- پایین بودن سطح کیفی سخت افزار
- خلاقیت نفوذگران در ایجاد طعمه
- پایین بودن سطح آگاهی کاربر
- نگاه ساده انگارانه و غیرواقعی کاربر

آشنایی با برخی از مهمترین ناامنی ها و مزاحمت های الکترونیکی

نرم افزار ویران گر[2]

نام دیگر نرم افزارهای ویران گر ، بدافزار[3] است. این نرم افزارها بیشتر برای آسیب رساندن یا ویرانی سامانه ها طراحی می شوند.

نخستین ویروس رایانه ای در سال ۱۸۹۱ شناسایی شد، مفهوم کرم رایانه در ســال ۱۹۷۵ معرفی شد و اوایلScience Fictionای در کتاب دهه ۱۹۸۰، اولین فعالیت های محسوس خود را آغاز کرد. جالب است بدانید که این کرم ها نخستین بار برای این طراحی شده بودند که عملکرد مثبت و مفیدی داشته باشند. پیدایش اسب های تروای رایانه ای هم به نخستین روزهای ایجاد سامانه های اشتراک زمانی (دهه ۱۹۶۰) باز می گردد. با وجود تاریخ و سابقه طولانی این نرم افزارها، به تازگی تأثیرهای ویران گری آنها برای کاربران عادی پررنگ بوده است.[۹و۸].

ویروس

برنامه ای است که به انتهای برنامه دیگری متصل و یا وارد بدنه آن می شود. وقتی این برنامه به اجرا در می آید، ویروس همراه آن اجرا شده، نسخه های خود را وارد فایل یا قسمت های دیگری از حافظه می کند و به این ترتیب نسخه های بیشتری منتشر می شوند. با هر بار اجرای یکی از فایل ها یا برنامه های آلوده، این روند تکرار می شود. البته، ویروس ممکن است افزون بر این موارد، کارهای دیگری نیز انجام دهد.

کرم‌اینترنتی[4]

کرم ها از این جهت که نســـخه ای از خود را منتشـــر می کنند، مشـــابه ویروس ها هســـتند، اما برای اینکار بـــه برنامه میزبان نیاز دارند. همانند ویروس ها، یک کرم ممکن است تنها نسخه هایی از خود را در جاهای متفاوت تکرار کند و یا اینکه افزون بر آن عملیات دیگری نیز انجام دهد. کرم تنها زمانی کار می کند که سامانه توانایی پذیرفتن منابع خارجی را داشته باشد و از راه آن منابع بتواند به اجرای آن برنامه بپردازد. برخی از فروشندگان ابزارهای شناسایی بدافزارها، کرم ها را نیز نوعی ویروس به حساب می آورند.

اسب تروا[5]

نام این نوع نرم افزار از افسانه جنگ شهر تروا در یونان گرفته شده است. در آن افسانه، یونانی ها یک اسب چوبی بزرگ را از دروازه شهر به داخل می فرســـتند و هنگامی که اسب وارد شهر می شود، شمار زیادی سرباز یونانی از آن خارج می شـــوند و شـــهر را در خواب و غفلت ساکنین به تصرف خود در می آورند. از آن زمان به بعد "اسب تروا" به عنوان سمبلی از ظاهری عادی و باطنی خطرناک و آســـیب رسان شناخته می شود. در مفاهیم رایانه ای ، اسب تروا می تواند خرابی های زیادی به بار آورد و یا اعمالی غیر از آنچه کاربر انتظار دارد، انجام دهد. این اصطلاح به تازگی به برنامه های ویران گری گفته می شود که بیشتر بدون آگاهی و اجازه کاربر وارد سامانه می شوند و به جمع آوری و ارسال داده ها می پردازند.

نرم افزار جایزه[6]

نرم افزارهای جایزه حاوی بسته های دیگر نرم افزاری است که گاهی همـــراه با نرم افزار اصلی نصب می شـــود. به عنـــوان مثال، اگر یک مرورگر[7] وب نصب نمایید، ممکن است در کنار آن برنامه هایی نظیر Flash Player، Acrobat Reader و یا چند نوار ابزار نیز وجود داشته باشد که مسلماً باعث افزایش کارایی نرم افزار اصلی می شود. در اکثر موارد برای نصب نرم افزارهای جایزه از شما سؤال می شود. نرم افزارهای جایزه که اکثراً حامی مالی نرم افزار اصلی هستند و این همراهی بُعد تبلیغاتی برای آنها دارد، جاسوسانه عمل می کنند و اکثرا در صورت اتصال سیســـتم به اینترنت، با ســـایت اصلی خود ارتباط برقرار کرده، هر آماری از سیستم را ارسال می دارند.

نرم افزار ردیابی و اعمال تغییر در شبکه[8]

این دسته از برنامه ها، پایگاه هایی را که مشاهده می کنید رصد می کنند و می توانند علاوه بر آنچه که شما در حالت معمول می بینید، صفحات دیگری را نیز به نمایش درآورند. همچنین می توانند محتویات یک پایگاه وب را با تبلیغات خود جایگزین نمایند و اطلاعاتی را در مورد کامپیوتر شـــما و تعاملاتی که با تولید کننده آن داشـــتید، برای پدیدآورنده خود بفرستد. این نرم افزارها در بسیاری از موارد دارای کنترل کامل بر روی مرورگر شما هستند، آنچه را انجام می دهید، تحت نظر دارند و این آمار را به مقصد مورد نظر خود گزارش می دهند[۱۱و۱۰].

درب های مخفی[9]

معمولا برای دسترســـی به یک سیستم کامپیوتری نیاز به وارد کردن نام کاربری و رمز عبور دارید. اگرچه این سطح از امنیت، گاهی اوقات برای

1 . Cyber Space
2. Malicious Software
3. Malware
4. Internet Worm
5. Trojan
6.Bonus Software
7. Web Browser
8.Web Tracking /Modification Software
9. Backdoors

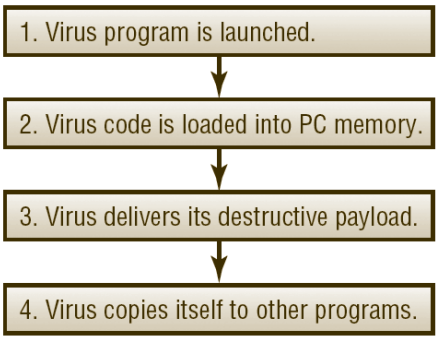
سیستم هایی که از لحاظ فیزیکی ایمن هستند و تنها اشخاص خاصی می توانند از پشت صفحه کلید وارد آنها شوند وجود ندارد. نرم افزار درب مخفی با بی اثر کردن کلیه حفاظت های ایمنی به کاربر راه دور (نفوذگر) اجازه دسترسی به کامپیوتر شما را می دهد. این نرم افزار حتی ممکن است حفاظت های ایمنی خود را کار بگذارد تا تنها پدید آورنده آن بتواند از سیستم استفاده نماید.

ثبت کننده های کلید[1]

ثبت کننده کلید، تمامی کلیدهای فشرده شده صفحه کلید را ثبت و در یک فایل ذخیره می کنند، این فایل می–تواند در آینده از طریق دسترسی درب مخفی مورد استفاده قرار گیرد و یا از طریق پست الکترونیکی یا وب برای مقصد مورد نظر ارسال شود. شایان ذکر است که ثبت کننده کلید تمامی آنچه واقعا ماشین نویسی می کنید را نظاره می کند و نه آنچه که از طریق شبکه ارسال می شود. بنابراین حتی اگر شماره کارت اعتباری را روی صفحه وب ایمن وارد نمایید (به این معنی که در زمان انتقال اطلاعات از رمزنگاری استفاده شود)، این برنامه دقیقاً آنچه را که ماشین نویسی می کنید، پیش از رمز شدن و بدون ارتباط با سیستم رمز نگاری ثبت می نماید[۱۲و۹].

ویروس نویسان

فناوری اولیه ویروس های کامپیوتری بر اساس یک روش بسیار ساده برنامه نویسی بود که در آن برنامه ای تولید می شد (شکل ۱) که می توانست از خودش یک یا چند نسخه دیگر به وجود بیاورد (یا به اصطلاح رونویسی کند) و در دایرکتوری (یا مکان) دیگری قرار دهد که در آن مکان جدید دوباره به اجرا در آمده و این فرایند را تکرار کند. مهندسین کامپیوتر در آن زمان بر آن بودند که از این روش برای آزمایش سخت افزار مین فریم ها[2][۱۳] استفاده کنند که آیا مکان یاب حافظه های آنها عملکرد صحیحی دارند یا خیر.



شکل ۱: فناوری اولیه ویروس های کامپیوتری: ۱. ویروس به کامپیوتر مقصد میرسد. ۲. در حافظه کامپیوتر اجرا می شود. ۳. ویروس تاثیر مخرب خود را می گذارد. ٤. ویروس نسخه ای از خود را در برنامه ای دیگر کپی می نماید.

امروزه بسیاری از ویروس هایی که اکنون منتشر شده اند،در واقع توسط کیت های ساخت ویروس و توسط افرادی ایجاد می شوند که شاید هیچ پیشینه ای در رایانه نداشته باشند.افرادی که از کدهای دیگران استفاده می کنند و سعی می کنند طوری وانمود نمایند که با برنامه نویسی آشنایی دارند.[۱٦و٤۱].

تعریف ایمنی سیستم

رهایی از هر گونه خطر و هلاکت احتمالی، برقراری ایمنی و رهایی از ترس و نگرانی را ایمنی سیستم می گویند.

تعریف ایمنی اطلاعات

مفهومی است که به اقدامات پیشگیرانه ای اطلاق می شود که ما را قادر می سازد از اطلاعات خود در برابر حملات خارجی و بهره برداری های غیر مجاز محافظت کنیم. به عبارت بهتر ایمنی اطلاعات، فرآیندی است جهت حفظ اطلاعات از دسترسی غیر مجاز، افشا شدن، خرابکاری، تغییر و یا از بین رفتن آنها[۱۷].

نحوه ارزیابی آنتی ویروس ها

بیش از یک دهه است که شرکت های بزرگ آنتی ویروس نقشه های ویروس را نشان می دهندو به ما در ارتباط با آلودگی کامپیوتر هشدار می دهند و امروز آنتی ویروس جزء اصلی رایانه های شخصی تبدیل شده است.برخی شرکت های آنتی ویروس به دلیل اثری که در پایین آوردن سرعت سیستم ها و بالا بردن زمان کاری دارند، شهرت پیدا کرده اند. هرکسی که با این شرکت های بزرگ کار کرده است یک نکته را با اطمینان می داند و به آن عمل می کند: اجتناب از خریدن محصولات آنتی ویروس آنها! در حال حاضر شرایط تغییر کرده است. بررسی های اخیر نشان می دهد که بیش از ۷۰٪ کاربران جهان بیشتر به برنامه های آنتی ویروس رایگان علاقمند هستند تا برنامه های پولی. ولی به هر صورت تصور کنید که روزی شرکت تولید کننده سیستم عامل مورد استفاده شما پس از یک سال از ورود شما به سیستم عامل جلوگیری کند و شما را مجبور به خرید نسخه به روز رسانی آنتی ویروس نصب شده شما نماید. پس به هر صورت چیزی که مهم است تشخیص برتری یک آنتی ویروس بر دیگران است نه پولی و یا مجانی بودن آن. اگر بخش پاداش ها در باره آنتی ویروس های شناخته شده، دیده شود (نشانی اینترنتی پائین)، نشان ها و پاداش های داده شده، گویای اعتبار و استقلال آنهاست. در تأیید اعتبار و استقلال این سازمان ها تنها می توان گفت که کلیه شرکت های تولید کننده آنتی ویروس برای دریافت این نشان ها، رقابت می کنند و دریافت نشان ها را افتخاری برای شرکت خود می دانند. هر ساله، با بررسی های گوناگون به برترین شرکت ها نشان هایی داده می شود.پیشنهاد می شود، کاربران پیش از گزینش یک آنتی ویروس برای سامانه مورد نظر خود هم به سنجش ها و هم به رتبه

1 . Key loggers
2. Main-Frame Computers

بندی های این شرکت ها توجه داشته باشند.آدرس زیر نمونه ای از یک رتبه بندی برای سال ۲۰۱۱ می باشد:
http://www.av-comparatives.org/en/compar – tivesreviews/detection-test

سنجش های مهم یک آنتی ویروس که دو سازمان جهانی AV-Co-paratives و VirusBulletin آنهـا را مورد ارزیابی قرار می دهند، به ترتیب اهمیت عبارتند از:
۱. قدرت شناسایی بالا
۲. هوش مصنوعی مطمئن در راستای شناسایی ویروس های ناشناخته جدید
۳. تاثیر کم بر میزان کارایی و بهره وری سامانه مورد کاربری
٤. سرعت جستجوی ویروس ها
۵. میـزان توانایـی آنتی ویـروس در تعمیر فایل های آلوده شـده به ویروس (این پارامتر جزء معیارهای شرکت AV-Test است.)
از دید غیرفنی، مسـائلی چون نداشـتن در پشـتی (ارسال اطلاعات سیسـتم کاربر برای شـرکت تولید کننده آنتی ویـروس) و همچنین تحریم نبودن نیز مطرح می شود[۲۰و۱۸و۱٦].

نقش شرکت های تولید کننده آنتی ویروس در تولید ویروس

بـا توجه به اینکه ویروس ها و بدافزارهای فراوانی برای توجیه نیاز به برنامه های آنتی ویروس وجود دارند، شـکی نیست ایجاد ویروس به افزایش سود و حضور فعال شرکت های آنتی ویروس در بورس، کمک می کند. اگر شرکت های آنتی ویروس واقعاً به این مطلب اعتقاد داشتند که انتشـار ویروس ها به افزایش سود و فروش هایشان کمک می کند احتمالا کمر به ساخت ویروس ها و بدافزارهای بیشتر می بستند و حتی برای انتشار آن برای سیستم عامل های دیگر سخت تلاش می کردند. هرچند امکان اینکه فردی وابسـته به یک شرکت آنتی ویروس، چنین کار غیر اخلاقی انجام دهد، دور از ذهن نیست، ولی برای پاسخ به این سوال موارد زیر نیز قابل تامل است:
۱. شرکت های آنتی ویروس از خطرهای موجود در برخورد با ویروس های رایانه ای آگاهی دارند. این شرکت ها فرصتی برای استخدام افرادی که ویروس ها را ایجاد کرده اند، نخواهند داشت. زیرا با توجه به اینکه ایجاد ویروس های رایانه ای برای هرکسی که با رایانه و برنامه نویسی آشـنایی دارد،کار چندان دشـواری نیست و نیز با توجه به خیل عظیم ویروس های تولید شده که در هر ثانیه وارد شبکه های جهانی می شود، آنها دیگر فرصتی برای به روز رسـانی در کشف و پاک سازی تمامی ویروس ها و سایر تهدیدات رایانه ای نخواهند داشت.
۲.یک ویروس برای اینکه آزمون خود را پس دهد، نخست باید در یک شـبکه بدون اینکه بد گمانی آنتی ویـروس های آن را برانگیخته کند، گسترش یابد؛ بنابراین ،در چنین شرایطی یک شرکت آنتی ویروس نمی تواند خود را از آن دور بدارد. بدین معنی که یک ویروس باید پس از آماده سـازی در بستری آزمایش شود. برای یک شرکت آنتی ویروس، ایجاد چنین بستر مجازی هزینه بر است؛ زیرا نمی تواند در شبکه خود شـرکت آنرا در مهک آزمون بگذارد. در آن صورت ویروس نخسـت فرآورده های خود آن شـرکت را آلوده خواهد کرد که این امر منجر به نارضایتی مشتری می شود.
۲. بیشتر ویروس ها اثر انگشت نویسنده را روی خود دارند. نویسنده ها سـهوی یا عمدی روی کدی که می نویسـند، اثری از خود به جای می گذارند. کدی که ویروسـی را تشـکیل می دهد، پس از انتشار ویروس، توسط ده ها کارشناس امنیتی بازنگری می شود. تحلیل آن کد می تواند منجر به شناسایی ریشه ویروس، یعنی همان شرکت آنتی ویروس شود. اگر یک شرکت آنتی ویروس مسئول ایجاد ویروسی شناخته شود، این نه تنها برای وجهه آن شرکت بد خواهد بود، بلکه باعث دادگاهی شدن آن شرکت نیز می شود. [۲۲و۲۱و۱۸].

نتیجه گیری

به نظر می رسد دنیای سایبر دوره جدیدی در تاریخ زندگی بشر خلق کرده اسـت و ارائه گسترده خدمات الکترونیک خواه ناخواه مردم را به سمت این محیط به ظاهر امن اما پرخطر سوق می دهد و این گسترش و بسامد بالا حساسیت پرداخت به ایمنی شبکه را کهً توسط غیر بومی ها انجام می شود افزون می کند؛ درست مثل این که نگهبانی و پاسداری از مردم یک کشور توسط ملل دیگر انجام شود.! درست است که ما خالق این فضا نبوده ایم اما جایگاه امروز بشر به حکم سنت و توارث بر پایه دانش مشترک بنا شده و در دنیای امروز این به اشتراک گذاری لحظه ای متوقف نمی شود؛ ما هم باید در این راه سهیم باشیم.
اصولاً فناوری ها با هدف مرتفع سازی نیازهای بشر زاده می شوند اما به دنبال افزوده شدن فناوری وارداتی به جرگه ابزار های مورد استفاده جامعه، طبعاً نیازها و کاربردهای آن نیز وارداتی می شود. در آن حال گاهی دیده میشـود که ناچیزترین مولفه یعنی نام آن فن مشـکل ساز شـده و تا مدتی دعوا بر سـر واژه های منصوب فراگیر آن می شود. جلوگیری از ورود فناوری هم شدنی به نظر نمی رسد.
تولیدکنندگان امروزی افزون بر نیازهای جامعه خود، جوامع دیگر را هم مد نظر دارند هرچند نیازها و ابزارهای بومی ما را نمی شناسـند یا نمی خواهند آن طور که باید بشناسـند. بهتر اسـت بگوییم آنها در قبال این شناخت مسئولیتی ندارند، این ما هستیم که باید به سرعت در جهت بومی سازی و فراتر از آن مشارکت در ایجاد فناوری گام برداریم. نمونه ابتدایی این بومی سـازی تولید نرم افزار فارسی است که آن هم برای اتصال به مرکز و دریافت قلم های الکترونیکی مورد نیاز سامانه همان دیوار آتش و محافظ سامانه عامل را غیر فعال کند. این در حالی است که آنتی ویروس رایانه شما و شرکت سازنده آن از این مورد بی خبر است!
در این باره، فرایند بومی سازی کاری است پایه ای که نیازمند پشتکار و همت کارگزاران و بانیان آن می باشد. باید با سرمایه گذاری در این راه و تلاش کارشناسان و نخبگان کشور، روش های ایمنی سامانه تعریف و تدوین شود. این رویه در بیشتر کشورها در حال اجراست. بنابراین، زمانی که سخن از ایمنی سامانه به میان می آید، با آزمون و خطا راه به جایی نمی بریم و با واردات بی رویه و آسان انگاری، همچنان دست ما کوتاه خواهد ماند. اما، با سرمایه گذاری هدفمند و برنامه ریزی درست و ریزبین، می توان به گسترش سایبر امن در کشور، همت گماشت.

منابع و مآخذ

[1] Chen, T.M (2003). Trends in Viruses and Worms. The Internet Protocol Journal, Vol.6, No.3 P.P 23-33.
[2] Cluley G. (2000).Trends in Virus Writing and Anti-Virus Technology. Available from: http://www.securitywatch.com/TRE/092100.html.
[3] Anandarajan, M. (2002). Internet Abuse in the Workplace. Communications of the ACM, Vol.45, No.1, P.P 53–54.
[4] Dhillon, G., & Backhouse, J. (2000). Information System Security Management in the New Millennium. Communications of the ACM, Vol.43, No.7, P.P 125–128.
[5] Holmes, J. (2003). Formulating an Effective Computer Use Policy. Information Strategy: The Executive's Journal, Vol.20, No.1, P.P 26–33.
[6] Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. Information Resources Management Journal, Vol.18, No.4, P.P 21–38.
[7] Leach, J. (2003). Improving User Security Behavior. Computers & Security, Vol.22, No.8, P.P 685 – 692.
[8] Huang, D. L., Rau, P-L., Rau, P., & Salvendy, G. (2008). Perception of Information Security. Behaviour & Information Technology, November, 1–12.
[9] Ng, B.Y., Kankanhalli, A., & Xu, Y. (2009). Studying Users' Computer Security bBehavior: A Health Belief Perspective. Decision Support Systems, Vol.46 No.4, P.P 815–825.
[10] Information Management & Computer Security, Vol.5, No.5, P.P 182–190.
[11] Patel, S. C., Graham, J. H., & Ralston, P. A. (2008). Qualitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Eenhancements. International Journal of Information Management, Vol.28, No.6. P.P 483–491.
[12] Stephen, B., & Petropoulakis, L. (2007). The Design and Iimplementation of an Agent-Based Framework for Acceptable Usage Policy Monitoring and Enforcement. Journal of Network & Computer Applications, Vol.30, No.2, P.P 445–465.
[13] Alizadeh, N. (2008). From Super Computers to Pen Computers. Rahyaft, No.41, pp. 89 - 92.
[14] Ettredge, M., Richardson, V.J. (2003). Information Transfer among Internet Firms: the Case of Hacker Attacks. Journal of Information Systems, Vol.17, No.2, P.P 71-82.
[15] Siau, K., Nah, F. F., & Teng. (2002). Acceptable Internet Use Policy, Communications of the ACM, Vol.45, No.1, P.P 75–79.
[16] Whitman. (2004). In Defense of the Realm: Understanding Threats to Information Security. International Journal of Information Management, Vol.24, No.1, P.P 43–57.
[17] Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A Policy Framework for Information Security. Communications of the ACM, Vol.46, No.7, P.P 101–106.
[18] Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The Information Security Policy Unpacked: A Critical Study of the Content of University Policies. International Journal of Information Management, Vol.29, No.6, P.P 449–457.
[19] Doherty, N. F., & Fulford, H. (2006). Aligning the Information Security Policy with the Strategic Information Systems Plan. Computers & Security, Vol.25, No.1, P.P 55–63.
[20] Herath, H. M. P. S., & Wijayanayake, W. M. J. I. (2009). Computer Misuse in the Workplace. Journal of Business Continuity & Emergency Planning, Vol.3, No.3, P.P 259–270.
[21] Albrechtsen, E. (2007). A Qqualitative Study of Users' View on Information Security.
Computers & Security, Vol.26, No.4, P.P 276–289.
[22] Dhillon, G.,&Torkzadeh, G. (2006). Value-Focused Assessment of Information System Security in Organizations. Information Systems Journal, Vol.16, No.3, P.P 293–314.