امنیت اطلاعات

محمد مهدی واعظی نژاد

به نام خداوندی که به انسان برخاسته از خاک خرد بخشید، از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشــکار فــرو فرستاد تا انسان ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.

تقدیم به ساحت مقدس حضرت فاطمه الزهرا سلام الله علیها

فهرست مطالب

	عنوان	شماره صفحه
۰	سخنی با خوانندگان	۷
۱	الزام های امنیتی و حفظ حریم خصوصی در برنامه های بهداشت و درمان ابری	۱
۲	شناخت و پاک سازی ویروس Viper	۱۶
۳	همه چیز در مورد استاکس نت	۲۵
۴	انتشار استاکس نت قبل از آسیب پذیری فایل lnk.	۴۳
۵	عبور از پسورد Windows 7 در ۹ ثانیه	۴۶
۶	نحوه گذشتن از پسورد بایوس	۵۲
۷	امنیت بانکداری همراه	۵۹
۸	امنیت پیامک های تلفن همراه	۶۴
۹	امنیت سیستم عامل های تلفن همراه	۶۶
۱۰	امنیت همراه در شبکه های اجتماعی	۷۰
۱۱	امنیت مرورگرهای وب	۷۸
۱۲	امنیت مرکز داده	۸۴
۱۳	استانداردهای امنیت اطلاعات سازمانی	۸۷
۱۴	سامانه مدیریت امنیت اطلاعات	۹۳
۱۵	ممیزی امنیتی و مستندسازی سیستم های کامپیوتری	۹۷
۱۶	آشنایی با استاندارد امنیت اطلاعات در صنعت کارت پرداخت	۱۰۱
۱۷	شبکه ملی اطلاعات (اینترنت ملی)	۱۰۶
۱۸	گوگل کروم، سیستم عامل اینترنت	۱۱۸
۱۹	اینترنت، فیلترینگ و بازی با پورت ها	۱۲۳
۲۰	رمزنگاری اطلاعات در سازمان با IPsec	۱۲۷

۲۱	VPN، روشی جدید برای سرقت اطلاعات	۱۳۱
۲۲	شرحی بر آسیب پذیریWebkit	۱۳۳
۲۳	Jailbreak؛ مرکز حملات جدید علیه iPhone	۱۳۶
۲۴	نرم افزار L0phtCrack 6	۱۳۸
۲۵	نحوه صحیح بازکردن CD و Flash	۱۴۴

سخنی با خوانندگان

امروزه با گسترش روز افزون فناوری اطلاعات در سازمان ها و بهره گیری از ابعاد گسترده آن در امر خدمات رسانی و حتی تولید محصولات، عنصر ارزشمندی به نام "اطلاعات" در پیکره سازمان ها پدید آمده که مهمترین دارایی هر سازمان نیز به شمار می رود.

استفاده از فناوری اطلاعات و بهره مندی از سیستم های ذخیره و پردازش اطلاعات، به عنوان ابزاری قدرتمند، باعث متمایز شدن سازمان ها از یکدیگر گشته و آن هایی که از این فرصت های بی بدیل تکنولوژیکی بتوانند در زمان مناسب خویش، به بهترین نحو ممکن بهره برداری نمایند، گوی سبقت را از سایر رقبا ربوده و باعث سودآوری کسب و کار خود خواهند شد.

بنابراین در دنیای رقابتی امروز، اطلاعات به عنوان عنصری حیاتی که بقای سازمان ها به شدت به آن وابسته است، نیازمند راه کارهای حفاظتی مناسب جهت جلوگیری از تخریب، دستکاری، حذف و یا ایجاد وقفه در خدمات می باشد.

کتابی که پیش رو دارید، مجموعه ای از مقالات اینجانب در طول دو سال گذشته است که با نگاهی به امنیت اطلاعات و تمرکز بر حفظ و نگهداشت اطلاعات، تألیف گشته و اکنون با نام "امنیت اطلاعات"، تقدیم خوانندگان گرامی می شود.

محمد مهدی واعظی نژاد

خدمتگزار امام المهدی عج الله تعالی فرجه الشریف

۱

الزام های امنیتی و حفظ حریم خصوصی در برنامه های بهداشت و درمان ابری

با توجه به سیاست های ابلاغی وزارت بهداشت، درمان و آموزش پزشکی کشورمان مبنی بر الزام بیمارستان ها و مراکز درمانی به تشکیل پرونده های الکترونیک سلامت[1] و همچنین یکپارچه سازی این پرونده ها در یک پایگاه داده واحد کشوری، لزوم ایجاد یک محیط امن به اشتراک گذاری پرونده الکترونیک سلامت، که مورد تأیید کارشناسان بهداشت و درمان و همچنین متخصصان امنیت فناوری اطلاعات باشد، بیش از پیش نمایان است.

به کارگیری الگوی رایانش ابری[2] که به روزترین و پیشرفته ترین فناوری در زمینه زیرساخت های فناوری اطلاعات به شمار می رود، با بهره مندی از قابلیت های پویای خویش، معمول ترین روش برای اشتراک گذاری پرونده های الکترونیک سلامت و یکپارچه سازی آن ها می باشد که در کشورهای توسعه یافته جهان، زیرساخت های آن به شدت در حال توسعه و خدمات مبتنی بر ابر نیز با سرعت، رو به گسترش است.

در این مقاله، سعی می شود تا با تعریف مفاهیم مهم و اساسی پرونده الکترونیک سلامت و رایانش ابری، مسایل مرتبط با امنیت سیستم ها و تجهیزات پزشکی، حفظ حریم خصوصی بیماران و دست اندرکاران امر پزشکی، دسترسی و مدیریت امن EHRها، بر اساس استانداردهای ISO/IEC 27001 و استاندارد ملی ایران به شماره ۱۳۲۲۰ بررسی گردیده و یک مدل جامع امنیتی برای سیستم های EHR که مبتنی بر رایانش ابری است، معرفی گردد. یک مدل جامع امن برای سیستم مراقبت های بهداشت و درمان ابری که ضمن رعایت تمامی

---

[1] Electronic Health Record (EHR)

[2] Cloud Computing

نکات امنیتی، تکنیک های مورد استفاده آن نیز برای پیاده سازی بهتر، به راحتی توسط کارشناسان، قابل فهم و درک باشد.

کلمات کلیدی: پرونده الکترونیک سلامت، رایانش ابری، بهداشت و درمان ابری، امنیت، حریم خصوصی

مقدمه:

رایانش ابری، یک تکنولوژی جدید و به عبارتی بهتر، یک نگرش صحیح در پروژه های سرمایه گذاری فناوری اطلاعات است که علاوه بر کاهش شدید هزینه ها، عملکرد بهتر و قابلیت های فراوانی را به ارمغان آورده است. این فناوری، راهی برای تغییر مدل های کسب و کار نبوده، بلکه همچون پدیده اینترنت، انقلابی در زیرساخت های فناوری اطلاعات، قلمداد می شود که معماری نوینی را در توسعه، استقرار، اجرا و ارایه خدمات نرم افزاری به همراه داشته است.

هم اکنون، شرکت های بزرگی همچون مایکروسافت، گوگل و آمازون، علاوه بر ارایه نرم افزارهای مبتنی بر ابر، اعلام کرده اند که اهداف آتی آن ها، انتقال برنامه های کاربردی به محیط های ابری خواهد بود. برنامه هایی که بر روی ابرها مستقر شده و به راحتی، همچون ابر، بر روی سرورهای پیشرفته شناور هستند. پایگاه های داده ابری، تحول بزرگی را در تمرکز داده ها و اطلاعات ایجاد نموده اند.

تعریف های EHR، EMR، CDO، PHR و بررسی رابطه میان آن ها

توجه به پرونده الکترونیک سلامت و مدارک الکترونیک پزشکی[1]، در چشم انداز فراگیر دیجیتالی مراقبت های بهداشتی برای بهبود ایمنی، کیفیت مراقبت از بیمار و کاهش هزینه مراقبت های بهداشتی و درمانی، ضروری است. EHRها معمولاً متشکل از برخی از زیرمجموعه های EMR هستند در حالی که EMRها توسط ارایه دهندگان مراقبت های بهداشت فردی ارایه می شوند. تعامل مناسب میان EHRها باعث می شود تا EMR به پتانسیل های لازم جهت تحول در ارایه مراقبت های بهداشتی با کیفیت بالا و هزینه های مقرون به صرفه، نایل شود.

پرونده الکترونیک سلامت، در واقع شرح قانونمند مواردی است که برای بیمار در یک سازمان تحویل مراقبت[2]، چه به صورت بستری یا سرپایی، اتفاق افتاده است. EMR توسط دست اندرکاران بهداشت و درمان، به عنوان یک سند، برای نظارت و مدیریت ارایه مراقبت های بهداشتی در درون یک CDO، ایجاد، حفظ و نگهداری می شود.

معمولاً یک سیستم EMR از چندین سیستم زیرمجموعه مختلف، شامل مخزن اطلاعات بالینی[3]، سیستم پشتیبان تصمیم گیری بالینی[4]، واژگان کنترل شده پزشکی[5]، ارایه دهنده جهت ورودی کامپیوتری[6]، سیستم مدیریت داروخانه[7]، پرونده مدیریت پزشکی الکترونیک[8] و بعضی از سیستم های مستندات بالینی تشکیل شده است.

---

[1] Electronic Medical Record (EMR)

[2] Care Delivery Organization (CDO)

[3] Clinical Data Repository (CDR)

[4] Clinical Decision Support System (CDSS)

[5] Controlled Medical Vocabulary (CMV)

[6] Computerized Provider Order Entry (CPOE)

[7] Pharmacy Management System (PMS)

[8] electronic Medication Administration Record (eMAR)

EHR که توسط بیمار ایجاد می شود، متعلق به او بوده و زیرمجموعه ای از EMR است که توسط CDOها نگهداری می شود. پرونده سلامت شخصی[1] نیز، خلاصه کامل و دقیقی از تاریخچه بهداشتی و درمانی یک فرد است که با جمع آوری اطلاعات از منابع مختلف، شامل EMR و EHR به دست می آید. بنابراین، با توجه به تعاریف استاندارد ISO/TS 18308 و تحلیل های انجمن سیستم های مدیریت و اطلاعات مراقبت سلامت[2]، می توانیم نتیجه بگیریم که پرونده پزشکی بیمار، ممکن است به PHR، EMR و EHR اشاره داشته باشد.

مدل های بهداشت و درمان ابری

بهداشت و درمان ابری را می توان بر اساس مدل های سرویس ابری و الگوهای استقرار ابرها، به موارد مختلفی تقسیم بندی نمود.

بر اساس مدل های سرویس ابری، ارایه دهندگان مراقبت های بهداشت و درمان ابری به ۳ دسته تقسیم می شوند:

- برنامه های کاربردی در ابر (نرم افزار به عنوان یک سرویس[3]): در این مدل، برنامه های بهداشت و درمان از طریق یک رابط کاربری سبک مانند مرورگر وب، بر روی زیرساخت های ابری، اجرا می شوند.

در این نوع مدل از خدمات ابری، امنیت و حفاظت از حریم خصوصی، به عنوان بخشی جدایی ناپذیر از SaaS، به دریافت کنندگان مراقبت های بهداشتی ارایه می شود.

---

[1] Personal Health Record (PHR)

[2] Health Information and Management System Society (HIMSS)

[3] Software as a Service (SaaS)

- سیستم عامل در ابر (پلت فرم به عنوان یک سرویس[1]): این مدل، توانایی استقرار یا به دست آوردن برنامه های نوشته شده با استفاده از زبان های برنامه نویسی و ابزارهای پشتیبانی آن را توسط ارایه دهنده خدمات ابری، به دریافت کنندگان ارایه می دهد.

در این نوع مدل، برنامه های کاربردی مورد استفاده، قابل پیکربندی و کنترل بوده و تلاش می شود تا با مکانیزم های امنیتی اساسی در ارایه دهنده خدمات ابری، مانند رمزگذاری اطلاعات، تأیید هویت و مجوزهای لازم و همچنین در سطح برنامه های کاربردی، با تعیین میزان دسترسی و کنترل آن، سازوکارهای حفاظتی لازم برای تأمین امنیت و حفظ حریم خصوصی به عمل آید.

- زیرساخت در ابر (زیرساخت به عنوان یک سرویس[2]): در این مدل، ارایه پردازش، ذخیره سازی، کنترل محدود امور شبکه ای (مانند فایروال ها)، بعضی از منابع محاسباتی، اجرا و کنترل نرم افزارهای دلخواه شامل سیستم عامل و برنامه های کاربردی، توسط دریافت کنندگان خدمات ابری، قابل تنظیم است.

در این نوع مدل از خدمات ابری، توسعه دهندگان نرم افزارهای بهداشتی و درمانی، مسئول کامل حفاظت از امنیت و حفظ حریم خصوصی بیماران، به شمار می روند.

در مدل های استقرار رایانش ابری برای برنامه های بهداشت و درمان ابری نیز می توان به موارد زیر اشاره نمود:

- ابر خصوصی: زیرساخت ابری است که تنها برای یک CDO اجرا شده و متعلق به آن می باشد.

---

[1] Platform as a Service (PaaS)

[2] Infrastructure as a Service (IaaS)

لحاظ نمودن نکات امنیتی و حفاظت از حریم خصوصی کسانی که در یک EHR در حال اجرا توسط CDO هستند، برعهده ارایه دهنده خدمات ابری که در اینجا همان CDO می باشد، است.

- ارتباطات ابری: زیرساخت ابری به اشتراک گذاشته شده توسط چندین CDO که نگرانی های بهداشتی، درمانی و امنیتی مشترکی مانند مأموریت ها، سیاست ها، نیازمندی های امنیتی و سایر ملاحظه ها را دارند.
- ابر عمومی: زیرساخت ابری که در دسترس عموم مردم یا یک گروه صنعتی بزرگ بوده و متعلق به یک ارایه دهنده خدمات ابری است.

در این نوع مدل از استقرار ابری، توسعه دهندگان نرم افزار و ارایه کنندگان مراقبت های بهداشتی، مسئول کامل حفاظت از امنیت و حفظ حریم خصوصی بیماران هستند.

به طور خلاصه، باید اذعان داشت که امنیت و حفظ حریم خصوصی، چیزی بسیار فراتر از اجرای دسترسی های کاربری و رمزهای عبور بوده و به کارگیری و اعمال الزام های امنیتی، یک ضرورت بزرگ برای سیستم هایی است که از اطلاعات حساس و حیاتی برخوردار هستند.

با اجرای دقیق یک مدل مبتنی بر ابر، می توان بالاترین سطوح امنیت فیزیکی، شبکه ای، برنامه های کاربردی، داده ها و سیستم های داخلی را تضمین نمود که استراتژی هایی همچون تهیه نسخه های پشتیبان از اطلاعات، روش ها و سیاست های امن داخلی، شیوه های استاندارد تنظیم های امنیتی و صدور گواهینامه ها نیز در بطن آن گنجانده شده است. موارد مهمی همچون رمزنگاری اطلاعات و احراز هویت کاربران نیز به طور مرتب در حال اجرا است.

آیا رایانش ابری می تواند در بهداشت و درمان هم استفاده شود؟

امروزه، بسیاری از ارایه دهندگان خدمات مراقبت های بهداشتی و درمانی و همچنین شرکت های بیمه، از سیستم های مدارک پزشکی الکترونیک استفاده کرده و سوابق پزشکی بیماران را در قالب فرم های مخصوص پرونده های الکترونیک، در پایگاه های داده متمرکز، ذخیره و نگهداری می کنند.

معمولاً یک بیمار، مراجعات متعددی به ارایه دهندگان خدمات مراقبت های بهداشتی و درمانی مختلف، از جمله پزشکان، دندانپزشکان، متخصصین، درمانگران و دیگر دست اندرکاران امر پزشکی دارد که ممکن است، هر کدام از این بیماران، بیمه های درمانی مختلفی هم داشته باشند.

در حال حاضر، هر یک از ارایه دهندگان خدمات بهداشت و درمان، دارای پایگاه داده مخصوص به خود، برای ذخیره پرونده های الکترونیک سلامت است. به اشتراک گذاری اطلاعات، بین دست اندرکاران بهداشت و درمان، با عنوان اشتراک اطلاعات بین سیستم های مدارک الکترونیک پزشکی، توصیف می شود که در آن، در واقع، مدارک الکترونیک بیماران، میان EMRهای مختلف، به اشتراک گذاشته می شود.

از مهم ترین موانع پیش روی سلامت الکترونیک به شیوه های سنتی، می توان به هزینه زیاد و قابلیت های ضعیف استفاده از آن اشاره نمود که ضمن تحمیل هزینه های گزاف به مراکز بهداشتی و درمانی (که حتی بعضی از آن ها با امورات خیریه اداره می شود)، امکان بهره مندی از آن بسیار پایین بوده و در عمل، در بسیاری از موارد، علیرغم تلاش های بسیار، با شکست مواجه گردیده است.

در رایانش ابری، مراکز بهداشتی و درمانی می توانند ضمن کاهش شدید هزینه ها، از طریق ادغام سیستم ها وتجهیزات سخت افزاری و به اشتراک گذاری آن ها بر اساس نیاز کاربران، یک محیط پویا را در ارایه خدمات بهداشتی و درمانی ایجاد نموده که علاوه بر

مالکیت سیستم، هزینه های تعمیر و نگهداری آن، تهیه نسخه های پشتیبان از اطلاعات و استخدام کارشناسان فنی، به ارایه دهندگان خدمات ابری واگذار می شود.

همزمان با رشد و گسترش این فناوری، استانداردهای مخصوص به آن نیز در حوزه سلامت، در حال تدوین و اجرا است که هدف آن ها بیشتر بر روی چگونگی نگهداری پرونده های الکترونیک سلامت، نحوه نظارت بر بیماران، مدیریت بیماری ها و نحوه همکاری مراکز درمانی برای ارایه مراقبت های بهداشتی کارآمد و مؤثر و همچنین تحلیل و بررسی قاعده مند داده های نظام الکترونیک سلامت، متمرکز شده است.

پیش بینی می شود که با حرکت و انتقال نرم افزارهای درمانی به الگوهای مبتنی بر رایانش ابری و مدیریت آن ها از طریق ابرها، انقلابی در راه انجام مراقبت های بهداشتی و درمانی به وقوع بپیوندد که نتایج آن، امکان دسترسی به مراقبت های بهداشتی را برای همگان و در همه جا فراهم ساخته و علاوه بر کاهش شدید هزینه مسافرت های درمانی بیماران و پزشکان، گام های اساسی برای ارایه و بهره مندی از نظام الگومند سلامت که جهت رفاه حال بیماران، با فناوری ادغام، همگام و همسو شده است، برداشته شود.

مسایل امنیتی و حریم خصوصی در بهداشت و درمان

در چند سال گذشته، تحقیقات فراوانی بر روی مسایل امنیتی و حفظ حریم خصوصی در سیستم های اطلاعات بهداشتی و درمانی انجام شده است. استاندارد ISO/TS 18308، تعریف هایی را از امنیت و مسایل مربوط به حفظ حریم خصوصی در EHR ارایه می دهد.

انجمن بین المللی IMIA[1] نیز برای بررسی مسایل مرتبط با حفاظت از داده ها و امنیت در محیط های بهداشت و درمان تشکیل شده است که به طور عمده، بر روی امنیت در سیستم های EHR و ارایه راه حل های امنیتی مشترک برای برقراری ارتباط داده های بیمار متمرکز

[1] International Medical Informatics Association (IMIA)

شده است. در اروپا هم، یک پروژه به نام "انفورماتیک پیشرفته در پزشکی/محیط امن برای سیستم های اطلاعات در پزشکی[1] " برای بررسی طیف گسترده ای از مسایل امنیتی در مراقبت های بهداشتی، آغاز شده است که دستورالعمل هایی عملی نیز برای ایجاد مراقبت های بهداشتی امن منتشر کرده است.

اخیراً، خدمات بهداشتی و انسانی آمریکا[2] گزارشی با هدف توسعه پرونده سلامت شخصی منتشر کرده است که در آن، PHR بیماران، بدون توجه به جایی که بیمار، خواستار مراقبت های پزشکی است، می تواند به صورت امن از طریق اینترنت در دسترس پزشکان و دیگر ارایه دهندگان خدمات مراقبت های بهداشتی و درمانی قرار گیرد.

در ادامه این مقاله، مروری بر مسایل امنیتی و حفظ حریم خصوصی در EHR مبتنی بر ابر داشته و سعی می کنیم تا الزام های مورد نیاز برای دسترسی امن به داده های EHR در ابر را بررسی نماییم. از آن جا که امنیت و حفظ حریم خصوصی و همچنین حفاظت از مدارک الکترونیکی بیماران، از بالاترین درجه اهمیت برخوردار است، می توان ۳ اصل مهم را برای اطمینان از حفظ حریم خصوصی، صحت محتوا و قابلیت اعتماد منبع سوابق پزشکی الکترونیکی در نظر گرفت. اول این که، تمامی پرونده های الکترونیک سلامت (شامل PHR، EHR یا EMR) باید از طریق رمزنگاری توسط مالکان آن ها، کنترل، محافظت، ذخیره سازی، انتقال و مورد دسترسی امن قرار گیرند. دوم این که، در ایجاد و نگهداری EHRها باید اصالت محتوا و جامعیت داده ها با توجه به امکان سفارشی ساختن حفظ حریم خصوصی بیماران در فرآیندهای ادغام EHR در نظر گرفته شود. و سوم، دسترسی و به اشتراک گذاری EHRها باید از طریق امضای دیجیتال و فرآیندهای صدور گواهینامه، جهت جلوگیری از تغییرات غیرمجاز در محتوای اطلاعات حساس پزشکی، صورت گیرد.

---

[1] Advanced Informatics in Medicine/Secure Environment for Information Systems in MEDicine (AIM/SEISMED)

[2] Health and Human Services

امنیت بهداشت و درمان ابری و الزام های حفظ حریم خصوصی

اگرچه بعضی از نیازهای امنیتی و حفظ حریم خصوصی در برنامه های بهداشت و درمان ابری به مدل سرویس یا استقرار ابری مورد استفاده، بستگی دارد ولیکن ما در این قسمت، سعی می کنیم تا به طور خلاصه، مهم ترین این موارد را مورد بررسی قرار دهیم:

- ممکن است یک بیمار، پرونده های الکترونیک سلامت متعددی در EMRهای CDOهای مختلف داشته باشد که اطلاعات آن ها، برای بیمار حساس بوده و جزء حریم خصوصی وی قلمداد می شود و او با توجه به نگرانی هایی که دارد، نخواهد اطلاعات این پرونده ها فاش شده یا در دسترس افراد غیر مجاز قرار بگیرد. بنابراین، دسترسی به اطلاعات EHR باید از طریق یک روال کنترل شده و بر اساس مجوزهای لازم صورت گیرد.
- ممکن است یک پزشک، بیمارانی در سیستم های EMR مختلف داشته باشد که لازم است تا از طریق مکانیزم های احراز هویت، دسترسی وی به مدارک بیماران امکان پذیر شود. صحت اطلاعات نیز، پس از پایان بررسی پرونده بیمار، باید به تأیید وی برسد.
- ذخیره سازی امن اطلاعات و تضمین یکپارچگی داده ها توسط CDOها.
- در مواردی که اطلاعات EHR در CDOهای مختلف به اشتراک گذاشته می شود، باید مالکیت EHR به صورت دقیق و شفاف مشخص بوده و مالک آن، تمامی الزام های امنیتی را در خصوص EHR به عمل آورد. مالک EHR موظف است تا تمهیدهای لازم را برای محافظت از اطلاعات در برابر دسترسی های غیرمجاز و یا سوء استفاده از اطلاعات پزشکی بیمار از طریق روش های فیزیکی مانند توکن های احراز هویت کاربران سیستم EMR و همچنین رمزنگاری اطلاعات به عمل آورد.
- برای ورود کاربران به سیستم EHR، باید از روش های صحت و تصدیق هویت کاربران استفاده شود.

- استفاده از گواهینامه های SSL و پروتکل های رمزنگاری اطلاعات برای تأمین امنیت داده های در حال انتقال در طول شبکه های عمومی نظیر اینترنت، توسط CDO.
- با استفاده از روش هایی همچون امضای دیجیتالی، نهان نگاری و رمزگذاری اطلاعات، باید از عدم انکار اطلاعات توسط افراد دخیل در امر مراقبت های بهداشتی جلوگیری نموده و تمامی افراد، ملزم به انجام تعهدات خویش گردند.
- در سیستم مراقبت های بهداشتی و درمانی، اطلاعات باید از یکپارچگی و جامعیت به معنای حفظ دقت، صحت و قوام داده ها برخوردار بوده و از دستکاری غیرمجاز، مصون بمانند. همچنین محرمانگی این اطلاعات نیز طبق استاندارد ISO 17799 به معنای این که "اطمینان حاصل شود که اطلاعات تنها در دسترس کسانی است که مجاز به دسترسی به آن ها هستند" تضمین شود که این امر نیز، به کمک روش های رمزنگاری امکان پذیر است.
- اطلاعات EHR بر اساس اصل دسترس پذیری امنیت، باید در زمانی که به آن ها نیاز است، در دسترس افراد مجاز قرار گیرد.
- سیستم های کامپیوتری که EHR در آن ها ذخیره و پردازش می شود، باید از کنترل های امنیتی لازم برخوردار باشند و در برابر کمترین مخاطرات، همچون نوسانات و قطع برق، خللی در ارایه خدمات پزشکی برای بیماران ایجاد نگردد.
- ارتقاء سیستم ها و تجهیزات و همچنین خرابی های ناشی از فرسودگی سخت افزار، نتواند اختلال هایی را در ارایه خدمات به بیماران ایجاد کند.
- سیستم های مراقبت های بهداشتی و درمانی، در فواصل زمانی معین جهت اطمینان از صحت عملکرد و رعایت نکات امنیتی لحاظ شده، توسط کارشناسان مربوطه، مورد ممیزی قرار گیرند.
- تهیه نسخه های پشتیبان از اطلاعات، بر اساس قواعد مشخص، توسط CDOها صورت پذیرد.

- تمامی تعریف های جدید در سیستم EMR از قبیل اضافه نمودن پزشکان، بیماران و یا کاربران سیستم، باید بر اساس یک روش اصولی و قاعده مند و طبق ضوابط مشخصی که از قبل توسط CDO وضع گردیده است، صورت پذیرد.
- هر بیمار در سیستم EMR باید دارای ID منحصر به فرد بوده که ردیابی فعالیت ها و اقدام های انجام شده توسط ارایه دهندگان مراقبت های بهداشتی و درمانی، از طریق آن شناسه صورت پذیرد. برای تعریف این PID بهتر است که از کدهای یکتا همچون کد ملی به جای کدهای انتخابی که ممکن است با دیگر CDOها همخوانی و/یا ناهمخوانی داشته باشد و یا به کار بردن نام و نام خانوادگی که در آن، افراد مشابهت های زیادی با یکدیگر دارند، استفاده شود.
- در مواردی که کاربران سیستم EMR و دست اندرکاران امر مراقبت های بهداشتی و درمانی، دچار اشتباه یا خطایی در روند ورود اطلاعات در سیستم EMR و یا حذف ناخواسته اطلاعات از پرونده الکترونیک سلامت بیمار می شوند، باید CDO با دید باز با این موارد برخورد نموده و ضمن دادن شهامت لازم، آنان را برای اعلام موارد اشتباه تشویق نماید، چرا که پرونده بیمار باید در تمام شرایط، حاوی اطلاعات صحیح و درستی از اطلاعات حساس بیمار باشد. با آموزش اصولی کاربران، باید از تکرار موارد این چنینی جلوگیری نمود.
- طرح های رمزنگاری مورد استفاده توسط سیستم، در حین کارآمدی، باید آسان به استفاده بوده و به راحتی نیز در تمام فرآیندهای سیستمی جدید، قابل توسعه و گسترش باشد. بهتر است از طرح هایی که به شدت وابسته به کلید خصوصی افراد هستند، جلوگیری شده و از الگوریتم های رمزنگاری مناسب استفاده نمود.
- کنترل های امنیتی لازم برای هنگامی که یکی از کاربران سیستم EMR تغییر شغل یافته و یا از سازمان اخراج می گردد، اعمال گردد تا از افشاء یا تغییرات ناخواسته و نامجاز در سیستم جلوگیری شود.
- امضای دیجیتال یک ابزار بسیار مفید برای ارایه صحت، صداقت و عدم انکار است. باید از هویت امضاء کننده جهت استراق سمع و موارد دیگر، حفاظت های لازم توسط CDOها به عمل آید.

مدل امنیتی جامع EHR

در این قسمت، مدل امنیتی جامعی را از EHR مبتنی بر محیط های بهداشت و درمان ابری ارایه می کنیم که بیانگر نگرش مان از لحاظ رعایت موارد امنیتی و مصونیت از چالش های حفظ حریم خصوصی بیماران است. این مدل جامع، ضمن لحاظ نمودن موارد فوق، می تواند به عنوان الگویی در ارایه خدمات بهداشتی و درمانی به مردم در نظر گرفته شود. مدلی که علاوه بر تمرکز روی "بیمار محوری"، درصدد است تا حفاظتی جامع و پیشگیرانه را از مخاطرات امنیتی، سرلوحه فعالیت های خویش قرار دهد.

این مدل جامع، از سه مؤلفه اصلی زیر تشکیل می شود:

1. *جمع آوری و یکپارچه سازی امن EHR*

بر اساس تعاریفی که از PHR، EHR، EMR و CDO بیان گردید و ارتباطی که میان آن ها برقرار است، نخستین امر در استقرار امنیت، یکپارچه سازی EHRها در یک محیط امن است که توسط CDO فراهم می گردد.

CDOها علاوه بر ذخیره سازی این اطلاعات، بر اشتراک گذاری امن داده های EHR نیز نظارت کاملی داشته و تلاش می کنند که در روابط خود با دیگر CDOها، تمامی نکات امنیتی را رعایت نمایند. حفظ اصالت داده ها، محرمانگی، یکپارچگی، حصول اطمینان از عدم انکار، ادغام و ترکیب EHRها با یکدیگر در درون EMRهای مختلف، تأیید و تصدیق اطلاعات، اعمال گواهینامه های امنیتی در ارتباطات، به کارگیری روش های احراز هویت، امضاء دیجیتالی، نهان نگاری و رمزنگاری، به طور مشخص جزء وظایف CDO بوده و بر عهده آن می باشد که ملزم است دستورالعمل ها و تمهیدهای لازم را در این خصوص به عمل آورد.

لازم به ذکر است که EHRها در فرمت های خاصی تهیه می شوند که قابل استفاده در تمام سیستم های EMR بوده و مشکلی به نام عدم انطباق اطلاعات در فرآیندهای بهداشتی و

درمانی، هرگز به وقوع نخواهد پیوست. لذا اشتراک گذاری EHRها به سهولت امکان پذیر بوده و جستجوی ایمن و دسترسی به اطلاعات بیمار به راحتی صورت می گیرد.

۲. *ذخیره سازی امن EHR و مدیریت دسترسی*

EHRها با فرمت خاصی، در سرورهای امنی که در مکان هایی ایمن واقع شده اند، ذخیره می شوند که کنترل دسترسی آن ها در مرحله قبل انجام شده است. رمزنگاری داده ها در حین ذخیره سازی و انتقال اطلاعات همواره در حال جریان است و هیچ یک از افراد، قادر به دخالت در این امر نیستند. دسترسی ها، بر اساس مجموعه ای از کنترل های مبتنی بر نقش و یا سیاست های مبتنی بر ویژگی، شکل گرفته و اعمال می شود. اجرای سیاست های امنیتی در هر سطحی از CDO لازم الاجرا بوده و توسط پارامترهای قابل سنجش، ارزیابی[1] می گردد. دسترسی به اطلاعات رمزنگاری شده، از طریق مکانیزم های رمزگشایی مبتنی بر هویت و اخذ مجوز بر اساس کلیدهای خصوصی صورت می گیرد.

۳. *مدل استفاده امن از EHR*

مدل استفاده امن، جزء سوم از مدل جامع امنیتی EHR پیشنهادی ما است که دسترسی به داده ها و اطلاعات EHR را برای بیماران، پزشکان و دست اندرکاران امر مراقبت های بهداشتی و درمانی بر اساس امضاء دیجیتال و تأیید هویت میسر می سازد. به نحوی که حتی بیماران نیز برای دسترسی به پرونده الکترونیک سلامت خویش، دارای کلید خصوصی خاص خود بوده و تمام مشاهدات و عملکردهای آنان در هر لحظه، به صورت طولانی مدت در سیستم های پیش بینی شده، ذخیره و نگهداری می شود.

علاوه بر سه مؤلفه اصلی ذکر شده در بالا، ارتباطات و فرآیندهای میان آن ها نیز باید به صورت امنی که از طریق الگوریتم های رمزنگاری حاصل می شود، صورت بگیرد تا اطمینان حاصل شود که اطلاعات در حال انتقال، از شنود[2] و دستکاری غیرمجاز در شبکه های

---

[1] Assess

[2] Sniff

عمومی، محفوظ هستند. استفاده از پروتکل ها و گواهینامه های امنیتی همچون SSL، TLS و IPSec می تواند کمک شایان توجهی را در تحقق این امر نماید.

نتیجه گیری:

ما در این مقاله، رویکردی روش مند را برای بررسی مدل های امنیتی و الزام های حفظ حریم خصوصی برای نرم افزارهای بهداشت و درمان ابری اتخاذ کردیم. تحلیل های مختصری از مخاطرات امنیتی که می تواند یک EHR را تحت تأثیر خویش قرار دهد، ارایه نمودیم و راه های حفاظت از آن ها را برشمردیم و سعی کردیم تا با ارایه یک مدل جامع امن برای EHR، نشان دهیم که چگونه می توان در عین استفاده از فناوری های نوین همچون رایانش ابری، مراقبت های بهداشتی و درمانی را نیز به نحو مطلوبی انجام داد.

۲

شناخت و پاک سازی ویروس Viper

مقدمه

آغاز دومین حمله بزرگ سایبری سازمان یافته به تأسیسات زیربنایی کشورمان در قالب ویروس هوشمند اینترنتی **"Viper"**، آثار و پیامدهای بسیار مخربی را در بیشتر سازمان های دولتی ایران بر جای گذاشته و منجر به از دست رفتن اطلاعات بسیار زیادی گردیده است.

ویروس Viper که توسط رژیم متخاصم اسرائیل، در ابتدا به منظور کاهش تولیدات نفتی، طراحی و به پیکره سیستم های وزارت نفت منتقل و سپس در سراسر شبکه دولتی ایران منتشر شده است، قادر به پاک کردن برگشت ناپذیر تمامی اطلاعات از سرورها بوده و بازیابی اطلاعات را تحت هر شرایطی، غیر ممکن می نماید. در ضمن، به علت ناشناخته بودن آن، تاکنون هیچ یک از شرکت های امنیتی موفق به شناسایی و تجزیه و تحلیل کدهای آن نشده اند.

به نظر می رسد که هدف اصلی این ویروس، نفوذ در همه سیستم های موجود در شبکه، به منظور پاک نمودن تمام اطلاعات موجود بر روی هارد دیسک های آن ها می باشد.

لازم به ذکر است که این تهدید، دومین حمله بزرگ سایبری در طی دو سال اخیر است که منجر به خسارات جبران ناپذیری به اطلاعات و سیستم های تأسیسات زیربنایی کشورمان گردیده است. نخستین حمله توسط رژیم اسرائیل، با ورود کرم اینترنتی Stuxnet به نیروگاه هسته ای بوشهر در سال ۱۳۸۹ با هدف تأخیر در راه اندازی ژنراتور برق هسته ای بوشهر، آغاز گردید که توانست تعداد بسیار زیادی از سانتریفیوژها را از چرخه تولید خارج نماید.

سایر نام ها

این ویروس، به نام های زیر شناخته می شود:

Viper , Wiper

بهتر است یادآوری شود که ویروس Viper هیچ ارتباطی با ویروس Wipe که از تهدیدات امنیتی سال گذشته به شمار می رود، نداشته و اشتباهاتی که در این خصوص مطرح می شود، به دلیل نداشتن دانش و تخصص فنی و همچنین شباهت نزدیک اسمی آن ها به یکدیگر است.

سیستم های آسیب پذیر

Microsoft Windows Server 2003 SP2 , Windows XP on 32-bit Platforms

پراکنش جغرافیایی

Viper فقط برای حمله سایبری به جمهوری اسلامی ایران، طراحی و منتشر شده است. هدف اصلی این نرم افزار مخرب، تأسیسات زیربنایی ایران می باشد که با توجه به شواهدی که از حمله و نفوذ آن به وزارتخانه ها و سازمان های مهم کشورمان موجود است، این فرضیه قوت بیشتری می گیرد.

لازم به ذکر است که تاکنون به جز ایران، هیچ گزارشی از فعالیت های مخرب این ویروس در سایر کشورها گزارش نشده است.

تاریخچه کشف

اوایل اردیبهشت ماه سال جاری (۱۳۹۱)، نخستین بار ویروس Viper در سیستم های وزارت نفت و شرکت های تابعه آن گزارش گردید و منجر به ایجاد مرکز بحران در این وزارتخانه برای مقابله با آسیب های آن و همچنین آمادگی برای حملات مشابه بعدی شد. بر این اساس و به منظور کنترل این حمله سایبری، دسترسی به اینترنت برای کارکنان وزارتخانه نفت و کارکنان شرکت ملی نفت، شرکت های پتروشیمی، پالایشگاه و توزیع قطع گردید. همچنین، خدمات اینترنت در خارگ، بهرگان، سیری، لاوان، قشم و کیش نیز مسدود شد.

اگر چه این ویروس، مدتی قبل وارد سیستم های وزارت نفت گردید ولی به علت عدم تخصص و دانش کافی متخصصان امنیت اطلاعات این وزارتخانه، اقدام مناسبی برای مقابله با آن صورت نگرفت که در نهایت، به چنان مرحله بحرانی و حساسی رسید که حتی چند روز، منجر به قطع کامل تمامی ارتباطات و خدمات رسانی در سطح وزارتخانه نفت و شرکت های تابعه آن گردید. بلافاصله بعد از چند روز، این ویروس در سایر وزارتخانه ها و سازمان های مهم کشورمان نیز کشف گردید.

اگرچه هنوز در مورد زمان آغاز به کار Viper اتفاق نظر وجود ندارد ولی بنابر اظهارات و شواهد موجود، این ویروس از یک ماه پیش، در سیستم های وزارت نفت موجود بوده و در طول این مدت، بدون شناسایی شدن به کار خود ادامه داده است که البته این مطلب، از طریق بررسی تاریخ نشانه های دیجیتالی این ویروس، به خوبی قابل استناد و درک خواهد بود.

نام گذاری

Viper در اصلاح لغوی به معنای "آدم خائن و بد نهاد" می باشد که از همین نام نیز برای نفوذ در رایانه ها استفاده می کند.

طراحی و سازماندهی

این ویروس، به چندین زبان مختلف از جمله C، ++C و سایر زبان های شیء گرا نوشته شده است. Viper، چنان در نفوذ به سیستم ها، حتی با عبور از فایروال های قدرتمند و با تنظیمات صحیح و پیچیده همچون ISA، ماهر است که به طور یقین، متخصصانی با پشتوانه فنی قوی و دارای انواع تخصص ها، آن را ایجاد کرده و هدایت می کنند.

با توجه به شناسایی کاملی که این ویروس انجام می دهد، پیچیدگی کد، خطرناک بودن حمله آن، نفوذ به مراکز خاص و همچنین منابع و هزینه های مورد نیاز برای انجام این حمله به همراه ریسک بالایی که پروژه در پی داشته است، تنها دولت ملی می تواند توانایی های آن را داشته باشد.

در شرایط فعلی، محتمل ترین سناریو در مورد این ویروس، سرویس جاسوسی سایبری رژیم متخاصم اسرائیل می باشد چرا که از مدت ها قبل، وعده حمله به ایران در فروردین ماه امسال را داده بود که اکنون با حمله سایبری و هدف قرار دادن تأسیسات زیربنایی کشورمان، به این وعده خویش، جامه عمل پوشانده است. هر چند که این موضوع، تاکنون به تأیید مقامات اسرائیلی نرسیده است ولی اکثر کارشناسان، معتقد به این قضیه هستند.

عملکرد

با توجه به ناشناخته بودن نحوه نفوذ این ویروس، حتی با عبور از ISA، هنوز مشخص نیست که این ویروس از چه آسیب پذیری ها و حفره هایی در ویندوز بهره می برد.

با توجه به تجربیات اینجانب، احتمالاً این ویروس پس از نفوذ به شبکه، با سوء استفاده از یک آسیب پذیری ویندوز، می تواند حق دسترسی Admin به سایر pc ها را برای خود ایجاد کرده، سپس با استفاده از آسیب پذیری های دیگری،کنترل شبکه را در دست گرفته و با انتشار خود در تمام سیستم ها، اقدام به از بین بردن همه اطلاعات هارد دیسک ها کند.

آن گاه پس از موفقیت آمیز بودن این عمل، ارتباط سیستم ها در شبکه قطع شده، هیچ سیگنالی به مانیتورها ارسال نگردیده و صفحه نمایشگر، مشکی می شود. پس از راه اندازی دوباره سیستم نیز، فقط تا مرحله بارگذاری بایوس پیش رفته و ویندوز بارگذاری نمی گردد. در بعضی از موارد نیز، صدای بوق ممتد از سیستم به گوش می رسد که بیانگر آسیب های سخت افزاری به آن می باشد. همه این ها، از عجایب ویروس Viper است.

به احتمال بسیار زیاد، Viper از یک آسیب پذیری منحصر به فرد دیگر نیز برای دور زدن [1]فایروال ها و اتمام فرآیندهای امنیتی سیستم، استفاده می کند. هر چند که، برای به دست آوردن اطلاعات بیشتر در این خصوص، باید کد ویروس مورد بررسی و تحلیل عمیق قرار گیرد.

تغییرات در سیستم

هنوز از فایل ها و سرویس هایی که توسط این ویروس در سیستم آلوده ایجاد می شود، اطلاعاتی در دست نیست و همچنین مشخص نیست که چه تغییراتی در Registry ویندوز به وجود می آید اما همان طور که اشاره گردید، تمامی فایل ها از روی هارد دیسک حذف گردیده و چنانچه فایلی نیز باقی بماند از هر نوع فرمت نوشتاری همچون .doc , .docx , .xls , pdf , ... و حتی فرمت های تصویری، پس از باز شدن فایل مربوطه، تمامی اطلاعات آن به یکباره پاک می گردد. اگرچه ممکن است هیچ تغییری در حجم فایل ها ایجاد نگردد و در ظاهر، فایل ها دارای محتویات باشند، اما در اصل، فاقد هر گونه اطلاعاتی بوده و اطلاعات آن ها نیز غیر قابل بازیابی می باشد.

در ضمن، هنوز مدارکی در دست نیست که این ویروس، اطلاعاتی را از طریق HTTP به آدرس های مشخصی که سرورهای آن هستند، ارسال می نماید یا خیر.

---

[1] Bypass

با این تفاسیر، حذف تمامی فایل ها، حتی فایل های سیستمی سیستم عامل، از مهمترین مشخصه های این ویروس محسوب می شود.

انتشار

Viper علاوه بر اینترنت، با کپی کردن خودش در درایوهای USB یا فایل های به اشتراک گذاشته شده در شبکه های رایانه ای، منتشر می شود.

جلوگیری

شرکت های امنیتی به دلیل نشناختن این ویروس و عدم مواجهه با آن، تاکنون هیچ تحقیق یا گزارشی را به شرکت مایکروسافت ارایه نکرده اند و بنابراین، به روز رسانی و یا اصلاحیه ای نیز برای از بین بردن آسیب پذیری های مورد استفاده این ویروس، عرضه نشده است. هم اکنون، هیچ یک از ضد ویروس ها نیز قادر به شناسایی و پاک سازی این ویروس نیستند.

با این وجود، انجام فعالیت های زیر توسط همه مدیران و کاربران سیستم می تواند باعث جلوگیری و یا کاهش خطر این ویروس شود:

- غیر فعال کردن ویژگی AutoRun یا AutoPlay سیستم برای جلوگیری از اجرای خودکار فایل های قابل اجرا در درایوهای قابل جابجایی.
- تهیه نسخه های پشتیبان از داده ها و اطلاعات، به صورت مرتب و در فاصله های زمانی کم و مشخص و نگهداری آن ها بر روی یک سیستم دیگر، جدا از شبکه.
- غیر فعال کردن درایوهای قابل جابجایی و تمامی درایورها (Floppy , CD , DVD) از طریق Setup سیستم و در نظر گرفتن یک رمز عبور قوی برای Setup
- اصلاح نقاط آسیب پذیر نرم افزارهای نصب شده در سیستم.
- به روز رسانی سیستم عامل و نصب آخرین وصله های امنیتی بر روی آن.

- به روز رسانی نرم افزار ضد ویروس[1] در فاصله های زمانی کوتاه مدت و فعال کردن گزینه به روز رسانی خودکار[2] برای دریافت خودکار آخرین به روز رسانی[3] ها.
- محدود کردن شدید دسترسی به آدرس های اینترنتی، با استفاده از فایروال و مسیریاب[4] تا زمان برطرف شدن خطر و رفع تهدید.
- استفاده از رمز عبور پیچیده که ترکیبی از عدد، حروف بزرگ و کوچک و نمادها[5] می باشد برای کلمه عبور کاربران، به نحوی که این رمزها توسط dictionary attackها به راحتی قابل شناسایی و کشف نبوده و در عین حال، برای کاربران هم به یاد ماندنی باشد.
- همه ارتباطات ورودی از اینترنت به سرویس های سازمان که نباید در دسترس عموم باشد را با استفاده از فایروال، مسدود[6] کرده و تنها به سرویس هایی اجازه دهید که به مردم خدمات ارایه می دهند.
- هرگز نباید با نام کاربری administrator به سیستم وارد شد. کاربران و برنامه ها هم باید پایین ترین سطح دسترسی لازم را داشته باشند.
- غیرفعال کردن اشتراک گذاری منابع و فایل ها در شبکه، اگر به اشتراک گذاری آن ها نیازی نیست. در صورت نیاز، از لیست های کنترل دسترسی[7] استفاده کرده و مشخص نمایید که چه افراد یا کامپیوترهایی اجازه دسترسی به آن ها را دارند.
- غیرفعال کردن و حذف سرویس های غیرضروری فعال در سیستم. اگر هم کد مخربی علیه یکی از سرویس ها پیدا شد، تا زمانی که وصله امنیتی[8] آن سرویس در

---

[1] Antivirus
[2] Automatic updates
[3] Update
[4] Router
[5] Symbols

[6] Deny
[6] Access Control List (ACL)
[8] Patch

سیستم نصب نشده است، آن سرویس را غیر فعال کرده و یا دسترسی به آن را محدود نمایید.

- سرویس هایی همچون HTTP، FTP، Mail و DNS مهمترین سرویس های یک شبکه متصل به اینترنت هستند. بنابراین، همیشه وصله های امنیتی این سرویس ها را مهم در نظر گرفته و به روز نگهدارید. همچنین توسط فایروال، دسترسی به آن ها را کنترل نمایید.
- پیکربندی email سرور در جهت حذف نامه های الکترونیکی که حاوی فایل ضمیمه است. از این فایل ها برای گسترش تهدیداتی همچون vbs. ، bat. ، exe. ، pif. و scr. استفاده می شود.
- کامپیوترهای آلوده را به سرعت برای جلوگیری از گسترش بیشتر آلودگی در شبکه ایزوله کنید و تا زمانی که از برطرف شدن آلودگی مطمئن نشده اید، آن ها را وارد شبکه نکنید.
- استفاده نکردن از بلوتوث[1] در شبکه. در صورت نیاز، دید دستگاه را در حالت پنهان[2] تنظیم کنید تا توسط دستگاه های دیگر پیدا نشده و حتماً از رمز عبور نیز برای برقراری ارتباط بین دستگاه ها استفاده نمایید.

پیشگیری

پیشگیری از حوادث و کنترل امنیت سیستم نیاز به یک رویکرد چند لایه دارد که از آن با عنوان "دفاع در عمق" یاد می شود. این لایه، شامل سیاست ها و رویه ها، آگاهی و آموزش، تقسیم بندی شبکه، کنترل دسترسی ها، اقدام های امنیتی فیزیکی، سیستم های نظارتی همچون فایروال و ضد ویروس، سیستم های تشخیص نفوذ[3]، رمز کاربری و ... است.

---

[1] Bluetooth
[2] Hidden
[3] Intrution Detection System (IDS)

بهترین روش برای پیشگیری هم معمولاً تجزیه و تحلیل خطر، شناسایی نقاط آسیب پذیر سیستم ها و شبکه، کنترل سیستم ارزیابی امنیتی و همچنین توسعه برنامه های اولویت بندی برای از بین بردن یا به حداقل رساندن ریسک خطر است.

۳

همه چیز در مورد استاکس نت[1]

مقدمه

"Stuxnet" کرم اینترنتی که آرام و بی صدا در دل صنعت ایران می خزید و قلب تپنده صنایع تولیدی کشورمان را نشانه رفته بود، یکدفعه با کشف ناگهانی اش آنچنان هیاهویی برپا کرد که در کمتر از چند دقیقه به عنوان اول اغلب خبرگزاری های مهم بین المللی همچون CNN[2]، Reuters[3] و Washington Post[4] تبدیل گردید.

محققان مراکز امنیتی هم با اظهار نظرهایی سریع، سعی در تشریح این کرم داشته و شرکت امنیتی سیمانتک[5] اعلام می کند که رایانه های ایران مورد هجوم شدید کرم خطرناکی به نام Stuxnet قرار گرفته اند که اطلاعات سیستم های کنترل صنعتی[6] را سرقت کرده و بر روی اینترنت قرار می دهد.

محمود لیالی رئیس شورای فناوری اطلاعات وزارت صنایع و معادن کشورمان نیز علاوه بر اینکه هدف گیری این کرم را در راستای جنگ الکترونیکی علیه ایران می داند، از شناسایی شدن ۳۰ هزار IP صنعتی آلوده به این کرم در ایران خبر داده است.

---

[1] Stuxnet

[2] September 24,2010 title: Cyberworm "targets Iran" (October 5,2010 title: Stuxnet : Fact vs.Theory)

[3] September 24,2010 title: Cyber attack appears to target Iran-US tech firm

[4] October 1,2010 title: U.S. power plants at risk of attack by computer worm like Stuxnet

[5] Symantec

[6] Industrial Control Systems

Stuxnet، نخستین کرم صنعتی جهان است که با هدف حمله سایبری به زیرساخت های حیاتی صنعت ایران، آسیب به تأسیسات هسته ای نطنز و در نهایت، تأخیر در راه اندازی نیروگاه اتمی بوشهر طراحی و منتشر شده است.

این کرم قادر به ایجاد اخلال در تجهیزات حساس، مانند تخریب سرعت چرخش روند بالا از آرایه های سانتریفیوژ و کاهش تعداد سانتریفیوژهای غنی عملیاتی، کنترل فعالیت های صنعتی، محدودیت دور توربین، روغن کاری و یا بستن سیستم های خنک کننده، تخریب لوله های گاز و حتی انفجار دیگ های بخار کارخانجات مختلف است.

سایر نام ها

این کرم در شرکت های امنیتی، به نام های زیر شناخته می شود:

Troj/Stuxnet-A [Sophos], W32/Stuxnet-B [Sophos], W32.Temphid [Symantec], WORM_STUXNET.A [Trend], Win32/Stuxnet.B [Computer Associates], Trojan-Dropper:W32/Stuxnet [F-Secure], Stuxnet [McAfee], W32/Stuxnet.A [Norman], Rootkit.Win32.Stuxnet.b [Kaspersky], Rootkit.Win32.Stuxnet.a [Kaspersky]

سیستم های آسیب پذیر

Microsoft Windows 2000 , Windows 95 , Windows 98 , Windows Me , Windows NT , Windows Server 2003 , Windows Vista , Windows XP on 32-bit Platforms

پراکنش جغرافیایی

Stuxnet برای حمله به نقاط جغرافیایی خاص، طراحی و منتشر شده است. علاوه بر ایران، کشورهای اندونزی و هند نیز مورد هجوم این نرم افزار مخرب قرار گرفته اند.

خبرگزاری چین هم در خبری اعلام کرده است که: "Stuxnet در بیش از شش میلیون رایانه چینی نفوذ کرده و مقامات پکن نگران هستند این کرم رایانه های بیشتری را در چین مورد حمله قرار دهد".

تاریخچه کشف

بیست و دوم تیرماه سال جاری[1]، شرکت امنیتی VirusBlockAda بلاروس، نخستین بار Stuxnet را در رایانه یکی از مشتریان ایرانی خود مشاهده و کشف نمود.

این موضوع، در تاریخ بیست و چهارم تیرماه هم توسط شرکت زیمنس[2] آلمان گزارش گردید و یک ماه بعد، هنگامی که شرکت مایکروسافت تأیید کرد که این کرم در حال هدف قرار دادن سیستم های ویندوز در مدیریت سیستم های کنترل صنعتی بزرگ موسوم به SCADA[3] است، به شهرت رسید.

اگرچه متخصصان امنیت هنوز در مورد زمان آغاز به کار Stuxnet اتفاق نظر ندارند ولی به گفته "الیاس لووی" مدیر ارشد فنی بخش "پاسخگویی ایمنی سیمانتک" با توجه به تاریخ نشانه های دیجیتالی که از این کرم رایانه ای به جا مانده، می توان گفت که از دی ماه

---

[1] July 13,2010

[2] Siemens

[3] Supervisory Control And Data Acquisition (SCADA)

۱۳۸۸ این کرم میان رایانه ها در گردش بوده و ماه ها بدون شناسایی شدن به کـار خـود ادامـه داده است.

نام گذاری

فایل ایجاد شده توسط Stuxnet از نام میرتاس[1] برای نفوذ در رایانه ها استفاده مـی کنـد. میرتاس کلمه ای با ریشه عبری است که اشاره به داستان "اسـتر" دارد. اسـتر، زن دوم خشـایار شاه در ایران باستان است که زنی یهـودی بـوده و بـا وسـاطت عمـوی خـود مردخـاوی کـه از مشاوران پادشاه ایران بود، خشایار راضی به ازدواج با او می شود. بـر ایـن اسـاس، اسـتر ملکـه یهودیان شناخته می شود.

علاوه بر این، MYRTUS ممکن است به قطعات معروف به RTU[2] کـه یکـی از ویژگـی های مدیریت سیستم های SCADA اسـت اشـاره داشـته باشـد. همچنـین عـدد ۱۹۷۹۰۵۰۹ در درون کد این کرم، شاید بیانگر تاریخ ۹ مه ۱۹۷۹ یعنـی روز "Habib Elghanian" ، یـک یهودی فارسی که در تهران اعدام شد نیز باشد.

طراحی و سازماندهی

Stuxnet که تقریباً نیم مگابایت حجم دارد به چندین زبان مختلـف از جملـه C، C++ و سایر زبان های شیء گرا نوشته شده است. این کرم، چنان در اسـتفاده از آسـیب پـذیری هـای اصلاح نشده ویندوز ماهر است که کارشناسان امنیت معتقدند تیمی متشکل از متخصصـانی بـا پشتوانه قوی و دارای انواع تخصص ها از Rootkit گرفته تا Database، آن را ایجاد کرده

---

[1] MYRTUS
[2] Remote Terminal Units (RTU)

و هدایت می کنند. Symantec هم تخمین می زند که پنج تا ده نفر، شش ماه روی این پروژه کار کرده اند.

محققان سیمانتک و کسپرسکی[1] اعتقاد دارند با توجه به شناسایی کاملی که این کرم انجام می دهد، پیچیدگی کد و خطرناک بودن حمله آن، صرفاً نمی تواند کار یک گروه حرفه ای هک خصوصی باشد.

به نظر آن ها، منابع و هزینه های مورد نیاز برای انجام این حمله به همراه ریسک بالایی که پروژه در پی داشته است، آن را خارج از قلمرو یک گروه هک خصوصی قرار داده و تنها دولت ملی می تواند توانایی های آن را داشته باشد. همچنین، تیم ایجادکننده کرم به سخت افزار فیزیکی واقعی نیز برای تست نیاز داشته اند.

متخصصان با در نظر گرفتن تمامی شرایط، محتمل ترین سناریو در مورد این کرم را یک گروه هک وابسته به سرویس جاسوسی یک کشور می دانند. گمانه های موثق نیز حاکی از آن است که Stuxnet برای مقابله با برنامه های هسته ای نیروگاه بوشهر، توسط اسرائیل طراحی و به وسیله لپ تاپ پیمانکاران روسی در بوشهر، به تأسیسات هسته ای ایران منتقل شده است.

اگرچه این موضوع هنوز توسط رژیم اشغالگر اسرائیل تأیید و اثبات نشده است اما اطلاع از آن می تواند اقدام های پیشگیرانه ایران برای مقابله با سایر روش های جاسوسی را با آگاهی بیشتری همراه کند.

عملکرد

محققان ابتدا فکر می کردند که Stuxnet فقط از یک آسیب پذیری اصلاح نشده ویندوز سوء استفاده می کند[1] و از آن به عنوان کرم نفوذ کننده از میان برهای ویندوز نام می بردند.

[1] Kaspersky

متخصصان Symantec و Kaspersky برای به دست آوردن اطلاعات بیشتر، کد این کرم را مورد بررسی و تحلیل عمیق تر قرار دادند. نخست در مدت یک هفته تا یک هفته و نیم، حفره Print spooler [2] توسط محققان Kaspersky پیدا شده، سپس حفره EoP [3] (تغییر حق دسترسی) ویندوز هم توسط این شرکت امنیتی کشف و حفره دوم EoP نیز توسط کارشناسان مایکروسافت شناسایی گردید. محققان Symantec هم به طور جداگانه آسیب پذیری Print spooler و دو آسیب پذیری EoP را در مرداد ماه پیدا کرده و کدهای مخربی که این سه آسیب پذیری اصلاح نشده ویندوز را هدف قرار می دهد، شناسایی نمودند.

اما عجایب Stuxnet که همزمان می تواند از چهار نقص امنیتی اصلاح نشده ویندوز، برای دسترسی به شبکه ها سوء استفاده کند به اینجا ختم نمی شود. این کرم همچنین از یک حفره ویندوز [4] که در سال ۲۰۰۸ توسط به روز رسانی MS08-067 اصلاح شده بود نیز استفاده می کند. این نقص امنیتی همان آسیب پذیری مورد استفاده کرم Conficker در اواخر سال ۲۰۰۸ و اوایل سال ۲۰۰۹ بود که به میلیون ها سیستم در سراسر جهان آسیب وارد کرد.

هنگامی که Stuxnet از طریق درایو USB آلوده وارد یک شبکه می شود، با سوء استفاده از آسیب پذیری های EoP حق دسترسی Admin به سایر رایانه ها را برای خود ایجاد کرده و سیستم هایی که برنامه های مدیریت Siemens SIMATIC WinCC و pcs 7 scada را اجرا می کنند پیدا می کند. سپس کنترل آن ها را با سوء استفاده از یکی از

---

[1] Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732)

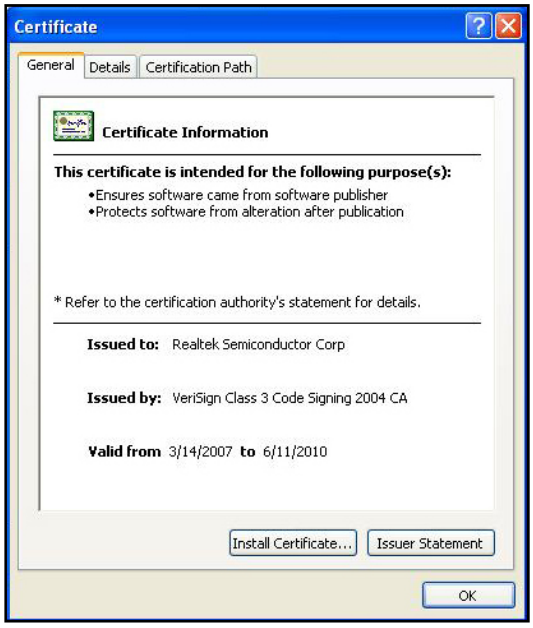
[2] Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073)

[3] Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)

[4] W32.Downadup (a.k.a Confiker)

آسیب پذیری های Print spooler یا MS08-067 در دست گرفته و رمز عبور پیش فرض زیمنس را برای در اختیار گرفتن نرم افزار SCADA آزمایش می کند[1]. بعد، کد خودش را همچون یک Rootkit درون PLC[2] بارگزاری و پنهان می کند تا قابل مشاهده نباشد. آن گاه نرم افزار PLC را دوباره برنامه ریزی کرده و دستورات جدید را طبق اهداف خود صادر می نماید.

نکته قابل توجه این است که Stuxnet برای قانونی نشان دادن کدهای حمله خود و اعتباردهی به درایوهایش، دو گواهی معتبر[3] دیجیتالی امضاء شده Realtek و JMicron را سرقت می کند:



[1] Server = .\wincc -- vid = wincccconect -- pwd = 2wsxcder

[2] Programmable Logic Control (PLC)

[3] Valid

نصب

هنگامی که یک درایو USB آلوده به کامپیوتر وصل می شود، Stuxnet خودش را به عنوان فایل های زیر به کامپیوتر غیرآلوده کپی می کند:

%System%\drivers\mrxcls.sys
%System%\drivers\mrxnet.sys

سپس فایل mrxcls.sys را به عنوان یک سرویس با مشخصات زیر ثبت می کند:

Display Name: MRXCLS
Startup Type: Automatic
Image Path: %System%\drivers\mrxcls.sys

آن گاه برای این سرویس، مسیر زیر را در registry ایجاد می کند:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\"ImagePath" = "%System%\drivers\mrxcls.sys"

این کرم، همچنین فایل mrxnet.sys را به عنوان یک سرویس با مشخصات زیر ثبت می کند:

Display Name: MRXNET
Startup Type: Automatic
Image Path: %System%\drivers\mrxnet.sys

برای سرویس بالا نیز، مسیر زیر را در registry ایجاد می کند:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"

این کرم، همچنین فایل های زیر را که هر کدام نسخه های رمز شده Stuxnet هستند، ایجاد می کند:

- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF

- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF

در ضمن، اگر کرم از روی سیستم آلوده پاک شود، فایل %System%\drivers\mrxcls.sys فایل های بالا را برای تأثیرگذاری مجدد در کامپیوتر رمزگشایی می کند.

تغییرات در سیستم

فایل(های) زیر ممکن است در کامپیوتر آلوده دیده شود:

- %System%\drivers\mrxcls.sys
- %System%\drivers\mrxnet.sys
- %DriveLetter%\~WTR4132.tmp
- %DriveLetter%\~WTR4141.tmp
- %DriveLetter%\Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk
- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF

این کرم فایلی را از سیستم، پاک و یا اصلاح نکرده و در Registry سیستم آلوده نیز به جز ایجاد دو مسیر زیر، هیچ کدام از Subkeyها حذف یا تغییر دیگری صورت نمی گیرد:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\"ImagePath" = "%System%\drivers\mrxcls.sys"

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"

دو پردازش زیر در سیستم ایجاد می شود:

- iexplorer.exe
- lsass.exe

Stuxnet یک بسته قابل اجرا در کامپیوتر را از سرور C&C[1] خود دانلود و اجرا نموده و همچنین اطلاعاتی را از طریق HTTP به آدرس زیر ارسال می کند:

http://[C&C SERVER ADDRESS]/index.php?data=[DATA]

DATA شامل اطلاعات زیر است:

- نسخه سیستم عامل ویندوز
- نام کامپیوتر
- نام گروه شبکه
- نشانه برای آگاهی از نصب بودن نرم افزار SCADA
- آدرس IP همه کارت های شبکه موجود

این اطلاعات با استفاده از یک کلید ۳۱ بایتی XOR رمزگذاری و ارسال می شود. پاسخ دریافت شده از سرور C&C هم با XOR اما توسط یک کلید ۳۱ بایتی متفاوت رمزنگاری شده که هر دو این کلیدها در فایل های dll. قرار داده شده در سیستم آلوده موجود است.

با اتصال کامپیوتر به اینترنت، کرم از طریق پورت ۸۰ با سایت های زیر که سرورهای C&C آن هستند، ارتباط برقرار می کند:

- www.mypremierfutbol.com

[1] Command & Control

- www.todaysfutbol.com

سرور C&C پس از دریافت این اطلاعات، به دو روش می تواند پاسخ دهد: نوع نخست پاسخ، دستورالعمل کرم برای اجرای یکی از شیوه های موجود در کد تهدیدات آن است و نوع دوم پاسخ، یک فایل dll. به سیستم آلوده ارایه و به بارگزاری آن دستور می دهد.

از پاسخ نوع اول به عنوان پوششی برای RPC[1]ها که می خواهد به سیستم فرستاده شود، استفاده می شود. RPC پس از فراخوانی شدن در کامپیوتر می تواند اقدام های زیر را انجام دهد:

- خواندن فایل؛
- نوشتن در فایل؛
- حذف فایل؛
- ایجاد پردازش؛
- تزریق یک فایل dll. به lsass.exe؛
- بارگزاری و اجرای یک فایل dll. اضافه؛
- استخراج منبع ۲۱۰ از فایل dll. اصلی (از این منبع برای تزریق به پردازش های دیگر استفاده می شود)؛
- به روز رسانی پیکربندی اطلاعات کرم؛

این کرم پس از نفوذ به شبکه، فقط کامپیوترهایی که نرم افزار SCADA شرکت زیمنس برای کنترل و مدیریت فعالیت ها در آن ها نصب شده است را هدف قرار می دهد. سپس برای به دست آوردن اطلاعات مشخصی، تعداد زیادی پرس و جو[2] در پایگاه داده نرم افزار Siemens Step 7 انجام داده و با فایل های dll. نرم افزار تعامل برقرار می کند.

---

[1] Remote Procedure Call (RPC)

[2] Querie

آنگاه تلاش می کند به فایل های زیر که توسط نرم افزار Step 7 ایجاد شده اند دسترسی یافته تا کد آن ها را برای طراحی پروژه ها سرقت کند:

- GracS\cc_tag.sav
- GracS\cc_alg.sav
- GracS\db_log.sav
- GracS\cc_tlg7.sav
- *.S7P
- *.MCP
- *.LDF

Stuxnrt همانند یک Rootkit، کد خودش را به PLC در یک سیستم کنترل صنعتی که توسط سیستم های SCADA نظارت می شود، تزریق و پنهان می کند. PLC کامپیوتری است که از ویندوز برنامه ریزی شده تشکیل شده و حاوی کد ویژه ای می باشد که اتوماسیون فرآیندهای صنعتی را کنترل می کند.

این کرم که با نوشتن کد در PLC ، سیستم را کنترل کرده و یا فعالیت های آن را به تعویق می اندازد، برای جلوگیری از تشخیص فایل %DriveLetter%\~WTR4132.tmp آن را با رابط های برنامه های کاربردی[1] زیر از kernel32.dll و Ntdll.dll مرتبط می کند:

از Kernel32.dll:

- FindFirstFileW
- FindNextFileW
- FindFirstFileExW

از Ntdll.dll:

- NtQueryDirectoryFile

[1] API

- ZwQueryDirectoryFile

کرم کد اصلی این توابع را هم با کدی که برای چک کردن فایل ها با مشخصات زیر است، جایگزین می کند:

- نام فایل با پسوند ".lnk"
- آغاز نام فایل با "~WTR" و با پسوند ".tmp"

آن گاه فایل %DriveLetter%\~WTR4132.tmp به فایل dll. دیگری به نام %DriveLetter%\~WTR4141.tmp بارگزاری می شود. Stuxnet برای انجام این کار، از رویکردی متفاوت استفاده کرده و به جای این که "LoadLibrary" رابط های برنامه های کاربردی را برای بارگزاری فایل dll. در حافظه اصلی فراخوانی کند، توابعی را به Ntdll.dll مرتبط کرده و سپس LoadLibrary را با نام فایل خاصی که ایجاد شده است، فراخوانی می کند. این فایل درخواست شده برای بارگزاری، در disk وجود ندارد اما توابع مرتبط شده به Ntdll.dll که به بارگزاری نام خاص فایل برای درخواست ها نظارت دارد، فایل dll. را از یک ناحیه در حافظه اصلی که قبلاً در آن رمزگشایی و ذخیره شده است، بارگزاری می کند. توابع مرتبط شده در Ntdll.dll برای این منظور عبارتند از:

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwCloseFile
- ZwQueryAttributesFile
- ZwQuerySection

سپس فایل dll. فراخوانی شده و کنترل سیستم را در دست می گیرد. این کرم کد خود را نیز به iexplorer.exe به منظور دور زدن فایروال ها تزریق کرده و فرآیندهای امنیتی زیر را به پایان می رساند:

- vp.exe
- Mcshield.exe

- avguard.exe
- bdagent.exe
- UmxCfg.exe
- fsdfwd.exe
- rtvscan.exe
- ccSvcHst.exe
- ekrn.exe
- tmpproxy.exe

انتشار

Stuxnet با کپی کردن خودش در درایوهای USB، نامه های الکترونیک[1] آلوده و یا فایل های به اشتراک گذاشته شده در شبکه های رایانه ای که دارای نقاط آسیب هستند، منتشر می شود.

این کرم خودش را به عنوان فایل های زیر در درایوهای قابل جابجایی کپی می کند که هر دو نام فایل، hardcoded و در واقع فایل های dll. هستند:

- %DriveLetter%\~WTR4132.tmp
- %DriveLetter%\~WTR4141.tmp

همچنین فایل های زیر را به درایوهای بالا کپی می کند:

- %DriveLetter%\Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk

[1] Email

هنگـامی کـه ایـن درایوهـا بـا برنامـه ای کـه توانـایی نمـایش آیکـون هـا را دارد (ماننـد Windows Explorer) مورد دسترسی قرار می گیرد، به جای نمایش آیکـون بـرای فایـل های lnk. کدی را که قابلیـت اجـرای فایـل %DriveLetter%\~WTR4132.tmp را دارد، اجـــرا مـــی کنـــد. هـــدف اصـــلی ایـــن فایـــل، اجـــرای فایـــل DriveLetter%\~WTR4141.tmp است که در درایوهای قابل جابجایی کپـی شـده و سپس در حافظه اصلی سیستم بارگزاری می شود. این فایل است که دو گـواهی معتبـر امضـاء شده Realtek و JMicron را جعل می کند.

این کرم همچنین از یک کد مخرب RPC هم برای منتشر شدن استفاده می کند[1]. عـلاوه بر این، از کد مخرب دیگری[2] نیز که اجـازه مـی دهـد یـک فایـل بـه شـاخه %System% کامپیوتر آسـیب پـذیر نوشـته شـود، بـرای کپـی نمـودن خـودش از کـامپیوتر آلـوده بـه سـایر کامپیوترها استفاده کرده و برای اجرای آن فایل از راه دور[3] هم از یک ویژگی WBEM بهره می برد.

Stuxnet همچنین با کپی نمودن خودش بـه منـابع اشـتراک گذاشـته شـده در شـبکه بـه عنوان فایل زیرکه در حقیقت یک فایل dll. است، منتشر می شود:

%DriveLetter%\ "DEFRAG[RANDOM NUMBER].tmp

البته یک راه که مهاجمان با استفاده از آن ریسک شناسایی شدن و جلوگیری از گسـترش بیش از اندازه این کرم را کم کرده اند، قرار دادن یک شمارنده در درایـو USB آلـوده اسـت که اجازه انتشار کرم از طریق یک داریو USB خاص به بیش از سه کامپیوتر را نداده و بعـد از ۲۱ روز نیز خودش را پاک می کند.

---

[1] Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)

[2] Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073)

[3] Remote code-execution

نکته قابل توجه در خصوص Stuxnet آن است که درون کد پیچیده آن مشخص شده که این کرم در تاریخ ۲۴ ژوئن ۲۰۱۲ انتشار خود را متوقف کرده و خودش را نیز از سیستم آلوده پاک خواهد نمود.

جلوگیری

شرکت مایکروسافت در روز یازدهم مرداد ماه سال جاری، یک به روز رسانی مهم و فوری برای اصلاح نقص ابتدایی Stuxnet عرضه کرد[1]. سپس شرکت های سیمانتک و کسپرسکی نتایج تحقیقات خود را به شرکت مایکروسافت گزارش کردند که باعث شد آسیب پذیری Print spooler به سرعت اصلاح شده[2] و وعده اصلاح دو آسیب پذیری کم خطرتر EoP هم در به روز رسانی امنیتی بعدی داده شود.

اگر چه هم اکنون تمامی ضد ویروس ها قادر به شناسایی و پاک کردن این کرم هستند اما انجام فعالیت های زیر توسط همه راهبران[3] و کاربران سیستم می تواند باعث جلوگیری و یا کاهش خطر این کرم شود:

- غیر فعال کردن ویژگی AutoRun یا AutoPlay سیستم برای جلوگیری از اجرای خودکار فایل های قابل اجرا در درایوهای قابل جابجایی.
- غیر فعال کردن درایوهای قابل جابجایی از طریق Setup سیستم. در صورت نیاز، تنها حالت "فقط خواندنی[4]" را فعال کرده و حتماً یک رمز عبور هم برای Setup در نظر گرفت.
- اصلاح نقاط آسیب پذیر سیستم عامل و نرم افزارهای نصب شده.

---

[1] Microsoft Security Bulletin MS10-046

[2] Microsoft Security Bulletin MS10-061 (September 14,2010)

[3] Administrator

[4] Read-Only

- به روز رسانی نرم افزار ضد ویروس در فاصله های زمانی کوتاه مدت و فعال کردن گزینه به روز رسانی خودکار، برای دریافت خودکار آخرین به روز رسانی ها.
- Stuxnet با سوء استفاده از نقاط آسیب پذیر مشخصی انتشار پیدا می کند. نصب وصله های امنیتی زیر می تواند باعث کاهش خطر این کرم شود:
  - Microsoft Security Bulletin MS10-046
  - Microsoft Security Bulletin MS08-067
  - Microsoft Security Bulletin MS10-061
- دسترسی به آدرس های زیر که سرورهای C&C کرم هستند با استفاده از فایروال و مسیریاب باید مسدود شده و با اضافه کردن به فایل local hosts، به آدرس 127.0.0.1 تغییر مسیر داده شود:
  - www.mypremierfutbol.com
  - www.todaysfutbol.com
- استفاده از رمز عبور پیچیده که ترکیبی از عدد، حروف بزرگ و کوچک و نمادها می باشد برای کلمه عبور کاربران، به نحوی که این رمزها توسط dictionary attackها به راحتی قابل شناسایی و کشف نبوده و در عین حال، برای کاربران هم به یاد ماندنی باشد.
- همه ارتباطات ورودی از اینترنت به سرویس های سازمان که نباید در دسترس عموم باشد را با استفاده از فایروال مسدود کرده و تنها به سرویس هایی اجازه دهید که به مردم خدمات ارایه می دهند.
- هرگز نباید با نام کاربری administrator یا root وارد سیستم شد. کاربران و برنامه ها هم باید پایین ترین سطح دسترسی لازم را داشته باشند.
- غیرفعال کردن اشتراک گذاری منابع و فایل ها در شبکه، اگر به اشتراک گذاری آن ها نیازی نیست. در صورت نیاز، از لیست های کنترل دسترسی استفاده کرده و مشخص نمایید که چه افراد یا کامپیوترهایی اجازه دسترسی به آن ها را دارند.
- غیرفعال کردن و حذف سرویس های غیرضروری فعال در سیستم. اگر هم کد مخربی علیه یکی از سرویس ها پیدا شد، تا زمانی که وصله امنیتی آن سرویس در

سیستم نصب نشده است، آن سرویس را غیر فعال کرده و یا دسترسی به آن را محدود نمایید.

- سرویس هایی همچون HTTP، FTP، Mail و DNS مهمترین سرویس های یک شبکه متصل به اینترنت هستند. بنابراین، همیشه وصله های امنیتی این سرویس ها را مهم در نظر گرفته و به روز نگهدارید. همچنین توسط فایروال، دسترسی به آن ها را کنترل نمایید.
- پیکربندی email سرور در جهت حذف نامه های الکترونیکی که حاوی فایل ضمیمه است. از این فایل ها برای گسترش تهدیداتی همچون .vbs ، .bat ، .exe ، .pif و .scr استفاده می شود.
- کامپیوترهای آلوده را به سرعت برای جلوگیری از گسترش بیشتر آلودگی در شبکه ایزوله کنید و تا زمانی که از برطرف شدن آلودگی مطمئن نشده اید، آن ها را وارد شبکه نکنید.
- استفاده نکردن از بلوتوث در شبکه. در صورت نیاز، دید دستگاه را در حالت پنهان تنظیم کنید تا توسط دستگاه های دیگر پیدا نشده و حتماً از رمز عبور نیز برای برقراری ارتباط بین دستگاه ها استفاده کنید.

پیشگیری

پیشگیری از حوادث و کنترل امنیت سیستم نیاز به یک رویکرد چند لایه دارد که از آن با عنوان "دفاع در عمق" یاد می شود. این لایه، شامل سیاست ها و رویه ها، آگاهی و آموزش، تقسیم بندی شبکه، کنترل دسترسی ها، اقدام های امنیتی فیزیکی، سیستم های نظارتی همچون فایروال و ضد ویروس، سیستم های تشخیص نفوذ، رمز کاربری و ... است.

بهترین روش برای پیشگیری هم معمولاً تجزیه و تحلیل خطر، شناسایی نقاط آسیب پذیر سیستم ها و شبکه، کنترل سیستم ارزیابی امنیتی و همچنین توسعه برنامه های اولویت بندی برای از بین بردن یا به حداقل رساندن ریسک خطر است.

۴

انتشار استاکس نت قبل از آسیب پذیری فایل lnk.

کرم اینترنتی استاکس نت برای انتشار خود توسط درایوهای قابل جابه جایی، از ترفندی اتوران که ایجاد یک فایل autorun.inf در ریشه درایوهای قابل جابه جایی است، بهره می برد.

برای اجرای فایل های دستکاری شده و مخرب در سیستم هدف می توان آن ها را به صورت فایل اجرایی یا یک فایل autorun.inf در رایانه قرار داد. هنگامی که ویندوز فایل autorun.inf را تجزیه می کند، هر کاراکتری را که نتواند درک کند، به عنوان بخشی از دستورات اتوران، محسوب نکرده و همچون کدهای زاید در نظر می گیرد و با توقف عملیات بر روی آن ها، همچنان به تجزیه فایل ادامه می دهد.

استاکس نت با قرار دادن فایل MZ ابتدا در فایل autorun.inf از این واقعیت به نفع خود سوء استفاده می کند. هنگامی که ویندوز، فایل autorun.inf را تجزیه می کند، همه مقادیر MZ را به عنوان کدهای زاید، نادیده گرفته و تنها دستورات اتوران را که در انتهای فایل است، اجرا می نماید. سرصفحه و پاورقی فایل autorun.inf را می توان در شکل های زیر مشاهده کرد:

سرصفحه فایل autorun.inf :

```
00000000: 4D5A9000 03000000 04000000 FFFF0000  MZ▌.........ÿÿ..
00000010: B8000000 00000000 40000000 00000000  ¸.......@.......
00000020: 00000000 00000000 00000000 00000000  ................
00000030: 00000000 00000000 00000000 E0000000  ............à...
00000040: 0E1FBA0E 00B409CD 21B8014C CD215468  ..º..´.Í!¸.LÍ!Th
00000050: 69732070 726F6772 616D2063 616E6E6F  is program canno
00000060: 74206265 2072756E 20696E20 444F5320  t be run in DOS 
00000070: 6D6F6465 2E0D0D0A 24000000 00000000  mode....$.......
00000080: CF7A777C 8B1B192F 8B1B192F 8B1B192F  Ïzw|▌../▌../▌../
00000090: ACDD642F 9D1B192F ACDD622F 9C1B192F  ¬Ýd/▌../¬Ýb/▌../
000000A0: 8B1B182F 6D1B192F ACDD6B2F DA1B192F  ▌../m../¬Ýk/Ú../
```

پاورقی فایل autorun.inf :

```
00041000: 0D0A5B61 75746F72 756E5D0D 0A6F626A  ..[autorun]..obj
00041010: 65637444 65736372 6970746F 723D7B42  ectDescriptor={B
00041020: 33313535 33372D36 3341422D 39353132  315537-63AB-9512
00041030: 2D393941 392D3246 34363737 32333541  -99A9-2F4677235A
00041040: 34347D0D 0A                          44}...
00041050: 636F6D6D 616E643D 2E5C4155 544F5255  command=.\AUTORU
00041060: 4E2E494E 460D0A           5C4D656E  N.INF...    \Men
00041070: 753D4025 77696E64 6972255C 73797374  u=@%windir%\syst
00041080: 656D3332 5C736865 6C6C3332 2E646C6C  em32\shell32.dll
00041090: 2C2D3834 39360D0A                    ,-8496..
000410A0:     0D0A 55736541 75746F50 4C41593D    ..UseAutoPLAY=
000410B0: 300D0A                               0..
```

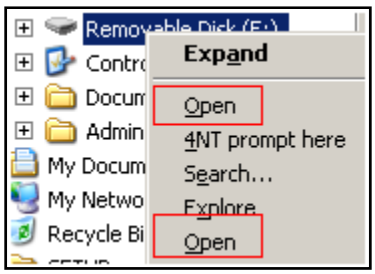
با استخراج کدهای پاورقی، مشاهده می شود که این فایل از دستورات عادی اتوران تشکیل شده است:

```
.?AVZdhrnpIdcahnGvqzdhRnpIdcahn@gfjjefwq@sr@@
[autorun]
objectDescriptor={B315537-63AB-9512-99A9-2F4677235A44}
      Menu\command=.\AUTORUN.INF
      Menu=@%windir%\system32\shell32.dll,-8496

UseAutoPLAY=0
```

توجه کنید که در دستورات، مشخص شده که autorun.inf به عنوان فایل اتوران اجرا شود (کادر مشخص شده در تصویر بالا). با استفاده از این ترفند، autorun.inf ابتدا همانند یک فایل اتوران معمولی و سپس همچون فایل اجرایی، کد کرم را اجرا خواهد کرد.

علاوه بر این شگرد فریبنده، استاکس نت از ترفند دیگری نیز برای افزایش احتمال اجرا شدن خود استفاده می کند. در دستورات اتوران نشان داده شده در شکل بالا، ویژگی AutoPlay نخستین بار خاموش است و یک دستور جدید نیز به منوی راست کلیک اضافه می شود. این دستور، در مسیر %Windir%\system32\shell32.dll,-8496 ایجاد شده و همان طور که در تصویر زیر دیده می شود، کاربر در هنگام مشاهده منوی زمینه برای درایو قابل جابه جایی، در واقع دو دستور "بازکردن" را مشاهده خواهد کرد:



یکی از این دستورات بازکردن، توسط استاکس نت به این منو اضافه شده است. اگر کاربر با استفاده از گزینه اضافه شده به وسیله کرم اقدام به بازکردن درایو کند، کد کرم طبق دستور فایل autorun.inf اجرا شده و سپس یک پنجره اکسپلورر را باز کرده و محتویات درایو را نمایش می دهد. موفقیت این ترفند، به تنظیمات AutoPlay و AutoRun در رایانه هدف بستگی داشته که در صورت غیرفعال کردن این گزینه ها، گسترش کرم هم توسط درایوهای قابل جابه جایی متوقف خواهد شد.

لازم به ذکر است که در اواخر فروردین ماه ۱۳۸۹ نسخه جدیدی از کرم استاکس نت منتشر شده است که برای انتشار خود از یک کد مخرب یعنی آسیب پذیری فایل lnk.[1] به جای ترفندهای فوق، استفاده می کند.

[1] BID 43073

۵

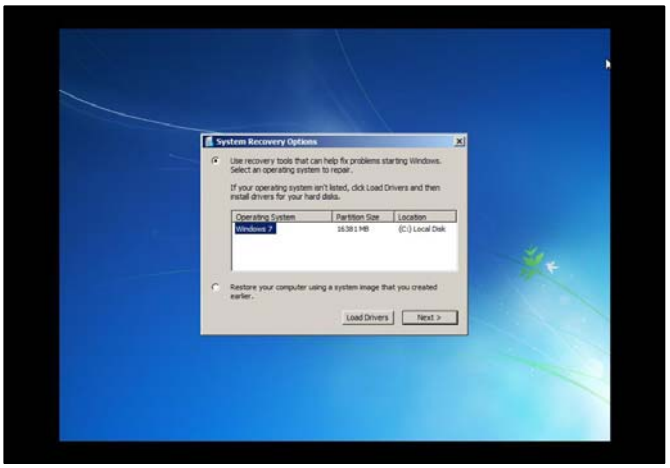
عبور از پسورد Windows 7 در ۹ ثانیه

شرکت مایکروسافت که با ارایه دو محصول جدید Windows 7 و Windows Server 2008 تلاش فراوانی داشت تا سرانجام به همه شایعاتی که در خصوص امنیت ویندوزهایش مطرح می شود، پایان دهد، هیچ گاه تصور نمی کرد که تنها با گذشت چند ماه از ارایه آخرین دستاوردهایش، مثل همیشه با مشکلات امنیتی متعددی دست به گریبان باشد.

رخنه ها و مسایل امنیتی، انگار بخشی جدایی ناپذیر از محصولات این شرکت شده اند و همچون غولی شکست ناپذیر، در برابر عظمت آن قد برافراشته اند. برای اثبات این ادعا، کافی است که مراحل زیر را اجرا کرده و فقط در چند مرحله، با گذشتن از کلمه عبور ویندوز، حتی به بازیابی دوباره آن اقدام نمایید:

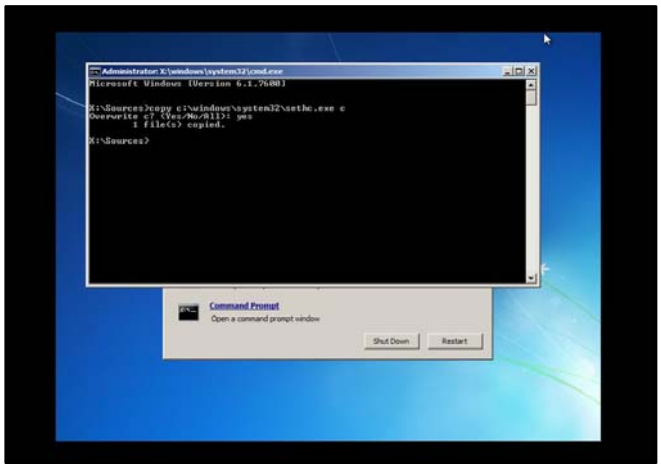
ابتدا DVD ویندوز 7 را در داخل درایو کامپیوتر قرار داده و با restart نمودن سیستم، آن را از روی DVD راه اندازی کنید. پس از بالا آمدن صفحه نصب ویندوز، دکمه Next را زده و در پنجره بعدی، گزینه Repair your computer را انتخاب نمایید.

سپس در پنجره باز شده، پس از انتخاب سیستم عامل، دکمه Next را زده و در صفحه بعدی، بر روی گزینه Command Prompt کلیک کنید.



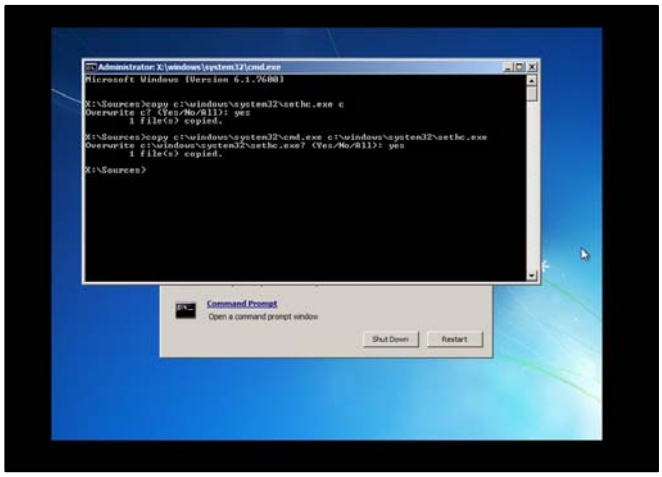
پس از اجرا شدن برنامه cmd، باید از فایلی که قرار است برای ورود به ویندوز دستکاری شود، در محل دیگری نسخه پشتیبان بگیرید. برای انجام این کار، دستور زیر را تایپ کنید:

```
copy c:\windows\system32\sethc.exe c
```

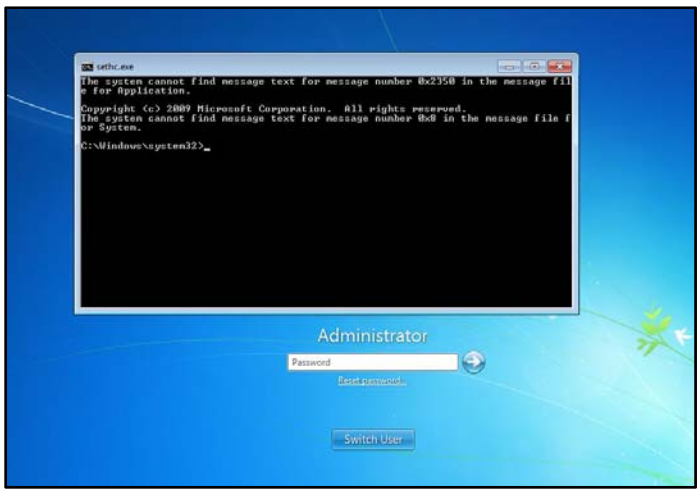


حالا فقط کافی است که فایل اجرایی cmd را کپی کنید. برای این کـار، از دسـتور زیـر استفاده نمایید:

```
Copy c:\windows\system32\cmd.exe
C:\windows\system32\sethc.exe
```

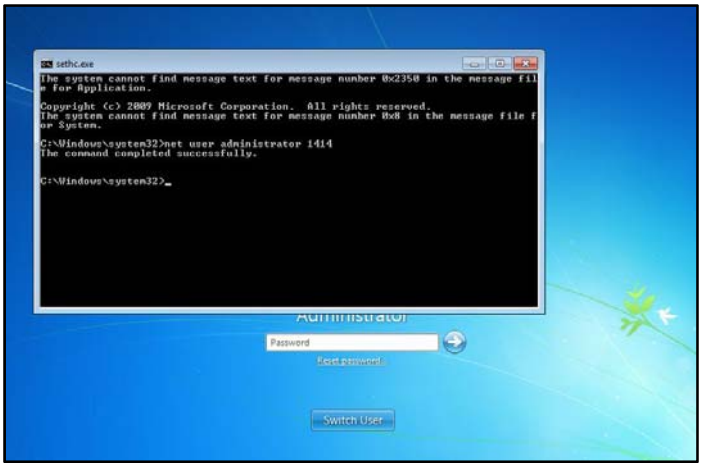


آن گاه، برنامه cmd را بسته، دکمه Restart را از پنجره جاری، انتخاب نموده و اجازه دهید تا به صورت عادی، ویندوز بارگذاری شود. هنگامی کـه صـفحه خـوش آمـد گـویی و درخواست کلمه عبور را مشاهده کردید، دکمـه Shift صـفحه کلیـد را ۵ مرتبـه بفشـارید تـا پنجره command prompt در حالت مدیر سیستم، نمایش داده شود.



هم اکنون، زمان تغییر کلمه عبور ویندوز است. بنابراین، دستور زیر را تایپ کنید:

net user administrator NewPassword



توجه داشته باشید که به جای کلمه administrator، باید نام کاربری ویندوز و به جای NewPassword، رمز عبور جدیدی که می خواهید جایگزین پسورد فعلی شما شود را تایپ نمایید.

سپس برنامه cmd را بسته و با کلمه عبور جدیدی که داده اید، وارد ویندوز شوید. به همین راحتی!

در آخر هم باید فایل اصلی sethc.exe را که از آن نسخه پشتیبان گرفته اید، جایگزین فایل فعلی نمایید. برای انجام این کار، دوباره سیستم را از روی DVD ویندوز راه اندازی کرده و زمانی که بعد از قسمت Repair your computer پنجره cmd نمایش داده شد، دستور زیر را برای جایگزینی آن تایپ کنید:

```
Copy :\sethc.exe c:\windows\system32\sethc.exe
```

در نهایت، برای اعمال تغییرات، لازم است که سیستم دوباره راه اندازی شود.

٦

نحوه گذشتن از پسورد بایوس[1]

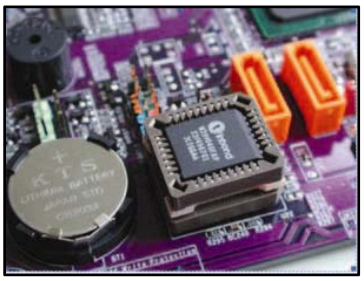
بایوس در سال ۱۹۸۷ به عنوان یک تکنولوژی و استاندارد برای کامپیوترهای شخصی IBM معرفی شد و این تکنولوژی برخلاف دیگر تکنولوژی های جدید و به روز شده، کماکان بدون هیچ تغییری هم چنان مورد استفاده قرار می گیرد.

مقدمه

شاید اولین باری که واژه بایوس مورد استفاده قرار گرفت و به عنوان یک تکنولوژی مطرح شد، زمانی بود که سیستم عامل CP/M توسط Gray Kildall نوشته شد. Kildall به همراه همسرش Dorothy McEwen بعد از تأسیس شرکت Intergalactic Digital Research که بعدها Digital Research Inc نامگذاری شد، توانستند این سیستم عامل را بر روی میکرو کامپیوتر IMSAI 8080 که مدل شبیه سازی شده از میکرو کامپیوتر Altair 8800 بود، پیاده سازی کنند که جهش بزرگی برای این شرکت محسوب شد. به مرور زمان با خرید روز افزون این سیستم عامل توسط شرکت های معروف، اجبار برای پشتیبانی از سخت افزارهای متعدد به وجود آمد که در این بین Kildall پیشگام ارایه مفاهیم بایوس شد.

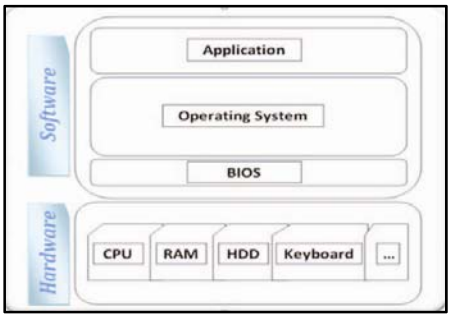
[1] Basic Input/Output System (BIOS)

با ارایه این تکنولوژی که هنوز زمان زیادی برای فراگیر شدن آن مانده بود، Kildall توانست با ذخیره مجموعه ای از روتین ها درون حافظه فقط خواندنی[1]، قابیلت اجرا در سامانه های مختلف، بدون اعمال تغییرات را به CP/M دهد.



Altair 8800 whit 8 inch floppy disk system

بایوس چیست؟



یک سیستم کامپیوتری، از دو بخش کلی زیر تشکیل شده است:

۱. سخت افزار؛ که شامل اجزای فیزیکی سیستم می شود.
۲. نرم افزار؛ که قابلیت استفاده از سخت افزار را فراهم می آورد و شامل سه نوع می باشد:
   - برنامه های کاربردی؛ که بالاترین سطح در لایه نرم افزار است.

[1] Read Only Memory (ROM)

- سیستم عامل؛ که وظیفه مدیریت منابع سیستم را برعهده دارد.
- بایوس؛

نوع سوم که در پایین ترین سطح از این لایه قرار دارد و مشتمل بر مجموعه ای از دستورالعمل ها است، به عنوان واسط بین سخت افزار و سطوح بالاتر نرم افزاری مطرح می شود.

وقتی سیستم روشن شد، ریزپردازنده اقدام به اجرای اولین دستورالعمل می کند که این دستورالعمل را باید از جایی به دست آورد. امکان ارایه دستورالعمل، قابل اجرا از سوی سیستم عامل نیست چون روی هارد دیسک بوده و هنوز بارگذاری نشده است. ریزپردازنده نیز بدون اینکه دستورالعملی به او بگوید که چطور با قطعات کار کند، توانایی برقراری ارتباط با آن ها را ندارد. پس نیاز به بخشی است تا این وظیفه را برعهده بگیرد، که بایوس به عنوان مسئول راه انداز سیستم، نخستین نرم افزاری است که بعد از روشن شدن سیستم به اجرا درمی آید.

بایوس، درون ROM یا روی یک چیپ از نوع حافظه فلش قرار گرفته است. همچنین تمام اطلاعات از قبیل تاریخ، ساعت و تنظیمات اولیه آن بر روی یک حافظه غیر فرّار به نام CMOS ذخیره می شود. وظیفه اصلی و می توان گفت مهمترین وظیفه بایوس، بارگذاری سیستم عامل است که این کار، نیازمند طی شدن یک سری مراحل و روال هاست و بدون آن ها، عمل بارگذاری سیستم عامل با شکست روبرو می شود.

مراحل بارگذاری سیستم عامل توسط بایوس:

- بررسی تنظیمات CMOS؛
- بارگذاری وقفه ها و درایور قطعات؛
- آماده سازی ثبات ها و مدیریت برق رسانی؛

- انجام عملیات POST [1]؛

عملیات POST سه وظیفه دارد:

۱. بررسی وضعیت و اطمینان از این که تمام قطعات سخت افزاری به درستی کار می کند.
۲. فعال سازی دیگر چیپ های بایوس بر روی برخی قطعات سخت افزاری (برای مثال، SCSI و کارت های گرافیک اغلب بایوس مخصوص به خود را دارند).
۳. فراهم سازی یک سری وقفه ها و روتین های سطح پایین، تا به وسیله آن ها سیستم عامل توانایی برقراری ارتباط و تعامل با قطعات سخت افزاری مختلف را داشته باشد. این روتین های واسط، توانایی برقراری ارتباط با برخی قطعات همچون صفحه کلید (INT 16h)، صفحه نمایش، پورت های سری و موازی، مخصوصاً زمان بوت شدن کامپیوتر را دارا می باشند.

در آخر، بایوس با استفاده از وقفه INT 19h پایان عملیات POST را اعلام کرده و به انجام مراحل بعدی می پردازد.

قبل از شروع عملیات POST، بایوس بررسی می کند که آیا سیستم راه اندازی مجدد [2] شده یا این که هم اکنون روشن شده [3] است. تشخیص این وضعیت، تنها با خواندن مقدار از آدرس 0472:0000 صورت می گیرد. اگر مقدار خوانده شده برابر با 1234h بود، بایوس متوجه می شود که سیستم راه اندازی مجدد شده، بنابراین از عملیات POST صرف نظر می کند. همچنین اگر هر مقداری به جز این مقدار خوانده شود، به منزله روشن شدن سیستم است و عملیات POST به صورت بالا انجام می گیرد.

- نمایش تنظیمات و اطلاعات سیستم (INT 11h)؛
- چه مقدار حافظه اصلی روی سیستم نصب است (INT 12h)؛

---

[1] Power-On Self-Test (POST)
[2] Reboot
[3] Cold Boot

- دیسک سخت و CD/DVD درایوها از چه نوعی هستند؛
- نوع پردازنده و سرعت آن؛
- نسخه بایوس نصب شده و تاریخ آخرین به روز رسانی آن؛
- بررسی ترتیب راه اندازی[1]؛

در پایان، بایوس به بررسی ترتیب مشخص شده تجهیزات ذخیره سازی برای راه اندازی می پردازد تا سیستم عامل را بارگذاری کند. این ترتیب در پیکربندی بایوس به عناوین First Boot Device, Second Boot Device و ... مشخص شده است.

اگر اولین دستگاه مشخص شده، بدون هیچ مشکلی راه اندازی شد و بایوس توانست سیستم عامل را بارگذاری و کنترل سیستم را به آن واگذار کند، دستگاه های دیگر بررسی نمی شوند ولی اگر به مشکلی اعم از سخت افزاری یا نرم افزاری برخورد کرد، اقدام به بارگذاری سیستم عامل از روی رسانه بعدی به همان ترتیب مشخص شده در پیکربندی بایوس می کند و باز به همین صورت این عمل تکرار می شود تا بتواند سیستم عامل را بارگذاری نماید.

در صورتی که بایوس نتواند هیچ رسانه قابل راه انداز که از طریق آن سیستم عامل بارگذاری شود را پیدا کند، با ارسال وقفه INT 18h پایان ناموفق بارگذاری سیستم عامل[2] را اعلام می کند.

پسورد بایوس و نحوه گذشتن از آن

حال، با وجود همه توضیحاتی که داده شد، به ۳ روش زیر می توانیم از رمزهای عبور بایوس ها عبور کنیم:

---

[1] Boot Sequence
[2] Boot Failure

روش اول: امروزه چون حدود ۹۹٪ بایوس ها ساخت شرکت AWARD هستند، می توانیم از shift+AWARD_SW به جای رمز عبور استفاده کنیم. همچنین کلمات عبور زیر را نیز می توان به کار برد:

AWARD SW, AWARD_SW, Award SW, AWARD PW, _award, awkward, J64, j256, j262, j332, j322, 01322222, 589589, 589721, 595595, 598598, HLT, SER, SKY_FOX, aLLy, aLLY, Condo, CONCAT, TTPTHA, aPAf, HLT, KDD, ZBAAACA, ZAAADA, ZJAAADC, djonet

اگر بایوس، ساخت شرکت AMI باشد، از کلمات عبور زیر استفاده می کنیم:

AMI, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD, HEWITT RAND, Oder

از پسورد های زیر هم می توان برای بایوس های ساخته شده توسط شرکت های مختلف استفاده کرد:

LKWPETER, lkwpeter, BIOSTAR, biostar, BIOSSTAR, biosstar, ALFAROME, Syxz, Wodj

البته باید توجه داشته باشیم که هنگام وارد کردن رمزهای عبور، حروف بزرگ را به صورت بزرگ و حروف کوچک را به شکل کوچک وارد نماییم.

روش دوم: پاک کردن رمز عبور بایوس

ابتدا DEBUG را در Run اجرا کرده و اگر بایوس، ساخت شرکت AWARD یا AMI بود، عبارت های زیر را در آن تایپ می کنیم:

O 70 17

O 71 17

Q

و اگر بایوس، ساخت شرکت PHOENIX باشد، از عبارت های زیر استفاده می شود:

O 70 FF

O 71 17

Q

عبارت های زیر نیز، برای بایوس های ساخته شده توسط شرکت های عمومی و غیر معتبر به کار می رود:

O 70 2E

O 71 FF

Q

توجه کنید که حرف اول، کاراکتر O است و نه عدد صفر.

روش سوم: سخت افزاری

شما می توانید با برداشتن و گذاشتن باطری مادربرد سیستم، رمز بایوس را پاک کنید.

۷

امنیت بانکداری همراه

با گسترش روز افزون فناوری های نوین بانکی و ارایه خدمات بیشتری مبتنی بر بانکداری الکترونیک توسط بانک های عضو شبکه شتاب کشورمان، هر روز به تعداد افرادی که از این خدمات بانکی جدید توسط تلفن همراه خود بهره می برند، افزوده می شود. پدیده نوظهور بانکداری همراه که حاصل رشد این تکنولوژی است، به ارایه خدمات بانکی غیرحضوری از طریق سامانه های تلفن همراه گفته می شود.

همزمان با پیشرفت این فناوری به خاطر خدمات ۲۴ ساعته شبانه روزی و ۷ روز هفته آن بدون مراجعه به شعبه یا واحد بانکی و همچنین استقبال گسترده مردم برای پرهیز از اتلاف وقت در صف های طولانی که گاهی اوقات به چند ساعت هم می رسد، فراهم کردن امنیت آن نیز به علت حملات گسترده، از اهمیت ویژه ای برخوردار است.

مطابق با ماده ۴ آیین نظام بانکداری الکترونیکی کشورمان که توسط هیأت وزیران در جلسه مورخ ۱۳۸۶/۱۲/۲۲ به تصویب رسید، بانک مرکزی موظف است با همکاری وزارت ارتباطات و فناوری اطلاعات، تمهیدات لازم را در جهت تأمین امنیت بانکداری الکترونیکی فراهم آورد. مسئولیت برقراری امنیت بانکداری الکترونیکی هم بر اساس استانداردهای بین المللی بر عهده بانک مرکزی است که این امر نافی مسئولیت بانک ها در خصوص برقراری امنیت بانکداری الکترونیک نبوده و تبعات ناشی از آن برعهده بانک ها می باشد.

امروزه حمله به شبکه های بانکی چنان رشد فزاینده ای دارد که با وجود تمام تلاش هایی که متخصصان امنیت برای جلوگیری از نفوذ به شبکه های بانکی و جعل اسناد و هویت اشخاص می کنند، اما هنوز هم به نظر می رسد مردم بیشتر از گذشته در معرض خطر ترفندهای طراحی شده هستند تا آن ها را از پول و اطلاعات شخصی شان جدا کند. متأسفانه آماری که از سوی مراکز دادگستری کشورهای مختلف جهان در سال گذشته میلادی منتشر

شده است، نشان می دهد که بیشترین کلاهبرداری های ۲۰۱۰، همه یا بخشی از آن ها بر روی اینترنت رخ داده است.

اگرچه در ماده ۱۶ آیین نظام بانکداری الکترونیکی، وزارت امور اقتصادی و دارایی مکلف شده است تا سقف یک درصد بودجه فناوری اطلاعات هر بانک را جهت جبران هزینه های نفوذ غیرمجاز به اطلاعات حساب های مشتریان تأمین نموده و از ضرر و زیان ناشی از استفاده خدمات بانکی الکترونیکی پیشگیری نماید ولی بهترین راه برای جلوگیری از قربانی شدن توسط کلاهبردارهای آنلاین، این است که کاربران در فضای مجازی بسیار مراقب بوده و به هر کسی اعتماد نکنند. در زیر به پنج روش برای حفاظت از حمله به حساب های بانکی و اطلاعات خصوصی شما اشاره می شود:

پیش پرداخت زودهنگام:

همه کلاهبرداری های اخیر در یک چیز مشترکند و آن هم درخواست کلاهبردار از شما برای پرداخت هزینه های کوچک در جهت پیشبرد طرحی مشخص و وعده پول بیشتری بعد از سرمایه گذاری است. این درخواست های جعلی پیشرفت اغلب عبارتند از درخواست سرمایه اندک برای اخذ وام، سرمایه گذاری برای کار در خانه، هزینه مصاحبه برای شغل جدید یا ودیعه شرکت در مراسم قرعه کشی که در صورت برنده شدن پول بسیار زیاد یا جایزه های ارزشمند دیگری به شما تعلق می گیرد.

پرداخت آنلاین با کارت های اعتباری:

هدف کلاهبردارها در پرداخت آنلاین توسط کارت های اعتباری، دسترسی به شماره حساب های بانکی شما همراه با رمز آن ها است. هرچند که پرداخت ها و خریدهای انجام شده با کارت اعتباری در بیشتر کشورهای جهان توسط قانون انتقال الکترونیکی وجوه

محافظت می شوند و پس از صدور صورتحساب بانکی در دوره های زمانی مشخص و ارسال آن به صاحب حساب و اخذ تأییدیه مربوطه، از حساب کاربر کسر می شود، اما با توجه به اینکه این قانون در ایران وجود ندارد، همچنان شما باید از پرداخت های غیرمجاز یا نامشروع از حساب تان جلوگیری کنید.

وظیفه شما برقراری ارتباط امن با سایت های بانکداری آنلاین و رعایت تمامی نکات امنیتی هنگام استفاده از خدمات بانکداری همراه برای جلوگیری از انتقال غیرمجاز اطلاعات در طول تراکنش است.

تغییر در اطلاعات شخصی:

یک روش که در چند سال اخیر کلاهبردارها بهره زیادی از آن برده اند، ایجاد نام سایت های بسیار مشابه با سایت بانک ها است. آن ها معمولاً پس از راه اندازی این سایت های دروغین و طراحی صفحاتی که بسیار مشابه با بانک اصلی است، یک نامه الکترونیک یا پیام کوتاه را با عنوان بالاترین مسئول بانک، به صورت عمومی منتشر کرده و از صاحبان حساب ها می خواهند که مثلاً به دلیل تغییرات امنیتی در سیستم بانک مورد نظر، تا ظرف چند روز آینده، رمز کارت های خود را تغییر دهند.

در این روش از صاحبان حساب ها خواسته می شود که به سایت اینترنتی جعلی مراجعه نموده و هنگام ورود به سایت، از آن ها شماره حساب، رمز قدیم و تغییر آن به رمز جدید خواسته می شود. همان طور که اشاره شد، هدف از این روش، فریب مردم به ارسال شماره حساب های بانکی همراه با رمز آن ها و در مواردی خاص نیز به دست آوردن سایر اطلاعات حساس شخصی است.

توصیه می شود در صورت مشاهده چنین پیام هایی، قبل از تغییر مشخصات و اطلاعات خود، حتماً بررسی های لازم را با مراجعه حضوری و یا تلفنی به نزدیکترین شعبات بانک یا

شعبه افتتاح کننده حساب، به عمل آورده و مسئولین شعبات بانکی را نیز در جریان موضوع قرار دهید.

نمایش اطلاعات حساب بانکی در شبکه های اجتماعی:

چرا شما باید اطلاعات حساب بانکی خود را در شبکه های اجتماعی همچون فیس بوک قرار دهید؟ مگر نمی دانید که شاید هزاران نفر هر روز این صفحات شخصی شما را مشاهده می کنند؟ پس لطفاً اطلاعات شخصی خود را تسلیم کلاهبردارها نکنید.

بسیاری از کلاهبردارها در شبکه های اجتماعی رخنه کرده اند و با متقاعد کردن شما به منظور تکمیل یک فرم یا ثبت نام در یک اشتراک مجازی جدید، تلاش می کنند تا شماره حساب، تلفن شما و یا دوستانتان را به دست آورده و برای اهداف شوم خود و کسب اطلاعات بیشتر، از آن ها بهره ببرند.

هرگز فراموش نکنید که سهل انگاری در شبکه های اجتماعی، آسیب های جدی به حریم خصوصی شما، خانواده و حتی دوستانتان وارد خواهد کرد.

خرید از کسی که نمی شناسید:

این روزها همه کلاهبردارها بر روی اینترنت تمرکز نموده اند. همان طور که قبلاً هم گفته شد، تا زمانی که اطمینان لازم را کسب ننموده اید، از خریدهای اینترنتی در سایت های غیرمعتبر جدداً خودداری کنید چرا که در اثر بی توجهی در هنگام خرید آنلاین، به راحتی شماره حساب و رمزتان در اختیار کلاهبردارها قرار می گیرد.

در پرداخت وجوه آنلاین به مؤسسات خیریه نیز کماکان باید مسایل امنیتی را رعایت نموده و اطمینان لازم را با مشاهده و پیگیری شماره ثبت و مرکز ثبت کننده آن به دست آورید.

بهترین شیوه های امنیتی آنلاین:

همواره بکوشید تا از حریم خصوصی خود در فضای مجازی هر چه بیشتر محافظت کنید. یادتان باشد که هر روز گزارش های تازه ای از کلاهبرداری های آنلاین توسط پلیس و مراکز دادگستری منتشر می شود.

۸

امنیت پیامک های تلفن همراه

امروزه با توجه به موج جدیدی از حملات و تهدیدات امنیتی به سیستم ها و شبکه های مخابراتی، ایمن سازی این سیستم های ارتباطی در برابر دسترسی های نامجاز، امری ضروری و اجتناب ناپذیر به شمار می رود.

یکی از مهمترین مباحثی که در روزهای اخیر، بسیار مورد توجه متخصصان و کارشناسان امنیتی سازمان های مخابراتی بزرگ جهان قرار گرفته است، لزوم استفاده کاربران تلفن همراه از سیستمی امنیتی برای ارسال و دریافت پیامک های تلفنی می باشد. این سیستم که بر مبنای کدگذاری پیامک ها بنا شده، امکان ارسال و دریافت پیامک های محرمانه را برای کاربران فراهم می کند.

در حالت عادی، هنگامی که پیامکی توسط تلفن همراه و یا اینترنت فرستاده می شود، متن پیامک برای مسئولین مخابرات، سرویس دهندگان، هکر[1]ها و نفوذگران قابل ملاحظه می باشد. بنابراین، هیچگونه امنیتی برای حفظ محرمانگی پیامک وجود ندارد. اما با استفاده از این سیستم، متن پیامک به صورت رمز شده و غیر قابل فهم درآمده و صرفاً پیامک، برای ارسال کننده و دریافت کننده اصلی قابل رمزگشایی و ملاحظه است.

عملکرد این سیستم بدین صورت است که برای حفظ محرمانگی پیامک، نرم افزار رمز گذارنده[2] بر روی سیستم ارسال کننده پیامک، اعم از دستگاه تلفن همراه و وب سایت ارسال کننده نصب گردیده و پیامک ها، قبل از ارسال کاملاً رمزگذاری می شود. همچنین در سیستم دریافت کننده پیامک نیز نرم افزار رمزگشا[3] نصب می گردد و توسط این برنامه، متن پیامک های دریافتی، رمزگشایی شده و برای دریافت کننده اصلی قابل مشاهده خواهد بود. بدین ترتیب، در صورتی که پیامک، در دسترس افراد غیر مجاز قرار بگیرد، به دلیل استفاده از الگوریتم رمزنگاری چند لایه و بسیار قوی، متن پیامک برای وی قابل ملاحظه نخواهد بود.

از مهمترین موارد کاربرد این سیستم، می توان مراکز اطلاعاتی و امنیتی، مراکز نظامی و انتظامی، بانک ها و تمامی مراکز و اشخاصی که خواهان ارسال پیامک محرمانه هستند را برشمرد.

---

[1] هکر یعنی کسی که به بیشتر زبان های برنامه نویسی مسلط بوده، به سیستم ها و شبکه ها برای شناسایی نقطه های ضعف و آسیب پذیریشان بدون اجازه و بدون هیچ گونه خرابکاری وارد و خارج می شود و آن ضعف ها را می پوشاند و یا از طریق مهندسی معکوس، ضعف سیستم ها و نرم افزارهای مذکور را شناسایی و با تلاش خود سعی در رفع آن نواقص می کند.

[2] Coder
[3] Decoder

۹

امنیت سیستم عامل های تلفن همراه

هنگامی که صحبت از امنیت تلفن همراه می شود، بسیاری از مردم تصور می کنند که منظور از امنیت، همان امنیت فیزیکی گوشی و گذاشتن رمزهای پیچیده یا قفل کردن دستگاه پس از مکالمه است. اگرچه این موضوع هم از اهمیت ویژه ای برخوردار است اما تنها بخش کوچکی از امنیت تلفن همراه را شامل می شود و بخش مهمتر، مربوط به پلت فرم آن است.

هم اکنون سه پلت فرم آندروید گوگل، ویندوز فون ۷ و iOS اپل[1] از مهمترین پلت فرم های تلفن همراه به شمار می روند که هر کدام با مشکلات امنیتی خاصی روبرو هستند. اگرچه نگرانی های امنیتی که کارشناسان امنیت دارند، عمدتاً نظری بوده و تهدیدها نیز جزء جدایی ناپذیر هر سیستم عامل به شمار می رود ولی شناخت این تهدیدات، آگاهی ما را در مواجه با خطرات بیشتر می سازد. در زیر، اشاره ای به مشکلات امنیتی این سه پلت فرم مشهور می شود:

آندروید گوگل

این روزها گرایش به سیستم عامل آندروید هر لحظه در حال افزایش است، اما مشکلات امنیتی آن باعث نگرانی و هشدار کارشناسان شده است. کارشناسان امنیتی اعتقاد دارند به علت متن باز بودن آندروید که اجازه دسترسی به معماری و اصول اولیه طراحی آن را می دهد، از سایر سیستم عامل ها در برابر حملات هکرها و ویروس نویسان آسیب پذیرتر است. اگرچه گوگل هدف از متن باز بودن آندروید را ارایه برنامه های کاربردی بیشتر برای تلفن

[1] Apple

همراه می داند، اما این قابلیت، تولید برنامه های مخرب فراوان را نیز برای آن در پی داشته است.

تا مدتی پیش، دو آسیب پذیری مهم در سیستم عامل آندروید وجود داشت که مهاجمان را قادر به دور زدن تأییدیه کاربر برای نصب برنامه های مخرب روی گوشی می نمود. یکی از این آسیب پذیری ها به این صورت عمل می کرد که توسط یک افزونه ساختگی برای بازی معروف Angry Birds و با فریب کاربر به مراحل اضافی و دریافت جایزه بازی، به صورت مخفیانه سه برنامه مخرب که امکان پرداخت آنلاین جعلی، سرقت اطلاعات مخاطبین از دفترچه تلفن همراه و ردگیری مکان کاربر را داشت، بر روی گوشی نصب می کرد. مدتی پس از انتشار خبر جنجالی این آسیب پذیری، گوگل توانست با انتشار وصله ای، آن را رفع نموده و از حملاتی که به فضای کاربری گوشی های هوشمند آندرویدی می شود، جلوگیری نماید.

گوگل که در حال سرمایه گذاری عظیم و حضور قدرتمندانه در بازار سیستم عامل گوشی همراه است، با رونمایی از آخرین نسخه آندروید با عنوان Android 3.0 Honeycomb در نمایشگاه CES امسال، یک جنگ رسانه ای را در خصوص پایان دادن به مشکلات امنیتی سیستم عامل خود برپا کرده است.

گوگل که آندروید را با اندیشه فتح دنیای گوشی های همراه هوشمند و لوح-رایانه ها عرضه نموده، تلاش کرده است تا در این نسخه، علاوه بر ارتقاء بهتر رابط کاربری سیستم عامل و همچنین رفع برخی از مهمترین مشکلات امنیتی آن، با ایجاد ابزارک هایی برای امکانات مورد نیاز کاربران بر روی نمایشگر، همچون تسریع دسترسی به سرویس های جیمیل، نقشه، تقویم، چند سایت پرطرفدار اینترنتی و نسخه به روز شده مرورگر کروم خود، توجه کاربران را بیشتر جلب نماید. این غول جستجوگر اینترنتی با اعطای جوایز بسیار ارزشمند برای کشف و گزارش حفره های امنیتی سیستم عامل خود، به شدت در تلاش است تا اعتماد کاربران را همچنان حفظ کند.

iOS اپل

در این میان سیستم عامل iOS اپل نیز به دلیل استفاده در تلفن های لوکس هوشمند، هر روز مورد هجوم گسترده تری قرار می گیرد؛ ویروس هایی که اختصاص به iOS داشته و سعی دارند تا خودشان را به صورت های مختلف، تکرار کرده یا با تجزیه نمودن و دوباره نویسی خود، در نبرد با ضد ویروس ها پیروز شوند.

اپل در سیستم عامل تلفن همراه هوشمند آیفون[1] خود می کوشد تا امنیت را با کنترل امضای امنیتی برنامه ها برقرار نموده و از نصب برنامه های کاربردی غیر مجاز یا مخرب بر روی گوشی جلوگیری کند. اپل نکات امنیتی را هم در iOS دقیق تر از آندروید رعایت می نماید، در نتیجه ویروس ها نمی توانند به راحتی در این سیستم عامل نفوذ کنند.

ویندوز فون ۷ مایکروسافت

ویندوز فون ۷ که آخرین نسخه سیستم عامل مایکروسافت در دنیای تلفن های همراه هوشمند به شمار می آید هم نتوانسته از حملات هکرها در امان بماند و با انتشار نرم افزارهای مخرب ویندوزی که به تعامل با کاربر نیاز داشته و بیشتر آن ها نیز توسط روش هوشمندانه مهندسی اجتماعی تولید می شوند، از سایر سیستم عامل ها در معرض خطر بیشتری قرار دارد.

گوشی های مبتنی بر ویندوز فون ۷، تمرکز بیشتری روی بازی، عکس، شبکه های اجتماعی همچون فیس بوک و نرم افزارهایی با کاربردهای چند منظوره برای دسترسی به اخبار آب و هوا، تنظیم جلسات، نرم افزارهای Office و Exchange دارد. مایکروسافت نیز همچون اپل می کوشد تا با کنترل امضای امنیتی خاص هر برنامه، علاوه بر این که از استفاده رایگان و غیرمجاز برنامه ها جلوگیری کند، مانع نصب برنامه های مخرب هم شود.

---

[1] iPhone

حال با توجه به مواردی که مطرح شد، توصیه ای که ما به کاربران تلفن همراه داریم این است که تنها برنامه های کاربردی را روی گوشی خود نصب کنند که به شرکت تولیدکننده آن نرم افزار اعتماد کامل دارند. همچنین پیشنهاد می کنیم که برای حفاظت از اطلاعات شخصی خودتان، همواره از ضد ویروسی که شما را در برابر حملات و نرم افزارهای مخرب محافظت نموده و قابلیت فیلتر کردن پیام های متنی آلوده را دارد، استفاده نمایید.

۱۰

امنیت همراه در شبکه های اجتماعی

ظهور فناوری های نوین ارتباطی و استقبال شگفت انگیز مردم از گوشی های تلفن همراه که از کارکرد سنتی خویش خارج شده و در اتصال به شبکه های اجتماعی آنلاین تمرکز نموده اند، موج جدیدی از تولید دستگاه های گوشی هوشمند را به همراه داشته است. در این میان، امنیت کاربران به علت هویت و ارتباطات مجازی افراد در شبکه های اجتماعی، به نوبه خود حایز اهمیت بسیار زیادی می باشد که باید به صورت فراملی مورد توجه قرار گیرد.

امروزه دسترسی به شبکه های اجتماعی مجازی از طریق تلفن همراه، الویت مهم کاربران در انتخاب دستگاه گوشی به شمار می رود. به همین منظور، شرکت های بزرگی همچون مایکروسافت و گوگل هم تلاش کرده اند تا در سیستم عامل جدید تلفن همراه خود، به این خواسته کاربران تحقق بخشند.

در نخستین گام، سال گذشته میلادی مایکروسافت اقدام به ساخت گوشی های هوشمند Kin کرد که تمرکز ویژه ای روی شبکه های اجتماعی داشتند. مایکروسافت برای تبلیغات و عرضه این گوشی ها که فقط ۶ هفته در بازار موجود بودند، یک میلیارد دلار هزینه کرد. سپس این شرکت در ویندوز فون ۷، سیستم عامل جدید تلفن همراه خود با مورد توجه قرار دادن دسترسی سریع به شبکه های اجتماعی و سازماندهی تماس‌ها، تغییر پلت فرم کاملی نسبت به نسخه قبلی ویندوز موبایل داد. استیو بالمر، مدیر اجرایی مایکروسافت، در نمایشگاه کنگره جهانی تلفن همراه بارسلون، با توصیف ویندوز فون ۷ به عنوان نرم‌افزاری متفاوت، آن را نقطه آغازی برای تلفن‌هایی دانست که بازتاب سرعت زندگی مردم و نیاز آن‌ها برای ارتباط با دیگران است.

در میان سیستم عامل های تلفن همراه، ویندوز فون ۷ و رابط کاربری آن با اختصاص بخش هایی تحت عنوان هاب[1]، بیشترین تمرکز را روی شبکه های اجتماعی و فعالیت های آنلاین دارد. این سیستم عامل دارای ۶ هاب با نام های مردم، تصاویر، موسیقی و ویدئو، بازار، آفیس و بازی است که فعالیت های متداول را شامل شده و هر هاب، همانند یک پوشه، موارد مرتبط به هم را ازمیان وب، برنامه ها و سرویس ها در یک جا جمع می کند.

هاب مردم ویندوز فون ۷ را که امکان تعامل با افراد موجود در فهرست تماس‌های کاربر و همچنین دریافت به روزرسانی‌های مستمر از دوستان فیس‌بوک و توییتر را فراهم می‌کند، می توان مرکز ارتباطات نامید و جایی است که کاربران می توانند تمامی موارد مربوط به یک تماس را هر لحظه از شبکه های اجتماعی مشاهده کنند.

هاب تصاویر هم، تمامی عکس ها را از داخل گوشی و آلبوم های آنلاین در یک جا گرد آورده و اشتراک گذاری آن ها در شبکه های اجتماعی نظیر فیس بوک و ویندوز لایو و همچنین مشاهده آلبوم های به روز شده دیگران که آن ها را به اشتراک گذاشته اند، به سادگی امکان پذیر می کند. در این هاب، پس از به روزرسانی عکس های دوستان در شبکه های اجتماعی، یک نمای "Live tile" بر روی صفحه نمایش گوشی ظاهر می شود که آخرین عکس ها را نشان می دهد.

از آن جا که مایکروسافت در فیس بوک[2] سهم دارد، در پلت فرم جدید تلفن همراه خود توجه ویژه ای به این بزرگ ترین و پرعضوترین وب سایت جهان نموده است. لازم به ذکر است که فیس بوک از مهمترین شبکه های اجتماعی دنیا با ۵۰۰ میلیون کاربر، یعنی حدود ۱ نفر از هر ۱۳ نفر روی کره زمین است که از حضور مستمر کاربران تلفن همراه نیز برخوردار می باشد. نیمی از اعضای فیس بوک، به صورت روزانه وارد این سایت شده و ۴۸ درصد نیز که سنی بین ۱۸ تا ۳۴ سال دارند، به محض بیدار شدن از خواب، صفحات شخصی خود در فیس بوک را توسط گوشی های هوشمندشان چک می کنند.

---

[1] Hub
[2] Facebook

در گوشی های لوکس مبتنی بر ویندوز فون ۷، خبرهای فیس بوک در نمای " Live tile" بر روی صفحه نمایش تلفن همراه ظاهر می شود که با اشاره روی هر تماس، می توانید برای آن فرد، پیام گذاشته و یا به او زنگ بزنید. هرچند که مایکروسافت با نوآوری های خلاقانه ای که انجام داده، معتقد است کاربران فیس بوک، عاشق گوشی های ویندوز فون ۷ خواهند شد ولی قول ارایه برنامه اختصاصی بهتری را هم به معتادان این شبکه اجتماعی داده است.

گوگل نیز اگرچه در زمینه پشتیبانی از شبکه های اجتماعی آنلاین به پای مایکروسافت نمی رسد ولی در آخرین نسخه سیستم عامل تلفن همراه خود تلاش کرده تا کاربران آندروید را با اتصال به وب سایت یوتیوب، با دنیای مجازی پیوند دهد. متأسفانه iOS شرکت اپل که از پلت فرم های خوب تلفن همراه به شمار می رود، با وجود نصب در گوشی های گران قیمت آیفون، از قابلیت پشتیبانی از شبکه های اجتماعی برخوردار نمی باشد.

حال پس از تمامی این توضیحات، بهتر است نگاهی هم به مهمترین تهدیداتی که این شبکه های اجتماعی مجازی برای کاربرانشان دارند، بیندازیم:

اشتراک مجازی جدید:

مهمترین خطری که همیشه در شبکه های اجتماعی شما را تهدید می کند، کوشش برای متقاعد کردن شما به منظور تکمیل یک فرم اینترنتی یا ثبت نام در یک اشتراک مجازی جدید با فریب به دست آوردن امتیازات خاص است. این کار که با هدف دسترسی به شماره حساب، تلفن، پست الکترونیک و رمز عبور آن، مشخصات شما، خانواده و یا دوستانتان صورت می گیرد، می تواند اطلاعات حساس شما را در اختیار کلاهبردارها قرار داده تا برای دستیابی به اهداف خود، از آن ها بهره ببرند.

فراموشی رمز عبور:

برای استفاده از خدمات شبکه های اجتماعی، شما باید ابتدا عضو آن شبکه شده و نام کاربری و رمز عبورتان را اعلام نمایید. در تمامی این سایت ها، گزینه ای به نام "فراموشی رمز عبور" در نظر گرفته شده که از آن برای بازیابی کلمه عبور حساب کاربری در مواقعی که اشخاص رمز عبور خود را فراموش می کنند، استفاده می شود. این گزینه با طرح سؤالاتی که کاربر در هنگام ایجاد حساب کاربری پر کرده، تحت عنوان سؤالات امنیتی، مطمئن می شود که فرد پاسخ دهنده، همان کاربر ایجاد کننده حساب است و به او اجازه تغییر کلمه عبور را می دهد.

روش دیگری که کلاهبردارها از آن بهره های فراوانی می برند، استفاده از گزینه "فراموشی رمز عبور" حساب های کاربری است. کلاهبردارها با جستجوی افراد خاص و پس از بررسی علاقه مندی ها، زمینه های مطالعه و سایر اطلاعات مفیدی که در خصوص شخصیت آن فرد می توانند به دست آورند، و یا مهمتر از همه با طرح دوستی و سؤال از کاربر هنگام گفتگوهای اینترنتی، پاسخ سؤالات امنیتی را به دست آورده و اقدام به تغییر کلمه عبور حساب آن شخص می کنند. این مسئله تاکنون ده ها بار در سایت های اجتماعی به وقوع پیوسته و افراد بی شماری حساب های کاربری خود را راحت از دست داده اند.

مرا به خاطر بسپار:

کاربران معمولاً برای تنبلی و پرهیز از دوباره وارد کردن رمز عبور حساب کاربری خودشان، گزینه "مرا به خاطر بسپار" را در صفحه ورودی وب سایت شبکه های اجتماعی انتخاب می کنند که انجام این کار، باعث ذخیره شدن کلمه عبور شده و در ورودهای بعدی، شخص را از دوباره وارد نمودن رمز عبور بی نیاز می کند.

لازم است بدانید که این کلمات عبور، در کوکی های مرورگرها ذخیره شده و کلاهبردارها با دزدیدن این کوکی ها توسط حمله های XSS ، می توانند رمز عبور شما را به

دست آورند. پس هرگز این گزینه را به خصوص هنگامی که از کامپیوتر در مکان های عمومی همچون کافی نت ها استفاده می کنید، انتخاب نکرده و مطمئن باشید که نه وب سایت ها شما را فراموش می کنند و نه شما آن ها را از یاد خواهید برد!

اعلام رمز عبور:

اعضای شبکه های اجتماعی همواره با خطراتی همچون اعلام ناخودآگاه رمز عبور حساب کاربری توسط روش هوشمندانه مهندسی اجتماعی یا ترغیب به کلیک بر روی صفحات ورودی دروغینی که مشابه با سایت شبکه های اجتماعی طراحی شده اند، روبرو هستند. در این روش، کلاهبردارها یک نام بسیار مشابه با دامنه[1] وب سایت شبکه اجتماعی خاصی ثبت نموده و با طراحی صفحه ای همانند صفحه اصلی ورودی همان سایت، به روش های مختلف از کاربر می خواهند که وارد شبکه اجتماعی مورد نظر شود. هدف کلاهبردارها از انجام این فریب زیرکانه، یافتن نام کاربری و کلمه عبور افراد، جهت تحقق اهداف بعدی خودشان می باشد.

از آن جا که بیشتر مردم برای راحتی به خاطر سپاری، از یک رمز عبور در تمامی حساب های کاربری و حتی کارت های اعتباری بانکی خویش استفاده می کنند، کلاهبردارها پس از فهمیدن نام کاربری و کلمه عبور، از روشی که آن را "Google Hacking" می نامم، بهره برده و با جستجوی همان حساب کاربری یا پست الکترونیک در وب سایت های جستجوگر، سایر سایت هایی که فرد در آن ها عضویت دارد را یافته و از نام کاربری و رمز عبوری که قبلاً به دست آورده اند، برای ورود به آن سایت ها نیز استفاده می کنند.

کلاهبردارها معمولاً پس از وارد شدن به حساب کاربری افراد و به خصوص زنان، به تغییر عکس ها و ویدئوهای خیلی شخصی آن ها اقدام نموده و ضمن برقراری ارتباط با کاربر، وی را به منظور سوءاستفاده های جنسی یا مالی تهدید می نمایند. در صورتی هم که فرد به این

[1] Domain

موضوع توجهی نکنـد، تصـاویر و ویـدئوهای شخصـی او را در شـبکه هـای اجتمـاعی منتشـر خواهند کرد. همچنین کلاهبردارها ممکن است پس از دسترسی بـه اطلاعـات و عکـس هـای دوستانتان، با حساب کاربری شما برای آن ها پیام هایی بفرستند که شما هرگز به آن ها چنـین پیام هایی نخواهید فرستاد!

نصب برنامه های مخرب:

بیشتر مواقع، کلاهبردارها برنامه های مخربی را که عموماً تروجان هستند با عنوان نرم افزار یا فایل های جالبی که علاقه مندان زیادی دارند، در شبکه های اجتماعی منتشر می کنند. ایـن برنامه ها که معمولاً حجم کـم و نصـب بسـیار آسـانی دارنـد، مـی تواننـد اطلاعـاتی همچـون رمزهای عبور، حروف تایپ شده بر روی صفحه کلید و موارد مشابهی را تشـخیص داده و آن ها را به پست الکترونیک خاصی که قبلاً در برنامه مخرب مشخص شده، ارسال نمایند.

این تروجان ها، اغلـب همـراه فایـل هـای اسـکرین سـور، ویـدئویی یـا عکـس در اختیـار کاربران قرار گرفته که فرد پس از کلیک بر روی فایل اصـلی، همزمـان برنامـه مخـرب را نیـز اجرا می نماید.

رعایت حریم خصوصی:

از مهمترین چالش های پیش روی دست انـدرکاران شـبکه هـای اجتمـاعی و کارشناسـان امنیت فناوری اطلاعات، حفظ حریم شخصی کاربران در فضای مجازی است. هر چنـد وقـت یکبار، مدیران شبکه های اجتماعی به منظور سیاست های امنیتی بیشتر، در سرورها و صفحات سایتشان تغییراتی را اعمال نموده و با انتشار اطلاعیه ای از کاربران می خواهند که تنظـیم هـای حریم خصوصی خود را دوباره انجام داده و یا برنامه های خاصی که توسط کاربران آن شبکه استفاده می شود را به روز رسانی کنند.

متأسفانه بعضی از شبکه های اجتماعی، آن چنان تنظیم های حریم خصوصی را برای کاربران عادی دشوار نموده اند که آن ها نه به دلیل نخواستن، بلکه به خاطر ندانستن نحوه انجام آن، از خیر تنظیم های حریم شخصی خویش گذشته و در این خصوص اقدامی نمی کنند. در صفحه تنظیمات حریم خصوصی، معمولاً تعاریفی همچون مشخص نمودن کسانی که اجازه جستجو و پیدا کردن کاربر در شبکه اجتماعی، ارسال درخواست دوستی یا پیام برای او، مشاهده لیست دوستان وی و ... را دارند، وجود دارد. لازم است که کاربران، این سطح دسترسی ها را با دقت کامل نموده و حتی برای مواردی هم که به اشتراک می گذارند آن ها را اعمال نمایند.

مسدود کردن افراد مزاحم:

اگرچه شبکه های اجتماعی، پیدا کردن دوست و در تماس بودن با افرادی که دوستشان دارید را برای شما بسیار ساده نموده اند، اما این سایت های دوست یابی سریع، گاهی موجب آشنایی با افرادی می شود که هدفی جز آزار و اذیت شما نداشته و با ارسال مداوم پیام های مزاحمت، باعث رنجش خاطرتان می شوند.

در چنین مواقعی، می توانید فرد مزاحم را از درون همان وب سایت شبکه اجتماعی مسدود کرده و برقراری ارتباط را برای او دشوارتر نمایید. برای انجام این کار، به قسمت تنظیمات حریم خصوصی یا گزینه مشخص شده در پایین صفحه شخصی کاربری خودتان رفته و نام کاربری یا پست الکترونیک شخص مزاحم را از طریق لیست مسدودی های سایت، مسدود نمایید.

اگرچه فرد مزاحمی که شما آن را مسدود کرده اید، هیچ وقت از اقدام شما مطلع نمی شود ولی ممکن است پس از مسدود شدن، با ایجاد یک حساب کاربری جدید، باز هم اقدام به مزاحمت شما نماید که در این صورت یا باید از خیر آن حساب کاربری گذشته و کاربری جدیدی برای خودتان ایجاد کنید و یا دوباره حساب کاربری شخص مزاحم را مسدود نمایید!

حذف حساب کاربری:

این که چگونه به شیوه ای امن یک حساب کاربری را در شبکه های اجتماعی پاک کنیم، سؤالی است که ذهن بسیاری از افراد را به خود اختصاص داده است. گاهی اوقات، کاربران به دلایلی از یک حساب کاربری خسته شده و با ایجاد یک حساب کاربری جدید، می خواهند که حساب کاربری قبلی خود را غیر فعال نمایند.

در این مواقع، بهترین روش برای حذف یک حساب کاربری، استفاده از گزینه "مشاوره برای غیر فعال کردن حساب" در همان شبکه اجتماعی است. با استفاده از این روش، می توانید تمام مراحل پاک نمودن حساب خود را به شیوه ای مطمئن، دنبال نموده و از حذف کامل اطلاعات حساب خویش، علاقه مندی ها، عکس ها، به روز رسانی ها، پیام ها، برنامه ها، یادداشت ها، پیوندها، لینک دوستان، گروه ها، صفحات هواداری و ... مطمئن شوید.

پیشنهاد آخر:

هرگز فراموش نکنید که سهل انگاری در شبکه های اجتماعی، آسیب های جدی به حریم خصوصی شما، خانواده و حتی دوستانتان وارد خواهد کرد.

۱۱

امنیت مرورگرهای وب

مرورگرها، نرم افزارهایی هستند که برای گشت و گذار در اینترنت از آن ها استفاده می کنیم. امنیت مرورگرها و این که کدام مرورگر، امنیت بیشتری را به ارمغان می آورد و همچنین رعایت چه نکاتی از طرف کاربران در مرورگرها، باعث افزایش ضریب امنیتی سیستم می شود، از مهمترین موضوعات در انتخاب یک مرورگر وب به شمار می رود.

بهتر است بدانید که امروزه بالاترین درصد حملات و خطرات امنیتی که ممکن است متوجه یک کامپیوتر شود، از سوی اینترنت خواهد بود و در کنار آن، بیشترین نرم افزارهایی که با اینترنت در ارتباط هستند نیز مرورگرها هستند. بنابراین، نفوذگران و افرادی که قصد کلاهبرداری های اینترنتی و یا آسیب رساندن به سیستم را دارند، تمرکز خود را بر روی مرورگرها گذاشته اند. به همین دلیل، استفاده از مرورگری مناسب و امن، در کنار دقت و توجه به جزییات، راز امنیت مرورگر، سیستم عامل و مهمتر از همه، اطلاعات کاربران به حساب می آید.

انتخاب مرورگر امن

نخستین و مهمترین مسأله در رابطه با امنیت به هنگام وب گردی، این است که از چه مرورگری استفاده کنیم؟ اگر چه، هر کدام از مرورگرهای موجود، امکانات و قابلیت های خاصی را در اختیار کاربران قرار می دهند، اما نکته مهم برای بسیاری از افراد، فاکتورهای سرعت مناسب و قابلیت های کافی است که البته در کنار آن، باید امنیت را نیز مد نظر قرار داشت.

هر چند که همه مرورگرها در رابطه با این سه فاکتور، ضعف ها و قوت هـایی دارنـد، امـا مرورگرهای فایرفاکس[1]، گوگل کروم[2] و اُپرا[3] انتخاب هایی به مراتب بهتر از سایر مرورگرهـا به حساب می آیند.

قسمت های مختلف مرورگر و لزوم توجه به جزییات

همه مرورگرها ظاهری مشابه هم دارند که توجه بـه بعضـی از قسـمت هـای آن در هنگـام مرور صفحات وب، کمک زیادی به پیشگیری از بروز خطرات می کند.

در قسمت بالای مرورگر، یک بخش با نـام نـوار آدرس[4] وجـود دارد کـه در آن، آدرس اصلی صفحه ای که در حال بازدید است، قابل مشـاهده مـی باشـد. توجـه بـه نـوار آدرس، بـه خصـوص قبـل از پـر کـردن فیلـدهای صـفحات ورود[5] حسـاب هـای کـاربری اهمیـت دارد. همچنین، آگاهی از وضعیت امنیتی و رمز گذاری صفحات وب، توسط این نـوار امکـان پـذیر است.

در قسمت پایین مرورگر نیز نوار وضعیت[6] که از مهمترین قسمت های مرورگـر محسـوب می شود، قرار گرفته است. این نوار، اطلاعاتی از وضعیت مرورگر و لینک هـایی کـه کلیـک می شود را نمایش می دهد. بهتر است که قبل از کلیـک نمـودن بـر روی لینـک هـا، بـا بـردن نشانگر ماوس بر روی آن ها، از آدرس اصلی لینک که در ایـن قسـمت قابـل مشـاهده اسـت، آگاه شویم.

---

[1] Firefox
[2] Googel Chrome
[3] Opera
[4] Address Bar
[5] Login
[6] Status Bar

توجه به این نوارها، از اهمیت ویژه ای برخوردار است چرا که ممکن است در صورت سهل انگاری، کاربران را در معرض خطراتی همچون فیشینگ، کلیک جکینگ و ... قرار داده و باعث سرقت اطلاعات، کلاهبرداری و یا سوء استفاده از کاربران شود.

مسدود کردن اسکریپت ها و کدهای اجرایی در مرورگر

همه مرورگرها برای افزایش قابلیت هایشان وابسته به رابط های نرم افزاری مانند Flash، Active X، Java و Scripts (VBScript) هستند. اگرچه بسیاری از وب سایت ها برای نمایش صحیح، نیاز به اجرای این کدها دارند اما این تکنولوژی ها می توانند راه هایی برای دسترسی غیر مجاز یا اجرای کدهای مخرب از طریق حملات XSS باشند. بعضی مرورگرها با استفاده از افزونه هایی که به منظور مسدود کردن اسکریپت ها تولید شده اند، امکان غیر فعال سازی و جلوگیری از اجرای خودکار آن ها را دارند.

در این میان، بیشترین تعداد افزونه های امنیتی، متعلق به مرورگر فایرفاکس است. با نصب افزونه NoScript در فایرفاکس، به راحتی می توان از اجرا شدن کدهایی که امکان آسیب رساندن به کامپیوتر را دارند، جلوگیری نمود. البته در این افزونه، امکان اجرای کدهای جاوا اسکریپت[1] و فلش برای هر سایت به صورت جداگانه قابل تعیین است. استفاده از این افزونه، تا حد زیادی می تواند جلوی حملات XSS را گرفته و امنیتی بسیار بیشتر از گذشته را فراهم کند.

یکی دیگر از افزونه های امنیتی فایرفاکس، افزونه Everywhere Https است که نصب آن بر روی مرورگر، این امکان را می دهد تا تمام سرویس هایی که امکان SSL روی آن ها فراهم است، به صورت پیش فرض روی این حالت باز شوند. SSL یک پروتکل امن اینترنتی است که تمامی اطلاعات در حال مبادله را رمزنگاری می کند.

[1] JavaScript

برای امنیت بیشتر، بهتر است پلاگین هایی مانند Flash Player که وظیفه پخش فایل های فلش در صفحات وب را بر عهده دارند نیز غیر فعال نمود اما اگر نیاز به استفاده از این پلاگین است، باید آخرین نسخه آن نصب گردد.

نگهداری رمزهای عبور در مرورگر

بسیاری از مرورگرها از قابلیت ذخیره کردن رمزهای عبور حساب های کاربری صفحات login وب سایت ها برخوردارند. با توجه به این که کلمات عبور، در فایلی به نام کوکی نگهداری می شوند و امکان دزدیدن آن ها در حملات XSS وجود دارد، بنابراین، نباید هرگز اقدام به انجام این کار نمود.

اگرچه وارد کردن رمز عبور در هر بار login کردن، اندکی از وقت شما را می گیرد اما انجام این کار، ارزش محافظت از اطلاعات حساس تان را دارد. استفاده از مرورگر برای نگهداری رمزهای عبور به هیچ وجه توصیه نمی شود و در موارد ضروری نیز باید از نرم افزارهای مدیریت رمزهای عبور قدرتمند مانند LastPass استفاده کرد.

پاک کردن حافظه مرورگر و کوکی ها

مرورگرها می توانند اطلاعاتی همچون آدرس وب سایت های بازدید شده، زمان مشاهده و اطلاعاتی از این قبیل را در حافظه خود ذخیره کنند که جهت افزایش امنیت سیستم، لازم است تا این اطلاعات پس از مدتی کوتاه پاک شوند. نرم افزارهای زیادی در این خصوص وجود دارد ولی در صورت عدم استفاده از این برنامه ها نیز می توان مرورگر را طوری تنظیم کرد که این فایل ها و اطلاعات پس از هر بار بستن مرورگر، به صورت خودکار از کامپیوتر پاک شوند.

در ضمن، برای حفظ حریم خصوصی و باقی نماندن هیچ رد پایی در مرورگر و کامپیوتر پس از مشاهده وب سایت ها، استفاده از Private Browsing Mode توصیه می شود. در این حالت، صفحات وب بازدید شده، اطلاعات ورودی در فرم ها و فیلدهای جستجو، رمزهای عبور، کوکی ها و کش صفحات، در کامپیوتر ذخیره نمی شود. نام این حالت در مرورگر کروم Incognito است و استفاده از آن در فایرفاکس نیز از طریق منوی Tools و گزینه Start Private Browsing امکان پذیر است.

به روز رسانی مرورگر و افزونه ها

مرورگرها به این دلیل که بیشترین نقطه اتصال بین کامپیوتر و دنیای خارج هستند، همواره خطری بالقوه محسوب می شوند. چرا که نفوذگران با سوء استفاده از حفره های امنیتی مرورگرها می توانند به کامپیوتر کاربران نفوذ نمایند.

در این میان، توسعه دهندگان مرورگرهای اینترنتی هم به صورت متناوب در حال به روز رسانی مرورگرها و رفع حفره ها و باگ های امنیتی آن ها هستند. به همین دلیل، یکی از مهمترین عوامل در جلوگیری از سوء استفاده هکرها، به روز رسانی منظم مرورگر و افزونه های نصب شده در آن است.

جلوگیری از نصب افزونه های اضافی

بسیاری از کاربران بدون آن که از قابلیت های افزونه ها استفاده نمایند، اقدام به نصب افزونه های گوناگون بر روی مرورگر می کنند که این امر، سیستم آن ها را در معرض تهدیدهای جدی قرار می دهد.

توصیه می شود تنها افزونه هایی که بیشتر مورد استفاده قرار می گیرند، بر روی مرورگر نصب نموده و از نصب افزونه های اضافی خودداری شود. همچنین، در صورت ارایه نسخه

های به روز شده افزونه ها نیز حتماً نسخه قبلی را پاک کرده و از نسخه جدیدتر استفاده گردد.

۱۲

امنیت مرکز داده[1]

مرکز داده، مکانی است که سیستم های کامپیوتری و تجهیزات جانبی مربوط به آن ها مانند سیستم های ذخیره سازی و ارتباطی را در خود جای می دهد. این مرکز، می تواند اتاقی از یک ساختمان، طبقه ای از آن و یا کل ساختمان باشد.

مراکز داده به علت آن که حجم بسیار بزرگی از اطلاعات را در خود نگهداری می کنند، می توانند مورد تهدیدهای جدی از سوی نفوذگران حرفه ای قرار بگیرند. بنابراین، اتخاذ تدابیر امنیتی در آن ها جهت حفاظت از اطلاعات، امری ضروری به شمار می رود. به دلیل اهمیت مراکز داده، امروزه استانداردهای بین المللی نیز در این خصوص وجود دارند که مراکز داده در هر جایی که باشند، مجبور به رعایت تمامی نکات آن هستند.

برخی از مهم ترین تدابیر امنیتی که در این مراکز باید لحاظ شود به شرح زیر است:

- تجهیز مرکز داده به سیستم های پشتیبان برق که در صورت قطع برق شهری، به صورت آنی و خودکار به تأمین برق آن اقدام نموده و در مدت زمان طولانی هم، بی وقفه قادر به سرویس دهی باشد.
- وجود تجهیزات اضافی که در صورت خرابی سیستم اصلی، بتوان از آن ها به عنوان پشتیبان استفاده نمود.
- تعبیه کنترل کننده های محیطی مانند دستگاه های تهویه هوا و کنترل رطوبت؛
- استفاده از تجهیزات آتش نشانی و اعلام حریق مجهز به سنسورهای حساس به دود؛
- بهره گیری از ابزارها و سامانه های کنترل دسترسی فیزیکی به داده ها؛
- تجهیز به سیستم های کنترل برق که در هنگام تغییرات ولتاژ برق شهری، اقدام به توزیع یکنواخت و با ولتاژ ثابت برق به مرکز نماید.

---

[1] Data Center

- تجهیزات امنیتی همچون فایروال، ضد ویروس، ضد جاسوس افزار[1] و سایر سامانه های امنیت شبکه همچون DMZ؛
- سیستم های مدیریتی و پایش شبکه (IDS، IPS)؛
- سیستم های ثبت وقایع و اعلام خطر در صورت احتمال حملات سایبری به مرکز داده؛
- سرورهای پشتیبان از پایگاه داده؛
- سامانه های امنیت اطلاعات و حفظ امنیت داده ها؛
- سیستم های بازیابی اطلاعات؛
- استفاده از پروتکل های امنی همچون SSL برای ارتباطات اینترنتی و خارج از محیط مرکز داده؛
- معماری مرکز داده باید به صورتی باشد که در آن اعمال تغییرات، به صورت پویا امکان پذیر بوده و پیش بینی فضای مورد نیاز آینده نیز در نظر گرفته شود.
- طراحی توپولوژی شبکه در مرکز داده باید به صورت ستاره ای باشد که امکان مدیریت، اضافه شدن یا کاستن سرورها و سیستم ها را با کمترین زمان از کار افتادگی، فراهم کند.
- نگهداری داده ها در پایگاه داده، به صورت رمزنگاری شده؛
- تمامی کابل ها حتماً Shield دار بوده و از طریق داکت های فلزی محافظت شوند.
- استفاده از سیستم های شناسایی بیومتریک پیشرفته برای کارمندان مرکز؛
- انجام ارزیابی های امنیتی و تست های نفوذ به صورت مداوم و در بازه های زمانی مشخص؛
- تهیه دستورالعمل های لازم در هنگام مواجهه با مخاطرات؛
- استفاده از دوربین های مدار بسته با قابلیت دید در تاریکی و سیستم های مانیتورینگ؛

[1] Anti Spyware

- وجود نقشه مرکز داده که در آن به خوبی مسیر کابل ها، Backbone ها، جایگاه تجهیزات شبکه، سرورها و ... مشخص باشد.
- استفاده از الگوریتم های رمزنگاری برای ذخیره داده ها در دیسک های سخت؛
- دستگاه های خردکننده دیسک های سخت برای از بین بردن دیسک های فرسوده؛
- سازمان ها و شرکت هایی که اطلاعات خود را در مرکز داده ذخیره می کنند بهتر است که استانداردهای امنیت اطلاعات سازمانی همچون ISO/IEC 27001 را دریافت نمایند.
- از نظر معماری و فیزیکی، باید هرگونه دسترسی به محیط داخل مرکز را به غیر از درب ورودی اصلی کاملاً مسدود نمود. فضای مرکز داده، نیازی به پنجره یا هواکش ندارد.
- اگر نیاز به نصب نرم افزار خاصی است، حتماً با هماهنگی کارشناس امنیت مرکز صورت گیرد.
- چیدمان رک ها به ترتیبی باشد که در مواقع لازم، امکان عبور از میان آن ها به آسانی صورت پذیرد.

۱۳

استانداردهای امنیت اطلاعات سازمانی

پرداختن به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری، مستلزم توجه همه کاربران صرفنظر از موقعیت شغلی و سنی آنها بوده و می بایست به این مسأله در سطح کلان توجه شود. وجود ضعف امنیتی در شبکه های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح کاربران، عدم وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست های مشخص و مدون به منظور برخورد مناسب و به موقع با اشکالات امنیتی، مسایلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می دهد.

در دنیای رقابتی امروز، اهمیت اطلاعات به عنوان دارایی ارزشمند و ابزار رقابت بر هیچ کس پوشیده نیست. از این رو، صیانت و حفاظت از این دارایی ارزشمند یکی از وظایف ذاتی سیستم مدیریت در هر بنگاه اقتصادی و سازمان می باشد. به خصوص با پیشرفت ابزارهای فناوری اطلاعات و مدل های مرسوم در بهره گیری از اطلاعات تولید شده، این امر از اهمیت دوچندانی برخوردار شده است. مسلماً بهره گیری از مدل های مدیریتی در چارچوب استانداردهای بین المللی می تواند سازمان را در این وظیفه خطیر یاری دهد. اطلاعات به عنوان یک دارایی مهم و با ارزش برای هر سازمان به حساب می‌آید و در نتیجه نیازمند ارایه راه کارهای حفاظتی لازم برای نگهداری است.

بزرگترین چالش شرکت ها و سازمان های سرویس دهنده خدمات فناوری اطلاعات، صرف کمترین هزینه ممکن و ارایه بهترین کیفیت می باشد. این امر در بخش های مختلف سازمان نمود پیدا می کند که از آن جمله می توان به مواردی چون افزایش بهره وری نیروی انسانی، استفاده بهینه از ظرفیت های موجود و ایجاد امکانات و ظرفیت های جدید منطبق بر نیاز واقعی کسب و کار اشاره نمود. در اختیار داشتن تکنولوژی پیشرفته و نیروی انسانی متخصص به تنهایی کارگشا نبوده و مسأله بسیار مهمی به نام روال های مدیریت سرویس مطرح می گردد که در واقع حلقه مرتبط کننده تکنولوژی و افراد می باشد.

استاندارد ISO 20000 اولین استاندارد مستقل در زمینه مدیریت و امنیت خدمات فن آوری اطلاعات است که سازمان جهانی استاندارد ISO آن را منتشر نموده است.

سامانه مدیریت امنیت اطلاعات[1]

نیاز روزافزون به استفاده از فناوری های نوین در عرصه اطلاعات و ارتباطات، ضرورت استقرار یک نظام مدیریت امنیت اطلاعات را بیش از پیش آشکار می‌نماید. یک سیستم استاندارد و کارآمد مدیریت امنیت اطلاعات، ضمن مقابله با تهدیدهای امنیتی، آمادگی سازمان را در مواجه با وقایع امنیتی احتمالی، تضمین می نماید. این استاندارد بین المللی جهت طراحی[2]، اجرا، بازنگری و بهبود سامانه های مدیریت امنیت اطلاعات می باشد.

سامانه مدیریت امنیت اطلاعات در واقع قسمتی از سیستم مدیریت کلان سازمان است که بر مبنای دیدگاه مخاطرات کسب و کار بنا شده است (اساس این سیستم، مدیریت مخاطرات

---

[1] Information Security Management System (ISMS)
[2] Design

می‌باشد) و به منظور ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات در سازمان، به کار می‌رود.

از مهمترین فواید این سامانه، می توان به موارد زیر اشاره نمود:

- کمینه نمودن زیان‌های وارده به کسب و کار، ناشی از عدم حفاظت اطلاعات؛
- حفظ امنیت اطلاعات سازمان؛
- افزایش فرصت‌های مرتبط با کسب وکار؛
- هموار نمودن زمینه‌های تداوم کسب و کار؛
- فراهم‌آوری حاشیه رقابتی در بازاریابی و سودآوری؛
- زمینه‌سازی برای حضور در بازارهای جهانی؛
- چارچوبی مناسب در راستای تجارت الکترونیک؛

BS 25999

در شرایط کسب و کارکنونی و با پیشرفت ها و تحولات جهانی، فرآیند تداوم کسب و کار، خود را به عنوان یک موضوع مهم در تمامی سازمان ها مطرح کرده و مدیریت این فرآیند به عنوان یک بخش ضروری در تمام قسمت های کسب وکار شناخته می شود.

توانایی یک سازمان برای نگهداشت و استمرار فعالیت های محوری و حیاتی خود پس از بروز یک حادثه و همچنین سرعت بازیابی سازمان به حالت عادی، می توانند عامل های اساسی موفقیت و یا شکست یک سازمان را تعیین نمایند. با این توضیح، احتیاج به یک استاندارد مناسب بر اساس مدیریت تداوم کسب و کار شدیداً انتظار می رفت که در این

زمینه، استاندارد BS 25999 منتشر شده توسط مؤسسه استاندارد انگلستان[1] بـه عنـوان یـک چارچوب مناسب برای مدیریت تداوم کسب و کار انتخاب شده است.

تمامی فعالیت های کسب و کار به نوعی با خطر انقطاع در ارتباط خواهنـد بـود، مـواردی همچون اختلالات تکنولوژیکی، سیل، انقطاع تجهیزات و حملات تروریستی از آن جمله مـی باشد. استمرار عملیات در زمان انقطاع حاصله از یک فاجعه عظیم و یا حتی حوادث کوچک، یک نیاز اساسی و بنیادی برای سازمان به شمار می رود. این استاندارد به عنوان اولین استاندارد مدیریت تداوم کسب و کار، با ایجاد یک سیستم مدیریت تداوم کسـب و کـار مناسـب سـعی می نماید تا سازمان حتی در سخت ترین شرایط پیش بینی نشده به فعالیت های خود ادامه دهد و بدین ترتیب ریسک حاصـل از انقطـاع را کـاهش داده، از رفـاه و امنیـت کارکنـان و اعتبـار سازمان حمایت کرده و توانایی هدایت و استمرار فعالیت های اصلی را فراهم می آورد.

ویژگی های استاندارد BS 25999:

- قابل فهم بودن و روانی زبان استاندارد؛
- امکان پیاده سازی[2] و زیرساخت های موجود در سازمان های ایرانی؛
- اعتبار، گستردگی و مقبولیت جهانی استاندارد؛

BS 25999 استانداردی ملموس و کاربردی به منظـور حفـظ تـداوم کسـب و کـار در هنگام بروز موقعیت های غیر قابل پیش بینی و مخاطره برانگیز می باشـد. پیـاده سـازی سیسـتم مدیریت تداوم کسب و کـار، زیـر سـاختی مناسـب جهـت بررسـی، طراحـی، پیـاده سـازی و مدیریت تداوم کسب و کار را در سازمان ارایه داده و با توجه به عملیـات ممیـزی کـه در پـی پیـاده سـازی هـر اسـتانداردی قابـل انجـام اسـت، بـه سـازمان گـواهی نامـه BS 25999

[1] BSI
[2] Implementation

توسط BSI اعطاء شده و چارچوبی برای بهبود مداوم و توانایی به نمایش گذاردن این قابلیت به ذینفعان ایجاد می گردد که بر اساس بهترین تجارب بین المللی بنا گردیده است.

هدف اصلی استاندارد مذکور، ارایه مفاهیم پایه ای جهت درک، ایجاد و پیاده سازی تداوم کسب و کار در یک سازمان و کسب نوعی اطمینان از روابط سازمان با مشتریانش و دیگر سازمان ها می باشد. این استاندارد سازمان را قادر می سازد تا با روشی یکپارچه و از پیش تعیین شده، قابلیت مدیریت تداوم کسب و کار را در درون خود مورد ارزیابی و اندازه گیری قرار دهد. احتیاج ها و الزام های مشخص شده در این استاندارد انگلیسی به صورت عام می باشد و انتظار می رود که بدون توجه به نوع، اندازه و طبیعت کسب و کار، در تمامی سازمان ها قابل اجرا باشد.

ITIL

در دو دهه اخیر، فعالیت های بسیاری در زمینه مدیریت سرویس های امنیت اطلاعات در دنیا صورت گرفته است. در این میان سازمان OGCI انگلستان، با گذشت حدود ۲۰ سال از اولین تلاش ها، ITIL را به عنوان استاندارد پذیرفته شده در دنیا معرفی کرده است.

ITIL یک روش یا توصیه پیشنهاد شده توسط یک سازمان یا مؤسسه نیست، بلکه مجموعه ای از بهترین تجربیات شرکت های بزرگ دنیا طی سال های گوناگون در مدیریت سرویس های فناوری می باشد. این استاندارد در دنیا با استقبال بسیاری مواجه شده است و آمار های معتبر نشان دهنده تمایل شرکت ها و سازمان های مختلف در ارایه سرویس های ITIL در مدیریت سرویس های فناوری اطلاعات می باشد.

SSE/CMM

استاندارد **SSE/CMM** (مدل بلوغ) نقاط مرجعی برای سازمان مهیا می‌کند تا خود را در برابر راه کارهای برتر مطابق یک دستورالعمل ویژه یا چند دستورالعمل ارزیابی نماید. همچنین این مدل فرآیندگرا به پیشرفت سازمان ها برای رسیدن به سطوح بلوغ بیشتر، با در نظر گرفتن راه کارهای امنیتی کمک می‌کند.

منظور از یک سازمان بالغ، صرفاً تحصیلات و دانش کارکنان سازمان نمی باشد، بلکه مجموعه‌ای همچون انگیزه، علاقه‌مندی، دانش و مهارت، سابقه، اطلاعات و ده ها مؤلفه دیگر موجب می شود تا سازمان بالغ گردد و به اصطلاح فرآیندها ی موجود، بهبود یافته و بلوغ سازمانی پیاده سازی شده است.

١٤
سامانه مدیریت امنیت اطلاعات

امروزه امنیت اطلاعات، بزرگترین چالش در عصر فناوری اطلاعات محسوب می شود و حفاظت از اطلاعات در مقابل دسترسی غیر مجاز، تغییرات، خرابکاری و افشاء، امری ضروری و اجتناب ناپذیر به شمار می رود. از این رو، امنیت دارایی های اطلاعاتی، برای تمامی سازمان ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش می باشد.

فراهم آوری صحت و تمامیت اطلاعات، به گونه ای که در زمان مناسب، اطلاعات در دسترس افراد مجازی قرار بگیرد که نیازمند آن می باشند، عاملی است که منجر به اثربخشی کسب و کار می گردد. امنیت اطلاعات شامل سه بُعد مهم است:

۱. محرمانگی[1]؛
۲. یکپارچگی[2]؛
۳. دسترس پذیری[3]؛

استاندارد ISO/IEC 27001:2005 زمینه مناسبی را برای طراحی و استقرار سامانه مدیریت امنیت اطلاعات و ارزیابی آن در سازمان ها و بهره گیری از منافع این رویکرد، فراهم آورده است. سیستم مدیریت برحسب امنیت اطلاعات، به یک سازمان این امکان را می دهد تا موارد زیر را ایجاد نماید:

- رضایت نیازمندی های امنیتی مشتریان و سایر ذینفعان؛

---

[1] Confidentiality

[2] Integrity

[3] Availability

- بهبود طرح ها و فعالیت های سازمان؛
- تأمین اهداف امنیت اطلاعات سازمان؛
- تطابق با آیین نامه ها و قوانین و مقررات مربوط به کار؛
- مدیریت دارایی های اطلاعاتی در یک روش سازمان یافته که به بهبود مستمر و تعدیل با اهداف سازمانی کنونی کمک می کند.

لذا ضروری است که سامانه مدیریت امنیت اطلاعات، با توجه به نیازها و الزام های هر سازمان و منطبق با رویه ها و استانداردهای ISO/IEC 27001 و ISO/IEC 27002 طبق فازهای زیر، طراحی و پیاده سازی شود:

۱. ارزیابی و شناخت اولیه[1]:

در فاز ارزیابی و شناخت اولیه، میزان انطباق سازمان با الزام ها و کنترل های استاندارد ISO/IEC 27001 مورد بررسی قرار می گیرد. این مرحله، کمک شایانی به تعیین دامنه[2] پیاده سازی سیستم و فاز طراحی خواهد نمود. فعالیت هایی که در این مرحله اجرا می شود، عبارتند از:

- شناسایی وضعیت موجود و ارزیابی میزان انطباق سازمان با الزام ها و کنترل های استاندارد ISO/IEC 27001 ؛
- مستندسازی و تهیه گزارش از وضعیت موجود؛
- تعیین دامنه پیاده سازی سامانه مدیریت امنیت اطلاعات؛
- تهیه و تدوین خط مشی امنیت اطلاعات؛
- کمک به سازماندهی و تشکیل کمیته راهبری امنیت در سازمان؛

۲. آگاه سازی و آموزش[3]:

---

[1] Gap Analysis

[2] Scope

[3] Awareness & Training

در این مرحله، تمامی افراد درگیر در فرآیند پیاده سازی سامانه مدیریت امنیت اطلاعات، آموزش دیده و با مفاهیم و الزام های سامانه مدیریت امنیت اطلاعات آشنا می شوند.

۳. طراحی سامانه مدیریت امنیت اطلاعات:

به منظور موفقیت در پیاده سازی سامانه مدیریت امنیت اطلاعات، می بایست این سیستم را مطابق با الزام های استاندارد و نیازمندی های سازمان طراحی نمود. فعالیت هایی که در این مرحله اجرا می شود، عبارتند از:

- تهیه لیست دارایی های واقع در دامنه؛
- طبقه بندی و ارزش گذاری دارایی های اطلاعاتی؛
- تعیین و تدوین متدولوژی ارزیابی مخاطرات؛
- تدوین خط مشی ها، دستورالعمل ها و روش های اجرایی مورد نیاز سامانه؛
- تدوین طرح تداوم کسب و کار[1]؛
- تدوین طرح برطرف سازی مخاطرات[2]؛
- تدوین بیانیه کاربست پذیری[3]؛

٤. پیاده سازی سامانه مدیریت امنیت اطلاعات:

در این مرحله، کنترل ها، طرح ها و سیاست های امنیتی تهیه شده در فاز قبلی، پیاده سازی می شود.

٥. ممیزی داخلی و همراهی تا صدور گواهینامه بین المللی[4]:

---

[1] BCP

[2] RTP

[3] Statement of Applicability (SOA)

[4] Internal & External Audit

پس از پیاده سازی و استقرار کامل سامانه مدیریت امنیت اطلاعات در سازمان، سرممیزان انتخاب شده توسط سازمان، با پیش ممیزی سیستم پیاده سازی شده قبل از ممیزی نهایی، موارد انحرافی و عدم انطباق ها را شناسایی می کنند و با ارایه اقدام های اصلاحی و پیشگیرانه مناسب به منظور رفع عدم انطباق های شناسایی شده، سازمان را تا اخذ گواهینامه بین المللی ISO/IEC 27001 همراهی می نمایند.

مزایای پیاده سازی سامانه مدیریت امنیت اطلاعات در یک سازمان:

- امنیت اطلاعات و دارایی های اطلاعاتی؛
- حفظ محرمانگی و در دسترس بودن اطلاعات؛
- حفظ اطلاعات از بروز تهدیدات، آسیب پذیری ها و مخاطرات در حد امکان؛
- آمادگی برای مواجه با حوادثی که امنیت اطلاعات را به مخاطره انداخته اند.
- ایجاد اطمینان بیشتر برای مدیران، کارکنان، مشتریان و سایر ذینفعان سازمان در مورد امنیت اطلاعات؛
- بازگشت هزینه صرف شده برای پیاده سازی سامانه مدیریت امنیت اطلاعات در بلند مدت؛
- کاهش هزینه های ترمیم خسارات ناشی از کمبود و نقص موازین امنیتی؛
- شناسایی، ارزیابی و حفاظت از دارایی های مهم سازمان همچون پرسنل کلیدی، دانش پرسنل، اطلاعات، وجهه و اعتبار سازمان؛
- اطمینان از تداوم کسب و کار و کاهش آسیب ها از طریق ایمن ساختن اطلاعات و کاهش تهدیدها؛
- امکان رقابت بهتر با سایر سازمان ها؛

۱۵

ممیزی امنیتی و مستندسازی سیستم های کامپیوتری

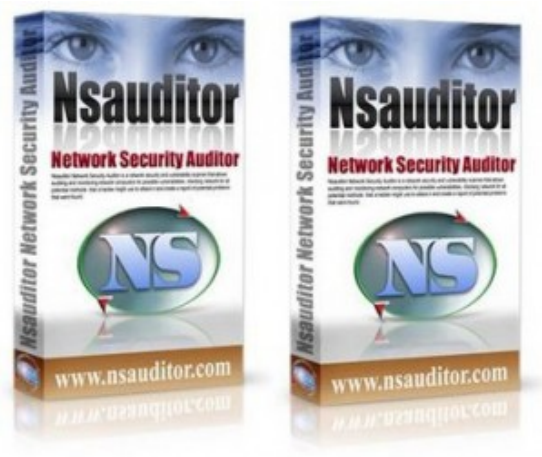
ممیزی امنیتی سیستم های کامپیوتری در سازمان ها سبب پیدایش رخنه های امنیتی، شناسایی مخاطرات و تهدیدها شده و به سازمان ها این اطمینان را می دهد که شبکه ها و سیستم های اطلاعاتی و کامپیوتری موجود، در سطح مطلوبی از امنیت بوده و به بهترین نحو در جهت پیشبرد اهداف سازمان عمل می نمایند و یا در غیر این صورت، تمامی ضعف های امنیتی موجود در سیستم ها شناسایی شده و می توان در جهت رفع آنها اقدام نمود.

به بیان دیگر، اجرای ممیزی امنیتی در سازمان ها به نوعی انجام "ارزیابی و شناخت اولیه" می باشد که همواره میزان انطباق یا فاصله سازمان و یا فرآیندهای مورد ارزیابی را با معیارهای امنیتی، سنجیده و ابزار مناسبی جهت به روز نگه داشتن سازمان از منظر امنیتی می باشد که امروزه اجرای آن در فواصل زمانی مشخص برای سازمان ها از اهمیت به سزایی برخوردار است.

نگهداری از شبکه های کامپیوتری و مدیریت سیستم ها و نرم افزارها از جمله وظایف یک مدیر شبکه می باشد. مدیر شبکه علاوه بر دانش کافی در زمینه نگهداری شبکه، باید دقت بسیاری را در نحوه اعمال تنظیم های امنیتی بر روی سیستم ها داشته باشد. تنظیم های نرم افزاری و سخت افزاری همیشه به صورت یکسان نبوده و مدیران شبکه می بایست با توجه به نوع توپولوژی و ساختار شبکه خود، این تنظیم ها را اعمال نمایند. بهترین حالت برای مطمئن شدن از تنظیم های صحیح، به کارگیری افراد متخصص در زمینه ممیزی نمودن و یا استفاده از نرم افزارهای ارزیابی ممیزی می باشد.

پس از انجام ممیزی امنیتی، کلیه فرآیندهای سیستم های مورد بررسی اعـم از اطلاعـاتی و کامپیوتری (شبکه) مستندسازی شـده و در قالـب روش اجرایـی، دسـتورالعمل و ... ارایـه مـی گردد که این امر سبب می شود تـا همـه فرآینـدهای کلیـدی سـازمان بـه شـکل سیسـتماتیک تدوین و همه الزام های امنیتی را پوشش دهند و از طرفـی همـه پرسـنل شـرکت را بـه اجـرا و رعایت این مستندات الزام می نماید. در نتیجه ممیزی و مستندسازی تنها راه اطمینان از صحت تدابیر سازمان برای محافظت از دارایی های خود اسـت. از ایـن رو، ممیـزان بـا مسـئولیت هـا، چالش های سنگین و مسایل پیچیده ای در روند کار خود مواجه هستند.

بررسی و ممیزی نمودن تنظیم های امنیتی در شبکه با استفاده از نرم افزار:



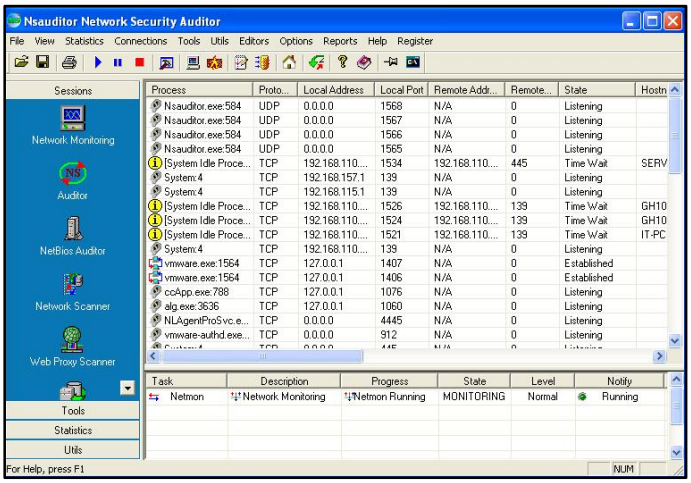
Nsauditor Network Security Auditor نرم افزاری قدرتمنـد در خصـوص بررسی و ممیزی نمودن تنظیم های امنیتی در شبکه است. این نـرم افـزار، بـا در اختیـار داشـتن بیش از ۴۵ نوع مختلف از ابزارها، این توانایی را به مدیر شبکه می دهد تـا بـا بررسـی قسـمت های مختلف تنظیم های امنیتی، از نوع تنظیم های اعمـال شـده و امنیـت شـبکه خـود اطمینـان حاصل کند.

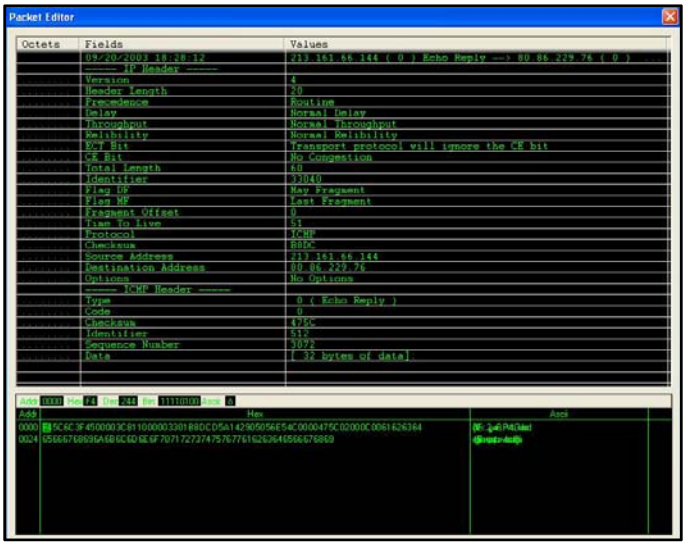
این نرم افزار که محصولی از شرکت Nsasoft می باشد، در رابطه با کشف مشکلات و نقاط ضعف موجود در شبکه که ممکن است موجب بروز مشکلاتی از جمله نفوذ هکرها شود، کمک شایانی به مدیران می کند.

از مهمترین ویژگی های این نرم افزار می توان به موارد زیر اشاره نمود:

- بررسی قسمت های مختلف شبکه و ارایه گزارش در قالب فرمت های HTML و XML؛
- توانایی نظارت بر شبکه؛
- بررسی تنظیمات مربوط به NetBios؛
- بررسی تنظیمات نرم افزار MS SQL؛
- قابلیت فیلتر گذاری بر Packet ها در شبکه؛
- دارای ابزار Port Scanner؛
- توانایی شناسایی سیستم عامل در سیستم های راه دور؛
- دارای ابزار بازیابی و کشف پسورد های LM و NTLM؛

تصاویری از محیط برنامه:




Packet Editor
Octets
Fields
Values
09/20/2003 16:28:12
213.161.66.144 (0) Echo Reply --> 80.86.229.76 (0)
----- IP Header -----
Version
4
Header Length
20
Precedence
Routine
Delay
Normal Delay
Throughput
Normal Throughput
Reliability
Normal Reliability
ECN Bit
Transport protocol will ignore the CE bit
CE Bit
No Congestion
Total Length
60
Identifier
33040
Flag DF
May Fragment
Flag MF
Last Fragment
Fragment Offset
0
Time To Live
51
Protocol
ICMP
Checksum
88DC
Source Address
213.161.66.144
Destination Address
80.86.229.76
Options
No Options
----- ICMP Header -----
Type
0 (Echo Reply)
Code
0
Checksum
475C
Identifier
512
Sequence Number
3072
Data
[32 bytes of data]
Hex
Ascii

آشنایی با استاندارد امنیت اطلاعات در صنعت کارت پرداخت[1]

امروزه نیاز دارندگان کارت های اعتباری به امنیت اطلاعاتشان به طور غیر قابل باوری افزایش یافته که بازتاب این نیاز، در استاندارد های امنیتی داده های مربوط به حساب های پرداخت کارتی متبلور است. مشاهده اطلاعات حساس سرقت شده و در معرض خطر حدود ۳ میلیون از کارت های اعتباری مردم کشورمان در روزهای اخیر در اینترنت، آشکارا نشان داد که به کارگیری استانداردی مربوط به امنیت اطلاعات صنعت کارت های پرداخت، مانند PCI DSS جهت حفاظت از داده های مشتریان، جداً ضروری بلکه چه بسا ناکافی هم بوده و ایمنی اطلاعات کارت های اعتباری باید خیلی بیشتر از آنچه که در حال حاضر است، رعایت شود.

استاندارد امنیت اطلاعات در صنعت کارت پرداخت، چیست؟

استاندارد امنیت اطلاعات در صنعت کارت پرداخت، مجموعه جامعی از قوانین است که برای ارتقاء سیستم امنیتی داده های مربوط به صنعت کارت های پرداخت وضع گردیده و هدف آن، کمک جهت تسهیل روند اتخاذ تمهیدهای امنیتی مربوط به داده های پایدار در یک جامعه جهانی است. این استاندارد، توسط مؤسسین سیستم پرداخت مارک های تجاری شورای استانداردهای امنیتی PCI ایجاد شده است که از میان آن ها می توان به سازمان های بزرگ پرداخت الکترونیک همچون American Express، Discover

[1] Payment Card Industry Data Security Standard (PCI DSS)

MasterCard Worldwide و JCB International ،Financial Cervices Inc اشاره نمود.

استاندارد امنیت اطلاعات در صنعت کارت پرداخت، یک استاندارد امنیت اطلاعات است که هر کسب و کاری با هر حد و اندازه، برای استفاده از کارت های پرداخت و همچنین ذخیره سازی، پردازش و یا ارسال اطلاعات صاحب کارت باید آن را دریافت نماید. بنابراین، اخذ استاندارد امنیت اطلاعات صنعت کارت های پرداخت، برای فروشندگانی که از فناوری کارت پرداخت در سیستم فروش خود استفاده می کنند و شرکت هایی که اطلاعات شخصی دارندگان این نوع کارت را پردازش می نمایند، یک موضوع مهم و ضروری می باشد.

این استاندارد جامع، در واقع نوعی استاندارد امنیتی چند وجهی است که شامل نیازمندی هایی برای مدیریت امنیت، سیاست ها، رویه ها، معماری شبکه، طراحی نرم افزار و دیگر تمهیدات حفاظتی حساس بوده و کمک به بانک ها و مؤسسات مالی، جهت حفاظت از داده های مربوط به حساب های مشتریانشان را به عنوان هدف خود در نظر می گیرد.

شورای استانداردهای امنیتی PCI، علاوه بر تشویق سازمان ها برای پیروی از این استاندارد، سیستم استاندارد امنیت اطلاعات در صنعت کارت پرداخت را در صورت نیاز، ارتقاء خوهد داد تا اطمینان حاصل شود که این استاندارد، همه نیازهای نوین، برای کاهش ریسک های مربوط به پرداخت را در بر گیرد.

استاندارد امنیت اطلاعات در صنعت کارت پرداخت با زمینه کاری استانداردهای ISO/IEC 27001 و ISO/IEC 27002 مطابقت داشته و سازمان هایی که در زمینه کارت های پرداخت فعالیت دارند و استاندارد ISO/IEC 27001 (سامانه مدیریت امنیت اطلاعات) را قبلاً اجرا نموده اند با کمترین اقدام های اضافی قادر خواهند بود تا استاندارد امنیت اطلاعات در صنعت کارت پرداخت را نیز در سازمان خود، به منظور مدیریت بهتر حفاظت اطلاعات، پیاده سازی نمایند.

الزام های استاندارد امنیت اطلاعات در صنعت کارت پرداخت:

این استاندارد در ۶ اصل مشخص، ۱۲ الزام را برای هر کسب و کاری، اعم از فروشندگان، شرکت های ارایه دهنده خدمات کارت و بانک ها که اطلاعات دارندگان کارت های پرداخت را ذخیره، پردازش و یا منتقل می کنند، در نظر گرفته است که این ملزوم ها، یک چارچوب کاری برای محیط امن پرداخت کارتی را تعریف می کند. این الزام ها عبارتند از:

۱. ایجاد و حفظ یک شبکه امن

الزام ۱: نصب سیستم های دیواره آتش[1]، جهت حفاظت از اطلاعات مربوط به دارندگان کارت های پرداخت الکترونیک؛

الزام ۲: عدم استفاده از تنظیم های پیش فرض انجام شده توسط فروشندگان و سازندگان تجهیزات، مانند رمز عبور و دیگر پارامترهای امنیتی؛

۲. حفاظت از اطلاعات دارنده کارت

الزام ۳: محافظت از داده های ذخیره شده مربوط به دارندگان کارت ها؛

الزام ۴: رمزنگاری نقل و انتقال اطلاعات دارندگان کارت ها در شبکه های باز و عمومی؛

۳. استفاده از برنامه های مدیریت آسیب پذیری

الزام ۵: نصب نرم افزار ضد ویروس و به روز رسانی مداوم آن؛

الزام ۶: توسعه و نگهداری سیستم های ایمن و برنامه های کاربردی امن؛

---

[1] Firewall

۴. اعمال تمهیدهای قوی در کنترل دسترسی ها

الزام ۷: محدود کردن دسترسی به اطلاعات دارندگان کارت ها در حداقل احتیاج هر کسب و کار؛

الزام ۸: اختصاص یک شناسه کاربری[1] یکتا به هر یک از کاربران؛

الزام ۹: محدود کردن دسترسی فیزیکی به اطلاعات دارندگان کارت ها؛

۵. پایش و ارزیابی مداوم شبکه

الزام ۱۰: پایش و ردیابی مداوم هرگونه دسترسی به منابع اطلاعاتی، تجهیزات شبکه و همچنین اطلاعات مربوط به دارندگان کارت ها؛

الزام ۱۱: ارزیابی منظم و قاعده مند امنیت سیستم ها و فرآیندهای امنیتی لحاظ شده؛

۶. اتخاذ یک سیاست امنیت اطلاعات

الزام ۱۲: سیاستی اتخاذ شود که خط مشی های امنیت اطلاعات در آن مشخص گردد.

این استاندارد، همچنین سه اقدام اصلی زیر را نیز الزام می کند:

۱- **ارزیابی**: فرآیندی است که در آن یک فهرست از دارایی های اطلاعاتی و پروسه تجاری مرتبط با فرآیند کارت های اعتباری تهیه شده و از نظر آسیب پذیری هایی که ممکن است اطلاعات شخص دارنده کارت را تحت الشعاع قرار دهد، بررسی می گردد.

[1] ID

هدف اولیه این ارزیابی، شناخت آسیب پذیری های تکنولوژی و فرآیندها است که ممکن است امنیت اطلاعات صاحب کارت را هنگام انتقال، پردازش یا ذخیره سازی، در معرض خطر قرار دهد.

۲- **رفع آسیب پذیری ها**[1]: فرآیند پوشش دهی و رفع آسیب پذیری های امنیتی شناسایی شده در مرحله قبل است که این آسیب پذیری ها ممکن است شامل نقاط ضعف فنی در کد نرم افزار[2] یا اقدام ها و رویه های غیر امن پردازش اطلاعات دارنده کارت پرداخت، در سازمان باشد.

۳- **گزارش**: شامل جمع بندی سابقه های ثبت شده توسط استاندارد امنیت اطلاعات در صنعت کارت پرداخت، برای کنترل پروسه بازیابی، رفع آسیب پذیری ها و تحویل گزارش های رعایت استاندارد به بانک و شرکت تأمین کننده خدمات کارت پرداخت مورد نظر است که کارهای تجاری با آن انجام می گیرد.

این ۱۲ الزام و ۳ اقدام اصلی، یک روند مستمر برای انطباق با استاندارد امنیت اطلاعات در صنعت کارت پرداخت است که در نهایت، همه آن ها، تضمین کننده امنیت اطلاعات دارنده کارت بوده و به کارگیری این استاندارد، می تواند به منزله گام ابتدایی و مهمی باشد که در جهت حفاظت از اطلاعات مشتریان توسط بانک ها، مؤسسات مالی –اعتباری و سازمان ها برداشته می شود.

---

[1] Remediate

[2] Bug

۱۷

شبکه ملی اطلاعات (اینترنت ملی)

با همزمانی ایجاد اختلالات و کندی سرعت در لایه دسترسی به شبکه جهانی اینترنت و بروز شایعات و ابراز نگرانی ها پیرامون ارتباط آن با راه اندازی فاز نخست پروژه ای تحت عنوان شبکه ملی اطلاعات یا همان اینترنت ملی، این مقوله تبدیل به یکی از بحث برانگیزترین موضوعات در روزهای اخیر شده است.

با توجه به اظهار نظرهای منتشر شده از سوی نهادها و منابع رسانه ای رسمی و غیر رسمی که اخیراً بنا بر شرایط موجود، بازتاب وسیعی میان مردم داشته است، لزوم یک نگاه صحیح به این موضوع، بیش از پیش احساس می شود. در این مقاله، سعی بر آن است تا ضمن بررسی تمامی جوانب این پروژه، به دغدغه های مخاطبان نیز پاسخی جامع ارایه داده تا در نهایت، موجب منطقی شدن سطح نگرانی ها و افزایش سطح آگاهی جامعه شود.

شبکه ملی اطلاعات یا اینترنت ملی

در ابتدای ورود اینترنت به کشور در سال ۱۳۶۸، بحثی میان پژوهشگاه دانش های بنیادی (مرکز تحقیقات فیزیک نظری و ریاضیات) به عنوان متولی ورود اینترنت، و مخابرات مطرح بود که نشان از مخالفت شدید مسئولان مخابرات با ورود اینترنت به ایران داشت. دکتر سیاوش شهشهانی، جانشین ریاست وقت پژوهشگاه، در مصاحبه ای ضمن اشاره به این موضوع، اعلام می کند:

"از همان ابتدا، در مخابرات ایران کسانی بودند که اعتقادی به اینترنت نداشتند. آن ها فکر می‌کردند اینترنت یک مد روز است و زود فراموش می‌شود. آن ها کوشش می‌کردند

شبکه ای محدودتر به نام X25 را راه‌اندازی کنند و می‌گفتند هر نوع فعالیت شبکه‌ای، باید تحت همین شبکه انجام شود".

اما در تمام این سال ها، نه تنها اینترنت رو به افول نگذاشت، بلکه هم اکنون دو میلیارد نفر در جهان کاربر اینترنت هستند که پیش بینی می شود این رقم در سال ۲۰۲۰ به پنج میلیارد نفر هم افزایش یابد. در کشور ما نیز ۳۶,۵ میلیون کاربر وجود دارد که بیشترین تعداد در بین کشورهای منطقه است.

نخستین فردی که واژه "شبکه ملی اینترنت" را مطرح کرد، عبدالمجید ریاضی، معاونت سابق فناوری اطلاعات وزارت ارتباطات بود که مرداد ماه ۱۳۸۵ضمن ارایه این مفهوم، در تعریف و توجیهش گفت:

"اینترنت در دنیا به یک کلمه خاص تبدیل شده است و از هرکس هم بپرسید، می‌گوید اینترنت شبکه‌ای است که کامپیوترهای دنیا را به هم متصل می‌کند. اما از نظر من که کارم را به صورت تخصصی دنبال می‌کنم، اینترنت تعریف دیگری دارد. اگر بشود شبکه‌ای درست کرد که ویژگی‌های اینترنت را داشته باشد، در سطح محدود، توزیع شده و در نهایت قابلیت اتصال به شبکه جهانی را هم داشته باشد، برای من اهمیت دارد. حالا شما هر اسمی که می‌خواهی روی آن بگذار. ما اسم آن را می‌گذاریم اینتر نت ملی ".

محمد سلیمانی، وزیر سابق ارتباطات و فناوری اطلاعات، مدتی بعد در مصاحبه ای با خبرگزاری فارس، ضمن اعلام خبر اجرایی شدن شبکه اینترنت ملی از مهر ماه سال ۱۳۸۵، گفت:

"طبق برنامه ریزی زمان بندی شده، چارچوب کلی این شبکه طراحی و تعیین شد و طراحی مفهومی آن نیز مراحل پایانی خود را طی می کند ... طراحی جزیی این شبکه نیز در شهریور ماه سال جاری صورت خواهد گرفت و از مهر امسال اینترنت ملی اجرایی خواهد شد. البته شاید با توجه به منابع مالی در نظر گرفته شده به صورت وسیع و یا محدود اجرا شود ... این شبکه طبق پیش بینی ها ظرف دو یا سه سال آینده به شکل مطلوب خواهد رسید".

وی در بخش دیگری از سخنان خود با اشاره به واژه اینترنت ملی، عنوان کرد:

"اینترنت ملی تنها یک نام است و شاید اسم آن تغییر کند. چون اینترنت برای مردم قابل حس و فهم تر بود، ما این نام را برای آن برگزیدیم که فکر می کنیم نام زیبایی نیز است ... با اجرای این شبکه، اینترنت و سرویس های متنوع اینترنتی ارزان قیمت در اختیار مردم قرار می گیرد. مباحثی چون امنیت و حفظ اطلاعات در درون کشور نیز با اجرای اینترنت ملی تحقق می یابد".

رضا تقی پور، وزیر ارتباطات و فناوری اطلاعات، در اواخر بهمن ماه سال جاری، در آیین امضای منشور همکاری بین وزارت ارتباطات و فناوری اطلاعات و اتاق بازرگانی، صنایع و معادن ایران، ضمن بیان این که: "شرایط کشور ما طوری نیست که سرعت اینترنت را بدون قید و شرط افزایش دهیم، شبکه ملی اطلاعات، راه حلی است که برای رفع مشکل سرعت اینترنت پیدا کرده ایم"، اظهار داشت: "با راه اندازی شبکه ملی اطلاعات، پهنای باند لازم برای کسب و کارها فراهم خواهد شد".

پشتوانه این اظهار نظرها، مبحثی بود که نخست در برنامه چهارم توسعه مورد توجه قرار گرفت و بعدها به قانون پنجم توسعه هم راه پیدا کرد. در فصل چهارم برنامه پنجم توسعه و طبق مفاد ذیل ماده ۴۶ آن که مهم ترین ماده مربوط به فناوری اطلاعات در برنامه پنجم قلمداد می شود، شبکه ملی اطلاعات، عبارت است از:

"شبکه‌ای مبتنی بر قرارداد اینترنت[1]، به همراه سوئیچ ها و مسیریاب ها و مراکز داده‌ای، به صورتی که درخواست های دسترسی داخلی و أخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود".

در یک نگاه کلی و با توجه به برنامه پنجم توسعه که به موجب آن، وزارت ارتباطات و فناوری اطلاعات ملزم به اجرای این طرح شده است، هدف طراحان اینترنت ملی را می توان ایجاد شبکه ای یکپارچه یا به قول مهندس عبدالمجید ریاضی، یک ابر شبکه شامل دیتا سنتر های عظیم در داخل کشور دانست که ضمن یکپارچه سازی و توانمند سازی شبکه داخلی کشور، همه سایت های ایرانی، میزبانی وب سایت های خود را به آن دیتاسنترها سپرده تا در

[1] Internet Protocol (IP)

نهایت، کاربران بتوانند با سرعت بیشتر و بدون پرداخت هزینه پهنای باند خارجی و همچنین با امنیت و نظارت بهتر، به وب سایت های ایرانی متصل شوند.

متولی شبکه ملی اطلاعات

دکتر شهشهانی، قائم مقام وقت پژوهشگاه دانش های بنیادی که از آورندگان اینترنت به کشور محسوب می شود، اردیبهشت ماه ۱۳۸۵ در گفتگویی با روزنامه شرق، تفکر راه اندازی اینترنت ملی را نتیجه دعوا بر سر تولیت اینترنت دانسته و می گوید:

"مرکز ما از سال‌ها قبل این طرح را دنبال می کرد چرا که اعتقاد داشتیم با افزایش روز افزون کاربران اینترنتی، ما باید یک نقطه تماس داخلی داشته باشیم. ولی گاهی به نظر می آید بعضی کسانی که در پروژه اینترنت ملی شریک هستند با چنین تفکری جلو نیامده‌اند و تفکر بر سر تولیت است، به جای این که مطرح شود اگر ما نقطه تماس داخلی داشته باشیم این کار به نفع مصرف کننده داخلی است. به همین علت من فکر می‌کنم باید سعی کنیم این تمایل به انحصار و تولیت را کنار بگذاریم و به سوی منافع استفاده کننده گام برداریم".

اگر چه در حقیقت، سازمان هایی نظیر شورای‌عالی فناوری اطلاعات، شورای‌عالی انفورماتیک، مرکز توسعه فناوری اطلاعات و رسانه‌های دیجیتال وزارت ارشاد، شورای‌عالی اطلاع‌رسانی، وزارت ارتباطات و فناوری اطلاعات، معاونت علمی و فناوری ریاست‌جمهوری، پژوهشگاه دانش‌های بنیادی (مرکز تحقیقات فیزیک نظری و ریاضیات)، شورای‌عالی انقلاب فرهنگی، مرکز پژوهش‌های مجلس شورای اسلامی، سازمان نظام صنفی رایانه‌ای و چند سازمان دیگر، هر کدام خود را از مناظر مختلف محتوایی، نظارتی و یا ارتباطی، متولی کل یا بخشی از اینترنت کشور می داند و به قولی، در حال حاضر اینترنت کشور نه از نبود متولی، بلکه از وفور متولی رنج می برد، اما در این میان، از منظر زیرساختی و ارتباطی، از همه بیشتر نقش شرکت ارتباطات زیرساخت (به نمایندگی از وزارت ارتباطات و فناوری اطلاعات) از سویی و پژوهشگاه دانش های بنیادی (به نمایندگی از وزارت علوم، تحقیقات و فناوری) از طرفی دیگر، پررنگ تر است.

به هر حال، پس از همه بحث ها بر سر متولی گری اینترنت ملی، مجلس هشتم در برنامه پنجم توسعه، مشخصاً وزارت ارتباطات و فناوری اطلاعات را مکلّف به ایجاد و توسعه شبکه

ملی اطلاعات می نماید که می توان آن را متولی اصلی راه اندازی اینترنت ملی در کشور نیز دانست.

طرح های مشابه اینترنت ملی در جهان

اینترنت ملی، از نظر فنی، البته با کاربردها و تفاوت های ساختاری مختلف، نمونه های مشابهی در دنیا دارد. برای مثال، در مقیاس های وسیع این طرح، می توان از شبکه باند وسیع استرالیا[1] و طرح پهنای باند ملی ایالات متحده آمریکا نام برد. شبکه Kwangmyong در کره شمالی و internet II میان برخی مراکز پژوهشی آمریکا، از مقیاس های محدودتر آن به شمار می رود.

در کره شمالی، این پروژه به موازات شبکه اینترنت اما به صورت مستقل از آن، با هدف محدودیت ارتباطات خارجی کاربران و تأمین نیازهای ارتباطی داخلی راه اندازی شده است ولی در استرالیا و ایالات متحده آمریکا، در جهت تقویت دسترسی کاربران به منابع اطلاعاتی شبکه جهانی اینترنت با سرعت بیشتر و کیفیت بالاتر اجرا گشته است.

نکته ای که در بررسی شبکه هایی چون شبکه باند وسیع استرالیا و طرح پهن باند ملی ایالات متحده آمریکا حایز اهمیت است، مقیاس زمان بندی و هزینه های بالای اجرای اینگونه پروژه ها است. به عنوان مثال، در پروژه شبکه باند وسیع استرالیا که صرفاً به بهبود زیرساخت های ارتباطی می پردازد، بالغ بر ۳۵٫۹ بیلیون دلار (بیش از پنجاه هزار میلیارد تومان) هزینه گشته و با وجود صرف هزینه های گزاف، پیش بینی شده است که تا پایان سال ۲۰۲۱ بتواند در حدود ۹۳٪ از جمعیت بیست میلیون نفری استرالیا را تحت پوشش خود قرار دهد.

ایجاد امنیت با شبکه ملی اطلاعات

اهمیت امنیت فضای مجازی و حفظ و حراست از اطلاعات ملی و شخصی هم وطنان، یکی از اهدافی است که باعث شده تا دولتمردان، پروژه شبکه ملی را کلید زده و تلاش نمایند که آن را در کوتاه ترین زمان ممکن عملیاتی کنند. با ایجاد شبکه ملی اطلاعات که مهمترین

[1] NBN

دستاورد آن، ایجاد امنیت و مصون ماندن از حملات اینترنتی عنوان شده است، به طور قطع با یک تحول و انقلاب بزرگ در تأمین امنیت فضای مجازی کشور، روبرو خواهیم بود.

معاون فنی وزارت اطلاعات در نخستین همایش ملی دفاع سایبری که با همکاری پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی و سازمان پدافند غیر عامل کشور برگزار شد، با اشاره به لزوم استفاده از ضد بدافزار ملی و به روز، اظهار داشت که: "شبکه اینترنت عامل تهدید یا ابزار جاسوسی نیست، بلکه خود تهدید و جاسوس است".

رضا تقی پور، وزیر ارتباطات و فناوری اطلاعات نیز در این همایش، با اشاره به تصمیمات راهبردی کشور در عرصه راه اندازی زیرساخت های دفاع سایبری، گفت: "حمایت از بومی سازی نرم افزار و ایجاد زیرساخت های امن ارتباطی از جمله مهمترین تصمیمات راهبردی در عرصه دفاع سایبری است که در این راستا اولین مرحله از این شبکه، خردادماه سال ۱۳۹۱ به زیر بار می رود".

وی ایجاد سامانه امنیتی و راه اندازی مرکز ۲۴ ساعته رخدادهای امنیتی در سازمان فناوری اطلاعات ایران را از دیگر اقدام های صورت گرفته در زمینه امنیت و دفاع سایبری عنوان کرد و گفت: "تمامی سازمان ها و نهادهای اجرایی کشور باید نسبت به راه اندازی گروه فوریت های امنیت رایانه ای اقدام کنند که این تکلیف، از سال آینده مورد نظارت وزارت ارتباطات و فناوری اطلاعات قرار می گیرد".

تقی پور، همچنین در آیین امضای منشور همکاری بین وزارت ارتباطات و فناوری اطلاعات و اتاق بازرگانی، صنایع و معادن ایران، ضمن اعلام این که "اینترنت ذاتاً ناامن و شبکه ملی اطلاعات ذاتاً امن است و امیدواریم با راه اندازی شبکه ملی اطلاعات، موضوع امنیت فضای مجازی نیز حل شود"، گفت: "در حال حاضر، واردات نرم افزارهای امنیتی ممنوع و بازار به سمت استفاده از محصولات داخلی هدایت شده است ... در زمینه ورود نرم افزارهای امنیتی محکم ایستاده ایم، چرا که امنیت وارداتی، امنیت نیست و مانند قفلی است که کلید آن را از دزد خریده باشند".

ایشان ابلاغ سیاست های نظام در فضای افتا را از جمله برنامه های راهبردی برای صیانت از اسرار کشور و ایمنی آن در برابر هجمه های دشمن عنوان کرد و ادامه داد: این سیاست ها

کـه در ۹ بنـد بـه آن تأکیـد شـده اسـت تمـامی دسـتگاه هـا و نهادهـای اجرایـی را در جهـت یکپارچگی امنیت فرا می خواند.

وی ایجاد آزمایشگاه ها، حمایت از صنعت داخلی و شرکت های دانش بنیان، ایمن سازی زیر ساخت ها و ممنوعیت خرید خارجی به صورت غیر کنتـرل شـده را از جملـه اقـدام هـای وزارت ارتباطات و فناوری اطلاعات در ارتباط با دفاع سایبری برشمرد.

بنابراین با عملیاتی شدن پروژه شـبکه ملـی اطلاعـات، سـازمان هـای تـأمین کننـده امنیـت کشور در نظر دارند که هر ایرانی، هنگام اتصال به شبکه، علاوه بر شناسه اینترنتی خـود دارای یک شناسه اینترانتی منحصر بـه فـرد نیـز شـده و تمـامی اطلاعـات صـاحب آن شناسـه، بـرای مسئولان امنیتی به سهولت قابل دسترس باشد تا در پیگیری جرایم اینترنتی و امنیتـی بـا مـوانعی نظیر عدم همکاری شرکت های توزیع کننده خارجی در اعلام اطلاعات شخص خاطی روبرو نباشند. از طرف دیگر، در صورت قطع ارتباط ایران با شبکه جهانی اینترنت به هـر دلیلـی (چـه از طرف نهادهای مربوطه داخلی، چه بر اثر حوادث غیر مترقبه بر بسـترهای ارتبـاطی بـا شـبکه جهانی و چه به علت تحریم های خارجی)، ارتباطات درونی کشـور بـا مشـکل مواجـه نشـود. همچنین، به دنبال میزبانی وب سایت های ایرانی در داخل کشـور، نظـارت و کنتـرل محتـوای وب سایت ها هم به سهولت امکان پذیر باشد.

اینترنت ملی و شبکه جهانی اینترنت

قطع ارتباط ایران با شبکه جهانی اینترنت، ضمن این که از بحـث برانگیزتـرین موضـوعات در مقوله شبکه ملی اطلاعات می باشد، بیش از همه، موجبات نگرانی مشترکین فعلی اینترنـت را فراهم کرده است.

آن چنان که در بخشـنامه هـای مختلـف صـادر شـده توسـط وزارت ارتباطـات بـه توزیـع کنندگان اینترنت کشور و همچنین سخنان مسئولان این وزارتخانه مشـهود اسـت، قـرار نیسـت که ارتباط ایران با شبکه جهانی اینترنت قطع شود بلکـه یکـی از اهـداف طـرح اینترنـت ملـی،

فراهم آوردن امکانی است که در صورت قطع احتمالی ارتباط ایران با شبکه جهانی اینترنت، دسترسی به شبکه داخلی اطلاعاتی کشور، به صورت کامل برقرار باشد.

تقی پور، در آیین امضای منشور همکاری بین وزارت ارتباطات و فناوری اطلاعات و اتاق بازرگانی، صنایع و معادن ایران، تأکید کرده است که شبکه ملی اطلاعات، جای اینترنت را نمی گیرد بلکه مکمل آن بوده و بستر اصلی تعاملات دولت الکترونیک می باشد که با راه اندازی آن، مشکل پهنای باند و امنیت فضای مجازی نیز حل خواهد شد.

همچنین ایشان بیان کرد که: "در کنار شبکه ملی اطلاعات، اینترنت را به عنوان یک سرویس به همان شکلی که تاکنون وجود داشته است، کماکان خواهیم داشت و پهنای باند داخل را به صورت امن و حفاظت شده، برای کسب و کار اقتصادی و حریم شخصی خانوارها توسعه خواهیم داد".

وی تلویزیون اینترنتی، ویدئو درخواستی، آموزش از راه دور، دورکاری، سلامت الکترونیکی و تجارت الکترونیکی را از جمله برنامه‌های قابل ارایه بر روی شبکه ملی اینترنت عنوان کرده و افزود: "شبکه ملی اینترنت یا شبکه اطلاعات ملی بر پایه پروتکل اینترنت طراحی شده و یکی از زیر ساخت های اصلی دولت الکترونیک محسوب می شود و پهنای زیاد باند، ارسال تصویر، صوت و حجم زیاد اطلاعات، از ویژگی های این شبکه است".

قابل ذکر است که در ذیل ماده ۴۶ برنامه پنجم توسعه، وزارت ارتباطات در کنار راه اندازی شبکه ملی اطلاعات، مکلّف به افزایش ضریب دسترسی خانوارها به اینترنت و نیز متعاقب آن، افزایش پهنای باند اینترنت بین الملل شده است. بدین صورت که در برنامه پنجم توسعه، وزارت ارتباطات باید:

"امکان دسترسی پرسرعت مبتنی بر توافقنامه سطح خدمات را به صورتی فراهم نماید که تا پایان سال دوم کلیه دستگاه های اجرایی و واحدهای تابعه و وابسته و تا پایان برنامه، ۶۰٪ خانوارها و کلیه کسب و کارها بتوانند به شبکه ملی اطلاعات و اینترنت متصل شوند. میزان پهنای باند اینترنت بین‌الملل و شاخص آمادگی الکترونیک و شاخص توسعه دولت الکترونیک باید به گونه‌ای طراحی شود که سرانه پهنای باند و سایر شاخص های ارتباطات و فناوری اطلاعات در پایان برنامه در رتبه دوم منطقه قرار گیرد".

به عبارت بهتر، برنامه پنجم توسعه علاوه بر این که اشاره ای به جایگزینی شبکه ای به جای اینترنت ندارد، به معنای ایجاد بیش از دوازده میلیون پورت پر سرعت اینترنت در کشور است. بدین ترتیب که قرار است یک شبکه ملی اطلاعات، تدارک دیده شده و بستر امنی برای اشتراک اطلاعات در درون کشور فراهم گردد تا با پیوستن همه ارگان ها به آن، گامی کارساز در راه رسیدن به دولت الکترونیک در کشور برداشته شود. گامی بزرگ که قرار است کشورمان را در سال ۱۳۹۵ (سال پایانی برنامه پنجم توسعه) به جایگاه دومی منطقه برساند.

مشکلات و موانع فراروی پروژه اینترنت ملی

یکی از مهمترین مشکلات و موانع ایجاد شبکه ملی اطلاعات را می توان عدم وجود دیتا سنتر عظیم داخلی جهت میزبانی تمام وب سایت های ایرانی دانست که به دلیل هزینه های بالا و محدودیت منابع از یک سو و شرایط تحریمی در جهت خرید سرورهای مورد نیاز و همچنین نبود تخصص کافی نسبت به تأمین امنیت آن، عملاً راه اندازی آن دور از ذهن است. چنان چه در حال حاضر، به دلیل همین محدودیت ها، حتی سایت برخی از بانک ها مانند بانک پارسیان و بعضی از خبرگزاری های دولتی هم بر روی سرور های خارجی میزبانی می شوند.

تقی پور، ضمن اعتراف به موفق نبودن در زمینه تولید تجهیزات و سخت افزار در داخل کشور، می گوید: "بدون هیچ سابقه فنی، چگونه می توانیم وارد بازار فناوری های نوین شویم که توسط چند کمپانی بزرگ تسخیر شده است".

مسئله مهم دیگر، عدم وجود DNS سرور یا به عبارتی صحیح تر root سرور مناسب جهت راهنمایی مرورگرها در شبکه ملی اطلاعات به سمت سرورهای مقصد است.

هم اکنون در دنیا سیزده root سرور وجود دارد که ۹ تا از آن ها در ایالات متحده قرار دارد. برای مثال، ICANN که در واقع پایگاه اطلاعاتی اصلی آدرس های عمومی ثبت شده در شبکه جهانی اینترنت بوده و سایر DNS سرورها یا به اصطلاح Mirror ها از آن تغذیه اطلاعاتی می شوند، از معروف ترین آن ها است.

یکی از ابهام هایی که تا کنون مسئولان وزارت ارتباطات و فناوری اطلاعات به آن پاسخ روشنی نداده اند، جایگزین مناسب برای این root سرورها است. زیرا به دلیل شرایط تحریمی ایران، اخذ مجوز و دسترسی احداث حتی یک Mirror در داخل کشور نیز دور از تصور است.

با این وجود، اخیراً وزارت ارتباطات و فناوری اطلاعات با بخشنامه طرح جداسازی اینترنت از اینترانت که به شرکت های توزیع کننده اینترنت در کشور ابلاغ شد، این گونه پاسخ به این ابهام را به آینده موکول کرده است که: مراکز ارایه‌دهنده خدمات میزبانی داخلی باید نام دامنه‌های سایت‌های میزبانی‌شده به آدرس‌های عددی خصوصی اینترنتی متناظر با آنها را صرفاً از طریق سرورهای DNS که در آینده توسط سازمان فناوری اطلاعات ایران اعلام خواهد شد، تبدیل کنند.

مشکل و مانع مهم دیگر را می توان این گونه بیان کرد که بنابر شواهد، قرار است در طرح اینترنت ملی به هر کاربر دو آدرس IP یکی برای اتصال به شبکه جهانی اینترنت و دیگری برای اتصال به شبکه کشوری اینترانت اختصاص داده شود که آدرس IP معتبر برای اینترنت و آدرس IP نامعتبر[1] برای اینترانت کشوری استفاده می‌شود. پیرو آن، تمامی توزیع کنندگان اینترنت می باید تغییرات عمده‌ای در سیستم‌های صورتحساب‌گیری و سایر نرم‌افزارهای ارتباط با مشتری خود اعمال کنند که این امر، علاوه بر صرف هزینه‌های زیاد، مستلزم زمان کافی است، چرا که با اختصاص دو IP به هر کاربر، باید تمام ظرفیت‌های موجود هم تا دو برابر افزایش یابد.

در عین حال، با اصرار مسئولان وزارت ارتباطات بر اعمال تنظیمات در لایه دسترسی، همه مودم‌های سمت مشترکان نیز باید تعویض شود که هزینه جدیدی را به کاربران تحمیل می‌کند. این موضوع در حال حاضر به شدت موجب اختلاف میان شرکت های توزیع کننده اینترنت و وزارت ارتباطات و فناوری اطلاعات شده است به صورتی که شانه ساز زاده، از اعضای هیأت مدیره سازمان نظام صنفی رایانه‌ای کشور، می گوید: "به وزارت ارتباطات و فناوری اطلاعات پیشنهاد داده‌ایم این تغییرات در دیتا سنترهای شرکت‌های تأمین‌کننده پهنای

[1] Invalid

باند صورت گیرد اما آن ها به دنبال این هستند تا این طرح بر روی مودم مشترکان اجرا شود". اضافه بر این، در مواردی همچون اتصال تلفن های همراه به اینترنت، حتی پیاده سازی این موضوع در لایه دسترسی، از لحاظ تئوریک هم محل ابهام است.

یکی دیگر از موانع بر سر راه پروژه اینترنت ملی، سرویس جستجوگر ملی و ایمیل ملی است. جستجوگری که بتواند تمامی وب سایت های میزبانی شده در داخل کشور را پایش کرده و جوابگوی نیازهای کاربران در جستجوی اطلاعات خاص باشد و از طرف دیگر، نیاز به یک ایمیل داخلی است که بتواند در صورت قطع ارتباط ایران با شبکه جهانی اینترنت، قابل سرویس دهی به کاربران ایرانی باشد.

در سال های اخیر، طرح های مختلفی برای اجرای این دو سرویس، توسط وزارت ارتباطات و فناوری اطلاعات مورد بررسی قرار گرفته و در بعضی از موارد هم به صورت جزیی تا حدودی به مرحله اجرا درآمده است که در نتیجه تمامی آن تلاش های نافرجام، عدم امکان عملیاتی راه اندازی این سرویس ها به صورت متمرکز در داخل کشور، بیش از پیش نمایان شده است.

سازمان فناوری اطلاعات در فراخوانی تحت عنوان مشارکت در فجر (فراهم‌سازی جویشگر رایانه‌ای) و فخر (فراهم‌سازی خدمات رایانامه‌ای) از همه شرکت های فعال در حوزه فناوری اطلاعات دعوت به همکاری نمود تا شاید بتواند با بهره گیری از ظرفیت و تخصص شرکت های خصوصی، این سرویس ها را در داخل کشور راه اندازی نماید. حال آن که در نگاهی کلی، اطمینان به شرکت های خصوصی در جهت تأمین امنیت اطلاعات محرمانه و شخصی کاربران نظیر اطلاعات حساب های بانکی و ... قطعاً ابهام بزرگی را در جهت استفاده از این گونه سرویس ها برای کاربران فراهم می کند تا جایی که حتی در صورت عملیاتی شدن، نمی توان اقبال عمومی و بهره گیری از این سرویس ها را انتظار داشت.

جمع بندی و نتیجه گیری

حقیقت آن است که در جمع بندی های فنی کارشناسان و صاحب نظران حوزه فناوری اطلاعات، با در نظر گرفتن حجم بزرگ شبکه اتصال کشور و همچنین تحریم ها و

محدودیت منابع موجود و علی الخصوص، فقدان تخصص و دانش کافی، امید به اجرای موفق پروژه ای تحت عنوان اینترنت ملی، دور از تصور است.

به هرحال، قضاوت در خصوص پروژه شبکه ملی اطلاعات را بهتر است به گذشت زمان سپرد اما با توجه به وضعیت موجود و به دلیل منابع میلیاردی اختصاص داده شده برای اجرای این پروژه از محل بودجه کشوری، وزارت ارتباطات و فناوری اطلاعات مکلّف است هر از چندگاهی از جهت گزارش عملکرد و پیشرفت آن، یک فاز آزمایشی از این پروژه را افتتاح نماید. امسال نیز به همین منوال، از دهه مبارک فجر، قرار است با تغییرات آزمون و خطایی در شبکه داخلی کشور که به موجب آن چند روزی است اختلالات وسیعی در ارتباط کاربران با شبکه جهانی اینترنت مشاهده می شود، فازی دیگر از پروژه شبکه ملی اطلاعات آغاز گردد.

۱۸

گوگل کروم، سیستم عامل اینترنت

در ماه های اخیر، شرکت گوگل تصاویر اسکرین شات همراه با توضیحات بسیار مختصری از نخستین پلت فرم رایانه ای خود با نام "گوگل کروم" را منتشر کرده است. این پلت فرم، علاوه بر ظاهر گرافیکی و کاربر پسندانه خوب، یک سیستم عامل کد باز و سبک بر اساس لینوکس بوده که ابتدا نت بوک ها را هدف قرار داده است.

گوگل کروم که در واقع آن را "سیستم عامل اینترنت" می توان نامید، سیستم عاملی بر مبنای مرورگر کروم است که برای کاربرانی طراحی شده که بیشتر زمان خود را در وب می گذرانند. سرعت، سادگی و امنیت از مهمترین ویژگی های این پلت فرم به شمار رفته و قابلیت کدباز بودن آن، به برنامه نویسان امکان می دهد تا در جهت توسعه و گسترش هرچه بیشتر سیستم عامل گام بردارند.

معماری و سخت افزار:

معماری سیستم عامل گوگل کروم بسیار ساده و مبتنی بر مرورگر است و تمام برنامه ها، اسناد و تنظیمات به صورت مطمئن در وب ذخیره می شود. بنابراین حتی اگر شخصی رایانه خود را هم از دست بدهد، با یک نوت بوک کروم دیگر می تواند دوباره به اطلاعات خویش دسترسی داشته باشد.

تمام نرم افزارهای تحت وب، روی این سیستم عامل قابل اجرا بوده و ابزار توسعه آن نیز همان نرم افزارهای طراحی صفحات وب می باشد. از مهمترین ویژگی های برنامه های تحت وب، می توان به قابلیت انعطاف پذیری بیشتر نسبت به برنامه های بسیار انعطاف ناپذیر و استاتیک ویندوزی، محیط کاربری ساده و آسان، همیشه آنلاین و در دسترس بدون و

همچنین بی نیاز از به روز رسانی مداوم اشاره کرد که کاربران را فارغ از محل و زمان نموده و اجازه دسترسی به اطلاعات را با هر اتصال به اینترنت و از هر کامپیوتری می دهد. گوگل کروم به کاربران امکان می دهد تا همه برنامه های مورد نیاز خود را از فروشگاه وب سایت برنامه ها به صورت آنلاین دریافت کرده و از طریق نوار آدرس بار، بدون نیاز به cd نصب نمایند.

در نوت بوک های مبتنی بر پلت فرم گوگل کروم، کاربران با سیستم wi-fi و از طریق شبکه بی سیم شرکت مخابراتی ورایزون آمریکا به اینترنت متصل شده و از 100 MB تبادل اطلاعات رایگان در هر ماه به مدت دو سال برخوردار می باشند که برای انجام کارهای روزانه و چک کردن صدها نامه الکترونیک کافی بوده که با پرداخت مبالغ اندکی، قابل افزایش هم می باشد.

گوگل کروم نیاز به ویژگی های سخت افزاری خاصی نداشته و از HTML5 ، CSS و JavaScript برای پشتیبانی از برنامه های کاربردی پیچیده برخوردار است. این سیستم عامل فقط برای رایانه های با صفحه کلید فیزیکی ساخته شده و خاصیت لمسی نیز نخواهد داشت.

رابط کاربری:

رابط کاربری گوگل کروم، بسیار مختصر و مشابه مرورگر کروم است. بنابراین این سیستم عامل، شباهت زیادی به محیط وب داشته و بیشتر شبیه مرورگر است تا یک سیستم عامل واقعی.

مهمترین اهدافی که برای رابط کاربری سیستم عامل گوگل کروم علاوه بر کاربر پسند بودن آن در نظر گرفته شده، عبارتند از مشاهده همه برنامه ها و صفحات وب در زبانه های جداگانه و در کنار هم برای استفاده کمتر از فضای صفحه نمایش، دسترسی راحت به برنامه های چت و پخش موسیقی، نمایش تمام صفحه نرم افزارها، امکان تقسیم صفحه نمایش به دو

قسمت در گوشه ها و همچنین دسترسی آسان به برنامه های کاربردی با استفاده از زبانه های مرورگر.

سرعت:

گوگل کروم حدود ۱۰ ثانیه راه اندازی شده و وب سایت های مورد علاقه کاربران را با پشتیبانی کامل از آخرین استانداردهای وب، به سرعت بارگذاری و اجرا می نماید.

این سیستم عامل طوری طراحی شده تا بسیار سریع و سبک، راه اندازی شده و در کمترین زمان ممکن کاربر را به اینترنت متصل کند و در این میان، زمانی برای راه اندازی سیستم عامل تلف نشود. گوگل کروم، همواره مانند روز اول کار کرده و در طول زمان، سرعت خود را از دست نمی دهد. به همین خاطر، نوت بوک های مبتنی بر این پلت فرم را می توان بیشتر شبیه تلویزیون دانست که به محض روشن کردن، کمتر از چند ثانیه راه اندازی می شود.

در سیستم عامل گوگل کروم، پس از برقراری ارتباط با اینترنت، به صورت فوری تمام برنامه ها، بوک مارک ها و دیگر تنظیمات مرورگرها که کاربر قبلاً انجام داده، بر روی صفحه نمایان می شود و تنظیم سیستم، کمتر از یک دقیقه زمان خواهد برد. گوگل در این سیستم عامل، دسترسی سریع به وب، سریع مرور وب و مهمتر از همه، سرعت در عملکرد را مد نظر قرار داده است.

امنیت:

گوگل در خصوص امنیت این سیستم عامل بسیار محکم و قاطع است و از لحاظ امنیتی، آن را سیستم عاملی "سخت" در برابر نفوذگران می داند که در طراحی آن از فناوری های

پیشرفته ای برای جلوگیری از دسترسی تروجان ها، ویروس ها و کدهای مخرب بـه اطلاعـات کاربران، استفاده شده است.

صفحات وب آلوده و برنامـه هـای مخـرب همچـون تروجـان هـا مـی تواننـد از نقـص در مرورگرها سوء استفاده کرده و منجـر بـه سـرقت رمزهـای عبـور، اطلاعـات شخصـی و مـالی کاربران شود. در گوگل کروم برای کاهش این خطـر، برنامـه هـا و هـر صـفحه وب در یـک محیط محدود به نام "sandbox" اجرا می شود. بنابراین اگر کاربر یـک صـفحه وب آلـوده را مشاهده کند، کدهای مخرب نمی تواند در زبانـه هـا، برنامـه هـا یـا هـر چیـز دیگـری روی کامپیوتر شخص اثر بگذارد. حتی اگر نرم افزارهای مخرب موفق به گذر از محدوده حفـاظتی sandbox شوند، هر بار که رایانه راه اندازی می شود، سیستم عامل یک کنترل خودکـار راه اندازی تأیید شده را انجام داده و اگر تشخیص دهد که سیستم به طریقی دستکاری یـا خـراب شده است، خودش آن را تعمیر می کند.

این سیستم عامل همچنین از به روز رسانی خودکار بهره مند است که مـؤثرترین راه بـرای محافظت از سیستم در برابر برنامه های مخرب به شـمار مـی رود. همـواره همـه نـرم افزارهـای رایانه، به روز شده و آخرین وصله های امنیتی را دارند. ویژگی های به روزرسانی خودکـار و sandbox، قرارگرفتن در معرض نرم افزارهای مخـرب را بـه شـدت کـاهش داده و همیشـه جدیدترین و امن ترین نسخه های برنامه ها را اجرا می نمایند.

هنگام استفاده از برنامه های مبتنی بر وب در سیسـتم عامـل گوگـل کـروم، همـه اسـناد بـا خیال راحت در وب ذخیره می شود، اما انواع خاصی از فایل ها، مانند بارگذاری هـا، کـوکی ها و فایل های حافظه موقت مرورگر، ممکن است در رایانه موجـود باشـد کـه گوگـل کـروم همه این اطلاعات را با استفاده از روش های خاصی، رمزگذاری نموده و دسترسی به آن ها را بسیار دشوار می سازد.

حساب کاربری مهمان که در تمامی سیستم عامل ها موجـود اسـت، در گوگـل کـروم بـه گونه ای خاص تعریف شده است به نحوی که در این حالت، دوستان کاربر با استفاده از نوت بوک وی، آزادانه از وب استفاده می کنند ولی نمی توانند به نامه هـای الکترونیـک یـا دیگـر

اطلاعات کاربر دسترسی داشته باشند و زمانی هم که ارتباط اینترنتی آن ها قطع شود، همه اطلاعات مربوط به مشاهده های آن ها در وب، به طور دائم از رایانه پاک می شود.

گوگل کروم اقدام های احتیاطی دیگری نیز برای حفاظت از اطلاعات کاربران در نظر گرفته است. بدین صورت که با استفاده از اصل "دفاع در عمق"، چند لایه حفاظتی در سیستم فراهم کرده که اگر نفوذگر بتواند از هر یک از لایه ها عبور کند، هنوز لایه های حفاظتی دیگر، مؤثر بوده و می توانند به خوبی از اطلاعات محافظت نمایند.

ذخیره سازی:

یکی دیگر از ویژگی های مهم گوگل کروم، روش ذخیره سازی آن است. این سیستم عامل، اطلاعات را فقط در حافظه موقت، آن هم برای افزایش سرعت فعالیت ها نگهداری نموده و در نهایت تمامی اسناد را در وب ذخیره می نماید. بنابراین، کاربران می توانند آنلاین به همه اطلاعات خویش، در هر زمان و مکانی دسترسی داشته باشند.

به هر حال، در همه اجزای گوگل کروم، سرعت و راحتی کاربر مد نظر است و در نوت بوک های ارزان قیمتی هم که با این سیستم عامل عرضه می شوند همه فعالیت ها در محیط وب انجام شده و فضای زیادی برای ذخیره سازی روی سیستم در نظر گرفته نشده است.

۱۹

اینترنت، فیلترینگ و بازی با پورت ها

مقام معظم رهبری حضرت آیت الله العظمی خامنه ای دامت برکاته، در سال ۱۳۸۰ خطاب به شورای انقلاب فرهنگی در دیدار با اعضای این شورا، وضعیت اینترنت را در کشور "نابسامان" عنوان کرده و ضمن هشدار، بحث کنترل و پالایش پایگاه های مخرب و لزوم برخورد با تخلفات اینترنتی را در رأس اولویت های فرهنگی دانستند و حتی برای انجام این کار، مهلت یک ماهه هم مقرر فرمودند.

همچنین، ایشان در جلسه پرسش و پاسخ دانشجویان دانشگاه شهید بهشتی در تاریخ ۱۳۸۲/۲/۲۲، فرمودند: "در همه جای دنیا، وقتی جهاز عظیم و فراگیر اینترنت وارد می شود، معمولاً فیلترهایی هم وجود دارد که هر کشور به فراخور تمایلات و تفکرات و مصالحی که دارد، آن ها را کار می گذارد، این یک امر طبیعی است. در این جا هم، در آغاز کار، مقداری بی توجهی شد، لیکن بعد اقداماتی کردند و باید بکنند، این درست است. البته که باید فیلترهای مناسب و لازم را بگذارند".

با توجه به اهمیت بحث فلیترینگ از دیدگاه مقام معظم رهبری، مسئولان کشور تلاش نموده اند تا با بهره گیری از روش های گوناگون و اتخاذ تمهیدات و نظارت دقیق، به این خواسته مهم تحقق بخشند. بر این اساس، در ماده ۲۱ و ۲۲ قانون جرایم رایانه ای، قوانینی برای بحث فیلترینگ مطرح شد که ارایه دهندگان خدمات دسترسی اینترنت، موظف هستند این قوانین را رعایت کنند.

اما، با وجود همه این تلاش ها، در روزهای اخیر، بسیاری از کاربران اینترنت داخل کشور برای گذشتن از سد فیلترینگ مخابرات، به سراغ نرم‌افزارهای فیلترشکن، سایت‌های پروکسی

و همچنین VPN [1] رفته و این رجوع کاربران به استفاده از این روش‌های عبور از فیلترینگ، باعث رشد فزاینده فروش اکانت‌های نرم‌افزارهای فیلترشکن و VPN شده است.

در این میان، مخابرات هم گاهی اوقات با بستن همه پورت های VPN همراه با برخی پورت های دیگر مانند SSL، اقدام به ایجاد فیلترینگ برای این دسته از کاربران می نماید. اگر چه اطلاعات تبادل شده توسط VPN، از طریق ارتباط امن SSL صورت می گیرد و به جز خود کاربر و رایانه سرور، هیچ فرد دیگری به آن اطلاعات دسترسی ندارد ولی به علت رمزنگاری، رمزگشایی و بازرسی محتویات هر بسته، این سرویس عملکرد کندی دارد.

بنابراین، با توجه به بسته شدن پورت های VPN در بعضی از روزها، اکانت های HTTPS [2] و SOCKS از محبوبیت قابل توجهی در بین کاربران برخوردار شده اند. این دو اکانت، نوعی سرویس Secure Tunnel هستند که تقریباً کار VPN را انجام می دهند، البته با ضریب امنیتی بالاتر و سرعت بهتر.

SOCKS یک پروتکل اینترنتی امنیتی است که در لایه ی نشست شبکه ارتباطی عمل می کند و دو نسخه دارد که هرکدام ویژگی های خود را دارند: SOCKS v4 و SOCKS v5. البته نسخه ی ۵ آن پیشرفته تر و کامل تر است و مرورگر اُپرا مینی هم که در بعضی از کامپیوترها و تلفن های همراه نصب گردیده، با استفاده از همین پروتکل، می تواند از فیلترینگ عبور کند.

از مهمترین مزایای اکانت های HTTPS و SOCKS علاوه بر تغییر هویت کاربران به آن کشوری که می خواهند [3]، می توان به امنیت بالا که معمولاً با نصب فایروال های سخت افزاری در سمت سرور و رمزگذاری داده ها تأمین می شود، سازگاری کامل با انواع سیستم عامل ها (Windows 32 & 64 Bit – Mac – Ipad – Android – Linux -

[1] Virtual Private Network (VPN)

[2] Hypertext Transfer Protocol Secure (HTTPS)

[3] Ip Dynamic

Iphone)، بدون محدودیت در سرعت، زمان و پهنای باند، کیفیت و پایداری بالا، پشتیبانی از تمام سرویس های اینترنتی (همراه اول، ADSL، Wireless، Wimax، GPRS و ...)، امکان تبادلات مالی با تمام وب سایت های تجارت الکترونیک (E-Gold، Paypal و ...)، سازگار با وب سایت های ارتباط جمعی (Orkut، Gazzag)، جلوگیری از شنود و پیگیری اطلاعات محرمانه کاربران، دور زدن تحریم هایی که برای کاربران ایرانی در اینترنت اعمال شده، امکان به روز رسانی ویندوز و ضد ویروس ها، دسترسی به وب سایت های اینترنتی فیلتر شده و قابلیت اجرا بر روی تلفن همراه را علاوه بر ایمنی ارتباطات و معاملات تجاری آنلاین آن، برشمرد.

در صورت بستن پورت SSL، سایت هایی که با این پروتکل امن، رمزگذاری داده ها را انجام می دهند همچون بانک ها و مؤسسات مالی و اعتباری، خدمات الکترونیک آن ها قابل دسترس نمی باشد. همچنین، سرویس های ایمیل Gmail و Yahoo نیز به دلیل استفاده از پروتکل SSL، در صورت مسدود شدن این پورت، غیر قابل استفاده می شوند. در صورت بستن پورت SSL، عملاً بخشی از اینترنت، با مشکل دسترسی مواجه می شود. البته بعضی از سایت ها مانند Facebook دو نسخه HTTP و HTTPS دارند که در این هنگام، نسخه HTTP آن ها قابل مشاهده می باشد. در این مواقع، استفاده از پراکسی HTTPS هم برای مشاهده این وب سایت ها، کاربردی ندارد.

معمولاً از HTTPS برای تراکنش های پرداخت آنلاین و همچنین تراکنش های حساس سامانه های اطلاعات سازمانی استفاده می شود. لازم به ذکر است که HTTPS را نباید با پروتکل انتقال ابر متن امن[1] که در RFC 2660 مشخص شده است و غیر قابل فیلتر شدن می باشد، اشتباه گرفت. گاهی وقت ها، محدودیت های فیلترینگ شامل پورت های SOCKS و SSH در داخل کشور نیز می شود.

[1] S-HTTP

در بعضی از روزها نیز، محدودیت پورت PPTP[1] بعد از ساعت اداری اعمال گردید که کاربران، قبل از ساعت اداری، با استفاده از این پورت و بعد از آن، با استفاده از پورت L2TP اقدام به عبور از فلیترینگ می نمودند.

پورت PPTP برای ساخت شبکه‌های خصوصی مجازی (VPN) مورد استفاده قرار می‌گیرد و نیاز به هیچ گونه تنظیمی نداشته و در تمامی ویندوزها قابل استفاده است. مسدود کردن این پورت امکان استفاده از VPN ها را غیر ممکن می‌کند که با بروز خطای ۸۰۰، ۸۰۶ و ۶۸۷ در هنگام اتصال به وب، می توان از این موضوع آگاه شد. L2PT[2] و SSTP[3] نیز کاربرد مشابهی دارد.

پورت SSTP هم که ترکیبی از پروتکل HTTP و SSL/TLS است، بعضی وقت ها شامل این محدودیت شده و مخابرات برای کم کردن سرعت SSTP، کل پورت 443 را که مربوط به آدرس های HTTPS است، محدود می کند که به این مسئله، با چک کردن ایمیل ها در Gmail (بدون استفاده از VPN) می توان پی برد. البته باید توجه داشت SSTP که از پروتکل های جدید و امن مایکروسافت می باشد، فقط در ویندوزهای 7 و Vista قابل استفاده است. هدف این پروتکل، فراهم آوردن ارتباطات رمز شده و شناسایی امن یک کارگزار وب است. برای اتصال به این پورت، نیاز به تنظیم خاصی نبوده و فقط باید تاریخ کامپیوتر به روز باشد.

گاهی اوقات نیز، عدم آشنایی با تنظیمات پورت ها در فایروال ویندوز و ضد ویروس های نصب شده در سیستم، مشکلی جدی برای کاربران مبتدی در عبور از فیلترینگ بود.

---

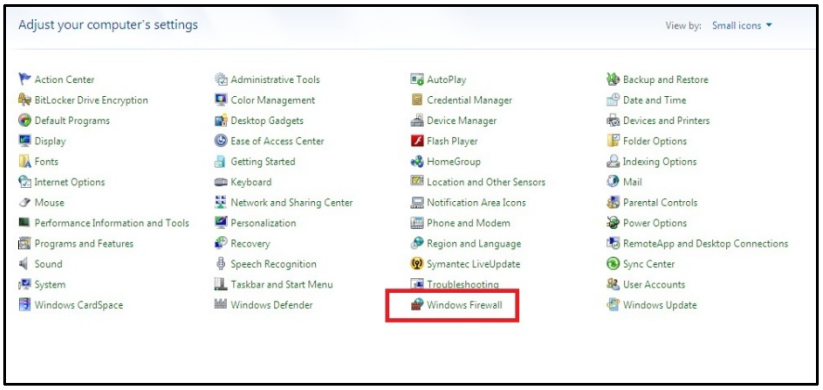
[1] Point-to-Point Tunneling ProtocoL (PPTP)
[2] Layer 2 Tunneling Protocol (L2PT)
[3] Secure Socket Tunneling Protocol (SSTP)

رمزنگاری اطلاعات در سازمان با IPsec

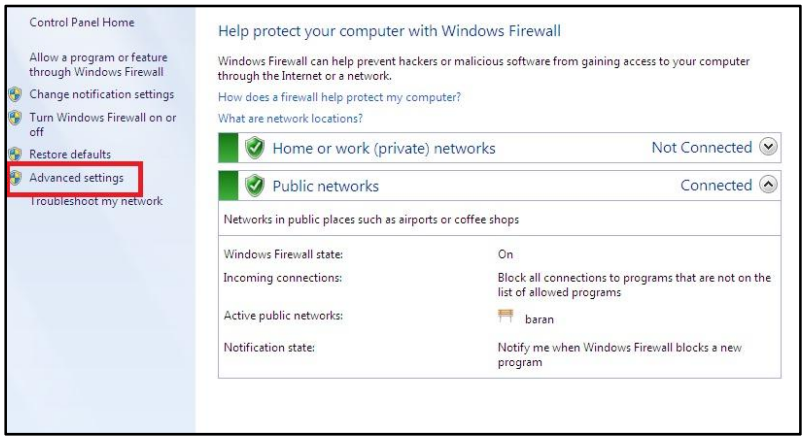
امروزه با رشد سریع تکنولوژی های اطلاعات و ارتباطات و آسیب پذیری هایی که از این رهگذر، جوامع بشری را تهدید می کند، حفاظت و نگهداری از اطلاعات، امری بسیار مهم است که باید توجه زیادی به آن نمود.

معمولاً، اطلاعاتی که بین سیستم ها در یک شبکه منتقل می شود، اگر به صورت صحیح رمزگذاری نشود، به راحتی توسط نفوذگران، قابل شنود بوده و با توجه به حساسیت اطلاعات، ممکن است قشر گسترده ای از کاربران را تحت تأثیر عوامل مخرب ناشی از دسترسی غیر مجاز به آن ها قرار دهد. بنابراین، در این مقاله سعی می شود تا با آموزش تنظیمات IPsec که اعمال آن، نقش مهمی در رمزنگاری اطلاعات در حال تبادل دارد، گام ارزنده ای در خصوص تأمین امنیت اطلاعات برداشته شود.

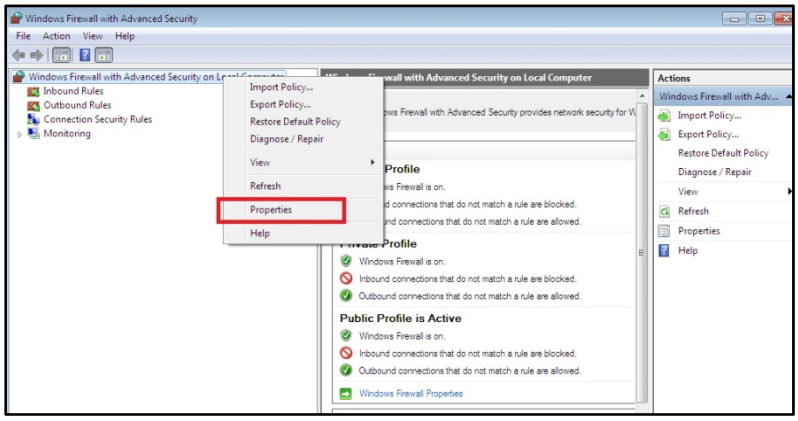
ابتدا از طریق Control Panel ویندوز، وارد قسمت Windows Firewall می شویم:



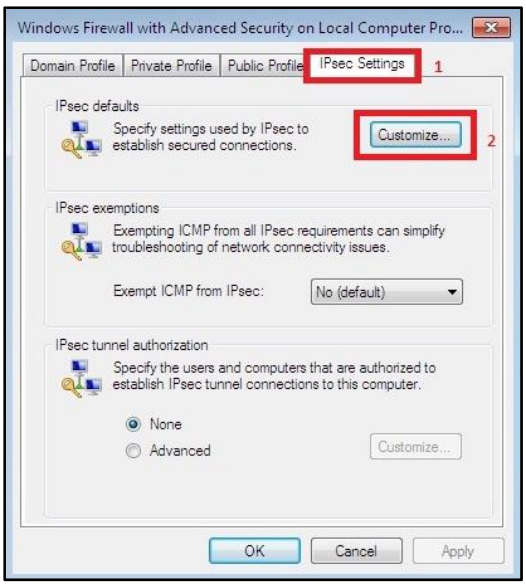
سپس بر روی گزینه Advanced Settings از منوهای سمت چپ صفحه کلیک می نماییم:



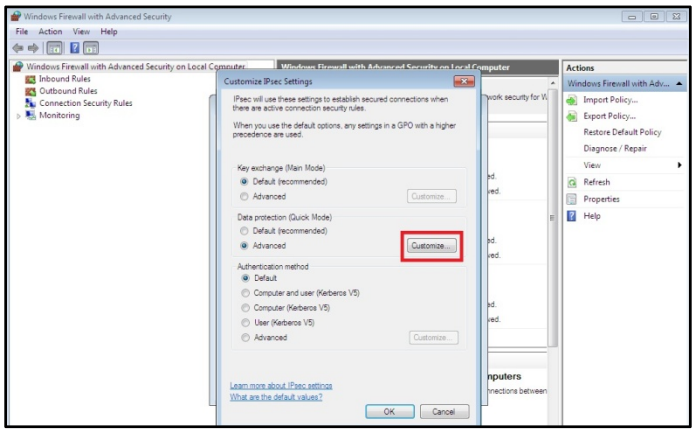
آنگاه بر روی گزینه Windows Firewall with on Local Computer Advanced Security راست کلیک نموده و Properties را انتخاب می کنیم:



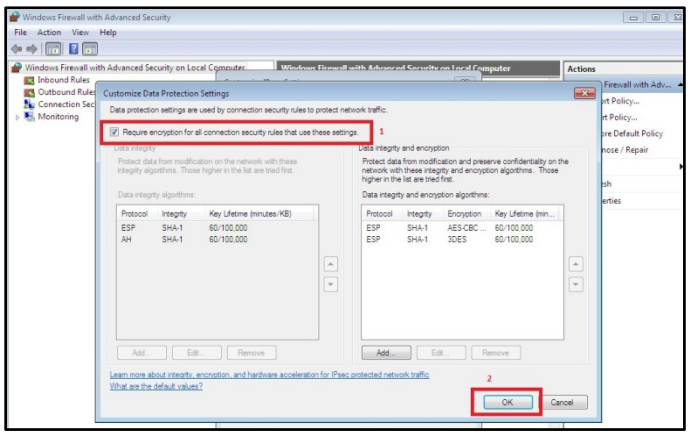
در داخل پنجره Windows Firewall with on Local Computer Advanced Security گزینه IPsec Settings را انتخاب کرده و در قسمت IPsec defaults بر روی دکمه Customize کلیک می نماییم:



از درون پنجره Customize IPsec Settings در قسمت Data protection (Quick Mode) گزینه Advanced را انتخاب کرده و بر روی دکمه Customize مقابل آن، کلیک می کنیم:



در قسمت Customize Data Protection Settings گزینه Require encryption for all connection security rules that use these settings را انتخاب می کنیم:



لازم به ذکر است که برای رمزنگاری اطلاعات، به صورت پیش فرض از الگوریتم کد گذاری استاندارد AES-128 استفاده می شود که اگر سرویس گیرنده[1] یا سرویس دهنده[2] این سطح از رمزگذاری را پشتیبانی نکند، از الگوریتم 3DES استفاده می گردد.

سپس بر روی OK کلیک می نماییم. بدینوسیله IPsec پیش فرض ویندوز، جهت رمزگذاری داده ها ایجاد می شود که این امر می تواند به امنیت تبادل اطلاعات داخلی در سازمان ها کمک به سزایی نماید.

---

[1] Client
[2] Server

۲۱

VPN، روشی جدید برای سرقت اطلاعات

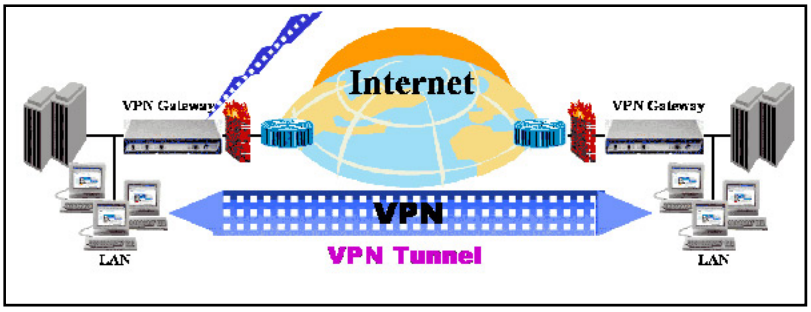
در روزهای اخیر، استفاده گسترده کاربران از سرویس VPN به دلیل اختلالات موجود در اینترنت و همچنین عبور از سد فیلترینگ کشور، مشکلات فراوانی را برای استفاده کنندگان در پی داشته است.

رشد فزاینده فروش اکانت های VPN و نرم افزارهای فیلترشکن که با قیمت های بسیار نازل و حتی تست های چند روزه رایگان، عرضه می شود، تهدیدات بی شماری را متوجه رایانه های کشورمان نموده است و باعث شده تا کاربران به دلیل عدم آگاهی، بخش عظیمی از اطلاعات درون کشور را در اختیار کشورهای بیگانه قرار دهند.

متأسفانه، بیشتر سرورهایی که اشتراک VPN را در اختیار کاربران قرار می‌دهند، نه تنها تمامی اطلاعات رد و بدل شده را بررسی می کنند، بلکه توسط پورت‌های باز رایانه کاربر، به اطلاعات درون رایانه وی نیز دسترسی داشته و با استفاده از نرم افزارهای پیشرفته، بدون اطلاع کاربر، اقدام به کپی‌برداری یا دیدن اطلاعات داخلی رایانه وی می کنند. این موضوع، زمانی که کاربر از طریق رایانه محل کار، اقدام به برقراری ارتباط VPN می کند، از اهمیت دو چندانی برخوردار است چرا که موجب دسترسی به اطلاعات سازمان می گردد.

کاربر، با استفاده از سرویس VPN و یا نرم‌افزارهای فیلترشکن، به یک سرور در خارج از کشور که معمولاً در کشورهای آمریکا و انگلیس مستقر هستند، متصل می شود. این اتصال از هر نقطه دنیا، موجب اختصاص یک آدرس IP خارجی به رایانه کاربر شده و موقعیت مکانی وی را به آن کشور تغییر داده و در اینترنت، به عنوان کاربری از آن کشور شناخته می شود. پس از برقراری ارتباط، کاربر توسط سرور خارجی، وارد اینترنت شده و بدین وسیله، از فیلترینگ داخلی کشور یا تحریم های خارجی عبور می کند.

اگر چه اطلاعات تبادل شده توسط VPN، از طریق ارتباط امن SSL صورت می گیرد و به جز خود کاربر و رایانه سرور، هیچ فرد دیگری به آن اطلاعات دسترسی ندارد ولی به علت رمزنگاری، رمزگشایی و بازرسی محتویات هر بسته، این سرویس گاهی اوقات عملکرد کندی دارد.



علاوه بر این، گرایش به سوی سرویس VPN، تلاش عده زیادی از کلاهبرداران اینترنتی را نیز در بر داشته است تا با فریب کاربران به نصب نرم افزارهای مخرب که اغلب Trojan یا key logger هستند، در قالب برنامه های VPN، به دزدیدن اطلاعات نام کاربری، کلمه عبور افراد و همچنین اطلاعات محرمانه آن ها اقدام نمایند.

اگر چه به گفته رضا باقری اصل، مدیر دفتر مطالعات فناوری های نوین مرکز پژوهش های مجلس، "VPN غیر قانونی نیست و در قانون جرایم رایانه ای هیچ ماده ای مبنی بر این که پروتکل VPN غیر قانونی است، وجود ندارد" و به طور مثال، بانک ها و مؤسسات مالی از این پروتکل برای تبادل اطلاعاتشان استفاده می کنند چرا که از امنیت بالاتری برخوردار است، اما به کاربران توصیه می شود که همچنان تدابیر امنیتی را برای حفظ حریم خصوصی خویش به کار گیرند.

۲۲

شرحی بر آسیب پذیریWebkit

در تاریخ ۱۶ شهریورماه ۱۳۸۹[1] یک آسیب پذیری مهم در نرم افزار Webkit شناسایی گردید که به مهاجم اجازه می دهد تا کدهای مخرب خودش را درون برنامه در حال اجرای کاربر، اجرا نماید. این آسیب پذیری که از راه دور قابل اجرا است ، در صورت عدم موفقیت، منجر به شرایط انکار سرویس[2] بر روی سیستم هدف خواهد شد.

نرم افزار WebKit

WebKit یک موتور جاوا اسکریپت است که برای پردازش کدهای جاوا اسکریپت موجود در صفحات وب پویا استفاده می شود. موتورهای جاوا به کاربر اجازه می دهد که بدون ارتباط با سرور، عملیاتی را روی آن صفحه انجام داده و یا در صورت اعمال تغییر کوچکی در صفحه مورد نظر، کل صفحه را دوباره بارگذاری نکند.

WebKit از دو قسمت تشکیل شده که یکی از این قسمت ها به عنوان موتور جاوا اسکریپت مورد استفاده قرار گرفته و از قسمت دیگر برای پردازش اِلمان های گرافیکی صفحات استفاده می شود. این نرم افزار، محصول شرکت اپل و یک پروژه کد باز است که به علت سرعت بالایی که در بارگذاری صفحات وب دارد، امروزه به عنوان یکی از مهمترین موتورهای مرورگرها شناخته می شود.

---

[1] September 7, 2010

[2] Denial-of-Service (DoS)

لازم به ذکر است که اولین موتور جاوا اسکریپت توسط شرکت نت اسکیپ برای مرورگر نت اسکیپ نوشته شد و سپس با توجه به گستردگی مرورگرها، موتورهای دیگری همچون SpiderMonkey فایرفاکس، V8 گوگل کروم، WebKit سافاری، Presto اُپرا و موتور Trident برای اینترنت اکسپلورر هم تولید شد.

سیستم های آسیب پذیر:

آسیب پذیری Webkit Floating Point Datatype علاوه بر تحت تأثیر قرار دادن نسخه های مختلف نرم افزارهای Apple Safari 4 ~ 5.0.1 ، Apple iOS 3.2 ~ 4.2 ، Apple iPad ~ 3.2.2 ، Apple iPod Touch 2.1 ~ 3.1.3 ، در مدل های iPhone زیر نیز تأثیرگذار است:

- Apple iPhone 2.0
- Apple iPhone 2.0.1
- Apple iPhone 2.0.2
- Apple iPhone 2.1
- Apple iPhone 2.2
- Apple iPhone 2.2.1
- Apple iPhone 3.0
- Apple iPhone 3.0.1
- Apple iPhone 3.1
- Apple iPhone 3.1.2
- Apple iPhone 3.1.3
- Apple iPhone 3.2
- Apple iPhone 3.2.1
- Apple iPhone 4.0
- Apple iPhone 4.0.1
- Apple iPhone 4.1

پیشنهاد:

برای کاهش خطر این آسیب پذیری، توصیه می شود که اجرای کدهای جاوا اسکریپت یا محتوای فعال را در مرورگر وب سافاری غیرفعال کنید، هر چند که این موضوع ممکن است اثرات منفی در نمایش وب سایت هایی که از کدهای اسکریپت در صفحات خود استفاده می کنند، داشته باشد.

۲۳

Jailbreak ؛ مرکز حملات جدید علیه iPhone

در روزهای اخیر، کدهای نفوذ باگی که در اثر Jailbreak کردن گوشی های آیفون به وجود می آید، به صورت عمومی منتشر شده است که باعث تشدید حملات علیه این تلفن هوشمند شرکت اپل گردیده است. با استفاده از این کدها که به زبان PHP و توسط یک هکر اسرائیلی به نام Pr0T3cT10n نوشته شده اند، نفوذگران می توانند اقدام به کرش دستگاه و انتقال کدهای مخرب بر روی گوشی نمایند.

هم اکنون شرکت های امنیتی در حال تجزیه و تحلیل کدهای مخرب انتشار یافته هستند و هنوز اطلاعاتی در این خصوص، در دسترس عموم قرار نگرفته است اما به نظر می رسد که این کد مخرب، از دو آسیب پذیری منحصر به فرد برای دستیابی به اهدافش استفاده می کند که نخستین مسئله آن مربوط به وجود یک آسیب پذیری در مرورگر سافاری است که پس از حمله موفقیت آمیز توسط این باگ، در مرحله دوم نفوذگر تلاش می کند تا با استفاده از دسترسی محلی[1] بر روی گوشی، با بالا بردن امتیازات خود، به کاربر اصلی سیستم عامل[2] تبدیل شود.

اگر چه این آسیب پذیری، بیشتر بر روی گوشی های هوشمند نسل ۳ که از سیستم عامل iOS 4.0.1 بهره می برند، بیشتر گزارش شده است ولی به کاربران توصیه می شود که با دقت و توجه کافی نکات امنیتی را به خصوص در هنگام اتصال به اینترنت رعایت نموده و از نگهداری اطلاعات محرمانه بر روی گوشی خودداری نمایند.

---

[1] local

[2] Root

لازم به ذکر است که Jailbreak به عمل شکستن و باز کردن قفل گوشی های آیفون گفته می شود که این امر با استفاده از کاربر اصلی سیستم عامل و همچنین برای ایجاد تغییرات اضافی در تلفن صورت می گیرد. به کمک Jailbreak می توان قسمت هایی از سیستم عامل گوشی را که در حالت عادی، کنترلی بر روی آن وجود ندارد، تغییر داد که این امر می تواند سیستم عامل iOS این گوشی ها را در معرض تهدید جدی قرار دهد. این عمل علاوه بر خطرات بسیار، باعث در معرض آسیب قرار گرفتن گوشی توسط بدافزارها نیز شده و می تواند در انجام حملات مخرب علیه کاربران تلفن مورد استفاده قرار گیرد.

نرم افزار L0phtCrack 6

نرم افزار L0phtCrack 6 که شاهکار گروه هکری L0pht Heavy Industries می باشد، به LC6 معروف بوده و از الگوریتم های پیچیده ای در برنامه نویسی آن استفاده شده است.

نرم افزار LC6 بهترین کراکر[1] جهان و آخرین نسخه از سری کراکرهای L0phtCrack است که در تاریخ ۱۱ مارس ۲۰۰۹ عرضه شد. این برنامه علاوه بر پشتیبانی از سیستم عامل ۶۴ بیتی ویندوز، به طور شگفت انگیزی قادر به کراکینگ کلمات بسیار پیچیده از جمله چک کردن یک میلیارد ترکیب حروف ها در ثانیه است. LC6 پسوردهای هش شده یونیکس[2] را هم کرک نموده و همانند نسخه[3] های قبلی، دارای قدرت شنود داده ها است.

نرم افزارهای LC از ۴ روش برای کرک نمودن پسوردها استفاده می کنند که شامل User Info و Dictionary Attack و Hybrid Attack است و اگر هیچ کدام از متدهای فوق به جواب نرسد، از روش Brute Force که آخرین متد موجود است، بهره می

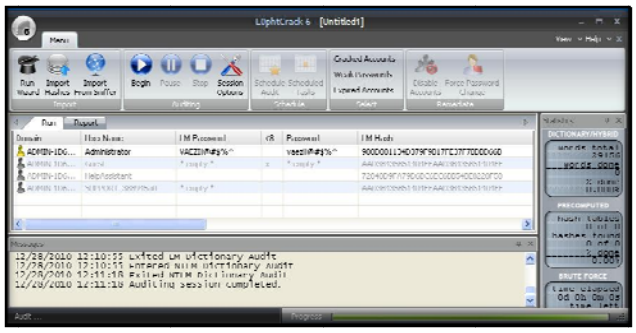
---

[1] Cracker

[2] Unix

[3] Version

برند. اگرچه روش Brute Force مقداری زمانبر است که آن هم بستگی به نوع کلمه و ترکیب حروف (حروف کوچکند یا بزرگ)، به کار رفتن اعداد و نشانه ها دارد ولی به هر حال بعد از گذشت مدت زمان لازم حتماً به جواب می رسد.



آشنایی با گروه L0pht Heavy Industries:

LOPHTCRACK

گروه L0pht Heavy Industries یکی از قدیمی ترین گروه های هک است که در اوایل دهه ۸۰ میلادی، هم زمان با ورود کامپیوترهای اپل به بازار، توسط Dr Mudge و DilDog تأسیس گردید.

Dr Mudge

DilDog

آقای Dr Mudge که اسم واقعی اش Zatko می باشد، یکی از بزرگترین هکرهای دنیا و با تجربه ترین فرد L0pht است که ریاست این گروه را برعهده دارد. او که در حدود ۳۸ سال سن دارد، تحصیلات دانشگاهی خود را در رشته موسیقی تا دریافت مدرک دکتری ادامه داده و عضو گروه هکری کلاه مشکی ها به نام Cult of the Dead Cow نیز است.

اگرچه در ابتدا اعضای گروه L0pht بیشتر از حال حاضر آن بود اما هم اکنون فقط هشت مرد جوان اعضای این گروه را شامل می شوند که اسم های مجازی آن ها به صورت زیر است:

The L0pht boys, from left: Silicosis , Brian Oblivion , John Tan , Mudge , Kingpin (standing) , Space Rogue (front) , Weld Pond and DilDog

هر کدام از این افراد که سنی بین ۲۷ تا ۳۸ سال دارند، علاوه بر تسلط شگفت انگیزشان به زبان های برنامه نویسی، در زمینه خاصی مهارت دارند. جوانترین فرد این گروه Silicosis و مسن ترینشان هم Dr Mudge است.

در لابراتوار تحقیقاتی این گروه که تا چند سال پیش، در طبقه دوم یک ساختمان قدیمی در حومه شهر بوستون منطقه ماساچوست[1] ایالات متحده آمریکا واقع شده بود، حدود ۲۰۰ کامپیوتر از سیستم های پرقدرت مثل Sun Microsystems تا قطعاتی از سیستم های Commodore 64 و Apple 2 ، چندین سرور و مسیریاب، مودم های DSL و ISDN وجود داشت که در ۷-۶ اتاق این ساختمان نیز چند شبکه داخلی برای هک های گروهی خودشان طراحی کرده بودند.

از جمله کارهای بسیار مهم گروه L0pht پیدا کردن باگ های سیستمی در شبکه ها است. به این صورت که ابتدا بر روی سیستم های داخلی خودشان حفره هایی را پیدا کرده و سپس برای آن باگ ها Expliot نوشته و یا ویژگی ها و مشخصات آن آسیب پذیری را به روش های مختلف در اختیار دیگر هکرها قرار می دهند و هکرها هم با آگاهی از آسیب پذیری های جدید، برای آن حفره ها Exploit می نویسند. بسیاری از Exploit هایی که گروه های هکری برای نفوذ به سیستم ها استفاده می کنند را همین گروه کشف و در دنیا ثبت نموده است.

[1] Boston, Massachusetts area

Space Rogue

Brian Oblivion

Kingpin

گروه L0pht از آسیب پذیری هایی که خودشان کشف و یا دیگران پیدا می کنند برای نفوذ به سیستم ها بهره می برند. تفاوت این گروه با سایر هکرها آن است که در صورت پیدا نکردن هیچ حفره ای در کامپیوتر هدف، برای سیستم شرایطی را فراهم کرده و به آن طوری القاء می کنند که از خود شرایط باگ را نشان بدهد، سپس از همین آسیب پذیری برای نفوذ استفاده می کنند. مثالی که خودشان برای این مسئله می زنند آن است که : "اگر با خانه ای مواجه شدید که همه درها و پنجره هایش بسته است و راه نفوذی مثل یک پنجره نیمه باز یا حتی در اصلی خانه (بی توجهی به مسایل امنیتی) یا در پشتی[1] آن باز نبود، آنگاه با یک سنگ کوچک می توانید قسمتی ازکنار یک پنجره را شکسته، قفل را باز کرده، پنجره را بالا کشیده، بعد به داخل خانه بروید". منبع مالی این گروه، درآمد حاصل از دادن خدمات مشاوره ای امنیت داده ها و طراحی شبکه های امن به متقاضیان بود.

از ژانویه سال ۲۰۰۰ میلادی تاکنون، بعضی از اعضای اصلی گروه L0pht به علت این که تحت تعقیب دولت ایالات متحده آمریکا قرار داشتند، برای جلوگیری از بازداشت خود، مسئولیت تحقیقات امنیت شبکه شرکت دولتی @stake را به ناچار پذیرفته و آدرس سایت این گروه از www.L0pht.com به www.atstake.com تغییر یافت.

[1] Back Door

هم اکنون این گروه به عنوان مرکز تحقیقاتی شرکت @stake که از سال ۲۰۰۴ میلادی به عنوان یکی از شرکت های زیر مجموعه سیمانتک می باشد، در حال تولید چندین نرم افزار از جمله Web Proxy و Anti Sniff ، Windows password auditing tool و ... بوده و اعضای آن از کارشناسان امنیتی سیمانتک محسوب می شوند.

نحوه صحیح بازکردن CD و Flash

همواره یکی از متداولترین خطراتی که کامپیوترهای شخصی را تهدید می کند، نصب بدافزارها و برنامه های مخرب از طریق عدم آشنایی با نحوه صحیح بازکردن CD و Flash ها است. معمولاً بدافزارها به گونه ای نوشته می شوند که با دوبار کلیک بر روی درایور یا انتخاب گزینه های Open و Auto Play قابل اجرا هستند.

حال برای این که کامپیوتر شما از حمله بدافزارها در امان بماند، تنها کافی است که به جای باز کردن CD و Flash ها توسط سیستم عامل کامپیوترتان، آن ها را از طریق سیستم عامل های نصب شده در یک برنامه ماشین مجازی باز کنید. بدین صورت، بدون نگرانی می توانید مطمئن باشید که بدافزارهای موجود روی آن ها، هیچ دسترسی به کامپیوتر شما نداشته و سیستم شما از آلودگی مصون خواهد ماند.

سیستم عامل های نصب شده در ماشین های مجازی، هیچ گونه ارتباطی با سیستم عامل میزبان خود نداشته و در صورت آلودگی، می توان تنها با یک کلیک و در مدت چند ثانیه، سیستم را به حالت اولیه برگرداند. همچنین با این کار علاوه بر امنیت بیشتر در برابر بدافزارها، یک سیستم عامل مجزای دیگر برای استفاده های مختلف در اختیار دارید.

لازم به ذکر است که ماشین مجازی، به معنی راه اندازی یک سیستم عامل درون یک سیستم عامل دیگر است. برای این کار می توان از نرم افزارهایی همچون VirtualBox ، Windows Virtual PC و یا VMware Workstation استفاده کرد.