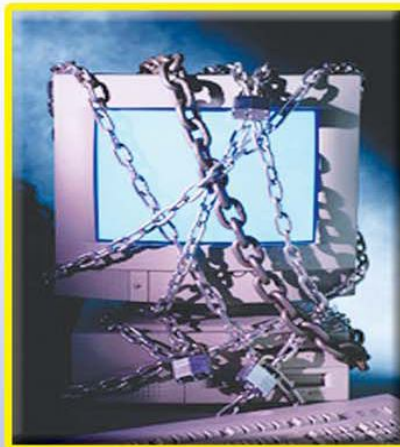




دفاع سایبری و امنیت رایانه (۱)

کلیات امنیت در فناوری اطلاعات

آسیب پذیری ها، تحولات اینترنت در آینده
تحلیل بد افزار های سال ۲۰۱۱ و راه کارها
جاسوس افزار استاکس نت
امنیت سایبری و راهکارها



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

دفاع سایبری و امنیت رایانه [1]

کلیات امنیت در فناوری اطلاعات

تدوین:

حمید اسکندری

سرشناسه	: اسکندری، حمید، 1338 -
عنوان و نام پدیدآور	: کلیات امنیت در فناوری اطلاعات / تدوین حمید اسکندری.
مشخصات نشر	: تهران: بوستان حمید، 1390.
مشخصات ظاهری	: ج. ۱: مصور، جدول.
فروست	: دفاع سایبری و امنیت رایانه
شابک	: دوره: 3-02-6412-978-600، ج. 1 03-0-6412-978-600
وضعیت فهرست نویسی: فیبا	
یادداشت	: کتابنامه .
عنوان دیگر	: کلیات امنیت در فناوری اطلاعات.
موضوع	: شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع	: اینترنت -- اقدامات تامینی
موضوع	: تکنولوژی اطلاعات -- اقدامات تامینی
رده بندی کنگره	: 1390 5/TK5/105 الف
رده بندی دیویی	: 005/8
شماره کتابشناسی ملی	: 2498878



انتشارات

عنوان: دفاع سایبری و امنیت رایانه (1) - کلیات امنیت در فناوری اطلاعات

گردآوری و تدوین: حمید اسکندری

ناشر: بوستان حمید

نوبت چاپ: چاپ اول (پاییز 1390)

شمارگان: 2500

قیمت: 3500 تومان

• کلیه حقوق اعم از چاپ و تکثیر، نسخه‌برداری برای ناشر محفوظ است.

(نقل مطالب با ذکر مأخذ بلامانع است).

صندوق پستی 1775-331

تلفن ناشر: 33700927

پیش گفتار

امروزه سازمان‌های تروریستی مخالف دولت‌ها بدون نیاز به استفاده از رسانه‌های جمعی از قبیل رادیو، تلویزیون و جرائد برای ارتباط با مخاطبان خود از بستر اینترنت بهره می‌گیرند. بسیاری از مردم و سازمان‌هایی که به طور فزاینده‌ای متکی به فضا رایانه‌ای هستند، از میزان آسیب پذیری و بی دفاع بودن خود، بی خبر می‌باشند و بسیاری از استفاده کنندگان و کاربران این فضا، از آموزش ضعیف و تجهیزات ناکافی، برخوردار هستند.

در نهایت، جامعه انتظار دارد تا سامانه‌های رایانه‌ای، قابل اعتماد گردیده و علیرغم اختلال‌های موجود، خطاهای کاربر و تهاجم رایانه‌ای طرف‌های متخاصم، بتوانند به کار خود با رایانه ادامه دهند و همچنین نیاز نباشد که اقدامات دیگری را انجام دهند. اعتماد سازی دارای ابعاد زیادی شامل صحت، اعتبار، ایمنی، ماندگاری و نیز امنیت می‌باشد.

دزدی و تخریب اطلاعات منجر به قطع خدمات می‌گردد و این شایع‌ترین شکل حمله اینترنتی و رایانه‌ای می‌باشد. حملاتی که معطوف به سیستم‌های کنترل می‌گردد، در راستای کنترل یا از کار انداختن زیر ساخت‌های فیزیکی

(پنج)

هدایت می‌شوند. به عنوان مثال نفوذ به سیستم‌هایی چون شبکه های برق، سازمان‌های آب، مؤسسات مالی و بانک ها منطقه وسیعی را تحت مخاطره قرار می‌دهد. این فرایند با استفاده از اینترنت برای ارسال اطلاعات و یا با نفوذ به سیستم‌های امنیتی صورت می‌پذیرد.

مدیر کل صنایع برق، الکترونیک و فناوری اطلاعات وزارت صنایع و معادن از شناسایی 30 هزار آی‌پی صنعتی آلوده به جاسوس افزار "استاکس نت" خبر داد و گفت: این ویروس، اطلاعات مربوط به خطوط تولید را به خارج از کشور منتقل می‌کند. هدف‌گیری این ویروس در راستای اهداف تحریم و جنگ الکترونیکی (سایبری) علیه ایران است¹.

با توجه به اهمیت و کاربردی بودن موضوع در سطوح مختلف اقشار جامعه بخصوص مدیران و کارشناسان تصمیم گرفته شد تا مباحث تهدیدات و امنیت در فضای سایبر و اینترنت و راهکارهای مطرح که دارای اعتبار علمی می باشد به صورت سری کتاب های مستقل گردآوری و تدوین گردد. بدون شک مورد استفاده محققین و مخاطبین گرامی در این حوزه ، قرار خواهد گرفت.

¹ - پایگاه اطلاع رسانی وزارت صنایع و معادن - روابط عمومی - 13 شهریور 1389

فهرست مطالب

11.....	1- تعاریف و کلید واژه ها
21.....	2- ده تهدید موجود در شبکه های اجتماعی
29.....	3- خلاصه
38.....	4- مدیریت رخداد ها
40.....	5- نتیجه گیری و پیشنهادات
90.....	6- قانون جرایم رایانه ای
102	- کتابنامه

مقدمه

در بند 11 سیاست‌های کلی نظام در خصوص پدافند غیرعامل که به تصویب مقام معظم رهبری رسیده و ابلاغ شده است این چنین آمده است:²

« اصول و ضوابط مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای.»

تهدیدهای امنیتی متعددی در حوزه فناوری اطلاعات وجود دارد که از منابع مختلف و بنا بر علت‌های مختلفی سرچشمه می‌گیرند. این تهدیدها می‌توانند در گروه‌های محدودی مثل قطع، خرابی، حوادث بد، دسترسی‌های غیر مجاز، وقفه، حائل شدن، جعل کردن و تغییر دادن داده‌ها باشد. بقیه تهدیدها نتیجه‌ی استفاده نادرست، اجرای نا صحیح، افشای اطلاعات و فقدان جامعیت است.

با تشکر

مؤلف

² - این سیاست‌ها که در 13 بند تصویب شده و به تأیید مقام معظم رهبری رسیده است.

1- تعاریف و کلید واژه ها

تهدید در فضای سایبر:

به هر رویداد (پیش بینی شده یا تصادفی) یا واقعه با احتمال اثر معکوس بر سیستم اطلاعاتی از طریق دسترسی غیر مجاز، تخریب، افشاء، تغییر داده ها و یا ممانعت از انجام خدمات، تهدید گفته می شود. یک تهدید از آسیب پذیری شناخته شده ای استفاده می کند.

امنیت رایانه:

امنیت رایانه، تلاش برای ایجاد یک بستر امن رایانه ای است و طراحی آن بگونه ای است که فقط امکان انجام اقدامات مجاز در آن وجود داشته باشد. که شامل تعیین و اجرای یک سیاست امنیتی می باشد.

آسیب پذیری:

یک نقص یا نقطه ضعف در طرح، پیاده سازی یا عملیات و مدیریت یک سیستم که می تواند برای نقض سیاست امنیتی سیستم، مورد بهره برداری قرار گیرد.

ویروس:

ویروس یک برنامه خود تکرار است که با تکثیر نسخه هایی از خودش به سایر مستندات و برنامه های اجرایی دیگر گسترش می یابد و ممکن است باعث اختلال در عملکرد برنامه ها شود. یک ویروس رایانه ای نظیر یک

ویروس زیستی عمل می کند که از طریق تولید مثل خود در سلول های بدن میزبان پخش می شود. بعضی از ویروس های مشهور عبارتند از: نیلما، اسلمر، ساسر و ...

فضای سایبر:

رایانه های به هم متصل شده، سرورها، روترها، سوئیچ ها و کابل ها که زیرساخت های حیاتی بوسیله آنها کار می کنند، فضای سایبر گفته می شود.

تروریسم سایبر:

هر حمله از پیش طراحی شده توسط گروه های تحت حمایت کشورها یا عامل های پنهانی با انگیزه سیاسی علیه داده ها و اطلاعاتی که نتیجه آن ضربه به اهداف غیر رزمی باشد.

تروریست های سایبر برای پیشبرد مقاصد سیاسی خود، هر روز در حال ایجاد روش ها و ابزارهای هوشمندانه تر برای حمله به سیستم های رایانه ای و دولتی هستند. در چنین جایگاهی، امنیت ملی و جهانی در خطر می باشد. دلیل وجود این خطر را می توان عدم وجود قوانین کافی حاکم بر اینترنت، وسعت مخاطبان بالقوه، ناشناس بودن ارتباط و سرعت جریان اطلاعات دانست. این موارد ویژگی هایی هستند که برای مبارزه با تروریسم سایبر باید تحت تحقیقات بیشتری قرار گیرند.

هکر:

هکر: شخصی که بدون اجازه دستیابی وارد سیستمی می شود یا کسی که سطح دسترسی خود به اطلاعات را افزایش می دهد تا آنها را مرور، کپی، تعویض، حذف یا نابود نماید.

هکر به شخصی اطلاق گردد که از دانش شبکه خود و سیستم‌های رایانه‌ای در جهت حصول دسترسی غیرمجاز به سیستم‌های رایانه‌ای بهره می‌گیرد.

جنگ سایبری:

معادلی برای جنگ اطلاعاتی است که کاربرد های قدرتمند رایانه و شبکه در جنگ اطلاعات را مورد تأکید قرار می دهد.

جنگ اطلاعاتی¹:

اقداماتی که به منظور حفاظت، انفجار، تخریب، ممانعت یا نابودی اطلاعات یا منابع اطلاعاتی به منظور دسترسی به اهداف، منافع مشخص یا پیروزی بر دشمن صورت می گیرد .

هفت دسته جنگ اطلاعاتی² ارائه شده که با مجموعه اصطلاحات نظامی سازگاری دارد: جنگ فرماندهی و کنترل³، جنگ مبتنی بر تجسس⁴، جنگ الکترونیک، جنگ فیزیولوژیک، جنگ هکر⁵، جنگ اطلاعات اقتصادی و جنگ سایبری.

تیم واکنش اضطراری رایانه ای⁶:

یک مرکز تحقیق و توسعه است شامل خبرگان امنیت رایانه و اینترنت که در زمان حادثه و اضطرار عکس العمل نشان می دهد.

¹ . IW

² - Information Warfare

³ - Command and Control

⁴ - Intelligence-based

⁵ - hacker

⁶ . CERT

امواج الکترومغناطیس¹:

یک جریان قوی از انرژی الکترومغناطیسی که می توان از یک رعد و برق، یک تنفگ امواج الکترومغناطیس یا انفجار یک بمب اتمی حاصل شود. امواج الکترومغناطیس بقدر کافی قوی است که می تواند سبب از کار انداختن موقت یا دائمی رایانه و دستگاه های الکترونیکی گردد.

جاسوسی:

عمل تجسس با بدست آوردن اسرار محرمانه از دشمنان یا رقبای برای رسیدن به مقاصد نظامی، سیاسی یا تجاری، پیشرفت های رخ داده در فناوری اطلاعات و توسعه و تکامل ابزار ذخیره سازی کوچک و پنهان به مخاطرات جاسوسی به شکل قابل ملاحظه ای افزوده اند.

تجسس سیگنالی²:

بطور قابل اندازه گیری، بیشتر داده های تجسس، حاصل از منابع تجسس سیگنالی می باشد. این می تواند شامل امضاهای الکترونیک³ یا تحلیل محتوای ارتباطات⁴ باشد. حوزه تجسس سیگنالی بواسطه مقدار داده هایی که در روز ارائه می دهد و چون نیاز به یافتن سوزن در انبار کاه، چالش هایی جدی پیش روی MIS و مدیریت دانش قرار دهد.

¹. EMP

². SIGINT

³. ELINT

⁴. COMINT

فرکانس رادیویی پر انرژی¹:

یک اسلحه فرکانس رادیویی پر انرژی می تواند تجهیزات رایانه ای را از کار بیاندازد و این عمل با قرارداد آنها در معرض تشعشعات مخرب امکان پذیر است.

جرائم سازمان یافته:

فعالیت های غیر قانونی که توسط سازمان های خلافکار رسمی بصورت سیستماتیک انجام می شود. فناوری اطلاعات پیشرفته اشکال بدیهی از جرائم سایبری سازمان یافته را تعریف می نماید.

مدیریت اذهان:

اعمالی را با هدف تأثیر گذاری و نفوذ در آراء عمومی، یا حتی فرهنگها تشریح و بیان می کند و می تواند با طیفی از حوزه های سیاسی، مدنی، فرهنگی و نظامی تلاقی پیدا کند. فناوری های اینترنت به شکل روز افزونی جهت تأثیر و نفوذ بر ادراکات عمومی از طریق رسانه ها مورد استفاده قرار می گیرند.

زیر ساخت حیاتی:

سیستم ها و دارایی هایی که اگر نابود شوند، تأثیراتی روی امنیت فیزیکی، امنیت اقتصاد ملی و سلامت یا ایمنی همگانی خواهند داشت.

زیر ساخت پایه ای:

یک زیر ساخت فیزیکی یا فناوری کی؛ این احتمالاً در اغلب موارد حیاتی ترین زیر ساخت است.

¹. HERF

زیرساخت مشتری:

زیرساختی که وابسته یا نتیجه یک زیرساخت پایه‌ای می باشد.

زیرساخت اجتماعی:

زیرساخت مشتری شامل افرادی که تصمیم به استفاده کردن یا نکردن از زیرساخت پایه‌ای می گیرند.

انگشت نگاری مجازی:

این یک الگوگذاری دیجیتال منحصر به فرد است که قابل استفاده برای شناسایی یک فایل خاص (ویژه) است.

سندیت :

توانایی حصول اطمینان از اینکه اطلاعات معین با هویت و نام کسی که آن را تولید نموده است ، حمل می شود و این مسئله نباید جعلی باشد یا دچار تغییر شود.

پنهان نگاری:

به طور کلی، این فرایند پنهان کردن اطلاعات یا « پوشیده نوشتن » است. به شکل تخصصی تر، در محیط دیجیتال، پنهان نگاری شامل داده ها یا عکس های پنهان در فایل های دیگر است به طوریکه از منظر افرادی که از مضمون سری (مخفیانه) آنها بی اطلاعند، بدون تغییر به نظر می رسند.

تجزیه و تحلیل پنهان نگاری:

فرایند کشف داده های پنهان در فایل های دیگر است. تجزیه و تحلیل پنهان نگاری به طور نوعی با بررسی انحرافات کوچک در یک نمونه فایل مورد انتظار، انجام می شود.

رمزنگاری:

یک روش برگشت پذیر رمزدار کردن داده ها است که به یک کلید برای کشف رمز نیاز دارد. رمزنگاری می تواند در ارتباط با پنهان نگاری به کار رود که سطح دیگری از محرمانه بودن (اختفاء) را فراهم می کند.

رمزنگاری ، پیاده سازی و مطالعه رمزنگاری و رمزگشایی داده ها است به طوری که تنها توسط افراد خاص رمزگشایی می شود. سیستمی که برای رمزنگاری و رمزگشایی داده هاست، سیستم رمز می باشد.

رمزنگاری یک ابزار قدرتمند برای نگهداری اطلاعات مهم و خصوصی در هنگام قرارگرفتن در معرض تهدیدات ناشناسان و مجرمین است ، و همچنین برای مخفی نگهداشتن فعالیت های غیرمجاز از دید مجریان قانون می باشد. همانطوریکه رایانه ها سریع تر رشد می کنند و روش های شکست رمز مطمئن تر می شوند، الگوریتم های رمزنگاری به تحکیم پایدار جهت جلوگیری از ناامنی، نیاز دارند.

کلید عمومی، گواهی: یک بلوک از قالب شکل داده شده خاص داده ها است که شامل یک کلید عمومی و نام مالک آن می باشد. گواهی نامه (تأییدیه)، امضای دیجیتال یک مقام دارای صلاحیت را جهت تصدیق آن، دربردارد.

کلید خصوصی: کلید به کار رفته در رمزنگاری کلید عمومی که به یک هویت فردی تعلق دارد و باید به طور سری نگه داشته شود ، می باشد.

سیستم کلید عمومی: سیستم کلید عمومی، سیستمی است که از دو کلید استفاده می کند، یک کلید عمومی، که برای هرکسی شناخته شده است و کلید خصوصی که تنها گیرنده پیام آن را به کار می برد.

نیازمندی محرمانگی:

تهیه کنندگان خدمات اطمینان می‌دهند که اطلاعات خصوصی مشتریان حافظت شده است و مشتریان بر دسترسی به اطلاعات خصوصی شان کنترل دارند.

تالار گفتگو (چت روم):

از لحاظ فنی، چت روم یک مسیر ارتباطی است اما عبارت اتاق برای توسعه کنایه‌های چت برای یک مکان آنلاین که گروهی از افراد می‌توانند درباره موضوع خاص ارتباط (گفتگو) برقرار کنند، استفاده می‌شود. کانال‌های صوتی و تصویری ممکن است برای افزایش ارتباط بکار روند. بعضی از تالارهای گفتگو به کاربران اجازه می‌دهند تا بدون دیدن مخاطب خود با او ارتباط (گفتگو) برقرار کنند. اغلب تالارهای گفتگو به کاربران اجازه می‌دهند تا کسی را که در مکالمه شرکت کرده، ببینند. خدمات پیام‌رسانی کوتاه:

خدمات پیام‌متنی پیشنهادی توسط سیستم تلفن سلولی دیجیتالی GSM است. پیام‌های متنی کوتاه از تلفن همراه، دستگاه فکس یا آدرس IP انتقال داده می‌شوند. پیام باید بیشتر از حداکثر 160 کاراکتر الفبا عددی و فاقد عکس و گرافیک باشند. حتی اگر تلفن همراه گیرنده غیر فعال باشد، پیام با شبکه GSM انتقال می‌یابد تا وقتی که تجهیزات کاربر، فعال شود.

معامله الکترونیکی امن:

پروتکل پرداخت آنلاین برای معاملات با کارت اعتباری امن روی اینترنت طراحی شده است. استاندارد معامله الکترونیکی امن به طور مشترک توسط Master Card، ویزا و شرکت‌های رایانه‌ای مختلف مثل: IBM، Netscape،

مایکروسافت، توسعه یافته است. معامله الکترونیکی امن محرمانگی و انکارناپذیری را برای کارت اعتباری فراهم می نماید؛ و مانع تاجران از گرفتن شماره های کارت اعتباری می شود.

حمله انکار خدمات:

یک حمله انکار خدمات¹ حادثه ای است که در آن، یک کاربر یا سازمان از خدمات یک منبع که طبق معمول انتظار بهره گیری از آن را دارد، محروم می گردد. قطع سرویس، به معنی ناتوانی موقت یک سرویس شبکه خاص مانند پست الکترونیک از حضور یا قطع موقت اتصال یا خدمات شبکه می باشد.

حمله انکار خدمات یک حمله به شبکه است که با درخواست های اضافی بسیار زیاد شبکه اشباع می شود. به طوریکه هیچ منبعی را رها نمی کند و از اینرو مانع ارائه خدمات نسبت به کاربران می شود. این حملات باعث آسیب به ارائه سرویس به کاربران، به نوعی آسیب به اتصال شبکه و سرویس ها با صرف پهنای باند شبکه هدف یا تحمیل بار اضافه به منبع محاسباتی سیستم هدف، می شوند.

حمله مهندسی اجتماعی:

روش به دست آوردن اطلاعات مجرمانه با استفاده از کاربران مجاز. یک مهندس اجتماعی به طور کلی از تلفن و اینترنت برای فریب یک شخص جهت آشکار کردن اطلاعات حساس استفاده می کند یا آنها را وادار به انجام کاری می کند که مخالف سیاست اداری پیش می رود.

¹. DOS

2- گزارش ها و مصادیقی از آسیبها و خسارات در حوزه سایبر

ویروس ها توسط نفوذگرهای زیادی که در اینترنت فعالیت داشتند به سرعت گسترش پیدا کردند ، چون تولید و روانه کردن ویروس برای تازه کارها آسانتر از هر چیزی بود. قابلیت استفاده آسان از رایانه ها ، باعث گسترش استفاده رایانه ها در خانه ها، سازمان ها ، مشاغل و تعداد زیاد افراد جوانی که با رایانه در اتاق خوابشان بزرگ می شوند، شده است. افزایش فوق العاده علاقه به رایانه، بی نام و نشان بودن کاربرهای اینترنت و وابستگی رو به رشد به رایانه و شبکه های رایانه ای، همگی دست به دست هم داند تا این فضای سایبر ناامن تر و نا مطمئن تر شود .

از سال 2000 تا کنون یک دوره جدیدی مطرح است ، حمله ها و ویروس های این دوره تا کنون از حمله های کوچک و ضعیف ولی انتخاب کننده و هدفدار تشکیل شده اند . هدف ها از قبل برای بیشترین بهره برداری مالی انتخاب شده اند. هدف ها به دقت برای به دست آوردن مشخصات شخصی فرد انتخاب شده اند که سبب بهره برداری مالی می شوند . حمله ها بر مؤسسه های مالی ، نهادها و شغل هایی که مخزن اطلاعات فردی هستند، متمرکز شده اند. لیست این قربانیان، طولانی و در حال افزایش است. به عنوان مثال :

- بانک بازرگانی آمریکا گرپ¹: طبق گزارشات اعلام شد ، اسناد داخل رایانه که عبارت بوده از کارت های اعتباری اعضای مجلس آمریکا و بیش از یک میلیون از کارکنان دولت آمریکا مفقود گردیده و

¹ Bank of America Corp

مشتریان این بانک را در معرض خطر سرقت اطلاعات شخصی و مالی قرار داده است .

- شرکت چویس پوینت اینک¹: طبق گزارشات بخش اعتبارات ایالت جورجیا ، شخصی که با نفوذ در پایگاه داده های رایانه، اطلاعات فردی حدود 145000 نفر را دزدیده است.
- عمده فروش اطلاعاتی: بخش کمکی ریدِ السویر² اقرار کرد اطلاعات فردی حدود 310000 نفر از مشتریان آمریکایی اش ربوده شده است.

- چویس پوینت³ دیگر شرکت گزارش دهنده اعتبارات، صورت حساب بیش از 100000 نفر را گم کرد.

در سال جاری یک بدافزار خطرناک به نام "استاکس نت"⁴ در همه کشورهای جهان و به خصوص ایران گسترش پیدا کرده است که هدف آن ایجاد اختلال در شرکت ها و سازمان های مرتبط با زیرساخت های حیاتی همچون نیروگاه ها است. بدافزار مذکور با سوء استفاده از یک حفره امنیتی در ویندوز گسترش پیدا می کند و به دنبال سیستم هایی است که از نرم افزار WinCC Scada متعلق به شرکت زیمنس ، استفاده می کنند. نرم افزار مذکور معمولاً توسط سازمان های مرتبط با زیرساخت های حیاتی کشورها، استفاده می گردد. شرکت سایمانتک در این رابطه اطلاعاتی را منتشر ساخته است که در ادامه می آید. بنا بر اطلاعات ارائه شده توسط سایمانتک، کرم رایانه ای

¹ Choice Point Inc

² Reed Elsevier

³ Chioce point

⁴ Stuxnet

Scada که هدف آن شرکت ها و سازمان های مربوط زیرساخت های حیاتی هستند، نه تنها به سرقت اطلاعات می پردازد، بلکه یک درب پشتی¹ را نیز بر روی سیستم قربانی قرار می دهد تا بتواند از راه دور و به طور مخفیانه کنترل عملیات زیرساخت های مذکور را در اختیار گیرد. کرم Stuxnet، شرکت های مربوط به سیستم های کنترل صنعتی در سراسر جهان را آلوده ساخته است، با این وجود بنا بر گزارش های دریافت شده، بیشتر آلودگی ها در ایران و هند مشاهده شده است. همچنین بد افزار یاد شده توانسته است به صنعت انرژی در ایالات متحده آمریکا نیز وارد شود.

بنا بر نظر محققان امنیتی، بدافزار مذکور یک توسعه جدی در زمینه تهدیدات رایانه ای محسوب می شود و متأسفانه کنترل سیستم های فیزیکی در محیط های کنترل صنعتی را در اختیار هکرها قرار می دهد. این بدافزار که تیتراخبار ماه گذشته بود، برای سرقت کد و طرح پروژه هایی نوشته شده است که از نرم افزار Siemens Simatic WinCC استفاده می کنند. از نرم افزار مذکور معمولاً برای کنترل سیستم های صنعتی و سیستم های زیرساخت های حیاتی مانند سیستم های آب و برق استفاده می شود. این بدافزار از نام کاربری و کلمه عبوری که در نرم افزار زیمنس به صورت hard-coded وجود دارد، سوءاستفاده می کند و ...، از طرف دیگر مشخص شده است که بدافزار Stuxnet یک کد رمزنگاری شده را بر روی PLCs² سیستم قربانی بارگذاری می کند که از آن برای کنترل اتوماسیون پروسه های صنعتی استفاده می شود. در حال حاضر هنوز فعالیت های کد مذکور به صورت دقیق مشخص نشده است. یک

¹. back door

². Programmable Logic Controller

مهاجم با استفاده از درب پشتی می تواند از راه دور به انجام فعالیت هایی همچون دریافت فایل ها، اجرای پرده ها، پاک کردن فایل ها و فعالیت های مشابه بپردازد. وی همچنین امکان این را دارد که در فعالیت های حیاتی یک کارخانه تداخل ایجاد کند و کارهایی مانند بستن دریچه ها و خاموش کردن سیستم های خروجی را انجام دهد. بنا بر گفته یکی از محققان امنیتی، مهاجمان می توانند برای مثال در یک نیروگاه تولید انرژی، نقشه چگونگی عملکرد ماشین آلات فیزیکی را دریافت کرده و آنها را تحلیل کنند تا دریابند چگونه می توانند تغییرات مورد نظر خود را در آنها اعمال کنند. سپس کد دلخواه خود را وارد ماشین آلات کرده تا شیوه عملکرد آنها را تغییر دهند. کرم Stuxnet با سوءاستفاده از یک حفره امنیتی در ویندوز، خود را منتشر می سازد.

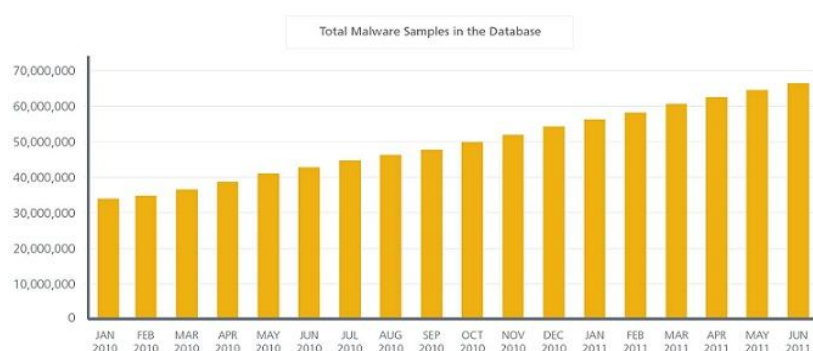
گزارش تحلیلی شرکت McAfee در سه ماهه دوم سال 2011

شرکت امنیتی McAfee در گزارشی به بررسی تهدیدات امنیتی سه ماهه دوم سال 2011 در زمینه های مختلف پرداخته است، در ادامه به مواردی از مهمترین بخش های این گزارش اشاره می شود:

تهدیدات بدافزارها

چشم انداز بدافزار در این سه ماهه شگفتی های زیادی را به ما نشان می دهد. اگرچه این دوره از لحاظ عددی شلوغ ترین دوره در تاریخ بدافزارها نیست، ولی زمانی که با سه ماهه اول همراه می شود، در نیم سال اول شلوغ ترین دوره را در این بردار داشته ایم و شاهد افزایش 22 درصدی نسبت به سال 2010 هستیم! در طول این سه ماهه آزمایشگاه های مک آفی تقریباً شش میلیون نمونه

یکتا از بدافزار را شناسایی کردند. این باعث می شود تا پایان سال، مجموعه بدافزارهای تجمعی "zoo" به 75 میلیون نمونه برسد. تنها به منظور مشاهده رشد قابل توجه بدافزارهای یکتا در طول چند سال گذشته، در اینجا نگاهی به این رشد افزایشی به صورت ماهانه می اندازیم:



در حال حاضر در هر ماه به طور متوسط نزدیک به دو میلیون نمونه‌ی جدید جمع آوری می شود. این قطعاً یک افزایش خوشایند نیست، اما با توجه به چگونگی کسب و کار و زندگی خصوصی افراد که در حال حاضر وابسته به تکنولوژی است، پایدار و قابل پیش بینی است.

در میان خانواده هایی که ما آنها را بررسی کردیم، نرم افزارهای آنتی ویروس تقلبی یک رشد پایدار را نشان می دهند و حتی صعود در پلت فرم Mac را نیز شروع کرده اند. در حال حاضر آنتی ویروس تقلبی برای پلت فرم شرکت اپل یک واقعیت است. این موضوع آزمایشگاه های مک آفی را متعجب نکرده است. اکنون کاربران مکیتاش بیشتر از گذشته هستند. این امر پلت فرم های اپل را مستقیماً در معرض دید نویسندگان بدافزار قرار می دهد.

در این سه ماهه تروجان‌های سرقت رمز عبور تنها کمی کاهش داشته‌اند، در حالی که بدافزارهای autorun تا حد زیادی کاهش داشته‌اند. تهدیدات Koobface نیز به پایین ترین سطح خود در این سال‌ها رسیده است.

روت کیت ها و بدافزار مخفی کاری

یکی دیگر از رده های بدافزاری که اخیرا رشد ثابتی را نشان می‌دهد، روت کیت است. یک روت کیت (گاهی اوقات بدافزار مخفی کاری نامیده می‌شود) یک کد است که عناصر خود را از سیستم عامل و نرم افزار امنیتی مخفی می‌کند. مجرمان سایبری از روت کیت‌ها برای ساختن بدافزارهای مخفی کارتر و پایدارتر دیگر استفاده می‌کنند. هر چه یک بدافزار بهتر مخفی شود، مدت زمان بیشتری روی سیستم باقی می‌ماند و فعالیت‌های مخرب خود را انجام می‌دهد. همان‌گونه که در نمودار زیر می‌بینید، روت کیت‌ها همه جا در حال افزایش هستند. درنیمه اول سال 2011، روت کیت‌ها با تقریبا 38 درصد افزایش نسبت به سال 2010، شلوغ ترین دوره خود را تجربه کرده‌اند. پرکارترین روت کیت‌هایی که ما با آن‌ها مواجه هستیم، koutodoor و TDSS هستند. هر دو پر دردسر بوده و برای سرقت اطلاعات، بدافزار را مخفی می‌کنند.

شرکت امنیتی Sophos در گزارشی به بررسی تهدیدات امنیتی نیمه اول سال 2011 در زمینه های مختلف پرداخته است. در ادامه خلاصه ای از بخش های مهم این گزارش را مطالعه می کنید:

موتورهای جستجو دروازه‌ای برای رفتارهای مخرب

موتورهای جستجو دروازه وب هستند، به همین دلیل مجرمان اینترنتی نتایج جستجو را دستکاری کرده و صفحات خرابکار خود را در میان آن جای می‌دهند. بهینه‌سازی موتور جستجو یا SEO یک روش بازاریابی اینترنتی استاندارد است که توسط اکثر شرکت‌ها به منظور جلب مشتری به سایت‌های خود از آن استفاده می‌شود. اما همین روش نیز می‌تواند مورد سوء استفاده قرار بگیرد. سوء استفاده از SEO به عنوان آلودگی SEO یا Black Hat SEO شناخته می‌شود.

مهاجمان با استفاده از تکنیک‌های آلوده سازی SEO سایت‌های خود را در میان نتایج موتورهای جستجو به رتبه‌های بالا آورده و کاربران را به سایتهای خرابکار هدایت می‌کنند

تهدیدات وب: یک تهدید جدید در هر 4/5 ثانیه

مجرمان سایبری از محبوبیت وب برای راه اندازی حملات مخرب سوء استفاده می‌کنند. در نتیجه وب بزرگترین راه برای مجرمان سایبری است تا از طریق آن ابزارهای مخرب خود را توزیع کنند. در طول نیمه اول سال 2011، در هر روز به طور متوسط شاهد 19000 URL مخرب جدید بودیم که معادل یک URL مخرب در هر 4/5 ثانیه است.

هنوز هم بسیاری از کاربران کامپیوتر متوجه نمی‌شوند که هنگامی که آن‌ها به ظاهر یک وب سایت معتبر را مشاهده می‌کنند، چیزی ناخوشایند می‌تواند کامپیوتر آن‌ها را آلوده کند. با این وجود بیش از 80% از URL های مخربی که پیدا کرده ایم، وب سایت های معتبری بوده اند که توسط مجرمان سایبری هک شده‌اند. این مجرمان با سوء استفاده از آسیب پذیری‌های موجود

در نرم افزارها یا به وسیله سرقت گواهینامه های دسترسی از ماشین های آلوده به بدافزار، عملیات هک را انجام می دهند.

در سومین گزارش سالیانه IT در بررسی که بیش از 8200 نفر از مدیران امنیت از 63 کشور در 6 قاره جهان کرده اند اطلاعات نتایج ناراحت کننده ای را نشان می دهد. اطلاعات این نقص ها را نشان می دهد (Berinato, 2005):

- نبود تمرکز قابل توجه روی استراتژی هایی که می تواند از این اتفاقات در همان قدم اول جلوگیری کند
- اختلاف نظر قابل توجه بین قوانین دولتی در برخورد با جرایم رایانه ای
- نبود روش مشخصی برای مدیریت ریسک
- ناتوانی مداوم برای ایجاد یک سازمان امنیتی با قابلیت تعقیب اطلاعات در انبوهی از اطلاعات امنیتی

به عنوان مثال آمار نشان می دهد تنها 37 درصد ، یک استراتژی امنیتی اطلاعات دارند و فقط 24 درصد از مابقی آمار گفته اند که یکی از این طرحها را برای سال آینده اجرا خواهند کرد . گزارش ها همچنین نشان می دهند زمانی که تعدادی حوادث ، وقفه ای را ایجاد می کنند ، آسیب ها همانگونه باقی می مانند. افزایش هایی که زنگ خطری می باشند عبارتند از :

- افزایش آشکار مخاطبانی که بصورت " نا شناخته " خرابکاری هایشان را انجام می دهند تا حدود 47 درصد افزایش یافته است
- همکاری با گروه های ناشناخته رو به افزایش در طول سال های گذشته
- افزایش مهارت و پیچیدگی حمله ها برای رسیدن به اهداف پیچیده تر

امنیت

لغت امنیت بر طبق تعدادی از فرهنگ لغت‌ها مانند وبسترز¹ به معنای حالتی از سالم بودن و دور بودن از خطر یا ریسک است، همچنین به معنای محافظت نیز می‌تواند باشد. معنای امنیت بسته به چیزی است که ایمنی به آن بر می‌گردد. به عنوان مثال در فناوری اطلاعات یا IT و همچنین علم رایانه، ایمنی به معنای جلوگیری از استفاده غیر مجاز از سامانه و نرم افزار است. در مخابرات راه دور امنیت به این معنی است:

- حالتی که از تاسیس و ابقای واحد محافظ که مصونیت از اعمال خصومت آمیز یا نفوذ را تضمین می‌کند، نتیجه می‌شود.
 - وضعیتی است که با توجه به طبقه بندی اطلاعات، از دسترسی اشخاص غیر مجاز به اطلاعات رسمی که زیر نظر امنیت ملی محافظت می‌شود، جلوگیری می‌کند.
- در کل امنیت می‌تواند یک معنی برای جلوگیری از : دستیابی غیر مجاز، سوء استفاده، دگرگونی و سرقت یا آسیب فیزیکی به اموال تعریف شود. امنیت این سه عامل را در بر دارد:

1- محرمانگی: برای جلوگیری از افشای غیرمجاز اطلاعات است، این امر برای تعدادی از کشورها شامل افشای اطلاعات شخصی مانند اطلاعات پزشکی، مالی، فرهنگی و مدارک جنایی می‌باشد.

¹ Webster's

2- صحت: جلوگیری از تغییرات غیر مجاز پرونده‌ها و نگهداری وضع موجود با استفاده از امانت داری کارکنان است. ممکن است به دلیل یک سود جویی شخصی یا انتقام جویی، تخریب صورت گیرد.

3- دسترسی: برای پیش‌گیری از پنهان ماندن اطلاعات از آن‌هایی که اطلاعات را در زمانی خاص نیاز دارند.

ایمنی در کل، موارد مختلفی را پوشش می‌دهد که کانون توجه ما ایمن سازی زیر ساخت اطلاعات است. هدف کلی، ایجاد یک زیر ساخت ایمن برای اطلاعات موجود در شبکه است. عوامل زیر برای ایمن سازی زیر ساخت اطلاعات ارائه شده است:

- امنیت فیزیکی
- امنیت اطلاعاتی
- امنیت مالی
- امنیت انسانی
- امنیت رایانه‌ای
- امنیت شبکه
- استانداردهای ایمنی

3- تحولات اینترنت در آینده

انتظار می‌رود که اینترنت وارد یک تکامل انقلابی شود. بسیاری از مردم با استفاده از شبکه تلفن‌های موبایل به اینترنت وصل خواهند شد، در حدود 1 میلیارد از جمعیت کشورهای در حال توسعه از تلفن‌های موبایل بیشتر از

رایانه استفاده خواهند نمود. توسعه شبکه (وب) «معنایی»¹ کاربران را قادر خواهد ساخت که اطلاعات آنلاین را به نسبت بسیار بالاتری وارد فرایند پردازش خودکار نمایند. چپ های الکترونیکی «شناسایی از طریق امواج الکترونیکی»² و استفاده گسترده از حس گر ها و فعال کننده ها³ یک «اینترنتی متشکل از اشیاء» را بوجود خواهد آورد که با محیط فیزیکی بزرگتر ادغام می شود.

فناوری های پردازشی و ارتباطاتی که به اینترنت نیرو می بخشند، با سرعت زیادی در حال توسعه هستند. قدرت پردازش تقریباً در هر دو سال، دو برابر می شد و نسبت به سال 1965 یک میلیون برابر افزایش یافته است. ظرفیت ذخیره سازی و پهنای باند با سرعت بیشتری در حال افزایش هستند و تقریباً هر دوازده ماه یکبار دو برابر می شوند. در میان مدت، هیچ دلیلی وجود ندارد که باعث شود این نرخ های استثنایی رشد، کاهش یابند.

با این حال، تغییر اساسی در ساختار اینترنت با توجه به استقرار گسترده اجزاء این سیستم، بسیار مشکل است. تغییرات کوچک به مانند ارائه نسخه 6 پروتکل اینترنتی و یا «بخش همزمان»⁴ یک دهه بیش از آنچه انتظار می رفت زمان برد. شبکه های خصوصی و جهانی سیستم های تحت پروتکل اینترنتی که توسط شرکت های ارتباطات راه دور مورد استفاده قرار می گیرند، انعطاف پذیری بیشتری دارند. یکچنین شبکه هایی کیفیت خدمات خود را ضمانت می کنند و شبکه های خصوصی مجازی و همچنین قابلیت انتقال صدا تحت

¹ . Semantic

² . RFID tags

³ . Actuators

⁴ . Multicast

پروتکل اینترنتی را ارائه می کنند. این شرکت ها همچنین بزودی خدمات ایمن رایانش ابری را نیز ارائه خواهند نمود. هم اکنون شرکت گوگل شبکه ارتباطات خصوصی جهانی خودش را بکار انداخته و احتمالاً دیگر غول های آنلین نیز به همین مسیر خواهند رفت.

در حوزه تقاضا، اینترنت یکی از مکانیسم های کلیدی برای کارایی بوده و همچنین مجرای اصلی کنش متقابل اجتماعی بین مردم سراسر جهان است. براساس تحقیقاتی که توسط پروژه مورد حمایت اتحادیه اروپا، با نام «به سوی اینترنت آینده» انجام گرفته، چهار پنجم شرکت کنندگان اروپایی اعلام کرده اند که طی 5 تا 10 سال آینده اینترنت به بخشی حیاتی از زندگی روزمره آنها تبدیل خواهد شد.

بسیاری از کاربران اینترنتی در دهه آتی در کشورهای در حال توسعه ساکن خواهند بود و علائق آنها نیز در مهندسی اینترنت تبدیل به مهمترین عامل تأثیرگذار خواهد بود. این امر بر موارد زیر تأکید خواهد کرد: هزینه پایین و زیر ساخت های بی سیم با پلت فرم هایی که می توانند توسط میلیون ها کاربر با آموزش پایین (مسأله ای که در جوامع صنعتی شاهد آن نیستیم) مورد استفاده قرار گیرد. (به سوی اینترنت آینده (2010)؛ اندرسون و راینی¹ (2010)

تغییر کاربردهای تجاری

در شرکت های بزرگ و دولت ها سیستم های کسب و کار نسبت به سیستم های رایانه ای، شاهد تغییرات بزرگ کمتری بوده اند، اما بسیاری از روندها و الگوهای قبلی تداوم یافته اند. تجهیزات قدیمی با سخت افزارها و

¹ . Anderson and Rainie

نرم افزارهای ارزان تر، سریع تر و سهل الوصول تر جایگزین گشته اند. وابستگی سازمان ها به زیر ساخت های فناوری افزایش بسیاری یافته است. دو تحول شایان توجهی که در این حوزه رخ داده اند عبارتند از: «تدارک بلادرنگ خدمات»¹ و همچنین «سیستم های کنترل نظارتی و کسب داده ها»² (SCADA).

یک شرکت بزرگ در فرایند تولید، از سیستم بلادرنگ رایانه ای استفاده می کند تا پیش بینی نماید که در کدام مرحله از فرایند تولید به مواد و قطعات ساخته شده توسط پیمانکاران و قطعه سازان نیاز خواهد داشت و سپس سفارش ها را براساس همین پیش بینی، تنظیم می کند. با این روش هزینه نگهداری مواد اضافی در انبار کاهش یافته و بهره وری بیشتر از سرمایه در گردش، افزایش می یابد. فروشگاه های زنجیره ای در زمان سفارش مواد غذایی از همین فرایند استفاده می کنند: رایانه ها به طور مداوم دارایی انبار را بررسی می کنند، سپس آن را با شرایط آب و هوایی و دیگر تغییرات فصلی می سنجند، و در آخرین لحظه ممکن سفارشات را ارائه می دهند. اگر رایانه ها و یا تجهیزات ارتباطات راه دور خراب شوند، تولید کننده نمی تواند کالا تولید کرده و فروشگاه نیز قادر به ارائه مواد غذایی به مشتریانش نخواهد بود.

در انگلستان، که در حدود 80 درصد هزینه های خواروبار در 4 یا 5 فروشگاه زنجیره ای بزرگ مصرف می شود، روش های «بلادرنگ» بدین معنا هستند که در هر لحظه از زمان بطور متوسط به مدت 4 روز ذخیره غذایی در

¹ . just- in- time service provision

² . Supervisory Control and Data Acquisition Systems (SCADA)

قفسه های فروشگاه وجود دارند. در سال 2007، لرد کامرون¹، رئیس «سازمان روستایی»² اعلام داشت که انگلستان فقط 9 وعده غذایی با وضعیت هرج و مرج فاصله دارد.

صنعت غذایی انگلستان تقریباً به طور کامل به نفت وابسته است (95 درصد غذای تولیدی انگلستان به نفت وابسته است) و بر اساس تخمین های لرد کامرون، اگر واردات نفت بنا به هر دلیل ناگهان متوقف شود در این صورت تنها بعد از سه روز نظم و قانون فرو می پاشد. در کشورهای صنعتی هنوز هم زنجیره های تولید سنتی خواروبار وجود دارند، بدین صورت که تولیدکنندگان محلی محصولات غذایی فصلی را ارائه می کنند و این محصولات توسط خرده فروش ها از بازارهای عمده فروشی محلی خریداری می گردد. اما این فرایند با واردات عمده مواد غذایی از خارج و فراوری و بسته بندی آنها در کارخانجات داخلی، کاهش بسیاری یافته است. در سال 2000، مؤسسه مشاوره ای «بست فود فوروارد»³ تخمین زد که شهروندان لندن هر سال در حدود 6/9 میلیون تن غذا مصرف می کنند که 81% از این میزان از غذاهای وارداتی از خارج انگلستان تأمین می شود.

شبکه های هوشمند⁴ و «کنترل نظارتی و کسب داده ها»

به منظور کارایی مناسب خدمات همگانی مانند برق، گاز، آب و نفت می بایست سیستم های توزیع به طور مداوم تحت کنترل باشند. از دهه

¹. Lord Cameron

². Countryside Agency

³. Best Food Forward

⁴. smart grid

1960، این سیستم ها با استفاده از ابزار رایانه ای «سیستم های کنترل نظارتی و کسب داده ها» تحت کنترل و نظارت قرار داشته اند. سیستم های اخیر قابلیت پیش بینی نیز دارند و بدین ترتیب وضعیت شبکه های توزیعی را قبل از طرح شدن تقاضا، متناسب با شرایط پیش رو پیش بینی می کنند. سیستم های اولیه کنترل نظارتی و کسب داده ها مختص به شرکت های خاصی بودند اما هم اکنون در حال گذار به سوی یک مدل شبکه ای باز هستند. ابزار جدیدتر «سیستم کنترل نظارتی و کسب داده ها» با استفاده از پروتکل های اینترنتی، به دریافت و ارسال اطلاعات می پردازند تا هزینه استفاده از شبکه های ارتباطاتی اختصاصی را حذف کنند. این نوع سیستم ها در برابر حملات، آسیب پذیری بسیار بیشتری دارند. در جولای 2010، مشخص شد که یکی از «سیستم های کنترل نظارتی و کسب داده ها» ساخته شده توسط شرکت زیمنس که به صورت گسترده ای نیز کاربرد دارد، دارای یک رمزعبور پیش فرض ثابت بود و همین امر این سیستم را هدف آسانی برای حملات می کرد. اندکی پس از این ماجرا یکی از همین حمله ها، یعنی استاکس نت، رخ داد. (Bond, 2010)

بسیاری از سیستم هایی که خدمات و کالاهای اساسی را ارائه می کنند از ویژگی های «خود سازمانده¹» بهره می برند. برنامه های رایانه ای بخش اعظمی از امور مدیریتی را انجام می دهند در حالی که نیروی انسانی فقط پارامترهای عملیاتی را تعریف می کنند. این نوع خود سازمان دهی به مدیریت عملیات های سیستم های رایانه ای و ارتباطاتی نیز تسری می یابد. فرایند مذکور تقاضاهایی که بر انواع زیرسیستم ها مواد می شود را ارزیابی و

¹ . self-organising qualities

متوازن می کند و در صورتی که بار ورودی بیش از حد مجاز باشد، آنها را خاموش می کند. نوربرت وینر¹ و استفورد بییر² به ترتیب در دهه های 1960 و 1970، ظهور ویژگی خود- سازماندهی را با عنوان «سایبرنتیک» پیش بینی نمودند. این امر می تواند به نوبه خود باعث آسیب به دیگر سیستم های مستقل شود.

محاسبه ابری

هم اکنون مهمترین روندی که در تجارت الکترونیکی بکار می رود و دارای پیامدهای امنیتی است، گرایش روزافزون به زیرساخت های «ابری» می باشد. تأمین کنندگان ثالث بطور فزاینده ای در حال ارائه فضای ذخیره سازی و منابع پردازشی به مشتریان خود هستند. «گوگل داکس»³، جی میل و زیر ساختی به مانند «ابر محاسبه گر الاستیک»⁴ از جمله این خدمات هستند. بازار این نوع خدمات در سال 2009 بالغ بر 17 میلیارد دلار آمریکا بود و انتظار می رود تا سال 2013 به 44/2 میلیارد دلار برسد (ENISA, 2009:3).

زیر ساخت های ابری داده ها، منابع را متمرکز می سازند و بدین ترتیب تبدیل به هدفی جذاب برای مهاجمین می شوند. این خدمات در تمام جهان گسترده هستند. این بدین معناست که احتمالاً داده های محرمانه بین چندین قلمرو ملی متفاوت نگهداری می گردند. با این حال، زیر ساخت های ابری می توانند از طریق تعدد سیستم ها و یک امنیت عملیاتی قوی و قابل

¹ . Norber Wiener

² . Stafford Beer

³ . Google Docs

⁴ . Elastic Compute Cloud

تقویت به سطوح بالاتری از امنیت، نسبت به اکثر سیستم های کوچکتر، دست یابند.

خدمات ابری با برخی خطرات ویژه ای رودررو هستند برای مثال کارمندان این نوع شرکت ها می توانند حجم انبوهی از داده های حساس را فاش سازند. با این حال، چنین به نظر می رسد که ارائه کنندگان این نوع خدمات، تاکنون سطوح امنیتی متفاوتی برای خدمات خود ارائه کرده اند (ENISA, 2009: 7-10). با بکارگیری استانداردهای صنعتی مناسب و با توجه به رقابت بین ارائه کنندگان خدمات، سازمان ها می توانند خطرات امنیتی روزمره حوزه رایانش ابری را از سر بگذرانند. با این حال توجه بسیار کمی به وقوع حوادث فاجعه بار در حوزه خدمات ابری شده است. بدون وجود برنامه ریزی های منعطف، مشتریان در معرض خطر از دست دادن ظرفیت پردازشی و داده ها قرار می گیرند.

پیچیدگی / خطوط کد منبع / خطاهای برنامه ای

یکی از شاخصه های غیرقابل بازگشت در تاریخ رایانه اینست که سیستم عامل ها، نرم افزارها و اطلاعات رمزگذاری شده بر روی قطعات سخت افزاری به مانند برد اصلی، کارت های گرافیکی، مودم ها، سوئیچ ها، پرینترها و ... ، بسیار پیچیده تر شده اند. «خطوط کد برنامه»¹ یکی از روش های سنجش اندازه یک برنامه است. در سال 1993، سیستم عامل «ویندوز ان تی 3/1» مایکروسافت دارای 4/5 میلیون خطوط کد منبع بود. جانشین این سیستم عامل یعنی «ویندوز ان تی 3/5» دارای 7/5 میلیون

¹ . Source Lines of Code

خطوط کد منبع بود. «ویندوز xp» که در سال 2001 به بازار ارائه شد دارای 40 میلیون خطوط کد منبع است. تعداد خطوط کد منبع سیستم عامل های ویستا و «ویندوز 7» در دسترس نیستند (Perrin, 2010). این رشد تنها منحصر به مایکروسافت نیست و ناشی از بازار تقاضا برای امکانات جدید است. اگر ما فرض کنیم که در 100 خط یک ایراد و اشتباه برنامه ای وجود دارد در این صورت در ویندوز xp شاهد 40000 ایراد برنامه ای محتمل خواهیم بود. این تخمین ها در کنار کنش های متقابل فزاینده، نشان می دهند که چرا سیستم عامل ها و نرم افزارهای مدرن اینچنین مستعد خطا هستند، خطاهایی که می تواند آنها را خود بخود از کار اندازد و یا در معرض سوء استفاده قرار دهند. یکی دیگر از دلایل نگرانی، تعجیل برخی تولیدکنندگان نرم افزارها در ارائه محصول به بازار است. این تولیدکنندگان به منظور حفظ موقعیت خود در بازار و افزایش درآمدها، محصولات تولیدی خود را بدون گذراندن دوره های آزمایشی کافی روانه بازار می کنند.

زیرساخت های حیاتی: عناصر سایبری

پیوستگی متقابل بین انواع خدمات دولتی بزرگ و سیستم های بزرگ بخش خصوصی منجر به پیدایش چیزی شد که از آن تعبیر به «زیرساخت های حیاتی»¹ می شود. رهیافت دولت ها در قبال زیرساخت های حیاتی در بخش های بعدی مورد بررسی قرار می گیرند.

¹ . Critical Infrastructures

4- آسیب پذیری ها و تهدیدات امنیتی

1-4- مقدمه

شاید برخی از بزرگترین مشکلات امنیتی که در رایانه‌ها و دیگر سیستم‌های اطلاعاتی به وجود می‌آیند تهدیدهای امنیتی و آسیب‌پذیری‌هایی هستند که به طور متوسط کاربران رایانه از آنها اطلاعی ندارند. حتی کسانی که اندکی آگاهی در مورد این تهدیدها دارند هنوز هم نمی‌دانند چگونه آنها را بشناسند و از آنها دوری کنند. موضوع اصلی این بخش شناختن این موارد است و این که در فعالیت‌های روزانه چگونه با آنها برخورد کنیم.

تهدید امنیتی در سیستم‌های رایانه‌ای، یک گروه از رویدادهاست که تا کنون به طور واقعی وجود نداشته‌اند. اما ممکن است به وجود آیند و باعث ضرر و زیان شوند. برای مثال بارش باران زیاد در یک منطقه باعث به وجود آمدن سیل می‌شود.

از طرف دیگر آسیب‌پذیری، نقص و ضعفی است که به طور معمول در سیستم وجود دارد، یا در نظام نامه امنیتی، طراحی و انجام یک کار به طور قطعی یا به صورت تصادفی موجب ضرر و زیان می‌شود. برای مثال، وجود یک قفل شکسته روی یک درب یک نوع خطر است، چون اگر یک دزد این موضوع را بداند می‌تواند وارد خانه شود و این موجب از دست دادن مال و اموال می‌شود. پس باید برای جلوگیری از خطر، یک ساز و کار کنترل برای کنترل آسیب‌پذیری به کار گرفته شود. مثلاً خریدن یک قفل جدید و تعویض قفل قدیمی.

2-4- انواع تهدیدات و آسیب پذیری ها

با توجه به ماهیت سیستم اطلاعاتی، تهدیدات و آسیب پذیری هایی وجود دارد که به طور کامل نمی توانیم آنها را بیان کنیم اما ماهیت گروهی از آنها به شرح زیر مطرح شده است:

➤ انواع تهدیدهای امنیتی

تهدیدهای امنیتی متعددی وجود دارد که از منابع مختلف و بنا بر علت های مختلفی سرچشمه می گیرند. این تهدیدها می توانند در گروه های محدودی مثل قطع، خرابی، حوادث بد، دسترسی های غیر مجاز، وقفه، حائل شدن، جعل کردن و تغییر دادن داده ها باشد. بقیه تهدیدها نتیجه استفاده نادرست، اجرای نا صحیح، افشای اطلاعات و فقدان جامعیت است.

- **تهدیدهای منتج شده از عدم بکارگیری:** می تواند نتیجه ی وقفه در یک سرویس باشد، مثلاً به دلیل عدم پذیرش سرویس، دزدی و خراب کاری، آتش سوزی و حوادث طبیعی.

- **تهدیدهای منتج شده از افت کارایی:** می تواند به دلیل وقفه، تغییر دادن و یا جعل کردن باشد. وقفه ممکن است به دلیل عدم پذیرش یک سرویس باشد که می تواند کارایی سیستم را تنزل دهد. تغییر اطلاعات و رمز سیستم به دلیل دست یابی غیر مجاز نیز ممکن است باعث کاهش کارایی سیستم شود.

- **تهدیدهای منتج شده از افشاء اطلاعات:** خیلی وقت ها افشاء اطلاعات شکلی از استراق سمع است که از دسترسی غیر مجاز به سیستم نتیجه می شود، و ممکن است باعث نسخه برداری غیر مجاز از اطلاعات

ضروری شود. این تهدیدات همچنین می‌تواند نتیجه یک تصادف یا اشتباهات انسانی باشد. اخیراً افشاء اطلاعات به مشکل بزرگی تبدیل شده است، همان طور که کوکی‌ها¹ در رایانه‌ها اطلاعات را گرفته و انتقال می‌دهند.

- **تهدیدهای منتج شده از فقدان جامعیت:** ممکن است نتیجه دسترسی غیر مجاز در جایی که یک مزاحم می‌تواند راهی برای کپی برنامه‌ها و اطلاعات به دست آورد، باشد.
- **وقفه:** این یک دست‌یابی غیر مجاز به منابع سیستم است که برنامه یا اطلاعات را تغییر می‌دهد یا حذف می‌کند و موجب درست کار نکردن برنامه و خراب شدن سخت افزار می‌شود.
- **تغییر:** نتیجه دست‌یابی غیرمجازی است که برنامه یا اطلاعات جدیدی را جایگزین برنامه‌ها یا اطلاعات سیستم می‌کند.
- **جعل:** ساخت یا تغییر وضعیت برنامه‌ها یا داده‌های سیستم توسط قواعد یا داده‌های جعلی است.
- **رهگیری - دریافت:** نتیجه دست‌یابی غیر مجاز در سیستم است که سیستم را به کپی غیر قانونی رمزها و داده‌ها هدایت می‌کند.

➤ انواع آسیب پذیری

پی فلیگر² (2006) آسیب پذیری سیستم را بر اساس بعضی از تهدیدهای بالا محاسبه و آنها را طبقه‌بندی می‌کند. طبقه بندی آسیب پذیری‌ها بر اساس سخت افزار، نرم افزار و داده‌ها به صورت زیر است:

¹ cookies

² Pfleeger and Pfleeger

- سخت افزار مرکب از:
وقفه - رهگیری - دریافت - جعل - تغییر
- نرم افزار مرکب از:
وقفه - رهگیری - دریافت - جعل - تغییر
- داده مرکب از:
وقفه - رهگیری - دریافت - جعل - تغییر

5- منابع تهدیدهای امنیت اطلاعات

تهدیدهای امنیتی در سیستم های رایانه ای از متنوع بودن منابع شروع می شوند. مطابق اظهارات کیزا (2005) منابع اصلی تهدیدهای امنیتی عبارتند از:

ضعف فلسفه ی طراحی، آسیب پذیری زیر ساخت شبکه و پروتکل ارتباطی، رشد سریع فضای سایبر، رشد تعداد نفوذگرها، آسیب پذیری در سیستم عامل و نرم افزار رایانه، مهندسی اجتماعی، دزدی فیزیکی، عوامل اجرایی داخلی

1) فلسفه طراحی

فلسفه طراحی به ویژه در اینترنت و در شبکه جهانی باعث پیشرفت زیادی شد. اگر چه همین مورد یک منبع همیشگی از مشکلات زیان آور شبکه بوده است، در اصل رشد اینترنت و شبکه جهانی بر اساس یک فلسفه معماری باز (متن باز) و در حال توسعه بوده. این فلسفه در طی سال ها باعث

رشد اینترنت و شبکه جهانی شده است و ذهن های خلاق و ماجراجو را به سمت کمک داوطلبانه برای زیر بنای شبکه جهانی و پروتکل جذب کرده است. این فلسفه بر اساس یک طرح واضح و کامل نبوده و فقدان طرح جامع طراحی و پیشرفت به درخواست کمک برای پروتکل «RFPS» پاسخ داده و موجب آسیب پذیری در زیر بنای شبکه رایانه شده است.

(2) آسیب پذیری های زیر ساخت شبکه و پروتکل های ارتباطی

بر اساس یک معماری باز وسیع اما موفق و فلسفه طراحی در حال ساخت، زیربنای شبکه رایانه ای و پروتکل های متناظر آنها جانشین هم می شوند و پیشرفتی همراه با آسیب پذیری شدید و نا شناخته را دنبال می کنند. نمونه هایی از این آسیب پذیری های متعدد شامل سه راهی تبادل¹ است، سه راهی تبادل در حالتی که موفقیت آمیز عمل کند، ارتباطی مجازی بین سرور و کاربر ایجاد می کند. قبل از هر گونه ارتباط بین دو طرف، به ارتباط مجازی نیاز است. این فرایند با ارسال یک بخش TCP به همراه یک سری پالس همزمان کننده²، به وسیله میزبان یا مشتری شروع می شود. سرویس دهنده اینترنتی با یک نشانه شناخته شده معتبر³ به همراه یک نشان همزمان کننده پاسخ می دهد و کاربر اول با یک بسته که تنها با یک نشان شناخته شده، پاسخ را می دهد. و روش سه راهی تبادل از این جاست که از یک مشکل شکاف نیمه باز آسیب می بیند. وقتی که کاربر یک راه ارتباطی به وجود می آورد سرویس دهنده به او اعتماد کرده و درگاه ورودی را برای

¹ Three way handshake

² SYN

³ ACKN

ارتباطات آینده کاربر باز می‌کند. به محض این که درگاه نیمه باز به حالت باز شده باقی می‌ماند یک مزاحم می‌تواند وارد سیستم شود. زیرا وقتی که یک درگاه باز می‌ماند، سرویس دهنده هنوز می‌تواند مسیرهای دیگری با دیگر کاربران که می‌خواهند ارتباط برقرار کنند، ایجاد کند. چندین درگاه نیمه باز این اجازه را به حمله کنندگان امنیت پروتکل‌های شبکه‌های TCP/IP و UDP می‌دهد که کلاهبرداری کنند و آدرس‌های اینترنتی که از عناصر منبع اصلی بوده‌اند را مخدوش کرده و آدرس‌های جعلی و ساختگی را جایگزین کنند. پس کاربر اصلی از بین رفته و سرویس دهنده نیز با بسته‌های اینترنتی مخرب پر شده و از بین می‌رود. نمونه‌های دیگر آسیب‌پذیری طراحی زیر ساخت می‌تواند در طراحی درگاه¹ باشد. درگاه‌ها در ارتباط شبکه بسیار مورد استفاده قرار گرفته‌اند. درگاه‌های معروفی وجود دارد که توسط فرایندها استفاده شده و خدماتی را ارائه داده‌اند. برای مثال درگاه‌های صفر تا 1023 به طور گسترده توسط سیستم به کار گرفته می‌شوند که افراد مزاحم می‌توانند این درگاه‌ها را شناسایی کنند و با ردیابی آنها درگاه‌های جدیدی به وجود بیاورند و سیستم هم با آنها مصالحه کند.

طراحی ضعیف دیگر، استفاده از تسلسل شماره‌ها در مدت ارسال موارد TCP و UDP است. ترتیب شماره‌ها عددهای اختصاص داده شده به هر مورد است که نظم ورود موارد ارسال شده را نشان می‌دهد. (به محض دریافت بسته‌های اینترنتی، در یک ارتباط دو طرفه در مدتی که هر دو عناصر فرستنده هم‌زمان در سیستم دو طرفه ارتباط دارند، این مورد دریافت می‌شود). در یک حمله، شماره تسلسل حمله کننده از ارتباط بین دو یا

¹ Port

تعداد بیشتری از عناصر جلوگیری می‌کند و تسلسل شماره بعدی را حدس می‌زند. در یک جلسه ارتباطی، مزاحم آدرس‌های اشتباهی را به وسیله بسته‌های اینترنتی برای سرویس دهنده می‌فرستد و سرویس دهنده یک بسته برای کاربر ارسال می‌کند.

دیگر حملات آسیب‌پذیری، حملات دوره‌ای، بسته‌های اینترنتی خالی، پر شدن حافظه میانیجی¹ و ربودن اطلاعات است.

(3) رشد سریع فضای سایبر

رشد شگرف در فضای سایبر و تعداد کاربران آن، بدون هیچ گونه تشویقی، وجود داشته است. افزایش تعداد کاربران مشکلات امنیتی را به وجود می‌آورد، همان‌طور که خیلی از افراد به شبکه اینترنت می‌پیوندند، شبکه اینترنتی نیز با این افراد با انگیزه‌های مشکوک محصور می‌شود و این افراد یک ریسک بالقوه را در اطلاعات اینترنت و تهدیدهای امنیتی که با آن سروکار دارند، مطرح کرده‌اند. آمار گرفته شده از شرکت امنیتی سیمانتیک² نشان داده است که فعالیت‌های اینترنتی حدود 64 درصد در هر سال رشد می‌کند. همین آمار نشان داده است که در طول 6 ماه اول سال 2002، شرکت‌هایی که به اینترنت وصل شده‌اند به طور متوسط 32 بار در هفته مورد حمله قرار گرفته‌اند بودند در حالی که در 6 ماه آخر سال 2001 این حمله‌ها فقط 25 بار در هر هفته بود.

سیمانتیک در هر ماه بین 400 تا 500 نوع ویروس جدید و حدود 250 نوع آسیب‌پذیری در برنامه‌های رایانه‌ای را گزارش می‌دهد (مبارزه با

¹ Buffer

² Symantec

تهدیدهای شبکه امنیتی، 2002¹. در واقع، افزایش میزان رشد اینترنت بزرگترین تهدید امنیتی است. در این مورد نفوذگرهای بسیاری وجود دارند که آسیب رسان هستند.

(4) رشد تعداد نفوذگرها

اگر چه دیگر عوامل به میزان قابل توجهی در تهدیدهای امنیتی شرکت کرده اند، اما شاید بیشترین میزان رشد عوامل مربوط به نفوذگرها باشد. کلمه نفوذگر معانی مختلفی دارد که در اینجا معنی منفی آن مد نظر است. نفوذگر یک کارشناس رایانه بوده که اطلاعات زیادی در مورد محاسبات و برنامه نویسی دارد. در اینجا نفوذگر عامل آسیب رسانی است که می خواهد اطلاعات را با پردازش آن، به دست آورد، مثلاً به منظور اهداف مختلفی مثل سرقت اطلاعات و داده ها و تغییر آن ها در سیستم، از راهی غیر مجاز به سیستم دسترسی پیدا می کند.

نفوذگرها سه نوع هستند: شکننده ها یا کرکر²، هکتیویست ها³ و تروریست های شبکه. کرکرها نفوذگرهای بدی هستند. (به خاطر بیاورید که اگر معنای بد نفوذگر را کنار بگذاریم، معنی ساده آن یک کارشناس خبره رایانه است) نفوذگرهای خوب به شرط وجود کرکرها بوجود می آیند، نه فقط به این خاطر که کرکرها وقتی در حال کار با رایانه هستند لقمهء خوبی برای جویدن هستند، بلکه به خاطر تفکیک خودشان از آدم های بد، نمی توان یک تفکیک بین نفوذگرهای خوب و بد به دست آورد و شرایط مجدداً با هم عوض می شوند. نکته جالب توجه این است که به تازگی گونه ای از

¹ Battling the Net Security Threat

² crackers

³ hackers

کرکرهای اصلاح شده به وجود آمده‌اند که در اجرای قانون، مهارت‌هایشان را توسط نمایندگی‌ها برای به دام انداختن افراد مهاجم به کار می‌برند. کسانی که عملیات هک انجام می‌دهند نفوذگرهای باهوش، ماهر و با انگیزه هستند. مانند افراد عمل‌گرا، نفوذگرها دارای تعصب و پشت‌کار هستند (مثال: بمباران توسط پست الکترونیکی).

تروریست‌های شبکه‌های کسانی هستند که تهدید به حمله می‌کنند یا می‌توانند به سازمان و حتی به سیستم‌های رایانه‌ای ملی حمله کنند. آن‌هم به دلایلی مثل:

- انتقام‌گیری یا کینه‌جویی
- شوخی، دست‌انداختن و شوخی‌های فریبنده
- ایجاد ترس و وحشت
- جاسوسی‌های سیاسی و نظامی
- نفرت
- منفعت / شهرت / سرگرمی و بدنامی اشخاص
- جهالت

نفوذگرها موفق شده‌اند این تهدیدها را در عنوان خبرها در رایانه‌ها، به صورت ویروس‌ها و عدم پذیرش خدمات ارائه شده مطرح کنند. بر اساس اخبار موجود درباره ویروس‌ها و هویت سارقین شکست خورده که به صورت امری عادی در آمده‌اند، کاربران رایانه، طراحان خط‌مشی‌ها و وضع‌کنندگان قانون به خاطر رشد تهدیدها در امنیت شخصی و ملی‌شان سر در گم شده‌اند.

5) آسیب پذیری در سیستم نرم افزاری

طراحی نرم افزار و توسعه آن با طراحی سخت افزار و توسعه آن بسیار متفاوت است و به دلیل زیاد بودن میزان جزئیات، احتمال ایجاد اشتباهات بیشتر می شود. در طول عمر یک نرم افزار، اشتباهات به وجود آمده در هر مرحله به راحتی می توانند تشخیص داده شوند و نیز تصحیح گردند. همان طور که مشخص است، آسیب پذیری در بین منابع نرم افزاری به خاطر اشتباهات انسانی و پیچیدگی نرم افزار بوده است.

- چگونگی برخورد با آسیب پذیری نرم افزار

راه حل های مختلفی برای برخورد با آسیب پذیری وجود دارد، مثل آزمون رشد برای بازبینی و تصحیح کردن.

- **آزمون رشد:** هر برنامه نویس می داند که برنامه ها پیچیده هستند و طراحی آنها مشکل است و برای تثبیت نتایج آنها، اغلب با مشکل مواجه می شوند. حتی بعد از صرف زمان زیاد و هزینه بسیار، برنامه شناخته شده ای وجود ندارد که بتواند با دقت مشکلات برنامه را تست کند. برای مطمئن شدن از عملکرد یک نرم افزار باید هنگام آزمایش آن دقت زیادی کرد. آزمایش برنامه اطمینان می دهد که برنامه دارای خصوصیات قانع کننده ای است و مشکلات آن کشف شده و عیب و نقص ها رفع شده اند. اما آزمایش به خاطر بعضی شرایط محدود می شود. مثلاً یک آزمایش کامل برای یک پروژه بزرگ خیلی پر هزینه و گاهی غیر عملی و ناموفق است، بنابراین تعداد دیگری از روش های آزمایش به کار گرفته شده اند. یکی از این روش ها آزمون رشد است، چیزی که شامل یک گروه از آزمایش های تصادفی درباره

نرم افزار در مدت مرحله توسعه آن است. در آزمون رشد از روش های ریاضی به خاطر اطمینان بخش بودن آن استفاده می شود. البته این روش ها کاملاً بدون خطا نیستند چون ممکن است همه اشتباهات در این قسمت مورد محاسبه نباشد، بنابراین این آزمون تنها نمی تواند همه این اشکالات را رفع کند.

• **بازبینی و تصحیح:** این یک جریان است که دارای اصول رسمی مثل دلیل صحت و اصول رسمی غیر ثابت مثل آزمایش برای نشان دادن ارتباط بین قوانین و خصوصیات اولیه ، می باشد.

یک شبکه که بزرگترین تهدیدهای امنیتی را به سامانه های رایانه ای عرضه می کند، خطاهای سیستم عامل است. سیستم عامل یک نقش اساسی را در اداره کردن شبکه رایانه، کنترل کردن و آماده کردن خدمات اساسی و همچنین در امنیت شبکه و دستیابی به منبع جامع سامانه ایفا می کند. یک سیستم عامل ضعیف به هر کسی اجازه می دهد به سامانه راه پیدا کند و هر کاری، که کاربر مجاز می تواند انجام دهد را انجام دهند. مثل تغییر دادن پرونده ها، نصب کردن یا عوض کردن نرم افزار و یا فرمت کردن مجدد درایوها. هر سیستم عامل با تعدادی آسیب پذیری امنیتی مطرح شده است. در واقع خیلی از آسیب پذیری های امنیتی مخصوص سیستم عامل ها هستند. هکرها اطلاعات خصوصی سیستم عامل را جست و جو می کنند. مثلاً جست و جوی پرونده ها برای بهره برداری.

هرچه سطح برنامه نویسی پایین تر باشد اشکالات نرم افزار سخت تر پیدا می شوند و میزان بازبینی و تصحیح مانع شکست خوردن آن می شود.

تهدیدهای امنیتی نا مشخص: اثر عوامل داخلی

وقتی یک اتفاق برای سیستم اطلاعاتی سازمان داده شده می افتد، فرصت برای افراد سودجو زیاد می شود. طبق مطالعات مختلف، اجرای داخلی، خود یک تهدید امنیتی بزرگتر از نفوذگرهای بیرونی است. در سال 1997 شرکت های حسابداری ارنست و یانگ¹ با حدود 4220 مدیر فنی اطلاعات و افراد حرفه ای از کل جهان درباره امنیت شبکه هایشان مذاکره کردند. از بین آنها 75 درصد از مدیران به این اشاره کردند که به کاربران خود اطمینان کرده اند و کارمندان آن ها از سیستم اطلاعاتی شان سوء استفاده کرده اند. 42 درصد از ارنست و یانگ گزارش داده اند که در سال گذشته حدود 43 درصد از دست کاری ها در سیستم توسط کارمندان خودشان اتفاق افتاده است. حوزه تجاری دولتی که مأمور یافتن و ورود به اطلاعات امنیتی است، دریافت که در شرکت های کوچک، 32 درصد از بدترین وقایع اتفاق افتاده توسط عوامل داخلی روی داده و این عدد به 48 درصد در شرکت های بزرگ رشد یافته است، هر چند اعدادی کمی خفیفتر مشابه در ممیزی جرایم رایانه ای سال 2001 به دست آمده بودند (نشریه ماهانه NISCC 2002). در آن بررسی، 25 درصد از کارمندان سازمان یا کارمندان سابق در مقایسه با 75 درصد از نفوذگرها و دیگر جرم های سازمان داده شده، مرتکب جرم اینترنتی شده بودند.

دیگر مطالعات نشان داده اند که درصد کمی از عوامل داخلی به امنیت شرکت خسارت وارد می کنند. همان طور که داده ها دلالت می کنند، خیلی از

¹ Ernst & Young

هیأت‌های اجرایی و مدیران امنیتی شرکت برای مدت طولانی در معاملات با افراد بدی که اسرار شرکت را به شرکت‌های رقیب می‌فروشنند، اهمال می‌کنند.

(6) مهندسی اجتماعی

این یکی از منابع تهدیدات امنیتی است، چیزی که به صورت تصاویری جذاب اما جدی است. مهندسی اجتماعی شامل یک سری از روش‌های یک مهاجم، نفوذگرهای داخل سازمانی یا خارج سازمانی است که با تغییر هویت دادن به عنوان یک کاربر مجاز، می‌توانند از سیستم بهره ببرند. این کار می‌تواند با استفاده از روش‌های مختلفی مثل جعل هویت یک شخص شناخته شده برای دستیابی به سیستم یا از طریق تلفن و حتی از طریق نوشته‌ها باشد.

(7) سرقت فیزیکی

دزدی فیزیکی دستگاه‌های اطلاعاتی مثل لپ‌تاپ‌ها، رایانه‌های جیبی (PDA ها)¹ و دیسک‌ها، در حال افزایش است. با کوچک سازی دستگاه‌های ذخیره سازی مثل حافظه‌های فلش این نوع دزدی بیشتر می‌شود.

¹ Personal Digital Assistant

همچنان که درخواست برای اطلاعات به وسیله مشاغل برای باقی ماندن در رقابت و به وسیله ملت ها برای نیرومند باقی ماندن، داغ تر می شود دزدی لپ تاپ ها و رایانه های جیبی بیشتر می شود. یک لیست کلی از وقایع اتفاق افتاده به وسیله دزدان لپ تاپ وجود دارد، از قبیل گزارش مفقود شدن یک لپ تاپ که برای ثبت وقایع رخ داده در مورد گسترش پنهانی فناوری هسته ای استفاده می شده از یک ساختمان شش طبقه در قرارگاه مرکزی سازمان سیاسی آمریکا در ژوئن 2000. در مارس همان سال یک حسابدار انگلیسی برای M15 کار می کرد، این شهروند انگلیسی در حالی که در ایستگاه پدینگتون لندن منتظر ترن ایستاده بود عامل جاسوسی لپ تاپش را از بین پاهایش ربود. در دسامبر 1999 شخصی یک لپ تاپ را از ماشین بونو (Bono)، رهبر خواننده های ارکستر u2 دزدید، این لپ تاپ حاوی ماه ها کار بسیار سخت در متن موسیقی بود.

کادر 2 - سرقت لپ تاپ ها

روزانه در رسانه های خبری داستان های زیادی وجود دارد از کسانی که لپ تاپ خود را همراه با اطلاعاتی حساس از دست داده اند. طبق گزارش شرکت بیمه رایانه، تقریباً 319000 لپ تاپ در سال 1999 دزدیده شده است. (در کل مبلغی بیش از 800 میلیون دلار فقط برای سخت افزار می شود). هر ساله هزاران لپ تاپ از مدیران شرکت ها به سرقت می رود که حاوی اطلاعات سری چند ساله شرکت ها می باشد.

6- بدافزار ها ی رایانه ای و راهکارهای مقابله

تهدیدات سیستمی ویژه

در این تحقیق به خطرات جهانی می پردازیم نه رویدادهایی که بر افراد و یا سازمان های معمولی تجاری و غیردولتی تأثیر می گذارند. اما این احتمال وجود دارد که رویدادهای کوچک تبدیل به وقایعی بزرگ گردند. از طرف دیگر تفاوت بین یک واقعه بزرگ و یک رویداد کوچک لزوماً از تفاوت های فناوری ناشی نمی شود بلکه اختلاف صرفاً در مقیاس و اندازه یک واقعه است. از این رو باید نگاه جامعی به تهدیدات اصلی فناوری محور و همچنین واژه شناسی مخصوص آن داشته باشیم:

- حوادثی که بر زیرساخت ها تأثیر می گذارند: این حوادث می توانند ماهیتی فیزیکی داشته باشند، مثلاً آتش سوزی و یا وقوع سیل در یک مکان حیاتی؛ و یا «منطقی» باشند، که معمولاً به معنای خرابی در فعالیت های نرم افزاری است.

- ورود بار بیش از حد به سیستم: سیستم های اطلاعاتی به گونه ای طراحی شده اند که دارای سطوح مشخصی از ظرفیت و توان انتقال داده ها هستند. معمولاً پیش بینی هایی در مورد نیازها و تقاضاها انجام گرفته و این داده ها تبدیل به شاخصه های حجم بار در نرم افزارها و سخت افزارهای حوزه فناوری اطلاعاتی می شوند. در شرایط غیرعادی، اگر منابع کافی خدماتی وجود نداشته باشند، سیستم ها از کار می افتند. این سیستم ها به طور معمول خود را خاموش می کنند و یا فعالیت شان مختل می گردد. در جاهایی که مجموعه ای از سیستم های به هم پیوسته فعالیت می کنند، یک

خطا و یا بار بیش از حد در یک سیستم، در صورتی که بدرستی مسدود نشود، ممکن است منتج به زنجیره ای از خطاها شود.

حملات منطقی عمدی:

اینها حملاتی هستند که بیشترین توجه را معطوف به خود می کنند و عبارتند از:

بمب منطقی

بمب منطقی ابتدایی ترین و ساده ترین نوع بدافزار است. این بدافزار برنامه ای پنهانی است و نتایجی را ایجاد می کند که طراحان سیستم انتظار آن را ندارند. برون داد این نوع برنامه ها ممکن است عبارت باشند از: لطیفه ای که در صفحه ظاهر می گردد، خاموشی کل سیستم، یا زنجیره ای پیچیده از رویدادها که می تواند به یک کلاهبرداری بینجامد. حمله با بمب های منطقی احتمالا از دهه 1960 آغاز شد. یکی از نمونه های اولیه این نوع حملات می تواند واقعه خط لوله ترانس سبیریا باشد که در سال 1982 رخ داد. در این واقعه انفجار بسیار بزرگی روی دادند اما گفته می شود که رایانه ها نیز دستکاری شده بودند. از دیگر نمونه ها می توان به موارد زیر اشاره نمود: تلاش برای پاک کردن داده های موشک ها در شرکت صنایع تسلیحاتی "جنرال داینامیکس"، اقدامات برنامه نویسی ها در بانک "دویچه مورگان گرنفل" در سال 2000، شرکت خدمات درمانی "مدیکو هلت سولوشنز" در سال 2003.

اسب تروجان

اسب تروجان برنامه ای است که درب پشتی در رایانه ها ایجاد می کند. این امر در اصل با ایجاد دسترسی مخفی از راه دور پدید می آید. پس از ظهور اینترنت، می توان از هر نقطه در شبکه به رایانه ها دسترسی داشت. از تروجان می توان برای بررسی فعالیت های کاربران و یا پاک کردن و سرقت داده ها استفاده نمود. از این نوع بدافزارها می توان برای بدست گرفتن کنترل یک رایانه استفاده کرد و سپس همین رایانه را برای پنهان نگه داشتن هویت مهاجمین واقعی بکار برد. رایانه ای که تحت کنترل گرفته شده در اصطلاح با نام "زامبی" خوانده می شود و تبدیل به پلت فرمی (خط مشی) برای انجام حملات دیگر می شود.

کی لاگر¹

کی لاگر برنامه ای است که ضربات وارده بر صفحه کلید یک رایانه را ثبت می کند. هدف از اجرای این برنامه معمولاً دستیابی به رمزهای کاربران است.

ویروس

ویروس برنامه ای است که می تواند خود را باز تولید کند و معمولاً یک تروجان و یا بمب منطقی را با خود حمل می کند. باز تولید بدین معناست که موفقیت مهاجمین در گرو دسترسی سریع به رایانه هدف نیست. ویروس ها در دهه 1980 و با ظهور رایانه های شخصی و استفاده گسترده از فلاپی دیسک ها قدرت زیادی یافتند. عنوان ویروس در سال های 1984 و 1986 بدین بدافزارها اطلاق گردید یعنی زمانی که اولین حامل ویروس "بخش راه

¹ - Key logger

انداز سیستم¹ با موفقیت ظاهر شد. در سال 1995 روش هایی کشف شد تا کدهای شرور² را بصورت زیر برنامهء ویروس پنهان سازد. در سال 1999 با توسعه تکنیک هایی ، نفوذ به ایمیل ها ، برنامه های ایمیلی (Happy99,Melissa) و ایجاد درب های پشتی ویروس ها نیز رشد داشتند. براساس برآوردها در سال 2000 ویروس « I LOVE YOU » در حدود 10 میلیون دلار آمریکا خسارت وارد کرد. یکی از دلایل این رویداد، سرعت بالای این ویروس در انتقال و پخش بود.

روت کیت³

عبارت روت کیت در ابتدا برای اشاره به برنامه ای بکار می رفت که کنترل یک رایانه را بطور کامل بدست گرفته و در اختیار فرد مهاجم قرار می داد ، امروزه این عبارت به بد افزاری گفته می شد که در سیستم عامل یک رایانه به خوبی پنهان می شود و بنابراین شناسایی و حذف آن مشکل می شود. یک روت کیت ممکن است کلاهی برای حمل یک ویروس باشد.

بد افزارهای وب محور

بد افزار می تواند در صفحات وب سایت ها نیز جاسازی شود. وب سایت ها معمولاً شامل زبان هایی مانند جاوا اسکریپت هستند . از این زبان برای نمایش یک تصویر متحرک و یا تبدیل درون داد به یک شکل بر روی صفحه استفاده می شود .اما از این زبان می توان برای نصب بدافزار نیز

¹ - Boot sector

² - rough codes کد های که برای تولید ویروس بکار می روند

³ - Root-kit

استفاده کرد. تکنیک دیگر، استفاده از پیکسل بر روی صفحه وب سایت است. این پیکسل ها معمولاً توسط کاربران رؤیت نمی شوند اما شامل اشاره گر و یا لینکی به یک بدافزار مخرب هستند.

در حمله انکار سرویس مقادیر زیادی از ترافیک شبکه ای به یک ماشین خاص در سیستم های متصل به اینترنت و شبکه های آن منتقل می گردد. اگر حمله از یک رایانه صورت پذیرد براحتی می توان آن را کنترل کرد، بنابراین مهاجمین از تعداد زیادی ماشین تحت کنترل خود استفاده می کنند تا حملات انکار سرویس توزیع شده¹ (DDoS) را انجام دهند. مهاجمین در ابتدا باید رایانه هایی که برای حمله مورد استفاده قرار خواهند گرفت از طریق ایمیل یا بدافزارهای وب محور، کنترل نمایند. مهاجم فعالیت های خود را از طریق یک رایانه فرماندهی و کنترل نیز توسط مهاجم تسخیر شده از جای دیگری هدایت می کند.

بات نت ها

یکی از عوامل خطرات امنیت سایبری سیستمی عبارت است از تعداد زیادی رایانه متصل به اینترنت که توسط نرم افزارهای زیان آور تسخیر شده اند. این بات نت ها به یکدیگر متصل شده و بات نتی بالغ بر صدها، هزاران و یا حتی میلیون ها رایانه را تشکیل می دهند. از نمونه های اخیر بات نت ها می توان به شبکه کونفیکر² اشاره نمود که 7 میلیون رایانه را آلوده کرده بود و یا شرکت ماریپوسا در اسپانیا که از 7/ 12 میلیون رایانه

¹- Distributed Denial of service

²- Conficker

تشکیل شده بود. (McMillan, 2010). بات نت ها در سراسر جهان پخش هستند. بر اساس یافته های پروژه هانی نت¹ (2006-2007) بیشترین میزان شیوع بات نت ها را به ترتیب کشورهای برزیل، چین، مالزی، تایوان، کره و مکزیک شاهد هستیم. بیشترین تعداد سرورهای فرمان و کنترل این رایانه ها به ترتیب در کشورهای آمریکا، چین، کره، آلمان، هلند مستقر بودند. (Zhuge et al., 2007) در بازار های غیر قانونی می توان بات نت ها را با قیمتی حداقل تا 400 دلار آمریکا برای هر بات، اجاره نمود و حتی سرویس های پشتیبانی نیز برای آنها ارائه می گردد. بات نت ها زیر ساخت هایی برای حمله هستند که پهنای باند لازم را ارائه کرده و مهاجم را قادر به دور زدن محدودیت های شبکه ای می کنند و همچنین مکان آنها را نیز پنهان می نمایند، منبع نهایی چنین حملاتی را به ندرت می توان با اطمینان به یک کشور خاص نسبت داد چه برسد به یک فرد خاص. (کمیته اتحادیه اروپا در مجلس اعیان، 9:2010)

سوءاستفاده / حملات روز صفر

سوء استفاده روز صفر، حمله ای است که از آسیب پذیری های تکنیکی ناشناخته برای تأثیرگذاری استفاده می کند. بیشتر این حفره های امنیتی به صورت تدریجی و ابتدا از آزمایشات یا مقالات محققین آغاز می شوند و سپس به آهستگی از طریق شبکه ها و رایانه ها توسعه می یابند. در چنین شرایطی معمولاً ارائه کنندگان فناوری های امنیتی مانند ویروس یاب ها، فایروالها و اسکنر های شناسایی نفوذهای پنهانی، می توانند بدافزار را قبل از

¹ - Honeynet project

اینکه آسیبی جدی وارد کند، شناسایی و مسدود نمایند. در وضعیت روز صفر، قبل از اینکه ابزار شناسایی و پیشگیری ارائه شوند، حمله در سطح وسیعی گسترده می شود.

در سال 2009، شرکت سیمتک 12 عدد از این نوع آسیب پذیری ها را ثبت نمود. چهار عدد از این آسیب پذیری ها در نرم افزار Adobe PDF Reader و شش تا نیز در نرم افزار های مایکروسافت به مانند برنامه آفیس و سرور اطلاعات اینترنت¹ قرار داشتند. این آسیب پذیری ها هم در حملات کلی و معمولی سرقت رمز کاربر و هم در کدهای مضر که برای حمله به مدیران ارشد سازمان ها طراحی شده اند، مورد استفاده قرار می گیرند. (symantic, 2010:45). تنها یکی از این آسیب پذیری های روز صفر در نرم افزار internet explorer کافی بود تا به سیستم های شرکت های گوگل، ادوب و تعدادی دیگر از شرکت های فناوری نفوذ کند.

شبکه های اجتماعی: تهدیدهای گسترده، محدودیت دسترسی به

اطلاعات شخصی

برای دیدن بسیاری مسائل امنیتی ناشی از رویکرد شبکه های اجتماعی، مؤسسه Sophos به تازگی یک نظرسنجی رسانه اجتماعی را انجام داده است که آیا سازمان ها ی پاسخگو با رخدادهایی از قبیل هرزنامه، سرقت هویت یا بدافزار مواجه شده اند. از تقریباً 2000 نفر که در این نظرسنجی شرکت کرده اند، 71 درصد گزارش داده اند که برای آن ها یا یکی از همکارانشان روی

¹ - Internet routers

سایت شبکه اجتماعی هرزنامه ارسال شده، 46 درصد: سرقت هویت صورت گرفته و 45 درصد: بدافزار فرستاده شده است. از میان باقی پاسخ دهندگان، برخی قربانی این رخدادهای نشده اند و برخی دیگر مطمئن نبودند. در نظرسنجی اخیر شبکه های اجتماعی نیز از کاربران کامپیوتر پرسیده شده که به نظر آن ها کدام شبکه اجتماعی به عنوان بزرگترین خطر امنیتی محسوب می شود. شبکه فیس بوک با 81 درصد آرا به عنوان بزرگترین خطر در رده اول قرار گرفت. در نظر سنجی سال گذشته که برای اولین بار این سوال مطرح می شد، شبکه فیس بوک با 60 درصد آرا به عنوان پرخطرترین شبکه محسوب شد. در نظرسنجی امسال شبکه توییتر و مای اسپیس هر کدام با 8 درصد آرا در رده های بعدی قرار گرفتند.

هرزنامه ایمیل و سرقت هویت هدفدار هنوز یک تهدید هستند: گزارش اخیر comScore نشان می دهد که یک کاهش بزرگ 59 درصدی در استفاده از ایمیل در بین افراد 12 تا 17 ساله و یک کاهش 34 درصدی برای رده سنی 25 تا 34 سال وجود دارد. بسیاری از افراد به عنوان یک روش ارتباطی ترجیح می دهند از فیس بوک، پیام متنی و توییتر استفاده کنند. در مقایسه با سه ماهه اول سال 2010 که 27٪ از پیوست های ایمیل حاوی تهدید بودند، در سه ماهه اول سال 2011 تنها 16٪ این پیوست ها حاوی تهدید بوده اند. در حال حاضر کلاهبرداران ترجیحا به عنوان ابزار ارسال بدافزار، بیشتر از پیوست های HTML نسبت به فایل های اجرایی ".exe" استفاده کنند.

در نیمه اول سال 2011، ایالات متحده یکبار دیگر با توزیع حدود 13 درصد از ترافیک هرزنامه های جهان در میان کشورهای توزیع کننده هرزنامه در صدر جدول قرار گرفت. کشورهای هند، روسیه، کره جنوبی و برزیل در طی شش ماه اول سال با مسدود کردن 6 درصد از هرزنامه ها و با توجه به جمعیت زیاد آنلاین (به اینترنت) این کشورها، به طور آشکاری از نقص حفاظت سیستم ها در مقابل بدافزارهای هرزنامه ای رنج می برند.

در مقیاس جهانی، در نیمه اول سال 2011 آسیا در تولید هرزنامه از اروپا پیش افتاده و نسبت به نیمه اول سال 2010 از 33 درصد به 40 درصد رشد داشته، در حالیکه در اروپا در این زمینه به 29 درصد کاهش یافته است.

رایانه قابل حمل: مراقب autorun ویندوز باشید

بین ماه های مارس و می امسال، کاهش قابل ملاحظه ای در تعداد کامپیوترهای آلوده شده به وسیله بدافزارهایی که از ویژگی autorun ویندوز سوء استفاده کرده بودند، وجود داشت. آلودگی های autorun حدود 59 درصد روی رایانه های با سیستم عامل xp و 74 درصد روی رایانه های با سیستم عامل ویستا کاهش یافته اند.

با این حال، یک مطالعه که اخیراً توسط وزارت امنیت داخلی ایالات متحده انجام شده دریافت شده است که بزرگترین خطر رسانه های قابل حمل از تصمیم گیری ضعیف کاربران ناشی می شود. با توجه به گزارش بلومبرگ، مطالعه DHS نشان می دهد که کارمندان دولت در استفاده از درایوهای thumb و سی دی ها بی توجهی می کنند.

گزارش تهدیدات سایبری سیکو که هر سه ماه یک بار منتشر می شود، با استفاده از داده های جمع آوری شده از چهار بخش اصلی امنیت

سیسکو به دست می آید. این چهار بخش عبارتند از: سیستم پیشگیری از نفوذ (IPS)، IronPort، سرویس مدیریت از راه دور (RMS) و ScanSafe. در اینجا به مهمترین بخش های این گزارش می پردازیم:

رویدادهای بدافزاری وب

کاربران سیستم های بزرگ نرم افزاری شاهد به طور متوسط 135 بدافزار در هر ماه 2010 بوده اند که بیشترین میزان آن مربوط به ماه اکتبر با 250 بدافزار است. همچنین ماه اکتبر شاهد بیشترین میزان میزبان های بدافزار مخصوص وب با 16,905 عدد بوده است. در مجموع 38,811 میزبان یکتای بدافزار وب در سه ماهه چهارم 2010 مشاهده شده است.

بد افزار جاسازی شده

امروزه ریز رایانه ها با کارکردهایی محدود در بسیاری از اشیاء روزمره جای گرفته اند. این امر در مورد بسیاری از ماشین آلاتی که در فرآیندهای صنعتی، تجهیزات ارتباط راه دور و سیستم های تسلیحاتی بکار می روند نیز صادق است. توانایی پردازش برخی از این رایانه ها بسیار محدود است اما در برخی دیگر از ماشین آلات سیستم عامل هایی مشابه آنچه در رایانه های خانگی می بینیم بکار گرفته شده اند. نسخه های ویژه ای از ویندوز اکس پی همینک در سیستم های خودپرداز بانکی و یا در سیستم های صدور بلیط حمل و نقل بکار گرفته شده اند. نسخه هایی از سیستم عامل لینوکس در روترهای اینترنتی و نرم افزار های چند رسانه ای بکار گرفته می شوند. نسخه های سنتی نرم افزار سیستم عامل و برنامه ها در زمان استفاده در

رایانه های شخصی براحتی قابل اصلاح هستند اما بروز رسانی نرم افزار های تعبیه شده در سیستم ها سخت تر است . علاوه بر این تولید کنندگان اصلی و همچنین متخصصین تعمیرات می توانند نرم افزارهای مضر را در سیستم ها جای دهند که فرمان های پنهانی دیگری را قبول می کنند . ژنرال ویزلی کلارک و پیتربوین در مقاله ای در نشریه امور خارجی گزارش دادند که انفجار 3 کیلو تنی در خط لوله گاز سبیری در سال 1982 نتیجه فعالیت های سیا در جاسازی قطعات نادرست در تجهیزاتی بود که از روسیه خریداری شده بود . آنها همچنین اضافه نمودند که در زمان حمله هوایی اسرائیل به تأسیسات هسته ای سوریه در سال 2007 یک بد افزار ، سیستم پدافند هوایی سوریه را از کار انداخته و همین امر حمله هوایی را آسانتر نمود (Clark and Levin, 2009) . در سال 2009 دولت هندوستان از وجود یک بدافزار جاسازی شده در تجهیزات ارتباط راه دور ساخته شده در شرکت چینی هاوایی اظهار نگرانی نمود (spam fighter, 2009) .

شناسایی بدافزارهای وارد شده به رایانه های معمولی خانگی ساده است اما آزمایش سیستم های تعبیه شد بلاخص زمانی که آزمایشگر نمی داند یک سیستم پاک باید به چه شکلی باشد، بسیار سخت است .

حملات فیزیکی عمدی:

علاقه وافرانی که به حملات منطقی وجود دارد می تواند توجه را از حملاتی که دارای ماهیتی فیزیکی هستند منحرف سازد. از بسیاری جهات، استفاده از بمب ها، حمله مستقیم به سخت افزار رایانه ای و تخریب اتصالات کابلی ساده تر بوده و قابلیت تأثیرگذاری طولانی مدت آنها نیز بیشتر است زیرا تجهیزات آسیب دیده باید دوباره تهیه شده و نصب گردند.

مدتی طولانی است که گروه های سیاسی مخالف رایانه ها را هدف حملات خود قرار می دهند. در سال 1969، گروهی از طرفداران صلح با نام «بیویر 55» با استفاده از آهن ربا 1000 نوار حاوی اطلاعات را پاک کردند. بین سال های 1979 تا 1983 یک گروه فرانسوی به نام «کلودو» تعدادی رایانه را در شهر تولوز تخریب کردند. هیچکدام از این حوادث عوارض جانبی زیادی نداشتند. اما از آن زمان تاکنون، وابستگی اجتماعی به رایانه و سیستم های ارتباطی و همچنین به هم پیوستگی بین سیستم های حیاتی افزایش بسیار زیادی یافته است. پس از بمب گذاری سال 1993 در لندن توسط ارتش آزادی بخش ایرلند، شرکت بیمه لیودز در حدود 35 میلیون پوند غرامت بیمه ای پرداخت کرد و تقریباً به مرز ورشکستگی رسید (Coaff, 2003). در همان سال انفجار بمب در مرکز تجارت جهانی به بسیاری از شرکت های وابسته به رایانه تأثیر گذارد؛ 40 درصد از این شرکت ها در عرض 2 سال ورشکست شدند.

اگر به کابل های حامل ترافیک اینترنتی و دیگر سیستم های ارتباطی آسیب برسد، مسائل بسیار حادی ممکن است پدیدار شوند. در ژانویه 2008 و همچنین در دسامبر همان سال، قطع دو کابل، یعنی «کابل فیبر نوری جهانی اروپا-آسیا» و «سی می - وی» باعث قطع ارتباط در خاورمیانه و بخش هایی از آسیای شرقی شد (البته عربستان سعودی به علت استفاده از ماهواره تأثیر کمی از این واقعه پذیرفت) (Singel, 2008).

بمب الکترومغناطیسی

بمب الکترومغناطیسی (EMP) عبارت است از یک انفجار تابشی با انرژی بسیار بالا برای ایجاد یک موج با ولتاژ بسیار قوی تا بدین ترتیب قطعات رایانه ای از کار افتاده و دستگاه هایی که به این قطعات وابسته هستند بلا استفاده گردند. بمب الکترومغناطیسی یکی از چند نوع حمله سایبری راه دور است که منجر به آسیب های مستقیم دائمی می شود. بهترین عامل راه اندازی این بمب می تواند یک انفجار هسته ای در فاصله ای بسیار دور باشد. این مسأله برای اولین بار در سال 1962 و طی آزمایشات هسته ای «ستارفیش پرایم»¹ در اقیانوس اطلس تجربه گردید. در برخی تحقیقات، تأثیرات احتمالی این نوع حملات بر سیستم انتقال نیرو در آمریکا مورد بررسی قرار گرفته است. (Oak Ridge National Laboratory, 2010)

تلاش هایی انجام گرفته اند تا روش هایی غیر هسته ای برای ایجاد پالس الکترومغناطیسی ایجاد نمایند. «فرکانس رادیویی با انرژی بالا» (HERF) یکی از همین روش ها است. در تبدیل پدیده پالس الکترومغناطیسی به یک سلاح کاربردی برخی مسائل و مشکلات وجود دارند. اول اینکه، در یک چنین سلاحی نیاز به انتشار مداوم مقادیر زیادی از انرژی است که ابتدا باید ذخیره شده و سپس به سرعت آزاد گردد البته به گونه ای که خود اسلحه را تخریب نکرده و به افراد نزدیک آن نیز آسیب نرساند. دوم وسیله ای لازم است تا این انرژی را هدف گیری و هدایت نمایند تا به رایانه های خود مهاجم تأثیر نگذارد. سوم، شاید پیش بینی نتایج این حمله امکان پذیر نباشد. اگر قطعات رایانه ای در یک اطاق زیر زمینی و حفاظت شده قرار داشته باشند شاید از

¹- Starfish prime

این حمله جان سالم به در برند. تجهیزات رادیویی، که به آنتن نیاز دارند، آسیب پذیرتر هستند. (Crabbyolbastard, 2010).

روزنامه ساندی تایمز لندن در ژوئن 1996 گزارش داد که سلاح های فرکانس رادیویی با انرژی بالا برای سرقت 400 میلیون پوند از شرکت های مالی لندن مورد استفاده قرار گرفته اند. اما این گزارش تکذیب شد و البته مساله تعجب آور اینجا بود که هیچ اثری از عوارض جانبی به مانند تأثیرگذاری بر چراغ های راهنما رؤیت نشد.

تشعشعات خورشیدی عبارتند از مقادیر زیادی انرژی که در نتیجه انفجارهای بزرگ در خورشید ساطع می شوند. در هر 11 سال شاهد اوج فعالیت های خورشیدی هستیم. این تشعشعات، پرتوهایی در طیف الکترومغناطیسی ایجاد می کنند. در زمان بروز این تشعشعات، برخی انتقالات رادیویی - فرکانس بالا یا رادیو موج کوتاه - تقویت می شوند اما تأثیر اصلی بر ماهواره ها و رادارها وارد شده و فعالیت آنها دچار اختلال می گردد. انفجارهای شدید می توانند منجر به سوختن برخی قطعات رایانه ای موجود در ماهواره ها و یا شبکه های ارتباطی گردند. پس از یک طوفان خورشیدی بزرگ در سال 1989، برق اعظمی از ایالت کبک امریکا قطع شد. قبل از آن، بزرگترین طوفان در سال 1895 رویت شده بود. واحد هایی که دارای کابل ها دراز هستند و یا دیگر تجهیزات دارای آنتن در معرض بیشترین خطر هستند زیرا این قطعات می توانند انرژی آزاد شده را به سوی اجزای آسیب پذیر هدایت کنند. با این حال دانشمندان در مورد تناوب زمانی وقوع این تشعشعات و همچنین میزان انرژی لازم برای وارد آوردن آسیب های جدی بر قطعات

مدرن رایانه ای اختلاف نظر دارند. (Dyer and Owen, 2010) اوج فعالیت آتی خورشید در سال های 2012-2013 خواهد بود.

سلاح سایبری چیست؟

بین چیزی که باعث تأثیرات ناخوشایند و حتی کشنده می شود و یک سلاح، تفاوتی اساسی وجود دارد. سلاح یک نیروی هدایت شده است شلیک آن را می توان کنترل نمود، یک پیش بینی منطقی در مورد تأثیرات آن وجود دارد، و این سلاح به کاربر، دوستان وی، و یا اشخاص ثالث بیگناه آسیب نمی رساند.

بنابراین سؤالاتی که در ارزیابی هر نوع سلاح سایبری مطرح می شوند عبارتند از:

- آیا این چیزی است که هدف گیری و تأثیراتش را می توان کنترل نمود (آیا خطر شلیک به سوی دوستان وجود دارد؟)
- در حوزه هدف گیری انتظار چه موفقیت هایی را می توان داشت؟
- آیا آسیب های جانبی نیز وجود دارند؟
- چه منابع و مهارت هایی لازم هستند؟
- به چه میزان دانش و یا دسترسی داخلی به هدف نیازمند هستیم؟ و دسترسی بدین عناصر چقدر راحت است؟
- آیا سلاح را می توان قبل و یا در حین شلیک شناسایی کرد؟
- آیا ممکن است مهاجم بعد و یا در حین شلیک شناسایی شود؟
- تأثیرات واقعی حمله چه بوده و تا چه زمانی تداوم خواهند یافت؟

- یک حمله را تا چه زمان و قبل از اینکه توسط فناوری متقابل خنثی گردد می توان ادامه داد؟

آنهايي که می خواهند احتمال حمله با اسلحه سایبری به خود را بسنجند باید سؤال دیگری نیز پاسخ دهند: این نوع حمله تا چه حدی با جهان بینی و اهداف اعلام شده مهاجمین همخوانی دارد؟

بر این اساس، اغلب اشکال معمولی ویروس ها و نیز بمب های الکترومغناطیسی را نمی توان به عنوان سلاح های سایبری معتبر در نظر گرفت، زیرا کنترل آنها به نسبت سخت است. اما یک حمله انکار سیستم هدفمند را می توان یک سلاح سایبری خواند.

طیف متنوع تسلیحات سایبری مهاجمین را دارای قابلیت انعطاف پذیری می کند. تسلیحات سایبری سطح پایین به مانند تغییر صفحه وب سایت ها و یا اسپم های مرتبط با عملیات های روانی در ترغیب و شکل دهی به افکار عمومی نقش مهمی می توانند داشته باشند. حملات اندکی سطح بالا به مانند انکار خدمات نیز می توانند کارهایی هم ردیف انجام مانور و یا نفوذ های تصادفی به داخل قلمرو کشوری دیگر انجام دهند.

یکی از مزایایی که تسلیحات سایبری در مقابل تسلیحات جنبشی دارند این است که حین استفاده از این نوع تسلیحات، ابهام آفرینی در مورد اینکه چه کسی حمله را کنترل می کند آسانتر است.

یکی دیگر از مزایا، هزینه بسیار پایین این نوع تسلیحات است. یک فرد واحد می تواند تنها با استفاده از یک رایانه شخصی یک حمله انکار سرویس انجام دهد. توسعه این کار تمام توسط رایانه هایی انجام می گیرد که در مالکیت افراد دیگر هستند و به عنوان بخشی از یک بات نت تسخیر شده اند.

نسبت دهی حملات سایبری

اکثر حملات سایبری توسط رایانه هایی انجام می گیرند که تسخیر شده و از راه دور توسط اشخاص ثالث، و نه صاحبان واقعی شان، کنترل می شوند؛ اغلب صاحبان واقعی از آنچه روی می دهد بی اطلاع هستند. ابزار اصلی کارآگاهان اینترنتی نت استات¹ است که آدرس های آی پی رایانه های حمله کننده را ثبت و ارائه می کند. بنابراین، کارآگاه باید نام صاحب رایانه را بیابد که اغلب این کار را با رجوع به ارائه دهنده خدمات رایانه ای انجام می دهند. اگر کارآگاه در یک کشور بوده و ارائه دهنده خدمات رایانه ای در قلمرو قضایی کشوری دیگر، این کار بسیار سخت تر خواهد بود.

روتنبرگ (2010) برخی از موانع حقوقی را تشریح می کند. اما وی بیشتر بر حقوق خصوصی و بشر تمرکز می کند در حالیکه مسائلی نیز در حوزه معاهدات همکاری حقوقی دو جانبه وجود دارد. زمانی که به رایانه حمله کننده دست یافته شد باید برای تشخیص وجود نرم افزار فرماندهی و کنترل مورد بررسی قرار گیرد؛ این امر باید منجر به یافتن رایانه کنترل از راه دور شود، اما این رهیافت ممکن است ما را به رایانه ای برساند که خود توسط رایانه ای دیگر و از راه دور کنترل می شود. بنابراین، نسبت دهی حمله همیشه کاری سخت بوده و زمان برتر از آن است که فوراً تلافی شود. این شاخصه مظنونین به تهاجم را قادر می سازد که دخالت خود را در ماجرای بوجود آمده انکار کنند. برای مثال، اتهام زدن به نهادهای تحت حمایت دولت های روسیه و چین ممکن است این جواب را در پی داشته باشد که خود این رایانه ها توسط مهاجمین از کشور ثالث تسخیر شده اند و یا اینکه

¹- Netstat

حمله را عده ای هکر میهن پرست انجام داده اند (Hutchinson, Margulies, 2008)
(Hunker)

تاکتیک های همیشگی عبارت است از اختلال در ارتباطات رادیویی دشمن از طریق تولید پارازیت روی امواج و یا ایجاد ترافیک رادیویی گمراه کننده.

در جنگ های امروزی که شبکه ها نیز دخیل هستند، فرایند ایجاد اختلال باید بر شبکه ها متمرکز باشد نه بر رادیوها. عملیات های آمریکا و متحدانش در کویت (91-1990) و عراق (2003) توأم با «جنگ های الکترونیکی» بودند. طی مناقشه گرجستان/اوستیای جنوبی در سال 2008، ترافیک اینترنتی منطقه دچار اختلال زیادی شد (Shachtman, 2008). همچنین در سال 2008، ادعاهایی در مورد حملات سایبری حماس به اسرائیل مطرح شدند (Home Security Newswire, 2009).

حملات مجرمانه وسیع

پرداخت ها و انتقالات مالی به طور فزاینده ای بصورت آنلاین انجام می گیرند. هم اکنون 70 درصد از جوانان انگلیسی کارهای مالی خود را بصورت آنلاین انجام می دهند و در حدود دو سوم افراد بالغ نیز به خریدهای آنلاین می پردازند (UK Payments Council 2010:20). همانگونه که انتظار می رود، کلاهبرداران، تکنیک هایی خلق کرده اند تا به عمق این جریان های مالی جدید نفوذ کنند. آنها به جای حمله به سیستم های داخلی بخوبی حفاظت شده نهادهای خدمات مالی، از نرم افزارهای جاسوسی برای نفوذ به

رایانه های شخصی و دسترسی به رمز و اطلاعات شخصی کاربران بهره می گیرند تا از حساب بانکی آنها سرقت نمایند.

علاوه بر این، کاربران به سوی وب سایت های کلاهبرداری (که اغلب در بات نت ها قرار دارند) هدایت می شوند. این وب سایت های تقلبی خود را به عنوان وب سایت بانک معرفی می کنند و جزئیات حساب و رمزهای کاربران را سرقت می کنند.

پول توسط افراد ساده لوحی که به نام «حمالین پول»¹ از حساب بیرون کشیده می شود و بدین ترتیب شناسایی مقصد اصلی انتقال پول بسیار سخت می شود. کلاهبرداران همچنین از اطلاعات شخصی بسرقت رفته برای ثبت نام و گرفتن کارت های اعتباری و وام استفاده می کنند و بدین ترتیب افرادی که هویت شان جعل شده، مجبور می شوند آسیب های وارده را بر طرف ساخته و بانک ها نیز خسارت ها را جبران نمایند (Brown, Edwards and Marsden, 2009).

نهادهای مالی تاکنون توانسته اند که این نوع کلاهبرداری را مدیریت نمایند. آنها خسارت وارده بر مشتریان را جبران کرده و از تاجرین درخواست کرده اند که به خطرات ناشی از پرداخت های راه دور «بدون کارت»² آگاه باشند. خسارات وارده چشمگیر هستند (براساس داده های جمع آوری شده، در سال 2009، مجموع کلاهبرداری های آنلاین بانکی در انگلستان بالغ بر 59/7 میلیون پوند بوده است)، اما نسبتاً در سطوح پایینی قرار دارند. شرکت کارتهای اعتباری «ویزا اروپا» اعلام داشته که نرخ کلاهبرداری از کارت های اعتباری این مؤسسه در ژوئن 2009 نسبت به زمان مشابه سال قبل 0/06

¹. money mules

². card not present

درصد کاهش یافته است (Visa Europe, 2009: 30). هرلی و فلورنسیو¹ تخمین می‌زنند که مجموع خسارات ناشی از سرقت اطلاعات شخصی مشتریان بانکی آمریکا در 12 ماهه منتهی به آگوست 2007 بالغ بر 61 میلیون دلار بوده است (2008: 9).

با این حال، صنعت غیرقانونی تولید و پشتیبانی از نرم افزارهای جاسوسی و نیز پیوستگی جهانی بین مجرمین و قربانیان که توسط اینترنت ایجاد شده در حال رشد است. این امر باعث کاهش هزینه های جانبی و افزایش سود تبهکاران می شود (van Eeten and Bauer, 2008: 16). هرلی و فلورنسیو چنین نتیجه گیری کرده اند که استراتژی ورود به بازار و رفتارهای «سارقین رمزها» منطقی است و اینکه وجود موانع کم در ورود بدین نوع فعالیت ها باعث شده «سرقت رمز» تبدیل به حرفه ای شود که نیاز به مهارت کمی دارد و درآمد ناشی از آن نیز پایین است. این دو محقق در ادامه می افزایند: «نتایج تحقیقات قابل تردید و همچنین گزارشات غیرقابل اثبات نشان می دهند که وضعیت بدتر می شود و شاهد جریان مداومی از ورودیها بدین حوزه هستیم.» (2008: 1).

مدیریت کلاهبرداری ها توسط بانک ها و مؤسسات خدمات مالی، اگر چه خوشایند مشتریان است اما انگیزه لازم برای کاهش دادن ریسک های سیستمی گسترده در وضعیت امنیتی رایانه های خانگی را کم می کند. ریسک دیگری باقیست مبنی بر اینکه فعالیت های مجرمانه موفقیت آمیز باعث خواهند شد یک بی اعتمادی سیستماتیک از جانب مصرف کنندگان به سیستم های پرداخت و بانکداری ایجاد گردد. این امر هزینه کلاهبرداری ها را برای

¹ . Herley and Florencio

عرصه تجاری به صورت غیر قابل پذیرشی افزایش داده و همچنین جرایم مالی فزاینده ای در اختیار دیگر فعالیت های مجرمانه خواهد گذارد.

نوع معمول اخاذی سایبری بدین گونه است که با استفاده از بات نت ها یک حمله انکار سرویس انجام گرفته و متعاقب آن پیشنهاد «خدمات مشاوره ای» برای حل این مسأله ارائه می شود. در سال 2005، سه مرد هلندی به اتهام طرح ریزی برای انتشار کدهای رایانه ای جاسوسی در صدها هزار رایانه بازداشت شدند (Brandt, 2005). جوزف من¹ گزارشی مستند در مورد استفاده از بات نت ها علیه تعدادی از وب سایت های قماربازی آنلاین ارائه نموده است. وی کشف کرد که مافیای آمریکا، گروه های تبهکاری مستقر در سنت پترزبورگ و یک «ارائه دهنده خدمات اینترنتی» (ISP) در این قضایا دخیل بودند. این «ارائه دهنده خدمات اینترنتی» در برخی مواقع تسهیلات میزبانی در اختیار تعدادی از فعالیت های مجرمانه قرار می داد. یکی از این موارد مجرمانه عبارت از انتشار تصاویر مستهجن سوء استفاده از کودکان بود (Menn, 2010).

هک با هدف سرگرمی

هک با انگیزه سرگرمی نوعی فعالیت است که در سال 1983 و در فیلم «بازی های جنگ» ظاهر شد. هدف از این نوع اقدامات تحت تأثیر قرارداد دیگر هکرها از طریق کارهای برجسته و استادانه است نه کسب منافع مادی (Cornwall, 1985). مسأله اینجاست که این نوع فعالیت های لذت جویانه می تواند عواقب ناخواسته ای داشته باشند و تبدیل به یک خطر جهانی شود. نمونه هایی از این نوع فعالیت ها عبارتند از:

¹ . Joseph Man

- کرم «موریس»¹ در سال 1998. این کرم توسط یک دانشجو و به صورت آزمایشی نوشته شده بود اما در همان روزهای آغازین اینترنت بسیاری از رایانه های یونیکس را آلوده کرد.
- در سال 1994 دو هکر انگلیسی به نام های «کابوی» و «کوجی» به رایانه های نیروهای هوایی آمریکا، ناتو، ناسا، لاکهید مارتین و دیگر نهادها حمله کردند (GAO, 1996; Sommer, 1998).
- ویروس ملیسا که در سال 1999 توسط دیوید اسمیت منتشر شد، بنا بر تخمین ها، به بیش از 1 میلیون رایانه در سراسر جهان گسترش یافته و خسارتی بالغ بر 400 میلیون دلار پدید آورد. این ویروس می توانست در داخل فرمت های Word 97 و Word 2000 جاسازی شده و همچنین خود را از طریق برنامه Microsoft Outlook در تعداد بالا ایمیل ارسال کند (F-Secure, 2006).
- بنا بر ادعاها در اوایل سال 2000 یک پسر 15 ساله کانادایی ظاهراً توانست حملات موفقیت آمیزی به وب سایت های برخی از بزرگترین شرکت های تجاری جهان انجام دهد؛ شرکت هایی چون: آمازون؛ ای بای و یاهو. (Evans, 2001)

هک گرای

هکتویسم یعنی استفاده از تکنیک های هک به مانند تغییر صفحه وب و یا انکار سرویس توزیعی به منظور تبلیغ یک جنبش ایدئولوژیکی و نه انجام یک عمل مجرمانه (metac0m, 2003). اولین نمونه های این نوع فعالیت ها به

¹. Morris

دوران قبل از راه اندازی اینترنت باز می گردند: در سال 1989 دستگاه های «وکس وی ام اس»¹ وزارت انرژی آمریکا و ناسا توسط گروهی که خود را «کرم های ضد قاتلین هسته ای»² می نامیدند مورد حمله واقع شدند (Assange, 2006). یکی دیگر از نمونه های بارز این حملات عبارت است از گروه «هرج و مرج شهری»³ که در سال 1997 برنامه ای تبلیغاتی علیه دولت اندونزی به راه انداخت. گروه «تأثر اختلال الکترونیکی»⁴ که فعالیت وب سایت های جمهوریخواهان را طی نشست مجمع ملی این حزب در سال 2004 دچار اختلال کرده و به تبلیغات علیه جنبش دست راستی مینوتمن⁵ در سال 2006 و نیز علیه قطع کمک های بهداشتی در سال 2007، می پرداخت، و نیز یک گروه ناشناخته که به وب سایت «گروه تحقیقات آب و هوایی» در دانشگاه آنجلیای شرقی حمله کرده و برخی از ایمیل های سرقت کرده از آنجا را منتشر نمودند. بنا بر ادعاهای این گروه، ایمیل های مذکور نشان دهنده ایمان بد و علم نادرست در حوزه مباحث پیرامون گرایش جهانی بودند.

در سال 2009 و طی حمله رژیم صهیونیستی به غزه، طرفداران هر دو طرف اسرائیلی و فلسطینی حملاتی چون تغییر صفحه وب سایت ها، تغییر نام دامنه، سرقت کلمه عبور و انکار سرویس را انجام دادند. (Graham, 2009).

گروهی به نام «گمنام» ظاهراً فعالیت های تبلیغاتی انجام داده اند عبارتند از: برنامه تبلیغاتی در حمایت از مخالفین دولت ایران، برنامه های تبلیغاتی

¹ . Vax VMS

² . Worms Against Nuclear Killers

³ . UrBaN KaOs

⁴ . Electronic Disturbance Theater

⁵ . Minutemen

علیه کلیسای حقیقت شناسی¹، علیه نهادها و وکلای عرصه موسیقی و فیلمسازی که هدفشان مجازات دانلودکنندگان فیلم ها و موسیقی های دارای حق کپی رایت است، علیه برنامه دولت استرالیا برای فیلتر اینترنت، و مهمتر از همه، در سال 2010، علیه شرکت هایی به مانند مسترکارت، ویزا و پی پال که تسهیلات حمایتی مالی خود به وب سایت ویکی لیکس را متوقف کرده بودند (Ernesto, 2010 and Halliday and Arthur, 2010).

مهمترین محدودیت های عملی هکتیویسم چنین است که اصرار بر تداوم حمله، احتمال طرح ریزی و اجرای تمهیدات متقابل، شناسایی مهاجمین و نیز نفوذ مأموران به درون گروه ها را افزایش می دهد. هکتیویسم اولین گروه های متعارف عمل مستقیم است که با چالش مشابهی مواجه هستند: فعالیت های اولیه در جذب حمایت عمومی موفق هستند اما پس از مدتی افکار عمومی ممکن است چنین بیندیشند که این گروه ها «دیگر خیلی زیاده روی کرده اند». از آنجایی که تمام هکتویست ها از فناوری های پنهان ساختن هویت استفاده می کنند، تشخیص فعالیت های آنها از حملات سایبری انجام گرفته توسط سازمان های دولتی ساده نیست. (Hunker, Hutchinson, Margulies, 2008; House of Lords European Union Committee, 2010).

برای اینکه یک فعالیت هکتویستی به سطح یک شوک جهانی برسد باید تحقیقات خوب انجام گرفته، تداوم داشته و توسط افرادی پیاده سازی شود که هیچ اهمیتی به عواقب آن نمی دهند. حملات بی نام سال 2010 را می توان «جهانی» نامید، زیرا در این حملات فعالیت تعداد زیادی از

¹. Church of Scientology

شرکت هایی که برای جمع آوری مبالغ به تجهیزات کارت های اعتباری وابسته بودند، متوقف شد. این امر باعث گردید کارمندان آنها بیکار شوند و حتی شاید ضررهای مالی دیگری بر حامیان آنها وارد آید. حتی می توان چنین فرض کرد که تلاش یک گروه طرفدار محیط زیست نیز تبدیل به یک شوک جهانی غیرعمدی شود. این گروه ممکن است از تکنیک حمله انکار سرویس توزیع شده به عنوان اقدامی نمادین علیه مجموعه های صنعتی و یا ارتباطاتی که می پندارند به آینده محیط زیست جهانی توجهی ندارند، استفاده نمایند. اما این حمله آشنایی از اختلالات شبکه ای پدید می آورد که باعث قطع گسترده جریان نیرو شده و بدین ترتیب زیان های اقتصادی زیادی را پدید می آورد.

جاسوسی های دولتی و صنعتی گسترده

جاسوسی صنعتی و یا جاسوسی صنعتی تحت حمایت دولت ها چیز جدیدی نیست. در سال 1981، سرهنگ ولادیمیر و تروو¹، در حدود 4000 سند را در اختیار سرویس اطلاعات فرانسه گذارد. این مدارک نشان می دادند که سازمان کا.گ.ب در حال انجام عملیات های گسترده جاسوسی «علمی و فناوری» است. اسناد ارائه شده بعدها توسط سازمان سیا مورد تحلیل و تشریح قرار گرفت (Weiss, 1996). در سال 1994، مایکل جان اسمیت² در دادگاه اولد بیل³ در لندن به جرم جاسوسی در فعالیت های علمی و فناوری

¹. Col Vladimir Vetrov

². Michael John Smith

³. Old Bailey

انگلستان برای کا.گ.ب، محکوم شد. امروزه این فعالیت ها وارد فضای سایبری شده اند.

محققین کانادایی دو گزارش مشروح در مورد جاسوسی های سایبری در سال های 2009 و 2010 منتشر کرده اند. اولین گزارش به تشریح فعالیت های چین برای ردیابی فعالیت های دولت در تبعید «تبتی دالایی لاما» و طرفداران آنها با استفاده از یک بدافزار کنترل از راه دور، می پردازد. محققین ادعا می کنند که حداقل 1295 رایانه آلوده را در 103 کشور جهان شناسایی کرده اند (Information Warfare Monitor, 2009). در گزارش دوم اطلاعات جامعی در مورد تلاش های بشدت سازماندهی شده چینی ها برای هدف قرار دادن رایانه های دولت چین و دیگر کشورها، ارائه شده است. (Information Warfare Monitor, 2010).

اهداف جاسوسی صنعتی عبارتند از: صرفه جویی در مخارج انجام تحقیقات، ارائه قیمتی پایین تر از قیمت رقیب در مناقصات، و انجام خرابکاری در یک برنامه بازاریابی. یک عملیات جاسوسی صنعتی موفقیت آمیز می تواند تأثیر بسزایی در شرکت قربانی داشته باشد. این فعالیت ها در بلند مدت می توانند بر قابلیت های رقابت ملی تأثیر گذارند. یکی از مأمورین امنیتی سرویس های مخفی سیا که از سال 2008 به عنوان مشاور امنیتی تجاری فعالیت می کند، گزارش مفیدی در مورد فعالیت های اخیر علیه آلمان، ژاپن، تایوان، استرالیا، نیوزیلند، کانادا، انگلستان، فرانسه، جمهوری چک، قطر، کره جنوبی و آمریکا ارائه نمود (Burgess, 2008).

می توان بدون نیاز به فناوری های پیچیده جاسوسی های کارآمد زیادی انجام داد. آنچه در وهله اول مهم است کسب اطلاعات می باشد و

روش های فنی مورد استفاده برای دستیابی بدین اطلاعات از اهمیت فرعی برخوردار هستند. در دهه 1970 - 1980، بیشترین علاقه در حوزه فناوری متوجه فرستنده های رادیویی کوچک یا همان «میکروفن های مخفی» بود. روش های غیر فنی عبارتند از:

- جمع آوری و تحلیل اقلام متن باز (اطلاعات رقابتی). صفحات وب سایت های شبکه های اجتماعی ، عمل تحقیق از پشت میز را ساده تر و ثمربخش تر ساخته است.
- هدف قرار دادن افراد خاص به منظور کاوش ضعف هایی که در استفاده از امنیت فیزیکی دارند و یا بررسی فرصت هایی برای اخاذی از این افراد.
- اغوای کارکنان، شاید از طریق پیشنهاد یک شغل جدید.
- وارد کردن کارکنان نفوذی
- استفاده از طرف های سوم به مانند روزنامه نگارها و مشاورین، سازمان های تبلیغاتی و چاپگرها.
- بررسی مواد دور ریخته شده.

باید اشاره شود که به منظور موفقیت آمیز بودن روش های فنی، باید تحقیق زیادی در مورد چگونگی هدف قرار دادن افراد و تجهیزات ارتباطاتی و اطلاعاتی انجام گیرند. تحقیقات خام و ناکافی ممکن است منجر به شناسایی پیش از موعد جاسوسی شوند. برخی از نویسندگان و بازاریاب ها برای اشاره به مجموعه ای از فعالیت ها شامل ابزار فنی و پنهانی برای

دستیابی به اطلاعات در مورد سازمان ها و افراد هدف ، از عبارت «تهدید مزمن پیشرفته»¹ استفاده می کنند. (Sterling, 2010)

جاسوسی سایبری این پتانسیل را دارد که خسارات مالی زیادی به قربانیان وارد آورد؛ همچنین می تواند از نظر نظامی و اقتصادی بر امنیت دولت ملت ها تأثیر گذارد. با این حال تجسم سناریویی که دارای معیارهای یک «شوک جهانی» است، بسیار سخت می باشد.

فریب در فضای سایبر:

فریب می تواند به عنوان یک اثر متقابل بین دو گروه، یک فریب دهنده و یک هدف، تعریف شود که فریب دهنده به طور موفقیت آمیزی سعی می کند تا هدف، نوعی واقعیت نادرست را که به نفع فریب دهنده اجرا می شود را، به عنوان حقیقت بپذیرد.

فریب در شناسایی هویت: چون جعل هویت در فضای سایبر آسان است، بسیاری از حملات، آن را به کار می برند. اینها به طور کلی فریب هایی از انواع: هدف کلی، ابزار، نوع برتر و ... هستند. پرسنل نظامی اهدافی را برای حملات مهندسی اجتماعی شامل جعل هویت یک شخص به جای دیگری را، ترغیب می کنند.

حملات می توانند درون نرم افزار بی ضرر پنهان شوند که اینها اسب تروjan نامیده می شوند. جهت فریب کاربر برای اجرای آنها، می توانند به صورت نرم افزار مجانی، در وب سایت ارائه شوند و به عنوان ضمیمه های ایمیلی با آدرس های جعلی فرستاده شوند، در وسایل ذخیره سازی

¹ . Advanced Persistent Threat

چند رسانه‌ای ذخیره شوند یا حتی هنگامی که نرم‌افزار تولید می‌شود، در آن قرار گیرد. نرم‌افزار پوشش می‌تواند یک برنامه سودمند، یک بازی یا یک ماکرو (کد جاسازی شده) بزرگ در یک فایل متنی باشد. نصب یک قسمت از نرم‌افزار برای اثبات اینکه مضر است، کافی نبوده چرا که خرابکاری یا جاسوسی ممکن است ماهرانه باشد یا ممکن است جهت راه اندازی بعدی طبق زمان یا دستوراتی از یک مهاجم از راه دور، مستقر شود. خرابکاری می‌تواند از تغییر اعداد در داده‌ها تا شکست کامل برنامه‌ها، متغیر باشد. ویروس‌ها و کرم‌های رایانه‌ای، شکل‌های مهم اسب‌های تروجان هستند، اما آنها معمولاً برای استفاده در کاربری‌های نظامی، بسیار آشکار هستند.

یک نوع مهم اسب‌های تروجان، جاسوسی خودکار در فضای سایبر، است. این برنامه به طور پنهانی اطلاعات مفیدی را درباره فعالیت‌های رایانه‌ای به یک مهاجم منتقل می‌کنند و بنابراین از نوع فریب‌آمیز کننده (تجربه‌گر) هستند.

فریب‌های مختلف:

- فریب‌های دیگر از این گروه می‌توانند در فضای سایبر به کار روند:
- بار اضافی بر حافظه میانی می‌تواند با ارسال ورودی‌های زیاد ریاکارانه به برنامه‌ها اجرا شود.
- جهت غافلگیری، حملات می‌توانند از نرم‌افزار، پورت‌ها یا سایت‌های شبکه که به ندرت به کار می‌روند، استفاده کنند.
- حملات می‌توانند اهداف غیرمنتظره‌ای مثل قابلیت‌های یک نرم‌افزار کم کاربرد، داشته باشند.

- حملات می‌توانند در زمان‌های غیرمنتظره‌ای رخ دهند (اما همه می‌دانند اینترنت همیشه فعال است).
- حملات می‌توانند از سایت‌های غیرمنتظره‌ای رخ دهد (اما همه میدانند حملات می‌توانند از هرجایی انجام شوند).
- جهت افزایش اختفا، حملات می‌توانند بسیار آرام، با ارسال یک فرمان در روز به رایانه قربانی، انجام شوند.
- حملات می‌توانند فایل یا رکوردها را همزمان و با جزئیات ایجاد کنند که در ظاهر نشان دهند که مهاجمان در حال انجام کاری متفاوت هستند.
- مهاجمان می‌توانند کارهایی را برای اهداف اخاذی خود، مثل قابلیت از کار انداختن سیستم رایانه ای، ادعا کنند.

برون سپاری بین المللی

اطلاعات شخصی افراد می‌تواند کالای با ارزشی برای تروریست‌ها باشد. تروریست‌ها می‌توانند از این اطلاعات در بسیاری از فعالیت‌های غیرمجاز مثل ایجاد حساب‌های بانکی ساختگی، تهیه اسناد رسمی مختلف یا حتی ایجاد ترس و وحشت زیاد استفاده کنند. متأسفانه، این اطلاعات شخصی به طور کلی براحتی قابل دسترسی، مبادله یا جمع‌آوری از طریق رسانه‌های آنلاین مانند وب سایت‌ها، اتاق‌های گفتگو یا ایمیل‌ها هستند. علاوه بر این، روش‌های رایج تجارت، به ویژه آنهایی که در ارتباط با پردازش اطلاعات در برون سپاری بین المللی هستند می‌توانند این فعالیت‌ها را با قراردادن اطلاعات شخصی در یک ناحیه قانونی که سوءاستفاده از آن آسان است، تسهیل کنند. بنا بر این دلایل، سازمان‌ها و افراد باید از پتانسیل سوء استفاده از این اطلاعات

آگاه باشند و همچنین باید از مراحلی که می‌توانند برای جلوگیری از این سوءاستفاده‌ها به کار برند، نیز آگاه شوند.

شرکت‌ها و سازمان‌ها در صنایع می‌توانند این مشکلات سوءاستفاده از داده‌ها را با پذیرش پنج رویکرد نسبتاً ساده در رابطه با برون سپاری بین المللی نشان دهند:

روش 1: توسعه سیستم دسته بندی داده های حساس و اشتراک این سیستم با کارمندان. راه حل جلوگیری از سوءاستفاده از داده‌ها، تعیین اطلاعاتی است که به طور ویژه حساس هستند و باید برای محافظت در داخل شرکت باقی بمانند. داده‌های غیرحساس می‌توانند بدون نگرانی به راه دور فرستاده شوند. پردازش داده‌های حساس، درجائیکه سازمان‌ها و قوانین ملی می‌توانند کاربردهای آن را مدیریت می‌کنند و از آن درمقابل سوءاستفاده‌ها حافظت کنند، در سازمان باقی خواهند ماند. سازمان‌ها باید زمان و پولی را که برای بررسی انواع داده‌هایی دارند، استفاده می‌کنند و سپس به دسته‌بندی انواع مختلف داده‌های حساس اختصاص دهند. اطلاعات شخصی می‌توانند رمز شوند و طبق این دسته‌ها توزیع شوند.

روش 2: ایجاد یک سایت روی شبکه داخلی که کارمندان و مدیران را درباره چگونگی سازماندهی و نشان دادن سوءاستفاده از داده‌های مختلف که آنها ممکن است هنگام کار کردن در روابط برون سپاری با آنها مواجه شوند آموزش دهد. برای کمک به جلوگیری از اشتباهات برون سپاری، سازمان‌ها ممکن است سایتی روی شبکه داخلی ایجاد کنند که دستورالعمل‌هایی را برای شناسایی انواع سوءاستفاده‌ها از داده‌ها را نشان داده و لیستی از اداره یا

نماینده‌گی همکار دولتی که در تماس‌ها بیشتر باید مواظب باشند را فراهم کنند.

روش 3: کار با کارمندان خارجی که با تهیه نقشه‌هایی داده یا اطلاعات به روز که برای کارگران خارجی فرستاده می‌شود، فهرست کنند. این نقشه باید شامل اسامی و اطلاعات تماس برای تمامی افراد مشغول به کار در هر بخشی از فرآیند برون سپاری شده باشد. از جنبه امنیت داده‌ها، بزرگ‌ترین مشکل منحصر به فرد، ردیابی مکان‌هایی است که داده‌ها وقتی به خارج فرستاده می‌شوند، از آنها عبور می‌کند. نقشه‌ای که به طور واضح چگونگی حرکت این داده‌ها را وقتی که به خارج فرستاده می‌شوند، ردیابی می‌کند، می‌تواند به طور گسترده‌ای به سازمان‌ها کمک کند تا مکان‌هایی که سوءاستفاده از داده‌ها رخ می‌دهد و یا مکان‌هایی که از آنها داده‌ها، انتشار می‌یابند را بیابند.

روش 4: افزایش آگاهی مدیریتی در مورد پیمانکارانی که خود از پیمانکاران فرعی استفاده کرده و خط مشی‌هایی برای زمان استفاده از پیمانکاران فرعی در برون سپاری را بررسی و توسعه دهند. مراحل را برای ثبت پیمانکاران فرعی بوسیله مشتری یا شرکت دربرمی‌گیرد به طوریکه مشتریان بتوانند جریان اطلاعات را به این پیمانکاران فرعی ردیابی کنند.

روش 5: همکاری با شرکت‌های دیگر جهت توسعه یک شبکه اشتراک اطلاعات درباره برون سپاری‌های بین المللی در صنایع خاص و در سرتاسر صنایع مختلف انجام شود.

در حالت ایده آل، شرکت‌ها در یک صنعت می‌توانند با یکدیگر جهت ایجاد روشی برای ثبت آسان اسامی و جزئیات (مانند یک وب سایت) شرکت‌هایی که برای برون سپاری از آنها استفاده می‌کنند و یا شرکت‌هایی که

می‌توانند برایشان پیمانکار پیدا کنند، همکاری کنند. شرکت‌ها می‌توانند از این سایت برای اشتراک اطلاعات و عقایدشان درباره اثربخشی نحوه فعالیت یک تهیه‌کننده برون سپاری، استفاده کنند.

مواردی از راه حل‌ها

هم اکنون به بررسی دکترین‌های امنیت سیستم‌های اطلاعاتی می‌پردازیم زیرا این نظریه‌ها ابزار اصلی پیشگیری و یا حداقل مدیریت یک «واقعه» را ارائه می‌کنند. «دکترین» یک رهیافت فلسفی است. راه حل‌های دیگر به چگونگی طراحی یک سیستم می‌پردازند. برخی مسائل مختص به فناوری وجود دارند. در پایان به وضعیتی می‌پردازیم که در آن، این راه چاره‌ها با شکست مواجه شده‌اند، یک «واقعه» امنیتی رخ داده است، تأثیرات آن باید کاهش یابند و سیستم نیز به نوعی بازسازی گردد.

راه‌های چاره: دکترین‌های امنیتی

متعاقب پیچیده‌تر شدن سیستم‌ها و چگونگی استفاده از آنها، دکترین‌های امنیتی نیز لاجرم تکامل یافته‌اند.

اولین دکترین در این حوزه «مشکل فنی/راه حل فنی» نام داشت. هر مسأله‌ای در حوزه فنی، با نگاهی کاملاً فنی مورد بررسی قرار می‌گرفت و چنین فرض می‌شد که به نحوی یک راه حل فنی نیز برای آن وجود دارد. بنابراین: استفاده غیرمجاز از یک رایانه باید از طریق بکارگیری تجهیزات کنترل دسترسی، حل گردد و ویروس‌ها را نیز می‌توان با استفاده از پوشگر

ویروس حذف نمود. این دکترین هنوز هم در برخی تمهیدات بکار می رود اما به عنوان یک واکنش کلی و جامع کاملاً ناکافی به نظر می رسد.

در اواخر دهه 1960، استفاده از روش حسابرسی رشد چشمگیری یافت. این روش برای بررسی کمبودها و نواقص کنترل موجود در سیستم ها بکار می رفت. حسابرسی «پردازش الکترونیکی داده ها»¹ (EDP) به صورت گسترده ای از حسابرسی های مدل حسابداری عاریت گرفته شد. اما حسابرسی را باید براساس استاندارد انجام داد که نشان می دهد چه چیزی «خوب» و یا «قابل پذیرش» است. از این امر می توان برای اشاره به مشکل اصلی حسابرسی «پردازش الکترونیکی داده ها» استفاده نمود: چه کسی باید محتوای این استانداردها را تعیین نماید؟ آیا ماشین آلات کافی برای هماهنگی با تغییرات سریع فناوری وجود دارند و این ماشین آلات چگونه باید بکار گرفته شوند؟ آیا در فرایند حسابرسی تهیه گواهی معتبر تطابق با یک «استاندارد»، استاندارد که ریسک ها و استفاده های کنونی را منعکس نمی کند، آسان است؟ امروزه استانداردهای امنیتی هنوز هم در برخی محافل کاربرد دارند، اگرچه استانداردهای مدرن تر به مانند ایزو 27000 بیشتر بر فرایند تحلیل ریسک متمرکز است نه ارائه لیستی بلند از عناصری که باید مورد بررسی قرار گیرند.

در دهه 1990، با استفاده از ایده هایی که از قبل در صنعت بیمه تدوین شده بودند، تغییر جهتی به سوی مفاهیم مدیریت ریسک انجام شد. ریسک ها را می توان شناسایی، تحلیل و اولویت بندی نمود. یک مدیر ریسک می تواند با عدم انجام فعالیتی مرتبط با یک ریسک، از ریسک مذکور، اجتناب نماید، با

¹ . Electronic Data Processing

استفاده از تمهیدات فنی ریسک‌ها را کاهش دهد، ریسک‌ها را بیمه نماید، و یا احتمال بروز یک ریسک را پذیرا شود زیرا هزینه‌های هر نوع روش جایگزین بالا، بسیار بالاتر است. از تکنیک‌های مدیریت ریسک برای کنترل ریسک بازار، ریسک اعتبار و ریسک عملیاتی استفاده می‌شود.

رهیافت‌های مدیریت ریسک، زمانی بیشترین فایده را خواهند داشت که سطحی منطقی از داده‌های قابل اعتماد و در دسترس در مورد ریسک‌های مورد نظر وجود دارند و همچنین در حالتی که احتمالات و خسارت‌های مالی بالقوه شفاف و قابل تعریفی مطرح شوند. برای مثال، در حوزه بیمه‌های معمولی، مجموعه‌ای از داده‌های آماری در مورد احتمال تصادفات موتوری، آتش‌سوزی و طول عمر زندگی بشر وجود دارد. مقدار تعهد بیمه‌گر در قرارداد بیمه‌ای ذکر می‌شود. با این حال ارزیابی ریسک‌های حوزه فناوری بسیار سخت است زیرا نرخ تغییر چنان سریع است که هیچ داده‌های آماری در مورد آنها نمی‌توان تهیه نمود. همچنین محاسبه خسارت‌های غیر ملموس به مانند آسیب به اعتبار و آبرو نیز بسیار سخت است.

خسارت‌های بالقوه در برنامه‌های شرایط اضطراری ملی بیشتر ناملموس هستند - برای مثال چگونه می‌توان خطرات ناشی از فروپاشی اجتماعی را محاسبه کرد؟ در پاسخ بدین سؤال باید ماتریسی متشکل از سه سطح احتمال کم، متوسط و بالا برای احتمالات و ماتریسی دیگر برای تأثیرگذاری تهیه نمود. بدین ترتیب می‌توان برخی از شاخه‌های مدیریت ریسک را بدون نیاز به محاسبات مالی دقیق، بکار برد. (Cashell, 2004).

در پایان دهه 1990، تحلیل گران شروع به استفاده از واژه بیمه اطلاعات نمودند. این رویافت در مجموع، نوع «نرم‌تری» از تحلیل است. براساس این

نوع تحلیل، در غیاب داده های قابل اطمینان در مورد ریسک بهتر است تمام عناصری که احتمال بروز خطر امنیتی را افزایش و یا کاهش می دهند شناسایی نمود. این رهیافت به استفاده از اغلب عناصر تحلیل ریسک ادامه داده و در مجموع حسن استفاده استانداردهای امنیتی را نادیده نمی گیرد. اما سعی دارد ایده هایی را نیز از علوم اجتماعی قرض بگیرد: علم مدیریت به منظور فهم چگونگی فعالیت سازمان ها و چگونگی عملکرد ملاحظات امنیتی در آنها؛ انسان شناسی و جرم شناسی به منظور فهم اینکه چگونه افراد و گروه ها رفتار کرده و انگیزه آنها چیست؛ روانشناسی به منظور بسط فهم رفتار در مورد فاکتورهای «مردم» در طراحی فناوری اطلاعات و ارتباطات و امنیت؛ و اقتصاد برای فهم چگونگی اتخاذ تصمیمات امنیتی توسط سازمان ها می باشد (Backhouse and Dhillon, 2000).

راه های چاره: طراحی سیستم

الزامات سیستمی / طراحی / امنیتی

این رهیافت شاخصه های امنیتی را در «مهندسی الزامات» مقدماتی ادغام می کند. تلاش زیادی صرف می شود تا مشخص گردد کدامیک از کارکردهای سیستمی، شامل امنیت، مناسب مشتریان بوده و لازم هستند. اگرچه این رهیافت منجر به پدید آمدن سیستمی امن خواهد شد اما اغلب جاذبه ای برای طرفداران یک سیستم جدید ندارد. فرایند شناسایی الزامات و نیازمندی ها می تواند منجر به دیر کرد شده و هزینه های بیشتری وارد آورد. با این حال، اضافه نمودن ویژگی های امنیتی پس از بروز وقایع، اغلب رضایت بخش نبوده و هزینه بر است. سازمان همکاری و توسعه اروپا اخیراً

گزارشی بدین عنوان منتشر کرده است: «دستورالعمل هایی برای امنیت سیستم ها و شبکه های اطلاعاتی: به سوی فرهنگ امنیتی» (OECD, 2002).

تخریب امن

علاوه بر پیش بینی نفوذهای محتمل امنیتی، الزامات دیگری نیز وجود دارند مبنی بر اینکه سیستم های تخریب امن¹ می توانند هنگام بروز هر نوع حادثه ای خود را در حالت بی خطر² خاموش کند. از این رهیافت معمولاً در وضعیت های فی النفسه خطرناک به مانند مدیریت نیروگاه های هسته ای و خطوط مونتاز خودکار استفاده می شود. سیستم های تخریب امن معمولاً بسیار ساده هستند. همچنین کارکردها و واسط های پیچیده در این سیستم ها که می توانند منبعی برای خطاهای برنامه ای باشند به حداقل رسانده شده اند. یکی از خطرات طراحی تخریب امن این است که هر زمان بخشی از یک سیستم بزرگتر خود را خاموش می کند، حجم ترافیک آن به یک دستگاه دیگر منتقل می شود. این دستگاه نیز به منظور جلوگیری از ورود بار بیش از حد خود را خاموش می کند. این امر می تواند منجر به یک اثر زنجیره ای کلاسیک گردد، به مانند آنچه در جریان قطع برق شمال شرقی آمریکا و کانادا در سال 1993 رخ داد. در زمان تعیین ویژگی ها و خصوصیت سیستم های تخریب امن باید تحلیل های بسیار دقیقی صورت پذیرد.

¹ . fail-safe systems

² . Safe mode

راه حل های دیگر

یک ویروس در برنامه های طراحی شده برای خراب کردن و از بین بردن منابع شبکه رایانه منتشر می شود. به عبارتی دیگر همانند ویروس های طبی، ویروس ها راهی در رایانه شما پیدا می کنند و آن را ضعیف می کنند. بطور کلی ویروس ها، یک عامل مضر برای شبکه رایانه و محاسبات بوده اند. همان طور که ویروس ها بهتر طراحی شده اند، ما هم می توانیم آنها را مهار کنیم. بعضی از دلایل انتشار ویروس ها در رایانه عبارتند از:

✓ ویروس ها برای ساخته شدن آسان هستند. توسعه دهندگان ویروس از ابزار های اینترنت استفاده می کنند و می توانند از این طریق آنها را بنویسند.

✓ ویروس ها خیلی سریع می توانند جا به جا شوند. برای مثال ویروس 'لاو بوی' چیزی است که از فیلیپین به سمت آسیای شرقی، اروپا و آمریکای شمالی در کمتر از یک روز توسعه یافته بود.

✓ کپی شدن آنها آسان، سریع و زیاد است.

✓ ایجاد و پخش کردن یک ویروس آسان است اما متأسفانه پیدا کردن جایی که ویروس از آنجا شروع شده است سخت است.

جاهایی که می توان ویروس ها را در آنجا پیدا کرد، عبارتند از:

- دیسک های رایانه ای، مثل فلاپی ها و سی دی ها. این ها ابزارهای معمول پخش ویروس هستند، اما اخیراً روش پخش ویروس

¹ Love Boy

از طریق بارگذاری از اینترنت و حافظه فلش بیشتر از سایر روش هاست.

- نرم افزارهای قابل بارگذاری در اینترنت:

تأکید می شود که دقت داشته باشید چه چیزی را بارگذاری می کنید. به طور متداول، نرم افزار بارگذاری راه اصلی انتقال ویروس ها است. اما سریع ترین راه پخش آن فرستادن در پست الکترونیکی است.

- **ضمیمه های پست الکترونیک:** این یک پست الکترونیکی

از طرف aunt maple! است. او همراه این پست الکترونیکی چه چیزی فرستاده است؟ آن را باز کن و ببین. بعد می فهمی که همه کسانی که در فهرست دوستان شما هستند (آدرس بوک) همان پیام را دریافت کرده اند.

انواعی از ویروس ها می توانند باعث خرابی شبکه های رایانه ای شوند. اشتباهات، ویروس ها را به وجود می آورند و ویروس ها به نرم افزارها حمله می کنند و این به خاطر اشتباهات ایجاد شده است. مخرب های برنامه ها و داده ها، به نرم افزار متصل شده و تکثیر می شوند و سپس به آن حمله می کنند. مخرب های سیستم، همان طور که شما ممکن است فکر کنید، بدترین نوع ویروس ها هستند و به طور کامل برنامه ای که شما با آن کار می کنید را خراب می کنند.

مخرب های سخت افزاری، سخت افزار شما را از بین می برند. در آخر بمب های زمان دار/ منطقی، مثل مخرب های داده ها و برنامه ها که به نرم افزار رایانه متصل می شوند و در یک لحظه به آن حمله می کنند.

کاری که در این باره می توان انجام داد:

➤ نرم افزار ضد ویروس: این یک سرمایه گذاری با ارزش است. بعضی از رایانه ها دارای نرم افزار از قبل نصب شده ای هستند که ممکن است زمان نامحدودی دوام داشته باشند یا این که تا یک دوره معین از زمان عمر داشته باشند. بعضی از تهیه کنندگان خدمات اینترنتی (ISPs) مثل AOL که شامل حفاظت در مقابل ویروس هاست این نرم افزارها را تهیه می کنند.

➤ آگاه باشید: با دقت به ضمیمه های پست الکترونیک نگاه کنید. اگر مشکوک به نظر می رسد، به آن فرصت ندهید. اگر چه این یک بررسی ارزشمند است اما برای تصمیم گرفتن تحقیق کنید.

➤ واقعی یا شوخی؟ بین آگاه بودن و فرستادن اخطارهای ویروس که سر راه شما قرار می گیرند متفاوت است. اول بایستی با دقت آن را ببینید. برای مثال سایت Snopes Urban Legends را در <http://snopes.com/computer/virus/virus.asp> چک کنید.

➤ مواظب باشید که چه چیزی را بارگذاری می کنید.
هیولای کوکی¹

منابع دیگر از تهدیدهای سیستم، کوکی ها هستند. کوکی ها قسمت کوچکی از داده ها هستند که یک وب سایت روی دیسک سخت شما ذخیره خواهد کرد. با استفاده از کوکی ها، وب سایت ها قادر هستند اطلاعات ویژه درباره یک کاربر، هنگامی که یک سایت را بازدید می کند را ذخیره کنند.

همچنین کوکی‌ها به وب سایت‌ها اجازه می‌دهند، هر آنچه که یک کاربر در سایت بازدید شده انجام داده است را پی‌گیری کنند.

کاری که در این باره باید انجام داد:

اگر شما زیاد کوکی‌ها را در رایانه‌تان دنبال نمی‌کنید، سیستم عامل را برای یافتن اطلاعاتی درباره حذف آنها بررسی کنید. همچنین شما می‌توانید از برنامه‌های حذف کوکی‌ها استفاده کنید. اما بدانید که اگر از آنها دور باشید، از وب سایت‌های متغیر دور خواهید بود و از این گذشته بعضی وب سایت‌ها برای بارگذاشتن اطلاعات به کوکی‌ها نیاز دارند.

جاسوس افزار¹

جاسوس افزار نرم افزاری است که اطلاعاتی در باره شما گردآوری میکند و آن‌ها را بدون اطلاع شما برای شخص ثالث می‌فرستد. این نرم افزار چه نوع اطلاعاتی درباره شما به دست می‌آورد؟ این نرم افزار می‌تواند عادت داشته باشد چیزهای واقعی مثل علایق شما یا کارها و چیزهایی که شما ترجیح می‌دهید و دیگر اطلاعات را استنباط کند. جاسوس افزار نیز اتصال شما را به اینترنت کند می‌کند و این دلیلی برای سرقت رفتن بسیاری از اطلاعات است.

کاری که در این باره باید انجام داد

سایت‌های اینترنتی مثل <http://www.pcpitstop.com/spycheck/sw> را برای لیست‌هایی از جاسوس افزارهای شناخته شده دنبال کنید. شما می‌توانید رایانه‌تان را توسط <http://geekssquad.com/securitycenter> وایروس یابی کنید.

¹ spyware

اسپم¹

اسپم یک پست الکترونیک خودکار ناخواسته است. به واسطه اسپم، شما باید هزینه بیشتری برای اتصال به اینترنت بپردازید. برای جا دادن پست های الکترونیکی که توسط اسپم ایجاد شده است، نیاز به خریداری رایانه های بیشتر، به اینترنت سریع تر، فضای اینترنتی بیشتر و هزینه نیروی کار بیشتر هست و اگر برای این موارد هزینه ی بیشتری پرداخت شود، ما هم باید پول بیشتری پرداخت کنیم.

کاری که در این مورد می توانیم انجام دهیم:

چند راه برای از بین بردن اسپم ها وجود دارد:

- محدود کردن آدرس های پست الکترونیک ارسال شده در فضای الکترونیکی عمومی: آدرس های پست الکترونیک که معمولاً در پایین سایت اینترنتی های شخصی چسبیده اند اهداف اسپم ها هستند. اسپم ها یک روش پیشرفته جستجو در اینترنت دارند که آدرس ها را جستجو کرده و به دست می آورد. اگر شما مجبور هستید پست الکترونیک شخصی خود را روی یک سایت اینترنتی بگذارید، راهی برای پنهان کردن آن پیدا کنید. همچنین پست های الکترونیکی خارج از شغل و حرفه، یا راهنمای اعضای که آدرس های پست الکترونیک دوستان برخط شما هستند را انتخاب کنید.
- از جواب دادن فرم هایی که آدرس پست الکترونیک شما را خواسته اند خودداری کنید: اگر می توانید آدرس های پست الکترونیک برای

¹ Spam

فرم هایی که درخواست پست الکترونیک می کنند، تهیه کنید. آدرس ها را برای فرم هایی که پاسخ هایشان برخط هستند پر کنید.

- از آدرس های پست های الکترونیکی استفاده کنید که حدس زدن آنها آسان نیست، زیرا رمز عبور آنها برای حدس زدن آسان است.

- از آدرس های پست الکترونیک های چندگانه استفاده کنید. همیشه از چندین آدرس پست الکترونیک استفاده کنید، برای کارهای شخصی تان از یک آدرس پست الکترونیک استفاده کنید. برای کارهایی که زیاد مهم نیستند و یا برای سرگرمی تان از آدرس های پست الکترونیک مختلف استفاده کنید. در حقیقت، از این راه می فهمید که چه کسی از آدرس پست الکترونیک شما سوءاستفاده کرده است. با یادداشت گذاشتن آدرس به کار برده شده در یک شکل و برای یک شخص می توان به راحتی سایتی را که منشاء اسپم است پی گیری کرد. از یک آدرس پست الکترونیک یک بار مصرف استفاده کنید چیزی که بتواند مطلب را به راحتی بگیرد و بدون کمترین تلاش استفاده کند.
- همیشه از یک فیلتر اسپم در هر قسمت شبکه یا برنامه برای مرور کردن پست الکترونیک ناخواسته استفاده کنید. در هر مورد از رسیدن اسپم توسط فیلتر جلوگیری می شود. خیلی از ISP ها فیلتر اسپم عرضه کرده اند.

- **ایجاد قوانین اسپم:** اعتراض های موجود به خاطر اسپم ها باعث شده خیلی از دولت های ملی و محلی قوانین آنتی اسپم را تصویب کنند. در اروپا قوانین خصوصی اتحادیه اروپا تصویب شده اند، و روش این است که باید شرکت ها قبل از فرستادن پست الکترونیک رضایت بگیرند، داده های شخصی را در وب پی گیری می کنند، به وسیله ی تلفن های سیار متصل به

ماهواره موقعیت تماس گیرنده را به دقت مشخص می‌کنند. همان قوانین، توانایی شرکت‌ها را برای استفاده از کوکی‌ها و دیگر برنامه‌ها که اطلاعات کاربر را جمع‌آوری می‌کند، محدود کرده است (مؤسسه تحقیقات 2006). در ایالات متحده تلاش بر این بوده که قوانین اسپم را برای دو سطح دولت مرکزی و ایالتی تصویب کنند:

قوانین اسپم دولت مرکزی: مجلس یک فهرست بدون اسپم را تصویب کرد و فرستادن پست الکترونیک تجاری ناخواسته و نیز استفاده از آدرس برگرداننده غلط یا موضوعات گمراه‌کننده را تحریم کرده است. قوانین اسپم ایالتی: همه ایالت‌ها شکل‌هایی از قوانین اسپم را در کتاب‌ها دارند.

بهترین تمرینات امنیت برخط

معمولاً افراد آسیب‌پذیر مثل بچه‌ها از اینترنت برای سرگرمی و برای مدرسه استفاده می‌کنند. اینترنت به آنها اجازه می‌دهد به انواع ابزار آموزشی و سرگرمی دسترسی داشته باشند. متأسفانه زمانی که سایت‌ها را برای کسب اطلاعات باز می‌کنند. به سایت‌های خطرناکی مراجعه می‌کنند مثل بازاریابی (چیزی که ممکن است آنها را وادار به فاش کردن اطلاعات کند). خبر خوب آن است که راه‌هایی برای مبارزه با آن وجود دارد.

- رایانه را در قسمت مناسبی از خانه بگذارید. این راه برای کنترل و مشاهده فرزندان هنگامی که آنلاین هستند، راحت است.
- بعضی اوقات، مدتی را با فرزندان در اینترنت بگذرانید. از آنها بخواهید سایت‌هایی را که مشاهده می‌کنند به شما نشان

دهند، و با آنها در مورد این که در رایانه چه کارهایی را انجام می دهند صحبت کنید. بعد از آن شما می توانید سایت هایی را که اخیراً بیشتر مشاهده شده اند در مرورگر تان چک کنید تا ببینید کجاها رفته.

- در مورد اطلاعات شخصی با فرزندان تان صحبت کنید. به آنها بگویید که چه چیزهایی را بدون این که از شما اجازه بگیرند نباید به دیگران بگویند و دلیل آن را نیز توضیح دهید. مطمئن شوید که آنها برای هر سوالی به شما مراجعه می کنند. قوانین را به وسیله رایانه تایپ، چاپ کرده و روی دیوار بچسبانید.

- کنترل های والدینی را به کار ببرید. نصب فیلترها در کاوشگر اینترنت¹ برای استفاده راهنمای مضمون داخلی آسان است. شما همچنین می توانید به نرم افزار سد کننده سایت نظری بیندازید (یک توصیه خوب: تحقیق کنید بچه هایتان چه کارهایی انجام می دهند و چگونه) حداقل این است که نرم افزار سد کننده سایت ممکن است سایت های مورد نیاز را هم مسدود کند.

- یک نقل قول خوب این است که ولو این که بچه ها ممکن است مهارت های فنی بهتری داشته باشند، به خاطر این دانش از آنها نترسید. بچه ها هنوز مشورت، راهنمایی، و محافظت نیاز دارند. راه های ارتباطی را باز بگذارید و اجازه دهید فرزند شما بداند که شما می توانید به هر سوالی که آنها ممکن است در باره طرز رفتار یا رویارویی با مشکلات در رایانه دارند، برسید.

¹ internet explorer

پورتال‌های کاربری

پورتال‌های کاربری، برنامه‌های کاربردی هستند که اغلب نیازهای روزمره یک کاربر را در ارتباط با جهان خارج پوشش می‌دهند. این شامل برنامه‌هایی از قبیل پست الکترونیک، کاوشگرهای وب، ابزارهای چت، انتقال ویدئو، نرم افزار کنترل راه دور، نرم افزار مبتنی بر شبکه و حوزه‌ای از نرم افزارهای مشابه می‌باشد. حمله‌کننده‌ها از امکانات موجود علیه خود سیستم میزبان بهره‌گیری می‌نمایند و یا از آنها در حمله به سیستم دیگر بهره می‌گیرند.

گفته می‌شود که گسترده‌ترین برنامه مورد استفاده برای ارتباطات امروزی، پست الکترونیک می‌باشد. ما از ایمیل برای نوشتن نامه، ارسال فایل‌های پیوست از قبیل تصاویر و فایل‌های متنی استفاده می‌کنیم و بسته به تنظیمات برنامه پست الکترونیک کاربر امکان دریافت محتوای وب نیز از طریق ایمیل وجود دارد. این پورتال کاربری، وقتی که یک دانشجوی فیلپینی ویروس love Bug را ساخت و منتشر نمود، موجب تحمیل خساراتی به ارزش کل 15-3 میلیارد دلار در سراسر جهان گردید. این ویروس کوچک به نحوی برنامه نویسی شده بود که از طریق رایانه میزبان که پیغام آلوده به این ویروس را باز می‌کرد خود را برای تمام افرادی که در لیست آدرس پستی آن قرار داشتند ارسال می‌نمود. محموله یک ویروس بود، پورتال برنامه ایمیل و هدف بعدی افرادی بودند که با قربانی اول مکاتبه الکترونیک داشتند لذا آسیب از طریق تکثیر و صدمه به سیستم رایانه میزبان وارد می‌گردید.

این یکی از کارهایی بود که یک ویروس با این پورتال می‌تواند انجام دهد. طراحی برخی ویروس‌ها بگونه‌ای است که با ارسال مقادیر انبوه نامه

الکترونیک به نحوی که از قدرت پردازش سرور پست الکترونیک یک سازمان خارج باشد، خدمات عادی سرور مذکور را دچار اختلال و قطع می‌نمایند.

درمورد کاوش‌گرهای وب نیز مطلب به همین صورت است. با وجود بیش از 8 تریلیون صفحه وب در جهان، احتمال آماری این که برخی از این صفحات به منظور اختلال، دزدی یا آسیب به یک رایانه متصل طراحی شده‌اند را نمی‌توان نادیده گرفت. در داخل این کاوشگرهای وب، اسکریپت‌ها و ابزارهایی وجود دارد (مانند جاوا اسکریپت، وی بی اسکریپت و غیره) که می‌توان از آنها علیه خود سیستم بهره گرفت. همان ابزاری که به یک کاوشگر وب امکان اجرا و پخش یک ویدیو در یک سایت خبری را می‌دهد قابل بهره‌گیری برای اجرای راه دور برخی برنامه‌ها و زیر برنامه‌های آلوده برای به کنترل درآوردن بخشی از رایانه میزبان می‌باشد. از این ابزارها می‌توان برای دستیابی به اطلاعات شخصی یا محرمانه موجود بر روی رایانه میزبان استفاده نمود. اتاق‌های گفتگوی آنلاین، نرم افزارهای ریموت و برنامه‌های کاربردی تحت وب همگی از امکاناتی هستند که در صورت دقت نکردن در مورد استفاده از آنها ممکن است به عنوان ابزارهایی در دست مهاجمین سایبر قرار گیرند. فایل‌های به روزرسانی¹ نیز از جمله مواردی هستند که در نصب آنها حداکثر دقت باید صورت پذیرد.

حمله‌کنندگان با استفاده از مکانیزم‌ها و ابزار فوق اقدام به تزریق کدهای آلوده‌ای به رایانه میزبان می‌نمایند که بصورت فایل‌های اجرایی مخفی نیازهای

¹ -Update

برنامه‌ریزی شده آنها را چه در قالب جمع‌آوری اطلاعات و چه برقراری امکان کنترل رایانه قربانی یا وارد آوردن صدمه به آن، تأمین می‌نمایند. این بسته‌های آلوده شامل ویروس‌ها، کرم‌ها، تروجان‌ها و اسکرپت‌های اجرایی می‌باشند.

مکانیزم‌های مذکور، روش‌های نفوذ خارجی مستقیم به سیستم‌ها و روش‌های علمی و عملی پیشرفته مقابله با آنها، همگی مطالبی هستند که درفصول مختلف این کتاب توصیف و ارائه شده است.

مواردی از امنیت

- اغلب سازمان‌ها و مدیران سیستم با تکنیک‌های آزمون نفوذ و کشف مداخله آشنا هستند. این تکنیک‌ها، بنیادهایی در ارزیابی امنیت هستند و بیشتر روی استخراج آسیب‌پذیری‌ها و رفتار مشکوک/بد اندیشی (برای مثال: تجزیه و تحلیل فایل ثبت موقوف) متمرکز هستند. اما، یک سازمان متکی بر این تکنیک‌ها ممکن است میزان اطلاعاتی که به طور بی‌نام (مبهم) از محتویات عمومی قابل دسترسی از اینترنت به دست می‌آیند را به شکل قابل توجهی کمتر از حد واقعی تخمین بزند. این مبحث مروری بر تکنیک‌های جمع‌آوری اطلاعات شبکه بصورت غیر فعال را ارائه می‌دهد. ممکن است برخی بر این باور باشند که تکنیک‌های غیر فعال از چشم انداز داخلی بسیار مفید هستند، زیرا ترافیک در شبکه داخلی را کاهش می‌دهند (برای مثال: انگشت‌نگاری غیر فعال سیستم عامل‌ها، جهت محاسبه سیستم

عاملهای در حال استفاده). سازمان ها باید جهت محافظت خودشان به دقت اطلاعات عمومی قابل دسترسشان را چک کنند.

بعضی از اطلاعات باید منتشر شوند (مثلاً ایمیل تماس)، اما اگر امکان سوء استفاده از آنها وجود دارد باید تمهیدات حفاظتی جهت جلوگیری از کشف این اطلاعات توسط مرورگرهای نفوذی خودکار، صورت پذیرد. یک روش رایج برای جلوگیری از مرور اطلاعات حساس، محافظت از آن با مکانیسم هایی است که برای انسان ها ساده اما برای دستگاه ها پیچیده است. قاعده کمترین اولویت دسترسی باید با انتشار حداقل مطلق اطلاعات، رعایت شود و تا آنجا که ممکن است از مرور اطلاعات عمومی اما حساس، ممانعت بعمل آورد. این توصیه برای DNS¹ قانونی است؛ اسامی میزبانها یا ابزاری که نباید از اینترنت به دست آیند را منتشر نمی کند. همچنین برای فایل های پیکربندی نیز قانونی است. اگر فایلی نباید مشترک باشد خصوصی نگه داشته می شود.

صفحات کد و صفحات وب از نظر پاکسازی آنها و جلوگیری از توضیحات، علایم طولانی، شماره نسخه و غیره، بررسی شوند. میزان زیادی از اطلاعات می تواند از صفحات خطا، علایم و اطلاعات به ظاهر بی ضرر جمع آوری شوند. توضیحات به طور باور نکردنی منبع نشت اطلاعات هستند؛ حضور یک بلوک کامل از کد سرور در صفحات مشتری چنین غیر منتظره نیست.

¹ - DNS مسئولیت حل مشکل اسامی کامپیوترها (ترجمه نام به آدرس) در یک شبکه و مسائل مرتبط را بر عهده دارد. (مخفف Domain Name Server)

بطور کلی، جمع آوری اطلاعات ابتدایی ترین گام یک حمله و احتمالاً قاطع ترین قدم در رسیدن به هدف توسط مهاجم است. اطلاعات جمع آوری شده در این گام، مطالب اولیه ای است که جهت تدارک یک حمله محکم به کار رفته است. مهاجمان می توانند یک دید کلی از هدف را به دست آورند، می توانند روی ضعیف ترین اتصال امنیتی تمرکز کنند و می توانند اطلاعات کافی را جهت هدایت مهندسی اجتماعی به دست آورند. اگر این گام به طور درست از طریق تکنیک های غیر فعال استفاده از اطلاعات قابل دسترس عموم هدایت شود، گمنام و عملاً کشف نشدنی است. از اینرو سازمان ها باید در مورد محتویات بی نام و نشان موجود در اینترنت بسیار دقیق باشند و باید تمهیدات ساده اما مؤثری را انجام دهند.

صندوق پستی فیزیکی شما باید برای همه، حداقل نامه رسان شما، در دسترس باشد. اما، هیچ کس در دنیای واقعی، شماره تأمین اجتماعی، تاریخ تولد یا شغل خود را در جعبه پستی اش نمی نویسد. این اطلاعات باید از دید نامه رسان و رهگذر پنهان نگه داشته شود همچنان که در دنیای سایر باید چنین باشد.

پایان

کتابنامه

- 1- ابراهیم نژاد محمد ، مقدمه ای بر جنگ سایبر و تروریسم سایبر – جلد یک ، انتشارات بوستان حمید ، 1389
- 2- سایت مرکز مدیریت امداد و هماهنگی عملیات رخداد های رایانه ای (certcc)، گزارش های تحلیلی ، شرکت فناوری اطلاعات ایران، 1390
- 3- مرکز مدیریت امداد و هماهنگی عملیات رخداد های رایانه ای ، امنیت فضای تولید و تبادل اطلاعات ، شرکت فناوری اطلاعات ایران، 1388
- 4- مقامی علی، مبانی امنیت اطلاعات، انتشارات انستیتوایز ایران، 1389

منابع لاتین:

- 1- Anderson j. q. and L. Rainie (2010) , the future of the internet, pew research center, Washington, D. C.
- 2-Peter Sommer and I. Brown (2011) , Reducing system cybersecurity Risk,information system and Innovation Group , London Schol of Economics
- Kizza, J. M. (2005). Computer network security. New York: Springer
- 3- securing the information infrastructure – joseph M. Kizza Florence M. Kizza.

4-Levine, J. R., Everett-Church, R., & Stebben, G. (2002).

Internetprivacy for dummies. Indianapolis: Wiley.

5- National Cyber Security Alliance. (2007). Top 8 cyber practices

Texas A&M Research Foundation (2006). National security threat list.

6-Retrieved from <http://rf-web.tamu.edu/security/SECGUI1DtEh/rTeamstl.htm#National%20Security>

7- Bond . A. (2010), Siemens, Stuxnet attack sophisticated, targeted.Available:

<http://www.controlglobal.com/industrynews/2010/163> . last accessed 13 august 2010.

^- Pfleeger, C., & Pfleeger, S. L. (2006). Security in computing (4th ed.). Boston: Prentice Hall

کتاب های منتشر شده در این حوزه

