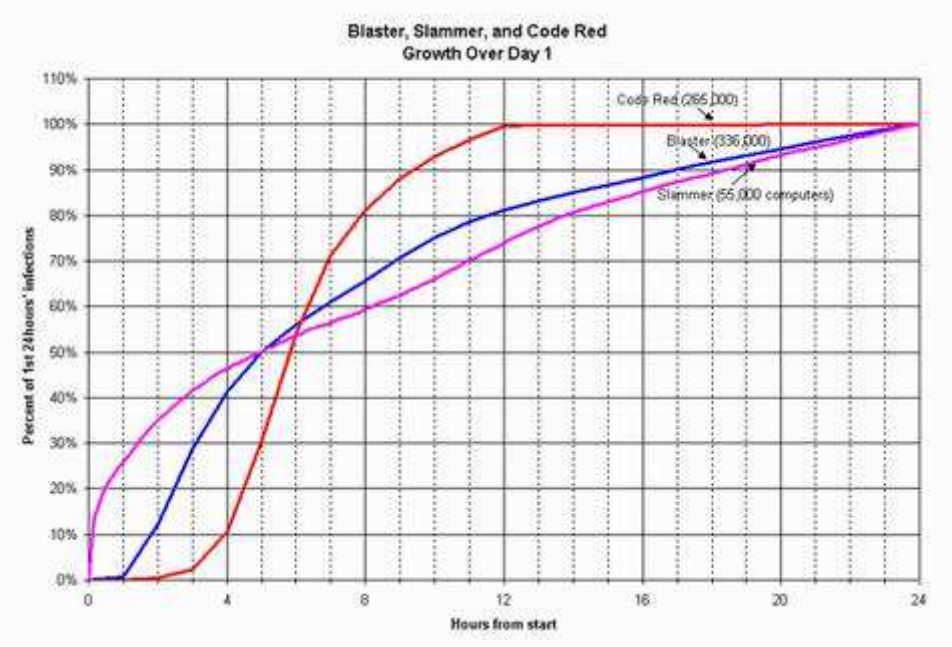
دفاع در مقابل کرم ها و ویروس ها ی کامپیوتری

کرم ها و ویروس ها نوع خاصی از برنامه های کامپیوتری موسوم به " کد مخرب " می باشند. علت ظهور کرم ها و ویروس ها ، وجود ضعف در برنامه ها ی کامپیوتری است . آنان نسخه هائی از خود را تکرار و یا به سایر برنامه ها متصل، بسرعت گسترش و بسادگی از سیستمی به سیستم دیگر توزیع می شوند.درابتدا لازم است که تعریف مناسبی برای هر یک از آنان ارائه گردد . کرم ها ، نوع خاصی ازبرنامه های کامپیوتری می باشند که پس از آغاز فعالیت خود ، بدون مداخله انسانی منتشر و توزیع خواهند شد. ویروس ها ، نوع دیگری از برنامه های کامپیوتری می باشند که بمنظور انتشار و توزیع خود نیازمند انجام عملیات خاصی توسط کاربر نظیر فعال شدن فایل همراه یک نامه الکترونیکی می باشند.کاربران در اغلب موارد و در مشاهده با فایل های ضمیمه همراه نامه های الکترونیکی ، اغوا و بدون لحاظ نمودن مسائل امنیتی آنان را باز و به عاملی برای گسترش یک ویروس تبدیل می شوند. کاربران بدلیل کنجکاوی مربوط به موضوع یک نامه و یا ظاهر شدن نامه بگونه ای که برای مخاطب خود آشنا است ، اقدام به باز نمودن ضمائم یک نامه الکترونیکی می نمایند. کرم ها و ویروس می توانند اقدامات پیشگیرانه امنیتی نظیر فایروال ها و سیستم های حفاظتی را نادیده و اهداف خود را

دنبال نماید.

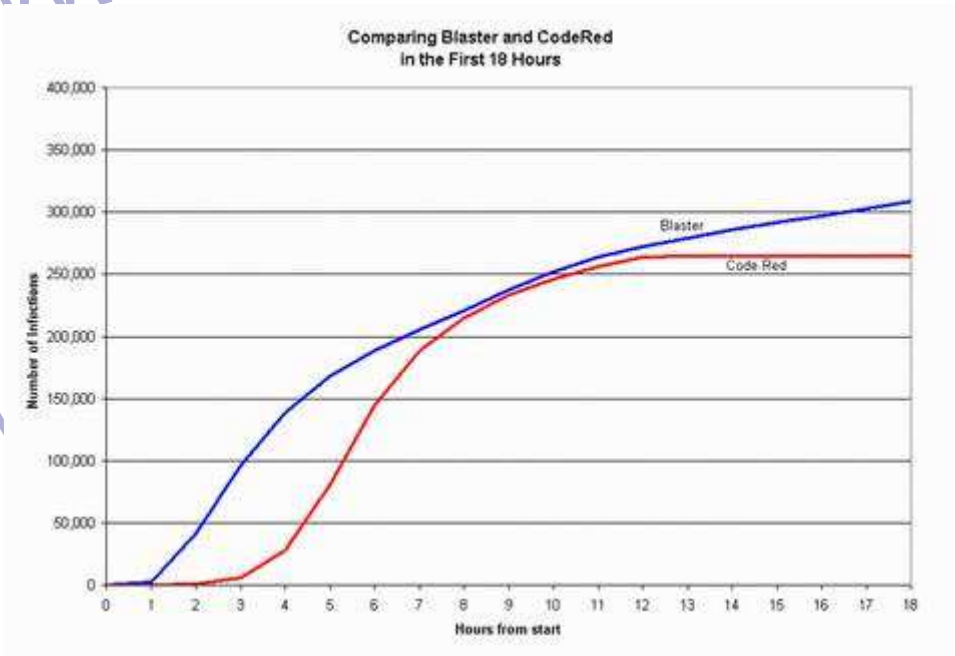
کرم ها و ویروس ها در مقایسه با گذشته با سرعت بمراتب بیشتری اقدام به خرابی سیستم های آسیب پذیر نموده و در این راستا نسخه هائی از خود را برای اکثر سیستم های فوق ، توزیع و منتشر می نمایند. کامپیوترهای موجود در منازل ، نمونه مناسبی از سیستم های آسیب پذیر بوده که شرایط و استعداد مناسبی را در این رابطه دارند. کرم Red Code در سال ۲۰۰۱ بسرعت در سطح جهان منتشر گردید . سرعت انتشار کرم فوق، بمراتب بیشتر از کرم Morris در سال ۱۹۸۸ و ویروس ملیزا در سال ۱۹۹۹ بود. بدیهی است، افزایش سرعت انتشار این نوع از کدهای مخرب ، سرعت در بروز خرابی و آسیب را بدنبال خواهد داشت. مثلا" فاصله زمانی بین شناسائی اولین نسخه کرم Code Red و خرابی گسترده آن، صرفا" چندین روز بیشتر نبوده است و دراین فاصله زمانی محدود، Code Red بسرعت اشاعه و گسترش پیدا کرده بود. پس از گذشت یک ماه از ظهور کرم Red Code ، کرم دیگری با نام "نیمدا" توانست در اولین ساعت فعالیت خود ، خرابی بسیار گسترده ای را ایجاد نماید . در ژانویه همان سال ، "اسلامر" توانست صرفا" در مدت چندین دقیقه خرابی گسترده ای را بوجود آورد .شکل زیر،سرعت انتشار و میزان آسیب رسانی " اسلامر" ، بلستر و Code red در اولین روز فعال شدن را نشان می دهد . همانگونه که مشاهده می

شود ، اسلامر توانسته است با سرعت بیشتری در اولین ساعات فعال شدن خود ، تعداد زیادی از سیستم ها را آلوده نماید. سرعت انتشار بلستر از اسلامر کندتر ولی از Code Red سریعتر بوده است . پس از گذشت بیست و چهار ساعت، بلستر به ۳۳۶،۰۰۰ ، Code Red. به ۲۶۵،۰۰۰ و اسلامر به ۵۵،۰۰۰ دستگاه کامپیوتر آسیب رسانده بودند. دقت داشته باشید که بلستر در هیجده ساعت اولیه فعالیت خود تواسنه است بیش از ۳۳۶،۰۰۰ کامپیوتر را آلوده نماید. بلستر نسبت به اسلامر توانسته است علیرغم کند بودن انتشار در ساعات اولیه ، تعداد بمراتب بیشتری از سیستم ها را آلوده نماید . بنابراین ، ما از یکطرف سرعت در انتشار و از طرف دیگر افزایش بالای تعداد سیستم های آسیب پذیر را می توانیم مشاهده نمائیم.



منبع : CERT.org

شکل زیر، عملکرد کرم بلستر و Code Red در هیجده ساعت اولیه فعالیت آنان را نشان می دهد. در هر دو حالت در ساعات بین سه تا پنج اولیه فعالیت ، نزدیک به ۱۰۰،۰۰۰ کامپیوتر آلوده شده بود. سرعت انتشار و آسیب به اندازه ای سریع بوده است که اغلب مدیران سیستم و کاربران زمان لازم بمنظور ایمن سازی سیستم ها پس از اعلام ضعف امنیتی را نداشته اند .



منبع : CERT.org

عملکرد کرم ها و ویروس ها در بهترین حالت ، کرم ها و ویروس ها بمنزله مزاحمینی می باشند که بمنظور برخورد با آنان می بایست هزینه های زیادی صرف گردد. در بدترین حالت ، آنان بمنزله دشمنان خانمان سوزی بوده که قادرند سرمایه های اطلاعاتی را نابود و ویران نمایند. بر اساس گزارشات

منتشر شده ، صرفا" در دوازده ماه گذشته ، حملات کرم ها و ویروس ها میلیون ها دلار خسارت را متوجه سازمان ها و موسسات نموده است . براساس نظر سنجی انجام شده توسط CSI/FBI در سال ۲۰۰۳ ، بیش از هشتاد و دو درصد از پاسخ دهندگان با نوع خاصی از حملات توسط ویروس ها و کرم ها برخورد داشته که هزینه ای معادل ۳۸۲،۳٤۰،۲۷ دلار صرف برطرف نمودن مشکلات مربوطه شده است . کمترین هزینه گزارش شده ٤۰،۰۰۰ دلار و بیشترین هزینه گزارش شده بالغ بر ٦،۰۰۰،۰۰۰ دلار بوده است . در یک نظر سنجی دیگر و در استرالیا نیز نتایجی مشابه بدست آمده است . در این نظر سنجی بیش از هشتاد درصد از پاسخ دهندگان با نوع خاصی از حملات توسط کرم ها و یا ویروس ها مواجه بوده اند . در بررسی انجام شده توسط موسسه تحقیقاتی استرالیا ، ۳۳ ٪ درصد از پاسخ دهندگان اعلام نموده اند که مشکل آنان در کمتراز یک روز ، ۳۰ ٪ اعلام نموده اند که مشکل آنان بین یک تا هفت روز و ۳۷ ٪ دیگر اعلام نموده اند که بیش از یک هفته صرف برطرف نمودن مشکل آنان شده است . (برخی از سازمان ها و موسسات نیز اعلام نموده اند که مشکل آنان هرگز برطرف نشده است) . میزان صدمات وخرابی گزارش شده در ارتباط با کرم بلستر، بالغ بر ٥۲٥ میلیون دلار و در ارتباط با سوبیگ (نوع F) ، بین ٥۰۰ میلیون تا یک میلیارد دلار برآورد شده است.هزینه فوق ، شامل ازدست دادن بهره وری ، ساعات

تلف شده ، عدم فروش کالا و یا خدمات و هزینه های اضافی مربوط به پهنای باند است . بر اساس اظهارات ارائه شده در نشریه اکونومیست ۲۳ اگوست ۲۰۰۳ ، سوبیگ (نوع F)، مسئول یکی از شانزده نامه الکترونیکی ارسال شده بر روی اینترنت بوده است . برخی سازمان های بزرگ ، صرفا" طی یک روز بیش از ۱۰،۰۰۰ نامه الکترونیکی آلوده را دریافت نموده اند (در هر ۸.٦ ثانیه ، یک پیام) . سوبیگ ، قادر به ارسال چندین نامه الکترونیکی در یک زمان بود و بدین ترتیب ضریب نفوذ و اشاعه آن بشدت بالا بود . (هزاران پیام در یک دقیقه) . با توجه به اینکه، سوبیگ چندین مرتبه تغییر و نسخه های جدیدتری از آن ارائه می شد، برخورد و غیر فعال نمودن آن با مشکل مواجه می گردید . (حرف F نشاندهنده نسخه شماره شش سوبیگ است) .

وضعیت آینده

نتایج و تجارب کسب شده ، صرفا" محدود به عملکرد خاص برخی از کرم ها و ویروس ها نظیر بلستر و سوبیگ بوده و ما می بایست به این واقعیت مهم توجه نمائیم که کرم ها و ویروس ها یک تهدید جدی در رابطه با امنیت اینترنت بوده و می توانند مسائل متعدد و غیرقابل پیش بینی را در آینده برای هر یک از شهروندان حقوقی و یا حقیقی اینترنت بدنبال داشته باشند .بنابراین می توان این ادعا را داشت که اینترنت نه تنها در حال حاضر در مقابل اینگونه

حملات آسیب پذیر است بلکه آسیب پذیری آن در آینده نیز قابل پیش بینی و واقعیتی غیرقابل کتمان است. کامپیوترهای موجود در سازمان ها ، موسسات دولتی و خصوصی ، مراکز تحقیقاتی ، مدارس ، دانشگاه ها در حال حاضر نسبت به ضعف های امنیتی کشف شده آسیب پذیر بوده و قطعا" نسبت به ضعف هائی که در آینده مشخص می گردند، نیز آسیب پذیری خود را خواهند داشت . بنابراین ، سیستم های کامپیوتری هم در مقابل حملات در حال حاضر و هم برای حملات در آینده ، دارای استعداد لازم بمنظور پذیرش آسیب خواهند بود. بدیهی است ، همزمان با افزایش وابستگی سازمان ها و موسسات دولتی و خصوصی به اینترنت ، انجام فعالیت های تجاری، تهدیدات و خطرات خاص خود را بدنبال خواهد داشت .

محدودیت راه حل های واکنشی

پس از گذشت قریب به پانزده سال از عمومیت یافتن اینترنت و مطالعات گسترده انجام شده بمنظور کاهش خطرات ، خرابی و سرعت در تشخیص و غلبه بر حملات ، می توان این ادعا را نمود که راه حل های واکنشی به تنهائی کافی نخواهند بود. ادعای فوق ، ماحصل توجه به عوامل زیر است :

- اینترنت در حال حاضر بیش از ۱۷۱،۰۰۰،۰۰۰ کامپیوتر را بیدیگر متصل و رشد آن همچنان ادامه دارد . در حال حاضر ، میلیون ها

کامپیوتر آسیب پذیر در اینترنت وجود دارد که مستعد یک نوع خاص از حملات توسط مهاجمین می باشند.

- تکنولوژی حملات بسیار پیشرفته شده و مهاجمان می توانند با اتکاء بر آخرین فنآوری ها ی موجود ، بسادگی از نقاط ضعف موجود در سیستم های آسیب پذیر استفاده و به آنان آسیب مورد نظر خود را برسانند(حملات مبتنی بر آخرین تکنولوژی موجود).
- تعداد زیادی از حملات در حال حاضر بصورت کاملا" اتوماتیک عمل نموده و با سرعت بسیار بالائی در اینترنت و صرفنظر از منطقه جغرافیائی ویا محدودیت های ملی ، توزیع و گسترش می یابند.
- تکنولوژی بکارگرفته شده در حملات بسیار پیچیده و در برخی موارد تعمد پنهانی در آنان دنبال می گردد . بنابراین ، کشف و آنالیز مکانیزمهای استفاده شده بمنظور تولید پادزهر و برطرف نمودن مشکل ، مستلزم صرف زمان زیادی خواهد بود .
- کاربران اینترنت وابستگی زیادی به اینترنت پیدا کرده و از آن بمنظور انجام کارهای حیاتی خود نظیر: فعالیت های تجاری Online استفاده می نمایند. کوچکترین وقفه در ارائه خدمات می تواند ازدست دادن منابع اقتصادی و بمخاطره افتادن سرویس های حیاتی را بدنبال داشته باشد .

توجه به هر یک از موارد اشاره شده ، شاهدی است بر این ادعا که ما همچنان در معرض طیف گسترده ای از حملات قرار گرفته ایم . حملاتی که از دست دادن منابع اقتصادی و عدم امکان عرضه سرویس ها را بدنبال خواهد داشت .در این راستا می بایست از تمامی امکانات و پتانسیل های موجود بمنظور سرعت در پاسخ و برخورد با حملات استفاده نمود. بازنگری در راه حل ها ی موجود و استفاده از رویکردهای علمی و جامع می تواند عاملی موثر در جهت برخورد مناسب با حملات باشد.

وظایف مدیران سیستم

شناسائی تهدیدات کرم ها و ویروس ها عملیات ساده و ایستائی نبوده و در این رابطه می بایست از رویکردهای کاملا" پویا و مبتنی بر آخرین دستاوردهای تکنولوژی استفاده گردد. با کشف بیش از چهار هزار نوع نقطه آسیب پذیر در طی هر سال ، مدیران سیستم و شبکه در وضعیت دشواری قرار دارند . آنان با چالش های جدی در ارتباط با تمامی سیستم ها ی موجود و Patch های مورد نظر که برای برطرف نمودن نقایص امنیتی ارائه می گردد ، مواجه می باشند . استفاده و بکارگیری Patch ها ی ارائه شده در عین مفید بودن بمنظور مقابله با مشکل امنیتی ایجاد شده ، می تواند زمینه بروز مسائل و اثرات جانبی غیرقابل پیش بینی را فراهم نماید . در این رابطه لازم است به

این نکته مهم نیز اشاره گردد که پس از ارائه یک Patch امنیتی ، مدت زمان زیادی طول خواهد کشید که مدیران سیستم و یا شبکه مشکل تمامی سیستم های آسیب پذیر خود را برطرف نمایند. مدت زمان برطرف سازی مشکلات و اشکالات بوجود آمده در برخی موارد می تواند ماه ها ویا حتی سالها پس از ارائه patch پیاده سازی شده ،بطول می انجامد . مثلا" هنوز گزاشاتی در رابطه با ویروس ملیزا که چهار سال از فعال شدن آن گذشته است ، توسط برخی سازمان ها و موسسات در سطح جهان ارائه می گردد. ریشه کن نمودن یک کرم و یا ویروس شایع ، با توجه به گستردگی اینترنت ، عملیاتی نیست که در یک بازه زمانی محدود، بتوان موفق به انجام آن گردید ومی بایست برای نیل به موفقیت فوق ، زمان زیادی صرف گردد . شاید این سوال مطرح گردد که دلایل اینهمه تاخیر در ریشه کن نمودن یک ویروس و یا کرم چیست ؟ در پاسخ می توان به موارد متعددی نظیر صرف زمان زیاد ، پیچیدگی گسترده آنان و عدم اختصاص اولویت مناسب برای مقابله با آنان در یک سازمان و یا موسسه ، اشاره نمود.متاسفانه ، بسیاری از مدیران شناخت کامل و جامعی نسبت به تهدیدات نداشته و هرگز به مقوله امنیت با یک اولویت سطح بالا نگاه نکرد و حتی منابع لازم را به این مقوله اختصاص نمی دهند. علاوه بر این ، سیاست های تجاری در برخی موارد سازمان ها را بسمت انتخاب یکی از دو گزینه : اهداف تجاری و نیازهای

امنیتی هدایت که در اکثر موارد رسیدن به اهداف تجاری دارای اولویت و جایگاه بالاتری برای آنان می باشند. علاوه بر تمامی مسائل فوق، می بایست به این نکته مهم نیز اشاره گردد که تقاضا برای مدیران سیستم ورزیده و کارشناس بیش ازمیزان موجود بوده و همین امر همواره استفاده از متخصصین و کارشناسان امنیتی را با مشکل جدی مواجه می سازد(عدم توازن بین عرضه و تقاضا) .

بمنظور برخورد مناسب با وضعیت فوق ، مدیران سیستم در یک سازمان می توانند با دنبال نمودن مراحل زیر عملیات لازم در جهت تسهیل در امر حفاظت سیستم های سازمان را انجام دهند:

اتخاذ روش های امنیتی

.انتخاب سیستم های ارزیابی امنیت اطلاعات ، مدیریت سیاست ها و تبعیت از روش های امنیتی برای تمامی سازمان ها (بزرگ و کوچک) امری حیاتی است . سازمان ها و موسسات می توانند بر اساس وضعیت موجود خود ، یکی از روش های مناسب امنیتی را انتخاب نمایند. در این راستا می توان از پتانسیل ها و تجارب بخش دولتی و یا خصوصی استفاده گردد. در این رابطه می توان از منابع متعدد اطلاع رسانی موجود بمنظور اتخاذ سیاست های کلی

امنیتی استفاده و پس از بررسی آنان نسبت به تدوین و پیاده سازی سیاست امنیتی در سازمان مربوطه ، اقدام نمود.

- بهنگام نمودن دانش و اطلاعات . مدیران سیستم می بایست بمنظور ارتقاء سطح دانش و معلومات خود ، دوره های آموزشی خاصی را بگذرانند . شرکت در دوره های آموزشی مستمر و اختصاص وقت لازم برای استفاده مفید از دوره های آموزشی می بایست در دستور کار مدیران سیستم در سازمان ها و موسسات قرار گیرد . مدیران سیستم لازم است ضمن آشنائی با آخرین تهدیدات و حملات با ابزارهای لازم در جهت افزایش حفاظت سیستم ها نیز شناخت مناسبی را پیدا نمایند .لازم است به این نکته مهم اشاره گردد که امنیت ، دارای ماهیتی کاملا" پویا بوده که همزمان با بروز حملات جدید و شناسائی نقاط آسیب پذیر جدید بصورت روزانه تغییر و ارتقاء می یابد. با دانش استاتیک و محدود نمی توان با مقوله های پویا و گسترده برخوردی مناسب و علمی داشت .
- آموزش کاربرانی که از سیستم ها استفاده می نمایند . مدیران سیستم می بایست برنامه های آموزشی خاصی را در رابطه با امنیت ، بمنظور ارتقاء دانش کاربران نسبت به مسائل امنیتی ، ارائه نمایند. دوره ها و

برنامه های آموزشی می بایست کاملا" هدفمند بوده و کاربران پس از شرکت وگذراندن دوره های فوق ، به سطح مطلوبی از توانائی بمنظور تشخیص یک مسئله ، انجام عملیات لازم بمنظور افزایش حفاظت سیستم، برخورد مناسب در صورت مواجه با یک مشکل امنیتی دست پیدا کرده باشند. بمنظور پیاده سازی سیاست امنیتی در یک سازمان ،وجود کاربران آگاه با مسائل ایمنی اطلاعات و حفاظت از اطلاعات حساس ، امری ضروری و لازم است .

وظایف ارائه دهندگان تکنولوژی

مدیران سیستم با دنبال نمودن پیشنهادات ارائه شده، صرفا" قادر به حل بخش هائی از مسئله امنیت اطلاعات می باشند. با توجه به جایگاه شرکت های ارائه دهنده تکنولوژی، حرکات و تدابیر مثبت آنان می تواند تاثیر زیادی در جهت ممانعت و گسترش کرم ها و ویروس ها را بدنبال داشته باشد . با اینکه برخی شرکت ها بسمت ارتقاء و بهبود امنیت در محصولات خود حرکت نموده اند ، ولی هنوز راهی طولانی در پیش است . متاسفانه ، پیاده کنندگان نرم افزار از تجارب گذشته در رابطه با نقایص امنیتی در ارائه نسخه ها ی جدید نرم افزار خود استفاده نمی نمایند. بر اساس مطالعات انجام شده ، مشاهده شده است که برخی از نقاط آسیب پذیر جدید در نسخه های جدید

برخی محصولات در نسخه های قبلی هم وجود داشته و تلاش مناسبی در جهت بهسازی وضعیت امنیتی نسخه جدید صورت نگرفته است .

وجود برخی از نقاط آسیب پذیر بدلیل عدم پیکربندی ایمن سیستم های عامل و برنامه های کاربردی است . محصولات فوق ، بسیار پیچیده بوده و اغلب با غیر فعال نمودن برخی از ویژگی ها ی امنیتی به مشتریان عرضه می شوند .شرکت های ارائه دهنده بر این اعتقاد می باشند که همزمان با استفاده از محصول ارائه شده ، کاربران می توانند ویژگی های امنیتی غیر فعال شده را در زمان لازم و بدلخواه خود فعال نمایند. بدین ترتیب تعداد زیادی از سیستم های متصل شده به اینترنت دارای پیکربندی مناسب در رابطه با امنیت اطلاعات نبوده و شرایط مناسبی را برای نفوذ کرم ها و ویروس ها فراهم می نمایند.

ارائه محصولاتی که در مقابل کرم ها و ویروس ها نفوذناپذیر باشند ، برای هر شرکت ارائه کننده محصولات ،امری ضروری و حیاتی است . اعتقاد به این رویکرد امنیتی که " کاربر می بایست مواظب باشد " ، در عصر حاضر پذیرفتنی نیست ، چراکه سیستم ها بسیار پیچیده بوده و سرعت حملات نیز باورنکردنی است و در برخی موارد فرصت مناسب برای برخورد با نقص امنیتی از کاربر سلب می گردد . تولید کنندگان محصولات می توانند با اتکاء و

استفاده از روش های مهندسی نرم افزار تلاش خود را در جهت تولید محصولات مقاوم در برابر حملات ، مضاعف نمایند. در این راستا موارد زیر پیشنهاد می گردد :

- نرم افزار ضد ویروس / مقاوم در مقابل ویروس . کامپیوترها و نرم افزارها دارای امکانات ذاتی بمنظور ایمن شدن در مقابل تهدیدات و حملات کرم ها و ویروس ها نمی باشند. طراحی کامپیوترها و یا نرم افزارهای کامپیوتری بگونه ای است که امکان توزیع و انتشار ویروس ها و آلودگی سیستم ها را فراهم می نماید. در برخی موارد طراحی انجام شده بگونه ای است که شرایط لازم برای حملات و نفوذ کرم ها و ویروس ها را فراهم و استعداد فوق در بطن محصول ارائه شده وجود خواهد داشت . اجراء یک کد نامشخص و وارده از یک منبع ناشناس و گمنام نمونه ای از استعداد اشاره شده در بطن محصولات بوده که امکان فعال شدن یک کد اجرائی بدون محدودیت و نظارت خاصی بر روی یک ماشین ، فراهم می گردد.بدین ترتیب سیستم در مقابل حملات ویروس ها آسیب پذیر و لازم است تولید کنندگان، سیستم ها و نرم افزارهای خود را بگونه ای ارائه نمایند که باعث محدودیت در اجرای کدهای وارده ، خصوصا" کدهائی که از منابع

تائید نشده و ناشناخته سرچشمه می گیرند، گردند. در این رابطه می توان از روش های شناخته شده و مبتنی بر مهندسی نرم افزار متعددی استفاده نمود.

- کاهش خطاء پیاده سازی . اکثر نقاط آسیب پذیر موجود در محصولات از خطاهای موجود در مرحله پیاده سازی نرم افزار، ریشه می گیرد. این نوع خطاها در محصولات باقی مانده و شاید منتظرند که در زمان بکارگیری نرم افزار شناسائی گردند ! تشخیص و برطرف نمودن این نوع خطاها ، صرفا" زمانی میسر می گردد که محصول در حال استفاده و کاربری است . در موارد زیادی ، نقایص امنیتی مشابه بصورت پیوسته در نسخه های جدید محصولات، مجددا" مشاهده و کشف می گردد.مهمترین علت بروز اینگونه نقاط آسیب پذیر، طراحی سطح پائین و یا عدم برخورد مناسب با خطاها در زمان پیاده سازی است . تولیدکنندگان و ارائه دهندگان محصولات نرم افزاری لازم است با مطالعه و بررسی اشتباهات گذشته و بکارگیری روش های موثر موجود در مهندسی نرم افزار سعی در کاهش حفره ها و نقایص امنیی در محصولات خود نمایند .
- پیکربندی پیش فرض با امنیت بالا . امروزه با توجه به پیچیدگی محصولات نرم افزاری ، پیکربندی مناسب سیستم ها و شبکه ها

بمنظور استفاده از تدابیر امنیتی پیش بینی شده ، امری دشوار بنظر می رسد . حتی در برخی موارد افرادیکه دارای مهارت های فنی قابل قبولی بوده و آموزش های لازم را نیز فراگرفته اند ، بمنظور استفاده و بکارگیری امکانات امنیتی در یک محصول نرم افزاری، دارای مشکلات خاص خود می باشند.اشتباهات کوچک می تواند سیستم ها را در معرض تهدید و کاربران را با حملات غیر قابل پیش بینی مواجه نماید. تولید کنندگان و ارائه دهندگان تکنولوژی می توانند محصولات خود را با پیکربندی پیش فرض ایمن،ارائه نمایند . در چنین مواردی اکثر گزینه ها و امکانات امنیتی موجود ، بصورت پیش فرض و در زمان نصب فعال خواهند بود. بدین ترتیب کاربران در آغاز استفاده از یک محصول نیازمند تغییرات خاصی در رابطه با پیکربندی محصول نداشته و در ادامه و در صورت ضرورت ،می توانند پیکربندی های پیش فرض را متناسب با خواسته خود تغییر نمایند . بنابراین ، کاربران با یک سطح امنیتی قابل قبول استفاده از محصول را آغاز می نمایند.

وظایف تصمیم گیرندگان

تصمیم گیرندگان در یک سازمان ، موسسه و سایر بخش ها ی کلان یک کشور، می توانند بمنظور افزایش امنیت از رویکردهای متفاوتی استفاده نمایند . در این راستا موارد زیر پیشنهاد می گردد :

- تقویت انگیزه های لازم برای ارائه محصولات با ایمنی بیشتر و کیفیت بالا . بمنظور ترغیب ارائه دهندگان بمنظور تولید محصولات باکیفیت و ایمنی مناسب ، پیشنهاد می گردد که تصمیم گیرندگان از قدرت خرید خود بمنظور تقاضای نرم افزار با کیفیت بالا استفاده نمایند . در هنگام تهیه نرم افزار و عقد قرارداد مربوطه می بایست عبارت " کد بی نقص " با صراحت در متن قرارداد آورده شود. بدین ترتیب تولید کنندگان و ارائه دهندگان محصولات در مواردی که نقایص خاصی نظیر نقایص امنیتی در محصول مربوطه تشخیص و کشف می گردد ، ملزم به رفع عیب و اشکال موجود خواهند بود. پایبندی به رویکرد فوق ، انگیزه های مناسبی را برای تولیدکنندگان ایجاد و هر تولید کننده که محصول بی نقصی را تولید و ارائه نمائید ، شانس موفقیت بیشتری را خواهد داشت .

دراین رابطه لازم است ، تصمیم گیرندگان با مسائل متعددی همچون فرآیندهای تهیه یک محصول آشنا و بصورت مستمر اطلاعات خود را

نیز ارتقاء تا بتوانند در زمان لازم تصمیمات منطقی و مبتنی بر دانش را برای تهیه یک محصول اتخاذ نمایند.بمنظور حمایت از چنین فرآیندهائی، تهیه کنندگان می بایست آموزش های لازم در خصوص نظارت ، سیاست های امنیتی ، اصول و مفاهیم امنیتی و معماری مربوطه را فرا بگیرند .بهرحال هدف ، تهیه و بکارگیری سیستمهائی است که با روح یک سازمان مطابقت و افزایش کارآئی و بهره وری را بدنبال داشته باشند .

- تحقیق در رابطه با تضمین ایمن سازی اطلاعات . تصمیم گیرندگان ، می بایست همواره بدنبال راه حل های تکنیکی بمنظور افزایش ضریب امنیت اطلاعات بوده و در این راستا لازم است تحقیقات گسترده و سازمان یافته ای را بمنظور آگاهی از روش های کنشگرایانه وپیشگیرانه در دستور کار خود قرار دهند (استفاده از روش های واکنشی و انفعالی به تنهائی کفایت نخواهد کرد) . بنابراین ، تصمیم گیرندگان می بایست از یک برنامه منسجم تحقیقاتی حمایت تا بکمک آن بتوان با رویکردهای جدید در ارتباط با امنیت اطلاعات و سیستم آشنا گردید.رویکردهای فوق ، شامل طراحی و پیاده سازی استراتژی ها ، روش های بازسازی اطلاعات ، استراتژی های مربوط به مقاومت در مقابل تهاجمات ، آنالیزهای مستمر و پیاده سازی معماری های

امنیتی باشد . از جمله فعالیت هائی که می بایست در این خصوص مورد توجه و برای آنان راهکارهای مناسب ایجاد گردد، عبارتند از :

– ایجاد یک چارچوب یکپارچه و یکنواخت برای آنالیز و طراحی تضمین اطلاعات

- – ایجاد روش های مستحکم و مطمئن بمنظور دستیابی و مدیریت خطرات برخاسته از تهدید سرمایه های اطلاعاتی

– ایجاد روش های ارزیابی بمنظور مشخص کردن و بدست آوردن نسبت هزینه / مزیت ، استراتژی های ریسک

– ایجاد و استفاده از تکنولوژی های جدید بمنظور مقاومت در برابر حملات ، تشخیص حملات و بازیابی خرابی ها

– ایجاد روش های سیستماتیک و ابزارهای شبیه سازی برای آنالیز حملات ، تصادمات و خرابی بین سیستم های وابسته

- استفاده از متخصصین فنی بیشتر . تصمیم گیرندگان ، می بایست از مراکز امنیتی بمنظور ارتقاء سطح دانش عمومی امنیت حمایت نموده تا از این طریق بتوان کارآموزان و دانشجویان را جذب و با تدوین یک برنامه آموزشی هدفمند نسبت به تربیت کارشناسان ماهر امنیتی اقدام نمود .بدیهی است استفاده از کارشناسان فوق ، بمنظور ایمن سازی سیستم ها و شبکه امری ضروری و اجتناب ناپذیر است . برنامه های

آموزشی تدوین شده در فواصل زمانی خاصی می بایست بازنگری تا بتوان افرادی را تربیت که همواره پاسخگوی نیازهای امنیتی در سطح سازمان ها و موسسات بوده و با دانش روز نیز کاملا" آگاه باشند.

- ارائه آموزش و آگاهی لازم به کاربران اینترنت : دستیابی آسان و وجود اینترفیس های مناسب ، باعث شده است که کاربران با هر نوع شرایط سنی از اینترنت در تمامی سطوح زندگی استفاده نمایند.تعداد زیادی از کاربران اینترنت دارای شناخت اندکی نسبت به تکنولوژی اینترنت و یا روش های امنیتی لازم برای استفاده ، می باشند . تصمیم گیرندگان ، می توانند با دنبال نمودن پیشنهادات زیر ، سطح دانش کاربران اینترنت را افزایش دهند :

– طراحی و پیاده سازی برنامه ها و مواد آموزشی لازم در خصوص ارتقاء سطح دانش عمومی تمامی کاربران اینترنت .آموزش و افزایش آگاهی کابران در خصوص : خصایص امنیتی ، تهدیدات ، فرصت ها و رفتار مناسب در اینترنت به امری ضروری و حیاتی تبدیل شده است . در این رابطه لازم است به این نکته مهم اشاره گردد که بقاء سیستم وابسته به امنیت سیستم ها در سمت دیگر بوده و حل مشکل سیستم خود به تنهائی کافی نخواهد بود و در این رابطه لازم است به تمامی کاربران در خصوص نحوه استفاده از کامپیوترهای خود با لحاظ

نمودن پارامترهای ایمنی و امنیتی ، آموزش های لازم و مستمر ارائه گردد .علاوه بر موارد فوق ، لازم است به مصرف کنندگان محصولات نرم افزاری آموزش های خاصی در رابطه با نحوه تهیه و نصب نرم افزارهای ایمن ارائه گردد . بدین ترتیب تولیدکنندگان محصولات نرم افزاری ترغیب به ارائه محصولات خود با نقاط آسیب پذیری کمتر خواهند شد .

- طراحی و پیاده سازی برنامه های آموزشی خاص در زمینه استفاده مناسب و اولیه از کامپیوتر . آموزش های فوق ، می بایست بهمراه آموزش های عمومی ارائه و نحوه استفاده از کامپیوتر بدرستی تبین گردد . این نوع از آموزش ها را می توان از سطوح پائین آموزشی ، آغاز نمود. کاربران نوجوان و جوان اینترنت می بایست نسبت به رفتارهای درست و ناشایست در زمان استفاده از کامپیوتر خصوصا" در زمان استفاده از اینترنت بدرستی توجیه و آموزش های لازم به آنان ارائه گردد .(مشابه آموزش های ارائه شده به کودکان در زمان استفاده از کتابخانه ها ، چه نوع رفتاری قابل قبول است و چه نوع رفتاری پذیرفتنی نیست) معلمان مدارس و والدین نیز می بایست در این رابطه آموزش های لازم را فراگرفته تا از یکطرف قادر به رفتاری قابل قبول در زمان استفاده از کامپیوتر وشبکه های کامپیوتری

خصوصا" اینترنت بوده و از طرف دیگر و در جایگاه خود بتوانند نظارت لازم را انجام دهند .

خلاصه

وابستگی ما به سیستم های کامپیوتری بهم مرتبط خصوصا" اینترنت ، بسرعت در حال افزایش بوده و حتی بروز اختلال اندک توسط ویروس ها و کرم ها می تواند پیامدهای ناگواری را بدنبال داشته باشد . راه حل های واکنشی استفاده شده برای مقابله با کرم ها و ویروس ها به تنهائی کفایت نخواهد کرد. افزایش قدرت و سرعت حملات باعث شده است که زیرساخت های اطلاعاتی در معرض تهدید و خطر قرار داشته باشند. با دنبال نمودن راه حل های موجود می توان سطح مناسبی از حفاظت در مقابل تهدیدات را ایجاد نمود. بمنظور ارتقاء و بهبود وضعیت موجود ، مدیران سیستم ، ارائه دهندگان تکنولوژی و تصمیم گیرندگان می توانند با رعایت و پیگیری برخی اصول اولیه ، زمینه برخورد با کرم ها و یا ویروس ها را از ابعاد متفاوت فراهم نمایند. تغییر در طراحی نرم افزارها ، روش های پیاده سازی ، افزایش تعداد مدیران سیستم آموزش دیده ، بهبود سطح آگاهی کاربران ، افزایش تحقیقات در رابطه با سیستم های ایمن و پایدار، طراحی و پیاده سازی دوره های آموزشی خاص دررابطه با کامپیوتر و امنیت شبکه ، نمونه هائی در این زمینه بوده که می تواند دستاوردهای مثبتی را در ارتباط با امنیت اطلاعات برای

تمامی شهروندان اینترنت بدنبال داشته باشد.حرکات مثبت هر یک از شهروندان اینترنت (حقوقی و یا حقیقی) در خصوص پایبندی به اصول امنیتی ، تاثیری مثبت در ایمن سازی سرمایه های اطلاعاتی را بدنبال خواهد داشت .