شناسایی تهدیدات سایبری و عوامل کلیدی در مقابله با آن

مهندس مجتبی ذنوبی

مهندس کامپیوتر نرم ا فزار- کارشناسی ارشد مدیریت کارافرینی سازمانی

مدیر فناوری اطلاعات دانشگاه علوم پزشکی شهید بهشتی

تهران ، ایران

mojtaba_zonoobi@yahoo.com

چکیده:

در این مقاله سه مقوله اساسی درخصوص تهدیدات سایبری مورد بررسی قرار می‌گیرد.در ابتدا دو هدف کمی از تهدیدات سایبری نفوذ به سیستم‌ها جهت ایجاد اختلال و یا دسترسی به اطلاعات در یک سازمان شرح داده می‌شود.در مقوله دوم ، عوامل موثر بر تهدیدات سایبری مورد بحث و بررسی قرار می‌گیرد و در نهایت با توجه به شناخت اهداف و عوامل موثر بر تهدیدات سایبری به بیان عوامل کلیدی جهت پیشگیری و مقابله با تهدیدات سایبری پرداخته می‌شود.

کلمات کلیدی:

تهدیدات سایبری، پدافند غیرعامل، تجهیزات و امکانات پایدار، کاربران

۱- مقدمه

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار IT ، این بستر به یکی از نقاط بالقوه آسیب پذیر و خطرناک در جهان بدل شده است؛ که ضرورت توجه و پرداخت سریع و در عین حال نظام مند، معقول و هدفمند به منظور مصون سازی این بستر از تهدیدات موجود در جهت حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین المللی را می‌طلبد.

با توسعه سریع فناوری اطلاعات و شبکه، انواع بسیاری از تهدیدات از قبیل کرم‌ها، نفوذهای بدون مجوز از راه دور و سرویسهای انکار توزیع شده (DDoS)، هاست‌ها و شبکه را مورد هدف قرار دادند. به منظور تصمیم گیری درخصوص کنترل امنیت کل شبکه و سیستم‌ها باید هوشیاری و معرفت کافی در خصوص وضعیت امنیت وجود داشته باشد.

امروزه شاهد افزایش روز افزون کاربرد فضای مجازی و همچنین آمیختگی مسائل و جزئیات زندگی بشر مدرن با اماکن عمومی ظاهرا" مجازی هستیم. فضای مجازی برخلاف آنچه که نامش می‌نماید، نه تنها غیر واقعی نیست بلکه اساس و واقعیت این فضا متشکل و ریشه دار در واقعیت های غیر مجازی زیر است:

- اطلاعات طبقه بندی شده[1]
- تجهیزات و امکانات پایدار[2]
- مدیریت فضای مجازی خاص بوجود آمده
- کاربران

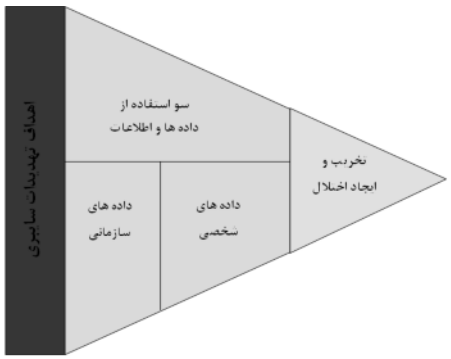
حال با این دیدگاه، بدیهی است زمانی که بحث بررسی امنیت فضای مجازی یا سایبر به میان می‌آید، می‌بایست موضوع امنیت را از ۴ زاویه فوق مورد تجزیه تحلیل و بررسی قرار داد.

۲- تهدیدات سایبری و ضرورت مقابله با آن

در اولین روزهای استفاده از رایانه‌ها در سیستم های به اشتراک گذاشته شده تنها از نـام کـاربری برای شناسایی افراد استفاده می‌شد و نیازی به وارد کردن رمز عبور نبود . بعد از آنکه کاربران بدخواه آغاز به سوء استفاده از این سیستم کردند رمزهای عبور نیز به آن سیستم‌ها اضافه شدند.

شکل شماره یک اهداف یک تهدید سایبری را نشان می‌دهد. امروزه راهبران بیش از هر زمان دیگر باید به امنیت شبکه و رایانه‌ها بیاندیشند .مهمترین دلایل این مسئله عبارتند از:

- ارزش سرمایه‌گذاری روی تجهیزات سخت افزاری و برنامه‌های نرم‌افزاری - نکتهٔ قابل توجه این است که رایانه‌ها و بسته های نرم‌افزاری بسیار گرانقیمت هستند و جایگزینی آنها پرهزینه و دشوار است . حتی اگر در یک رخداد امنیتی نرم‌افزارها و سخت افزارها کاملا از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همهٔ نرم‌افزارها کنند و متعاقبًا لازم شود کلیهٔ نیازهای اساسی مجددا تعریف گردند . این امرمستلزم صرف زمان بسیار زیادی است؛ خصوصا اگرفرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.
- ارزش داده های سازمانی - این داده‌ها ممکن است شامل لیست مشتری ها ، پروژه های مالی ، طرح های پژوهشی مهم و یا برنامه های تجاری باشند که توسط کاربر نوشته شده اند.
- ارزش داده های فردی - ممکن است داده های فردی ارزش مادی چندانی نداشته باشند ولی از دست دادن آنها بسیار زیان آور باشد و برای ایجاد دوبارهٔ اطلاعات زمان بسیار زیادی لازم باشد.
-



شکل ۱- اهداف تهدیدات سایبری

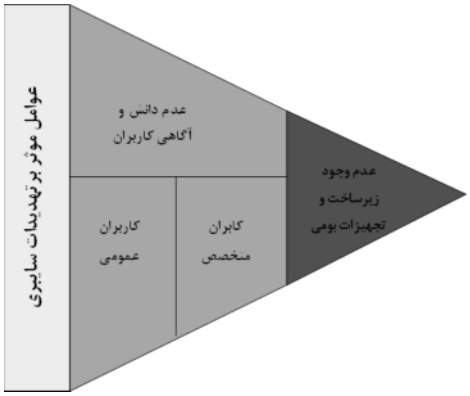
- تهدیدات جنایتکاران رایانه ای - همگام با پیشرفتهای فناوری، گروهی از خرابکاران که از دزدی داده های رایانه ای سود می‌برند نیز بوجود آمده اند . در مواردی اینکار صرفًا برای لذت و سرگرمی صورت می‌گیرد و برخی افراد نیز تنها بخاطر خودنمایی در برابر دوستان خود دست به چنین کارهایی می‌زنند؛ اما در بعضی موارد اینکار برای دستیابی به منافع شخصی و سازمانی انجام می‌گیرد (دزدی اطلاعات کارت اعتباری یا ورود به معاملات

[1] Assortment Information
[2] Stable Accouterment

فریبکارانه). در تمامی موارد مذکور این اشخاص باعث ایجاد خسارت و گسترش بی اعتمادی میشوند و در حد گس ترده تر مشکلات بحرانی بوجود می‌آورند که به اشخاص و موقعیتهای شغلی صدمه وارد می‌کند .باید گفت از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفته، تعقیب و متوقف کردن مهاجمین هرچند همچنان امکانپذیر می‌باشد ولی بسیار پیچیده شده است.

۳- عوامل موثر بر تهدیدات سایبری

همانطور که در شکل ۲ نشان داده شده است بیشترین عوامل تاثیر گذار در تهدیدات سایبری عدم دانش وآگاهی کاربران و فقدان تجهیزات وزیرساخت های بومی می‌باشد که این عوامل توضیح داده خواهند شد.



شکل۲- عوامل موثر بر تهدیدات سایبری

۳- ۱ عدم آگاهی ودانش کافی کاربران

مایکروسافت با انتشار "گزارش امنیت هوشمند ۲۰۱۱" چشم اندازی از وضعیت تهدیدات آنلاین و روند حفاظت از شبکه در نیمه نخست سال جاری را منتشر کرد و نشان داد که در بسیاری از موارد، ناآگاهی کاربران مسبب پذیرش حملات سایبری است.
آگاهی و آموزش کاربر در رابطه با حفظ و نگهداری اطلاعات موجود در ایستگاه کاری برای کاربران فضای مجازی اهمیت قابل ملاحظه ای دارد و این از اصول اولیه امنیت کاربران محسوب می‌شود.[3]

تهدیداتی از قبیل نشر ناخواسته اطلاعات شخصی و یا پاسخ به سوالات و هرزنامه‌ها و روش هایی که دزدان سایبری بصورت حرفه ای از خود کاربران اطلاعات آنها را به سرقت می‌برند، همه و همه از موارد عدم امنیت کاربر در فضای مجازی محسوب می‌شوند که با آگاهی و آموزش قابل پیشگیری و مقابله می‌باشند. [4]

کاربران شامل دو گروه می‌باشند کاربران عمومی وکاربران متخصص. عدم آگاهی و دانش در کاربران عمومی منجر به از دست دادن اطلاعات شخصی و خانوادگی می‌شود که گاها منجر به پرداخت هزینه های سنگینی می‌گردد. منظور از کاربران متخصص افرادی که مسئولیت نگهداری از شبکه و زیرساخت در سازمان‌ها را برعهده دارند می‌شود. همچنین افراد متخصصی که در زمینه تخصصی خود به ناچار می‌بایست از فناوری اطلاعات استفاده کنند، مثل پژوهشگران ، صنعتگران ، دانشجویان و.... جزء کاربران متخصص محسوب می‌شوند که بالتبع با توجه به حساسیت شغلی آنها عدم آگاهی ودانش در حوزه مسائل امنیت IT خسارات جبران ناپذیری را به سازمان وکشور وارد خواهد نمود. لذا با توجه به توضیحات ذکر شده ایجاد فرهنگ استفاده صحیح از تکنولوژی وآگاهی بخشی کاربران، بویژه فعالیت در دنیای مجازی ، گام نخست مبارزه با تهدیدات در حوزه سایبری می‌باشد.

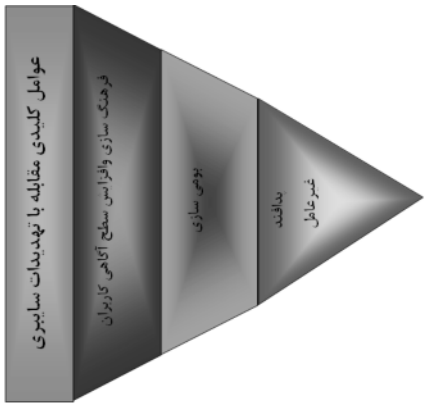
۳- ۲ عدم وجود زیرساخت وتجهیزات بومی

امنیت فناوری اطلاعات به عنوان یکی از شریان‌های اصلی در حوزه ICT مطرح بوده که با توجه به رشد فناوری و به ویژه فناوری اطلاعات در کشور نیاز به توسعه آن احساس شده و به نظر می‌رسد که در سال‌های آتی به عنوان اصلی‌ترین حوزه تخصصی ICT مطرح باشد.[5] رشد فناوری اطلاعات و ارتباطات بدون توجه به مقوله امنیت اطلاعات، امکان‌پذیر نبوده و عدم توجه به این مقوله ضررهای جبران ناپذیری بر پیکره فناوری اطلاعات کشور وارد می‌سازد که اخیراً شاهد بروز مشکلاتی در این حوزه می‌باشم. جایگاه امنیت فناوری اطلاعات و ارتباطات به طور مشخص در تمامی حوزه‌های مختلف ICT الزامی بوده که در تمامی سطوح از لایه فیزیکی تا لایه برنامه‌های کاربردی را تحت پوشش خود قرار می‌دهد. در این راستا استانداردها و رویه‌های

اجرایی مدونی در دنیا طرح شده که نیاز است در کشور بومی-سازی گردد. با رشد تصاعدی فراگیر شدن فناوری اطلاعات در سیستم های دولتی و خصوصی و افزایش روز افزون خدمات و سرویس های ارائه شده به اقشار مختلف جامعه در بستر فن آوری اطلاعات، این سوال را در ذهن ایجاد می‌کند که با این سرعت پیشرفت تکنولوژی و و وابستگی شدید مردم به فن آوری اطلاعات و قرارگرفتن خدمات IT در امور روزمره مردم در صورت ایجاد و قفه در خدمات رسانی چه معضلات و مشکلاتی گریبانگیر جامعه و سرویس دهندگان خواهد شد؟آیا کلیه موارد امنیتی در سرویس های مبتنی بر اینترنت از جمله بانکداری های الکترونیک، تجارت الکترونیک، خریدهای اینترنتی، بانک های اطلاعاتی سازمانهای دولتی و... رعایت گردیده و اگر رعایت شده با تکیه بر چه استانداردها و ابزارهایی؟ آنچه مسلم است در صورتیکه پیش بینی های آینده و گام های اساسی در این خصوص جهت دستیابی به تکنولوژی بومی برداشته نشود، و به زیرساختهای بومی و ابزارهای امنیتی بومی توجه جدی صورت نپذیرد، هر چه جلوتر می‌رویم وابستگی مردم به خدمات الکترونیک بیشتر و از طرفی وابستگی زیر ساخت های سرویس دهندگان به صاحبان اصلی تکنولوژی این صنعت در خارج از کشور نیز بیشتر خواهد شد.

۴- عوامل کلیدی مقابله با تهدیدات سایبری

دربخش قبل عوامل تاثیرگذار بر تهدیدات سایبری مشخص گردید، در شکل ۳ عوامل کلیدی مقابله با این عوامل به عنوان عوامل کلیدی مشخص گردیده است.



شکل۳- عوامل کلیدی مقابله با تهدیدات سایبری

۴-۱ فرهنگ سازی و افزایش سطح آگاهی کاربران

نخستین گام کلیدی در مقابله با تهدیدات سایبری افزایش سطح آگاهی کاربران می‌باشد.نقش آگاهی و آموزش بر امنیت اطلاعات طبقه بندی شده در فضای مجازی بسیار مهم می‌باشد. آگاهی و آموزش کاربر در رابطه با حفظ و نگهداری اطلاعات موجود در ایستگاه کاری برای کاربران فضای مجازی اهمیت قابل ملاحظه ای دارد و این از اصول اولیه امنیت کاربران محسوب می‌شود.

تهدیداتی از قبیل نشر ناخواسته اطلاعات شخصی و یا پاسخ به سوالات و هرزنامه‌ها و روش هایی که دزدان سایبری بصورت حرفه ای از خود کاربران اطلاعات آنها را به سرقت می‌برند، همه و همه از موارد عدم امنیت کاربر در فضای مجازی محسوب می‌شوند که با آگاهی و آموزش قابل پیشگیری و مقابله می‌باشند.[6]

این امکان وجود دارد که کاربر در فضای مجازی در مسیر جستجو و موج سواری تا رسیدن به اطلاعاتی خاص ، بصورت ناخواسته اطلاعات محرمانه و یا ارزنده ای را هرچند ناچیز در اختیار دیگران قرار دهد که در صورت آگاه نمودن کاربر از این نوع خطر و آموزش شیوه درست کار می‌توان این نوع ناامنی را از میان برد.[7]

این امکان وجود دارد که کاربر در حین افزودن اطلاعاتی به مجموعه اطلاعات طبقه بندی شده در فضای مجازی بصورت نا خواسته ، ویروس ، آلودگی و یا هر گونه برنامه مخرب دیگری را به پایگاه اطلاعاتی وارد کند و باعث بروز اشکالات جبران ناپذیری گردد. و این امر نیز با آگاه نمودن کاربر از خطر و همچنین با آموزش حفاظت و پاکسازی داده‌ها قبل از استفاده در فضای مجازی و یا تجهیزبه برنامه های فایر وال ، قابل پیگیری و قابل ایمن سازی می‌باشد.

بدون شک آگاهی و آموزش کارشناسان طی دوره های خاص طراحی و مهندسی شبکه های مجازی، شناخت لایه های شبکه و آشنایی با حفره های امنیتی هر لایه می‌تواند سبب راه اندازی تجهیزات پایدار (Stable Accoutement)، عدم ورود بار اضافی و ناخالص و قابل اعتماد بودن یک شبکه امن با سرعت و دقت مناسب شود.[8]

آگاهی و آموزش موجب رعایت شئونات در محورهای اخلاقی، حرفه ای، سیاسی، فرهنگی و ... می‌گردد. قصور در این حیطه

ناامنی های اخلاقی، حرفه ای، سیاسی، فرهنگی خاص خود را به دنبال خواهد داشت.

۴-۲ بومی سازی در حوزه فناوری اطلاعات

بدون شک با تکیه دادن به ابزارها وتجهیزاتی که ساخته کشورهای بیگانه می‌باشد، هیچ گاه نمی توان امنیت کامل را برقرار نمود. زیرا در لایه فیزیکی امنیت وابستگی وجود داشته ودر شرایط مختلف از جمله بروزرسانی امکان اختلال وسو استفاده وجود خواهد داشت. اگرچه دامنه تجهیزات وابزارها بسیار وسیع می‌باشد به برخی از مهمترین آنها اشاره خواهیم کرد.

۴-۲-۱.ضرورت وجود سیستم عامل ملی

اکثر سرویس های ارائه شده تحت وب و یا درون سازمانی توسط سرورهایی که سیستم عامل های ویندوز سرور مایکروسافت یا سیستم عامل های لینوکسی توسعه داده شده توسط کشورهای دیگر بر روی آن نصب گردیده است ارائه می‌شود. بروز رسانی ویندوزها جهت دریافت آخرین UPDATEها برای جلوگیری از بروز مشکل و بعضا از بین بردن حفره های امنیتی شناخته شده، امری اجتناب ناپذیر می‌باشد. اگرچه بروز رسانی ویندوزهای سرور به صورت رایگان و بدون مشکل صورت می‌پذیرد.(که همین خود جای اندیشه و سوال دارد) ولی چه تضمینی وجود دارد که BACKDOOR ها(درهای پشتی) به همراه Patchهای بروزرسانی مختص سیستم عامل های شناسایی شده در ایران، که اکثرا به علت نوع IP VALID که روی آن قرار داردقابل شناسایی می‌باشند، ارسال نگردد؟! و کلیه اطلاعات حیاتی سازمان‌ها به سهولت قابل دستیابی نباشد و یا در سرویس های ارائه شده وقفه ای ایجاد نکنند؟؟ اگرچه در این زمینه اقداماتی صورت گرفته ولیکن به سرانجام نرسیده و می‌بایست لایحه ای در مجلس جهت مجبور نمودن سازمان های دولتی به استفاده از سیستم عامل ملی به تصویب برسد.

۴-۲-۲.وجود آنتی ویروس بومی قابل رقابت

در حال حاضر علی رغم وجود برخی آنتی ویروس های بومی ولیکن به علت قابل رقابت نبودن با نوع های خارجی از نظر فنی و ضریب اطمینان اکثر سازمان های دولتی و خصوصی از آن استفاده نمی‌کنند لذا تولید آنتی ویروس بومی و حمایت دولت از شرکت های فعال در این زمینه ضروری می‌باشد. در حال حاضر امنیت اکثر سیستم های عامل سازمان‌ها از نظر جلوگیری از ویروسی شدن و حمله های اینترنتی توسط آنتی ویروس های خارجی تامین می‌گردد. که در صورت عدم رعایت تعهدات این شرکت‌ها عملا دچار مشکلات جدی خواهیم شد و می‌بایست برای رهایی از این وابستگی تلاش های جدی صورت پذیرد.

۴-۲-۳.وجود فایروال بومی قابل رقابت

امنیت شبکه های داخلی سازمان های بزرگ در دنیای مجازی توسط فایروال‌ها تامین می‌شود اکثر سازمان های دولتی به علت بالا بودن قدرت و کیفیت فایروال های معروف خارجی از آنها در سازمان های خود استفاده می‌کنند که چندین فایروال موجود ساخت داخل بهعلت ضعیف بودن از نظر پشتیبانی و فنی در مقابل نوع خارجی استفاده نمی‌گردد که باید با حمایت دولت این بخش نیز تقویت شود والا در آینده نزدیک تهدیدات جدی در این زمینه به وجود خواهد آمد. اگرچه شرکت های خارجی به علت نیاز به بازار ایران از عرضه محصولات و خدمات خود دریغ نمی کنند و به فکر منافع مادی خود می‌باشد ولیکن باید این موضوع را زنگ خطری درنظر داشت که تکنولوژی در دست آنها بوده و احتمال استفاده سیاسی، و منفی همیشه بعنوان خطری بزرگ صنعت IT کشور را تهدید می‌نماید.

۴-۳ پدافند غیرعامل در حوزه سایبری

ازآنجا که هیچ گاه نمی توان امنیت را صددرصد برقرار نمود، لذا حتی با رعایت نمودن کلیه موارد ذکرشده ، امکان بروزحوادث غیرمترقبه و تهدیدات پیش بینی نشده وجوددارد. لذا دراین جا اهمیت پدافند غیرعامل محرز می‌باشد. دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کمترین هزینه فراهم می‌سازد[۱]. همواره اشکال متفاوتی در برخورد با

فعالیت های مجرمانه در یک فضای سایبر وجود دارد. در اینجا لازم است که دو مرحله از مراحل دفاع بررسی شود.

۱. جلوگیری[1]

عبارت است از شناسایی راه‌های نفوذ وحمله و مقابله با آنها جهت افزایش ضریب امنیت، ایمنی و پایداری .[۱]

از جمله روشهای جلوگیری می‌توان به موارد ذیل اشاره نمود:

- طراحی امن و ایمن و پایدار سیستم ها[2]

در صورتیکه امنیت جزو معیارها و اصول طراحی سیستم‌ها، قرار بگیرد، سیستم‌ها بسیار امن تر و ایمن تر و پایدارتر از قبل خواهند بود.

- متوقف نمودن حملات[3]

از دیگر راه های جلوگیری از حملات، متوقف نمودن آنها می‌باشد این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم، میسر است.

۲. مدیریت حادثه[4]، محدود کردن خرابی ها[5]

روش های مدیریت حوادث و محدود نمودن اثرات زیانبار حوادث، راه هایی هستند که با استفاده از آنها می‌توانیم اثر حملات صورت گرفته را در کمترین زمان کاهش دهیم.

- تعیین آثار، نشانه‌ها و هشدارها

بدین معنی که وقتی حمله ای اتفاق می‌افتد، ابتدا در گام اول باید آثار و خطراتی که این حمله می‌تواند داشته باشد را شناسایی کنیم، زیرا با شناسایی آثار یک حمله می‌توانیم از پیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شوند، جلوگیری کنیم.

- امن، ایمن و پایدار کردن سیستم ها[6]

جهت جلوگیری از نفوذهای بیرونی، ضروری است تا موانعی ایجاد کنیم. از قدیمی ترین موانع نفوذ ، استفاده از کلمه عبور است که البته روش های جدیدتر، استفاده از تکنیک هایی مانند دیوار آتش و یا پروکسی سرور ها[7] است. البته همان طور که شیوه های رمزنگاری شکست خوردند، شیوه های جدید نیز می‌تواند منجر به شکست شوند. در مورد حملات فیزیکی نیز لازم است که ابتدا تمام حملات و نفوذهایی که می‌تواند انجام شود را، شناسایی کنیم. مثلاً در مورد یک شبکه اطلاعاتی، باید استراتژی های فیزیکی مناسب جهت امن، ایمن و پایدار نمودن مراکز داده آن اتخاذ نمود.

- خاموشی و تخصیص مجدد[8]

یک راه حل دیگر این است که سیستم به طور کامل یا به طور جزئی خاموش شود و دوباره تخصیص مجدد شود. سیستمی که متوجه شود تحت یک حمله قرار دارد، باید موانع و دفاع هایی از خود را بنا نهد که شاید در مواقع عادی از آنها استفاده نمی‌کند و سعی کند قسمتهایی از سیستم را که مواجه با حمله شده‌اند، ایزوله کند. البته مراحل خاموش کردن و تخصیص دهی مجدد باید به صورت بلادرنگ[9] و به سرعت انجام گیرد.

- پشتیبانی[10]

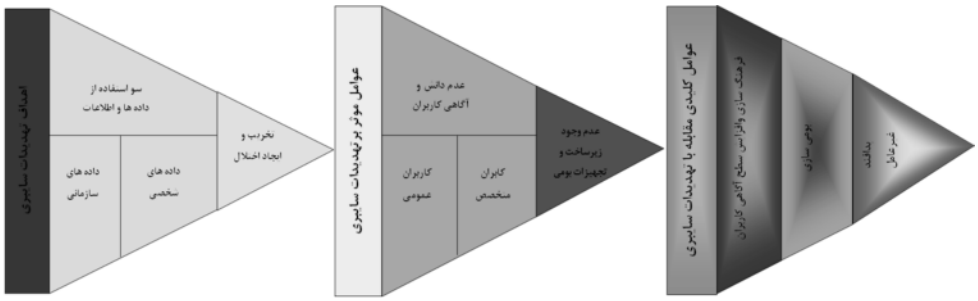
نکتهٔ قابل توجه این است که باید همواره از اطلاعات جمع‌آوری شده، قبل از هر حمله‌ای پشتیبانی کنیم. این تاکتیک از طریق تهیه نسخه پشتیبان اطلاعاتی که ذخیره شده‌اند، به دست می‌آید. بسیاری از روش‌های دفاع، نیاز به این دارند که حالت صحیح سیستم قبل از حمله را، جهت تسهیل در بازیابی و تجدید مجدد بدانند. این روش برای مواقعی است که حملات براساس نقطهٔ شروع دقیق و مشخصی انجام می‌شود و پشتیبان‌ها به طور منظم گرفته می‌شوند. بسیاری از حملات موذیانه به کندی و بطور محرمانه، مشکلات زیادی را نسبت به زمانی که اطلاعات سالم بودند، ایجاد می‌کنند (یعنی در اینگونه از حملات ما زمان دقیق سالم بودن اطلاعات را نداریم و تاثیر حملات هنوز ایجاد نشده است). در این حالت، جهت ایجاد فضای سالم، سیستم های سازمان باید خودشان برنامه هایی برای تهیه نسخه پشتیبان داشته باشند.

۵- نتیجه گیری

آنچه در این مقاله بیان شد به طور خلاصه در شکل شماره ۴ نشان داده شده است. اهداف حملات سایبری، عوامل تاثیرگذار برحملات سایبری و عوامل کلیدی مقابله با حملات سایبری.

[1] Prevention
[2] Embed Security into design
[3] Ban attacks
[4] Incident management
[5] damage limitation
[6] harden the system
[7] proxy servers

[8] Shutdown and reallocation
[9] real time
[10] Backup



شکل ۴- اهداف حملات سایبری، عوامل تاثیرگذار برحملات سایبری و عوامل کلیدی مقابله با حملات سایبری

متأسفانه پس از ۱۰ سال تجربه در حوزه فناوری اطلاعات، به نظر می‌رسد که مقوله امنیت فناوری اطلاعات در سازمان‌ها، ارگان‌ها و نهادهای مختلف فراموش یا در اولویت پایینی قرار گرفته است. دلیل اصلی این امر از یک سو عدم اطلاع مدیران دستگاه‌های اجرایی از نحوه اجرای پروژه‌های فوق و از سوی دیگر برخورد سنتی امنیتی با این مقوله است.

باید توجه داشت که امنیت اطلاعات وابستگی ماهوی و اساسی به شناخت پایه و مهار بنیادین فناوری اطلاعات دارد و باید فعالان در این زمینه از نخبگان فناوری و باهوش‌ترین افراد باشند که متأسفانه این واقعیت در کشور درک نشده است. شناخت فرهنگ، پیچیدگی و ویژگی‌های فضای مجازی و مبانی حاکم بر آن، از دیگر الزامات مغفول این زمینه است. مضافاً اینکه در این حوزه عدم وجود متولی مشخصی برای ساختار دادن و همچنین پیگیری پیاده‌سازی استانداردهای امنیتی بوده که .این امر باعث شده است که بسیاری از پروژه‌ها و طرح‌های امنیتی توسط شرکت‌هایی که تجربه پیاده‌سازی امنیت اطلاعات را ندارند، صورت پذیرد که این دلایل باعث شکست پروژه و طرح‌های امنیت اطلاعات شده است. البته نتایج این عدم کارایی در هنگام عمل و بروز حمله مشخص می‌شود که در چنین زمانی معمولاً سازمان‌ها سعی در پوشش این گونه اتفاق‌ها دارند و به راحتی نمی‌توان تاثیرات سوء این کاستی جدی را در جامعه مشاهده کرد.[۲]

لازم است مدیران به این نکته توجه کنند که امنیت اطلاعات دارای بعدهای بسیاری است که لایه برنامه کاربردی تا امنیت فیزیکی را در برمی‌گیرد و وجود رویه و یا سیاست‌های امنیتی در سازمان‌ها ضروری‌تر از خرید فایروال می‌باشد. در دنیا و به تبع آن کشور خودمان، دوره‌های امنیتی بسیاری تدوین شده که لازم است مدیران ارشد سازمان‌ها، مدیران شبکه، برنامه‌نویسان و کاربران در دوره‌ها و آموزش‌های تخصصی شرکت نموده و آگاهی لازم را در خصوص امنیت فناوری اطلاعات داشته باشند. در همین راستا، دولت نسبت به الزامی شدن دوره ICDL اقدام نموده که به نظر می‌رسد که مهارت‌های هفتگانه اشاره شده در ICDL مقوله امنیت اطلاعات را در برنگرفته و نیاز است تدبیری اندیشیده شود. درخصوص ارائه مهارت هشتم در خصوص امنیت فناوری اطلاعات برای کاربران می‌بایست اقدام شود.

منابع:

[۱]اندیشگاه شریف واندیشکده کاوشگران آینده ،جنگ و دفاع سایبر،دی ماه ۱۳۸۴

[۲]ماهنامه دنیای کامپیوتر و ارتباطات مهرماه ۱۳۸۹

[3]Other countries developing cyber attack capability, CIA says, Feb, 2000, http://www.networkworld.com/news/2000/0224cia .html.

[4]Howard F. Lipson, Ph.D.CERT® Coordination Center., Tracking and Tracing Cyber-Attacks:Technical Challenges and Global Policy Issues, November 2002

[5]http://www.computer.org/portal/web/csdl/doi/10.1109/CIS.2007.130

[6]M.Kuhl, J.Kistner, K.Costantini, and M.Sudit, "Cyber attack modeling and simulation for network security analysis," Proc. of the 39th Winter Conference on Parallel and Distributed Simulation, vol.78, Atlanta, USA, 16-December, pp. 1180-1188, 2007.

[7]E.J.Canavan, Fundamentals of network security, Library of Congress Cataloging-in-Publication Data, 2000, ISBN= 1-58053-176-8.

[8]Cyber Threats to National SecurityCountering Challenges to the Global Supply Chainو July 2010

[9] CACI International Inc ,Cyber Threats to National Security, September 2011

[10]Conway, Maura (2005). Terrorist Use of the Internet and Fighting Back. Available WWW: http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/maura_conway.pdf

[11] Wilson, Clay (2005). Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Available WWW: http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf

[12] Snyder, William (2010). Thresholds for Cyberwar. Available WWW: http://blog.cybersecuritylaw.us/2010/10/thresholds-for-cyberwar-center-for-strategic-and-international-studies.htm

[13] Palmer, Shelly (2010). Cyberterrorism vs. Cyberwarfare: Defending the United Networks of America. Available WWW: http://www.shellypalmermedia.com/2010/02/07/cyber-terrorism-vs-cyber-warfare-defending-the-united-networks-of-america/

[14] Clarke, Richard and Robert K. Knake (2010). The Growing 'Cyberwar' Threat. Available WWW: http://www.npr.org/templates/story/story.php?storyId=126097038