بسم الله الرحمن الرحیم

"و علمناه صنعه لبوس لکم لتحصنکم من باسکم فهل انتم شاکرون" (سوره مبارکه انبیا آیه ۷۹)

"و ما به او (حضرت داود علیه السلام) ساخت زره را تعلیم دادیم تا شما را از آسیب جنگ در امان بدارد، پس آیا از شکر گزارانید؟"

رهنمود امام(ره) :

من مجددا به همه ملت بزرگوار ایران و مسئولین عرض می کنم چه در جنگ و چه درصلح بزرگترین ساده اندیشی این است که تصور کنیم جهانخواران خصوصا آمریکا و شوروی، از ما و اسلام عزیز دست برداشته اند. لحظه ای نباید از دشمن غافل بمانید.

فرمایش مقام معظم رهبری:

کمیته دائمی پدافند غیرعامل به منظور هماهنگ سازی، سیاست گذاری،کنترل ، نظارت و تصویب طرح های پدافند غیرعامل پروژه های عمرانی کشور در ستاد کل نیروهای مسلح تشکیل گردد.

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 می طلبد.

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. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند.

فصل ۱ - تعاریف و مفاهیم

پدافند غیرعامل[1]: پدافند غیرعامل شامل کلیه اقدامات به منظور حفظ امنیت، ایمنی و پایداری شبکه و تجهیزات وابسته به شبکه می باشد.

جنگ سایبر[2]: استفاده از کامپیوترها به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت ترساندن و یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی و یا آرمانی انجام می گیرد و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل‌ونقل، ارتباطات، سرویس‌های ضروری (مانند پلیس و خدمات پزشکی) را هدف قرار می‌دهد و از شبکه‌های کامپیوتری به عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می کند.

جرائم سایبر[3]: هرگونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و کنترل داده ها و نرم افزارهای رایانه ای و ایجاد یا وارد کردن انواع ویروسهای رایانه ای و امثال آن جرم محسوب می شود.

[1] Passive Defense
[2] Cyber warfare
[3] Cyber crime

فصل ۲ - مراکز تحت پوشش :

مراکز حیاتی[1]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری در سراسر کشور گردد.

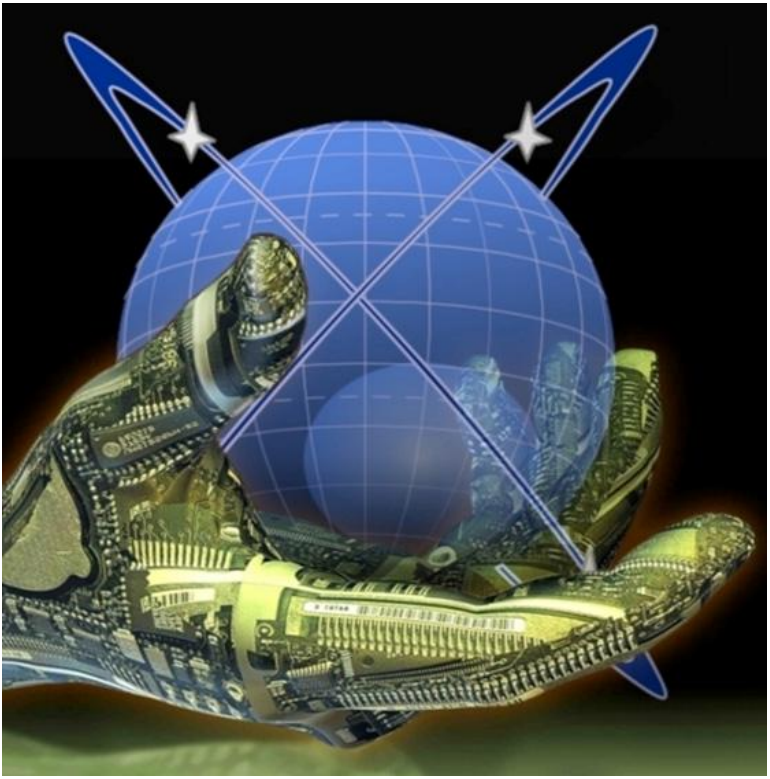
مراکز حساس[2]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل‌توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیر گذاری منطقه‌ای در بخشی از کشور گردد.

[1] Vital Centers
[2] Critical Centers

مراکز مهم[1]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی، دفاعی با سطح تأثیر گذاری محلی در کشور وارد می‌گردد.



[1] Important Centers

فصل ۳ – سازمان پدافند غیرعامل در حوزه IT

اهداف کلان

۱. تأمین امنیت و حصول اطمینان از عدم دسترسی های غیر مجاز به اسرار و اطلاعات کشور (ملی و بخشی)
۲. ایمن سازی و حصول اطمینان از پایداری و خلل ناپذیری در فعالیت شبکه های الکترونیکی مدیریت و کنترل کشور(ملی و بخشی)
۳. حفظ و تأمین آرامش اجتماعی و عمومی از طریق توسعه اطمینان و اعتماد آحاد جامعه
۴. نسبت به صحت و تداوم کارکرد شبکه و سامانه های الکترونیکی سرویس و خدمات عمومی
۵. توسعه ظرفیت دفاع الکترونیکی در برابر تهاجم فرهنگی و نرم از طریق شبکه های بین المللی و ملی اینترنت
۶. تقویت ضریب امنیت و پایداری در حوزه زیر ساختهای ملی و حیاتی

رسالت

تأمین و توسعه امنیت، ایمنی و پایداری در فضای تبادل اطلاعات کشور.

ماموریت

سیاست گذاری، هدایت، نظارت راهبردی و توسعه امنیت، ایمنی و پایداری فضای تبادل اطلاعات کشور و پشتیبانی از برنامه دستگاه ها و بخش های زیرساختی در جهت کاهش آسیب دربرابر تهدیدات و جنگ از طریق ساماندهی و بکارگیری منابع و ظرفیت های ملی.

راهبردهای اصلی

۱. نهادینه سازی فرامین و قانونمندسازی تدابیر مقام معظم رهبری در خصوص پدافند غیرعامل در سازمان ها و دستگاه های ذیربط

۲. ساماندهی، انسجام بخشی وهدایت راهبردی مجموعه های علمی، پژوهشی، آموزشی و صنعتی مرتبط با حوزه تخصصی فاوا در راستای تولید و توسعه دانش و فن‌آوری های بومی و ملی مورد نیاز پدافند غیرعامل

۳. توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فن‌آوری‌های بومی

۴. نهادینه کردن اصول و ملاحظات پدافند غیرعامل در طرح‌های توسعه شبکه های ارتباطی و الکترونیکی

۵. توسعه فرهنگ پدافند غیرعامل و ارتقاء دانش و شناخت مسئولین و کارشناسان حوزه ارتباطات و الکترونیک از پدافند غیرعامل

۶. خوداتکایی از دستگاه های پشتیبان آسیب پذیر و خودکفایی از منابع خارجی فن‌آوری ها

۷. حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مولفه های امنیت، ایمنی، پایداری و متکی بر فن آوری های بومی

۸. توسعه و تقویت سیستم پست کشور (بهره‌مندی از پست بسیار سریع و امین)

۹. بهره‌مندی از شبکه ارتباطی ویژه مدیریت کشور در شرایط بحران جنگ (با مولفه های امنیتی و پایداری و ایمنی بسیار بالا و دسترسی سریع)

۱۰. توسعه توان کنترل و مدیریت بحران و برنامه های حراست، حفاظت و ضد جاسوسی

۱۱. نهادینه کردن ملاحظات دفاع غیرعامل و امنیت ملی در تعاملات و همکاری با کشورها و شرکت های خارجی در حوزه ICT

فصل ۴ – نقش پدافندغیرعامل در تامین امنیت فضای تبادل اطلاعات

به هرگونه اقدام با هدف ایجاد اختلال، ناکارآمدی یا محروم سازی از منابع موجود در فضای تبادل اطلاعات، جنگ سایبر اطلاق می گردد.

چنین عملیاتی بطور مشخص با اهداف تهدید امنیت و یا حفظ امنیت در ابعاد ملی انجام می‌پذیرد. جنگ سایبر دارای اهمیت روزافزون برای بخشهای دفاعی و امنیتی، اقتصادی و تجاری، سیاسی، فرهنگی و ... است.

لازمه یک دفاع موفق در جنگ سایبر همانا بالا بردن سطح امنیتی عناصر درگیر است و این مهم جز با افزایش دانش در حوزه سایبر میسر نخواهد بود.

بر اساس استانداردهای امنیتی قابل قبول، بطور خلاصه هر یک از عناصر درگیر در فضای سایبر، باید به اندازه ارزش خود حفاظت گردند. در غیر این صورت، انتخاب مکانیسم‌های دفاعی چندان بهینه نخواهد بود و بدون شک دارای هزینه‌های غیر ضرور است.

بدیهی است آنهایی که قصد حمله داشته باشند تا دندان مسلح می شوند. پس باید ابتدا دارائی‌ها و عناصراصلی و اساسی اطلاعاتی اشیاء مهم در فضای سایبری را تعریف و تعیین نموده و براساس سیاست‌های کلان و با در نظر گرفتن تمامی تهدیدات، باید همه تمهیدات دفاعی را پی‌ریزی نمائیم.

فصل ۵ - انواع حملات

حملات خاموش[1]

این حملات شامل فعالیت هایی می شوند که در آنها بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سیستم های آسیب پذیر، به آنها نفوذ شده و منجر به سوء استفاده از منابع سیستم می گردد.

حملات فعال[2]

این حملات، حملاتی هستند که به سیستم های کامپیوتری زیرساختهای حیاتی نفوذ می‌کنند و می‌توانند اطلاعات حساس را دستکاری کنند و باعث بروز حوادث و فجایع ملی و جبران ناپذیر می گردند. از اهداف آنها می‌توان، از کار انداختن شبکه های خدماتی عمومی مثل شبکه برق، گاز و ... و همچنین ایجاد وحشت و ترس در جامعه و کاهش میزان اعتماد به دولت و نظام را برشمرد.

فصل ۶ - آناتومی و مراحل یک حمله

۱- ابتدا یک هدف مشخص تعیین می‌شود که می‌تواند قسمتی از یک زیرساخت حیاتی مانند شبکه راه‌آهن، شبکه برق، شبکهٔ ATM و یا وب سایت های دولتی باشد.

1 The Silent Killers

2 Active

۲- مهاجم‌ها شروع به جمع‌آوری اطلاعات می‌کنند.

- از طریق شبکه اینترنت/ مقالات/ مطالعات و ...
- از طریق وب سایت های هدف.
- انجام آزمایش‌های تست نفوذ[1] بر روی وب.
- شناسایی مؤلفه های تکنیکی هدف مانند سیستم عامل و ...
- جمع‌آوری اطلاعات از طریق مهندسی اجتماعی (توسط کارکنانی که در آن ساختار کار می‌کنند)

۳- حملهٔ سایبر اتفاق می‌افتد.

- بعد از اینکه دسترسی حاصل شد، ممکن است که حمله تا مدتی نگهداشته شود.
- ممکن است که حمله موفقیت آمیز بوده و یا شکست بخورد.
- اگر حمله موفقیت آمیز باشد، هکر آن را از طریق مالتی مدیا منتشر و یا ردپا و اثر خود را مخفی می‌کند.

۴- تحقیق و بررسی جهت حملات دیگر انجام می‌گیرد.

فصل ۷ - مراحل دفاع

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.

[1] Pen- testing

۱. جلوگیری[1]

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

از جمله روشهای جلوگیری می توان 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 می باشد این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم، میسر است.

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

[1] Prevention
[2] Embed Security into design
[3] Ban attacks
[4] Incident management
[5] damage limitation

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[1]

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[2] 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

[1] harden the system
[2] proxy servers

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[1]

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[2] و به سرعت انجام گیرد.

- پشتیبانی[3]

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

[1] Shutdown and reallocation
[2] real time
[3] Backup

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.

فصل ۸ - جمع بندی:

۱. تهدید و جنگ سایبری را باید به اندازه جنگ فیزیکی مهم پنداشت.
۲. فضای سایبری را می بایست جامع و شامل کلیه عناصر فیزیکی و غیر فیزیکی، نیروی انسانی و ... تصور نمود.
۳. علی‌رغم خالص دانستن فضای سایبری، بر نقش فاکتور انسانی تاکید ویژه شود.
۴. مسلماً کشورهائی آسیب‌پذیرتر هستند که به شبکه های فناوری اطلاعات نا امن اتکای بیشتری دارند.

۵. با توجه به گسترش روز افزون کاربری و کاربران فضای سایبری در ایران، نیاز به افزایش توانمندی‌های امنیتی بومی کشورمان بسیار محسوس است.
۶. می بایست به شاخصه امنیت(امنیت، ایمنی و پایداری) همپای شاخصه توسعه توجه شود.
۷. با توجه به عقب ماندن شاخصه امنیت نسبت به توسعه در کشور می بایست در حداقل زمان ممکن اقدامات مقتضی صورت پذیرد.