به نام خدا

"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؟"

سوره مبارکه انبیا آیه ۷۹

فهرست :

مقدمه

با توجه به اهمیت فناوری اطلاعات و ارتباطات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار IT[۱]، 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

[۱] Information Technology

چنین طرح‌هایی فراهم می‌گردد ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند.

فصل ۱ - تعاریف و مفاهیم

- **پدافند غیرعامل[1]؛** شامل کلیه اقدامات به منظور حفظ امنیت، ایمنی و پایداری شبکه و تجهیزات وابسته به شبکه می باشد.
- **جنگ سایبر[2]؛** به معنی استفاده از رایانه ها به عنوان اسلحه یا ابزاری برای انجام کارهای خشونت بار جهت ترساندن و یا تغییر عقیده یک گروه یا کشور می باشد. جنگ سایبر به قصد کارهای سیاسی و یا آرمانی انجام می‌گیرد و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل‌ونقل، ارتباطات و سرویس‌های ضروری (مانند پلیس و خدمات پزشکی) را هدف قرار می‌دهد و از شبکه‌های کامپیوتری به عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند.

❖ **جرائم سایبر**[۱]؛ شامل 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 ویروس های رایانه ای و امثال آن می باشد.

[۱] Cyber crime

فصل ۲ - زیرساخت های تحت پوشش

زیرساخت‌ها برمبنای نقش و میزان تأثیر کارکردشان در ضرایب امنیت، ایمنی و پایداری هرکشور، به سه دسته اساسی ذیل تقسیم بندی می گردند:

- **زیرساخت های حیاتی**[۱]:

زیرساخت هایی هستند که 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.

- **زیرساخت های حساس**[۲]:

زیرساخت هایی هستند که انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل‌توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی،

---

[۱] Vital Centers

[۲] Critical Centers

پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیر گذاری منطقه‌ای در بخشی از کشور گردد.

❖ **زیرساخت های مهم[۱]:**

زیرساخت هایی هستند که انهدام کل یا قسمتی از آنها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی، دفاعی با سطح تأثیر گذاری محلی در کشور وارد می گردد.

[۱] Important Centers

فصل ۳ - سازمان پدافندغیرعامل در حوزه فناوری اطلاعات

در این فصل اشاره ای به اهداف کلان، رسالت، مأموریت و راهبردهای اساسی سازمان پدافند غیرعامل کشور درحوزه فناوری اطلاعات خواهیم داشت.

❖ **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 مدیریت و کنترل کشور(ملی و بخشی)
۳. حفظ امنیت و تأمین آرامش اجتماعی و عمومی از طریق توسعه اطمینان و اعتماد آحاد جامعه نسبت به صحت و تداوم کارکرد شبکه و سامانه های الکترونیکی سرویس و خدمات عمومی
۴. توسعه ظرفیت دفاع الکترونیکی در برابر تهاجم فرهنگی و نرم از طریق شبکه های بین المللی و ملی اینترنت
۵. 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.

❖ **مأموریت:**

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 فناوری های بومی و ملی مورد نیاز پدافند غیرعامل

۳. توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فناوری‌های 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 فناوری ها

۷. حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مؤلفه های امنیت، ایمنی، پایداری و متکی بر فناوری های بومی

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

۹. بهره‌مندی از شبکه ارتباطی ویژه مدیریت کشور در شرایط بحران جنگ (با مؤلفه 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

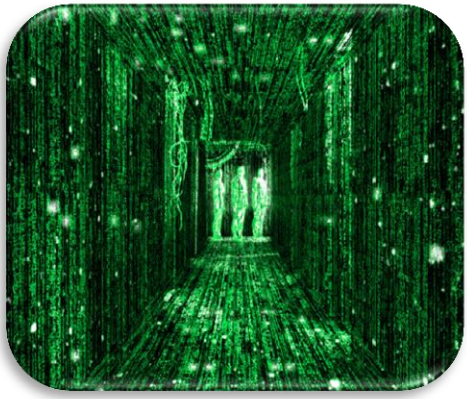
۱۱. نهادینه کردن ملاحظات دفاع غیرعامل و امنیت ملی در تعاملات و همکاری با کشورها و شرکت های خارجی در حوزه فناوری اطلاعات و ارتباطات

فصل ٤ – نقش پدافندغیرعامل در تأمین امنیت فضای تبادل اطلاعات

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، 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، تمهیدات دفاعی را پی‌ریزی نمائیم.



فصل ۵ - بررسی حملات سایبر

حملات سایبری بطور کلی به دو دسته ذیل تقسیم می شوند:

- **حملات خاموش[۱]:**

در این حملات بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سامانه های آسیب پذیر، به آنها نفوذ می شود. حملات خاموش نهایتاً منجر به سوء استفاده از منابع سامانه هدف می گردد.

- **حملات فعال[۲]:**

در این نوع حملات به سامانه های رایانه ای زیرساخت ها نفوذ می‌شود و کنترل این سامانه ها در اختیار مهاجم قرار می گیرد. حملات فعال ممکن است نهایتاً باعث دستکاری در اطلاعات حساس و یا بروز حوادث و فجایع ملی و جبران ناپذیر گردد. از اهداف متصور برای این حملات می‌توان «از کار انداختن شبکه های خدماتی عمومی مثل

۱ The Silent Killers

۲ Active

شبکه برق، گاز و ...»، همچنین «ایجاد وحشت و ترس در جامعه» و «کاهش میزان اعتماد به دولت و نظام» را برشمرد.

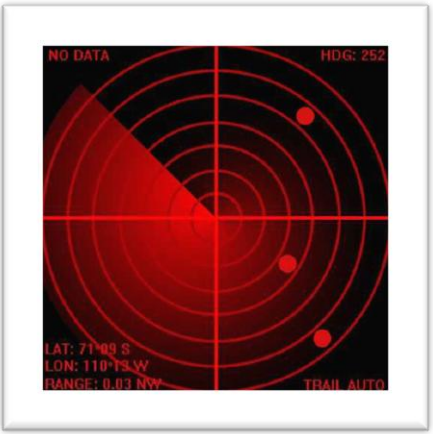
مراحل انجام یک حمله از سوی مهاجمین یا سناریوی یک حمله سایبر بصورت ذیل می باشد:

۱- ابتدا یک هدف تعیین می‌شود؛ این هدف می‌تواند قسمتی از یک زیرساخت حیاتی یا وب سایت های دولتی باشد.

۲- مهاجم‌ها شروع به جمع‌آوری اطلاعات می‌کنند.

- از طریق شبکه اینترنت/ مقالات/ مطالعات و ...
- از طریق وب سایت های هدف.
- انجام آزمایش‌های تست نفوذ[۱] 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)

[۱] Pen- testing



۳- حمله سایبر اتفاق می‌افتد.

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

۴- بر مبنای نتایج، تحقیق و بررسی جهت انجام حملات دیگر صورت می گیرد.

❖ چند نمونه سناریوی حملات سایبری

- **اختلال در شبکه حمل و نقل و ترافیک کشور :**

امروزه در صورت بروز جنگ سایبر خسارات ناشی از آن تمام ابعاد زندگی را فرا خواهدگرفت. می دانیم که شبکه های ارتباطی و حمل و نقل مترو توسط سامانه های مکانیزه کنترل می شود، فرض کنیم مهاجمی به سامانه مدیریتی چنین شبکه هایی حمله کرده، با بدست آوردن کنترل آن و دادن برنامه ای اشتباه به سامانه هادی مترو، باعث برخورد قطارها شود، چنین حادثه ای باعث مجروح و کشته شدن عده زیادی از مردم خواهد شد.

بطور مشابه فرض کنید به سامانه هدایت شبکه کنترل ترافیک در سطح شهر تهران توسط مهاجمی نفوذ و اطلاعات غلط در رابطه با ترافیک بخش های مختلف مخابره شود. بعنوان مثال در جایی از شهر که ترافیک عادی است اعلام شود تصادفی رخ داده و راه بسته شده است؛ و رانندگان را به بخش دیگری از شهر که تصادفی واقعی صورت گرفته هدایت کند، در نتیجه تعداد زیادی از ماشین ها به یک منطقه پر ترافیک وارد می شوند که باعث تصادفات، راه بندان شدید و هرج و مرج خواهد شد.

- **اختلال در شبکه برق کشور:**

تصور کنید سامانه توزیع برق منطقه ای یا شهری که به کمک شبکه های رایانه ای کنترل می شود مورد تهاجم نفوذگران قرار گیرد و بطور کلی قطع گردد یا کنترل آن بدست مهاجمان بیافتد؛ در این صورت فعالیت تمام سامانه هایی که وابسته به شبکه برق می باشد، مختل خواهد شد. بعنوان مثال این اتفاق باعث از کارافتادن سامانه های بانکی، راه و ارتباطات، کنترل ترافیک، برق منازل، آبرسانی، خدمات درمانی و... می شود که این عوامل جدا از احتمال خسارات جانی و مالی سبب نارضایتی و ترس و وحشت در مردم خواهد شد.

- **اختلال در شبکه مالی و بانکی کشور:**

با توجه به این نکته که کنترل و دسترسی به سامانه های خودپرداز (ATM) یا POS توسط سامانه مرکزی رایانه ای کنترل و هدایت می شود؛ اگر هکری به این سیستم نفوذ کرده و کنترل آن را به دست گیرد، می تواند پول های حساب های مختلف را جابجا کند یا باعث تغییر کلمه عبور کلیه کاربران شود. این عمل باعث می شود که کاربران نتوانند از حساب بانکی خود پول برداشت کنند و این منجر به ترس مردم و بی اعتمادی و هجوم آنها به بانک ها و اختلال در اقتصاد کشور می شود.

عدم کنترل سریع چنین وضعی و ادامه یافتن آن می تواند منجر به از بین رفتن اعتبار پولی و ارزی یک کشور در سطح جهانی شود.

فصل ٦ - مراحل دفاع

همواره اشکال متفاوتی در برخورد با فعالیت های مخاصمه جویانه در فضای سایبر وجود دارد. در اینجا لازم است که دو مرحله از مراحل دفاع بررسی شود.

۱. جلوگیری[۱]:

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

از جمله روش های جلوگیری می توان به موارد ذیل اشاره نمود:

- طراحی امن و ایمن و پایدار سامانه ها[۲]:

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

- متوقف نمودن حملات[۱]:

---

[۱] Prevention

[۲] Embed Security into design

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[۲]، محدود کردن خرابی ها[۳]:

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:

وقتی حمله ای اتفاق می‌افتد، در گام اول باید آثار و خطراتی که این حمله می‌تواند بدنبال 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 سامانه ها[۴]:

---

[۱] Ban attacks

[۲] Incident management

[۳] damage limitation

[۴] harden the system

جهت جلوگیری از نفوذهای بیرونی، ضروری است تا موانعی ایجاد کنیم. از قدیمی ترین موانع نفوذ، استفاده از کلمات عبور بوده است؛ امروزه با توجه به پیشرفت روش های نفوذ می بایست از تکنیک های نوین رمزنگاری و حفاظت اطلاعات سایبری؛ و تجهیزاتی همچون دیواره آتش و یا پروکسی سرورها[۱] استفاده گردد و از ضروری ترین اقدامات بومی نمودن این دانش ها و بروز نگه داشتن توان بازدارندگی می باشد. همچنین قراردادن تمهیدات لازم بمنظور جلوگیری از به خطر افتادن پایداری سامانه ها و عدم ایجاد اختلال در صورت رخداد حملات فیزیکی و یا بلایای طبیعی همواره می بایست لحاظ گردد تا زیرساخت ها امن، ایمن و پایدار به ارائه سرویس های مد نظر بپردازند.

- خاموشی و تخصیص مجدد[۲]

یک راه حل مقابله به حمله سایبر این است که سامانه بطور کامل یا جزئی خاموش و دوباره تخصیص مجدد شود. سامانه ای که تحت تأثیر یک حمله قرار دارد، باید موانع و دفاع هایی از خود را بنا نهد که شاید در مواقع عادی از آنها

---

[۱] proxy servers

[۲] Shutdown and reallocation

استفاده نمی‌کند و سعی کند قسمت هایی را که با حمله مواجه شده‌اند، ایزوله نماید. البته مراحل خاموش کردن و تخصیص مجدد باید به صورت بلادرنگ[۱] و بسرعت انجام گیرد.

- پشتیبانی[۲]

نکته قابل توجه این است که باید همواره از اطلاعات سامانه پشتیبانی شود. این تاکتیک از طریق تهیه نسخه پشتیبان اطلاعاتی که ذخیره شده‌اند، اجرا می شود. بسیاری از روش‌های دفاع، نیاز دارند که حالت صحیح سامانه قبل از حمله را، جهت تسهیل در بازیابی و تجدید مجدد بدانند. این روش برای مواقعی است که حملات براساس نقطه شروع دقیق و مشخصی انجام می‌شود و پشتیبان‌ها به طور منظم گرفته می‌شوند. بسیاری از مهاجمین، موذیانه به کندی و بطور محرمانه، مشکلات زیادی را نسبت به زمانی که اطلاعات سالم بودند، ایجاد می‌کنند. در این حالت، جهت ایجاد فضای سالم، سامانه های سازمان باید خودشان برنامه هایی برای تهیه نسخه پشتیبان داشته باشند.

---

[۱] real time

[۲] Backup

فصل ۷ - جمع بندی:

۱. تهدید و جنگ سایبر را باید به اندازه جنگ فیزیکی مهم پنداشت.
۲. فضای سایبر 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 می بایست تأکید 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 سایبر در ایران، نیاز به افزایش توانمندی‌های امنیتی بومی کشورمان بسیار محسوس است.
۶. می بایست به شاخصه امنیت(امنیت، ایمنی و پایداری) همپای شاخصه های 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.

باید به فکر روزی باشیم که به دلیل وابستگی تجهیزات، نرم افزارها، پروتکل های ارتباطی، شبکه و ... قادر نخواهیم بود سرویس های مورد نظرمان را ارائه دهیم و یا از آن سرویس ها بهره مند شویم.