حملات سایبری

مهدیه شیخ
سازمان فناوری اطلاعات
شیما آتش پنجه
سازمان آموزش و پرورش
حسین نهتانی
سازمان فناوری اطلاعات

چکیده

این سند به بررسی حملات سایبری و مفاهیم مرتبط با آن می‌پردازد. حملات سایبری به عنوان اقداماتی تعریف می‌شوند که با هدف به خطر انداختن اطلاعات، سیستم‌ها و شبکه‌های کامپیوتری انجام می‌گیرند. تاریخچه‌ی این حملات از دهه‌ی ۱۹۷۰ تاکنون نشان می‌دهد که آنها به تهدیدی جدی برای امنیت ملی و زیرساخت‌های حیاتی تبدیل شده‌اند. ابزارهای مورد استفاده شامل نرم‌افزارهای شناسایی، نفوذ و مهندسی اجتماعی است. دفاع در برابر این حملات نیازمند افزایش امنیت، آموزش کاربران، تدوین قوانین و همکاری بین‌المللی است. امنیت سایبری یک مسئله‌ی جهانی است.

کلمات کلیدی:

حملات سایبری،فضای سایبری،امنیت سایبری،مهندسی اجتماعی،زیرساخت اطلاعات

مقدمه

اینترنت یکی از فضاهای توسعه خدمات فنی عمومی می باشد که به سرعت در حال رشد است . امروزه فناوری اطلاعات و ارتباطات(ICT) در همه جا وجود دارد و روند دیجیتال سازی در حال رشد است .تقاضا برای اتصال به رایانه و اینترنت منجر به ورود فناوری رایانه به محصولاتی شده است که به طور معمول بدون آن تاکنون کار کرده اند مثل ماشین ها و ساختما نها تامین برق، خدمات حمل و نقل، خدمات نظامی و سازمان های مختلف، در حقیقت همه خدمات مدرن به استفاده ازICT وابسته می باشند.تأثیرICTروی جامعه فراتر از ساخت خدمات اطلاعات پایه است .در دسترس بودنICT زیربنایی برای توسعه در ایجاد، دسترسی و استفاده از سرویس های بر پایه شبکه میباشد.پست های الکترونیکی جایگزین نامه های نوشتاری شده اند، نمایش وب آنلاین امروزه برای امور بازرگانی مهمتر از تبلیغات چاپی هستند و ارتباطات اینترنتی و سرویس های تلفنی در حال رشدی سریعتر از ارتباطات با سیم های زمینی هستند. کاربردهای ICT ا ز قبیل دولت الکترونیکی، تجارت الکترونیکی، تحصیل الکترونیکی، سلامت الکترونیکی و محیط الکترونیکی به عنوان پایه های توسعه در نظر گرفته می شوند، بطوریکه کانال مؤثری برای ارایه دامنه وسیعی از سرویس های پایه در مناطق دور افتاده و روستایی فراهم می کنند.هزینه های خدمات اینترنت اغلب خیلی پایی نتر از سروی سهای همسان شبکه بیرونی هستند. خدمات پست الکترونیکی اغلب به صورت رایگان در دسترس می باشند یا در مقایسه با خدمات پستی سنتی هزینه خیلی پایین تری دارند. دایره المعارف آنلاین ویکیپدیا را می توان به صورت رایگان استفاده کرد همانطوری که صدها خدمت آنلاین هم اینکار را انجام میدهند. هزینه های پایین مهم هستند بطوریکه کاربران زیادی میتوانند از این سرویس ها استفاده کنند، مانند افراد با درآمد پایین، به کارگیری منابع مالی محدود، بسیاری از افراد در کشورهای در حال توسعه م یتوانند از خدمات اینترنتی استفاده کنند که ممکن است در خارج از شبکه به آنها دسترسی نداشته باشند.دسترسی کامل به اطلاعات، پشتوانه مردم سالاری است، بطوریکه سیل اطلاعات از کنترل دولت مردان خارج می شود.توسعه های فنی، زندگی روزمره را بهبود میبخشند برای مثال بانکداری و خرید آنلاین،استفاده از سرویس های اطلاعاتی موبایل و قابلیت مکالمه صوتی در اینترنت(VoIP) تنهامثالهایی از وارد شدنICT به درون زندگی روزمره ما می باشند.اگرچه، رشد جامعه اطلاعاتی با تهدید های جدید و جدی همراه است .خدمات زیربنایی مثل آب و برق هم اکنون با اتکا بهICTفراهم میشوند. ماشین ها، کنترل ترافیک،آسانسورها، تهویه هوا و تلف نها هم به عملICTبستگی دارند .حمله به خدمات زیر بنایی اطلاعاتی و خدمات اینترنتی هم اکنون پتانسیلی برای ضربه زدن به جامعه به شیوه های جدید و خطرناک میباشد.حمله به خدمات زیر بنایی اطلاعاتی و خدمات اینترنتی هم اکنون پتانسیلی برای ضربه زدن به جامعه به شیوه های جدید و خطرناک میباشد. حملات علیه ساختار زیربنایی اطلاعات و خدمات اینترنت در قبل اتفاق افتاده است. کلاهبرداری آنلاین، انتشار عکس های خصوصی افراد و هک، تنها برخی از نمون ههای جرایم رایانه ای هستند که هر روز در حجم وسیعی انجام م یشوند. ضرر و زیان مالی ایجاد شده توسط جرایم سایبری خیلی زیاد است.

مفاهیم اولیه

برای تفهیم حمله سایبری ابتدا باید فضای سایبری و عناصر آن را ادراک نمائیم .بنابراین ابتدا ببینیم اصولا سایبر(Cyber) به چه مفهوم است:

سایبر، پیشوندی برای اسامی متعدد و متنوعی است که همگی براساس انتشار روزافزون رایانه پدید آمده اند .ضمنا اغلب عناصر درگیر با اینترنت با این پیشوند قابل تشریح می باشند.

اولین اصطلاح در این وادی،Cyber Spaceیا همان فضای سایبری است که استعاره ای برای تشریح سرزمین غیرفیزیکی تشکیل شده توسط سیستم های کامپیوتری می باشد .در فضای سایبری نمیتوان بوئید یا شنید (منظور توسط حواس رایج است) ولی این گستره نیز دارای عناصر و اشیاء(object) خاص خود است؛ فایلها، پیغام های الکترونیکی، عکس ها و ... این فضا دارای مدل های انتقالی و حمل نقل نیز می باشد. بر خلاف فضای حقیقی، سیر و گشت در این سرزمین بدون هیچگونه حرکتی فیزیکی مقدور است، بله تنها با حرکت موشواره یا فشردن کلیدی در صفحه کلید.

تعریف حمله سایبری

حمله سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحا به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستمهای اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی(اطلاعات، پروسه های مبتنی بر اطلاعات، سیستمهای اطلاعاتی، شبکه های رایانه ای) دشمن در یک فضای سایبری است. چنین عملیاتی بطور مشخص با اهداف نظامی، تجاری، سیاسی، فرهنگی و ... انجام می پذیرد .بنابراین باید دارای ارزش افزوده و به اصطلاح، بهره برداری از عناصر دشمن را شامل شود .کما اینکه هر نوع جنگ دیگر نیز نهایتا به سوءاستفاده از منابع دشمن ختم خواهد شد. حمله سایبری دارای اهمیت روزافزون برای مراکز نظامی، سرویسهای جاسوسی، اطلاعاتی، سری و دنیای تجارت است ولی در کل، دید نظامی و غیرنظامی را باید مدنظر داشت.

برخی از لغات و اصطلاحاتی که در فضای سایبری مطرح است عبارتند از:
-ایمنی سایبری(Cyber Security): امنیت و آسایش سایبری نیز از جنب ههای زندگی انسان امروزی است.
- حمله سایبری (Cyber Attack): برخی در این محیط اقدام به حمله و تهاجم مینمایند.
- سرباز سایبری(Cyber Soldier\Cyber Warrior) : جنگ سایبری نیز مانند هر جنگی نیاز به نیروی انسانی دارد که البته در اینجا نیروی الکترونیکی (سربازان صرفا سایبری)نیز حضور دارد.
- تهدید سایبری(Cyber Threat) : مخاطرات چندی در فضای سایبری وجود دارد.
- پلیس سایبری(Cyber Police) : برای جلوگیری از جرائم سایبری باید دارای پلیس آن فضا نیز بود.

تاریخچه حملات سایبری

بنابر شواهد، اولین جنگ این چنینی، بین ایالات متحده آمریکا و شوروی(سابق)در اواسط دهه ۱۹۷۰ در گرفته است.
*کره شمالی و آمریکا – از دهه ۱۹۸۰– کره شمالی اقدام به تاسیس مدرسه هک با بیش از ۱۰۰ سرباز آموزش دیده می نماید .البته این عمل در حقیقت عکس العملی در برابر توان مضاعف دشمن است .جنگ های این دهه را می توان پی آمدهای مشخصی از جنگ سرد دانست .بنابراین انگیز ها کاملا مشخص هستند.
*سال ۱۹۹۴ - حمله به مراکز هوائی-تحقیقاتی در نیویورک و همزمان به انستیتو تحقیقات اتمی کره جنوبی و نهایتا مرکزیRome علمی در لاتویا (از کشورهای تازه استقلال یافته شوروی سابق). شبکه در دستان حمله کننده ها بود ولی منبع آن کاملا نا مشخص بود تا اینکه ردی از انگلستان کشف شد.
*سال ۱۹۹۵ - بانک معروف آمریکائی، CitiBank و گروه هکرهای روسی و از دست دادن ۴۰۰ هزار دلار !در نهایت حمله گرهای روسی شناسائی شده و بخشی از زیا نها جبران شد.

*اوایل آگوست سال ۲۰۰۰– هنگ کنگ و استفاده از جنگ سایبری علیه چین. چین، هنگ کنگ را از ایالات کشور خود می داند ولی آنها به دنبال استقلال بوده و هستند. استفاده از ویرو سها در هدف قرار دادن مراکز انرژی، نظامی وبانـک هـا. ارائه نقشه هنگ کنگ/چین بدون تاریخ دقیق امکان پذیر نیست .هنگ کنگ زمانی مستعمره انگلستان نیز بوده است.

حمله سایبری در ایران

تابستان ۲۰۰۳ ، نیروهای مسلح ایران به عربستان سعودی نزدیک می شوند تا تولید نفت در خاور میانه را کنتـرل کننـد . ایالات متحده متفقین خود را برای دفع ایران جمع می کند ولی ناگهان در می یابد که بطور مجازی و توسط کامپیوترهای مهاجم پنهان و غیرقابل ردیابی فلج شده است؛ آنها شبکه نیرو را می خوابانند ، باعث تصادم قطارهـا مـی شـوند، تبـادلات مالی را مختل می کنند و سیستمهای مخابرات را تهدید می نمایند .جنگ دوم خلیج فارس تبدیل به اولین جنگ سایبری می گردد و همچنین جنگ معروف سال ۲۰۰۱ بین آمریکا و چین و نهایتا جنگ ماه می سال ۲۰۰۳ بین عـراق و آمریکـا که تاثیرات نه چندان عمیقی بر فضای سایبری ایران گذاشتند.

محدوده عملیاتی سایبری

محدوده عملیات سایبری بسیار گسترده است؛ از تولید پارازیت مخابراتی گرفته تا عملیات روانی، از تغییر صفحات وب یک سایت گرفته تا بمباران ایمیلی. ولی نهایتا، اصل، تهدیدات منابع اطلاعاتی است به نحوی کـه امنیـت ملـی دشـمن مـورد مخاطره قرار گیرد .بنابراین بستر عملیات سایبری همانا زیرساخت های اطلاعاتی می باشند.محدوه عملیات سایبری بطـور مشخص در حدود منابع دشمن است ولی میتواند دربرگیرنده اشیاء خود حمله کننده نیز باشـد و یـا در محـدود سـایبری دیگر عوامل وابسته یا غیر وابسته باشد.

در مورد محدوده عملیاتی باید این نکته را مد نظر داشته باشیم که با انتخاب نادرست محدوده عملیـات، بـروز مشـکل در محدوده سایبری خود حمله کننده نیز محتمل است.

تصور کنید که حمله کننده سایبری مبادرت به تهاجم به یک سایت اینترنتی م ینماید و نهایتـا موجـب پـائین آمـدن آن سایت م یگردد...ولی علت

سرور اصلی بوده است...و یکی از سرورهای محدوده جغرافیائی حمله کننده بطور ناخواسته در پائین آمدن سـایت هـدف، انهدام

محدود عملیاتی بوده است...این مشکل به ویژه با انتشار و نامتمرکز بودن خدمات ثبت دامنه، میزبـانی فضـای وب، ثبـت آدرس اینترنتی و ارائه

پهنای باند بسیار محتمل و رایج است.

به محدود ههائی از عملیات سایبری توجه نمائید:

-اشیاء بسترساز شبکه(روترها، سوئی چها، ماهواره ها و...)

-عناصر وب (سایت های وب، پایگا ههای اطلاعاتی مبتی بر وب و...)

-ایمیل، رایج ترین عنصر گذشته و حال در فضای سایبری

مشخصات عملیات سایبری

شاید بتوان مشخصه های یک عملیات سایبری را عینا از روی عمایات جنگی فیزیکی نمونه برداری نمود .نحوه عملکرد که همان حمله و دفاع
است، باید دارای آیت مهای ذیل باشد:

۱ -انگیزه

بدون شک، حمل هکننده باید ابتدا دارای انگیز های مشخص باشد .امکان دارد این انگیـزه مسـتقیما تولیـد شـده (ماننـد زمانی که شما مورد حمله سایبری قرار گرفته باشید و در عین دفاع قصد دارید پیشروی کنید)یا به شکلی غیـر مسـتقیم (مانند زمانی که یک نزاع سیاسی شما را به راه حمله می کشاند) نیرو وارد نماید. به هر صورت، باید انگیزه تعیین و تفسیر گردد، در غیر این صورت، مراحل بعدی دارای بستر و پایه منطقی نخواهند بود.

۲ -هدف

با توجه به انگیزه حمله، محدوده عملیات مشخص م یگردد .این همان چیزی است که آن را هدف یا Target می نامیم . هدف می تواند به بزرگی و گستره سیستم و شبکه توزیع نیرو در یک کشور باشد، و یا میتواند بـه کـوچکی یـک سیسـتم مشخص در یک شبکه محلی باشد .دقت نمائید که بزرگی و کوچکی هدف نیست کـه تعیـین کننـده ارزش آن اسـت؛ در عملیات سایبری، یک هدف که در شکل فیزیکی بسیار کوچـک اسـت مـی توانـد دارای ارزشـی بزرگتـر و بیشـتر از یـک پالایشگاه داشته باشد.

۳ -جمع آوری اطلاعات

هر عملیاتی، چه فیزیکی و چه سایبری باید با چشمان کاملا باز صورت پذیرد .اجرای عملیات سایبری بدون اطلاعات مانند بمباران مکانی است که از مسکونی یا نظامی بودن آن مطلع نیستیم؛ بدون اطلاعات فقط نیرو و منابع خود را از دست می دهیم .ضمنا احتمال ردیابی و شناسائی خود را برای دشمن افزایش خواهیم داد. کسب اطلاعات از عناصر سایبری دشمن بعنوان مهم ترین بخش از عملیات سایبری مورد توجه است .از دید کارشناسان، جم عآوری اطلاعات از اهداف سایبری به مفهموم انجام ۵۰ درصد از کل عملیات است.

۴ -نقاط ضعف

وقتی اطلاعات حمله کننده درباره ماهیت سایبری هدف کامل شد، مرحله تعیین نقاط ضعف آغاز می شود .ایـن بخـش از کار به واقع ساده ترین قسمت عملیات است .با دانستن مشخصات هدف، تعیین عیوب سخت افزاری و نرم افزاری چنـدان دشوار نبوده و فقط زمان لازم است .اگر دشمن در مورد شما به چنین مرحل های برسد، فقط تیـک تـاک عقـرب ههـای ساعت را دنبال نمائید تا حمله آغاز شود.

۵ -نفوذ

پس از تعیین نقاط ضعف و با در نظر گرفتن اطلاعات بدست آمده و با آگاهی از مکانیسم های ردیابی، عملیات سایبری در جهت نفوذ به هدف پیش می رود .این مرجله، اگرچه بخش پایانی عملیات است ولی زمان بیشتری را به خـود اختصـاص داده زیرا دارای قسم تهای متعدد است. عموما لفظ hack را با عبارت" نفوذ "همراه م یکنند ولـی منظـور مـا از نفـوذ بـا عبارت دقیق Penetration همراه است .نفوذ همیشه به مفهوم دسترسی کامل به منابع هدف نیست؛ حمله کننده گاهی وادار به ارتقاء مزایا می گردد، مجبور می شود اطلاعات بیشتری کسب نماید، ردپاهای خود را بپوشاند، در بهـای پنهـان و پشتی ایجاد نماید یا حتی در نهایت فقط به یک حمله DoS اکتفا نماید.

در مورد عملیات سایبری باید توجه داشته باشیم که تنها مدیوم رایج در این فضا، مدیوم شبکه های مبتنی بر TCP/IP نیست .در اینترانت ها ممکن است پروتکل ها و با عبارتی، عناصر سایبری متفاوتی حضور داشته باشند .ضمنا هنوز هم رایج ترین مدیوم ارتباطی شبکه، خطوط تلفن شهری یا همان PSTN است .بنابراین حملاتی نظیرWardialing یا جنگ با مود مها به عنوان یک تهدید بزرگ محسوب م یگردند. مثال دیگر، مدیوم بدون سیم یا همان Wireless است که نوع عملیات موسوم به Wardriving را ایجاد می نماید.

نیروی انسانی، توان تخصصی

عمده ترین نیاز، توان تخصصی است ولی به یاد داشته باشیم که شرط لازم، داشتن اطلاعات از دشمن است .در مورد نیروی انسانی متخصص باید اذعان کنیم که کیفیت بیش از کمیت دارای اهمیت است .در حقیقت تعداد نیروی انسانی یک عملیات سایبری ملاک نیست بلکه به هر صورت، نیروی انسانی، راهبر عملیات سایبری است .از طرح ریزی و جمع آوری اطلاعات گرفته تا تحلیل و اجرای حمله .بطور مشخص، متدهای مورد استفاده ایشان و نحوه عملکرد آنها مد نظر است. اولین توان تخصصی مورد لزوم در یک عملیات سایبری، دانش شبکه یا اصطلاحا Networking است .سرباز سایبری باید بداند که بستر ارتباطی چگونه عمل م ینماید و مدیوم شبکه دارای چه خصوصیات ذاتی است.

دومین قابلیت مهم در یک عملیات سایبری، شناخت اجتماعات مختلف است، به عبارت دیگر، سربازان سایبری شما باید به نوعی مهندسان اجتماعی (Social Engineer) باشند .آمار و ارقام مستند حاکی از این موضوع هستند که مهندسی اجتماعی اکنون بالاترین تهدید فضای سایبری محسوب می گردند زیرا به شکل بسیار ظریفی بر تعامل بین این فضا و مجیط فیزیکی تکیه دارند.

ابزار و سلاح های حملات سایبری

سلاح جنگ سایبری، مخلوطی از دانش و تجهیزات است. ما بر این باور هستیم که دانش تخصصی بالاترین اثر را دارد ولی بدون شک ابزار نیز ملزوم است. در مورد استفاده از ابزار باید به این نکته توجه نمائیم که هرگز راه عکس را نپیمائیم؛ ابتدا باید تکنیک طراحی گردد و سپس ابزار آن تولید گردد.

با حضور در بزرگراه اطلاعاتی نظیر شبکه اینترنت، بسیاری از ابزارها، بدون صرف وقت زیادی در دسترس هستند و مجددا خاطر نشان می کنیم که نحوه استفاده از آنها و زمینه دانش مهم است. ابزارهای جنگ های سایبری را میتوان در اجتماع نفوذگران (Hacker Community) یافت .ضمنا توجه داشته باشید که اجتماع نفوذگران از بسیاری از ابزارهای جامعه ایمن گران برای تهدید ایشان استفاده می نمایند.

اگر بخواهیم سلاح های سایبری را دسته بندی نمائیم م یتوانیم گرو ههای ذیل را در نظر بگیریم:

۱ -ابزارهای شناسائی

عموم سلاح های شناسائی در خود فضای سایبری یا همان اینترنت وجود دارند مانند اطلاعات عمومی،موتورهای جستجوی دامنه ها،ثبات دامنه اینترنتی،ثبات آدرس اینترنتی و غیره...

۲ -ابزارهای وارسی

وارسی هدف، همانند کوبیدن به دیوارها برای پیدا کردن درب ها و پنجر ه هاست. با سلاح های وارسی باید سیستم های زنده و فعال (alive) و آنهایی را که از طریق اینترنت قابل دسترسی هستند را مشخص نمود مانند انواع جاروب کنند ه ها(Sweep) و انواع وارسی کنند ههای پورت های TCPوUDP .

۳ -ابزارهای کنکاش

سلاح های کنکاشکر عموما در خورد سیست مهای عامل حضور دارند .این ابزارها مبادرست به بیـرون کشـیدن اطلاعـات خاصOS ها و شبکه ها،نظیر عناصر کاربری و تولیدات نر مافزاری می نمایند.

هدف اصلی جنگجو بطور مشخص کسب اطلاعات بیشتر در خصوص منابعی است که شاید تابحال بر وی مستتر بوده انـد ولی این اطلاعات در نظر اول کاملا بی ضرر به نظـر مـی رسـند: منـابع اشـتراکی (share)، کـاربران (user)، گـرو ه هـا (group) و برنامه ها (application).

۴ -ابزارهای نفوذ

همانطور که قبلا هم اشاره شد، با دارا بودن اطلاعات کافی از هدف، تکنیک و ابزار نفوذ چندان دور از دسترس نیست.

-ابزارهای صرفا سایبری

-سلاح های فیزیکی/سایبری .مانند امواج کوتاه و بلند دستکاری شده که موسوم به E-Bomb یا بمب الکترونیکـی نیـز می باشند.

-ابزارهای ارتقاء مزایا

حمله کننده همیشه پس از نفوذ به تمام امکانات هدف خود دسترسی ندارد .بنابراین باید به دنبال رو شها و ابزارهائی باشد تا مزیت وی را به روی هدف افزایش و ارتقاء دهند مانند روش ها و ابزارهای تزریق، متدهای فریبکارانه و استراق سمع.

-سلاح های پنهان

گاهی نفوذ مجدد به یک هدف سایبری شامل تکرار تمام مراحل کنکاشگرانه و نفوذ است .لذا حمله کننده باید مبادرت به جادادن سلا ح های پنهان نماید تا بعدا نیز به دخول نائل گردد .به عناوین این بخش از ابزارها توجه کنید:

-انواع اسب های تروآ

-انواع ویروس ها و کر مها

-نقاط پنهان در سیست مهای عامل

-جنگ افزارهای حملاتDoS

شاید سرباز سایبری که نتواند نهایتا به عنصر سایبری نفوذ نماید، مبادرت به تعدیـد جنبـه در دسـترس بـودن آن هـدف نماید .بنابراین استفاده از متدها و ابزارهای حملات DoS محتمل است.

تائیرات جنگ های سایبری

میزان تاثیر چنین جنگی بستگی کامل به میزان تداخل فضای سایبری با فضای حقیقی دارد .هر چـه از زیرسـاخت هـای اطلاعاتی مبتنی بر رایانه بیشتر استفاده گردد، تاثیر پذیری بیشتر است.

بدون شک نقطه و هدف حمله کننده نیز بی تاثیر نیست .حمله به بانک اطلاعـاتی یـک بیمارسـتان را بـا حملـه بـه بـرج مراقبت فرودگاه مقایسه نمائید!.

شاید بتوان کمترین اثر حمله سایبری را، از دسترس دور نمودن منابع سایبری دانست:

۱ -در بهترین شرایط:

-حملاتDoS

-ویروس ها و کر مهای رایانه ای

۲ -در شرایط خوب:

-حمله کنند هها به سیستمهای کامپیوتری دولتی نفوذ نموده و اسرار نظامی و فنآوری رمزبندی را می ربایند.

-خطوط نیرو مختل می گردند.

-سیستمهای اورژانسی مورد مخاطره قرار گرفته، بدین شکل سعی و کوشش در رساندن کمک و نجات مختل می گردد.

۳ -در شرایط بد:

-فیبرهای نوری مابین نقاط اصلی تهدید م یگردند.

-بمباران سرورهای دامنه و بانکها.

۴ -در بدترین شرایط:

در نهایت : بمباران عناصر اینترنتی محقق گردیده و پائین آوردن اینترنت محتمل است.

راه های جلوگیری یا پدافند جنگ سایبری

بهترین دفاع و حمله در جنگ سایبری همانا بالا بردن سطح ایمنی عناصر درگیر است و این میسر نخواهد بود، جز با افزایش اطلاعات.

هر یک از عناصر درگیر در فضای سایبری (فنآوری اطلاعاتی)، باید به اندازه ارزش خود حفاظت گردند .در غیر این صورت، انتخاب مکانیس مهای دفاعی چندان بهینه نخواهد بود و بدون شک دارای هزینه های سربار است.پس باید ابتدا دارائی ها و عناصر اصلی و اساسی اطلاعاتی(اشیاء مهم در فضای سایبری)را تعریف و تعیین نموده و براساس سیاس تهای کلان و با در نظر گرفتن تهدیدات موجود در برابر آن عناصر، تمهیدات دفاعی را پیریزی نمائیم. امنیت سایبری نقش مهمی را در توسعه فناوری اطلاعات و همچنین خدمات اینترنتی بازی میکند .تقویت امنیت سایبری و حفاظت از زیرساختهای اطلاعات برای امنیت و رشد اقتصادی هر ملتی ضروری است .ایمن تر کردن اینترنت(و حفاظت از کاربران اینترنت) برای توسعه سرویس های جدید و سیاست های دولتی بسیار ضروری است .توقف جرایم سایبری قسمتی مهم از رویکرد حفاظت از ساختار زیر بنایی اطلاعات و امنیت سایبری هر کشوری می باشد، بویژه این عمل شامل وضع قانونی مناسب علیه سوء استفاده ازICT برای تبهکاری یا دیگر اهداف و فعالیت ها به منظور رخنه به ساختار زیربنایی ملی م یباشد .در سطح ملی این مسؤلیتی مشترک است، که نیازمند کاری هماهنگ برای پیشگیری، آمادگی،پاسخگویی بین بخش دولتی، بخش خصوصی و شهروندان م یباشد .در سطح منطقه ای و بین المللی، شامل همکاری و هماهنگی با شرکای مربوطه می باشد .بنابراین قاعده مندسازی و اجرای چهارچوب و استراتژی ملی برای امنیت سایبری نیازمند رویکردی مفصل م یباشد. استراتژی های امنیت سایبری برای مثال، توسعه سیستم های محافظ الکتریکی یا تعلیمات کاربران برای جلوگیری از قربانی شدن آنها در جرایم سایبری، می تواند به کاهش خطر جرایم سایبری کمک کند. توسعه و حمایت از راهبردهای امنیت سایبری عناصری حیاتی در نبرد علیه جرایم سایبری می باشند. دبیر کلITU برنامه عملیاتی امنیت سایبری جهانی (GCA) را درمی۲۰۰۷، در کنار شریکانی از دولت ها، صنعت، سازمان های منطقه ای و بین المللی،مؤسسات تحقیقاتی و دانشگاهی شروع کرد.GCA چهارچوبی جهانی برای گفتگو و همکاری بین المللی برای هماهنگ کردن پاسخ بین المللی به چالش های در حال رشد نسبت به امنیت سایبری و برای تقویت اعتماد و امنیت در جامعه اطلاعاتی می باشد.

GCAدارای هفت هدف راهبردی مهم برپایه پنج حوزه کاری م یباشد:

۱ .اعمال قانونی

۲ .اعمال فنی واسطه

۳ .ساختارهای سازمانی

۴ .صلاحیت

۵ .همکاری بین المللی

نبرد علیه جرایم سایبری نیازمند رویکردی جامع م یباشد .با وجود اینکه اعمال فنی به تنهایی نـم یتواننـد از هـر جرمـی جلوگیری کنند، مهم است که به پلیس امکان پیگیری و تحت تعقیب قرار دادن جرایم سایبری به طور مؤثر داده شود. در میان حوزه های کاریGCA،اعمال قانونی، روی چگونگی نمایان ساختن چالش های قانونی ایجاد شده توسط فعالیت های خلافکارانه انجام شده در شبکه ICT

در شیوه سازگارانه بین المللی تمرکز می کند" .اعمال فنی واسطه "روی اعمال کلیدی برای رشد رویکردهای تقویت شده برای بهبود امنیت و مدیریت بحران در فضای سایبری تمرکز می کند، مثل طرح های اعتباری ،پروتکل ها و اسـتانداردها. "ساختارهای سازمانی "روی جلوگیری، ردیابی، پاسخ و مدیریت بحران حملات سایبری شامل حفاظـت از سـامان ه هـای زیربنایی اطلاعات حیاتی تمرکز می کند.

"ظرفیت "روی راهبردهای ماهرانه برای ساختارهای ظرفیتی برای بالا بردن آگاهی، انتقال دانش و رشد امنیت سایبری در دستور جلسه سیاست ملی تمرکز می کند .در نهایت" همکاری بین المللی "روی همکاری بین المللی، گفتگو و هماهنگی در سروکار داشتن با تهدیدات سایبری تمرکز می کند. توسعه مناسب قانون در ایـن رویکـرد، توسـعه چهـارچوب قـانونی مربوط به جرایم سایبری بخشی ضروری از راهبرد امنیت سایبری است .اول از همه این مسئله نیازمند تهیه قانون جزایی برای جریمه کردن اعمالی مثل کلاهبرداری رایانه ای، دسترسی غیر قانونی، تداخل در اطلاعـات، تخلـف از کپـی رایـت و انتشار عکس های مستهجن م یباشد .این حقیقت که ماده های موجود در قانون کیفری قابل اجرا برای اعمال مشابه انجام شده بیرون شبکه وجود دارند به این معنی نیست که آنها را می توان به اعمال انجام شده مشابه روی اینترنت اعمال کرد . بنابراین تجزیه و تحلیل دقیقی از قوانین ملی جاری برای شناخت هر مفر قانونی احتمالی، مهم است .جـدا از مـاده هـای قانون کیفری، پلیس نیاز به ابزارهای ضروری و دستگاههایی برای پیگرد جرایم سایبری دارد .این قبیل پیگرد ها خودشان چالش های زیادی دارند .متخلفان میتوانند تقریباً از هر مکانی در دنیـا مرتکـب تخلـف شـوند و اعمـالی بـرای پوشـاندن هویتشان انجام می دهند .ابزارهای مورد نیاز برای پیگرد جرایم سایبری می تواننـد بـه طـور کامـل از آنهـایی کـه بـرای پیگردهای جرایم معمولی استفاده می شوند متفاوت باشند.

توصیه هایی برای مراکز،مسئولین،کارشناسان و متخصصین تصمیم گیری IT کشور

-اشتراک، همکاری و ارتباط میان آژانس های سری و اطلاعاتی کشور

-گزینش استانداردها و استفاده از استانداردهایISO

-اطلاع رسانی

-تقویت متخصصین رایانه در جهت فراگیری زبان های انگلیسی، روسی و چینی

-حفاظت از زیرساخ تهای اصلی(Critical Infrastructure Protection) و مشخصا زیرساخ تهای ف نآوری اطلاعاتی کشور

-عدم تکیه مطلق بر هرگونه منبع خارجی و غیر معتمد و انتخاب مدلTrustبهینه و مقتضی
-تعلیم و تربیت و بکارگیری متخصصین علوم سایبری از جنب ههای فنی و حقوقی تا مجریان قانون
-افزایش مکانیس مهای کنترل و مانیتورینگ و تخصصی نمودن قابلی تهای ردیابی و جمع آوری مدرک
-آزمایش و انتخاب ف نآوری های جدید و تطبیق آنها با نیازهای امنیتی کشور
-تدوین و تثبیت قوانین داخلی
-برخورد جدی با مجرمین داخلی
-تدوین و بکارگیری و اعمال سیاست های مرتبط
-طراحی استانداردها و الگوهای رمزنگاری ایرانی؛ این بدان مفهوم نیست که الگوهای فعلی/غربی به نـا کارآمـد هسـتند، بلکه به کارما نمی آیند .مثلا فن آوری پیشرفته و بسـیار مسـتحکم در رمزنگـاری(PGP (Pretty Good Privacy در دستان وازرت دفاع آمریکا است.
-تبعیـت از اصـول ایمنـی و حفاظـت شـامل مکـانیس مهـای جلـوگیری(Prevention)، ردیـابی(Detection) و ترمیم(Recovery)
-استفاده گسترده تر ازIDS ها وNIDS ها در جهت تقویت امر کنترل و ردیابی
-بکارگیری هانی نت (HoneyNet) در جهت تحقیق و توسعه فنون نظامی سایبری

جمع بندی

- تهدید و جنگ سایبری را باید به اندازه نمون ههای فیزیکی مهم پنداشت.
- فضای سایبری را نمی توان مطلق تصور نمود.
- علی رغم خالص دانستن فضای سایبری، فاکتور انسانی را نم یتوان در نظر نگرفت.
- مسلما کشورهائی آسیب پذیرتر هستند که دارای هویت سایبری محسوس تری هستند.
- جنگ و نزاع هرگز و در هیچ زمانی به نفع هیچ کشوری نبوده است.
- علی رغم وسعت فضای سایبری در ایران، لزوم افزایش توانمند یهای کشورمان بسیار محسوس است.
- هرگز نباید با کشوری وارد جنگ سایبری شد که دارای اشیاء محدودتر در این فضا است.

امنیت سایبری یک مسئله جهانی است که از مرزهای ملی فراتـر مـی‌رود و بـه همـین دلیـل، نیازمنـد تلاش‌هـای جمعـی کشورهای مسئولیت‌پذیر برای رسیدن به یک توافقنامه بین‌المللی جامع مشـابه تمهیـداتی اسـت کـه در زمینـه تسـلیحات هسته‌ای، بیولوژیکی و شیمیایی اتخاذ شده است.

مراجع

سایتهای اینترنتی:

http://cve.mitre.org/
http://usinfo.state.gov/
http://www.2600.com/
http://www.altavista.com/
http://www.astalavista.com/
http://www.cia.gov/
http://www.cis.unisa.edu.au/
http://www.clickz.com/
http://www.defenselink.mil/
http://www.fbi.gov/
http://www.glreach.com/
http://www.google.com/
http://www.guardian.co.uk/

http://www.hartford-hwp.com/
http://www.lnkworld.com/
http://www.mit.edu/
http://www.nipc.gov/
http://www.nsa.gov/
http://www.packetstormsecurity.org/
http://www.psycom.net/
http://www.securityfocus.com/
http://www.taipeitimes.com/
http://www.usdoj.gov/
http://www.yahoo.com/

مقالات جالب توجه:

http://vmyths.com/hoax.cfm?id=281&page=3
http://www.mosnews.com/news/2004/08/27/internetterror.shtml

کتب:

* Cyberwar 2.0: Myths, Mysteries & Reality (Alan D. Campen, Douglas H. Dearth)
* Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Alan D. Campen, Douglas H. Dearth)
* Cyberwar: Point. Click. Destroy (Francha Roffe Menhard, Francha Roffe Menhard)
* Cyberwar: Security, Strategy, and Conflict in the Information Age (Alan D. Campen)
* Cyberwars: Espionage on the Internet (Jean Guisnel)
* Hacktivism and Cyberwars: Rebels With a Cause (Tim Jordan, Paul A. Taylor)
* Mapping Cyberspace (Martin Dodge, Rob Kitchin)
* Secrets and Lies : Digital Security in a Networked World (Bruce Schneier)
* The Art of War (Sun Tzu)
* The Atlas of Cyberspace (Martin Dodge, Rob Kitchin)
* The New Face of War: How War Will Be Fought in the 21st Century (Bruce D.Berkowitz)