دیتا سنترهای[1] اطلاعات مکان محور هدف قابل توجه هکرها[2]

سرتیپ دوم ستاد
مهندس محمد حسن نامی

چکیده

مرکزداده یا دیتا سنتر حاوی بیشترین اطلاعات مکانی با ارزش بوده و میزان قیمت آن در مورد برخی از دیتا سنترها مانند سایتهای IGN فرانسه (Institute Geography National) و یا OS انگلیس (Ordance Survey) و یا NIMA آمریکا (National Imagery Mapping Agency) بین چهار تا دوازده میلیارد دلار تخمین زده می‌شود. لذا با اهمیتی که اطلاعات موجود در این مراکز داده دارند، بدون شک این گونه سایت‌ها یکی از مهمترین اهداف هکرها خواهند بود.

برابر اعلام کمیته امنیت ملی آمریکا، شبکه‌های رایانه‌ای، اطلاعاتی و مراکز داده‌ها هر ساله حدود بیست هزار بار مورد هجوم هکرها قرار می‌گیرند. شایان ذکر است که سایت NIMA تنها در سال ۲۰۰۷ سی و سه مرتبه مورد حمله قرار گرفت که چهار نوبت هکرها موفق شدند قسمتی از اطلاعات مکانی مورد نظر را برباید.

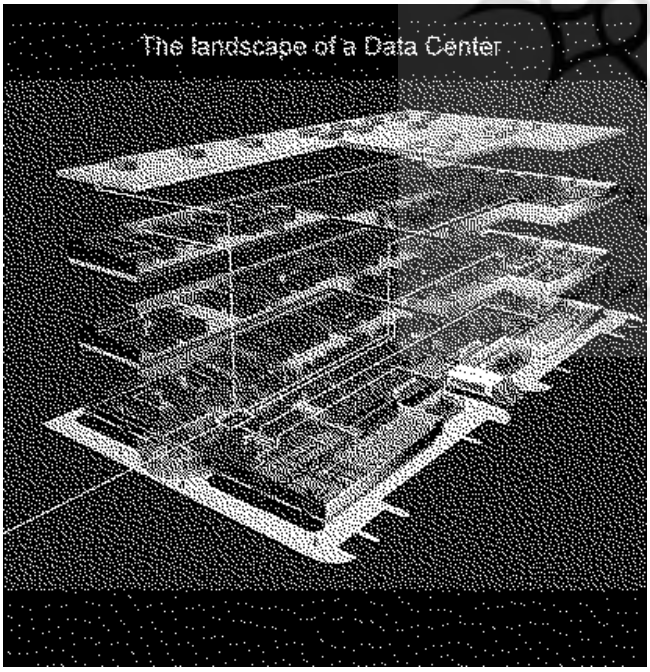
در جامعه امروز، اینترنت[3]، رایانه، دیتا سنتر، دیتا استوریج[4]، شبکه‌های رایانه‌ای، در کلیه امور و جنبه‌های مختلف زندگی بشر به ویژه در مسائل امنیتی دفاعی، نظامی، سیاسی، اجتماعی، اقتصادی، فرهنگی و... نقش حیاتی و بسیار تأثیرگذاری را ایفا می‌نمایند. علاوه بر ویژگی‌های مثبت و بسیار گسترده و حاکمیت فضای مجازی بر فضای عینی در اکثر حوزه‌ها، تهدیدات جدیدی را نیز در پی داشته و ارکان و اساس سازمان‌ها را در بسیاری موارد هدف قرار داده است. متخصصینی که در این حوزه فعالیت می‌نمایند عقیده دارند هر چه جامعه ما به سمت بکارگیری بیشتر از رایانه‌ها پیش می‌رود به همان اندازه میزان تهدید افزایش می‌یابد. در این میان، دیتا سنترها و دیتا استوریجها که عموماً اطلاعات آنها هم از نظر مادی و هم از نظر معنوی دارای ارزش بالایی است از طریق راهزنان رایانه‌ای و یا هکرها مورد دستبرد قرار می‌گیرد.

واژه‌های کلیدی: دیتاسنتر، اینترنت، هکر، داده، رایانه، اطلاعات مکان محور.

دیتا سنتر چیست؟

مرکز داده یا دیتا سنتر عبارتست از یک ساختار نظام یافته از منابع، فناوریهای اطلاعاتی و ارتباطی داده تأسیسات امنیتی و حمایتی که امکان بهره‌مندی بدون وقفه از سیستم‌ها و سرویسهای اطلاعاتی را با قابلیت مدیریت بهینه منابع به کاربران مجاز ارائه می‌نماید. در اوایل دهه ۱۹۴۲ میلادی که برون سپاری خدمات فناوری اطلاعات به عنوان رویکردی غالب مطرح گردید، اولین زمینه پیدایش در رشد سریع مراکز داده در جهان ایجاد شد و حاصل آن کاهش هزینه تمام شده خدمات IT برای مصرف کننده و رشد سریع فناوری برای صنعتها بود.

اصولاً مرکز داده یا دیتا سنتر از دو جنبه ذخیره سازی داده‌ها و معماری مدیریت داده‌ها، در شبکه‌های اینترنتی قابل اهمیت می‌باشد. امروزه سازمانهایی همانند سازمان جغرافیایی در سطح جهان دیدگاه و وظایف حاکمیتی با برداشت اطلاعات از زمین توسط ماهواره‌ها و سیستمهای تصویر برداری هوایی و لیزر اسکن در عملیات دریایی و هیدروگرافی با برداشت اطلاعات از بستر دریا توسط سیستمهای عمق یاب و ساید اسکن سونار و همچنین دستگاههای ثقل سنج و گراویمتر امکان برداشت اطلاعات و داده‌های مکانی و زمین مرجع را فراهم می‌کنند. لذا این مراکز حاوی حجم وسیعی از داده‌های مکانی و زمین مرجع اعم از تصاویر ماهواره‌ای و به ویژه تصاویر ماهواره‌ای با دقت زیر ۱ متر، داده‌های ثقلی و جاذبه سنجی جهت تعیین ژئوئید و همچنین داده‌های عمق یابی حاصل از عملیات هیدروگرافی و اسکن سونار و داده‌های زمینی برداشت شده به روش لیزر اسکن هوایی می‌باشند که حجم وسیعی از داده‌های را شامل می‌گردد.



نگاره (۱): دیتا سنتر

حمله هکرها با هدف تخریب

از اهداف دیگر هکرها یا جنگجویان شبکه‌ای، علاوه بر دستیابی به

اطلاعات با ارزش، تخریب سامانه‌ها، یا انتقال ویروسها و یا کرم واره‌ها[۵] و عوامل نفوذی نرم‌افزاری به مراکز داده‌ها می‌باشد.

پیشرفتهای چشمگیر در مباحث فن آوری و ظهور نسل‌های هوشمند هکرها و توانمندی تکنولوژیکی، آنها را به مرحله‌ای سوق داده که قادرند به عنوان یک بازیگر سرنوشت ساز در فضای سایبری ظاهر شوند.

وین شوارتو مشاور فنی موسسه INTERPACT در این مورد اظهار می‌دارد که «با وجود چندین میلیارد رایانه‌ای که از طریق پیچیده‌ترین زنجیره سامانه‌های ارتباطی مستقر در زمین و ماهواره‌ها، که ما را به گونه‌ای جدا نشدنی به یکدیگر پیوند داده حفاظت رایانه‌های دولتی و بازرگانی به اندازه‌ای ضعیف است که آنها را اساساً می‌توان ناتوان در دفاع قلمداد کرد.»

در گزارش کمیته امنیت ملی آمده است: پیچیدگی ذاتی و فناوری پیچیده و به هم پیوسته سامانه اطلاعاتی، به مختل کنندگان و تروریستها یا کشورهای متخاصم این فرصت را می‌دهد که به شیطنت بپردازند و وابستگی روز افزون ما بر این سامانه‌های اطلاعاتی موجب شده است تا هر گونه گسست در آنها باعث بروز مشکلاتی جدی در جامعه گردد که اگر از این زاویه به آن بنگریم هیچ کشوری در این زمینه آسیب‌پذیرتر از آمریکا نیست. چنانچه در دستورالعمل عملیات اطلاعاتی مبارزه از طریق اینترنت آمریکا آمده است:

راهبردها بایستی بر این اساس باشد که وزارت دفاع به عنوان یک سامانه جنگ‌افزاری دشمن با اینترنت بجنگد و شبکه اینترنتی آمریکا در مقابل حملات هکرها که قصد دارند اطلاعاتی را از مرکز داده‌ها ربایش و آنها را تخریب کنند دفاع نمایند. البته شبکه‌ها خیلی سریعتر از آنکه بتوانیم از آنها حفاظت کنیم گسترش می‌یابند ضمن اینکه خطر حملات ماهرانه نیز روز بروز افزایش می‌یابد. لذا نیروهای آمریکایی بایستی قادر باشند کل سامانه ارتباطات الکترونیکی دنیا را قطع یا نابود کنند.

نمونه حمله هکرها به دیتا سنترها

در سال ۲۰۰۴ هکرها توانستند به سایت OS انگیس ضمن ربایش میزان قابل توجهی از اطلاعات مکان محور به ویژه اطلاعات مربوط به TPC[۶] و ONC[۷] سایت مذکور را برای مدتی غیر قابل استفاده نمایند.

در سال ۱۹۹۱ هکرها با حمله به دیتا سنترداده‌های اطلاعات مکانی وزارت دفاع عراق که در سال‌های ۱۹۸۹ تا ۱۹۹۱ با تسلط متخصصین اطلاعات مکانی روسیه تأسیس شده بود توانستند اطلاعات مکانی مورد نیاز منطقه مرکزی و جنوب را عراق بربایند. شایان ذکر است درنقشه‌های دیجیتالی که آمریکا در سال ۱۹۹۴ منتشر نمود میزان قابل توجهی از این اطلاعات مکانی ربوده شده در آن به وضوح قابل رؤیت بود.

هکرها به راحتی می‌توانند با مهارت بالای خود برنامه‌های پیشرفته را تنظیم و اهداف مورد نظر خود شامل سایت دولتی و نظامی، مؤسسات مالی، دانشگاهها و مراکز علمی دارای روابط نزدیک با سازمان‌های اطلاعاتی و شرکت‌های نرم‌افزاری را مورد هجوم قرار دهند.

بسیاری از صاحبنظران بخش امنیت رایانه معتقدند که دولت‌های متخاصم خارجی، هکرهای حرفه‌ای را استخدام می‌کنند تا اطلاعات سری را جمع آوری و یا با توانایی آنها به عملیات روانی علیه دشمن بپردازند. فعالیت جنگی با هدف تخریب زیر ساختارهای یک کشور مانند شبکه داده‌های اطلاعاتی، ارتباط راه دور، انرژی، حمل و نقل، بانکداری، خدمات اضطراری و دولتی و... از طرق مختلف انجام می‌گیرد. این اقدام نوعی اقدام تروریستی بوده و بسیاری از ناظران معتقدند که عرصه اصلی حملات هکرها در آینده همین بخشها خواهد بود (جی کاپ ۱۳۸۳: ص ۶۷).

مرکز مطالعات راهبردی کانادا در گزارش ۱۹۹۹ خود تحت عنوان جنگ سایبرنتیک ضمن اعلام ضعیف بودن تمهیدات موجود آمریکا در شبکه‌های اینترنتی کشور اعلام می‌دارد که تنها بیست نفر هکر حرفه‌ای در امور رایانه با قرار گرفتن در محل‌های مناسب و صرف بودجه‌ای معادل ۱۰ میلیون دلار می‌توانند آمریکا را زمین گیر کنند.

نمونه‌هایی از اقدامات هکرها

– خاخام آبراهام کوپر جانشین مرکز سیمون در لوس آنجلس با اعلام اینکه سایت لابی اسرائیلی در سال ۱۳۸۵ مورد هک قرار گرفته آن را مهمترین مسئله این سایت لابی‌های پشتیبان رژیم صهیونیستی اعلام کرد.

– روزنامه هاآرتص چاپ رژیم صهیونیستی: هکرهای ایرانی در ماههای اخیر سعی کرده‌اند به رایانه‌های شرکت برق این رژیم نفوذ و درتوزیع برق اختلال ایجاد کنند.

– در سال‌های ۲۰۰۰ و ۲۰۰۱ یک نوجوان ۱۲ ساله، سایت آمریکایی را مورد حمله قرار داده و بیش از ۲/۷ میلیارد دلار به آنها خسارت وارد نموده است.

– در سال ۲۰۰۰ میلادی یک گروه هکر رژیم صهیونیستی سایت حزب اللّه لبنان را مورد حمله قرار داده و پرچم و سرود ملی اسرائیل را روی آن قرار دادند. در مقابل حزب اللّه وب سایت اصلی دولت رژیم صهیونیستی را در یک پاتک مورد هجوم قرار داده و برای مدت چند روز آن را مختل نمود.

هکرها

در دنیای امروز هکرها هم در پالایش اطلاعات و هم در مختل نمودن سامانه‌های رایانه به عنوان نیروهایی هستند که می‌توانند کیلومترها دور از صحنه عملیاتی، بیشترین نتیجه و اثر گذاری را به ارمغان آورند.

این افراد، متخصصین خبره‌ای هستند که در حوزه نرم‌افزار و سخت‌افزار رایانه دارای توانایی ذهنی و عملی بالایی بوده و با ورود غیر قانونی به سامانه‌های رایانه‌ای به ربایش اطلاعات و یا تغییر، تحریف و حذف آنها اقدام می‌نمایند. در حال حاضر هکرها از مهمترین بازیگران جنگهای سایبری بوده و تعدادی از ارتشهای پیشرفته جهان به منظور تفوق در این صحنه اقدام به جذب و آموزش هکرها نموده و به صورت پنهان، زمینه مانور را برای انجام عملیات در کشورهای هدف فراهم می‌نمایند.

در این زمینه حتی برای هکرهای مورد نظر تلاش می‌کنند نیروهای هکری را خارج از کشور خود و در سایر کشورها مستقر نمایند.

هک و اهداف آن

به هر نوع نفوذی که در یک سامانه امنیتی شبکه رایانه‌ای و یا دیتا سنتر انجام می‌گیرد، به نوعی هک گفته می‌شود. البته نفوذ می‌تواند ورود به سامانه اطلاعاتی باشد یا ممکن است نفوذ جلوتر رفته و بخشی از اطلاعات رایانه را مورد حمله قرار داده و نابود کند. به میزان نفوذ انجام شده مدیریت وب سایت یا سامانه شبکه رایانه‌ای را در دست گرفته و کاربر واقعی را دچار مشکل می‌کند.

از اهداف هکرهای غیر حرفه‌ای می‌توان به موارد ذیل اشاره نمود:

۱- دستیابی به اطلاعات و اسناد و مدارک موجود رایانه‌های مورد نظر

۲- اعلان ضعف امنیت شبکه رایانه‌ای

۳- دستیابی به اموال مجازی افراد یا شرکتها

۴- انتقام شخصی، گروهی، سازمانی و یا کشوری

۵- اعلام توانایی و تسلط بر فناوری اطلاعات

انواع نفوذگران رایانه

هکرها را می‌توان بر اساس نوع فعالیت و دانش به پنج گروه تقسیم‌بندی نمود:

۱- هکرهای کلاه سفید (Hacker)

به این گروه هکرهای سامورایی یا هکرهای واقعی گفته می‌شود. هکرهای کلاه سفید متخصصان رایانه و آشنا به فناوری اطلاعات بوده و هدف آنها از نفوذ به سامانه‌های رایانه‌ای، کشف عیوب امنیتی در سامانه و بر طرف نمودن آنهاست نه سوء استفاده. به عبارت دیگر کلاه سفیدها برای این کار باید مانندهکرهای کلاه سیاه عمل کنند تا ضعفهای سامانه را بپوشانند. در حال حاضر بسیاری از شرکتها از این هکرها برای کنترل سامانه‌های رایانه‌ای خود استفاده می‌کنند. در حقیقت با انجام این اقدام میزان توانمندی پدافند غیر عامل شبکه‌های خودی و نقاط ضعف را مورد ارزیابی قرارمی دهند.

۲- هکرهای کلاه سیاه (Wacker)

از نظر کاری این هکرها دقیقاً عکس هکرهای کلاه سفید عمل می‌کنند. بدین معنی که هدف آنها نفوذ به سامانه‌های رایانه‌ای و سوء استفاده از اطلاعات است. این گروه بیشترین آسیب را به سامانه‌های رایانه‌ای وارد می‌کنند که بی سابقه‌ترین و بزرگترین حمله توسط این گروه از هکرها در تاریخ ۲۱ اکتبر سال ۲۰۰۲ ساعت ۴ بعد از ظهر به وقت آمریکا رخ داد. این حمله که نوع DDOS بود بر روی ۱۳ سرور اصلی اینترنت صورت گرفت. در این حمله ۹ سرور به طور کامل از کار افتاد. اهمیت موضوع آنقدر بود که کاخ سفید موضع‌گیری کرده و آن را حمله تروریستی مجازی نامید.

۳- قفل باز کن (Cracker)

از نظر ماهیت کار این گروه جزء کلاه سیاه‌ها می‌باشد. فعالیت این گروه در مورد نرم‌افزارها و سامانه‌های رایانه‌ای می‌باشد که دارای قفل بوده و به صورت مجانی و یا اختصاصی مورد استفاده قرار می‌گیرد. فعالیت این گروه در حوزه نرم‌افزار بسیار گسترده می‌باشد.

۴- پراکر (Preacker)

این گروه در واقع از نسلهای اولیه هکرها بوده که برای کارشناسان نیاز به رایانه نداشتند و هدف آنها اغلب نفوذ به خطوط تلفن برای تماس مجانی استراق سمع و... بود.

۵- هکرهای جوان (Scriptkiddies)

این گروه از هکرها با سایر گروههای هک تفاوت دارند و هکرهای جوان بر خلاف سایر هکرها که ابزار و برنامه‌های مورد نیاز را خودشان می‌نویسند و برای هک از معلومات خود استفاده می‌کنند، با استفاده از برنامه‌های خدماتی ویژه هک که به وسیله دیگران نوشته شده و به راحتی از طریق اینترنت و یا فروشگاهها قابل تهیه می‌باشد به سامانه‌های رایانه‌ای خسارت می‌زنند.

این گروه بیشتر با هدف سرگرمی و یا اثبات برتری خود به دوستان و همتایان اقدام به این کار می‌نمایند. بسیاری کارشناسان معتقدند که ظهور رو به رشد هکرهای جوان مهمترین تهدید برای امنیت سامانه‌های رایانه‌ای است زیرا با وجود ابزارهای موجود در اختیار این گروه و نیز وقتی که این گروه از هکرها صرف می‌کنند از کارانداختن سامانه‌های رایانه‌ای و یا نفوذ به شبکه نیاز به داشتن اطلاعات کامل در مورد رایانه ندارد.

توانایی مانور هکرها

جنگ اطلاعاتی صرفاً محدود به دستیابی به اطلاعات دشمن نیست بلکه تخریب سامانه‌های اطلاعاتی و فرآیندهای پردازشی اطلاعات پایه‌ای از مهمترین ارکان این جنگ است. شبکه‌های اطلاعاتی کنونی در سامانه‌های رایانه‌ای به هم مربوط می‌شوند و حفظ شبکه از ورود کاربرهای غیر مجاز و حضور آنها در شبکه‌های اطلاعاتی به یک معضل جدی در فناوری اطلاعات و حفظ سامانه‌های اطلاعاتی بدل گردیده است. این کاربردهای غیر مجاز که امروزه در سامانه‌های اطلاعاتی و رایانه‌ای به هکرها معروفند به دو گروه تقسیم می‌گردند: هکرهای منفرد یا آماتور و هکرهای سازمانی یا حرفه‌ای.

هکرهای آماتور درصدد هستند تا تخریب سامانه‌ها و فرآیندهای اطلاعاتی را هدف قرار داده و بگونه‌ای عمل کنند که نحوه دسترسی به سامانه‌های اطلاعاتی را محفوظ نگاه دارند. آنها می‌کوشند تا با ورود به سامانه‌ها و تخریب فعالیت‌های اطلاعاتی دولتها و سامانه‌های تجاری، اهداف منفعت طلبانه خود را پیگیری نمایند. این اعمال در اصطلاح به جرایم رایانه‌ای و ارتباطاتی معروفند.

هکرهای حرفه‌ای هم در انگیزه و هم در نوع فعالیت با هکرهای آماتور تفاوت دارند. این هکرها که بیشتر درچارچوب سامانه‌های حکومتی و یا گروهها و سازمان‌های پنهان تعریف می‌شوند این نوع فعالیت را جنگ تلقی و در ارتکاب به آن اهداف وسیعتر و بزرگتری را دنبال می‌کنند. این هکرها بجز دستیابی به اطلاعات و سامانه‌های اطلاعاتی دشمن علاقه وافری به نحوهٔ سامانه‌های پردازشی دراطلاعات آشکار و پنهان دشمن دارند و حوزه

فعالیت این نوع هکرها غالب موضوعات امنیتی و دفاعی را در بر می‌گیرد. همکاریهای فردی و سازمانی با شناسایی شبکه‌های اطلاعاتی می‌کوشند تا به منظور دستیابی به اطلاعات تصمیم‌گیری مدار مصرف و تولید اطلاعات را کشف کنند. این مدار می‌تواند موجب شناخت یک ارتباط سازمانی شده و متغیرهای زیر را در اختیار قرا دهد:

۱- نیازهای اطلاعاتی تصمیم‌گیرندگان

این نیازها حوزه فعالیتی و علاقمندی تصمیم‌گیرندگان را نشان و از سوی دیگر این افراد به عنوان مصرف کنندگان اطلاعاتی می‌کوشند مستقیم‌ترین اطلاعات مربوط به طرحها و جزئیات و تفصیلات آنها را در دست داشته باشند.

سامانه‌های حفاظتی اطلاعاتی شبکه‌ای این پدیده را به عنوان خطرناک‌ترین مرحله کشف طرحهای سری مورد نظر قرار می‌دهند اما اجبار در جمع آوری اطلاعاتی همیشه موجب آسیب پذیری‌های متفاوتی در سطوح گوناگون می‌گردد.

۲- شیوه‌های کشف دسترسی به رفع این نیازها

سیر و سفرهای اطلاعاتی در شبکه‌ها و سامانه‌های ارتباطی و جمع آوری اجزای اطلاعات، اطلاعات و منابع بیشتری جهت رفه نیاز در اختیار تصمیم‌گیرندگان خواهند گذاشت. در مقابل متخصصان رایانه‌ای علاقه وافری دارند تا از طریق بررسی شیوه این سیر و سفرها بتوانند نوع برآورد کردن نیازهای اطلاعاتی تصمیم گیرندگان را دریابند.

۳- ارتباط ارگانیک و سیستماتیک تولید - مصرف اطلاعاتی

سومین متغیری که می‌تواند در شبکه‌های آشکار اطلاعاتی در اختیار هکرهای حرفه‌ای قرار گیرد کشف ارتباطات منطقی و سیستماتیک در مدار تولید - مصرف اطلاعاتی است. ارزیابی اطلاعات خام در جمع آوریهای آشکار اطلاعاتی همواره از مهمترین مراحل است ولی در این مرحله هکر خود دیگر به تنهایی نمی‌تواند ارتباط سیستماتیک میان تولید و مصرف را به راحتی پیش بینی و ارزیابی کند. لذت هکر با در اختیار گذاشتن این ارتباط از بررسی کننده اطلاعات کمک می‌گیرد تا ارزیابی واقعی را بدست آورد. کشف ارتباط منطقی بین اجزا در موارد اطلاعاتی هر چند که به ارزیابی اطلاعاتی جزئی‌تر بستگی دارد اما از دیگر مزایای آن این است که از وجود شبکه‌های آشکار نیز به راحتی استفاده می‌کنند. در حوزه دفاعی مباحث مربوط به خریدهای تسلیحاتی، صنایع نظری، توان تجهیزاتی، علاقه‌مندی‌های مطالعاتی و بررسی‌های تحقیقاتی می‌تواند مورد ارزیابی اطلاعات خام قرار گیرند و به کشف مدار سیستماتیک تولید - مصرف اطلاعاتی تا اندازه زیادی کمک می‌کنند. گاهی این هکرها در سطوح بالاتری قرار دارند بگونه‌ای که خود می‌توانند به جز یافتن شیوه‌هایی برای کسب اطلاعات نظیر اطلاعات جزئی‌تر، به کشف ارتباطات سیستماتیک نیز نایل شوند. این افراد را به عنوان جنگجویان حرفه‌ای رایانه‌ای، یا سربازان مزدور رایانه‌ای تعبیر می‌نمایند زیرا اغلب آنها صرفاً به منظور دسترسی به پول بیشتر تجربیات و تخصص خود را در اختیار سازمانها و دولت‌های دیگر قرار می‌دهند. این سربازان مزدور رایانه‌ای که دارای تخصصهای گوناگون هستند با ایجاد یک شبکه تخصصی می‌توانند به یک سامانه ارزیابی دقیق تبدیل گردند. عمده این افراد از کنار گذاشته شدگان سامانه‌های اطلاعاتی در جهان یا مؤسسات علمی هستند و بسیاری از آنها متخصصان رایانه‌ای در کشورهایی مانند روسیه، بلغارستان و... بوده‌اند که امتیازات ویژه خود را از دست داده‌اند.

محققان بررسی‌های اطلاعات این افراد را تهدیدی جدی برای امنیت ملی محسوب می‌نمایند.

عمق نفوذ و دسترسی آنها به اطلاعات حوزه دفاع، حدو حصر معینی ندارد و بیشتر به یک جنگ اطلاعاتی شبیه است. از سویی دستیابی به اطلاعات و تحلیل و ارزیابی تنها تهدید در حوزه دفاع نبوده و تخریب سامانه‌ها نیز از تهدیدات جدی به شمار می‌رود. کشف و سپس تخریب سامانه‌های اطلاعاتی که پیوسته در حال جمع آوری اطلاعات است، امروزه به یک جنگ جدی مبدل گردیده است. این جنگها که بیشتر در حوزه نرم‌افزاری مورد بررسی قرار می‌گیرند موضوعی را موسوم به «جنگ اطلاعاتی نرم‌افزاری» به وجود آورده‌اند. این نوع جنگ شامل فعالیت‌هایی است که جنگجویان اطلاعاتی برای هجوم یا نفوذ به شبکه‌های خاص اطلاعاتی به منظور تخریب سامانه‌ها وکارکردهای نرم‌افزاری آنها انجام می‌دهند.

نقش هکرها در حوزه سایبری

جنگ اطلاعاتی نظامی را در حوزه سایبری باید در زمینه‌های نفوذ و تخریب در سامانه‌های نظامی بررسی کرد. از آنجاکه امروزه فضای مدیریت راهبردی در حوزه نظامی را با پنج رکن فرماندهی، کنترل، ارتباطات، رایانه و اطلاعات ترسیم می‌کنند، این فضا به نحو مناسبی به سبب وابستگی بسیار به شبکه‌های رایانه‌ای از یک سو و اهمیت اطلاعات از سوی دیگر آسیب پذیریهای جدی را در برابر یورشهای هکرهای اطلاعاتی نشان می‌دهد. موفقیت در صحنه اجرای این فرماندهی به مثابه موفقیت در یک میدان نبرد تلقی خواهد شد. دارا بودن یک شبکه مناسب اطلاعاتی می‌تواند در حداقل زمان حداکثر ارتباطات را برقرار و بالاترین حجم اطلاعاتی را مبادله نماید. اهمیت این رکن و سایر ارکان را می‌توان با نقش سامانه‌های عصبی و ارتباطی آنها با سامانه‌های دفاعی بدن تشبیه کرد. هکرهای فعال در جنگ اطلاعاتی که به این نوع جنگ به منزله جنگ اصیل و واقعی می‌نگرند و در پی بهره برداری حداکثر از آسیب‌های این فضای مدیریتی و فرماندهی هستند.

هکرهای اطلاعاتی در جنگ‌های اطلاعاتی، آنچه را که در یک نظام اطلاعاتی از اهمیت خاصی برخوردار است با دست یا زیدن به نفوذ بدست می‌آورند و تا حداکثر بهره برداری از آن پیش می‌روند و سپس به تخریب آن می‌پردازند. برخی کارشناسان امور اطلاعاتی شیوه‌های بکارگیری جنگ اطلاعاتی را برای هکرهای اطلاعاتی در سه مقوله تعریف کرده‌اند. مقوله اول به کار بردن شیوه‌های نوین در حوزه فعالیت‌های قدیمی، مقوله دوم: بکار بردن شیوه‌های قدیمی در حوزه فعالیت جدید و شیوه سوم بکارگیری

شیوه‌های نوین در عرصه فعالیت‌ها و کنش و واکنشهای جدید است. مفهوم بکارگیری شیوه‌های نوین در عرصه فعالیت‌های جدید و قدیمی بکارگیری همان روش هایی است که در برخوردهای اطلاعاتی در چارچوب مفهوم قدیم و جدید مطرح است.جمع آوری اطلاعاتی با سرقت‌های اقتصادی و ایجاد ارتباط وسیع و استفاده از این نوع ابزار برای جنگهای روانی و تبلیغاتی را امروزه در مقوله اول و به مثابه روش‌های نوین در حوزه جنگهای اطلاعاتی طبقه بندی می‌کنند. استفاده هکرهای اطلاعاتی از شبکه‌های اطلاعاتی در حوزه آسیب رسانی فیزیکی به سامانه‌ها در مقوله دوم یعنی به بکار بردن روش‌های قدیمی در حوزه فعالیت‌های جدید طبقه بندی می‌شوند. اما مهمتر از همه دست یازیدن به جنگ اطلاعاتی هجومی در حوزهٔ نظامی به شیوه مندرج در مقوله سوم یعنی بکارگیری شیوه‌های نوین در عرصه فعالیت‌های جدید است. در مقوله سوم می‌توان از بکارگیری فنون و روشهای دیجیتالی علیه فعالیت‌های اطلاعاتی یک هدف نام برد. حوزه نظامی گری که در آن، اعمال فرماندهی و کنترل نسبت خاصی با ارتباطات و اطلاعات پیدا کرده است به همان اندازه که این ارتباط را می‌توان مغتنم شمرد باید آن را به عنوان یک آسیب پذیری جدی در مقابل روش‌های اطلاعاتی هجومی تلقی کرد. هکرها که از شبکه‌ها به عنوان کانال‌های ورود و خروج استفاده می‌کنند در مرحله نفوذ به سامانه‌های نظامی و آسیب رسانی به آنها اهداف ذیل را دنبال می‌کنند.

الف) بررسی و برآورد توان اطلاعاتی در طرح ریزی و ارزیابی اطلاعاتی راهبردی

ب) بررسی و برآورد توان اجرایی در حفظ و مراقبت از تأسیسات و سامانه‌های خودی

ج) بررسی و برآورد توان تهاجمی در اجرای ضربات مهلک بر دشمن

د) بررسی و برآورد توان ارتباطی در ایجاد شبکه‌های متناسب ارتباطی در حال جنگ و صلح

هکرهای اطلاعاتی در جنگ خود پس از بررسی موارد مورد نیاز درصدد بهره برداری از این بررسی‌ها بر می‌آیند و با تمسک به روش‌های تخلیه‌های اطلاعاتی تا آن‌جا که ممکن است حوزه نفوذ خود راگسترش می‌دهند. این مرحله خود ضربه اساسی به پیکره هر سامانه نظامی وارد می‌کند و در صورت استمرار نفوذ در این حوزه می‌تواند به مرحله تخریب سامانه‌ای بیانجامد. تروریست‌ها در مرحله اول به آسیب رسانی به سامانه‌های اطلاعاتی و اطلاعات نظامی مبادرت می‌ورزند. در مرحله دوم سازمان یا فرد نفوذ کننده با داشتن برآوردی از توان تهاجمی و در اختیار گذاری توان به دشمنان و یا بررسی عملیات تهاجمی علیه این تسهیلات و امکانات می‌تواند درجنگ چریکی ضربه را جایی وارد سازد که با کمترین تلفات مفاصل راهبردی هر سامانه نظامی را جدا کند. در مرحله سوم هکرهای اطلاعاتی در جنگ خود با شناسایی ارتباطی و طبقه بندی آنها از نظر راهبردی در یک سامانه نظامی دست یافته و این توان را در حین عملیات نظامی، رزم منطقه‌ای و... محک می‌زنند هکرهای اطلاعاتی در مرحله نفوذ با وارد شدن در این شبکه‌ها در مناطق خاصی از این شبکه‌ها کمین و در فرصت مناسب و با استفاده از زمانهای غافلگیر کننده و به وسیله ایجاد ارتباط‌های ساختگی قطع ارتباطات کلیدی و مهم و تعریف چارچوبهای اطلاعاتی جدید به نحوی غافلگیر کننده ضربات اساسی خود را وارد می‌کنند. انجام مجموعه عملیات شبکه‌ای و گسترده از زمان‌های بسیار پیش از انجام عملیات نظامی فرصتی را به وجود آورده که از رهگذر آن هکرهای اطلاعاتی یک جنگ شبکه‌ای منظم را سامان و سازمان می‌دهند. ارزیابی مداوم توان ارتباطی شبکه‌ای ایجاد یک بستر مناسب برای آسیب رسانی به موقع به این شبکه و در عین حال حضور و ورود به صحنه و میدان این ارتباطات می‌تواند بگونه‌ای مؤثر، تأثیر این ضربات وارده را دو چندان سازد.

جنگ هکرها در جریان حمله آمریکا به عراق در سال ۲۰۰۳

هم زمان با حمله آمریکا و انگلیس و حتی پیش از آن موجی از جنگ دیجیتالی آغاز و فعالیت گسترده نفوذ گران و خرابکاری شبکه رایانه‌ای را به یکی دیگر از تبعات این جنگ بدل کرد. خبرگزاری رویتر گزارش داد حملات مخرب به سایت‌ها و شبکه‌های رایانه‌ای دست کمی از حملات نظامی و فیزیکی به مواضع خاکی نیروی مهاجم عراق ندارد. و این جلوه روشنی از جنگ دیجیتال در عصر نوین بود. این تهاجم به طرز سرسام آوری شدت یافت و تعداد سایت‌هایی راکه فعالیتشان مختل می‌شد از شمارش خارج کرد.

شبکه امنیتی zone-h در ستونی که حملات تخریبی هکرها را علیه وب سایت‌ها ردیابی و ثبت می‌کند حملات بسیاری راکه به بیش از ۲۰ هزار سایت اینترنتی ثبت کرد اکثر این اقدامات به ازکار افتادن وب سایت‌ها منجر و روزانه ۲۵۰۰ حمله هکرها در ارتباط با جنگ از منابع دولتی آمریکا و انگلیس گزارش می‌شد. طبق اعلام BBC از زمان آغاز حمله به عراق آمار نفوذ به سایت‌های دولتی رشد چشمگیری داشته و در این میان سایتهای اسرائیلی از اهداف اصلی مهاجمان بود. هکرهای فعال در طول این جنگ را می‌توان به گروه‌های زیر تقسیم کرد:

گروه اول: هکرهای آمریکایی که به پست الکترونیکی سفارتخانه‌های عراق و سایت‌های وابسته به این کشور حمله می‌کردند.

گروه دوم: گروه‌های مخالف جنگ که در سراسر جهان به منظور مبارزه با آمریکا به سایت‌های آمریکایی حمله می‌کردند.

گروه سوم: هکرهایی که به سایت‌های منتشره کننده مطالب و اخبار مخالف با سیاست آمریکا حمله می‌کردند.

گروه چهارم: گروههای طرفدار صلح که فقط علیه جنگ فعالیت داشته و به اقداماتی نظیر انتشار ویروس دست می‌زدند. ویروسهای LIOTEN یا VOTE.D, CANADA – IRAQ – OIL از ویروسهای مرتبط با جنگ عراق بودند. اما آنچه بیش از همه در خبرها به آن پرداخته شده حمله چند باره نفوذ گران آمریکایی به نام «میلیشای آزادی بخش ارتش سایبر» به سایت اینترنتی شبکه تلویزیون و ماهواره الجزیره قطر بود. این سایت قربانی حمله‌ای به نام Denial of Service شد. شبکه‌ای با پخش تصاویر سربازان کشته شده و اسرای انگلیسی و آمریکایی خود را بر سر زبان‌ها انداخت. با

گذشت چند روز از حمله به این سایت بخش انگلیسی زبان آن هنوز آماده بازدید کاربران نبود.

الجزیره در جریان جنگ عراق بخش انگلیسی زبان سایت خود را نیز راه اندازی کرد اما درست در اولین روز افتتاح نفوذگران فعالیت آن را متوقف کردند. در حالیکه کاربران اینترنت با شنیدن خبر افتتاح این بخش به سایت هجوم آورده بودند، هرها با مجموعه بی شماری از پستهای الکترونیکی ناخواسته سایت را هدف قرار دادند. بازدید کنندگان از این سایت یا به سایت‌هایی هدایت می‌شدند که پیغامهایی در طرفداری از آمریکا فرستاده می‌شد یا سایتهایی را مشاهده می‌کردند که در آنها تصویر و پرچم آمریکا با نوشته‌ای به این مضمون که: «اجازه دهید طنین انداز شود» دیده می‌شد و یا به سمت سایت‌های با محتوای پورنوگرافی منحرف می‌شدند. به گفته تحلیلگران هک شدن این سایت به دلیل پوشش ویدئویی وضعیت جنگ از جمله تصاویری از سربازان کشته شده یا اسیر آمریکایی بود. کلیپها، فایلهای صوتی و تصویری کم حجم و قابل دانلود مناسب تصاویر و نوشته‌هایی جذاب و مبتنی بر اصول ژورنالیسم الکترونیک این سایت منجر شد تا سایت این شبکه از حجم بالای مخاطبان خاص و عام برخوردار شود. (خرازی ۱۳۸۲:ص ۹۵).

همگرایی و ارتباط

هکرها عموماً افرادی با روحیه تقریباً انزوا گرا بوده و اقدام آنها حالت فردیت دارند و تجمع‌ها و ارتباط آنها به دلیل تعارض این فعالیت‌ها با قوانین موجود دارای جنبه پنهان است لیکن آنها دارای جلساتی به ویژه به صورت منطقه‌ای می‌باشند.

در اولین نشست هکرها تحت عنوان دفکان در سال ۱۹۹۲ تعداد ۱۵۰ نفر ولی در سال ۲۰۰۱، حدود ۶۲۰۰ نفر حضور داشتند. در این همایش علاوه بر هکرها، ویروس نویسان و کارشناسان امنیتی به منظور بررسی برنامه‌ها، معماری شبکه و شناسایی ساز و کارهای امنیتی و تعدادی از عناصر FBI و CIA و دیگر سازمان‌های امنیتی حضور داشته‌اند.

مهمترین نواقص و موارد رایج در هک نمودن سایت‌ها

۱- *Cross Site Scripting* یا *XSS* (اضافه نمودن فایلهای آغازگر به سایت)

این مشکل زمانی ایجاد می‌شود که اطلاعات ارسالی بین کاربران و سایت بدون بررسی و اعتبار سنجی لازم توسط نرم‌افزار سایت صورت گیرد. در این حالت هکرها می‌توانند اسکریپتهایی را همراه اطلاعات به نرم‌افزار سایت تزریق کنند و این اسکریپتها هنگام نمایش اطلاعات در مرورگر دیگر کاربران سایت اجرا شده و مشکلاتی همچون سرقت اطلاعات نشست (Session) و دسترسی به اختیارات و اطلاعات دیگر کاربران و یا تغییر در صفحات سایت را ایجاد کند.

۲- *Injection Flaws* (درج نقص و نقیضه)

در این شیوه هکر به همراه بخشی از اطلاعات یا پارامترهای ارسالی به سایت دستورات غیر مجازی که امکان خواندن، تغییر یا حذف یا درج اطلاعات جدید را فراهم می‌کند نیز تزریق می‌نماید. یکی از معمول‌ترین این روشها Injection SQL است که امکان تغییر در اطلاعات و جداول بانک اطلاعاتی یا تغییر در در خواست‌ها از بانک اطلاعات (مانند تعیین اعتبار کاربر و کلمه) را امکان‌پذیر می‌کند.

۳- *Malicious File Execution* (اجرای فایلهای معاند)

این مسئله به هکرها اجازه اجرای برنامه یا کدی را می‌دهد که امکاناتی در تغییرات یا مشاهده اطلاعات یا حتی تحت کنترل گرفتن کل نرم‌افزار سایت یا سیستم را می‌دهد. این مشکل در سایت‌های که امکان ارسال فایل به کاربران بدون بررسی ماهیت اطلاعات را می‌دهد اتفاق می‌افتد (مثلاً ارسال یک اسکریپت ASP [۸] یا PHP [۹] به جای فایل تصویری توسط کاربر)

۴- *Insecure direct object reference* (عدم‌امنیت‌درمراجعه‌مستقیم‌به‌موضوع)

این مشکل عموماً در دستکاری پارامترهای ارسالی به صفحات یا اطلاعات فرم هایی هست که به صورت مستقیم به فایل، جداول اطلاعاتی، فهرست‌ها یا اطلاعات کلیدی اتفاق می‌افتد و امکان دسترسی یا تغییر فایلهای اطلاعاتی دیگر کاربران را ایجاد می‌کند. (مانند ارسال کد کاربر یا نام فایل مخصوص او به صورت پارامتر در آدرس صفحه که با تغییر در اطلاعات کاربر دیگری وجود خواهد داشت).

۵- *Cross Site Request forgery* (درخواست‌های جعلی از سایت)

در این گونه حملات هکر کنترل مرورگر قربانی را بدست آورده و زمانی که وی وارد سایت (Login) می‌شود درخواستهای نادرستی را به سایت ارسال می‌کند. (نمونه آن چندی پیش در سایت Myspace اتفاق افتاده بود و هکری با استفاده از یک کرم اینترنتی پیغامی را در میلیون‌ها صفحه کاربران این سایت نمایش داد)

۶- *Information leakage and improper error handling* (بررسی خطای اطلاعات پراکنده و نا مناسب)

همان طور که از نام این مشکل مشخص است زمانی که خطاهای نرم‌افزار سایت به شکل مناسبی مدیریت نشوند، در صفحات خطا اطلاعات مهمی نمایش داده می‌شود که امکان سوء استفاده از آنها وجود داشته باشد. (نمونه از همین مشکل چندی پیش برای یکی از سایتهای فارسی نیز به وجود آمد و اطلاعات کاربری و کلمه عبور اتصال به بانک اطلاعات در زمان خطا نمایش داده می‌شد و باعث سوء استفاده و تغییر اطلاعات کاربران این سایت شد)

۷- *Broken Authentication and Session Management* (شکست اعتبار و مدیریت استاندارد *OSI / OS* [۱۰])

این مشکل در زمانی که نشست کاربر (Session) و اطلاعات مربوط به ورود کاربر به دلایلی به سرقت می‌رود یا به دلیلی نیمه کاره رها می‌شود ایجاد می‌گردد. یکی از شیوه‌های جلوگیری از این مشکل رمز نگاری

اطلاعات و استفاده از SSL[11] است.

۸- *Insecure Cryptographic Storage* (عدم امنیت در کدهای رمزگشایی ذخیره‌شده)

این مشکل نیز چنانچه از عنوان آن مشخص است به دلیل اشتباه در رمز نگاری اطلاعات مهم (استفاده از کلید رمز ساده یا عدم رمز نگاری اطلاعات کلیدی) می‌باشد.

۹- *Insecure Communications* (نا امنی ارتباطی)

ارتباط نا امن نیز مانند مشکل قبلی است با این تفاوت که در لایه ارتباطات شبکه است. هکر در شرایطی می‌تواند اطلاعات در حال انتقال در شبکه را مشاهده کند و از این طریق به اطلاعات مهم نیز دست پیدا کند. همانند مشکل قبلی نیز استفاده از شیوه‌های رمزنگاری و SSL راه حل این مشکل است.

۱۰- *URL access Failure to Restrict*[12] (دستیابی افراد غیر مجاز به URL)

برخی از صفحات سایت‌ها (مانندصفحات‌بخش‌مدیریت‌سایت)می‌بایست تنها در اختیار کاربرانی با دسترسی خاص باشند. اگر دسترسی به این صفحات و پارامترهای ارسالی آنها به شکل مناسبی حفاظت نشده باشد ممکن است هکرها آدرس این صفحات را حدس بزنند و به نحوی به آنها دسترسی پیدا کنند.

انواع تهدیدات

در کل، تهدیدات به دو دسته تهدیدات طبیعی و انسان ساز تقسیم می‌گردند. (نگاره ۲)

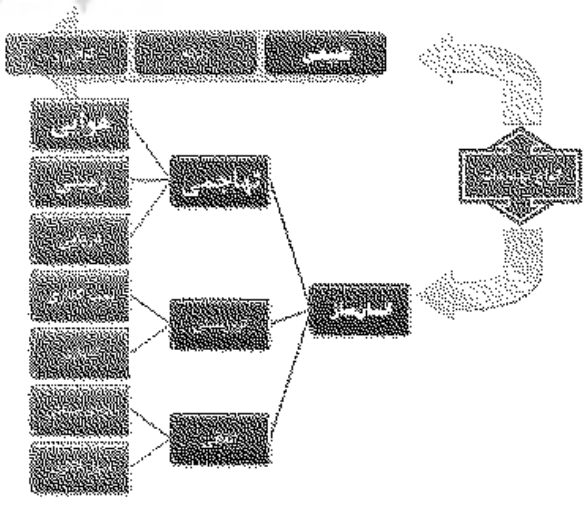
تهدیدات طبیعی شامل سیل و زلزله و توفان و.. می‌باشد که مشمول مقررات این مبحث نمی‌گردد. به این تهدیدات در مباحث دیگر مقررات ملی ساختمان به صورت مناسب پرداخته شده است.

تهدیدات انسان ساز نیز به سه دسته تقسیم می‌گردد:

۱- تهدیدات نظامی

۲- تهدیدات تروریستی

۳- تهدیدات اتفاقی



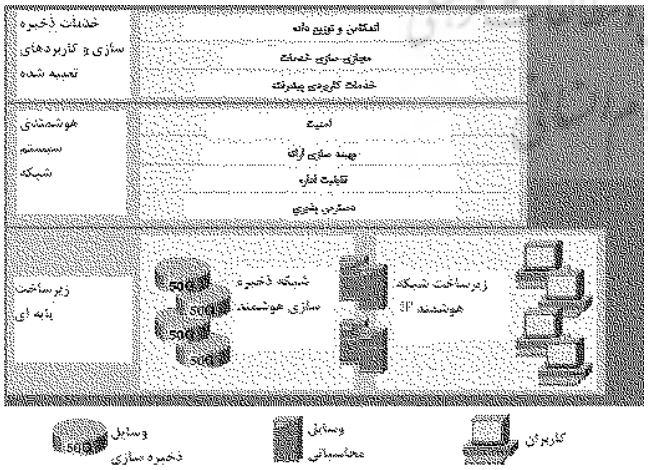
نگاره ۲: انواع تهدیدات

امنیت اطلاعات و برنامه‌های کاربردی

امنیت اطلاعات و برنامه‌های کاربردی نیز از طریق سرویس‌های مراکز داده فراهم می‌شود. امنیت اطلاعات در مراکز داده به معنای حفظ محرمانگی، یکپارچگی و در دسترس بودن اطلاعاتی است که در مزرعه‌های سرور ذخیره شده است. این امنیت با کاهش اثرات حملات به سرورها، برنامه‌های کاربردی، سیستم‌های ذخیره سازی اطلاعات و زیر ساخت شبکه، توسط سیستم‌های حفاظتی طراحی و تأمین می‌گردد. با توجه به این نکته که ترکیب فضاها در مراکز داده نسل جدید ساختار امنیتی مناسب و مستحکم‌تری را می‌طلبد، سیستم‌های نرم‌افزاری و سخت‌افزاری بسیار پیشرفته‌تر از سیستم‌های قبلی خواهند بود. به طور کلی امنیت در مراکز داده نسل جدید، در سه لایه سرورهای برنامه‌های کاربردی، اطلاعات و زیر ساخت پیاده سازی می‌شود.

امنیت در سرورها و برنامه‌های کاربردی

امنیت سرورها و برنامه‌های کاربردی در مراکز داده شامل تقسیم کردن سرورهای مختلف در لایه کاربرد[13] در مزرعه‌های سرور، محافظت در برابر عدم ارائه سرویس[14]، عدم ارائه سرویس به صورت توزیع شده[15] و حفاظت و تشخیص تهاجم و حفاظت در برابر انواع ویروس‌های شبکه می‌باشد. برای پیاده سازی این امکانات امنیتی در مرکز داده، از سرویس‌های شبکه‌ای استفاده می‌شود. این سرویس‌ها با بهره مندی از امکانات یک کلاینت بر روی سرور، برنامه‌های کاربردی محیط اجرای برنامه را تحت کنترل قرار می‌دهند. این سرویس‌ها معمولاً عبارتند از: سیستم‌های IDP، IDS، ابزار پیشگیری از عدم ارائه سرویس، آنالیز ترافیک و دیواره آتش.



نگاره ۳: ساختار شبکه‌های هوشمند

حفاظت از داده‌ها

به طور کلی امنیت اطلاعات شامل محافظت اطلاعات ذخیره شده در مرکز داده می‌شود. این اطلاعات ممکن است به صورت مستقیم روی

سرورها نگهداری شوند (دستگاه‌های ذخیره سازی دسترسی مستقیم)[16] (DASD) و یا از طریق شبکه IP به شبکه‌های ذخیره سازی انتقال یابند. به هر حال، این اطلاعات باید مستقل از محیط نگهداری شان محافظت شوند. زمانی که اطلاعات در شبکه IP نگهداری می‌شود، کلید تمهیداتی که برای محافظت از سرورها لازم است، در اینجا نیز به کار گرفته می‌شوند.

در مواردی که اطلاعات در شبکه‌های ذخیره‌سازی نگهدای می‌شود، مکانیزم‌های امنیتی از طریق امنیت زیر ساخت اعمال می‌گردند. به این ترتیب که با استفاده از مکانیزم‌های تعریف ناحیه[17] احراز هویت و امنیت پورت‌های ارتباطی، راه نفوذ بسته می‌شود.

درموارد نگهداری اطلاعات در شبکه‌های ذخیره سازی و انتقال آن‌ها از طریق IP به منظور تکرار و یا انتقال به سایت پشتیبان، برای برقراری امنیت در انتقال اطلاعات تدابیر امنیتی نظیر رمزنگار و استفاده از تونل زنی در VPNها (صفحات مجازی شبکه) برای محیط انتقال اتخاذ می‌گردد.

امنیت زیر ساخت

امنیت زیر ساخت به معنای حفاظت تجهیزات و ارتباطاتی است که ترافیک را از مزرعه‌های سرور[18] خارج و یا وارد آن می‌نمایند. حفاظت تجهیزات شامل مکانیزم‌های احراز هویت در روترها، ایجاد محدودیت در ظرفیت ترافیک به منظور جلوگیری از اشباع شبکه و فیلتر کردن ترافیک ناخواسته با استفاده از امکانات Dos/DDOS[19] می‌شود. برای ایجاد امنیت بیشتر زیر ساخت در مقابل حملات و نفوذهای ناخواسته، علاوه بر استفاده از امکانات تعریف VLANهای (شبکه‌های محلی مجازی) متفاوت برای هر قسمت، در تعریف پلان‌های کنترلی، محدوده کننده‌های ترافیکی و امنیت پورت‌ها از سیاست‌های امنیتی استفاده می‌شود. برای مثال، تجهیزات برق فشار قوی (HVAC) می‌توانند عمداً یا سهواً خاموش شوند، ژنراتوری که باتری‌ها را شارژ می‌کند احتمال دارد به سرقت برود یا کنسول مدیریت هوشمند سیستم احتمالاً به اشتباه سیستم اطفای حریق را فعال سازد.

نتیجه گیری

با توجه به اهمیت اطلاعات مکان محور و اینکه تمامی امور عمرانی و توسعه‌ای و هر اقدام تاکتیکی، عملیاتی و استراتژیکی با تکیه بر این اطلاعات قابل اجرا و یا انجام خواهد بود؛ همچنین توانمندی خاص و ویژگی‌های قابل توجه هکرها و ارتباط دو جانبه و مستقیم بین کاربران و اشرافیت بر فعالیت‌های کاربران، بهره‌مندی از ابزارهای سنجش و رویکرد و تمایلات نا محدود مخاطبین و ظرفیت بسیار بالای انتقال داده‌ها از طریق اینترنت و سرعت تحولات تکنولوژیکی در عرصه نرم‌افزاری و سخت‌افزاری و بهره‌مندی عمومی از فضای سایبر، دیتا سنتر به شدت آسیب‌پذیر می‌باشند و مسئولین امر بایستی راهکارهای ویژه‌ای در حفاظت از این سایت‌های با ارزش را پیش بینی و با دقت آن را مورد توجه قرار دهند.

شایان ذکر است پیشرفت در عرصه‌های معروضه به گونه‌ای است که حتی با استفاده از یک دستگاه رایانه قابل حمل و کوچک حتی در سایر رادیوهای جیبی و تنها با استفاده از آنتن‌های نصب شده بر روی این دستگاه و بدون نیاز اتصال به شبکه اینترنت دسترسی داشته باشند دور از ذهن نبوده و این امر به معنای حذف بسیاری از محدودیت‌های در خصوص اینترنت می‌باشد. (البته اینگونه تجهیزات در سطح بسیار محدود مورد استفاده عوامل اطلاعات پنهان قرار می‌گیرد).

منابع

۱-جمالی-حمیدرضا و اسدی سعید (۱۳۸۴) سایبرنتیک چیست. تهران، ماهنامه تدبیر، شماره ۱۵۵، فروردین ۱۳۸۴.

۲-حسن پور، جعفر، سربازان جنگهای آینده، فصلنامه نگاه، شماره ۵، سال دوم، پائیز ۱۳۸۷.

۳-خرازی، رها (۱۳۸۳) جنگ دیجیتالی، زاویه دید. فصلنامه پژوهش و سنجش، سال دهم شماره ۳۴، تابستان ۱۳۸۲.

۴-کاپ جی (۱۳۸۳)، امنیت شبکه‌ها برای همه-معاونت پژوهشی دانشکده امام باقر (ع) تهران

۵-کاستلز، مانوئل (۱۳۸۰) عصر اطلاعات، اقتصاد، جامعه شبکه‌ای دانشکده امام باقر (ع) تهران.

۶-کافمن، ادوارد (۱۳۸۲) استراتژی آمریکا در جنگهای رسانه‌ای، فصلنامه عملیات روانی، شماره ۴، زمستان ۱۳۸۲، معاونت فرهنگی ستاد مشترک.

۷-کمیسیون تدوین استراتژی امنیت ملی آمریکا (۱۳۸۰)، تهران مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر.

پی نوشت

1- Data center

2- Hacker

3- Internet

4- Data Storage

5- Worm

6- TPC= Tactical Pilotage Chart

7- ONC= Operational Navigation Chart

8- Active Server Pages

9- Is a Scripting Language

10- Open Systems Interconnection

11- Solid Stage Logic

12- Uniform Resource Locators

13- Application

14- Denial of service: DOS

15- Distributed Denial of Service:DDos

16- Direct Access Storage Device

17- Zone

18- Server Farm

19- Distributed Denial of Service