تهدیدات جنگ سایبری مهمترین عنصر در جنگ ترکیبی

سید محسن صدرالساداتی[1]

چکیده

جنگ‌های آینده، جنگ‌هایی هستند که هیچ گلوله‌ای در آن شلیک نخواهد شد. بزرگترین جنگ، جنگ‌هایی است که در فضای سایبری و از طریق اینترنت و محیط دارک وب انجام می‌گیرد. جاسوسی توسط افراد جاسوس در خاک دشمن انجام نمی‌شود. با تحلیل اطلاعات بر روی داده‌ها در فضای مجازی، ایستگاه‌های راداری و ماهواره‌ای و سیگنال‌های الکترومغناتیسی دشمن به اهداف خود می‌رسد. دیگر درگیری سخت برای از کار انداختن تجهیزات صورت نمی‌پذیرد و تنها با اختلال و یا هک سامانه‌ها، مراکز داده و ... به مقصود خود می‌رسند. فاجعه‌ای که ذکر شد در عصر جدید به جنگ سایبری یا جنگ‌های نوین نامگذاری شده است. هدف این مقاله ارائه قابلیت‌های ویرانگر جنگ سایبری است، همچنین نشان دادن روش‌هایی است که ممکن است بر روی داده‌ها، ارتباطات و حفره‌های موجود امنیتی از طرف دشمن تهدید ایجاد کند و در نهایت یافتن راه‌هایی برای جلوگیری از این خطرات و آسیب‌های در حال و آینده است.

واژگان کلیدی: جاسوسی، هک، اینترنت اشیا، محاسبات و فضای ابری، ابزار امنیتی، امنیت سایبری

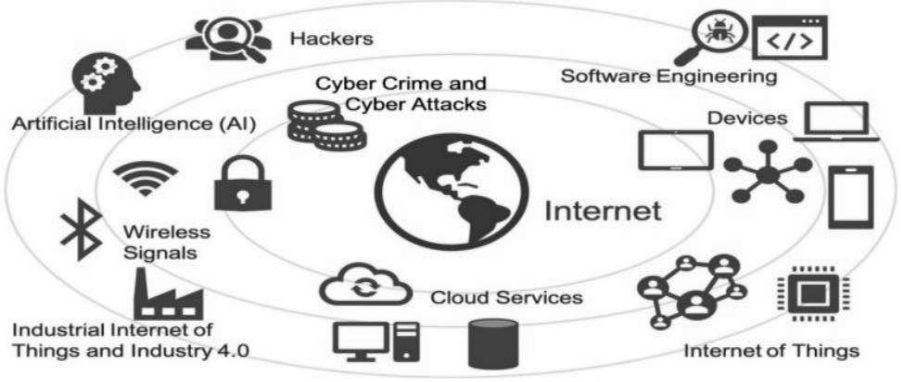
---

۱ . مدرس دانشگاه افسری و تربیت پاسداری امام حسین (ع).

مقدمه

قبل از توضیحات دیگر لازم است در مورد چگونگی اتصال همه چیز از طریق اینترنت، یا نحوه دسترسی به هر دستگاه در جهان از هر دستگاه دیگر که در نقطه‌ای دیگر از جهان قرار دارد صحبت کنیم. برخی از بخش‌هایی که به شدت وابسته به فناوری اطلاعت شده است و معمولا از طریق اینترنت به آنها متصل هستند به شرح زیر است:

۱. بانکداری و مالی (بانکداری برخط)؛
۲. فرودگاه‌ها (مدیریت ناوگان آنلاین و رزرو بلیط)؛
۳. راه آهن (اسکادا و رزرو بلیط)؛
۴. پرداخت‌های آنلاین عوارض؛
۵. دوربین‌های مداربسته؛
۶. تلفن‌های همراه (برنامه‌هایی مانند شبکه‌های اجتماعی، دسترسی به موقعیت مکانی، ایمیل و ...)؛
۷. بیمارستان‌ها؛
۸. شبکه برق؛
۹. شناسه‌های افراد و اطلاعات اشخاص؛
۱۰. تجهیزات هوشمند؛
۱۱. سامانه‌های خدمات محور
۱۲. و سایر مواردی که قابلیت اتصال به اینترنت را دارند و در اینجا مجال برای ذکر عنوانین آن نمی باشد.



شکل ۱-۱ فضای سایبری

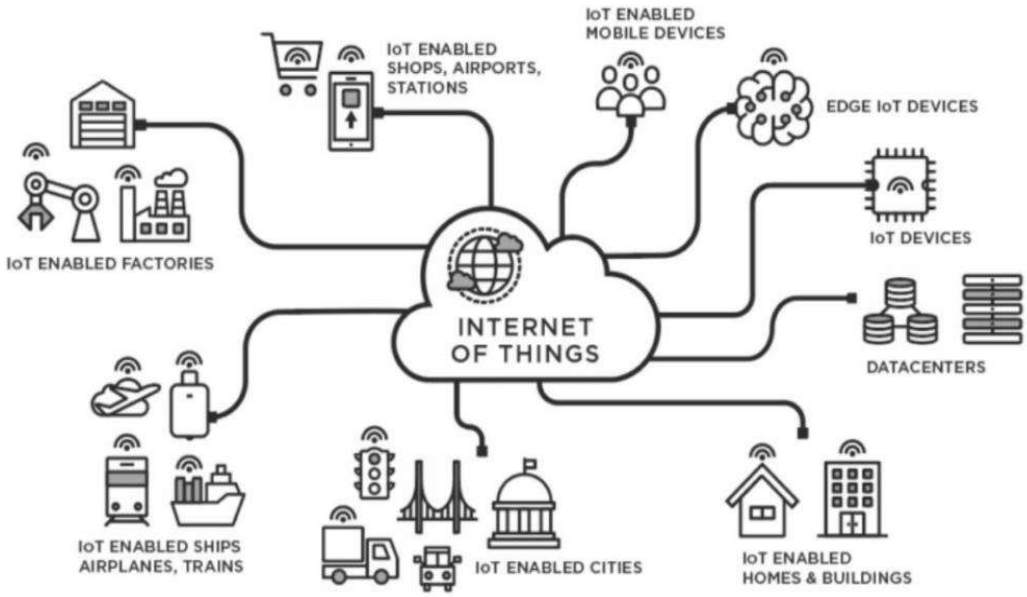
۱-۱ .اینترنت اشیا

اینترنت اشیا (IOT) چالش جدیدی را برای حوزه امنیت سایبری ایجاد کرده است. قبلا فقط رایانه‌ها، روترها، تلفن‌ها به اینترنت متصل بودند. اما پس از معرفی اینترنت اشیا، همه چیزها به آرامی از طریق اینترنت به هم متصل می‌شوند.

ما در عصری زندگی می‌کنیم که در آن می‌توانیم کولر گازی خانه را با تلفن همراه به سادگی در محل کار روشن کنیم، حتی خودرو خود را از کیلومترها دورتر روشن کنیم و با حضور هوش مصنوعی خودرو خود را به محل کار خود برسانیم. توسعه فناوری به هکرها این امکان را می‌دهد در هر جایی از دنیا که هستند. از طریق اینترنت متصل شوند. و تجهیزات IOT را هک کنند و غوغایی فراتر از درک ما اتفاق خواهد افتاد.

IOT معمولی عمدتا شامل ۴ قسمت است:

۱. دستگاه هوشمند مجهز به اینترنت اشیا؛
۲. نرم افزار و سیستم عامل آن؛
۳. رابط گرافیکی برای دسترسی به دستگاه هوشمند؛

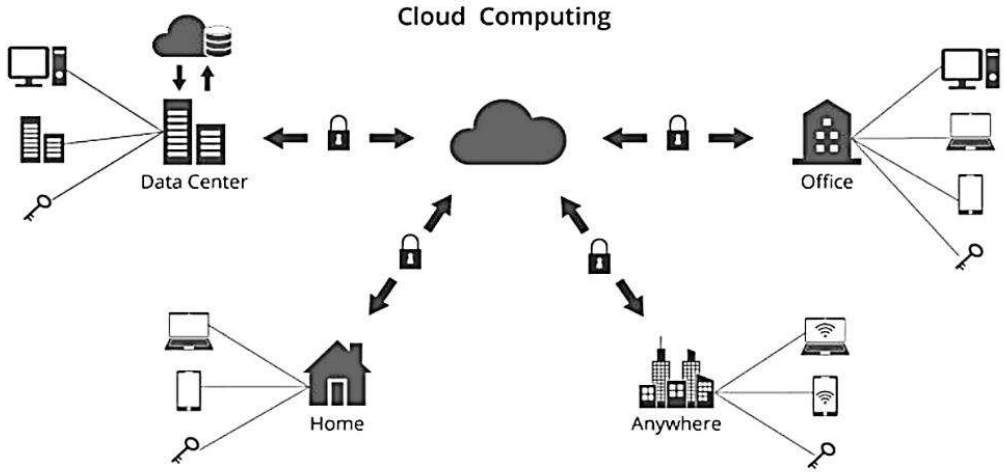


۴. کانال‌های ارتباطی (شبکه و اینترنت).

شکل ۱-۲ اینترنت اشیا

۱-۲ .مراکز داده و ابر

قبل از تکامل اینترنت، رایانه‌ها غیر متمرکز بودند و از این رو در برابر تهدیدات سایبری محافظت می‌شدند. اما پس از طلوع اینترنت، همه دستگاه‌های متصل به اینترنت در معرض تهدیدات سایبری قرار دارند و در نهایت مراکز تجمیع رایانه‌های متصل که می توان گفت مراکز داده یا ابر در واقع تهدیدی بالقوه و مهمترین هدف برای دنیای سایبری هستند. زیرا اکنون داده‌ها به صورت مرکزی ذخیره می‌شوند، درست مانند پولی که به صورت مرکزی در بانک ذخیره می‌گردد و بیشتر از پول ذخیره شده در خانه افراد در معرض سرقت قرار دارد. شرکت‌هایی که برنامه خود را در اینترنت از طریق مرکز داده محلی اجرا می‌کنند نسبت به شرکت‌هایی که داده‌ها را در فضای ابری ذخیره می‌کنند و از طریق اینترنت به آنها دسترسی



دارند کمتر در معرض تهدیدات سایبری هستند.

شکل ۱-۳ رایانش ابری

۱-۳. جنگ سایبری

فنون مرسوم جنگ با ظهور جنگ سایبری منسوخ می شوند. جبهه جنگ، زمین دشمن نخواهد بود، بلکه مراکز داده و سرورهای دشمن است. جنگ سایبری در جبهه‌های جدید مانند:

الف) جاسوسی

جاسوسی در حال حاضر به امور نظامی محدود نمی‌شود بلکه به عناوین مختلفی مانند جاسوسی صنعتی-تجاری، انتخابات آنلاین-الکترونیکی و غیره پیشرفت کرده است. امروزه

تقریبا همه سازمان‌ها هزاران گروه ارتباطی مانند چت، شبکه اجتماعی، ایمیل و .. را در خود دارند و احتمالا تمام اطلاعات مربوط به آن سازمان از طریق این گروه‌های ارتباطی مورد بحث قرار می‌گیرد. برای جاسوسانی که در کمین داده‌ها هستند، این گروه‌ها لقمه چرب و نرمی خواهند بود.

ب)خرابکاری

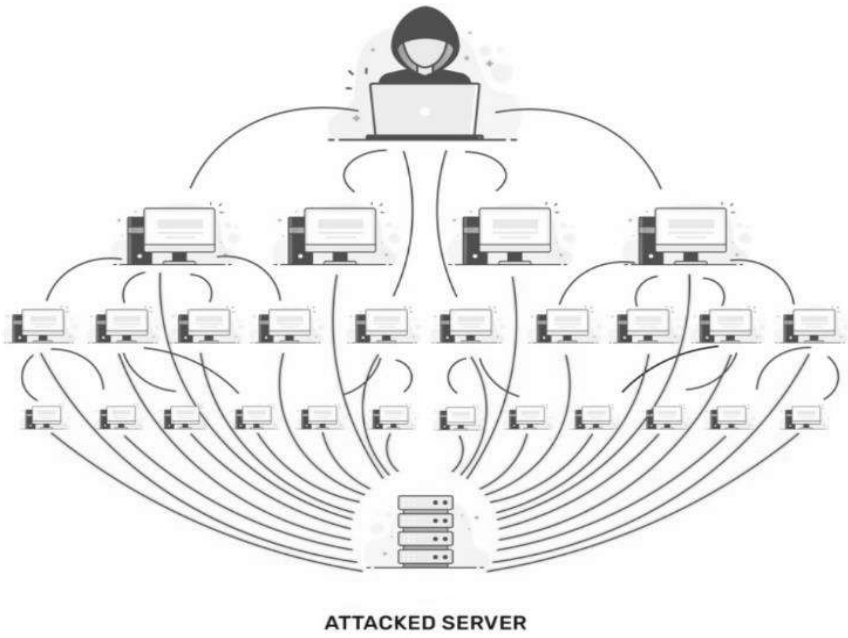
خرابکاری سایبری کار معمول یک سامانه نرم افزاری را مختل می‌کند و به نوعی سامانه را گول می‌زند و آن را مجبور به انجام رفتارهای مخرب می‌کند.

پ)حمله انکار سرویس (DOS)

حمله انکار سرویس شامل شلوغی بیش از حد یک سرویس دهنده (معمولا وبگاه) با درخواست‌های جعلی است، بنابراین سرعت پردازش سرویس دهنده به حداکثر محدودیت‌های خود می‌رسد و در نتیجه سامانه و سیستم را قطع می‌کند و سامانه از مدار خدمات دهی خارج می‌شود.

- حملات متداول لایه ۷ شبکه (برنامه‌های کاربردی) عبارتند از Slow Post، Slow Loris، حملات سیل HTTP، Challenger Collapse.
- حملات پروتکلی که گاهی اوقات حملات محاسباتی یا شبکه ای نامیده می شوند. مانند Ping-of-Death، SYN Flood، Smurf.

❖ حملات حجمی همچنین به عنوان سیل شناخته می‌شود. حملات رایج از این دست



شامل حملات UDP، سیل ICMP (ping) است.

شکل ۱-۴ حملات DDOS

ت) شبکه برق

بخش برق مانند سایر بخش‌ها کاملا دارای فناوری اطلاعات است. سیستم اسکادا (SCADA) سامانه کنترل نظارتی و جمع‌آوری داده‌ها – امکان کنترل تجهیزات الکتریکی را از طریق اینترنت (یا شبکه) فراهم می‌کند. از این رو آنها مستعد هک هستند. ربودن شبکه برق می‌تواند به دشمن توانایی بی حرکت کردن را بدهد. سامانه‌های حیاتی، زیرساخت‌ها را از کار باندازد و حتی منجر به مرگ افراد نیز شود. حتی منجر به قطع سامانه‌های ارتباطی شود. به طور کلی انرژی برق در حال حاضر عنصر حیاتی زیرساختی در تمامی سطوح جامعه و کشورها است.

ث) تبلیغات (پروپاگاندا)

جنگ تبلیغاتی جنگ جدیدی است که توسط دولت‌ها ویا شخصیت‌های متخاصم برای انتشار روایت دروغ برای ملت از طریق رسانه‌های اجتماعی و غیره اجرا می‌شود.

ج) اختلال اقتصادی

امروزه عملکرد سامانه اقتصاد وابسته به IT شده است. حمله به شبکه‌های رایانه‌ای بخش‌های مالی مانند بازارهای سهام، سامانه‌های پرداخت یا بانک‌ها می‌تواند به هکرها اجازه ورود به اسناد مالی داده ویا موانعی را برای رونق اقتصادی در جامعه ایجاد کنند.

چ) حمله سایبری غافلگیرکننده

این نوع حملات دشمن باعث می‌شود دفاع از حملات خود را کاهش دهد و می‌توان گفت دشمن از آن برای از بین بردن آمادگی خودی برای حمله فیزیکی(سخت یا نیمه سخت) استفاده کند. این حمله به عنوان نوعی جنگ ترکیبی قابل استفاده است.

ح)اختلال ارتباطات

ایمیل‌ها، تلفن‌های ثابت و همراه یا دیگر انواع شبکه‌های ارتباطی ممکن است هک، دستکاری و یا رهگیری شوند و در نتیجه کل شبکه ارتباطی را مختل کنند.

د) تزریق SQL

این حمله شامل وارد کردن کد یا ویروس مخرب به پایگاه داده نرم افزار از طریق نقص در فرآیند اعتبارسنجی ورودی نرم افزار است.

ذ)حملات زنجیره تامین

شامل رویارویی با زنجیره تامین یک شرکت یا سازمان برای دسترسی به نرم افزار یا داده‌های آن است.

ر) شکستن رمز

این حمله با دستکاری ارز رمزنگاری شده با کنترل الگوریتم‌های رمزنگاری اشاره دارد.

ز) بهره برداری روز صفر

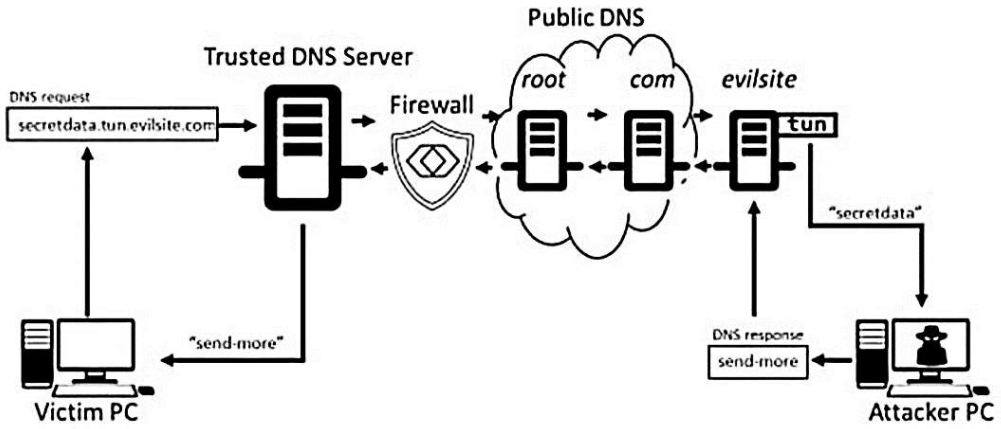
یک بهره برداری روز صفر پس از اعلام حساسیت شبکه نسبت به حفره امنیتی ناشناخته رخ می‌دهد. هیچ راه حلی برای جلوگیری از این نوع حمله در بیشتر مواقع وجود ندارد. از این رو فروشندگان ابزار حمله به حفره (Exploit) معمولا کاربران را درجریان حفره‌های جدید می‌گذارند. این موضوع دو روی یک سکه است و این امکان را برای استفاده توسط مهاجمین نیز ایجاد می‌کند.

س) حمله آبیاری

هدف در اینجا یک گروه حساس از یک انجمن است. در چنین حمله ای، مهاجم پروتال‌هایی را هدف قرار می‌دهد که به طور منظم توسط گروه هدف مورد استفاده قرار می‌گیرد.

ش) حمله تونل DNS

هکرها از DNS برای فرار از اقدامات ایمنی و صحبت با سرور از راه دور استفاده می‌کنند. (مانند رد کردن دیواره آتش) این حمله با استفاده از تکنیک اسب تروا (تروجان) که در آن هکرها کد مخرب را در یک پیام قرار می دهند که شبیه یک درخواست DNS است. از آنجایی که DNS بخش مهمی از اکثر شبکه‌ها و اینترنت است، این نوع ترافیک به ندرت می



تواند از دیواره‌های آتش و تجهیزات مدیریت حمله تجزیه و تحلیل شود.

شکل ۱-۵ تونل DNS

ط) حمله جعل DNS

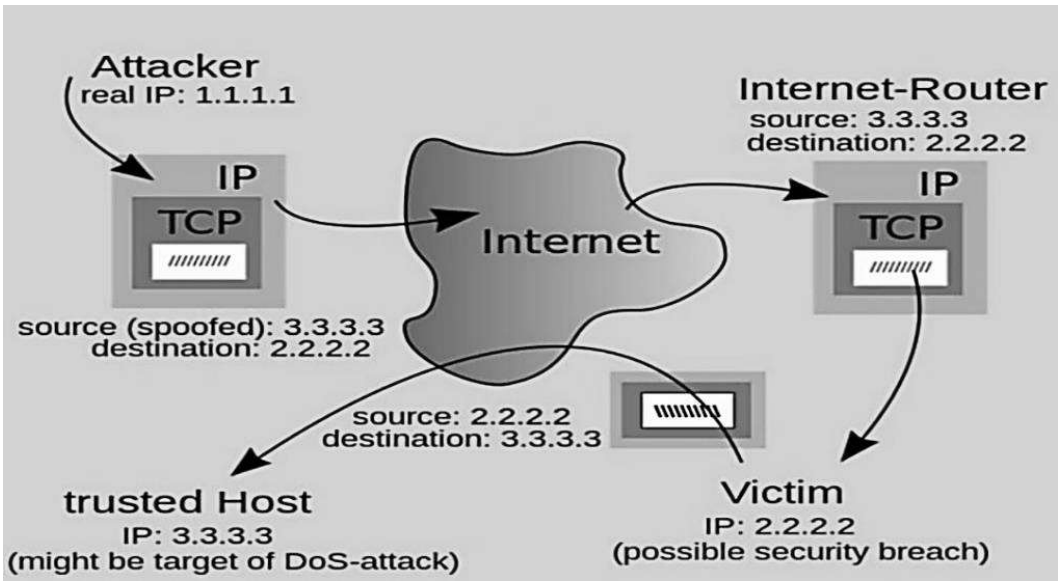
حمله سایبری که در آن حساب DNS را از یک پورتال دستکاری می کند تا ترافیک آن را به مکان دیگر یا وبگاه مهاجم هدایت کند.

ظ)برنامه نویسی بین وبگاهی (XSS)

حمله ای است که در آن یک هکر اسکریپت‌های اجرایی مخرب را به کد یک برنامه قابل اعتماد یا پورتال تزریق می‌کند. هکرها اغلب با ارسال یک آدرس وبی مخرب به کاربر و وسوسه کردن او برای کلیک کردن روی آن، یک حمله XSS را انجام می‌دهند.

ل) حمله جعل IP

جعل IP یک حمله بدخواهانه است که در آن هکر منبع واقعی بسته‌های IP را پنهان می‌کند تا دانستن منشا آنها را دشوار کند. هکر بسته‌هایی را تولید می‌کند، آدرس مبدا را برای تقلید از یک سیستم متفاوت یا مسیر ارسال تغییر می‌دهد و یا هر دوکار را انجام می‌پذیرد. بخش عنوان بسته جعلی برای آدرس IP منبع حاوی آدرسی است که با آدرس IP منبع واقعی



متفاوت است.

شکل ۱-۶ جعل IP

م) دستکاری ATM

هکرها از دستگاه خودپرداز بانک به روشی برای کلاهبرداری در توزیع پول استفاده می کنند.

ن) حملات فشینگ

در این مورد هکرها با استفاده از سیستم مهندسی اجتماعی کلاسیک، افراد با سابقه را هدف قرار می‌دهند تا داده‌های مورد نیاز خود را بدست آورند.

و) تفسیر URL

در این حمله با دستکاری بخشهای از URL یک هکر می تواند یک وب سرور را برای نمایش صفحات وب که اجازه دسترسی به آنها را ندارد، دریافت کند. مثل

http://target/forum/?cat=**********

ه) ربودن نشست

هکر حق ورود به شناسه نشست (Session-ID) کاربر را دارد تا جلسه کاربر را با یک برنامه وبی تایید کند و از جلسه کاربر استفاده کند.

ی) حمله Brute Force

یک هکر با امتحان کردن رمزهای عبور مختلف تا زمانی که رمز عبور مناسب پیدا شود، تلاش و در نهایت دسترسی پیدا می‌کند. این روش در برابر گذرواژه‌های ضعیف بسیار موثر است.

۲. انواع حملات سایبری پیشنهادی در این مقاله

۲-۱. UPI فشینگ

تحول صنعت دیجیتال ارز و پول دیجیتال را نیز معرفی کرده است و نرم افزارهای مختلفی مبتنی بر UPI برای ارسال و دریافت پول در بازار موجود است. دشمن می تواند در صورت فشینگ از طریق UPI، اقتصاد را مختل کند. فشینگ UPI را می توان با استفاده از تکنیک‌های زیر اجرا کرد:

- شبیه سازی تلفن؛
- گرفتن تلفن از راه دور (مثل any desk، skype،TeamViewer)؛
- تقلب OTP ؛
- کلاهبرداری‌های مبتنی بر بدافزار(پیوندهای جعلی)؛
- نصب برنامه‌های مخرب؛
- استفاده از WIFIهای باز و بدون رمز؛
- استفاده از کد QR تکراری از کد QR اصلی.

۲-۲ . هک سیستم اسکادا

راه آهن و مترو از اسکادا برای کنترل کشش و دیسکم‌های الکتریکی از اسکادا برای کنترل فیدرها یا DTRها و غیره استفاده می‌کنند. هک کردن این سیستم اسکادا به معنای اختلال در توزیع نیروی برق و اختلال در مدیریت ترافیک راه آهن و مترو است.

۲-۳ . هک سامانه‌های خدمات عمومی

امروزه بسیاری از سامانه‌های خدمات عمومی مانند سیگنال‌های ترافیکی، پرداخت آنلاین صورت حساب برق و آب و شهرداری و ...، سامانه‌های ثبت آنلاین زمین و ملک، سامانه‌های آنلاین مراقبت از مشتری و... خودکار هستند. اگر موارد فوق هک شوند، بین مردم هرج و مرج ایجاد خواهد شد.

۲-۴ . هک ویدیو کنفرانس

امروزه تقریبا همه سازمان‌ها جلسات خود را از طریق ویدئو کنفرانس برگزار می‌کنند، در این صورت هک کردن سامانه‌های مربوط به معنای دریافت تمام اطلاعات درباره جلسه است.

۲-۵ . جعل عمیق (با استفاده هوش مصنوعی)

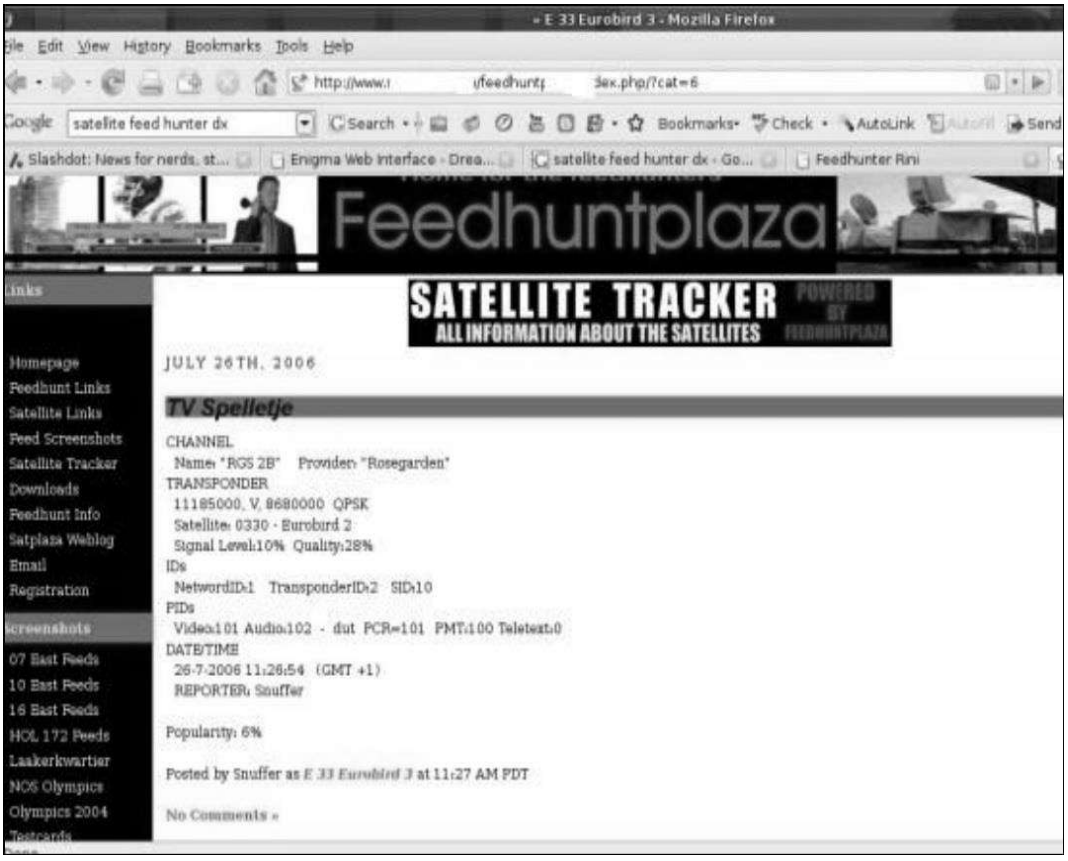
ویدئو یا عکسی که عمدا آلوده و دستکاری شده است تا سلبریتی یا سیاست مداری وانمود کند کاری را انجام می‌دهد یا حرفی را می‌گوید که واقعا انجام نشده یا گفته نشده است.

۲-۶ . هک شبکه ارتباطات نظامی، پایگاه داده نظامی، شبکه‌های رادار، ماهواره‌ها، GPS، ATC، AWACS

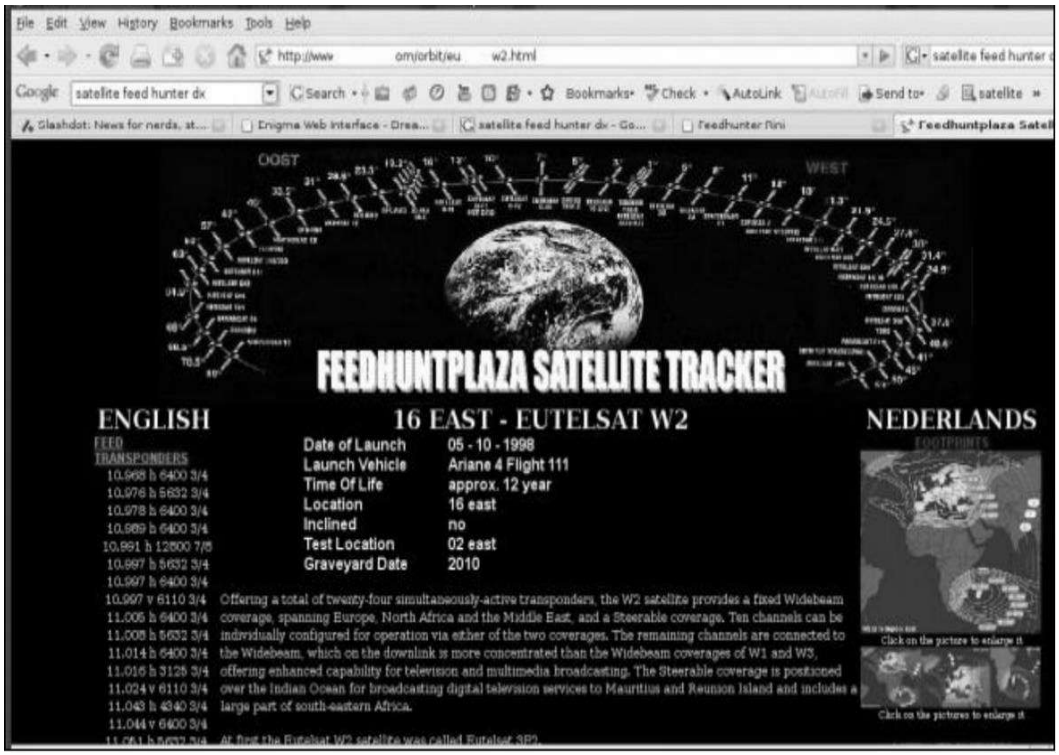
الف) هک ماهواره

برای ربودن لینک DVB-S ماهواره‌ای به موارد زیر نیاز دارید:

- دیش ماهواره، ابعاد به موقعیت جغرافیایی و ماهواره بستگی دارد؛
- یک مبدل کم نویز بلوک پایین LNB؛
- تیونر اختصاصی PCIe کارت DVB-S ؛
- یک رایانه باسیستم عامل لینوکس.



شکل ۲-۱ هک ماهواره [۱]



شکل ۲-۲ هک ماهواره[۲]

بخش دفاعی کشورها برای ارتباط صرفا به ماهواره‌های بومی خود وابسته است. اگر ماهواره‌ها هک شوند، ارتباطات نظامی به خطر می‌افتد. به عنوان مثال ماهواره‌های سری GSAT نیروی دفاعی هند را چند برابر کرده است و ارتباط با پهپادها و هواپیماهای هشدار دهنده و کنترل اولیه هوابرد را فراهم می‌کنند. بدین ترتیب با شناسایی ماهواره و شگردهای جاسوسی و هک، این امکان رهگیری رادارهای زمینی و همچنین نظارت الکترونیکی وجود دارد که بتوان سیستم دفاعی یک کشور را ضعیف یا حتی اطلاعات نادرست داد و از بین برد.

ب) هک موشک‌ها و بمب‌های هوشمند

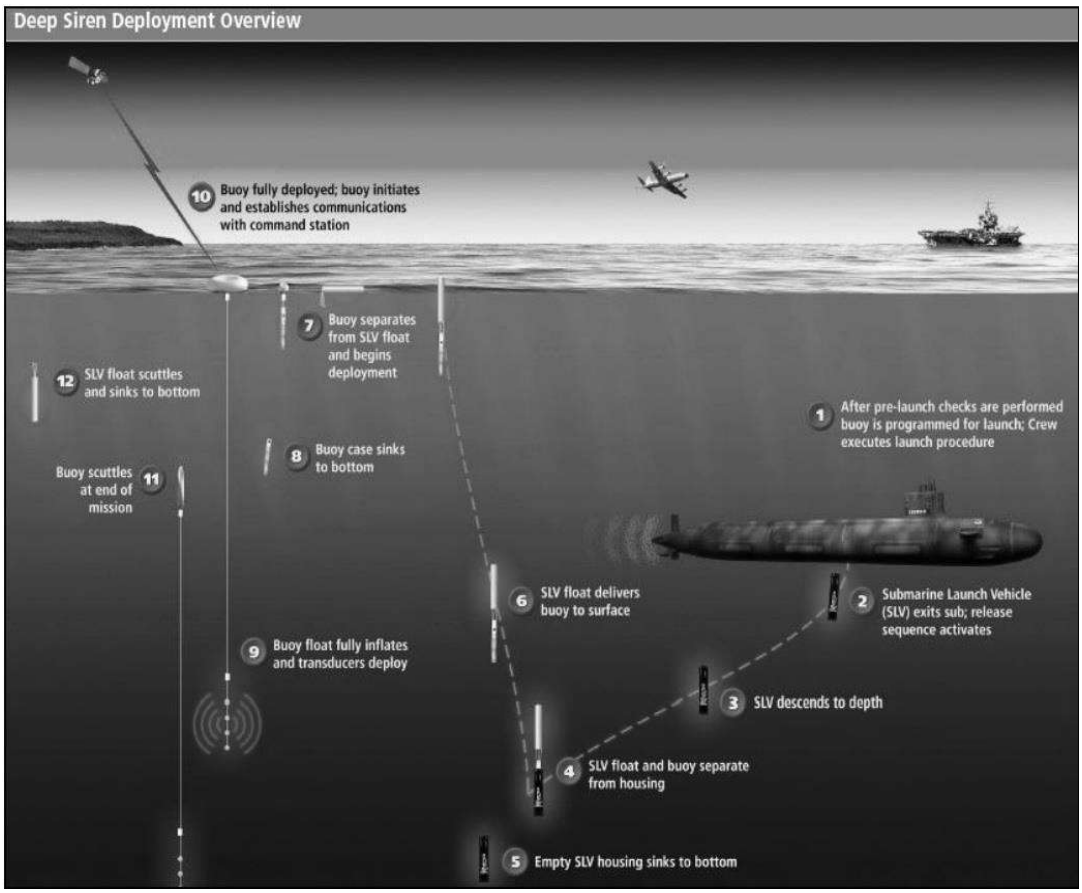
پرتاب موشک به روشی که از طریق آن اطلاعات به تاسیسات پرتاب موشک و نحوه انتقال اطلاعات به موشک‌های در حال پرواز بستگی دارد. راه‌های زیادی برای حمله سایبری تهاجمی علیه سیستم‌های موشکی وجود دارد. اینها شامل بهره برداری از طرح‌های موشک، تغییر نرم افزار یا سخت افزار،یا ایجاد مسیرهای مخفی برای سیستم‌های فرماندهی و کنترل موشک است. سیستم‌های موشکی از رایانه استفاده می‌کنند و بنابراین در واقع همه آنها در برابر حملات سایبری و الکترونیکی آسیب پذیر هستند.

شایعاتی مبنی بر هک کردن یکی از موشک‌های بالستیک آزمایشی کره شمالی توسط آمریکا و جلوگیری از آن وجود دارد. همچنین در نبرد کنونی غزه نیز شایعه هک سامانه گنبد آهنین نیز در خبرها ذکر شده بود.

به طور مشابه، بمب‌های هوشمند هدایت شونده توسط GPS نیز هستند که اطلاعات هدف را در زمان پرتاب توسط شلیک کننده تغذیه می‌شود، بنابراین هرگونه نقض ارتباط ممکن است منجر به تغذیه مختصات اشتباه در بمب شده و ممکن است منجر به فاجعه شود. نمونه‌ای از شواهد فنی در مورد وجود این اتفاق در مقالات وجود دارد.

ج) هک ارتباطات زیردریایی

یکی از قوی‌ترین‌ها در سه‌گانه هسته‌ای زیردریایی است. زیردریایی‌های هسته‌ای حامل موشک‌های بالستیک هسته‌ای خود در اعماق اقیانوس‌ها کمین کرده و آماده شلیک سلاح‌های هسته‌ای در هر زمان هستند. اما قبل از شلیک آنها باید از مرکز فرماندهی ارتباط برقرار کنند و سیگنال سبز را دریافت کنند. برقراری ارتباط با مرکز فرماندهی دشوارترین قسمت است



و دشمنان در تعقیب دائمی برای رهگیری این ارتباطات هستند. هنگامی که این ارتباطات رهگیری می‌شود، جنگ نصف برنده می‌شود.

شکل ۲-۳ ارتباطات زیردریایی

د) هک جت جنگنده و هواپیماهای بدون سرنشین

جهان دارای هواپیماهای نسل پنجم مانند SU-57، J-20، F-22، F-35 و غیره است و به زودی شاهد هواپیماهای نسل ششم و هواپیماهای بدون سرنشین خواهیم بود. هواپیماهای فوق همه به صورت دیجیتالی خودکار هستند و با استفاده از ابررایانه‌ها کار می‌کنند و به شدت به کانال‌های ارتباطی مانند ماهواره‌ها، آواکس و رادارها متکی هستند. بنابراین آنها بسیار مستعد هک می‌باشند.

یک جنگنده از گره‌های دیجیتالی زیر تشکیل شده است:

- سامانه پرواز دیجیتال برای کنترل پرواز؛
- GPS، رادار، رادار دریافت هشدار و سامانه هشدار موشک؛
- نمایشگرهای چند منظوره و HUD ؛
- سیستم توزیع اقدامات متقابل و احتمالا غلاف ECM ؛
- سامانه محاسباتی کنترل آتش و ماموریت؛
- رادیو VHF و UHF و ارسال داده؛
- سیستم هدف گیری؛
- سیستم کنترل موتور؛
- و ....

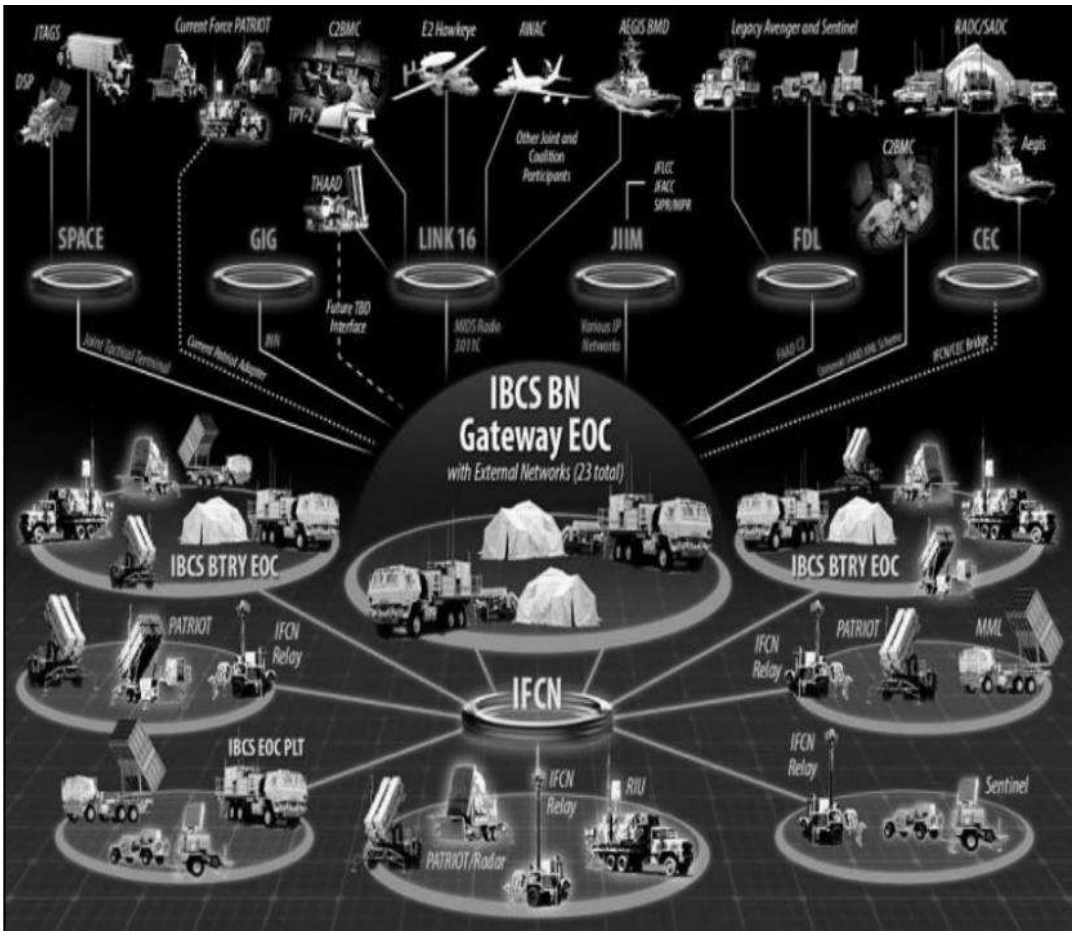
در گذشته هکرها حتی F-15 را هک کرده و DEFCON را افزایش داده اند. هک یک هواپیمای جنگنده همچنین به معنای هک کردن بمب‌های هوشمندی است که با خود دارند نیز هست.

ه) هک ایستگاه کنترل یکپارچه رادار

هر کشوری چندین رادار در مرزهای خود دارد و برای برنامه ریزی جنگ تاکتیکی، رادارها باید به هم متصل شوند تا یک تصویر واحد از کل تهدید دشمن ترسیم گردد. از آنجایی که رادارها به یکدیگر متصل هستند و با هم ارتباط برقرار می‌کنند، بنابراین در معرض

حملات سایبری قرار دارند. سامانه فرماندهی نبرد یکپارچه دفاع هوایی و موشکی قلب فناوری رادار است و می‌تواند کاملا خودکار عمل کند. که خود مستعد حملات سایبری خواهد بود.

معمولا روش متداول برای آلوده کردن این سامانه‌ها درگاه‌های رایانه‌ها و رسانه‌های قابل جابجایی است. هنگامی که هر سامانه دارای حفره آلوده می‌شود، بدافزار می‌تواند به سامانه‌های دیگر در یک شبکه تکثیر شود. داده‌ها آلوده گردد. بدافزار می تواند داده‌ها را در یک موقعیت مناسب از طریق رسانه‌های ذخیره ساز، داخل آن قرار دهد. در این مرحله داده در صورتی که رسانه مورد نظر در رایانه متصل به اینترنت قرار گیرد داده از طریق اینترنت به مرکز فرماندهی و کنترل هکر منتقل می‌شود.



شکل ۲-۴ ایستگاه کنترل یکپارچه رادار

۳. چگونگی حفاظت از سامانه‌ها در برابر جنگ سایبری

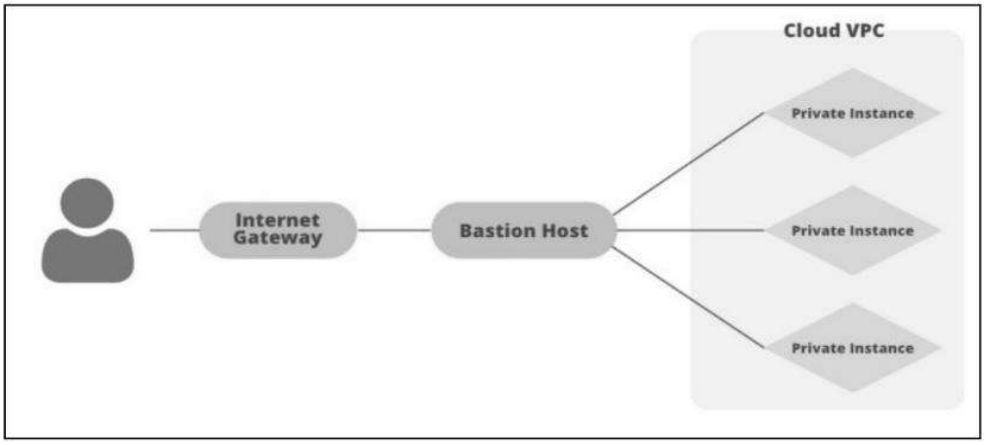
الف) استفاده از فایروال وUTMها (مدیریت یکپارچه تهدید)

برای سازمان‌ها و شرکت‌هایی که به مرکزداده یا ابر متکی هستند، استفاده از فایروال و UTM ضروری است. اینترنت باید ابتدا روی UTM و سپس روتر قرار گیرد. آدرس‌های شبکه باید طبق رفتارشان در لیست سیاه یا سفید قرار گیرند و در پایگاه داده ذخیره شوند، به همین ترتیب فقط پورت‌های ضروری باز گذاشته می‌شوند. برخی از پورت‌های مهم که نیاز به توجه دارند عبارتند از : FTP, HTTP, HTTPS, SMTP, SSH, RDP, SMB,DNS و سایر پورت‌هایی که بسته به نیاز سامانه از آن استفاده می شود.

سازمان‌ها برای دسترسی‌های آدرس‌های شبکه نیز باید لیست سیاه و سفید IP داشته باشند به طور مثال دسترسی به سرورهای VPN، دسترسی به سامانه‌های نرم افزاری و شبکه‌های اجتماعی و ....

ب) استفاده از میزبان پوششی

میزبان پوششی یک سرور اختصاصی است که به کاربران مجاز امکان دسترسی به یک شبکه خصوصی از طریق اینترنت را می دهد. این سرور در خارج از فایروال قرار دارد و میزبان پوششی تنها مسیر ورودی سرور به داخل است. در این روش کاربر با استفاده از دسترسی که فایروال به او داده است به کنسول یک ماشین مجازی متصل می شود و از آن

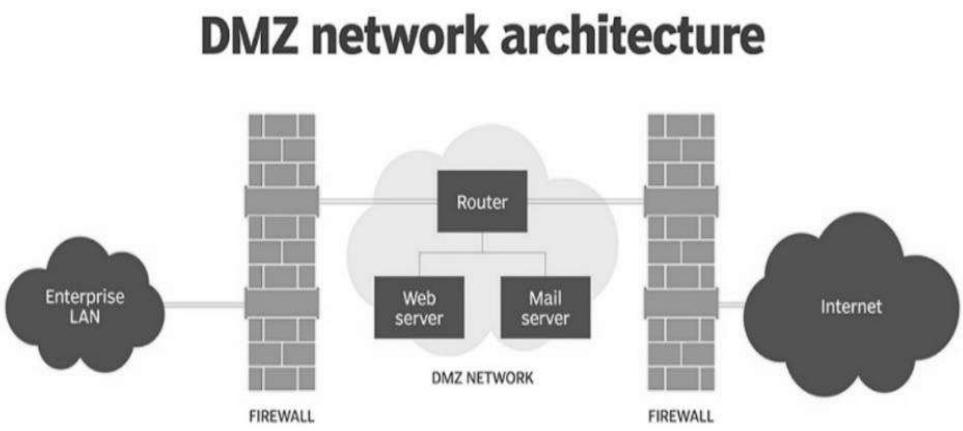


طریق یک سیستم عامل کامل و یا یک یا چند نرم افزار را دسترسی خواهد داشت. ماشین‌ها از طریق فایروالی دیگر به اینترنت متصل می باشند.

شکل ۳-۱ میزبان پوششی

ج)استفاده از DMZ

DMZها به عنوان یک منطقه بافر بین اینترنت و شبکه محلی خصوصی عمل می‌کنند. شبکه فرعی DMZ بین دو دیوار آتش قرار می‌گیرد سپس تمام ترافیک ورودی قبل از رسیدن



به سروری که در DMZ قرار دارد با استفاده از دیوار آتش بررسی می‌شود.

شکل ۳-۲ معماری DMZ

د) استفاده از آنتی ویروس یا آنتی ویروس متمرکز

برای هر سازمانی، داشتن یک سرور آنتی ویروس متمرکز اجباری است. سرور آنتی ویروس متمرکز این امکان را می‌دهد که تمام سیستم‌های موجود در شبکه LAN را زیر نظر بگیرد و سلامت آنها را ببیند و در صورت نیاز می‌تواند به روزرسانی‌هایی را انجام دهد. همچنین در حوادث حمله ویروسی ساختار حمله و مشارکت‌های آن را بررسی می کند و سپس در پایگاه داده ای برای کمک در تجزیه و تحلیل حوادث آینده ذخیره می‌کند.

ه) تحلیل رفتار کاربر با استفاده از نرم افزار امنیت سایبری

تجزیه و تحلیل رفتارکاربر از هوش مصنوعی و یادگیری ماشین برای تجزیه و تحلیل مجموعه داده‌های بزرگ یا رویدادها با هدف شناسایی الگوهایی استفاده می کند که نشان می دهد که :

نقض امنیت روی داده؛

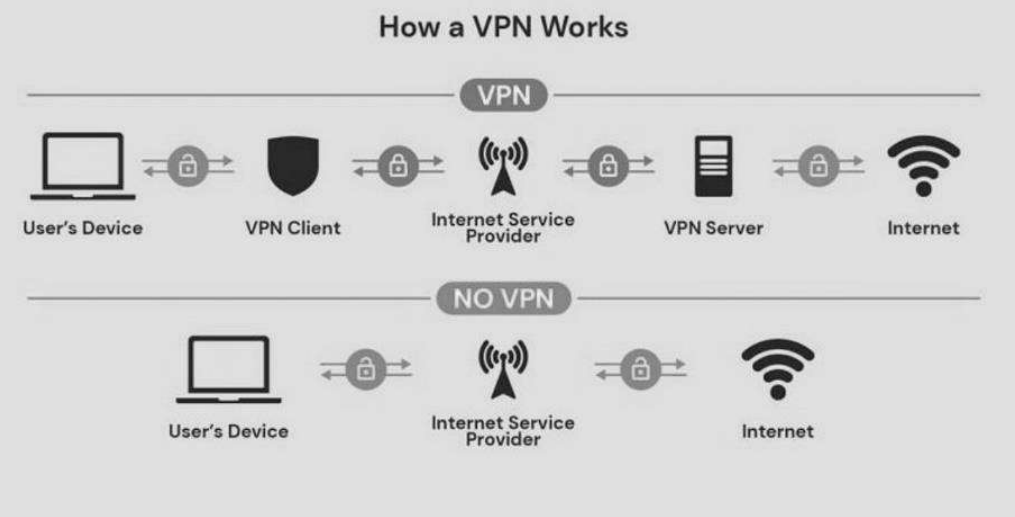
داده ای استخراج شده؛

یا سایر فعالیت‌های مخربی که در غیر این دو صورت ممکن است وجود داشته و مورد توجه تا به حال قرار نگرفته است.

تجزیه و تحلیل رفتار کاربر به شرکت یا سازمان کمک می‌کند تا قبل از ورود هکرها به شبکه و آسیب رساندن به آن، خطرات را ارزیابی کرده و تهدیدات را کاهش دهد.

و) استفاده از VPN

VPN یک تونل امن بین رایانه شخصی و سرور VPN ایجاد می کند که فعالیت و موقعیت آنلاین را پنهان می کند. VPN تضمین می کند که از حریم خصوصی آنلاین محافظت می



کند و ISP و شبکه‌های مابین در حین پایش فعالیت‌ها و ردیابی شبکه، آن را نادیده می‌گیرد.

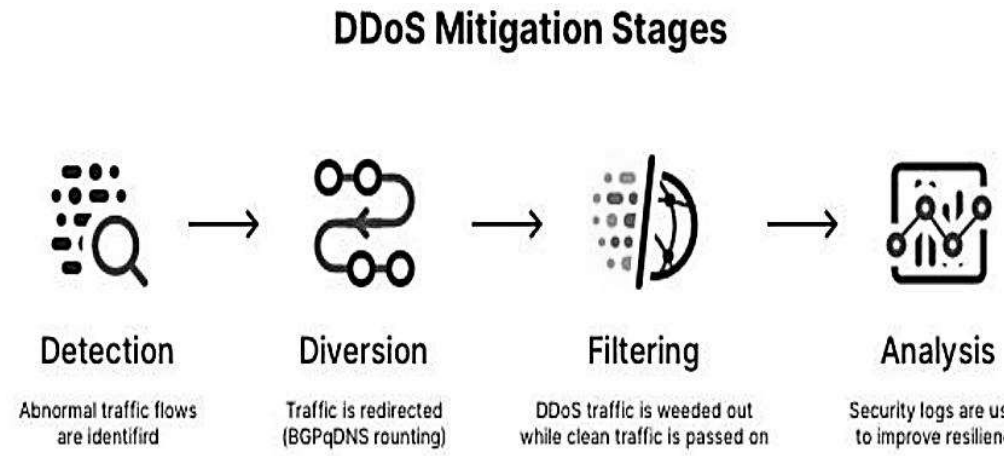
شکل ۳-۳ نحوه عملکرد VPN

ز) کاهش حملات DDOS

روش کاهش حملات DDOS فرآیندی هدفمند در جهت محافظت از سرور یا شبکه در برابر این نوع حمله است که ابتدا توسط یک شناسا (Detection) تشخیص داده می‌شود. سپس انحراف صورت می پذیرد و ترافیک حمله فیلتر شده و در نهایت از رویداد امنیتی ثبت شده تحلیل و بررسی انجام می‌شود و اقدامات مقتضی نسبت به آن انجام می‌گردد.

ح) رمزگذاری داده‌ها

رمزگذاری داده‌ها، داده‌ها را قبل از ذخیره در پایگاه داده و ذخیره ساز به هم می‌ریزد. این کار داده را در برابر سوء استفاده از داده‌ها توسط کاربران غیرمجاز و نقض امنیت داده محافظت می‌کند. شرکت‌ها و سازمان‌ها باید از سرویس مدیریت کلید برای انجام رمزگذاری



داده‌ها استفاده کنند.

شکل ۳-۴ گام‌های کاهش DDOS

ط) یک سیاست تکرار مناسب تعریف کنید.

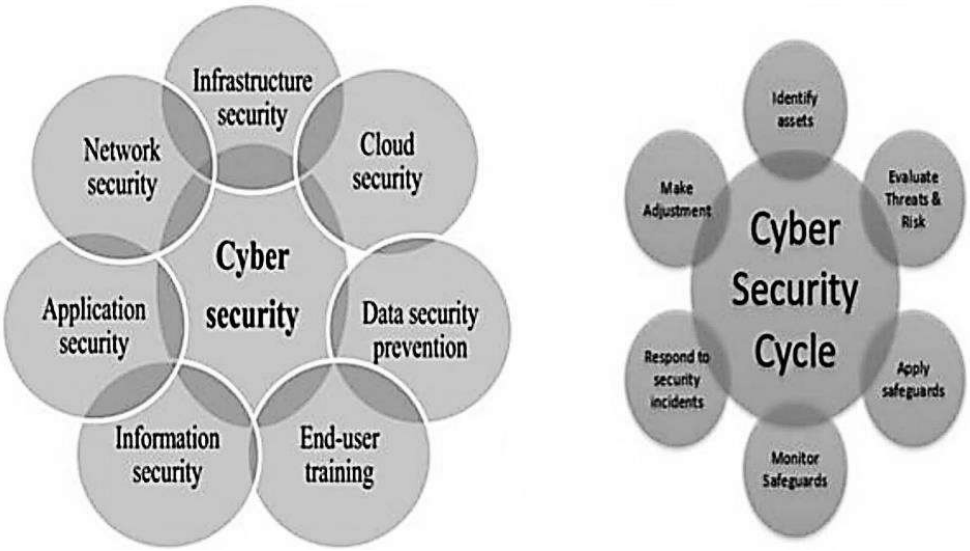
سیاست تکثیر داده و انتقال آنها به سرور ویا مکان دیگر را Data Replication می‌گویند. در واقع مفهوم تکثیر داده به این معنی است که از داده‌ها کپی‌های متعددی در مکان‌های مختلف داشته باشیم که حتی اگر در ناگوارترین رویداد و یا حمله سایبری داده دچار مشکل شد، از اطلاعات مهم و ضروری خود یک نسخه پشتیبان داشته باشیم. خطی مشی درست امنیت داده را تضمین می‌کند و براساس نیاز می تواند به صورت فعال یا غیرفعال عمل کند.

ی) سیاست امنیت سایبری

همه شرکت‌ها باید الزاما یک سیاست امینت سایبری مرکزی داشته و باید به شدت به آن پایبند باشند. خط مشی امنیت سایبری باید در صورت لزوم به روز شود.

این سیاست باید با در نظرگرفتن موارد قابل اجرا زیر تدوین شود:

۱. زیرساخت؛
۲. شبکه؛
۳. نرم افزار؛
۴. ابر؛
۵. مرکزداده؛
۶. پایگاه داده؛
۷. و....



شکل ۳-۵ سیاست امنیت سایبری

ک) مدیر ارشد امنیت اطلاعات

داشتن یک مدیر ارشد امنیت اطلاعات برای همه سازمان‌ها الزامی است. او کسی است که از اطلاعات سازمانی، سایبری و امنیت فناوری مراقبت می‌کند. نقش و مسئولیت یک مدیر ارشد امنیت اطلاعات عبارتند از:

۱. پیاده سازی و نظارت بر برنامه امنیت سایبری سازمان؛
۲. تعادل بین امنیت سایبری و اهداف کاری؛
۳. نظارت بر رخدادهای امنیتی و واکنش مناسب به آن؛
۴. مدیریت تداوم کار و بازیابی اطلاعات؛

۵. آگاهی و آموزش امنیت سایبری.

۴. چند نمونه عملیات جنگ سایبری

۴–۱ . برخی ادعاهای جهانی

الف) در فوریه ۲۰۲۲ جنگ اوکراین و روسیه آغاز شد و جنگ همچنان ادامه دارد مشاهده شده است که بدافزار جدید Viper برای حمله به اهداف اوکراینی استفاده می شود و بر روی حداقل چند صد دستگاه در سراسر اوکراین نصب شده است. چندین سازمان اوکراینی نیز تسلیم حملاتی شده اند که از بدافزار Kill Disk و Hermetic Wiper استفاده کرده اند که داده‌های دستگاه را از بین برده است.

ب) مقامات امریکایی و ژاپنی هشدار می‌دهند که هکرهای تحت حمایت دولت چین نرم افزارهای اصلاحی را در داخل روترها قرار داده اند تا صنایع و شرکت‌های دولتی واقع در هر دو کشور را هدف قرار دهند هکرها برای مخفی ماندن و جابجایی در شبکه‌های هدف، خود از بخشی‌های سیستم عامل استفاده می‌کنند. چین این اتهامات را رد کرده است.

ج) هکرهای ایرانی یک حمله سایبری علیه شبکه راه آهن اسرائیل انجام دادند. هکرها از یک کمپین فیشینگ برای هدف قراردادن زیرساخت‌های الکتریکی شبکه استفاده کردند طبق گزارش‌ها، شرکت‌های برزیلی و اماراتی نیز در همین حمله هدف قرار گرفتند.[۱]

د)هکرهای مرتبط با روسیه یک حمله DDOS علیه سرورهای شهر واتیکان انجام دادند و وب سایت رسمی آن را آفلاین کردند. این حمله سه روز پس از آن صورت گرفت که مقامات دولتی روسیه از پاپ فرانسیس به دلیل اظهاراتش درباره جنک در اوکراین انتقاد کردند.

د) پس از حمله طوفان الاقصی و سپس حملات اسراییل به غزه گروه هکری انتقام جویان به صورت گسترده زیرساخت‌های رژیم جعلی اسرائیل را هدف قرار داد و طبق گزارشات این حملات موجب از کارافتادن سایت‌ها و موسسات زیادی در رژیم صهیونیستی شده است.

---

۱. هیچ منبع در ایران این اتهامات را تایید نکرده است.

یکی از حملات حاکی از هک شدن تمام زیرساخت‌های تصفیه آب اسراییل می‌باشد. شرکت‌های امنیت سایبری این گروه را به ایران نسبت داده اند.[۱]

۴-۲. برخی حملات سایبری علیه سازمان‌ها و شرکت‌های ایرانی

با توجه به فراوانی حملات سایبری علیه ایران در چند ساله اخیر مخصوصا بعد از ترور حاج قاسم در بخشی از حملات را در جدول زیر ذکر کرده ایم. البته تمامی مطالب زیر با توجه به اخبار رسیده توسط خبرگزاری‌های ایران، ادعاهای هکری ذکر شده در سایت‌ها و شبکه‌های اجتماعی صورت پذیرفته است.

قربانی حمله	عامل مدعی	نتایج حمله
شرکت راه آهن جمهوری اسلامی	گنجشک درنده	خارج شدن سرورهای این شرکت از ارائه سرویس و درج محتوا بر روی تابلو اعلانات سالن اصلی شرکت راه آهن
وزارت راه و شهرسازی	گنجشک درنده	نمایش شعار در رایانه کارمندان و اختلال در فرآیند اداری در تکمیل حمله به شرکت راه آهن حذف دیتای مسکن خوداظهاری
دوربین‌های زندان اوین	عدالت علی	افشا تصاویر مربوط به دوربین‌های مدار بسته زندان و نمایش پیام بر روی نمایشگرهای اتاق مانیتورینگ زندان
فولاد اصفهان، خوزستان، هرمزگان	گنجشک درنده	هرمزگان: کوره‌ها اصفهان: تخرب plcهای خط تولید فولاد خوزستان: پاک شدن‌هارد دوربینها، دسترسی به اتوماسیون صنعتی و ذوب ریزی تخریبی
سازمان صدا و سیما	عدالت علی	تغییر در محتوای خبر ۲۱ شبکه یک و شبکه خبر
دادستانی کل کشور	Anonymous	افشاء محتوای ایمیل‌های ارسالی و دریافتی معاونت فضای مجازی دادستانی کل کشور به شرکت‌ها و سازمان‌های مختلف که افشاکننده سیاست‌های فیلترینگ کشور و نحوه تعامل بخش خصوصی با دادستانی است.

۱ .همان.

خبرگزاری فارس	Black Reward	حذف بخشی از آرشیو خبرگزاری فارس و انتشار گسترده برخی محتوای محرمانه
سازمان سنجش	Anonymous	هک و استخراج اطلاعات ۹۳۵ هزار شرکت کننده در کنکور ۱۴۰۱ از سایت سازمان سنجش
دیجیکالا	Anonymous	هک و استخراج دیتابیس دیجیکالا
پتروشیمی خلیج فارس	Anonymous	هک ایمیل‌های داخلی پتروشیمی خلیج فارس و انتشار ۲۰ هزار ایمیل از این شرکت
ریاست جمهوری	قیام تا سرنگونی	سرقت و افشای اطلاعات و از دسترس خارج شدن سرویس‌های نهاد
بنیاد شهید و امور ایثارگران	بختک	سرقت اطلاعات – افشائ اطلاعات – پاک شدن اطلاعات اصلی – دیفیس
مرکز آپا دانشگاه صنعتی اصفهان	آروین	سرقت و افشای اطلاعات و دسترسی غیرمجاز به سرورهای سازمان فناوری اطلاعات
ثبت احوال	آنتی ملا	مهاجم مدعی سرقت اطلاعات ۱۰۰ میلیون ایرانی شده است و ۱۰۰۰ نفر را برای نمونه و بخشی دیگر از اطلاعات سازمان ثبت احوال را منتشر کرده است.
وزارت علوم، تحقیقات و فناوری اطلاعات	قیام تا سرنگونی	تغییر در بازه زمانی لاگ‌ها و سرقت اطلاعات و دسترسی به تمام سامانه‌های وزارت علوم
نهاد رهبری در دانشگاه‌ها	قیام تا سرنگونی	کل شبکه زیرساخت نهاد از دسترس خارج شده و بسیاری از اطلاعات توسط مهاجم پاک شدند
سامانه هوشمند سوخت	گنجشک درنده	کل جایگاه‌های سوخت که در زور حمله به سامانه متصل بودن از مدار سرویس دهی خارج شدند
اسنپ فود	irLeaks	اطلاعات ۲۰ میلیون کاربر و ۳۵ هزار پیک و ۲۴۰ هزار فروشنده و ۸۸۰ میلیون سفارش به سرقت رفت.

جدول ۴-۱ حملات سایبری به ایران

۵. نتیجه گیری و کار آینده

با ظهور فن‌آوری‌هایی مانند محاسبات کوانتومی و هوش مصنوعی، جنگ سایبری اجتناب ناپذیر است، مدیران مرکز داده، ارائه دهندگان خدمات ابری باید همیشه به طور مناسب به روز شوند تا از هر گونه حمله سایبری جلوگیری شود. مدیر امنیت سایبری هر سازمانی در این الگو نقش تعیین کننده ای خواهد داشت. با معرفی پول و ارز دیجیتال موسسات مالی بسیار مستعد به آسیب‌های ناشی از جنگ سایبری هستند.

با ورود هوش مصنوعی، یادگیری ماشین و یادگیری عمیق، حملات سایبری افزایش می‌یابد و به شیوه‌ای مخفیانه‌تر خواهد بود. هوش مصنوعی فرآیند ایجاد ایمیل‌های فیشینگ با استفاده از ربات‌ها را خودکار می‌کند. جعل عمیق از هوش مصنوعی استفاده و حوزه اجتماعی جهان را مختل می‌کند. پس از استفاده از هوش مصنوعی، شکستن رمز عبور آسان‌تر خواهد بود.

با اتصال دستگاه‌های بیشتری به اینترنت (IOT)، نظارت بر حملات سایبری دردسر بیشتری خواهد داشت. زیرا اکنون هکرها نقاط پایانی بیشتری برای ورود به سیستم خواهند داشت.

محاسبات کوانتومی نگاه ما به جرایم سایبری را کاملا متحول خواهد کرد. قدرت عظیم محاسبات کوانتومی باعث ایجاد رخنه‌های می شود که در محاسبات معمول قابل قیاس نیست. با بکارگیری محاسبات کوانتومی، هر شرکتی در جهان که داده‌ها را ضبط و پردازش می‌کند، به شدت مستعد حملات سایبری خواهد بود.

منابع

۱.https://www.blackhat.com/presentations/bh-dc-09/Laurie/BlackHat-DC-09-Laurie-SatelliteHacking.pdf

2.https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932

3.https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/

4.https://www.livemint.com/news/india/top-russian-missile-makers-data-breached-by-hackers-ofnorth-korea-says-reportmashinostroyeniya-11691457476142.html

5.https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-anaircraft/?sh=1c2e7f0c41d1

6.https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-usfighter-jet-plans

7.https://www.popularmechanics.com/military/aviation/a25100725/f-35-vulnerability-hacked/

8.https://news.sophos.com/en-us/2017/06/29/hacking-nuclear-submarines-how-likely-is-thenightmare-scenario/

9.https://www.theguardian.com/uk-news/2017/jun/01/uks-trident-nuclear-submarines-vulnerable-tocatastrophic-hack-cyber-attack

10.https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

11.K.B.Vlahos,Special report:The cyberwar threat from north korea, Fox News, accessed 26/05/14 (February2014). URL:http://www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-northkorea-cyber-capabilities/

12. R.Wilking, Expert: Us in cyberwar arms race with china, russia, NBC News, accessed 25/05/14

(February 2013). URL: http://investigations.nbcnews.com/_news/2013/02/20/ 17022378-expert-usin-cyberwar-arms-race-with-china-russia

13. I. Traynor, Russia denounces ukraine 'terrorists' and west over yanukovich 680 ousting, BBC News,accessed 25/05/14 (February 2014).URL http://www.theguardian.com/world/2014/feb/24/russiaukraine-west-yanukovich

14. Ukraine says donetsk 'anti-terror operation' under way, BBC News, accessed 25/05/14 (April 2014). URL: http://www.bbc.com/news/world-europe-27035196

15.FBI, Terrorism definition, Online, accessed 25/05/14(2014).URL http://www.fbi.gov/aboutus/investigate/terrorism/terrorism-definition

16. Sanger, The Perfect Weapon; Healey, 'A Non-State Strategy for Saving Cyberspace'; Nye Jr, 'Deterrence and Dissuasion in Cyberspace'; Mehmetcik, 'A New Way of Conducting War:

Cyberwar, Is That Real?'; Singer and Friedman, Cybersecurity and Cyberwar; Healey, 'The Spectrum of National Responsibility for Cyberattacks.'

17. Healey, 'The Spectrum of National Responsibility for Cyberattacks', 57.

18. Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', Security Studies 22, no. 3 (2013): 365–404; Michael Stohl, 'Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?', Crime, Law and Social Change 46, no. 4–5 (2006): 223–38.

19. Bryan Bender, 'World More Dangerous, Top General Tells Harvard', BostonGlobe.com, 2012,
https://www.bostonglobe.com/news/nation/2012/04/12/world-more-dangerous-top-general-tellsharvard-world-more-dangerous-top-general-tells-harvard/XrSM8cTzyZ0YstKv36JhJN/story.html.

20. Gopal Ratnam and Gopal Ratnam, 'Cybersecurity Budget up 5 Percent in 2020, White House Says', Roll Call, March 20, 2019, sec. whitehouse, https://www.rollcall.com/news/whitehouse/cybersecurity-up-5-percent-in-2020-budget-white-housesays; Sanger, The Perfect Weapon.

21. Lindsay, 'Stuxnet and the Limits of Cyber Warfare'; Alex Gibney, Zero Days, Documentary, 2016.

22. Jerry Brito and Tate Watkins, 'Loving the Cyber Bomb - The Dangers of Threat Inflation in Cybersecurity Policy', Harvard National Security Journal 3, no. 1 (2011): 39–84.

23. Thomas Rid, 'Cyber War Will Not Take Place', Journal of Strategic Studies 35, no. 1 (2012): 5–32; Jon Randall Lindsay, 'Restrained by Design: The Political Economy of Cybersecurity', Digital Policy, Regulation and Governance, 2017; Erik Gartzke, 'Making Sense of Cyberwar', Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, January, 2014, 41–73.

24. Justin Joque, Deconstruction Machines: Writing in the Age of Cyberwar (University of Minnesota Press, 2018), chap. Introduction.

25. Lindsay, 'Restrained by Design: The Political Economy of Cybersecurity', 498.

26. https://owasp.org/

۲۷https://en.wikipedia.org/wiki/Ministry_of_Electronics_and_Information_Technology

28. https://www.wired.com/2014/11/airhopper-hack

۲۹. سایت گرداب به آدرس https://gerdab.ir

۳۰. سایت گروه سایبری ایران هک به آدرس https://www.iranhack.com

۳۱. خبرگزاری فارس به آدرس https://www.farsnews.ir

۳۲. خبرگزاری مهر به آدرس https://www.mehrnews.com