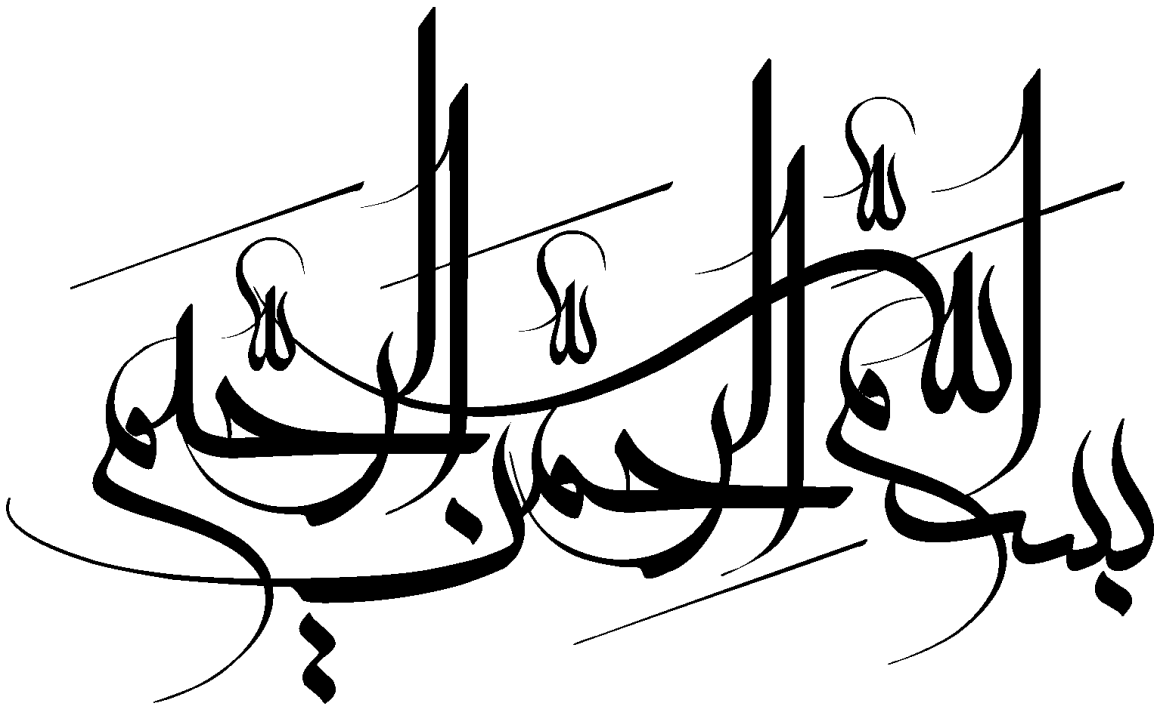
کتابچه آموزشی
پدافند سایبری ۱

ویژه دوره آموزشی عمومی پرسنل دانشگاه علوم پزشکی تبریز


بسم الله الرحمن الرحیم

شناسنامه سند: پدافند سایبری	
نام سند	پدافند سایبری
نگارش	پاییز ۱۴۰۱
تاریخ صدور	پاییز ۱۴۰۱
نام کامل فایل	پدافند سایبری
شرح سند	پدافند سایبری(ویژه کلیه کارکنان بعنوان دوره عمومی)
نویسنده/مترجم	مرکز ملی آموزش مدیریت سلامت NPMC

فهرست مطالب

عنوان **صفحه**

۱– مقدمه

دوران کنونی نقطه ی برجسته ای در روند تکامل آن چه که از آن بعنوان دفاع سایبری یاد می شود، است. تخریب داده ها، سرقت ایده ها، حمله به کارت های اعتباری، جعل هویت، خطرات پیش روی حریم خصوصی، حملات ایجاد وقفه در سرویس دهی و دیگر تهدیدات تبدیل به جزیی از زندگی روزمره ما شده اند. از سوی دیگر امکانات دفاعی بی شماری همچون ابزارها و تکنولوژی های امنیتی، استانداردها، کلاس های آموزشی، گواهینامه های امنیتی، اطلاعات آسیب پذیری ها، راهنماها و چک لیست های گوناگون امنیتی، معیارها و توصیه های ایمنی و بسیاری دیگر در اختیار متخصصان امنیت سایبری قرار دارد. هم چنین برای کمک به درک بهتر خطر حملات به اهمیت اطلاع رسانی از شیوه های حملات ،گزارشات، ابزارها و سرویس های هشدار دهنده، استانداردها و ابزارهای اشتراک گذاری اطلاعات خطرات پی برده ایم. در واقع می توان گفت هم اکنون هیچ گونه کمبودی در زمینه تامین اطلاعات لازم جهت ایمن سازی سازمان ها برای متخصصین وجود ندارد. ازسویی دیگر این حجم عظیم اطلاعات و تکنولوژی های گوناگون و روند رو به رشد استفاده از فناوری های مختلف، وجود کاربران سیار و پیچیده تر شدن حملات باعث سردرگمی سازمان ها برای انتخاب بهترین شیوه مقابله با حملات شده است. تکنولوژی های جدید با وجود مزایای بی شماری که دارند، موجب شده اند که داده ها و برنامه های ما در مکان های گوناگون و بعضا خارج از مرزهای سازمان انتشار یابند. دردنیای پیچیده و به هم متصل امروزی هیچ سازمانی نمی تواند به امنیت بعنوان یک چالش شخصی و صرفا منحصر به محدوده خود بنگرد. سوالی که اکنون مطرح میشود آن است که چگونه می توانیم در قالب یک اجتماع (اجتماع به معنای کلی و هم چنین اجتماعات درون صنایع، بخش ها و حوزه های گوناگون) با یکدیگر متحد شده و اولویت ها، تکنولوژی ها و معیارها و دانش خود را - در شرایطی که خطرات و امکانات امنیتی بطور مداوم در حال تغییر و پیشرفت هستند - به روز نگه داریم؟ چگونه مهم ترین فاکتورهایی که موجب تامین امنیت سازمان می شوند را تعیین نموده و اولین گام را در راه ایجاد برنامه های مناسب مدیریت بحران سازمان برداریم؟ چگونه به جای آنکه تنها پس از وقوع حملات به آنها واکنش نشان دهیم به طور اصولی نیازهای امنیتی سازمان را برطرف نماییم؟

در این بسته آموزشی اصول و مبانی پدافند سایبری در ۴ گام تشریح می شود.

گام ۱: آشنایی با مفهوم سایبر

تعریف فضای سایبری

شبکه های وابسته به یکدیگر، از زیرساخت های فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های تعبیه شده (جاگذاری شده)، کنترل گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط وانسان به منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات است. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه های فناوری اطلاعات و شبکه های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد.

فضای سایبر (Cyberspace) عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. به نظر می رسد به کارگیری این اصطلاح در این زمینه و برای ارجاع به امور فنی به آن رنگ و بویی صرفا

فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشان می‌دهد که این واقعیت، وجوه و جنبه های متنوعی از جمله خصلت های روانشناختی قابل توجه نیز دارد. در منابع موجود آمده است که:

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر[۱] در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم ها در سیستم‌های انسانی، ماشینی (و کامپیوتر ها) است.

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر بوجود آمده است که به تعدادی از آنها اشاره می‌کنیم: فضای سایبر[۲]، شهروند سایبر [۳]، پول سایبر[۴]، فرهنگ سایبر[۵] ، راهنمایی فضای سایبر[۶]، تجارت سایبر[۷]، کانال سایبر[۸] و....

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون[۹] نویسنده داستان علمی تخیلی در کتاب نورومنسر[۱۰] در سال ۱۹۸۴ به کار برده است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرارکنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد.

---

1 Norbert Wiener
2 Cyberspace
3 Cybercitizen
4 cybercash
5 Cyberculture
6 CyberCoach
7 Cyberbusiness
8 Cyberchannel
9 William Gibson
10 Necromancer

فضای سایبر گستره ایی از ذهن است که می تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد. شما می توانید حالت های متنوع و متفاوت ذهنی را از قبیل تخیلات (خیال پردازی ها) خیال پروری ها، توهمات، حالات هیپنوتیستیک و سطوح گوناگونی از هوشیاری را در فضای مجازی تجربه کنید.

تحت این چنین شرایط است که فضای سایبر همانند دنیای "رویا" می شود. دنیایی که وقتی ما به خواب فرو می رویم، پدیدار می شود. فضای سایبر را نمی توان تنها یک"بزرگ شاهراه اطلاعاتی" ساده دانست. زیرا تجربه ذهنی ما در فضای مجازی با تجربه ذهنی ما زمانی که بی هیچ هدف و ارزشی خیالبافی می کنیم، کاملا متفاوت است.

در واقع همانگونه که علم روانشناسی خواب شبانه را برای حفظ سلامتی، توسعه عاطفی و رشد شخصیت یک فرد ضروری می داند، این فضای مجازی هم بیش از هر چیز دیگری در خدمت روان انسان است. زیرا مرزهای بین وا قعیت های آگاهانه و نا آگاهانه را به هم نزدیک ساخته و می تواند درباره معنای "واقعیت" چیز هایی به ما بگوید.

سرمایه های ملی سایبری

سرمایه ملی

به سرمایه ای اطلاق می گردد که نقش حیاتی در امنیت ملی، اقتصاد ملی و سلامت، ایمنی و اطمینان عمومی داشته باشد.

طبقه بندی سرمایه های ملی

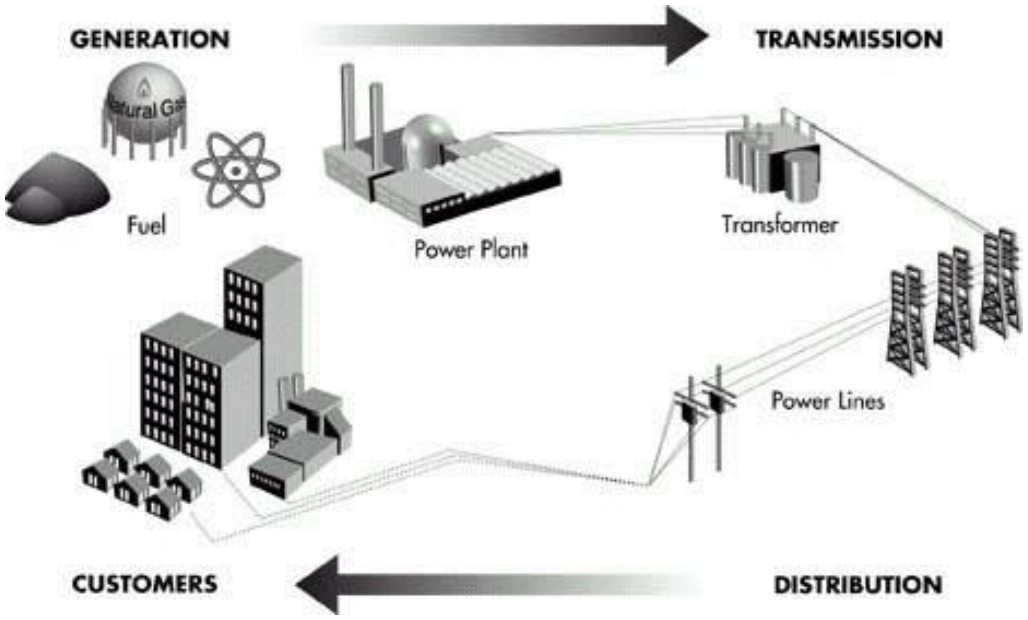
- سرمایه های فیزیکی
- سرمایه های انسانی
- سرمایه های سایبری

❖ سرمایه های ذهنی یا اعتباری

بخشی از دارایی های کشور اعم از زیرساخت ها، سامانه ها، تجهیزات، نرم افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از داده های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مستقیم و تعیین کننده داشته باشند و در فضای سایبری قابل حفظ، نگهداری و تهدید است. سرمایه های ملی سایبری را می توان به سرمایه های ملی سایبری حیاتی، حساس و مهم طبقه بندی کرد.

سرمایه های ملی فیزیکی که در فضای سایبر قابل مدیریت، کنترل و محافظت و تهدید باشد هم سرمایه ملی سایبری محسوب می شود.

❖ زیرساخت های سایبری حیاتی یا حساس
❖ سامانه های سایبری حیاتی یا حساس
❖ اطلاعات سایبری حیاتی یا حساس



ایجاد مفاهیم جدید در فضای سایبر

- خدمات الکترونیکی
- پست الکترونیکی (E- Mail)
- تجارت الکترونیکی
- آموزش الکترونیکی
- دولت الکترونیکی
- شهروند الکترونیکی
- شهر الکترونیکی

- سرقت الکترونیکی
- جاسوسی الکترونیکی
- تهدیدات الکترونیکی
- سرباز الکترونیکی
- حملات الکترونیکی
- ارتش سایبری
- .....

معماری فنی اینترنت اشیا (IOT[11])

اینترنت اشیا یا Internet of Things واژه‌ای نسبتا آشنا که چند وقتیست وارد حوزه‌ی تکنولوژی و زندگی ما شده است، شاید به درستی با معنا و مفهوم آن آشنا نباشیم، اما باید بدانیم در آینده‌ای نه‌چندان دور این فناوری به شکل بسیار گسترده‌ای در زندگی ما نقش خواهد داشت.

اینترنت اشیا (IoT) به طور کلی به فناوری اطلاق می‌شود که در آن تمام اشیا و وسایل اطراف ما به شبکه‌ی اینترنت و یا اینترانت (شبکه‌ی محلی) متصل شده‌اند و می‌توانند از طریق آن برای هم داده ارسال کرده و با هم در ارتباط باشند، در ضمن به راحتی و از طریق اپلیکیشن‌های خاصی توسط انسان‌ها قابل کنترل هستند.

[11] Internet of Things

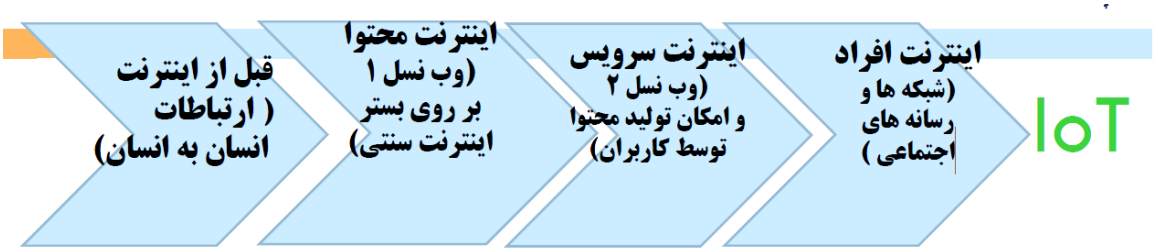
حتما تا به حال نام خانه‌های هوشمند را شنیده‌اید، یکی از کاربردهای وسیع و گستره‌ی IoT در خانه‌های هوشمند نمود پیدا می‌کند، خانه‌ای را در نظر بگیرید که بسیاری از اشیای موجود در آن از طریق یک شبکه به هم متصل‌اند.

به عنوان مثال هنگامی که شما خانه‌تان را ترک می‌کنید، لامپ‌ها خاموش شده و درب‌ها به صورت خود کار قفل می‌شوند، یخچال خانه به صورت اتوماتیک مواد غذایی موجود را بررسی کرده و در صورت کمبود برای فروشگاه مورد نظر شما پیامی ارسال می‌کند و محصولات مورد نظر را سفارش می‌دهد.

هم چنین هنگامی که شما مجددا در حال بازگشت به خانه هستید تلفن همراهتان موقعیت شما را برای شبکه‌ی خانگی ارسال کرده و با نزدیک شدن شما به خانه، سیستم سرمایشی یا گرمایشی فعال شده و محیط خانه را برای حضور شما دلچسب و آماده می‌کند. این یک نمونه‌ی بسیار ساده از کاربرد اینترنت اشیا در زندگی روزمره بود، مبحث IoT می‌تواند در موارد بسیار زیادی، از خانه‌های هوشمند گرفته تا مسائل پزشکی مورد استفاده قرار بگیرد.

نحوه‌ی شکل‌گیری و تاریخچه‌ی اینترنت اشیا

کلمه‌ی اینترنت اشیا واژه‌ی چندان قدیمی نیست، این مفهوم برای نخستین بار در سال ۱۹۹۹ میلادی استفاده شد و در آن جهانی را متصور می‌شدند که تمام افراد و همچنین اشیای بی‌جان از طریق شبکه و ابزارهای دیجیتال به هم متصل شده و بتوانند به برقراری ارتباط با یکدیگر بپردازند. همانطور که می‌دانید اینترنت هم‌اکنون تمام افراد جهان را به هم متصل کرده، اینترنت اشیا (IOT) نیز همانطور که از نامش پیداست قرار است تمام اشیا را به هم متصل کند.



IoT به لحاظ فنی چگونه عمل می‌کند؟

در اینجا سعی می‌کنیم به صورت خیلی ساده و ابتدایی این مقوله را بررسی کرده و اطلاعاتی کلی راجع به آن به شما ارائه دهیم. فرایند رد و بدل کردن داده در اینترنت اشیا می‌تواند از طریق پروتکل‌های مختلفی همچون بلوتوث، پروتکلZigBee ، ارتباط وای‌فای، پروتکل MQTT و... انجام پذیرد، در هر صورت هر شئ دارای یک شناسه‌ی یکتا و آدرس آی‌پی خواهد بود، شاید به نظر اختصاص دادن یک آدرس IP برای هر دستگاه معقول نباشد اما در اینجا لزوم به وجود آمدن آی‌پی ورژن ۶ (IPV6) را در می‌یابیم، در این نسل مشکل کمبود آی‌پی را نخواهیم داشت.

پس از اتصال وسایل به شبکه‌ی داخلی یا اینترنت آن‌ها می‌توانند برای یکدیگر داده ارسال کنند و در نهایت با هم در ارتباط بوده و با هم تعامل داشته باشند، در حقیقت این ارتباط، ارتباط "انسان با انسان" یا "انسان با ماشین" نخواهد بود بلکه یک ارتباط کامل بین "ماشین و ماشین" برقرار خواهد شد، در این حالت مودم‌ها، میکروپروسسورها و بردهای مختلف می‌توانند با هم به تبادل اطلاعات بپردازند.

ایده‌هایی از کاربرد اینترنت اشیا در زندگی روزمره

می‌توان از IoT در مقوله‌های بسیار زیادی استفاده کرد که ما در اینجا نمونه‌هایی از آن‌ها را ذکر می‌کنیم.

سلامت هوشمند: سنسورهایی به بدن بیمار متصل شده، علائم حیاتی وی را کنترل کرده و آن‌ها را به یک مرکز بررسی سلامت ارسال می‌کند.

خودروهای هوشمند: به عنوان یک نمونه، سنسوری که میزان باد تایرهای ماشین را بررسی کرده و در صورت وجود مشکل به راننده اطلاع می‌دهد.

خانه‌های هوشمند: موقعیت جغرافیایی صاحب خانه از طریق تلفن همراهش دریافت شده و با توجه به نزدیک شدن او به خانه، سیستم گرمایشی یا سرمایشی را کنترل می‌کند.

شهر هوشمند: کنترل ترافیک، روشنایی سطح شهر، مدیریت جای پارک خودروها، آبیاری هوشمند فضای سبز و... همه و همه می‌توانند ایده‌هایی برای ایجاد یک شهر هوشمند باشند.

سیستم‌های امنیتی: بررسی خودکار درب‌های ورودی و دوربین‌های مدار بسته و اطلاع‌رسانی در خصوص بروز مشکل.

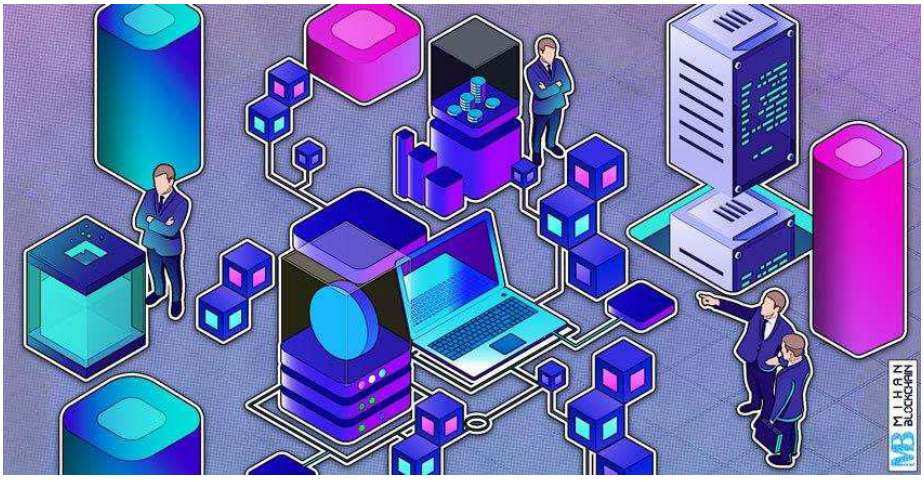
اگر بخواهیم IoT را بررسی کنیم مطمئنا به ایده‌های خلاقانه‌ی بسیار زیادی خواهیم رسید، از آنجایی که اینترنت اشیا یک مقوله‌ی نسبتا جدید و به‌روز در حوزه‌ی تکنولوژی است، کشورها به سرعت در حال کار کردن روی آن بوده و کشور ما نیز در صورت توجه به این حوزه می‌تواند به راحتی در آن پیشرفت کند.

آیا اینترنت اشیا امن و قابل اطمینان است؟

مانند هر تکنولوژی دیگری اینترنت اشیا نیز می‌تواند مورد نفوذ و سو استفاده قرار بگیرد و این مورد به یکی از چالش‌های پیش‌روی آن تبدیل شده است، همانطوری که بالاتر نیز گفتیم، برخی از اشیای اینترنتی می‌توانند موقعیت جغرافیایی ما را نیز رصد کرده و آن را پردازش کنند. هرچند این موضوع به تنهایی چندان نگران کننده نخواهد بود، اما مسئله‌ی اصلی وقتی شروع می‌شود که کنترل شبکه‌های ارتباطی و کنترل سیستم‌های مورد استفاده‌ی ما به دست افراد سودجو و خرابکار بیفتد.

در چنین مواقعی این تکنولوژی می‌توانند به شدت خطرناک بوده و حتی آسیب‌های جبران‌ناپذیری به جوامع انسانی وارد سازد، به عنوان مثال اگر چنین اتفاقی برای سیستم‌های یک بیمارستان اتفاق بیفتد می‌تواند بسیار مشکل‌زا و وحشتناک باشد.

فناوری بلاکچین و رمز ارز



این روزها کلمه بلاکچین[12] را بسیار می شنویم و این لغت جزء پرتکرارترین مفهومی است که از آن استفاده می شود و طبیعتا سوال بسیاری از ما این است که این فناوری جدید چیست؟ چگونه کار می کند و چه کاربردی دارد؟ اینها سوالاتی است که در مورد این فناوری بسیار پرسیده می شود. در این قسمت به ساده ترین شیوه ممکن توضیح داده می شود

تاریخچه فناوری بلاکچین

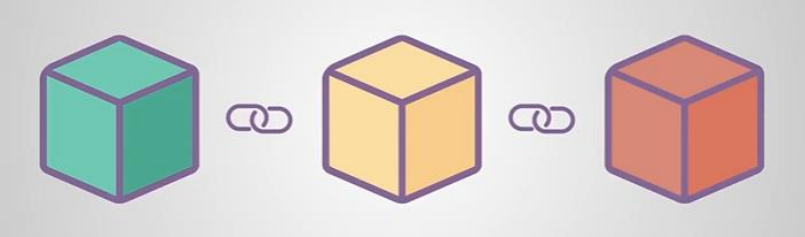
بلاکچین اولین بار در سال ۱۹۹۱ توسط گروهی از محققین استفاده شد. در ابتدا هدف استفاده از بلاکچین، زدن برچسب زمانی به اسناد دیجیتالی بود تا با این روش هیچکسی نتواند تاریخ انتشار اسناد را تغییر دهد یا اطلاعات آن را دستکاری کند. در واقع بلاکچین به عنوان یک دفتر اسناد معتبر عمل میکرد.

در آن زمان کمتر کسی از این فناوری استفاده میکرد تا زمانیکه در سال ۲۰۰۹ شخصی به نام ساتوشی ناکاموتو با استفاده از بلاکچین ارز دیجیتال بیت کوین را طراحی کرد. پس از آن علاوه‌بر بیت کوین، ارزهای دیگری توانستند از این فناوری استفاده کنند و کوین خود را راه اندازی کنند، بعدها با شناخت بیشتر و بهتر نسبت به این تکنولوژی، متخصصان دریافتند که تنها استفاده و کاربرد بلاکچین در ارزهای دیجیتالی نیست بلکه این تکنولوژی کاربردهای فراوانی دارد. در نتیجه می‌توان در زمینه‌های مختلف از آن استفاده کرد. در حال حاضر بلاکچین‌هایی با کاربردهای متفاوت در حال به کارگیری هستند که هر کدام از آنها متناسب با ویژگی‌هایشان، استفاده‌های متفاوتی دارند که در ادامه به آنها اشاره خواهیم کرد.

بلاکچین چیست؟

این واژه که از دو کلمه block و chain تشکیل شده به معنی زنجیره بلوکی است. در واقع زنجیره ای از بلوک هایی است که اطلاعات خاصی را در خودشون نگهداری میکنند. بلاکچین مثل یک دفتر کل توزیع شده برای ثبت اسناد هست که همواره دسترسی به آن برای همه افراد شبکه امکان پذیر است. ویژگی منحصر به فرد بلاکچین این است که اطلاعات ثبت شده در آن به راحتی قابل تغییر دادن نیستند.

[12] blockchain



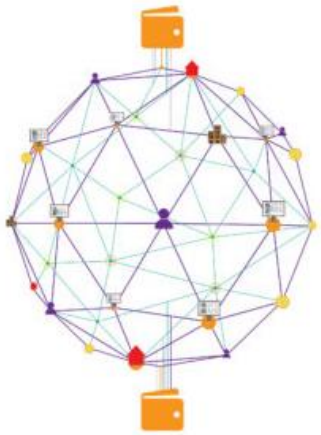
بلاکچین چطور کار میکند؟

به طور کلی هر بلاک از سه بخش تشکیل شده است که شامل:

- اطلاعات مربوط به بلاک (Data)
- هَش بلاک (Hash)
- هش بلاک قبل (Hash of previous block)

این اطلاعات بر اساس نوع بلاکچین ذخیره میشوند. به عنوان مثال در بلاکچین بیت کوین اطلاعات مربوط به معاملات از جمله طرفین معامله و تعداد بیت کوین ها نگهداری میشوند. هر بلاک یک هَش منحصر به فرد دارد که مانند اثر انگشت عمل میکند و میتواند بلاک را با تمام محتویات آن شناسایی کند.

در واقع به محض استخراج هر بلاک هش مخصوصی به آن بلاک نسبت داده می‌شود و با هر تغییری در هر بلاک هش مربوط به آن تغییر میکند. به عبارتی برای بررسی تغییرات اعمال شده در هر بلاک می شود به هش بلاک مراجعه کرد. اگر هش یک بلاک تغییر کند در واقع به بلاک جدید تبدیل میشود و هش بلاک قبلی بخش سوم هر بلاک را تشکیل میدهد. وجود هش بلاک قبل در بلاک جدید آنها را به صورت زنجیروار به همدیگر متصل میکند و باعث می شود بلاکچین ها امنیت بالایی داشته باشند.



شاید تصور کنید که فناوری بلاکچین مانند یک پایگاه داده میماند اما چنین نیست. اگر بخواهیم ساده بگوییم **پایگاه داده**، فضایی است برای ذخیره اطلاعات که طبیعتا این پایگاه داده توسط یک فرد یا مرکزیت، ایجاد و کنترل می‌شود. **فناوری بلاکچین** را می‌توان شبکه‌ای در نظر گرفت که کارکردی مانند پایگاه داده دارد اما مرکزیت خاصی ندارد و توسط نهاد یا ارگانی کنترل نمی‌شود.

اطلاعاتی که در بلاکچین ذخیره می‌شوند یک سری تفاوت‌هایی با اطلاعات ذخیره شده در پایگاه داده‌ها دارد، در بلاک چین تمامی اطلاعات ثبت شده بین تمام اعضای شبکه به اشتراک گذاشته می‌شود و همانطور که گفتیم نکته مهم فناوری بلاکچین این است که این اطلاعات به هیچ عنوان قابل ویرایش و یا حذف نیستند مگر اینکه دیگر بلاک ها نیز تغییر کنند که برای این کار تمام شبکه باید این تغییر را تایید کنند. در غیر این‌صورت هیچ اعتباری ندارد و تغییرات اعمال نمی‌شود. پس این دیدگاه که اطلاعات در بلاک چین غیرقابل تغییر است، درست نیست.

به عنوان مثال فرض کنید فردی شناسه یک فایل موسیقی را در یک بلاک چین قرار داده و ذخیره می‌کند. همه اعضای شبکه به آن دسترسی دارند حتی اگر خود فرد شناسه موسیقی را حذف کند یا تغییر دهد، بقیه اعضای شبکه این اتفاق را نمی‌پذیرند زیرا کپی نسخه اصلی آن شناسه موسیقی را دارند. برای حذف این فایل راهی نیست جز اینکه بیش از نصف کامپیوترهای شبکه را تصرف کرده و آن فایل را حذف کنید که عملا چنین اتفاقی امکان‌پذیر نیست.

کاربردهای بلاک چین

فناوری بلاکچین منحصر به بازار ارزهای دیجیتال نیست. همانطور که در تعریف این فناوری اشاره کردیم، بلاکچین بستری برای ذخیره اطلاعات به روشی مخصوص به خود است. هرچند حوزه ارزهای دیجیتال به دلیل ارتباط با مباحث اقتصادی و مالی و مسائل سرمایه گذاری و کسب درآمد بیشتر مورد توجه قرار گرفته است، اما بلاک چین کاربردهای بیشتری دارد.

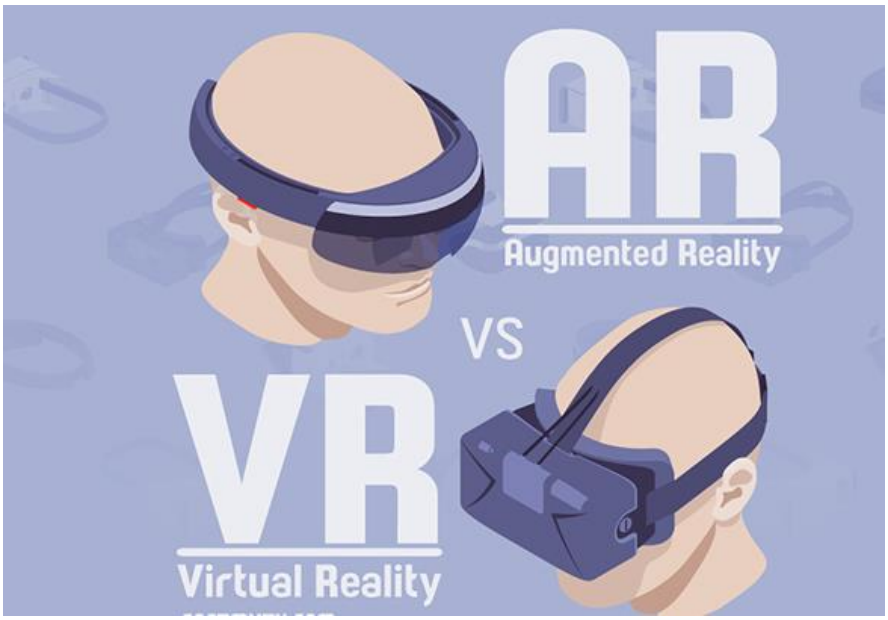
برخی از افراد معتقدند که از کاربردهای فناوری بلاک چین، محافظت از حقوق افراد است. به عبارتی، می‌توان از فناوری بلاک چین به خوبی در محافظت از حق امتیاز و مبارزه با جعل داده‌ها استفاده کرد. به دلیل شفافیت و قابلیت ردیابی اطلاعات در شبکه‌های بلاکچین، می‌توان از آن در حفظ حقوق مادی و معنوی افراد در تولید اثر استفاده کرد.

بسیاری از شرکت‌هایی که به تولید و عرضه تلفن‌های همراه مشغولند، از بلاک چین در محصولات خود استفاده می‌کنند. شرکت سامسونگ در گوشی‌های سری جدید گلکسی خود از تکنولوژی بلاک چین استفاده کرده است.

یکی دیگر از کاربردهای بلاکچین در صعنت پزشکی است. در این حوزه حتی محصولاتی کاربردی عرضه شده که مورد استفاده قرار گرفته است. برای مثال، پلتفرم ClinTex با هدف رساندن منابع دارویی به بازار با قیمت رقابتی، به صورت مستقیم به افرادی که بیشترین نیاز را به آنها دارند مورد استفاده قرار می‌گیرد. فرایند به اشتراک‌گذاری داده‌ها برای آزمایش‌های بالینی موجب ایمن‌سازی انتقال اطلاعات بلاک چین، فراگیری ماشین و پروتکل‌های هوش مصنوعی برای تجزیه و تحلیل پیش‌بینانه داده می‌شود.

واقعیت مجازی (VR[۱۳]) و واقعیت افزوده (AR[۱۴])

فناوری در تمام عرصه های زندگی ما نفوذ کرده و همه سیستم ها و ساختارهای معاملاتی را متحول کرده است. در همین حال، فناوری‌های مدرن مانند متاورس ها و بسیاری از مفاهیم دیگر به نوعی در ارزهای دیجیتال ادغام شده‌اند و تجربیات جدیدی را برای انسان‌ها فراهم می‌کنند که هرگز رویایی بیش نبودند. در این بخش می خواهیم به بررسی تفاوت واقعیت مجازی و واقعیت افزوده بپردازیم.



واقعیت مجازی (VR) چیست؟

واقعیت مجازی یک شبیه سازی کامپیوتری است که تلاش می کند یک جهان یا واقعیت جایگزین برای انسان ها ایجاد کند. این فناوری اساساً یک واقعیت خیالی تولید شده توسط رایانه است که سعی می کند واقعیت را به قدری نزدیک کند که یک تجربه سه بعدی واقعی را برای کاربر ایجاد کند. با استفاده از واقعیت مجازی، کاربر می تواند رویدادهایی را تجربه کند که می تواند چالش برانگیز یا کاملاً تخیلی باشد و تجربه آنها در دنیای واقعی غیرممکن است. این فناوری تجربه زندگی در واقعیتی است که در واقع وجود ندارد یا

[13] Virtual Reality
[14] Augmented Reality

ممکن است در جایی واقع شده باشد اما به دلایلی در دسترس نیست. مثلا غواصی که برای همه امکان پذیر نیست.

واقعیت مجازی مبتنی بر مجموعه‌ای از ابزارهای خاص مانند عینک واقعیت مجازی، هدفون، دستکش‌های لمسی است که هم‌اکنون در دسترس عموم قرار گرفته‌اند. این ابزارها تصاویر یا ویدئوها را از طریق هدست و سیستم صوتی نمایش می دهند و سعی می کنند محیطی کاملا واقعی را برای کاربر ایجاد کنند. به عنوان مثال، کاربر می تواند با استفاده از دستکش های مجازی، واقعیت مجازی را با دستان خود احساس کند، جسم را حرکت دهد یا حتی گیتار بزند.

تا به امروز، واقعیت مجازی راهی طولانی را پیموده است و کار بزرگی برای ایجاد یک محیط تعاملی انجام داده است. تصور کنید بتوانید وارد یک داستان نزدیک به واقعیت شوید، می توانید به اتفاقات آنجا متصل شوید و آنها را کاملا احساس کنید! این تجربه می تواند بسیار شگفت انگیز بوده و هیجان انگیز باشد.

بررسی مزایا و معایب واقعیت مجازی(VR)

مزایای واقعیت مجازی

۱- واقعیت مجازی وارد عرصه های بسیاری شده است و با ایجاد یک فضای سه بعدی، تجربه پرواز، نگاه، آزمایش و ... را در اختیار کاربر قرار می دهد.

۲- این فناوری با ایجاد یک محیط تعاملی در بسیاری از زمینه ها مانند آموزش، کار را تسهیل می کند. علاوه بر این، به کاربران اجازه می دهد تا آزمایشات خود را در یک محیط مصنوعی انجام دهند.

۳- این فناوری به کاربر کمک می کند دنیایی واقع گرایانه بسازد و دنیا را تجربه کند و به انسان فرصتی برای تجربه هایی می دهد که شاید در دنیای واقعی چندان ساده به نظر نرسند. یکی از بهترین نمونه های واقعیت مجازی، سفر به قعر اقیانوس ها است که مورد استقبال بسیاری قرار گرفته است.

معایب واقعیت مجازی

۱- واقعیت مجازی ذاتاً دارای نقص است. زیرا انسان ذاتاً علاقه مند است که در محیطی طبیعی و واقعی قرار گیرد که شاید واقعیت مجازی به تنهایی نتواند تجربه ای طبیعی برای انسان ایجاد کند و به دلیل کارکردی که دارد قادر به غلبه بر دنیای واقعی نباشد.

۲- این فناوری برای کار کردن به ابزارها و دستگاه های واقعیت مجازی نیاز دارد که برای برخی از افراد جامعه آسان نیست.

۳- کاربران نمی توانند برای مدت طولانی به طور مداوم از این ابزار استفاده کنند زیرا هر یک از ابزارهای لازم برای این فناوری وزن دارد و در دراز مدت پشتیبانی آن آسان نیست.

۳- مشکل دیگری که گاهی برای این فناوری در نظر گرفته می شود این است که برای کار در آن، کاربر هیچ ارتباطی با دنیای واقعی ندارد و کاملا در فضای دیگری قرار می گیرد که به هر حال واقعی نیست.

۵- علاوه بر موارد فوق، آموزش مهارت های مختلف در محیط VR هرگز نتایجی مشابه با آموزش و کار در دنیای واقعی نخواهد داشت و برای فردی که وظایف خود را به طور کامل در محیط VR انجام داده است، تضمینی برای موفقیت وجود ندارد .

کاربردهای واقعیت مجازی چیست؟

فناوری واقعیت مجازی تنها به حوزه بازی و سرگرمی محدود نمی شود، بلکه کاربردهای مختلفی را در بسیاری از زمینه های صنعتی، تجاری و آموزشی ارائه می دهد. بسیاری از شرکت های بین المللی مانند آمازون، متا (فیسبوک سابق) و گوگل روی این فناوری ها سرمایه گذاری کرده اند. به همین خاطر در ادامه به معرفی برخی از این کاربردها می پردازیم.

- بهداشت و درمان

از جمله کاربردهایی که می توان برای واقعیت مجازی در حیطه بهداشت و درمان بیان کرد، شبیه سازی جراحی، جراحی رباتیک و درمان فوبیاست. به علاوه، این فناوری قابلیت های آموزش جراحی را افزایش داده و دانشجویان از این طرق می توانند به درمان بیماران به صورت مجازی بپردازند .

- آموزش

واقعیت مجازی می تواند یادگیری را با ارائه تجربیات فراموش نشدنی (مجازی) به دانش آموزان افزایش دهد زیرا با کمک این فناوری می توان دانش آموز را به خارج از کلاس و هر مکانی منتقل کرد و علاوه بر آن استعداد و تخیل دانش آموزان را نیز شکوفا کرد.

- بازی

می توان از فناوری واقعیت مجازی برای ایجاد یک واقعیت خیالی در دنیای بازی استفاده کرد. اکنون بازی های زیادی برای سیستم عامل های مختلف از جمله اندروید و iOS وجود دارد که می توانید به راحتی آنها را دانلود کرده و هدست واقعیت مجازی خود را در فضای بازی قرار دهید و بازی کنید.

- ارتش

برای شبیه سازی شرایط ارتش نیز می توان از واقعیت مجازی استفاده کرد. این فناوری تاثیر فوق العاده ای بر روی نیروهای ارتش، درمان سربازان و کاهش تلفات نظامی دارد .

- ورزش

به لطف فناوری واقعیت مجازی، کاربر می تواند به طور مجازی ورزش مورد علاقه خود را بدون نیاز به ترک خانه برای رفتن به باشگاه یا استادیوم ارائه دهنده این فناوری انجام دهد. علاوه بر این، از این فناوری می توان برای اندازه گیری عملکرد یک ورزشکار و بسیاری موارد دیگر استفاده کرد

- واقعیت مجازی اجتماعی(Social VR)

از مهم ترین کاربردهای فناوری واقعیت مجازی بوده که این قابلیت را به کاربران می دهد تا در محیط واقعی با یکدیگر ملاقات و تعامل داشته باشند. در فعالیت های مشترک همچون تماشای فیلم، شرکت کنسرت یا حتی همکاری در محل کار حضور داشته باشید.

واقعیت افزوده (AR)

واقعیت افزوده (AR) ترکیبی عالی از دنیای دیجیتال و دنیای واقعی برای ایجاد یک محیط مصنوعی است که هدف آن شبیه سازی دنیای واقعی در دنیای دیجیتال است. به عبارت دیگر، این فناوری صحنه ای ترکیبی را برای کاربر ایجاد می کند. برای مثال، اگر گوشی هوشمند خود را در مقابل پلان ساختمان قرار دهید، این فناوری می تواند به شما کمک کند تا طرح سه بعدی ساختمان را ببینید و ساختمان ساخته شده بر روی این پلان را درک کنید. در واقع این فناوری صحنه واقعی مشاهده شده توسط کاربر و صحنه مجازی تولید شده توسط کامپیوتر را با یکدیگر ترکیب می کند.

هدف اصلی AR ایجاد محیطی است که درک تفاوت بین دنیای واقعی و آنچه که با استفاده از فناوری واقعیت افزوده به محیط اضافه شده است، کار آسانی نباشد. برای تجسم یک عنصر در دنیای واقعی، می توان بدون حضور این عنصر و با استفاده از این فناوری و ابزارهای مرتبط، عنصر را در دنیای واقعی شبیه سازی کرد. با این اقدام، فناوری AR سعی می کند درک حسی کاربر از دنیای واقعی که با آن در تعامل است را بهبود بخشد. واقعیت افزوده را می توان در طیف گسترده ای از زمینه ها مانند آموزش، سرگرمی، تجارت و موارد دیگر، مورد استفاده قرار داد. این فناوری نه تنها دنیای مجازی را به عنوان دروازه اصلی ما به متاورس ها تحت الشعاع قرار می دهد بلکه جایگزین اکوسیستم فعلی تلفن ها و رایانه های شخصی شده است. AR به‌عنوان رابط اصلی ما با محتوای دیجیتال عمل می‌کند و به ما کمک می‌کند با یک نگاه یا یک اشاره، دنیای خود را تغییر دهیم.

فناوری AR مبتنی بر استفاده از تلفن همراه، لنزهای تماسی، عینک، صفحه نمایش و دوربین است. این فناوری با محیط واقعی تعامل دارد و از طریق دستگاه های هوشمند مجهز به دوربین (برای جمع آوری اطلاعات در مورد محیط) و حسگرهای بسیار حساس (برای تجزیه و تحلیل محیط واقعی) کار می کند.

مزایای واقعیت افزوده (AR)

۱- با توجه به ساختار واقعیت افزوده می توان این فناوری را به سرعت به بازار معرفی کرد .

۲- در مقایسه با سایر فناوری‌ها مانند VR که نیاز به استفاده از ابزارهای رابط دارند، این فناوری (AR) به دستگاه خاصی نیاز ندارد و کافی است دستگاه دیجیتال شما (موبایل و تبلت) از این فناوری پشتیبانی کند.

۳- AR کاربر را قادر می سازد تا کارهای حساس و جالبی را در مکان خود انجام دهد که منجر به استفاده گسترده از این فناوری می شود.

۴- این فناوری را می توان به عنوان کمک قابل توجهی به طیف وسیعی از زمینه ها مانند سرگرمی، نظامی، آموزش و پرورش و به عنوان مثال، واقعیت افزوده می تواند روند یادگیری کاربران را بهبود بخشد.

معایب واقعیت افزوده (AR)

علاوه بر مقیاس و مزایای واقعیت افزوده، که برخی معتقدند در آینده ای نسبتا نزدیک زمین را پوشش می دهد، باید توجه داشت که این فناوری شگفت انگیز نقاط ضعف خود را نیز دارد.

۱- اجرا و نگهداری پروژه های مبتنی بر فناوری AR بسیار پرهزینه است.

۲- فقدان حریم خصوصی و امنیت در این فناوری ممکن است برای برخی از کاربران خوشایند نباشد و بر اصل کلی واقعیت افزوده تأثیر بگذارد.

۳- پایین بودن عملکرد دستگاه های سخت افزاری AR از دیگر معایب این فناوری است.

۴- یکی از مشکلاتی که ممکن است در درازمدت متوجه شویم، تعامل شدید با این فناوری است که می‌تواند منجر به مشکلات سلامتی مانند مشکلات چشمی و چاقی شود.

کاربردهای فناوری واقعیت افزوده

پتانسیل واقعیت افزوده بی پایان است و هنوز به آن نقطه نرسیده است که وارد بخش زیادی از زندگی انسان شود. در این میان تعدادی از شرکت ها و سازمان ها در حال انجام کارهای بزرگی با این فناوری است. در ادامه برخی از کاربردهای این فناوری را بیان می کنیم.

- اپلیکیشن موبایل ایکیا

یکی از اولین شرکت هایی که از فناوری واقعیت افزوده به خوبی استفاده کرد، شرکت ایکیا است. با استفاده از این فناوری، این شرکت به خریداران این قابلیت را می دهد که هر محصولی را که دوست دارند از کاتالوگ انتخاب کنند، از آن در محیط خانه خود عکس بگیرند، ترکیب آن را با طراحی فعلی خانه خود ارزیابی کنند و علاقه مند شوند و محصول را با خانه خود تطبیق داده و در نهایت آن را بخرند.

- اپلیکیشن Pokemon go

از شناخته شده ترین اپلیکیشن هایی که از فناوری واقعیت افزوده استفاده کرد است بازی Pokemon go است. در این بازی و به کمک این فناوری، کاربر این قابلیت را خواهد داشت تا محتوای دیجیتالی (کاراکتر بازی) رادر دنیای واقعی نمایش دهد .

- کتاب رنگ آمیزی دیزنی

چند سال پیش، دیزنی از فناوری AR استفاده کرد و این قابلیت را به کاربران خود داد تا شخصیت مورد علاقه خود را به صورت سه بعدی تماشا کنند. همچنین این شرکت از واقعیت افزوده استفاده می کند تا به کودکان اجازه دهد تصاویر رنگی یک کتاب رنگ آمیزی سه بعدی را در تلفن همراه یا تبلت مشاهده کنند. این اپلیکیشن هنوز در مراحل اولیه بوده و در دسترس عموم قرار نگرفته است.

- ارتش ایالات متحده

همه پارامترهایی موجود در واقعیت افزوده سرگرمی و بازی نیستند. از سوی دیگر، دولت ها از فناوری برای مسائل سیاسی و حتی جنگی استفاده می کنند. به عنوان مثال، ارتش ایالات متحده در حال کار بر روی برنامه های واقعیت افزوده است تا از آن برای کمک به سربازان در ایجاد تمایز بین سربازان دوست و دشمن در جنگ و بهبود دید در شب استفاده کند. اگرچه AR همچنان به تکامل خود ادامه می دهد، مقامات جنگ می گویند این فناوری کارایی جنگ را بهبود می بخشد و می تواند به جلوگیری از تلفات غیرنظامیان کمک کند

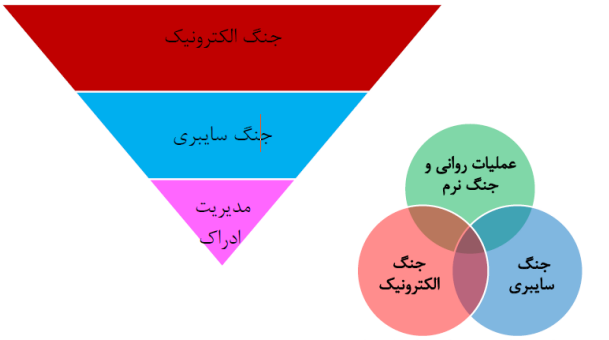
تفاوت های واقعیت افزوده با واقعیت مجازی

بسیاری از مردم تصور غلطی دارند که واقعیت مجازی و واقعیت افزوده با یکدیگر برابر هستند. البته این دو فناوری شبیه هم هستند اما تفاوت های زیادی با هم دارند. وجه اشتراک واقعیت مجازی و واقعیت افزوده

تغییر درک ما از جهان است. در جایی که این دو فناوری با هم تفاوت دارند، درک حضور ما در محیط ایجاد می شود. در ادامه به برخی از تفاوت واقعیت مجازی (VR)و واقعیت افزوده (AR) اشاره خواهیم کرد.

- تفاوت واقعیت مجازی (VR)و واقعیت افزوده(AR)، این است که در واقعیت افزوده کاربر با دنیای واقعی تعامل دارد اما در واقعیت مجازی کاربر با دنیای واقعی ارتباط برقرار نمی کند و تنها ارتباط آن با دنیای مجازی است .
- ابزارهای رابط فناوری واقعیت مجازی که برای استفاده از این فناوری ضروری هستند، بیش از ابزارهای لازم برای فناوری واقعیت افزوده هستند. حتی تلفن های هوشمند نیز منابع لازم برای اجرای AR را دارند اما واقعیت مجازی به تجهیزات اختصاصی نیاز دارد.
- فناوری AR برای جمع آوری داده ها از دنیای واقعی نیاز به حسگر دارد اما در فناوری واقعیت مجازی کاربر از دنیای واقعی جدا شده و نیازی به تجهیزات این چنینی ندارد.
- اختلاف دیگری که دو واقعیت با یکدیگر دارند اجرای واقعیت افزوده هزینه کمتری نسبت به اجرای واقعیت مجازی دارد.
- محصولات AR در حال حاضر در دسترس هستند. عینک گوگل نمونه خوبی از یک محصول واقعیت افزوده است. از سوی دیگر هیچ سیستم واقعیت مجازی که بتواند کاربر را به طور کامل در دنیای دیجیتال و متفاوت غرق کند وجود ندارد.
- قدرت پردازش گرافیکی برای واقعیت مجازی ضروری تر از واقعیت افزوده است.
- از دیگر تفاوت **واقعیت مجازی و واقعیت افزوده**، الگوریتم و نرم افزار است. الگوریتم ها و نرم افزارهای واقعیت مجازی بزرگتر و پیچیده تر از آنهایی هستند که در واقعیت افزوده مورد استفاده قرار می گیرند.

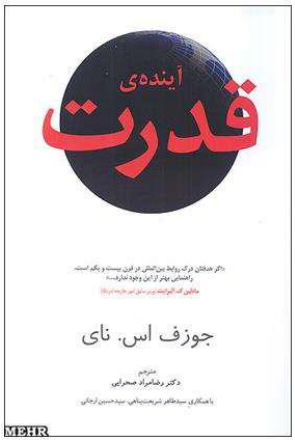
گام ۲: عصر اطلاعات / جنگ اطلاعات



مدل لایه ای جنگ اطلاعات بومی شده

مبانی عملیات سایبری

جوزف ساموئل نای مبتکر تئوری قدرت نرم و استاد دانشگاه هاروارد در کتاب آینده ی قدرت، پس از تفکیک فضای سایبر به دو لایه زیرساخت فیزیکی و مجازی (اطلاعات)، با اشاره به جنبه اقتصادی تهدید در فضای سایبر، تأکید دارد که لایه اطلاعاتی فضای سایبر، از بازده فزاینده نسبت به مقیاس برخوردار بوده و عرصه و حوزه سیاسی آن به گونه ای است که کنترل قانونی را مشکل می سازد، لذا بهتر است از حوزه اطلاعاتی که هزینه ها در آن پائین است، تهدید را علیه لایه فیزیکی که منابع آن کمیاب و گران هستند، اعمال نمود.



زمینه سازان جنگ سایبری

- اتکاء زیاد به فناوری غیر بومی
- اعتماد به ابزار و تجهیزات غیر خودی
- وابسته شدن زیرساختهای حیاتی به فناوری آسیب پذیر
- وابسته شدن خدمات حیاتی به بستر اینترنت
- عدم رعایت ملاحظات و توصیه های امنیتی و پدافندی در استفاده از فناوری

جنگ سایبری و نفوذ های هد فمند

در این قسمت تعریف برخی از مفاهیم حوزه سایبر آورده شده است

تهدید سایبری

هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریتها، وظایف، تصویر(پنداره)یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا پرسنل دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، تخریب، افشاء، تغییراطلاعات و / یا ممانعت از(ایجاد اختلال در)ارائه خدمت.

تهدیدات ناشی از فعالیت ها در فضای سایبری حداقل سه مشخصه دارند:

۱- گسترده:

طبیعت تهدید راهبردی در فضای سایبری همانند خود فضای سایبری گسترده است. هر بخشی از جهان که وابسته به فضای (حوزه) سایبر باشد حداقل به صورت بالقوه در معرض خطر قرار دارد. بنابراین کشورها با فعالیت های خصمانه ای روبرو هستند که می تواند تهدید کننده یکپارچگی زیرساخت های حیاتی آنها باشد به طوری که می تواند سامانه های مالی را از پایداری خارج سازد و یا به سارقان مالکیت معنوی امکان سرقت بدهد و یا به هر روش مهم دیگر توانایی کشورها برای اتکاء بر فناوری در جهت نیل به اهداف مهم امنیت ملی آنها را کاهش دهد.

۲- نهفته:

تهدیدات مربوط به یکپارچگی اطلاعات و امنیت در فضای سایبری عمیقاً در حوزه سایبر نهفته هستند. این تهدیدات ناشی از آسیب پذیری های بالقوه موجود یا قرار داده شده در سیستم های عامل نرم افزاری پیچیده و همچنین ناشی از سخت افزارهای بالقوه معیوب یا ناقص هستند. لفظ نهفته به این دلیل به کار می رود که تهدید بالقوه، ویژگی ذاتی فضای سایبری بوده و لذا هرگز نمی توان آن را بطور کامل کشف و آشکار نمود. این تهدیدات گاهی در زمان عبور کالاها از زنجیره تأمین در آنها تعبیه می گردند.

۳- متنوع:

تهدیدات در فضای سایبری متنوع هستند. گروه های جنایتکار و خرابکار با سازماندهی مناسب، سازمانهای مستقل مدیریتی و هکری از هر عنوانی، در صحنه حضور دارند. هر یک از این عاملان خرابکاری، نوع مجزایی از تهدید را تحمیل می نمایند.

هجوم سایبری:

به هرگونه اقدام غیرمجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دستیابی به اطلاعات سرمایه سایبری مذکور انجام گیرد، تهاجم سایبری اطلاق می گردد.

جنگ سایبری

جنگ سایبری، بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت. یکی از ویژگی های اصلی جنگ سایبری، آن است که این نوع از تهاجم سایبری، توسط ارتش سایبری کشورها و یا با حمایت دولت ها انجام می گیرد.

آسیب پذیری سایبری

آسیب پذیری، به ضعف موجود در داخل یک سرمایه، رویه های امنیتی یا کنترل های داخلی، یا پیاده سازی آن سرمایه ملی سایبری، که قابلیت بهره برداری یا فعال شدن توسط تهدیدات داخلی و خارجی به منظور انجام جنگ سایبری را داشته باشد، اطلاق می گردد.

رخداد سایبری

رخداد سایبری، پیامد یک تهاجم سایبری است و در تعریف، رویداد منتهی به نقض یا در شرف نقض قرار گرفتن سیاست امنیتی یک سرمایه سایبری است. ویژگی های اصلی رخداد سایبری، عبارت از غیرمنتظره بودن، اثرات سوء داشتن و اختلال ایجاد نمودن در عملکرد سرمایه سایبری است. رخدادهای سایبری نیز همانند تهاجمهای سایبری، قابل طبقه بندی های از منظرهای مختلف هستند که از آن جمله می توان به طبقه بندی حوادث سایبری از نظر فاکتورهای امنیتی نقض شده (نقض محرمانگی، حریم خصوصی، صحت و

...)، سامانه هایی که رخداد برای آنها بروز نموده (سامانه های وب، سامانه های پست الکترونیکی و...)، نوع پیامدهای رخداد سایبری (پیامدهای فیزیکی، اقتصادی، اجتماعی، سیاسی و ...)، پیچیدگی رخداد سایبری و گستردگی ابعاد رخداد سایبری اشاره نمود.

پیامد رخداد سایبری

پیامد رخداد سایبری، خسارت است .در اغلب موارد، خسارت، علاوه بر جنبه سایبری، جنبه غیرسایبری نیز دارد .برای نمونه، از دست دادن زمان موردنیاز برای ترمیم خرابی های ناشی از رخداد، خسارت اقتصادی ناشی از بروز رخداد، هزینه های بازیابی و رفع خرابی ها و صدمه به اعتبا ر کشور در سطح بین المللی بواسطه از کار افتادن سرمایه ملی سایبری، بویژه در مقاطع زمانی حساس برای کشور، اشاره نمود.

مهم ترین خسارات عمده یا مهم ترین پیامدهای عمده رخدادهای سایبری، برای سرمایه های ملی سایبری، می تواند یکی از موارد ذیل باشد:

- براندازی نظام حاکمیتی یا تهدید فاجعه بار امنیت ملی
- آغاز همزمان جنگ فیزیکی یا زمینه سازی و تسهیل شروع جنگ فیزیکی در آینده نزدیک
- تخریب یا صدمه فاجعه بار به وجهه کشور در سطح بین المللی
- تخریب یا صدمه فاجعه بار به روابط سیاسی و اقتصادی کشور
- تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی(از طریق ایجاد آلودگی هسته ای، شیمیایی یا بیولوژیک)
- هرج ومرج و شورش داخلی
- اختلال گسترده در اداره امور کشور

- تخریب (یا صدمه گسترده به) اطمینان عمومی یا باورهای دینی، ملی و قومی
- خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی
- تخریب یا اختلال گسترده در عملکرد سرمایه های ملی سایبری

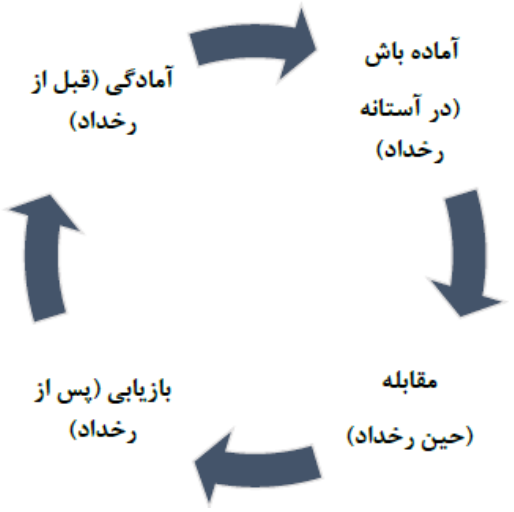
سطح رخداد سایبری

سطح رخداد سایبری، همانند سطح تهدید، مخاطره و تهاجم سایبری، عبارت است از:

- فراملی : رخداد گسترده دارای ابعاد بین المللی برای کشور
- ملی : رخداد در کل یا بخش گسترده ای از فضای سایبری کشور
- منطقهای : رخداد در فضای سایبری یک یا چند استان کشور
- محلی : رخداد در فضای سایبری یک یا چند شهر
- سرمایه ای : رخداد در یک یا چند سرمایه ملی سایبری
- سازمانی (دستگاهی :) رخداد در فضای سایبری یک یا چند دستگاه
- فردی : رخداد برای منافع یک یا چند فرد در فضای سایبر

چارچوب و الگوی طرح پاسخ اضطراری به تهدیدات سایبری:

چارچوب و الگوی طرح پاسخ اضطراری به تهدیدات سایبری در شکل زیر نشان داده شده است.



مراحل اصلی طرح پاسخ اضطراری به تهدیدات سایبری عبارتند از:

آمادگی(قبل از رخداد)

آماده باش (در آستانه رخداد)

مقابله (حین رخداد)

بازیابی (پس از رخداد)

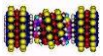
سلاح های سایبری و ویژگی های آن

فنون متعددی در جنگ سایبری وجود دارد که در دو بخش سخت افزار و نرم افزار قابل اجرا هستند.

الف) سلاح های سخت افزاری

۱- بمب تراشه ای (**Chipping Bomb**) 

تراشه های پیشرفته محتوی میلیون ها مدار الکترونیکی مجتمع هستند که شرکت های سازنده قادرند به راحتی آنها را برای بروز نقص و یا حتی انفجار در زمان معین یا پس از دریافت یک سیگنال با فرکانس خاص برنامه ریزی نمایند. حتی با ارسال فرکانس های خاص می توان موقعیت دقیق استقرار این تراشه ها را در سازمان یا کشور هدف تعیین کرد. تنها مشکل باقیمانده حصول اطمینان از استقرار این تراشه ها در نزدیکی هدف مورد نظر رزمنده سایبری است. ساده ترین راه کار تعبیه این ویژگی ها در کلیه تراشه های صادراتی به کشور هدف است.

۲- نانو ماشین ها (Nano Machines)(مورچه آتشین) 

ای‌ن ماشین ها روبوت های بسیار ریزی هستند که با انرژی خورشیدی کار می کنند و دارای حواس بینایی، بویایی، شنوایی و توان حرکت و انفجار بنابه دستور را دارا هستند. این روبوت ها قادرند از سوراخ های دستگاه های الکترونیکی وارد شده و مدارات الکترونیکی آنرا تخریب نمایند.

۳- میکروب های خورنده سیلیکن (Microbes) 

میکروبها باکتری های زنده ای هستند که بر روی مواد خاصی از قطعات سخت افزاری سیستم ها نظیر سیلیکون و پلاستیک رشد کرده و تکامل می یابند. این باکتری ها اگر وارد تجهیزات الکترونیکی شوند مدارهای الکترونیکی و مواد عایق را خورده و سیستم را غیر قابل استفاده می نمایند.

۴- درهای نفوذ

یک در نفوذ یا درپشتی، مکانیسمی است که در یک سیستم توسط سازنده آن تعبیه شده است و راه عبوری به سیستم مورد نظر و عبور از گره های امنیتی عادی برای وی محسوب می شود. کلیه سیستم های سخت افزاری تولید ایالات متحده مجهز به سیستم درهای نفوذ هستند به نحوی که به سادگی در جنگ اطلاعاتی بر علیه کاربران مورد استفاده قرار بگیرند.

۵- بمب پالس الکترومغناطیسی

منبع پالس می تواند یک انفجار هسته ای یا غیر هسته ای باشد. نیروهای ویژه پس از نفوذ به مناطق عقب دشمن می توانند در نزدیکی تجهیزات آسیب پذیر اقدام به تولید انفجار پالس الکترومغناطیسی نمایند که سیستم های رایانه ای و ارتباطی را در شعاع عمل خود مختل می نماید.

۶- پارازیت دهنده ها

ابزارهایی هستند که در مراکز C4I، سامانه های پدافند هوایی، رادارها و سایر سلاح هایی که توسط رایانه کنترل می شوند پخش شده و پارازیت یا صداهای باند کوتاه قوی را برای خراب کردن سیستم های حساس الکترونیکی تولید می نمایند.

۷- فرکانس رادیویی پر انرژی

این فرکانس ها توسط فرستنده های رادیویی بر روی اهداف الکترونیکی ارسال و موجب اختلال در عملکرد آن می شود

۸- دستگاه های الکترومغناطیسی ناپایدار

این دستگاه ها پالس های تیرک مانندی را تولید می کنند که دارای طول موج بسیار کوچکی بوده و می توانند بر روی طیف وسیعی از ابزارهای الکترونیکی تاثیری شبیه صاعقه را ایجاد نمایند.

الف) سلاح های نرم افزاری

این فنون همه کدها و برنامه های نرم افزاری مرتبط را شامل می شود که برخی از آن ها به شرح زیر است.

۱- ویروس

ویروس های رایانه ای برنامه های نرم افزاری هستند که پس از ورود به رایانه هدف نظیر ویروس های واقعی تکثیر کرده و زیاد می شوند. این امر سبب سردرگمی نرم افزار رایانه ای و نقص در سامانه می گردد. اگر رایانه در محیط شبکه باشد ویروس ها از آن طریق از یک رایانه به رایانه دیگر منتقل شده و کل سامانه را مختل خواهندکرد. ویروس ها می توانند از طریق ابزارهای آلوده نظیر دیسکت ها و فلش ها از یک رایانه به رایانه دیگر منتقل شوند. ویروس ها برای منظورهای متعدد و با دامنه راهبردی حملات مشخص از اختلال موقت در اطلاعات خاص تا غیر فعال شدن دائمی روند ذخیره داده ها و حافظه اطلاعات در سامانه ها طراحی می گردند. یک ویروس محتوی دستوراتی برای وقوع تعدادی از رویدادها می باشد که بر عملکرد سیستم آلوده تاثیر نامطلوب دارد. این تاثیرات می توانند از کاملا بی ضرر تا کاملا مخرب ارزیابی شوند. برخی از این تاثیرات به شرح زیر است:

- برنامه زمان زیادتری برای اجرا صرف می کند.
- عملیات مورد نیاز روی دیسک ها بیش از اندازه معمولی است.
- رجوع منابع سیستم به دیسک ها بدون دلیل و به طور متناوب تکرار می شود.
- شماره سریال دیسک تعویض می شود.
- فایل های پنهان و سکتورهای خراب روی دیسک زیاد می شود.
- اندازه فایل های اجرایی تغییر می نماید.
- تغییرات غیر منتظره در تاریخ و ساعت سیستم پدید می آید.
- حافظه آزاد سیستم کاهش محسوس پیدا می نماید.
- خطاهای غیر منتظره و متفاوت در سیستم مشاهده می شود.

۲- اسب تروا (Trojan Horse)

در افسانه ها آمده است که سربازان یونانی با مخفی شدن در یک اسب چوبی عظیم الجثه و پیشکش آن به شهر تروا وارد شهر شده و آنان را شکست دادند. در دنیای دیجیتال یک اسب تروا عبارت از یک برنامه بدخواهانه ضد امنیتی است که در ظاهری خوشایند مخفی گردیده است. برای مثال هنگامی که یک فایل

حاوی تصاویر و یا موسیقی دلخواه را دریافت و باز می نمایید یک برنامه خطرناک را در محیط سیستم رها کرده اید که می تواند کل دیسک شما را پاک کرده و یا شماره کارت اعتباری شما و گذرواژه آن را به یک مقصد ناشناس ارسال نماید.

۳- کرم (Worms)

کرم ها برنامه هایی هستند که خود را مکررا تکثیر کرده و فضای حافظه و دیسک ها را اشباع می نمایند. گاهی کرم ها برای تکثیر از طریق شبکه طراحی شده و و قادرند با تاخیر فعال شده و خود را در سراسر فضای شبکه تکثیر نمایند. یک کرم یک برنامه مستقل است که قادر است خود را به صورت تصاعدی افزایش داده و از یک رایانه به رایانه دیگر در شبکه رسوخ نماید. کرم ها معمولا در صدد تغییر برنامه های دیگر نیستند و همچنین داده ها را تخریب نمی نمایند بلکه تنها در صدد آنند که منابع سیستم و شبکه را مصرف کرده و سبب افت سیستم گردند.

۴- شنود (Man in the Middle OR Sniffing)

برنامه ای است که کلیه مکالمات و تبادلات مالی را شنود و از این راه نام ها، شناسه ها و گذرواژه ها را به دست می آورد. برنامه های شنود و دیدبان، گذرواژه ها و اطلاعات با ارزش سیستم ها را گل چین و شکار می نمایند.

۵- برنامه های رمزشکن

این برنامه ها اولین برنامه های به کارگرفته شده در نفوذ سایبری بودند. ساده ترین شکل این برنامه ها با استفاده از روش آزمون و خطای خودکاربه کد و رمزسیستم ها دست پیدا می نماید. برنامه های رمز شکن پیچیده توان بالقوه از کار انداختن سامانه حفاظتی سیستم های مورد حمله را دارند.

۶- برنامه های برچسب

این برنامه ها یک برچسب شناسایی را در یک رایانه نصب و آن را برای نفوذ سایبری در آینده نشان گذاری می کنند. برخی از این برنامه ها قادرند تا برچسب را در درایو راه انداز سیستم نصب نمایند.

۷- بمب منطقی

یک بمب منطقی قطعه کدهای مخرب جاسازی شده ایست که با ایجاد صدا در زمان تعیین شده و یا هنگام انجام عمل خاصی در سیستم منفجر شده و پس از رهایی در محیط سیستم اثرات نامطلوب نظیر تخریب BIOS از خود به جای می گذارند.

جدول ابزارها و سلاح های مورد استفاده در جنگ سایبری

	ابزار تهدید	نوع اقدام	هدف
۱	بدافزارهای پیشرفته (APT)	آلوده کردن سیستم ها و از کار انداختن آن ها	اختلال و یا از کار انداختن مراکز داده یا سرورهای مراکز حیاتی و حساس
۲	اسب های تروا	انتشار از طریق ایمیل، محل های اشتراک فایل	ثبت کلیدهای فشرده شدن صفحه کلید، مشاهده صفحه نمایش کاربر
۳	عدم دسترسی به سرویس	قطع دسترسی به وب سایت توسط شرکت ارائه کننده خدمات میزبانی	عدم دسترسی به سرویس
۴	دروازه شتی (حفره نفوذ مخفی)	قرار دادن یک حفره نفوذ مخفی در تجهیزات تولیدی توسط تولید کننده	ورود به شبکه در زمان دلخواه و به صورت مخفیانه
۵	نرم افزارهای جاسوسی	در پوشش نرم افزارهای کاربردی مانند دیکشنری بابیلون	سرقت اطلاعات رایانه ها و شبکه های کاربران
۶	نرم افزارهای تبلیغاتی اینترنتی	قرار گرفتن در رایانه حریف و اصرار بر حداقل یک بار استفاده از آن ها	سرقت هویت کاربران و کلمه عبور آنها

۷	شبکه های "بات نت"	در اختیار گرفتن غیرقانونی سرورها و کامپیوترهای سازمان ها و مردم	سایبری حملات در غیرارادی مشارکت به عنوان سرباز الکترونیکی
۸	حملات DOS[۱۵]	بالا بردن کاذب ترافیک ارتباطی دسترسی به سایت	از کار انداختن سرورها و جلوگیری از ارائه خدمات به مردم
۹	حمله (هک و نفوذ)	ورود غیرقانونی به شبکه ها از طریق پورت های آسیب پذیر	اختلال و یا جلوگیری از ارائه خدمات

انواع حملات سایبری

سربازان جنگ سایبری، **" نفوذگران "** در عرصه اطلاعات دیگران هستند که کارشناسان این حوزه، آنها را به چند گروه تقسیم کرده اند:

گروه نفوذگران کلاه سفید: هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه ای انجام ندهد را یک هکر کلاه سفید می خوانند که در حقیقت متخصصین شبکه ای هستند که حفره های امنیتی شبکه را پیدا کرده و به مسئولان گزارش م یدهند.

گروه نفوذگران کلاه سیاه: اشخاصی هستند که وارد رایانه قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن بدافزار و غیره می پردازند.

گروه نفوذگران کلاه خاکستری: اشخاصی هستند که حد وسط دو تعریف بالا می شوند.

گروه نفوذگران کلاه صورتی: این افراد آدم های کم سوادی هستند که با چند نرم افزار خرابکارانه به آزار و اذیت بقیه اقدام می کنند.

[15] Denial of Service

اصلی ترین حملات نفوذگران عبارت است از:

شنود: در این روش نفوذ گر م یتواند به شکل مخفیانه از اطلاعات نسخه برداری کند.

تغییر اطلاعات: در این روش نفوذگر به دستکاری و تغییر اطلاعات می پردازد.

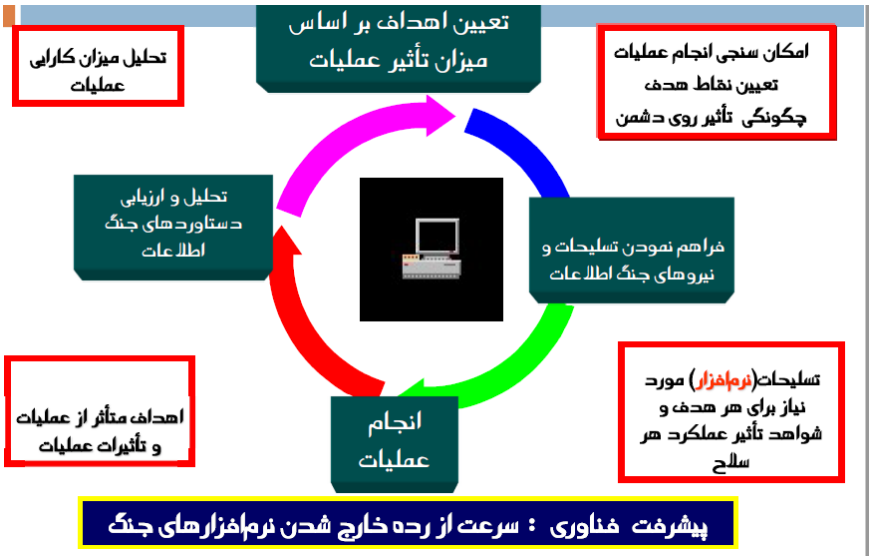
افزودن اطلاعات: در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می کند.

وقفه: در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می شود.

بر اساس آنچه کارشناسان مبارزه با جنگ سایبری اعلام می کنند، بررسی هویت و مکان مهاجم، شناسائی نیت مهاجم، تشخیص حمله های از قبل طراحی شده و بررسی و ارزیابی تلفات بعد از جنگ، از مهم ترین نقاط ضعف اصلی در دفاع سایبری است.

روش های حمله در مهندسی اجتماعی

مراحل فرآیند طرح ریزی جنگ سایبری (تهاجمی / تدافعی)



مروری بر آسیب پذیری های احصا شده

گام ۳: تهدیدات سایبری

تصور شما از یک تهدید سایبری چیست؟

آیا به یک سارق تنومند و زشت فکر می‌کنید که از دیوار شما بالا می‌آید؟ یا به یک نوجوان ۱۷ ساله ۵۰ کیلویی که آرام و ساکت در اتاق خود نشسته و به رایانه خود متمرکز شده است؟

البته تفکر مجرمان هزاران سال است که تغییر نکرده، مجرم همان مجرم است با این تفاوت که در گذشته دارای هیکل‌های بزرگ و مغزی کوچک بودند اما امروز دارای جثه کوچک و مغزی بزرگ هستند. لذا در فضای سایبر نه سلاح سرد و گرم و نه اندام و جثه بزرگ و نه قدرت بدنی هیچ‌یک تهدید محسوب نمی‌شوند.

ممکن است روزی فراموش کنیم که وای‌فای تلفن همراهمان را خاموش کنیم و نوجوان کنجکاو همسایه توانسته به تلفن ما نفوذ کرده و فایل‌های شخصی‌مان را تغییر داده، حذف یا کپی کند. پس در اینجا، وای‌فای روشن و عدم استفاده از رمز عبور، بستر مناسبی برای وقوع جرم شده است.

هویت مهاجمان سایبری

این یک واقعیت است که اگر ساکنان و اهالی یک محل، یکدیگر را بشناسند، کمتر مرتکب رفتارهای غیرمتعارف و غیراخلاقی می‌شوند. حتی یک مجرم نیز زمانی که با اهداف شوم و غیراخلاقی از منزل خود خارج و به محل ارتکاب جرم نزدیک می‌شود، تمام تلاش خود را می‌کند تا ناشناخته باقی مانده و دیرتر شناسایی شود تا بتواند همچنان به کارش ادامه دهد.

مثلاً از دید سارق، یک سرقت فیزیکی، مشکلات زیادی ممکن است داشته باشد:

- باید صورت خود را بپوشاند یا تغییر چهره دهد.
- در اماکنی که او را نمی‌شناسند اقدام به سرقت کند.
- از هویت جعلی، ساختگی یا ناشناخته استفاده کند.
- مجبور به بالا رفتن از دیوار، شکستن قفل یا عبور از موانع سختی باشد.

اما در فضای سایبر، برای مخفی شدن، نیاز به تلاش و تدبیر زیادی نیست. با توجه به موارد فوق می‌بینیم که فضای سایبر، برای مجرمان، بهشت محسوب می‌شود. او می‌تواند تمام فعالیت‌های مجرمانه‌اش را با خیالی آسوده انجام داده و فقط برای کسب نتیجه یا خرج کردن پول از مخفیگاه خود خارج شود، بدون اینکه کوچک‌ترین نگرانی از شناسایی خودش داشته باشد.

با توجه به نکات آموزشی و به کار بستن آن‌ها باعث می‌شود تا جرئت و جسارت مجرمان در انجام جرم کاهش یافته و راه‌های ورود آن‌ها به حریم خصوصی ما محدود و مسدود شود و حتی اگر زمانی جان و مال ما مورد تعرض قرار گرفت، با مراجعه به پلیس، امکان پیگیری و شناسایی وجود داشته باشد.

بنابراین تهدیدات سایبری عبارتند از هر نوع تهاجم نرم‌افزاری که امنیت جان، مال و اطلاعات افراد را به خطر می‌اندازد.

- چه بسیارند افرادی که تلفن آن‌ها ویروسی شده و همه اطلاعات خود را از دست داده‌اند.
- یا افرادی که رایانه آن‌ها ویروسی شده و چاره‌ای جز تعویض ویندوز ندارند.

- یا اطلاعات شخصی و شغلی آن‌ها سرقت شده و دچار خسارت‌های جبران ناپذیری شده‌اند.
- یا کارت‌هایی که از حساب متصل به آن‌ها میلیون‌ها تومان کسر شده.
- یا فایل‌های مهمی از افراد سرقت شده اما قربانی برای حفظ آبرو و اعتبار خود، سکوت می‌کند.

حملات سایبری این روزها به یک ابزار جدی برای تقابل گروه‌های متخاصم تبدیل شده است. این حملات با اهداف مختلفی همچون دسترسی غیرمجاز به اطلاعات، خرابکاری، ایجاد نارضایتی در کاربران، سرقت، باج‌گیری و حتی قدرت‌نمایی صورت می‌گیرد. شرکت مک‌آفی خسارت حملات سایبری در سال ۲۰۲۰ را حدود ۱۰۰۰ میلیارد دلار برآورد کرده بود؛ یعنی بیش از ۱ درصد تولید ناخالص داخلی جهان. اما نکته جالب‌تر، سرعت رشد این خسارات بود که بیش از ۵۰ درصد افزایش نسبت به سال ۲۰۱۸ را نشان می‌داد.

کشور ما نیز از این وضعیت مستثنی نبوده و روزانه حملات زیادی به زیرساخت های شبکه های اینترنتی سازمان ها و نهادهای مختلف کشور صورت می گیرد. البته بسیاری از این حملات توسط متخصصان ما در این حوزه خنثی می‌شود اما به هرحال در برخی مواقع نیز شبکه های اینترنتی و خدمات رسانی بعضی دستگاه ها برای مدتی با مشکل مواجه شده است. حمله سایبری به دستگاه های سوخت رسانی و همچنین ایجاد اختلال عمدی در صفحه داخلی سامانه شهرداری تهران از اصلی‌ترین اتفاقاتی است که طی یک سال گذشته رخ داده است.

جرم سایبری

جرم سایبری یک فعالیت مجرمانه است که در آن هدف اصلی، یک کامپیوتر یا شبکه است. برخی از جرائم سایبری با هدف حمله مستقیم به رایانه‌ها یا دستگاه‌های دیگر به منظور شکستن یا غیرفعال کردن آن‌ها انجام می‌شود. سایر جرائم سایبری، رایانه‌ها را برای پخش بدافزارها، سرقت اطلاعات و ... درگیر می‌کند.

تقسیم‌بندی جرائم سایبری به دسته‌های جداگانه کار ساده‌ای نیست زیرا اغلب آن‌ها با هم در ارتباط هستند. با این حال، به طور کلی انواع زیر قابل تشخیص است:

۱- جرایم مالی

جای تعجب نیست که بسیاری از مجرمان فضای مجازی از اینترنت برای کسب منافع مالی از طریق انجام حملات زیر استفاده می‌کنند:

الف- فیشینگ: مجرمان سایبری دوست دارند هنگام آلوده کردن رایانه‌های کاربران، راه ساده‌ای را انتخاب کنند. به همین دلیل، ایمیل یک وسیله مناسب برای حمله است. ماهیت کلاه برداری فیشینگ، مجبور کردن گیرنده برای کلیک بر روی لینک وب، باز کردن فایل پیوست یا تکمیل فرم آنلاین است. پیام‌ها اغلب از طرف یک سازمان بزرگ و معتبر مانند خدمات مالیاتی، بانک‌ها و فروشگاه‌های آنلاین ارسال می‌شود. در بسیاری از موارد کلاه برداران می‌خواهند کلمات عبور شما را بدست آورند یا دستگاه را با بدافزار آلوده کنند.

ب- باج‌خواهی آنلاین: یکی دیگر از جرائم سایبری با انگیزه مالی، اخاذی است. پس از آلوده کردن کاربر یا شرکتی به بدافزار، همه پرونده‌ها مسدود می‌شوند. سپس مجرمان پیشنهادی را برای بازگرداندن پرونده‌ها در ازای پاداش پولی ارسال می‌کنند. بیشتر اوقات، هکرها خواستار پرداخت‌هایی با رمزارزها هستند.

ج- تقلب: تقلب مالی پیچیده شامل هک کردن شبکه‌های خرده فروشی برای به دست آوردن اطلاعات کارت اعتباری مشتریان آن‌ها است. روش‌های دیگر می‌تواند فیشینگ هدفمند برای جعل هویت مدیران کسب و کارها و انتشار دستور از طرف آن‌ها باشد. لازم به ذکر است کشف برخی از انواع تقلب‌های مالی بسیار دشوار است.

د- نقض قوانین کپی‌رایت: این یکی از رایج‌ترین شکل‌های جرم آنلاین است. استفاده از محتوای محافظت شده از حق چاپ برای منافع شخصی به طور گسترده در وب سایت‌های تورنت مشاهده می‌شود. هم چنین سایت های زیادی محتوایی که دارای کپی‌رایت است را به صورت غیر قانونی منتشر می کنند.

۲– جرائم مربوط به نفوذ به حریم‌های خصوصی

هدف از انجام چنین جرائمی دستیابی به اطلاعات محرمانه است. انواع مختلفی از چنین تخلفاتی وجود دارد. بعضی اوقات هکرها با انگیزه های عمیق‌تر مانند پول یا نفوذ سیاسی هدایت می شوند. روش این نوع حملات دور زدن قوانین و یافتن آسیب‌پذیری در فناوری هایی است که باید از داده های محرمانه محافظت کنند.

الف– سرقت هویت: سرقت اطلاعات شخصی با هدف تعویض هویت دیجیتالی یک قربانی رخ می‌دهد. به عنوان مثال، کلاه برداران اطلاعات شخصی یک قربانی (شماره تلفن، آدرس و غیره) را به دست می‌آورند و برای دریافت وام بانکی بزرگ اقدام می‌کنند.

ب– جاسوسی: جاسوسی و نظارت مخفی بر زندگی افراد ممکن است شامل هک شدن دوربین های مدار بسته، نفوذ به کانال های ارتباطی مانند پیام کوتاه، ایمیل و غیره باشد.

ج– هرزنامه‌ها: اسپم یک نوع بسیار رایج از جرایم رایانه‌ای است . هرزنامه ها ممکن است از ایمیل های ناخواسته، پیام کوتاه و سایر کانال های ارتباطی استفاده کنند. به طور کلی به هر پیام ارسال شده بدون دریافت رضایت قبلی کاربر، اسپم یا هرزنامه گفته می‌شود.

۳– فعالیت‌های سیاسی و اجتماعی غیرقانونی آنلاین

برخی از انواع جرائم با هدف تغییر نگرش سیاسی یا ایجاد آسیب و یا کاهش تأثیر افراد یا گروه ها انجام می‌شود.

الف- آزار و اذیت و نفرت‌پراکنی: ایمیل‌های توهین‌آمیز و پیام های فوری علیه یک فرد یا گروهی از افراد اغلب بر اساس ویژگی‌های نژادی، جنسیتی، مذهبی افراد انجام می‌شود.

ب- تروریسم سایبری: سازمان های افراطی و افراد متخاصم به طور فزآینده ای از فضای مجازی برای آسیب رساندن به زیرساخت های فناوری اطلاعات، بحث در مورد اقدامات ترور، گسترش تبلیغات و غیره استفاده می‌کنند.

تعداد روز افزون مشاغل، خدمات و دستگاه‌های مرتبط، همه اهداف بالقوه تروریست های سایبری را به وجود می‌آورد.

ج- تحقیرسایبری: استفاده از دستگاه های متصل به منظور تحقیر یا ارعاب، در دسته حمله سایبری قرار می گیرد. خط بین جرائم آزار و اذیت و نفرت و تحقیر سایبری گاهی مبهم است. برخی از انواع حمله سایبری، مانند انتشار تصاویر حساس از کودکان، غیرقانونی است و به آن استثمار کودکان گفته می‌شود.

۳– سایر فعالیت‌های غیرقانونی

قسمت بد اینترنت که وب تاریک نامیده می‌شود، برای انجام انواع مختلفی از فعالیت‌های غیرقانونی استفاده می‌شود.

الف- محتوای غیر اخلاقی: انتشار محتوای غیر اخلاقی از طریق اینترنت در بسیاری از کشورها به عنوان یک جرم تعبیر می‌شود. در برخی از مناطق، فقط خشونت شدید و یا محتوای مربوط به حیوانات ممنوع است. گسترش محتوای غیر اخلاقی کودکان در اکثر کشورها ممنوع است.

ب- توزیع اسلحه و مواد مخدر: بازارهای بی‌شماری که در وب تاریک وجود دارند، به مجرمان کمک می‌کنند تا در حالی که دور از چشم پلیس می‌ماند به فروش مواد مخدر و اسلحه بپردازند.

طبقه بندی تهدیدات سایبری

از نظر نوع

- جنگ، مخاصمه یا تجاوز سایبری
- نزاع سایبری
- جاسوسی سایبری
- تروریسم سایبری
- جرم سایبری
- حمله سایبری منتهی به حوادث سایبری

از نظر منشاء یا عامل تهدید

۱- تهدیدات با منشاء انسانی (مهاجم سایبری یا متجاوز سایبری)

- دولت های متخاصم
- مزدوران سایبری (گروه های تحت حمایت پنهان دول متخاصم)
- جاسوسان سایبری
- تروریست های سایبری
- مجرمین سازمان یافته سایبری
- هکرهای دارای انگیزه سیاسی

۲- تهدیدات با منشاء ماشینی (سازه مخرب سایبری، بدافزار یا سلاح سایبری)

- سلاح های سایبری
- بد افزارها (جاسوس افزارها، ویروس ها، کرم ها، هرزنامه ها و ...)
- سازه های مخرب

۳- تهدیدات با منشاء طبیعی (زلزله، سیل، طوفان، رعد و ...)

۴- تهدیدات با منشاء صنعتی (تشعشع حرارتی یا الکترومغناطیسی و ...)

۵- تهدیدات با منشاء خرابی

از منظر نیت منشاءتهدید

- تهدیدات عمدی
- تهدیدات تصادفی
- تهدیدات محیطی

برخی نمونه ها و مصادیق تهدیدات سایبری

- اختلال در شبکه های مخابراتی کشور اعم ازشبکه ثابت و موبایل و ... (شنود، اختلال، انهدام)
- اختلال درشبکه حمل و نقل و ترافیک کشور (مترو، بین شهری، زمینی، هوایی، راه آهن)
- اختلال در شبکه برق کشور (خروج نیروگاه از مدار)
- اختلال در شبکه نفت و گاز (انفجار خطوط لوله، پالایشگاه)
- اختلال و سرقت در شبکه بانکی و مالی کشور
- اختلال در شبکه های صدا و سیما
- و...

شدت تهدید سایبری

- **شدت خیلی کم:** تهدید سایبری تحت کنترل
- **شدت کم:** تهدید سایبری حادثه آفرین
- **شدت متوسط:** تهدید سایبری مخل امنیت
- **شدت زیاد:** تهدید سایبری بحران زا
- **شدت خیلی زیاد:** تهدید سایبری فاجعه بار

تعیین سطح هشدار سایبری

تعیین سطح هشدار سایبری، بیانگر وضعیت سایبری کشور است و از منظر نظام دفاع سایبری کشور، وضعیت سایبری کشور، قابل طبقه بندی در ۴ سطح هشدار به شرح ذیل است:

- وضعیت تحت کنترل (وضعیت سفید)
- وضعیت تهدید سایبری (وضعیت زرد)
- **وضعیت بحران سایبری (وضعیت نارنجی)**
- **وضعیت جنگ سایبری (وضعیت قرمز)**

ویژگی های هر یک از چهار سطح هشدار فوق، در جداول زیر، ارائه شده است:

احتمال وقوع / شدت پیامد	خیلی غیرمحتمل	غیرمحتمل	ممکن	محتمل	قریب الوقوع
خیلی کم (رویداد)	۰	۱	۲	۳	۴

کم (حادثه امنیتی کوچک)	۱	۲	۳	۴	۵
متوسط (حادثه امنیتی عمده)	۲	۳	۴	۵	۶
زیاد (بحران)	۳	۴	۵	۶	۷
خیلی زیاد (فاجعه)	۴	۵	۶	۷	۸

۰ و ۱ و ۲ = وضعیت سفید = تحت کنترل سایبری

۳ و ۴ و ۵ = وضعیت زرد = اضطرار سایبری (تهدید سایبری)

۶ و ۷ = وضعیت نارنجی = بحران سایبری (نزاع سایبری، تروریسم سایبری، جاسوسی سایبری)

۸ = وضعیت قرمز = جنگ سایبری

ویژگی های مشترک حملات ارتش های سایبری

- حملات همگی هدفمند بودند.
- حملات با شناسایی قبلی از هدف طراحی شده بودند. این شناسایی شامل اطلاعات سیستم ها به ویژه آسیب پذیری های امنیتی بود.
- روش انتشار به گونه ای است که عدم اتصال به اینترنت هم راهکار مفیدی نبوده است.
- حملات با دانش فنی بالا و خیلی پیچیده طراحی شده بودند.
- همگی از آسیب پذیری های جدید و نا شناخته بهره می بردند.

گام ۴: پدافند سایبری

به مجموعه اقداماتی گفته می شود که موجب بازدارندگی، پیش گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه های ملی سایبری توسط متخاصمین سایبری، اعم

از ارتش سایبری کشورهای متخاصم، گروه های تحت حمایت پنهان دولت های متخاصم، جاسوسان سایبری، تروریسم های سایبری می شود.

حفاظت از زیرساخت های اطلاعاتی خودی با تمرکز بر هدف های ۳ گانه کاهش آسیب پذیری ها ، تداوم فعالیت های ضروری و ارتقا پایداری در مقابل تهاجمات دشمن از طریق ایجاد و بکارگیری الزامات پدافند غیر عامل در فضای سایبر و سیستم های اطلاعاتی.

فاکتورهای مهم در حوزه پدافند سایبری

۱– کاربران و نیروی انسانی

الف) کاربرانی که در فضای سایبر با اطلاعات سروکار دارند.

هرکس تنها اطلاعاتی در اختیار داشته باشد که برای پیشبرد کار تعریف شده سازمانی خود، بدان احتیاج دارد و نه بیشتر

ب) بخش روانی این حوزه که درواقع شامل افرادی است که مخاطب فضای مجازی هستند و همیشه تحت تاثیر سناریوهای متخصص روانشناسی و جامعه شناسی دشمن در بستر فضای سایبر قرار دارند.

نفوذ دشمن از حفره خلا علمی کاربران می تواند با آموزش مستمر و

بروزرسانی این آموزشها مسدود گردد.

۲– داده ها و اطلاعات

الف) برای صیانت از داده های اطلاعاتی باید به میزان حساسیت و منافعی که آن اطلاعات فراهم می کند، هزینه نگهداری پرداخت نمود و تلاش امنیتی انجام داد.

ب) اینکه چه نوع اطلاعاتی و بر روی چه مکانی از فضای سایبر قرار گیرد و یا کدام پایگاه دانش روی کدام سرور فعالیت نماید.

۳– روش ها و رویه های اجرایی

الف) دستورالعملهای درج و استخراج اطلاعات، نگهداری داده ها، تهیه نسخه های پشتیبان که درصورت بروز حملات سایبری، سامانه در کوتاهترین زمان به حالت پایدار قبلی بازگردد.

ب) تمامی این موارد باید توسط یک نگاه کارشناسی و متخصص به دقت تهیه و تنظیم شده و جهت اجرای صحیح به نیروی انسانی و کاربران فضای مجازی ابلاغ گردد.

۴– نرم افزارهای رایانه ای

- این حوزه یکی از نقاط آسیب پذیر فضای سایبر است.
- یک نرم افزار کاربردی می تواند بطور کاملا نامحسوس یک جاسوس سایبری باشد که در لایه های پنهان سیستم عامل فعالیت های مخربی همچون سرقت اطلاعات و یا تخریب آنها را انجام می دهد.
- این جاسوس مجازی تنها زمان کمی پس از اتصال به شبکه، داده های به سرقت برده را به مقصد ارسال می کند.
- خود سیستم عامل که بستر فعالیت نرم افزار است می تواند کلیه فعالیت های کاربر را رصد کرده و جاسوس اصلی این سناریو باشد.
- پدافند موثر در این حوزه، بومی سازی خط طراحی و تولید نرم افزار است.

آیا می توان کلیه نرم افزارها را کنار گذاشت و فقط از نرم افزار های بومی قا بل اعتماد استفاده کرد؟

به طور حتم این کار غیرمنطقی است و در دهکده جهانی امروز نمی توان در یک فضای سایبر بسته زندگی کرد.

راه حل:

- **بومی سازی نرم افزارهای پدافندی فضای مجازی** (نرم افزارهایی مثل دیواره های آتش، آنتی ویروس ها و ضدجاسوس ها
- **تولید یک سیستم عامل مطمئن بومی** با اتکاء به دانش داخلی، بستر امنی برای فعالیت های نرم افزاری خواهد بود. در این راه توجه ویژه به برنامه های کد باز ، و سیستم عامل هایی چون لینوکس کار ساز هستند. این گونه برنامه ها به متخصصین امکان می دهند که تا ریزترین لایه ها فرورفته و از کارکرد همه بخشها اطمینان حاصل نمایند و علاوه بر آن، برنامه یا سیستم عامل را به دلخواه خود سفار شی نموده و مطابق نیازهای سازمانی کدنویسی کنند.

۵– سخت افزارهای رایانه ای

- سناریو این حوزه می تواند جاگذاری یک قطعه سخت افزاری خاص درون رایانه یا تجهیزات شبکه مثل روترها و سوئیچ ها باشد. ماموریت این قطعه جمع آوری اطلاعات و ارسال به مقصد تعیین شده خواهد بود.

- بومی نمودن سخت افزاری برای کشورهای درحال توسعه به علت تکنولوژی بالای فناوری در این عرصه، بسیار مشکل است اما غیرممکن نخواهد بود و می تواند به عنوان یک ایده بلند مدت هدف گذاری گردد.
- تولید سخت افزارهای کنترلی مثل دیواره های آتش سخت افزاری و تجهیزات شبکه که در خط مقدم فضای سایبری خودی قرار می گیرد از اولویت های این بومی سازی هستند.

ریشه مشکلات و آسیب پذیری های امنیتی

ضعف در فناوری: به طور مثال وجود تهدید در پروتکل ها، سیستم های عامل و سخت افزار و نرم افزار

ضعف در پیکربندی: پیکربندی پیش فرض اغلب تجهیزات مورد استفاده در شبکه های رایانه ای ضعف های امنیتی مشهودی دارند

ضعف در سیا ست گذاری: سیا ست های امنیتی در یک شبکه ، نحوه و زمان پیاده سازی و جزئیات اجرای قوانین امنیتی را بیان می کند که عدم تدوین یک سیاست امنیتی مدون می تواند زیرساخت فناوری اطلاعات و ارتباطات یک سازمان را با مشکل مواجه نماید.

تعریف امنیت فضای سایبر

امنیت فضای سایبر تعریف پیچیده ای دارد که این پیچیدگی شامل موارد مختلفی است که بنا به تعریف *ریک فیشر* اجزای فضـای سـایبر و ذات بالفعل آن موجب این پیچیدگی گردیده اسـت. تعریف امنیت فضـای سـایبر در زمینه های مختلف معنا می شود به طور مثال در زمینه اقتصادی، اجتماعی، فرهنگی، سیاسی و یا نظامی اما بطور معمول امنیت سایبری عموما به سه مورد اشاره دارد:

۱- مجموعه ای از فعالیت ها که اشاره دارد به محافظت در برابر حمله و تهدیدات شبکه های کامپیوتری، نرم افزاری و سیستم های اطلاعاتی. در مجموع فعالیت هایی که شامل ممیزی امنیتی، مدیریت وصله های

امنیتی، ماژول های تصدیق هویت، مدیریت دسترسی ها و مسائلی از این دست می شود که فاکتورهای اشاره شده میزان امنیت زیر ساخت تجارت الکترونیک و ساختار سیاسی یک کشور را نشان می دهد و نیز شامل راهکارهایی است که منجر به شناسایی و برخورد با حوادث امنیتی و همچنین بهبود صدمات بوجود آمده از نقص امنیتی می شود.

۲- وضعیت یا کیفیت محافظت در برابر تهدیدات

۳- مجموعه فعالیت های پژوهشی و تحلیلی که کمک می کند به اجرا و بهبود راهکارهای امنیتی هفت عنصر خط مشی و سیاست گذاری ، تشکیلات و ساختار، هسته و شالوده اصلی، فرآیندها، افراد، مهارت و تخصص و تکنولوژی، امنیت فضای سایبری را تحت تاثیر قرار می دهد که عناصر اشاره شده ارتباط ذاتی با یکدیگر دارند به طوری که با توسعه همه موارد در یک سیستم می توان گفت امنیت در یک فضای سایبری محقق شده است.

عوامل مؤثر بر تهدیدات سایبری

بیشترین عوامل تاثیرگذار در تهدیدات سایبری عدم دانش و آگاهی کاربران و فقدان تجهیزات و زیرساخت های بومی است.

عدم آگاهی و دانش کافی کاربران: تهدیداتی نظیر نشر ناخواسته اطلاعات شخصی و یا پاسخ به سوالات و هرزنامه ها و روش هایی که دزدان سایبری به صورت حرفه ای از خود کاربران اطلاعات آن ها را به سرقت می برند و استفاده از شیوه های مهندسی اجتماعی از جمله مواردی است که موجب عدم امنیت کاربر در فضـای مجازی می شود که می توان با آگاهی و آموزش کاربران با تبعات بعدی مقابله و اجتناب نمود. کاربران نیز به طور کل شامل دو گروه هستند. **کاربران عمومی** و **کاربران متخصص**. عدم آگاهی و دانش در کاربران عمومی منجر به از دسـت دادن اطلاعات شخصی و خانوادگی می شود که گاهاً منجر به پرداخت

هزینه های سـنگین می گردد. منظور از کاربران متخصص افرادی که مسئولیت نگهداری از شبکه و زیرساخت در سازمان ها را به عهده دارند، می شود.

عدم وجود زیر ساخت و تجهیزات بومی: جایگاه امنیت فناوری اطلاعات و ارتباطات به طور مشخص در تمامی حوزه های مختلف ICT الزامی بوده که در تمامی سطوح از لایه فیزیکی تا لایه برنامه های کاربردی را تحت پوشش خود قرار می دهد. در این راستا استاندارد ها و رویه های اجرایی مدونی در دنیا طرح شده که نیاز است در کشور بومی سازی گردد. با رشد تصاعدی فراگیر شدن فناوری اطلاعات در سیستم های دولتی و خصوصی و افزایش روز افزون خدمات و سرویس های ارائه شده به اقشار مختلف جامعه در بستر فن آوری اطلاعات چنان چه به زیرساختهای بومی و ابزارهای امنیتی بومی توجه جدی صورت نپذیرد با گذر زمان وابستگی جامعه به خدمات الکترونیک بیشتر و از طرفی وابستگی زیرساخت های سرویس دهندگان به صاحبان اصلی تکنولوژی این صنعت در خارج از کشور نیز بیشتر خواهد شد.

قرارگاه پدافند سایبری کشور

از سال ۱۳۹۰ به منظور مقابله با تهدیدات سایبری دشمن و امن سازی زیرساخت های سایبری کشور، قرارگاه پدافند سایبری کشور توسط سازمان پدافند غیر عامل کشور و با هدف راهبری و هدایت دستگاه های اجرایی کشور جهت این امر مهم تشکیل گردید. براساس ابلاغیه قرارگاه پدافند سایبری، کلیه دستگاه های اجرایی کشور، پس از تعیین سطح اهمیت سرمایه های سایبری خود، موظف به امن سازی زیرساخت های حیاتی، حساس و مهم سایبری خود بوده و به منظور آمادگی جهت مقابله با حملات سایبری دشمن، نسبت به ایجاد مراکز پدافند سایبری در سطح وزارتخانه ها، سازمان ها، استان ها و مناطق ویژه اقدام نمایند.

پدافند جامع در حوزه سایبری باید در لایه های مختلف ۸ گانه زیر تعریف گردد:

۱- خط مشی ها، روش های اجرایی و دستورالعمل ها و کنترل های امنیتی

۲- پدافند فیزیکی (دوربین های مدار بسته،روش های بیومتریک و حفاظ های ایمنی)

۳- پدافند پیرامونی (کوزه عسل – دیوار آتش و مدیریت تهدید یکپارچه)

۴- پدافند درشبکه (ماژول امنیتی سخت افزاری ، سویچ لایه ۲ و ۳- روتر)

۵- پدافند در سطح داده و محتوا (بازیابی داده - رمزنگاری داده)

۶- پدافند در سطح سیستم عامل (مجازی سازی)

۷- پدافند در نقاط پایانی (آنتی ویروس – سیستم تشخیص نفوذ)

۸- پدافند در سطح برنامه های کاربردی

راهبردهای نظام پدافند سایبری کشور

- مصون سازی زیرساخت های حیاتی و حساس کشور در مقابل تهدیدات و حملات سایبری CCIP
  - معماری واستقرار پدافند سایبری در مراکز حیاتی وحساس کشور
  - استفاده از سیستم ها و سایت های جایگزین
  - داشتن نسخه پشتیبان از اطلاعات موجود
  - به کارگیری اصول عام پدافند غیرعامل برای تأسیسات فیزیکی در کلیه مراحل از طراحی تا بهره برداری از قبیل: مکان یابی، پراکندگی، مقاوم سازی و...
  - به کارگیری اصول پدافند غیرعامل سایبری برای فضای مجازی و متناسب با تهدیدات از قبیل فریب سایبری، اختفاء سایبری و...
  - مدیریت بحران سایبری و تهیه دستورالعمل های امنیتی و پدافندی
  - آموزش مداوم و مستمر کلیه پرسنل مرتبط
  - برگزاری مانورهای دوره ای پدافند غیرعاملی در فضای سایبر
- ایجاد و توسعه نظام های مورد نیاز پدافند سایبری
- ارتقاء کمی و کیفی منابع انسانی حوزه پدافند سایبری

- ارتقاء سطح آگاهی، دانش و مهارتهای بومی و فرهنگ سازی در حوزه پدافند سایبری
- تقویت صنعت بومی و توسعه خدمات و محصولات روزآمد پدافند سایبری

موارد عملیاتی مرتبط با مدیریت تداوم کسب وکار در پدافند سایبری

راهکارهای پدافند سایبری

با توجه به راهبردهای پدافند سایبری و با شناسایی تهدیدات و نقاط آسیب پذیر مرتبط باآنها راهکارهایی درقالب طرح های زیر توصیه می گردد:

طرح حفاظت فیزیکی و محیطی

طرح حفاظت از زیر ساخت های حیاتی

طرح حفاظت از تجهیزات

طرح حفاظت از سخت افزار و سکوها

طرح حفاظت از اسناد و اطلاعات محرمانه

طرح بازیابی در خصوص رخداد ها و تهدیدات سایبری

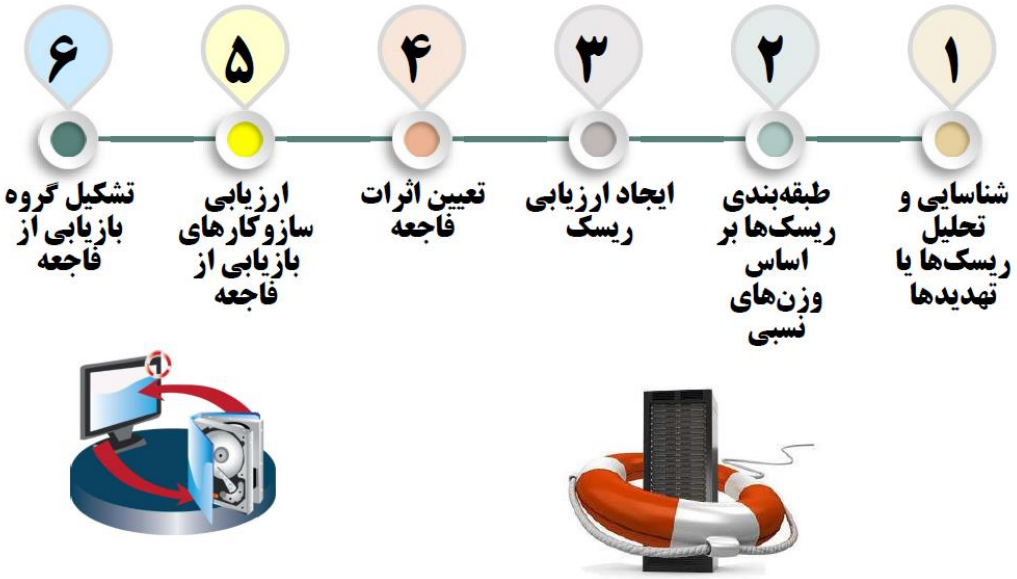
طرح بازیابی فاجعه

فاجعه، رویدادی ناگهانی و برنامه ریزی نشده است که به وارد آمدن آسیب یا زیان جدی بر سازمان منجر می گردد. فاجعه باعث می شود تا سازمان برای مدت زمانی نتواند کارکردهای تجاری حیاتی را فراهم آورد.

با افزایش استفاده از فناوری اطلاعات به عنوان توانمند سازی کسب و کاری در سازمان ها، آمادگی برای مدیریت هر اختلالیا فاجعه ای که باعث قطعی سیستم ها یا خدمات سازمان می شود بیش از پیش اهمیت یافته است.

یک برنامه بازیابی از فاجعه بیان می کند که در صورت وقوع فاجعه ای احتمالی، سازمان چگونه با آن روبه رو می شود، اثرات آن را به حداقل می رساند و عملیات اصلی خود را در سریع ترین زمان ممکن به حالت عادی باز می گرداند.

مراحل برنامه ریزی برای بازیابی از فاجعه



متدولوژی تاب آوری و بازدارندگی سایبری

پیشنهاداتی برای مدیران و کارکنان جهت حفظ امنیت در فضای سایبری

۱- تغییررمز عبور: تغییر دوره ای رمز عبور خود در سامانه های اداری، شبکه های اجتماعی، کارت های بانکی و پست الکترونیک و بانکداری مجازی، توصیه همیشگی پلیس سایبر و متخصصان امنیت در فضای مجازی به شمار می رود. تغییر رمز عبور را همواره در برنامه سبک زندگی دیجیتالی خود قرار دهید. قرار نیست که ۱ سال یا ۱۰ سال، با یک رمز عبور به پست الکترونیک، حساب بانکداری مجازی، پروفایل شبکه های اجتماعی و امثال آن وارد شوید. قدرت رمز عبور اولین خط دفاعی در برابر حملات مختلف است. استفاده از حروف کوچک، بزرگ، کاراکترها ترکیبی از نماد ها که معنی ندارند، تغییر رمز عبور به طور منظم و ذخیره نکردن آن یا به اشتراک گذاری آن، یک مرحله حیاتی برای محافظت از اطلاعات حساس شماست.

۲- احراز هویت دو مرحله ای: برخی از سامانه ها به کاربران اجازه می‌دهند تا احراز هویت دو مرحله‌ای را فعال کنند و این امر دسترسی هکرها به حساب کاربری را بسیار پیچیده‌تر می‌کند، اگر این گزینه را فعال کنید، هر بار که بخواهید به حساب کاربری خود دسترسی پیدا کنید، یک کد به تلفن همراه خود دریافت خواهید کرد، این بدان معناست که اگر شخصی موفق به شکستن رمز عبور شما شود، بدون کد نمی‌تواند به حساب کاربری دسترسی پیدا کند، اگر می‌خواهید از داده‌های حساس خود محافظت کنید، این یکی از بهترین راه‌ها برای انجام این کار است.

۳- **پرهیز از تک رمز مداری:** تک رمز مداری یعنی این که به جای آن که برای هر اکانت، یک رمز عبور مناسب اختصاص دهید، یک رمز عبور آسان و بعضا قابل حدس را برای چندین سامانه کاری و پروفایل در شبکه های اجتماعی استفاده کنید. بعضا مشاهده می شود که رمز عبور پست الکترونیک کاربری با رمز عبور اتوماسیون اداری، حساب بانکداری مجازی و فلان شبکه اجتماعی نیز یکی است و این راه را برای ضربه زدن دیجیتالی آسان می کند. به این موضوع مهم اما به ظاهر ساده توجه داشته باشید.

۶- کاهش انتقال داده ها: انتقال داده ها بین دستگاه های شخصی و کاری، اغلب به دلیل افزایش روز افزون کارمندانی که از راه دور کار می کنند، اجتناب ناپذیر است. نگهداری اطلاعات حساس در دستگاه های شخصی آسیب پذیری در برابر حملات سایبری را به میزان قابل توجهی افزایش می دهد.

۷- عدم اشتراک گذاری اطلاعات خصوصی: برای کاهش آسیب پذیری خود در شبکه های اجتماعی، از به اشتراک گذاشتن اطلاعات خصوصی خود پرهیز کنید. حتی اگر پروفایل شما در حالت private (خصوصی) قرار دارد، تضمینی برای لو رفتن اطلاعات و عکس های خصوصی شما و دوستانتان نیست. اطلاعات خصوصی دیگران را نیز چه به صورت متن و چه عکس و چه ویدیو، در صورتی که از آنها اجازه نگرفته اید به اشتراک نگذارید. گاها اطلاعات متنی و ویدیویی، اطلاعات خوبی را با مهندسی اجتماعی، در اختیار هکرها و مجرمان سایبر قرار می دهد.

۹- خطرات وای فای عمومی: استفاده از وای فای های عمومی، احتمال هک گوشی را افزایش می دهد. به همین خاطر همواره از وای فای های مطمئن استفاده کنید. به همین خاطر توصیه می شود که حتی الامکان، از وای فای عمومی یا کافی نت های غیر معتبر، برای ورود به حساب شبکه های اجتماعی و اینترنت بانک خود استفاده نکنید.

محافظت در برابر حملات مهندسی اجتماعی

۱- ایمیل های دریافتی را بررسی کرده و به آدرس فرستنده و نام دامنه آن ها دقت کنید.

۲- در تماس های تلفنی هیچ گاه اطلاعات مربوط به حساب های کاربری خود را بازگو نکنید.

۳- در گفت و گوهای روزمره در اماکن عمومی حواستان به صحبت هایی که می کنید، باشد. بسیاری از رمزها از طریق همین اطلاعات معمولی به دست می آیند.

۴- در مکالمات تلفنی حواستان به شخص مورد نظر باشد، چرا که امروزه تقلید صدا و ایجاد صدایی مشابه با صدای دوست و همکار شما کاری نسبتاً ساده است.

۵- پس از ترک میز کار، رایانه خود را قفل (Lock) کنید. کلیدهای ترکیبی Windows+L کار شما را برای انجام این کار آسان می کند. هم چنین می توانید کلیدهای Crrl+Alt+Del را فشرده و سپس گزینه Lock را بزنید.

۶- اگر به ایمیلی شک کردید و احساس کردید که ممکن است حمله فیشینگ باشد، سریعاً مسئولان مربوطه را باخبر کنید.

۷- اگر مجبور شدید رمز عبور خود را با شخص دیگری در میان بگذارید، سریعاً اقدام به تغییر آن کنید.

۸- همواره دانش خود را درخصوص تهدیدهای سایبری و به خصوص حملات مهندسی اجتماعی افزایش دهید.

۴ توصیه برای جلوگیری از "از دست دادن داده ها"

۱- نصب فایروال و آنتی ویروس: به دلیل حمله های باج افزارها و ویروس ها که از هرزنامه ها، کلاهبرداری فیشینگ، بدافزار، فایل های دانلود شده، وب سایت ها و ایمیل هایی که از طرف دوستان، مشتری ها و همکاران ایجاد می شوند، شما بدون آنتی ویروس به روزرسانی شده نمی توانید از سیستم ها و اطلاعات خود مخافظت کنید.

۲- به روزرسانی نرم افزار های امنیتی: شما همواره باید سیستم های خود را بروزرسانی کنید. مایکروسافت نرم افزارهای امنیتی را برای محافظت از داده های کاربران در مقابل آسیب پذیری های موجود منتشر می کند. هکرها از این آسیب پذیری های برای ایجاد یک اکسیلویت به منظور دسترسی به کامپیوترها و شبکه هایی که به روز رسانی نشده و نرم افزارهای امنیتی را نصب نکردند سوء استفاده می کنند.

۳- ذخیره کردن داده ها در فضایی خارج از سیستم: کاربر باید اطلاعات خود را از آتش، سیل یا سایر بلایای طبیعی و سرقت محافظت کند. در صورت ذخیره اطلاعات در فضای سرویس های ابر، اگر یک فاجعه رخ دهد و اینترنت قطع شود، کسب و کار افراد برای مدتی متوقف خواهد شد.

۴- همواره از فایل های خود بکاپ بگیرید و آن ها را ذخیره کنید: همواره باید از اطلاعاتتان بکاپ بگیرید و به منظور اطمینان از بازیابی آن ها را در زمان های مورد نیاز، اطلاعاتی را که ذخیره کرده اید را

همیشه تست و ارزیابی کنید. با توجه به احتمال خرابی هارد درایو، برای حفاظت از داده ها بهتر است که یک نسخه پشتیبان از آن ها که روی چندین درایو قرار دارد، تهیه کنید.