مرکز آموزش وپژوهشهای توسعه و آینده نگری

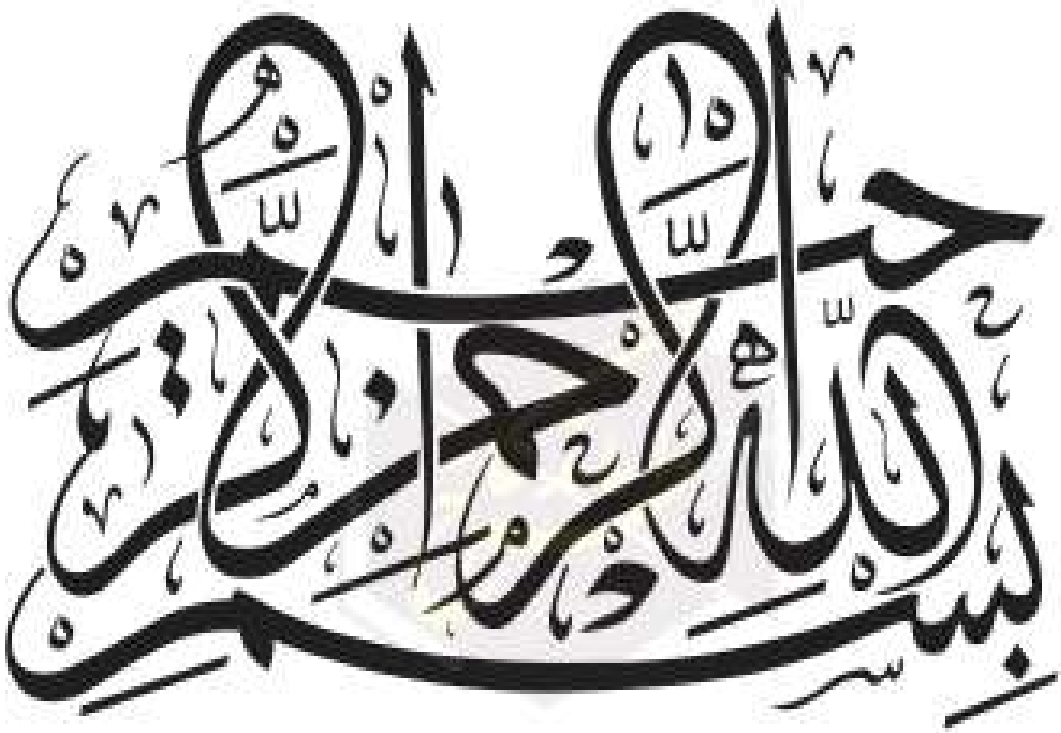
استان خوزستان

بنیان مدیریت امنیت اطلاعات

گردآوری و تدوین: احمدرضا امین زرگران

کارشناس ارشد مدیریت فن آوری اطلاعات

۱۳۹۹


بسم الله الرحمن الرحيم

فضای سایبری چیست

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 Norbert Wiener 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.

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون (William Gibson) نویسنده داستان علمی تخیلی در کتاب نورومنسر Neuromancer در سال ۱۹۸۴ به کار برده است.

در بعد چیستی ، فضای سایبر از دیدگاه سخت افزاری : شبکه ای جهانی از کامپیوترهای به هم پیوسته است که از طریق کانال های ارتباطی پرسرعت ،تارعنکبوتی را شکل داده که سریعتر از مصنوعات دیگر انسان در حال گسترش است. اینترنت که نمایشی از فضای مجازی است ، بستری هیجان انگیزی را ایجاد نموده که قابلیت ارائه خدمات متنوع ، سریع و جذاب را دارد. ارتباطات سریع، قابلیت ارسال پیام ؛ ارائه سرویس های ارتباطی ؛ تبادل اطلاعات با فرمت های مختلف از خدمات متنوع این ابر شبکه است.

فضای سایبر مجموعه متنوعی است از سخت افزارها، نرم افزارها، شبکه ها، کاربران و هر آنچه در این فضا تولید شده و یا تبادل می گردد.

فضای مجازی

مفهوم فضای مجازی در اصطلاح که در واقع حاصل تکنولوژی غرب است ، واژه ای است که در خلال دهه ی ۱۹۹۰ از طریق اینترنت کاربرد عمومی یافت. تعریفی که اکسفورد از فضای مجازی ارائه می دهد چنین است : فضای مجازی ،فضایی تئوری است که ارتباطات کامپیوتری در آن رخ می دهد.
فضای مجازی گسترده جهانی است که شبکه های گوناگون رایانه ای در اندازه های متعدد و حتی رایانه های شخصی را، با استفاده از سخت افزارها و نرم افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر وصل می کند.

فضای مجازی فقط مجموعه ای از سخت افزار نیست،بلکه مجموعه ای از تعاریف نمادین است که شبکه ای از باورها را در چارچوب داد و ستد بیت رد و بدل میکند.فضای مجازی به فضای تعاملی اینترنت اطلاق می شود،که در آن افراد دردرون آن با هویت هایی پنهان به مثابه پیام هایی بر صفحات رایانه حضور می یابند. نکته ای که در اینجا لازم به ذکر است این است که ، فضای مجازی بر خلاف ظاهر نام گذاری آن حقیقتا مجازی نیست، بلکه باتوجه به آثار آن یک دنیای حقیقی است.گسترش فناوری های اینترنتی ودر دسترس بودن آن ، فضای مجازی را شبیه ساز دنیای واقعی کرده استدر سال ۲۰۱۰، یک مدل پنج سطح در فرانسه طراحی شد. طبق این مدل، فضای مجازی از پنج لایهٔ مبتنی بر اکتشافات اطلاعاتی تشکیل شده‌است: زبان، نگارش، چاپ، اینترنت و غیره. این مدل اصلی دنیای اطلاعات را به فناوری‌های ارتباطی پیوند می‌دهد.

نمی‌توان فضای مجازی را مترادف با اینترنت دانست، اما اینترنت ابزار ورود به فضای مجازی است.
فضای مجازی عبارت است از محیطی که در آن برقراری ارتباطات، رؤیت و انتقال اطلاعات (به‌صورت غیرقابل لمس و با اشغال اندکی از محیط قابل‌لمس) در ساختارها و قالب‌هایی به‌عنوان خدمات به انسان‌ها، طراحی و کنترل می‌شود.

درواقع، در این تعریف به سه ویژگی فضای مجازی اشاره‌شده است:

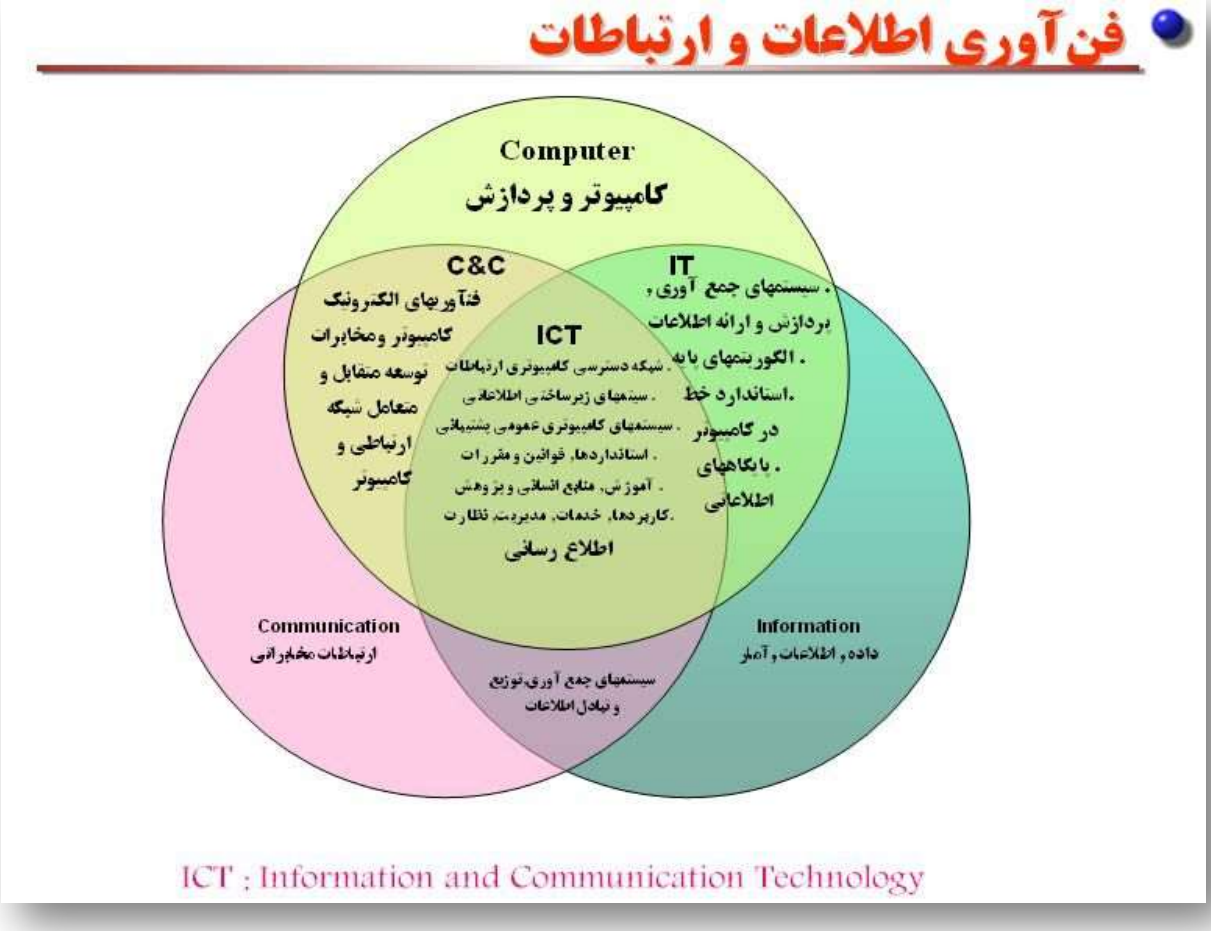
- **محیط است و نامحدود نیست؛**
- **در قالب خدمات ارائه می‌شود؛**
- **خدمات و ارتباطات کنترل می‌شود.**

آنچه امروز در فضای نخبگانی کشور ما به عنوان فضای مجازی شناخته می شود همان چیزی است که در غرب به عنوان فضای سایبری معرفی شده است و آنچه در فضای عرفی کشور ما به عنوان فضای مجازی شناخته می شود مفهوم محدودی از شبکه های اجتماعی عمدتاً هم برداشتی صرفاً با کارکردهای رسانه ای از امثال تلگرام، توئیتر و اینستاگرام و ... است.
و نهایتاً آنچه که در غرب به معنای فضای مجازی شناخته می شود اعم از واقعیت مجازی و فضای سایبری است.

فن آوری اطلاعات

ICT یافناوری‌اطلاعات‌وارتباطات(Information & Communication Technology) ، بدون شک تحولات گسترده ای را در تمامی عرصه‌های اجتماعی و اقتصادی بشریت به دنبال داشته و تاثیر آن بر جوامع بشری بگونه‌ای است که جهان امروز به سرعت در حال تبدیل شدن به یک جامعه اطلاعاتی است.
جامعه ای که در آن دانایی و میزان دسترسی و استفاده مفید از دانش، دارای نقشی محوری و تعیین کننده است.

اما در تعریف فناوری اطلاعات و ارتباطات می‌توان گفت؛ فناوری عبارت است از گردآوری، سازماندهی، ذخیره و نشر اطلاعات اعم از صوت، تصویر، متن یا عدد که با استفاده از ابزار رایانه‌ای و مخابرات صورت پذیرد.
صرفنظر از تعاریف متنوع و دامنه وسیع کاربرد فناوری اطلاعات و ارتباطات در بخشهای مختلف زندگی بشری، دسترسی سریع به اطلاعات و انجام امور بدون در نظر گرفتن فواصل جغرافیایی و فارغ از محدودیتهای زمانی محوری‌ترین دستاورد این فناوری است.



اجزای فن آوری اطلاعات و ارتباطات

فناوری اطلاعات متشکل از چهار عنصر اصلی (انسان، سازوکار، ابزار، ساختار) است، به طوری که در این فناوری، اطلاعات از طریق زنجیره ارزشی که از بهم پیوستن این عناصر ایجاد می شود جریان یافته و پیوسته تعالی و تکامل سازمان را فراراه خود قرار می دهد:

۱) **انسان: منابع انسانی، مفاهیم و اندیشه، نوآوری**
۲) **سازو کار: قوانین، مقررات و روشها، سازوکارهای بهبود و رشد، سازوکارهای ارزش گذاری و مالی**
۳) **ابزار: نرم افزار، سخت افزار، شبکه و ارتباطات**
۴) **ساختار: سازمانی، فراسازمانی مرتبط، جهانی**

فن آوری اطلاعات در سازمانها

بکار گیری تکنولوژی اطلاعات (فناوری اطلاعات) در سازمانها تغییرات بنیادین را در کلیه زمینه ها نوید می‌دهد. همانطوریکه امروزه دنیا را نمی توان بدون صنعت برق در نظر گرفت دنیای امروز را نیز نمی توان بدون فناوری اطلاعات و ارتباطات تصور کرد.

در جهان امروز تکنولوژی اطلاعات امکان سودمندی و کارآمدی اطلاعات را ممکن ساخته است. بکارگیری تکنولوژی اطلاعات (فناوری اطلاعات)، تحول گسترده ای را در امور اداری و سیستمهای اطلاعاتی باعث شده است، طوریکه امکان انتقال الکترونیکی داده ها ، مدارک، اسناد و مکاتبات مختلف از طریق کامپیوتر و خطوط ارتباطات مخابراتی فراهم‌شده است.

از ویژگیهای اساسی عصر حاضر، اطلاعات و تبدیل آن به دانش است . چنین ویژگی تاثیر زیادی روی نهادهای اجتماعی و اقتصادی جوامع خواهد گذاشت . نهادهای اجتماعی باید بر اساس آن تجدید بنا و تغییر ساختار دهند.

گفته می شود که تکنولوژی اطلاعات (فناوری اطلاعات) توانایی سازمان را افزایش می دهد با این وجود چنین پیشرفتهایی اغلب سبب بهبود عملکرد مالی سازمانها نمی شود.

محورهای سه گانه که در بکارگیری فناوری اطلاعات در سازمانها مورد توجه است شامل : مردم ، زیر ساخت و کاربردها است.

جنگ سایبری چیست؟

جنگ سایبری به استفاده از تکنولوژی در جهت حمله به ملت‌ها، دولت ها و شهروندان اشاره دارد که موجب خساراتی همچون جنگ تسلیحاتی می شود. در اصل جنگ سایبری یا رایا جنگ (Cyber War) ، به معنی استفاده از کامپیوتر ها و فضای تبادل اطلاعات به عنوان یک اسلحه و یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت ترساندن، تغییر عقیده و یا نابودی یک گروه یا کشور می باشد.

در جنگ سایبر از شبکه های کامپیوتری به عنوان بستر انجام این اعمال خرابکارانه استفاده می شود.

مگان برنز در سال ۱۹۹۹، با نگرشی کلی تعریف زیر را ارئه می‌دهد: «جنگ اطلاعاتی طبقه یا مجموعه‌هایی از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن، یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند».
مارتین لیبیکی ضمن وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل گوناگون جنگ اطلاعاتی را به شرح زیر نام می‌برد:

- **جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن است.**
- **جنگ بر پایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم‌هایی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.**
- **جنگ الکترونیک تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری.**
- **جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرز فکر دوستان، بی‌طرف‌ها و دشمنان استفاده می‌شود.**
- **جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.**
- **جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.**
- **جنگ سایبری ترکیبی از همه موارد شش‌گانه بالا.**

ویژگی های جنگ سایبر

۱) **بدون مرز بودن فضای سایبر**
۲) **کاهش هزینه جرم و یا حمله**
۳) **امکان وارد آوردن خسارات مالی ، بدون آسیب های جسمی**
۴) **تامین راحت امکانات و عوامل مورد نیاز برای اقدامات تروریستی**
۵) **انعکاس جهانی موفقیت، مکتوم ماندن شکست ها**
۶) **امکان هماهنگی لحظه ای در سراسر جهان با ضریب اطمینان بالا**
۷) **امکان یارگیری و جذب حامیان از سراسر جهان**

دلایل اصلی تغئیر ماهیت جنگ ها

۱) **کاهش تلفات انسانی(پیروزی بدون خونریزی)**
۲) **کاهش هزینه های جنگی**
۳) **کاهش زمان عملیات ها**
۴) **اثر بخشی بیشتر**
۵) **ابعاد گسترده تر(نظامی، اقتصادی، اجتماعی، سیاسی، صنعتی و....)**
۶) **امکان بکارگیری از همه مولفه های قدرت**
۷) **ریسک کم**
۸) **قدرت زیاد در کنترل احساسات**

تهدیدات سایبری

هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به ماموریت‌ها، وظایف، سامانه های سایبری یا پرسنل دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، تخریب، افشاء، تغییر اطلاعات، ممانعت یا اختلال در ارائه خدمت را تهدید سایبری گویند.

سه مشخصه تهدید سایبری

گستردگی: 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 خطر قرار دارد. بنابراین کشورها با فعالیت های خصمانه ای روبرو هستند که می تواند تهدید کننده یکپارچگی زیرساخت های حیاتی آنها باشد و به عنوان مثال سامانه های مالی را از پایداری خارج سازد و 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 تحلیل ببرد.

نهفتگی: تهدیدات مربوط به یکپارچگی اطلاعات و امنیت در فضای سایبری عمیقاً در حوزه سایبر نهفته می باشند. این تهدیدات ناشی از آسیب پذیری های بالقوه موجود یا قرار داده شده در سیستم های عامل نرم افزاری پیچیده و هم ناشی از سخت افزارهای بالقوه معیوب یا ناقص می باشند. 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 حین عبور کالاها از زنجیره تأمین در آنها تعبیه می شوند.

تنوع: تهدیدات در فضای سایبری متنوع می باشند. گروه های جنایتکار و خرابکار با سازماندهی مناسب، سازمانهای مستقل مدیریتی و هکری از هر مارکی در صحنه حضور دارند. هر کدام از این عاملان خرابکاری نوع مجزایی از تهدید را تحمیل می کنند که نیاز به پاسخ های مختص به خود را دارد.

منابع تهدید سایبری

منبع تهدید	توصیف
کشورهای خارجی	سرویس های اطلاعاتی کشورهای خارجی برای انجام بخشی از فعالیت های جمع آوری اطلاعات و جاسوسی خود از ابزار سایبری استفاده می کنند. در سطح جهان موارد متعددی از این دست برای سوء استفاده و تخریب زیرساخت های اطلاعاتی کشورها شامل اینترنت، شبکه های اطلاعاتی، سامانه های رایانه ای و پردازشگرها و کنترل کننده های نهفته در صنایع حیاتی مشاهده شده است.
گروه های خرابکار	به طور روزافزون تهاجمات سایبری این گروه ها که به منظور کسب درآمد به سامانه های سایبری حمله می برند رو به افزایش است.
هکرها	هکرها گاهی اوقات برای اظهار وجود خود وارد شبکه می شوند. در شرایط فعلی نفوذ به شبکه ها با حداقل دانش و مهارت امکان پذیر است به این طریق که آنها برنامه ها و پروتکل های لازم را اینترنت دریافت نموده و همان ها را بر علیه سایت های دیگر بکار می برند.
هکرهای سازمان یافته	حملات دارای انگیزه سیاسی به صفحات وب مورد نیاز عموم مردم یا میزبان های پست الکترونیک هکتیویسم نام دارد. این افراد معمولاً میزبان های پست الکترونیک را با افزایش بار مواجه نموده و با نفوذ به سایت های شبکه وب پیام های سیاسی خود را اعلام می نمایند.
عوامل ناراضی داخلی	عوامل ناراضی داخلی که از درون سازمان کار می کنند منبع اصلی جرایم رایانه ای هستند و این دسته از عوامل لازم نیست دانش قابل توجهی در خصوص تهاجمات رایانه ای داشته باشند زیرا اطلاع آنها از سیستم مورد هدف غالباً امکان دسترسی نامحدود برای وارد کردن ضربه به سامانه و یا سرقت اطلاعات سازمان را فراهم می سازد. تهدید عوامل داخلی شامل کارکنان پیمان کاران نیز می شود.
تروریستها	تروریست ها به دنبال تخریب، ناتوان سازی و یا بهره برداری بدخواهانه از زیرساخت های حیاتی به منظور تهدید کردن امنیت ملی، وارد آوردن خسارات سنگین، تضعیف اقتصاد کشور و تخریب روحیه و اعتماد عمومی می باشد.

تنوع حملات سایبری

- **استراق سمع به‌صورت عام ، (مکالمات، دیتا، تصویر) به روش‌های مختلف و از راه دور**
- **جاسوسی از راه دور و از طریق بستر شبکه**
- **اختلال یا قطع شبکه‌های اطلاع رسانی مانند قطع سیگنال رسانی به صدا و سیما**
- **قطع کامل یا اختلال در شبکه‌های ارتباطات تلفنی داخل و یا خارج از کشور (شهری، بین شهری، بین‌الملل، موبایل)**
- **اختلال در شبکه‌های مراکز مختلف خدماتی از قبیل: بانک‌ها، پالایشگاه‌ها، نیروگاه‌ها، سدها، مراکز صنعتی، مراکز کنترلی، شبکه‌های حمل و نقل و ترافیک، شبکه‌های توزیع برق و آب و...**
- **انهدام و یا آسیب‌رسانی به تاسیسات صنعتی کشور از قبیل پالایشگاه‌ها، نیروگاه‌ها و... با استفاده از نفوذ در سیستم های کنترلی این تاسیسات**
- **عضویت غیرارادی سرورها و رایانه های کشور در گروه‌های هکری و سربازگیری الکترونیکی موسوم به بات نت جهت سازماندهی و مشارکت غیرارادی در حملات سایبری**
- **ممانعت از استفاده برخی سرویس‌های شبکه جهانی اینترنت به بهانه تحریم‌ها**
- **قطع ارتباط با سامانه میزبانی Hosting(مراکز داده در مواقع حساس)**
- **حمله سایبری به مراکز نگهداری داده اعم از بومی و غیر بومی**
- **دسترسی غیر مجاز به بانک‌های اطلاعاتی مختلف از قبیل دسترسی غیر قانونی به بانک اطلاعاتی سازمان ثبت احوال کشور**
- **ورود غیر قانونی به حریم خصوصی افراد و امکان ایجاد مشکلات مختلف برای زندگی مردم**
- **حمله به وب سایت‌های متعلق به سازمان ها ، نهادها به منظور جلوگیری از ارائه خدمات به مردم**

انواع حملات از نظر تاثیر در ارتباط

حملات خاموش یا غیرفعال (Passive):

این حملات شامل فعالیت هایی می شوند که در آنها بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سیستم های آسیب پذیر، به آنها نفوذ شده و منجر به سوء استفاده از منابع سیستم می گردد. مانند:

افشای پیام (Release of message content)

تحلیل ترافیک (Traffic analysis)

حملات فعال (Active):

این حملات، حملاتی هستند که به سیستم های رایانه ای زیرساخت های حیاتی نفوذ می کنند و میتوانند اطلاعات حساس را دستکاری کنند و باعث بروز حوادث و فجایع ملی و جبران ناپذیر گردند .از اهداف آنها می توان، از کار انداختن شبکه های خدماتی عمومی مثل شبکه برق، گاز و ... و همچنین ایجاد وحشت و ترس در جامعه و کاهش میزان اعتماد به دولت و نظام را برشمرد. مانند:

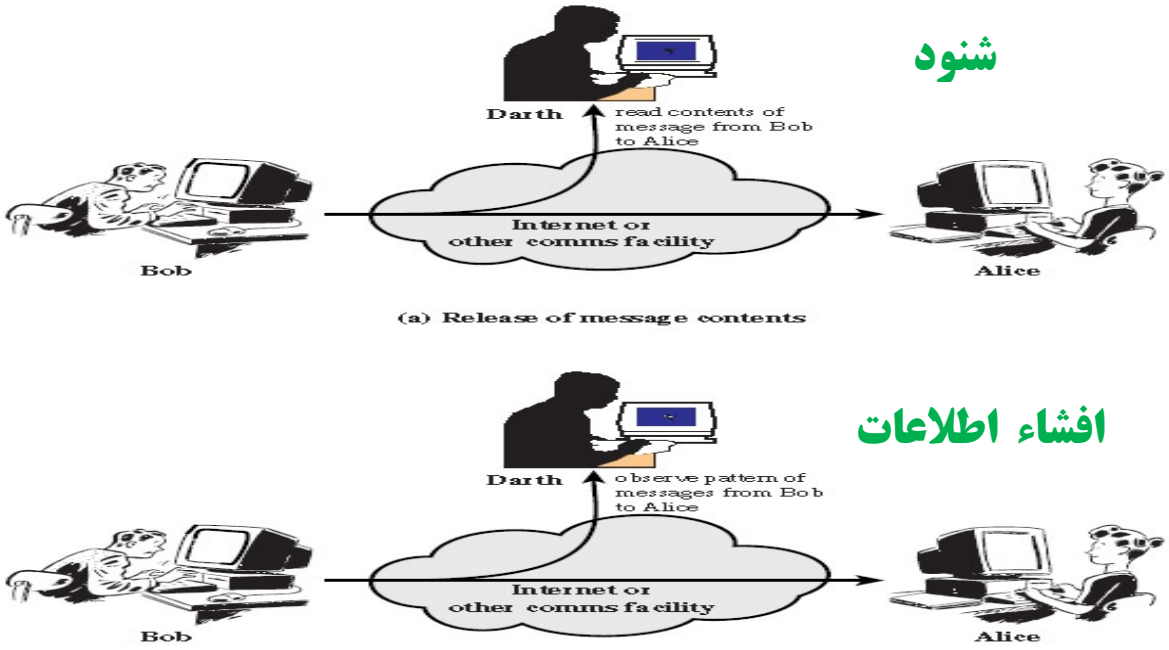
جعل هویت (Masquerade)

ارسال دوباره پیام (Replay)

تغییر پیام (Modification of message)

منع سرویس (Denial of Service – DOS)

نمونه حملات غیرفعال



نمونه حملات فعال

(a) Masquerade

(b) Replay

(c) Modification of messages

انکار

(d) Denial of service

انواع ابزارها و روشهای حملات سایبری

بدافزارها: (malicious software)

ابزارهای بد نیتی هستند که به صورت مخفیانه وارد سیستم کاربر میشوند و اعمال خاص بدافزارها خود را روی داده های قربانی انجام میدهند که ممکن است خساراتی به بار آورند و به علت آنکه معمولاً کاربر را آزار می دهند یا خسارتی به وجود می آورند، به این نام مشهورند. Malware واژه ای عمومی برای معرفی انواع ویروس ها، کرم ها، ابزارهای جاسوسی، تروآ و ... است.

ویروس (Virus) :

ویروس برنامه یا کد(اسکریپت) بسیار کوچکی است که بر روی برنامه های بزرگتر سوار می شود، یعنی در بین کد های اصلی یا فایل های اصلی یک برنامه دیگر که معمولا پر کاربرد می باشد قرار می گیرد و به محض نصب برنامه اصلی خود را وارد سیستم رایانه ای شخص قربانی می کند و هنگام اجرای برنامه به طور خود کار اجرا می شود و شروع به تخریب (کارهایی که نویسنده ویروس از آن خواسته) می کنند .

کرم اینترنتی (Worm) :

یک کرم در واقع کد خرابکاری است که خود را انتشار می دهد و قادر است به صورت خودکار در شبکه ها گسترش پیدا کند. یک کرم می تواند دست به اعمال مضری مانند مصرف پهنای باند شبکه یا مصرف منابع محلی سیستم بزند و منجر به حملات انکار سرویس شود .برخی از کرم ها می توانند بدون مداخله کاربر اجرا شده و گسترش پیدا کنند در حالی که برخی از کرم ها نیاز دارند کاربر آنها را مستقیماً اجرا کرده تا بتوانند گسترش پیدا کنند .کرم ها علاوه بر تکرار خود قادرند یک عملیات خرابکارانه را نیز بر سیستم قربانی اعمال کنند.

اسب تروا (Trojan) :

گونه دیگر از برنامه های مخرب اسب تروا یا همان تروجان است .این نوع از برنامه ها در ظاهر برنامه هایی مفید و بی ضرر هستند ولی در اصل کار این برنامه ها تخریب و دزدی اطلاعات است. تروجان می تواند از طریق ایمیل و یا سایت های گول زننده انتقال یابد از این نوع مخرب بیشتر برای دزیدن کلمه عبور ایمیل ها استفاده می شود که برای فرد قربانی به صورت عکس و یا برنامه های گول زننده مانند کرک نرم افزار فرستاده می شود.

: SYSTEM MONITOR

سیستم مانیتور برنامه ای خاص است که برای کنترل فعالیت کاربران استفاده می شود این گونه برنامه ها می توانند اطلاعاتی از قبیل آدرس ایمیل و کلمات عبور و کلماتی که توسط صفحه کلید تایپ شده را جمع آوری کنند .این نوع از برنامه ها حتی می توانند از فعالیت های کاربران عکس برداری کنند و به یک ایمیل خاص ارسال کنند.

BACK DOOR:

به زبان ساده تر از در پشتی وارد شدن .این نوع از برنامه ها که یک هکر بر روی یک سیستم اجرا کرده و راه را برای نفوذ مجدد باز می کند.

TRACE:

یک نوع دیگر از برنامه ها تریس می باشند این گونه از برنامه ها می توانند به صورت های مختلف اعمال تخریب را انجام دهند به صورتی که می توانند وارد محیط ریجستری شده و یا در حافظه رم و یا درون دیسکت ها مقیم شوند و حتی خود را با یک برنامه ترکیب کرده و اعمال تخریب را انجام دهند.

SPY :

هر برنامه ای که بصورت مخفیانه وارد سیستم شود اسپای یا جاسوس نامیده می شود که این نوع از مخرب ها کلمه عبور ایمیل و آی دی و حتی کارت های اعتباری را برای فرد هکر ارسال می کنند.

باج افزار Ransomware:

باج افزارها نوعی از بدافزارهای مخرب هستند که به سیستم های رایانه ای (کامپیوتر – لپ تاپ – تلفن همراه و ...) قربانی حمله کرده و دسترسی کاربر به اطلاعاتش را از بین میبرند و در ازای باز کردن دسترسی درخواست پرداخت مبلغ به حساب طراح باج افزار میکنند. نفوذگر از طریق ارسال ایمیل یا پیام کاربر را تشویق به کلیک روی لینک خاصی میکند که کاربر غافل از آن با کلیک روی لینک مربوطه باعث میشود باج افزار پنهان در لینک، به سیستم یا تلفن همراه وارد شده و باعث سوء استفاده از اطلاعات یا از بین رفتن آنها شود.

بطور معمول زمانی که سیستمی به باج افزار آلوده شود قربانی راهی جز فرمت سیستم (که باعث از بین رفتن تمامی اطلاعات میشود) و یا اطاعت از باج گیرنده، ندارد.


باج افزار چیست و چگونه کار می کند؟
باج افزار یک تهدید امنیتی جدی است که دسترسی به فایل ها و سیستم را محدود کرده و قربانی را مجبور به پرداخت باج می کند.
چگونه ممکن است سیستم عامل آلوده شود؟
سایر نرم افزارهای مخرب
ایمیل های اسپم
وب سایت های آلوده
داده ها چگونه از دست می روند؟
پیغام باج خواهی نمایش داده می شود.
فایل های شخصی را پیدا و رمز گذاری می کند.
صفحه نمایش را قفل می کند.
به دستگاه قربانی ورود پیدا می کند.
باج افزار رمزگذاری فایل ها چگونه کار می کند؟
هنگامی که باج افزار روی سیستم قرار بگیرد ،به یکی از دامنه های مشخص شده وصل می شود.
برای هر فایل یک رمز قرار می دهد.
باج افزار ، کلید رمز شده را اول هر فایل می نویسد.
باج افزار دنبال فایل های مهم با پسوند مشخص مانند pdf یا docx می گردد.
CYBER POLICE

مراحل هفت گانه حملات سایبری:

امروزه حملات سایبری، فقط یک حادثه مجزا و تک‌مرحله‌ای نیستند. به همین دلیل دفاع در برابر آن‌ها، احتیاج به مهارت‌های سایبری دارد. حملات سایبری دارای مراحلی است که آن‌ها را به ۷ دسته، تقسیم می‌کنند و در هر مرحله باید دفاع متناسب با آن صورت بگیرد تا بتوانیم دفاع فعال سایبری را انجام داده باشیم.

۱) **بازشناسی: در این مرحله دشمن، اهداف خود را تشخیص می‌دهد. معمولاً در این مرحله، هکرها به دنبال یافتن آسیب‌پذیری‌ها هستند.**
۲) **مسلح شدن: در این مرحله، دشمن ابزار حمله‌ی خود را انتخاب می‌کند.**
۳) **ارسال: دشمن در این مرحله، بدافزار یا هرگونه ابزار دیگر را به هدف موردنظر، انتقال می‌دهد.**
۴) **به کار انداختن: در این مرحله، ابزار موردنظر هکر، در کمین قربانی است تا به‌محض انجام هرگونه اقدامی، به هدف هجوم آورد.**
۵) **استقرار: بدافزار یا هر ابزار دیگری، در این مرحله، خود را از در سیستم وی، مخفی می‌کند.**
۶) **کنترل و فرماندهی: زیرساخت‌های کنترل و فرماندهی شامل سرورها و سایر زیرساخت‌های فنی است که برای کنترل بدافزار به کار می‌رود.**
7) **انجام مأموریت: در نهایت ابزار موردنظر هکر، به اهداف وی، جامه‌ی عمل می‌پوشاند و انتظارات هکر را برآورده می‌کند.**

امنیت شبکه های کامپیوتری

امنیت چیست؟

امنیت یک مفهوم آشنا و قابل شناخت برای تمام جوامع بشری از جوامع آغازین همانند قبایل کوچک گرفته تا امپراتوری های بزرگ جهان باستان بوده و حالت فراغت نسبی از تهدید یا حمله یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. بعبارتی امنیت یعنی : حفاظت از آنچه برای ما ارزشمند است. حفاظت در برابر حملات عمدی و غیر عمدی.

امنیت اطلاعات

امنیت اطلاعات (Information Security) یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری.

قواعد امنیت اطلاعات

- **محرمانگی :این بدین معنی است که اطلاعات تنها توسط کسانی که مجوز دسترسی به آن را دارند دیده یا مورد استفاده قرار می‌گیرند.**
- **جامعیت :این بدین معنی است که انجام هرگونه تغییرات بر روی اطلاعات توسط کاربرِ غیرمجاز، غیرممکن خواهد بود (یا در پائین ترین سطح، شناسایی خواهد شد) و تغییراتی که توسط کاربران مجاز انجام می‌شوند پیگیری خواهند شد.**
- **دسترس‌پذیری :این بدین معنی است که کاربر مجاز هرگاه که نیاز داشته باشد می‌تواند به اطلاعات دسترسی داشته باشد.**

امنیت اطلاعات در گذشته :

نگهداری اطلاعات در قفسه های قفل دار

نگهداری قفسه ها در مکانهای امن

استفاده از نگهبان

استفاده از سیستمهای نظارت

به طور کلی: روشهای فیزیکی و مدیریتی

امنیت اطلاعات نوین:

نگهداری اطلاعات در کامپیوتر

برقراری امنیت در کامپیوترها ی شبکه ها

برقراری ارتباطات بین شبکه ای کامپیوترها

اقدامات اولیه امنیت اطلاعات:

۱) پیشگیری (**Prevention**) : به منظور جلوگیری از خسارت
۲) ردیابی (**Tracking**): شامل تشخیص (**Detection**) میزان خسارت ، تشخیص هویت دشمن و تشخیص کیفیت حمله (زمان، مکان، دلایل حمله، نقاط ضعف ...)
۳) واکنش (**Reaction**) : یعنی بازیابی و جبران خسارت و همچنین تقویت ساختار جهت جلوگیری از حملات مجدد

مفاهیم اولیه امنیت اطلاعات :

حمله امنیتی (**Security Attack**) :عملی که امنیت اطلاعات سازمان را نقض کند

سیاست امنیتی(**Security Policy**): تعیین می کند که از جنبه امنیتی چه کارهایی مجاز یا غیر مجازند.

مکانیزم امنیتی(**Security Mechanism**) : روشی برای تشخیص، جلوگیری و بازیابی حملات، درواقع یکی از روشهای پیاده سازی یک سیاست امنیتی

سرویس امنیتی(**Security Service**) :سرویسهای تضمین کننده با استفاده از مکانیزمهای امنیتی

Hack: کنکاش به منظور کشف حقایق و نحوه کار سیستم

Attack: تلاش برای نفوذ به سیستم دیگران

انواع هکر

گروه نفوذگران کلاه سفید:

هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند که در حقیقت متخصصین شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا کرده و به مسئولان گزارش می‌دهند.

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 می‌پردازند.

گروه نفوذگران کلاه خاکستری:

اشخاصی هستند که حد وسط دو تعریف بالا می‌شوند.

گروه نفوذگران کلاه صورتی:

این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت دیگران اقدام می‌کنند.

گروه نفوذگران کلاه قرمز:

در مورد هکرهای کلاه قرمز هم می توان گفت در واقع مو ضع آنها هم مانند کلاه خاک ستری ها میان کلاه سفیدها و سیاه ها مشخص و شفاف نیست. آنها معمولا در سطح سازمان ها و وزارت خانه ها و مجموعه های حساس دست به عملیات هک می زنند و به طور کلی به دنبال اطلاعات حساس و فوق سری می باشند.

گروه نفوذگران کلاه آبی:

واژه کلاه آبی اولین بار از اصطلاح به کار گرفته شده توسط شرکت مایکروسافت برای مجموعه ای از هشدارها و تو ضیحات امنیتی در خصوص محصولات خود مورد بهره برداری قرار گرفت. یک هکر کلاه آبی به فردی گفته می شود که خارج از محدوده مشاوران امنیتی قرار گرفته و وظیفه وی آزمون و تست باگ های احتمالی سیستم قبل از ارائه و استفاده آن تو سط کاربران می با شد. بدین ترتیب فعالیت وی را می توان به عنوان یکی از مراحل توسعه سیستم جهت رفع و برطرف سازی باگ های احتمالی سیستم های اطلاعاتی در نظر گرفت.

هک تیویست:

واژه بکارگرفته شده از تلفیق دو کلمه هک و اکتیویسم (فعالیت اجتماعی) بوجود آمده است. هکتیویست‌ها هکرهایی هستند که برای اعلام و تبلیغ عقاید مذهبی، سیاسی، اجتماعی و غیره خود دست به این عمل

میزنند. نتایج هک این دسته از هکرها معمولا با تغییر صفحه اول یک سایت مخالف به شعار دلخواه خود و یا از دسترس خارج کردن آن همراه است.

فریکر:

این نوع هکرها معمولا متخصصین حوزه ارتباطات هستند که کارشان نفوذ به خطوط تلفن برای برقراری تماس مجانی و یا استراق سمع است. در گذشته برقراری تماس های راه دور از طریق اینترنت و خطوط تلفنی متصل به شبکه (VOIP) کمتر موجب شکل گیری این نوع هکرها می شد، ولی امروزه با توجه به افزایش پهنای باند اینترنت حملات از این قبیل به وفور در کشور خودمان نیز دیده می شود.

تفاوت هکر و کراکر:

در اینجا به یک دیگراز واژه های مصطلح در دنیای امنیت اطلاعات که ممکن است در برخی از موقعیت ها به جای کلمه هکر و یا در کنار آن مورد استفاده قرار گیرد، با عنوان کراکر یا کرکر (Cracker)اشاره می کنیم. در واقع تفاوت دو واژه هکر و کرکر به صورت کلان این گونه توضیح داده می شود که هکرها معمولا به دنبال رخنه های امنیتی هستند و در بسیاری از موارد حتی ممکن است به سیستم آسیب وارد نکنند. آنها معمولا از دانش نسبتا مناسبی در زمینه امنیت (در حوزه های مختلف برنامه نویسی، شبکه و غیره) برخوردار هستند. اما وقتی از کلمه کرکر استفاده می کنیم، در واقع از ماهیتی استفاده می کنیم که در آن فرد مهاجم درصدد نفوذ به سیستم و دستیابی به دسترسی های غیرمجاز است. مهم ترین مشخصه کرکر اقدام به تخریب کنترل های امنیتی و یا حتی سیستم مورد هدف می باشد که می تواند تمایز اصلی آن از هکر درنظر گرفته شود.

دلایل دشواری برقراری امنیت اطلاعات:

افزایش پیچیدگی و تهدید امنیت بدلیل تکامل پروتکلها

امنیت: قربانی افزایش کارایی و مقیاس پذیری میشود.

امنیت بالا: هزینه برمیباشد.

امنیت به عنوان مانعی در برابر انجام کار کاربران عادی است.

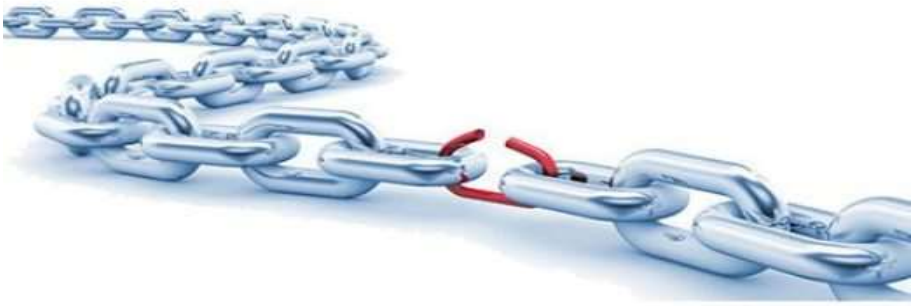
عدم پیروی از سیاستهای امنیتی بدلیل در اختیار بودن اطلاعات و ابزارهای دور زدن امنیت و همچنین

مبارزه و لذت بردن از دور زدن امنیت برای افراد داخل و خارج سیستم.

عدم در نظر گرفتن ملاحظات امنیتی در طراحی های اولیه سیستمها و شبکه ها سبب بروز مشکلاتی درزمان پیاده سازی ساختارهای امنیتی میگردد.

آسیب پذیری چیست؟

آسیب‌پذیری، به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی یا پیاده‌سازی آن سرمایه، که قابلیت بهره‌برداری یا فعال‌شدن توسط یک تهدید خارجی را داشته باشد، اطلاق می‌گردد.



منشاء آسیب پذیری های سایبری:

۱) **ضعف موجود در فناوری مورد استفاده در سامانه سایبری موردنظر**
۲) **ضعف پیاده سازی (تولید) سامانه سایبری موردنظر**
۳) **ضعف تنظیمات و بهره‌برداری از سامانه سایبری موردنظر**

ضد بد افزار Anti-Malware چیست؟

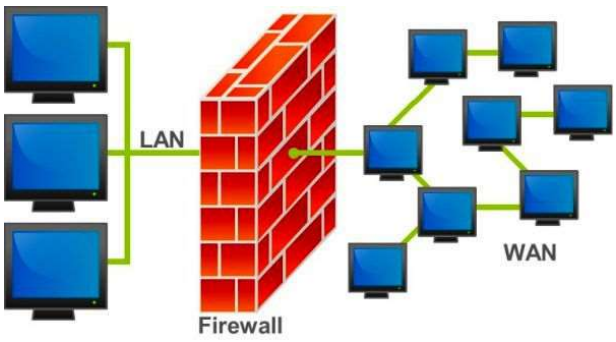
نرم افزاری که از ورود برنامه‌های مخرب به دستگاه جلوگیری کرده، یا آن‌ها را مورد شناسایی قرار داده و پاکسازی می‌کند.انواع آن عبارتند از:

- **آنتی ویروس**
- **آنتی ورم**
- **آنتی تروجان**
- **آنتی اسپای**
- ...
- **آنتی باج افزار**

دیوار آتش (فرهنگستان : بارو یا تار بارو) چیست؟

دیوار آتش مجموعه سخت افزاری و نرم افزاری است که از دستیابی غیر مجاز به یک سیستم رایانه ای و یا شبکه جلوگیری می کند. در اصطلاح فایروال سیستمی است که شبکه و یا کامپیوتر شخصی شما را در مقابل نفوذ مهاجمین، دسترسی‌های غیرمجاز، ترافیک‌های مخرب و حملات هکرها محافظت کند. با استفاده از دیوار آتش امکان ارسال و یا دریافت اطلاعات محدود می شود. همچنین درگاه ها و سطح های دسترسی نیز قابل تعریف برای افراد و یا نرم افزارهای مشخصی خواهند بود. انواع دیوار آتش عبارتند از:

- **فایروال های شبکه Network firewalls**
- **فایروال های نسل جدید Next-generation firewalls**
- **فایروال های برنامه تحت وب Web application firewalls**
- **فایروال های پایگاه داده Database firewalls**
- **مدیریت یکپارچه تهدید ها UTM**
- **فایروالهای ابری Cloud firewalls**
- **فایروال های تقسیم شبکه ISFW**



VPN چیست؟

VPNشما را به جای وارد کردن مستقیم به فضای شلوغ و ناامن اینترنت به یک شبکه خصوصی از اینترنت که فقط محدود به خودتان است، متصل می‌کند. VPNها مکان‌یابی شما را بر اساس آی‌پی، به جایی که اصلا معلق به شما نیست، انتخاب می‌کنند. از همین طریق است که شما خودتان می‌توانید امنیت‌تان را در فضای اینترنت تامین کنید. یکی دیگر از کاربردهای VPNها، ریموت کردن کارمندان یک کمپانی به شبکه خصوصی اداره بوده؛ حتی اگر به صورت فیزیکی در اداره حضور نداشته باشند!

WAFچیست؟

WAFیا Web Application firewallبا فیلتر کردن و نظارت بر ترافیک HTTPبین یک برنامه وب و اینترنت به محافظت از برنامه های وب کمک می کند. این برنامه به طور معمول از برنامه های وب در برابر حملاتی مانند : cross-site forgery ، cross-site-scripting (XSS) ، file inclusion ، SQL injection و سایر موارد محافظت می کند.

Honeypot چیست؟

یک Honeypot سیستمی است که در شبکه سازمان قرار می گیرد، اما برای کاربران آن شبکه هیچ کاربردی ندارد و در حقیقت هیچ یک از اعضای سازمان حق برقراری هیچگونه ارتباطی با این سیستم را ندارند. این سیستم دارای یک سری ضعفهای امنیتی است. از آنجاییکه مهاجمان برای نفوذ به یک شبکه همیشه به دنبال سیستمهای دارای ضعف می گردند، این سیستم توجه آنها را به خود جلب می کند. و با توجه به اینکه هیچکس حق ارتباط با این سیستم را ندارد، پس هر تلاشی برای برقراری ارتباط با این سیستم، یک تلاش خرابکارانه از سوی مهاجمان محسوب می شود. در حقیقت این سیستم نوعی دام است که مهاجمان را فریب داده و به سوی خود جلب می کند و به این ترتیب علاوه بر امکان نظارت و کنترل کار مهاجمان، این فرصت را نیز به سازمان می دهد که فرد مهاجم را از سیستمهای اصلی شبکه خود دور نگه دارند.

Honeypot»یک سیستم اطلاعاتی است که ارزش آن به استفاده غیر مجاز و ممنوع دیگران از آن است. »

پشتیبان گیری از اطلاعات:

اگر روزی اطلاعات شخصی شما توسط یک سری عوامل ناشناخته از بین برود احتمال اینکه اطلاعات شما برای همیشه از دست برود بسیار زیاد است. و گاهی اوقات بازیابی این اطلاعات دشوار است. لذاشما باید قبل از اینکه به این مسائل گرفتارشوید نسخه ای از این اطلاعات را در جای دیگری ذخیره کنید. به این عمل بک آپ گیری یا .پشتیبان گیری می گویند

به این معنا است که اگر روزی اطلاعات اصلی شما به هر دلیلی پاک شد یا از بین رفت بتوانید از طریق بک آپی .که قبلا از آن اطلاعات گرفته اید دوباره آن اطلاعات را بازگردانید

استانداردردهای جهانی امنیت اطلاعات:

اســتانداردهای مختلفی در زمینه فناوری اطلاعات و ارتباطات وجود دارد که منجر به امنیت اطلاعات می‌شــوند، مانند PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, PCI DSS, COSO, SOA, ITIL : و .COBITاما بعضی از این استانداردها به دلایل مختلف چندان مورد استقبال سازمان‌ها قرار نگرفته است . چهار اســتاندارد برتر شــامل,ISO27001 ، PCI DSS, ITILو COBIT هســتند. در ادامه به بررســی اجمالی کلیات هر یک از این چهار استاندارد می‌پردازیم:

ISO27001

اســتاندارد بین‌المللی ISO27001 الزامات ایجاد، پیاده‌ســازی، پایش، بازنگری، نگهداری و توســعه ISMS در سازمان را مشخص می‌کند. این استاندارد برای ضمانت انتخاب کنترل‌های امنیتی بجا و مناسب برای حفاظت از دارایی‌های اطلاعاتی، طراحی شده است. زمانی که یک سازمان موفق به دریافت گواهینامه مربوط به استاندارد ISO27001می‌شــود، به این معنی اســت که آن ســازمان توانســته امنیت را در زمینه اطلاعات خود مطابق با بهترین روش‌های ممکن مدیریت کند. این اســتاندارد (به خصــوص نســخه ۲۰۱۳ آن) برای پیاده‌ســازی در انواع سازمان‌های دولتی، خصوصی، بزرگ یا کوچک مناسب است. در ایران با توجه به تصویب سند افتا توسط دولت و الزامات سازمان‌های بالادستی در صنعت‌های مختلف، کلیه سازمان‌ها و نهادهای دولتی، ملزم به پیاده سازی ISMSشــدند و اکثر این ســازمان‌ها به پیاده‌ســازی الزامات اســتاندارد ISO27001 رو آوردند.علاوه بر اینکه استاندارد ISO27001 خود حاوی کنترل‌های امنیتی جامعی جهت تضمین امنیت سازمان است، همچنین می‌تواند به عنوان یک بستر مدیریتی جهت پیاده سازی کنترل‌های امنیتی بیشتری که در استانداردهای دیگر وجود دارد، مورد استفاده قرار گیرد.

PCI DSS

ا ستاندارد امنیت اطلاعات در صنعت کارت پرداخت (PCI DSS) یک ا ستاندارد امنیت اطلاعات جهانی ا ست که تو سط انجمن ا ستانداردهای امنیت صنعت کارت پرداخت برای افزایش امنیت کارت‌های اعتباری ایجاد شد. این استاندارد به طور اختصاصی برای سازمان‌هایی مفید است که در زمینه کارت‌های اعتباری، کیف الکترونیکی، ATM، POSو... اطلاعات مشتریان را نگهداری، پردازش یا مبادله می‌کنند.

اعتبار این ا ستاندارد به صورت سالیانه بررسی می شود. برای سازمان‌های بزرگ بررسی انطباق تو سط یک ارزیاب مستقل انجام می‌شود اما سازمان‌های کوچک‌تر می‌توانند انطباق خود را توسط پرسشنامه خود ارزیابی و بررسی کنند.

ITIL

ITILیک چارچوب عمومی ا ست که بر پایه تجارب موفق در مدیریت سرویس‌های آی‌تی در سازمان‌های دولتی و خصوصی در سطح بین‌المللی به وجود آمده است ITIL .در اصل یک استاندارد نیست بلکه چارچوبی است با نگاهی نوین برای بهبود ارائه و پ شتیبانی خدمات فناوری اطلاعات که امروزه از سوی سازمان‌های ارائه‌دهنده خدمات فناوری اطلاعات بسیار مورد توجه قرار گرفته ا ست. هدف اولیه این چارچوب این ا ست که مطمئن شود سرویس‌های آی‌تی با نیازهای کسب و کار سازمان منطبق، و در زمانی که کسب و کار به آن نیاز دارد پاسخگوی این نیاز است.

ITILبه عنوان مجموعه‌ای از کتاب‌ها به وجود آمده و بر پایه مدل دمینگ و چرخه PDCA ایجاد شده، نسخه فعلی ITIL که مورد استفاده قرار می‌گیرد، نسخه سوم است که پنج بخش اصلی را دربر دارد: استراتژی خدمات، طراحی خدمات، تحویل خدمات، اداره خدمات و بهینه‌سازی پیوسته خدمات.

همان‌طور که بیان شد، ITILبیشتر در شرکت‌هایی که کسب و کار آی‌تی دارند، مورد توجه قرار گرفته است.

COBIT

چارچوب کوبیت (COBIT) به حاکمیت فناوری اطلاعات در سازمان‌ها می‌پردازد و در سال‌های اخیر موردتوجه سازمان‌ها و مدیران قرار گرفته است تا به کمک آن بتوانند ارتباط خوبی بین اهداف و خط مشی‌های سازمان و فرایندهای سازمانی برقرار کرده و از توانمندسازهای سازمانی به خوبی و در یک راستا بهره بگیرند.

COBITمخفف Control Objectives for Information & related Technology به معنی کنترل اهداف و اطلاعات مربوط به فناوری های مرتبط است. این چارچوبی است که توسط) ISACA انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی) برای مدیریت فناوری اطلاعات ایجاد شده است. این طراحی به عنوان یک ابزار حمایتی برای مدیران طراحی شده است و اجازه می دهد تا شکاف اساسی بین موضوعات فنی، خطرات تجاری و

الزامات کنترلی پر شود .COBIT یک راهنمای کاملاً شناخته شده است که می تواند برای هر سازمانی در هر صنعتی اعمال شود.

به طور کلی، COBITکیفیت، کنترل و قابلیت اطمینان سیستم های اطلاعاتی را در یک سازمان تضمین می کند که یکی از مهمترین جنبه هر تجارت مدرن است.

بطور خلاصه می توان مزایای استفاده از چهارچوب COBIT را در چند مورد زیر خلاصه نمود:

۱- یک ابزار کارآمد برای بخش IT جهت پشتیبانی از اهداف تجاری یک سازمان

۲- ایجاد یک چرخه حیات کامل برای IT جهت پیش بینی هزینه های این بخش در تجارت یک سازمان

۳-بهبود هرچه بیشتر کیفیت سرویس های IT و موفقیت روزافزون در پروژه هایIT

۴- مدیریت موثر در مدیریت ریسک های مرتبط به بخش IT سازمان

همانطور که در شکل مشاهده می کنید هسته این چهارچوب را کنترل مستقیم بر روی فرایندهای IT تشکیل می دهد. فرآیندهایی که توسط این چهارچوب کنترل می شوند شامل:

۱- طراحی و سازماندهی فرآیندهایIT

۲- بدست آوردن و پیاده سازی فرآیندها

۳- تحویل و پشتیبانی فرآیندها

۴- پایش و ارزیابی مستمر فرآیندهای IT می باشد.

از یک منظر می توان گفت که COBIT یک هارمونی زیبا بین استانداردهایی مانندITIL ، PMBOKو ISO 27001و ISO 27002 می باشد که در درون خود چرخه حیاتIT ، نحوه مدیریت پروژه های IT و ایجاد یک چتر امنیتی استاندارد را در بر دارد.

پدافند سایبری چیست؟

بهره گیری از کلیه امکانات غیرمسلحانه سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی سایبری کشورهای متخاصم و گروه های تحت حمایت پنهان دولت های متخاصم، به نحوی که امکان تهاجم سایبری را از کلیه متخاصمین، سلب نماید.

چرخه پدافند سایبری:

متدولوژی پدافند سایبری

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری:

۱- شناسایی دارایی ها، مراکز و شبکه های سایبری و متکی به سایبر

۲- تعیین سطح اهمیت مراکز و شبکه های سایبری و متکی به سایبر به سطوح حیاتی، حساس و مهم

۳- تعیین تهدیدات سایبری مراکز و شبکه های تعیین سطح شده

٤- شناسایی آسیب پذیری های سایبری مراکز و شبکه های تعیین سطح شده

٥- تعیین مخاطرات سایبری در صورت اعمال تهدیدات بر آسیب پذیری ها

٦-محاسبه ریسک و تعیین ریسک قابل قبول

۷- ارائه راهکارهای پدافندی به منظور کاهش آسیب پذیری ها و مقابله با تهدیدات سایبری

۸- ارائه راهکارهای مقابله با حملات سایبری (تشکیل تیم cert و ...)

۹- ارائه طرح تداوم خدمات و فعالیت های ضروری در صورت بروز بحران سایبر ی

۱۰- پیاده سازی و اجرای راهکارهای ارائه شده

۱۱- نظارت، ارزیابی و کنترل اقدامات

۱۲- برگزاری رزمایش های سایبری

۱۳-رصد و پایش تهدیدات و آسیب پذیری ها و تعیین تهدیدات و آسیب پذیری‌های جدید

۱٤- تعیین پیامدهای تهدیدات و آسیب پذیری های جدید

۱٥- به روز رسانی راه کارهای پدافندی با توجه به تهدیدات و آسیب پذیری های جدید

۱٦- برگزاری آموزش های ارتقاء توانمندی های سایبری

دستورات اجرایی حوزه پدافند سایبری:

۱) سامانه ها و شبکه های فناوری اطلاعات و ارتباطات سطح بندی شود.

۲) دسترسی های فیزیکی و الکترونیکی به نقاط حساس سایت ها و شبکه ها و مراکز حیاتی، حساس و مهم کنترل شود.

۳) برنامه مدیریت بحران دفاع سایبری تهیه و تدوین شود.

۴) برای مقابله با تهدیدات سایبری، مانورهای عملیاتی در بخش فناوری اطلاعات و ارتباطات طراحی و اجرا شود.

۵) سازه های ویژه برای مراکز داده، اتاق سرور و اتاق کنترل و نظارت در مراکز حیاتی و حساس تامین شود.

۶) بخشهای حیاتی، حساس و مهم متناسب با اهمیت آن در برابر تهدیدات الکترومغناطیسی حفاظت گردد.

۷) از تجهیزات امنیتی بومی حوزه سایبری استفاده شود.

۸) درخرید تجهیزات و خدمات فناوری اطلاعات خارجی بر وجود قابلیت بومی سازی آن تاکید شود.

۹) از رمز کننده های سخت افزاری و نرم افزاری بومی و ساخت داخل استفاده گردد.

۱۰) برنامه ارتقاء امنیت برای نرم افزارهای سیستمی پایه در حوزه کارگزار(Server) و در حوزه کارخواه (Client) تهیه و تدوین شود.

۱۱) امنیت سرویس های تحت وب، سرویس دهندگان شبکه و همچنین سرویس کارگزار نامه امن(e-mail) ارتقاء یابد.

۱۲) اتصال تمامی نقاط شبکه یا کاربر منفصل در لایه های حیاتی و حساس از اینترنت قطع کامل ودر صورت ضرورت ارتباط با اینترنت، از نقاط جداگانه فاقد طبقه بندی استفاده گردد.

۱۳) از خطوط ارتباطی فیبر نوری استفاده حداکثری و از خطوط زمینی رادیوئی استفاده حداقلی شود و ارتباطات ماهواره ای در شبکه های حیاتی و حساس حذف گردد.

۱۴) از ظرفیت میزبانی بانکهای اطلاعاتی در داخل کشور استفاده گردد.

۱۵) نسخه پشتیبان از محتوی و اطلاعات موجود در شبکه در بازه های زمانی برنامه ریزی شده تهیه شود.

۱۶) جهت نگهداری، ذخیره سازی، بازیابی و پشتیبانی اطلاعات موجود در شبکه، برنامه امن سازی تدوین شود.

۱۷) طراحی و اجرای آموزش امنیت و قابلیت های دفاعی در حوزه سایبری برای کاربران و مدیران دستگاه در برنامه پیش بینی گردد.

قانون جرایم رایانه ای

این قانون مشتمل بر سه بخش و ۵۶ ماده در تیرماه سال ۱۳۸۸ ابلاغ گردید.

بخش یکم ـ جرائم و مجازات ها

فصل یکم ـ جرائم علیه محرمانگی داده ها و سامانه های رایانه ای و مخابراتی

مبحث یکم ـ دسترسی غیرمجاز

مبحث دوم ـ شنود غیرمجاز

مبحث سوم ـ جاسوسی رایانه ای

فصل دوم ـ جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی

مبحث یکم ـ جعل رایانه ای

مبحث دوم ـ تخریب و اخلال در داده ها یا سامانه های رایانه ای و مخابراتی

فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه

فصل چهارم ـ جرائم علیه عفت و اخلاق عمومی

فصل پنجم ـ هتک حیثیت و نشر اکاذیب

فصل ششم ـ مسؤولیت کیفری اشخاص

ماده۱۹ـ در موارد زیر، چنانچه جرائم رایانه ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه ای اختصاص یافته باشد.

سخنی با مدیران

امنیت در یک سازمان مستلزم :

داشتن سیاست ها

داشتن استاندارد ها

داشتن راهبرد ها(خط مشی ها)

سیاست ها سه نقش عمده ایفا می کنند :

۱) اول مشخص میکنند که از چه چیزی حفاظت می شود و چرا
۲) مسئولیت مربوط به تامین این حفاظت را مشخص می نمایند
۳) زمینه ای برای تفسیر وحل درگیری هایی که ممکن است در آینده به وجود آید ارائه می دهند

استاندارد ها :

۱) **از استاندارد ها برای معرفی راهکار های موفقیت آمیز امنیت در یک سازمان استفاده می شود .**
۲) **در عبارت های آن معمولاً از فعل "باید" استفاده می گردد .**
۳) **مستقل از بستر های فنی ارائه میشوند.**
۴) **حداقل یک معیار برای تعیین اینکه رعایت شده اند یا نه را ارائه می کنند.**
۵) **در طول زمان به آهستگی تغییر می کنند.**

راهبردها :

۱) **اسنادی هستند که معولاً در آنها فعل " بهتر است" به کار میرود.**
۲) **هدف راهبرد ها تفسیر استاندارد ها برای یک محیط خاص است .**
۳) **بر خلاف استاندارد ها ، در صورت نیاز تغییر می کنند.**

پیروزباشید