به نام خدا

اصول و مبانی فناوری اطلاعات

فصل پنجم

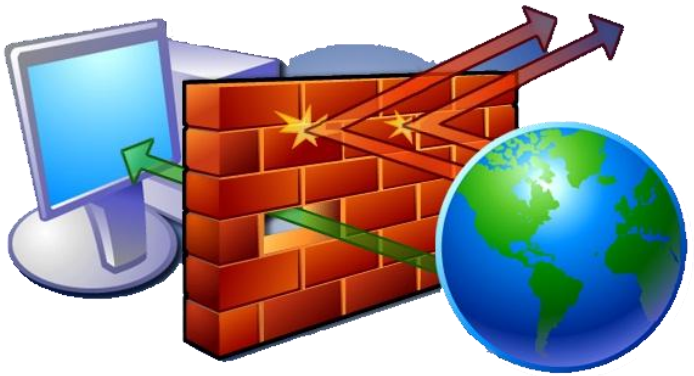
امنیت سایبری، قبول و تداوم کسب وکار

Chapter 5

CyberSecurity, Compliance, and Business Continuity

امنیت اطلاعات و شبکه چیست؟

- بسیاری از افراد استفاده از سخت افزار و نرم افزارها ذکر می‌کنند. مانند دیواره های آتش، رمزگذاری، نرم افزارهای ضد ویروس، ضد هرزنامه، ضد جاسوسی، ضد فیشینگ و غیره
- اما آیا استفاده از فناوری به تنهایی برای حفظ امنیت داده‌ها و کسب و کار کافی است؟



حفاظت از داده‌ها و کسب و کار

- شامل این موارد می‌باشد:
  - مهیا کردن و در دسترس قرار دادن داده‌ها و اسناد در تمام اوقات و همزمان محدود کردن دسترسی غیر مجاز
  - ترویج به اشتراک‌گذاری امن و قانونی اطلاعات در میان افراد و شرکای مجاز
  - تضمین پیروی از مقررات و قوانین دولتی
  - جلوگیری از حملات با مستقر کردن ابزارهای دفاعی در مقابل نفوذ به شبکه
  - کشف، تشخیص و واکنش بلادرنگ به حوادث و حملات
  - نگهداری و کنترل‌های داخلی جهت جلوگیری از دستکاری داده‌ها و رکوردها
- بنابراین علاوه بر فناوری، خط مشی کسب و کار، آموزش‌ها و طرح‌های بازیابی هم در امنیت اطلاعات نقش دارند.

- تا سال ۲۰۰۲، امنیت اطلاعات موضوعی بود که فقط به بخش فناوری اطلاعات سازمان محول می‌شد و به جای اتخاذ یک رویکرد پیش‌گیرانه، فقط سعی می‌شد هر زمان مشکلی پیش می‌آمد، به‌صورت موردی رفع و پاک‌سازی شود که برای سازمان هزینه بر بود.
- طبق گزارش Symantec در سال ۲۰۱۰، بزهکاران سایبری در هر ثانیه بیش از ۱۰۰ حمله را روی کامپیوترهای جهان به اجرا درآوردند.
- معمولا در هر ۴,۵ ثانیه یکی از حملات می توانست کامپیوتری را متأثر نماید.
- در یک دوره یکساله Symantec حدود ۲,۵ میلیون قطعه کد مخرب را شناسایی نمود.
- یکی از دلایل شیوع بدافزارها، در دسترس بودن رایگان یا ارزان بدافزارهای قدرتمند بود که بعضا خدمات پشتیبانی هم داشتند! و در مقابل هزینه پاک‌سازی پس از یک حادثه تا صدها میلیون دلار برآورد می‌شود.

چند اصطلاح امنیت فناوری اطلاعات

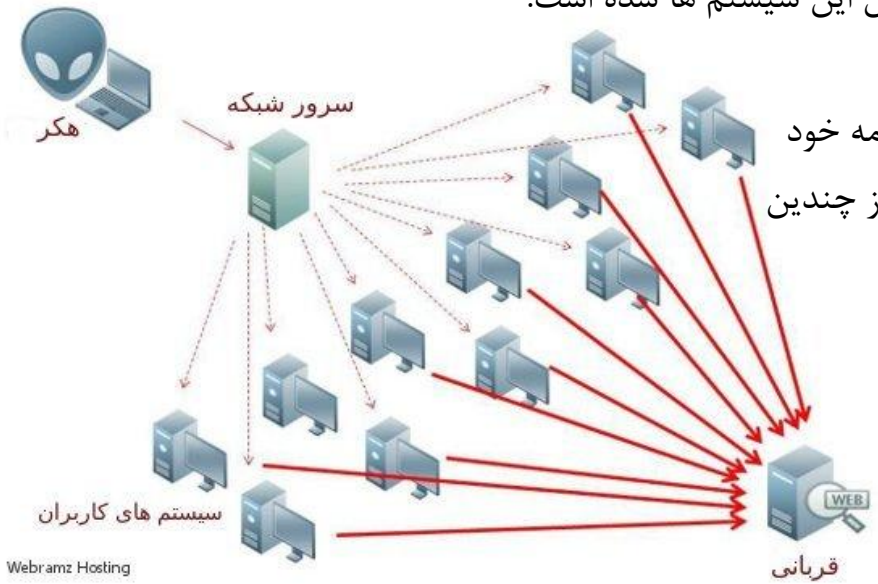
- تهدید: چیزی یا کسی که ممکن است موجب آسیب به یک دارایی شود.
- ریسک: احتمال اینکه یک تهدید از یک آسیب‌پذیری بهره‌برداری کند
- آسیب‌پذیری: ضعفی که محرمانگی، صحت یا در دسترس بودن یک دارایی را تهدید می‌کند.
- سه‌تایی محرمانگی، صحت و در دسترس بودن: سه اصل اساسی امنیت فناوری اطلاعات
- رمزگذاری: تبدیل داده‌ها به کد درهم آمیخته جهت حفاظت از آنها در مقابل خواندن و فهم آنها توسط کاربران غیرمجاز
- احراز هویت: روشی که معمولا برپایه نام کاربری و رمز عبور است تا بوسیله آن یک سیتم اطلاعاتی ادعای کاربری را راست آزمایی نماید.
- بدافزار (نرم‌افزار بدخواه): یک واژه کلی است که به یک ویروس، کرم، اسب تراوا و نرم افزارهای جاسوسی و تبلیغاتی اشاره دارد.
- نرم افزار ترساننده (نرم افزار/ضدویروس جعلی): برنامه‌هایی که وانمود می‌کنند کامپیوتر را جهت یافتن ویروس پویش می‌کنند و بعد اعلام می‌کنند کامپیوتر آلوده شده و از کاربر می‌خواهند با پرداخت وجهی از کارت اعتباریش، کامپیوتر وی را پاک‌سازی نمایند. سپس، بنظر می‌رسد که ویروس ناپدید شده اما در واقع سیستم به بدافزارهای دیگری آلوده می‌شود. این روش یکی از رایج ترین روش‌های کلاهبرداری اینترنتی است

چند اصطلاح امنیت فناوری اطلاعات

- بیومتریک‌ها: روش‌هایی برای شناسایی یک شخص بر اساس خصوصیات بیولوژیکی مانند اثر انگشت یا شبکیه
- امنیت پیرامون : اقدامات امنیتی جهت تضمین اینکه فقط کاربران مجاز به شبکه دسترسی دارند.
- امنیت نقاط انتهایی: اقدامات امنیتی حفاظت از نقاط انتهایی مانند کامپیوترهای رومیزی، لپ‌تاپ‌ها و دستگاه‌های همراه
- دیواره آتش: وسیله‌ای نرم‌افزاری/سخت‌افزاری که با کنترل ترافیک شبکه و تحلیل بسته داده‌های ورودی و خروجی، دسترسی به یک شبکه خصوصی از طریق اینترنت را کنترل می‌کند.
- زیرساخت کلید عمومی: سیستمی بر اساس رمزگذاری جهت شناسایی و احراز هویت فرستنده و گیرنده
- تحمل خرابی: توانایی یک سیستم برای ادامه دادن به عملیات در هنگام رخ دادن خرابی، هرجند برای مدت محدود یا در یک سطح کاهش یافته
- هایجکینگ : نوعی حمله ضد امنیتی در شبکه است، به طوری که حمله کننده ارتباط را در دست می‌گیرد. درست مانند یک هواپیماربا که کنترل پرواز را به دست می‌گیرد. یک نوع دیگر از hijackingها مربوط به مرورگرها هستند. در این نوع، کاربر به سایتی غیر از آن چه درخواست کرده است هدایت می‌شود.

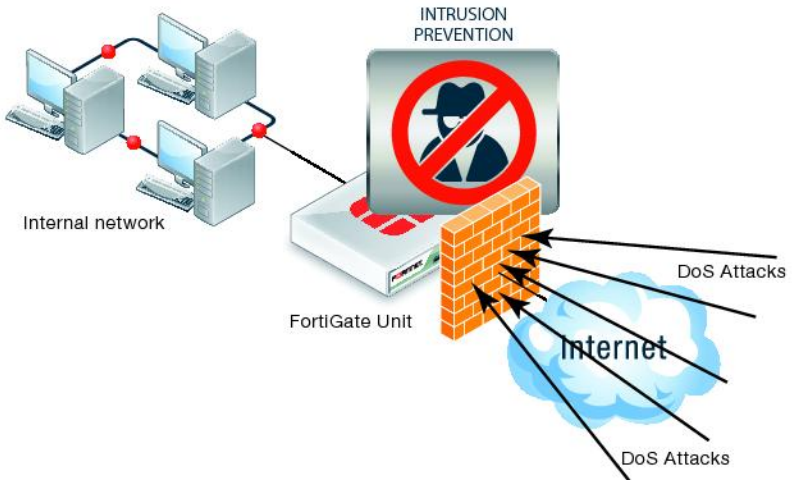
چند اصطلاح امنیت فناوری اطلاعات

- **انکار سرویس (Denial of Service attack-DoS):**
  - حمله‌ای که در آن یک سرویس با درخواستهای زیادی بمباران می‌شود به‌طوری که از کار می‌افتد و توانایی پاسخ دادن ندارد. حمله DOS کامپیوتر هدف را وادار به ریست شدن یا مصرف منابع اش (مانند cpu، Database، پهنای باند و ...) می کند، بنابراین نمی‌تواند به سرویس های مورد نظرش پاسخ بدهد و همچنین سیاست های مورد قبول فراهم کنندگان سرویس های اینترنتی را نقض می کنند.
- این حملات طیف گسترده ای از منابع و سایت های مختلف را هدف قرار داده اند از سرورهای بانک ها تا سایت های خبری و ... این حملات باعث ایجاد یک چالش بزرگ برای مدیران و کاربران این سیستم ها شده است.
- تفاوت بین DOSو DDOS:
  - در حملات DOS هکر از یک سیستم به صورت مستقیم برنامه خود را اجرا و درخواست ها را ارسال میکند ولی در حملات DDOS هکر از چندین سیستم مختلف و یا کامپیوترهای موجود در شبکه برای اجرای برنامه خود استفاده میکند.
- یکی از نشانه های حملات DDOSافت زیاد سرعت لود شدن سایت و سرور میزبان میباشد.



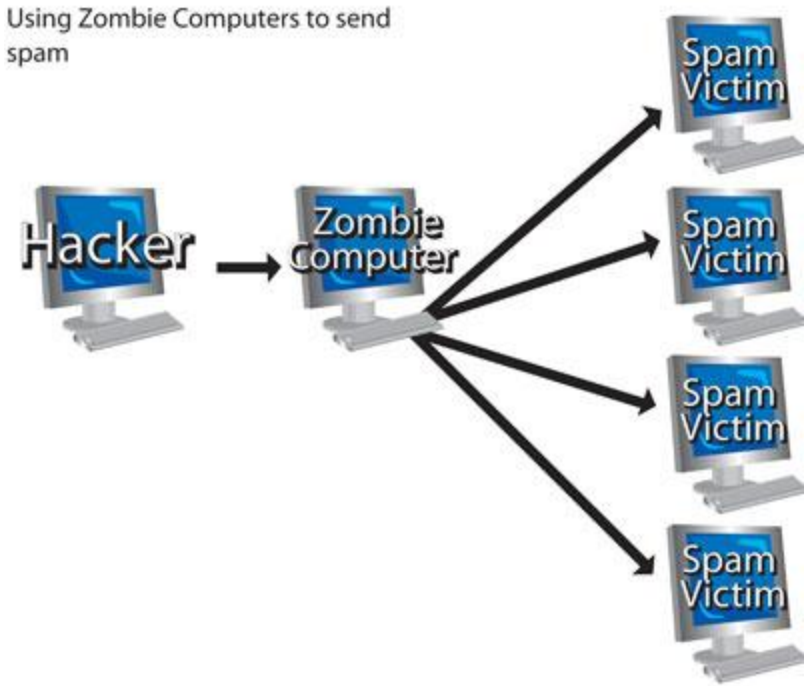
چند اصطلاح امنیت فناوری اطلاعات

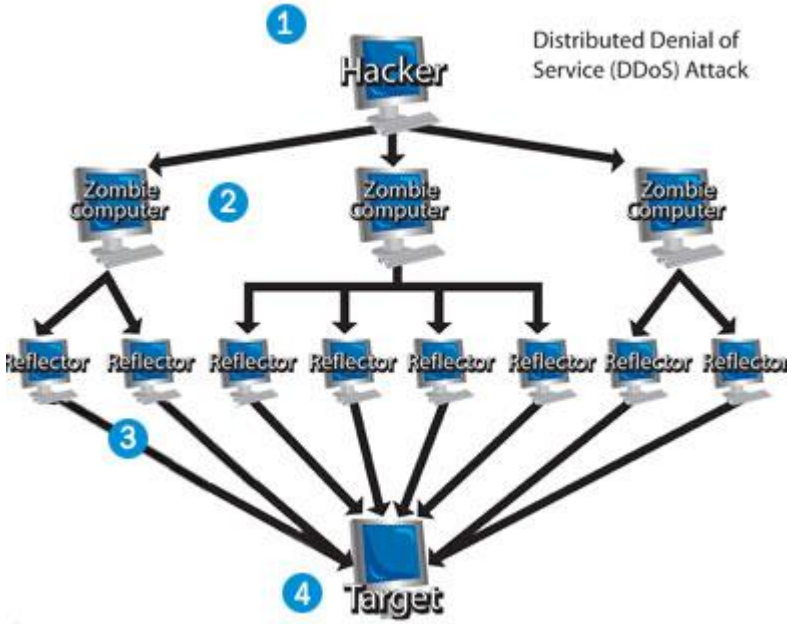
- روش جلوگیری از حملات DDOS
  - برای جلوگیری از چنین حملاتی ابتدا لازم است از سیستم عامل های آپدیت شده و به روز استفاده شود.
  - استفاده از برنامه فایروال قوی در سیستم ها و سرورها می‌تواند برای جلوگیری از چنین حملاتی مفید باشد. با استفاده از فایروال آی پی هایی که تقاضای زیادی به سرور ارسال کرده اند بلاک میشوند.
  - نصب ابزارهای امنیتی و بروزرسانی آنها باعث کاهش آسیب پذیری سرور می‌شوند.
  - چنانچه مدیر سرور از مصرف معمول منابع سرور آگاه باشد سریعا میتواند پی به وجود چنین حملاتی ببرد و آنها را برطرف نماید.
  - چنانچه کاربران مشکوک به انجام چنین حملاتی یا حملات مشابه شدند بهترین کار این است که این مورد را به مدیر سرور خود اطلاع دهند..!



چند اصطلاح امنیت فناوری اطلاعات

- **زامبی (Zombie):**
  - یک کامپیوتر آلوده شده که از راه دور و از طریق اینترنت بوسیله یک کاربر غیرمجاز (مثل فرستنده هرزنامه، هکر، ویروس رایانه‌ای یا کلاهبردار) کنترل می شود. اکثر مالکان رایانه‌های زامبی، از به کار گرفته شدن سامانه‌شان از این طریق بی‌خبر هستند. به این دلیل این کامپیوترها به استعاره با زامبی‌ها (مرده متحرک) مقایسه می‌شوند. معمول‌ترین کاربردهای زامبی‌ها عبارتند از ارسال هرزنامه و شرکت در حملات هماهنگ و در مقیاس بالا از نوع از کار انداختن سرویس (DoS)





چند اصطلاح امنیت فناوری اطلاعات

- **نرم افزار جاسوسی (Spyware):**
  - نرم افزاری که مستقیماً دارای اثر تخریبی نیست ولی برای سرقت اطلاعات مربوط به یک کاربر یا تحت نظر قرار دادن فعالیت آنلاین او را استفاده می‌شود. در نهایت این اطلاعات برای مقاصد خاص فرستاده می‌شود تا از آنها جهت اهداف تجاری، تبلیغی، نظامی، نظارتی و غیره استفاده گردد.
- **نرم‌افزار جاسوسی خانگی (Domestic Spyware)**
  - نرم‌افزاری است که معمولا توسط صاحبان کامپیوترها بمنظور آگاهی یافتن از تاثیرات اینترنت برروی شبکه های کامپیوتری خودشان، خریداری و نصب می گردد. مثلا مدیران برای آگاهی از فعالیتهای آنلاین کارمندان یا والدین برای اطلاع از فعالیتهای فرزندان
  - یک شخص ثالث نیز می تواند نرم‌افزار جاسوسی را بدون آگاهی صاحب کامپیوتر نصب کند. مجریان قانون از نرم افزارهای جاسوسی برای آگاهی یافتن از فعالیت مجرمانی استفاده میکنند که این مجرمان خود از همین نرم افزارهای جاسوسی برای حصول اطلاعات از کامپیوترهای شخصی به قصد دزدی دارایی‌ها استفاده کرده‌اند.
- **نرم افزار جاسوسی تجاری (Commercial Spyware)**
  - این نرم‌افزار که بعنوان adware نیز شناخته می‌شود، نرم‌افزاری است که شرکتها برای تعقیب فعالیتهای وبگردی کاربران اینترنت استفاده می کنند. این شرکتها اغلب اطلاعات حاصل را به بازاریابان می فروشند و آنها کاربران را با تبلیغات خاص مورد هدف قرار می‌دهند - منظور تبلیغاتی است که با علائق کاربر مطابقت دارد و به احتمال زیاد برای وی جذاب است.

چند اصطلاح امنیت فناوری اطلاعات

- علائم زیر می تواند نشان‌دهنده نصب Spyware بر روی یک کامپیوتر باشد :
  - نمایش مستمر پنجره های pop-up آگهی
  - هدایت ناخواسته کاربران به وب سایت هائی که هرگز نام آنان در مرورگر تایپ نشده است .
  - نصب Toolbarsجدید و ناخواسته در مرورگر وب
  - تغییر ناگهانی و غیرمنتظره صفحه اصلی مرورگر یا توقف ناگهانی و غیرمنتظره مرورگر وب
  - تغییر موتور جستجوی مرتبط با مرورگر پس از کلیک بر روی دکمه Searchهمراه مرورگر
  - نمایش تصادفی پیام های خطاء
  - کاهش ملموس سرعت کامپیوتر در زمان فعال نمودن برنامه ها و یا انجام عملیاتی خاص (ذخیره فایل ها و ...)
  - فعال شدن مرورگر و بدنبال آن وب سایت های آگهی بدون انجام عملیاتی خاص توسط کاربر
  - عدم کارکرد صحیح لینک های همراه یک برنامه
  - عدم عملکرد صحیح برخی از عناصر سیستم عامل و یا سایر برنامه ها
  - خاموش شدن دیوار آتش و ضدویروس

چند اصطلاح امنیت فناوری اطلاعات

- **نحوه پیشگیری از نصب Spyware**
  - **عدم کلیک بر روی لینک های موجود در پنجره های pop-up** . با توجه به این که پنجره های pop-upاغلب محصول و یا نوع خاصی از Spywareمی باشند ، کلیک بر روی آنان می تواند باعث نصب یک نرم افزار Spywareگردد . برای بستن این نوع پنجره ها از آیکون X در titlebar استفاده گردد
  - **پاسخ منفی به سوالات ناخواسته**
  - د**قت لازم در خصوص دریافت نرم افزارهای رایگان از اینترنت** : سایت های زیادی اقدام به ارائه Toolbarهای سفارشی و یا ویژگی های خاص دیگری می نمایند . تا زمانی که نسبت به ایمن بودن این نوع سایت ها اطمینان حاصل نشده است ، نمی بایست فایل و یا برنامه ای را از طریق آنان Downloadنمود .
  - **عدم کلیک بر روی لینک های موجود در Emailکه ادعای ارائه یک نرم افزار Anti-Spywareرا دارند** . نظیر ویروس های کامپیوتری ، لینک های موجود در نامه های الکترونیکی ممکن است اهداف سودمندی را دنبال ننموده و نصب Spywareبر روی سیستم شما را بدنبال داشته باشند .
  - **اعمال محدودیت در رابطه با پنجره های Pop-upو کوکی ازطریق تنظیمات برنامه مرورگر** : پنجره های-pop upتوسط نوع خاصی از اسکریپت ها و یا محتویات فعال (اپلت های جاوا ، کنترل های اکتیوایکس) ایجاد می گردند . با تنظیم مناسب پارامترهای برنامه مرورگر، می توان محدودیت لازم دراجرای اسکریپت ها ، اپلت های جاوا ، کنترل های اکتیو ایکس و تعداد پنجره های pop-upرا اعمال نمود . عملکرد برخی از کوکی ها مشابه Spywareمی باشند ، چراکه از طریق آنان مشخص خواهد شد که شما چه وب سایت هائی را مشاهده نموده اید . با تنظیم پارامترهای برنامه مرورگر می توان محدودیت لازم در خصوص ایجاد کوکی ها را اعمال نمود

چند اصطلاح امنیت فناوری اطلاعات

- بات نت: شبکه ای از کامپیوترهای ربوده شده که از راه دور کنترل می‌شوند و معمولا برای ارسال هرزنامه یا نرم‌افزارهای جاسوسی به‌کار می‌روند. به آنها ربات‌های نرم‌افزاری هم می‌گویند.
- بات‌نت‌ها کامپیوترهای آلوده و دیگر شبکه ها را در معرض این تهدیدات قرار می‌دهند:
  - نرم افزار جاسوسی: می‌توان به زامبی‌ها فرمان مشاهده و سرقت داده‌های شخصی و مالی داد.
  - ابزار تبلیغاتی مزاحم: می‌توان به زامبی‌ها دستور ارسال آگهی تبلیغاتی و یا مشاهده وب سایت‌های خاص را داد
  - هرزنامه: بیشتر ایمیل‌های ناخواسته از طریق زامبی‌ها ارسال می‌شود.
  - فیشینگ: زامبی‌ها می‌توانند سرورهای ضعیفی را که میزبان وب‌سایتهای فیشینگ هستند، شناسایی کنند و کاربران را برای وارد کردن داده‌های محرمانه‌شان فریب دهند.
  - حملات DoS
- بات‌نت‌ها خطرناک هستند زیرا می‌توانند دیگر کامپیوترها را جستجو نموده در آنها رخنه کنند و از آنها برای اعمال مجرمانه استفاده نمایند.

چند اصطلاح امنیت فناوری اطلاعات

چگونه یک بات نت ایجاد می‌شود و برای ارسال هرزنامه به ایمیل استفاده می‌شود؟

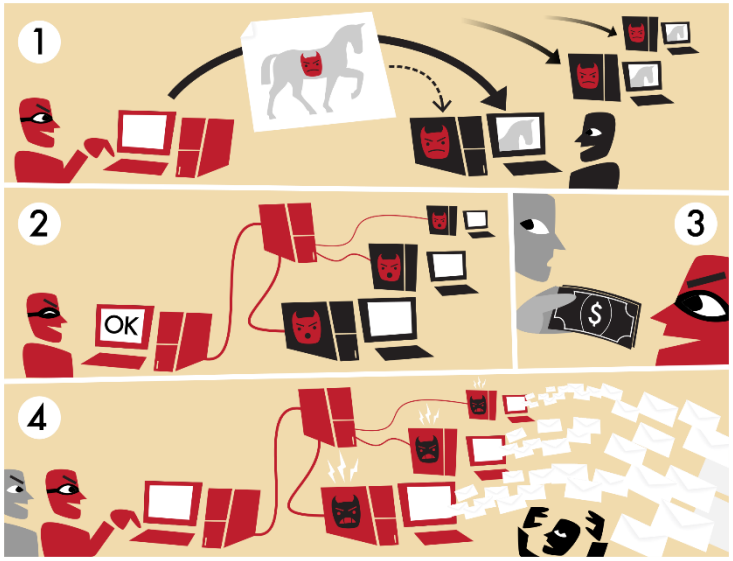
۱- یک اپراتور بات نت، ویروس‌ها یا کرم‌ها را به کامپیوترهای آلوده کاربران عادی می‌فرستد که دنباله آن یک برنامه مخرب است.

۲- بات از کامپیوتر آلوده به سرویس دهنده فرمان و کنترل خاص گزارش می‌دهد.

۳- spammerسرویس‌های بات نت را از اپراتور می‌خرد.

۴- spammerپیام‌های اسپم را برای اپراتور فراهم می‌کند، که ماشین‌های در معرض خطر را از طریق کنترل پنل روی وب سرور آموزش می‌دهد، و باعث می‌شود پیام‌های اسپم به آن‌ها فرستاده شود.

- بات نت‌ها برای اهداف مختلف مورد استفاده قرار می‌گیرند، شامل حملات حمله انکار سرویس، سوء استفاده برای اسپم، حیله کلیک کردن، و سرقت شماره‌های سریال کاربردها، شناسه‌های ورود به سیستم و اطلاعات مالی از قبیل شماره‌های کارت‌های اعتباری.



دفاع در مقابل بدافزارها و بات‌نت‌ها

- نرم افزارهای ضد ویروس
  - لازم است اما کافی نیست!
- سیستم‌ها تشخیص نفوذ (IDS)
  - این سیستم‌ها در جستجوی ترافیک نامعمول و مشکوک شبکه هستند و می‌توانند شروع یک حمله DoS را بوسیله الگوی ترافیکی آن شناسایی کرده و به مدیر هشدار دهند تا اقدامات دفاعی مانند تعویض آدرس IP و منحرف کردن سرورهای حیاتی از مسیر حمله را انجام دهد.
- سیستم‌های جلوگیری از نفوذ
  - با بلوکه کردن آدرس IP های خاص هنگام تشخیص یک حالت نامتعارف، سعی در جلوگیری از نفوذ به شبکه را دارند.

انواع تهدید در کسب و کار

- تهدیدات داخلی:
  - کارمندان با روش‌های مختلف می‌توانند سازوکارهای امنیتی سازمان را دور بزنند. زیرا اغلب محافظت‌ها برای جلوگیری از نفوذ خارجی تدارک شده است! مانند:
    - در ۲۰۱۰ یک مقام عالی رتبه سابق سازمان امنیت ملی امریکا متهم شد که از یک حساب ایمیل سری غیردولتی برای انتقال اطلاعات طبقه‌بندی شده استفاده کرده در حالی که مجاز به دسترسی به آنها نبوده است.
    - در ۲۰۰۶ دزدین لپ تاپ یک کارمند اداره امور سربازان بازنشسته برای مالیات دهندگان ۱۰۰ میلیون دلار هزینه داشت.
    - در ۲۰۰۷ اداره مالیات انگلستان فاش کرد که دیسک رمزگذاری نشده ای حاوی اطلاعات شخصی و بانکی ۲۵ میلیون نفر را گم کرده است. شرکت تحلیل‌گر گارتنر، هزینه بستن حساب‌های فاش شده و ایجاد حساب جدید برای بانک‌های بریتانیایی را حدود ۵۰۰ میلیون دلار تخمین زد.

انواع تهدید در کسب و کار

- مخاطرات مرتبط با رایانش ابری و شبکه‌های اجتماعی
  - رشد محبوبیت دستگاه‌های هوشمند، نت بوک‌ها، شبکه‌های اجتماعی مانند فیس بوک، یوتیوب، توییتر، لینکدین و غیره آسیب‌پذیری و در خطر افتادن اطلاعات حیاتی، شخصی و خصوصی افراد را افزایش می‌دهد.
  - متاسفانه هرچقدر امکانات متنوع و جدیدتری در شبکه‌های اجتماعی ارائه می‌شود ریسک آسیب‌پذیری نیز افزایش می‌یابد، زیرا زمان بهره‌برداری یعنی زمانی که یک آسیب‌پذیری کشف می‌شود تا زمانی که مورد سوء استفاده قرار می‌گیرد خیلی کوتاه شده و حملات خیلی سریع آغاز می‌شوند.
  - فیلترینگ وب، آموزش کاربران، خط مشی‌های سخت‌گیرانه و استفاده از خدمات رایانش ابری، می‌توانند ابزاری برای مقابله با این تهدیدات باشند.

انواع تهدید در کسب و کار

- **فیشینگ و تهدیدات تحت وب**
  - تلاشی فریبکارانه است که بزهکاران برای سرقت اطلاعات محرمانه یک شخص انجام می‌دهند و این کار را از طریق وانمود کردن به این که آنها یک سازمان مشروع مانند یک بانک، شرکت کارت اعتباری و غیره هستند، انجام می‌دهند.
  - انواع تکنیک هایی که در حقه فیشینگ مورد استفاده قرار می گیرد:
    - **دستکاری و تقلب در لینکها و آدرس ها** : یکی از شیوه های متداول و رایج در فیشینگ ارسال لینک ها و آدرس های متعلق به سازمانهای غیر واقعی و جعلی از طریق ایمیل می باشد. آدرس هایی که تنها تفاوت آنها با آدرس اصلی یک یا دو حرف است یا از دامین های فرعی گمراه کننده برای ایجاد آنها استفاده گردیده است.
    - **دور زدن فیلتر** : فیشرها با استفاده کردن از عکس به جای متن، کار فیلترهای ضد فیشینگ را که برای شناسایی متن هایی که عموماً در ایمیل های حاوی آدرس های جعلی یافت می شوند، را سخت می کنند.
    - **وب سایت جعلی**: تنها با ورودو بازدید یک قربانی به سایت جعلی عمل کلاهبرداری صورت نمی پذیرد . در برخی از روش های فیشینگ از دستورات جاوا اسکریپت استفاده می شود تا نوار آدرس را اصلاح کند و تغییر دهد. این کار با قرار دادن تصویر یک آدرس اینترنتی قانونی و موجه در نوار آدرس یا بستن نوار آدرس اصلی و باز کردن یک نوار آدرس جدید که حاوی آدرس اینترنتی قانونی و موجه است، انجام می شود. یک فیشر(مهاجم) حتی می تواند از نقایص موجود در برنامه جاوا اسکریپت یک سایت معتبر و قانونی علیه قربانیان خوداستفاده نمایند.

این نوع حمله ها (که به کراس سایت اسکریپتینگ معروف هستند) به طور خاص سخت و پیچیده هستند،

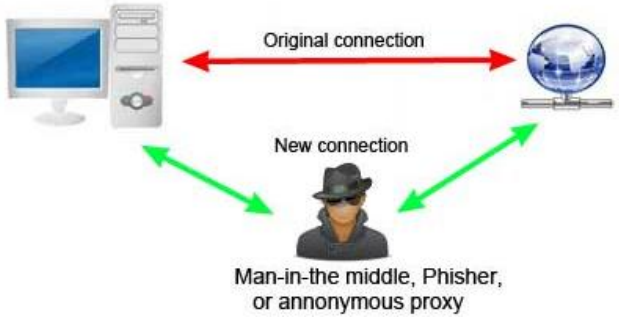
چون آنها قربانی را به صفحه اینترنتی ثبت نام خدمات بانکی خود ارجاع می دهند. صفحه ای که در آن همه چیز از آدرس سایت گرفته تا گواهی امنیتی، همه درست و صحیح به نظر می رسند. در حقیقت لینک دادن به صفحه اصلی حقه ای برای به ثمر رساندن سرقت و انجام دادن حمله است. با انجام این کار کشف این حمله

برای افرادی که دانش لازم را ندارند، کار بسیار سختی است. در سال ۲۰۰۶ چنین حمله ای علیه

سایت Pay Palانجام شد.

انواع تهدید در کسب و کار

- یک برنامه فیشینگ در سطح جهانی با عنوان Man-in-the-middle، که در سال ۲۰۰۷ کشف شد، از یک رابط ساده استفاده می کرد که به فیشر (مهاجم) اجازه می داد بدون هیچ مشکلی سایت هایی خاصی را مجدداً ایجاد کند و جزئیات اطلاعات ورود یا لاگین افراد (نام کاربری و رمز عبور) وارد شده در وب سایت جعلی را برای ورود به سایت های اصلی ثبت و ضبط کند.



- فیشینگ از طریق تلفن
  - تمامی حملات فیشینگ نیاز به استفاده از یک وب سایت جعلی و ساختگی ندارند. این نوع حملات شامل پیام هایی هم می شوند که ادعا می کند از طرف بانک هستند و از مشتری ها (استفاده کنندگان خدمات بانکی) می خواهند با توجه به مشکلی که برای حساب های آنها به وجود آمده است، با یک شماره تماس بگیرند. به محض این که مشتری با این شماره تلفن (که متعلق به مهاجم است و یک سرویس تلفن اینترنتی است) تماس بگیرد، دستوراتی به مشتری داده می شود تا شماره حساب و رمز خود را وارد کند. فیشرهایی که از سرویس تلفن اینترنتی استفاده می کنند، گاهی اوقات از داده های جعلی برای آی دی کالر استفاده می‌نمایند تا برای مشتریان این گونه به نظر برسد که این تماس از طرف یک سازمان مطمئن و معتبر انجام می شود.
- سایر روش ها
  - نوع دیگری از حمله که موفقیت آمیز بودنش ثابت شده است، ارجاع دادن قربانی به وب سایت اصلی بانک است. سپس یک پنجره پاپ آپ در بالای صفحه سایت به نمایش در می آید و به شکلی که به نظر برسد این صفحه و این سایت متعلق به بانک است، اطلاعات حساس قربانی را درخواست می کنند.
  - یکی از جدیدترین روش های فیشینگ تب نبینگ است. این برنامه از صفحاتی که کاربر باز کرده استفاده می کند و به طور آهسته کاربر را به سایت ساختگی ارجاع میدهد.
  - دوقلوهای شر یا Evil twinsروشی است که شناسایی و کشف آن کار بسیار سختی است. یک فیشر یک شبکه بی سیم (وایرلس) ساختگی ایجاد می کند. این شبکه همانند شبکه های معتبر عمومی و قانونی می تواند در مکان هایی مانند فرودگاه ها، هتل ها و کافی شاپ ها وجود داشته باشد. وقتی که یک نفر وارد شبکه جعلی می شود، کلاهبرداران سعی می کنند رمزهای عبور و یا سایر اطلاعات مرتبط با کارت اعتباری او را ثبت و ضبط کنند.

انواع تهدید در کسب و کار

- **ویروس**:
  - یک ویروس کامپیوتری خود را به یک برنامه یا فایل می‌چسباند، سپس می‌تواند از کامپیوتری به کامپیوتر دیگر برود و مانند یک بیماری عفونی مسری پخش شود. بعضی از این ویروس‌ها فقط خرابی جزیی به همراه دارند، در صورتی که انواع مختلفی از آنها می‌توانند اثرات مخرب شدیدی روی سخت‌افزار، نرم‌افزار یا فایل‌های اصلی بگذارند.
- **کرم** (worm):
  - کرم‌ها بعنوان زیرمجموعه ویروس‌ها درنظرگرفته می‌شوند. کرم‌ها ازکامپیوتری به کامپیوتر دیگر می‌روند اما نه به طریقی که ویروس‌ها منتقل می‌شوند. کرم‌ها با توانایی خاصی بدون نیاز به کمک و عملکرد انسان گسترش پیدا کنند. بزرگترین خطر همراه یک کرم توانایی او در تکرار شدن خود روی سیستم است. برای مثال یک کرم می‌تواند کپی خود را به تمام آدرس‌های موجود در کتاب آدرس الکترونیکی شما بفرستد. نتیجه نهایی در بیشتر موارد این است که حافظه زیادی از کامپیوتر را از بین می برد. در نتیجه سرورهای شبکه، سرورهای وب و کامپیوترهای شخصی از کار باز می‌مانند و متوقف می شوند. کرم بلاستر، نوعی کرم است که به گونه‌ای طراحی شده تا اجازه دهد کاربران متفرقه کنترل سیستم شما را در دست گیرند.
- **تروجان** (اسب تروا):
  - اسب تروا در نگاه اول یک نرم افزار مفید به نظر می‌آید، اما یکباره به تخریب برنامه‌های نصب شده می‌پردازد. آنها به صورت نرم‌افزار یا فایل‌های قانونی و سالم دریافت می‌شوند. هنگامی که یک تروا در کامپیوتری فعال می‌شود، نتایج گوناگونی به همراه دارد. بعضی تروا‌ها اثر تخریبی نا چیزی می‌گذارند (مانند تغییر زمینه یا همان دسک تاپ یا اضافه کردن آیکون‌ها). اما بعضی می‌توانند اسب‌های اساسی با حذف فایل و تخریب اطلاعات در سیستم ایجاد کنند. همچنین می‌توانند باعث شوند کاربران مزاحم دیگر به سیستم شما و اطلاعات محرمانه و شخصی شما دست پیدا کنند. متفاوت از کرم و ویروس، تروا توسط عملکرد فایل یا تکرار تولید نمی‌شود.

انواع تهدید در کسب و کار

- دستکاری موتور جستجو
  - بزهکاران سایبری با بهره برداری از الگوریتم‌های موتورهای جستجو، سعی می‌کنند وب‌سایت‌های هک شده را در رتبه بالاتری در نتایج جستجو نشان دهند.
- حملات چند پیوندی
  - حملاتی که بهم پیوند خورده و پیچیده‌تر شده‌اند. مثلا لینک‌های دستکاری شده موتورهای جستجو به سمت وبلاگی هک شده هدایت می‌کند که متصل به یک بدافزار است و بدون اجازه کاربر بدافزار دانلود شود.

انواع تهدید در کسب و کار

- حملات هدفمند در سازمانها
  - تهدید ماندگار پیشرفته (APT): بیشتر از طریق فیشینگ انجام می‌شود. با استفاده از مهندسی اجتماعی اطلاعات درباره شرکت و کارمندانش جمع آوری می‌شود. سپس از این اطلاعات برای ایجاد ایمیل‌های فیشینگ هدفدار استفاده می‌شود. یک حمله موفقیت آمیز می‌تواند باعث دسترسی مهاجم به شبکه سازمان شود.
  - حملات ATP برای جاسوسی درازمدت طراحی شده اند. هنگامی که این حملات در شبکه راه اندازی می شوند، کپی اسنادی مانند فایل‌های آفیس و PDF را به‌طور مخفیانه منتقل می‌کنند. پس از جمع آوری، رمزنگاری نموده و به سرورهایی که عموما در چین مستقرند، ارسال می‌کنند.

انواع تهدید در کسب و کار

- از دیدگاهی دیگر
  - تهدیدات غیرعمدی
    - خطاهای انسانی: خطا در طراحی سخت افزار یا سیستم های اطلاعاتی، در برنامه نویسی، عدم تغییر رمز پیش فرض، ناتوانی در مدیریت ترمیم‌ها و حفره های امنیتی. کاربران آموزش ندیده و ناآگاه
    - خطرات محیطی: اتفاقات طبیعت مانند فوران آتش‌فشان، سیل، زلزله، طوفان، آتش‌سوزی و قطع برق، تهویه نامطبوع، انفجار، تشعشعات رادیواکتیو و غیره. علاوه بر خسارتهای اولیه می توانند بر منابع کامپیوتری نیز تأثیر نامطلوب بگذارند و هزینه زیادی برای بازسازی به جا گذارند.
    - خرابی سیستم‌های کامپیوتری: در نتیجه تولید ضعیف، موارد اولیه نامرغوب و معیوب، نگهداری ضعیف شبکه‌ها، تست‌های ناکارآمد و فقدان تجربه
  - تهدیدات عمدی
    - سرقت داده‌ها، استفاده نامناسب از داده‌ها، دستکاری عمدی در مدیریت داده‌ها یا برنامه نویسی، اعتصاب کارگران، شورش و خرابکاری، ویروس‌ها و حملات مشابه، کلاهبرداری اینترنی

مقررات دولتی

- داده‌ها باید در مقابل طرح‌های حمله حال و آینده محافظت شوند. و روش‌های دفاعی فناوری اطلاعات باید مقررات سخت دولتی و بین المللی را رعایت کنند. قانون ساربنس-اوکلی (SOX)، قانون گرام-لیچ-بلایلی (GLB)، قانون فدرال مدیریت امنیت اطلاعات (FISMA)، قانون پاتریوت امریکا، قانون حفاظت از اطلاعات شخصی ژاپن و غیره قوانینی هستند که حفاظت از داده‌های شخصی را الزامی می‌دانند.
  - به عنوان مثال قانون SOX قانونی ضد کلاهبرداری است. در بخشی از آن مدیر عامل و مدیر مالی ملزم به تایید گزارش‌های مالی هستند و در صورت تخلف، شامل مجازات کیفری مانند زندان طولانی مدت می‌شوند.
- همچنین گروه‌های صنعتی نیز استانداردهای خود را برای حفاظت از مشتریان اعمال می‌کنند.

مدل دفاع در عمق امنیت فناوری اطلاعات

- این روش، رویکردی چند لایه در امنیت اطلاعات است. اصل اساسی در این رویکرد این است که وقتی یک لایه ناتوان می‌شود، لایه دیگر محافظت را به‌عهده می‌گیرد. مثلا اگر امنیت در یک شبکه بی‌سیم از بین رفت، آنگاه داشتن داده‌های رمزنگاری شده همچنان باعث می‌شود داده‌ها از دسترس سارقان در امان باشد.

گام ۱
- تعهد و پشتیبانی مدیریت ارشد

گام ۲
- آموزش امنیت اطلاعات و خط مشی های قابل قبول

گام ۳
- رویه های امنیت فناوری اطلاعات و اعمال آنها

گام ۴
- سخت افزار و نرم افزار (نگهداری به روز)

مدل دفاع در عمق امنیت فناوری اطلاعات

- گام ۱ اهمیت نفوذ مدیران ارشد برای اجرا و حفظ امنیت، استانداردهای اخلاقی و حریم خصوصی و کنترل داخلی را مورد توجه دارد.
- گام ۲ (آموزش امنیت اطلاعات و خط مشی های قابل قبول) برای ایجاد اطمینان از آگاهی و درک سیاستهای سازمان است. مهم‌ترین سیاست «خط مشی استفاده قابل قبول (AUP)» است که کاربران را از مسئولت‌هایشان آگاه می‌کند برای
  - ۱) جلوگیری از سوء استفاده از اطلاعات و منابع کامپیوتری
  - ۲) کاهش قرارگیری در معرض جریمه‌ها، تحریم‌ها و مسئولیت‌های حقوقی
- در گام ۳ (رویه های امنیت فناوری اطلاعات و اعمال آنها) عملکرد کاربران در مورد اجرای خط مشی استفاده قابل قبول پایش می شود
- در گام ۴ نرم افزارها و سخت افزارهای لازم برای اعمال و پشتیبانی از AUP و اقدامات امنیتی فراهم می شود.

کلاهبرداری، بزهکاری و مقابله با آن

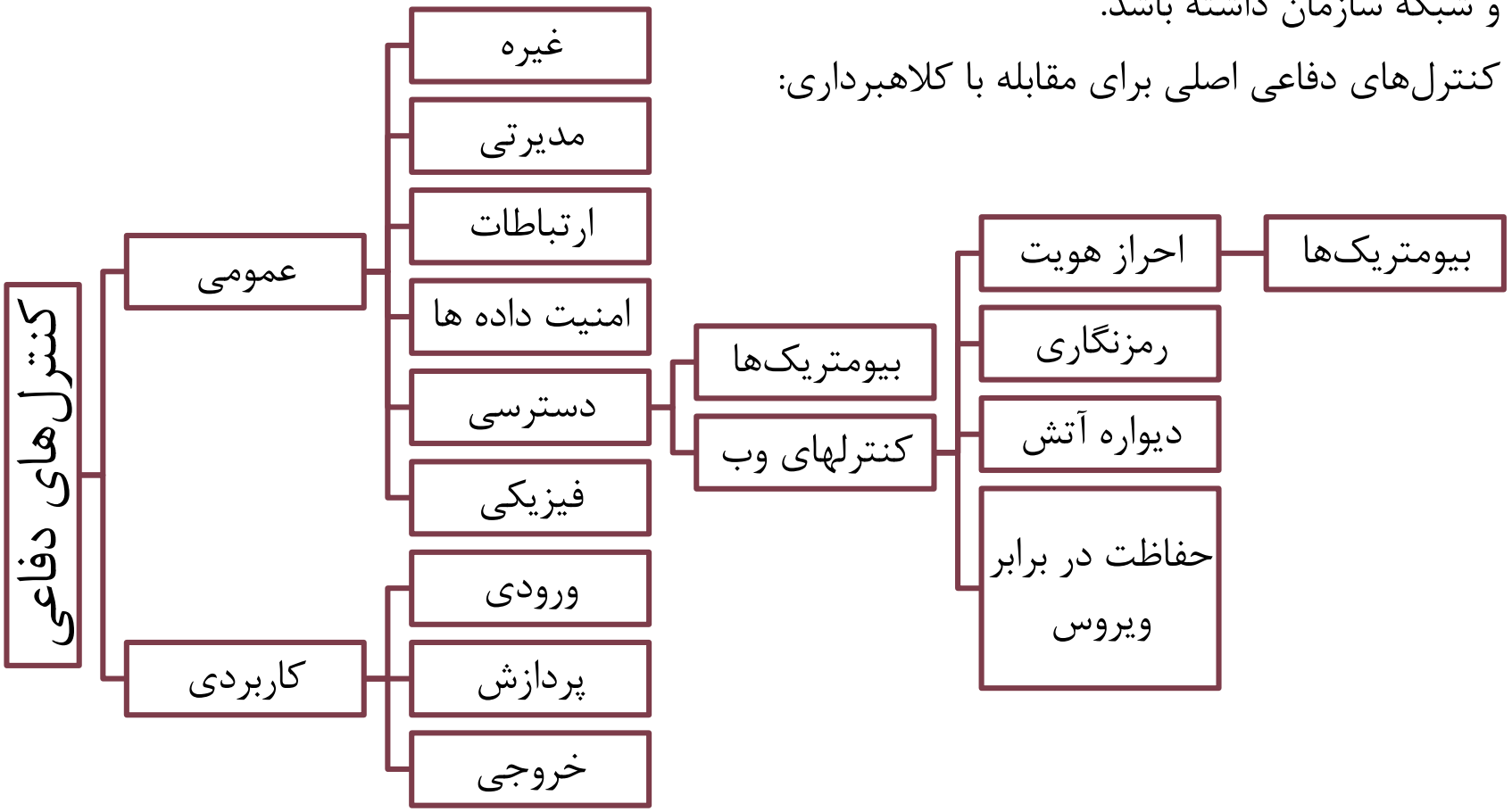
- انواع بزهکاری:
  - خشونت آمیز
  - غیر خشونت آمیز : مانند کلاهبرداری
    - کلاهبردار با سوء استفاده از قدرت موقعیتش یا با بهره بردن از اعتماد، نادانی یا تنبلی دیگران، جرمش را انجام می‌دهد.

جدول ۳-۵ انواع و خصوصیات کلاهبرداری سازمانی

نوع کلاهبرداری	آیا این کلاهبرداری بر صورت وضعیت مالی تأثیر می‌گذارد؟	خصوصیات عمومی
فساد مدیریت اداری	خیر	بدون ثبت شدن در گزارش‌های مالی رخ می‌دهد. ضرر متوسط به‌دلیل فساد: بیش از شش برابر بیشتر از ضرر متوسط به‌خاطر اختلاس (۵۳۰ هزار دلار در مقابل ۸۰ هزار دلار)
تضاد منافع	خیر	نقض محرمانگی، همچون فاش کردن پیشنهاد رقبا؛ اغلب با رشوه اتفاق می‌افتد.
رشوه	خیر	استفاده از قدرت یا پول برای اثرگذاری بر دیگران
اختلاس	خیر	سرقت کارمندان- دسترسی کارمندان به دارایی‌های شرکت فرصتی برای اختلاس مهیا می‌کند.
تقلب در گزارش مالی مدیریت ارشد	بلی	شامل نقض گسترده اعتماد و بهره‌گیری از موقعیت است.
تقلب در چرخه حسابداری	بلی	این کلاهبرداری را «مدیریت درآمد» یا مهندسی درآمد می‌نامند که تخلف در GAAP (اصول عمومی مورد قبول در حسابداری)[۳] و دیگر رویه‌های حسابداری است. aicpa.org را ببینید.

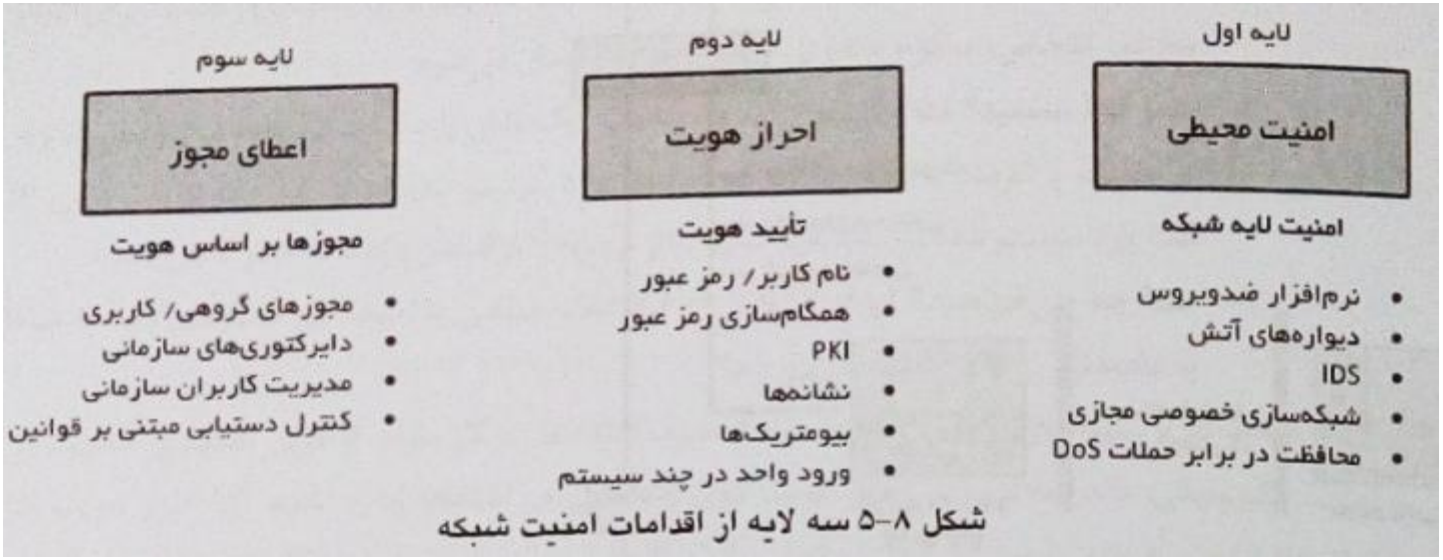
کلاهبرداری، بزهکاری و مقابله با آن

- فناوری اطلاعات می‌تواند نقش مهمی در مقابله با کلاهبرداری و حفظ امنیت داده‌ها، نرم/سخت افزار و شبکه سازمان داشته باشد.
- کنترل‌های دفاعی اصلی برای مقابله با کلاهبرداری:



امنیت شبکه

- اقدامات امنیت شبکه مشتمل بر سه نوع از اقدامات دفاعی است:
  - لایه اول: امنیت محیطی، کنترل دسترسی به شبکه
  - لایه دوم: احراز هویت، بررسی هویت شخصی که درخواست دسترسی به شبکه را دارد
  - لایه سوم: حق دسترسی، کنترل کارهایی که کاربر احراز هویت شده می‌تواند انجام دهد



شکل ۸-۵ سه لایه از اقدامات امنیت شبکه

تحلیل هزینه – فایده

- ایجاد آمادگی سازمان در برابر هر تهدید احتمالی، معمولا اقتصادی نیست. بنابراین برنامه امنیت فناوری اطلاعات باید فرآیندی را مهیا کند که تهدیدها ارزیابی شود و تهدیدات مهم شناسایی گردند.
- تحلیل مدیریت ریسک

$$\text{زیان مورد انتظار} = P_1 * P_2 * L$$

P_1 : احتمال حمله (به‌صورت تخمینی)

P_2: احتمال موفق بودن حمله (به‌صورت تخمینی)

L: میزان زیان وارده در صورت موفق بودن حمله

- مثال: اگر P1=0.02، P2=0.10 و L=$1,000,000 باشد، آنگاه زیان مورد انتظار از این حمله برابر است با: P1*P2*L = 0.02*0.1*$1,000,000 = #2,000
- بعضا طول مدتی که سیستم خارج از عملیات است را نیز به این تحلیل اضافه می‌کنند.

تمرین

- مهندسی اجتماعی
- سیستم‌های توصیه‌گر