امنیت سایبری
مفاهیم و تعاریف بنیادی ساحت امنیت

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

باج‌گیری شغلی است!

دانشگاه ماستریخت

- زمستان ۱۳۹۸
- نوعی باج‌افزار به نام کلاپ Clop
- طبق گزارشات بررسی‌ها منبع آن محتملا از لپتاب
- با کلیک روی پیوندی از ایمیل طله Phishing
  - منجر به اجازه دسترسی مجرمان سایبری به دستگاه‌های دانشگاه

ایمیل‌های طله

- در ظاهر مبدأئی معتبر
- در واقع از طرف مجرمان سایبری
  - جهت دستیابی به اطلاعات حساس
  - یا دسترسی به دستگاه

باج‌گیری شغلی است!

مورد پیچیدهٔ دانشگاه ماستریخت

- ضعف در جای دیگر
- بروز نبودن چند سرور دانشگاه برای مدتی
  - آسیب‌پذیر کردن آنها در مقابل حملات سایبری
  - شغل شریف نصب باج‌افزار روی دستگاه و گروگان‌گیری آن

باج‌افزارها

- از بزرگترین خطرهای نهادها، شرکت‌ها، بنگاه‌ها، آحاد
  - نفوذ مجرمان سایبری به دستگاه‌های فاوا
  - رمز کردن داده‌های مهم
  - جلوگیری از دسترسی به سیستم
  - معمولا درخواست مبلغ هنگفتی در قبال تحویل کلید بازیابی داده

باج‌گیری شغلی است!

- قربانی اول نبودن دانشگاه مذکور در این وادی
- چندین ماه قبل از آن حمله به دانشگاه انتورپ با کلاپ
- حمله به شرکت آلمانی سافتور آگ در پائیز ۹۹ با باج‌افزار مذکور
  - نمایش سودآوری چنین حمله‌ای در صورت موفقیت!
  - درخواست ۲۳ میلیون دلار پس از استخراج اطلاعات کارمندان، اسناد شرکتی، رمز داده
  - نبود اطلاعات تکمیلی بیشتر

- حمله به دانشگاه ماستریخت نمایش قدرت جرائم سایبری
  - اولین نفوذ در پاییز ۹۸، دو ماه پیش از گروگان‌گیری سیستم
  - در طول دو ماه افزایش گسترهٔ تصرف سیستم
  - بروز نبودن سرورها کاتالیزور گسترش مذکور
  - اولین‌روزهای دی ۱۳۹۸
    - غیرفعال کردن نرم‌افزار ضدویروس
    - رمزکردن ۲۶۷ سرور دانشگاه
    - از کار انداختن تمامی سامانه

باج‌گیری شغلی است!

برگزاری سمپوزیوم در این خصوص در اسفند ۹۸

- در یکی از گزارش‌ها
  - چرایی انتخاب دانشگاه ماستریخت
  - پخش پیام فدایت شوم در همه جا و سپس بررسی اصابت شده‌ها
  - حمله به بسیاری از دانشگاه‌ها و دیگر نهادها و بنگاه‌ها
  - [قرعهٔ کار] به نام دانشگاه ماستریخت
  - محتملا نتیجه‌گیری به چرب بودن لقمهٔ مذکور
    - به دلیل تکیه بسیاری دانشجو و هیات علمی بر آن
  - انتظار دریافت مقدار زیادی جهت بازگشت به وضعیت و شرایط معمول
  - داشتن اطلاعات محرمانهٔ بسیار که آسیب‌رسان به افراد و شرکت‌ها
    - داده‌های بیماران

باج‌گیری شغلی است!

تحلیل و بررسی دانشگاه

- عدم‌پرداخت به منجر به خسارات مالی بزرگتر نسبت به پرداخت
- در انتها پرداخت ۳۰ بیت‌کوین که در آن زمان حدود ۱۹۷۰۰۰ پوند بود.
- انتقاد شدید از پرداخت داخل و خارج هلند.
  - به عنوان مثال بودجهٔ دولتی دانشگاه‌های هلند
  - پرداخت پول مالیات‌دهندگان به مجرمان سایبری
  - حل کوتاه‌مدت مسئله
  - تحریم مرغ!

باج‌گیری شغلی است!

سختی تشخیص باج‌افزار

پس از وقوع چندین حمله

- گزارش تحلیل گر وابسته به مک‌کافی
  - دربارهٔ گواهی تائید مورداستفادهٔ کلاپ
  - گواهی تأئید- تایید اعتبار تارنامه
  - سخت شبیه موارد واقعی
  - یک قدم پیش بودن مجرمان

باج‌گیری شغلی است!

گروه سایبری TA505 پشت ماجرا

- فعال از ۸ سال پیش و حرفه‌ای
- ردگیری در سال ۱۳۹۸
- محتملا توسعهٔ کلاپ به دلیل پتانسیل پول‌سازی بالای آن
- با گروگان گرفتن سیستمی
  - درخواست مالی در قالب بیت‌کوین یا دیگر رمزارزهای دیگر
  - نگهداری کلید کشف داده‌ها روی سرور امن با دسترسی صرفا گروگان‌گیران
  - در صورت عدم اجابت، ارسال بخشی از اطلاعات حساس به وب تاریک
    - مثال- شرکت اکسکوفارم
    - عرضهٔ خدمات تحقیقی برای شرکت‌های در بخش داورسازی
    - مثال- افشای اطلاعات افراد استخدامی شرکت آگ

باج‌گیری شغلی است!

- تا۵۰۵ محتملا سازندهٔ درای‌دکس Dridex
  - بدافزاری حمله‌کننده به آحاد و نهادهای بانکی در هفت سال پیش
    - پیاده‌شدن از ایمیل‌های دارای پیوست ورد یا اکسل
    - اجازه به دزدیدن رمزها و دیگر اطلاعات مالی
  - افزایش قدرت بدافزار
- چگونگی پشتیبانی شرکت‌ها از خود
  - سیستم‌های از رده‌خارج آسیب‌پذیر در مقابل حملات بدافزارها
  - آگهی کارکنان از حملات طله، چون بازنکردن ایمیل‌های دارای پیوست و عدم پاسخ به ایمیل‌های شناخته نشده
    - دانشگاه ماستریخت مثالی از آن
  - نگهداری خارج از خط نسخه‌ای از داده‌ها
    - معمولا پیچیده و سخت به دلیل تغییر مداوم
      - اما کم‌هزینه‌تر در بلندمدت
    - اما پاسخی ناکافی در صورتی دستیابی به داده امکان افشای آن روی وب تاریک
  - عدم‌پرداخت به باج‌گیران
    - عدم تحویل کلید در بسیاری از موارد

باج‌گیری شغلی است!

- کلاپ تنها باج‌افزار؟
  - خیر
- سودینوکیبی
  - تراولکس- شرکت تبادل خارجی بریتانیائی
  - اختلال بسیاری از خدماتش
  - غیرممکن شدن سفارش برخط کارت پول تراولکس
  - پرداخت ۲,۳ میلیون دلار جهت آزادسازی سیستم

جنگ سایبری

تکامل جنگ‌افزارها در طول زمان

- از چوب و سنگ به تیر و نیزه به توپخانه و بمب و به سلاح‌های هسته‌ای
- تشخیص‌پذیری سریع جنگ‌افزارهای فیزیکی

امروزه نوع دیگری از جنگ‌افزار

- همه‌گیری و معمول‌شدن سریع
- ارتش مخفی هک‌کنندگان
  - مجهز به سلاح الگوریتم‌ها و کدهای رایانه‌ای

فضای سایبری به مثابهٔ میدان نبرد

- کشورها علیه دیگر کشورها
- کشورها علیه شرکت‌ها

جنگ سایبری

دو نوع هدف جنگ‌سایبری

- اهداف زیرساختی سخت
  - ساز و برگ‌های دفاعی
  - تجهیزات هسته‌ای
  - شبکه‌های مخابراتی و برق
  - نیروگاه‌ها و کارخانه‌های تولید
  - دیگر زیرساخت‌های عمومی
- اهداف نرم
  - بانک‌ها و نظام‌های مالی
  - شرکت‌های خصوصی
  - نظام‌های اطلاعات عمومی
  - نظام نگهداری اطلاعات بیمه و مدیریت سلامت

جنگ سایبری

هدف جنگ سایبری علیه اهداف سخت

- زمین‌گیری زیرساخت‌های فیزیکی و اصلی صنعتی خاص یا کل جامعه

هدف جنگ سایبری علیه اهداف نرم

- برهم‌زدن و ضعیف‌سازی جمعیت‌ها و سازمان‌ها و نهادها
- تنبیه شرکت‌ها
- گرداوری اطلاعات افراد و شرکت‌ها جهت مقاصد بعدی

تفاوت جنگ سایبری از جاسوسی سایبری

- نداشتن قصدی در جهت از کار انداختن خدمات اجتماعی اصلی
- تمرکز بر جمع‌آوری اطلاعات شامل مالکیت فکری
- احسن جاسوسی‌ها – مخفی و بی‌سروصدا و در سکوت

جنگ سایبری

انتخابات ریاست‌جمهوری اما مورخ ۱۸ آبان ۱۳۹۵

- نسل جدیدی از جنگ سایبری علیه اهداف نرم
  - برهم‌زدن و تاثیرگذاری بر فرایند سیاسی کل ملت مذکور
- مبتنی بر گزارش دی ۱۳۹۶
  - همکاری سایبری دولت روسیه و نیروهای ثالث برای طراحی داستان‌ها و تبلیغات غلط و افزایش تنش جهت پشتیبانی از دواطلب خاص «ترامپ»
    - روسیه‌دوست (روسوفیل)
    - تضعیف داوطلب مخالف

جنگ سایبری

اجرای طیفی وسیعی از فعالیت‌های سایبری جهت دست‌یابی به اهداف مذکور

- هک‌کردن ایمیل کمیته ملی دمکرات
  - افشای اطلاعات در ویکی‌لیکس و دس‌لیکس
- استفاده از صدها ترول اینترنتی جهت ایجاد حساب‌های جعلی در فیس‌بوک و تویتر
  - جهت تولید و انتشار داستان‌های دروغ
- استفاده از بستر باز تبلیغاتی فیس‌بوک و تویتر جهت دستیابی به گروه‌های جمعیتی با قصد افزایش تنش اجتماعی

جنگ سایبری

- فیس‌بوک و توییتر رد کردن ادعای استفاده از بسترها
- آذر ۱۳۹۶ در کنگره فیس‌بوک قبول ادعای وجود ۶۰۰ تبلیغات و ۴۷۰ حساب با منشا روسی که خود را امریکایی معرفی کرده بودند
  - پرداخت ۱۰۰۰۰۰ دلار جهت تبلیغاتی که میلیون‌ها عضو امریکایی را هدف گرفته بود
  - جهت پراکندن پیام‌های تفرقه‌افکنانه
- هم‌چنین تویتر مجبور به پذیرش هزاران حساب جعلی مرتبط با روسیه و صدها بات مرتبط استفاده شده جهت نشر اخبار جعلی در زمان رای‌گیری
- هر دو درگیر با مسئله حساب جعلی
  - تویتر ۸۴ میلیون حساب جعلی
  - فیس‌بوک ۱۲۰ میلیون حساب جعلی
  - بسیاری از آنها بات
    - ارسال پیام خودکار در هر چند ثانیه، چند برابر کردن تاثیر پیام‌های جعلی و در چند مورد در فهرست روندهای هر دو شرکت

جنگ سایبری

تلاش روسیه جهت تاثیر بر انتخابات امریکا و تلاش امریکا جهت تاثیر بر فرایند سیاسی روسیه

- چیز جدیدی نیست
- از پیش از جنگ سرد
  - استفاده از انواع روش‌های و ابزارها و سیاست‌ها
  - چون نهادهای امنیتی و دیپلمات‌ها و داستان‌های خبری و تبلیغات تلویزیونی و رادئویی و پرداخت به سیاست‌مداران و مشاوران
  - جهت مراتب تاثیر بر فرایند سیاسی و دستیابی به «منافع ملی» خود
- پس چه جدید است؟

جنگ سایبری

تلاش روسیه جهت تاثیر بر انتخابات امریکا و تلاش امریکا جهت تاثیر بر فرایند سیاسی روسیه

- چیز جدیدی نیست
- از پیش از جنگ سرد
  - استفاده از انواع روش‌های و ابزارها و سیاست‌ها
  - چون نهادهای امنیتی و دیپلمات‌ها و داستان‌های خبری و تبلیغات تلویزیونی و رادئویی و پرداخت به سیاست‌مداران و مشاوران
  - جهت مراتب تاثیر بر فرایند سیاسی و دستیابی به «منافع ملی» خود
- پس چه جدید است؟
  - استفاده از توانائی‌های هک‌کردن و شبکه‌های اجتماعی جهت تاثیر مستقیم بر عقیده‌ها و اعتقادات کل جمعیت

جنگ سایبری

جنگ سایبری علیه فرایندهای تصمیم‌گیری تهدیدی بزرگ

- امکان پیگیری و یافتن آن در سپهر سیاسی و محتملا توقف آن با نهادهای امنیتی و شبکه‌های اجتماعی
- جانی گرفته نمی‌شود

اما در جنگ سایبری سخت

- در توان جهت آسیب‌های اجتماعی و فیزیکی به جمعیتی بزرگ
  - محتمل جهت ضررهای جانی

جنگ سایبری

از مسائل جنگ‌افزارها

- دشمن شما همان را دارد که که شما دارائید
- نابودی حتمی طرفین
  - اضمحلال حتمی طرفین (اضمحلال حتمی دوطرف «احد») MAD
    - سبقت در تک، شکست و نابودی در پاتک
- به طریق اولی در جنگ سایبری

Mutual assured destruction (MAD)

جنگ سایبری

امریکا و چین و روسیه آماده شدن جهت جنگ سایبری هدف نرم و سخت

- با امید اتفاق نیفتادن آن با توسعهٔ سلاح‌های جدید و امتحان فنون دفاعی
- فروردین ۱۳۹۶ ناتو
  - هشتمین بازی‌های سپر مقاوم جنگ سایبری
- خرداد ۱۳۹۶ وزارت دفاع امریکا
  - ششمین بازی‌های محافظان جنگ سایبری
  - صد سازمان و هشتصد فرد از نیروهای نظامی و شرکت‌های خصوصی

جنگ سایبری

نادر بودن حملات علیه اهداف سخت چون زیرساخت‌های فیزیکی

- نیاز به اطلاع دقیق از زیرساخت
- معمولا نیاز به اطلاع داخلی از کنترل‌کننده‌های صنعتی
  - رایانه‌های کنترل دریچه‌ها و شیرآلات و دستگاه‌ها
- شناخته‌شده‌ترین و مستندشده‌ترین حملهٔ زیرساختی

جنگ سایبری

نادر بودن حملات علیه اهداف سخت چون زیرساخت‌های فیزیکی

- نیاز به اطلاع دقیق از زیرساخت
- معمولا نیاز به اطلاع داخلی از کنترل‌کننده‌های صنعتی
  - رایانه‌های کنترل دریچه‌ها و شیرآلات و دستگاه‌ها
- شناخته‌شده‌ترین و مستندشده‌ترین حملهٔ زیرساختی
  - استاکس‌نت
  - بدافزاری در سال ۱۳۸۹ محتملا حاصل همکاری امنیتی‌های اسرائیلی و امریکایی
    - جهت از کارانداختن سانتریفیوژهای هسته‌ای ایران
  - برنامه ویروسی بدافزار
  - کارگزاری شده در ماژول‌های کنترل‌کنندهٔ صنعتی سانتریفیوژهای سوخت هسته‌ای ایران
- اولین حمله سایبری مقیاس‌بزرگ به زیرساخت
- در پاسخ اتهام‌زنی امریکا به ایران بر تدارک و پشتیبانی ایران از حملهٔ به شرکت ارامکو سعودی با ویروس شمعون
  - پاک کنندهٔ ۳۰۰۰۰ رایانه در شرکت

جنگ سایبری

به دنبال معاهداتی شبیه معاهدات تسلیحات هسته‌ای

نمایشگر افزایش تهدیدپذیری حملات حجم بالا و متعاقبا ضررهای بزرگ

انجام حملات گروه‌های سازمان‌یافته

- کشورها علیه منابع اینترنتی دیگر کشورها

سختی پیش‌بینی و پاسخ به حملات

- هم برای دولت‌ها و هم برای فیاوری‌ها

اما

- مراحل و موادی نظری و عملی جهت محافظت تارمانه، ابزار همراه، اطلاعات شخصی از حملات معمول اینترنتی
  - از اهداف درس
  - همچنین مجالی برای تامل دربارۀ چگونگی حفظ منابع در قبال به خطر افتادن اینترنت

رایانه و اینترنت

رایانه

اینترنت

- ابزارهایی معمول در بین آحاد جامعه جهت انجام کارهای روزانه
- انتقال وجوه
- ذخیرهٔ اطلاعات
- آموزش
- اتوماسیون

تقریبا اکثر افراد مرتبط با آن

اشتباه در اطلاعات

- امکان ایجاد خسارت و ضرر و حتی جانی

رایانه و اینترنت

اشتباهات غیرعمد در مقابل عمدی

- سوءاستفادهٔ عمدی
- تغییر اطلاعات کارمندان ناراضی یا خاطیان
- ضرر به رقبا
- احساس تبعیض و بی‌عدالتی و واکنش به آن و در پی انتقام

رایانه و اینترنت

چرا امنیت اطلاعات

- تاریخچه تغییر امنیت
  - گاوصندوق و کمدهای کلیددار و استخدام راهیابی افراد مورد وثوق
  - سیستم اشتراک زمانی
  - ؟
  - شبکه تلفن عمومی
  - امنیت کامپیوتر
  - ابزارهای مقابله با هک‌کنندگان و جهت حفاظت داده
  - سیستم‌های توزیعی
  - استفاده از امکانات ارتباطی
  - امنیت شبکه
  - امنیت اینترنت

عدم وجود مرز مشخص بین امنیت رایانه و امنیت شبکه

تکیه بر موادی جهت بازداری و پیشگیری و تشخیص و اصلاح نقض امنیت

رایانه و اینترنت

برای مقید به قوانین
- اینترنت مأمن فضای بزرگ و راحت و دسترسی به اجناس و افراد و خدمات و کسب‌وکارها در پهنهٔ گیتی

برای مجرمان
- منبع عظیم سواستفاده از بسیاری مصرف‌کنندهٔ اینترنت
  - محصولات و خدمات و پول نقد و اطلاعات

کم خطری دزدی برخط
- امکان دزدی از دور به جای دستبرد به بانک و ناشناس ماندن
- به جای دزدی سی‌دی از مغازه، پیاده‌کردن راحت موسیقی
- پتانسیل گمنام ماندن عامل روحیه جهت سفارش‌های جعلی، دزدی اطلاع با ایمیل‌های فریب‌دهنده، از کار انداختن تارمانه‌ها با حملات ویروسی و خزنده

عدم برنامهٔ اینترنت جهت تجارت و فیاوری
- دارای مشکلات اینترنتی مانند شبکه‌های قدیمی‌تر
- شبکهٔ باز آسیب‌پذیر

رایانه و اینترنت

هزینه ضرر ناشی و همچنین هزینه‌های مشروط به

- امنیت شبکه
- جبران پس از حملهٔ هک،
- آسیب‌های ناشی از بدنامی ناشی از حمله اینترنتی و
- کاهش اعتماد مراجعان و مشتریان
- ازدست دادن اطلاعات مهم و حساس

مطالعه ۲۰۱۷

- میانگین هزینهٔ نقض داده در شرکت‌های ایالات متحده ۷,۳۵میلیون دلار

حوزهٔ مسئله

ناواضح بودن اندازه کل و حجم ضررهای جرائم سایبری
- مشکلات گزارش

ارزانی لوازم حملهٔ وب

کلاهبرداری کارت برخط

بازار اقتصاد زیرزمین
- فروش به جای استفاده

TABLE 5.2 THE CYBER MARKET FOR STOLEN DATA

DATA	PRICE*
Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV)	$5–$8
Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo)	$20–$60
Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card)	$60–$100
Bank account login credentials (depending on value and verification)	0.5%–10% of value
Online payment accounts (PayPal, etc.) (depending on value and verification)	0.5%–10% of value
Driver's license information	$20
Online account login credentials (Facebook, Twitter, eBay, Apple, Dropbox)	$10–$15
Medical information/health credentials	$10–$20
1,000 e-mail addresses	$1–$10
Scan of a passport	$1–$25
Social security number	$1

SOURCES: Based on data from Symantec, 2019; 2018; VPNOverview, 2019; Osborne, 2018.

*Prices vary based on supply and quality (freshness of data, account balances, validity, etc.).

امنیت مناسب

چیستی این گزاره؟

- هر بار مراجعه به فضای بازاری برابر با خطر از دست رفتن حریم خصوصی
  - اطلاعات آنچه که خریدید
- ابتدائی‌ترین خطر خریدار
  - عدم دریافت آنچه برایش پرداخت کردید
- ابتدائی‌ترین خطر فروشنده
  - عدم دریافت مبلغ آنچه فروختید
- دزدان در دست گرفتن تراکنش و خروج بدون پرداخت یا پرداخت از کیسهٔ دیگری

امنیت مناسب

مواجهه با خطرات مشابه موارد سنتی

- دزد دزد است فارغ از بستر
- کلاه‌برداری، شکستن، و ورود
- اختلاس
- تعدی و تجاوز (ورود به ملک غیر)
- خرابکاری

اما مواجهه پیچیده‌تر و شامل فناوری‌های نو و سیاست‌های سازمانی و قوانین

امنیت مناسب

مواد موردنیاز دستیابی به بالاترین سطح امنیت

- تکنولوژی‌های نو
- رویه‌ها و سیاست‌های سازمانی
- استانده‌های صنعتی و قوانین حکومتی

امکان شکستن امنیت در صورت داشتن منابع کافی

- پس مطلق نبودن امنیت

عوامل دیگر

- ارزش زمانی پول
- هزینه امنیت در مقابل ضرر محتمل
- شکستن امنیت معمولا در ضعیف‌ترین پیوندها

اهداف و ابعاد امنیت

در ابتدا محدود کردن دسترسی افراد

سپس دارای موارد بیشتر

- در طی چند دهه اهداف ثابت

شش بعد کلیدی

- یکپارچگی، عدم‌انکار، اعتبار، محرمانگی، حریم خصوصی، دسترسی

اهداف و ابعاد امنیت

محرمانگی
- اطمینان از اینکه پیام صرفا در اختیار افراد ذیصلاح باشد
- به دیگر سخن نامفهوم بودن اطلاع در رایانه و یا در حین ارسال برای فرد غیرمجاز

یکپارچگی (در بعضی متون تمامیت)
- اطمینان از اطلاع نمایشی در سیستم، یا ارسالی یا دریافتی را شخص غیرمعتبر تغییری نداده باشد
- به دیگر سخن مصونیت از تغییرات یا حذف یا ایجاد غیرمجاز داده
- تغییر مسیر مبلغ واریزی
- دارای دو نوع
  - یکپارچگی داده- اطمینان از تغییر صرفا مجاز اطلاعات و برنامه
  - یکپارچگی سیستم- اطمینان از اجرای سالم و بی‌عیب وظایف سیستم و فارغ از دستکاری عمدی یا غیرعمدی

موجود (دسترسی‌پذیری)
- اطمینان از کار و عملیاتی بودن همان‌گونه که موردانتظار است
- وجود دسترسی استفاده‌کنندگان مجاز

Confidentiality
Integration
Availability

اهداف و ابعاد امنیت

عدم انکار

- اطمینان از عدم قادر بودن شرکت‌کنندگان به انکار عملی که انجام داده‌اند
- افزودن نظرات با ایمیل رایگان یا با نام دیگری
- یا حتی با نام خود و سپس انکار در مرحلهٔ بعد

احراز (پیام یا شخص)

- امکان تصدیق هویت شخص که با آن در ارتباط هستید
- چگونه مشتری مطمین است که تارمانه همان است که مدعی است
- چگونه فروشنده از ادعای خریدار مطمئن است
- جعل- کسی خود را جای دیگری قلمداد کند

حریم خصوصی

- امکان کنترل بر استفاده از اطلاع مشتری که خود شخص در اختیار فروشنده گذاشته است
- مسئله‌های فروشندگان در رابطه با حریم خصوصی
  - ایجاد سیاسات داخلی جهت مدیریت استفادهٔ خود از اطلاعات مشتری
  - حفاظت از اطلاعات از دسترسی‌های غیرمجاز
  - دریافت اطلاعات کارت یا اطلاعات دیگر
  - هم از دست رفتن محرمانگی و هم از دست رفتن حریم خصوصی

Non-repudiation
Authentication
Privacy

اهداف و ابعاد متفاوت امنیت از مشتری و کارپرداز

جنبه	از منظر مشتری	از منظر کارپرداز
یکپارچگی	آیا اطلاعی که ارسال یا دریافت کردم تغییر کرده است؟	آیا دادهٔ موجود در مانه بدون داشتن مجوز تغییر یافته؟ آیا داده دریافتی از مشتری معتبر است؟
عدم‌انکار	آیا بخشی که با من کار کرده امکان انکار تعامل را دارد؟	آیا مشتری امکان انکار سفارش را دارد؟
احراز	با چه کسی معامله می‌کنم؟ چگونه از اینکه طرف با که خود را معرفی می‌کند یکی است؟	هویت واقعی مشتری چیست؟
محرمانگی	آیا شخص دیگر امکان دیدن پیام‌های مرا دارد	آیا هر کسی بدون مجوز به پیام‌ها و داده محرمانه دسترسی دارد؟
حریم خصوصی	امکان کنترل بر استفاده اطلاعات شخصی من منتقل شده به تاجر	چه استفاده‌هایی از داده‌های شخصی جمع شده می‌توان داشت؟ آیا اطلاعات گرداوری شده از مشتری‌ها بدون مجوز است؟
دسترسی	امکان دسترسی به مانه را دارم؟	آیا مانه عملیاتی است؟

تعریف امنیت

ساما NIST

- حفاظت در اختیار سیستم جهت دستیابی به اهداف یکپارچگی و دردسترسی و محرمانگی

و عدم‌انکار و تشخیص اعتبار و حفظ حریم خصوصی

چالش‌های امنیت

نصب‌العین و پیش چشم- ساده به نظر آمدن و موثر بودن اهداف امنیت اما پیچیدگی در عمل

حملات بالقوه در مقابل حملهٔ موفق

درگیر مباحث نرم‌افزاری
- انواع نرم‌افزارها و پدیده امکان‌ناپذیری بی‌خطائی
- سختی بی‌اشتباه درآوردن برنامه
- هرچه بزرگتر، اشتباهات بیشتر

چون وصلهٔ ناچسب دیدن

هزینهٔ بالا

ایراد در کار افراد به جای ایراد در کار ابزار

نبرد بین نفوذگر و طراح
- نفوذگر به دنبال منافذ و طرح در پی بستن آنها
- امتیاز مهاجم: کفایت یافتن صرفا یک ضعف در مقابل اجبار طراحی به یافتن تمامی ضعف‌ها

فرایندی مداوم

تنش بین امنیت و دیگر ارزش‌ها

همانند مورد سنتی

راحتی استفاده

- افزودن امنیت بیشتر، سخت‌تر شدن استفاده از سامانه و کندتر شدن آن
- کسب امنیت بیشتر به قیمت کاهش سرعت پردازنده‌ها و افزودن میزان زیادی درخواست‌های حافظه بر ابزارهای ذخیره‌سازی
- افزونه‌ای مختل فیاوری
- امنیت بیش ازحد مخل جهت سوددهی
- امنیت کمتر از حد محتملا بدر کردن از فضای فیاوری

برعهدهٔ کاربر گذاشتن

- از گزینه اتصال خودکار (کمترین امنیت) تا رمزهای یکبار مصرف (بیشترین امنیت)

تنش بین امنیت و دیگر ارزش‌ها

امنیت عمومی و استفاده‌های مجرمانه از اینترنت

- تنش بی‌پایان بین فعالیت ناشناس و نیازهای اجتماع جهت ایجاد امنیت عمومی
- استفاده مجرمان از تکنولوژی جهت طرح جرم یا تهدیدات ملی

شنود تلگراف در دوران جنگ داخلی امریکا ۱۶۰ سال پیش

- جهت به دام انداختن خائنان و ترورگرها

شنود تلفن در سال ۱۸۹۰

عدم اجازهٔ هیچ دولت ملتی به وجود فناوری که مجرمان بتوانند در آن جرم کنند یا تهدید کنند مگر با ترس نظارت و جستجو

- کارتل‌های مواد مخدر
- تعقیب قضایی تالارهای فروش کارت در امریکا
  - مانند shadowcrew و carderplanet

تنش بین امنیت و دیگر ارزش‌ها

- اعمال تروریستی
  - برنامه‌ریزی- رمزی یوسف
  - استخدام و بکارگیری- عمر فاروق عبدالمطلب
  - اسنودن- گزارش دسترسی به سرورهای شرکت‌هائی چون فیس‌بوک و گوگل و اپل و مایکروسافت
  - جستجوی اطلاعات شهروندان امریکا بدون مرجع قضائی

تهدیدات امنیتی در محیط رایانه و شبکه

سه نقطه اصلی آسیب‌پذیری محیط تجارت الکترونیک از منظر فناوری

- مشتری
- سرور
- خطوط ارتباطی
  - کانال‌های ارتباطی اینترنت

جرائم رایانی؟!

دلیل توجهات بیشتر به رایانش امن

- افزایش تعداد جرم‌ها در این زمینه
- حمله به پنتاگون در ۱۳۷۷
  - نزدیک حمله به عراق و ورود به سامانه جوانان ۱۸ ساله! قسم حضرت عباس و دم خروس
  - حمله به سیستم‌های دولتی
    - از طرف دشمن
    - مخالفان با دولت
    - تجارت
    - رقبا
    - بانک‌ها و موسسات مالی
- مجازات‌های جرائم رایانی
  - تفاوت با جرائم متعارف
  - تشخیص دستیابی اتفاقی یا عمدی به اطلاعات رده‌بندی شده
  - میزان خسارت

سخن کوتاه

- نیاز به تعریف احکام مناسب و همچنین رویه‌های بازدارنده

تخمین و مقابله با خطر

تخمین خطر و مقابله با خطر و اصلاح خسارات

اهداف تخمین خطر

- تعیین توان سیستم
- تصمیمات جهت بهبود امنیت سیستم

اطلاعات ناشی از تخمین خطر

- تشخیص و تعیین دارائی‌های بنیادی سازمان
- شناسائی تهدیدهایی که سازمان با آن مواجه است
- شناسائی نقاط آسیب‌پذیر
- شناسائی ضایعات مخفی
- شناسائی اقدامات متقابل کارا و موثر
- اجرای سیستم امنیتی کارا

فرضیهٔ تخمین

هدف یافتن مناطق خطرخیز و مستعد جهت حمله و راهکارهای مناسب حفاظت

استفاده از سه ویژگی خطر

- دارایی
  - اعمال روزانه در مقابل اسناد طراحی
- تهدید یا خطر
  - نوع تهدید معرف میزان توجه لازم سازمان
- آسیب‌پذیری
  - خودروی درب و داغان در مقابل خودروی نو

استفاده از این سه ویژگی جهت تبیین خطر نسبی

فرضیهٔ تخمین

سنجش ارزش دارائی از ترکیب سه معیار

- محرمانگی
- موجودی
- صحت و اعتبار

سنجش آسیب‌پذیری

- سیستمی دارای احتمال وقوع زیان یا خسارت
- هر دارائی درای یک ارزش اما امکان تعداد زیادی نقطه و امکان آسیب‌پذیری

سنجش تهدید

- نیروی درتوان جهت حمله و متفاوت از حملهٔ موفق
- به دیگر سخن توفّقِ «دانستن حملات درتوان» بر «دانستن حملهٔ موفق»
  - چرا؟
- نیاز به دسته‌بندی و درجه‌بندی تهدیدات
  - طبیعی و تولید انسانی
  - نوع انسانی
    - خصمانه و غیرخصمانه
    - آگاهانه و کور
    - درون‌سازمانی و برون‌سازمانی

فرضیهٔ تخمین

انواع مختلف حمله

۱- خصمانهٔ آگاهانهٔ درون‌سازمانی

۲- خصمانهٔ آگاهانهٔ برون‌سازمانی

۳- خصمانهٔ کور درون‌سازمانی

۴- خصمانهٔ کور برون‌سازمانی

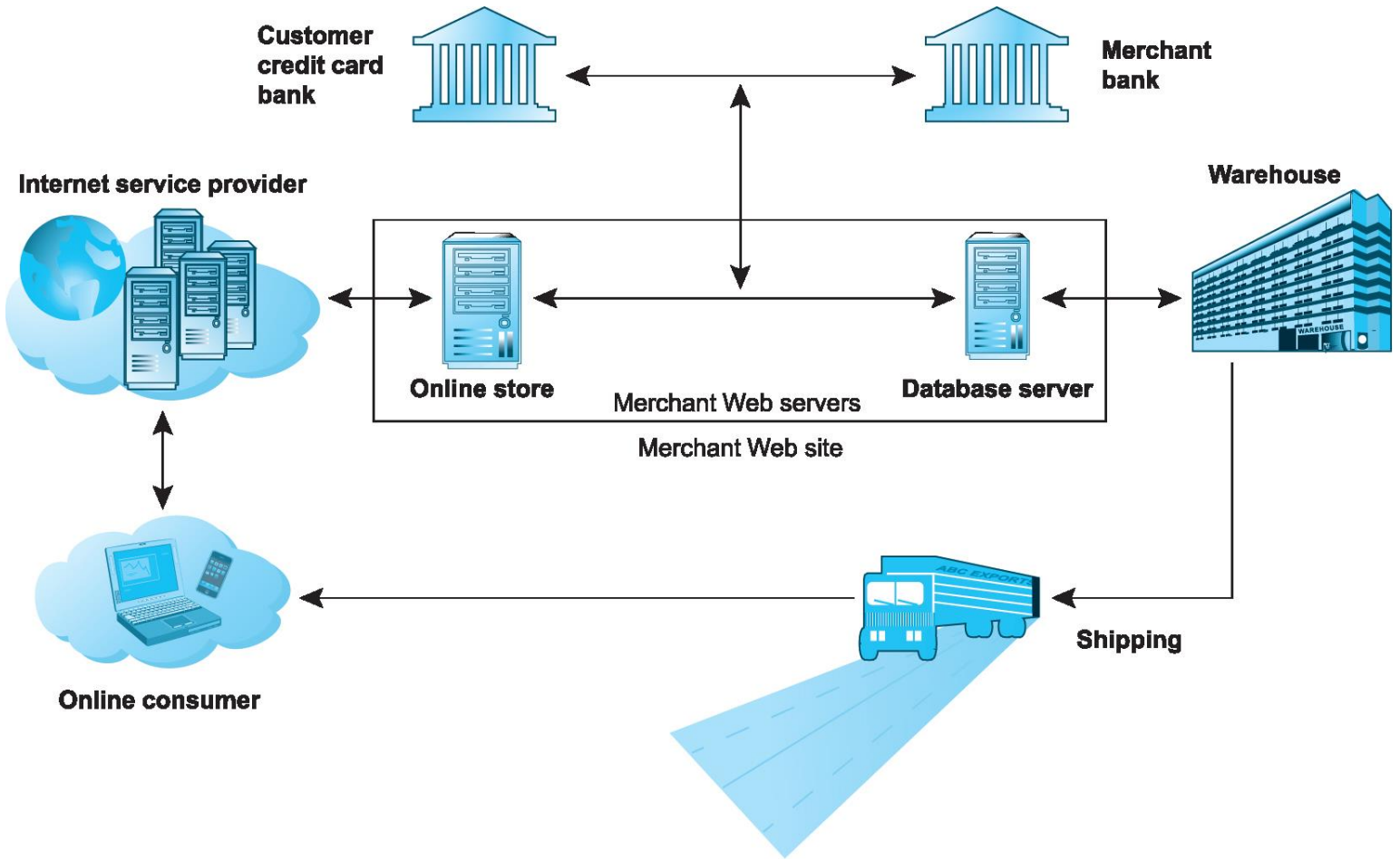
۵- خصمانهٔ آگاهانهٔ درون‌سازمانی

۶- خصمانهٔ آگاهانهٔ برون‌سازمانی

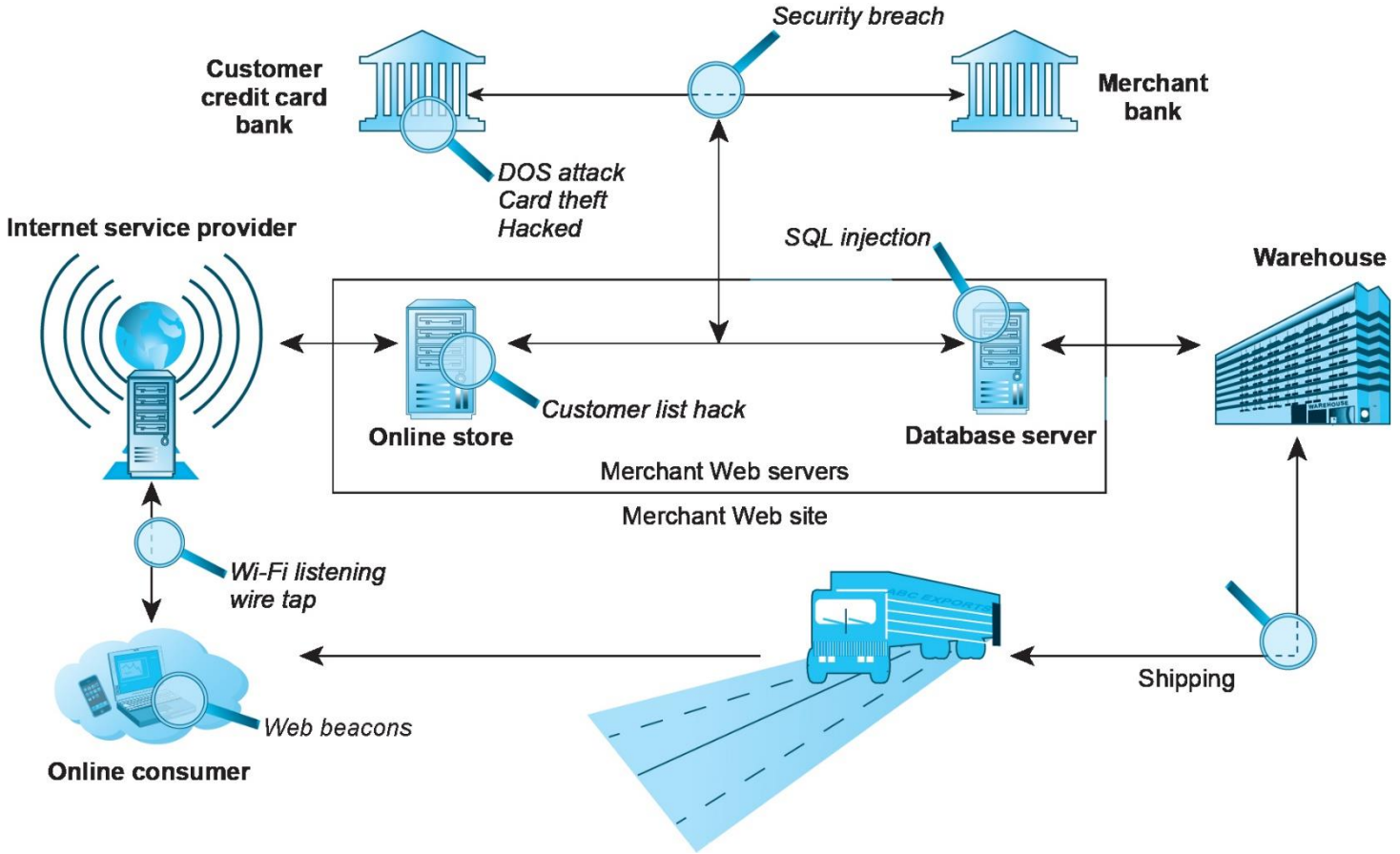
۷- خصمانهٔ کور درون‌سازمانی

۸- خصمانهٔ کور برون‌سازمانی

نمونه معمول تراکنش الکترونیکی



نقاط آسیب‌پذیر در تراکنش الکترونیکی



انواع اطلاع

فیزیکی و الکترونیکی

چگونگی تمایز

- تفاوت بین نسخهٔ اصلی و رونوشت در اطلاعات فیزیکی
- امکان ردگیری تغییرات نسخهٔ فیزیکی
- تعیین اصالت نسخه

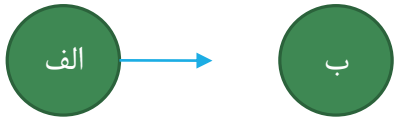
خدمات امنیتی

- محرمانگی
- احراز اصالت
- یکپارچگی
- عدم‌انکار
- کنترل دسترسی
- موجودی (دسترسی‌پذیری)

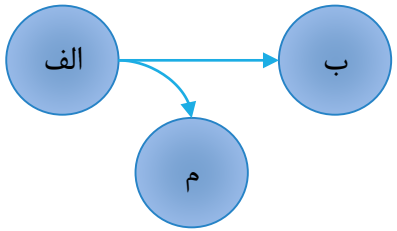
انواع حمله

- فعال-
  - نقاب، تکرار، تغییر، وقفه
- غیرفعال-
  - شنود

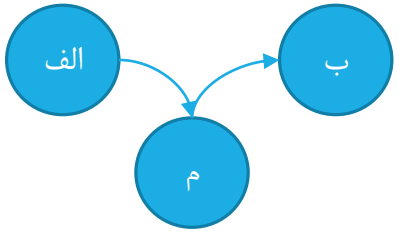
انواع حمله خدمات امنیتی



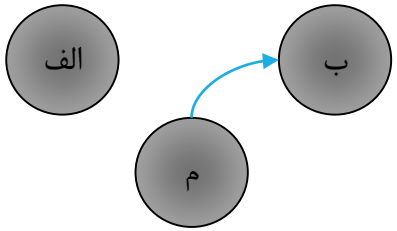
وقفه
- حمله به موجودی
- فعال



دستبرد
- حمله به محرمانگی و کنترل دسترسی
- غیرفعال



تغییر
- حمله به یکپارچگی و عدم‌انکار
- فعال



جعل
- حمله به احراز اصالت و کنترل دسترسی
- فعال

Interruption
Interception
Modification
Fabrication

راهکارهای امنیتی

فرایند یا سیستم کشف و پیشگیری حملهٔ امنیتی و اصلاح ناشی از وقوع آن

شامل

- رمزنگاری
- امضای دیجیتال
- کنترل دسترسی
- یکپارچگی داده
- احراز اصالت
- لائی ترافیک
- کنترل مسیریابی
- گواهی رسمی

منابع

[لاودن]

[استالینگز]

[بختیاری]