امنیت در عصر اطلاعات

مهندس توکلی

مدرس و مشاور

مدیریت پروژه (PRINCE۲)، معماری سازمانی (EA)، حاکمیت فاوا (IT_GOVERNANCE)، فرآیندهای ارائه خدمات (ITIL۳)، امنیت فاوا (ISMS)

امیرُالمؤمنین عَلی علیه السلام: مَنْ نامَ عَنْ عَدوهِ إنتَبَهَتهُ المکائِدُ

هر که از دشمن خود غافل شود دسیسه‌ها او را به خود آورد

غررالحکم ص۳۳

سخن آغازین

وقتی عرصه فناوری تغییر می‌کند،

مهارتهای قبلی به درد کارزار

جدید نمی خورد.

مثال تاریخی: جنگ چالدران(۸۹۳/۸/۲۳)

وضعیت شاه اسماعیل صفوی (قبل از جنگ)

- اهتمام به ترویج مذهب شیعه داشت.
- در هیچ جنگی شکست نخورده بود.
- مریدانی وفادار داشت.
- مهارت سوارانش در شمشیر زنی، نیزه و گرز، مثال‌زدنی بود.

اوضاع کارزار

- جنگ بین شاه اسماعیل صفوی و سلطان سلیم عثمانی
- حمله موفق سوار نظام قزلباش با شمشیر و گرز و نیزه به پیاده نظام عثمانی نتیجه عقب نشینی سلطان سلیم و در شرف فرار
- فرمان سنان پاشا به توپخانه برای نشانه گیری منطقه درگیری طرفین
- رم کردن اسبهای قزلباش با شنیدن صدای غرش توپخانه، زمین زدن سواران و پراکنده شدن در دشت

شکست سخت شاه اسماعیل

- شاه اسماعیل که در قلب سپاه شمشیر میزد و از بازو مجروح شده بود با به گل رفتن اسبش به زمین افتاد و دسته ای از عثمانی ها برای دستگیریش تاختند. میرزا سلطان علی افشار که شبیه شاه اسماعیل بود خود را به نام شاه زده و به جای او اسیر گردید.
- سپاهیان عثمانی به فرماندهی احمد پاشا تبریز را که بی دفاع بود به آسانی فتح کرده، خزاین و همسر مورد علاقه شاه را با خود بردند.

سرانجام کارزار چالدران

- شاه اسماعیل عبدالوهاب را در آماسیه به نزد سلطان سلیم فرستاد و تقاضای صلح و استرداد همسرش را کرد.
- شرط سلطان سلیم، دست برداشتن از ترویج مذهب شیعه و لعن خلفا و خطبه خواندن به نام آنان در مساجد و سرحد قرار دادن رود ارس بود که شاه اسماعیل قبول نکرد.
- اعتقاد مریدان به شاه اسماعیل کم شد چون قبل از این در هیچ جنگی شکست نخورده و زخم بر نداشته بود.

نتیجه گیری حال

- بعد از گذشت حدود ۵۰۰ سال از شکست چالدران، دوباره عرصه فناوری تغییر کرده است:
  - توپ تبدیل شده به به بدافزار
  - فرمانده تبدیل شده به سرورهای هدایت و کنترل C&C
  - سرباز تبدیل شده به رایانه تسخیر شده
  - لشکر تبدیل شده به Bot Hunter

یک نمونه: بدافزارهای پنهان گر

- تروجان BackDoor-FHI همچنین قادر به آلوده سازی منابع مشترک شبکه می باشد.
- آلودگی هنگامی رخ می دهد که فایل اصلی بدافزار اجرا شود که معمولاً shortcutجعلی از فایل ها و پوشه های موجود در حافظه است.
- این بدافزار از روش های متفاوتی برای انتشار خود استفاده می کند که از آن جمله می توان به انتشار از طریق e-mail، صفحات وب آلوده و هک شده، شبکه های peer-to-peerو IRCها اشاره کرد.

نمونه ۱: Stux.net

- هدف: سایت های هسته ای ایران
- ۱۳ روز جمع آوری اطلاعات
- تخریب سانتریفیوژهای هسته ای با در اختیار گرفتن PLC و فرمان به دورهای خارج از حد مجاز (بین ۸۰۰ تا ۱۲۰۰ دور در ثانیه)
- استفاده از چهار آسیب پذیری ویندوز که ۲ تا از آنها قبلا شناخته نشده بود
- استفاده از گواهی های موید اسناد الکترونیکی

Stux.net **ادامه**

- اولین علایم سال ۱۳۸۷، شناسایی توسط یک آنتی ویروس غیر مشهور بلاروسی و اعلام عمومی در سال ۱۳۸۹
- در ایران: ۱۶۰۰۰ کامپیوتر آلوده
- آلوده شدن ۳۰۰ پروژه سیستمهای کنترل صنعتی
- در دنیا: بیش از ۶۰۰۰۰ کامپیوتر

نمونه ۲: دیوکیو

- دو حمله متوالی در ۱۲ و ۲۴ مهر ۱۳۹۰
- هدف آلوده کردن کامپیوترهای کنترل گر نیروگاه، پالایشگاه های نفت و دیگر زیرساخت های حیاتی با هدف جمع آوری اطلاعات درباره تاسیسات صنعتی
- کرمی پیچیده تر از استاکس نت که طراحی آن نیاز به بودجه فراوان، زمان و دانش بسیار نیاز دارد
- تغییر برنامه امنیتی کامپیوتر برای جلوگیری از شناسایی آن

نمونه ۳: تخریب غیر قابل بازیابی اطلاعات وزارت نفت با نامه الکترونیکی

- از منبع ناشناس به زبان انگلیسی:" من از تو عکسی دارم، عکس ضمیمه را چک کن، خودت هستی؟" به همراه ضمیمه img۹۸۰۷.zip
- با کلیک روی ضمیمه با استفاده از روش Wipe، نسبت به انهدام کامل اطلاعات اقدام می کند.

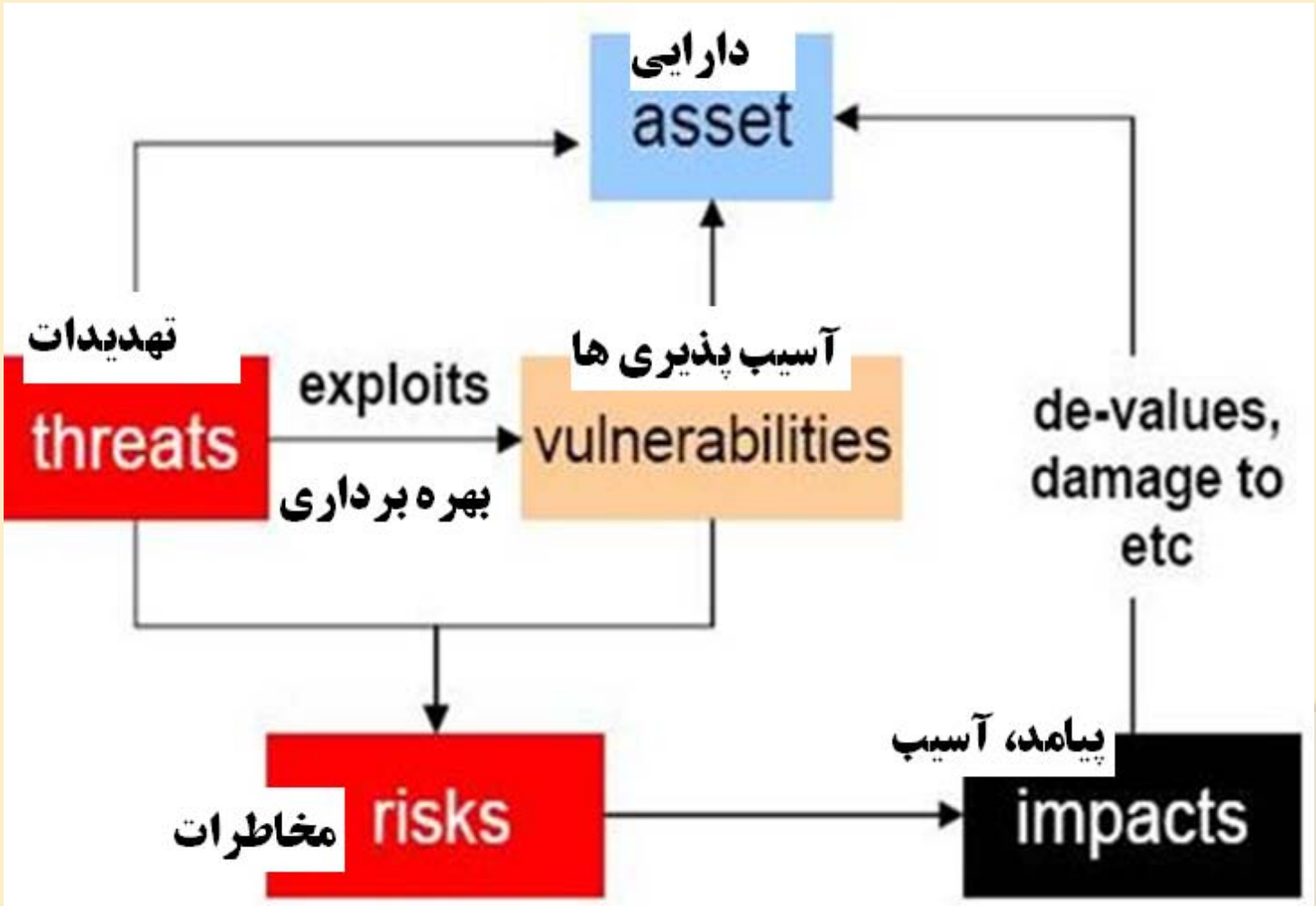
نمونه ۴: شنود محیطی با شعله (flame) ۹۱/۳/۸

- پویش شبکه، جمع آوری و ثبت اطلاعات منابع شبکه و رمز عبور سیستمهای مختلف
- ذخیره تصاویر نمایش داده شده از فعالیت های کاربر روی مونیتور
- ذخیره سازی صوت دریافتی از طریق میکروفون سیستم در صورت وجود
- ارسال اطلاعات ذخیره شده به سرورهای کنترل و فرماندهی خارج از کشور
- دارا بودن بیش از ده دامنه به عنوان C&C
- برقراری ارتباط امن با سرورهای C&C از طریق پروتکل های SSH و https
- آلوده سازی سیستم های شبکه در مقیاس بالا علاوه بر انتشار از طریق حافظه های فلش داخلی
- پویش دیسک کامپیوتر آلوده و جستجو برای فایلها با پسوندها و محتوای مشخص

جنگ سایبری شروع شده است!

- طراحی جنگ توسط کشورها
- تامین امنیت به دلیل محدودیت در دسترسی، هزینه، عدم پوشش تهدیدات به صورت مطلق امکان پذیر نیست.
- ابزارهای مهاجمین پیشرفته تر شده، دسترسی به ابزارها از طریق اینترنت ساده تر شده و بکارگیری این ابزارها به دانش تخصصی کمتری نیاز دارد
- تاثیر تخریبی و خسارت مالی حملات رو به افزایش است

مفاهیم پایه امنیت



مفاهیم مرتبط با جنگ سایبری

- Attack
- Infected
- Exploit
- Live system
- Zero-Day vulnerability
- Forensics
- Honey pot
- Bot Hunter
- C&C servers
- Hash (MD۵)
- Memory dump

- حمله
- آلوده
- تسخیر شده
- سیستم زنده
- آسیب پذیری اعلام نشده
- جرم یابی
- تله ظرف عسل
- شکار سربازان کامپیوتری
- شبکه کنترل و فرماندهی
- مهر و موم الکترونیکی
- ذخیره محتوای حافظه

راهکارهای برقراری امنیت ایجابی!

- حاکمیت فاوا
- مدیریت خدمات فاوا
- مدیریت پروژه سرآمد ایران

رویکردهای برقراری امنیت سلبی!

- رویکرد مدیریتی
- رویکرد فنی
- رویکرد انسانی (مهندسی اجتماعی)

فیلم امنیت مراکز داده گوگل

- امنیت فیزیکی
- امنیت اطلاعات
- روش های مطمئن عملیات

رویکرد مدیریتی به امنیت

- سیستم مدیریت امنیت اطلاعات (ISMS)
- استانداردهای خانواده ISO ۲۷۰۰۰

حوزه های یازده گانه ISO/IEC 27001

رویکرد فنی به امنیت

- مقابله با بدافزارها
- دیواره آتش
- رصد شبکه (مونیتورینگ)
- تست نفوذ
- سرور ظرف عسل
- رمزنگاری

مخاطرات ارتباطات در فضای مجازی

- در فضای مجازی تمام تعاملات سیستمی رصد می‌شود.
- هویت ها ممکن است مجازی باشند ولی به دلیل آنکه آنرا حیات خلوت خود می‌دانند معمولا حرف واقعی خود را می‌زنند و شخصیت واقعی خود را نشان می‌دهند.
- با توجه به حجم انبوه اطلاعات رد و بدل شده در فضای مجازی سیستمها بر اساس محتوا و مبدا و مقصد بعضی از مطالب را جدا می‌کنند و بعد انسان‌ها آنها را تحلیل می‌کنند
- رصد بر اساس IP و Mac Address (مشخصات کامپیوتر مقصد و مبدا)
- پس در رصد می‌توان به کامپیوتر مبدا و مقصد رسید ولی اگر قراینی وجود نداشته باشد، نمی توان لزوما به هویت فرد پی برد. (به شرطی که تصویر گذرنامه را با Email ارسال نکنیم)

انواع روش‌های ارتباطی

- Email
- Chat
- VOIP (ooVoo, Skype(رصد کامل توسط صهیونیست‌ها))
- Upload Center (۴share)
- Cloud
- Group (topbox)
- Weblog
- Mobile

امنیت در فضای مجازی

- رایانامه
- شبکه های اجتماعی
- نسل جدید تلفن همراه

رایانامه

- باز بودن محتویات نامه برای مسیر انتقال اطلاعات
- مشخص بودن ارتباطات و تعاملات
- امکان تحلیل محتوا
- به عنوان هویت در شبکه های اجتماعی
- تلاش google برای یکپارچه کردن کلیه سرویس ها با آن

شبکه‌های اجتماعی

- وب ۱: اطلاع رسانی
- وب ۲: تعاملی: از اظهار نظر تا شبکه‌های اجتماعی
- وب ۳: معنایی(هوشمند متناسب با هر نفر بر اساس سوابق)

شبکه های اجتماعی مطرح

- قاره Facebook: بیش از یک میلیارد نفر جمعیت
  - شبیه سازی روابط اجتماعی (دوست، صفحه، گروه، feed,like)
- کشور+google: بیش از ۲۵۰ میلیون نفر
  - مفهوم حلقه
  - تماس تصویری
- کشور Twitter: بیش از ۲۵۰ میلیون نفر
  - خبر
  - افرادی که خبر شما را دنبال می کنند
  - افرادی که شما خبر آنها را دنبال می‌کنید.

مثال هایی از وب هوشمند فضای مجازی

- تحلیل شخصیت در فضای مجازی
- مثلا از نام دوستان مانند محمد، حسین و زهرا (به مذهبی بودن او می‌توان پی برد و در جستجوی تصاویر، تصاویر مذهبی را نشان داد)
- مثلا با تحلیل ارتباطات و دوستان، مطالب آنها که تعامل بیشتری با آنها دارید، ابتدا نشان داده می‌شوند.
- با نوع گروه هایی که مرتبط هستید می‌توان جنسیت و حدود سنی را تشخیص داد.
- کتاب‌هایی که دوستان هم سلیقه فرد دیده‌اند به او پیشنهاد می‌شود.

نمونه ای از اطلاعات افراد در Face Book

- اطلاعات کاری
- آموزشی
- تولد
- علاقمندی‌ها
- زبان ها
- دیدگاه سیاسی و مذهبی
- جاهایی که تردد کرده
- اطلاعات افراد خانواده
- ایمیل ها و ایمیل ورودی به شبکه اجتماعی

کارزار در Face book

- اقامه دعاوی قانونی، اگر بیش از صدهزار نفر با دلایل مشابه اعلام کنند که صفحه‌ای غیر قانونی است توسط آن بسته می‌شود.
- با بدست آوردن ID و Password گروه‌ها یا صفحات مورد نظر می‌توان اختیار آنها را بدست گرفت
- با ساختن صفحه به نام افراد مشهور می‌توان از شهرت آنها سوء استفاده کرد.

مخاطرات تلفن همراه

- مکان یابی از طریق BTS, GPS,GPRS
- شنود محیطی، روشن کردن میکروفون از راه دور
- تایید هویت در شبکه های مجازی
- اطلاعات تماس ها و دفتر نشانی

امنیت در شبکه‌های موبایل

- ۲G (همراه اول، ایرانسل)
- ۳G (CDMA)
- Satellite
  - برای اپراتور (۱۰ متر تا ۵۰۰ متر)
  - برای GSM (با دقت ۱ تا ۱۰ متر)
  - شناسه سیم کارت و شناسه موبایل (IMEI) مشخص باشد.
  - امکان روشن کردن میکروفون از راه دور با یک شماره مشخص وجود دارد

ابزارهای فنی

- True crypt (AES)
- Zip (WinZip, ۷zip)
  - **استفاده از سیستم عامل دوم برای کارهای خاص**
  - **مثلا Windowsبرای ارتباط با اینترنت و Linuxبرای تهیه اسناد**

رویکرد انسانی به امنیت

- سوء استفاده از مهندسی اجتماعی
- ترفندهای روانشناسی که افراد را در به خطرانداختن خود تشویق می کند.

روش‌های مهندسی اجتماعی

- حضور در محل هدف
- تماس تلفنی
- استفاده از اسناد دور ریخته شده در سطل زباله
- استفاده از اینترنت
- استفاده از آسیب پذیریهای رفتاری انسان ها

آسیب پذیری رفتاری انسان ها

- زیر دین بردن
- فرمان پذیری از قدرت مافوق
- رقابت و کمیابی
- مجذوب شدن
- هیجانات روحی
- حجم بالای اطلاعات
- اعتماد نابجا
- در مضیقه بودن

راه کارهای مقابله با حمله های مهندسی اجتماعی

- لایه اول: خط مشی های امنیتی
- لایه دوم: آموزش همگانی
- لایه سوم: آموزش مقاومت برای افراد کلیدی سازمان (کارشان کمک به دیگران است یا اطلاعات/دسترسی های حساس دارند)
- لایه چهارم: تذکر
- لایه پنجم: مین های زمینی مهندسی اجتماعی
- لایه ششم: پاسخ به حوادث امنیتی

مسئولین از کارکنان بخواهند.

حوادث امنیتی

- **حوادث امنیتی (فناوری اطلاعات یا غیر از فناوری اطلاعات) را به میز امداد از طرق زیر گزارش دهید:**
  - **ایمیل داخلی به آدرس:**
  - **تماس تلفنی با شماره :**
  - **گزارش ناشناس به صندوق پستی شرکت**
- **برای مثال:**
  - **حادثه فناوری اطلاعات: حمله ویروسی، هک شدن و...**
  - **حادثه غیر فناوری اطلاعات: نشت اطلاعات، رساندن رسانه غیرمجازو...**

راجع به حوادث امنیتی با افراد خارج شرکت گفتگو نکنید.
سعی نکنید مانع از گزارش دادن کسی شوید و در امر گزارش دادن دیگری مداخله نکنید.

مسئولین از کارکنان بخواهند.

- اطمینان حاصل کنید که یارانه شخصی شما به آخرین به‌روزرسانی آنتی ویروس مجهز است.
- اطمینان حاصل کنید که سیستم شما وقتی که بیرون هستید قفل شده است.
- همواره لپ‌تاپ و رسانه‌های خود را در محل قابل قفل‌شدن قرار دهید.
- در هنگام استفاده از لپ‌تاپ در مسافرت مراقب باشید.
- اطمینان حاصل کنید که زمانی که از اطلاعات دیجیتال حساس استفاده نمی‌کنید، در محل مطمئنی قرار دارند.

مسئولین از کارکنان بخواهند.

- از دارایی‌های اطلاعاتی حساس و حیاتی، نسخه پشتیبان تهیه کنید.
- اگر پیامی از طرف فرد ناشناسی دریافت کردید، اعتبار آن را بررسی کنید. بدون بازکردن پیوست آن را حذف نمایید.
- همواره قبل از ترک محل کار در پایان روز، رایانه خود را خاموش کنید.
- همواره اطلاعات خود را در زمینه امنیت اطلاعات به‌روز نگهدارید.

تاکید بر رعایت

- مسئولیت برقراری و رعایت امنیت با مدیر است.
- همه از مدیران تا کارکنان مسئول تامین امنیت هستند.
- انتخاب رمز عبور مناسب و رعایت در خصوص فلش و نوت بوک
- پیاده سازی ITIL۳, IT Governance و مدیریت پروژه

سرآمد ایران، فرآیندها را منظم و زمینه را برای برقراری امنیت (ISMS) فراهم می کند.

یک روش کارآمد برای ساختن رمز عبور

- ویژگی های رمز عبور مناسب
- چگونه به خاطر بسپاریم؟
- برعکس عمل کنیم (یکی از اصول خلاقیت)

ملاحظات امنیت

- امنیت، تک بعدی نیست.
- امنیت، تنها خرید تجهیزات نیست. از خط مشی امنیتی تا توجه به مهندسی اجتماعی جزو امنیت است.
- یک لحظه غفلت ممکن است باعث یک عمر پشیمانی شود.
- برای تامین امنیت نمی توان به خارجی اتکا کرد.

سخن پایانی

برای انسان‌های بزرگ،
بن‌بستی وجود ندارد؛
زیرا آنها بر این باورند که:

یا راهی خواهند یافت،
یا
راهی خواهند ساخت.

پرسش و پاسخ