Datasäkerhet och integritet

OH-1 v1

- Data och IT-säkerhet
- Definitioner
- Hot
- Klassning och policies

Datasäkerhet?

- Det mesta kopplas upp via digital teknik
  - Elektroniska apparater av alla slag
  - Myndigheter och företag
  - Privatpersoner
- Accelererad utveckling och expansion
  - Ökade risker
- Komplexa IT-system
  - Ökar sårbarheten
  - Information saknas ofta inte – filtrera
- Inte alls bara datavirus, maskar etc.

Datasäkerhet och integritet?

- I informationssamhället kan ”därför” den personliga integriteten sättas på spel
- Den digitala utvecklingen berör därmed alla
  - På samma sätt som i den ”vanliga världen” måste man skydda viss egendom och information mot brott
- Grundtes? Det som inte är tillåtet i den vanliga världen är heller inte tillåtet i den digitala motsvarigheten

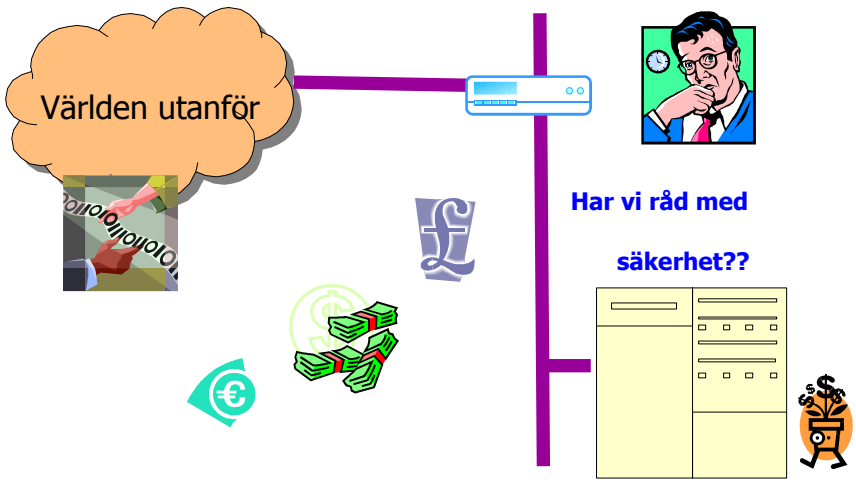
Varför IT-säkerhet?

- I den ”vanliga världen” har ”Svensson” ofta ett antal försäkringar för att skydda sig och närstående då något inträffar
- Vi utför ofta pro-aktiva åtgärder som att äta rätt, motionera, larma bilen/villan, vara extra försiktig i vissa situationer etc.
- God IT-säkerhet handlar om ungefär samma sak
  - Hitta rätt nivå på försäkring och pro-aktiva åtgärder
- Detta kallas för att ha en säkerhetspolicy
  - Inventera system och tjänster
  - Därefter klassa in allt i olika riskklasser
  - Ta fram åtgärdsplan med motåtgärder för varje riskklass

Varför IT-säkerhet?

- God säkerhet handlar om att.
  - Vara medveten
    - Kostnader
    - Vad är farligt
  - Ordning och reda
  - Processer
  - Motivation
  - Teknik satt i rätt sammanhang
- Det är ingen ny företeelse utan har alltid funnits och handlar inte alls bara om teknik

Varför säkerhet?



Varför säkerhet ? (forts)

- Har vi råd att inte ha säkerhet?
- Skadorna är ofta mer kostsamma än skyddet
  - Stulen kunskap/affärsidé
  - Dåligt rykte p.g.a. dålig säkerhet
  - Nätverkstjänster helt blockerade eller starkt reducerade
  - Du kan bli åtalad för att ej följa gällande lagstiftning rörande datasäkerhet

Säkerhetskrav

- **En definition av datasäkerhet**
  - Ett system/nätverk är säkert om du kan lita på att data är korrekt och konfidentiellt (skyddat från utomstående, hemligt) och systemet beter sig som förväntat
- **Autentisering (authentication)**
  - verifiering av motpart/identitet
- **Hemlighållande (privacy)**
  - läsning av data endast tillåten för aktoriserade parter
- **Integritet (integrity)**
  - förändring av data endast tillåten av aktoriserade parter

Definitioner, termer och begrepp

- I databranschen och speciellt inom datasäkerhet finns många svåra uttryck och förkortningar
- Se Handbok i IT-säkerhet, sid. 23-32 för de vanligaste, källa:
  - Swedish Standars Institute
    - Terminologi för Informationssäkerhet http://www.its.se/its/rapport/ITS6.htm i form av nedladdningsbar fil (Windows hjälpfil)
- National Institute Of standards & Technology
  - http://csrc.nist.gov - Glossary i form av pdf-fil
- Informationssäkerhet och IT-säkerhet
  - Definitioner av de båda begreppen (sid. 33, 34)

Definitioner, termer och begrepp

- Sekretess (subst.), konfidentiellt (adj.)
- Integritet
  - Inga modifieringar av oauktoriserade objekt
  - Inga oauktoriserade modifieringar av auktoriserade objekt
  - Datainnehåll konsistent
- Tillgänglighet - pålitligt
- ISO Standards
  - Standarden för informationssäkerhet
  - Ledningssystem för informationssäkerhet (LIS)

Definitioner, termer och begrepp

- Digitala signaturer vs ”traditionell” teknik
  - Exempel bankärende (sid. 37, sid. 41)
- Elektroniska ID
  - Mjuka, certifikat som fil i t.ex. datorn
  - Hårda, certifikat som token i t.ex. smartcard
- SAMSET regelverket
  - Standardarbete för att administrera certifikat för e-legitimationer
  - 24-timmars myndigheten (e-tjänster)
  - Återskapa de pappersbaserade funktionerna

Vad är det vi skyddar?

- Lagrad information
- Informationens korrekthet
- Informationsvärde
- Access till publika tjänster (web/mail)
- Access till interna tjänster (intranät)
- Din organisations integritet

Hotbild

- Hot + svaghet + sårbarhet = hotbild
- Identifiera (endast ett axplock)
  - Finns en god autentisieringfunktion?
  - Var och hur lagras användardata (user credentials)?
  - Krävs separat klientprogram?
  - Vilka nätverksprotokoll används?
    - Portar för kommunikation, för fildelning
  - Kända bakdörrar, virus hot
  - Kryptering?
  - Avlyssning av nätverket möjlig?

Riskanalys och hotscenario

- Typ av hot
  - Fysiska hot
    - Stöld, vandalisering, brand, komponentfel, naturkatastrof
  - Logiska hot (Kopplade till programvaran i IT-systemet)
    - Obehörig användning, manipulering etc.
  - Mänskliga/organisatoriska hot (Mänskliga faktorn)
    - Dåliga eller inga rutiner, dålig kunskap, oklar ansvarsfördelning
  - Insiderhot (hot från insidan, personalen)
    - Har redan passerat första skyddsbarriären…
    - Loggning?

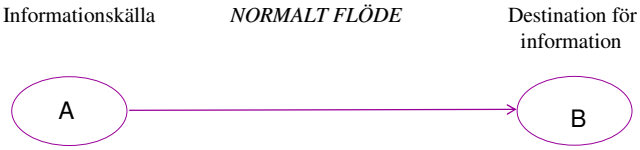
Vem/vad skyddar vi oss mot?

- ”Hackers” tar sig vanligen in via externa nätverksförbindelser, fokuserade på att visa att man **kan** ta sig in i system
  - ”Script kiddiez”: Kopierar existerande ”attack-mjukvara” från nätet och exekverar denna
  - ”Smarta hackers” eller admins: Har kunskap om hur protokoll och system fungerar, hitta exploits (svagheter) i dessa
  - ”Crackers” eller coders, fokuserade på hitta exploits (svagheter) i system och **ändra** befintlig kod i mjukvaran, tillverkar verktygen som utnyttjar dessa svagheter
- Kriminella inkräktare & lurendrejare
  - Har ofta mer och bättre resurser än ”hackers”
- Företagspirater (Corporate Raiders)
  - Har ofta omfattande resurser
- Uppdragstagare/”Torpeder”

En riskanalys - exempel

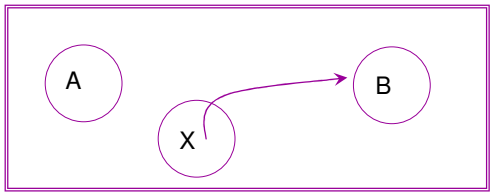
- Det kan börja brinna i datahallen
  - Detta innebär katastrof för organisationen och dess verksamhet
- ”Ha, det kommer aldrig inträffa”
  - Du ignorerar risken
- Du tecknar kontrakt med en firma som kan reparera utrustning och återskapa data efter en brand
  - Du accepterar att brandrisken finns men mildrar effekterna av den
- Du installerar ett avancerat brandsläckningssystem
  - Du tar brandrisken på allvar och etablerar ett försvar mot den
- Det existerar ändå en risk att sprinklersystemet inte fungerar när det väl behövs……
  - Du tecknar en försäkring
- Mot säkerhetsrisker finns dock normalt inga försäkringar att teckna……

En säkerhetsmodell och några vanliga hot



Säkerhetshot I

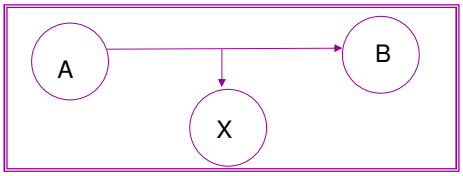
- ”Masquerade”; Någon utger sig för att vara annan person (”förklädnad”)



- Försvarsmetod: Authentication (identifikation, autentisering)
  - Skall förhindra otillåten access till system eller systemresurser
  - Skall förhindra obehörig att ändra enhetskonfigurationer

Säkerhetshot II

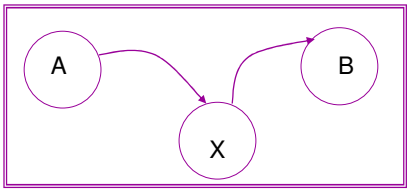
- Avlyssning (interception)



- Försvar: Sekretess/konfidentiellt (confidentiality)
  - Egenskap som skall tillse att information inte görs tillgänglig, eller yppad, för obehörig person, utrustning eller process

Säkerhetshot III

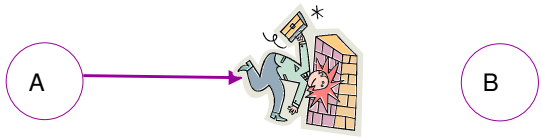
- Modifiering (modification); ”Man in the middle”



- Försvar: Integritet (integrity)
  - Egenskap som skall tillse att data inte har blivit ändrat, förstört eller gått förlorat p.g.a. obehörigs agerande eller vid olyckshändelse

Säkerhetshot IV

- DOS-attack (Denial Of Service)



- Försvar: Tillgänglighet (availability)
  - Egenskap som skall tillse att tjänst finns tillgänglig och användbar för behörig närhelst denne så önskar

Formell tillåtelse - Authorization

- Alla hot-former har en gemensam beröringspunkt; Frågan om rättigheter och behörighet!
- Vem får göra vad?
- Vi har rättigheter på systemnivå samt behörigheter på objektnivå (filer/mappar)
- När en användare bevisat sin identitet för ett system, kontrolleras och verifieras vilka rättigheter och behörigheter som finns kopplade till denna identitet
- Vissa tjänster kräver ingen identifiering alls, t.ex. publika webbtjänster
- Viktigt att definiera vilka rättigheter envar har!

God IT-säkerhet

- Tydlig organisation av IT-användningen
- Säkerhetspolicy
- ”Gyllene treenigheten” för god säkerhet
  - Människor - 40% fundamentet
  - Processer - 40%
    - Analys
    - Plan
    - Implementation
    - Uppföljning
  - Teknik - 20%

Teknik

- Många system har utvecklats utan tanke på säkerhet
- Mjukvara innehåller fel!
- Teknikutvecklingen går fort
- Standardiseringsprocesser tröga i jämförelse
- Ålderdomliga standards utan säkerhetstänk
- Grunden för allt tekniskt säkerhetsarbete är kontroll över systembehörigheter

Informationsklassning

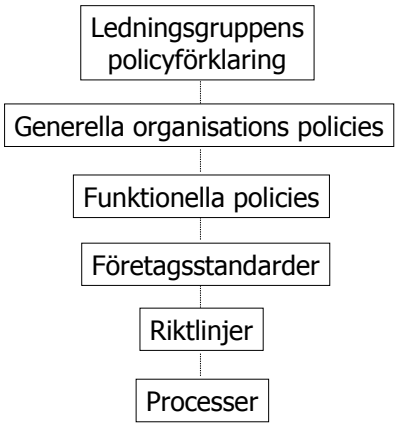
- Oklassad, publik information
- Känslig, oklassad information, ingen större skada
- Konfidentiell, privat information, viss skada uppstår
- Hemlig, konfidentiell information, allvarlig skada
- Topphemlig information, mycket allvarlig skada (denna kategori är ibland inte med)
- Sätta attribut till informationen (metadata)
  - Klass
  - Bäst före datum
  - Tillgång till informationen – från vilka roller?

Säkerhetspolicy

- Det är av störst vikt att alla organisationer har en väl genomtänkt säkerhetspolicy
- Formellt dokument som definierar organisationens säkerhetssyn
  - Vad som är tillåtet och vad som inte är tillåtet
  - Vilka tjänster skall finnas tillgängliga och för vem
  - Vilka åtgärder skall vidtagas vid brott mot säkerhet
  - Hur skyddet skall upprätthållas
- Kräver att en genomgripande riskanalys har gjorts innan
- Dynamiskt dokument som kräver ständig översyn och uppföljning
- Svårast är att definiera vad som är/skall vara förbjudet!

Säkerhetspolicy

- Kan även bestå av flera dokument i en hierarki
- Nivåer intressanta i denna kurs är de under funktionella policies som beskriver vilka verksamhetskrav som understöds av IT-system vilket definieras av en företagsstandard



Att reducera riskerna

Alla risker

Allmän policy/inställning inom organisationen

Tekniska insatser (kryptering, brandvägg etc.)

Acceptabel risknivå: ”Vi kan inte skydda oss mot allt”

Acceptabla risker I

- Det är en viktig skillnad mellan att ignorera en risk och att acceptera densamma
- En ignorerad risk gör vi ingenting åt
- En accepterad risk försöker vi mildra så långt det bara går
- Vissa risker kan med förnuft ignoreras om:
  - Sannolikheten att händelsen skall inträffa är extremt låg
  - Kostnaden för att skydda sig mot risken/hotet är så hög att det är oekonomiskt

Acceptabla risker II

- När accepterar vi en risk?
  - Organisationen kräver att vi tar denna risk
  - Kostnaden för att reparera eventuella skador som orsakats av risken är mycket oekonomisk (hög)
  - Säkerhetspolicyn måste tydligt visa att vi är beredda att acceptera denna form av risk

Försvarsmetodik

- Etablera lokala procedurer som förhindrar säkerhetshot
  - Regelverk för personal och utrustning gällande rättigheter och behörigheter
- Teknologibaserade lösningar
  - Skall fungera oberoende av mänskliga misstag men kräver ofta mänsklig konfigurering innan driftsättning!
- När riskbilden är reducerad så långt som är fysiskt och ekonomiskt möjligt återstår den så kallade överblivna risken, den som vi ej kan planera för eller som vi helt enkelt måste acceptera och ”får leva med”
  - Den måste självklart dokumenteras i säkerhetspolicyn så man är medveten om den och ansvar kan tas (det kan bli en rättslig fråga)

Slutord

- Det finns ingen ”magisk trollformel” som löser alla säkerhetsproblem!!
  - Säkerhet och säkerhetstänkande är och förblir en **attityd** och måste behandlas som en sådan oavsett vilken situation eller roll vi befinner oss i