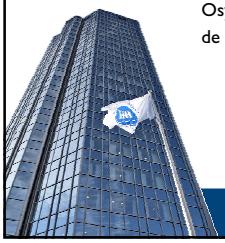
Spårbarhet i digitala system



Osynlig övervakning och
de spår vi lämnar efter oss

Biografi

- Mattias Weckstén – kontor på våning F3 – mattias.wecksten@hh.se
- Forskar på CC-lab i mijön CERES
- Undervisar bland annat i
  - Administration av datorsystem
  - Administration av operativsystem
  - Datautvinning från digitala lagringsmedia
  - (Systemanalys med hjälp av EnCase)
- Kommer att handleda projekt i introduktionskursen

Spårbarhet

- I den fysiska världen
  - Fysiska spår
    - Tappade hårstrån
    - Blod
    - Hudavlagringar
    - Fibrer från kläder eller andra tyger
  - Påverkan
    - Fingeravtryck
    - …

Spårbarhet

- I datorvärlden
  - Aktiv loggning
    - Inloggningsförsök
    - Felkoder
  - Passiv loggning
    - Filrester
    - Windows registryn
  - …

Spårbarhet = sårbarhet?

- Vad är hemligt i ett företag?
- Hur stor skada skulle läckor kunna orsaka?
- Vem tar hand om detta i företaget?
- Exempel:
  - Stulen laptop
  - Begagnad utrustning
  - Säkerhetsluckor

Filsystemet

- I datorn finns en hårddisk
- På hårddisken lagras filer i en struktur
- Hur representeras denna data på hårddisken?
- Exempel:
  - En hårddisk ser ut som flera
  - Filer lagras i en folderstruktur
  - Vad händer egentligen om jag sparar ett notepad-dokument på "Skrivbordet"?

Vad är en hårddisk?

- En trave med magnetiserbara skivor
- Ett läs/skriv-huvud
- För enkelhetens skull kan vi tänka oss hårddisken som ett rutat papper där vi kan skriva ett tecken i varje ruta eller sudda ut vad som skrivits i en ruta

Lagrings-lager-modellen

- Fysiskt
- Data
- Allokering
- Utrymme
- Information
- Applikation

Applikation

- Filer
- (236)

Information

- Foldrar
- Länkar

- (236)

Utrymme

- Filsystemet
  - Hanterar allokeringsenheterna
  - Fil-allokeringstabell
  - Exempel
  - Moderna filsystem
    - Fragmentering
    - Loggande

- (235)

Allokering

- Blockuppdelning
- Styr minsta upplösning = minsta filstorlek

- (234)

Data

- Segregering
  - Säkerhet
  - Optimering
  - Struktur
- BSD ej standard

- (233)

Fysiskt

- Sektorer/ block
  - 512 byte

  - (232)

Radera filer

- Vad händer när man raderar en fil?

- Filallokeringstabellen ändras.
- Inget mer!
- Filen är med andra ord fullt möjlig att återskapa

Formatera en disk

- Filallokeringstabellen töms.
- Data från filerna finns fortfarande kvar.

Vad händer i MS Office Word?

- Vi ska göra en inmatning via ett web-formulär.
- Vi ska göra en utskrift, men utan att spara dokumentet.
- Vi använder Word för att redigera meddelandet.

- Så fort vi påbörjar redigeringarna så sparar Word innehållet i en arbetsfil.
- Denna tas bort när vi stänger programmet
- MEN…

Registryn

- Registryn i Windows är en stor databas med inställningar och information om hela systemet.
- Här kan man göra egna inställningar
- Man kan även spåra vad andra gjort
- Det är inte säkert att data tas bort bara för att den inte används.

Vad händer när ny hårdvara läggs till?

- Registryn påverkas
- Vi kan i registryn se all hårdvara som någonsin varit installerad
- Vi kan se alla usb-diskar som varit anslutna
  - Varje usb-disk har en unik identifierare
  - = tumavtryck ?

Spår i nätverket

- Routingtabeller
- Loggar
- Cachar

- En switch kan se ut som en dum liten låda som bara växlar trafik
- Men tänk noga över vilka spår som den faktiskt sparar

Malware/ Virus

- När virus tar sig in i systemet lämnar de spår efter sig
- Hur kan man dra nytta av detta?
- Viruset kan vara ute efter dina spår!

Exempel: Sub-seven

- Man hade fått in en trojan i systemet. Systemet var möjligtvis infekterat.
- Detta upptäktes av antivirusmjukvaran.
- Grundinställningen i antivirusmjukvaran var att ta bort risker, vilket gjordes

- Nu kunde man i efterhand se att systemet hade varit utsatt men efterssom ”bevisen” hade raderats så kunde ingen vidare undersökning göras.
- Hade trojanen funnits kvar men i karantän så hade man kunnat analyserat den och sett vilken konfiguration den haft – vilka portar den jobbade på osv
  - Med denna information hade det gått att analysera vilka noder som smittats