Loggar = Spårbarhet ?

- IT relaterade brott
- Internet relaterade brott
- Uppgifter
- Metodik
- Loggar
- Tips och annat

IT-relaterad brottslighet

- tre huvudtyper

1. Datorn (informationsbäraren) kan vara *målet* för brottet
   ex dataintrång

2. Datortekniken kan vara *ett medel* för att begå brottet
   ex spridning av barnpornografi

3. Datorn kan, utan att vara ett mål eller medel, *ha beröring med* brottet
   ex för att registrera narkotikaleveranser, falsk bokföring

Internet-relaterade brott

Till stor del IT-relaterad ”mängdbrottslighet”

- ofredande
- olaga hot
- förtal
- sexuella ofredanden
- brott mot PUL
- bedrägerier
- dataintrång
- m. fl.

Vilka uppgifter har vi ?

- Analys av digitalt media
- *Utredningar på dataintrång* (BrB 4 kap 9c §)
- **9 c §** Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för dataintrång till böter eller fängelse i högst två år. Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling.

  Lag (*1998:206*).

Metodik – ”goda rutiner”

Bygger på process i fyra steg:

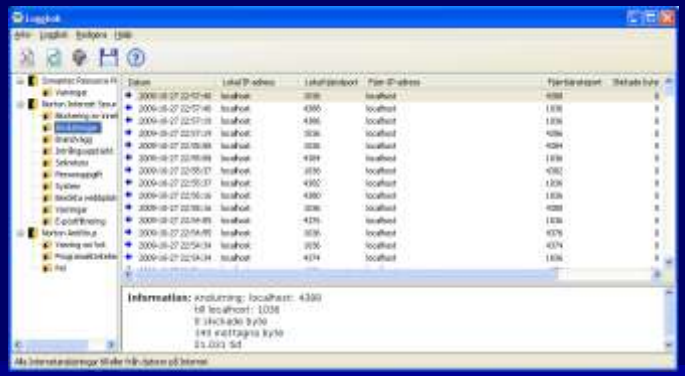
1. INSAMLING *(loggar)*

2. UNDERSÖKNING

3. ANALYS *(loggar)*

4. DOKUMENTATION

Loggar



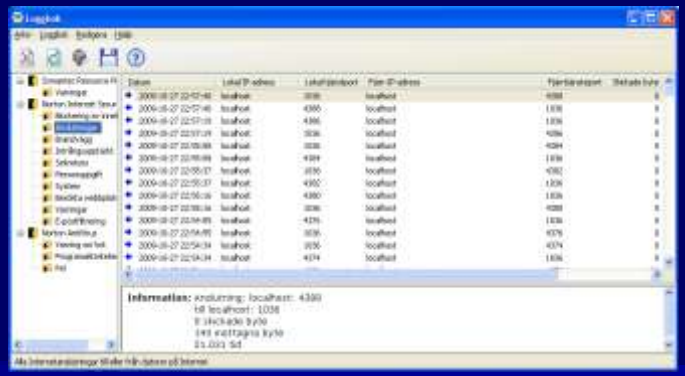
Problem som förekommer vid utredningar:

- Loggar inte alls
- Loggar alldeles för mycket

Typer av loggar:

- Loggar som man förstår
- Loggar som man tror att man förstår
- Loggar som man inte förstår

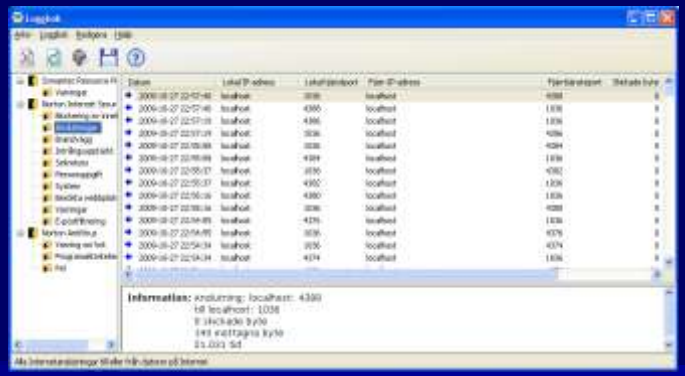
Loggar forts.



Beroende på vilken sorts verksamhet det rör

- Sjukhus
- Små företag
- Stora företag
- Myndigheter
- Privatpersoner

Loggar forts.



Andra problem:

- Bredband (trådlöst)
- ”Flatrate”
- IPRED lagen
- Ragga kunder

Lösningar:

- Utbilda teknikerna på att logga rätt och förstå loggarna
- Bra rutiner vid incidenthantering
- Någon form av datalagringsdirektiv

Polisanmälan – bevissäkringstips

- *Loggar* (oftast vid dataintrång)
  - IP-nummer + exakt tid (korrekt servertid?)
- Servrar, kunddatorer, om det går så försök (om möjligt) *byta ut den aktuella hårddisken eller låt någon "auktoriserad" firma låta göra speglingen men se till att de dokumenterar allt dom gör.*
- *En bra dokumentation* från målsägaren är A och O för att man skall kunna komma någon vart.
- *Ett nära samarbete* med någon inom förtaget är önskvärt.
- *En dialog under hela utredningen* mellan polis och företag är ett måste ex. information till pressen.

Kompletterande skriftlig anmälan

Fördelarna med att få en *kompletterande skriftlig anmälan* från målsägaren är de många typer av brott som har IT-brotts karaktär. En skriftlig anmälan om ett IT-relaterat brott underlättar för den kommande bedömningen av:

- Om något brott verkligen har begåtts
- Om förundersökning skall inledas
- Om det finns eller går att finna någon misstänkt för brottet.
- Varifrån brottet har begåtts rent fysiskt
- En utförligare, men enkel förklaring från målsägaren av det tekniska innehållet och av de eventuella facktermer som används för att händelseförloppet skall bli begripligt.
- I vissa fall kan målsägaren inneha viktiga uppgifter på datamedia, bestående av spår som gärningsmannen lämnat efter sig där han/hon har försökt undanröja sin identitet m.m.

Tack för mig !

Frågor ?

Paul Pintér
Länskriminalpolisen i Sthlms Län
LU/SIT
070-895 13 50