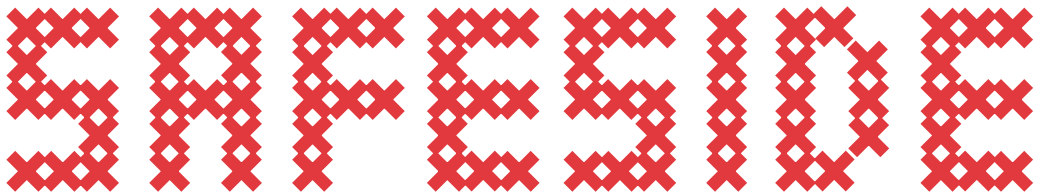

Rätt informationssäkerhet

Informationssäkerhetskonsult

niklas.eklov@safeside.se

IT-utredning ”Forensic”

Agenda

- Lagar, förordningar och olika kulturer
- Att tänka på innan
- Informell utredning
- Formel utredning
- Åtgärd
- Uppföljning
- Summering
- Frågor

IT-utredning ”Forensic”

Lagar, förordningar och olika kulturer

- Nationella lagar
- Internationella lagar
- Anställningsavtal
- Fackliga avtal
- Policys såsom Informationssäkerhetspolicy
- Olika företagskulturer
- Olika lokala kulturer

IT-utredning ”Forensic”

Att tänka på innan

- Vad har hänt?
- Vad skall bevisas?
- Avgränsningar på utredning
- Typ av utredning:
  - Informell (Intern)
  - Formell (Extern)
- Tekniska frågeställningar (mycket viktigt)
- Risker med utredning
- Mål med utredning

IT-utredning ”Forensic”

Informell utredning

- Hur skall utredning göras
  - Proaktivt
  - I efterhand
  - Finns krav på exakt spegelkopia på bevis?
- Dokumentation och protokollföring (mycket viktigt)
- Bevis finns på olika ställen
  - Nätverksresurser
  - På olika datorer och olika typer av elektroniskt media
  - I pappersform
  - I diverse loggar
  - Email och surftrafik

IT-utredning ”Forensic”

Informell utredning

- Allokering av resurser
- Val av tekniska verktyg
  - Kopieringsverktyg såsom Ghost eller vanlig filkopering (ändrar attribut på filer)
  - Kopieringsverktyg såsom Ilook och Encase (ändrar inte attribut på filer mm)
  - Nätverkssniffers och nätverkstrafikinspelare
  - Fysiska Keyloggers
  - Spyware
  - Diverse sökverktyg för sökning i uppsamlat data

IT-utredning ”Forensic”

Informell utredning

- Kontakt med olika funktioner internt
  - Diverse tekniska grupper såsom Nätverk, Mail och IT-Säkerhet
  - HR
  - Fackliga representanter
  - Säkerhetsansvariga
  - Ledning
- Kontakt med olika funktioner externt
  - Fack
  - Hjälp med revision och tolkning av data från extern resurs
  - Övriga

IT-utredning ”Forensic”

Formell utredning

- Hur skall utredning göras
  - Proaktivt
  - I efterhand
- Dokumentation och protokollföring (mycket viktigt)
- Bevis finns på olika ställen
  - Nätverksresurser
  - På olika datorer och olika typer av elektroniskt media
  - I pappersform
  - I diverse loggar
  - Email och surftrafik
  - Hos externa kontakter

IT-utredning ”Forensic”

Formell utredning:

- Allokering av resurser
  - Bör vara två eller fler resurser som jobbar ihop
- Val av tekniska verktyg (större krav på verktyg)
  - Kopieringsverktyg, här får endast Ilook och Encase användas (ändrar inte attribut på filer mm)
  - Special version av Knoppix kan också användas i nödfall
  - Nätverkssniffers och nätverkstrafikinspelare
  - Fysiska Keyloggers
  - Spyware
  - Cracking och hacking verktyg såsom L0hptcrck
  - Diverse sökverktyg för sökning i uppsamlat data

IT-utredning ”Forensic”

Formell utredning

- Kontakt med olika funktioner internt
  - Diverse tekniska grupper såsom Nätverk, Mail och IT-Säkerhet
  - HR
  - Fackliga representanter
  - Säkerhetsansvariga
  - Ledning
- Kontakt med olika funktioner externt
  - Fack
  - Hjälp med utredning och tolkning av data från extern resurs
  - Övriga såsom press och media
  - Polisiära myndigheter vid polisanmälan

IT-utredning ”Forensic”

Åtgärd

- Intern åtgärd
  - Rapportframtagande
  - Åtgärd > anställd
  - Åtgärd > teknisk
  - Fackliga förhandlingar
  - Uppsägning
  - Övrigt

IT-utredning ”Forensic”

Åtgärd

- Extern åtgärd
  - Rapportframtagande
  - Åtgärd > anställd
  - Åtgärd > teknisk
  - Fackliga förhandlingar
  - Uppsägning
  - Polisanmälan (offentlig handling)
  - Övrigt

IT-utredning ”Forensic”

Summering

- Viktigt att fundera först – agera sen
- Val av informell eller formell utredning
- Vad vill man uppnå med utredningen?
- Verktyg och kunskap är dyrt att underhålla, extern hjälp kan vara att föredra
- Ytterst viktigt: DOKUMENTERA OCH ÅTER DOKUMENTERA UTREDNINGEN!

Frågor?