Incidenthantering

Den börjar *inte* när Computer Sweden ringer!

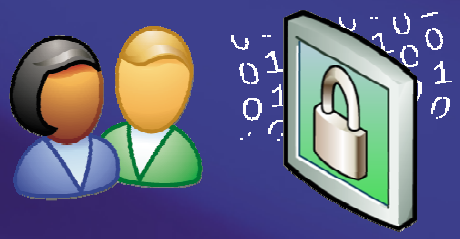
Michael Anderberg, CISSP
IT Pro Evangelist, Developer and Platform Evangelism Team
Blog: http://michaelanderberg.se

Microsoft AB

Microsoft TechNet

Du är i underläge… från början

- Den som attackerar väljer
  - Var
  - När
  - Hur
  - Varför
- Den som försvarar, måste alltid vara beredd på allt!



Om inte… din incidenthantering fungerar

- Man måste vara beredd
  - Otacksamt
  - Se igenom och inte luras av vargen kommer

- Konkreta punkter
  - Drabbas inte av panik
  - Var är säkerhetsplanen och hotbildsanalysen, är de uppdaterade
  - Finns rätt personal på rätt plats och med rätt förutsättningar
  - Identifiera orsaken inte symptomet
  - Isolera, analysera, informera, lös problemet och slutligen dra lärdom

Vad beror incidenterna på

- Ofta ej, eller felaktigt uppdaterad kod
  - Pratas oftast om operativsystemen
  - Men alla applikationer är lika viltiga
- Några varningsklockor
  - Körs koden som standard?
  - Körs koden med eleverade rättigheter eller som anonym?
  - Har koden nätverkskoppling?
  - Är koden öppen och synlig för vem som helst?
  - Påverkar koden privat eller känslig data?

Security Development Lifecycle

Microsoft Visual Studio

Kravspec	Design	Konstruktion/ kodning	Verifiering	Leverans	Uppföljning

Steg 0
- Medvetenhet
- Utbildning

Steg 1
- Projektstart

Steg 2
- Identifiera och följ design “Best Practices”

Steg 3
- Risk-identifiering

Steg 4
- Riskanalys

Steg 5
- Säkerhets-dokument-ation
- Verktyg
- “Best Practices” för kunder

Steg 6
- Säker kodning

Steg 7
- Säker testning

Steg 8
- Säkerhets-pushen

Steg 9
- “Final Security Review”

Steg 10
- Incident-hanterings-planering

Steg 11
- Leverans

Steg 12
- Säkerhets-incidents-hantering

Microsoft TechNet

Summering

- Var finns din dokumenterade process
- Är den uppdaterad
- Är den godkänd av VD

Microsoft®

Your potential. Our passion.™

Microsoft TechNet