Incidenthantering – brandsläckning eller oljesanering?

Sveriges IT-Incidentcentrum levererar konkurrensneutral IT-säkerhet för näringsliv och offentlig sektor

stefan.b.grinneby@sitic.se

Kort om presentatören, sbg

- På PTS / SITIC sedan 2004-08-16
  - Start som programvaru-/systemanalytiker (reverse engineer)
  - C Sitic sedan 070701
- 42 år, datavetare, pratig pragmatiker
  - 871202: {seismo,mcvax,cernvax}!enea!kuling!sbg (*geekpoäng: protokoll?*)
- Tar gärna frågor under presentationen
  - Korta svar kommer direkt
  - Längre svar tar vi under kaffepausen

Snabbfakta om SITIC

- Varför
  - Officiellt uppdrag till PTS 2002-05-30
  - Operationella sedan januari 2003
- Vad
  - Då : Utbilda, Varna, Koordinera, publicera Statistik
  - Nu : Svensk nationell/stats-CERT
- Med vem
  - Nationellt : ISPer, FRA, KBM, FMV, RPS, Verva, Försvaret, media
  - Internationellt : EGC, NCF, FIRST, TF-CSIRT, ENISA, IWWN

Incidenthantering - definition

- Incident
  - Oväntad och oönskad händelse i ett eller flera av de IT-system man på något sätt har ansvar för
- Hantering
  - Minimera eller helt förhindra den skada som verksamheten lider till följd av incidenten

Incidenthantering/Brandsläckning

- Ofta tacksamt att göra insats
  - Snabbt
  - Synligt
  - Alla förstår problemet
- Händelsestyrt
- När något händer är det lätt att gripas av panik
- Hög frekvens av ”små” incidenter
- Enklare fall kan hanteras av användare själv

Incidenthantering/Brandsläckning

- Snabb insats är avgörande – ha en plan!
- Lätt att öva många scenarion
- ”Lek med elden” är orsaken till många problem
  - ...så även ”dekorationer” som lämnas obevakade
- Farligt att ägna sig åt - det man bekämpar kan plötsligt skada en själv

Incidenthantering/Oljesanering

- Tröstlöst ibland
- Händelser av typen ”Får inte ske” inträffar
- Svårt att förstå konsekvenserna för hela miljön
- Många svårstyrda/-förståeliga hjälpmedel
- En del saker är nästan omöjliga att öva
- Hjälper att vara idealist med oändligt tålamod
  - …man vill gärna ha en hord av dem till hands

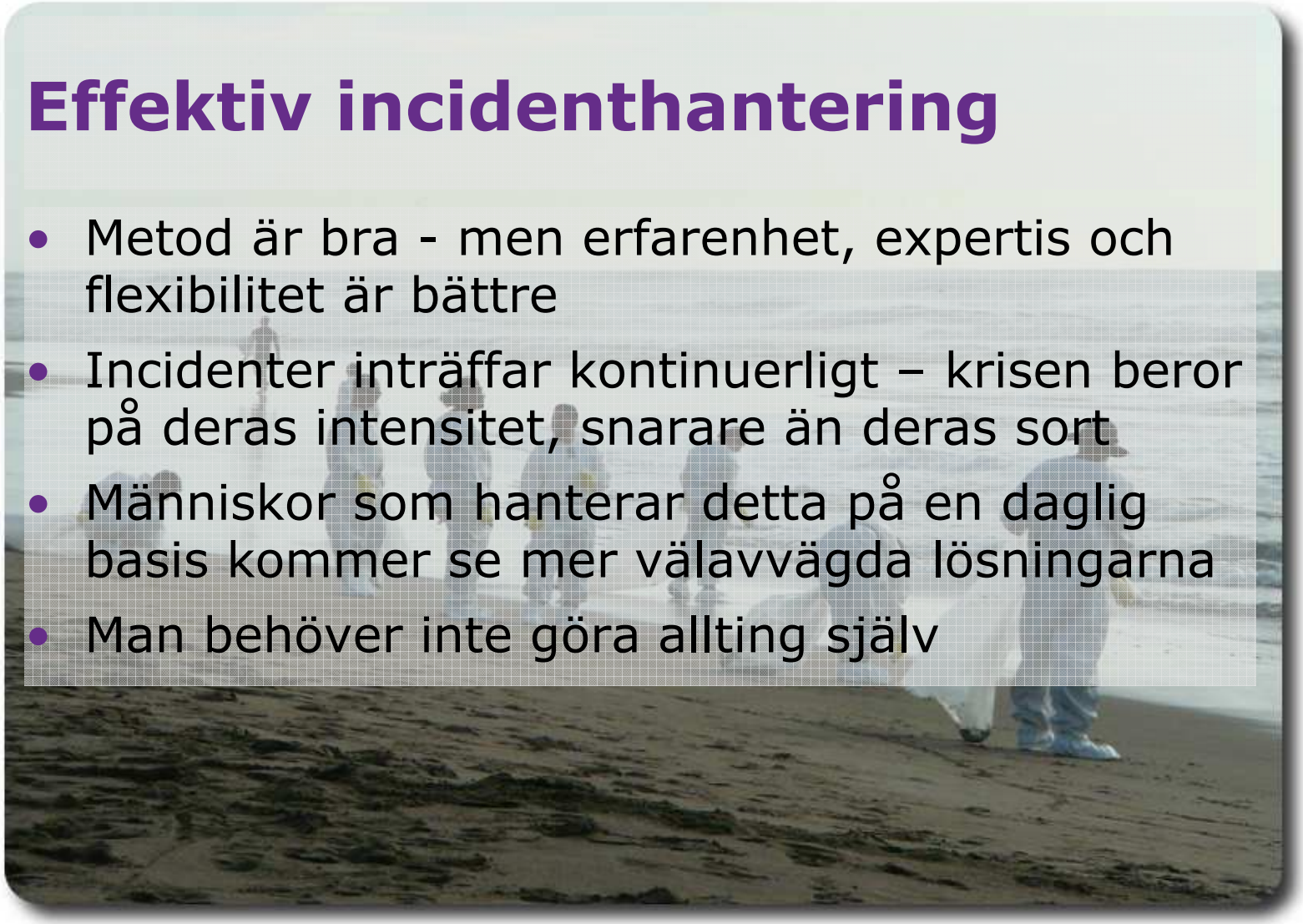
Incidenthantering förändras

- (Förr) De som vill ha uppmärksamhet ställer till en hel del problem
- (Nu) De som vill ha ekonomisk vinning ställer till en hel del problem

Det är en kombination!

- Det krävs djup kunskap
  - miljö, verktyg och egna förmågor
- Övning hjälper, men inte mot allt
- Ibland är ”mildra” det bästa man kan hoppas på
- Ju fler som är alerta och hjälper till desto bättre

Effektiv incidenthantering



- Metod är bra - men erfarenhet, expertis och flexibilitet är bättre
- Incidenter inträffar kontinuerligt – krisen beror på deras intensitet, snarare än deras sort
- Människor som hanterar detta på en daglig basis kommer se mer välavvägda lösningarna
- Man behöver inte göra allting själv

Hur gör Sitic det här?

- Handledning och kontaktskapande i alla stegen :

1. Avgöra – ” Är jag hackad? ”
2. Avbryta – ” Hur stoppa utan att stoppas? ”
3. Analysera – ” Hur gick det här till, egentligen? ”
4. Attributera – ” Vem var det som gjorde det här? ”
5. Återhämta – ” Var hade jag backupen nu igen...? ”
6. Avstyra – ” Aldrig mer samma sak! ”

Sitic, Sveriges IT-incidentcentrum

PTS / SITIC

Box 5398

102 49 Stockholm

Tel 08-678 57 99

Fax 08-678 55 05

sitic@sitic.se

www.sitic.se