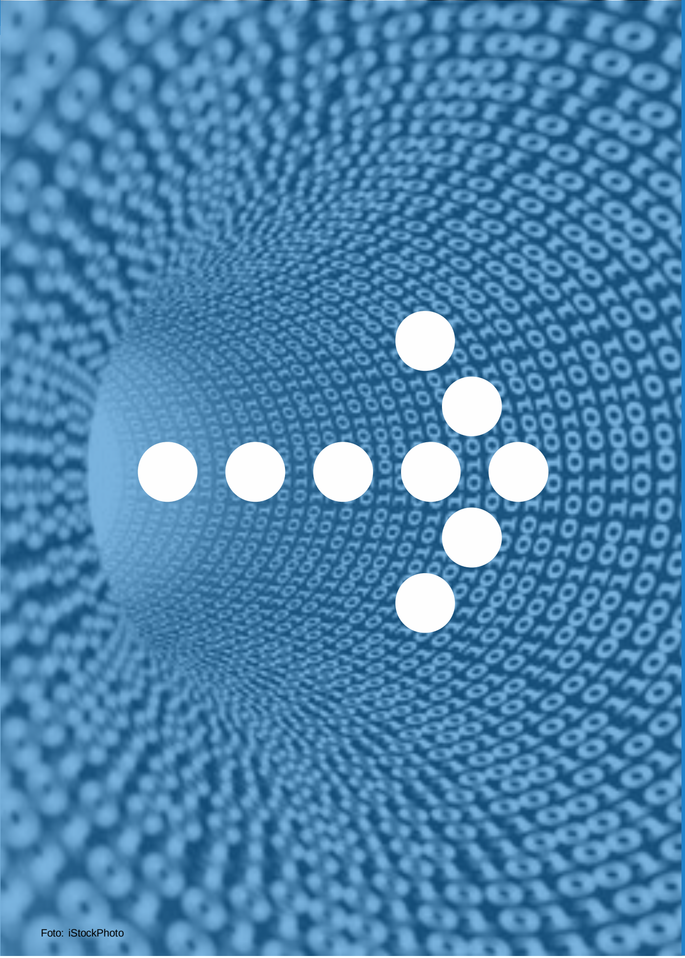


Foto: iStockPhoto

Pass 2 –
Metodik för Incidenthantering

Praktisk incidenthantering i industriella informations- och styrsystem

Myndigheten för
samhällsskydd
och beredskap

NCS3

FOI

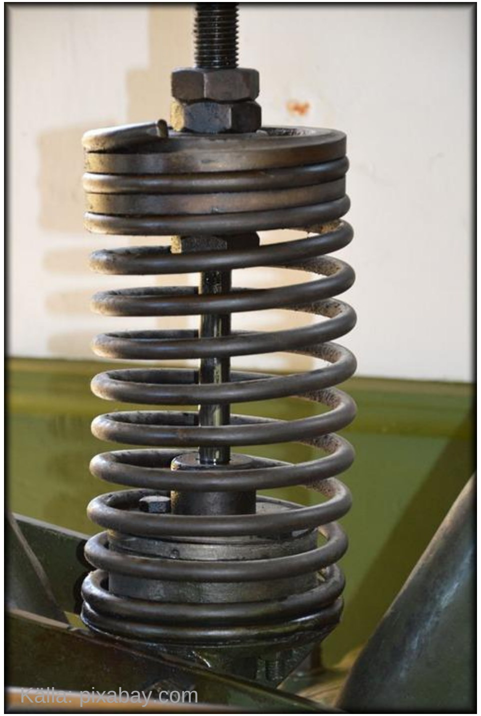
Varför incidenthantering?

https://www.businessinsider.com/heres-how-this-fake-photo-went-viral-and-tricked-the-internet-2014-5

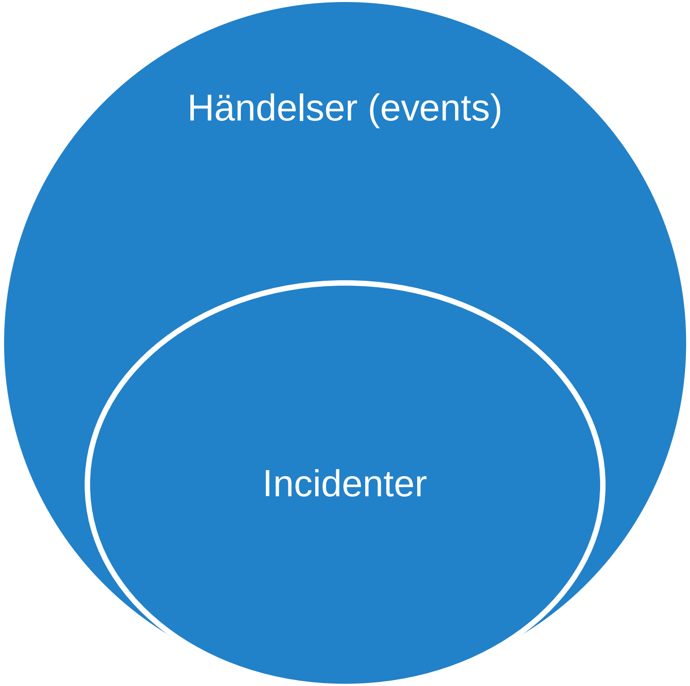
Motiv för incidenthantering

- För att säkerställa tillgång
  - till information
  - till system
- För att begränsa skador
- Lagkrav

- En silverkula mot problem!


Källa: pixabay.com

Begrepp – Händelser och incidenter



Händelse:

Ett observerbart skeende i it-systemen. En händelse behöver inte vara ett problem.

Incident:

En incident är en oplanerad och oönskad händelse som påverkar IT-system och verksamhet negativt.

I ITIL används incident synonymt med händelser.

Begrepp - Sverige

- Kontinuitetsplanering
  - planering och åtgärder för att en organisation ska kunna **fortsätta verksamheten** efter brand, naturkatastrof eller attentat (IDG, IT-ord)
- Kontinuitetshantering
  - handlar om att planera för att **upprätthålla sin verksamhet** på en tolerabel nivå (MSB)
- Incidenthantering
  - upptäckt, identifiering och rapportering av incidenter samt att man sätter in åtgärder enligt en förberedd plan (IDG.se, IT-ord)
- Katastrofberedskap
  - Förebyggande åtgärder för att en organisation ska kunna återuppta verksamheten (IDG.se, IT-ord)

Lagkrav

Myndigheter

- Förordning 2015:1052
  - Ansvar för att personalen får den **utbildning och övning** som behövs för att den ska kunna lösa sina uppgifter i samband med krissituationer.
- MSBFS 2020:7
  - Myndigheten ska, för att **säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser**
  - **Öva återställning av informationssystem** som är centrala för myndighetens förmåga att utföra sitt uppdrag
- MSBFS 2020:8
  - Typ av **incidenter som ska rapporteras**, att det ska ske **inom 6 timmar samt slutrapportering** inom 4 veckor.

Kommuner och regioner

- Lag (2006:544) och Förordning (2006:637)
  - Med extraordinär händelse avses i denna lag en sådan händelse som avviker från det normala, **innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner**
  - Kommuner och regioner ska ansvara för att förtroendevalda och anställd personal **får den utbildning och övning** som behövs för att de ska kunna lösa sina uppgifter vid extraordinära händelser i fredstid.
  - Kommunen och regionen ska vid en extraordinär händelse i fredstid ge den myndighet som regeringen bestämmer **lägesrapporter och information om händelseutvecklingen, tillståndet och den förväntade utvecklingen samt om vidtagna och planerade åtgärder.**

Leverantörer av samhällsviktiga tjänster

- Lag (2018:1174)
  - Leverantörer av samhällsviktiga tjänster **ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter** som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. **Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.**

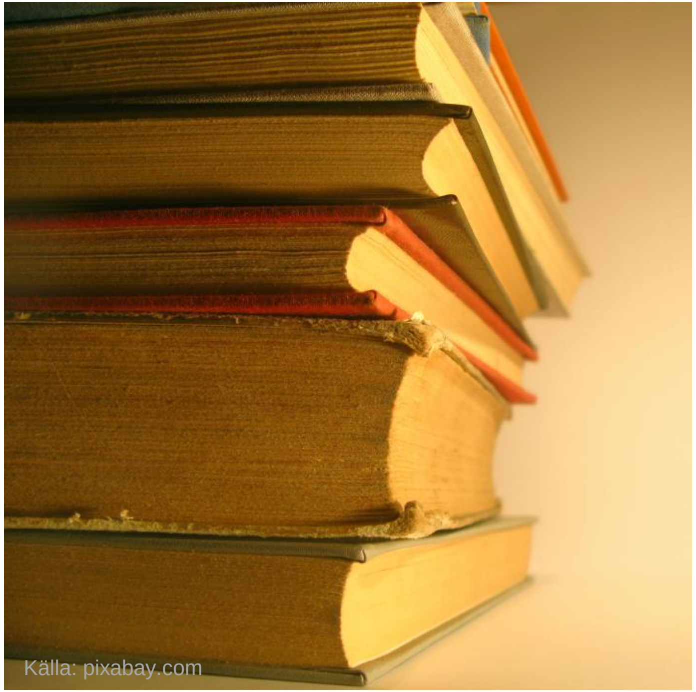
Leverantörer av samhällsviktiga tjänster

- MSBFS 2018:8
  - En leverantör ska ha **interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser** avseende informationshanteringen i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.
  - Efter avslutad incidenthantering ska leverantören **identifiera grundorsaker** till att incidenter och avvikelser inträffat samt **vidta åtgärder för att förhindra** att liknande incidenter och avvikelser inträffar på nytt.
  - **Arbetet ska dokumenteras**.

Metod

Standarder och guider

- Enisa
- MSB CERT - CIHSP
- ISO
- NIST
- NCSC
- MSB ICS
- SANS


Källa: pixabay.com

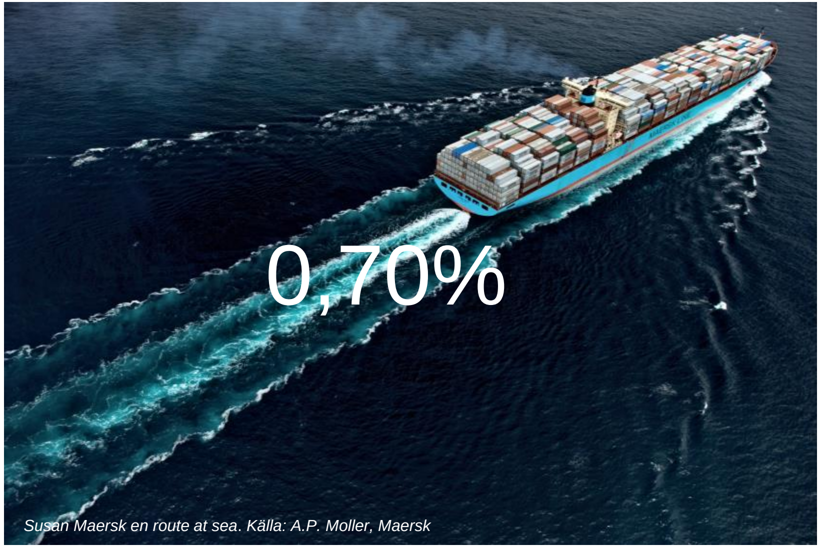
Metoder för incidenthantering

<table>
<tr><td>Enisa (2010)</td><td>(Incident management)</td><td>[1] Detection</td><td>[2] Triage</td><td>[3] Analysis</td><td>[4] Incident response</td><td>[5] Incident closure</td><td>[6] Post-analysis</td></tr>
<tr><td>CERT.SE (2012)</td><td>[1] Förebygga</td><td>[2] Identifiera</td><td colspan="2">[3] Begränsa</td><td>[4] Återställa</td><td colspan="2">[5] Erfarenheter</td></tr>
<tr><td>ISO (2012)</td><td>[1] Plan and Prepare</td><td>[2] Detection and Reporting</td><td colspan="2">[3] Assessment and Decision</td><td>[4] Responses</td><td colspan="2">[5] Lessons learnt</td></tr>
<tr><td>NIST (2012)</td><td>[1] Preparation</td><td>[2] Detection & Analysis</td><td colspan="3">[3] Containment, Eradication & Recovery</td><td colspan="2">[4] Post-Incident Activity</td></tr>
<tr><td>NCSC (2019)</td><td>[1] Prepare for incidents</td><td>[2] Identify what's happening</td><td colspan="3">[3] Resolve the incident</td><td>[4] Report incident to stakeholders</td><td>[5] Learn from the incident</td></tr>
<tr><td>MSB (2020)</td><td>[1] Förebygg</td><td>[2] Hantera - Identifiera</td><td colspan="2">[2] Hantera - Begränsa och städa</td><td>[2] Hantera - Återställa</td><td colspan="2">[4] Följ upp</td></tr>
<tr><td>SANS (2020)</td><td>[1] Preparation</td><td>[2] Identification</td><td>[3] Containment</td><td>[4] Eradication</td><td>[5] Recovery</td><td colspan="2">[6] Lessons Learned</td></tr>
<tr><td colspan="8"></td></tr>
<tr><td rowspan="2">Husets metod</td><td rowspan="2">Förebygg</td><td colspan="4">Hantera</td><td colspan="2" rowspan="2">Följ upp</td></tr>
<tr><td>Identifiera</td><td colspan="2">Begränsa</td><td>Återställ</td></tr>
</table>

Myndigheten för
samhällsskydd
och beredskap

NCS3

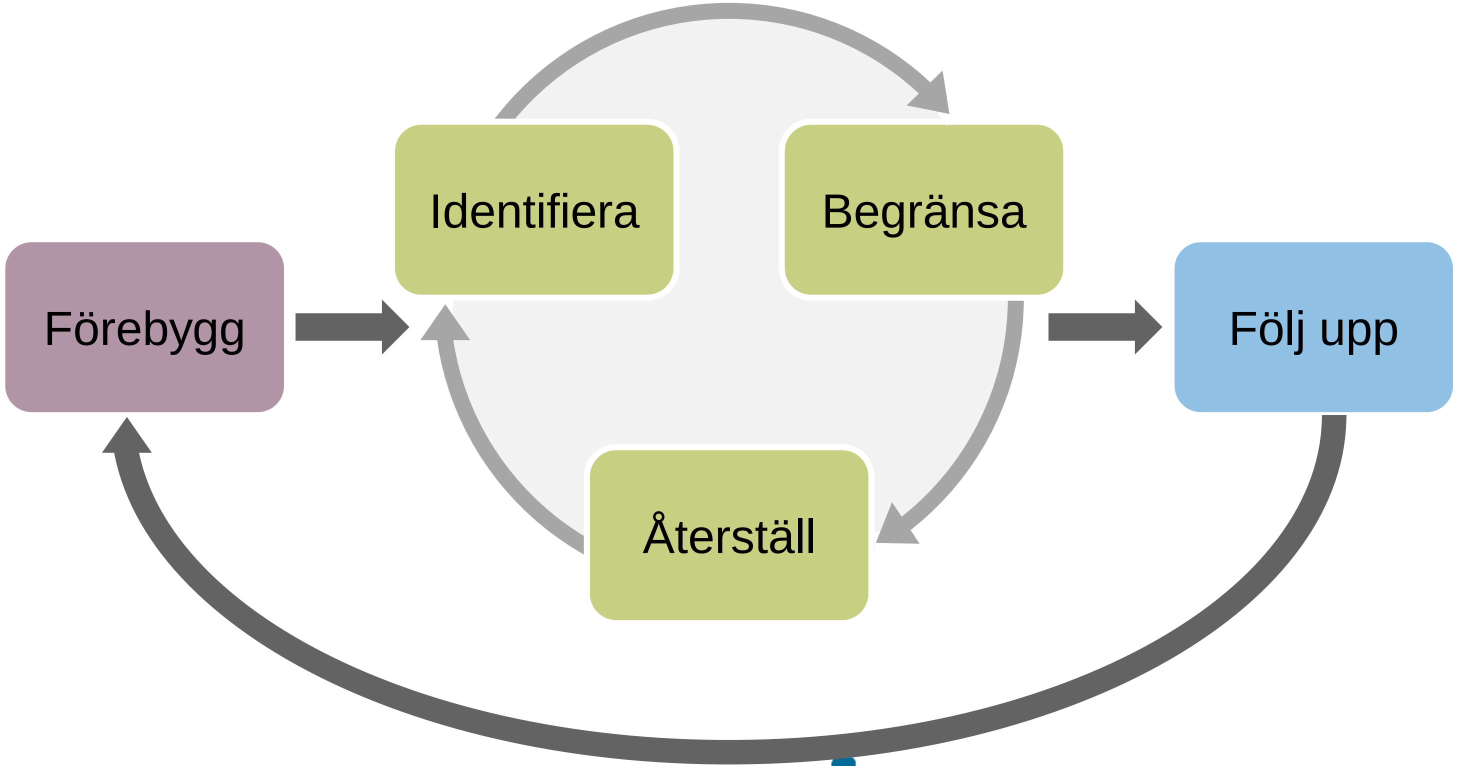
Men vilken är bäst?



Susan Maersk en route at sea. Källa: A.P. Moller, Maersk

Photo: Norsk Hydro

Incidenthanteringscykeln



Fördjupning Metodik

Förebygg – skapa goda förutsättningar

- Organisera
  - Utse ett team och se till att de har mandat
  - Välj en metod att luta er mot
  - Kontinuitetsplanera verksamheten
  - Kommunikationsplanera
- 1-10-60–regeln
  - 1 minut att identifiera
  - 10 minuter att analysera
  - 60 minuter att begränsa


Photo: Pixabay.com

Förebygg – skapa goda förutsättningar

- Teknik
  - Verktyg för teamet
  - Säker miljö och Skyddsåtgärder
  - Verktyg för detektion
- Testa och öva
- ”Beredskap” att övergå i incidentläge
- Rapportering och efterarbete

Photo: Pixabay.com

Hantera – identifiera

- Övervakningsverktyg
  - Avvikelser från det normala
  - Sammanställd data
- Observanta medarbetare
- Analysera vad som händer
- Bedöm vad som kan påverkas
- Planera åtgärder


Photo: Pixabay.com

Hantera – begränsa

- Prioritera åtgärder och resurser
- Isolera eller stäng av system
- Stäng av tjänster
- Begränsa nätverkstrafik
- Byt lösenord
- Uppdatera system
- Fortsätt lyssna


Photo: Pixabay.com

Hantera – återställ

- Under eller efter?
- Enligt återställningsplan
- Säkerställ att allt är borta
- Prioritera rätt system
- Kontrollera information och system
- Kontrollera skyddsåtgärder
- Incidentrapportera


Photo: Pixabay.com

Följ upp – lär för framtiden

- Utvärdera och dokumentera
  - – Följ faserna i metoden
- Prioriteras inom någon vecka
- Åtgärda brister som upptäckts
- Utveckla nya detektionsmetoder
- Kommunicera resultatet

Photo: Pixabay.com

Sammanfattning

- Man lyckas bättre om man är förberedd!
- Välj en metod att följa
  - Förebygg, Hantera och följ upp
  - Cykliskt arbete
- Det finns ingen evidens på vilken metod som är bäst
- Öva och pröva, inspireras av andra