Erfarenheter från att vara utsatt för ett allvarligt intrång i it-miljön – tips och trick i hanteringen

2016-09-14, Jan-Olof Andersson, Polismyndigheten

Polisen

Upplägg

- Tre händelser
- Tips kring hantering
- Allmänt om incidenthantering
- Sammanfattning

Tre händelser för att sätta ramen

- Tre händelser som beskriver:
  - Skadlig kod
  - Dåliga rutiner och tillit till andra
  - Intrång i it-miljö
- Kodnamn
- Medialt och internt kända fall

ADA 2013

Information från CERT-SE om att Polisens nät genererade trafik från s.k. trojaner.

- ”Surf nätet” konstaterades innehålla minst 8 smittade datorer med s.k. ”Remote Control” trojaner, minst en PC ingick i ett s.k. Botnet.
- Det kan konstateras att:
  - Polisens datorer och verksamhet som används på röda nätet har utsatts för brott.
  - Polisens it- miljö har gett en annan part förutsättningar att begå brott.
  - Polisens datorer har använts för att medverka till att andra personer och organisationers verksamhet utsatts för brott.
- Skadekostnad okänd men uppgår till flera miljoner.

Trojaner **kan** användas för att:

- Läsa och kopiera information som finns på datorn eller som skickas till och från datorn.
- Avlyssna omgivningen genom datorns mikrofon, ta bilder med datorns kamera och ta bilder av de programfönster som är öppna
- Dolt fjärrstyra datorn från okänd plats och land
- Sprida sig eller sabotera och utföra intrång mot andra datorer inom Polisen eller datorer på Internet

Polisen

Fotostationer 2012

- Vid uppdatering av fotostationerna för passystemet använde Polisens externa leverantör USB-minnen. Via dessa minnen smittades fotostationerna med skadlig kod.

  - Kostnad för utredning och hantering beräknas av verksamhetsskyddsenheten till ca 1.5 miljoner kr

Josef Pelle är passhandläggare i City polismästardistrikt.
Foto: Jimmy Gustafsson

Morgan 2012

I mars 2012 hade en extern leverantör intrång i sitt it- system. Leverantören tillhandahåller it-lösning som Polisens tjänsteleverantör använder.

En stor mängd data, bland annat personuppgifter, skyddade personuppgifter och annan känslig information, kopierades av gärningsmannen.

Det finns inget som tyder på att personuppgifter förändrats även om detta var möjligt för gärningsmannen att göra.

Skadekostnad ?……

måndag 2013-05-20

Så ska attackerna mot myndigheter och banker ha gått till

Attacken
1 Det attackerade systemet innehöll sårbarheter som var okända för Nordea. Svartholm Warg misstänks ha listat ut krypterade lösenord i systemet, samt lagt upp nya egna konton som kunde utföra transaktionerna.

Bevisen
2 Polisen har hittat bevis i de beslagtagna datorerna. Åklagaren kommer även att lägga fram chattloggar från Hack.se som bevis. Chattloggarna påstås visa konversationer mellan 36-åringen och Svartholm Warg.

Spåren
3 Den åtalade 36-åringen misstänks ha sopat igen sina spår och utfört attackerna via sina grannars trådlösa nät. Han hackade 100 grannar och säger själv i chattar på Hack.se att han även avlyssnade deras IP-telefoni, något som polisen inte funnit bevis för.

Musiken
4 I hacket mot Logica finns referenser till syntbandet Front 242: "Master, I'm so glad to feel your presence, but you don't seem to share my ambitions, I rely upon you to break the scilenacee", står i källkoden till programmet som manipulerar behörighetskontrollen.

Polisen
5 Hackarna fick via dataintrånget mot Logica tillgång till Polisens personsystem. I det systemet kunde de bland annat söka fram registreringsnumret till Polisens samtliga civilbilar i Sverige. De laddade också hem en databas med uppgifter om 20 000 poliser.

Kan ha varit största intrånget någonsin

Hackare. Med hjälp av Hollywoodadvokaten

Metro 13-05-20

Åklagaren: Ingen vet hur mycket som stulits

Bara hackarna själva vet hur mycket som stulits, och från vem. FOTO: SCANPIX

Polisen, Skatteverket, Kronofogden och Nordea blev alla av med känslig information. Men ingen, förutom hackarna, vet exakt vad och hur mycket som stulits – och från vem.

Under dataintrången har hackarna skapat så kallade bakdörrar, för att ha ständig åtkomst till systemen.

–Uppgifter som går ut via bakdörrar är svåra att spåra. Det finns en mängd omständigheter som gör att det inte går att veta exakt hur mycket data som hämtats ut, eftersom de haft fullständig tillgång till systemet, säger kammaråklagare Henrik Olin.

Av chattloggarna som polisen misstänker är mellan Svartholm Warg och 36-åringen, har en fil med ftp-adresser delats. Det första dataintrånget mot Logica skedde just via en filöverföringsförbindelse från riksdagen.

– Det finns saker som leder mot andra eventuellt drabbade än Logica och Nordea. Men det är inget som utredningen har kunnat vederlägga, säger Henrik Olin.

– Det finns indikationer i chatterna på att man haft avsikt att angripa fler, säger kammaråklagaren.

FRIDA SUNDKVIST

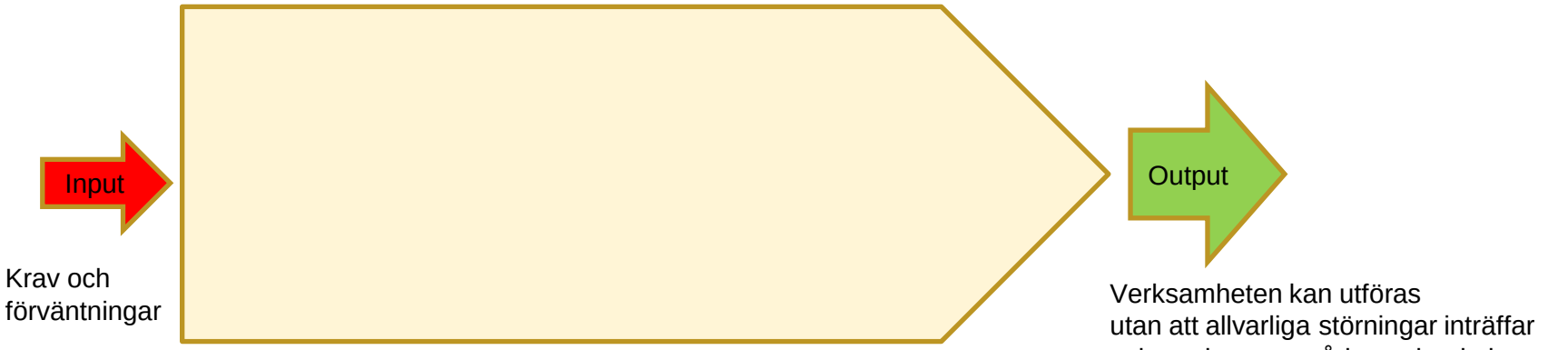
TIPS & TRICKS

Ni måste vara förberedda före det händer!

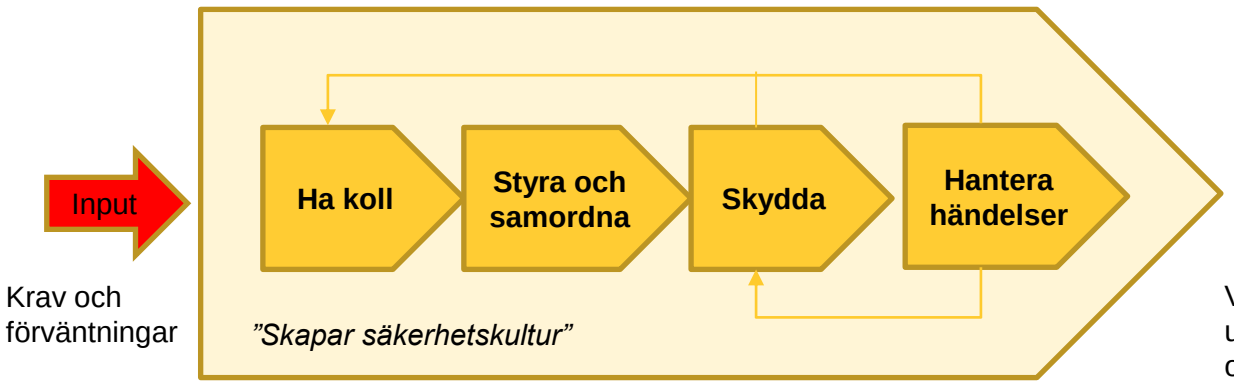
Polisen

Informationssäkerhetsprocessen

- Mål:
  - Verksamhetens information ska värderas, skyddas och finnas tillgänglig för den som är behörig när den behövs.



Har organisationen någon process att arbeta efter?



Krav och förväntningar

Verksamheten kan utföras utan att allvarliga störningar inträffar och uppkommer sådana ska de kunna hanteras.

Delprocessernas underprocesser

Ha koll	Styra och samordna	Skydda	Hantera händelser
•**Identifiera risker** •**Omvärldsanalys** •Samverkan •Dimensionerande hotbild •Säkerhetsanalys •**Gemensam lägesbild/lägesuppfattning**	•**Riskhantering** •Planering/budget •Resurssäkring •Uppföljning •Granskningar/kontroller •Mätning •Utbildningsplanering •**Ledningens genomgång** •Kompetensanalys •Kommunikation •Ärendehantering •Utveckling/Metodutveckling •Upprätta säkerhetsplan	•Framtagande av regler •Framtagande och införande av säkerhetsåtgärder •**Kontroll av nivån** •Övervakning/mätning •Stöd/rådgivning •Information/utbildning •Avvikelsehantering •SUA •**Kontinuitetsplanering** •Säkerhets- och skyddssamtal •Säkerhetsprövning	•**Incidenthantering** •**Krishantering**

Händelse

- Gemensam lägesbild
  - vad har hänt?
  - vad vet vi?
  - vad vill vi veta?
  - vem vet det vi veta?
  - när måste vi veta?
- Team för åtgärder
  - Dela in roller:
    - Leda,
    - Dokumentera,
    - Samverkan,
    - Kommunikation,
    - Specialister för hantering plattform, nätverk, it-säkerhet,
    - Stöd (mat, övernattning)

Polisiär stab:

1. Personaltjänst
2. Underrättelser
3. Operativ samordning
4. Logistik
5. Planering och strategisk insatsanalys
6. Tekniska ledningssystem
7. Kommunikation
8. Ekonomi och juridik
9. Samverkan

Händelse fortsättning

- Polisanmälan
  - Är det ett brott eller tekniskt fel?
  - Polisanmälan (Tvättad incidentrapport)
    - Skriv en bilaga med detaljer
    - Finns mer information att tillgå som kan vara av värde för fortsatt utredning (ex loggar, inspelad servertrafik, mailkonton etc.).
  - Utse kontaktperson i verksamhet
- Rapportera till MSB
  - Är det en händelse som omfattas av förskriften?
- Media hantering
  - Förhållningssätt
  - Förbered för det värsta

It-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ……

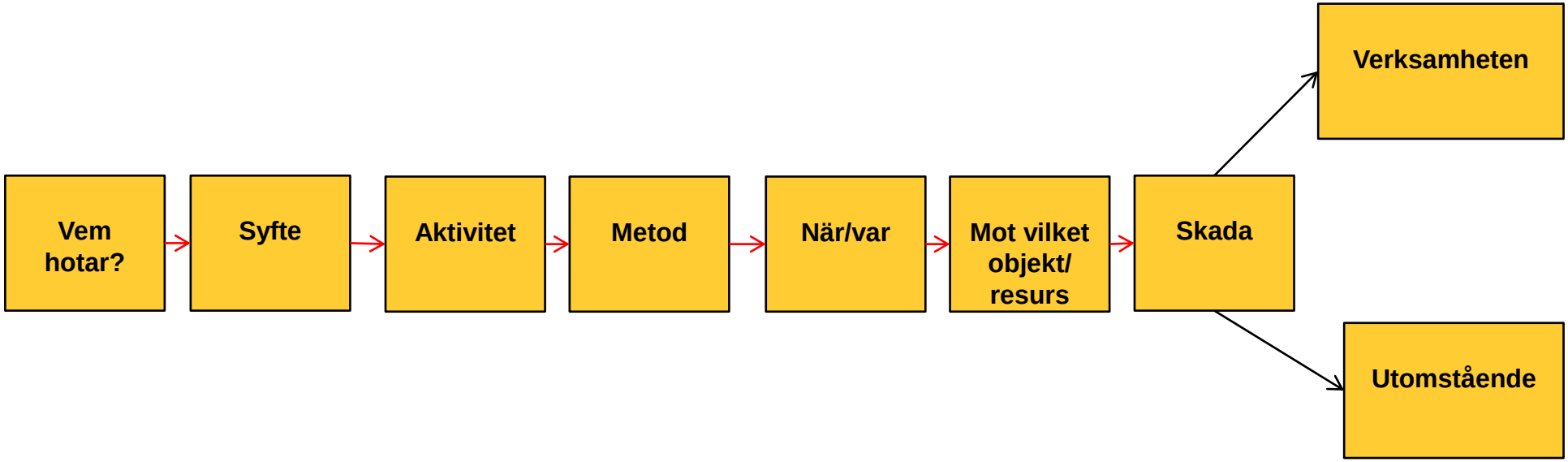
Händelse fortsättning

- Arbetssätt
  - Alla ska veta läget hela tiden…
  - Dokumentation/loggning (denna bör uppdateras 3 ggr/dygn)
    1. Händelsebeskrivning
    2. Omfattning
    3. Vidtagna åtgärder
    4. Huvudansvarig och aktörer inom verksamheten
    5. Övriga aktörer
    6. Resursinformation
    7. Utveckling/omfall
    8. Konsekvenser
    9. Planerade åtgärder/Inriktning/Prioritering/Behov av resurser och beslut
    10. Hur/var fås ytterligare information
    11. Samverkanbehov
    12. Övriga/egna synpunkter
    13. Mediabild
  - Uthållighet (gå i skift)
  - Teknik för att dela information, krypterade kommunikationskanaler

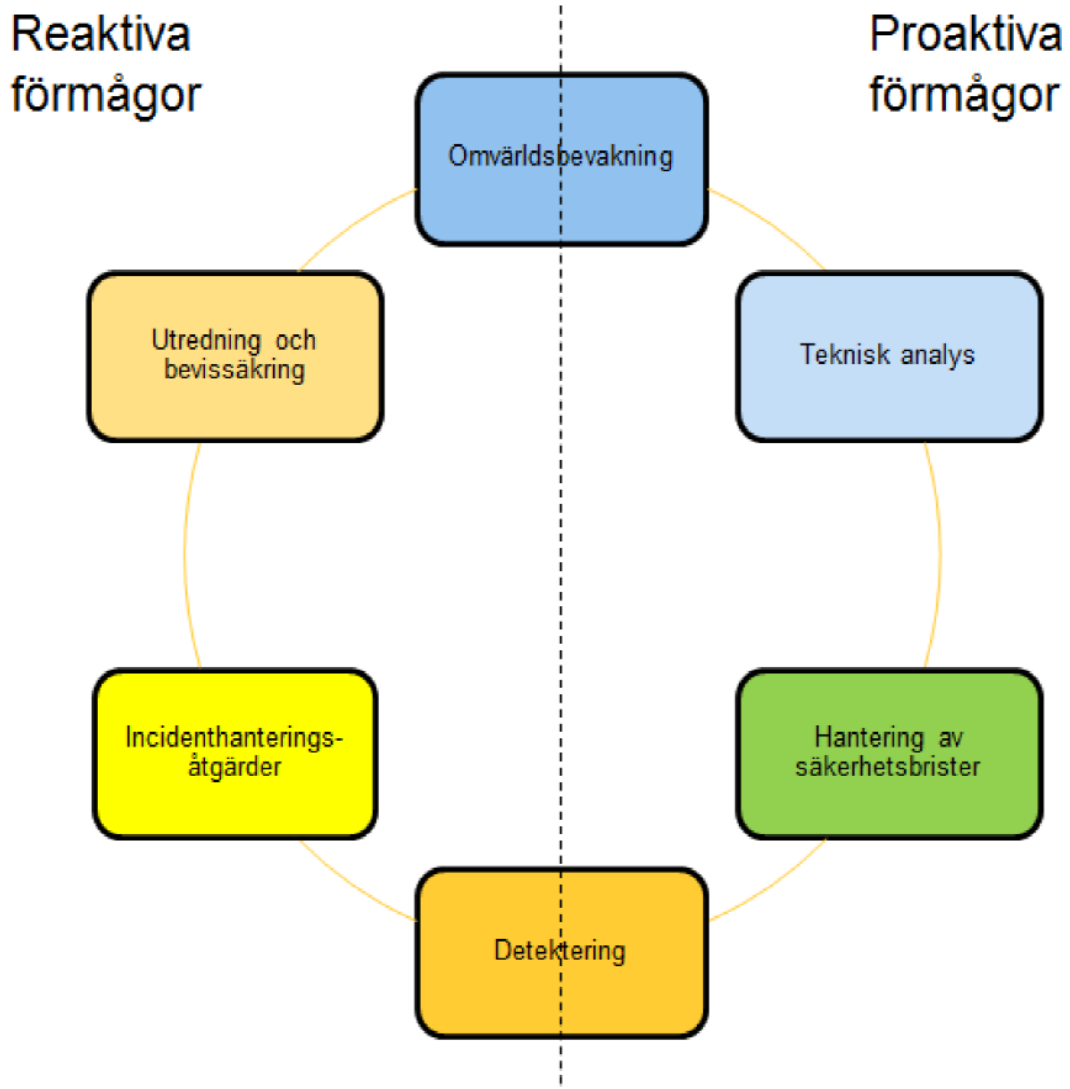
Händelse fortsättning

- Kommunikation med ledning
  - Vad vill jag de ska känna, veta och göra?
  - Hur ska man löpande hålla dem informerade?
- Eskalering var beredd på det värsta
  - Detta beror ofta på skadan….
  - Formellt och informellt…

Hotbildsanalys eller beskrivning av en händelse



Incidenthanteringprocessen



Polise

Steg i hantering av incidenter

- Planera och förbereda
  - organisation, process, rapporteringsvägar m.m.
- Identifiera och rapportera
  - vem och hur
- Ta emot, klassificera och analysera
  - utred och bedöm skadan, orsaken, prioritera
- Hantera
  - kommunicera, begränsa, återställ
- Stäng och återkoppla
  - dokumentera, informera, bevaka
- Utvärdera/Lärdom
  - vad gick bra och vad gick fel, utred orsaken
  - statistik (typ, volym, kostnad)

Översikt tre olika incidenttyper

Polisen

IT-incident

Definition: Avvikelse från normal IT-drift. En IT-incident kan eskalera till en IT-säkerhetsincident och/eller verksamhetsskyddsincident.

Omfattning: Polisens IT-miljö (IT-system/applikationer, fast/mobil telefoni, nätverk)

Anmälan av incident: *Via* Webbanmälan i ARS på Intrapolis eller Servicedesk 020-666 999

Verktyg: ARS
Ansvar: IT-drift och infrastrukturförvaltning och/eller Utveckling och applikationsförvaltning

IT-säkerhetsincident

***Definition*:** IT-relaterad händelse som hotar Polisens it-system och information.
En IT-säkerhetsincident kan bli så allvarlig att den eskalerar till en verksamhetsskyddsincident.

***Omfattning*:** Polisens IT-miljö: IT-system/applikationer, fast/mobil telefoni, nätverk.

Anmälan av incident: *Via* ARS eller e-post till cert.rps@polisen.se

Verktyg: ARS och POINT
Ansvar: IT-säkerhet (CERT-funktionen)

Verksamhetsskyddsincident

***Definition*:** Incident som påverkar säkerheten för information, medarbetare, utrustning eller lokaler på ett negativt sätt.

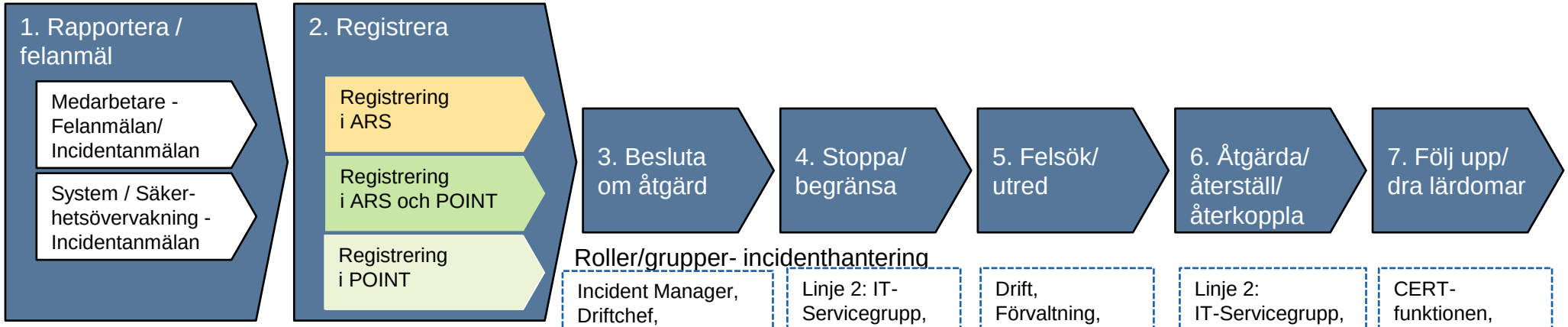
***Omfattning*:** Informationssäkerhet, egendomsskydd, medarbetarskydd inom Polisen.

Anmälan av incident: *Via* Webbanmälan i POINT på Intrapolis

Verktyg: POINT
***Ansvar*:** RPC kansli för nationella avdelningar eller Region kansli för regionerna.

Ska ses som exempel!

Hantering av incidenter hos Polisen



Rapporteringsalternativ:

- Webb-anmälan via Intrapolis
- Servicedesk telefon:020-666 999
- IT-säkerhet (CERT-funktionen) för IT-säkerhetsincident

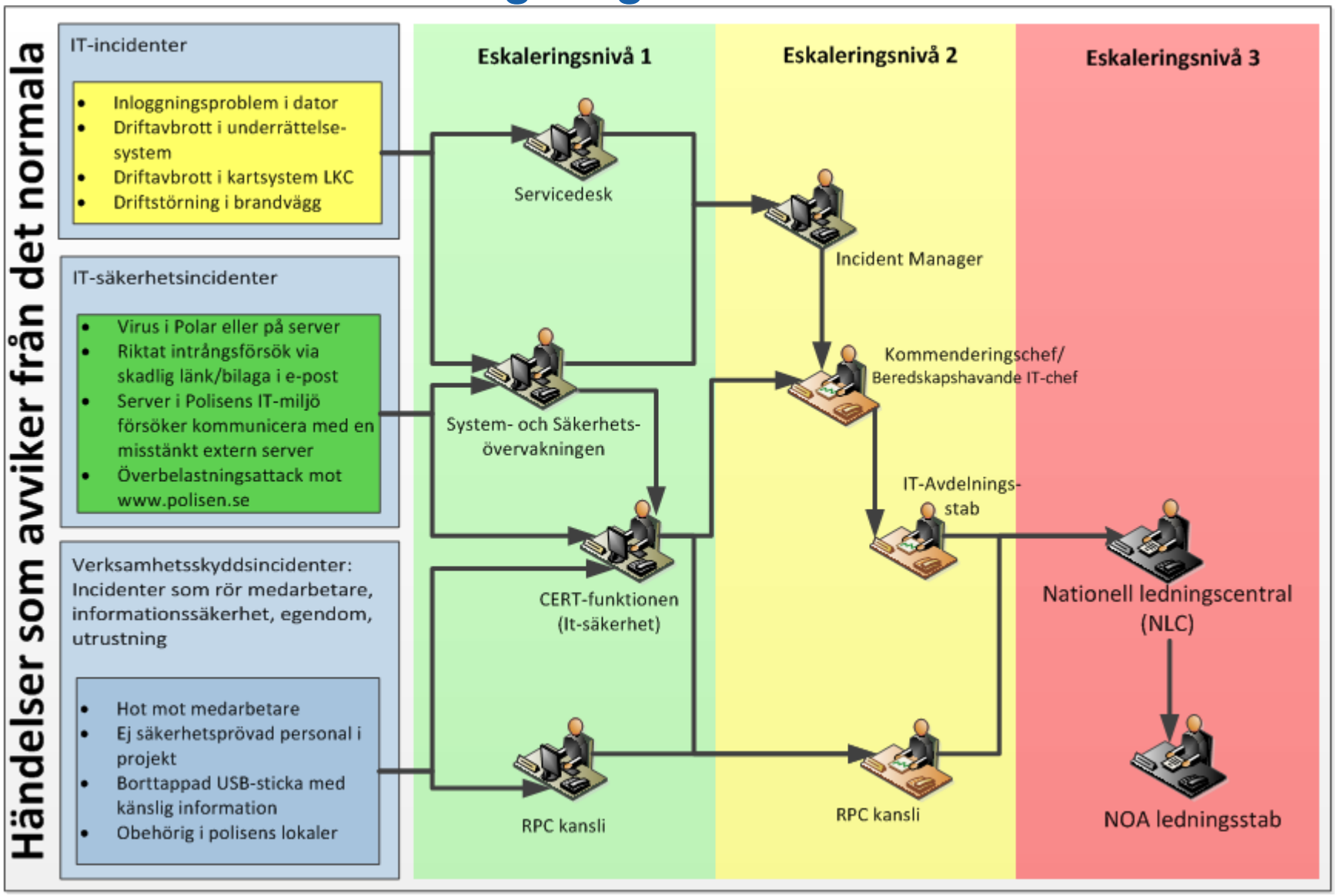
Hantering av IT- Incident

Hantering av IT-säkerhetsincident

Hantering av verksamhetsskyddsincident

Ska ses som exempel!

Polisens eskaleringsvägar och nivåer vid incidenter

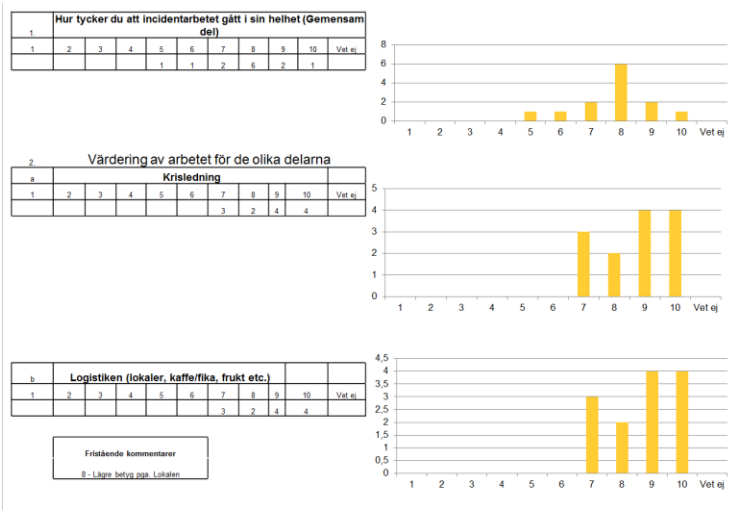


Polisen

Ska ses som exempel!

Glöm inte bort - Lärdomar

Förbättra förmågan att förhindra liknande incidenter i framtiden



- Förberett enkätverktyg i förväg
- Uppföljningsmöten så snart som möjligt
- Genomgång
  - Vad gick bra, vad gick fel
  - Orsaken till incidenten
- Finns det behov av justeringar?
  - Utrustning, ekonomi, personal, kommunikation
- Återkoppla på alla nivåer

Sammanfattning

- Det är inte om utan när och hur hårt ni blir träffade!
- Var förberedd för att kunna hantera händelsen
- Var beredd på att det är inte det ni tror som kommer att inträffa
- Omge dig med rätt medarbetare eller konsulter
- Lär dig av det som inträffat och kommunicera
- Utgå från standarder:
  - SS-ISO/IEC 27001:2013 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav
  - SS-ISO/IEC 27002:2013 Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder
  - SS-ISO/IEC 27035:2011Informationsteknik – Säkerhetstekniker – Styrning och hantering av informationssäkerhetsincidenter del 1-3

Frågor

”Förr i tiden hade vi Himmel och Helvete. Nu har en ny värld skapats däremellan - Cyberspace!”

Lars Nylén, tidigare chef för Rikskriminalen

För kontakt: jan-olof.andersson@polisen.se