UiO IN2120 høst 2019

Incident Response and Forensics

Frode Lilledahl

26.09.2019

sopra steria

whoami

- Fungerende Sikkerhetssjef (CISO) for Sopra Steria Operations
- Jobber for tiden med etablering av Security Operations Center
- Tidligere IRT leder og Incident Handler i DNB

frode.lilledahl@soprasteria.com

Disclaimer

- Basert på mine erfaringer og mine meninger
- Hva jeg har sett fungere i de situasjoner jeg har vært i
- Andre tilnærminger kan fungere like godt
- Utfyllende, men ikke dekkende for pensumlitteraturen

Agenda

- Incident Response
  - Hvorfor incident response?
  - Begrep
  - Forberedelser
  - Faser i håndtering av en sikkerhetshendelse
  - Debrief/læring
  - Organisering
  - Øvelser
  - SOC etablering og tjenestespekter
- Forensics
  - Hva er digital forensics
  - Computer forensics vs network forensics
  - Chain of custody (notoritet)
- Oppgave (case)

Hvorfor Incident Response?

Hvorfor Incident Response?

Hendelser vil skje, men vi kan forberede oss

- Planlegge for det uønskede
- Redusere negativ konsekvens

Incident Response vs. Incident Management

Incident Management

Reaktive prosesser
(Incident Response)

Prosesser for hvordan agere når en hendelse er oppstått

Proaktive prosesser

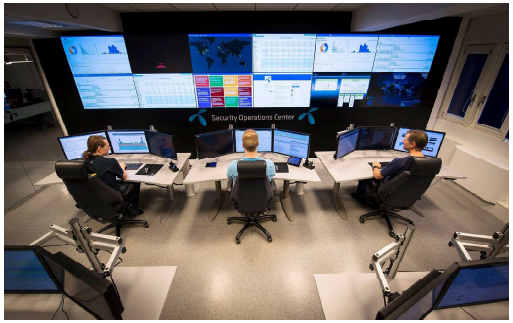
Prosesser for å være i stand til å oppdage hendelser:

- Monitorering og deteksjon
- Analyse (SIEM)
- Brukeropplæring

Noen enkle begrep

Kilde: www.edts.com

SOC vs IRT



Forberedelser

Forberedelser

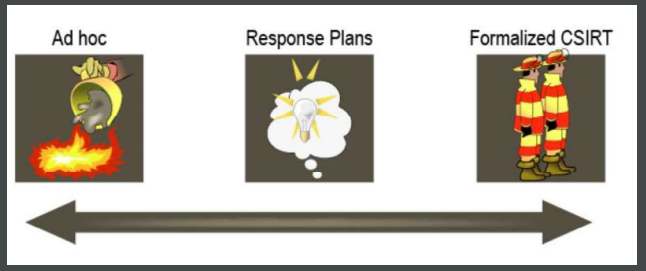
- Ledelsesstøtte
- Mandat
- Fullmakter
- Planer
- Organisasjon
- Verktøy

Range of CSIRT services

Reactive Services	Proactive Services	Security Quality Management Services
+ Alerts and Warnings	O Announcements	✓ Risk Analysis
+ Incident Handling – Incident analysis – Incident response on site – Incident response support – Incident response coordination	O Technology Watch O Security Audit or Assessments O Configuration & Maintenance of Security Tools, Applications, & Infrastructures O Development of Security Tools O Intrusion Detection Services O Security-Related Information Dissemination	✓ Business Continuity & Disaster Recovery Planning ✓ Security Consulting ✓ Awareness Building ✓ Education/Training ✓ Product Evaluation or Certification
+ Vulnerability Handling – Vulnerability analysis – Vulnerability response – Vulnerability response coordination		
+ Artifact Handling – Artifact analysis – Artifact response – Artifact response coordination		

Kilde: cert.org

Modenhet



Hendelseshåndtering – Slik det kan være


Pust ut

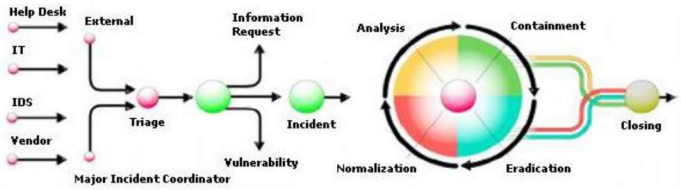
Noe skjer!


SYSTEM FAILURE


Få dritten igang igjen

Alle mann til pumpene

Faser i håndtering av en sikkerhetshendelse



Faser i håndtering av en sikkerhetshendelse

- Triage
  - Hva har skjedd
  - Samle fakta
  - Vurdere alvorlighet
  - Interessenter
  - Identifisere false positives
  - OBS: Loggføring
  - Statusrapportering
- Analyse
  - Innsamlig
  - Loggfiler
  - Malware
  - System
  - Nettverk
  - Tidslinje

Kategorisering – eksempel

Kategori	Forklaring
Lavt	Hendelsen som kan medføre at informasjon eller informasjonssystemer som er av lav betydning, kommer på avveie, blir korrupt/endret eller midlertidig utilgjengelig. Mindre brudd på/avvik fra regler og policyer, som ikke medfører anmerkninger fra tilsynsorganer eller andre sanksjoner.
Medium	Hendelsen kan medføre at informasjon eller informasjonssystemer som er av moderat betydning, kommer på avveie, blir korrupt/endret, eller midlertidig utilgjengelig. Moderat brudd på / avvik fra regler og policyer, som kan medfører anmerkning fra tilsynsorganer, men ingen sanksjoner.
Alvorlig	Hendelsen kan medføre at informasjon som er av høy betydning, kommer på avveie eller blir korrupt/endret. Hendelser som forårsaker langvarig stans i informasjonssystemer og/eller leveranser. Alvorlige brudd på / avvik fra regler og policyer som kan medfører anmerkning fra tilsynsorganer, varsel om mulige sanksjoner. Negative oppslag i media over flere dager, stort engasjement fra byrådet/bystyret. Sterk kritikk fra kommunerevisjonen. Eksempel: Personopplysninger på avveie
Svært alvorlig	Hendelsen kan medføre at informasjon eller informasjonssystemer som er av vesentlig betydning, kommer på avveie, blir korrupt/endret eller blir utilgjengelige. Lovbrudd eller svært alvorlig brudd på / avvik fra regler og policyer som kan medfører straffereaksjoner. Langvarige og svært negative oppslag i media, svært alvorlige konsekvenser. Eksempel: Store mengder med personopplysninger eller helseopplysninger kommer på avveie

Standard Operating Procedures (SOP)

C:\Users\pkh>netstat –an

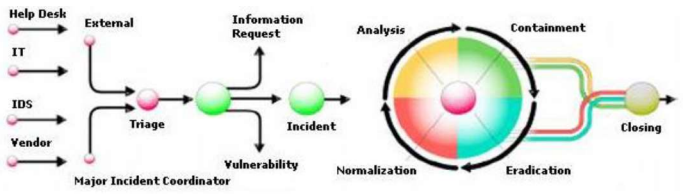
In the output look for patterns that show multiple connections from certain ip address(s) connecting to contiguous ports on server ip(s) and connections are timing out. In real scenario you will see hundreds (if not thousands) of this type of connections.

```
TCP    192.168.2.104:00       216.35.50.65:60973 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60974 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60975 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60976 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60977 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60978 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60979 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60980 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60981 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60982 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60983 TIME_WAIT
TCP    192.168.2.104:00       216.35.50.65:60984 TIME_WAIT
```

2.1.1.1 Enfo

- If the n
  - Block/blacklist attacker's source ip addresses on edge firewall/router.
- **If the number of attacker's ip addresses are too large but come from a certain geolocation(s):**
  - Block/blacklist attackers based on geolocation(s) the attack is originating from. This can be done on most NGFWs and advanced gateway routers.

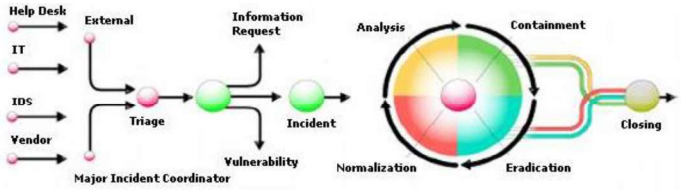
Faser i håndtering av en sikkerhetshendelse



Faser i håndtering av en sikkerhetshendelse

- Containment
  - Isolere hendelsen og hindre videre spredning
  - Isolere berørte systemer
  - Ta ned berørte tjenester
- Eradictation
  - Fjerne årsaken til hendelsen
  - Identifisere og fjerne sårbarhet
  - Oppgradere/patche systemet
  - Forensics

Faser i håndtering av en sikkerhetshendelse



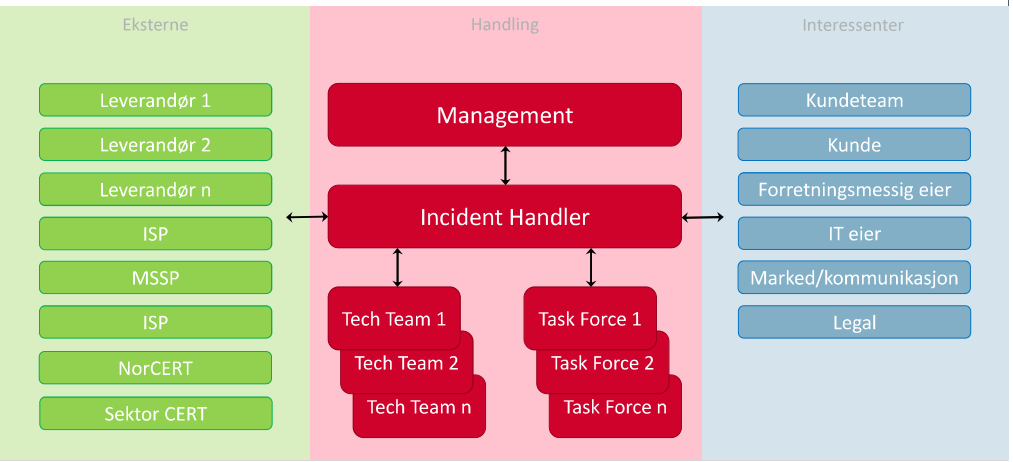
Faser i håndtering av en sikkerhetshendelse

- Normalization
  - Reetablere tjenester
  - Restore fra backup
  - Fortsette logging og monitorering
  - Samle og overlevere bevis
  - Herding og eventuelle andre permanente forbedringer
- Closing
  - Besluttes normalt av kunden
  - Avsluttende informasjon
  - Sluttrapport
  - Myndighetsrapportering
  - Debrief/Læring
  - Oppdatere prosesser
  - Systematisere dokumentasjon

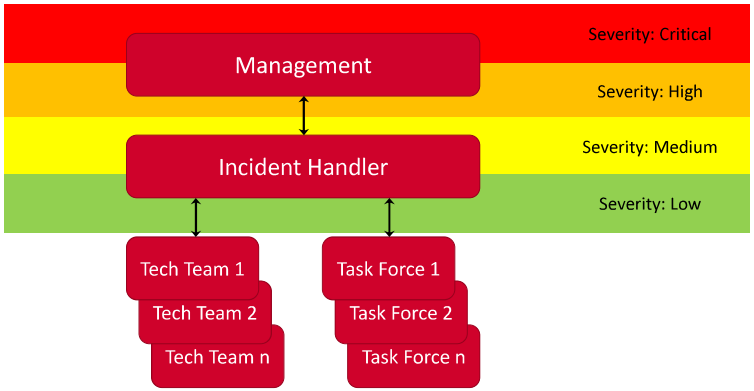
Debrief – Læring – Hot wash-up

- Oppsummere hendelsen og tiltak som ble utført
- Var forberedelsene tilstrekkelig?
- Ble hendelsen håndtert raskt og effektivt?
- Fungerte kommunikasjonen godt?
- Fungerte verktøy tilfredsstillende?
- La alle komme til orde
- Fokus på det positive og læringselementer, unngå skyld

Organisering av IRT



Eskalering



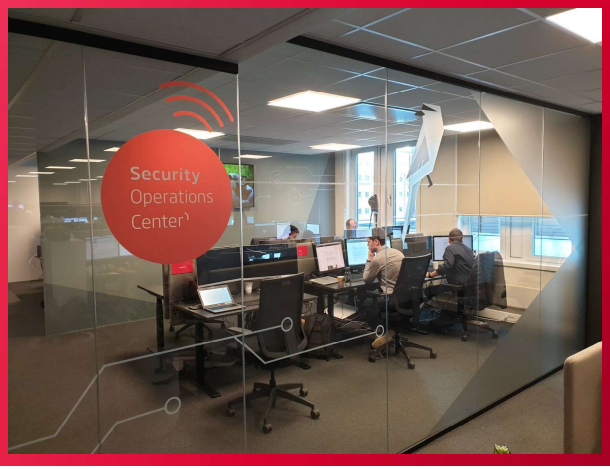
Øvelser

- Viktig???

- Øvingsstab
- Dreiebok
- Øvelser går sjelden helt etter plan
- Regler for å avbryte
- Læring

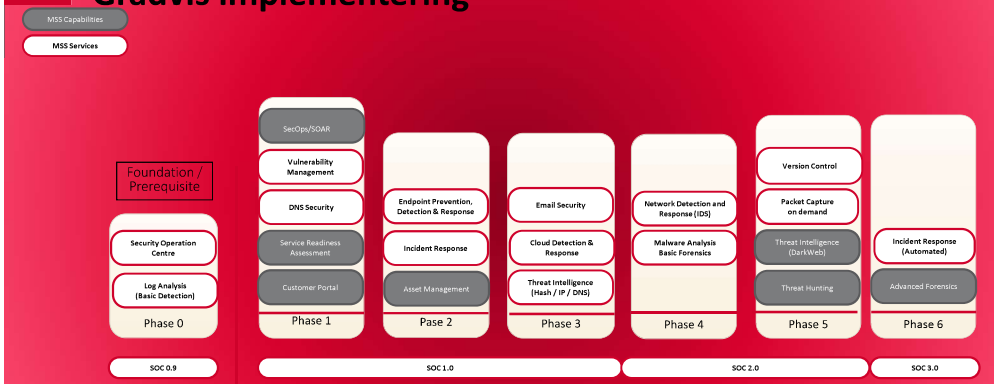
- Vesentlige målsetninger:
  - Mestring
  - Ha det gøy

Erfaringer fra Sopra Sterias etablering av SOC tjeneste



Managed Security Services tjenestespekter

Gradvis implementering



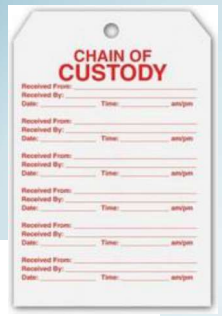
"Hallo" sa Nøff, "hva holder du på med?"

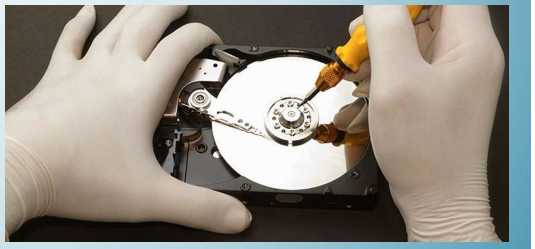
"Går på jakt" sa Brumm. "På jakt etter hva?" "Følger et spor" sa Brumm hemmelighetsfullt. "Hva slags spor?" spurte Nøff. "Det er nettopp det jeg spør meg selv om. Jeg spør meg selv: hva slags?"

"Hva tror du at du kommer til å svare?" spurte Nøff.

"Jeg vil vente med å svare til jeg har nådd igjen den som lager det" sa Brumm

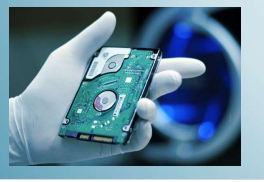
Digital Forensics





Computer forensics

"The goal of computer forensics is to **examine digital media** in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information."



Kilde: Wikipedia

Network forensics

Network forensics is "relating to the **monitoring and analysis of computer network traffic** for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations **deal with volatile and dynamic information**. Network traffic is transmitted and then lost, so network forensics is often a **pro-active investigation**."

Kilde: Wikipedia

Forensics spesifikt

Forensics generisk

«Forensics is a science and an art that requires specialized techniques for the recovery, authentication and analysis of electronic data for the purposes of a digital criminal investigation.»

- CISSP Exam guide

Forensics spesifikt

- Høyst spesialisert og krevende arbeid
- Primært for politi og rettsvesen
- Spesialisttjenester kan kjøpes

- Dataspeiling
- Harddiskanalyse
- Minneanalyse
- Gjenoppretting av slettede data

Etterforskningsprosess

Kilde: Digital Forensic Research Workshop, 2001

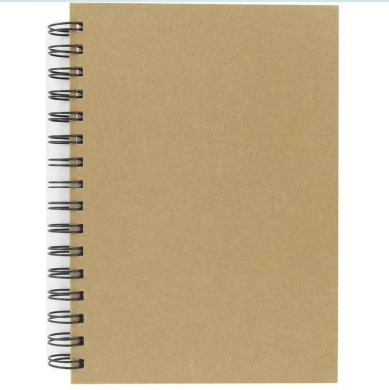
Forensics generisk

- Nyttig for alle som jobber med sikkerhetshendelser
- …også innen private virksomheter

- Chain of custody
- Dokumenterte rutiner …som etterleves
- Journalføring

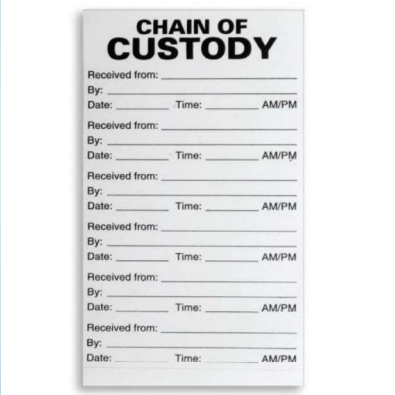
Noen legmannstips til digital forensics:

Før alltid journal

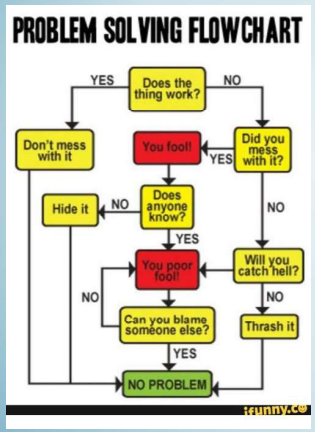


Jobb etter dokumenterte rutiner

Chain of Custody



Minimal intrusion, minimal force, minimal interuption



«Don't mess with it!»

Juridiske vurderinger

- Hendelseshåndtering kan ofte innebære innsyn i medarbeideres aktiviteter på IT-systemet
  - Surfehistorikk
  - Uttrekk av e-post
  - Filer på hjemmeområde
  - Oppslag i kunderegistre
- Misligheter
- Policybrudd
- Rettskonflikt

§

- Noen råd og tips
  - Tydelige fullmakter og ansvar
  - Personvernarbeid og risikovurdering
  - Informer de ansatte om hva som logges og hvilke regler og prosedyrer som gjelder ved innsyn
  - To par øyne samt rett til tilstedeværelse og representasjon
  - Sletting når man ikke lenger har behov for data

Kilder

- Carnegie Mellon University – cert.org
- SANS Institute – sans.org
- Internet Storm Center – isc.sans.org
- Forum of Incident Response and Security Teams (FIRST) – first.org
- National Institute of Standards and Technology (NIST) – nist.gov
- US-CERT – us-cert.gov
- NSM/NorCERT – nsm.stat.no/norcert/

Thanks for watching

sopra steria

Delivering Transformation. Together.

www.soprasteria.no