IT-beredskap i et totalforsvarsperspektiv

Simen Bakke, Politiets IT-enhet

Senior informasjonssikkerhetsrådgiver

Normkonferansen

Gardermoen, 22.11.2023

Agenda

1. Politiets avhengighet til IT-systemer
2. Risikostyring: Før, under og etter hendelser
3. Cybertrusler og -operasjoner
4. Hendelseshåndtering og krisehåndtering

Politiet har en bred IT-portefølje

- Forvalter både samfunnskritisk infrastruktur og grunnleggende nasjonale funksjoner.
- Flere av IT systemene må derfor fungere 24/7, 365.

Bilde: Politiet

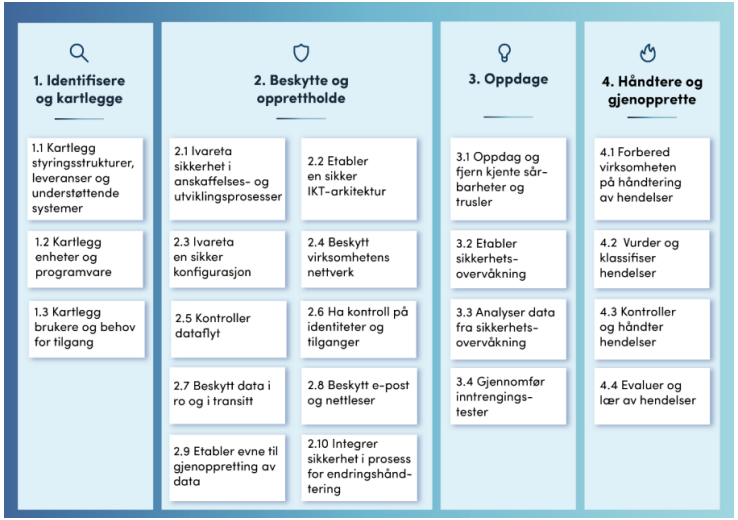
Politiet har en bred IT-portefølje

- Politiet: Forebygge og etterforske lovbrudd, også datakriminalitet.
- PIT: Utvikle, vedlikeholde, drifte og sikre politiets IT-systemer – også i luften.

Bilde: Politiet

Risikostyring før under og etter hendelser (og kriser)

- Forebygging – risikoreduserende tiltak utført *i forkant*
- Beredskap – *planlagte tiltak* for å håndtere hendelser
- Krisehåndtering – *håndtering av hendelser* og kriser
- Etterarbeid – evaluering, læring og forbedring (og øve!)



Bilde: Røde Kors, NSM og NIST

Hvorfor er *beredskap* viktig?

- *Beredskap* er **planlagte** og **forberedte tiltak** som gjør oss i stand til å håndtere uønskede hendelser slik at konsekvensene blir minst mulig.

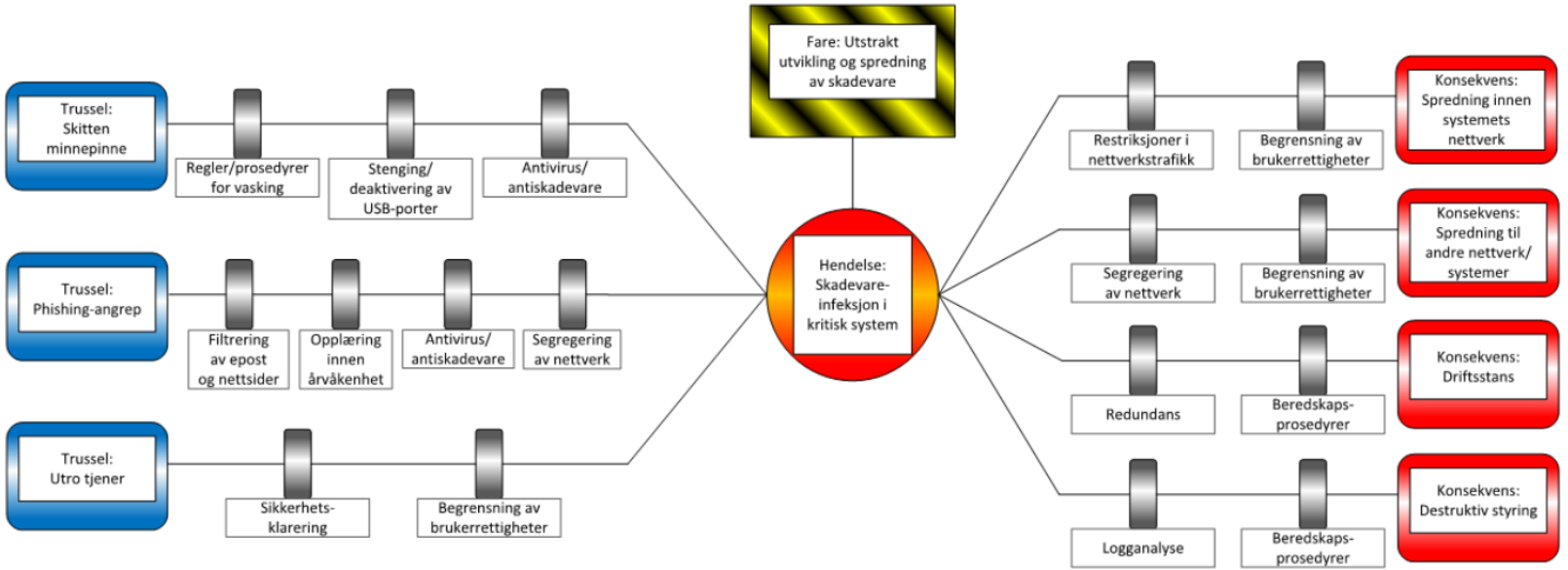
- Fordi vi ikke vil være i stand til å fjerne all risiko…
- … så vil hendelser, kriser og katastrofer inntreffe.
- Beredskapsapparatet bør dimensjoneres for *restrisikoen*.

«Det er sannsynlig at noe usannsynlig vil inntreffe».

«Fremtiden oppstår i variasjoner av fortiden.»

Bilde: DSB (2019) Analyser av krisescenarioer og E24

Risikostyring med bow-tie modellen



Hvorfor er IT-beredskap viktig?

Sensitiv pasientinformasjon kan være på avveie etter dataangrep

Datasystemet til Østre Toten kommune er angrepet og gjort utilgjengelig for alle ansatte. – Personnummer og helsedata kan være på avveie, sier ordføreren.

Norge | PST

PST etterforsker dataangrepet mot Helse sørøst som mulig etterretningsvirksomhet

PST mistenker at noen til fordel for fremmed stat står bak nettverksangrep mot Helse sørøst.

Bilde: NRK og Aftenposten

Krig skjerper trusselbildet

Aftenpo DN

Innlegg

Innlegg: Tjenestenektangrep kan være del av en påvirkningsoperasjon

Tjenestenektangrep mot sentrale norske samfunnsinstitusjoner bør ikke kun betraktes som it-tekniske hendelser – det er også en del av et pågående stormaktsspill mellom stater.

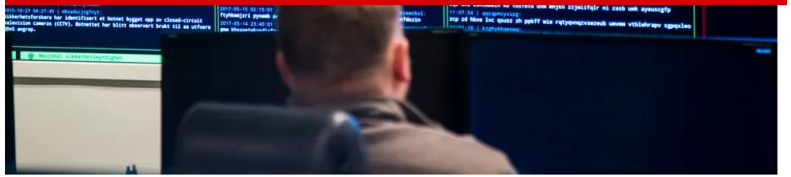
1 MIN | PUBLISERT: 07.07.22 – 16.43 | OPPDATERT: ETT ÅR SIDEN

Manipulerte bilder av utenriksminister Anniken Huitfeldt og Natos generalsekretær Jens Stoltenberg ble lagt ut som del av cyberoperasjonen til den russisk-tilknyttede grupperingen Killnet. Skjermdump hentet fra Telegram. (Foto: Beate Oma Dahle/NTB)

Flere sentrale norske samfunnsinstitusjoner som Arbeidstilsynet, Altinn,

Bergens Tidende

VGTV VG+ SPORT TV-GUIDE TIPS OSS KJØP VG+



FØLGER MED: Norges nasjonale cybersenter i Oslo er den operative delen av Nasjonal sikkerhetsmyndighet, og håndterer alvorlige dataangrep mot infrastruktur og informasjon. Foto: Heiko Junge / NTB

Nasjonal sikkerhetsmyndighet ber norske bedrifter om å være årvåkne

Cybereksperт mener et dataangrep kan bli brukt som hevn fra Russland, dersom Norge innfører sanksjoner mot landet. Nasjonal sikkerhetsmyndighet ber virksomheter ha lav terskel for å varsle myndighetene om mistenkelige forhold.

Av SILJE LIEN SVEEN
Oppdatert 26. februar 2022

Justis- og beredskapsminister Emilie Enger Mehl. Foto: Beate Oma Dahle

Justis- og beredskapsminister Emilie Enger Mehl ser ikke tegn til endring av trusselbildet i Norge som følge av krigen i Ukraina.

Russiske cyberoperasjoner i Ukraina

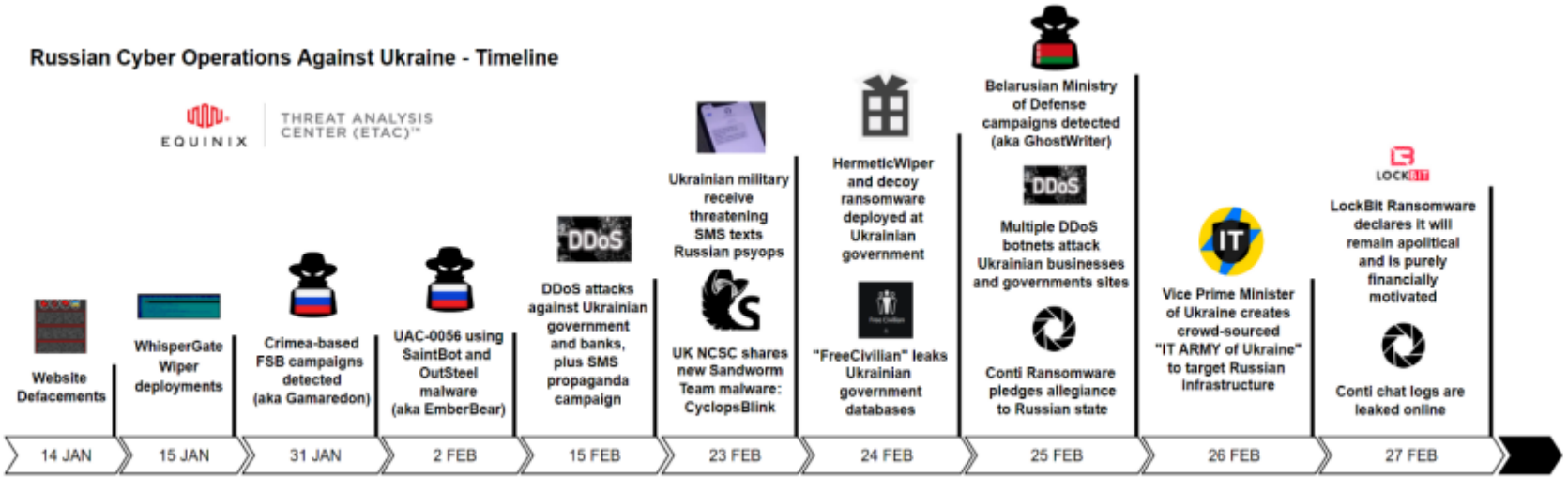


Figure 5: Timeline of significant cyber events (Source: CuratedIntel)

Bilde: Equinix

Hendelser vil inntreffe!

Spørsmålet er om man oppdager dem – tidsnok!

- Spionasje (konfidensialitet)
- Sabotasje (integritet / tilgjengelighet)

Og hvor godt forberedt man er på å håndtere dem!

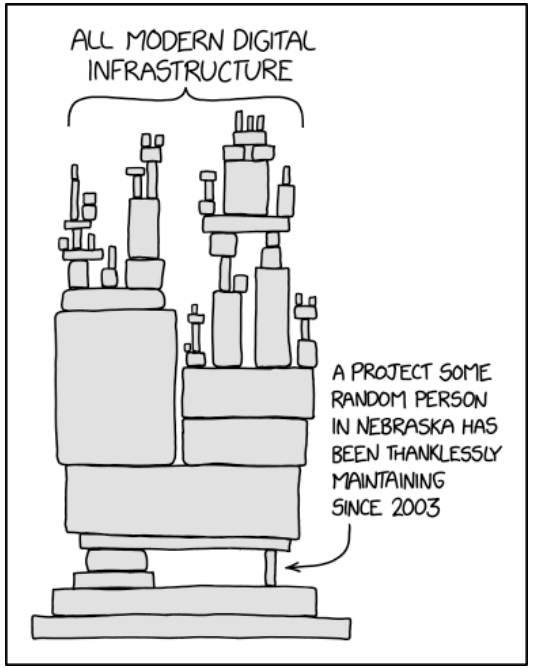
- Driftsovervåkning og alarmer
  - Kun dagtid eller 24/7, 365 drift? Hva med ferier?
- Deteksjonsevne- og hendelseshåndtering
  - Ingen, in-house eller innleie av profesjonelle?
- Beredskapsplanverk og stabsorganisering
  - Eskaleringsterskler (fra hendelse til krise)
  - Varslingsrutiner (internt og eksternt)
  - Bemanningsoversikter (med vaktordninger) ++

Sigbjørn Gjelsvik (til venstre) og NSMs Geir Arne Engh-Hellesvik fortalte om dataangrepene 24. juli. (Foto: Terje Bendiksby/NTB)

Bilde: DN og Stortinget

Helheten er viktig, fordi:

- IT systemer er **sårbare og komplekse –** samtidig blir trusselbildet mer krevende!
- Er det **forebyggende arbeidet mangelfullt** kan du få mange hendelser å håndtere!
- **Mangler dere deteksjonsevne** er det ikke sikkert du oppdager et sikkerhetsbrudd!
- Har du ikke **lagret nødvendige logger** blir det vanskelig å håndtere en hendelse!
- **Uten backup av data** kan det være vanskelig å gjenopprette normal drift!
- Beredskapsrutinene forutsetter en **IT- og fungerende sikkerhetsarkitektur**!
- **Øve for å verifisere** at beredskapsplanverket vårt fungerer etter hensikten!

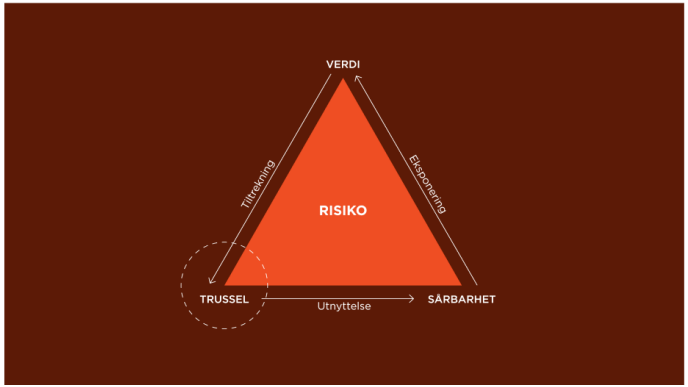


«***We don't rise to the level of our expectations, we fall to the level of our training.***»

Start med det enkleste!

- Hva er de viktigste systemene (og dataene) deres? Og hvor godt sikret er disse?
- Hvilke sårbarheter har vi og hvordan kan trusselaktørene utnytte disse?
- Vet IT-organisasjonen og ledergruppen hva de skal gjøre hvis…
  - IT-systemene går ned?
  - Et løsepengevirus krypterer data?
  - … Og krever utbetaling av kryptovaluta?
  - En statssponset trusselaktør er «på innsiden»?

- Hvis ikke, start med en enkel diskusjonsøvelse!
  - Bli kjent med hverandre og deres ulike roller!
  - Hva gjør at IT-avdelingen sover dårlig om nettene?
  - Vil dere være i stand til å detektere på et tidlig tidspunkt?
  - Vurder å gjøre endringer nå – så slipper dere være på etterskudd!



Takk for meg!

Og lykke til!

«*We don't rise to the level of our expectations, we fall to the level of our training.*»