



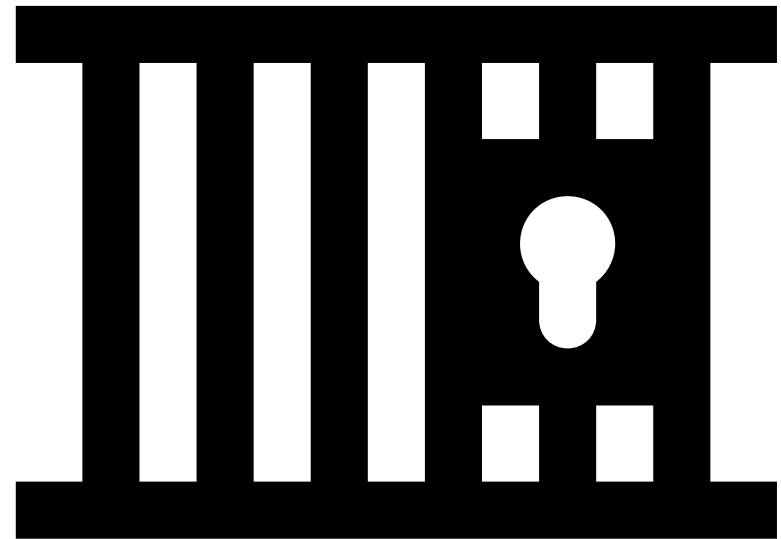
VALGdirektoratet

Sikkerhet

John Andreas Johnsen & Anders Skaalgaard

Sikkerhet

- Kartlegge og identifisere
 - Verdier
 - Trusler
 - Sårbarheter
- Sikkerhetsveilederen
- Nytt i regelverket



Kartlegge og identifisere

Verdier, sårbarheter og trusler

Verdier

“Det mest fundamentale med sikkerhet er forutsetningen om at man har noe – en verdi som man ønsker å beskytte”

Nasjonal sikkerhetsmyndighet

Verdier

- Materiell og utstyr
- Lokaler
- IT-systemer
- Personell
- IKT-utstyr

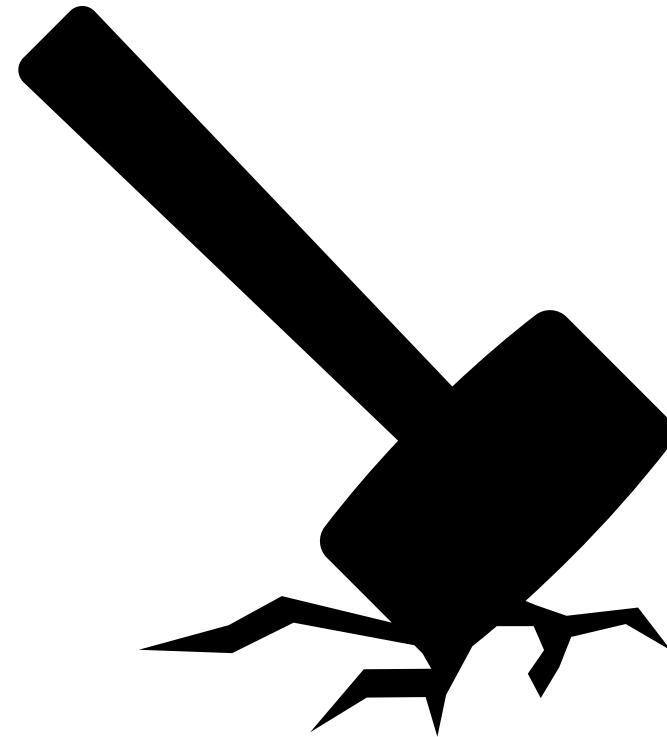


KI-generert bilde med Copilot.

Sårbarheter

Feil eller mangler i:

- Design/utforming
- Prosedyrer
- Vedlikehold
- Trening/Oppplæring



Trusler

- Hvem er trusselaktørene
- Hvilke intensjoner har disse
- Hvilken kapasitet har de



Trusselvurdering - Valgdirektoratet

- Russlands angrepskrig i Ukraina
- Stormaktsrivalisering
- Autoritære regimer vs. liberale demokratier
- Innsidetrussel

Eksempler

- Regjeringen
- Posten
- Romania
- Valgdirektoratet

Departementenes sikkerhets- og serviceorganisasjon har avdekket et dataangrep på IKT-plattformen til 12 departementer. Saken etterforskes av politiet.

Departementer utsatt for dataangrep

Fire uker langt hackerangrep mot Posten i fjor høst

Høsten 2023 hadde Posten det de kaller en alvorlig sikkerhetshendelse.

Rapport: Massive angrep mot Romanias valgsystemer

Beskytte, opprettholde og gjenopprette

Hva kan vi gjøre?

Tiltak

Rammebetingelser

- Økonomiske
- Praktiske
- Valg-tekniske

Verdiene

Mange tiltak finnes
allerede i
valgloven/forskriften

Risikovurderinger

Sikkerhetsveilederen

Veileder i sikkerhet ved valg

Fysisk sikkerhet

Forhindre

Avdekke

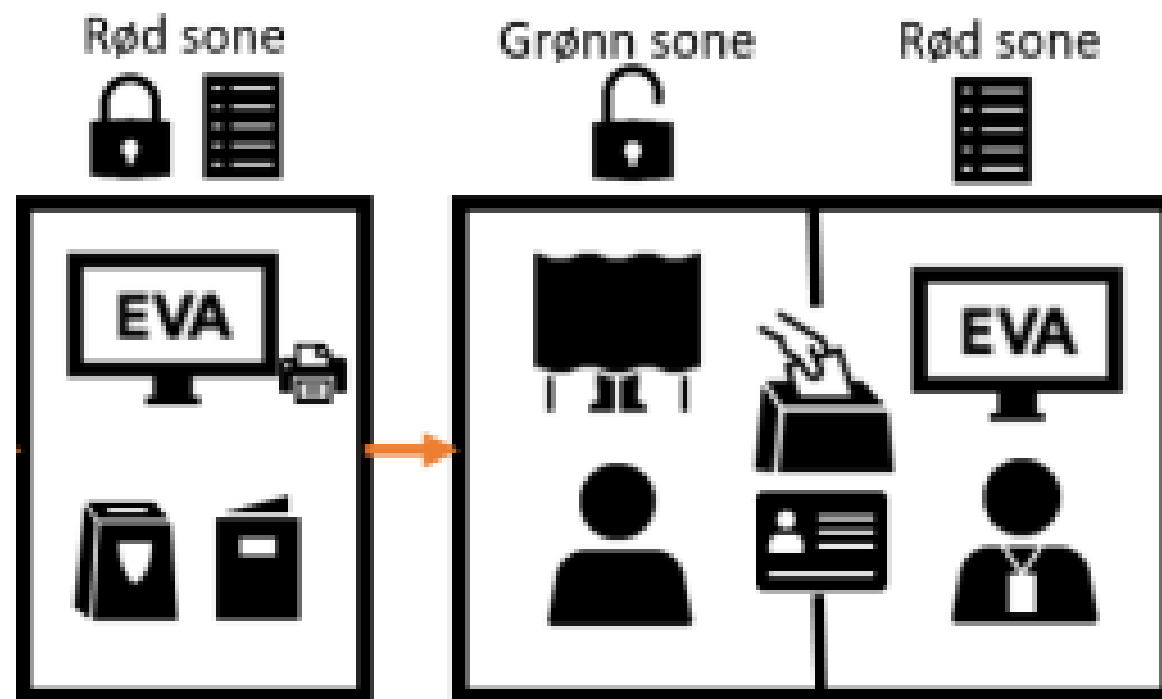
Forsinke

Tiltak

- Barrierer
- Deteksjon
- Verifikasjon
- Reaksjon

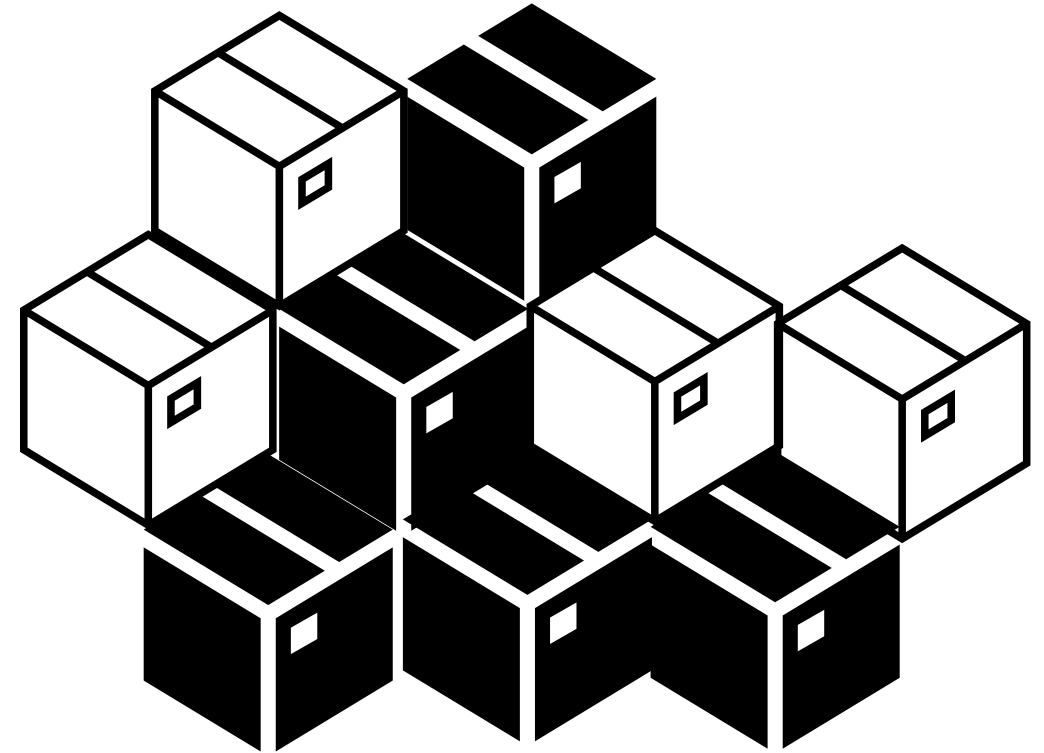
Soneinndeling

- Grønn Sone
- Rød Sone
- Begge i samme rom



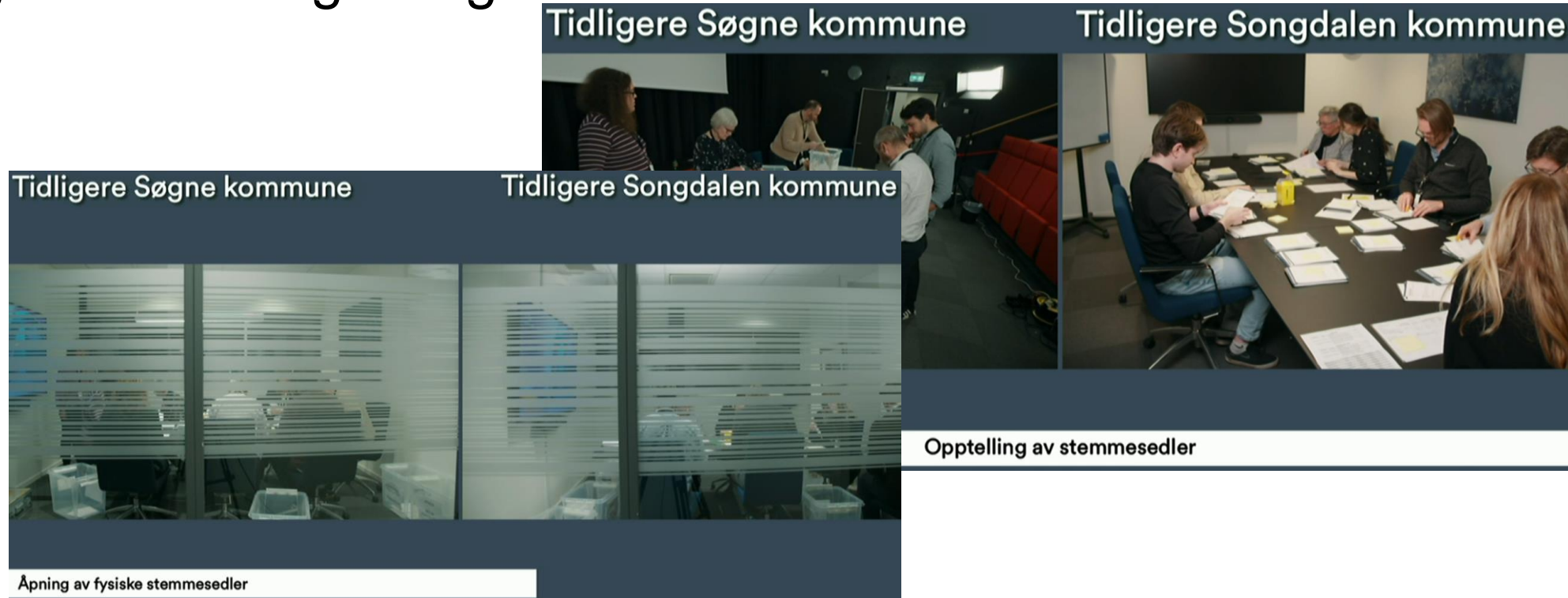
Oppbevaring og transport

- Oppbevares i rød sone
 - Materiell
 - IKT-utstyr
 - Avgitte stemmesedler
- Transport – rød sone
 - Forsegling
 - Kvittering



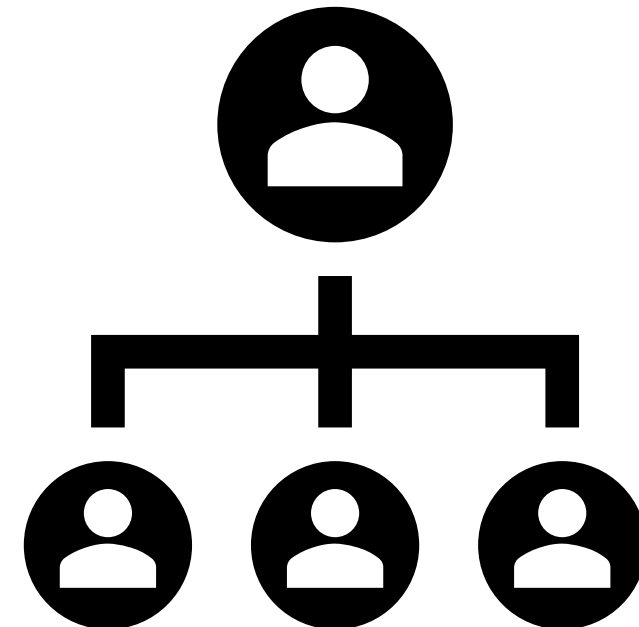
Folkeavstemming

- Håndtering av stemmegivninger
- Opptelling



Organisasjon og mennesker

- Personellsikkerhet
- Rutiner, prosedyrer og planverk
- Kompetanse
- Sikkerhetskultur
- Tjenesteutsetting



Logisk sikkerhet – informasjonssikkerhet ved bruk av EVA

Beskytte og opprettholde

Oppdage avvik

Håndtere og gjenopprette

Sertifikat og monitorering

- Sertifikat
 - Pålogging til EVA
 - Ett sertifikat per kommune
 - Varsle!
- Endepunktsmonitorering
 - Et tilbud til kommuner som ikke har dette selv.
 - Ser etter unormale handlinger

Case number:
OCD_INC2049024

Priority:
2 - High

Summary of the incident:

'Credential Gathering Protection - 797899178' generated by XDR Agent detected on host [REDACTED] involving user [REDACTED]
Alert id:274

Timestamp (UTC):
2025-01-14 14:07:26

Actions taken by incident handler:
No response actions have been taken

Next steps to be taken:
Check if this is a pentest or real case.

Entities affected by the incident:

User(s): [REDACTED]

Host(s): [REDACTED]

Destination(s): [REDACTED]

Analysis:

'Credential Gathering Protection - 797899178' along with 147 other alerts generated by XDR Agent detected on 2 hosts involving 2 users

PetitPotam NTLM relay attack

Remote Connection Details

remote connection ip: [REDACTED]

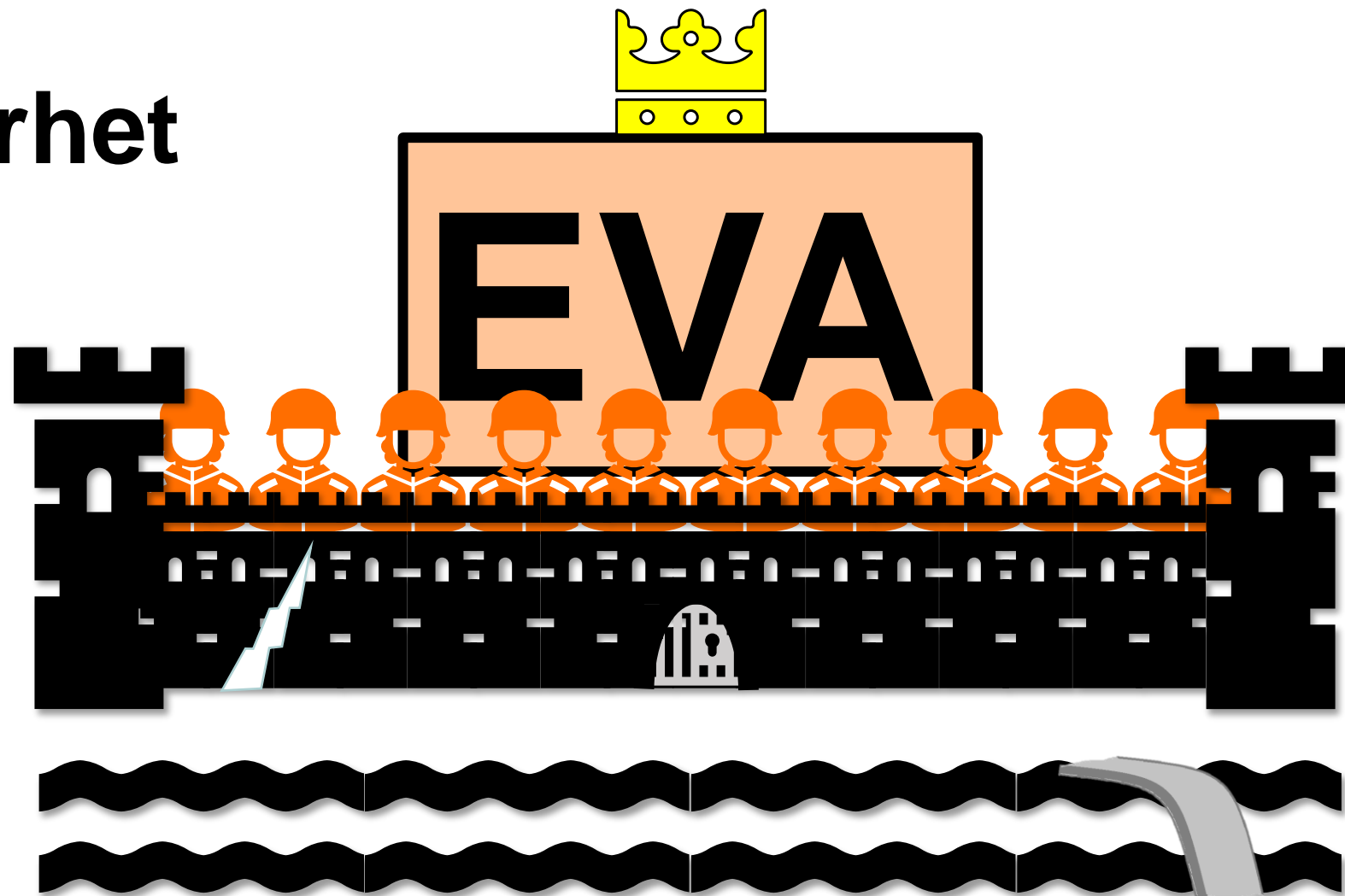
remote connection pipe name: [REDACTED]

Group Names: [REDACTED]

PetitPotam is an attack method disclosed in July 2021 that leverages NTLM relay in Windows environments. It specifically abuses Microsoft's EFSRPC (Encrypt System Remote Protocol) to coerce a Windows machine (often a Domain Controller) into authenticating to an attacker-controlled system using NTLM. The attack then relay those captured credentials (or challenge/response data) to other services, potentially gaining high-level privileges.

Logisk sikkerhet

- Sikkerhet i lag
- Sårbarheter
 - Skjulte
 - Innføres
- Et kappløp
- Flere bidragsytere



Nyheter

Nyheter

- Samarbeid med Helse- og KommuneCERT
- Valg som Grunnleggende Nasjonal Funksjon (GNF)

«Gjennomføring av frie, hemmelige og tillitsskapende valg til Stortinget, fylkesting, kommunestyre og Sametinget.»

Nytt i regelverket



Valglov og –forskrift

Ordensregler

Forsegling, oppbevaring og transport

Kvittering

Rutine for manuelle opptellinger

Stikkprøvekontroll



Storingsvalget 1949. Opptelling av oslostemmene i Rådhuset. Arbeiderbladet, [CC BY-NC-ND](#)



VALGdirektoratet

valg.no