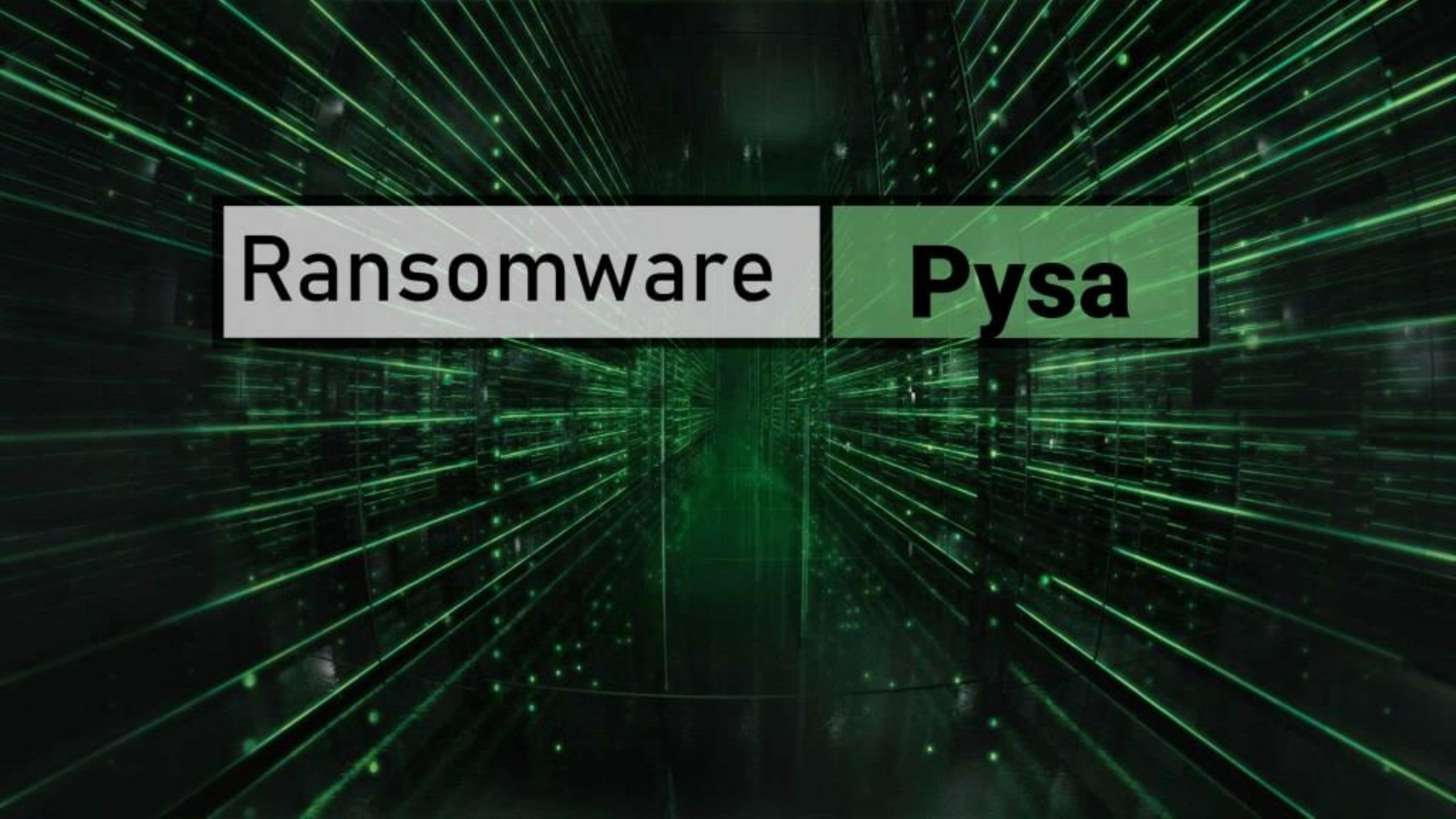
Datainnbrudd – erfaringer fra Østre Toten kommune

Faglig arena for informasjonsforvaltning og deling av data

Ole Magnus Stensrud
Kommunedirektør

Østre Toten
kommune

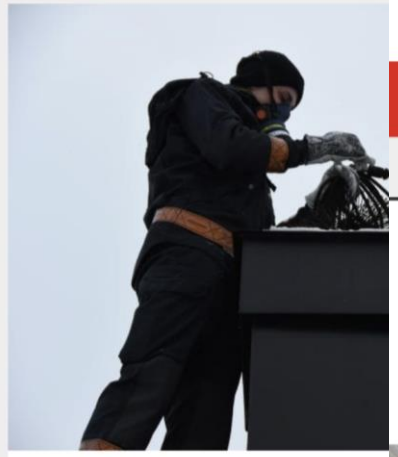

Ransomware
Pysa

Prioriteringer

Liv og helse

Miljø

Økonomi



Dataangrepet s
Marius opp på
mange tak

Så, hva s
lokalavisa
kanskje?

Totens Blad

Nyheter Eavis Min side Meny

NYHETER

Kommunen lever
men sliter med å
regninger for mil
kroner

Bente Løvaas Olsen, konsulent
og Ola Løvstad, leder for tildel
kommunen vil være imøtekom
innbyggerne ønsker å splitte o
Jan Rune Bakkelund)

ØSTRE TOTEN DATASIKKERHET HELSE OG OMSORG LABO FJELLVOLL

Helse- og omsorgssje
Østre Toten etter
dataangrepet: – Dett
helt surrealistisk

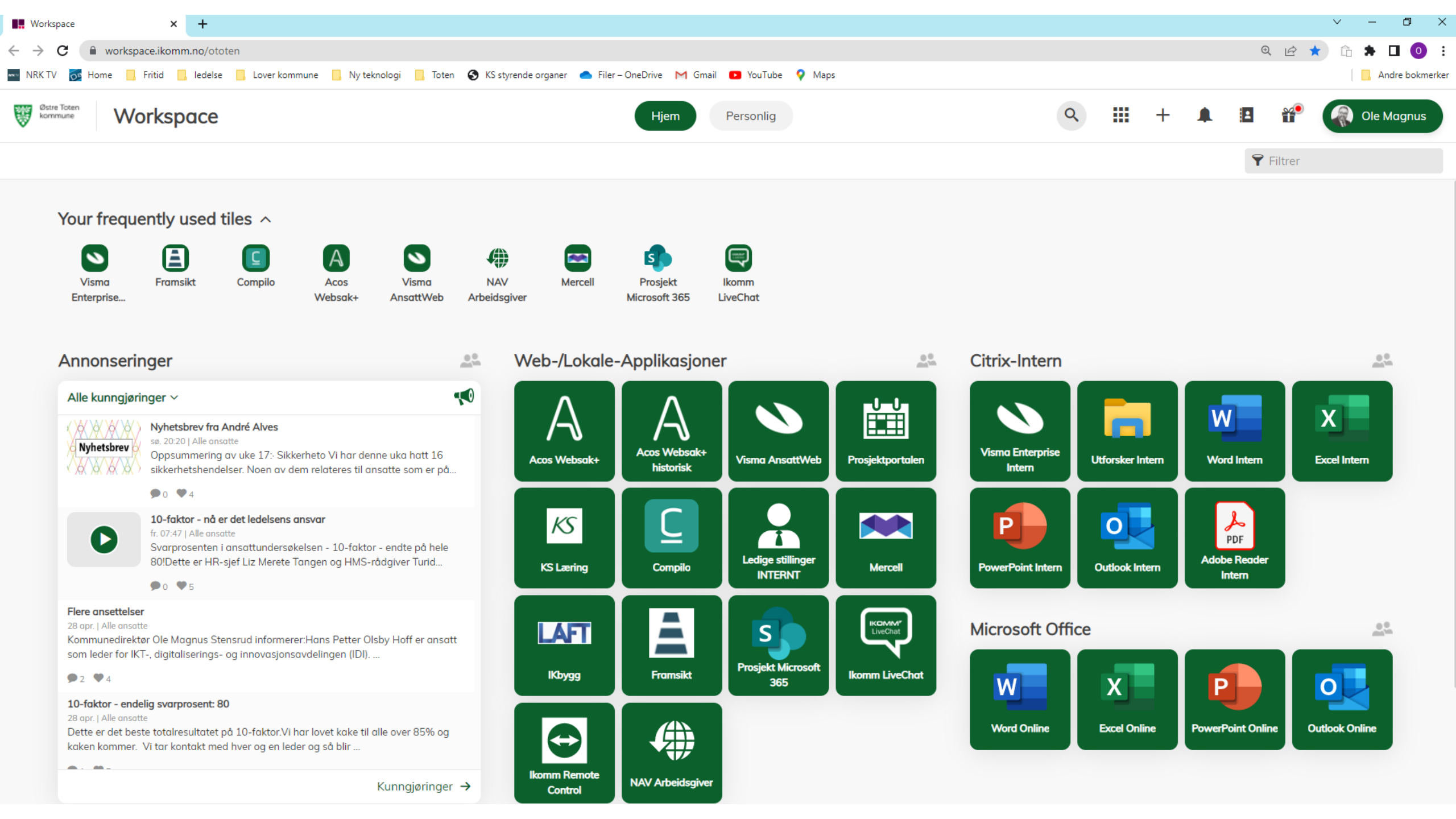
BJELLER I STEDET FOR ALARMARMBÅND: Diana Stepanova på Labo avdeling 4 viser fram
for å tilkalle hjelp. Det vanlige alarmsystemet er satt ut av drift etter dataangrepet. Foto:
kommune

TOTENIDAG MENY

ARBEIDSLIV

Arbeid som før tok to timer tar nå en hel dag

TUNGVINT: – Det er tungvint å jobbe uten tilgang til fagsystemene. Det som før tok to timer tar nå en hel dag, sier byggesaksbehandler Sohrab M. Kamaly. Foto: Sæmund Moshagen


Workspace
workspace.ikomm.no/ototen
NRK TV
Home
Fritid
ledelse
Lover kommune
Ny teknologi
Toten
KS styrende organer
Filer – OneDrive
Gmail
YouTube
Maps
Andre bokmerker
Østre Toten kommune
Workspace
Hjem
Personlig
Ole Magnus
Filtrer
Your frequently used tiles
Visma Enterprise...
Framsikt
Compilo
Acos Websak+
Visma AnsattWeb
NAV Arbeidsgiver
Mercell
Prosjekt Microsoft 365
Ikomm LiveChat
Annonseringer
Alle kunngjøringer
Nyhetsbrev fra André Alves
sø. 20:20 | Alle ansatte
Oppsummering av uke 17:· Sikkerheto Vi har denne uka hatt 16 sikkerhetshendelser. Noen av dem relateres til ansatte som er på...
0
4
10-faktor - nå er det ledelsens ansvar
fr. 07:47 | Alle ansatte
Svarprosenten i ansattundersøkelsen - 10-faktor - endte på hele 80!Dette er HR-sjef Liz Merete Tangen og HMS-rådgiver Turid...
0
5
Flere ansettelser
28 apr. | Alle ansatte
Kommunedirektør Ole Magnus Stensrud informerer:Hans Petter Olsby Hoff er ansatt som leder for IKT-, digitaliserings- og innovasjonsavdelingen (IDI). ...
2
4
10-faktor - endelig svarprosent: 80
28 apr. | Alle ansatte
Dette er det beste totalresultatet på 10-faktor.Vi har lovet kake til alle over 85% og kaken kommer. Vi tar kontakt med hver og en leder og så blir ...
Kunngjøringer
Web-/Lokale-Applikasjoner
Acos Websak+
Acos Websak+ historisk
Visma AnsattWeb
Prosjektportalen
KS Læring
Compilo
Ledige stillinger INTERNT
Mercell
IKbygg
Framsikt
Prosjekt Microsoft 365
Ikomm LiveChat
Ikomm Remote Control
NAV Arbeidsgiver
Citrix-Intern
Visma Enterprise Intern
Utforsker Intern
Word Intern
Excel Intern
PowerPoint Intern
Outlook Intern
Adobe Reader Intern
Microsoft Office
Word Online
Excel Online
PowerPoint Online
Outlook Online

Prioriteringer

Liv og helse

Miljø

Økonomi

Mener Østre Toten gjorde det riktige da angrepet rammet

Espen Torseth, seniorrådgiver hos Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU, roser Østre Toten kommune. (Foto: Torbjørn Aurvåg)

Håndtering av angrepet - læringspunkter

- Hendelseshåndtering / koordinering
- Oppbygging av ny digital infrastruktur
- Gjenoppretting av fagsystemer
- Tekniske undersøkelser
- Varsling, lekkede data
- Personvern
- Sikkerhet

IKT-sikkerhet i forut for dataangrepet

Kartlegging og ekstern vurdering

https://www.ototen.no/aktuelt/ny-versjon-av-sikkerhetsrapporten.13134.aspx

Sammendrag KPMGs rapport

KPMGs gjennomgang har identifisert en rekke svakheter.

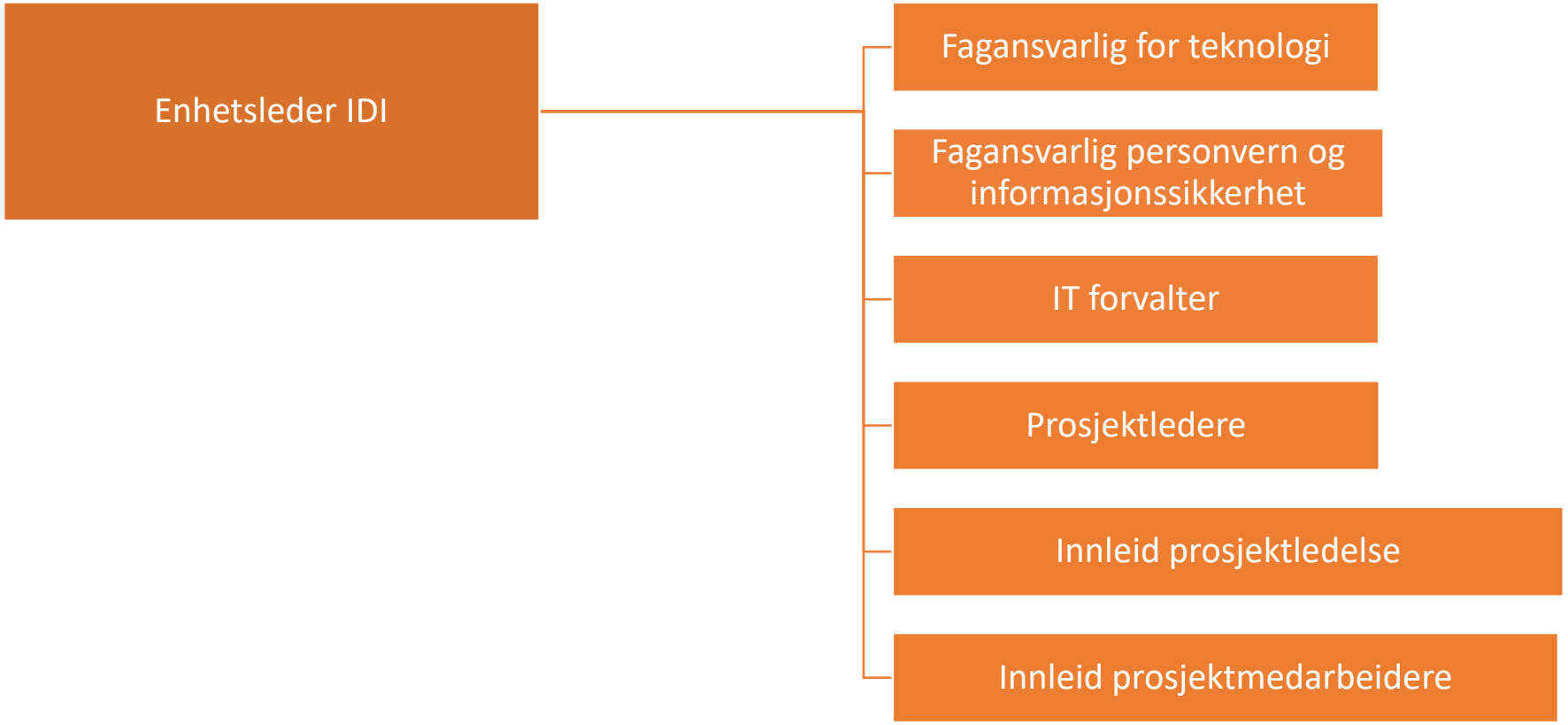
«KPMG antar at tilstanden i sammenliknbare kommuner ligger på omtrent samme nivå som Østre Toten kommune forut for hendelsen.»

«Implementasjon av få, men viktige tiltak kan gjøre stor forskjell på sikkerhetstilstanden i en kommune.»

KPMG, anbefalinger til kommunedirektøren

- Oppdater kommunedirektørens internkontroll på IKT-sikkerhet
- Kommunen må gjennomføre jevnlige risikovurderinger
- Styrke kompetansen innen IKT-sikkerhet og personvern
- Ivareta god bestillerkompetanse
- Styre etter NSMs grunnprinsipper
  - kommunen og
  - tjenesteleverandørene

Enhet for IKT, digitalisering og innovasjon (IDI)



Bot og pålegg fra Datatilsynet

oa.no MENY

ØSTRE TOTEN

Østre Toten må punge ut fire millioner kroner i bot etter dataangrepet: – Beklagelig og kjedelig

- For overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger.
- Pålegges å etablere og dokumentere at et egnet styringssystem for informasjonssikkerhet og personopplysningssikkerhet er implementert.
- Pålegges å gjennomføre risiko- og sårbarhetsanalyser for alle sentrale systemer/løsninger i infrastrukturen.

Datatilsynet har kommet til at Østre Toten kommune skal ilegges følgende vedtak:

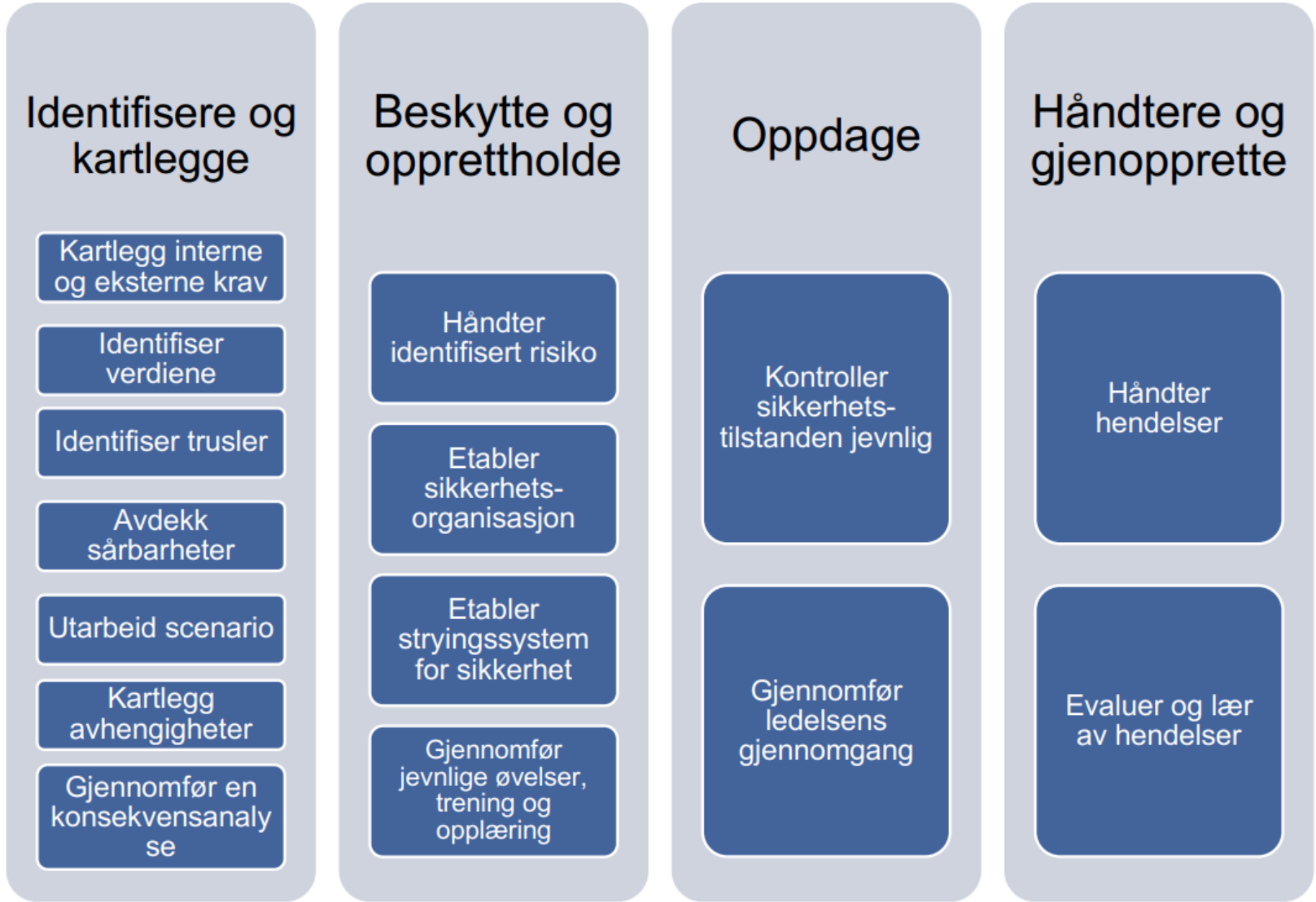
I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 og pasientjournalloven § 29, ilegges Østre Toten kommune et ***overtredelsesgebyr på 4 000 000 NOK*** *– fire millioner norske kroner – til statskassen, for* ***overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger****, jf. personvernforordningen artikkel 32 og artikkel 24, jf. personopplysningsloven § 26 første ledd. Kommunen har blant annet manglet effektive sikkerhetstiltak ved pålogging, tilstrekkelig sikrede backup-systemer og tilstrekkelig logging av viktige hendelser i sitt nettverk.*

Østre Toten kommune ***pålegges å etablere og dokumentere at et egnet styringssystem for informasjonssikkerhet og personopplysningssikkerhet er implementert****, jf. personvernforordningen artikkel 58 nr. 2 bokstav d. Som ledd i dette arbeidet* ***pålegges kommunen å gjennomføre risiko- og sårbarhetsanalyser for alle sentrale systemer/løsninger i infrastrukturen****, med det formål å identifisere behovet for risikoreduserende tiltak****. Analysene skal dokumenteres i styringssystemet.***

Russlands invasjon av Ukraina

Kommunal- og distriktsdepartementet og KS ber alle kommuner vurdere sin egen sikkerhets- og sårbarhetssituasjon.

- Sikkerhetsovervåkning
- Sikring av kritiske funksjoner og tjenester
- Beskytte tjenester som er tilgjengelig på Internett
- Årvåkenhet og teknologi



Figur 1 NSMs grunnprinsipper for sikkerhetsstyring

1. Identifisere og kartlegge

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 Kartlegg enheter og programvare
- 1.3 Kartlegg brukere og behov for tilgang

2. Beskytte og opprettholde

- 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser
- 2.2 Etabler en sikker IKT-arkitektur
- 2.3 Ivareta en sikker konfigurasjon
- 2.4 Beskytt virksomhetens nettverk
- 2.5 Kontroller dataflyt
- 2.6 Ha kontroll på identiteter og tilganger
- 2.7 Beskytt data i ro og i transitt
- 2.8 Beskytt e-post og nettleser
- 2.9 Etabler evne til gjenoppretting av data
- 2.10 Integrer sikkerhet i prosess for endringshåndtering

3. Oppdage

- 3.1 Oppdag og fjern kjente sårbarheter og trusler
- 3.2 Etabler sikkerhetsovervåkning
- 3.3 Analyser data fra sikkerhetsovervåkning
- 3.4 Gjennomfør inntrengingstester

4. Håndtere og gjenopprette

- 4.1 Forbered virksomheten på håndtering av hendelser
- 4.2 Vurder og klassifiser hendelser
- 4.3 Kontroller og håndter hendelser
- 4.4 Evaluer og lær av hendelser

«Arbeidspakker»

- **D1: Oversikt over egen infrastruktur**
- **D2: Tekniske beskyttelsestiltak**
- **D3: Bevisstgjøring av ansatte**
- **D4: Operativ IKT-sikkerhet**
- **D5: Gjenoppretting**

Vi jobber nå med 17 konkrete tiltak

Mapping mot NSMs Grunnprinsipper for IKT sikkerhet

Evaluering av hendelseshåndteringen

Grethe Østby

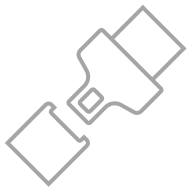
Stipendiat

NTNU
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Fakultet for informasjonsteknologi og elektroteknikk

Rapport kommer før sommeren 2022

Hva kan andre lære av oss?



Finn ut hvor sårbare dere er

Datasikkerhet må prioriteres

Ting tar tid

Samarbeid