# Drammen til sky

## IKT- sikkerhet og Drammen til sky

**Formannskapsmøte**
**9. mai 2023**

Virksomhetsleder IKT Svein Hilding Aasen

# Innhold.

IKT-sikkerhet og Drammen til sky:

- Kommunens målsettinger ift. digital transformasjon
- Skjerpet digitalt trusselbilde
- Drammen til sky som svar på utfordringene
- Risiko og sårbarhetsanalyse

# Digitaliseringsstrategien vedtatt av kommunestyret desember 2020

*Hovedmål*:
Enklere hverdag for innbyggere og næringsliv

*Strategien bygger på tre pilarer*:

- Innbyggere og næringsliv skal være inkludert og prioritert i digitaliseringen av samfunnet
- Digital transformasjon krever kompetanse og endringskultur hos alle i kommunen
- Infrastruktur, informasjonssikkerhet og personvern er grunnmuren for utvikling

# Skjerpet digitalt trusselbilde ( 2021)

SIKKERHET

## Drammen kommune har fjernet sårbarhet som tillot avløps-hacking

– Det var aldri fare for driften av de to pumpestasjonene, sier IT-sjefen i Drammen.

Dagbladet avslører:

## Russere angrep vannsystemet i Drammen

Kort tid etter at hackere forsøkte å forgifte drikkevannet til 15 000 i USA, brøt russiske hackere seg inn på vannsystemet til Drammen kommune. Da gikk alarmen.

## Hevder russere står bak hackerangrep mot Drammen

Dataangrepet mot infrastrukturen til vann- og avløp i Drammen fikk ikke konsekvenser for brukerne - og skal i følge kommunen aldri ha truet vannforsyningen. Foto: NTB/Håkon Mosvold Larsen

Av Arild Ø Hansen

Publisert: 01.09.22 09:34

Del

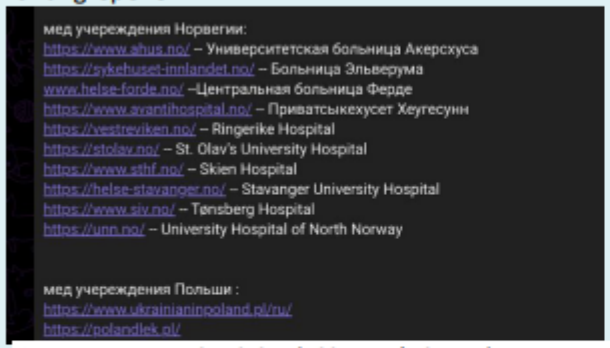
I februar i fjor ble det utført et angrep på infrastrukturen for vann og avløp i Drammen. Det kommer nå fram at det skal være en russisk hackergruppe ved navn Avaddon som står bak.

# Skjerpet digitalt trusselbilde

sårbarheter og hendelser i offentlig sektor i Norge 2023

**Norske sykehus angripes med tjenestenektangrep fra russiske hacktiviste**

Lørdag 28. januar opplevde en rekke norske sykehus tjenestenektangrep fra russisk støttede hackere som hevn for Norges støtte til Ukraina. Denne typen angrep skaper midlertidig trengsel og tjenestebrudd på nettsidene til sykehusene, men gjør ingen skade på de interne funksjonene og systemene. Angrepene var varslet på forhånд, og det var den russiske gruppen som kaller seg KillNet som truet og påtok seg ansvaret for angrepene.




Figur 1: Angrepstruede sykehus (Kilde: NRK/Telegram)

**Nordnorske kommuner kompromittert av hackere**

I starten av februar 2023 kom det meldinger om at både Vadsø kommune og Målselv kommune har blitt hacket av ondsinnede aktører som har kompromittert e-postkontoer og servere. Det viser seg at angrepet mot Målselv var mot servere, mens Vadsø og andre kommuner og virksomheter har blitt kompromittert gjennom overtagelse av brukerkontoer/e-postkontoer. Det er foreløpig ingen indikasjon på at Målselv-hendelsen har tilknytning til hackingen av brukerkontoer hos Vadsø og de andre virksomhetene. Men Vadsø-hendelsen ser derimot ut til å gjelde flere kommuner og virksomheter, og denne hendelsen ser ut til å være større enn først antatt.



Kommune-CSIRT: I Norge har vi nå i starten av 2023 sett kompromittering av kommuner og digitale hevnaksjoner som har blitt gjennomført mot norske sykehus. Dette viser at faren utvilsomt er høy uansett om vi opplever roligere perioder. Dette styrker vurderingen av at angrepsvolum og alvorlighet går i bølger, og at risikoen derfor fremdeles er høy for å bli angrepet og kompromittert.

I flere av rapportene som er lansert de siste 2 årene har man kunnet se hendelser mot vann og avløpssystemer over hele verden…]

# Hva er fordelene med å bruke skyløsning?

- **Prosjektet «Drammen til sky» igangsatt mars 2022, innebærer migrering ut av eget datarom (ca. 60 fagsystemer):**
  - Drammen kommunes Virtuelle datarom i sky (Azure) ferdigstilt februar 2023
  - Konkurranse ny hovedleverandør (drift) publisert 10. mars 2023. Driftsovertakelse i 2023 og ferdig migrert 1Q 2024.

- De store offentlige skyplattformene er mye sikrere enn lokalt dataromsdrift. Microsoft investerer milliarder i året for å sikre sin skyplattform og Azure har flere sikkerhetssertifiseringer enn noen annen drifts- og skyleverandør.

- Det er innarbeidet styrket informasjonssikkerhet utover det vi har mulighet til på dagens IKT-plattform (bla «microsegmentering, oppdeling av datarommet i små soner styrt av brannmurer som vanskeliggjør bevegelse «på tvers»).

- Nye tjenester, oppskalering eller nedskalering, og at endringer skjer umiddelbart, er en stor fordel.

- Microsoft har enorm kapasitet i sine datasentre, både per lokasjon og antall datasentre. Kommunens data vil ligge i 2 datasentre i Norge.

- Kommunen kvitter seg med «teknisk gjeld» (foreldet datarom) og sårbarhet.

Illustrasjonsfoto av Microsofts hovedkvarter i Paris: Thibault Camus / AP / NTB

- Det finnes ikke egne personvernbestemmelser som regulerer bruk av skytjenester.

- Likevel oppstår det noen særlige problemstillinger ved bruk av Microsoft Azure og skytjenestene deres.

- Microsoft er amerikansk og produserer sine tjenester i ulike land, som da gjerne har ulike personvern-regler og ikke minst regler for å begjære innsyn i lagrede opplysninger på plattformen.

# Advokathuset PwC- overordnet ROS

- Advokathuset PwC har bistått i arbeidet med å kartlegge personvernet.
- I ROS-vurderingen av skyløsningen er det lagt til grunn **de EU- baserte tilsynenes praktisering**. Dette gir det strengeste utgangspunktet og eksponeringen ved et evt. tilsyn.
- Rettstilstanden på dette området er uklar og i rask bevegelse, og i det norske juridiske fagmiljøet hersker det uenighet om helt grunnleggende forhold.
- Datatilsynets egne veiledere og uttalelser på området er kraftig utfordret av SKATE-utvalget, som har utgitt en egen veileder rettet spesielt mot bruk av skytjenester i offentlig sektor. Se, veiledning utgitt i fellesskap av **Digitaliseringsdirektoratet** (Digdir) og **Direktoratet for forvaltning og økonomistyring (**DFØ).
- **Den svært kjente Schrems II dommen fra 16. juli 2020**, gjaldt overføring av personopplysninger til USA. Amerikansk overvåkingslovgivning vurderes å gå utover det som er nødvendig og proporsjonalt i et demokratisk samfunn. USA sikrer heller ikke de registrertes mulighet til å klage til en uavhengig tilsyns-myndighet e.l. og de sikres ikke effektive rettsmidler for å ivareta sine rettigheter.
- Det arbeides med en **ny avtale mellom EU/EØs og USA knyttet EU-borgeres rettigheter i USA knyttet til personvern**, og denne kan være på plass i løpet av året, før de fleste av fagsystemene mot slutten av året og inn i 2024, er migrert til Azure. Ny avtale vil styrke rettsvernet, selv om det ikke er ventet at dette vil løse alt.


Microsoft Azure benyttes av kommuner som Ullensaker, Digitale Gardermoen, Bodø Kommune, Utdanningsetaten i Oslo og Stor Follo i tillegg til flere statlige etater. Flere og flere offentlige aktører går til sky.

# Advokathuset PwC- overordnet ROS

| | |
|---|---|
| **A) Risiko for overføring av personopplysninger til Tredjeland** | **Utleveringsanmodninger fra USA eller tredjelands myndigheter**<br>• Ingen tiltak som Drammen kommune kan gjøre vil hindre en lovpålagt utlevering fra Microsoft ✓<br>• Microsoft har oppgitt i sine svar på spørsmål fra PwC at de så langt aldri har gitt ut persondata fra offentlige sektorvirksomheter i Europa. ✓<br><br>**Tjenesteproduksjon i USA eller i land utenfor EU/EØS**<br>• EU data boundary Service – ny tjeneste fra 1. januar 2023 hvor Microsoft forplikter seg til å produsere tjenestene våre med ressurser innenfor EU/EØS sine grenser. ✓<br>• Alle kommunens data vil bli lagret i Norge ✓<br>• Ny hovedleverandør drift – det kreves at alle tjenester produseres innenfor EU/EØS ✓<br>• Kryptering benyttes på lagrede data i ro og på forbindelser i Microsoft sin skyløsning, men kryptonøkler tilgjengelig for Microsoft hvis de absolutt vil få tak i disse. ✓<br>• EU data boundary Service gjelder ikke alle Microsofts tjenester. Tjenesteproduksjonen gjennomgås for hvert fagsystem. ✓ |
| **B) Risiko for utlevering av personopplysninger til Microsoft** | • Ingen bruk av persondata utover til fakturering og forbedring av skyløsning. ✓<br>• Persondata blir pseudonymisert knyttet til hvem som har benyttet en tjeneste og når m.m. ✓<br>• I vilkårene for bruken av skytjenesten har Microsoft forbeholdt seg retten til tilgang til alle Kommunens data. De har dermed formelt adgang til å kunne benytte denne informasjonen. ✓ |

# Advokathuset PwC- overordnet ROS

| | |
|---|---|
| **C) Risiko for bruk av en databehandler som ikke er egnet (sine egne databehandleravtaler)** | • Advokathuset er ikke kjent med at tilsynsmyndighetene i praksis har håndhevet brudd på denne plikten isolert. ✓<br>• Skyleverandørene har egne bestemmelser som gjelder stort sett over hele verden. Disse er ikke helt i tråd med EU/EØS sine bestemmelser og er kontinuerlig under endring. ✓ |
| **D) Risiko for at kommunen mister kontroll med behandlingen** | • Endringer i Microsofts sine vilkår og rettstilstand ift. personvern er krevende å følge opp. ✓<br>• Kommunen har åpnet for bistand fra hovedleverandør – skal diskuteres i forhandlingene. ✓ |

Advokathuset PwC anbefaler bruk av tredjeparts kryptonøkler – et tiltak som understøttes generelt av datatilsynene i EU/EØS

Bruk av tredjeparts krypterings-nøkler ikke mulig uten å sterkt påvirke funksjonaliteten i det nye virtuelle datarommet i Azure. Det har foreløpig heller ikke ønsket effekt.

Det er konkludert med at risikoen er håndterbar ved flytting til sky. Det arbeides videre med kontinuerlig å styrke personvernet og se på f.eks. tredjeparts kryptering.