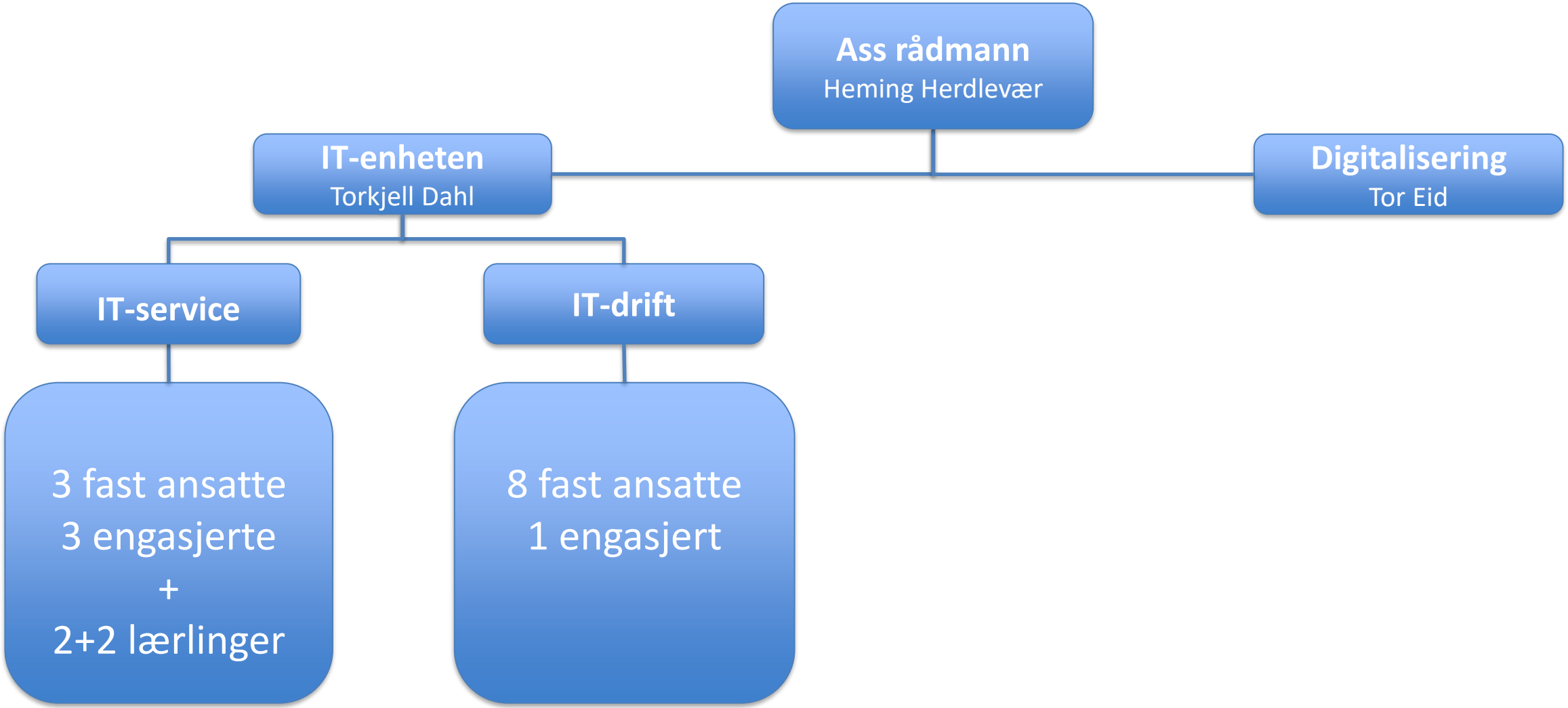
RINGERIKE
KOMMUNE

IT og digitalisering i Ringerike kommune

Ny plassering av IT og digitalisering fra 1. mai



Agenda

- Informasjonssikkerhet
- Status på oppfølging av digitaliseringsstrategien - satsningsområder fremover
- Forslag til styrket organisering
- Interkommunalt IT-samarbeid
- Bredbånd i Ringerike

RINGERIKE
KOMMUNE

Løsepengevirus

IT-enheten, Torkjell Dahl

Løsepengevirus hva er det?

- Program som tar til fange alle filer, dokumenter, systemer ved å kryptere de
- Kopierer ut data for å true med publisering og kartlegge nye offer
- Sikkerhetskopier ødelegges, slik at systemet ikke lar seg gjenopprette
- For å låse de opp igjen må man kjøpe nøkkelen fra angriper

Hvorfor?

- Det er anslått til å omsette for 20 milliarder dollar i 2021.

Hendelser

Kvi

En kvinne døde etter at hun måtte sende

NRK Nyheter Sport Kultur Humor Distrikt Mer Logg inn

Innlandet Tips oss Radio TV Langlesing Klassequizen 2020/2021

Østre Toten har vært uten datasystemer en måned etter hacking

ØSTRE TOTEN (NRK): PST mener dataangrep er en av de største truslene i 2021. I Østre Toten innrømmer ordføreren at sikkerheten ikke var god nok.

KREVENDE JOBB: Over 1000 PC-er måtte gjenopprettes i Østre Toten etter at noen tok seg inn bak brannmurene til kommunen, sletta alle sikkerhetskopier og krypterte alle data.
FOTO: ANDERS BAKKERUD LARSEN / NRK

Dag Kessel
Journalist

Knut Røsrud
Journalist

Publisert 8. feb. kl. 17:21
Oppdatert 8. feb. kl. 17:35

Østre Toten ble 9. januar offer for et stort dataangrep.

Dataangrepet på landbrukskommunen langs Mjøsa er det hittil verste som har rammet noen norsk kommune.

(Illustrasjonsfoto: Marius Jørgenrud)

ing-skandale-ryster-finland---pasient...

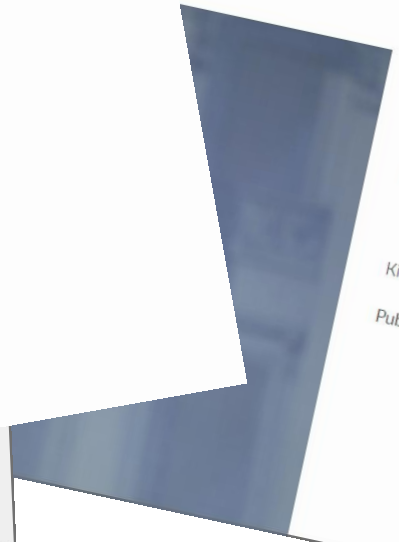
NRK P3 YR

kt Mer Logg inn Søk

t: Krig og fred Urix på NRK TV

er Finland - pasienter

etter hacking,



Bjørnar Hjellen
@bjornarhjellen
Journalist

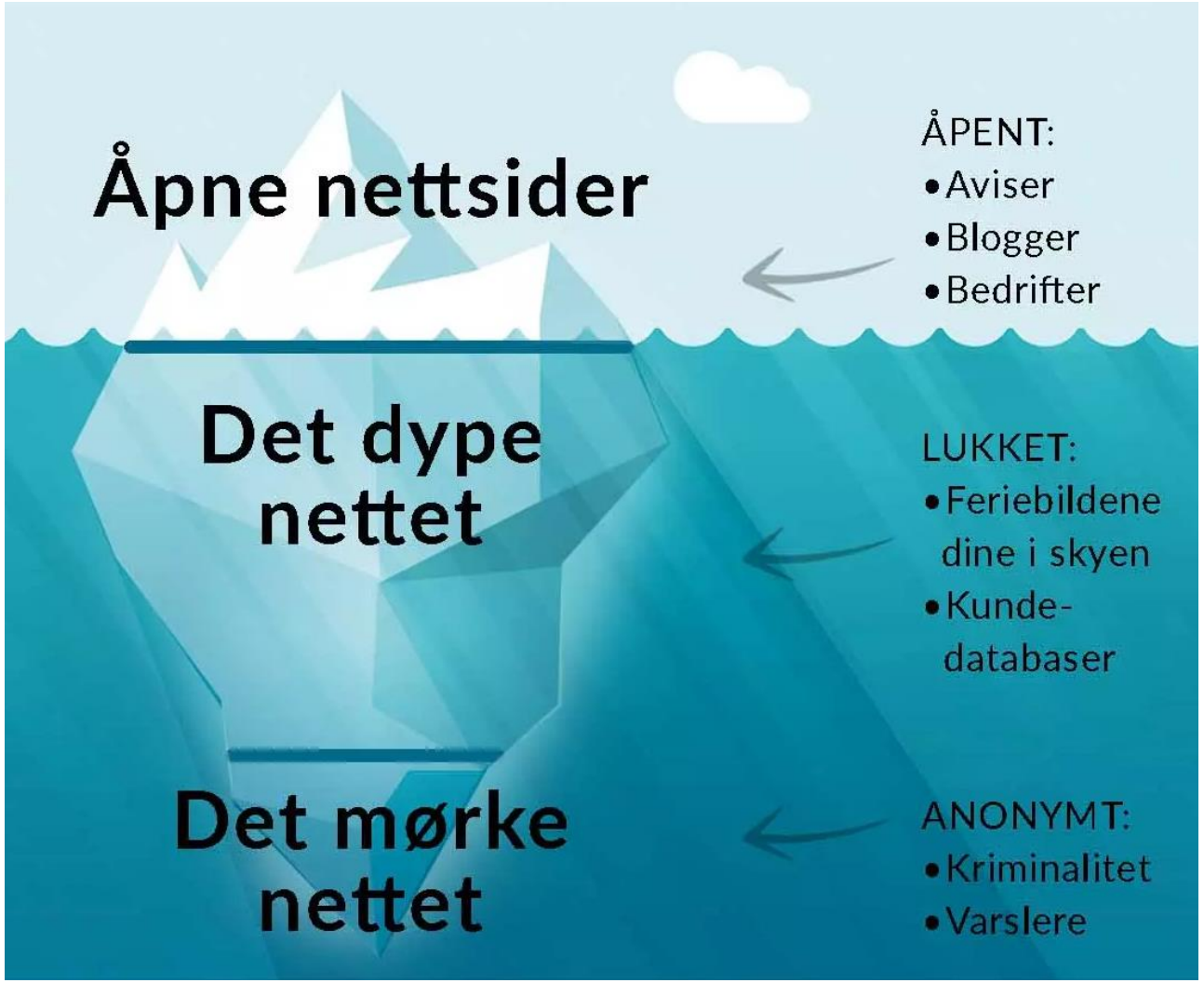
Kilde: NTB-NRK

Publisert 25. okt. 2020 kl. 12:58

Hendelsesforløp, innsamling

- Startet for lenge siden
- Phishing av informasjon fra brukere.
- Hacking av store samlinger av brukerdata.
- Dataene samles på det vi kaller det mørke nettet (Darkweb).
- 11,388,405,982 kontoer affektert.

- Sjekk deg selv på: www.haveibeenpwned.com



Darkweb

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords

Darkweb

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Darkweb

MyHeritage: In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, Passwords

Facebook

In April 2021, a large data set of over 500 million Facebook users was made freely available for download. Encompassing approximately 20% of Facebook's subscribers, the data was allegedly obtained by exploiting a vulnerability Facebook advises they rectified in August 2019. The primary value of the data is the association of phone numbers to identities; whilst each record included phone, only 2.5 million contained an email address. Most records contained names and genders with many also including dates of birth, location, relationship status and employer.

Breach date: 1 August 2019
Date added to HIBP: 4 April 2021
Compromised accounts: 509,458,528
Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, Names, Phone numbers, Relationship statuses
Permalink

Hendelsesforløp, hacker/løsepengevirus får tilgang

- Skygge IT, løsninger som tas i bruk utenfor standarder
  - Mangelfull: installasjon, vedlikeholds regime/oppdateringer, overvåkning
- Ansatte
  - Lenker eller vedlegg i e-poster, SMS – følges gjerne opp med manipulering
  - Installert «uautorisert» programvare på PC
- Teknisk gjeld
  - Hardware/software som ikke oppdateres.
  - Utstyr som det ikke er kapasitet til å vedlikeholde.
  - Installasjoner fjernes ikke skikkelig ved fraflytting/nedleggelse.
- Løsninger for fjernadministrasjon
  - Leverandør tilgang til server/tjenester
  - Utilsiktet åpning som ikke lukkes
- Feilkonfigurasjon ved installasjon av server/tjeneste
- Hackere lurer virus inn i legitime oppdateringer til viktige systemer
- Fysisk tilgang til infrastruktur

Hendelsesforløp, kartlegging av offer etter tilgang

- Automatisk og manuell kartlegging
- Leter etter sårbarheter på innsiden for å spre seg viere
- Tester ut brukernavn og passord fra darkweb
- Forsøker å logge seg på flere enheter (PC, servere, databaser, utstyr etc)
- Søker å få tilgang til høyere sikkerhetsnivåer
- Når bør offeret angripes
- Totaloversikt over systemer
- Ødelegge backuper
- Hvor mye penger skal kreves i løsepenger
- Kartleggingen varer
- Mål: hvordan lamme offeret mest mulig

Hendelsesforløp, gjennomføring

- Fjerning av backup
- Kopiering av interessant informasjon til angriper (også personinformasjon)
- Kryptering av kommunens servere og filer
- Gjennomføringen ferdigstilles på noen timer, gjerne om natta og i en helg
- Legger igjen informasjon for hvordan betale løsepenger for å få verktøy til å dekryptere servere og filer

Hvordan ser situasjonen ut etter et slikt angrep

- Alle IT systemer er ute av funksjon
- PCer må ikke brukes uten IT bistand
- Virus må letes opp og fjernes fra alle systemer og maskiner
- Gjenoppretting av servere en etter en, fra «offline» sikkerhetskopier. Offline sikkerhetskopier fjernlagres en gang hver mnd. Medfører tap av opp til 30 dagers produksjon.
- Systemene og PCene blir tilgjengelige for bruk en etter en.
- Det vil ta flere måneder før kommunen er i normaldrift igjen.
- Full stans i annen digitalisering. Ingen nye systemer, oppgraderinger eller nye bygg kan etableres i denne perioden.

Litt informasjon om Østre Toten

- Østre Toten kommune rammet av kryptovirus lørdag 9. januar
- De fleste måtte arbeide med papir og blyant
- Mange måneder før fagsystemer er tilgjengelig igjen
- Eksempler:
  - Utfordringer med å betale og sende ut regninger, lønnsutbetaling
  - Helsestasjonen viste ikke om sine timeavtaler
  - Forberedelser av saker til politisk behandling stoppet opp
  - Byggesaksbehandling uten tilgang til tidligere saksbehandling
  - Pasientbehandling uten tilgang til journal

Etterspill

- Østre Toten har inngått kontrakt om at IT-drift gjøres av «IKOMM», som nekter å ta imot gamle backuper fordi de kan inneholde bakdører/viruset
- Personopplysninger fra Østre Toten er publisert på «det mørke nettet»
- Erstatningsansvar ovenfor innbyggere som har fått sine personopplysninger publisert
- Tilsynet arbeider med gebyr

nrk

Nyheter Sport Kultur Humor Distrikt Mer

Innlandet Tips oss Radio TV Langlesing Klassequizen 2020/2021

Logg inn

Kommunen kan få kjempegebyr etter at de ble hacka

Personopplysningene til innbyggere i Østre Toten har havnet på «det mørke nettet». Kommunen kan både bli erstatningsansvarlig og få gebyr.

Innbyggertorg
Ordfører
Kommunedirektør
Østre Toten Boligstiftelse
Bibliotek
Studiesenter/Møterom
NAV
Fagforeninger
Hovedverneombud
Helse- og omsorgstjenester
Helsestasjon
Barnevern
Plan og Næring
Skole
Barnehage

Senterpartiordfører Bror Helgestad i Østre Toten, er bekymret for den sensitive informasjonen som har kommet på avveie.
FOTO: ANNE KARI LØBERG / NRK

Vibecke Wold Haagensen
@NRKvibecke
Journalist

Anne Kari Løberg
Journalist

Vi rapporterer fra Lena

Publisert 8. apr. kl. 09:43
Oppdatert 8. apr. kl. 13:30

Det var natt til lørdag 9. januar at Østre Toten ble utsatt for et dataangrep.

Noen tok seg inn bak brannmurene til kommunen, slettet alle sikkerhetskopier og krypterte alle data. Etterforskingen viste at data ble lagt ut på det mørke nettet. .

Ordfører Bror Helgestad, sier at av 1800 filer som er lekka er det 200 filer som inneholder personsensitive opplysninger.

– Et titalls personer på rødt nivå, er vi i gang med å varsle, sier Bror Helgestad.

KOMMUNAL RAPPORT

Datasikkerhet

Østre Toten ble varslet om sikkerhetshull

Like før jul ble Østre Toten **INFORMERT OM MANGLER** ved kommunens datasikkerhet. Få uker etter var datasystemet lammet.

Etter flere helger med mye jobbing startet kommunedirektør Ole Magnus Stensrud lørdag 9. januar med en kaffe på senga. På kommunens interne Facebook-side så han en melding fra IT-avdelingen om at systemene var nede, men at de jobbet med saken. Likevel var han helt uforberedt på økonomisjefen ringte få minutter etter. Østre Toten hadde hatt et stort datainnbrudd.

Mest omfattende

I løpet av kort tid var det klart at kommunen i Innlandet sto overfor det mest omfattende datainnbruddet noen norsk kommune har opplevd til nå. Alle data var blitt kryptert. Sikkerhetskopier og logger var slettet. Alle fagsystemer gjort utilgjengelige.

Tilbake lå en hilsen fra angriperne. Betal, og få dataene tilbake. Ellers legger vi dem ut på Internett. Signert «Protect your system, amigo».

– Det gikk nok litt tid før jeg skjønte omfanget. Jeg forsto at systemene var nede. Men omfanget - at vi ikke hadde sikkerhetskopi og konsekvensene av at vi måtte bygge opp alt på nytt - det tok lengre tid, sier Stensrud.

På et øyeblikk mistet Østre Totens ansatte tilgang til kommunens IT-systemer. Ansatte måtte ta fram penn og papir. På sykehjemmer fikk beboere utdelt bjeller de kunne bruke for å signalisere at de trengte hjelp. Ordfører Bror Helgestad (Sp) beskrev det som å rykke tilbake til 1975 på én helg.

Ble advart

Få uker før dette skjedde var selskapet Atea ferdig med en gjennomgang av IT-sikkerheten i Østre Toten. Rapporten, som kommunen likk tilsendt i desember, avdekket mangler ved kommunens datasikkerhet.

Rapporten er unntatt offentlighet. Men til formannskapet har Stensrud fortalt at selskapet blant annet anbefalte at sikkerhetskopier måtte lagres atskilt fra datanettverk. Og at det fantes måter å ta seg inn i datasystemene på, som kommunen ikke hadde vurdert.

– Noen av disse sårbarhetene visste vi kanskje om fra før. Andre var nye. Vi skulle ta tak i rapporten og gjøre noe med de sikkerhetsutfordringene som var avdekket. Men da kom hackerne oss i forkjøpet. Vi vet ikke om hackerne hadde kommet inn hvis vi hadde gjennomført noen av disse sikkerhetstiltakene før nyttår, sier Stensrud.

Hvordan skjedde det?

Hvordan kom dataangriperne seg inn? Politibetjent og etterforskningsleder André Hals ved Innlandet politidistrikt er ordknapp.

– Det kan jeg ikke si noe om, sier Hals.

Han sier at etterforskningen er godt i gang. Politiet samarbeider med Østre Toten og deres IKT-ansvarlige. Men hvilke etterforskningsskritt de har tatt, hvem de ellers samarbeider med, hva de har funnet ut eller når de tror de er ferdige, svarer han ikke på.

– Saken er høyt prioritert hos oss. Det er kriminalitet med alvorlige konsekvenser for dem som blir berørt. Slike saker er veldig kompliserte og krever omfattende arbeid. Vi kan derfor ikke si noe om saksforløpet, sier Hals.

– Er dataene spredd?

– Det kan jeg ikke svare på i det trinnet vi er på i etterforskningen, sier Hals.

Vil slite i et halvt år

Tre uker etter at dataangrepet ble oppdaget, er Østre Toten fremdeles i knestående.

De grunnleggende tjenestene blir levert, slik som omsorg for sykehjemsbeboere, undervisning og barnehagetilbud. Takket være Nav i Vestre Toten får sosialhjelpsmottakere utbetalt penger. Gjøvik kommune gir Østre Toten tilgang til deres felles økonomi-, HR- og personalsystemer fra rådhuset på Gjøvik. Så ansatte får lønn, og regninger blir betalt.

Men fagsystemene for øvrig er fremdeles utilgjengelige. Helsestasjonene har ikke tilgang til timeavtaler. Skolen kan ikke bruke digitale læringsplattformer. Saksbehandlere på byggesak mangler tilgang på historisk dokumentasjon. Forberedelse av saker til politisk behandling har stoppet opp. Kommunen får i hovedsak ikke sendt ut fakturaer. Det er full stans i rapportering til statlige myndigheter.

Stensrud opererte først med 8. februar som dato for når fagsystemene skulle være oppe igjen. Nå sier han at det trolig vil ta 4-6 måneder før alt er tilbake til normalen.

– Barnevernstjenesten har vår høyeste prioritet når det gjelder tilgang til fagsystemene. Tilgang til data er kritisk. Spesielt innenfor barnevernstjenesten, med barn som skal følges opp, sier Stensrud.

Han vet ennå ikke hva dataangrepet vil koste, annet enn at kostnadene er «betydelige».

Vi har ikke egen dataforsikring, men har ansvarsforsikring. Vi vet ikke hva den vil omfatte. Vi har vært i kontakt med statsforvalteren. Vi kommer til å søke om skjønnsmidler. Blir du rammet av en katastrofe, finnes det ulike ordninger for det. Dette er en katastrofe for oss når gjelder dataene våre, sier Stensrud.

Vil lære av egne feil

Østre Toten jobber nå langs tre spor: De skal bygge opp ny datainfrastruktur, bygge opp fagsystemene og avdekke hva som har skjedd og omfanget av det.

Til formannskapet sist uke hadde Stensrud noen gode nyheter. Selv om sikkerhetskopiene er slettet, ser det ut til at kommunen klarer å gjenopprette data fra et digitalt øyeblikksbilde som ble tatt dagen før innbruddet satte systemet ut av spill. Østre Toten har ikke fått noen indikasjoner på at personsensitive data er spredd. Det var og er kommuneledelsens største frykt.

– Noen stiller seg spørsmålet om kommunens systemer har vært sikre. I og med at noen har klart å trenge seg inn i dem, har de ikke vært sikre nok. Det kan vi konkludere med. Det med IT-sikkerhet ikke noe man blir ferdig med, men noe man må jobbe med hele tiden, sier Stensrud.

Parallelt med at innbruddet etterforskes har Stensrud bestilt en ekstern gjennomgang. En faktaundersøkelse av IT-sikkerheten i Østre Toten kommune. Når den er klar, vet han foreløpig ikke.

– Den skal gå gjennom selve hendelsen; hva skjedde, hva var årsaken, konsekvenser og læringspunkter. Hva kan vi lære av dette og hva kan Kommune-Norge lære av dette, sier Stensrud.

HANNE WIEN
hanne@kommunal-rapport.no

Kommunedirektør Ole Magnus Stensrud sier datainnbruddet er kjempeutfordrende. Hans første tanke var å sørge for at liv og helse ikke gikk tapt. Tjenestene innen pleie og omsorg måtte leveres, uansett datainnbrudd.
ARKIVFOTO: MAGNUS KNUTSEN BJØRKE

Advarer kommunene om løsepengevirus

Koronapandemien gjør offentlige virksomheter mer sårbare mot digitale trusler, advarer Nasjonal sikkerhetsmyndighet.

Dagen etter at dataangrepet lammet Østre Toten, sendte Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap og Kommune-CSIRT ut et felles varsel om løsepengevirus til kommunene.

I varselet skrev de at det aktuelle løsepengeviruset er kjent som Mespinoza/PYSA, og at de var kjent med lignende angrep mot lokale myndigheter i Frankrike. Fra disse og andre kjente hendelser vet de at aktørene forsøker å ta seg inn i datanettverket ved å bruke datakraft til å knekke brukernes passord.

Kommer de seg inn i nettverker, forsøker de å bevege seg mellom maskiner ved hjelp av fjernpåloggingsverktøy. De har brukt et dataverktøy som fanger opp passord idet man skriver dem. Hackerne har også forsøkt å hente ned passorddatabaser for å få tilgang til flere brukere.

Er de først inne, har de skrudd av antivirusløsninger, slettet sikkerhetskopier og hentet ut detaljer om nettverk, brukere og databaser.

I risikobildet som NSM laget for 2020 ble det advart om at økt bruk av digitale fjerntilgangsløsninger under koronapandemien gjør virksomheter mer sårbare mot digitale trusler.

NSM pekte også på at løsepengevirus i økende grad rammer norske virksomheter.

HANNE WIEN
hanne@kommunal-rapport.no

Kan Ringerike kommune bli rammet av løsepengevirus?

JA

Hva må organisasjonen gjøre?

- Fortsette å fokusere på ansattes sikkerhets kompetanse
- Hyppig gjennomgang med toppledelsen
- Fortsette arbeid med rutiner og opplæring i disse
- Gjøre bedre bestillinger i anbud, ta tid til å involvere IT og vente til det er kapasitet
- Fysisk sikring av tilgang til kontorer, dokumenter og infrastruktur
- Alle deler av organisasjonen har en plan/instruks for hvordan de arbeider når IT verktøyene ikke er tilgjengelige

IT arbeid som forhindrer

- Unngå skygge IT
  - Porteføljestyring og prosjektmetodikk
  - All digitalisering innom/gjennom IT
- Ekstern gjennomgang av sikkerhet
  - ISO27002
  - Skanning av nettverk internt og eksternt
- Tettere teknisk leverandøroppfølging
  - Oppfølging og kontroll av fjerndriftsløsninger
  - Nye systemer og teknologi
  - Byggeprosjekter
- Sikkerhetskopier
- Involvering og resurser til å avvikle teknisk gjeld
- Trygg og rett forvaltningskapasitet for IT-drift

PS! Selv om andre kommuner bruker en løsning eller at det er en stor aktør, er det ikke gitt at det vil fungere optimalt og trygt i Ringerike.

IT arbeider kontinuerlig med å forbedre sikkerhet og forhindre å bli utsatt for kryptovirus.

Her er litt fra sist ISO27002 samsvarsanalyse:

Rapport etter ISO 27002 samsvarsanalyse i Ringerike kommune (de enkelte sikringstiltakene)

Hovedområde 12	Driftssikkerhet
§	**12.1.3 Kapasitetsstyring** **Sikringstiltak:** Bruk av ressurser bør overvåkes og reguleres, og anslag over framtidige kapasitetsbehov bør utarbeides for å sikre nødvendig systemprestasjon.
 	**Funn** Alt er på plass rundt teknisk kapasitetsstyring. Derimot er det åpenbart at ITE er underbemannet i forhold til et økende antall systemer med økende kompleksitet og tilhørende økende supportbehov. Det er misforhold mellom det ansvaret en forvalter og de ressursene en har til rådighet. Dette kommer bl.a. til uttrykk ved at en ikke har dublisert systemkunnskap for kritisk viktige områder, og ved at supportnøkkeltallet (KPI'en) *Gjennomsnittlig rettetid* har økt fra 51 timer i 2016 til 100 timer i 2019. For lav bemanning = Økt risiko for sikkerhetshendelser.
 	**Anbefalt tiltak** 1. ISO 27002 12.1.3 understreker at kapasitetsstyring er vel så viktig relatert til menneskelige ressurser. Situasjonen i IT-enheten gjør det nødvendig at enhetens leder jevnlig adresserer kapasitetsstyring i planleggings /koordinerende/ rapporterende-møter med avdeling Økonomi og IT.

Rapport etter ISO 27002 samsvarsanalyse i Ringerike kommune (de enkelte sikringstiltakene)

Hovedområde 8	Forvaltning av aktiva
§	**8.1.1 Oversikt over aktiva (hvor aktiva er hardware og software som benyttes til informasjonsutveksling)** **Sikringstiltak:** Aktiva knyttet til informasjon og systemer for informasjonsbehandling bør identifiseres, og en oversikt over disse aktivaene bør utarbeides og vedlikeholdes.
 	**Funn** IT-enheten (ITE) har god oversikt over alle systemer som er etablert i henhold til besluttet rutine om at ITE skal orienteres om ethvert nytt system som tas i bruk. Dessverre er det en god del «skygge-IT» hvilket vil si at systemer tas i bruk uten at ITE involveres.. ITE arbeider derfor med å få etablert RÅDET FOR NYE SYSTEMER hvor alle planlagte systeminvesteringer skal godkjennes og registreres. ITE erkjenner at alle systemer skal ha eierskap ved klart definert systemeier.
 	**Anbefalt tiltak** 1. RÅDET FOR NYE SYSTEMER etableres og målet er å få bedre systemoversikt og kontroll med systemforvaltningen. Det etableres godkjenningsrutine for ethvert nytt system som ønskes implementert og rutinen skal inneholde spesifisering av sanksjoner ved brudd på rutinen. 2. Systemoversikten (nå fri for «skygge-IT») har records for alle relevante driftsparametre som systemnavn, systemeier, systemansvarlig, systembeskrivelse, versjons-ID, leverandør, end-of-life, fornyelsesdatoer osv. 3. I systemoversikten prioriteres det at alle systemer skal ha klart definert systemeier. *Ifølge Informasjonssikkerhet og personvern i Ringerike kommune* er det kommunalsjefene som har systemeierrollen, og ansvar er definert, Jfr. eksempel på rutine for systemoversikt som følger denne rapporten.

RINGERIKE KOMMUNE

Oppfølging av digitaliseringsstrategien

Digitaliseringssjef Tor Eid

Ringerikes digitaliseringsstrategi 2017-2019

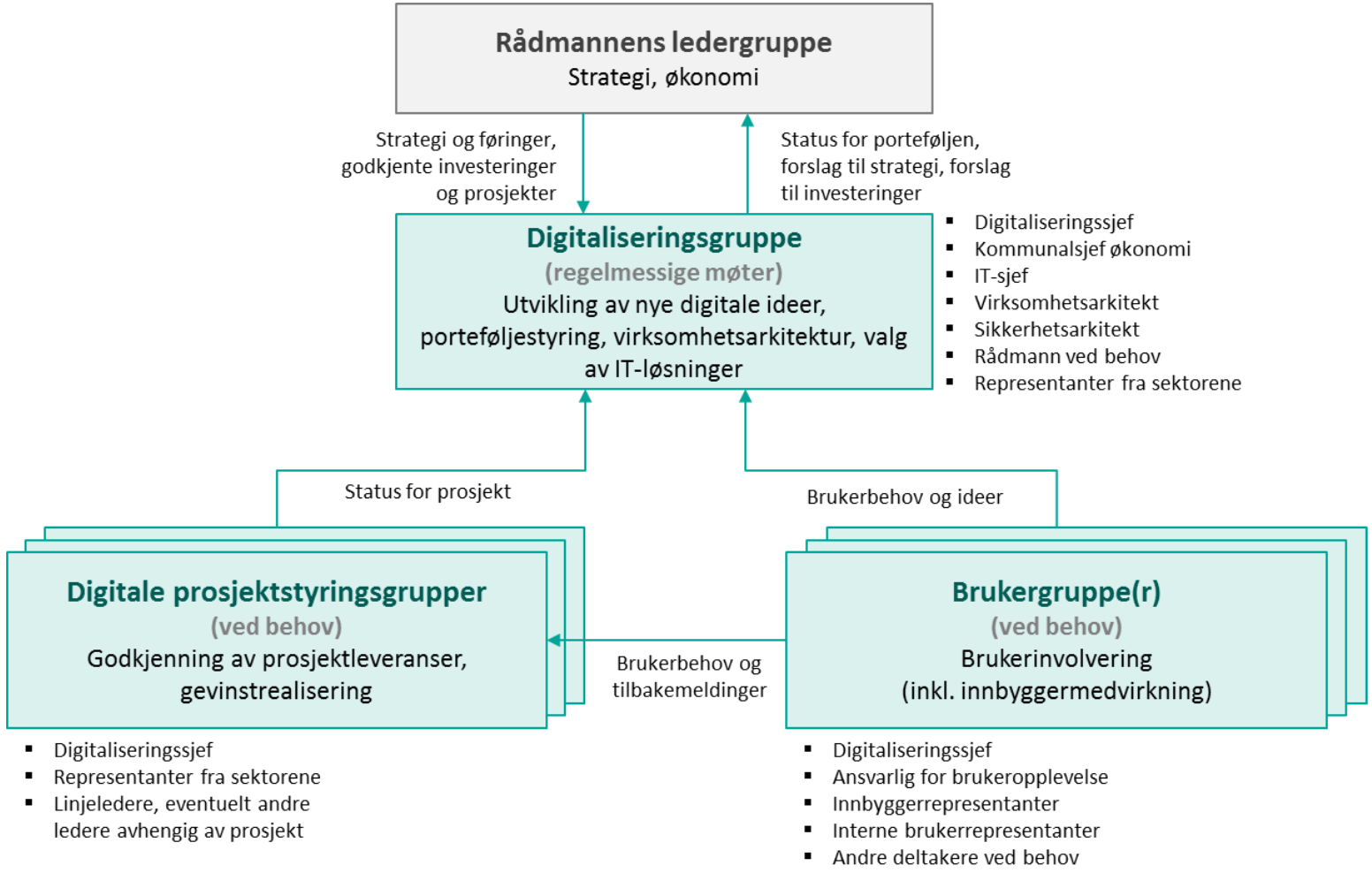
- Vi skal fornye og forenkle Ringerike inn i en ny tid

- Fornye
  - Utnytte de teknologiske mulighetene
  - Raskt ute med å ta i bruk digitale løsninger
- Forenkle
  - Lett tilgjengelige tjenester, enkle å bruke, når som helst og hvor som helst
  - Jobbe så effektivt som mulig
- Ny tid
  - Utvikle oss til en moderne kommune som folk og næringsliv ønsker å komme til
  - Enda bedre tjenester, tilpasset hver enkelt
  - Livskvalitet i alle livets faser

Strategiske målområder

A. Smartere og bedre velferds- og oppvekstttjenester
B. Levere tjenestene på en smartere og mer effektiv måte
C. Lytte til innbyggerne og næringslivet, enkel å kommunisere med
D. Digital kompetanse, for både innbyggere og ansatte
E. **Den digitale satsingen planlegges og styres på en systematisk måte**

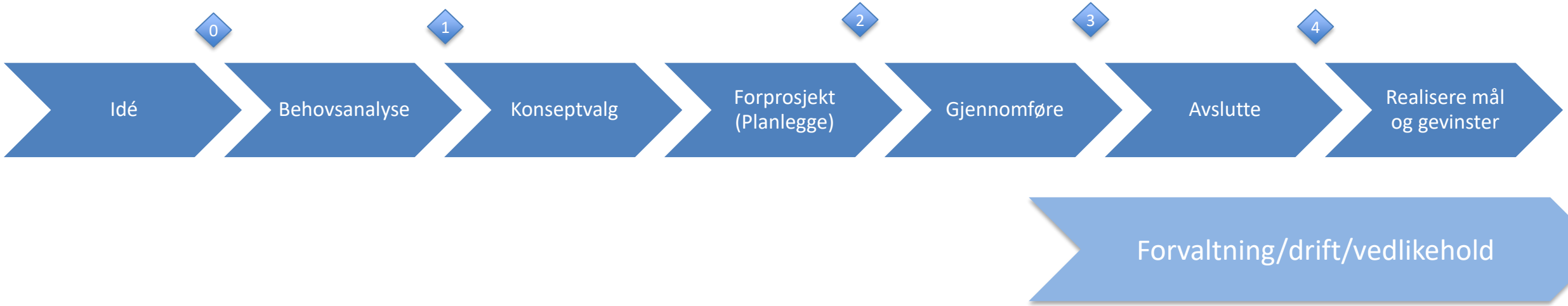
Styringsmodell for digitalisering



Samordning og standardisering

- 1. Digitaliseringsgruppe
  - Tverrsektoriell
  - Forankring i topp-ledelsen
  - Skal vurdere digitaliseringstiltak før gjennomføring/anskaffelse
  - Samordning
  - Øke digitaliseringskompetansen
- 2. Porteføljestyring
- 3. Felles modell for gjennomføring av digitaliseringsprosjekter

Prosjektmodell for digitaliseringsprosjekter



Viktige satsningsområder 1

- Informasjonssikkerhet og personvern
  - Lederfokus og kultur!
  - Styrende dokumentasjon, beredskapsplaner
  - Personvernombud
  - Økt bruk av skytjenester
  - Tilgangsstyring til nettverk, trådløst nett
  - VAR – sikkert nett, sikker arbeidsflate
  - Byggstyring

Viktige satsningsområder 2

- Effektiv samhandling på tvers
  - Microsoft 365, inkl Teams
  - Nytt saks-/arkivsystem
  - Nytt intranett
  - E-læring / kompetanseheving
  - Mobile løsninger

Viktige satsningsområder 3

- E-helse
  - Pandemi-støtte
  - Helsehjelp på nye måter:
    - Velferdsteknologi, teknologi i nye helsebygg
  - Fagsystemer/Pasientjournaler (legevakt, helsestasjon, fastleger, mm)
    - Modernisering og bedre samhandling
    - Legemiddelhåndtering
    - Nasjonalt arbeid – Felles kommunal journal (FKJ)

Viktige satsningsområder 4

- Digitale innbyggertjenester
  - Kommunikasjon, innsyn og selvbetjening
  - Innbyggerinvolvering
    - «E-demokrati», «folkebudsjettering»
  - Modernisering av og integrasjoner med bakenforliggende systemer
  - Automatisering og robotisering

Viktige satsningsområder 5

- Innsikt og dataanalyse
  - «Business Intelligence» (BI)
  - Kunstig intelligens
  - Prognosestyrt organisasjon
  - Kapasitetsanalyser
  - Deling av data på tvers

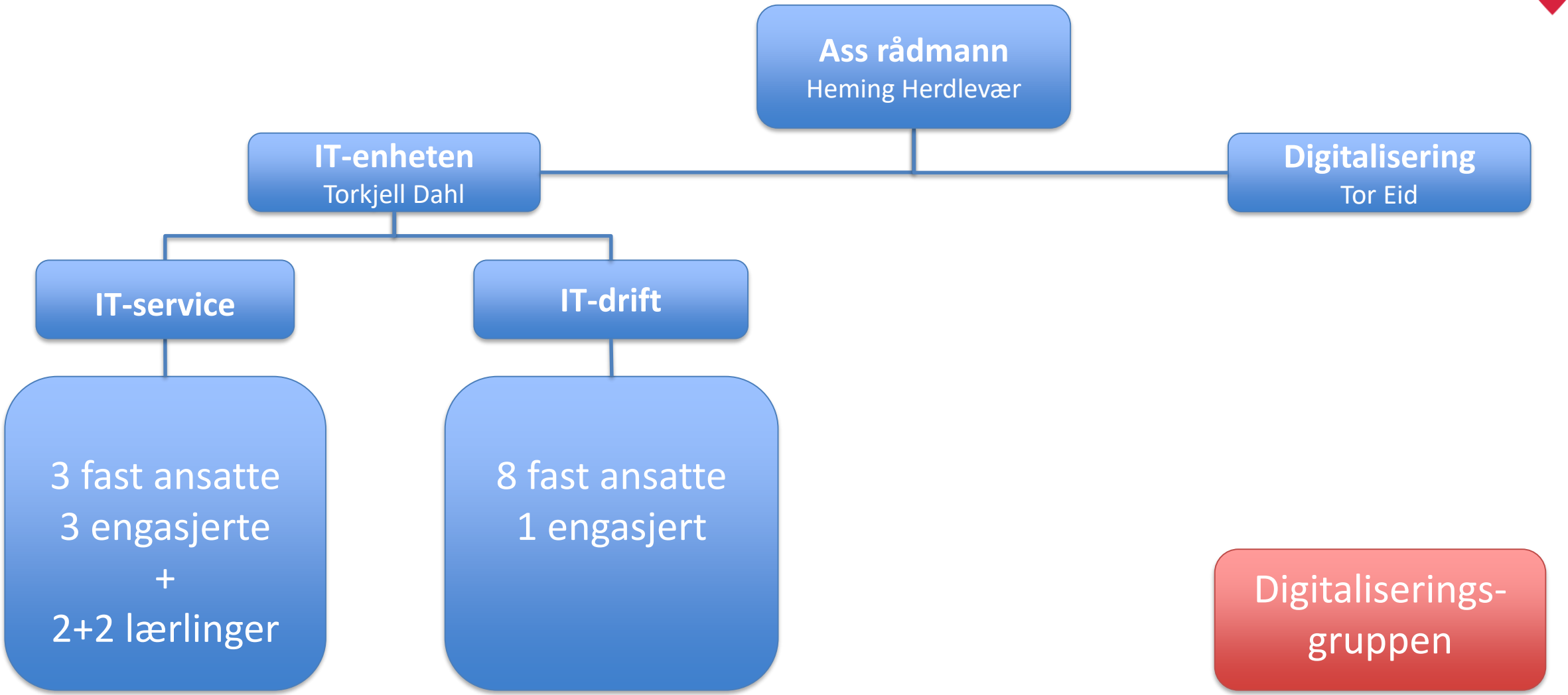
Viktige satsningsområder 6

- Kompetanse, styring og økt gjennomføringskraft
  - Sikre tilstrekkelig og riktig kompetanse
  - Videreutvikle en robust digital grunnmur
  - Kontinuerlig forbedring av vår digitale portefølje for å understøtte kommunens strategiske mål
  - Videre utvikling av kommunens digitaliseringsstrategi, virksomhetsarkitektur, porteføljeforvaltning, metoder og verktøy for prosjektledelse

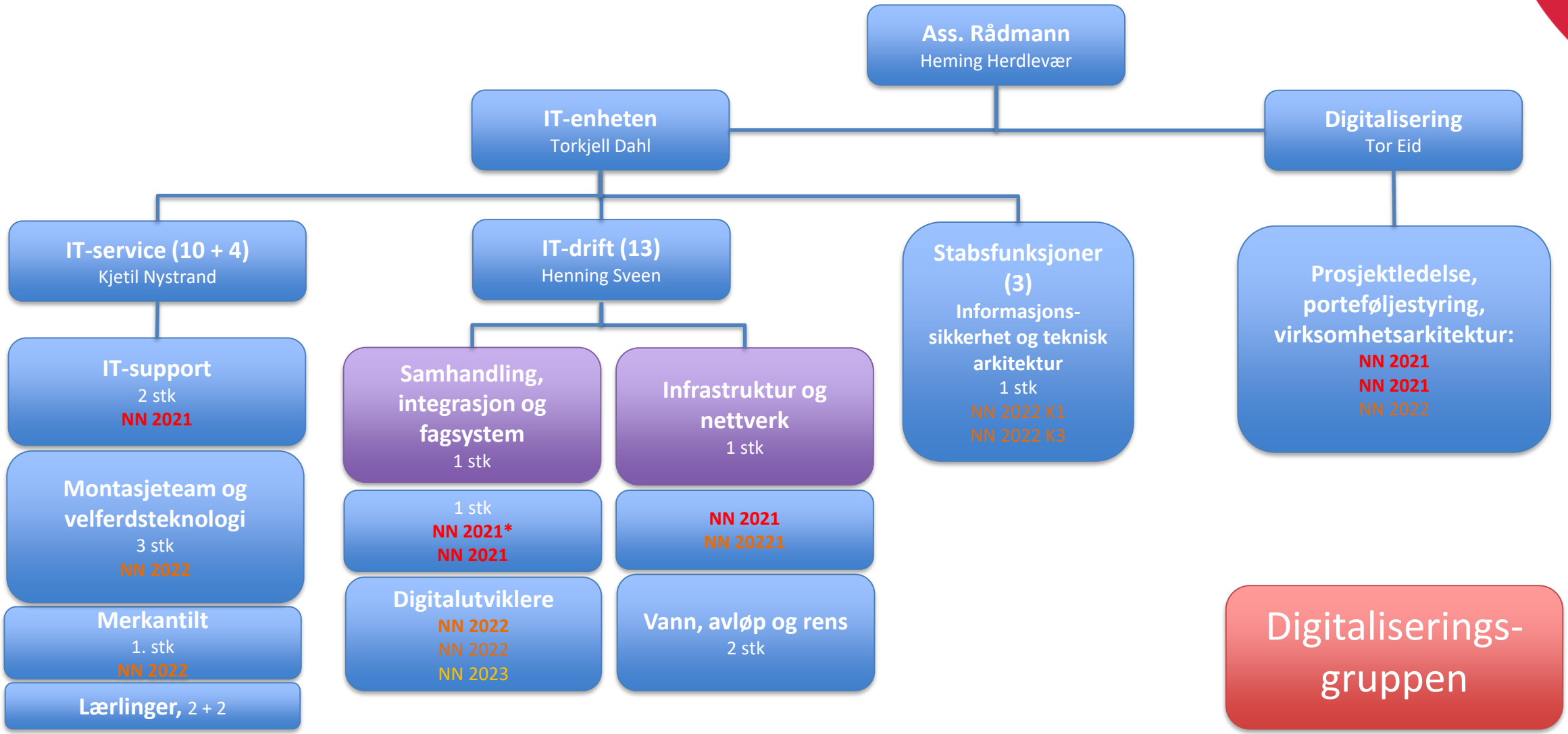
RINGERIKE
KOMMUNE

Stryket organisering

Dagens organisering av IT og digitalisering



Styrket organisering av IT og digitalisering



RINGERIKE
KOMMUNE

Interkommunalt samarbeid

Interkommunalt samarbeid

- DigiViken
  - Styrke kompetanse og gjennomføringskraft
  - Ivareta medlemskommunenes interesser i nasjonale digitaliseringstiltak
  - Sette en strategisk retning
  - Legge til rette for samarbeid

  - Interimsperiode i 2021, drift fra 2022
  - Programkontor, 2 ansatte, Bærum kommune er vert

Interkommunalt samarbeid

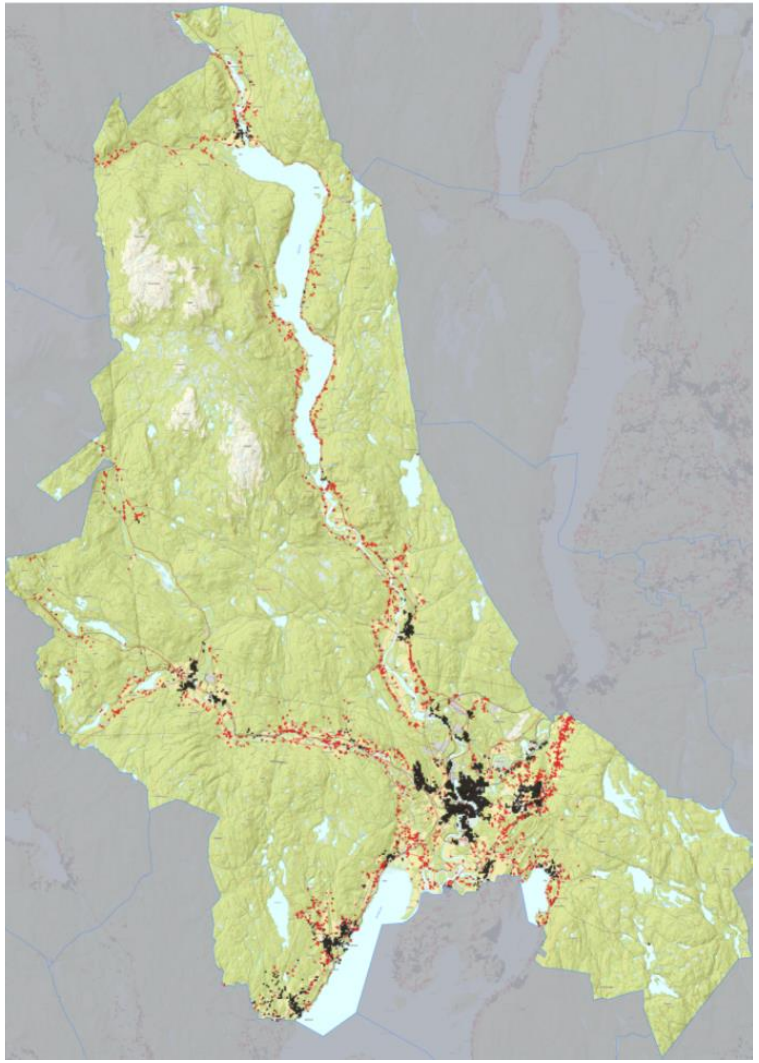
- Uformelt IT-forum (Hole, Jevnaker, Ringerike)
- Modum
  - Kommunestyrevedtak om å utrede samarbeid med Ringerike
- Jevnaker
  - Utreder nå organisering av IT-funksjonen – foreslår et interkommunalt IT-selskap med Ringerike, Modum, Hole, Jevnaker, Gran og Lunner

RINGERIKE
KOMMUNE

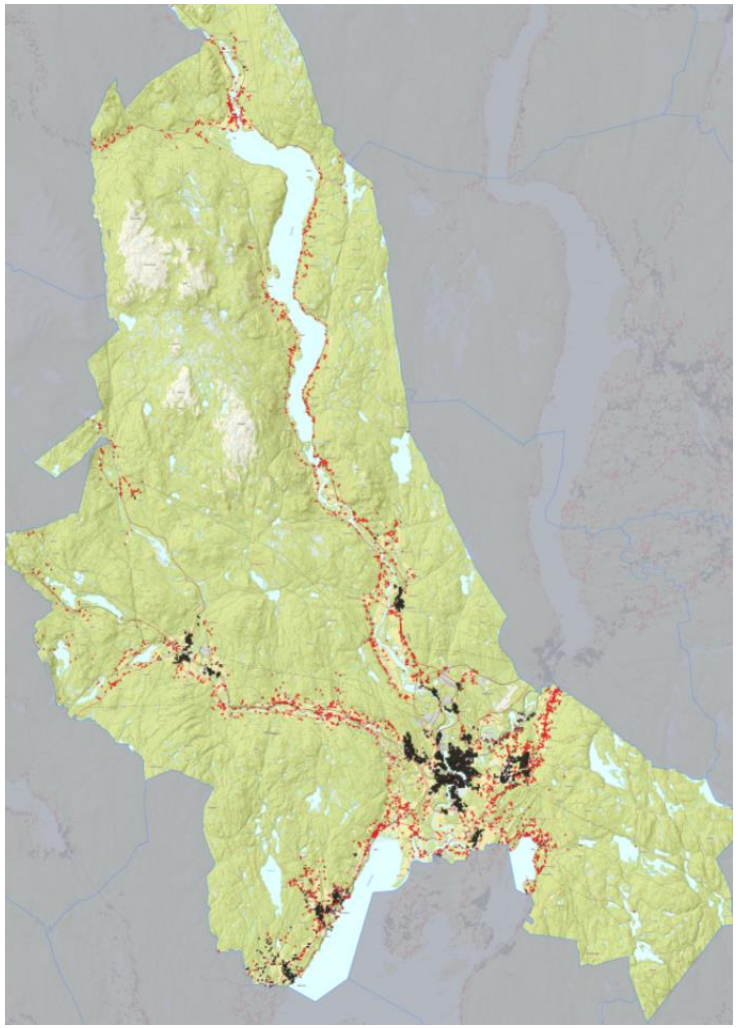
Bredbånd

Bredbånd i Ringerike – kartlegging 2020

30 Mb/S = 98% dekning



100 Mb/S = 78% dekning



Bredbånd i Ringerike

- Det utarbeides en bredbåndsstrategi for Ringerike
  - Definisjoner, ambisjoner og mål
  - Hvordan ny bredbåndslov påvirker
  - Kommunens rolle som tilbyder/utbygger av infrastruktur
    - Hvordan kan vi bruke egen (og andres) graving
  - Bruk av kommunens egen digitale infrastruktur

Takk for oppmerksomheten!

RINGERIKE
nærmest det meste

RINGERIKE
KOMMUNE