RINGERIKE KOMMUNE

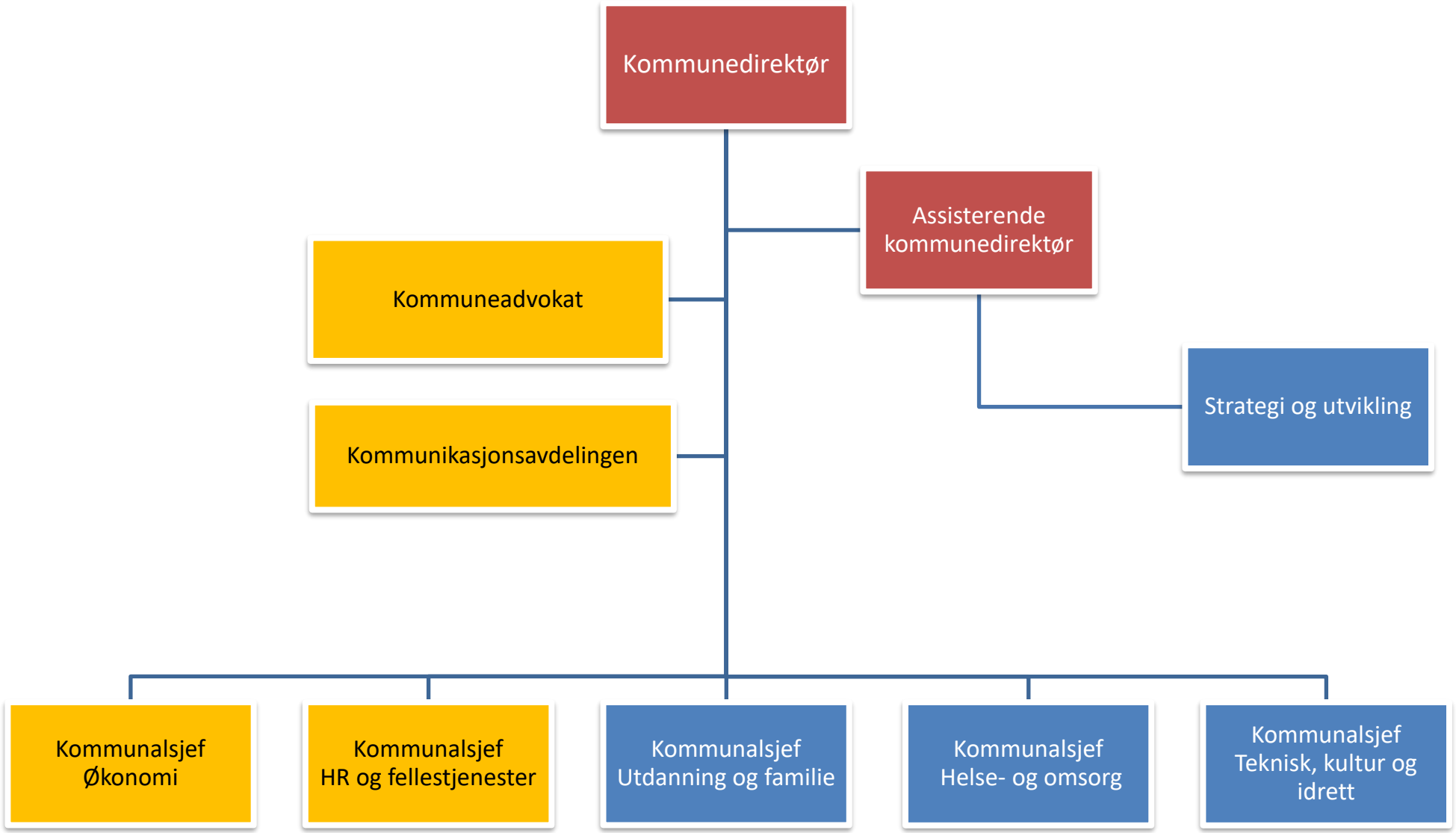
Digital Folkevalgt 2023

IT-enheten, Torkjell Dahl

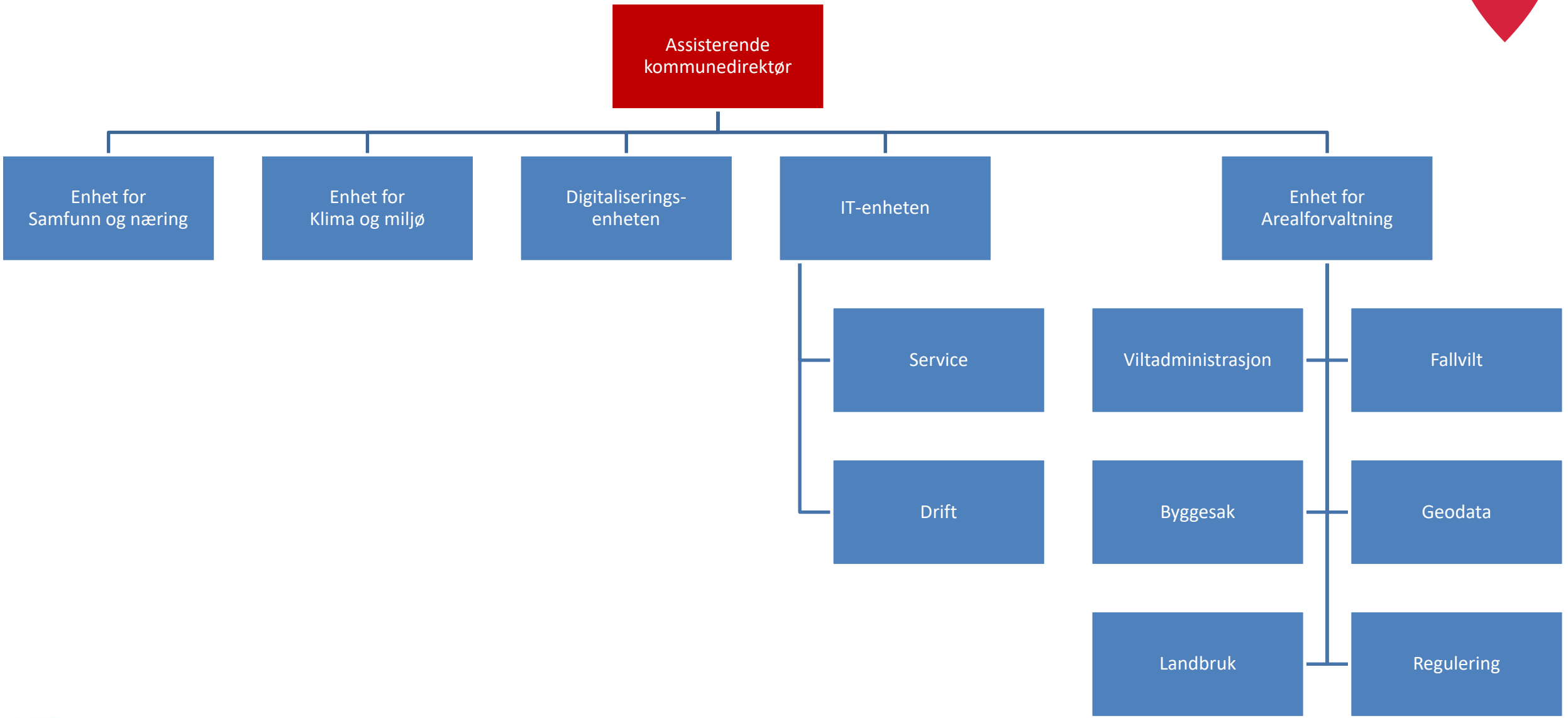
Innhold

- IT organisasjon og nøkkeltall
- Demonstrasjon av iPad og apper
- Hva kan vi få hjelp til?
- Hvordan få hjelp
- Privat bruk
- Sikkerhetssituasjonen
- Ansvarsforhold
- Lokal status
- Hvordan påvirkes politikerrollen
- Tips

Ringerike kommune - organisasjon

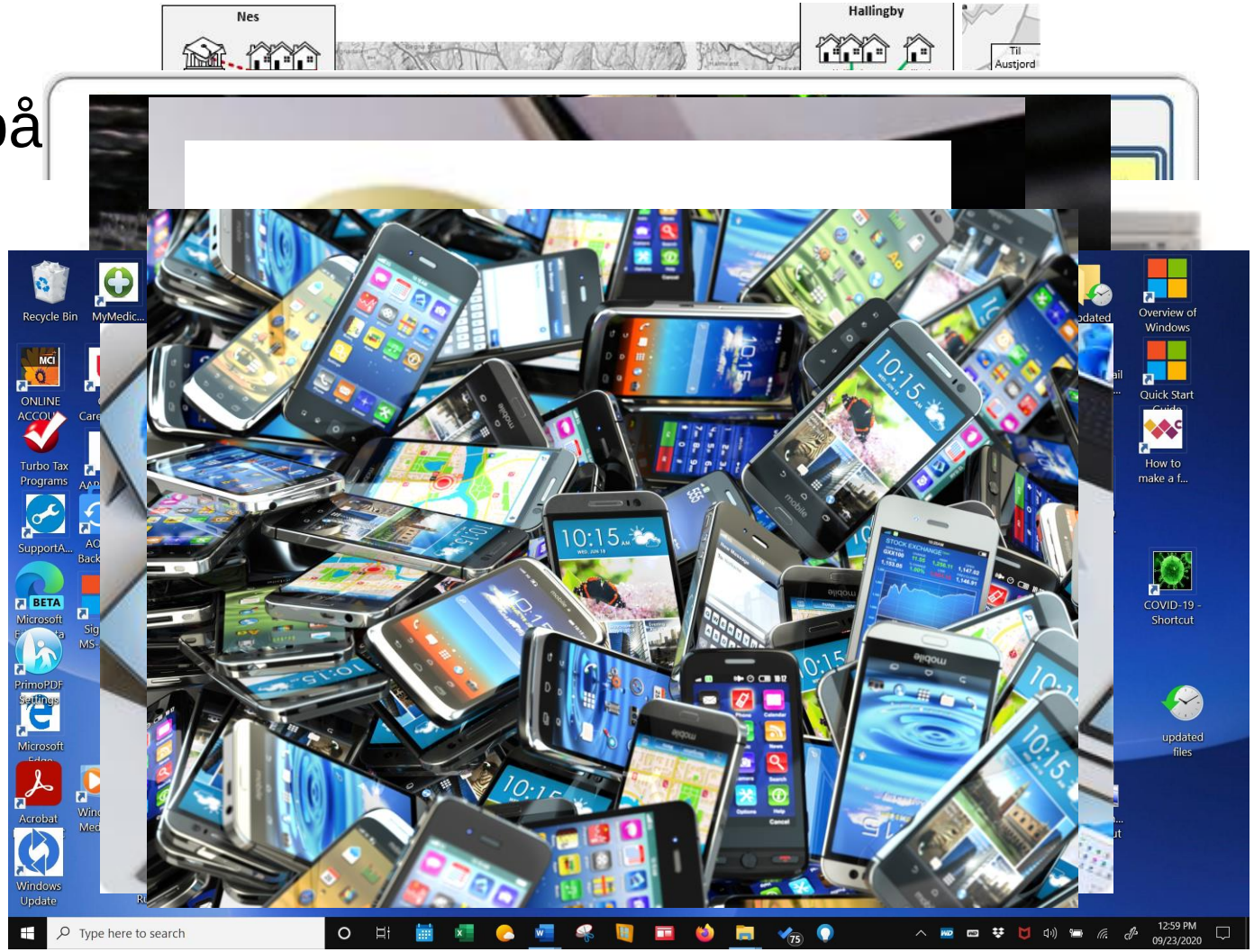


Sektor - Strategi og utvikling



IT tall

- 180 lokasjoner med nettverk
- Datasenter med 179 servere på 11 fysiske servere
- 94 Brannmurer
- 446 switcher
- 840 trådløspunkter
- 110 fagsystemer
- 8305 brukerkontoer
- 6633 datamaskiner
- 1210 mobiltelefoner/pads
- 89 Politiker pads

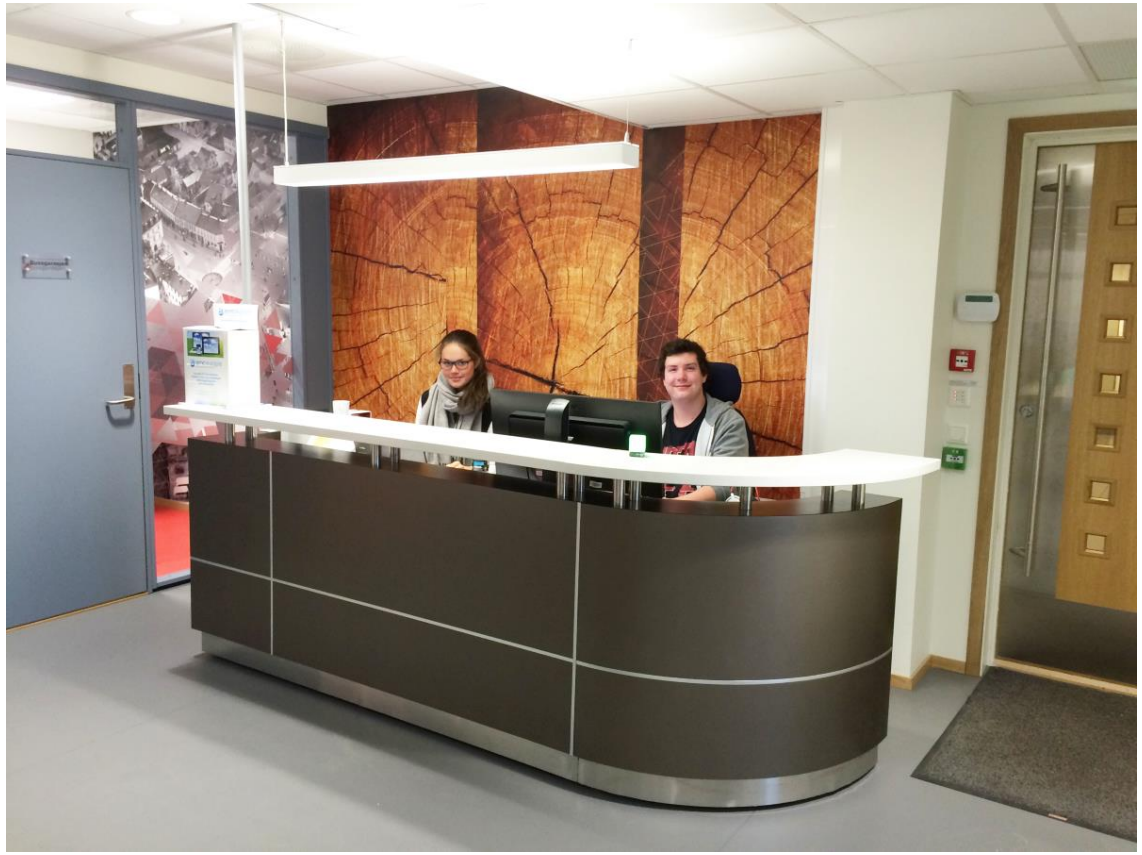


Besøke IT-enheten

- Hønefoss bru 3 / Alles Kulturhus
- 4. etg. sammen med Ringerike kulturskole
- Åpent 0800-1530, mandag – fredag
- I tillegg stiller IT til oppstart på første møtet i komiteer, råd og utvalg

Henvendelser vi bistår med

- Problemer med å koble til «Ringerike kommune» trådløst
- Kontoutfordringer
  - Aktivere Microsoft Autenticator (2 faktor)
  - Mistet passord, selvhjelp på: https://passwordreset.microsoftonline.com/
  - Påloggingsproblemer Teams, Outlook ol.
- Husk meld fra ved mistet/stjålet iPad!
- Avhending skal gjøres etter avtale med IT



Henvendelser til IT

- Dette krever full reset av iPad av IT:
  - Glemt skjermlåskode (pin)
  - iPad får ny bruker – arves sidelengs
- Sekretariatet kjenner appene
  - ACOS møteportal
  - Visma Expense
  - m.fl.
- Det er alltid en fordel å høre med sekretariatet før man kontakter IT

- IT kan ikke bistå med:
- Nettverksproblemer hjemme
  - Guide for å koble til nett hjemme". https://support.apple.com/no-no/HT204051
- Privat iOS konto (kontakt Apple)
  - https://support.apple.com/no-no/HT201487
  - https://iforgot.apple.com/

Privat bruk og reise i utlandet

- For å laste ned apper fra «App Store», må du ha privat iTunes konto
- Kommunedirektøren har vedtatt at det ikke er lov med TikTok og Telegram på kommunens enheter



- iPad er et personlig arbeidsverktøy for deg som folkevalgt
- Ikke overlat det til andre
- iPad fungerer i hele verden der Apple tillater trafikk
- Innholdet fra Ringerike kommune fungerer i Europa eksklusive Ukraina og Russland.
- Outlook e-post, teams m.fl. fungerer ikke i Amerika, Afrika, Oceania og Asia.

DEMO

Cybersikkerhet og personvern

INFORMASJONSSIKKERHET

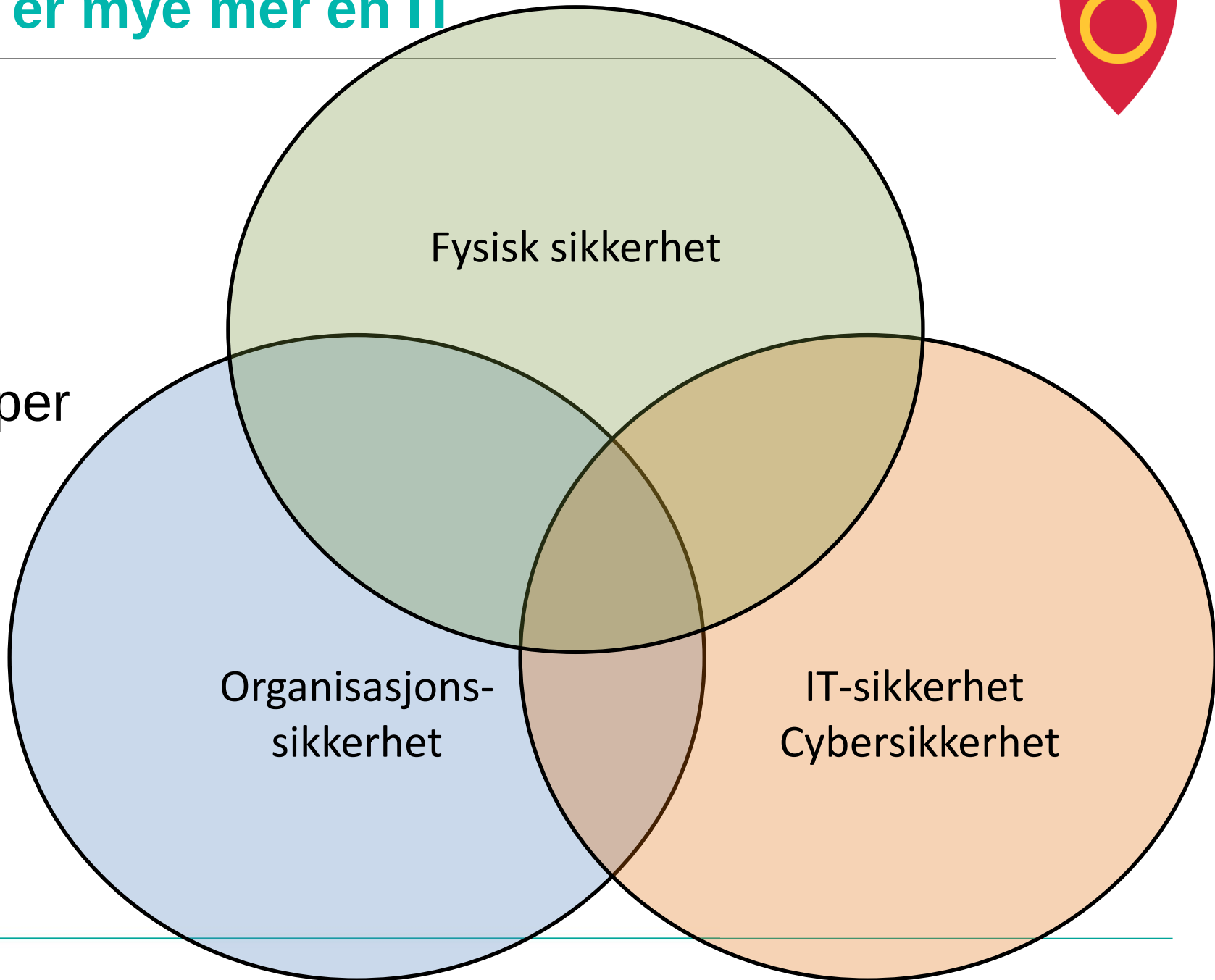
Om meg

- Leder av IT-enheten 2013
- Sikkerhet = lukket sone, backup, antivirus, passord, brannmur mm.
- Forvaltningsrevisjon i 2018
- Organisasjonen lener seg mot IT ved spørsmål rundt informasjonssikkerhet, behandlingsprotokoller ol.
- Styreleder i KiNS siden 2020

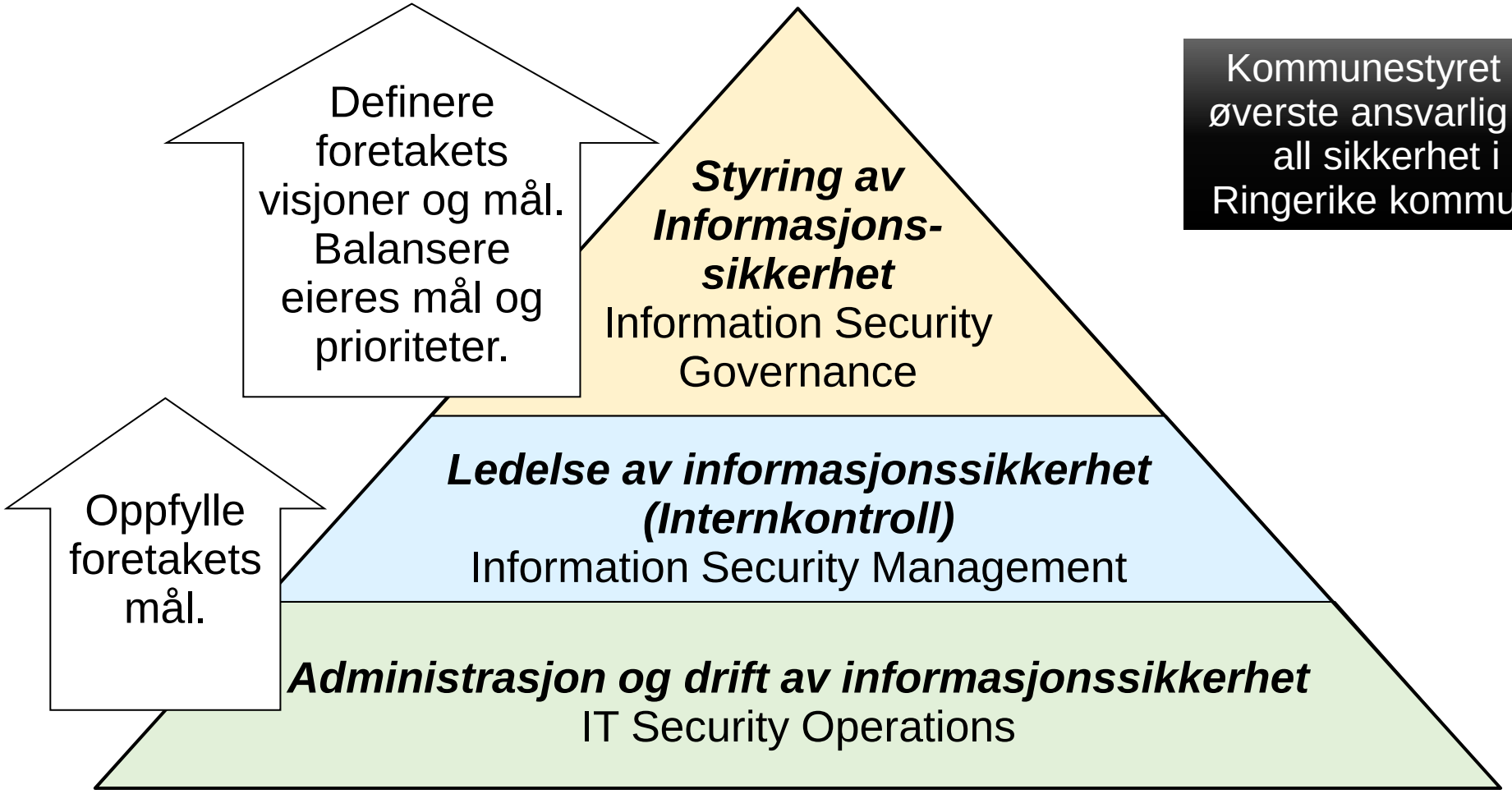

IRT

Informasjonssikkerhet er mye mer en IT

- Personvern
- Beredskap
- Arkiv
- NSMs Grunnprinsipper
- NIS-direktivet
- NIS2
- §§



Styringsnivåer for informasjonssikkerhet*



Kommunestyret er øverste ansvarlig for all sikkerhet i Ringerike kommune

*Informasjonssikkerhet Teori og praksis, 2. utgave 2023, s. 256, Audun Jøssang professor Cybersikkerhet ved UiO

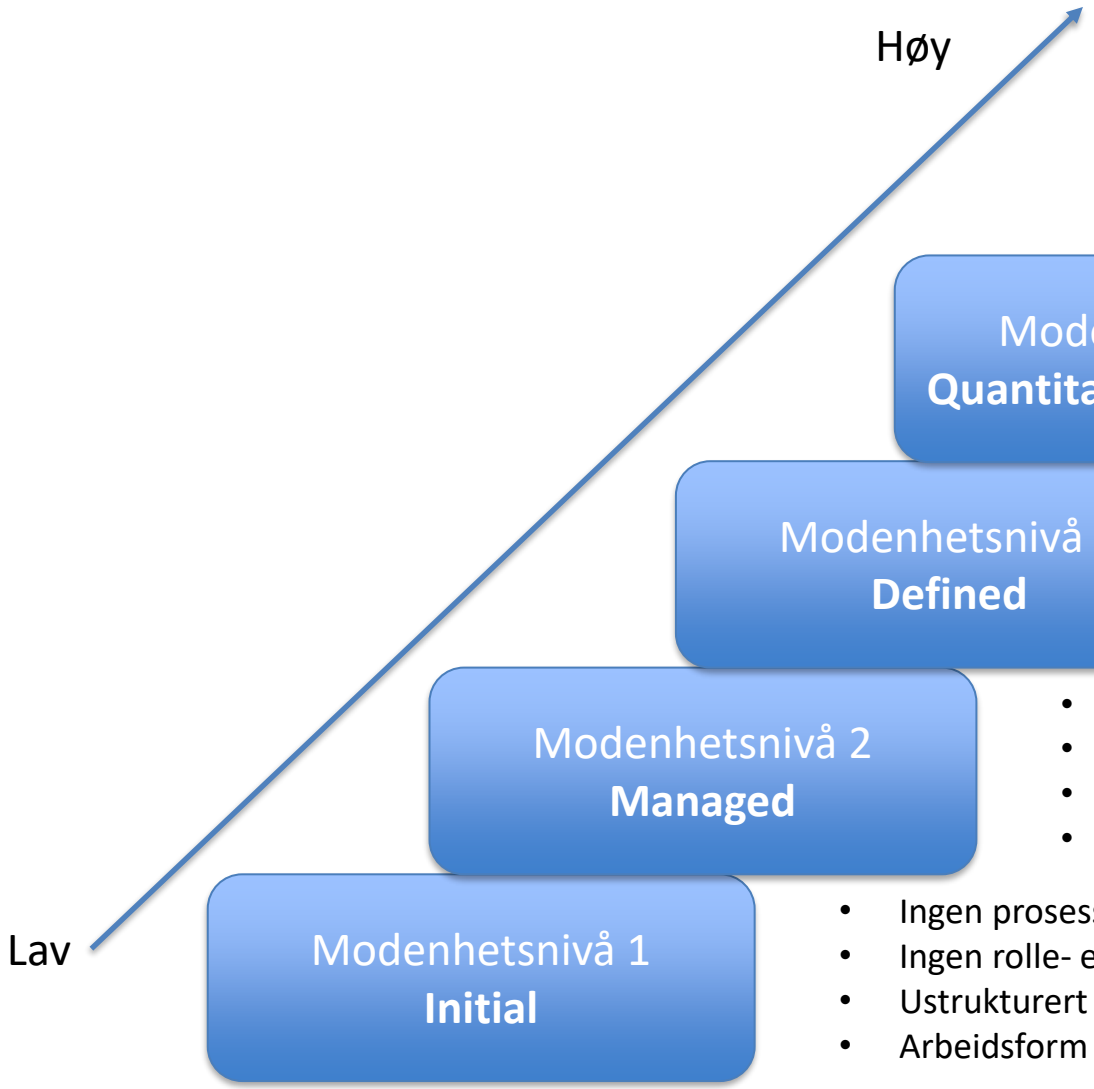
Sikkerhetssituasjonen

- De sikkerhetspolitiske utfordringene mot 2030 vil være preget av høy kompleksitet og stor usikkerhet
- Cyberoperasjoner blir mer effektive
- Deteksjonsevnen i cyberdomene er ikke tilstrekkelig
- Håndteringsevnen på cyberdomenet er ikke tilstrekkelig
- Trussel aktører kommer gjennom sikkerhetsbarrierene med sosial manipulering/innsidere
- Verdikjeder er under angrep
  - VA Oslo, valgte bort Kinesisk selskap i anbudskonkurranse pga. sikkerhet

Utvalgte aktiviteter

- Alle ansatte må gjennomføre eLæringsmoduler
- Årlige samlinger for systemeiere og systemansvarlige i Ringerike kommune
- IT-sikkerhet har NSMs grunnprinsipper som mål, som bygger på ISO2700X
- Forprosjekt for innføring av nytt styringssystem for informasjonssikkerhet (ISMS), basert på kjent standard som er utbredt brukt både privat og offentlig (ISO27001/27002)
  - Etablere en tverrfaglig gruppe som forvalter styringssystemet

Prosessmodenhet



Modenhetsnivå 5
Optimizing

- Kontinuerlig forbedringsfokus
- Arbeidsform - prosessoptimal

Modenhetsnivå 4
Quantitatively Managed

- Kvantifiserbare styringsparametere
- Kompetanse i alle organisasjonsledd
- Arbeidsform – prosessdrevet

Modenhetsnivå 3
Defined

- Detaljert beskrivelse av sentrale prosesser
- Uttømmende rolle- og ansvarsbeskrivelse
- Målbare evalueringskriterier
- Organisatorisk inkluderende

Modenhetsnivå 2
Managed

- Noe prosessdokumentasjon
- Delvis rolle- eller ansvarsbeskrivelse
- Enkle målepunkt
- Arbeidsform – erfaringsbasert og prosessinspirert

Modenhetsnivå 1
Initial

- Ingen prosessbeskrivelser
- Ingen rolle- eller ansvarsbeskrivelse
- Ustrukturert innhenting og bearbeiding av informasjon
- Arbeidsform – individavhengig og ad-hoc basert

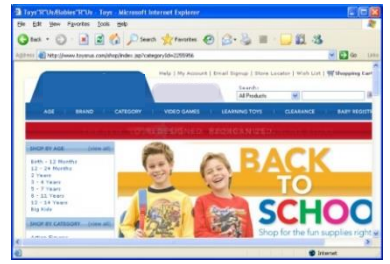
Angrepsvektorer

Ulovlig sporing og avlytting, f.eks. av mobiltelefoner, og ulovlig kartlegging av brukere gjennom apper og nettsteder.

12

Phishing-e-post, -SMS og -meldinger med skadevare og lenker til skadelige nettsider.

1



2

Drive-by-angrep fra kriminelle eller infiserte nettsider.

11

Overlastangrep mot nettsteder slik at legitim trafikk blokkeres.

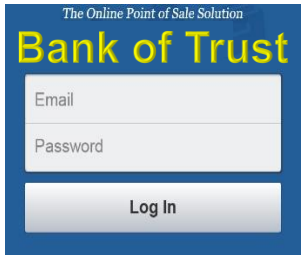
DDoS

Innsideangrep fra utro tjenere i virksomheten.

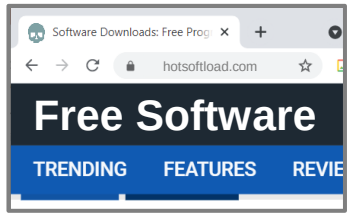
10

Angrep

3



Falske nettsider som stjeler bruker-ID og passord.



9

Skadelige programmer fra internett og andre lagringsmedier.

4

Deepfake lyd og video for å spoofe identitet i online møter og samtaler.

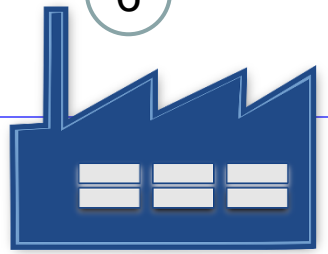
5

Direkte angrep mot sårbare systemer og applikasjoner.

7

Skadelige eksterne enheter.

6



Infisering og angrep gjennom leveransekjeden.

8

Hacking av upatchede sårbare IoT-enheter.

Phishing-angrep

- *Phishing* er en type sosial manipulering.
- Kan sendes som e-post, SMS eller andre meldinger.
- En phishing-e-post er f.eks. designet for å lure mottageren til å oppgi sensitiv informasjon, til å besøke en falsk nettside eller til å installere skadevare.
- Fra omtrent år 2020 er phishing den desidert vanligste angrepsvektoren for cyberangrep og datakriminalitet på internett.
- Sikkerhetskultur, kunnskap og bevissthet rundt phishing er viktig for å forhindre denne typen angrep.

Phishingeksempler

Dcure Global <etik@dcure.dk>

Etikkundersøkelsen 2019

To

Kjære kollega,

Du er en av de utvalgte til å motta etikkundersøkelsen 2019. Grunnet ny personvernlovgivning er Bergen kommune underlagt nye krav til etikk.

I den forbindelse ber vi om at du bruker ca. 3 minutter til å besvare spørsmål knyttet til etikk, holdninger og adferd.

Dine svar vil behandles fortrolig. Undersøkelsen gjennomføres av DCure Global Benchmarking Group, og du får tilgang via følgende link:

Klikk her for å svare på undersøkelsen

På forhånd takk for deltakelsen.

Vi ber om at du svarer på undersøkelsen innen 22. mai 2019.

Bergens Tidende | BT Magasinet | Sport | Økonomi | Meninger | Kultur

Denne falske e-posten lurte 2200 ansatte i Bergen kommune til å gi fra seg passordet sitt

Hver sjette ansatte i Bergen kommune ga fra seg brukernavn og passord da de ble forsøkt lurt under en gransking av datasikkerheten i kommunen.

COMPUTERWORLD | UNITED STATES | IDG TECH(TALK) COMMUNITY | WINDOWS | MOBILE | OFFICE SOFTWARE | APPLE | NEWSLETTERS | EVENTS

PHISHING-KAMPANJE – ET EKSEMPEL FRA FORSKNINGS- OG UTDANNINGSSEKTOREN

Forsknings- og utdanningssektoren har gjennom 2020 vært mål for en avansert, utenlandsk aktør. Angrepene bruker e-post og falske nettsider tilpasset den enkelte virksomhet, og har som mål å «høste» brukernavn og passord som gir tilgang til interne ressurser. Aktøren retter seg mot universiteter og forskningsmiljø i flere vestlige land, og samarbeid mellom sikkerhetsmiljø på tvers av landegrensene har vært avgjørende for å forstå framgangsmåten i Norge. Som sektorens responsmiljø, har Uninett CERT jobbet tett med sektoren og internasjonale samarbeidspartnere for å oppdage, forhindre og ikke minst bedre forstå kampanjene. Dette har gjort det mulig å flere ganger sette i gang forebyggende tiltak før angrepene kommer.

[Kilde: NSMs «Helhetlig digitalt risikobilde 2020»]

Home > Cybercrime

NEWS

Sony hackers targeted employees with fake Apple ID emails

Cylance CEO spells out scenario that may have used Sony's own software distribution tools to feed destructive malware to company's PCs

digi.no | Innhold | Ekstra | Lønnskalkulator | IT-jobber | Tips oss

PHISHING

Kommune sendte falske svindel-eposter til egne ansatte

– Jeg var en av dem som gikk fem på, forteller Ann-Helen Moum, digitaliseringssjef i Kristiansand kommune.

skadevare

Kategorier av phishing-angrep

- *Masse-phishing*
  - Stort volum som er ment å nå flest mulig
- *Spyd-phishing*
  - Målrettet mot bestemte personer eller virksomheter
- *Direktørsvindel (hval-phishing)*
  - Spyd-phishing rettet mot «store fisker» (f.eks. rike, høyprofilerte, tilgang til mye penger,…)
- *Klone-phishing*
  - Kopi av legitim melding/epost hvor lenker/vedlegg er erstattet av skadelige versjoner

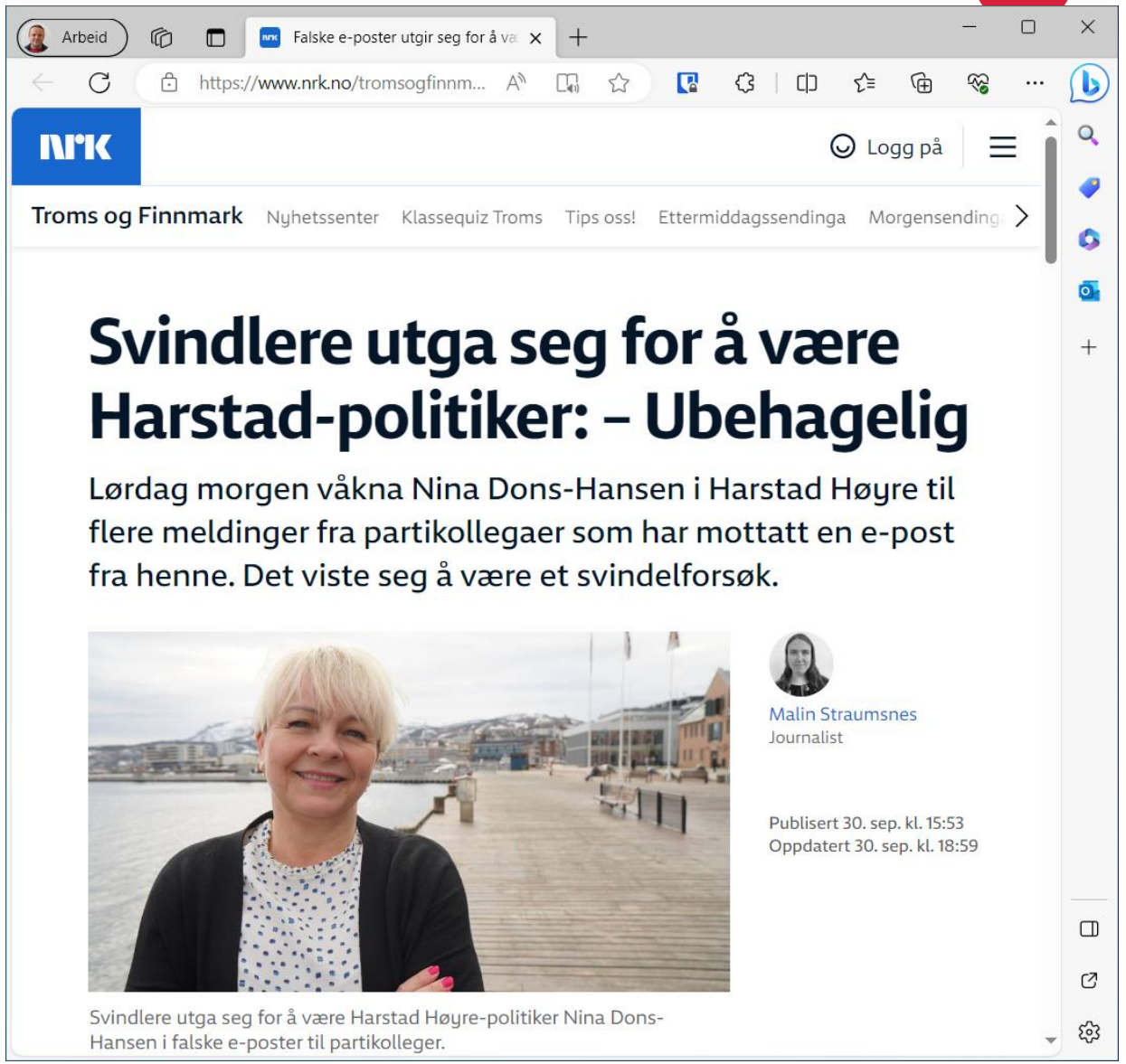
Andre former for sosial manipulering

- Spør pent
  - Folk er generelt hjelpsomme og gir fra seg mye informasjon
- Lur folk til å gi deg tilgang
  - «Hi, I`m calling from Microsoft»
  - Få tak i «hemmeligheter» til å resette glemte passord
- Falske adgangskort
  - Gir en følelse av fellesskap – «du og jeg har noe felles, og derfor stoler jeg på deg»
- Bruk av stjålne/falske kontoer på sosiale nettverk
  - Du tror du får melding fra en venn, men egentlig er det en angriper som har stjålet din venns identitet
  - Hvis det skjer, kontakt din venn gjennom annen «sikker» kanal, f.eks. vanlig telefon

PHISHING-E-POST ØVELSE

Politikere er et mål for trussel aktører

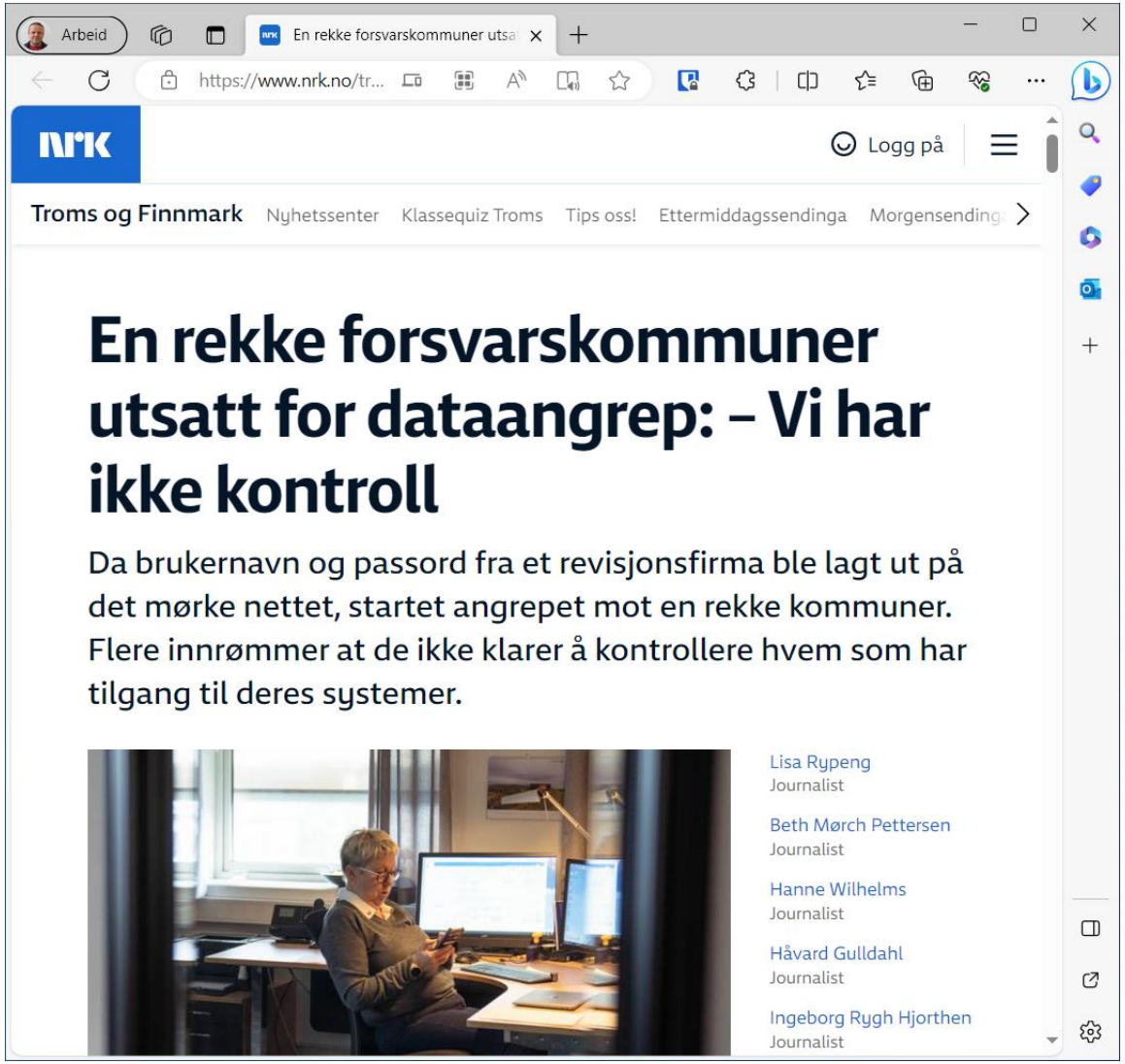
- E-posten var skrevet med godt språk
- E-post adressen virket reel, men var ikke Nina Dons-Hansen sin, noe partikollegaer oppdaget og meldte ifra
- I tillegg var det brukt bilde som Nina brukte under årets valgkamp



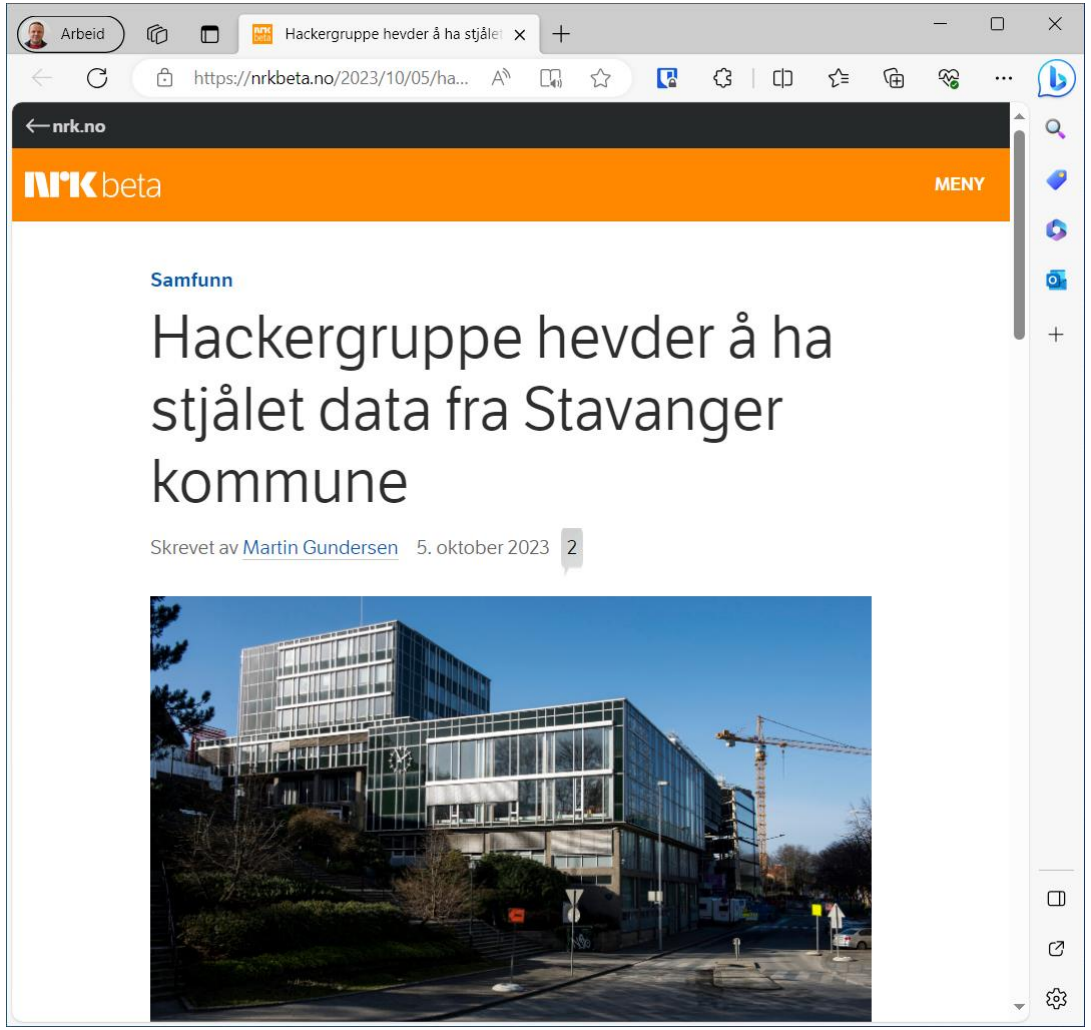
https://www.nrk.no/tromsogfinnmark/falske-e-poster-utgir-seg-for-a-vaere-harstad-politikere-1.16577766

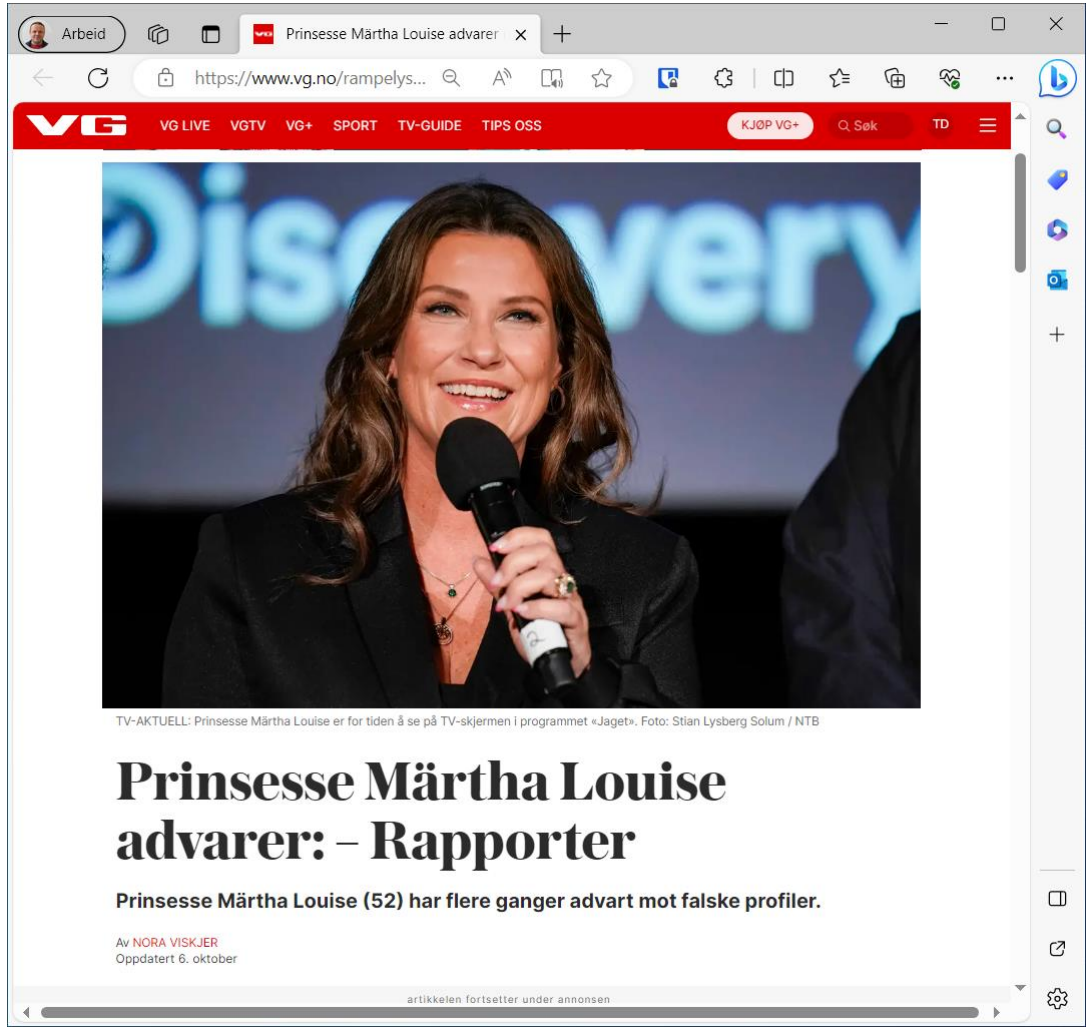
Forsvarskommuner under angrep

- Det hele skjedde i den mest hektiske tiden på året, når kommunen skulle levere årsregnskap.
- Brukernavn og passord fra revisjonsfirma var fisket (phishing) og lå tilgjengelig for trussel aktører på internett
- Firma leverer tjenester til over 10 kommuner, og brukte samme brukernavn og passord hos alle
- Firmaet oppdaget hendelsen og gjorde tiltak, men det slo dem ikke at angrepet gikk videre til kommunene
- Heldigvis ble dette stoppet ved rekognoseringsstadiet, før data ble hentet ut



Andre hendelser





Sosiale medier

- Vær obs og pass på hverandre
- Rapporter falske kontoer raskt
- Ikke forsterk hendelsen med å kommentere
- Politikere arrangerer ikke konkurranser eller deler ut bobiler e.l.

Passord håndtering tips

- Aldri oppgi passord til NOEN (til og med politiet)
- Aktiver 2-faktor der det er mulig
- Bruk setninger som passord for de 3 tjenestene du logger på oftest

- Ikke benytt samme passord på flere tjenester
  - Bedre å bruke PostIT lapper med passord nedskrevet
  - Microsoft Authenticator har mulighet til å lagre passord
  - Eventuelt bruk en passordmanager med aktivert 2-faktor (husk å ta vare på masterkey | opplåsning)

Politiker iPad

- Bruk kommunal e-post og pad til Politiker vervet, fordi:
  - 2 faktor pålogging, fornyet pålogging hver 60. dag
  - Kryptering av e-post, OneDrive og teams både på enheten og i sky
  - Filter hindrer det meste av skadevare
  - Sikkerhetskopi
  - IT driftstøtte
  - ..

Takk for oppmerksomheten!

RINGERIKE
KOMMUNE