KiNS
foreningen kommunal informasjonssikkerhet

RINGERIKE KOMMUNE

IT-sikkerhet

Torkjell Dahl, IT-sjef

IT-sikkerhet

Torkjell Dahl, styreleder

Denne presentasjonen

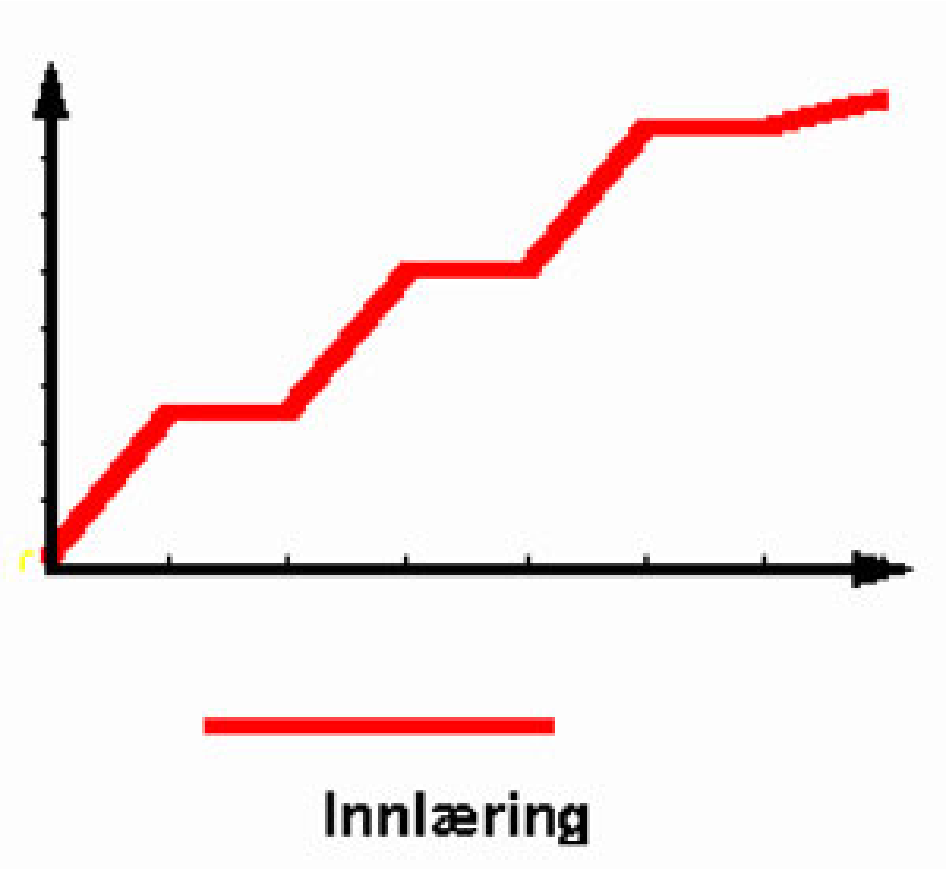
- Min reise
- Veiledningsaktører
- Risikoer og hendelser
- Tanker for revisjon

Min reise innen sikkerhet i Ringerike kommune

- Sikkerhet = lukket sone, antivirus, passord og brannmur
- Leder av IT-enheten 2013
- Organisasjonen peker på IT ved ubehagelige spørsmål
  - Økonomisystemer
  - Elektronisk godkjent arkiv
  - Elektronisk meldingsutveksling
  - Ny IT-lokasjon med serverrom
  - Arkivsystem for lukket sone
  - …
- Ser at det blir vanskelig å holde kontroll på dette alene
- Kommunen etablerer «Sikkerhetssekretariat»
  - IT (leder), PVO, Eiendom, Beredskapsleder, HR og Kommuneadvokat
- Føler jeg blir sittende med dette alene
- Jeg innser jeg må sette meg mer grundig inn i fagfeltet

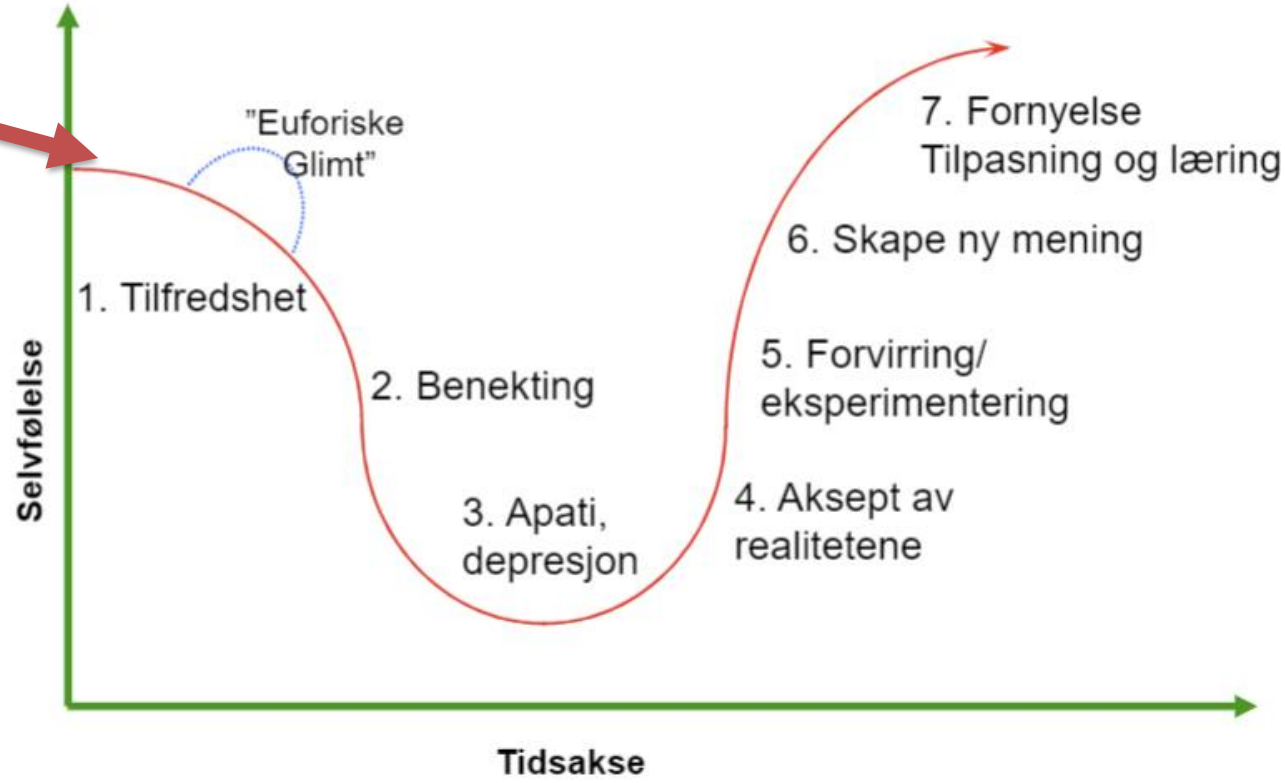
Hvor vanskelig kan det være?

- Engasjere meg i fagfora
- ISO27002 – 114 kontroller
- GDPR – 6-7 viktige grunnprinsipper
- ROS analyse
- DPIA metode
- Fysisk sikkerhet
- Organisasjonssikkerhet



Selvinnsikt?

- God mestringstroen
- Forvaltningsrevisjon
- Begynner og gå opp for meg hvor stort og komplekst dette området er
  - Hvert svar = 2-3 nye spørsmål
  - Hver løsning = 2-3 nye utfordringer
- Vil dette noen ende ta?
- Håper jeg nådd bunnen nå!



Oppdagelser

Områdene

- IT-sikkerhet / Cybersikkerhet
- Informasjonssikkerhet
- Fysisk sikkerhet
- Organisatorisk sikkerhet
- Sikkerhetsloven
- Personvern
- Personvernforo
- Digital etikk
- Beredskap
- ….

Roller

- Behandlingsansvarlig
- Driftsansvarlig
- CISO
- Informasjonssikkerhetsansvarlig
- IT-leder
- Personvernombud (PVO)

En utfordring at dette blandes sammen i en og samme sak.

Invitasjon til Revisorforeningen

nkrf – kontroll og revisjon i kommunene

– på vakt for fellesskapets verdier

Kurs og konferanser | Nyheter | Kontrollutvalg

Arena for forvaltningsrevisjon og eierskapskontroll 20

Tilbake til kursoversikten

14.30 - 15.15: Uavhengig gransking av hendelse v[illegible]d Kleppe vannverk 2019 (Askøy

- Stian Antonsen, NTNU Samfunnsforskning, professor ved institutt for indust[illegible] teknologiledelse

15.30 - 16.15: IT-sikkerhet

- Torkjell Dahl, IT-sjef, Ringerike kommune og styreleder i KiNS (Foreningen K[illegible] Informasjonssikkerhet)

BKR
Buskerud Kommunerevisjon IKS

Informasjonssikkerhet og personvern

Ringerike Kommune

Forvaltningsrevisjon

August 2018

Buskerud Kommunerevisjon IKS
Postadresse: Postboks 4197, 3005 DRAMMEN
Besøksadresse: Øvre Eiker vei 14, 3048 Drammen
Telefon: 409 10 200
e-post: post@bkr.no
URL-adresse: www.bkr.no

Veiledningsaktører

- Felles for aller er at de ønsker oss godt
- Men det kan fort føles på at det blir litt mye
- Overlapp, motstridigheter og konkurranse?

Min bakgrunn

Min forståelse av aktørene

Aktør	Veilednings-/tjeneste område	Fagområde
Datatilsynet	**Personvern,** informasjonssikkerhet som følge av personvern	Juridisk, IT-teknisk
Digdir	**Styringssystem og internkontroll**	Ledelse
NSM	**IT-sikkerhet, digitalt risikobilde**	IT-teknisk, fysisk, personell
KiNS	**Møteplass, kurs, dele mellom kommuner, maler og fellesløsninger**	Kompetanse, pådriver
NORMEN	**Informasjonssikkerhet og personvern i helse- og omsorgssektoren**	Ledelse, IT-teknisk, juridisk
NorSIS	**Råd og tjenester for innbyggere, små- og mellomstore bedrifter**	Bistand til privat(e)
DSB	**Øvelse og beredskap**	Ledelse
DFØ	**Strategisk støtte, maler**	Ledelse
KS	**Ledelsesstøtte, fellessystemer**	Ledelse, leverandør
Udir	**Internkontroll og personvern i skolen??**	Delegerer ansvaret?
NHN	**Sikkert helsenett, overvåkning og meldingstjenester**	IT-teknisk
Kommune CSIRT	**Digitalt trusselbilde, kommunespesifikke områder, meldingstjenester**	IT-teknisk, strategisk støtte

Personvern og/eller informasjonssikkerhet?

Personvern

Informasjonssikkerhet

Sikkerhet

Privatlivets fred

(privacy)

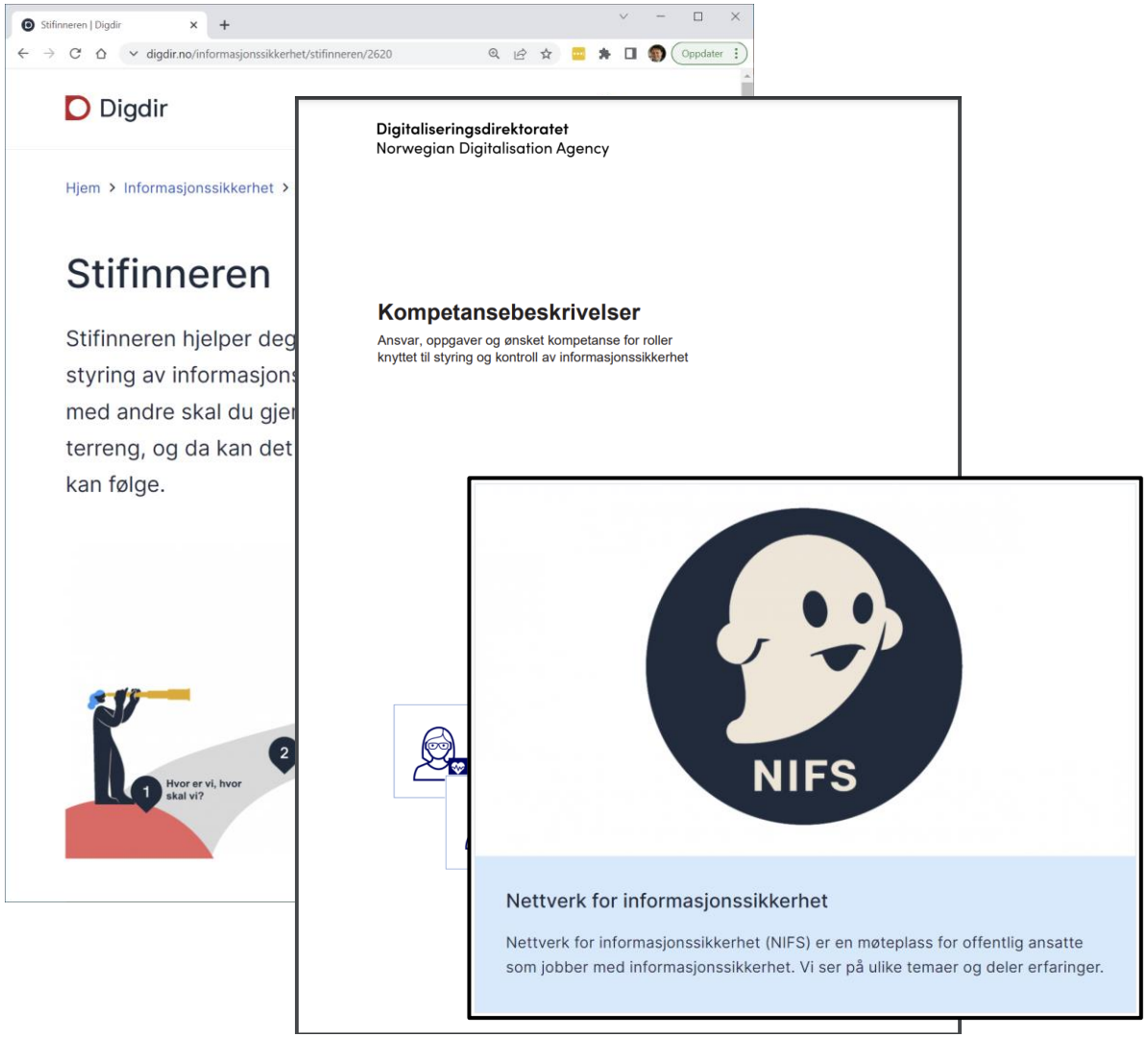
Personopp-lysningsvern

(data protection)

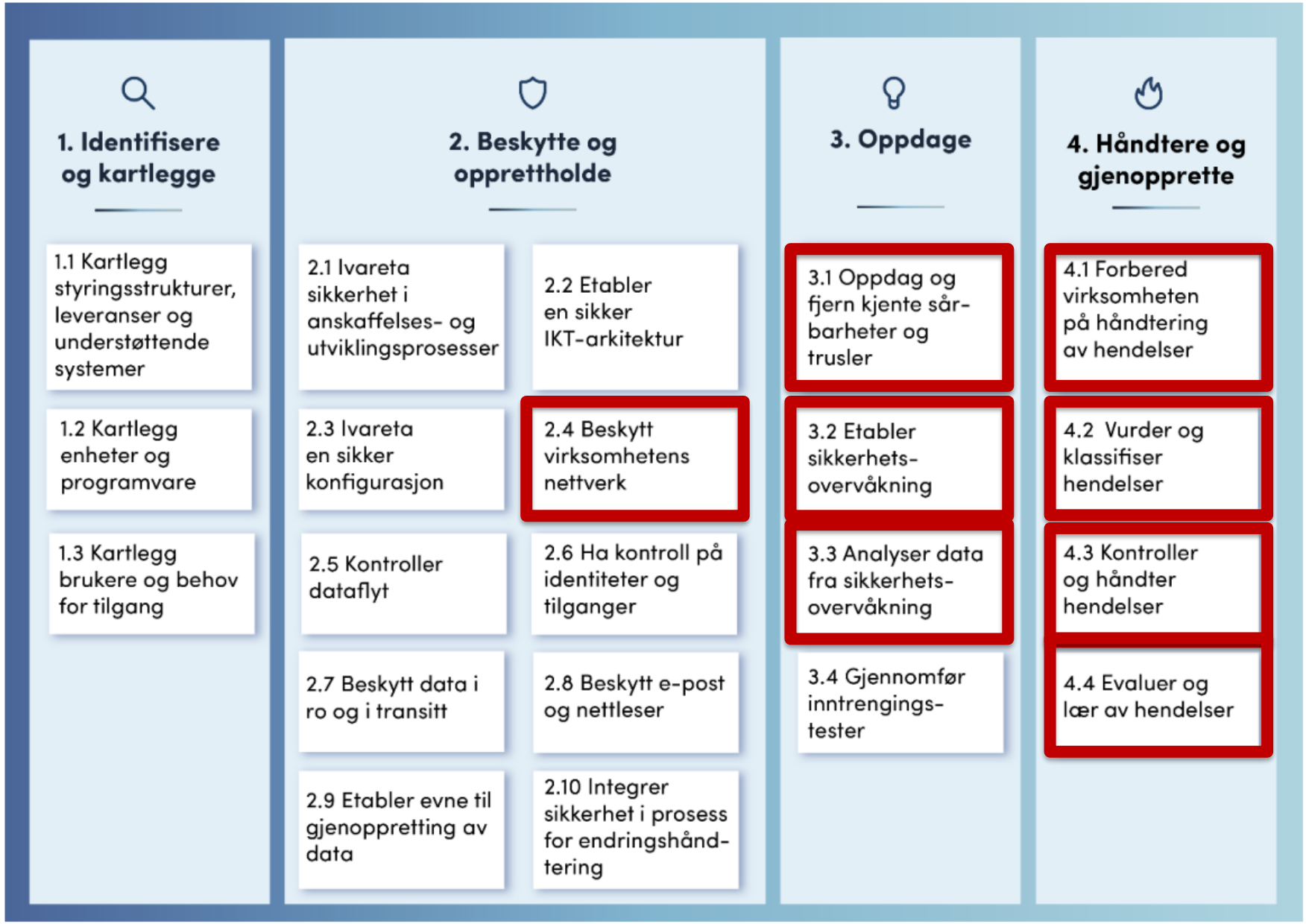
Personopplysnings-sikkerhet

Digdir

- Stifinneren
- Kompetansebeskrivelser
- NIFS
- …

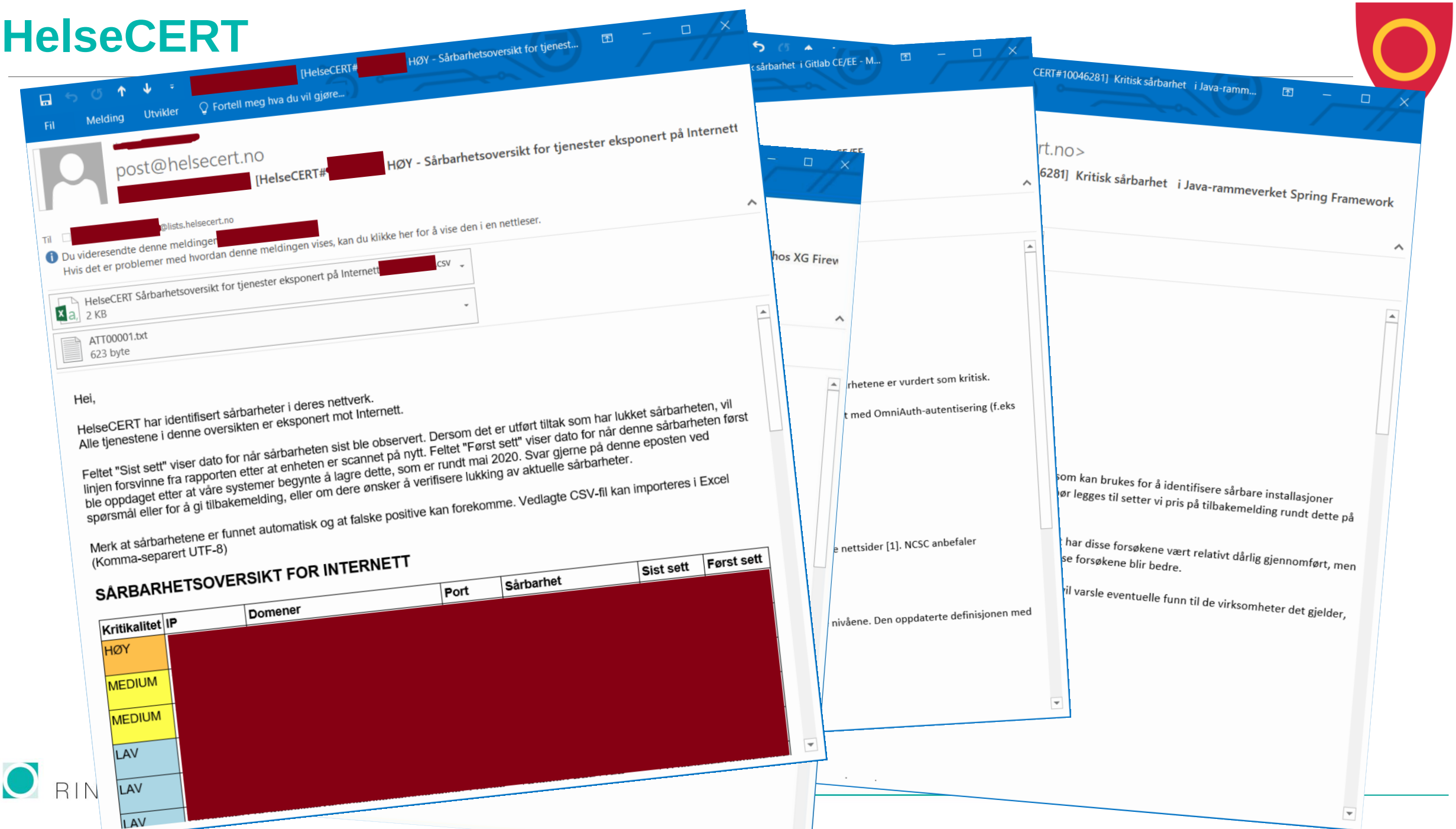


NSMs Grunnprinsipper for IKT-sikkerhet V2.0



RINGERIKE

HelseCERT



[HelseCERT# [redacted] HØY - Sårbarhetsoversikt for tjenest...

Fil Melding Utvikler Fortell meg hva du vil gjøre...

[redacted]

post@helsecert.no

[redacted] [HelseCERT# [redacted] HØY - Sårbarhetsoversikt for tjenester eksponert på Internett

Til [redacted]@lists.helsecert.no

Du videresendte denne meldingen [redacted]
Hvis det er problemer med hvordan denne meldingen vises, kan du klikke her for å vise den i en nettleser.

HelseCERT Sårbarhetsoversikt for tjenester eksponert på Internett [redacted].csv
2 KB

ATT00001.txt
623 byte

Hei,

HelseCERT har identifisert sårbarheter i deres nettverk.
Alle tjenestene i denne oversikten er eksponert mot Internett.

Feltet "Sist sett" viser dato for når sårbarheten sist ble observert. Dersom det er utført tiltak som har lukket sårbarheten, vil linjen forsvinne fra rapporten etter at enheten er scannet på nytt. Feltet "Først sett" viser dato for når denne sårbarheten først ble oppdaget etter at våre systemer begynte å lagre dette, som er rundt mai 2020. Svar gjerne på denne eposten ved spørsmål eller for å gi tilbakemelding, eller om dere ønsker å verifisere lukking av aktuelle sårbarheter.

Merk at sårbarhetene er funnet automatisk og at falske positive kan forekomme. Vedlagte CSV-fil kan importeres i Excel (Komma-separert UTF-8)

SÅRBARHETSOVERSIKT FOR INTERNETT

Kritikalitet	IP	Domener	Port	Sårbarhet	Sist sett	Først sett
HØY	[redacted]					
MEDIUM						
MEDIUM						
LAV						
LAV						
LAV						

sårbarhet i Gitlab CE/EE - M...

hos XG Firew

rhetene er vurdert som kritisk.

t med OmniAuth-autentisering (f.eks

e nettsider [1]. NCSC anbefaler

nivåene. Den oppdaterte definisjonen med

CERT#10046281] Kritisk sårbarhet i Java-ramm...

rt.no>

6281] Kritisk sårbarhet i Java-rammeverket Spring Framework

som kan brukes for å identifisere sårbare installasjoner
ør legges til setter vi pris på tilbakemelding rundt dette på

har disse forsøkene vært relativt dårlig gjennomført, men
se forsøkene blir bedre.

il varsle eventuelle funn til de virksomheter det gjelder,

RIN

KS brev til kommunedirektøren, c

KOMMUNESEKTORENS ORGANISASJON
The Norwegian Association of Local and Regional Authorities

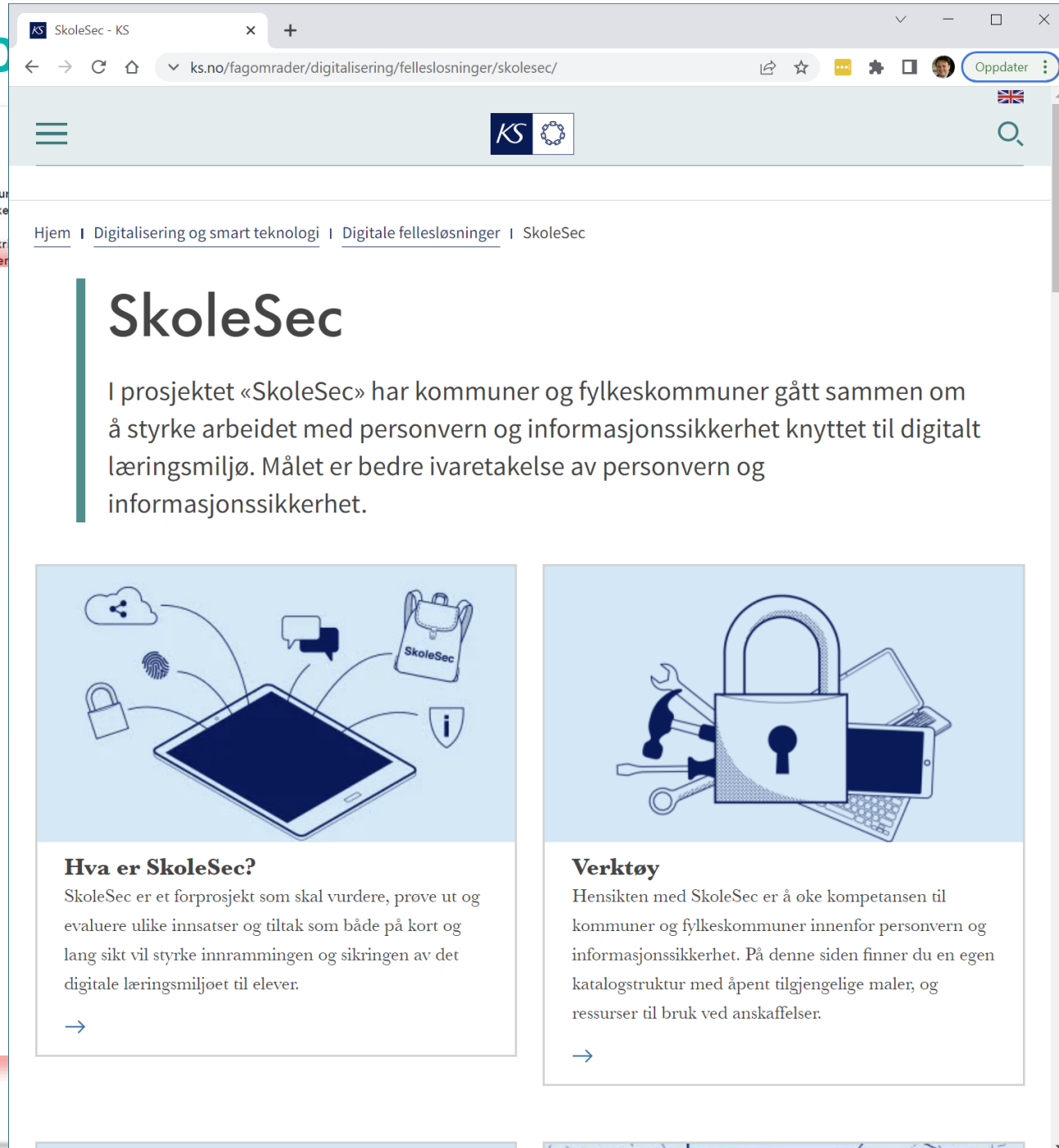
DET KONGELIGE
KOMMUNAL- OG DISTRIKTSDEPARTEMENT

1) Sikkerhetsovervåkning
   a) Verifiser om kommunen har nødvendig sikkerhetsovervåkning av IKT-systemer for å kunne oppdage dataangrep og datainnbrudd, og at kommunen har nødvendig bredredskap for å kunne håndtere dette.
   b) Hvis kommunen selv ikke har driftsansvaret for IKT-systemer, må driftsleverandør(er) kontaktes for å verifisere om de har nødvendig sikkerhetsovervåkning av IKT-systemer, og i en forlengelse av dette, nødvendig beredskap for å håndtere et dataangrep og datainnbrudd.

   c) Kommunen bør etterspørre og verifisere hos leverandøren hvilke tiltak som er gjennomført for sikkerhetsovervåkning og beredskap for å håndtere dataangrep og datainnbrudd.

2) Sikring av kritiske funksjoner og tjenester
   a) Verifiser om det er kartlagt hvilke funksjoner/tjenester i kommunen som anses som kritiske. Sjekk også hvilke konsekvenser det vil ha for kommunens funksjonsevne hvis IKT-systemene blir utilgjengelige, eller mister tillitt fordi data er manipulert eller på avveie.
   b) Verifiser om kommunen har oppdaterte beredskap- og kontinuitetsplaner for bortfall av tjenester. Vurder videre om kommunen har nødvendig kapasitet til å opprettholde sin funksjonsevne, spesielt på kritiske tjenester, hvis IKT-systemer faller ut over lengere tid.
   c) Verifiser om det finnes gjenopprettelsesrutiner, og om backup er plassert slik at denne ikke kan bli manipulert eller ødelagt.
   d) Flere leverandører av programvare har utviklings- og supportavdelinger i landene som nå er involvert i konflikten. Verifiser med leverandør om hvordan leverandøren håndterer situasjonen hvis de har utviklings- eller supportavdeling i de aktuelle landene.

KS
Besøksadr.: Haakon VIIs gate 9
Postadr.: Postboks 1378, Vika, 0114 Oslo
Nettside: www.ks.no
E-post: ks@ks.no
Telefon: +47 24 13 26 00
Org.nr.: 971 032 146
Bankgiro: 8200.01.65189
Iban: NO63 8200 0165 189



Forslag ved internrevisjon

Personvern

- Hvem er PVO?
- Vurder behandlingsprotokollen
- Avvik siste 2 år
- Behandlingsansvarlige for systemer med personopplysninger
  - Databehandleravtaler
- Har vi prosedyrer for:
  - Melding av avvik til tilsyn
  - Anskaffelse av nye systemer som håndterer personopplysninger
  - Håndtering av skyggesystemer
- Opplæring av ansatte som behandler personopplysninger
- Vurderes etiske spørsmål?
  - Kan kommunen måtte stå til ansvar for manglende kontroll på personopplysninger 15 år frem i tid?

Informasjonssikkerhet bygg/HR

- Er styringssystemet kjent og brukes det?
- Hvilke bygg inneholder arkiver og digitale systemer som må sikres?
- Adgangskontroll og/eller soneinndeling
- Rutiner for nøkkelhåndtering?
- «Offboarding»
- Brukes ID-kort?
  - Instruks om bruk på jobb?
  - Rutiner for ansatte om å opprettholde sikkerhet i bygningssoner?
  - Eskalerte rutiner hendelser

Forslag ved revisjon

IT-sikkerhet

- Styringssystem for vann og avløp
- Prosesser ved nye systemer
- Hvordan avvikles systemer
- Soneinndeling
- Overvåkning
- Backup
- Logging og tilgang til logger
- Endringshåndtering
- ISO27002 samsvarsanalyse
- Kriseplaner, ROS analyse, gjennomførte inntrengingstester ol.

Informasjonssikkerhet digitalt område

- Prosess ved ønske om nye systemer (digitalisering)
- Påloggingsløsninger
- Verdivurdering av systemer/data (BIA)
- Systemforvaltning
  - Behandlingsansvarlig
  - Daglig administrasjon
  - Drift av løsningen
- Rutine ved funn av skygge IT

Årene går – kommunale personvernutfordringer består….

Datatilsynet

Tilsyn mot 31 kommuner i 2003

Tema var internkontroll og informasjonssikkerhet med vekt på ledelsesforankring av dette.

- Funn:
  - Manglende struktur i forhold til ansvar og myndighet
  - Rådmann har svært liten medvirkning i forhold til implementering av regelverket
  - Manglende internkontroll
  - Mangler oversikt over behandlinger som skjer i kommunen
  - Mangelfulle databehandleravtaler
  - Informasjonssikkerhet
  - Mangelfull sletting
  - Mangelfull tilgangsstyring

På rett veg i skolesektoren

Torsdag 4. februar arrangerte Datatilsynet sin tredje rundbordskonferanse om personvern i skolen. Tema var som tidligere sentrale aktørers strategiske arbeid for å ivareta personopplysningssikkerheten til elever i grunn- og videregående skole i Norge, og det er grunn til en viss optimisme.

En liten «visjon»

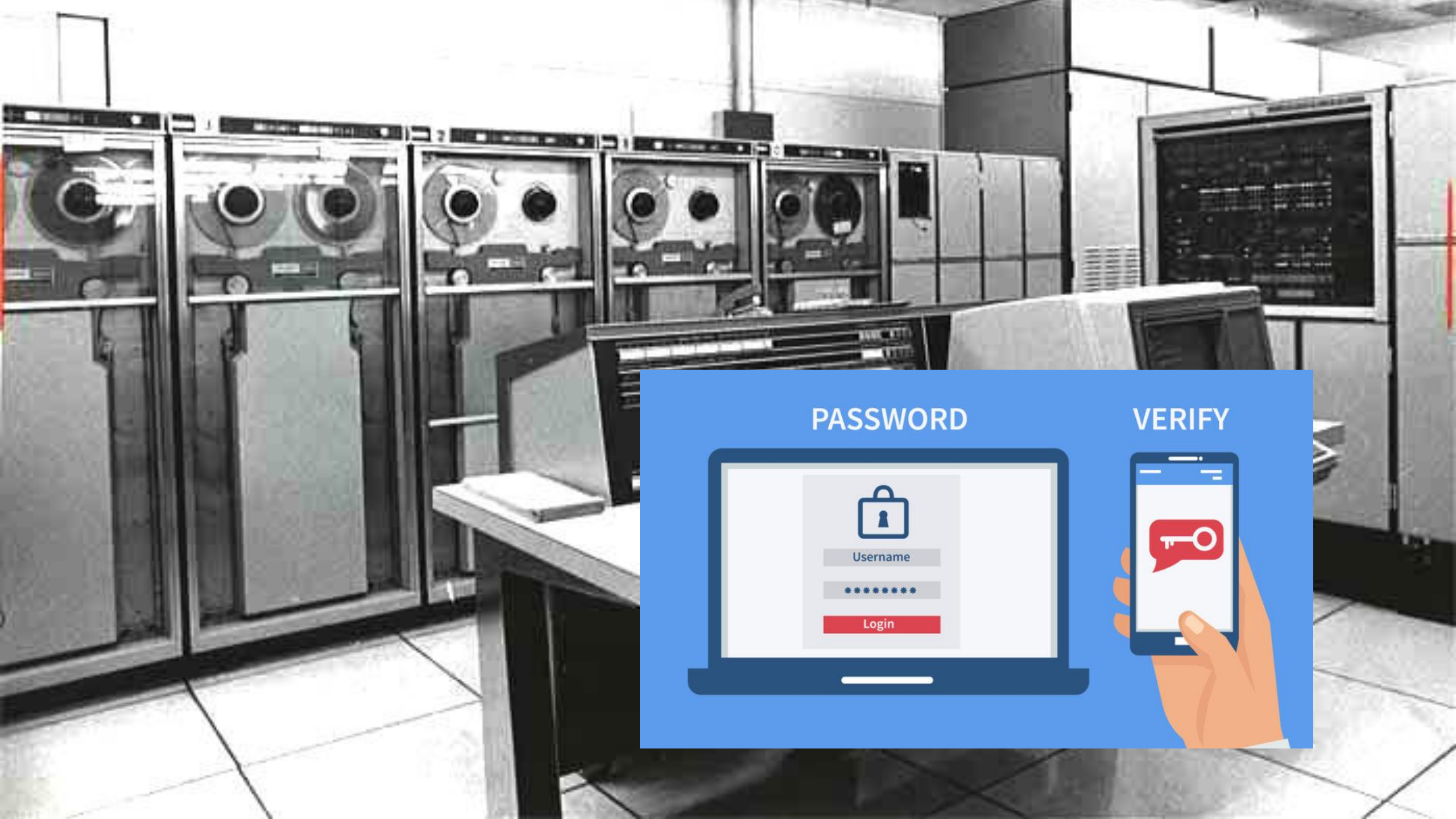
- En månedlig kjørelys rapport til kommunestyre
- Tilstand for:
  - Personvern
  - Informasjonssikkerhet
  - IT-sikkerhet
  - Fysisksikkerhet
- Kan det føre til økt fokus og bedre sikkerhet?!

«Når ingenting er sikkert er alt mulig»... (Ordtak Margaret Drabble)

Spørsmål?

RINGERIKE
nærmest det meste

RINGERIKE
KOMMUNE


PASSWORD
VERIFY
Username
Login

Tilbake til Forvaltningsrevisjon

- Jeg føler at den er skrevet i en annen tid (2018)
- Innholdet er fortsatt relevant, men kanskje lite håndfast
- God metode å samle inn data om systemer fra Behandlingsansvarlige

- Jeg ville hatt en helt annen dialog med revisjon i dag
  - Skygge IT
  - Hurtigdigitalisering
  - Digital grunnmur
  - Kapasitetsstyring
  - Overvåkning og beredskap
  - Manglende kontraktsforhold
  - Eierskapskontroll
- Jfr. egen ISO27002 revisjon

Oppslagsverk som kan sette revisjonskriterier

- ISO/IEC 27001 (Information technology)
- NSM Grunnprinsipper 2.0
- Personvernforordningen – GDPR (ISO27701)
- Direktoratet for e-helses Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Digitaliseringsdirektoratets veiledere til informasjonssikkerhet
- Nasjonal strategi for digital sikkerhet 05/2019