Riksrevisjonen

Riksrevisjonens revisjon av informasjonssikkerhet

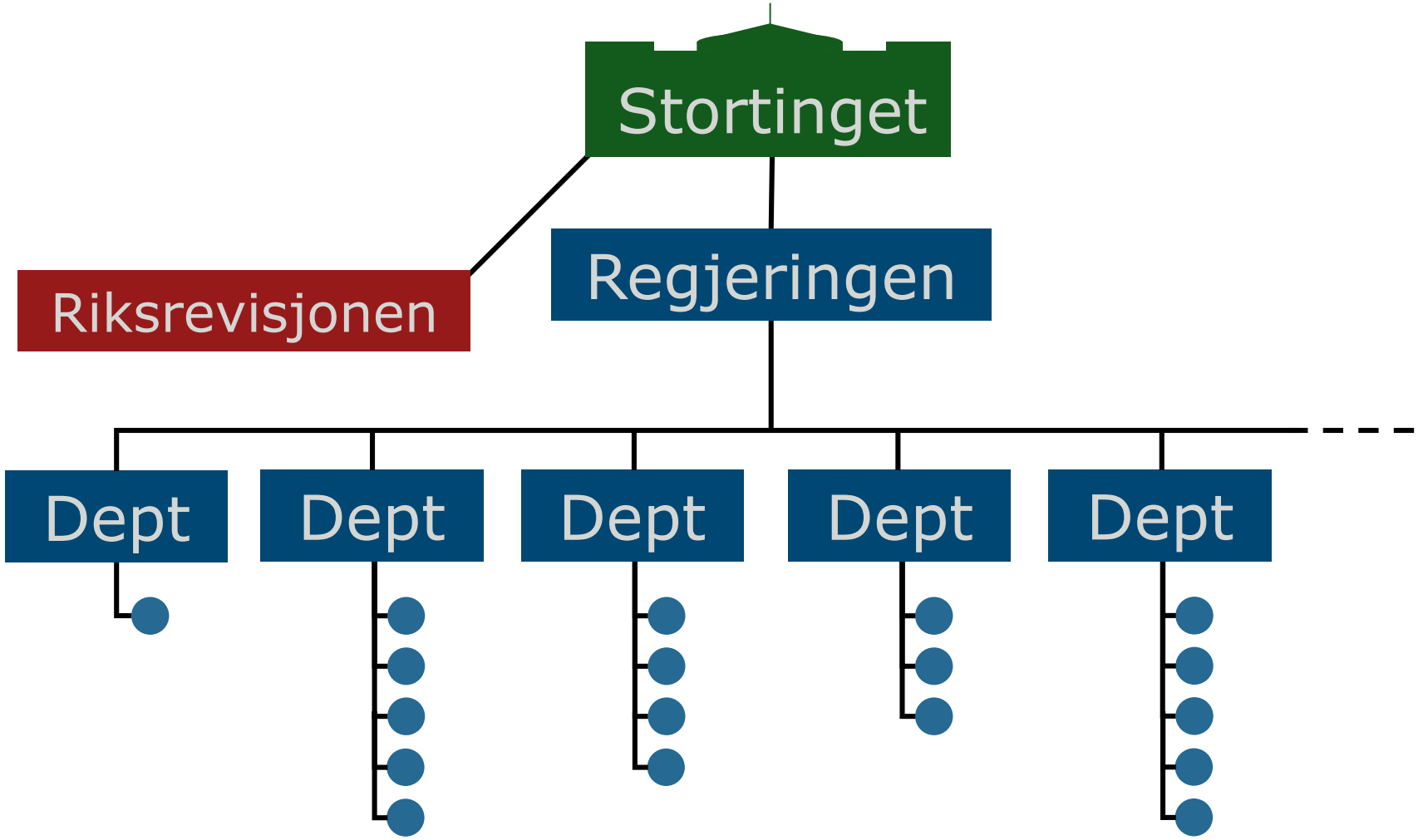
16. februar 2022 – IAA – nettverk statlig sektor

Vi skal snakke om

1. Kort om Riksrevisjonen
2. Hvorfor bryr vi oss informasjonssikkerhet?
3. Revisjonsprosessen
4. Eksempler på revisjoner – resultater og erfaringer
5. Spørsmål og diskusjon

1. Kort om Riksrevisjonen

Foto: Kai Myhre/Menon Economics


Stortinget
Riksrevisjonen
Regjeringen
Dept
Dept
Dept
Dept
Dept

Revisjonstyper

Type	Beskrivelse
Finansiell revisjon	Skal gi trygghet om at regnskapene ikke inneholder vesentlig feil eller mangler, og at regnskapene er utarbeidet i tråd med regelverket.
Etterlevelsesrevisjon	Kontrollerer at virksomheter bruker pengene slik Stortinget har bestemt, og at de følger lover og regler.
Forvaltningsrevisjon	Større, systematiske undersøkelser der målet er å vise hvordan regjeringen og statsforvaltningen gjennomfører det Stortinget har bestemt, og hvilke virkninger offentlige tiltak har hatt.
Selskapskontroll	Undersøkelser av om staten ivaretar sine eierinteresser i selskaper i tråd med det Stortinget har bestemt.

Retningslinjer for revisjon (riksrevisjonen.no)

Valg av revisjonstema

- Risiko og vesentlighet
  - Økonomi
  - Samfunnsmessig betydning
  - Betydning for befolkningen
  - M.v
- Aktualitet og relevans
  - Er revisjonstemaet aktuelt og relevant for Stortinget og forvaltningen?
  - Hvordan kan en undersøkelse av temaet bidra til å forbedre forvaltningen?
  - Er tidspunktet riktig?

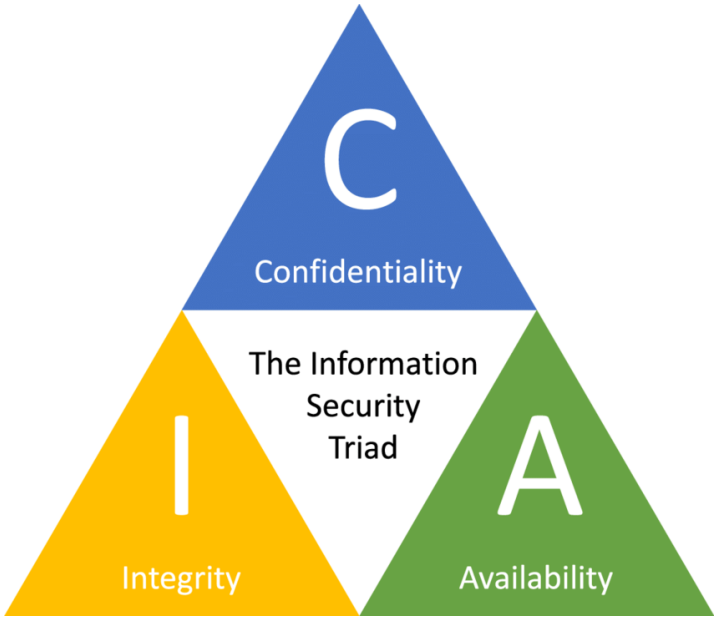
2. Hvorfor bryr Riksrevisjonen seg om informasjonssikkerhet?

Hva er informasjonssikkerhet?

Å sikre at informasjon i alle former (Digdir):

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

- Inkludert sikre digitale tjenester, IKT-systemer og IKT-komponenter som inngår i systemene.



Informasjonssikkerhet er viktig grunnlag for

- kritisk infrastruktur og tjenester
- tilliten til offentlig sektors digitale tjenester
- vellykket digitalisering av offentlig sektor
- personvern
- økonomiske hensyn
- kvaliteten på statens regnskaper

Angrepet av hackere – hele kommunen rammet

Dataangrepet på Østre Toten kommune har lammet nærmest hele kommunen. Over på penn og papir, sier ordfører.

Av IDA LYNGSTAD WERNØ

Ingen Amedia-aviser i trykken etter alvorlig dataangrep

Natt til tirsdag ble flere av Amedias sentrale datasystemer angrepet, og personopplysninger kan være på avveie. Onsdag kommer ingen av papiravisene ut.

Norge | Dataangrep

Stortinget utsatt for IT-angrep: «Et angrep på vårt demokrati».

– Dette er et større og mer avansert angrep enn det forrige, opplyser stortingspresident Tone W. Trøen. Hun mener Stortinget ikke kunne avverget det.

Stortingets president Tone W. Trøen og direktør Marianne Andreassen møtte pressen klokken 16.30 onsdag. T.h. kommunikasjonsrådgiver Gunnar Syverud. *Foto: Paal Audestad*

› PUBLISERT 04.01.2022 13:09

Fylkeskommune lammet av datainnbrudd

Da Nordland fylkeskommune oppdaget inntrengere i datasystemet, trykket de på av-knappen.

HANNE WIEN
995 15 493

Siden datainnbruddet ble oppdaget 23. desember, har alle fylkeskommunens datasystemer som er koblet til Internett, vært stengt ned. Det gjelder blant annet saksbehandlingssystemet og systemet for lønnsutbetaling.

MI

Forbereder til smitte

To ordførere i

Regjeringen f løsninger

NRK TV NRK RADIO

Distrikt Mer

je Siste nytt Dokumentar Klima NRK Ytring

Politiet på bar bakke i Norfund-saken: 100 millioner borte etter digitalt angrep

Norfund bekrefter å ha tapt store summer i en avansert, digital svindel. Politiet har etterforsket saken i det skjulte.

Styreleder Olaug Svarva og administrerende direktør Tellef Thorleifsson i Norfund holdt i dag pressekonferanse om svindel-saken som har rammet selskapet.
FOTO: VIDAR RUUD / NTB SCANPIX

Vegard Venli
Journalist

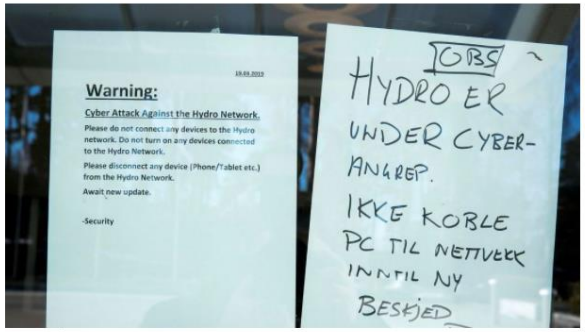
Publisert 13. mai 2020 kl. 12:36
Oppdatert 13. mai 2020 kl. 16:32

Børs

Hackerangrepet mot Hydro enda dyrere enn tidligere antatt: Ny prislapp på 800 millioner kroner

Den endelige prislappen på det massive hackerangrepet ender nå rundt 800 millioner kroner. Forsikringsutbetalingene har vokst til 780 millioner kroner.

2 min Publisert: 23.10.20 – 07.02 Oppdatert: 8 måneder siden



Prislappen på det det omfattende hackerangrepet i mars 2019 mot Hydro, som lammet selskapets fabrikker og anlegg over hele verden, ender rundt 800 millioner kroner. Her fra hovedkontoret i Oslo etter angrepet. (Foto: Terje Pedersen/NTB Scanpix)

Vi er opptatt av

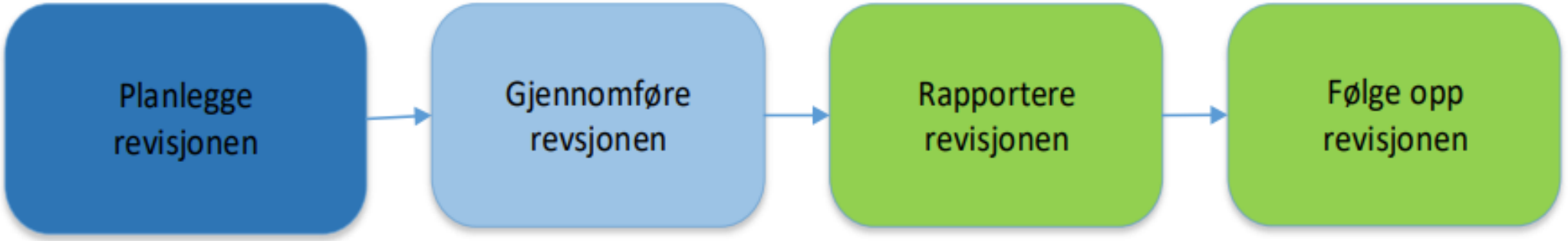
- Hvordan forvaltningen håndterer disse risikoene?
- Etterleves lover og regler?
- Kan vi bidra til å forbedre forvaltningen?
  - Beskyttelse av infrastruktur
  - Beskyttelse av data
  - Sikker digitalisering

3. Revisjonsprosessen

Revisjonsprosessen

INTOSAIs grunnprinsipper for offentlig revisjon

ISSAI 100/18 Generelt kan offentlig revisjon beskrives som en systematisk prosess der revisor objektivt innhenter og evaluerer bevis for å avgjøre hvorvidt saksforholdet (informasjon eller en tilstand) samsvarer med etablerte kriterier. Offentlig revisjon har avgjørende betydning for å fremskaffe relevant informasjon og uavhengige og objektive vurderinger til Stortinget, forvaltningen og borgerne om forvaltningens aktiviteter og gjennomføring av vedtatt politikk.



Planlegging

Målet gir rammen for undersøkelsen

Målet brytes ned i **problemstillinger** som skal besvares

Metoder skal gi tilstrekkelig og hensiktsmessig revisjonsbevis for å besvare problemstillingene og målet

Revisjonskriterier er grunnlaget og målestokken for problemstillinger og målet

Hvor skal vi starte og hvor dypt skal revisjonen gå?

Departementets styring	• Kontrollerer hvordan føringer fra Stortinget følges opp • Kontrollere hvordan departement styrer og følger opp underliggende virksomheter
Styring av informasjonssikkerhet	• Kontrollere hvordan en virksomhet styrer og følger opp egen informasjonssikkerhet
Implementerte sikkerhetstiltak	• Kontrollere om sikkerhetstiltak er implementert og om internkontrollen fungerer
Effekten av sikkerhetstiltak	• Teste om sikkerhetstiltak fungerer
Sikring i dybden	• Simulere angrep

Revisjonskriterier

Stortingets vedtak og forutsetninger utgangspunktet for utledningen av revisjonskriteriene

- Lovvedtak eller Stortingsvedtak

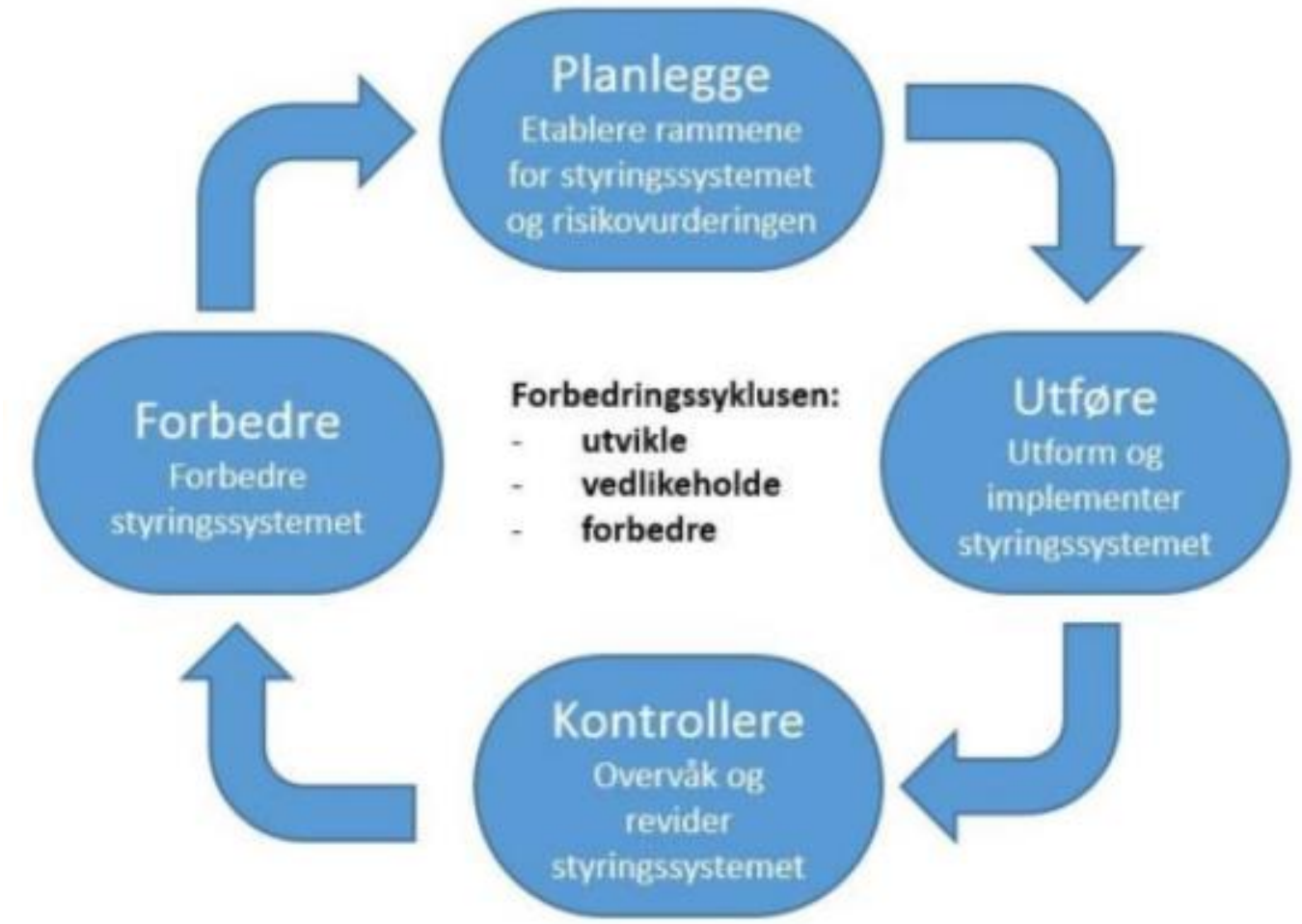
Aktuelt regelverk for IKT-sikkerhetsrevisjoner:

- Bestemmelsene om økonomistyring i staten
- Personopplysningsloven og personvernforordningen
- Forvaltningsloven med eForvaltningsforskriften
- Sikkerhetsloven med forskrifter
- Sektorvise regelverk

Revisjonskriterier styring

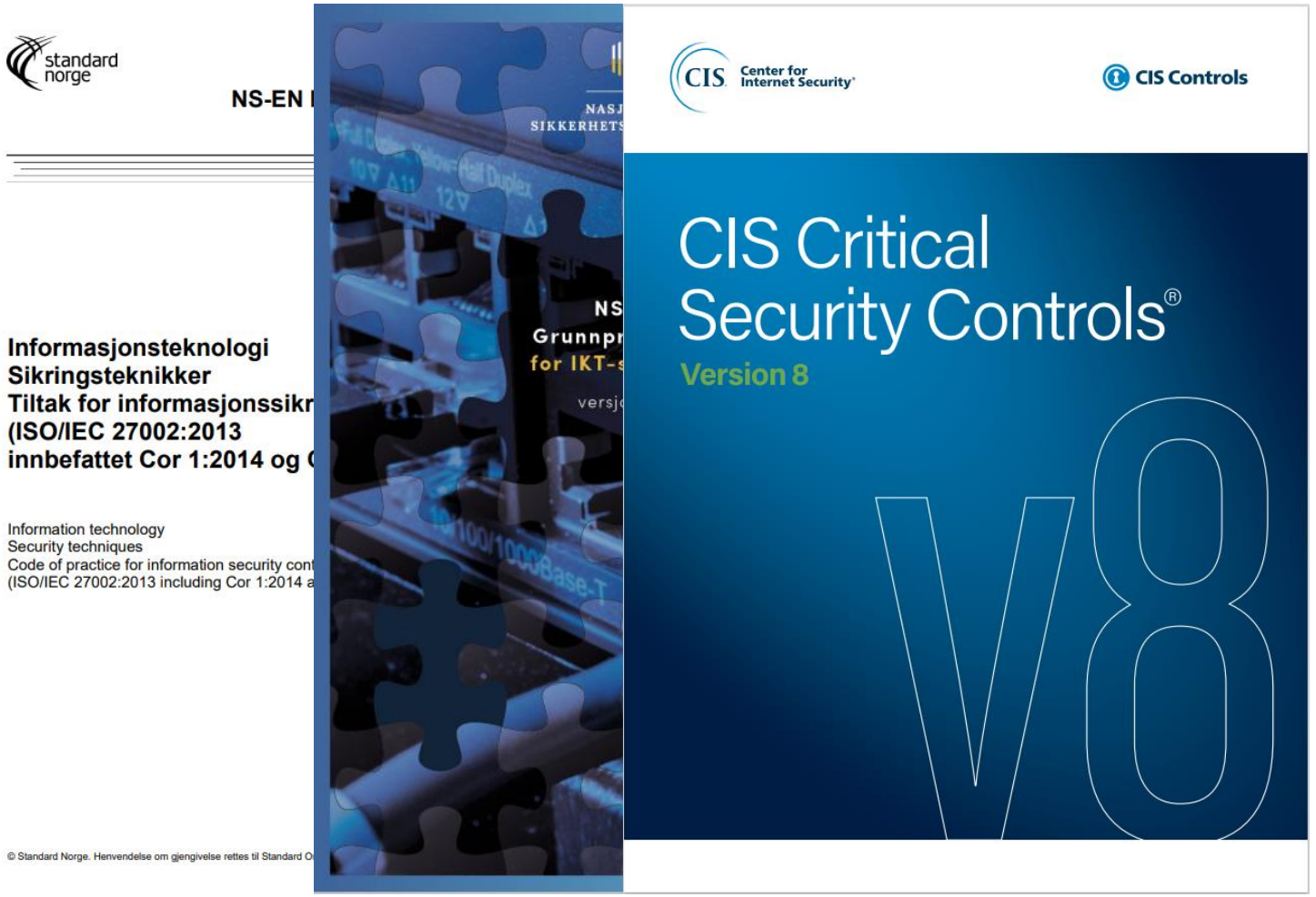
Regelverkene stiller i hovedsak krav om en risikobasert tilnærming til styring og kontroll

- Veiledninger for de ulike regelverkene
- NS-EN ISO/IEC 27001:2017



Kilde: NSM – Veileder i sikkerhetsstyring

Revisjonskriterier sikkerhetstiltak



National Cyber Security Centre

NIST National Institute of Standards and Technology U.S. Department of Commerce

Active Directory

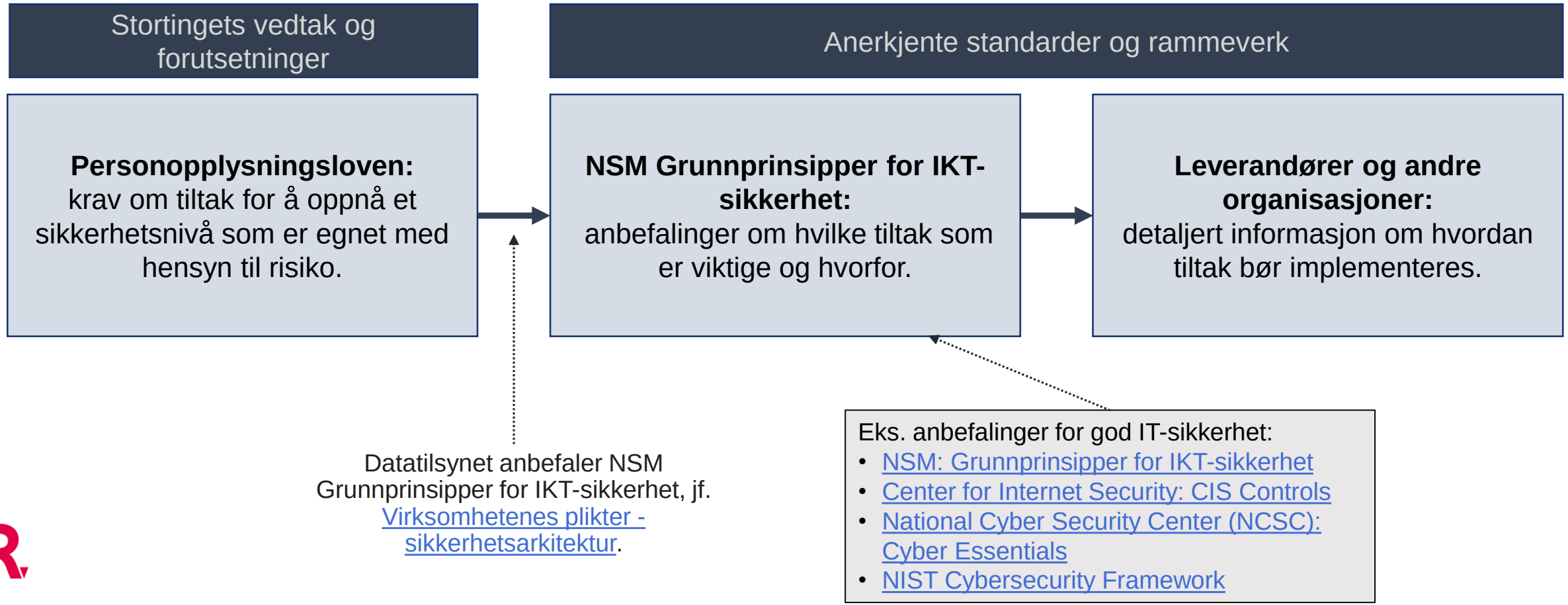
Microsoft SQL Server

Linux

CISCO

ORACLE

Utledning av revisjonskriterier



Metoder for revisjon av informasjonssikkerhet

- **Dokumentanalyse** (analysere interne og eksterne dokumenter)
- **Intervju og spørreundersøkelse** (innhente og analysere informasjon fra personer som har kjennskap til saksforholdet)
- **Dataanalyse** (analysere og sammenligne informasjon/data f.eks. for å identifisere forhold som er i strid med hva som er forventet/beste praksis)
- **Sikkerhetstesting (**anvende metoder fra etisk hacking for å verifisere faktisk sikkerhet i systemer)

Dokumentanalyse

Ved en revisjon av IT-sikkerhet analyseres f.eks.:

- Dokumentasjon av styringssystem for informasjonssikkerhet
- Risikoanalyser og dokumentasjon av håndtering av risiko
- Rutiner for drift av systemer, tilgangshåndtering mv.
- Dokumentasjon av systemer og konfigurasjon av disse

Måles opp mot revisjonskriteriene

Intervju og spørreundersøkelse

Intervju

- Strukturert samtale mellom revisor og ett eller flere intervjuobjekter
- Ofte med toppledelse, IT-ledelse og ikke minst fagfolk som drifter ulike systemer
- Kan bl.a. bidra til å forstå virksomhetens valg og dokumentere deres oppfatning av egen IT-sikkerhet

Spørreundersøkelse benyttes for å samle inn data fra et stort antall respondenter

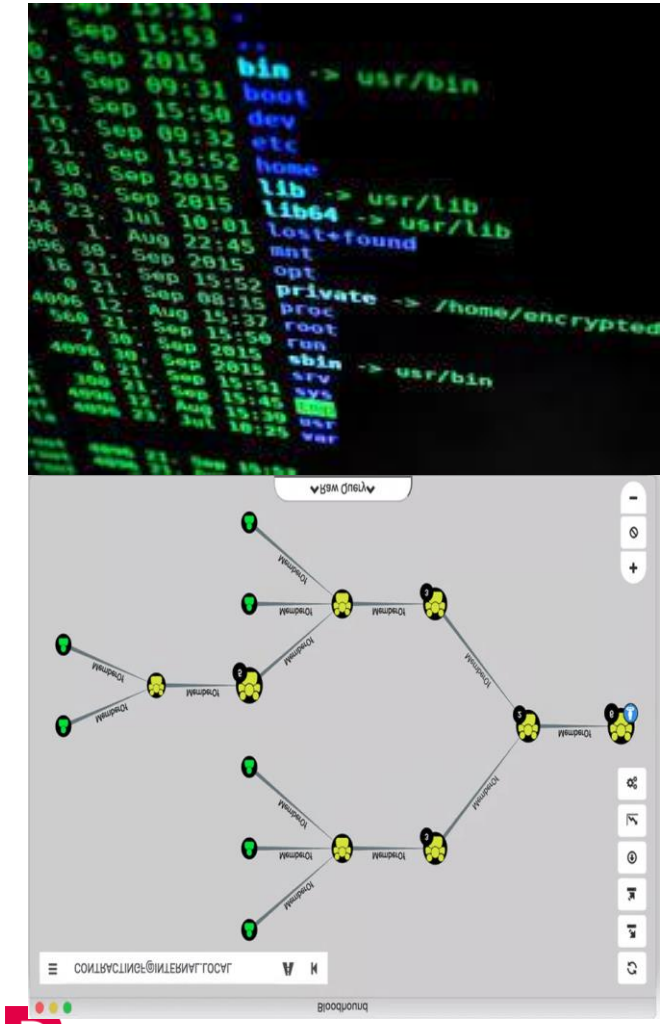
Dataanalyse

Kan for eksempel gjøre uttrekk av:

- Alle brukerkontoer, grupper og ressurser fra Active Directory
- Konfigurasjonsdata for operativsystem, databaser, applikasjoner
- Versjoner av programvare på en stikkprøve servere og PC-er

Uttrekk ses opp mot beste praksis for sikkerhet

Risiko ut fra avvik diskuteres med virksomheten



Sikkerhetstesting

Bruker ulike verktøy og teknikker som er vanlig å bruke for etiske hackere og simulerer angrep:

- Nmap
- BloodHound
- Phishing
- Ping
- Ulike scanningsverktøy
- Høste brukernavn og passord, og knekke passord
- Observere om overvåkingsmekanismene fanger opp «angrepene»

Resultater ses opp mot beste praksis for sikkerhet

Risiko ut fra avvik diskuteres med virksomheten

4. Eksempler på revisjoner – resultater og erfaringer

Betraktninger fra revisor – hvilke utfordringer ser vi?

- Sikkerhetsnivået er for lavt – det er ofte vesentlige svakheter i flere av de prioriterte sikkerhetstiltakene i Grunnprinsipper for IKT-sikkerhet.
- Mangelfull evne til å oppdage sikkerhetshendelser gjennom logging og overvåkning.
- Lavt/moderat modenhetsnivå i styringen av informasjonssikkerhet.

Styringssystem

Kilde: NSMs veileder for sikkerhetsstyring/Riksrevisjonen

NSM - Risiko 2022

Både private bedrifter og offentlige virksomheter som understøtter viktige verdier, må ha oppdaterte vurderinger av risiko og en gjennomgående risikostyringsprosess.

Arbeidet kan gjerne inngå som en del av den overordnede virksomhetsstyringen, men den må være kunnskaps- og risikobasert.

Det innebærer at styring og oppfølging må ledes av ansatte som kjenner virksomheten godt og som også har god og oppdatert forståelse for trussel- og risikobildet. De må også ha den øverste ledelsen i ryggen.

Informasjonssikkerhet i Norfund

NRK TV NRK RADIO NRK P3 YR

Distrikt Mer

je Siste nytt Dokumentar Klima NRK Ytring

Politiet på bar bakke i Norfund-saken: 100 millioner borte etter digitalt angrep

Norfund bekrefter å ha tapt store summer i en avansert, digital svindel. Politiet har etterforsket saken i det skjulte.

Vegard Venli
Journalist

Publisert 13. mai 2020 kl. 12:36
Oppdatert 13. mai 2020 kl. 16:32

Styreleder Olaug Svarva og administrerende direktør Tellef Thorleifsson i Norfund holdt i dag pressekonferanse om svindel-saken som har rammet selskapet.
FOTO: VIDAR RUUD / NTB SCANPIX

E24 AKSJELIVE BØRS E24+ TIPS OSS

Næringsliv | Børs og finans Næringsliv Olje og energi Den grønne økonomien Hav og sjømat Norsk økonomi

Schibsted E24 er en del av Schibsted. Schibsted er ansvarlig for dine data på denne siden. Les mer her

Annonse

Nordnet

Velg egen pensjonskonto hos Nordnet nå.

→ Flytt pensjonen d

DATAANGREP

Norfund ble svindlet for 100 millioner: – Dette er dobbelt så stort som Nokas-ranet

Det statseide Norfund har tapt 100 millioner kroner i et digitalt angrep, opplyser de onsdag.

Norfund

Undersøkelsen av Norfunds styring av informasjonssikkerhet viser at selskapet:

- Har undervurdert informasjonssikkerhet som en risiko
- Mangelfull oppfølging av tjenesteleverandør av IKT-tjenester
  - Innføringen av besluttede tiltak tok for lang tid
  - Uklare roller og ansvar for håndtering av sikkerhetshendelser
- Det er fortsatt svakheter i Norfunds IKT-sikkerhet per august 2020

Nasjonal sikkerhetsmyndighet

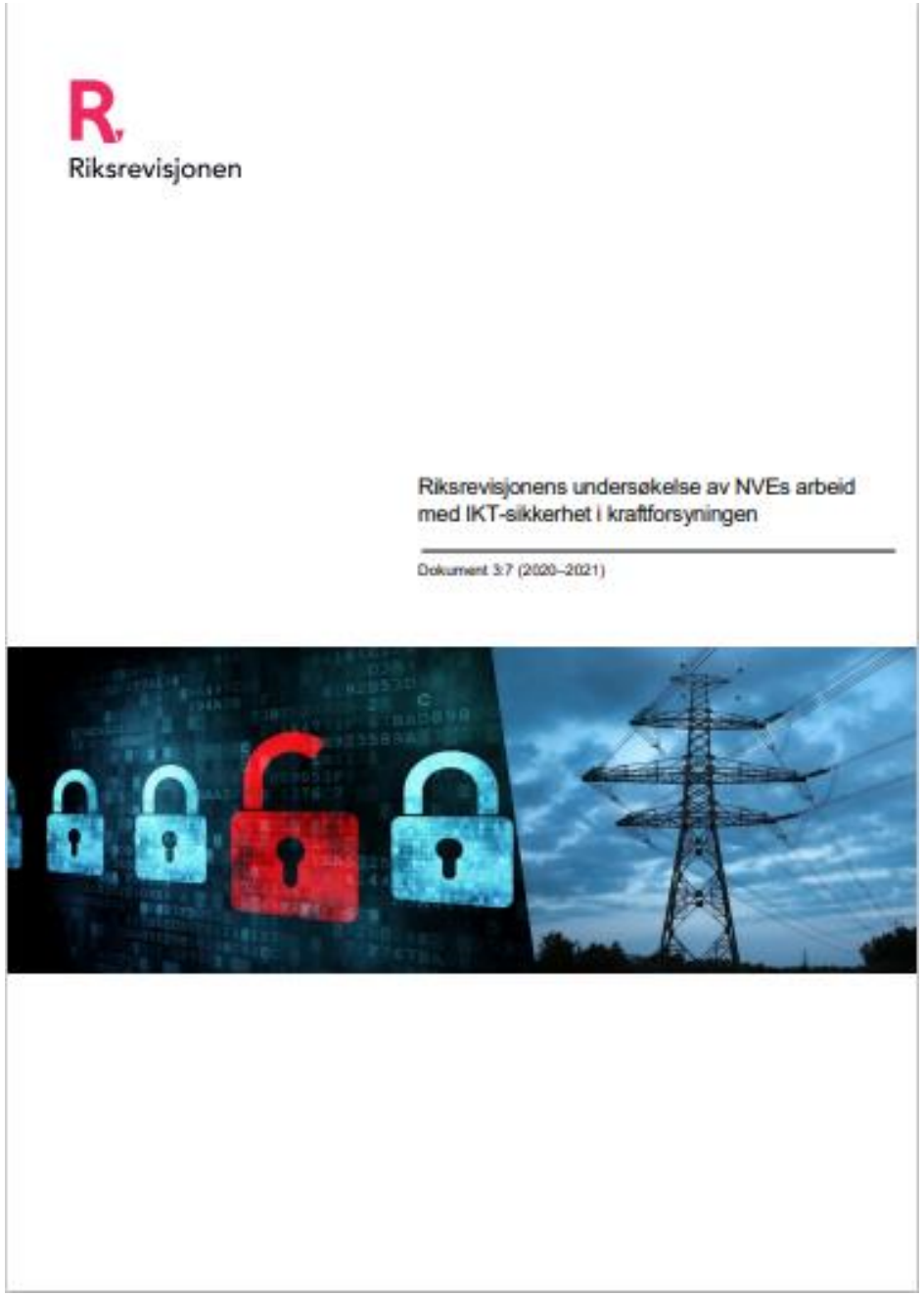
NSM

Sjekkliste nr 1 (S-01)
Oppdatert 2016-03-03

Fire effektive tiltak mot dataangrep

Dette dokumentet beskriver fire enkle, men effektive tekniske tiltak som systemeiere i offentlige sektor bør benytte for å beskytte sine ugraderte systemer mot internett-relaterte dataangrep. Tiltakene er beskrevet mer detaljert i NSMs dokument U-01 (se lenke nederst).

De mest vanlige dataangrep skjer via infiserte e-poster, nettsider, eller USB-minnepinner. De fleste av disse angrepene er teknisk sett relativt enkle å stoppe. NSM har i flere tiår utviklet tekniske sikkerhetstiltak for beskyttelse av nasjonens graderte systemer. Ut i fra disse og andre erfaringer ser vi at virksomheter enkelt kan stanse de mest vanlige angrepene (ca. 80-90%) med fire tekniske tiltak:



IKT-sikkerhet i kraftforsyningen

Målet med undersøkelsen er å vurdere i hvilken grad NVEs virkemiddelbruk bidrar til å styrke IKT-sikkerheten i kraftforsyningen.

Metoder:
Dokumentanalyse, intervjuer, saksgjennomgang av IKT-sikkerhetstilsyn, varsler og rapportering om hendelser, spørreundersøkelse til IKT-sikkerhetskoordinatorer i KBO-enhetene og caseundersøkelse om IKT-sikkerheten i utvalgte selskaper. I tillegg har vi sammenstilt og analysert tilgjengelig statistikk og deltatt som observatør på tre av NVEs IKT-tilsyn.

Case: 3 selskaper av ulik størrelse

Metoder: dokumentanalyse, intervjuer, observasjoner, analyser og tester av kontroller.
Kriterier: energiloven med kraftberedskapsforskriften og veiledning til selskapene fra NVE
Selskapene som deltok var med frivillig, alle tester gjennomført med deres tillatelse og resultater verifisert.

Hva viste caseundersøkelsen?

Svakheter i:

- rammeverket for IKT-sikkerhetsarbeidet

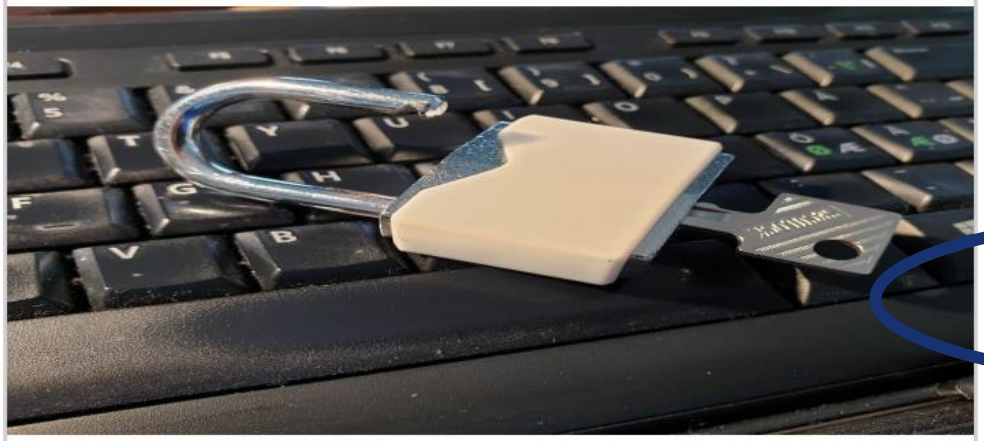
- aktiviteter som inngår i sikkerhetsarbeidet:
  - Identifisere og dokumentert verdier og verdikjeder og gjennomførte risikovurderinger
  - Gjennomføre evalueringer og sikkerhetsrevisjoner
  - Stille krav til og følge opp leverandører

- utvalgte sikkerhetstiltak som ble testet

Riksrevisjonen

Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer

Rapportvedlegg til Dokument 3:2 (2020-2021)



Forebygging av angrep i helseforetakene

Målet med undersøkelsen er å vurdere hvordan helseforetakenes IKT-systemer sikres mot dataangrep, hvordan de regionale helseforetakene understøtter dette arbeidet, og hvordan Helse- og omsorgsdepartementet følger opp.

	Alle helseforetak og regionale IKT-leverandører	De fem utvalgte helseforetakene	Regionale IKT-leverandører	Regionale helseforetak	Helse- og omsorgs-departementet
Dokumentanalyse	X		X	X	**X**
Spørrebrev	X				
Intervju[20]		X	X	X	**X**
Angrepssimulering og tekniske kontroller	X				
Phishingtest og observasjoner		X[21]			
Analyse av avviksmeldinger		**X**	**X**		

Kilde: Riksrevisjonen

Hva viste tekniske kontroller og de simulerte angrepene?

- Simulerte dataangrep ga høy grad av kontroll over IKT-infrastrukturen i tre av fire helseregioner, og tilgang til store mengder sensitive helseopplysninger i alle regionene
- I alle fire helseregioner er det vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak som skal forebygge og oppdage dataangrep
- Helseregionene er på etterskudd i informasjonssikkerhetsarbeidet, og de mangler oversikt over sikkerheten i IKT-infrastrukturen
- Atferden blant helse- og IKT-personell svekker IKT-sikkerheten

Betraktninger fra revisor – hvilke utfordringer ser vi?

- Sikkerhetsnivået er for lavt – det er ofte vesentlige svakheter i flere av de prioriterte sikkerhetstiltakene i Grunnprinsipper for IKT-sikkerhet.
- Mangelfull evne til å oppdage sikkerhetshendelser gjennom logging og overvåkning.
- Lavt/moderat modenhetsnivå i styringen av informasjonssikkerhet.

Betraktninger fra revisor – hvem er det som lykkes?

- Tilpasset virksomheten
- Arbeider systematisk
- Evaluerer

- Interesse og engasjement fra toppledelsen
- Kunnskap og bevissthet om IKT-sikkerhet

Aktuelle rapporter

Omtale av funn fra revisjon i Dokument 1 eller i 3-serien kan være unntatt offentlighet, sladdet eller gradert etter sikkerhetsloven

Aktuelle revisjoner:

- Undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen (Dokument 3:7 (2020-2021))
- Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer (Rapportvedlegg til Dokument 3:2 (2020-2021))
- Undersøkelse av informasjonssikkerhet i Norfund (Rapportvedlegg til Dokument 3:2 (2020–2021))
- Undersøkelser av informasjonssikkerhet i Dokument 1 (2019-2020):
  - IKT-systemer i politiet
  - Utenriksdepartementet
  - Oljedirektoratet (rapport offentlig)
- Undersøkelser av informasjonssikkerhet i Dokument 1 (2018-2019):
  - Arbeids- og velferdsetaten
  - Direktoratet for økonomistyring (DFØ)
  - Arbeidstilsynet
  - Fylkesnemndene for barnevern og sosiale saker
  - Statens Kartverk