NTNU

Kunnskap for en bedre verden

Informasjonssikkerhet i kommunene

Gaute Wangen, seniorrådgiver

Seksjon for digital sikkerhet, NTNU

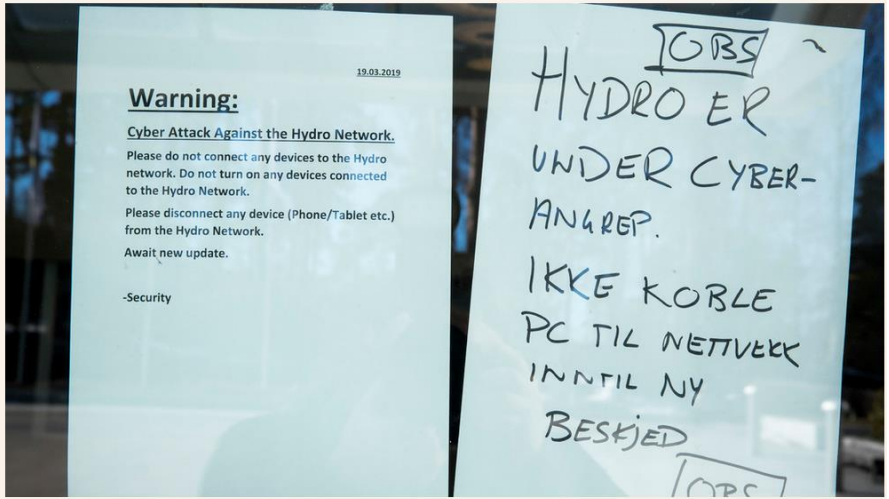
Innhold

1. Hvorfor informasjonssikkerhet?
2. Grunnleggende informasjonssikkerhet
    1. Pilarene in informasjonssikkerhet
    2. Eksempler på problemstillinger
3. Cyber-problem-space
    1. Hvorfor er cybersikkerhet et problem
    2. Eksempler fra NTNU
4. Har Norges kommuner kontroll?
    1. Eksempel på revisjonsområder av informasjonssikkerheten
    2. NSM sin grunnprinsipper for IKT-sikkerhet, v1.1
    3. Oppsummering

Hvorfor trenger vi informasjonssikkerhet?

Cyberangrep koster opptil 450 millioner

Cyberangrepet i mars har kostet Norsk Hydro opptil 450 millioner kroner, ifølge en oppdatering fra selskapet. Kvartalsrapporten er utsatt til juni.



UNDER ANGREP: Hydro sier tirsdag at regningen for cyberangrepet i mars får en økonomisk effekt på 450 millioner kroner i første kvartal. Selve kvartalsrapporten er utsatt til juni på grunn av angrepet. **FOTO:** TERJE PEDERSEN *NTB SCANPIX*

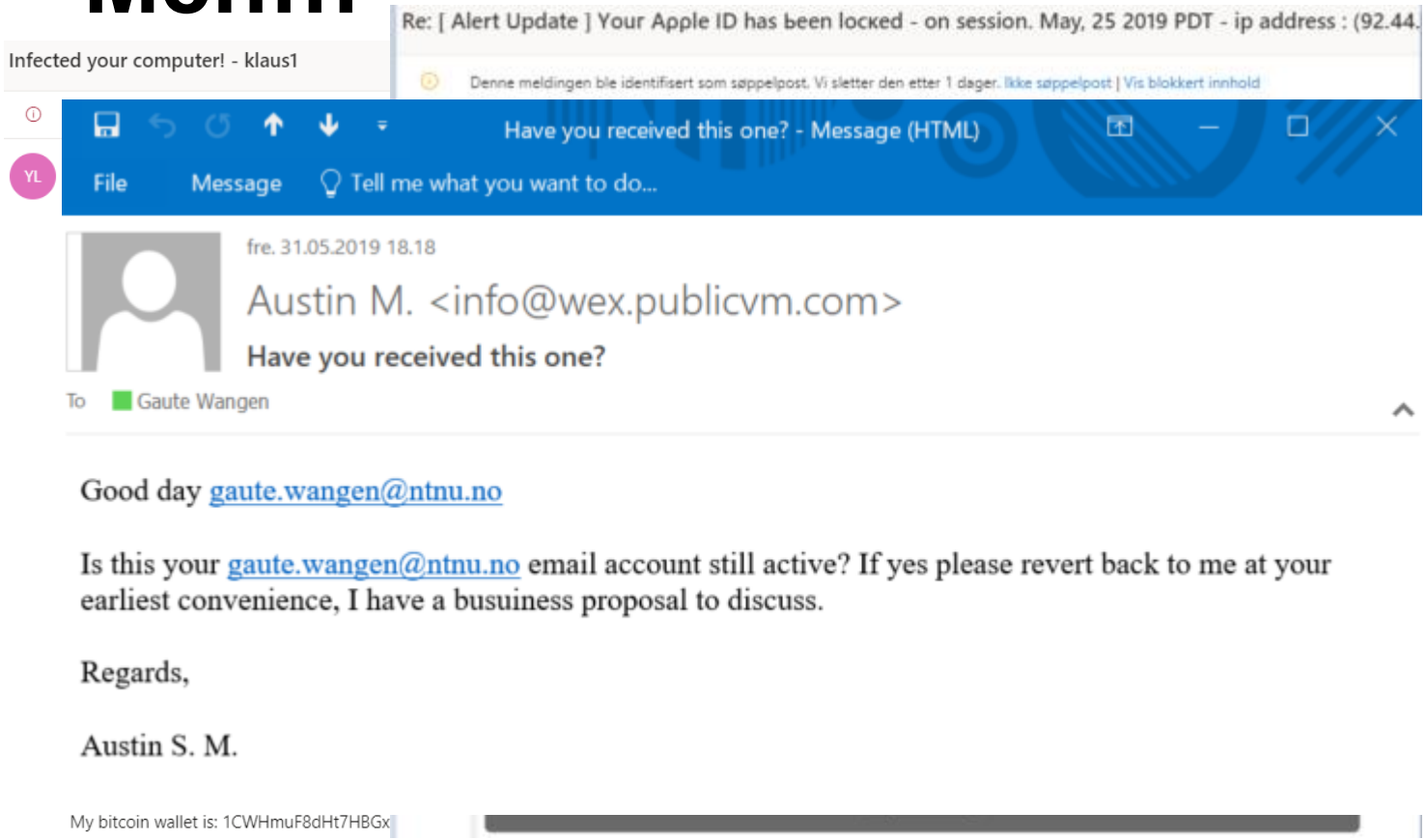
https://e24.no/boers-og-finans/norsk-hydro/cyberangrep-har-kostet-hydro-opptil-450-millioner/24612353

MEN JEG ER DA IKKE ET MÅL!?

1. Jeg har ingenting av verdi
2. Jeg har ingenting å skjule
3. Ingenting å frykte

100% Not a target.

Men…

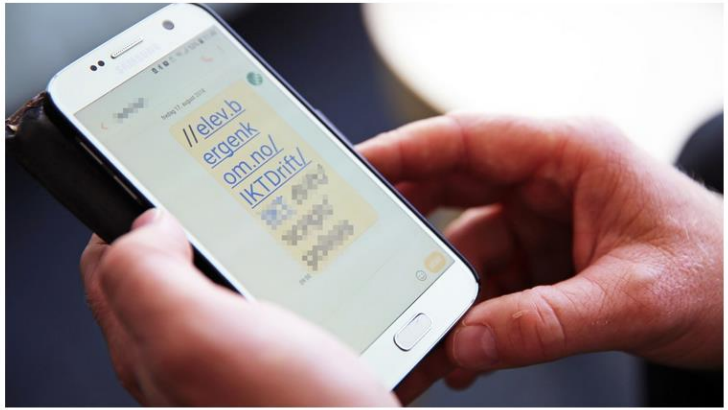

Infected your computer! - klaus1
Re: [Alert Update] Your Apple ID has been locked - on session. May, 25 2019 PDT - ip address : (92.44.
Denne meldingen ble identifisert som søppelpost. Vi sletter den etter 1 dager. Ikke søppelpost | Vis blokkert innhold
Have you received this one? - Message (HTML)
YL
File
Message
Tell me what you want to do...
fre. 31.05.2019 18.18
Austin M. <info@wex.publicvm.com>
Have you received this one?
To
Gaute Wangen
Good day gaute.wangen@ntnu.no
Is this your gaute.wangen@ntnu.no email account still active? If yes please revert back to me at your earliest convenience, I have a busuiness proposal to discuss.
Regards,
Austin S. M.
My bitcoin wallet is: 1CWHmuF8dHt7HBGx


HELLO, THIS IS MICROSOFT SUPPORT CALLING.
Microsoft
THERE IS SOMETHING WRONG WITH YOUR PC. PLEASE INSTALL THIS FILE.
imgflip.com

Hvorfor trenger vi informasjonssikkerhet?

Milliongebyr etter sikkerheitsflause blir ståande – historisk gebyr til Bergen kommune

Bergen kommune meinte dei ikkje burde få gebyr etter at ein elev avdekte fleire filer som låg opne på skulens datasystem. Datatilsynet står fast på bot på 1,6 millionar kroner.



VEG INN: På denne adressa fann den datakyndige skuleeleven tilgang til ein mappestruktur som gav han innsyn i brukarnamn og passord til potensielt 35.000 elevar og lærarar i bergensskulen.
FOTO: EVEN NORHEIM JOHANSEN / NRK

Even Norheim Johansen
@evennor
Journalist

Publisert 19. mars kl. 08:42
Oppdatert 19. mars kl. 12:27

https://www.nrk.no/hordaland/datatilsynet-star-fast-pa-milliongebyr-_-historisk-bot-til-bergen-kommune-blir-staande-1.14479734

Pilarene i informasjonssikkerhet

- Verdien av informasjonen du besitter:
  - Konfidensialitet: Krav til hemmelighold
  - Integritet: Krav til pålitelighet og riktighet
  - Tilgjengelighet: Krav til tilgjengelighet og oppetid
  - Monetær verdi?
- Datakvalitet:
  - Korrekthet
  - Kompletthet
  - Tidsriktighet
  - Konsistens

Når trenger vi informasjonssikkerhet?

Lagring

Bruk

Transitt

Eksempler på informasjonssikkerhetsproblematikk

1. Kan jeg sende dette dokumentet på epost til en kollega? — Transitt
2. Er dette lagringsområdet trygt nok for å lagre dokumentet og hvor tilgjengelig er det? — Lagring
3. Kan jeg åpne og arbeide på dette dokumentet inne i togkupeen? — Bruk
4. Kan jeg stole på innholdet i dokumentet? — Bruk

Informasjonsklassifisering

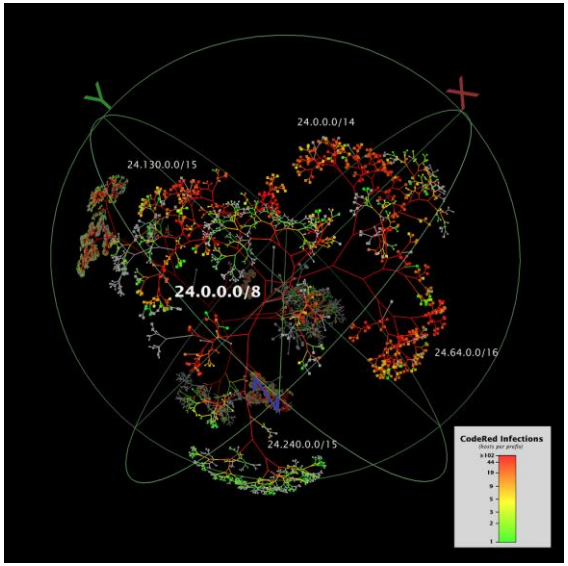
Nivå	Konfidensialitet	Integritet	Tilgjengelighet
1	Offentlig	Ingen betydning	Ingen betydning
2	Intern	Forventet	2 dager
3	Fortrolig	Avhengig	4 timer
4	Strengt fortrolig	Kritisk	Umiddelbar

Eksempler på informasjonssikkerhetsproblematikk

Scenario		Sikkerhetskrav
1. Transitt	Kan jeg sende dette dokumentet på epost til en kollega?	Konfidensialitet
2. Lagring	Er dette lagringsområdet trygt nok for å lagre dokumentet og hvor tilgjengelig er det? Hvem skal ha tilgang?	Konfidensialitet Tilgjengelighet
3. Bruk	Kan jeg åpne og arbeide på dette dokumentet inne i togkupeen?	Konfidensialitet
4. Bruk	Kan jeg stole på innholdet i dokumentet?	Integritet Datakvalitet

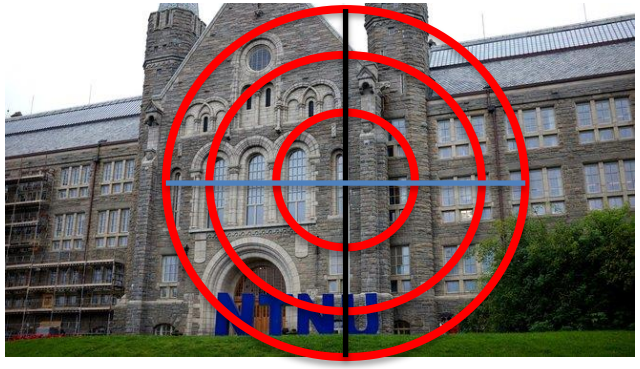
Hvorfor er cybersikkerhet et problem?

- Ingen grenser på internett
- Lett å angripe
- Lav sannsynlighet for konsekvenser
- Barrieren mellom det logiske til det fysiske viskes ut.



- Målrettet
- Tilfeldig
- Fordi det er mulig

NTNU som mål

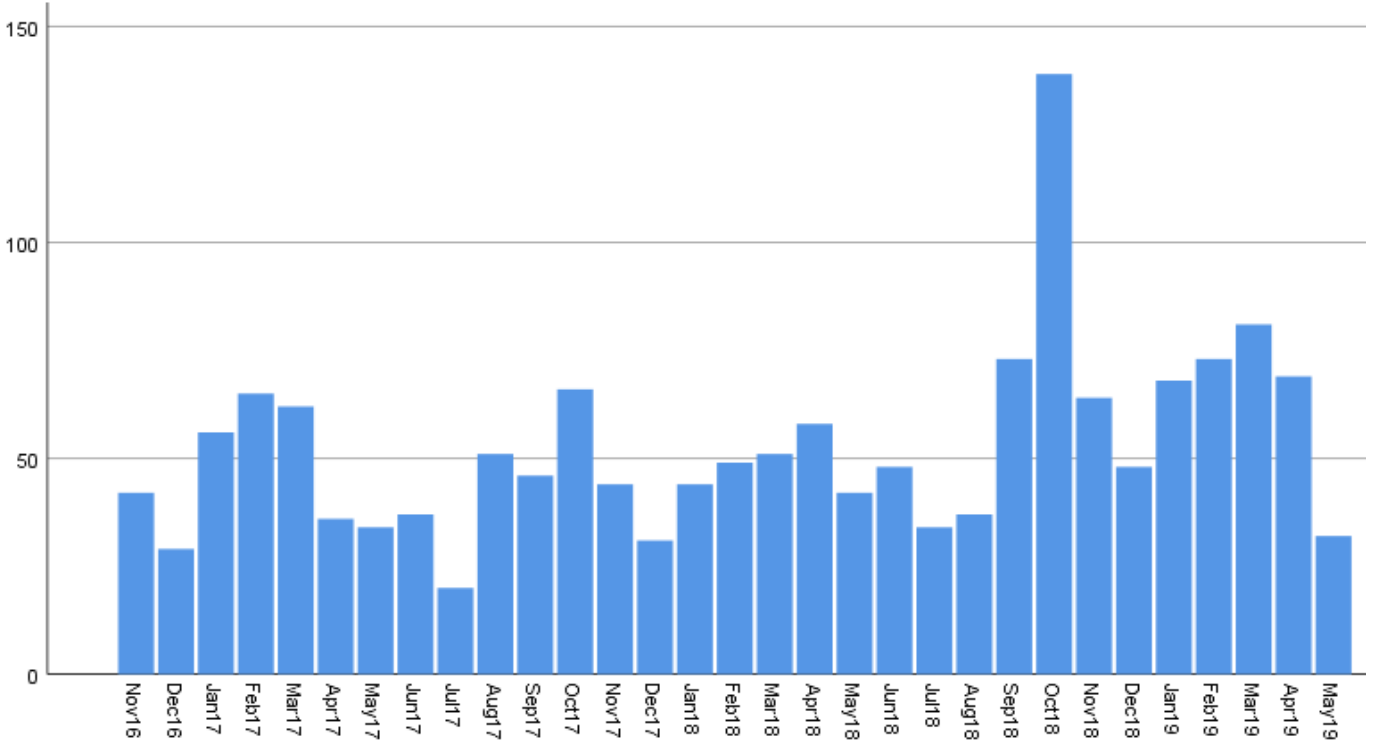


Norges største Universitet

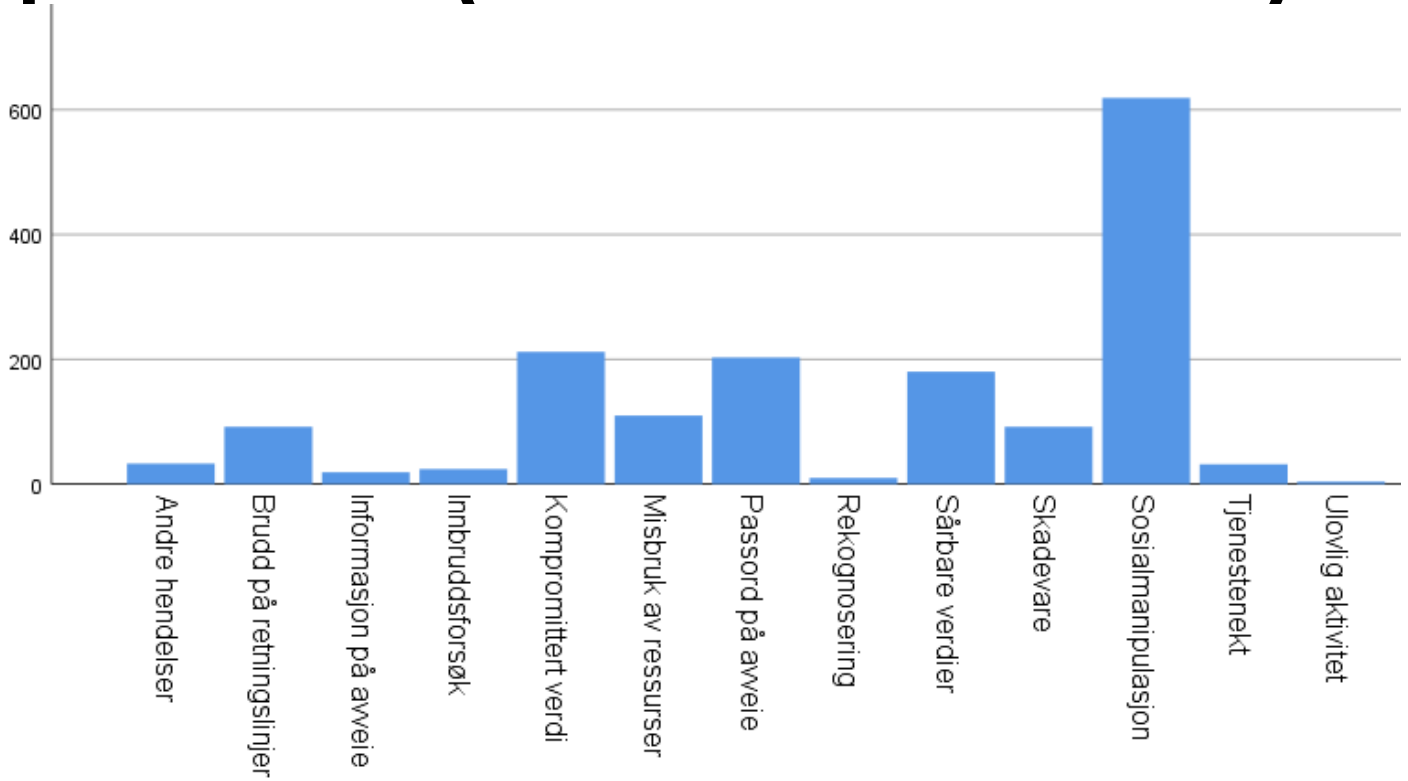
- Over 40 000 studenter
- Over 7400 ansatte
- Ca 1500 servere
- Ca 11 000 driftede klienter
- BYOD fra alle studenter og flere ansatte

Vi har state of the art forskning, men det er primært ikke det *the bad guys* er ute etter.

Antall cybersikkerhetshendelser på NTNU, 1. Nov 2016 – 15. Mai 2019



Hva forårsaker sikkerhetshendelser på NTNU? (01.11.16-15.05.2019)

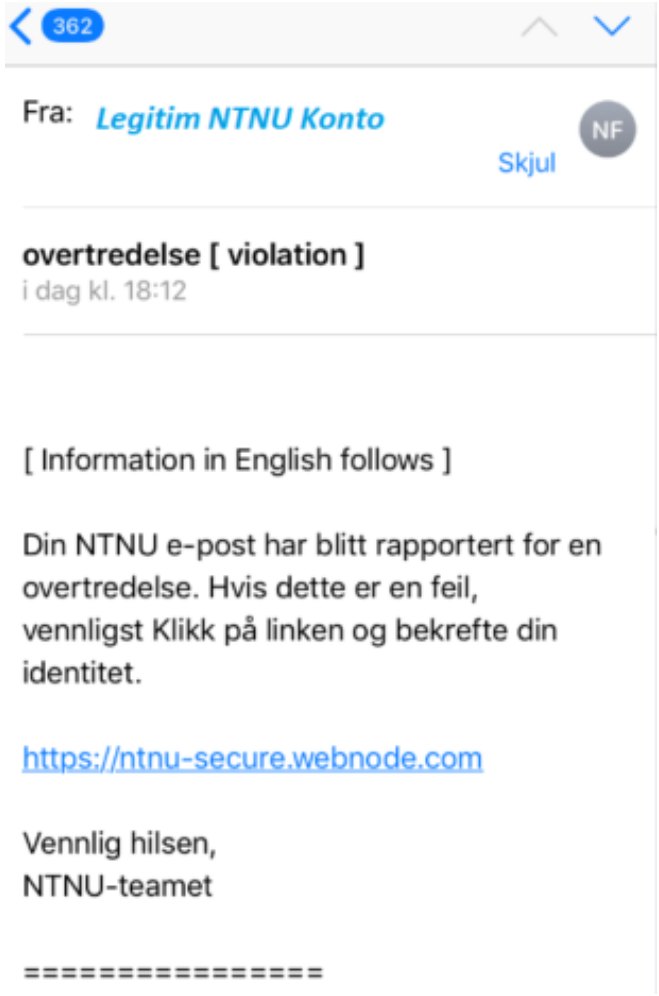


Hvem er trusselen?

- Attribusjonsproblemet:
  - Hvem er hvem på internett?
- Trusselprofilering / Klassifisering
  - Basert på motivasjon
  - Trussel -> menneske
  - Skadevare -> metode/verktøy -> oppnå mål
  - *En trussel er så spesifikk som den trenger å være.*
- To hovedklasser:
  1. De som velger mål basert på verktøy
  2. De som velger/utvikler verktøy basert på mål

Hva er de ute etter?

- Brukernavn og passord
- Båndbreddekapasitet og ressurser
- Regnekraft
- Tilganger
- Penger
- Informasjon
- *Vi vet ikke alltid hva de er ute etter!!!*


362

Fra: *Legitim NTNU Konto*

NF

Skjul

overtredelse [violation]

i dag kl. 18:12

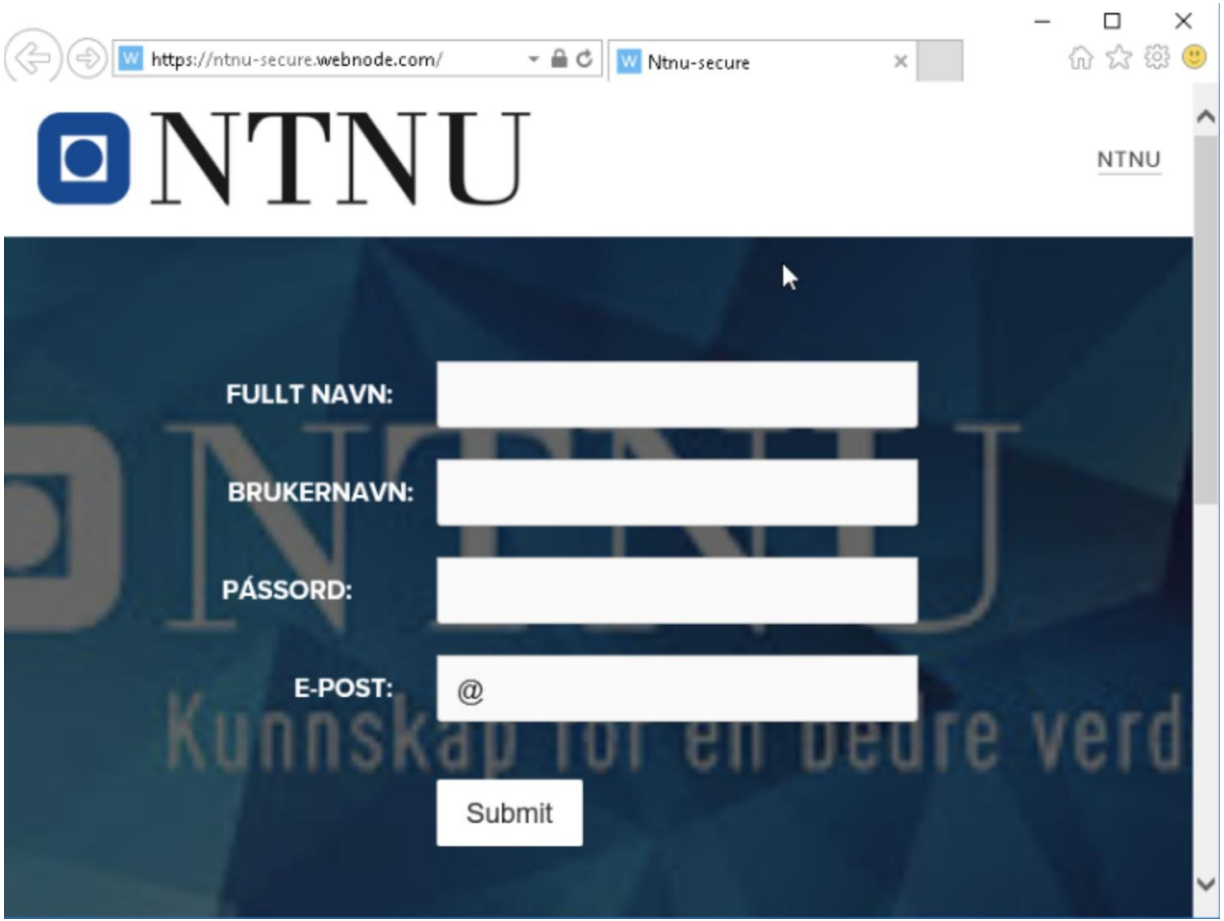
[Information in English follows]

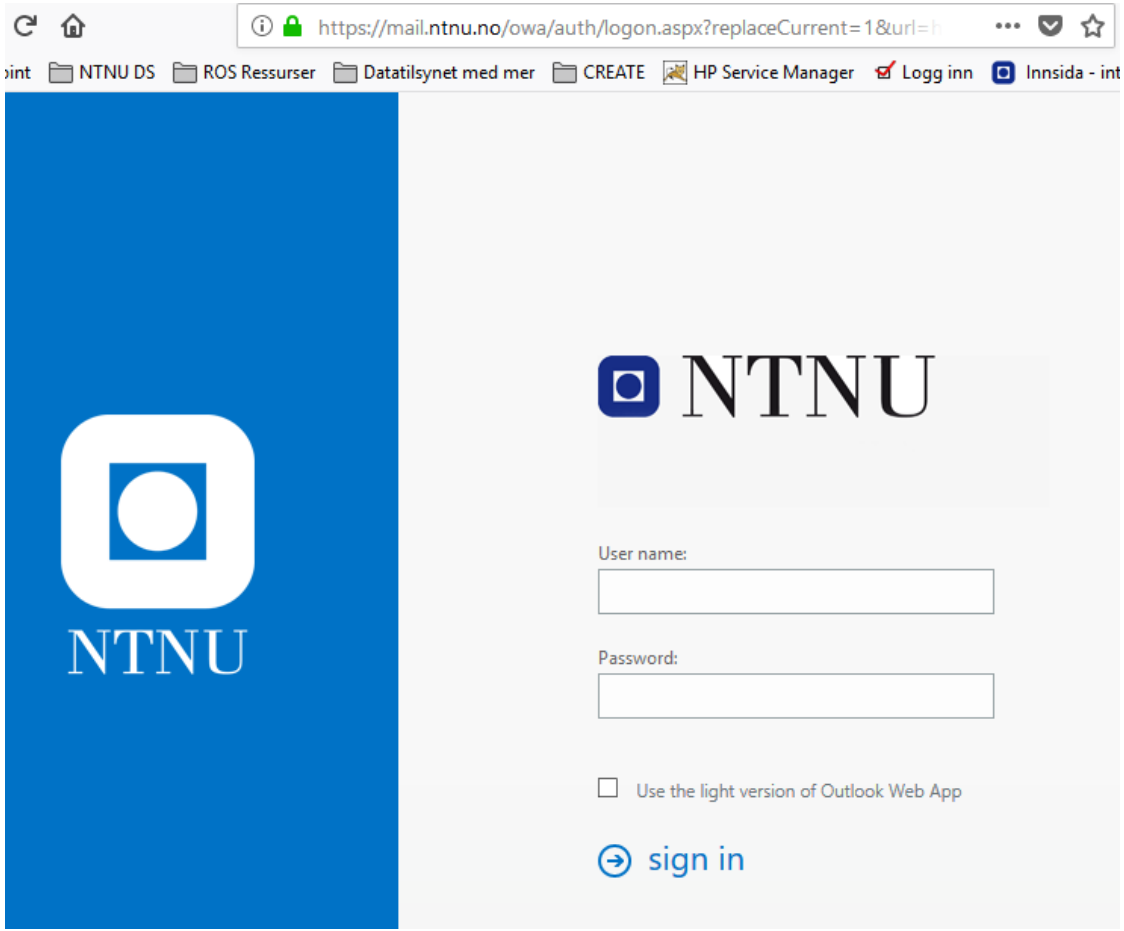
Din NTNU e-post har blitt rapportert for en overtredelse. Hvis dette er en feil, vennligst Klikk på linken og bekrefte din identitet.

https://ntnu-secure.webnode.com

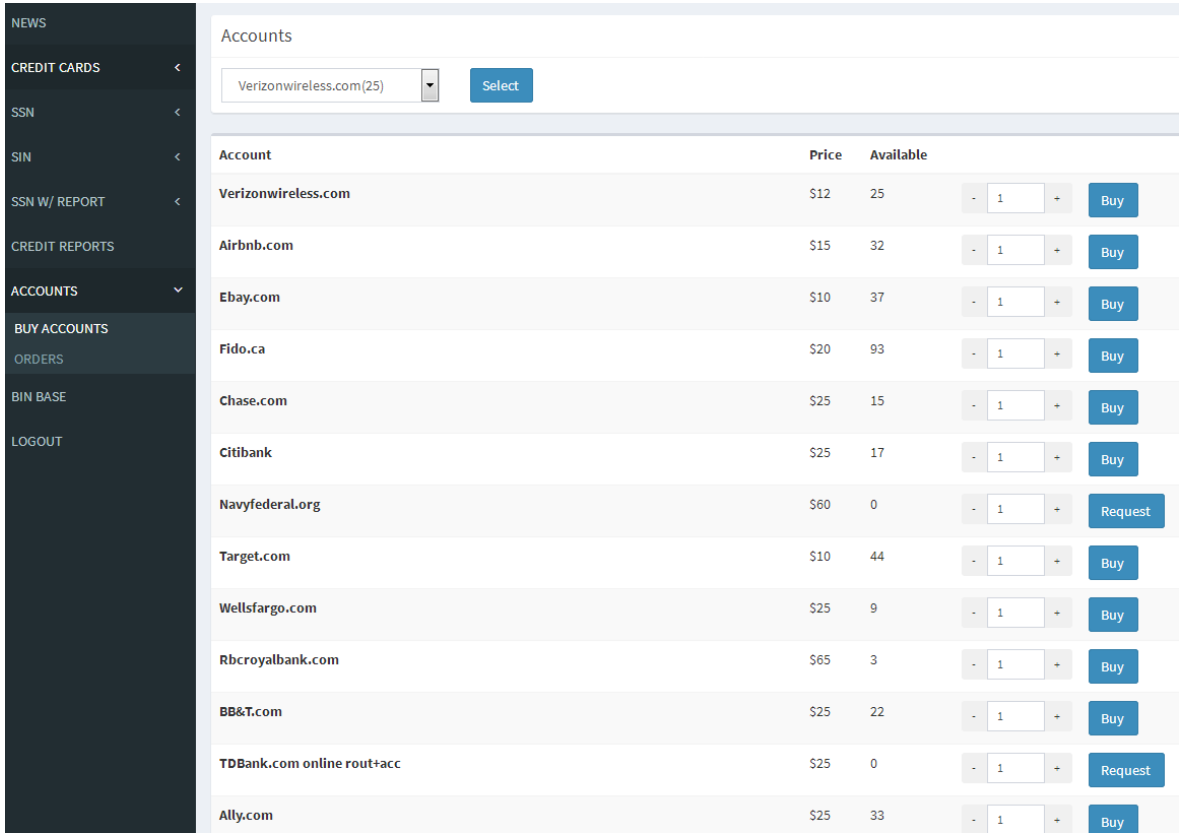
Vennlig hilsen,
NTNU-teamet

==========


https://ntnu-secure.webnode.com/
Ntnu-secure
NTNU
NTNU
FULLT NAVN:
BRUKERNAVN:
PÁSSORD:
E-POST:
@
Submit


https://mail.ntnu.no/owa/auth/logon.aspx?replaceCurrent=1&url=h
NTNU DS
ROS Ressurser
Datatilsynet med mer
CREATE
HP Service Manager
Logg inn
Innsida - int
NTNU
NTNU
User name:
Password:
Use the light version of Outlook Web App
sign in

Markedet for stjålne kontoer



Source: https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/

Hendelsesbildet

- Mange hendelser skjer bare fordi angriper har mulighet.
- Angriper og motivet er ofte ukjent
- Vi arbeider med trusselprofilering, men vanskelig å sikre seg mot alt
- Stort nettverk = stor angrepsflate
- Grunnsikring er viktig!

- Hvordan ser hendelsesbildet i kommunene ut?
  - Kommunene er store arbeidsgivere
  - Mangfoldige tjenester (inkludert kritisk infrastruktur)

Har Norske kommuner kontroll?

Samtlige Oslo-folk kunne ha blitt rammet dersom uvedkommende hadde logget seg inn med det enkle passordet. Her fra Maridalsvannet i Oslo. (Ill.: Oslo Kommune)

Og passordet var: 0-0-0-0

Av **Tore Neset**, 9. september 2011 kl 09:07

Kunne styre Oslos drikkevann.

Source: itavisen.no/2011/09/09/og-passordet-var-0-0-0-0/

Har Norske kommuner kontroll?

Norge

Datatilsynet åpner sak mot Oslo kommune etter personverntabbe

Illustrasjonsfoto: Mariam Butt / NTB scanpix **Foto: NTB scanpix**

Et søksmål på over 300 sider fra en tidligere ansatt lå usladdet på Oslo kommunes nettsider. Datatilsynet åpner sak mot kommunen, melder NRK.

NTB

11. juni 2019 06:54 – *Oppdatert 11. juni 2019 06:56*

Del (1) Tweet Epost

https://www.abcnyheter.no/nyheter/norge/2019/06/11/195585002/datatilsynet-apner-sak-mot-oslo-kommune-etter-personverntabbe

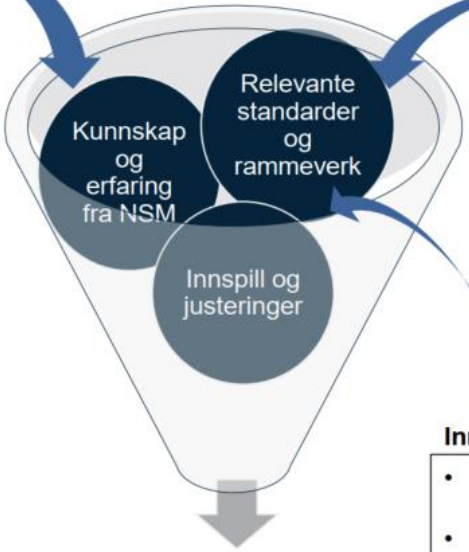
Hvordan ta kontroll?

https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

Hvordan har grunnprinsippene blitt til?

Kunnskap og erfaring NSM

- Rådgivning
- Penetrasjonstest
- Tilsyn
- Hendelser (NorCERT)
- Kravutvikling
- Samarbeids-partnere



Relevante standarder og rammeverk

- ISO 27002
- NIST CSF
- CIS CSC 20
- BSI Grundschutz
- Cyber Essentials
- Sikkerhetsloven
- ++

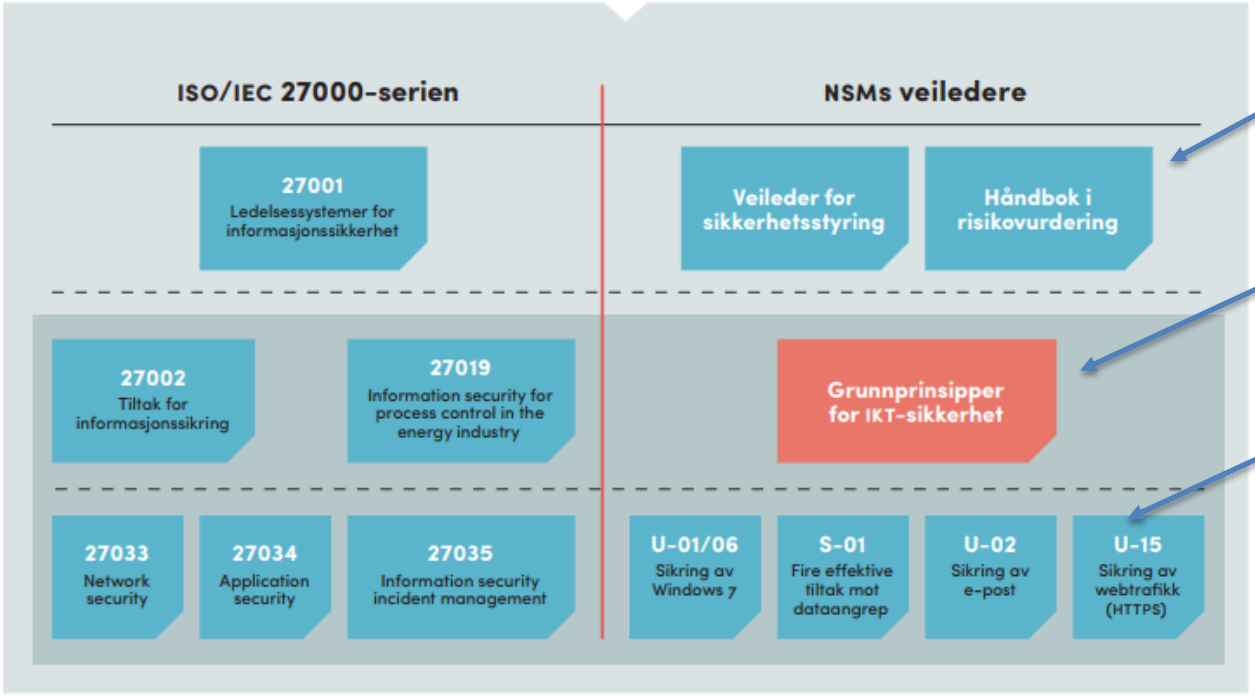
Innspill og justeringer

- Sektormyndigheter og myndighetsorganer
- Offentlige og private virksomheter

13 NASJONAL SIKKERHETSMYNDIGHET

Kilde: Jørgen Dyrhaug, NSM

Rammeverk for beste praksis sammenlignet med NSMs utgivelser



Styringssystem og Policy

Sikkerhetskrav

Prosedyrer

NSM Grunnprinsipper for IKT-Sikkerhet, 2018, side 10

Har de styringssystem for informasjonssikkerhet? (ISO27001 og Veileder for Sikkerhetsstyring)

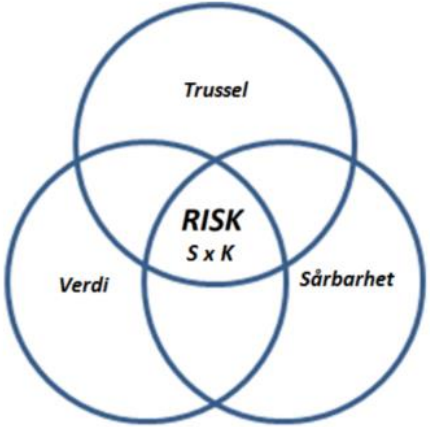
Sikkerhet tilpasset organisasjon/aktivitet

- Sikkerhetspolitikk og ledelsesforankring
- Styringshjul
- Tiltak, oppfølging og kontroll
- Rapportering
- Roller og Ansvar
- Avvikshåndtering

eForvaltningsforskriften §15 – *«Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.»*

Styring: Har kommunen et bevisst forhold til infosekrisiko?

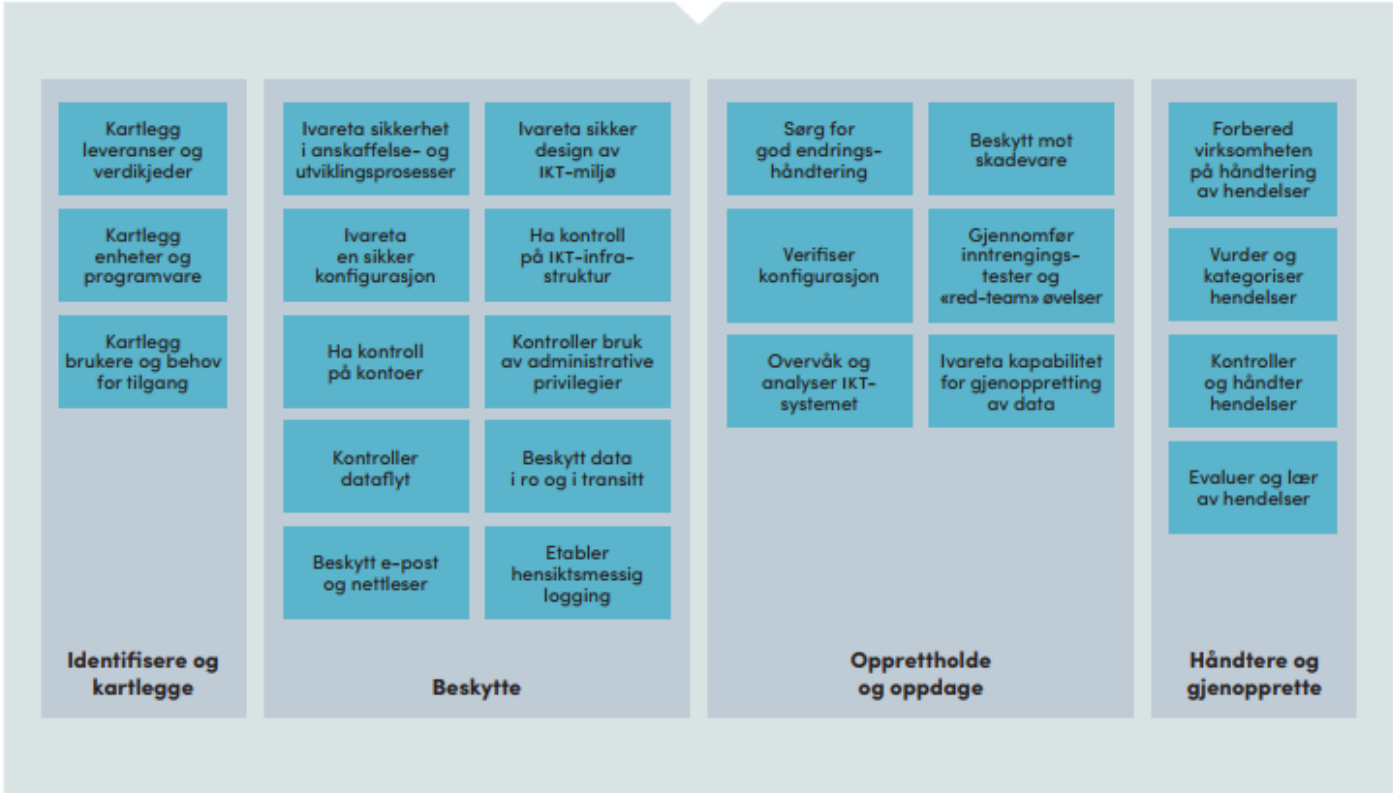
"Muligheten for at en gitt trussel vil utnytte sårbarheter og dermed få tilgang til verdier og forårsake skade på organisasjonen" - ISO/IEC 27005:2008



- *Er det definert en risikoaksept/kriterier?*
- *Gjennomføres risikovurderinger?*
- *Er de dokumentert?*
- *Oppdateres de jevnlig?*
- *Følges tiltakene opp?*
- *Gjennomføres det risikovurdering ved endringer?*

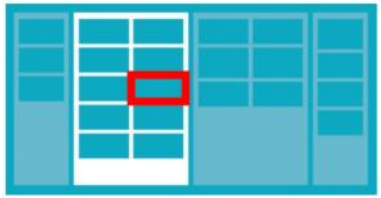
eForvaltningsforskriften §15 – *«Omfang og innretning på internkontrollen skal være tilpasset risiko.»*

Sikkerhetskrav: Grunnprinsippene



NSM Grunnprinsipper for IKT-Sikkerhet, v1.1

Oppbygning av hvert Grunnprinsipp



2.6 KONTROLLER BRUK AV ADMINISTRATIVE PRIVILEGIER

- **Mål:** Kontrollere, korrigere, og spore tildeling, bruk og konfigurering av administrative rettigheter for å hindre misbruk av datamaskiner, nettverk og applikasjoner.
- **Begrunnelse(Hvorfor?)**
  - Misbruk av administrative privilegier
    - Blant de vanligste metodene
    - Eks 1: Infisert epostvedlegg, nedlastbar fil med skadevare fra ondsinnet nettside, nettside med skadevare
    - Eks 2: Eskalering av privilegier (gjette eller knekke passord)

NASJONAL SIKKERHETSMYNDIGHET

Anbefalte tiltak:

ID	BESKRIVELSE
2.6.1	Personer med administrative privilegier (operatører) bør bruke separate
2.6.2	Minimer bruken av administrative rettigheter og bruk administrative kont bruk av administrative privilegerte funksjoner og monitorer systemene fo I de tilfeller sluttbruker har behov for administrative privilegier, bør dette vurderes.
2.6.3	Administratorer bør påkreves å logge på systemer med en personlig, ikke administrative privilegier utføres.
2.6.4	Etabler ulike administratorkontoer til de ulike delene av IKT-infrastruktur administratorkonto ikke gir fulle rettigheter til å endre hele infrastruktur
2.6.5	Administratorer bør benytte dedikerte maskiner for alle administrative op tilganger. Maskinen bør isoleres fra virksomhetens primære nettverk. Ma utarbeide dokumenter eller ha mulighet til å surfe på internett.
2.6.6	Bruk multi-faktor autentisering for å autentisere administrative brukere.

Kilde: Jørgen Dyrhaug, NSM

Har kommunen arbeidet med å identifisere og kartlegge verdier?

- Identifisere og kartlegge:
  - Verdier
  - Personopplysninger
  - Leveranser
  - Verdikjeder
  - Funksjoner
  - Ressurser
- Systemportefølje
- Verdivurdering
- Informasjonsklassifisering

Eks fra NVE: Har virksomheten identifisert og dokumentert verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer? Dokumentasjonen skal holdes oppdatert.

Har kommunen arbeidet med å identifisere og kartlegge verdier?

- Har kommunen kartlagt innsamling og behandlingene av personopplysninger?

- Hva er rutinene/ prosedyrene for å behandle personopplysninger?

GDPR, Artikkel 5
eForvaltningsforskriften, 15§ g) Prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Viktige revisjonsområder: Det Menneskelige

- Kompetanse
- Situasjonsforståelse
- Risikoerkjennelse, forståelse og aksept
- Samarbeid internt i kommunen og eksternt
- «Menneskelige sensorer»
- Forstå verdiene
- Kommunikasjon

Viktige revisjonsområder: Det Organisatoriske

- En systematisk tilnærming til risiko, sårbarhet, trussel og informasjonssikkerhet
  - Rapportering av avvik
  - Rapportering av hendelser
  - Risikovurdering
  - Trusselvurdering
  - Avvikshåndtering
  - Personvern
- Gode planer for hendelseshåndtering og IT beredskap, sett i sammenheng med øvrig beredskap
- Verdivurdering og kontekst

Viktige revisjonsområder: Det Tekniske

- Dybdeforsvar
- Robuste tjenester
- Ha et bevist forhold til muligheter og begrensninger i skyen
- Deteksjon
- Analyse
- Verktøystøtte for hendelseshåndtering

Oppsummering

Revisjonsområder:

1. Styringssystem for informasjonssikkerhet
2. Risikostyring
3. Identifisere og dokumentere
4. Beskytte
5. Opprettholde og oppdage
6. Håndtere og gjenopprette
7. Sikkerhetsrevisjon