KiNS

foreningen kommunal informasjonssikkerhet

Informasjonssikkerhet og GDPR

Harald Torbjørnsen (KiNS)

Medlems- og interesseorganisasjon

- **Medlemmer:**
  - Kommuner, fylkeskommuner og bedrifter

- **Samarbeidspartnere:**

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Utdannings-direktoratet

Datatilsynet

NorSIS
Norsk senter for informasjonssikring

KS

NASJONAL SIKKERHETSMYNDIGHET

Direktoratet for e-helse

NTNU CCIS
Center for Cyber and Information Security

dsb
Direktoratet for samfunnssikkerhet og beredskap

Kommune-CSIRT

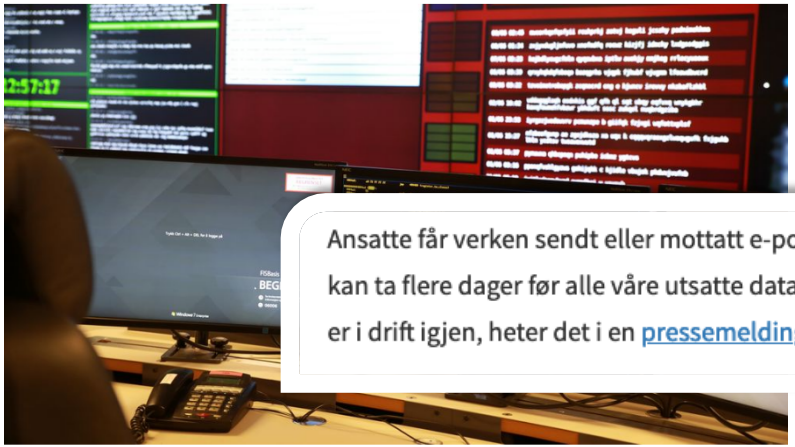
Betydningen av Informasjonssikkerhet

- Skal bidra til å **øke kvaliteten** på leveransene og arbeidet i kommunen/FK
  - God bruk av ressurser
  - Sikre riktig kompetanse hos ansatte
  - Bidra til innebygd informasjonssikkerhet i løsninger
  - Gjøre det mulig å måle effekten av sikkerhetstiltakene
  - Bidra til at informasjonssikkerheten revideres og evalueres

MESPINOZA/PYSA

Advarer om destruktivt angrep mot kommune: Alt innhold skal være kryptert, og alle sikkerhetskopier sletta

– Angriperne har fått tak i alle våre data, og vi er svært bekymra.



> Ansatte får verken sendt eller mottatt e-post. – Det kan ta flere dager før alle våre utsatte datasystemer er i drift igjen, heter det i en pressemelding.

Fra kommandosentralen til Nasjonalt cybersikkerhetssenter (NCSC), som overvåker digitale angrep og trusler mot norske interesser. (Illustrasjonsfoto: Marius Jørgenrud)

MARIUS B. JØRGENRUD LØSEPENGEVIRUS 11. JAN. 2021 - 09:45

Søknader og saksbehandling kan hope seg opp i Østre Toten: – Saksbehandlerne får ikke opp noe på PC-ene sine

Dataangrepet har sendt Guri (44) og kollegene i hjemmetjenesten tilbake til fortida

Varsel om overtredelsesgebyr på 3 millioner kroner til Bergen kommune

20. mai 2020 | Innsikt

Skrevet av Haakon Føyen og Thomas Olsen

Bergen kommune har meldt at de vil godta Norges hittil største overtredelsesgebyr for brudd på personvernforordningen.

Saken gjelder brudd på personopplysningssikkerheten som følge av mangelfull sikring av konfidensialitet i systemet Vigilo, en digital løsning brukt i Bergen kommune som kommunikasjonsportal mellom skoler, barnehager og foreldre.

Via kommunikasjonsportalen Vigilo ble det distribuert fortrolige adresser som var vernet med adressesperre etter folkeregisterloven § 10-4. Opplysningene omfatter barn som ikke skal kontaktes av den andre

typen opplysninger kunne medføre fare for liv og helse for de berørte. At interne prosedyrer rundt informasjonen ikke ble fulgt opp før innfasingen av Vigilo, ble ansett som ett brudd på personvernforordningen artikkel 24 nr. 2.

Skulebyråden i Bergen går av

Byråd Linn Kristin Engø (Ap) trekkjer seg etter Vigilo-skandalen.

GÅR AV: Linn Kristin Engø går av etter Vigilo-skandalen i Bergen.
FOTO: METTE ANTHUN / NRK

Christian Lura
Journalist

Even Norheim Johansen
Journalist

Roy Hilmar Svendsen
Journalist

Publisert 27. jan. kl. 15:10
Oppdatert 27. jan. kl. 18:54

Det varsla Engø sjølv og byrådsleiar Roger Valhammer (Ap) i ein hastig innkalla pressekonferanse klokka 15.00 i ettermiddag.

– Eg har i dag meddelt Roger Valhammer at eg går av som byråd. Eg tar konsekvensen av den politiske situasjonen i Bergen, seier Engø.

Tilsynet anser det som en skjerpende omstendighet at Bergen kommune ble varslet om brudd på personopplysningssikkerheten fra Vigilo uten å følge dette opp.

Informasjonssikkerhet

- **Konfidensialitet** – at informasjonen ikke blir kjent for uvedkommende
- **Integritet** – at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- **Tilgjengelighet** – at informasjonen er tilgjengelig ved behov
- **Robusthet** – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser

Risikovurderinger

- Kjernen i arbeidet med forebyggende informasjonssikkerhet.

- Nøktern vurdering av:
  - hvilke problemer som kan oppstå?
  - hvor store problemene er?
  - hva kan gjøres med de viktigste problemene?

- Kompetansehevende effekt
  - kartlegger og diskuterer IKT-praksis i virksomheter og administrasjon

Reguleringer og krav

- GDPR
  - Prinsipp for informasjonssikkerhet og ansvarlighet
    - Tilstrekkelig sikret
    - Behandlingsansvarlig
    - Krav til dokumentering av sikkerheten
    - Sikring gjennom tiltak
      - Artikkel 5, 24 og 32
  - E-forvaltningsforskriften
    - Krav til styringssystem for IS og standarder
    - Internkontroll

Bildet er tatt av Pete Linforth fra Pixabay

Ledelsessystem for informasjonssikkerhet (LSIS)

- Strukturert system for styring av informasjonssikkerheten i en organisasjon
  - Basert på standarder og rammeverk
  - Må forankres i ledelsen
  - Krever planlegging
  - Livssyklus

LSIS gjennomføres som en livssyklus

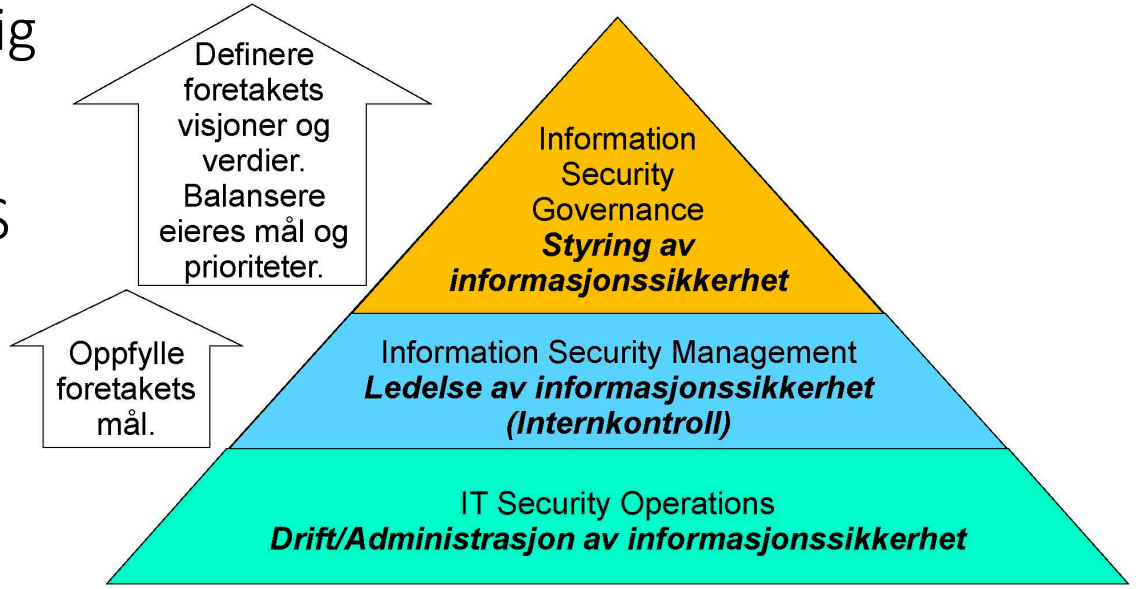
- Fire faser:

1. Planlegg og organiser
2. Implementer
3. Drift og vedlikehold
4. Kontroller og evaluer

NSM – styringshjul for sikkerhet
(Bygd på ISMS / ISO 27001)

Organisasjonsstruktur, roller og ansvar

- Toppledelsen ansvarlig
- Roller og ansvar for IS gjennom hele organisasjonen må konkretiseres og defineres



Hva må kommunen ha på plass?

- Oversikt over hvilke personopplysninger som behandles, hvorfor de behandles, hvem det behandles opplysninger om og hvor opplysningene kommer fra.

- Egnede tekniske og organisatoriske tiltak.
  - Kompetanse.
  - Instrukser, rutiner og retningslinjer – LSIS/ISMS.
  - Risiko- og sårbarhetsvurderinger.
  - Vurdering av personvernkonsekvenser.
  - Innebygd informasjonssikkerhet og personvern i teknologiske løsninger og systemer.
  - Avvikshåndtering.

Kompetanse, kompetanse, kompetanse

KiNS e-læring

Personvernforordningen (GDPR) innebærer at kommuner og fylkeskommuner skal gjennomføre og dokumentere at ansatte har gjennomført opplæring i personvern og informasjonssikkerhet.

Ansatte må ha god og relevant kunnskap om informasjonssikkerhet og personvern tilpasset sine oppgaver!

Opplæringsfilmer fra KiNS

Vi har en rekke filmer som dere kan bruke i arbeidet med opplæring og bevisstgjøring om informasjonssikkerhet og personvern i kommunen eller fylkeskommunen. Filmene finnes både i tekstet og utekstet format. De tekstede versjonene ser du nedenfor, og på YouTube-kanalen vår – som du også kan abonnere på – kan du se alle filmene!

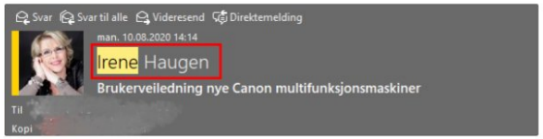
ANGREP MOT IKT HEDMARK

Innlandet IKT sikret seg etter alle kunstens regler – likevel gikk det galt

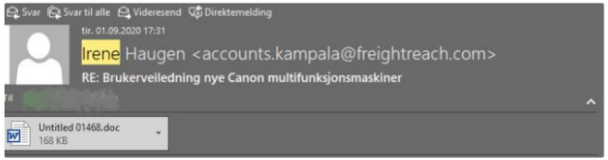
Angrepskoden som ble benyttet var bare noen timer gammel da epostene begynte å tikke inn.

Kommandosentralen til NorCERT, som overvåker angrep mot kritisk infrastruktur i Norge. Illustrasjonsfoto. (Foto: NSM)

MARTIN BRAATHEN RØISE SIKKERHET 2. SEP. 2020 - 12:52

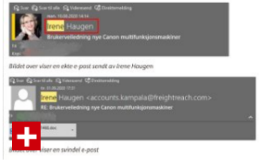


Bildet over viser en ekte e-post sendt av Irene Haugen



...et over viser en svindel e-post

Dataangrep mot kommunene: – Kommer fra utlandet



Fire lokale kommuner utsatt for dataangrep

Dataangrep mot Sykehuset Innlandet: – Har trolig hentet ut data

Takk for oppmerksomheten

Harald Torbjørnsen

harald@kins.no