Digital sikkerhet i Oppdal kommune

Orientering i kontrollutvalget 26.9.2022

Ola Andreas Stavne

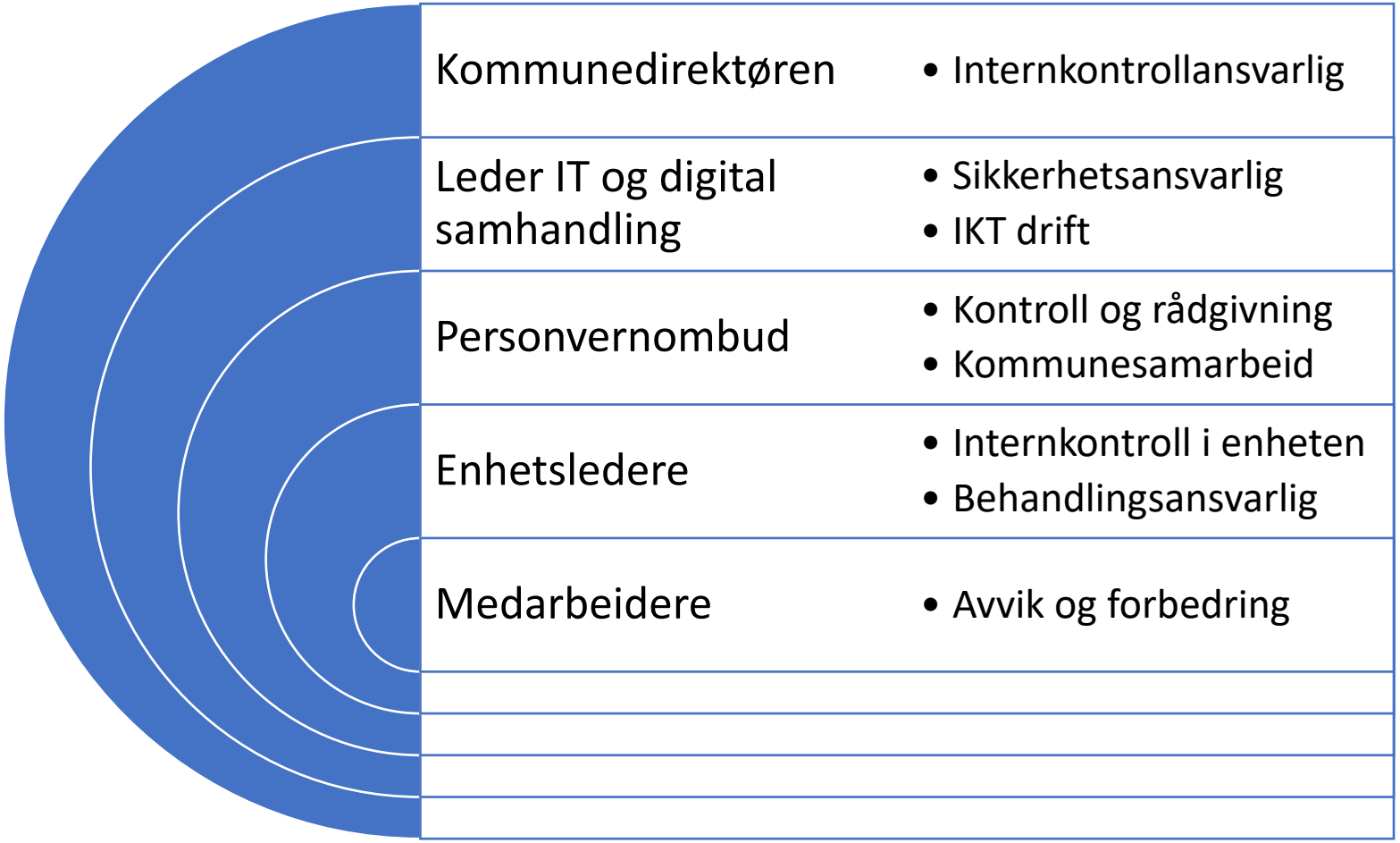
Leder for IT og digital samhandling

Organisering og ansvar

Kompetanse

Risiko- og sårbarhetsvurderinger

Organisering og ansvar // Lover og forskrifter



Kommunedirektøren	• Internkontrollansvarlig
Leder IT og digital samhandling	• Sikkerhetsansvarlig • IKT drift
Personvernombud	• Kontroll og rådgivning • Kommunesamarbeid
Enhetsledere	• Internkontroll i enheten • Behandlingsansvarlig
Medarbeidere	• Avvik og forbedring

- Kommuneloven
- Personopplysningsloven
- Sikkerhetsloven
- Sivilbeskyttelsesloven
- eForvaltningsforskriften
- Forskrift om kommunal beredskapsplikt

Internkontroll

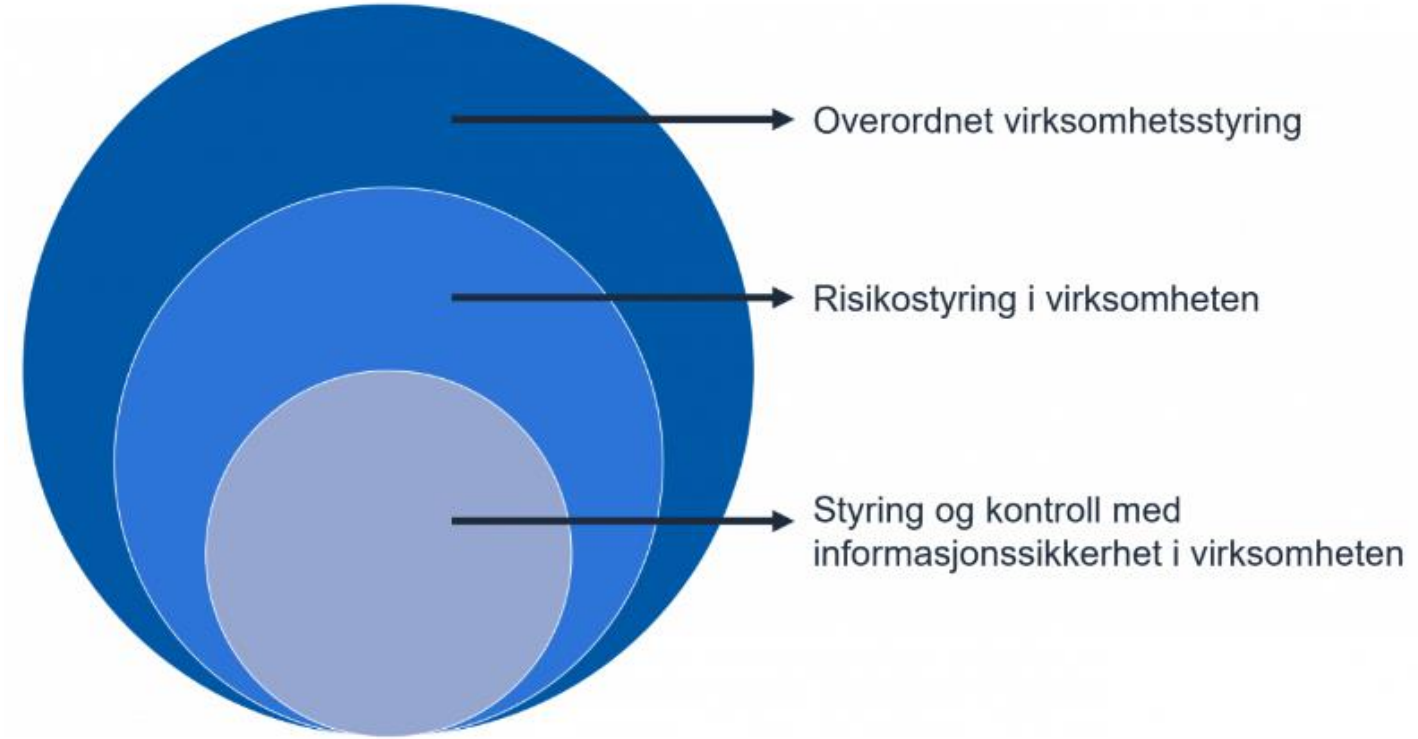
Kommuneloven § 25-1.

- Kommuner og fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges.
- Kommunedirektøren i kommunen og fylkeskommunen er ansvarlig for internkontrollen.

Internkontroll-/kvalitetssystem fra Compilo

- Kvalitetsdokumentasjon/rutiner
- Avvikshåndtering
- Risiko- og sårbarhetsanalyse

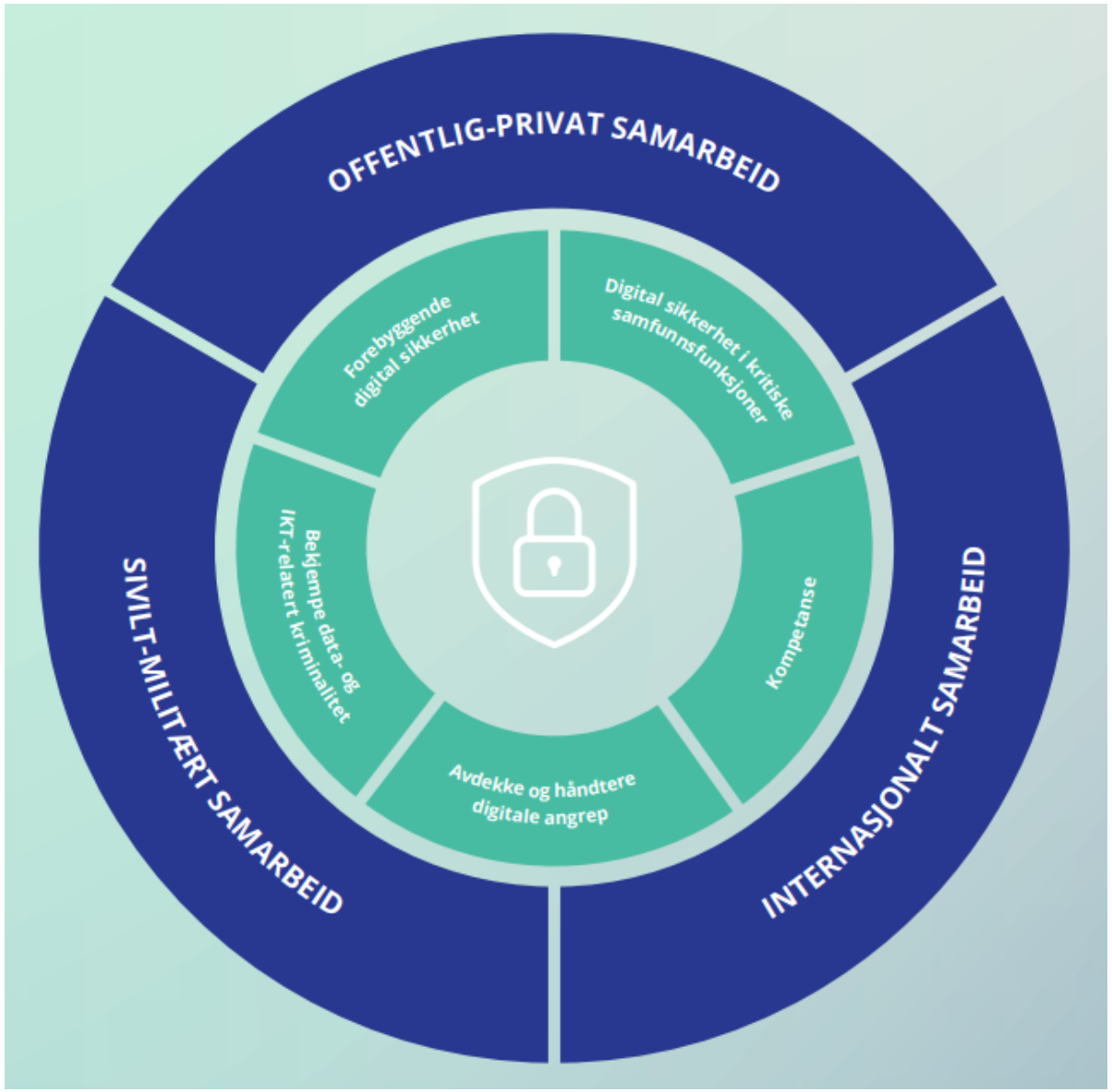
Helhetlig styring av informasjonssikkerhet



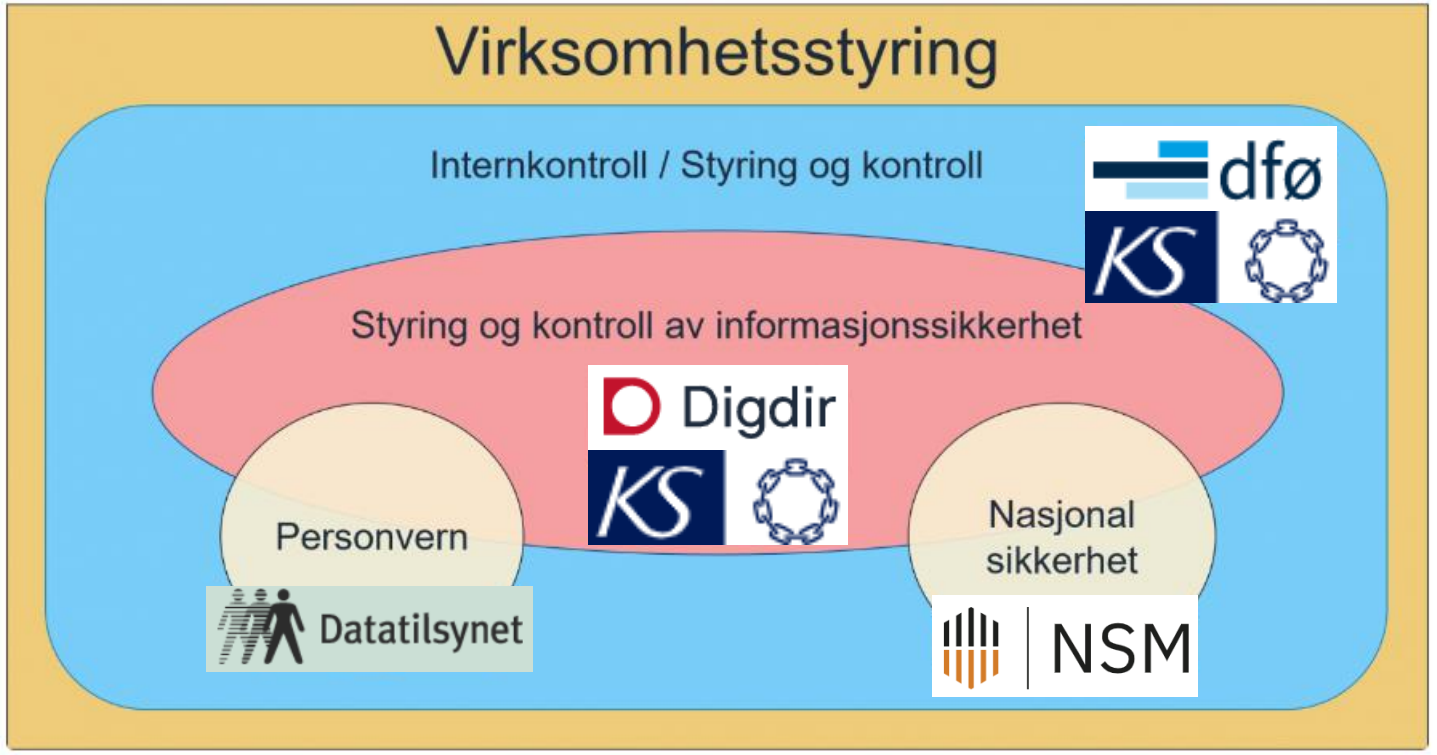
https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

Nasjonal strategi for digital sikkerhet

https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/



Veiledningsaktører innen styring og kontroll



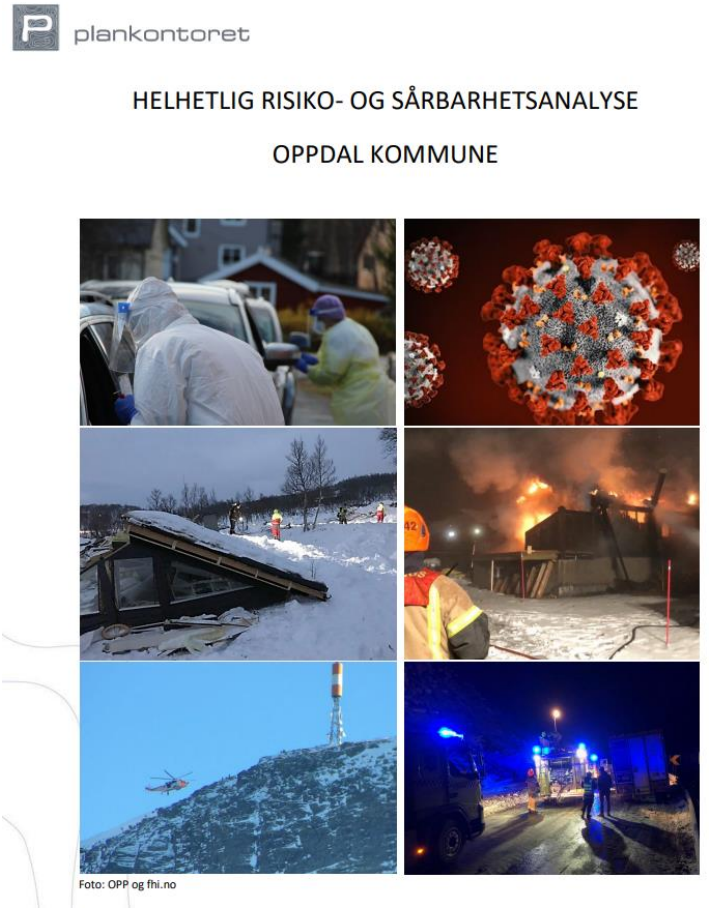
https://www.digdir.no/informasjonssikkerhet/veiledningsaktorer-innen-styring-og-kontroll/2280

Digitaliserings-strategi for Oppdal kommune

1. Styrket digital kompetanse
2. Digital selvbetjening
3. Digital tjenesteproduksjon
4. Åpenhet og medvirkning

Helhetlig risiko- og sårbarhetsanalyse for Oppdal kommune

- Vedtatt i kommunestyret 5.5.2022
- Scenario 12: Inntrengning i datasystemer
- Forslag til tiltak:
  - Duplisering av kritiske funksjoner
  - Økt sikkerhet
  - Oppdatere tekniske løsninger
  - Årlige øvelser
  - Forbedre rutiner og kompetanse



https://innsyn.oppdal.kommune.no/eInnsyn/RegistryEntry/ShowDocument?registryEntryId=248316&documentId=377726&sourceDatabase=EPHORTE

Risiko- og sårbarhetsvurderinger

1. Sikkerhetsovervåkning
2. Sikring av kritiske funksjoner og tjenester
3. Beskytte tjenester som er tilgjengelig på internett
4. Årvåkenhet og teknologi

Sikkerhetsovervåkning

Status:

- Nødvendig og god sikkerhetsovervåkning er etablert
- For det meste lokal drift
- Nye avtaler om fjerndrift (skyløsninger) inneholder nødvendige spesifikasjoner
- Eldre avtaler må gjennomgås

Tiltak til oppfølging:

- Etablere vaktordning eller kjøp av ekstern tjeneste for overvåkning 24/7
- Etablere rutine for regelmessig innhenting av oppdatert informasjon fra leverandører av skyløsninger
- Anskaffe DigiOrden for bedre oversikt og kontroll

Sikring av kritiske funksjoner og tjenester

Status:

- Kartlegging er gjennomført
- Gullstandard for sikkerhetskopiering
- Økt kapasitet på nødstrøm
- Fortsatt relativt stor grad av papir-drift
- Fjerndrift av IKT-systemer er etablert
- Nettverket er segmentert

Tiltak til oppfølging:

- Styrke og oppdatere beredskap- og kontinuitetsplaner
- Samle dokumentasjon om gjenopprettelse i en rutine
- Øke kompetanse ved deltakelse i regionale og nasjonale nettverk
- Vurdere adgangsbegrensning og besøksregistrering på rådhuset

Beskytte tjenester som er tilgjengelig på internett

Status:

- To-faktor bekreftelse er hovedregelen
- Lokasjonsbasert adgangsstyring er etablert
- Ingen servere har internettilgang
- Systemkritiske passord er ikke tilgjengelige fra server

Tiltak til oppfølging:

- Kvalitetssikre rutiner og policyer for mobile enheter

Årvåkenhet og teknologi

Status:

- Kartlegging av trusler baseres på vurderinger/varslinger fra NSM, HelseCERT og data fra sikkerhetsovervåkning
- Medarbeidere varsles om aktuelle trusler via teams og e-post
- Generelle interne trusler
  - Manglende sluttbrukerkompetanse
- Generelle eksterne trusler:
  - Tilsiktede hendelser via mottak av e-post/sms og fysisk oppmøte

Tiltak til oppfølging:

- Kurs, opplæring og holdningsskapende arbeid
- Økt bruk av sms-varsling
- Utarbeide kommunikasjons-plan for forebygging og dulting

Eksempler på varslinger via teams

Morten Sormbroen 4.5 21:12 Redigert 20

Krypteringsvirus - Kritisk informasjon

VIKTIG!
Hei Driftsmeldinger!
For å forholde meg i korthet blir dette litt dårlig forklart men det er særdeles viktig at dere leser og kontakter oss med minste tvil!

Det er de siste dagene blitt en endring i hvordan ransomware/krypteringsvirus spres og flere virksomheter, **også kommuner**, er rammet. Disse er per dags dato ikke offentlig kjent i media.

E-poster med vedlegg som inneholder vanlige filer som for eksempel excel-ark, word-filer og normale lenker inneholder kode for nedlastning av krypteringsvirus som slipper igjennom alle filtre som finnes og kan heller ikke tas i ettertid av de vanlige sikkerhetsmekanismene vi har. Kommer de inn er vi med andre ord nede.

Epostene kommer som regel fra **personer dere har kontakt med til vanlig, så stol heller ikke på at det ok fordi det kommer fra en kjent avsender**.

Ikke klikk på lenker eller åpne vedlegg om du finnes usikker på innholdet, selv om det som sagt kommer fra kjente personer du har eller har hatt kontakt med. Forventer du ikke å motta noe fra ukjente, eller mottar noe du **ikke** forventer fra en person du kjenner må alarm-klokkene ringe.

Er du i tvil, så er du ikke i tvil, kontakt oss uansett årsak, vi setter stor pris på det😊

Se mindre

Morten Sormbroen 6.5 11:03 6
Driftsmeldinger
Til info pågår det nå massive angrep mot både privat og offentlig sektor i Norge, og angreps trykket har eskalert veldig i dag. Vi har veldig god sikkerhet på alle områder etter flere års arbeid innenfor dette feltet, men som jeg skrev over så er denne varianten så godt som umulig å blokkere.

Vi har derfor skrudd igjen sikkerheten på epost filtrering ytterligere da det er det som er primær angreps flate per nå, og vil la den stå slik over helgen. Det vi nå har gjort vil dog medføre at legitime eposter kan bli stoppet i større grad, men vi skal overvåke og følge ekstra godt med på dette igjennom helgen og dagen i dag. Om vi ser noe er stoppet så skal vi sende det igjennom.

Se mindre

Svar

Morten Sormbroen 29.6 11:17 11

Russisk dataangrep mot Norge

!! Viktig !!
Driftsmeldinger
Hei!

Russland har i skrivende stund ett pågående massivt angrep mot offentlige instanser i Norge (Politiet, NAV, ID-Porten, Buypass, UDI, DigDir med flere, listen er lang).

Oppfordrer alle til å utvise forsiktighet med å klikke på lenker/vedlegg, i alle former (Chat, epost, nettsider o.l.)
Dette gjelder også nå spesielt om det kommer fra offentlige instanser/etater som normalt sett skal være trygge, vær spesielt kritisk til disse.

Ved minste tvil så ta kontakt med IT-Kontoret 😀

Se mindre

Norsk senter for informasjonssikring

Fakta og veiledninger

Nasjonal sikkerhetsmåned 2022

I oktober markerer vi i NorSIS Nasjonal sikkerhetsmåned for 12. gang. Tema for årets kampanje er løsepengeangrep og ulike former for sosial manipulering.

ENISA European cybersecurity month

Oktober er det også sikkerhetsmåned i hele Europa, og det koordineres av **The European Union Agency for Cybersecurity (ENISA)**. I år har **The European Cybersecurity Month (ECSM)** 10-årsjubileum. For tiende gangen arrangerer ENISA sikkerhetsmåneden i oktober, og NorSIS koordinerer disse aktivitetene i Norge.

10th anniversary EUROPEAN CYBER SECURITY MONTH