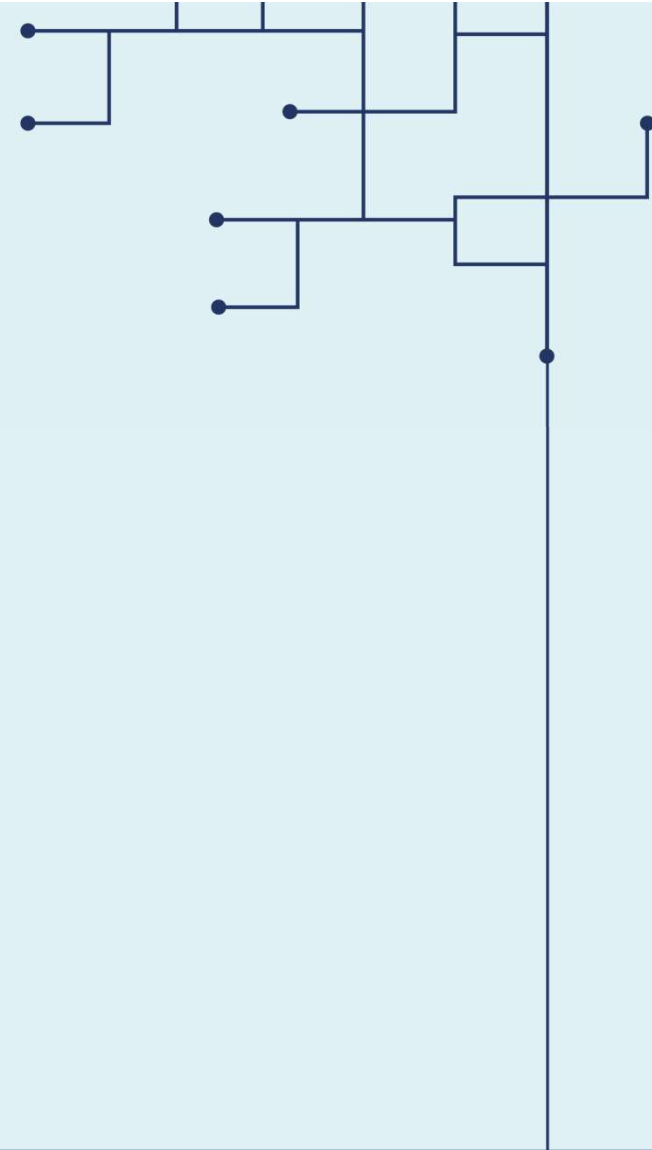


Kommune-CSIRT

Nasjonalt senter for informasjonssikkerhet i kommunesektoren



Kommune-CSIRT



Trusselbilde

Kommune-CSIRT IKS

Kommune-CSIRT IKS - et felles løft for informasjonssikkerhet
i kommunesektoren

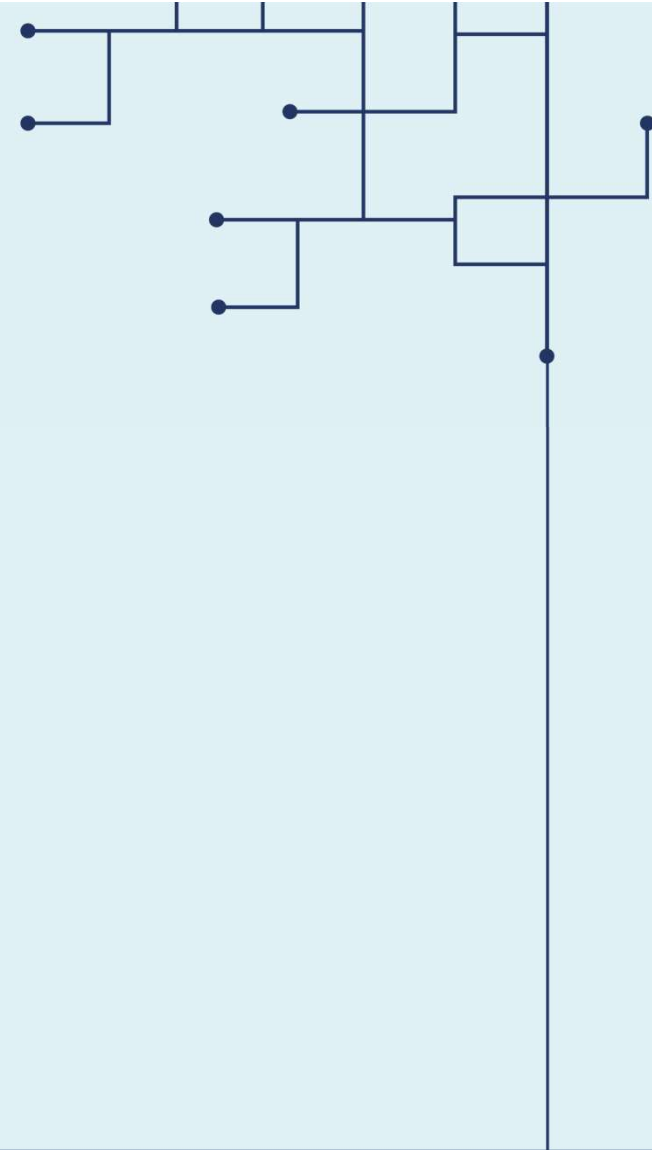


Kommune-CSIRT IKS

- Nasjonalt senter for informasjonssikkerhet for kommunesektoren
- Hovedsakelig en-til-en støtte og beskyttelse av medlemskommuner gjennom:
 - Informasjonsdeling og trusseletterretning
 - Rådgivning og kompetansesenter
 - Koordinering og støtte ved hendelser
- Deltar i det sektorvise resposmiljøet ledet av NSM og støtter opp om NCSC

Et felles løft mot en tryggere digital hverdag i kommunesektoren!

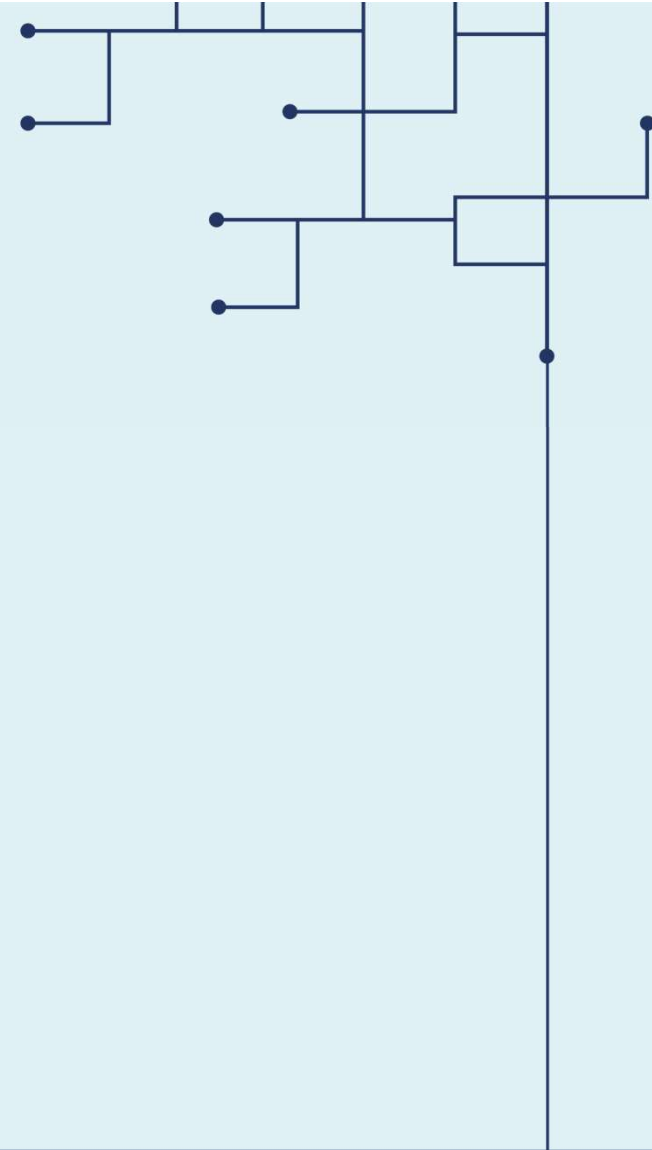
Vår ambisjon er å bli en vesentlig aktør i arbeidet med å nå dette målet.





Hendelser

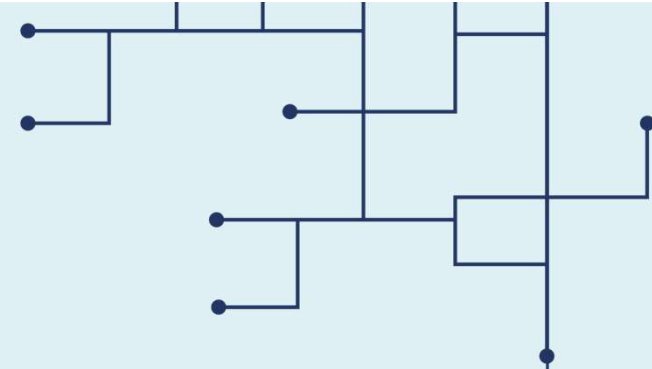
- Pulse secure VPN
 - 900 virksomheter berørt
 - Løst brukernavn og passord, ssh keys,
 - NHH fikk mest oppmerksomhet
 - Patch tilgjengelig fra April 2019
- Emotet
 - Botnet og skadevare
 - Daglig tilpassing og nye versjoner
 - Stjeler Informasjon om epost og hvem du snakker med
 - Gjenbraker sendte eposter med skadelig vedlegg
 - Tilgang selges videre til andre aktører
 - Dropper andre typer skadevare hvis målet er interessant: Trickbot/Zloader/Cobalstrike
 - Flere norske C&C servere





Hendelser

- Tjenestenekt (DDOS) utpressing
 - Telenor er eneste som har gått offentlig ut
 - Mye ISP og finans
 - Flere norske bedrifter truffet
 - Utgir seg for å være APT aktørene Fancy Bear eller Lazarus
 - Kan ta tid å oppdage pga kort tidsperiode
- Ransomware
 - Stadig utvikling og et helt økosystem er etablert rundt dette
 - Krypterer
 - Laster opp
 - Auksjonerer bort
 - DOS og lekkasje hvis en ikke betaler
 - Går etter bedrifter da disse har lettere for å betale
 - De fleste kommuner har gode rutiner på restore fra backup.
 - Må være forberedt på å håndtere stjålne data.
- Kompromitterte kontoer
 - Mange berørte kommuner.
 - Covid-19 eller Office365 som tematikk.
 - Benyttes som oftest til phishing og spamutsendelse.
 - Bruker kjente stjålne passord og brukernavn (password spray).



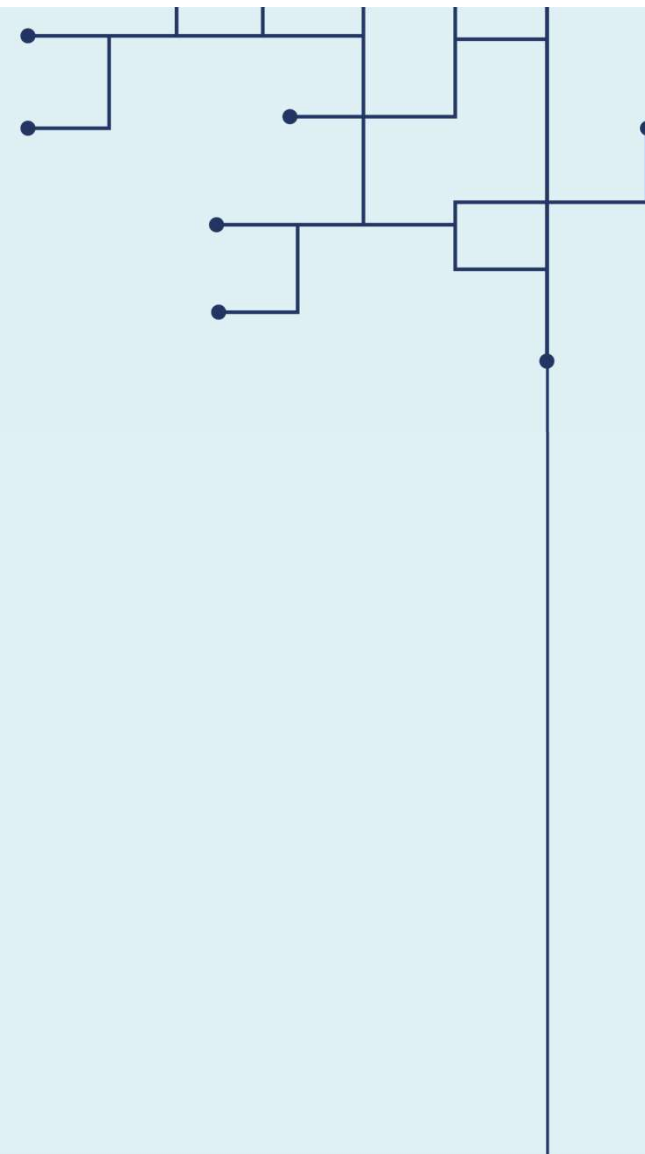


Kommune-CSIRT

Tar kommuneledelsene ansvar for digital sikkerhet?



Hvor opplever dere størst utfordringer med sikkerhet?



Trusler og trender



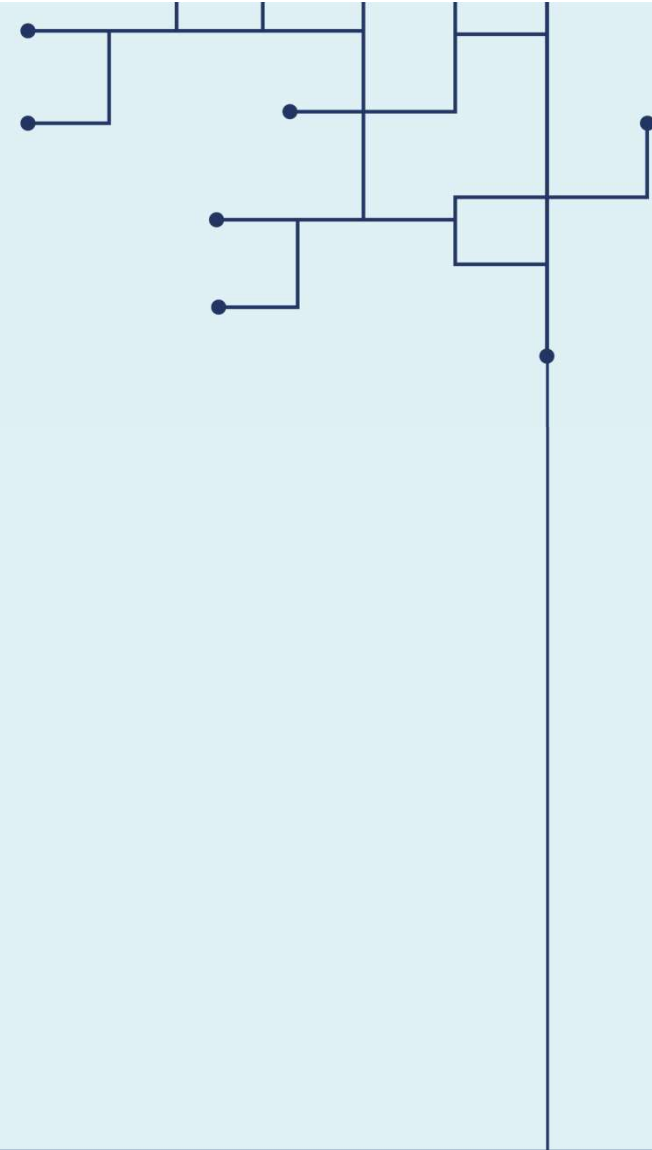
Covid-19

- Alle/Alt på hjemmekontor
 - Privat utstyr
 - Håndtering av informasjon
 - Endepunktet ble den nye perimeteren
 - Du snakker, hvem lytter?
- Skolene gjennomførte digitaliseringsprosjekter over natta
- Bruk av Office365 og ny teknologi med lite opplæring = utilsiktet deling



Fakturasvindel

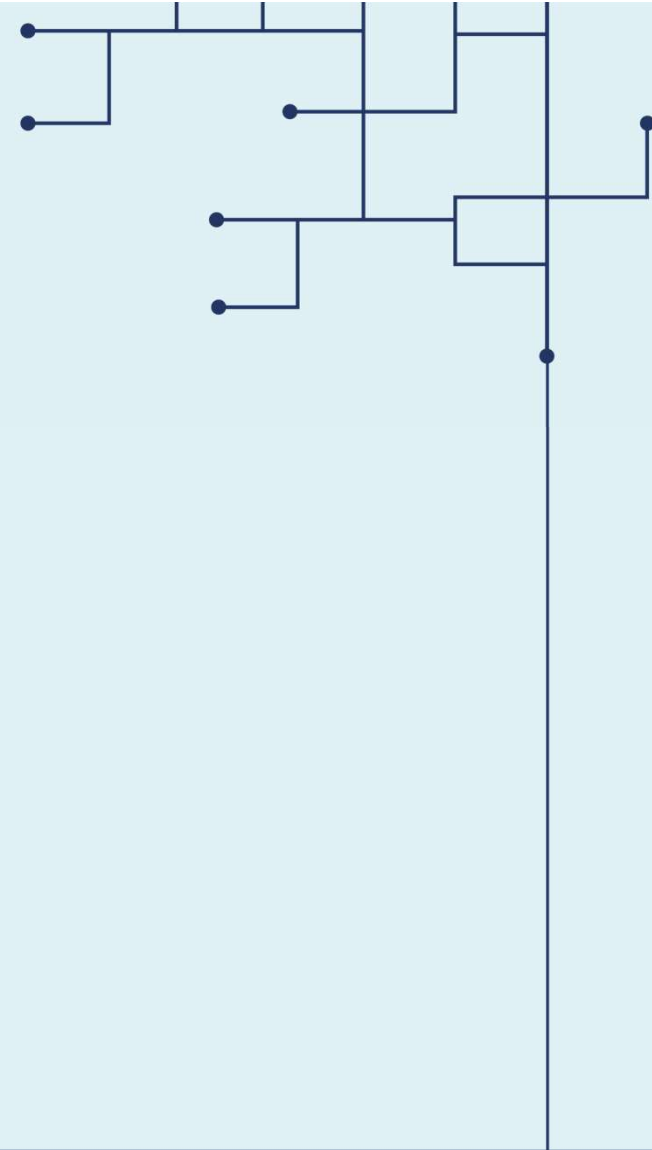
- Mer målrettet en noen gang
- Bruker anbudsportaler for å finne offer
- Benytter legitime signaturer
- Følger opp med telefonsamtaler
- Mulighet for god fortjeneste med liten innsats
- Perfekt timing med Covid-19 – mange rare innkjøp
- Antatt store mørketall
- PWC sin rapport om NorFund anbefales – 100mill svindlet.





Feilkonfigurasjon

- Vann og avløp
- SD-Anlegg
- Ønske om effektivisering
 - Enkel tilgang for support
 - Ønske om fleksibilitet i drift
- Leverandør – ønske om god support
- Leveransen går på siden av det etablerte drift/sikkerhetsregimet
- Involverer ikke IT-Avdeling
- Manglende oppdateringsregime





Offentlige anbud:

Virksomhetskritisk informasjon blir lagt ut på anbudsportaler.

- Teknisk informasjon og tegninger blir liggende offentlig tilgjengelig ifb. anbudsprosesser.
- Ikke tekniske ressurser gjennomfører anbudskonkurransen.
- Ikke alltid åpenbart hva dokumentasjon skal brukes til.
- Angriper slipper å drive kartlegging av virksomheten – får komplett dokumentasjon.
- Bør risikovurderes eventuelt innarbeide rutiner for utlevering av denne typen informasjon.



Utfordringer

Uavhengig av samarbeidskonstellasjon stilles det store krav til grunnleggende praktiske sikkerhetsmekanismer.

Utfordringene står i kø gjennom at:

- Informasjonssikkerhet må forankres hos ledelsen
- Antall digitaliseringsprosjekter øker – velferdsteknologi, IOT osv
- Kompleksiteten i kommunenes samhandlingsløsninger øker
- Trusselbildet forverres (mer avansert, større volum, flere aktører)
- Antall sårbarheter øker (nye produkter, nye funksjoner, nye sammenkoblinger)
- Underliggende virksomheter og etater har liten støtte på cybersikkerhet



Oppsummert:

- Digitalisering i alle deler av virksomheten – **kan** bidra til økt informasjonssikkerhet hvis muligheten utnyttes.
- Fortsatt høy aktivitet på løsepengevirus, som benytter hele spekteret av verktøy (infeksjon, kryptering, stjeling, offentliggjøring, salg, DOS)
- Anbud skaper utfordringer ifb informasjonsdeling
- Koronaens påvirkning/endring av jobbsituasjon - krav til fleksibilitet fra alle parter.



Kommune-CSIRT



Takk for meg

Kommune-CSIRT støtter kommunen i digitalt sikkerhetsarbeid på strategisk, operasjonelt og teknisk nivå.

Kontakt:

post@kommunecsirt.no

www.kommunecsirt.no

T. 90 85 00 42