# Kommune-CSIRT

Nasjonalt senter for informasjons-
sikkerhet 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 responsmiljøet ledet av NSM

*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.

Kommune-CSIRT

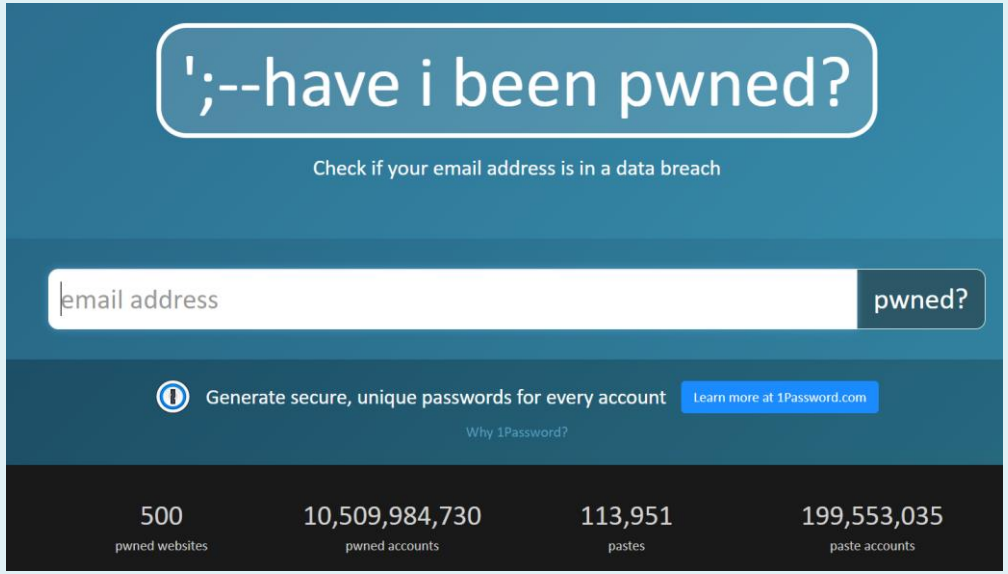
# Trusler og trender

# Tjenestenekt (DDOS)

- Telenor er eneste som har gått offentlig ut om angrep mot deres infrastruktur
- Mye mot internettleverandører og finans
- Siste 3 mnd. også mye mot norske kommuner
- Store konsekvenser
- Billig og svært effektivt
- Noen utgir seg for å være store kriminelle organisasjoner pga økt frykt
- Kan ta tid å oppdage pga kort tidsperiode
- Det nye er at det benyttes som utpressing, med kort angrep som forsmak

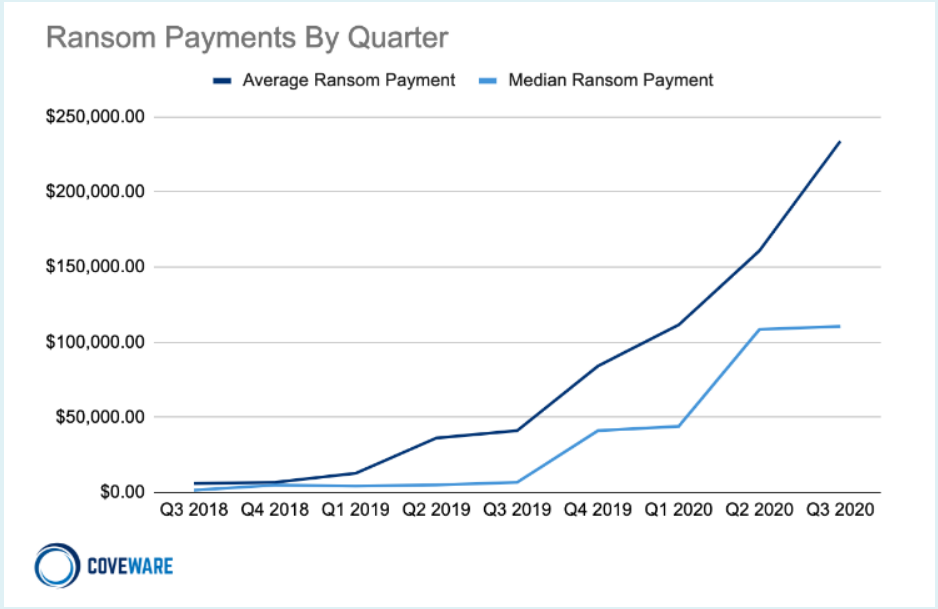
# Kompromitterte kontoer

- En konto der brukernavn og/eller passord er kjent.
- Mange bruker kommunal epost til private gjøremål
- Gjenbruk av passord
- Covid-19 eller Office365 som tematikk.
- Benyttes som oftest til phishing og spamutsendelse
- Bruker kjente stjålne passord og brukernavn for videre utnyttelse
- Manglende bruk av multifaktor
- Varslet på rundt 3500 kompromitterte kommunale kontoer
- Håndterer ukentlig henvendelser rundt dette



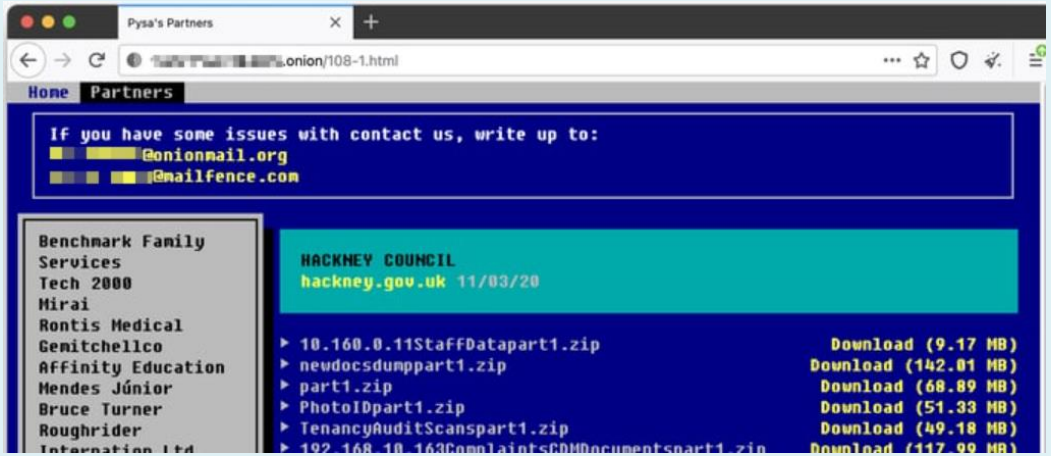
# Løsepengevirus

- Stadig utvikling og et helt økosystem er etablert rundt dette
- Krypterer
- Laster opp
- Auksjonerer bort
- Tjenestenekt og lekkasje av  hvis en ikke betaler
- Går etter bedrifter da disse har lettere for å betale
- De fleste kommuner har gode rutiner på gjennoppretting fra backup.
- Må være forberedt på å håndtere datalekkasje.
- Var inntil for 2 år siden håndterbart av IT avdelingen
- En aktør omsatt alene for 1.2 milliarder NOK.



# PYSA/Meziponosa

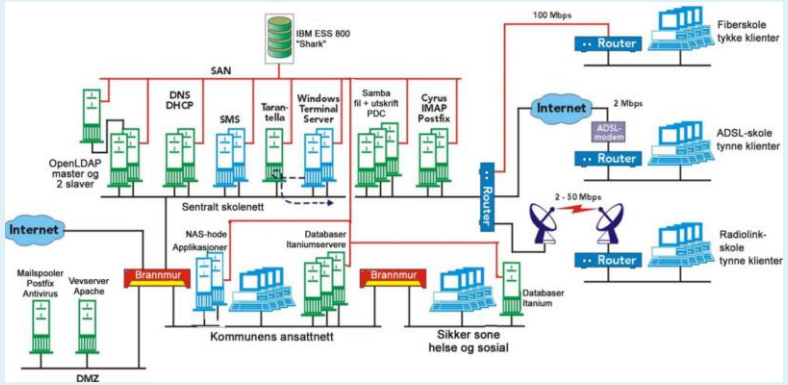
- Løsepengevirus aktør, selges som en tjeneste
- Avansert målrettet operatørstyrt aktør
- Benytter en rekke verktøy, sårbarheter og teknikker for tilgang.
- Kartlegger infrastruktur, skaffer seg god oversikt
- Tar seg god tid får å etablere fotfeste i infrastruktur. Rundt 30 dager fra tilgang til komplett kompromittering
- Benytter den teknologien som målet tilbyr for aksess – citrix, rdp, vpn
- Krypterer, sletter og laster opp.
- Fjerner backup!
- Revidere planverk for totalt bortfall av all infrastruktur – Hvordan starte fra bunn? Teknisk sett større og mer alvorlige konsekvenser en brann.
- Må være forbedret på lekkasje av data og hvordan håndtere media /publikum når lekkasje blir kjent



# 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.



Kommune-CSIRT

# Håndtering av løsepengesvirus

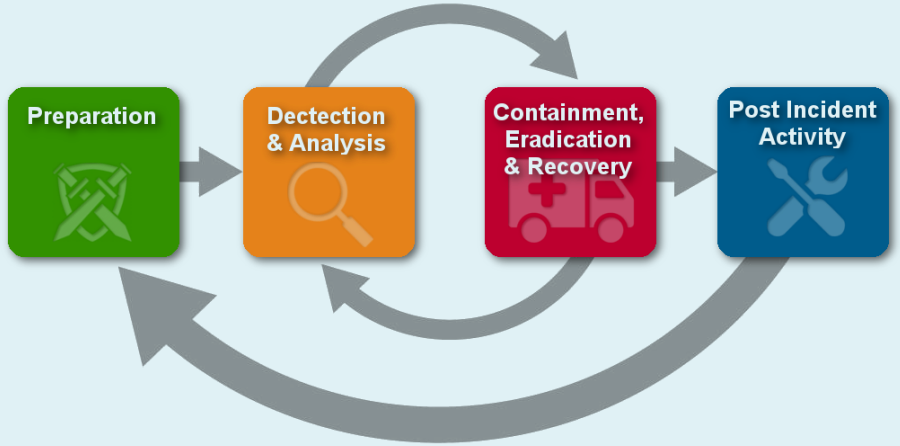
# Påstand:

Informasjonsikkerhetshendesler er abstrakt for de fleste.

Konsekvensene er enorme!

# Hvordan forberede seg:

- Hva er trusselen?
- Gjennomfør risiko og sårbarhetsredserende tiltak
- Lag en plan!
- Parallelle aktiviteter
- For IT avdelingen er dette «normalt»
- Gjenoppretting av sikreretilstand
- Dilemma rundt etterforsking kontra gjenoppretting



# Ha en plan: Planlegg flere løp

- Lag egne planer på IKT hendelser – ikke legg dette inn under «det andre» - avstem mot leverandør/IT avdeling
- Hva er premissene for at planen skal iverksettes. Når blir kommunen for liten.
- Lag en plan – En plan er bedre en ingen plan- sørg for å beholde handlingsrommet både taktisk og mentalt.
- Hvem ringer vi? Hvem kan hjelpe oss? Når skal myndighetene varsles?
- Overlapp av tjenester mot andre kommuner?
- Lag aktørkart og lag kontakt liste
- Hva gjør vi når krisen går over 24 timer - rullering av mannskap - IT avd trenger også søvn.
- Ha en plan når ting er nær utsletting, hvem ringer du, lag disse avtalene på forhånd.
- Lag en plan på hvordan informasjon på avveie skal håndteres, kan anvendes i andre sammenhenger også
- Finnes plan på papir/offline utgave, har vi penn og papir?

# Øve

- Øve hele organiasjonen – avdekker roller
- Faktisk gjennomfør de forskjellige momentene
- Skrivebords øvelse avdekker hull i planverket
- Fysiske øvelser avdekker det planverket ikke tok høyde for
- Øv samme med alle involverte aktører – nyttig for alle parter
- Mye fokus på media
- Utfordring på å skille leverandørene – hvem skal tjene penger på deg og din krise.

# Revisjoner

Organisatorisk

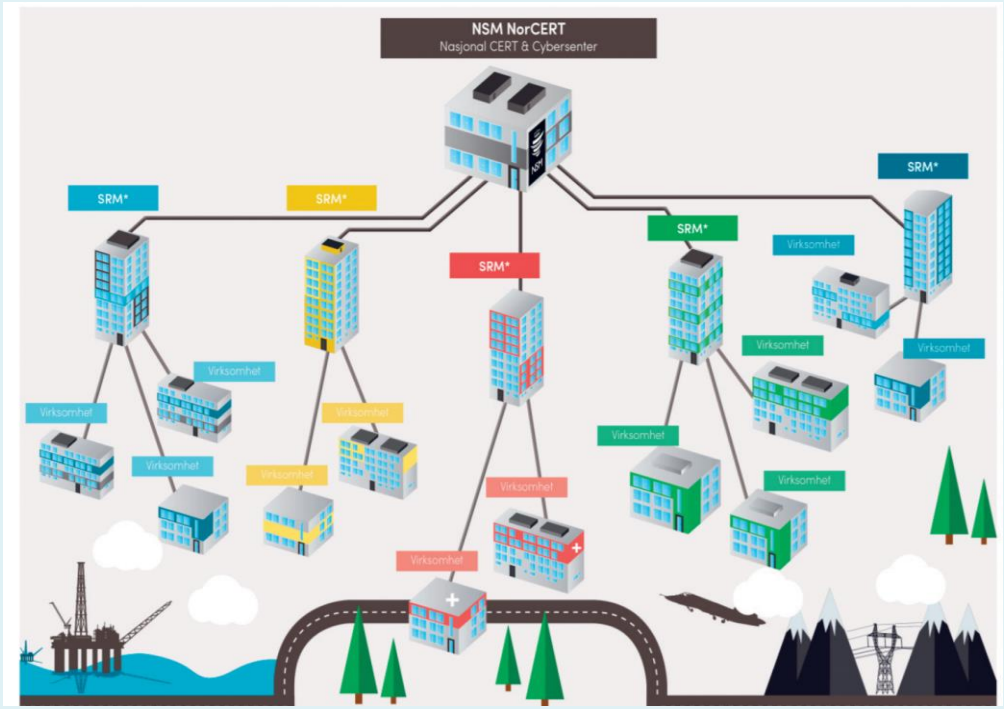
- Stadig endring i situasjonsbilde
- Krevende å gjøre trusseletterettning
- Endring i leverandører
- Tjenester spres på flere leverandører
- ROS Analyse sammen med IT-avdelingen
- Hva er kronjuvelene?

Teknisk

- Penetrasjonstester/ RED Team
- Latente feil
- NSM grunnprinsipper
- Herding av eksisterende miljø
- Revisjon av brannmur regler
- Ikke «tøm» teknologi på problemet
- Ikke vær et egg – forsvar i dybden

# Operative aktører:

- Cyberforsvaret CSS – Beskytter forsvarets egen infrastruktur
- NCSC – Nasjonalt cyber sikkerhetssenter.
- NC3 – Nasjonalt cyberkrim senter
- FCKS - Koordineringssenter mellom E-tjenesten, Kripos, PST og Politi. Ledet av NSM
- KraftCERT – Støtter Kraftbransje
- HelseCERT – Støtter primærhelsetjenesten
- Kommune-CSIRT – Støtter medlems kommuner og Fylkeskommuner



# 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**