



Trusselbilde og beredskap på 1-2-3

Alaa Ghanim, Christian Hagby,
Claudia Haubold
CSIRT, Oslo kommune



Hva kommer vi til å snakke om?

- ▶ Trusselbilde

- ▶ Oslo kommune

- ▶ Den enkelte ansatte

CSIRT Teamet



Claudia Haubold



Christian Hagby



Alaa Ghanim

Hva er CSIRT?

- ▶ Computer Security Incident Response Team

- ▶ Yte støtte til alle kommunens IKT-driftsmiljøer

Hva gjør CSIRT?





Trusselbilde



Digitalt samfunn

- ▶ En utviklende digitalisering av hele samfunnet
- ▶ Jobben og livet vårt er digitalt
- ▶ Store mengder enheter og systemer tilkoblet internett
- ▶ Mye gammelt...
- ▶ Mye nytt...



Oslo



Nasjonal sikkerhetsmyndighet oppfordrer norske virksomheter til «økt årvåkenhet»

Oppfordrer til å ha lav terskel for å kontakte dem eller Nasjonalt
cybersikkerhetssenter

Kilde: Digi.no 28.09.2022



NSM advarer mot økning i cyberangrep

De mest utsatte er teknologibedrifter, forskning og utvikling, og
offentlige forvaltningsorganer, ifølge NSM.

Kilde: Kode24.no 3.10.2022



Kommunalt risikobilde 2021

Oslo kommune

Kortversjon

Kommunen ser «svært alvorlig» på trusselbildet –
opplever en økning i antall hackerangrep

Kilde: ao.no 15.01.2022

Et hackerangrep ses på som så alvorlig at det
vurderes å ha større samfunnsmessige konsekvenser
enn en pandemi. Konsekvensene av en pandemi er vi
alle blitt godt kjent med de to siste årene

Kilde: Beredskapsetaten 2021



Potensielle konsekvenser

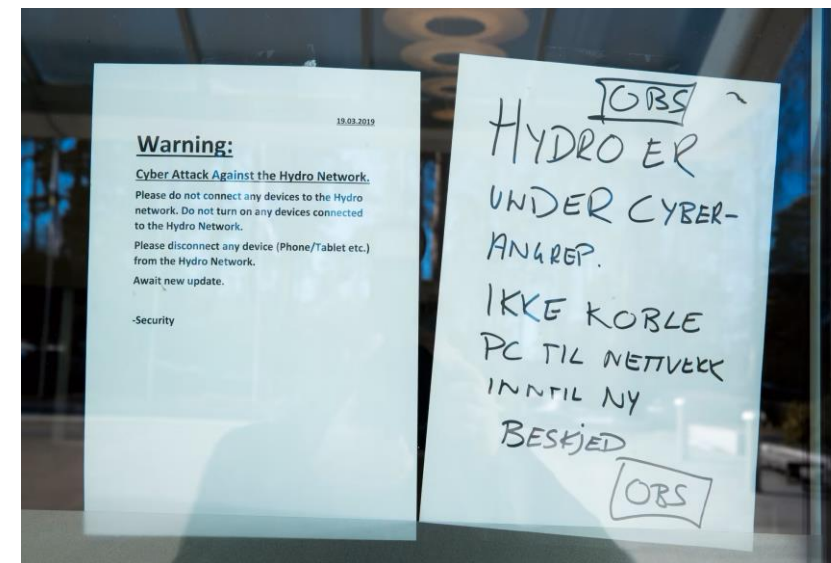
- ▶ Tap av verdier, omdømme og fortjenester
- ▶ En tid uten internett
 - Daglige nødvendigheter er utilgjengelige
- ▶ Liv på spill
 - Sykehus?
- ▶ «Blackout»
 - Hacking av strømmettverket



Nordland fylkeskommune
ble utsatt for dataangrep
23. desember 2021



Nordic Choice Hotels
angrepet av
løsepengevirus 2.
desember 2021



Element Nor angrepet av
løsepengevirus i september
2022



Amedia angrepet med
løsepengevirus i slutten av
2021.



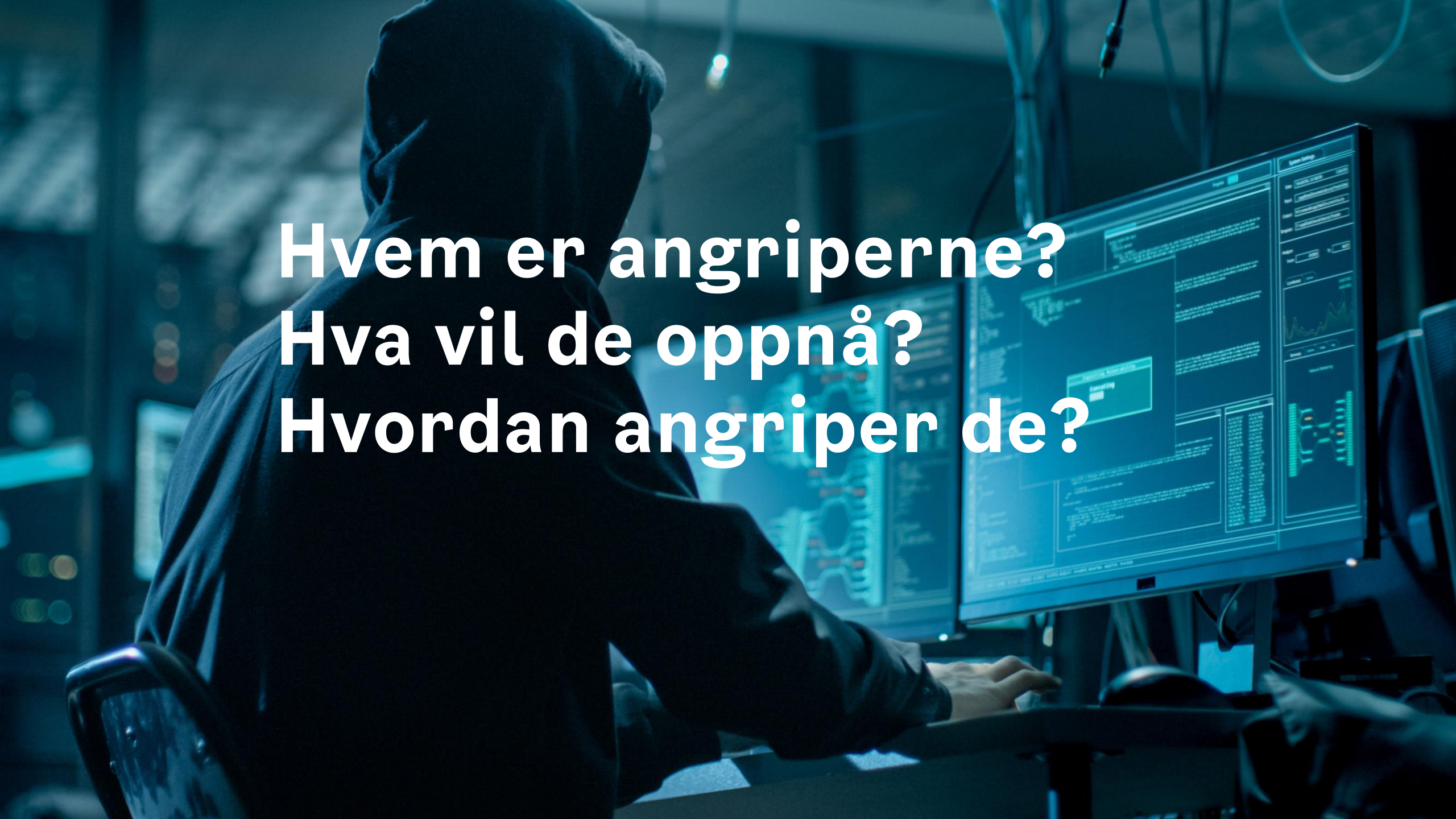
Coop i Sverige truffet av
løsepengevirus i juli 2021, angripere
krever 600 millioner



Cybertrusler og risiko mot Oslo kommune

- Løsepengevirus
- Utdatert programvare
- Manglende overvåking

- Sosial manipulering
- Phishing
- Svake passord



**Hvem er angriperne?
Hva vil de oppnå?
Hvordan angriper de?**

Hvem er hackerne?



White hat

- ▶ Tillatelse til å hacke
 - Etske hacker
 - Sikkerhetstester
- ▶ Ofte betalt for å oppdage sårbarheter eller feil
- ▶ Forbedrer sikkerheten



Grey hat

- ▶ Hacker uten tillatelse
- ▶ Uetisk, men ikke alltid ond hensikt
- ▶ Ønsker anerkjennelse og skryt
- ▶ Truer med publisering av sårbarheter

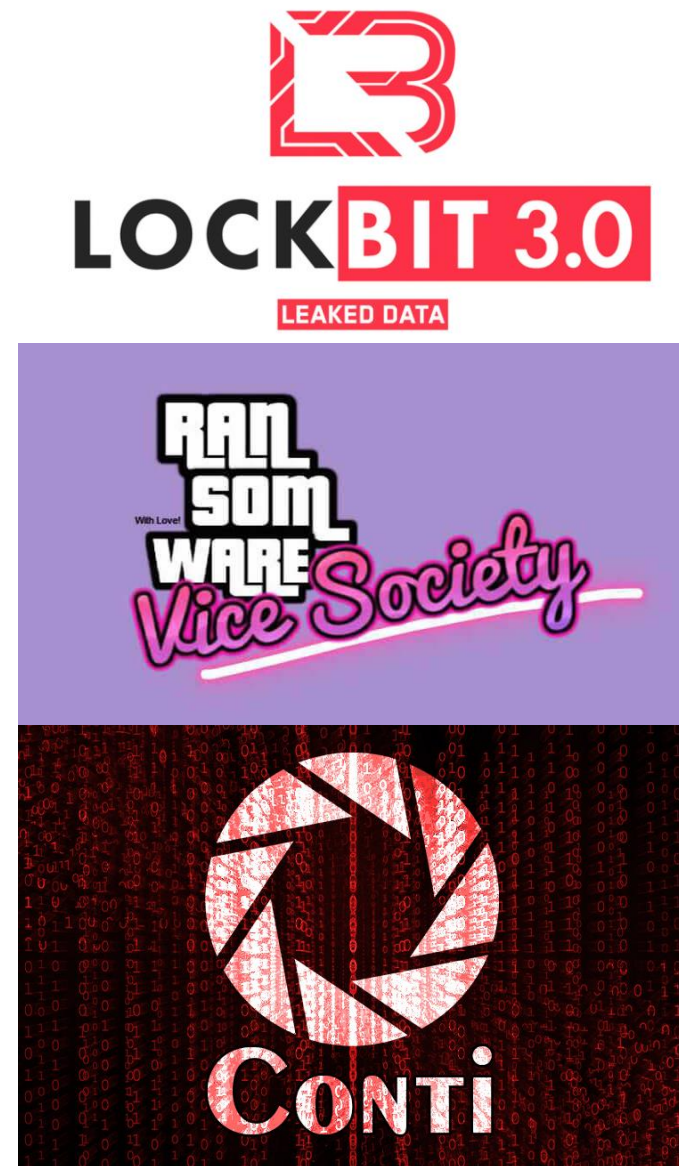


Black hat

- ▶ Hacker uten tillatelse
- ▶ Ond/kriminell hensikt
- ▶ Finansielt motivert
- ▶ Bruk av skadevare

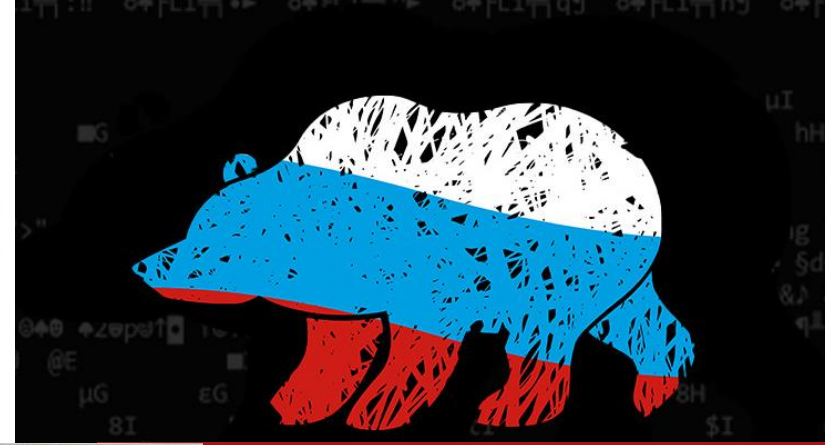
Løsepengevirus grupper

- ▶ Finansielt motivert
- ▶ Angriper store og små organisasjoner
- ▶ Store kriminelle organisasjoner
Fungere som et firma?
- ▶ Salg av løsepengevirus som tjeneste
Lite teknisk kunnskap kreves



Avansert og vedvarende trusselaktør (APT)

- ▶ Statlige aktører
- ▶ Veldig høy teknisk kompetanse
- ▶ Store finansielle midler
- ▶ Spionasje
- ▶ Finansielle gevinster
- ▶ Sabotasje
- ▶ Krigføring



"NotPetya" angrepet i 2017

- ▶ Lite familieselskap
- ▶ Føring av skatt
- ▶ Infiltrerte firmaet



- ▶ Løsepengevirus
- ▶ Massiv spredning
- ▶ Ikke ment å bli de-kryptert

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$388 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaRtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail monsmith123456@posteo.net. Your personal installation key:

zRNagE-CDBMfc-pD5A14-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.

Key: _

- ▶ Én maskin hadde installert programmet
- ▶ Ikke egentlig et mål
- ▶ 2,5 – 3 milliarder i tap



«Log4shell»

- ▶ Sårbarhet i populært verktøy
Apache Log4J
- ▶ Enkel å utnytte
- ▶ Fra gutterommet til statlige aktører...
- ▶ Ekstremt utbredt
- ▶ Dugnad i hele kommunen

Hadde ikke oversikt 41 dager ut i tidenes verste sårbarhet: - Det er svært omfattende arbeid

Kilde: Digi.no 13.02.2022

Mer enn 800.000 forsøk på å utnytte sikkerhetshull på nett: - Feilen bekymrer oss mer enn vanlig

Kilde: NRK.no 14.12.2021

Dataeksperter verden rundt kjemper for å tette gigantisk sikkerhetshull

Kilde: VG.no 14.11.2021

CSIRTs oppfølging av log4shell



STARTET ARBEID MED
TILTAK ØYEBLIKKELIG



KREVENDE OG
OMFATTENDE ARBEID



KRITISKE
SÅRBARHETER LUKKET

Situasjonen i Ukraina

Angrep mot Ukraina

- ▶ «Wiper» skadevare
- ▶ Ligner på løsepengevirus
- ▶ Destruktivt
- ▶ Russiske APT-grupper
 - Tilknyttet den russiske regjeringen



Oslo



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

Hva er risikoen for Norge?

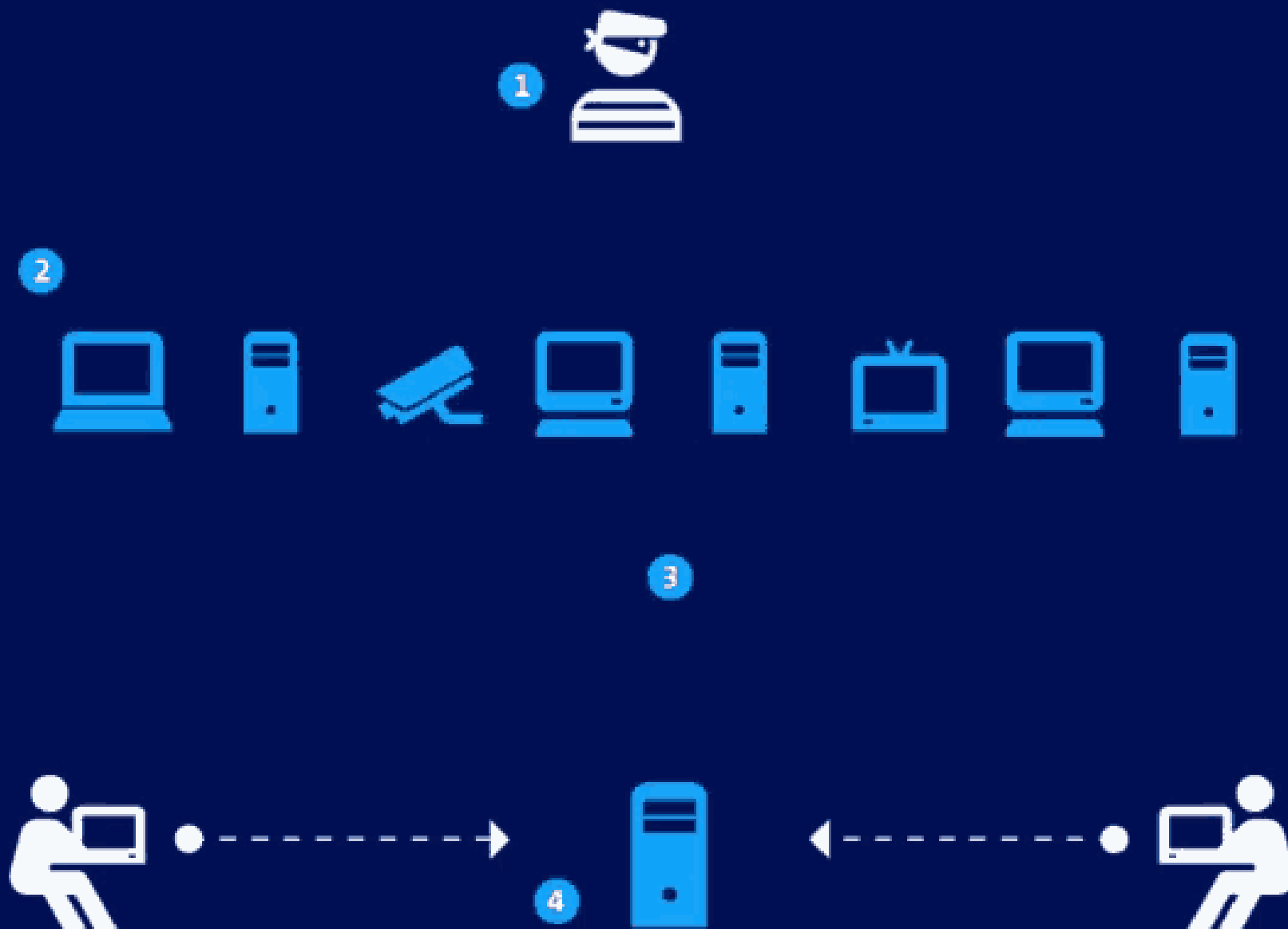
- ▶ Direkte angrep mot Norge
 - Olje og gass
 - Sikkerhetspolitisk verdi for Russland
- ▶ Hvem?
 - Statlige aktører
 - Pro-russiske aktivister
- ▶ Verdikjedeangrep
 - Tilkobling til Ukraina eller Russland
 - Ansatte
 - Programvare



Oslo

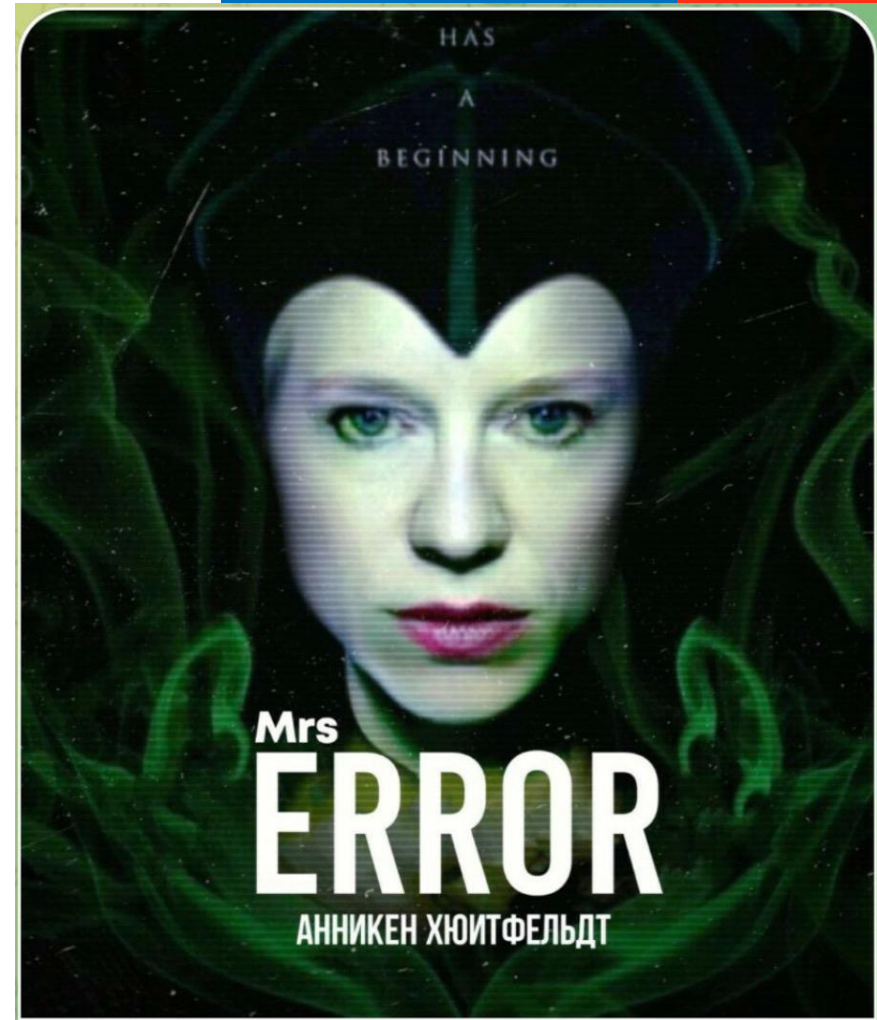


Hva er et tjenestenekt angrep?



Tjenestenektangrep mot Norge 29. Juni

- ♦ «Killnet»
- ♦ Pro-russisk aktør
- ♦ Ingen kjent tilknytning til den russiske regjeringen
- ♦ Respons på fraktnekt av varer på Svalbard
- ♦ Samfunnskritiske nettsider
- ♦ Skape frykt/kaos
- ♦ Lite skade gjort, men mye oppmerksomhet



Tjenestenekt angrepet mot Oslo kommunes nettside

<START
Guys 🇷🇺 DDoS - artelirists from <https://t.me/DDoSAlpha> joined our trip around NorwayGEI

Fire 🚀🚀🚀
Investments
⚡ <https://polpred.com/www.invinor.no>
Real estate
⚡ <https://www.globalpropertyguide.com/Europe/Norway>
Oslo website
⚡ <https://www.oslo.kommune.no/>
SLUTT>

- Oslo kommunes nettside utsatt for tjenestenekt angrep i juli 2022
- Ble først postet på telegram konto tilknyttet Russland

From Russia with Love 🇷🇺
Ребята 🇷🇺 к нашему путешествию по Норвегии присоединились DDoS - артелиристы из <https://t.me/DDoSAlpha>

Огонь 🚀🚀🚀
Доп Таргеты 🎯
Инвестиции
⚡ <https://polpred.com/www.invinor.no>
Недвижимость
⚡ <https://www.globalpropertyguide.com/Europe/Norway>
Сайт Осло
⚡ <https://www.oslo.kommune.no/>
🔥 74 ❤️ 8 👍 4 🍌 3 1626 edited 8:51 PM
4 comments
You joined this channel

US France, Paris	Connection read by peer
Germany, Frankfurt	Connection read by peer
Yangtze, Hong Kong	Connection read by peer
Japan, Tokyo	Connection read by peer
China, Peking	Connection read by peer
Kazakhstan, Almaty	Connection read by peer
Ukraine, Kyiv	Connection read by peer
Malaysia, Kuala Lumpur	Connection read by peer
Netherlands, Amsterdam	Connection read by peer
Spain, Madrid	Connection read by peer

KILLNET

Ikke så ille som man skal ha det til?

- Angrepet mot nettsiden varte i kun 20 minutter
- Ingen nevneverdige samfunnsmessige konsekvenser
- Oslo kommune har DDoS beskyttelse



🕒 Døgnåpne tjenester

Legevakt, barnevern, innføring, over-
repsmottak, vann- og avløp.

🦠 Koronavirus

Råd og anbefalinger, koronatest, vaksine,
psykisk helsehjelp

🏠 Barnehage

Søke eller bytte, finn barnehage,
oppsigelse.

🎒 Skole og utdanning

Ferie, skolekrets, AKS, utdanningstilbud,
skoler i Oslo.

💚 Helse og omsorg

Helsehjelp, nedsatt funksjonsevne,
barnevern, psykisk helse, gravferd.

🏗️ Plan, bygg og eiendom

Byggesøknad, saksinnsyn, planinnsyn,
kart, eiendomsinformasjon.

🚗 Gate, transport og parkering

Priser, sykkel, piggdekk, veiarbeid, TT,
HC-kort, drosje, luftkvalitet.

♻️ Avfall og gjenvinning

Gjenbruksstasjoner, kildesortering,
renovasjonstjenester.

🪑 Natur, kultur og fritid

Bading, bibliotek, kunst, fritidsklubber,
idrettshaller, marka, leie lokaler.

🏠 Bolig og sosiale tjenester

NAV-kontor, bostøtte, økonomisk rådgiv-
ning, fri rettshjelp, tolk.

💰 Skatt og næring

Eiendomsskatt, kommunale avgifter, salg,
servering, bevilging, leveranden.

🚰 Vann og avløp

Stengt vann, drikkevannskvalitet, kart,
vann- og avløpsgebyr.

🛡️ Brannvern, ildsted og feiling

Brannsikkerhet, feiling og tilsyn, bål og
grill, fyrverkeri.



Datasikkerhet for deg som ansatt



Sikkerhetsbevissthet

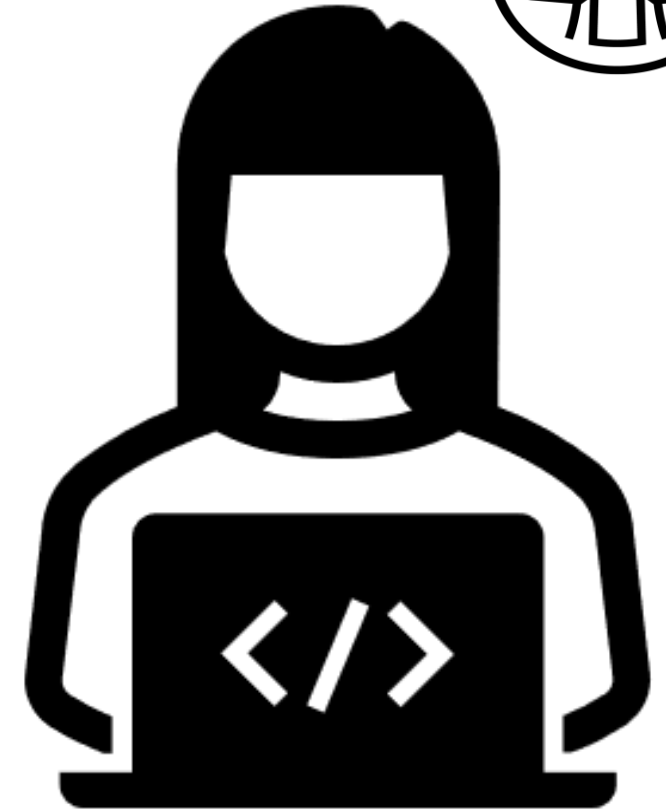
-praktiske råd for deg som ansatt og privatperson

- ▶ Phishing (Tenk ... og så eventuelt klikk)
- ▶ Sterke passord
- ▶ Holde enhetene dine oppdatert
- ▶ Følge med på nyhetsbildet
- ▶ Ta sikkerhetskopier
- ▶ Tenk over hva du legger ut på sosiale medier
- ▶ Vær obs på mistenkelig aktivitet
 - Meld ifra til CSIRT!



Datasikkerhet angår alle

- ▶ Hver og én i kommunen har ansvar
- ▶ Phishing er den største trusselen
 - 41 prosent av dataangrep starter med phishing
(<https://www.kode24.no/artikkel/fire-av-ti-dataangrep-starter-med-phishing/75452046>)
 - Oslo kommune har om lag 50 000 ansatte
- ▶ Konsekvenser: Virus, Løsepengevirus, datalekkasje
- ▶ **Derfor trenger vi din hjelp!**
- ▶ Vi kjører og skal kjøre mange phishing øvelser i framtiden



Phishing sjekkliste

1. Sjekk avsenderadresse
2. Sjekk lenken i eposten
3. Sjekk rettskrivning og generell ordlegging
4. Står innholdet i kontekst?
5. Er det satt en urimelig tidsfrist på deg?
6. Se på den generelle utformingen av eposten
7. Ikke last ned vedlegg umiddelbart
- (8. Bruk offisiell webside, ikke lenken)



----- Opprinnelig melding -----

Fra: BankID <noreply12187@poetic-selection.flywheelsites.com> 1.

Dato: 03.07.2021 10:35 (GMT+01:00)

Til: [\[redacted\]](#)

Emne: Siste varsel Påminnelse fra Sparebanken

5.



4.

Engangskode-appen 4.

kjære kunde, 3.

5.

du må aktivere deg Engangskode-appen før 04.07.2021. Når du har gjort alt dette; vil kontoen din bli aktivert umiddelbart, og du vil kunne fortsette bruke ditt navaerende kodekort kredittkort.

3.



2.

Sjekkliste:
1. Avsenderadresse
2. Lenken
3. Rettskrivning
4. Kontekst
5. Tidsfrist
(6. Utforming)
(7. Vedlegg)



Oslo

13.10.2022

31

Rapporter phishing til oss



Report Phishing

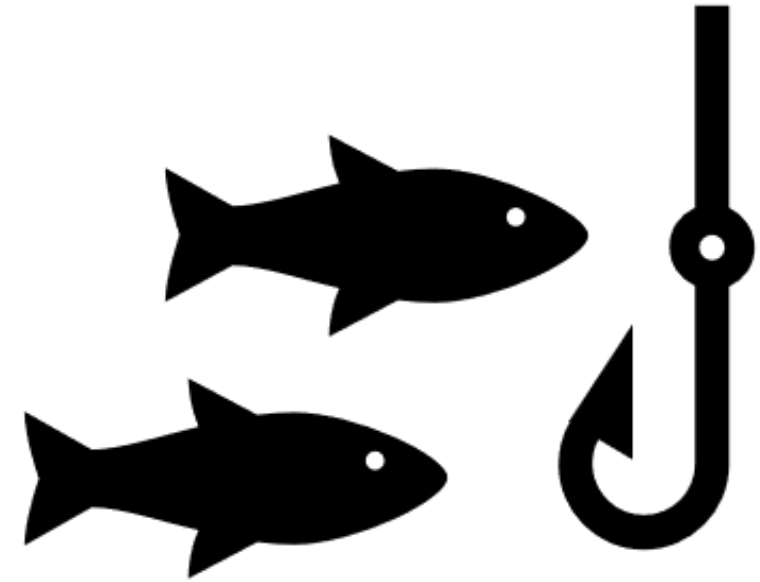
×

Vil du rapportere denne e-posten som svindel?

Du sender med dette et varsel om at du mistenker at dette er en svindel-e-post. Dette vil bli vurdert av ansatte i CSIRT i UKE. Ved behov for avklaring ta kontakt med csirt@oslo.kommune.no. Om din virksomhet har egne avviksrutiner for phishing skal du i tillegg rapportere iht. disse. Takk!

Report

Cancel



CSIRT går gjennom rapporterte eposter hver dag



Oslo

13.10.2022

32

Flere eksempler på sosial manipulering

Forfalsking av

SMS

Sosial manipulering (personlig)

Telefonsvindel



Nye svindelmetoder: «Hvis du tror dette er lureri kan du sjekke telefonnummeret mitt»

Kilde: vg.no – 24.07.2022



Kilde <https://www.istockphoto.com/photo/safety-access-construction-worker-gm175545425-21440458>



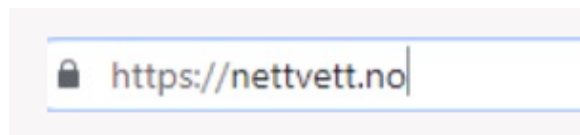
Kilde: nrkbeta.no – 20.04.2020

Oslo

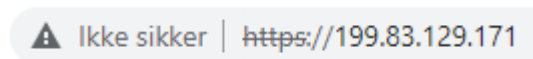
Er nettsiden jeg besøker sikker?

- Brukes sikker kommunikasjon?

Sikker



Ikke sikker



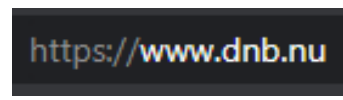
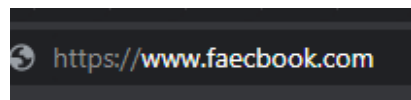
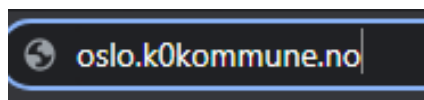
Tilkoblingen til 199.83.129.171 er ikke sikker

Du ser denne advarselen fordi dette nettstedet ikke støtter HTTPS. [Finn ut mer](#)

[Gå videre til nettstedet](#)

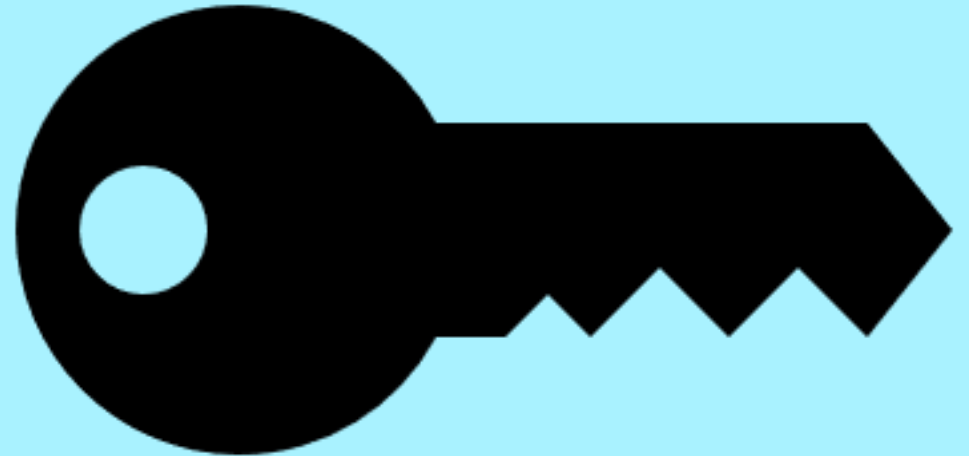
[Gå tilbake](#)

- Vær forsiktig med linker på sosiale medier, i epost og SMS
- Sjekk alltid nettadressen nøye før du logger deg inn



Passord

- ▶ Unike passord (ett passord per tjeneste)
- ▶ Passordhåndteringsprogrammer
 - Lastpass
- ▶ Bytt standardpassord på produktene du kjøper
- ▶ Bruk passord som er vanskelig å gjette
- ▶ Ikke gjenbruk passord i arbeidsforhold
- ▶ **To-faktor autentisering**
 - SMS, Epost, Push-melding, Yubikey



Gode passord

- Minst 12 tegn
- Unikt
- Spesielle karakterer (!?*&)
- Bruk noe praktisk (*Hjemmekontorersuperkult*)
- Eksempler på sterke, men enkle passord:
 - DetteErMittPassordTilPCenMin123
 - Loggmeginnerdusnill1
- Se gjerne anbefalingene fra NSM for setting av passord:
 - <https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet>



Hjemmekontor?



- ♦ Bruker du smartenheter?
- ♦ Har du sterkt passord på trådløst hjemmenettverket ditt?
- ♦ Ikke bland jobb og privat
- ♦ Hvem har tilgang til jobbpceen din?





Reise til utlandet?



Før oppholdet

- Oppdater enheten
- Fjern sensitiv informasjon
- Vurder låneutstyr om du reiser til høyrisikoland (Utenfor EU)

Under oppholdet

- Telefonsamtaler kan bli avlyttet
- Ikke la enhet være uten tilsyn
- Slå av WiFi, Bluetooth og mobildata
- Vær oppmerksom på nettverk du kobler deg til

Etter oppholdet

- Rapporter uvanlig aktivitet
- Endre passord på jobb-relaterte kontoer

Take-aways

- ▶ Usikkert trussellandskap
- ▶ Situasjonen kan endres raskt
- ▶ CSIRT følger, og det må du også!
 - <https://nsm.no/aktuelt/tilbyr-populart-sikkerhetskurs-gratis>
- ▶ Kontakt oss på:
 - CSIRT kanalen på workplace
 - csirt@oslo.kommune.no
- ▶ Kunnskap:
 - Nettvett.no
 - Slettmeg.no
 - Nsm.no



Veien videre for CSIRT

- ▶ Tilby(r) sikkerhetstesting for Oslo kommunes virksomheter
- ▶ Skape tettere samarbeid med virksomheter
- ▶ Gjøre mer forebyggende arbeid

Vi blir større!