Cybertrusler og –hendelser under pandemien og Ukrainakrigen

Linn Kristin Klausen

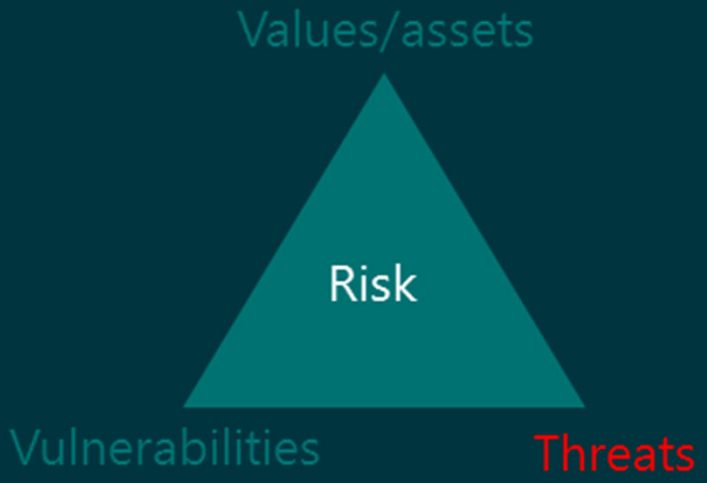
01 juni 2022

Hvem er jeg?

- Linn Kristin Klausen, 32 år
- Cyber Incident Responder, DNB Cyber Defense Center
- Tidligere Counter Threat Unit Lead, Santander Consumer Finance Nordics
- Tidligere Seniorkonsulent, Deloitte Norge Cyber Security Services
- MA Intelligence and International Security, Kings College London
- MA International Relations, University of St. Andrews

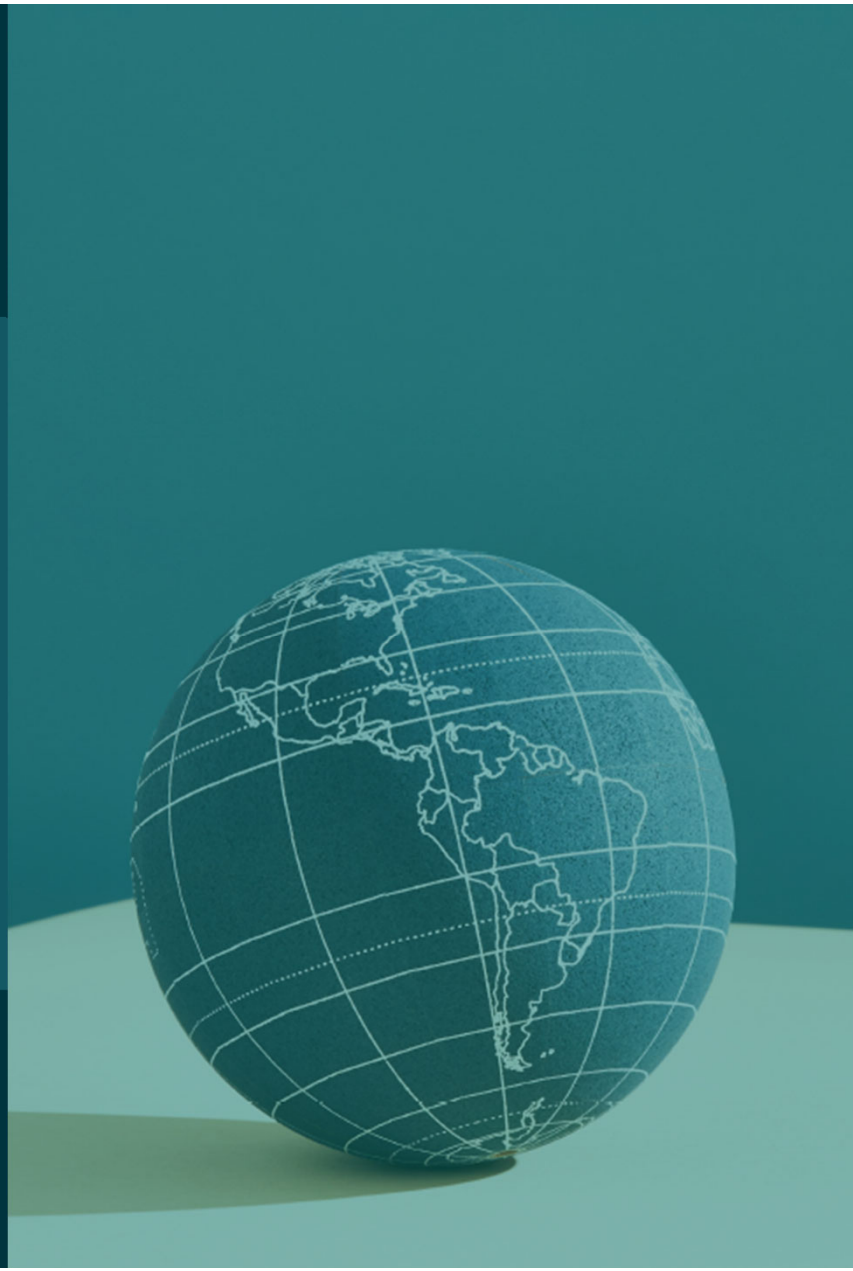
Trusseletterretning

- Etterretning er beslutningsstøtte
  - Beskrive, forklare og forutse
- Etterretning er prosess
- Fokusert på aktører, fenomener og delvis kontekst:
  - Identifisere
  - Analysere
  - Vurdere mulig virkning
  - Fordele kunnskap i organisasjonen
- Trusselbasert sikkerhetsarbeid
  - Trusseletterretning virker best hvis det settes inn før beslutninger fattes
  - Kan benyttes til å følge situasjonen underveis
  - Kan støtte avgrensede områder og enkeltsaker
  - Delgrunnlag for avveining/vurdering av sikkerhetstiltak
    - Beskyttelsestiltak, prosesser, arkitektur, opplæring, krisehåndtering



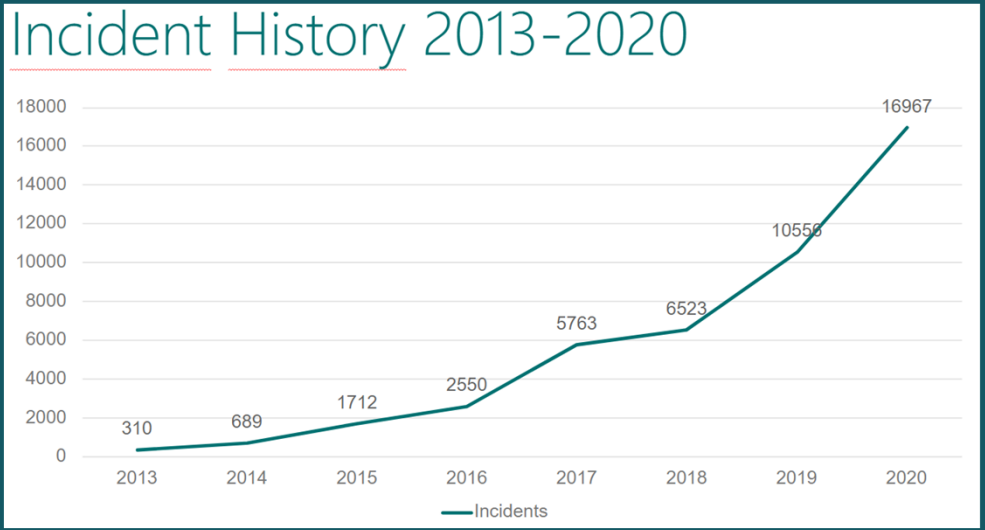
Covid-19

- Cyber-øvelse i begynnelsen av mars 2020
- Landet stengte ned: hjemmekontoret ble den nye normalen
- Utfordret og endret måten vi arbeider – og samarbeider - på
  - Digitaliseringen akselererte
  - Vi flyttet over på hjemmekontor
  - Vi måtte revurdere trussellandskapet i lys av endringene
    - Cyber Defense Center ble satt på high alert

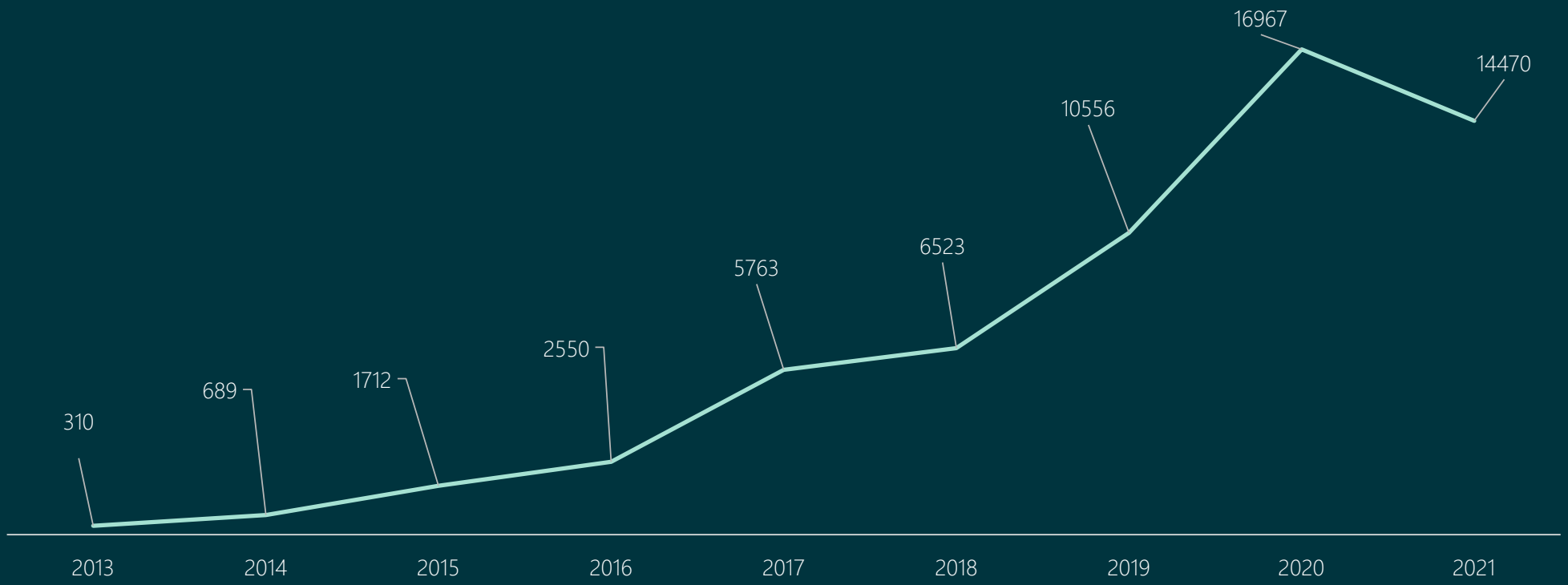


2020 – Pandemien

DNB Cyber Defense Center så en økning fra 10.500 til 17.000 håndterte saker fra 2019 til 2020



Security Incidents - Development



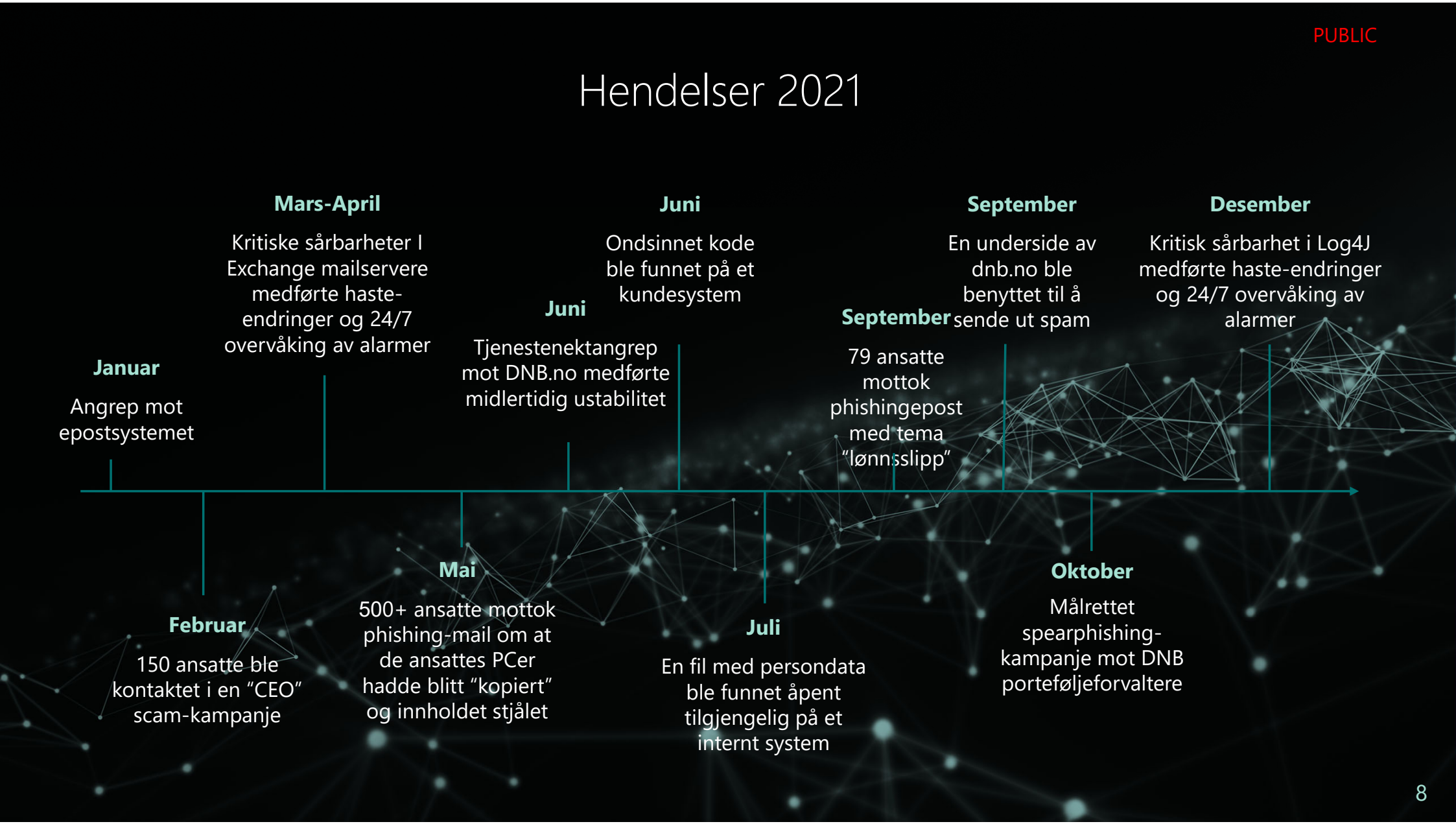
14 470 is a decrease in incidents from 2020. The reason for this is that numbers for 2020 where extraordinary high due to enhanced monitoring related to work from home during pandemic. This was normalized in 2021 and we experience an increase from 2019. Most of these cases are related to abnormal activity such as deviations and not actual intrusions resulting in breach of confidentiality, availability or integrity. Over the last two years, CDC has had a strong focus on automating the handling of alarms so that more time can be spent analyzing more serious incidents in depth. In 2020, 16% of alarms were automatically handled. In 2021 the number was 18%.

Covid-19 & Phishing

- April 2020: phishingkampanje med Covid-19-tema mot DNBs ansatte
  - Første av mange
- Trussel som endrer seg på hjemmekontor
- Phishing er en trend som fortsetter
- I 2021 stoppet DNB over 156 000 phishing-eposter sendt til ansatte

PUBLIC

Hendelser 2021

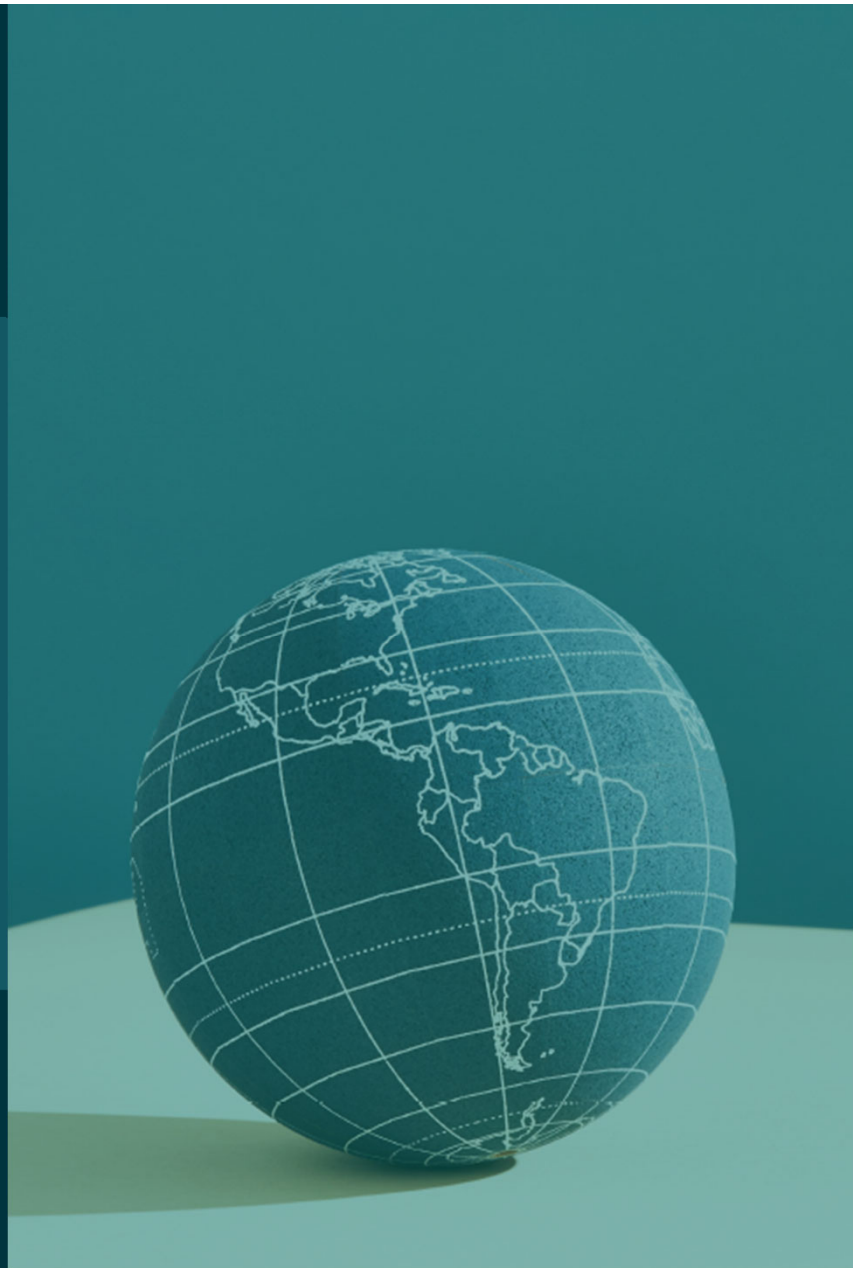


Storpolitikk

- Cyberangrep benyttes som ledd i hybrid krigføring
- Dette har blant annet blitt observert i forbindelse med krigen i Ukraina
- Bedrifter kan bli truffet av cyberangrep som en utilsiktet konsekvens, eller som ledd i at trusselaktører velger side i en konflikt
- Hackergrupper som Conti og Anonymous har valgt side i krigen i Ukraina, noe som påvirker hvem de velger seg som mål
- «Hacktivisme» er en trend i utvikling

Krigen i Ukraina

- Trusseletterretning som situasjonsforståelse og beslutningsstøtte
- Samarbeid og «avsjekker» ekstremt viktig
- Stille spørsmålet: «hvordan endrer dette de digitale truslene vi står ovenfor»
  - Phishingkampanjer rettet med tematikk fra krigen
  - Tjenestenektangrep
  - Risiko for skadevare som spres utenfor kontroll
  - Rekognosering
  - Informasjonskrig
  - Hacktivisme



Rekognosering

- **CDC har ikke observert økt mengde i angrepsforsøk**
- **CDC observerer rekognosering i form av skanning** av vår internett-eksponerte infrastruktur. Aktører skann
  internett for åpne sårbarheter de kan utnytte som et ledd i et cyberangrep.

Informasjonskrig

- Infrastruktur for kommunikasjon har blitt direkte målgjort, og falske nyheter blir spredt systematisk.
- Ukraina har bedt om at Russland blir "kastet ut" av internett.
- To internettleverandører har kuttet tjenester i Russland, med påfølgende forstyrrelser i internettilgang.
- IT-selskaper trekker seg ut av Russland
- Russland har opprettet et eget internett, «RuNet»
- Analytikere frykter et «splinternet»

Hacktivisme

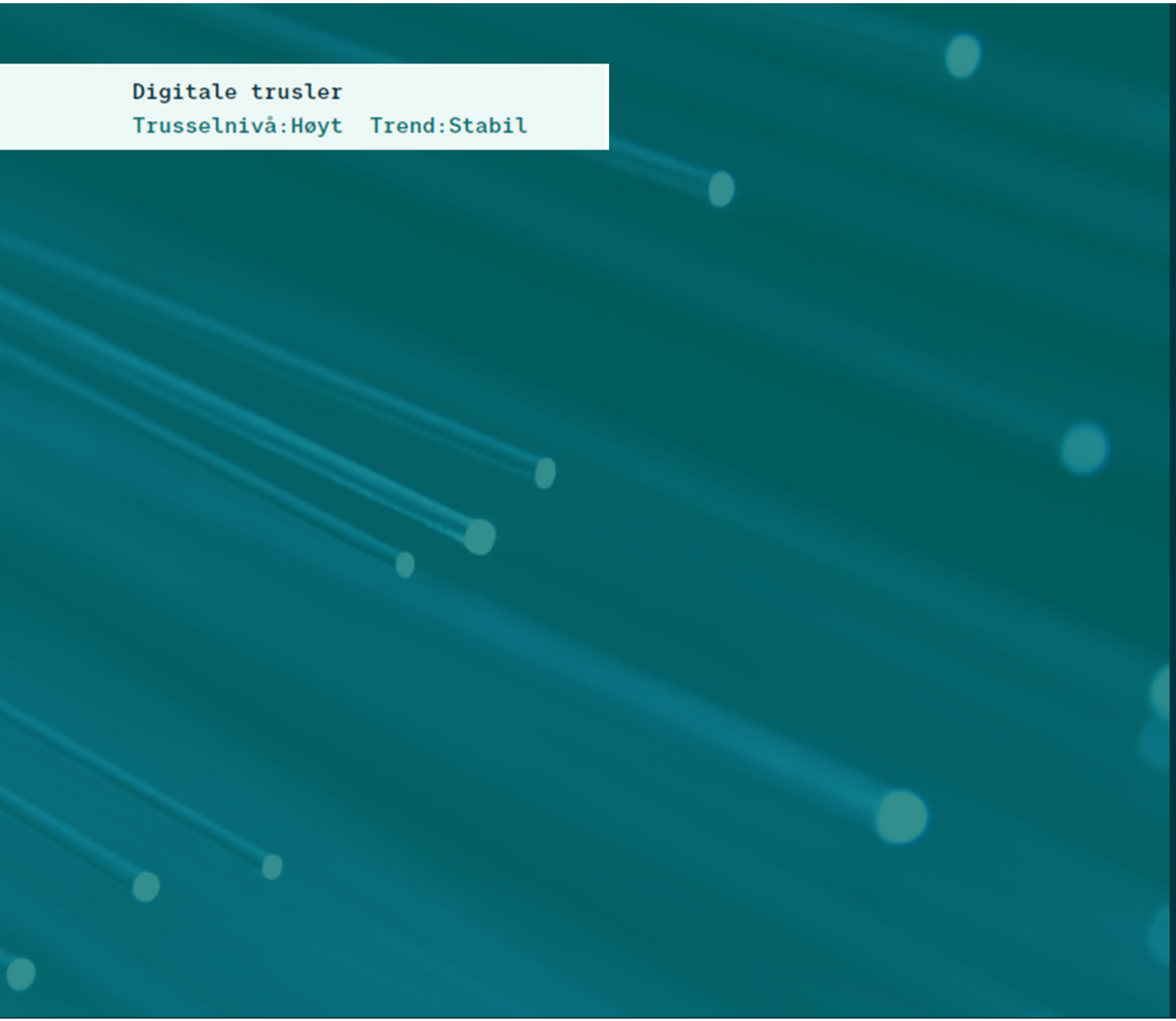
- Hacktivisme" kombinerer "hacking" og "aktivisme“
- Grupper som tradisjonelt har hacket for vinning velger nå side, og tar del i konflikten.
- **Å tolke situasjonsbildet blir stadig mer utfordrende.**

DIGITALE TRUSLER

- De digitale truslene mot DNB vedvarer
- Samfunnsproblem og konsekvenser for renommé, tapte inntekter, forpliktelser mot kunder og finansielle tjenester
- Krigen i Ukraina har skapt et uoversiktlig bilde
- «Collateral damage»

DIGITALE TRUSLER

- Først og fremst økonomisk motiverte organiserte kriminelle aktører
- Profesjonelle bedrifter med stillingsannonser, arbeidstider og ansattgoder
- E-post og sårbarheter på internett-eksponerte tjenester fortsatt mest aktuelt



DIGITALE TRUSLER

- Ransomware største trussel og risiko
- Nedgang i digitale bankran over flere år
- Vurderer at vi vil se en økning i leveransekjedeangrep

Spørsmål?

DNBs trusselvurdering for 2022 - DNB Nyheter

Linn Kristin Klausen
Linn.kristin.Klausen@dnb.no
Twitter: @LinnKlausen

DNB