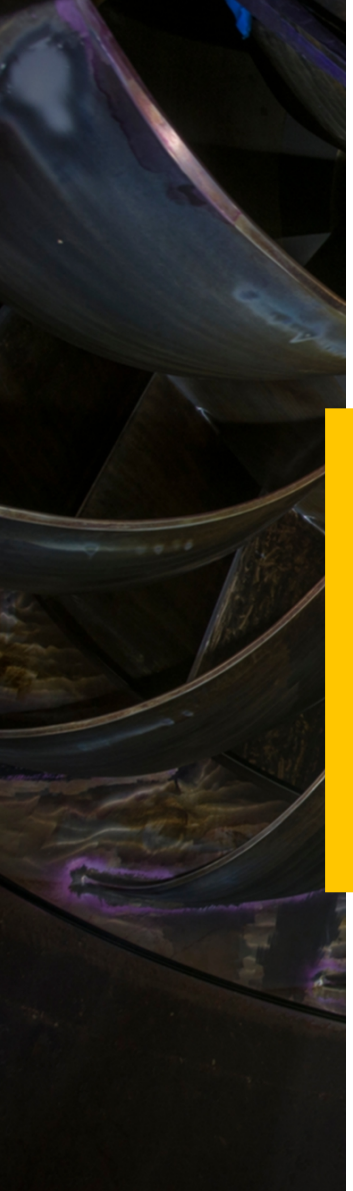
Trusselbildet

Margrete Raaum, KraftCERT/InfraCERT
margrete.raaum@kraftcert.no

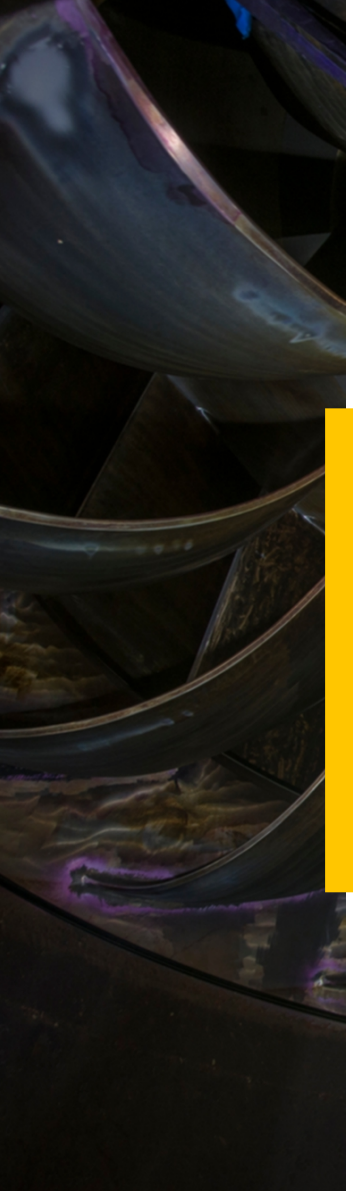
kraftCERT

infraCERT



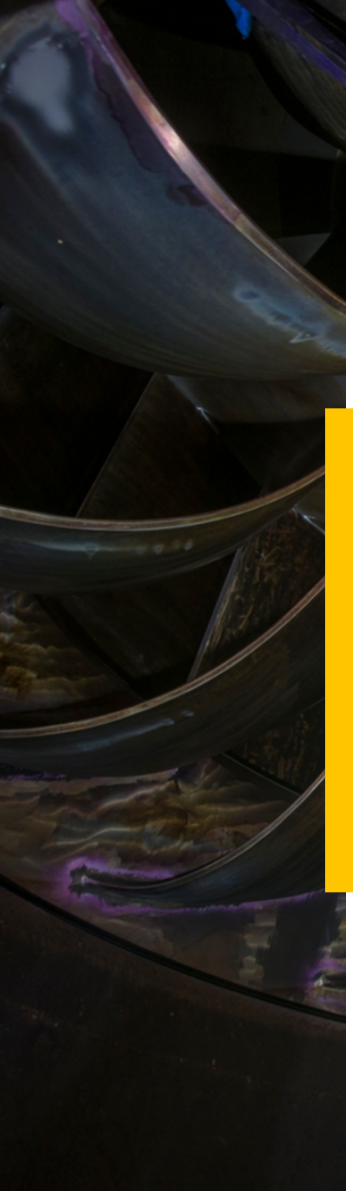
KraftCERT

- Initiativ fra NCSC og NVE - Norges vassdrags- og energidirektorat.
- Uavhengig, ideelt aksjeselskap
- Del av både Kraftbransjens BeredskapsOrganisasjon (KBO) og det norske Sektorresponsmiljøet
- Fokus på operasjonell teknologi, **OT**:
  elkraft, fjernvarme, olje&gass, industri og vann&avløp,
  52 + 175 selskap, 10 ansatte



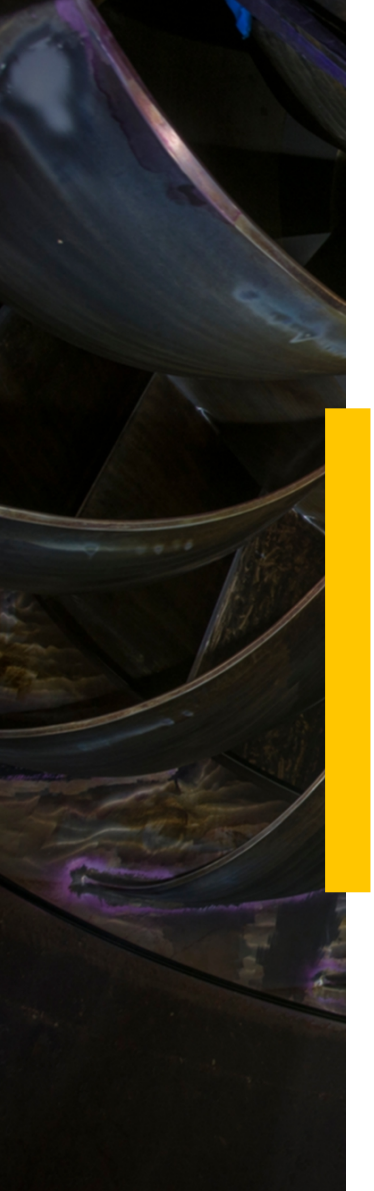
Struktur

- Angrepsmetodikk
- Konsekvenser
- Trusselaktører



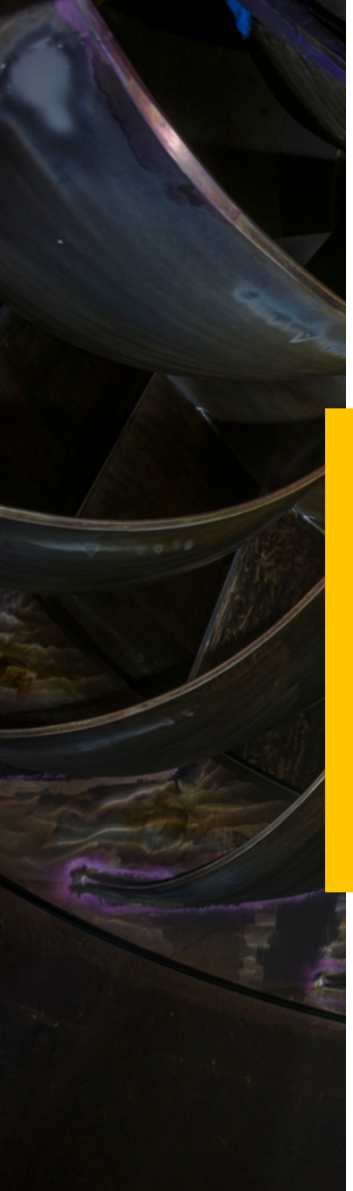
Phishingangrep

- Målrettede, automatiserte angrep med bredt utvalg angrepsmål
- Fisker etter innloggingsdata, fisker med fakturaer, leverer skadevare eller bedriver rekognosering
- Phishingnivået forblir høyt, og teknikker og språk vil forbedres.



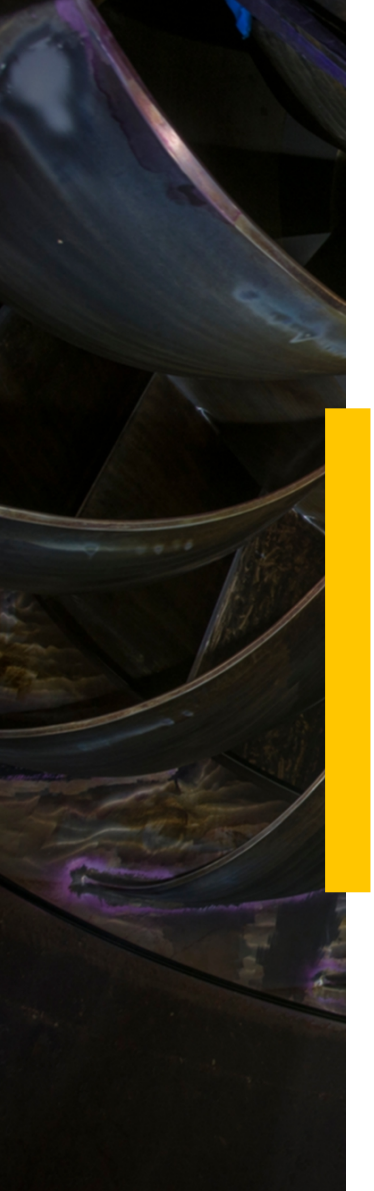
Tredjepartsangrep

- Økning i tredjepartsangrep, -gjennom produsenter og tjenesteleverandører.
- Flere leverandører viser utilstrekkelig trusselforståelse, dermed vanskelig å gjøre en god risikoevaluering av leverandører og deres tjenester.
- Høyt tillitsnivå gir potensiale for overfladisk revisjon, og lite transparens inn i leverandørkjeder og deres sikkerhetsløsninger.



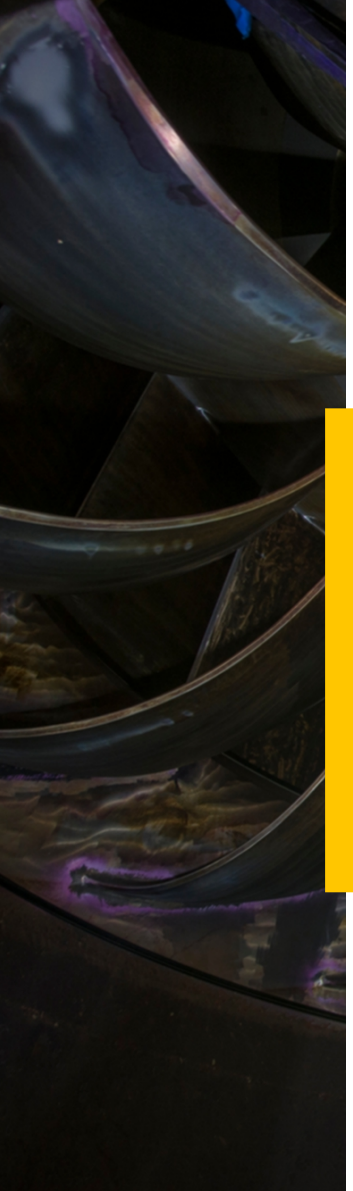
Internetteksponerte tjenester

- Høyt nivå av angrep. De utnytter sårbarheter, benytter stjålne passord eller foretar «brute force» angrep.
- Teknikker som inkluderer utnyttelse av gyldige innloggingsdata vil øke, der disse er skaffet til veie gjennom phishing, passordnekking, innbrudd eller salg på det mørke nettet.
- Ny teknologi vil komplisere dette ytterligere.



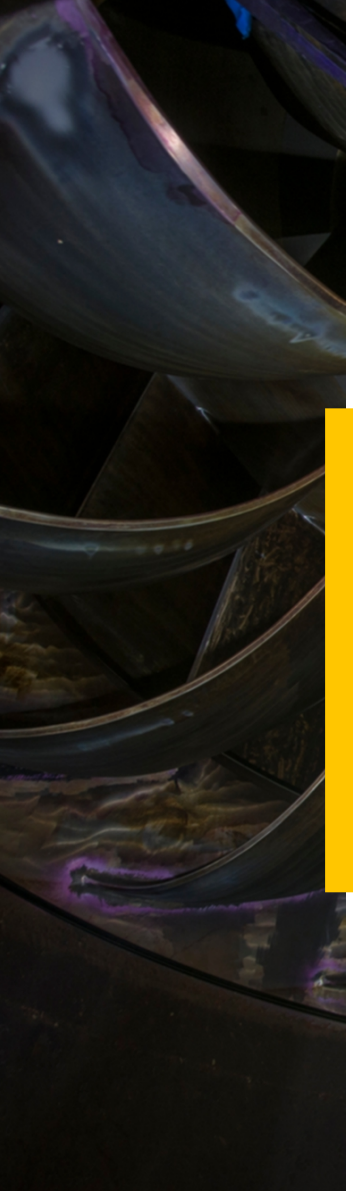
Kamuflasje

- Angripere bruker lokale verktøy og standard ekstern infrastruktur.
- Denne type kamuflasjeteknikk vil øke og vi vil se mer automatisering.
- Dette gjør at mange deteksjonsmekanismer blir verdiløse.



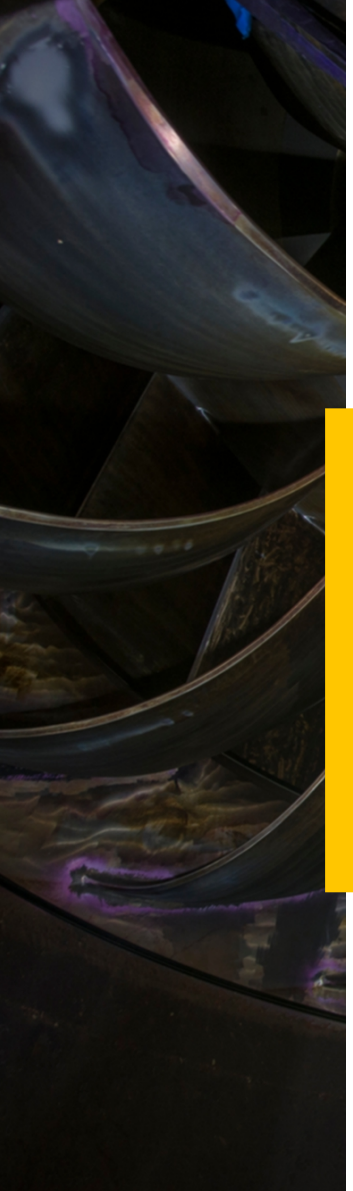
Utpresning

- KraftCERT anser det som sannsynlig at utpresningsmetodikker vil utvikle seg
- Kryptovare (krypteringsskadevare) dominerer bildet.
- For å øke presset på ofrene er det nå vanlig å også stjele data og true med å publisere.
- Det er også noen som går til kunder av ofrene for å få dem til å legge press på offeret om å betale.
- Digitalisering gir en bredere angrepsflate, men økte muligheter for deteksjon og logging av både rekognosering og angrep.



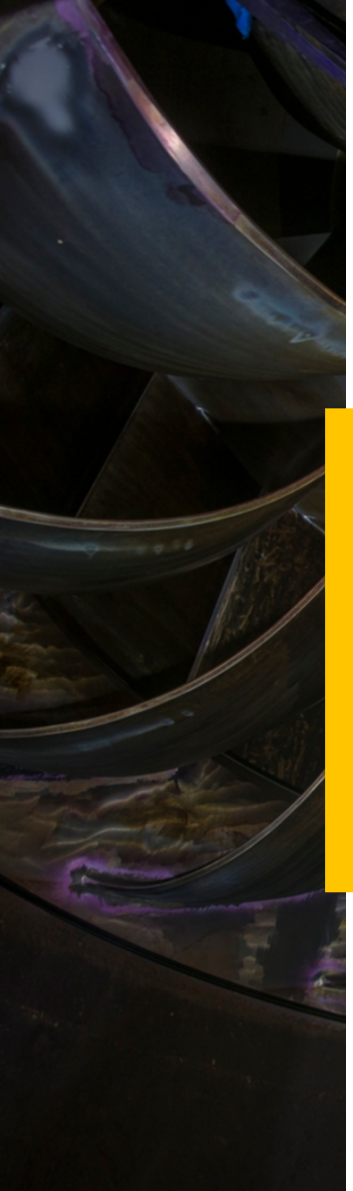
Lekkasjer og informasjonstyveri

- Tilfeldige kompromitteringer kan gi angripere verdifull informasjon som kan benyttes målrettet senere.
- Høyaktivitetsmarked for salg av informasjon som senere brukes til utpresning, videresalg eller andre operasjoner.
- Kan være vanskelig å detektere.
- Lekkasjer kan gjøre en hendelse til en krise.



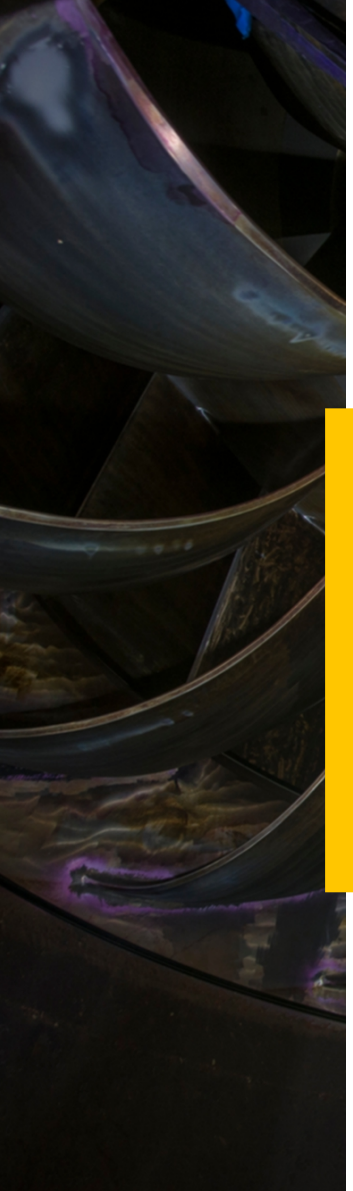
DDoS-angrep

- DDoS via (I)IoT øker, og dette vil ikke bedre seg før noen stiller krav til produsenter, da mye utstyr inneholder elementer/moduler som er trivielle å utnytte eller kompromittere.
- Økt bruk av 5G vil antagelig forverre situasjonen.



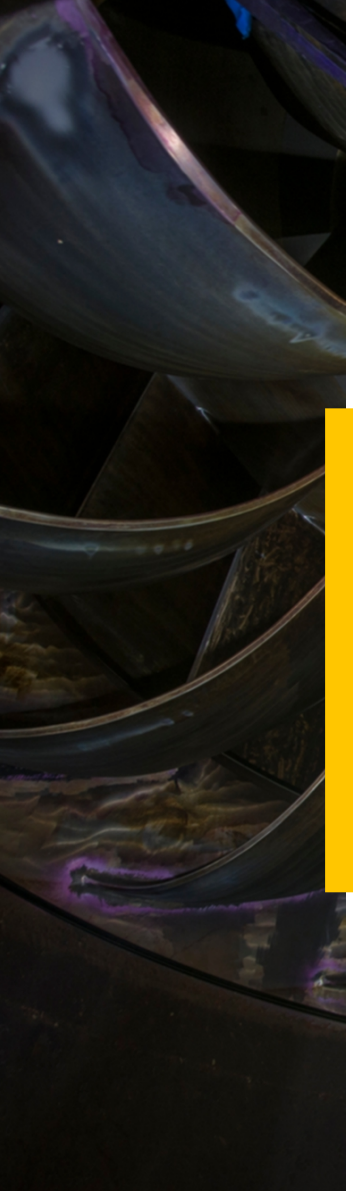
OT-spesifikt

- OT er ikke bare OT. Det er også produksjonsplanlegging og markedsoperatører.
- Risikovurdering bør også inkludere relevante adminisjasjonssystemer (f.eks. HVAC og sikkerhetssystemer), i tillegg til tjenesteleverandører, transport og produsenter.
- I nyere teknologi må sikkerhet rundt f.eks. digitale tvillinger, digitale stasjoner eller virtuelle kraftverk ivaretas spesielt.



Trusselaktører - overordnet

- Hovedmotivasjonen for det meste kriminell aktivitet vil fortsatt være penger. Det gjøres ved f.eks. direkte svindel, utpresning eller videresalg av informasjon. Det er mye salg av kompromitterte aksesser til selskapers nettverk.
- Politisk motiverte aktører er også aktive, spesielt som miljøvern og/eller energipolitikk kommer høyere på agendaen.



Integritetsfokuserte trusselaktører

- Stuxnet – Ukraina 1&2 - Trisis
- Stuxnet skulle ødelegge firmaets tiltro til egne systemer, og nasjonens tiltro til firmaet.
- Ukraina 2015 var relativt manuell, og uprofesjonell.
- Trisis og Ukraina2 var mer destruktive enn de fleste angrep er. Mange angrep som er avanserte og integritetsfokuserte er politisk motivert.
- I tilfeller der disse angriperne fokuserer på utbredte systemer er alle eiere utsatt.