kraftCERT infraCERT

Trusselvurdering

2025

Innhold

1 Trusselvurdering 2025

Trusselvurdering 2025 beskriver cybertrusler mot KraftCERTs sektorer, med hovedvekt på sannsynlighet for angrep. Rapporten danner grunnlag for tiltakspakken som publiseres høsten 2025. Begge dokumentene støtter lokal risikovurdering og prioritering.

Trusselvurdering 2025 er skrevet for beslutningstakere og sikkerhetsmiljøer som må navigere i et trusselbilde med høy kompleksitet og stor usikkerhet. Vurderingene er ikke allmenngyldige, og trenger kontekst for å være relevante i den enkelte virksomhet.

1.1 Nøkkelvurderinger

De fleste cyberangrep starter med kjente teknikker. Det er **meget sannsynlig** at eksponerte tjenester, phishing, og misbruk av legitime verktøy også fremover vil være de vanligste inngangsveiene til virksomhetenes IT-systemer.

Når angripere først har fått tilgang, er det **meget sannsynlig** at de bruker virksomhetens egne programmer og tjenester for å bevege seg videre i systemene uten å bli oppdaget. Fjerntilgang og delt infrastruktur med leverandører øker denne muligheten.

Utpressingsangrep er en svært aktuell trussel. Det er **sannsynlig** at et slikt angrep fører til driftsforstyrrelser, særlig der IT og kontrollsystem henger sammen. Det samme gjelder angrep via skytjenester eller leverandører.

Vellykkede destruktive cyberangrep på industrielle kontrollsystemer er **meget lite sannsynlig** på kort sikt. Med dette menes angrep som fysisk skader prosess, utstyr eller mennesker. Slike angrep krever kontroll over både styring og sikkerhetsfunksjoner. Kjente aktører har forsøkt det i Ukrainakrigen, uten å lykkes og uten å ha tilstrekkelig verktøy eller skadevare.

Driftsforstyrrelser som følge av angrep på IT er **sannsynlig**. Industrielle kontrollsystemer påvirkes indirekte, enten gjennom isolering eller avhengigheter mellom IT og drift.

Spionasje er en del av normalen, og det er **meget sannsynlig** at virksomheter kartlegges både teknisk og organisatorisk.

Usikkerhet rundt USAs rolle i Europa gjør trusselbildet mer uforutsigbart. Dersom Russland reduserer innsatsen mot amerikanske mål, er det **sannsynlig** at europeisk infrastruktur får økt oppmerksomhet – som mål for kartlegging, påvirkning eller sabotasje.

Det er **meget sannsynlig** at de fleste aktører tar i bruk kunstig intelligens (KI) i ulik grad. Angrepsformer blir allerede videreutviklet med KI. Først og fremst øker volum, effektivitet og angripers evne til å spesialtilpasse til målet, gjennom f.eks deepfakes.

2 Rammeverk for forståelse og bruk

2.1 Formål og avgrensning

Trusselvurdering 2025 beskriver utviklingstrekk, trusselaktører og angrepsformer som KraftCERT vurderer som mest relevante for våre sektorer. Rapporten ser 2–3 år frem i tid, med kort sikt vurdert til omtrent ett år. For enkelte områder innen industrielle kontrollsystemer vurderes lengre tidshorisonter. Vurderingen dekker aktørers intensjon, evne og mulighet, men omfatter ikke tekniske detaljer, individuelle trusselaktører eller helhetlige sårbarhets- og konsekvensvurderinger.

2.2 Om KraftCERT

KraftCERT er sektor-cyberresponsmiljø for sektorene kraft og petroleum, og ellers består målgruppen av prosessindustri, vann- og avløpssektoren samt energigjenvinning. KraftCERT har medlemmer både i Norge og på Island.

KraftCERT er både ISAC (Information Sharing and Analysis Center) og IRT (Incident Response Team) for våre medlemmer. Vi gir støtte ved digitale hendelser, og formidler relevant og verifisert informasjon om sårbarheter, trusler og angrep. KraftCERT er del av den nasjonale beredskapen, og samarbeider med både private og offentlige aktører nasjonalt og internasjonalt. Vi er medlem av Forum of Incident Response and Security Teams (FIRST) og sertifisert IRT i Trusted Introducer.

2.3 Sannsynlighetsbegreper

KraftCERT bruker faste begreper for å beskrive hvor sannsynlig det er at en hendelse eller utvikling vil inntreffe.

Sannsynlighetsgrad	Prosent	Synonymer
Meget sannsynlig	> 90 %	KraftCERT er overbevist om, stor grad av sikkerhet
Sannsynlig	60 - 90 %	KraftCERT fester stor tillit til, betydelig grad av sikkerhet
Mulig	40 - 60 %	Det er indikasjoner på, like sannsynlig som usannsynlig
Lite sannsynlig	10 - 40 %	Tvilsomt
Meget lite sannsynlig	< 10 %	Svært tvilsomt, nesten umulig, usannsynlig

3 Situasjonsbildet

Kjente trusler, aktører og teknikker vil fortsatt prege situasjonsbildet. Samtidig øker usikkerheten som følge av geopolitisk uro og uklare aktørgrenser. Cyberkriminelle, Russland og Kina vurderes som de mest relevante trusselaktørene for våre medlemmer. Norge og Island utsettes fortsatt for relativt få cyberangrep sammenlignet med mange andre deler av verden, men utviklingen i det sikkerhetspolitiske landskapet – særlig usikkerhet rundt USAs rolle i Europa – bidrar til en mer uforutsigbar fremtid. Spionasje er en del av normalbildet. Sabotasje vurderes oftere som en aktuell trussel, både i etterretningsvurderinger og offentlig diskusjon.

3.1 Sentrale trusler og aktører

Cyberkriminalitet er den mest vedvarende og sannsynlige trusselen. Cyberkriminelle er opportunistiske aktører drevet av økonomisk motivasjon. Angrepene rammer bredt og krever ofte lite innsats eller ressurser fra aktørene. For de fleste medlemmer vurderes denne aktørtypen som mest relevant i det daglige trusselbildet[1][2]. De fleste angrep har økonomisk motivasjon, men det finnes også aktører som handler på oppdrag eller i nær tilknytning til statlige interesser.

KraftCERT vurderer at Russland og Kina er de mest relevante statlige trusselaktørene for våre medlemmer. EOS-tjenestene (E-tjenesten[1] [3], NSM[2] [4], PST[3] [5]) beskriver i sine åpne vurderinger at Russland og Kina har intensjon og kapabilitet til å gjennomføre operasjoner mot vestlige mål, inkludert Norge. Kina og Kina-tilknyttede aktører har en bred tilnærming til informasjonsinnhenting, og forsøker å skjule både metode og tilknytning til operasjonene.

PST trekker i tillegg frem Iran og Nord-Korea. KraftCERT vurderer at Nord-Korea er særlig aktive innen kryptosvindel, mens Iran ofte driver hacktivisme mot mål i Israel og USA, eller mot utstyr laget av selskaper i landene. Det betyr ikke at disse to er irrelevante, men Russland og Kina har langt høyere relevans.

Sabotasje vurderes som en mulig trussel mot KraftCERTs medlemmer i 2025. Ifølge PST er det **sannsynlig** at russisk etterretning vil forsøke sabotasjeaksjoner i Norge, blant annet for å påvirke støtten og leveransene til Ukraina. PST peker også på at norsk-eid energiinfrastruktur kan bli mål, men angir ikke grad av sannsynlighet[3] [5]. KraftCERT vurderer at sabotasjetrusselen EOS-tjenestene beskriver i hovedsak er fysiske aksjoner.

KraftCERT deler vurderinger om at Russland fremstår mer risikovillig enn tidligere. Samtidig er flertallet av hendelser i Europa det siste året preget av uklar eller manglende aktørtilknytning, og flere har fått alternative forklaringer som teknisk svikt eller uhell. Dette gir stor usikkerhet, og gjør det krevende å si noe sikkert om omfang eller retning for sabotasjetrusselen.

Medlemmer med støtte- eller leveranseforhold til Ukraina vil etter KraftCERTs vurdering ha et høyere trusselnivå også for sabotasje. Spesielt gjelder dette for infrastruktur som kan direkte knyttes til finansiering av Ukrainas krigsinnsats.

[1] Etterretningstjenesten
[2] Nasjonal Sikkerhetsmyndighet
[3] Politiets Sikkerhetstjeneste

3.2 Spionasje og informasjonstap

Cyberspionasje er en vedvarende og sannsynlig trussel mot KraftCERTs medlemmer. Særlig virksomheter innen kraft og petroleum er attraktive mål. EOS-tjenestene har i flere år advart mot spionasje rettet mot kritisk infrastruktur, og formålene spenner fra generell situasjonsforståelse til målrettet industrispionasje.

Kripos omtaler tap av sensitiv informasjon som en "kumulativ trussel" [1] – en vurdering KraftCERT støtter. Uskyldig eller fragmentert informasjon kan over tid gi innsikt i systemer og sammenhenger. Når store mengder data spres, publiseres eller lekkes, kan de senere analyseres med nye verktøy og bidra til angrepsforberedelser. Energilovens begrep om kraftsensitiv informasjon (§6-1 og §6-2) illustrerer dette: Det er helheten som avgjør hvor skjermingsverdig informasjonen er.

3.3 Internasjonal strategisk usikkerhet

Trusselbildet for KraftCERTs medlemmer påvirkes av relasjonen mellom stormakter. Forsvarsanalysen 2025 beskriver et scenario der «USA isolerer seg eller inngår en slags forståelse med Kina og Russland om en uformell deling av verden i innflytelsessfærer. Det kan etterlate Europa alene med Russland.»[6]

Økt usikkerhet og uro forsterker staters behov for innsikt og posisjonering. KraftCERT vurderer det som **meget sannsynlig** at statlige aktører innhenter informasjon og etablerer tilgang i fredstid, for å være forberedt på mange ulike utviklinger. Dette gjelder også mål og virksomheter som foreløpig ikke er i fokus.

4 Sektorperspektiver

Hva som regnes som kritisk infrastruktur varierer med perspektiv. Enkelte virksomheter har nasjonal rolle, andre har betydning for europeisk forsyningssikkerhet. Begrepet brukes ulikt i rapporter og media, og det er lite felles forståelse. Vi vurderer hvordan virksomheter kan bli mål, uten å definere hva som er kritisk.

4.1 Sektorperspektiv petroleum

Det er lite sannsynlig at norsk olje og gass-sektor er spesielt utsatt for angrep på kort sikt. Det er historisk sett få angrep, og det er få tegn på økt aktivitet rettet mot sektoren. Ifølge NSMs Risiko 2025 sto petroleumssektoren for kun 1 % av rapporterte cyberhendelser i 2024 [4], ned fra 4 % i perioden sommeren 2022 til utgangen av 2023 [7]. Sett opp mot sektorens kritikalitet og profil, fremstår angrepsnivået som lavt. Merk at dette er en vurdering med høy usikkerhet, på grunn av potensialet for endring i geopolitisk situasjon og trusselaktørers prioriteringer.

Petroleumssektoren er strategisk viktig og vil forbli et attraktivt mål for trusselaktører. Norsk petroleum spiller en avgjørende rolle i energiforsyningen til flere allierte land, spesielt Storbritannia. Dersom land som Storbritannia eller Frankrike tar en enda mer aktiv rolle i Ukrainakrigen, kan dette påvirke hvordan Russland prioriterer mål i energisektoren. I et scenario der USA reduserer sin interesse for europeisk sikkerhet og samtidig trapper ned tiltak mot russisk-tilknyttede cybermiljøer, kan europeiske aktører og infrastruktur bli mer utsatt. Hvis Russland ikke lenger ser det samme behovet for å bruke kapasitet mot amerikanske mål, kan det gi mulighet for å rette kapasitet mot europeiske mål – inkludert norsk petroleumssektor.

4.2 Sektorperspektiv kraft

KraftCERT vurderer det som lite sannsynlig at kraftsektoren blir direkte rammet av større angrep det neste året. Det finnes foreløpig ingen informasjon som tilsier økt aktivitet mot sektoren. Ifølge NSMs Risiko 2025 sto kraftsektoren for 1 % av rapporterte cyberhendelser i 2024 [4], ned fra 5 % året før [7]. Til tross for at kritikaliteten og synligheten er høy, er angrepsnivået fortsatt lavt.

KraftCERT vurderer det som sannsynlig at cyberangrep på IT-støttesystemer kan svekke evne til forskriftsmessig drift. Angrep som setter vedlikeholdssystemer, dokumentstyring eller beredskapsverktøy ut av spill, kan føre til redusert driftssikkerhet, forsinket feilretting og svekket evne til å dokumentere etterlevelse.

Selv om kraftsystemet i Norge er robust, finnes det områder og systemer med lav redundans. Et cyberangrep som fører til strømavbrudd her kan få uforholdsmessig stor effekt på samfunnskritiske tjenester. Dette gjelder særlig spesialiserte funksjoner som er avhengige av kontinuerlig kraftleveranse uten tilgjengelig reservekapasitet.

4.3 Sektorperspektiv vann

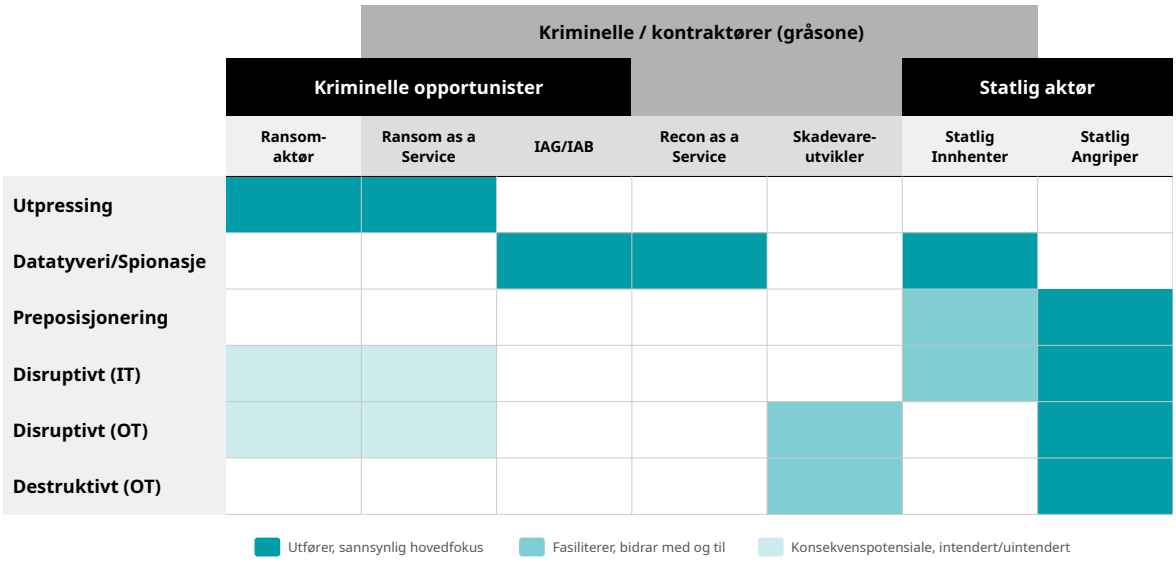
KraftCERT vurderer det som lite sannsynlig at det vil komme store og betydningsfulle angrep mot norsk vannsektor, selv om vi vurderer vannsektoren som mer sårbar enn mange andre, både teknisk og organisatorisk. Vannsektoren er geografisk spredt, og har stor variasjon i størrelse og ressurstilgang i sikkerhetsarbeidet.

I likhet med kraftsystemet er vannsektoren av stor samfunnsmessig betydning. Relativt lav terskel for påvirkning og stor offentlig synlighet gjør sektoren til et attraktivt mål – særlig for aktører som ønsker å spre usikkerhet. Andre nasjoner, som Danmark [8] og Frankrike [9], har satt drikkevannsektoren i fokus, og sektoren blir mye omtalt i den europeiske sikkerhetsdiskusjonen.

5 Aktører, angrep og hendelser

5.1 Aktørers motivasjon og organisering

Trusselaktører opererer i et økosystem av tjenester, verktøy og samarbeid. Modellen viser hvordan ulike aktørtyper (kriminelle, gråsoneaktører, stater) benytter eller kjøper tjenester som tilgangsmegling, skadevareutvikling og rekognosering, og hvordan dette muliggjør angrep som spionasje, utpressing, preposisjonering og direkte skade.



Figur 1: Sammenheng mellom aktører, tjenester og angrepsformer

5.2 Cyberkriminelle

Cyberkriminelle er opportunistiske aktører, primært drevet av økonomisk motivasjon.Tradisjonelt har dette kommet til uttrykk gjennom angrep der ofrene presses for penger, eller hvor stjålne data selges videre. De siste årene har det i tillegg vokst frem et marked og en egen økonomi rundt slike angrep, der spesialiserte tjenester og tilganger handles og leies ut.

Det er sannsynlig at muligheten til å utføre enkle angrep er en viktig del av målutvelgelsen for rent kriminelle aktører. Flere, enklere angrep gir totalt sett større avkastning enn mer kompliserte og ressurskrevende enkeltangrep med en mer usikker inntjening. Tilgang til informasjon om mål er også kritisk (**se kap.6 Angrepsforutsetninger**).

Gjenbruk av kjente sårbarheter og skadevare gjør at angrepstakten øker, så selv om risikoen for oppdagelse er større, vil fortsatt antallet vellykkede angrep gå opp. KraftCERT vurderer det som meget sannsynlig at risikoen for at cyberkriminelle blir tatt er lav nok til at enkle angrep vil fortsette.

Det er meget sannsynlig at antallet vellykkede løsepengeangrep vil fortsette å øke globalt[10][11]. Tidligere myndighetsaksjoner rettet mot etablerte aktørgrupper har fragmentert det kriminelle økosystemet. Det har likevel ikke hatt noen effekt på antallet angrep, siden grupper har fragmentert seg i flere mindre, mer fleksible aktører som opererer under nye aliaser. Disse bruker i større grad skjulte og varierende taktikker for å unngå deteksjon.

Små og mellomstore virksomheter er attraktive mål. Flere ransomware-aktører prioriterer SMB fordi

svakere forsvar gjør angrep enklere, og betalingsviljen ofte er høyere[12]. Trenden forsterkes av økt bruk av kjente sårbarheter og automatiserte verktøy, som gir høy avkastning med lav risiko.

5.3 Tilrettelegging

Mange aktører kjøper tjenester de ikke selv kan utføre. Tilrettelegging er en rolle, ikke en aktørtype – og brukes av både kriminelle, kontraktører og statlige. Dette bidrar til et ustabilt og flytende aktørbilde.[13][14][15]

KraftCERT vurderer det som sannsynlig at kriminelle tjenesteleverandører vil få økt betydning. Aktører som tilbyr «løsepengeangrep som tjeneste» er i vekst. Nykommeren RansomHub [16] gjør det mulig for alle aktører å gjennomføre både brede og målrettede operasjoner uten høy teknisk kompetanse.

Markedet for tilganger er i vekst og benyttes av flere aktørtyper. Etterspørselen etter kompromitterte innloggingsdata og tilgang til systemer øker[17]. Tilgangsgrupper (aktører som samler påloggingsinformasjon) og tilgangsmeglere (som videreformidler slike tilganger til andre) spiller en viktig rolle i angrepskjeden. KraftCERT vurderer det som **meget sannsynlig** at slike tilganger også benyttes av statlige og statstilknyttede aktører i et langsiktig arbeid. Tilgangsgrupper og -meglere vil også i fremtiden i all hovedsak være opportunistiske og økonomisk motivert, selv om det er **mulig** at statlige aktører og kontraktører søker å utvikle egne tilganger[18].

Det er sannsynlig at det blir flere grupper som opptrer som direkte kontraktører for nasjonalstatlige aktører. Rekognoseringstjenester senker terskelen for angrep. Enkelte tilbyr rekognoseringstjenester basert på automatiserte metoder og kunstig intelligens[13], og leverer både til andre kriminelle og til statlige aktører.

Skadevareutvikling skjer ofte utenfor de operative angrepsgruppene. Det er sannsynlig at utvikling og testing av skadevare skjer i egne miljøer, uavhengig av dem som til slutt bruker verktøyene. KraftCERT vurderer at denne spesialiseringen bidrar til høyere innovasjonstakt.

KraftCERT vurderer det som sannsynlig at aktør-tracking får redusert verdi, blant annet fordi aktører splittes, bytter navn og fyller flere roller samtidig. Rollene mellom utvikler, tilrettelegger og angriper er delvis overlappende. Det er vanlig at én aktør både utvikler, distribuerer og bruker skadevare – men også at de kun gjør en eller flere av delene. KraftCERT vurderer at dette gjør attribusjon enda mer usikker.

5.4 Oppdragsstyrte aktører

Målstyrte eller oppdragsstyrte aktører har vanligvis annen motivasjon enn det rent økonomiske. Dermed er muligheten for angrep ikke den viktigste driveren for målutvelgelse.

KraftCERT vurderer det som sannsynlig at russisk aktivitet mot Europa og Norge vil øke, som følge av endringer i relasjonen mellom USA og Russland. Økt intensjon og risikovilje tilsier at virksomheter bør oppdatere gamle trussel- og risikovurderinger – særlig med tanke på sannsynlighet.

Det er sannsynlig med forsøk på langsiktig preposisjonering fra nasjonalstatlige aktører. En oppdragsstyrt trusselaktør med god tid samler informasjon over tid, og vil søke å etablere dype posisjoner i leverandørkjeder og på denne måten forberede senere målrettede angrep[18]. Denne strategien gir dem en fordel når angrepsmulighetene modnes. Trusselaktører etablerer og opprettholder flere innganger til samme mål for å sikre vedvarende tilgang, oppnå bedre forståelse av infrastrukturen, og legge til rette for senere utnyttelse eller videresalg.[19]

Oppdragsstyrte aktører utnytter i økende grad samme tjenester, plattformer og skadevare som kriminelle aktører. Det gjør dem vanskeligere å identifisere og gir større handlingsrom i valg av framgangsmåte.[20]

Det er mulig at det vil skje forsøk på både digital og fysisk utnyttelse av leverandører, der innsatsen rettes mot nøkkelpersonell hos leverandør for å kompromittere deres legitime tilganger. Angriperen kan da oppnå en inngangsport mot større systemer eller manipulere fysiske enheter. Sannsynligheten for denne typen angrep bør ses i sammenheng med EOS sine vurderinger om økt sabotasjetrussel.

Enkle og ineffektive tjenestenektangrep er meget sannsynlige, gjerne kamuflert som hacktivisme. Mange av disse har bånd til statlig støttede aktører, i en strategi kjent som faketivisme.

KraftCERT vurderer at det er **lite sannsynlig** at det finnes norske hacktivister[4] som har intensjon eller evne til å utføre angrep på kort sikt.

5.5 Innsidere og utilsiktede hendelser

Innsidere som bevisst tilrettelegger for angrep utgjør en alvorlig, men lite sannsynlig trussel. De har stort skadepotensial, men det er få bekreftede hendelser i Norge, og påstander om økt trussel er sjelden godt dokumentert – heller ikke i graderte vurderinger.

Derimot er det meget sannsynlig at utilsiktede feil og mangler gir rom for angrep. Sikkerhetssvakheter – inkludert rene feil, manglende tiltak og hvordan brukere møter phishing – gir trusselaktører muligheter de ellers ikke ville hatt[21][22].

> **Change Healthcare-hendelsen** er et eksempel på hvordan ett enkelt stjålet passord, trolig fra en intetanende ansatt, kan få nasjonale konsekvenser. I februar 2024 ble det amerikanske selskapet Change Healthcare rammet av ransomware[23]. Angrepet utnyttet mangelfull flerfaktorautentisering. 190 millioner amerikanere ble berørt, og det ble betalt 22 millioner USD i løsepenger.

[4] Cyberaktivister med ideologisk utgangspunkt, som miljøaktivister og vindkraftmotstandere

6 Angrepsforutsetninger

Et vellykket angrep krever at aktøren har en kombinasjon av intensjon, evne og mulighet. Intensjonen definerer aktørens målsettinger, planer og risikovilje, evnen beskriver det tekniske nivået for hva de kan få til (kapabilitet og kapasitet), og muligheten omfatter både hva de kan utvikle av angrep og hva vi gir dem gjennom sårbarheter.

Informasjonstilgang avgjør hvor gjennomførbart et angrep oppleves. For å kunne vurdere angrepsmuligheter, trenger en angriper informasjon, og vi kan dele denne informasjonen etter tilgjengelighet:

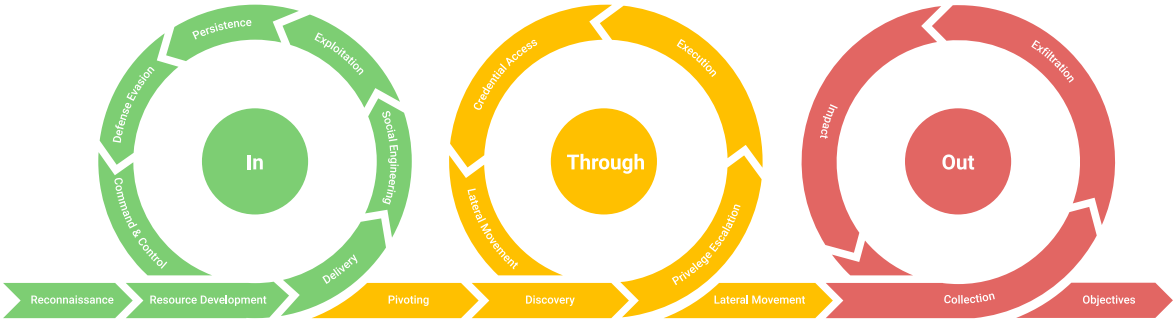
- Åpen informasjon: Data som kan hentes fra åpne kilder, offentlige registre og lekkasjer (eks. innloggingsdetaljer, bransje- og regulatoriske forhold, virksomhetens størrelse og økonomiske indikatorer).
- Delvis åpen informasjon: Data som krever aktiv teknisk rekognosering (eks. e-poststruktur, eksternt eksponerte tjenester, DNS/IP-informasjon, skytjenester og jobbannonser).
- Skjult informasjon: Data som sannsynligvis først blir tilgjengelig etter et innbrudd (eks. intern nettverksstruktur, Active Directory, patchstatus og sikkerhetsløsninger).

Angripere velger mål der informasjonsgrunnlaget gir lav risiko og høy nytte. Tilgang på teknisk og organisatorisk informasjon reduserer usikkerheten ved et angrep. Aktører med ulik motivasjon vurderer dette forskjellig: statlige aktører søker bred og varig innsikt i strategiske mål, mens kriminelle grupper og tilgangsmeglere fokuserer på mål som kan kartlegges raskt og automatisert. Når åpen og delvis skjult informasjon er lett tilgjengelig, reduseres kostnaden og øker sannsynligheten for at virksomheten blir valgt som mål.

Virksomheter blir mål fordi de fremstår som angripbare, ikke nødvendigvis viktige. Lett tilgjengelig informasjon, mangel på oversikt over eksponerte tjenester, svake sikkerhetstiltak og etterslep på vedlikehold og sikkerhetsoppdatering gjør enkelte virksomheter mer attraktive for angriper – uavhengig av sektor, størrelse eller myndighetsdefinert kritikalitet.

7 Angrepsteknikk

Trusselaktører bruker mange av de samme teknikkene, uavhengig av hvem de er og hva de vil. Angrep kan deles i tre faser: tilgang, bevegelse og iverksettelse, eller "in, through, out". Dette er grunnlaget for "Unified Kill Chain"[24], som er en oppdatert metode som brukes for å beskrive angriperes teknikk og taktikk. Hver av fasene kan igjen deles i flere steg, total 18 i hele kjeden.



Figur 2: Unified Kill Chain

7.1 Tilgang (In)

7.1.1 Direkte teknisk tilgang

Eksponerte tjenester vil sannsynligvis fortsatt være den viktigste inngangsporten[11]. Angrep som utnytter internettvendt utstyr eller tjenester vil øke, både i absolutte tall og andel, av vellykkede kompromitteringer. Trusselaktører skanner åpne porter til å ha oversikt over hvilke muligheter som finnes for direkte angrep.

For kriminelle grupper, og spesielt løsepengegrupper, er angrep mot sårbare eksponerte tjenester det som oftest leder til vellykket kompromittering. Økende bruk av SaaS- og skytjenester gir utvidet angrepsflate. Skytjenester og SaaS er særlig utsatt fordi angrepsflaten vokser jo flere tjenester som settes bort.

VPN og fjerntilgang vil fortsatt være attraktive mål. Slike angrep utnytter både sårbarheter og stjålet legitimasjon, og antallet vellykkede kompromitteringer øker. Ved vellykket kompromittering har angriperen sikret seg fotfeste, og kan bruke tilgangen til videre angrep.

Det er sannsynlig at sårbarheter i perimeterutstyr[5] **blir utnyttet av oppdragsstyrte trusselaktører**. Spesielt aktører som er ute etter umiddelbar effekt, som hacktivister, utnytter ofte at feilkonfigurerte tilgangssystemer gir en mulighet for kompromittering. Slikt perimeterutstyr kan også brukes som inngangsport til videre bevegelse inn i virksomhetenes nettverk.

Flere løsepengegrupper har i høy grad automatisert innbruddsprosessen. Disse har utviklet skanning og integrert sårbarhetsutnyttelse i arbeidsflyten, noe som gir høy suksessrate[25]. Dette er **sannsynligvis** hovedårsaken til at antallet vellykkede angrep mot utstyr og tjenester går opp.

Det er sannsynlig at kompromittering av identitetstjenester (IDP) brukes av oppdragsstyrte aktører for videre tilgang til andre mål. Bruken av identitetstjenester har økt kraftig, særlig i tilknytning til

[5] Brannmurer, VPN-konsentratorer, utstyr direkte tilgjengelig fra internett

skytjenester. Dersom en aktør får tilgang til slike tjenester, kan de skaffe seg videre tilgang til mange kunder. Angrepet på Okta i 2023 er et eksempel på dette.

7.1.2 Sosial manipulering og brukerrettet angrep

Angripere utnytter at brukerkontoer uten MFA[6] kompromitteres enklere og oftere. Dette er en gjentakende inngangsvei for trusselaktører i vårt område og sektorer. KraftCERT ser at små selskaper og leverandører i mindre grad har aktivert MFA, og kan derfor enklere utnyttes. Selv når MFA er aktivert, kan den omgås med teknikker som AitM-phishing[7] eller hvis den har tekniske sårbarheter.

Phishing er i vekst, både i volum og kvalitet[11]. Angrepene blir vanskeligere å oppdage, og KI muliggjør automatisert spearphishing på tvers av målgrupper som er svært vanskelig å oppdage i stor skala[13]. Det benyttes ikke lenger bare e-post og SMS – også krypterte meldingsapper og sosiale medier tas i bruk[26]. Selv om kvaliteten og volumet av phishing går dramatisk opp, går suksessraten ned.

Bruk av KI øker kvalitet, volum og hastighet i tilgangsgruppenes arbeid. Kunstig intelligens brukes til å masseprodusere meldinger og tilpasse phishing-sider, noe som gir raskere leveranse og høyere presisjon. Dette tilbys også som tjeneste i det kriminelle økosystemet[27].

Det er meget sannsynlig at flere og flere aktører aktivt bruker KI for å utvikle mer sofistikerte og tilpassede angrep. KI-hjulpet automatisering av angrepsprosesser brukes til redusere tiden fra tilgang til effekt, noe som kan gjøre deteksjon og forsvar vanskeligere.

7.1.3 Tilgang via leverandørkjeder

Det er sannsynlig at angrep skjer gjennom kompromittering og utnyttelse av leverandører. Kompromitterte selskaper i leverandørkjeden gir en ekstra mulighet for angriper, som skaffer seg viktig informasjon som kan brukes til å spisse phishing-eposter for å høyne troverdigheten. Dersom de finner informasjon om tekniske integrasjoner, kan dette også brukes.

> **Et angrep på BeyondTrust**[28], som leverer bl.a. løsninger for ID-federering og fjerntilgang, ble oppdaget i desember 2024. Flere kundeinstanser for fjernstøtte ble kompromittert, sammen med en API-nøkkel. Angrepet regnes som leverandørbasert tilgang, siden det skjedde hos BeyondTrust – i motsetning til angrepet på Okta, som berørte målorganisasjoner direkte.

7.2 Bevegelse (Through)

Angriperes bevegelse i nettverk skjer gjerne med verktøy som allerede finnes i systemet. Trusselaktører bruker i økende grad legitime programmer og verktøy som er forhåndsinstallert på kompromitterte systemer[11]. Dette omtales som Living off the Land (LOTL), og gir lavere risiko for deteksjon sammenlignet med ondsinnet programvare. Det åpner også for bevegelse mellom soner med ulike sikkerhetsnivå og for å krysse segmentering dersom tiltakene er svake eller fraværende.

Angripere bruker legitime internettverktøy til kommando og kontroll. De har også flere kanaler i bruk samtidig. Løsepengegrupper har for eksempel brukt Cloudflares tunnelfunksjonalitet til å styre skadevare

[6] Multi Factor Authentication, flerfaktorautentisering, tidl. 2FA - tofaktorautentisering
[7] Adversary in the Middle, angriper med automatiserte verktøy logger inn i sanntid med informasjonen som offer taster inn – inkludert multifaktorautentisering.

som AsyncRAT og Xworm[29]. Ved å installere en liten server deamon kan kommunikasjon kjøres via vilkårlig genererte subdomener hos en av internetts store infrastrukturleverandører, noe som gjør at trafikken ser legitim ut.

Ny skadevare utvikles med mål om å unngå analyse og deteksjon. Obfuskering – teknikker for å skjule skadevarens hensikt – og mekanismer som hindrer minneanalyse er nå vanlig. Dette forsinker forsøk på å forstå skadevarens funksjonalitet etter at den er oppdaget. Enkelte grupper lukker også koden etter bruk eller sletter skadevare etter kampanje, noe som vanskeliggjør attribusjon og teknisk etterforskning.[20]

7.3 Iverksettelse (Out)

Utpressingsgrupper kombinerer flere pressmidler[16]. Enkeltangrep kan inkludere:

- krav om betaling for å dekryptere data
- trussel om publisering av stjålne data
- løfte om taushet – at hendelsen ikke varsles til myndigheter eller samarbeidspartnere
- trussel om offentliggjøring av kompromitteringen
- løfte om å ikke gjennomføre nye angrep

Andelen grupper som stjeler data uten å kryptere øker. Dersom utpressing ikke fører frem, kan informasjonen likevel selges videre. Dette krever lavere innsats og innebærer mindre risiko for angriperen, men gir lavere inntjening.

Kryptering er fortsatt den vanligste metoden i utpressingsangrep. Selv om det er flere angrep som ikke krypterer data eller systemer før utpressing, er dette primærmetoden for å tvinge frem betaling fra ofrene.[10]

Utpressingsaktørene har høy grad av automatisering, også i utnyttelsesfasen. De store aktørene har effektivisert hele angrepskjeden. Dette gjør at de kan skalere til å ha mange pågående angrep samtidig. Ransomwareaktøren Cl0p utførte 335 vellykkede kompromitteringer bare i februar 2025[25].

Wipere eller wiperfunksjonalitet finnes ofte i skadevaresuiter[8]. Dette brukes som en siste utvei for utpressingsaktører, som en taktikk for å skjule det egentlige målet med angrepet, eller som metode for å oppnå disruptiv effekt. For statlige aktører er det viktig å skjule denne skadevaren slik at den kan brukes ved et senere tidspunkt.

[8] Skadevare som inneholder flere funksjoner

8 Trusler mot industrielle kontrollsystemer

Driftsforstyrrelser er den mest sannsynlige trusselen mot kontrollsystemer i KraftCERTs sektorer. Slike forstyrrelser kan være et tilsiktet mål, men kan også være en utilsiktet konsekvens av cyberangrep. De kan skyldes direkte angrep på egne systemer, eller være et resultat av hendelser hos leverandører og samarbeidspartnere.

Destruktive angrep er alvorlige, men meget lite sannsynlige på kort sikt. De er krevende å gjennomføre og forutsetter både kapabilitet og detaljert innsikt i målets infrastruktur og tilganger utenfra. Til tross for krig i Europa og økt stormaktsrivalisering, har det vært svært få slike angrep – også i Ukraina, der trusselaktørene har hatt både intensjon og tilgang. [30]

I august 2024 ble Halliburton i USA utsatt for et cyberangrep. De er en internasjonal leverandør med systemer spredt i flere land, inkludert her i Norge. Flere av våre medlemmer benytter seg av tjenester og systemer levert av Halliburton hvor disse er en del av leverandørkjede. En av konsekvensene i Norge var at flere virksomheter koblet seg fra nettverkene og tjenestene til leverandørens kompromitterte systemer. Dette for å isolere egne nettverk og for å hindre videre spredning. Hendelsen viser at systemer i Norge er sårbare som del av et større leverandørkjedeangrep.

8.1 Disruptive angrep og driftforstyrrelser

For en trusselaktør kan disruptive angrep være et mål for å oppnå driftsforstyrrelse, som et ledd i en utpressingssituasjon eller som en bieffekt av et løsepengeangrep. Disruptive angrep rettet mot industrielle kontrollsystemer bør derfor sees på fra ulike perspektiver for å forstå konsekvenser ved cyberangrep.

Driftsforstyrrelser spenner fra total stans til redusert effekt. Det kan være strømutfall eller -avbrudd, stans eller reduksjon i produksjonen eller leveranse, feil ved leveranse eller med produktet. En mildere konsekvens av en driftsforstyrrelse er dersom leveransene gjøres mindre effektive eller mer ressurskrevende pga. bortfall av støttesystemer eller -funksjoner.

Det er mulig at utpressingsangrep rettet mot IT-systemer indirekte fører til driftsforstyrrelser i kontrollsystemet. Angrep med løsepengeskadevare mot egne systemer, samarbeidspartnere eller leverandører kan føre til preventiv isolering av systemer eller nettverksforbindelser til produksjon[31]. Risikoen er særlig høy der det finnes driftsavhengighet eller informasjonsutveksling mellom IT-soner, skytjenester og kontrollsystemet.

Målrettede disruptive angrep fra nasjonalstater mot KraftCERTs medlemmer vurderes som lite sannsynlige på kort sikt. For at en trusselaktør skal kunne planlegge, kartlegge, utvikle destruktiv skadevare for og utføre et målrettet disruptivt angrep, kreves det dyp innsikt i og kunnskap om det utvalgte målet og det konkrete systemet.

8.2 Destruktive angrep

> **Destruktive angrep har som formål** å påføre fysisk skade på infrastruktur, miljø eller mennesker. Denne typen angrep rettet spesielt mot industrielle kontrollsystemer er svært ressurskrevende å gjennomføre. Et målrettet destruktivt angrep med fysiske konsekvenser krever spesialisert kompetanse og tilgang til både kontrollsystem, sikkerhetsfunksjoner og forriglinger – samt evne til å ramme disse samtidig.

Vellykkede destruktive angrep vurderes som meget lite sannsynlige det neste året. Selv under krigen i Ukraina har russiske aktører ikke klart å gjennomføre cyberangrep med direkte destruktive konsekvenser for strømforsyning eller industriell produksjon. I forkant av krigen gjennomførte de et angrep på kommunikasjonsutstyr (KSAT/Viasat-modemene) som satte enhetene varig ut av spill. Wipere ble brukt til å slette innhold og hindre gjenoppretting [32].

Så lenge Norge står utenfor væpnet konflikt, vurderes slike angrep som meget lite sannsynlige. Vurderingen er på linje med KraftCERTs analyser i både 2023 og 2024. Målrettede destruktive cyberangrep mot industrielle kontrollsystemer krever store ressurser[33].

> **Destruktive angrep mot industrielle kontrollsystemer** er svært teknisk vanskelig og ressurskrevende å gjennomføre fordi større kontrollsystemer er beskyttet med et eller flere separate safetysystem. Safetysystemer gjør at vanskelighetsgraden for et destruktivt angrep øker betydelig. I motsetning til disruptive angrep, vil et destruktivt angrep mot industrielle kontrollsystemer kreve samtidig deaktivering av safety-system og styring av prosess[a].
>
> [a] KraftCERTs Trusselvurdering 2023[34] (Kun tilgjengelig for medlemmer eller ved forespørsel)

Det er meget sannsynlig at trusselaktører søker å etablere bakdører som kan brukes i senere angrep. Dette er en teknikk for preposisjonering, der aktøren etablerer og vedlikeholder tilgang før angrepsøyeblikket. I Ukraina i 2022 forsøkte russiske aktører dette tidlig i konflikten, men endret senere taktikk til enklere disruptive angrep mot kontrollsystemer.

> **Volt Typhoon viser hvordan statlige trusselaktører kan kartlegge OT-systemer over lang tid.** Denne kinesisk-tilknyttede aktøren eksfiltrerte informasjon om en rekke OT-systemer i USA, særlig innen vannsektoren, og oppholdt seg i systemene i over 300 dager[11]. Kartlegging som dette kan senere muliggjøre både spionasje og målrettede angrep, og det går i praksis ikke å skille mellom de ulike formålene mens aktiviteten pågår[35].

Trusselaktøren innhenter teknisk informasjon for å planlegge angrep. Det er **meget sannsynlig** at statlige aktører forsøker å skaffe adresseringsdata og detaljer som nettverkstegninger, kontrolltrafikk-konfigurasjoner, topologier, IP-oversikter og brannmurkonfigurasjon. Denne typen informasjon reduserer behovet for rekognosering og gjør det enklere å utvikle skadevare tilpasset målet. Slike data kan finnes i virksomhetens egne IT- og dokumentsystemer, hos leverandører eller i dokumenter brukt i prosjekter og anbud.

8.3 Trusselaktørers teknikker og skadevare

Det er lite sannsynlig at trusselaktører angriper industrielle kontrollsystemer direkte med løsepengeskadevare. Internasjonalt er det ingen tegn på at slike systemer har vært mål for direkte løsepengeangrep. Det er likevel **mulig** med OT-nære løsepengeangrep, brukt som del av et bredere disruptivt angrep[37][38].

> **EKANS er det siste kjente eksemplet på løsepengeskadevare rettet mot OT-funksjoner.** Skadevaren ble brukt i 2020 og hadde innebygd kode for å påvirke komponenter som webbasert HMI, historian-servere og lisensservere[36]. Det er ikke observert tilsvarende skadevare siden.

Det er meget sannsynlig at trusselaktører utnytter svak segmentering mellom IT og OT for å få tilgang til kontrollsystemer. Når soneskiller er mangelfulle, kan angrep som starter i IT-sonen utnytte disse svakhetene og føre til konsekvenser også for kontrollsystemet. Økt datautveksling og usikrede fjernpåloggingsløsninger forsterker risikoen.

Det er sannsynlig at trusselaktører forsøker å utnytte fjerntilgang og tekniske grensesnitt mot kontrollsystemet. Behov for ekstern drift og datadeling har ført til flere sammenkoblinger mellom kontrollsystem og andre systemer, både internt og eksternt. Disse grensesnittene kan være teknisk sårbare, og samtidig ha høy betydning for drift. Et angrep – eller mistanke om angrep – kan gi driftsforstyrrelser, eller føre til at forbindelsen kobles fra som et forebyggende tiltak.

Det er meget sannsynlig at trusselaktører forsøker å utnytte IIoT i kontrollsystemers nettverk. Dersom en angriper har kommet seg innenfor perimeter, vil de søke å skaffe seg fotfeste for videre bevegelse ved å angripe de enhetene som er mest sårbare. IIoT-enheter har sjeldent tilstrekkelige overvåkings- og sikkerhetsfunksjoner, og er vanskelige å patche pga. sin posisjon i nettverket. Dette gjør at de er verdifulle mål for trusselaktører.

Det er sannsynlig at trusselaktører bruker LotL-teknikker for å unngå deteksjon i kontrollsystemsonen. Økt overvåking, hvitlisting og bedre kontroll gjør det vanskeligere for en trusselaktør å bruke tradisjonell skadevare. Dette øker insentivet til å benytte legitime verktøy og prosesser som allerede finnes i systemet. Mange industrielle kommunikasjonsprotokoller mangler mekanismer for å verifisere avsender. Det er **meget sannsynlig** at angripere vil forsøke å utnytte dette til å sende kommandoer ved å forfalske avsenderadresser. Slik trafikk fremstår som normal, og kan passere uoppdaget i overvåkingssystemer [31].

Det er mulig at målrettede trusselaktører vil prøve å bruke USB-pinner for å plante skadevare i kontrollsystemer. Selv svært beskyttede systemer kan fortsatt infiseres på denne måten. Metoden krever imidlertid lang planlegging og fysisk tilgang, og er derfor kun aktuell for aktører med spesifikke mål, mye ressurser og høy risikovilje[39][40].

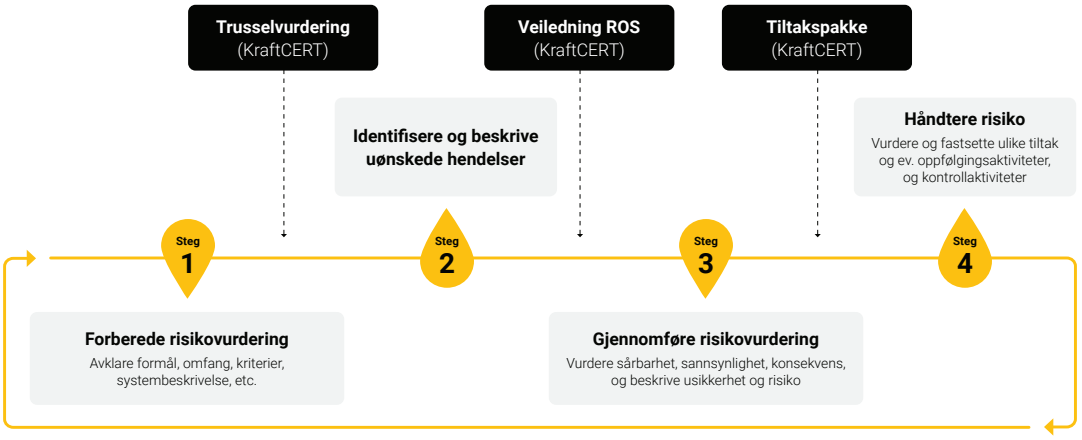
> **FrostyGoop er et eksempel på skadevare som utnytter manglende autentisering i kontrollsystemer.** Den ble demonstrert i Ukraina, april 2024 og brukte en standardisert industriell protokoll (Modbus TCP) til å sende kommandoer i kontrollsystemet uten å bli verifisert. [38]

Det er sannsynlig at skadevare introduseres via engineering-laptoper. Slike maskiner brukes til vedlikehold og konfigurasjon av kontrollsystemer, og eies ofte av leverandør. De kan mangle grunnsikring, benyttes på usikrede nettverk, og kobles deretter direkte til utstyr i kontrollsystemsonen. De overvåkes sjelden, og representerer derfor en reell angrepsflate. [41] [38]

9 Om rapporten

9.1 Trusselvurdering og tiltakspakke

Trusselvurderingen følges opp med en tiltakspakke for medlemmer høsten 2025. Den vil gi praktiske anbefalinger og søke å besvare hvordan truslene best kan møtes. Sammen kan disse bidra til virksomhetens ROS.

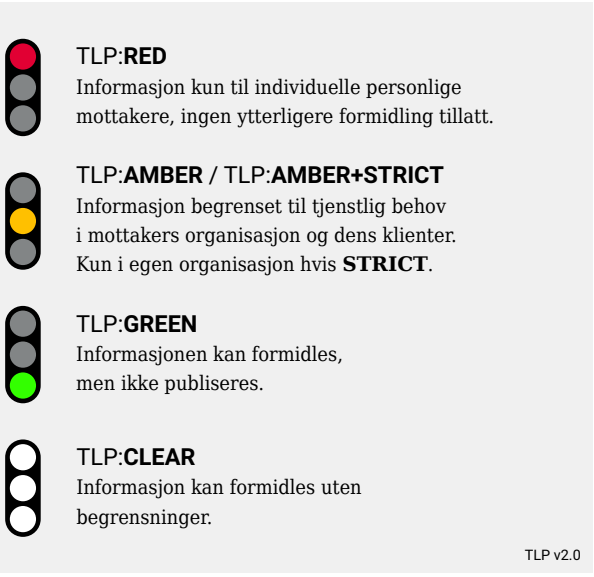


9.2 Trafikklysprotokollen

KraftCERT/InfraCERT bruker trafikklysprotokollen (TLP versjon 2.0) ved deling av informasjon for å angi hvordan informasjonen kan eller ikke kan deles videre.

Dette dokumentet er klassifisert som TLP:CLEAR. Informasjonen kan distribueres uten begrensninger.

Les mer om trafikklysprotokollen hos FIRST[9]



9.3 Endringslogg

Dato	Versjon	Beskrivelse
2025-05-05	1.0.0	Første versjon
2025-05-09	1.1.0	Rettet sannsynlighet

[9] https://www.first.org/tlp

Referanser

[1] Politiet. *Cyberkriminalitet 2025*. 10. feb. 2025. URL: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf.

[2] Google Cloud. *Cybercrime: A Multifaceted National Security Threat*. 15. feb. 2025. URL: https://services.google.com/fh/files/misc/cybercrime-multifaceted-national-security-threat.pdf.

[3] Etterretningstjenesten. *Fokus 2025*. 4. feb. 2025. URL: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2025%5C%20-%5C%20NO%5C%20-%5C%20Weboppslag%5C%20v4.pdf/.

[4] Nasjonal sikkerhetsmyndighet. *Risiko 2025*. 5. feb. 2025. URL: https://www.regjeringen.no/contentassets/6290dec36c374ee191e5c7dbba18a258/risiko-2025.pdf.

[5] Politiet. *Nasjonal trusselvurdering 2025*. 5. feb. 2025. URL: https://pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf.

[6] Forsvarets forskningsinstitutt. *Forsvarsanalysen 2025*. 17. feb. 2025. URL: https://www.ffi.no/publikasjoner/forsvarsanalysen-2025.

[7] Nasjonal sikkerhetsmyndighet. *Risiko 2024*. 12. feb. 2024. URL: https://nsm.no/getfile.php/1313477-1707733210/NSM/Filer/Dokumenter/Rapporter/Risiko%5C%202024.pdf.

[8] Center for Cybersikkerhed. *Cybertruslen mod vandsektoren*. 22. jan. 2025. URL: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/CFCS-cybertruslen-mod-vandsektoren-2025.pdf.

[9] ANSSI. *Secteur de l'eau : état de la menace informatique*. 28. nov. 2024. URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-011/.

[10] Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. 14. jan. 2025. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

[11] IBM Security. *IBM X-Force 2025 Threat Intelligence Index*. 17. apr. 2025. URL: https://www.ibm.com/downloads/documents/us-en/1227cc9e83cb97ae.

[12] Verizon Business. *2025 Data Breach Investigations Report*. 21. apr. 2025. URL: https://www.verizon.com/business/resources/T20f/reports/2025-dbir-data-breach-investigations-report.pdf.

[13] Fortinet. *Cyberthreat Predictions for 2025*. 1. des. 2024. URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-prediction-2025.pdf.

[14] U.S. Department of Homeland Security. *DHS' 2025 Homeland Threat Assessment Indicates the Threat of Domestic and Foreign Terrorism in the Homeland Remains High*. 14. jan. 2025. URL: https://www.dhs.gov/news/2024/10/02/dhs-2025-homeland-threat-assessment-indicates-threat-domestic-and-foreign-terrorism.

[15] Google Cloud. *M-Trends 2025*. 21. apr. 2025. URL: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf.

[16] Recorded Future. *RansomHub Draws in Affiliates with Multi-OS Capability and High Commission Rates*. 20. jun. 2024. URL: https://www.recordedfuture.com/research/ransomhub-draws-in-affiliates-with-multi-os-capability-and-high-commission-rates.

[17] Crowdstrike. *2025 GLOBAL THREAT REPORT*. 27. feb. 2025. URL: https://www.crowdstrike.com/explore/2025-global-threat-report.

[18] Recorded Future. *4 Main Threat Actor Types Explained for Better Proactive Defense*. 14. jan. 2025. URL: https://www.recordedfuture.com/threat-intelligence-101/threat-actors/threat-actor-types.

[19] Trend Micro. *Breaking Down Earth Estries Persistent TTPs in Prolonged Cyber Operations*. 8. nov. 2024. URL: https://www.trendmicro.com/en_no/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html.

[20] Mandiant. *M-Trends 2024: Our View from the Frontlines*. 14. jan. 2025. URL: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024.

[21] NSR. *Mørketallsundersøkelsen 2024*. 13. mar. 2025.

[22] ENISA. *ENISA Threat Landscape 2024*. 20. sep. 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024/@@download/fullReport.

[23] TechCrunch. *How the ransomware attack at Change Healthcare went down: A timeline*. 27. jan. 2025. URL: https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline.

[24] CyberEngage. *Unified Kill Chain: An evolution of Cyber Kill chain*. 7. des. 2024. URL: https://medium.com/@cyberengage.org/unified-kill-chain-an-evolution-of-cyber-kill-chain-0e06cba94432.

[25] HackRead. *Ransomware Hits Record High: 126% Surge in Attacks in February 2025*. 13. mar. 2025. URL: https://hackread.com/ransomware-attacks-hit-record-high-in-february-2025.

[26] Hacker News. *CERT-UA Warns Dark Crystal RAT Targets Ukrainian Defense via Malicious Signal Messages*. 20. mar. 2025. URL: https://thehackernews.com/2025/03/cert-ua-warns-dark-crystal-rat-targets.html.

[27] Cyber Threat Alliance. *CYBER THREAT ALLIANCE PUBLISHES 2025 CYBERSECURITY IN THE AGE OF GENERATIVE AI*. 14. jan. 2025. URL: https://www.cyberthreatalliance.org/cyber-threat-alliance-publishes-2025-cybersecurity-in-the-age-of-generative-ai.

[28] Hacker News. *BeyondTrust Zero-Day Breach Exposed 17 SaaS Customers via Compromised API Key*. 1. feb. 2025. URL: https://thehackernews.com/2025/02/beyondtrust-zero-day-breach-exposes-17.html.

[29] BleepingComputer. *Hackers abuse free TryCloudflare to deliver remote access malware*. 1. aug. 2024. URL: https://www.bleepingcomputer.com/news/security/hackers-abuse-free-trycloudflare-to-deliver-remote-access-malware/.

[30] Mandiant. *APT44: Unearthing Sandworm*. 17. apr. 2024. URL: https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf.

[31] Waterfall. *2025-OT-Cyber-Security-Threat-Report*. 21. mar. 2025.

[32] Dragos. *The Destructive Wipers from the Ukraine-Russia Conflict*. 16. mar. 2023.

[33] KraftCERT. *Trusselvurdering 2024*. 21. jun. 2024.

[34] KraftCERT. *Trusselvurdering 2023*. 10. jun. 2023.

[35] Security week. *China's Volt Typhoon Hackers Dwelled in US Electric Grid for 300 Days*. 12. mar. 2025. URL: https://www-securityweek-com.cdn.ampproject.org/c/s/www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days/amp/.

[36] Dragos. *EKANS Ransomware and ICS Operations*. 3. feb. 2020. URL: https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations.

[37] Nozomi Networks. *Nozomi-Networks-OT-IoT-Security-Report-January-2025*. 18. feb. 2025.

[38] Dragos. *2025 OT Cybersecurity Report: A Year in Review*. 25. feb. 2025.

[39] Norma Cyber. *Årlig trusselvurdering 2025*. 25. mar. 2025. URL: https://static1.squarespace.com/static/5fae4682cc2b52123f436f99/t/67ea8ab08ba25a5706a8cd33/1743424201283/Norma+Cyber+%5C%C3%5C%A5rlig+trusselvrudering.pdf.

[40] Dark Reading. *'The Weirdest Trend in Cybersecurity': Nation-States Returning to USBs*. 7. mar. 2024. URL: https://www.darkreading.com/ics-ot-security/weirdest-trend-cybersecurity-nation-states-usb.

[41] Forescout. *ICS Threat Analysis: New, Experimental Malware Can Kill Engineering Processes*. 17. des. 2024. URL: https://www.forescout.com/blog/ics-threat-analysis-new-experimental-malware-can-kill-engineering-processes/.

Tillegg

A Ordliste

AitM *Adversary in the Middle*. Teknikk for omgåelse av multifaktorautentisering for pålogging. Side 13.
CaaS *Crimeware as a Service*. Skadevare levert som en skytjeneste (SaaS) for angripere, vanligvis RaaS. Side 9.
IAB *Initial Access Broker*. Tilgangsmegler. Side, *se også* Tilgangsmegler.
IAG *Initial Access Group*. Tilgangsgruppe som spesialiserer seg på å skaffe tilgangsinformasjon for å kunne videreselge direkte eller til en IAB. Side 9, 13, *se også* IAB.
IDP *Identitetstjeneste*. Leverandør av tjeneste for identifisering og autentisering av brukere, gjerne over Internett. Side 12.
IIoT *Industrial Internet of Things*. Utstyr (sensorer, brytere, osv) benyttet i selskapenes nettverk. Side 17.
LotL *Living off the Land*. Betegnelse på når angriper benytter de verktøy hen har for hånden i nettverket der de har brutt seg inn, lokalt eksisterende systemverktøy. Side 17.
RaaS Ransomware as a Service. Side 9, 21.
RecaaS *Reconnaissaince as a Service*. Aktørgruppe som spesialiserer seg på informasjonsinnhenting, enten fa åpne kilder og/eller spionasjeoperasjoner. Side 9.
SaaS *Software as a Service*. Programvare som skytjeneste for bruk over Internett. Side 12.
Tilgangsmegler Aktør som videreselger stjålne tilganger til systemer. Side 9.
Wiper Programvare spesifikt laget for å permanent slette data. Side 14.