kraftCERT infraCERT

Trusselvurdering 2024

Innhold

Sammenfatning av KraftCERTs trusselvurdering

Det er sannsynlig at virksomheter i våre sektorer utsettes for angrep med driftsforstyrrende effekt. Det er meget lite sannsynlig at det på kort sikt skjer vellykkede destruktive angrep. Likevel er det meget sannsynlig at nasjoner og oppdragstyrte aktører kontinuerlig forsøker å utvikle evne til slike destruktive angrep. Manglende kontroll på informasjon i virksomhetene vil gjøre dette arbeidet lettere for dem.

Det vil komme leverandørangrep fremover, spørsmålet er hvilke konsekvenser det får for det enkelte selskap. Utpressingsangrep vil fremdeles være angrepsformen med mest omtale og konsekvenser, og LOTL (leve av lendet) vil fortsette å være en foretrukket teknikk. Hacktivister har lite potensiale for å oppnå alvorlige konsekvenser, selv om det er sannsynlig at det vil forekomme tjenestenektangrep i KraftCERTs sektorer.

1 Introduksjon

Velkommen som leser av KraftCERTs Trusselvurdering 2024. Før vi presenterer vår analyse, vil vi komme med noen meninger.

Verden blir farligere, men ikke så farlig som det noen ganger kan virke. Det er mange som har interesse av å fortelle deg at «Alt er farlig». KraftCERTs ambisjon i trusselvurdering er å gi en nøktern analyse av trusselbildet for våre medlemmer, uten kommersielle eller politiske bindinger. Det er lagt til grunn et stort antall kilder og observasjoner.

En lang rekke kilder hevder noe om cybertrusselbildet, for eksempel påstander om utvikling som har vært og utvikling som kan forventes fremover. Mange private selskap utgir trusselrapporter, og det benyttes ulike metoder, begrep, kategoriseringer, utvalg av hendelser osv. til å beskrive trusselbildet. Ofte er det uklart hvilke data påstander bygger på, og hvor troverdige og representative dataene er. Noen ganger er det motstridende påstander i ulike kilder, også i myndighetenes vurderinger. Samlet utgjør dette en betydelig utfordring for analysearbeidet.

KraftCERT er noen ganger uenige med myndigheters påstander. I NSM-rapporten *Risiko 2024* [1] kan man lese at en cyberoperasjon mot energisystemer i Ukraina førte til strømutfall i store områder i februar 2023. KraftCERT mener dette ikke er tilfelle. Det er uheldig at slike påstander blir presentert uten underlag. Det utfordrer vår felles situasjonsforståelse.

Innsidetrusselen er høyaktuell, men det er lett å blande begrep; utilsiktede feil er ikke det samme som spionasje. Ved å blande sammen disse begrepene står virksomheter i fare for å ikke kunne håndtere hverken normale feil eller faktisk innsidetrussel, fordi virkemidlene ikke er de samme.

Den enkelte trusselaktør er sjelden relevant som vurderingsgrunnlag. Både kommersielle og andre som vurderer trusselbildet beskriver ofte enkeltaktører. Det er svært sjelden disse opplysningene gir merverdi. Siste nytt om enkeltaktører har liten verdi om det ikke settes sammen til en vurdering av hva det betyr for utvikling av skadevare og angrepsformer i fremtiden.

Til slutt en oppfordring: Ta kontakt ved mistanke om angrep, angrepsforsøk og relevante hendelser. KraftCERTs medlemmer kan bidra til å utvikle og opprettholde et felles trusselbilde i sektorene gjennom å dele informasjon med KraftCERT.

God lesing!

Figur 1: Sammenheng mellom vurderinger

2 Om rapporten

2.1 Beskrivelse

Dette dokumentet er en rapport fra KraftCERT/InfraCERT, og deles med utvalgte samarbeidspartnere. Rapporten skal gi KraftCERTs medlemmer og sektorer en vurdering og forståelse av relevante trusler og deres utvikling, og beskriver hva KraftCERT mener om trusselbildet nå og fremover. Dette mener vi gir virksomheter grunnlag for å gjøre lokale vurderinger (se figur 1 på forrige side).

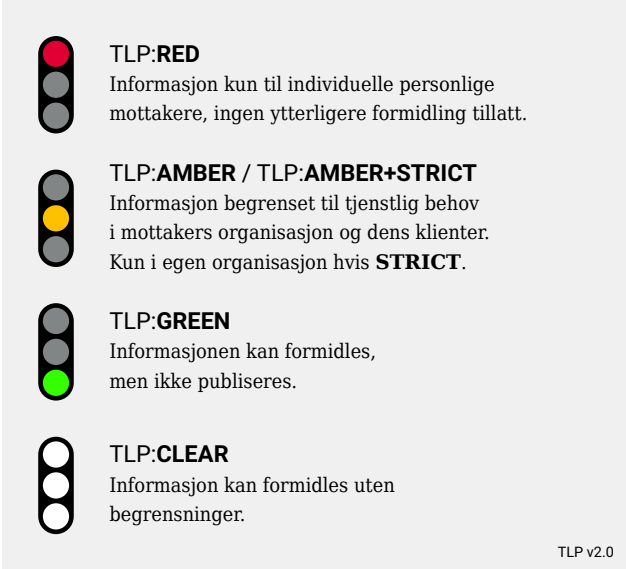
Spørsmål eller kommentarer kan sendes `cert@kraftcert.no`.

Endringslogg:

Dato	Versjon	Beskrivelse
2024-06-17	1.0.0	Første versjon

Forsidebilde: Ryssdalsnebba sett fra Trolltinden. © 2024 Ketil Elgethun

2.2 Trafikklysprotokollen



Figur 2: Trafikklysprotokollen

KraftCERT/InfraCERT benytter seg av 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[1] og NCSC[2].

[1] https://www.first.org/tlp
[2] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/kontakt-ncsc/retningslinjer-for-deling-av-informasjon/

3 Overordnede trusselvurderinger

3.1 Nasjonale vurderinger

Etterretningstjenesten [2] mener tjenestenektangrep fra pro-russiske aktører er sannsynlig, og at russiske aktører søker informasjon om energi-sektoren. PST [3] nevner at energi er en av mange sektorer som er mål for statlige aktørers cyberoperasjoner. NSM [1] mener at cybersikkerheten blir utfordret av «stadig mer avanserte cyberoperasjoner», og at «Kritisk infrastruktur må skjermes mot innsyn og påvirkning». Kripos [4] registrerer «en økning innen alle [cyberkriminalitets-]områder, med unntak av digitalt skadeverk som holder seg på et stabilt nivå», men påpeker at det er «større usikkerhet knyttet til mengden cyberrettet kriminalitet». Politiet [5] melder at «Den teknologiske utviklingen bidrar til å skape et utvidet handlingsrom for cyberkriminelle aktører».

3.2 KraftCERTs egne vurderinger

3.2.1 Cybertrusler mot virksomheter i Norge og på Island

Det er lite sannsynlig at norske og islandske[3] virksomheter er høyt prioriterte mål for trusselaktører/cyberangrep per i dag. Norge og Island trekkes ikke fram i analyser over hvilke land trusselaktører retter seg mot. Tvert i mot er Norge og Island langt nede på listen over land som opplever cyberangrep (se f.eks. [6], [7], [8]). USAs årlige trusselvurdering [9] mener lavinntektsland er mer attraktive for cyberkriminalitet pga. pågående digitalisering i kombinasjon med mangelfulle sikkerhetstiltak. Unntaket er tjenestenektangrep. Flere norske og islandske virksomheter erfarte tjenestenektangrep i 2023, og KraftCERT mener at slike angrep også vil forekomme i det kommende året.

Det kan komme endringer som påvirker Norge og Islands trusselbilde, for eksempel endringer i internasjonal politikk (som nordområdene), Ukraina-krigen, eller andre konflikter. Hvilke endringer som påvirker trusselbildet innen cyber på kort sikt er vanskelig å identifisere i dag.

3.2.2 Statlige og statstilknyttede aktører

Det er meget sannsynlig at Kina og Kina-tilknyttede aktører har en betydelig evne og vilje til industrispionasje, og til å unngå deteksjon. For KraftCERTs medlemmer betyr det i hovedsak industrispionasje mot utsatte områder som forskning og utvikling. Den Kina-tilknyttede aktøren Volt Typhoon har fått stor oppmerksomhet i 2023 og 2024. Trusselaktøren illustrerer utfordringer både med deteksjon, og at aktøren arbeider med lang tidshorisont. KraftCERT kjenner ikke til at saken har hatt konsekvenser i Norge eller på Island. (mer om aktører i kapittel 6 på side 13).

Cyberangrep med destruktive konsekvenser er lite sannsynlig fra Russland og Russland-tilknyttede trusselaktører. Aktørene utgjør trusler mot kritisk infrastruktur. Både PST og E-tjenesten mener trusler fra Russland mot norsk infrastruktur i petroleum- og gasseksport er vedvarende, men slik KraftCERT forstår rapportene er det i hovedsak knyttet til fysiske angrep/sabotasje. Cybertrusselen mot norske og islandske virksomheter fra Russland og Russland-tilknyttede aktører er stabil. Mange aktører er opptatt i krigen mot Ukraina, og retter oppmerksomhet mot systemer som er viktige for Ukraina eller for hjelp til Ukraina (mer om destruktive angrep i kapittel 7 på side 14).

[3] KraftCERT har medlemmer i Norge og på Island

3.2.3 Angrep og hendelser i KraftCERTs medlemssektorer

Det er meget sannsynlig at kraft- og petroleumssektorene vil bli indirekte berørt av angrep i leverandørkjeder, på kort og mellomlang sikt (1-3 år). Kraft- og petroleumssektorene består av mange leverandører og lange leverandørkjeder. Angrep på leverandørkjeder har vært omtalt i flere år (ref. [10]). Leverandørangrep inkluderer både utstyrsleverandører og leverandører av digitale tjenester og systemer (f.eks. skytjenester). Oversikter over cyberhendelser viser at produksjonsbedrifter ofte er utsatte mål, og på toppen av oversikter over hendelser[4]. Mange leverandører vil falle inn under denne kategorien. Alle typer leverandører kan bli truffet av cyberangrep. Det er avgjørende at virksomheter har oversikt over og forstår leverandørkjeder for digitale og ikke-digitale leveranser, og hvilke leverandører som er kritiske for virksomheten.

Det er lite sannsynlig at kraft- og petroleumssektorene blir direkte rammet av større cyberhendelser. NSM påpeker potensialet i at cyberoperasjoner «kan i verste fall føre til alvorlige fysiske skader på kritisk infrastruktur og personell», og nevner spesielt «styring og kontroll av kraftproduksjon, kraftdistribusjon samt produksjon og leveranse av olje og gass». Kraft og petroleum, eller «energi», er ofte langt nede på oversikter over sektorer som erfarer hendelser, og typisk med andel på mellom 4-12% av hendelser. Det viser for eksempel NSMs oversikt over hendelser i Norge [1], og ENISAs oversikt over hendelser i Europa [17], og lignende oversikter fra private selskaper[5]. Selv om nasjonale myndigheter over tid har pekt på kraft og petroleumssektorene som utsatte mål for cyberangrep, gjenspeiles ikke dette i statistikk og oversikt over hendelser.

KraftCERT har medlemmer fra en rekke sektorer med kritisk infrastruktur. Nylig har det vært mye fokus på økende cyberangrep mot drikkevannssystemer i USA, eksempelvis fra Environmental Protection Agency [18]. KraftCERT har ikke nok informasjon til å si noe om hvor mange hendelser eller hvordan angrepene har utviklet seg i vann og avløp, i Norge eller på Island.

[4] mange selskaper presenterer oversikter over sektorer og angrep, se f.eks. Dragos - *OT Cybersecurity The 2023 Year in review* [11], Microsoft - *Digital Defence Report 2023* [7], Palo Alto - *Incident Response Report 2024* [12], Artic Wolf - *2024 Threat Report* [13], GRF - *Semi annual Ransomware Report H2 2023* [8], Waterfall - *2024 Threat Report* [14], Crowdstrike - *2024 Global Threat Report* [15], IBM Security - *Threat Intelligence Index 2024* [16]

[5] Se fotnote 4

4 Utnytting av personell

4.1 Utnytting av innsidere

Med innsider menes personer som utnytter legitime tilganger til virksomhetens verdier for ondsinnede formål, på vegne av seg selv eller andre.

På kort sikt er det lite sannsynlig at innsidetrusselen øker for våre medlemmer. Nasjonale myndigheter har i mange år advart om innsidetrusselen (eller innsiderisiko/innsidevirksomhet). Særlig Russland og Kina blir trukket frem som stater som forsøker å rekruttere innsidere i norske virksomheter, også digitalt. PST rapporterer om at fremmede etterretningstjenesters bruk av sosiale medier og chatteapplikasjoner er et utviklingstrekk. I NSMs *Risiko 2024* [1] og *Nasjonalt digitalt risikobilde 2023* [19] trekkes innsidetrusselen frem som stadig viktigere, og at bedre cybersikkerhet vil øke betydning av personer på innsiden av norske virksomheter.

KraftCERT mener det er svakt grunnlag for å hevde at innsidetrusselen har økt. ENISAs trusselrapport inkluderer ikke innsidere som trussel på grunn av «exceptionally small number of publicly reported incidents» [17], Det er også få kjente hendelser eller straffesaker med innsidere i Norge. Innsidetrusselen og hvilke faktorer som driver innsidere er også svært sammensatt, og et område med begrenset kunnskapsgrunnlag (se f.eks. [20]).

Fremmede makters reelle evne til å rekruttere og utnytte innsidere kan være lavere enn før på grunn av høy oppmerksomhet og årvåkenhet. KraftCERT har fått flere spørsmål om innsidetrusselen og erfarer at medlemmers årvåkenhet er høy der innsidetrusselen er mest relevant. På samme tid er det et tema som er vanskelig å få innsikt i, og det finnes få klare svar eller føringer fra myndighetene. Ofte må ulike hensyn veies mot hverandre, for eksempel ved tilsettingsprosesser. Virksomheter må vurdere risiko, og navigere mellom behov for kompetanse og krav i ulike lover.

Det er meget sannsynlig at fremmede makters ønske om å utnytte innsidere vil øke når politiske konflikter og økonomisk konkurranse skjerpes. En trusselvurdering er et øyeblikksbilde, og endringer kan påvirke innsidetrusselen for KraftCERTs medlemmer. En virksomhet innen forsvarsteknologi eller som leverer utstyr til Ukraina har et annet trusselbilde enn de fleste av KraftCERTs medlemmer. Per nå er det vanskelig å se pågående eller potensiell konflikt eller økt økonomisk konkurranse som i betydelig grad påvirker fremmede makters ønske om å utnytte innsidere hos KraftCERTs medlemmer.

Innsidere kan gi muligheter for trusselaktører, men det kan også variasjon i menneskelig atferd.

4.2 Utnytting av variasjon i menneskelig atferd

Det er sannsynlig at trusselaktører i økende grad vil søke å utnytte variasjon i menneskelig atferd og ytelse, herunder å gjøre feil. I KraftCERTs *Trusselvurdering 2023* sto det at cybersikkerhet handler om mer enn ondsinnede handlinger. PST mener at flere cyberaktører «utnytter i større grad det menneskelige aspektet» [3]. NSM skriver at «ubevisste innsidere» er ansatte som åpner vedlegg med skadevare, feilaktig videreformidler data, eller «skjødesløst lar være å forholde seg til sikkerhetskrav og sikkerhetsoppdateringer» [19], og at disse står for over halvparten av innsidehendelser mot digitale verdier. KraftCERT mener NSM blander sammen ulike fenomener.

Innsidere som gjør tilsiktede handlinger, og variasjon i menneskelig atferd (med utilsiktede konsekvenser) er to ulike fenomener. Innsidetrusselen kan for eksempel reduseres med sikkerhetsklarering av personell, men det er ikke et tiltak for å redusere sannsynlighet for at feil og uhell kan skje. Det finnes også atferd som er grovt uaktsom. Figur 3 på neste side illustrerer forskjeller mellom de tre: Innsider, menneskelig variasjon i

atferd, grov uaktsomhet og gråsoner mellom disse. Felles for alle er at det kan gi trusselaktører muligheter til angrep, og at trusselaktører stadig utvikler måter å utnytte mennesker på. Gråsoner gjør dette ekstra utfordrende. Å ha ansatte betyr variasjon og at feil kan skje. Mennesker kan ikke «patches» på samme måte som digitale systemer.

Figur 3: Trusselaktørs utnytting av personell på innsiden

5 Angrepsformer

5.1 Utpressingsangrep

Utpressingsangrep er den vanligste angrepsformen globalt sett, og det er meget sannsynlig at volumet av disse vil øke. Utpressingsangrep har i flere år vært en topp-trussel, bl.a. i ENISAs årlige vurderinger [17]. Kripos viser i *Cyberkriminalitet 2024* [4, s.12] til en liten nedgang i antall anmeldte saker med løsepengevirus i Norge. Selv om vi i Norge har lite øvrig statistikk omkring cyberkriminalitet, vurderer KraftCERT utpressingsangrep som den mest sannsynlige angrepsformen å bli utsatt for, også i Norge.

Utpressing uten kryptering - hvor trusselen om offentliggjøring av sensitive data er grunnlaget for utpressingen - vil meget sannsynlig øke, men ikke overta majoriteten av angrep. Palo Alto Unit42 [21] skriver om BianLian, som eksemplifiserer denne formen for utpressing.

Selv om slike angrep stort sett alltid er rettet mot IT-systemer, kan det ha innvirkning på produksjon og leveranser når IT-systemene blir berørt. Et eksempel kan være at hvis logistikk- eller bestillingssystemer (som gjerne er en del av IT-systemene) blir rammet, kan det bli vanskelig eller umulig å få utført produksjon og leveranse av produkter og tjenester. KraftCERT anser at dette er den mest sannsynlige trusselen mot kontrollsystemer. Se også kapittel 7 på side 14.

De aller fleste utpressingsangrep er opportunistiske; de(n) som angriper finner en vei inn, og utnytter denne om det ser ut til å være lønnsomt for trusselaktøren.

Det er sannsynlig at mindre virksomheter vil bli vesentlig mer utsatt for vellykkede krypteringsangrep enn store, fordi større virksomheter har større ressurser til å forbedre sine forsvarstiltak. Dette er en trend som har vært observert av bl.a. Microsoft [7, s.18].

5.2 Hacktivisme

Det er sannsynlig at KraftCERTs medlemmer vil bli utsatt for hacktivisme, men at dette i liten grad vil ha skadevirkninger av betydning for de berørte. Hacktivisme gir seg gjerne utslag i tjenestenektangrep, og vandalisering av nettsider, noe som i de fleste tilfeller er ubeleilig, men ikke kritisk for virksomheten. Et unntak fra dette vil være virksomheter hvor tilgjengelighet på Internett faktisk er kritisk for forretningsdriften.

Det er lite sannsynlig at norske og islandske virksomheter vil være hovedmål for hacktivisters aksjoner. Derimot vurderer KraftCERT det som sannsynlig at hacktivister vil forsøke å gjennomføre angrep på leverandører av tjenester, teknologi og produkter, noe som også kan ha innvirkning på KraftCERTs medlemmer. Et eksempel er angrepene mot styringssystemer fra Unitronics som ble utført høsten 2023 - disse angrepene fikk mye omtale, men hadde ingen større skadeeffekter[6].

5.3 Kunstig intelligens og phishing

Siden *Trusselvurdering 2023*[10] har kunstig intelligens blitt et stort tema generelt, ikke minst innen cybersikkerhet.

KraftCERT mener det er meget sannsynlig at KI vil gjøre phishing mer sofistikert, at phishing i økende grad vil være assistert av KI, og at det blir vanskeligere å avdekke for brukeren.

[6] se for eksempel CISAs rapport om disse angrepene [22].

NCSC UK [23] mener rekognosering og sosial manipulering sannsynligvis vil påvirkes av KI de nærmeste to år , og at flere aktørtyper vil ta det aktivt i bruk. Særlig lavkost leiehackere, opportunistiske cyberkriminelle og haktivister[7] vil øke kapasitet innen phishing o.l. Microsoft/OpenAI har identifisert flere trusselaktørers bruk av KI til for eksempel forbedring av spear-phishing.

Sosial manipulering og phishing vil fortsatt være foretrukne tilgangsmetoder for trusselaktører. Disse krever relativt liten innsats, og med KI som assistent vil kapasiteten deres øke. Her er det verdt å sitere NSM [1] på at «Alle mennesker kan bli lurt i et svakt øyeblikk, selv den mest årvåkne» . Flere undersøkelser tyder på at det blir vanskelig å skille KI-generert og menneskapt kommunikasjon (f.eks. undersøkelse av IBM X-force [25]). Bruk av KI til phishing er identifisert som en trend av flere sikkerhetsselskaper.

Det er meget sannsynlig at bruken av QR-koder øker i forbindelse med phishing. QR-koder brukes i økende grad mange steder i samfunnet, i alt fra matbestilling til autentisering, og gjerne på mobile enheter. Måter å sikkerhetskontrollere QR-koder på er lite utbredt, og det er ikke mulig for mennesker å skille mellom skadelige QR-koder fra ondsinnede aktører og harmløse QR-koder fra legitime kilder. Cofense [26] beskriver en kampanje hvor QR-koder ble brukt mot et større energiselskap. KraftCERT har i 2023 sett phishing med QR-koder mot virksomheter i petroleumssektoren i Norge.

Det er sannsynlig at KI vil bli brukt til utvikling og tilpassing av skadevare, og at KI generelt vil øke kapasiteten til trusselaktører. Google/Mandiant [27] mener at KI vil skalere operasjoner til både angripere og forsvarere av digitale systemer. Myndigheter har stor oppmerksomhet mot KI, og samtlige nasjonale vurderinger (se kapittel 3 på side 7) omtaler KI. Kripos [4] mener KI har «potensial for cyberkriminalitet i dens hastighet, hukommelse og nesten ubegrensede utholdenhet». På den andre siden trekker de også frem KI som noe som kan gi kapasitet til dynamiske sikkerhetstiltak og å oppdage trusler tidlig.

5.4 Angrepsformer forøvrig

Det er sannsynlig at Living off the Land (LotL) vil være en foretrukket teknikk for avanserte trusselaktører fremover. Det er vanskeligere å oppdage uønsket adferd som utøves med legitime/allerede installerte verktøy. Den kinesiske trusselaktøren Volt Typhoon er et eksempel på en gruppering som benytter seg av denne teknikken. CISA [28] har skrevet utfyllende om dem.

Misbruk av leverandørers kommunikasjonsplattformer (som bl.a. filoverføring, VPN, fjernoppkobling og liknende) som springbrett i angrep vil sannsynligvis øke, dette beskrives bl.a. av Group-IB i deres *Hi-Tech crime trends report 2023/2024* [29, s13].

[7] «less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists» [24]

6 Aktørutvikling

Mange analyser og rapporter vektlegger enkeltaktører i for stor grad.

Rapportering om enkeltaktører kan gi bruddstykker av forståelse, og i beste fall indikatorer man kan se etter i egne overvåkningssystemer. Verdien øker når denne informasjonen er vurdert og sammenfattet med kunnskap om angrepsteknikker. KraftCERT analyserer trusselaktører langs flere akser, som størrelse, motivasjon, målretting og konsekvenser av angrep. Vi presenterer ikke et fullt bilde av dette økosystemet men fokuserer på våre viktigste slutninger.

Større trusselaktører vil meget sannsynlig fortsette å bruke spesialiserte underleverandører som f.eks tilgangsmeglere for å oppnå sine mål. ENISA mener Initial Access Broker (IAB)-markedet er «booming» [17], og Palo Alto/Unit 42 mener stjålne identiteter var en av hovedårsakene til at trusselaktører lyktes med angrep i 2023 [12]. Group-IB viser til at det i 2023 var en betydelig nedgang i snittpris for å kjøpe tilganger til virksomheter sammenlignet med 2022, og mener det er fordi det er flere selgere på markedet [29]. Økosystemet er dynamisk og påvirkes også av andre faktorer.

Myndighetsaksjoner mot trusselaktører vil mulig føre til fragmentering av metoder brukt av trusselaktørene, og dermed mindre forutsigbarhet i «økosystemet». Myndigheter har i 2023 aksjonert mot flere trusselaktører, bl.a. LockBit. [30]

Økonomisk motiverte trusselaktører vil meget sannsynlig unngå angrep mot mål som (de tror) gir sterk myndighetsreaksjon. Colonial Pipeline-hendelsen er et eksempel på et cyberangrep som har medført aksjoner fra myndighetene. Norsk politi deltok i aksjonen mot trusselaktøren Hive tidlig i 2023 [4]. Betalingsvilje i andre sektorer tiltrekker økonomisk motiverte trusselaktører, f.eks. i USA, der helsesektoren opplever betydelig økning i utpressingsangrep.

Det er meget sannsynlig at oppdragsstyrte trusselaktører vil forsøke å kamuflere sin aktivitet som andres. På denne måten vil de fremstå som tro til sine ord og også skjule aktivitet de ikke ønsker kjent. Dette kan gjelde innen hacktivisme, hvor såkalt faketivisme[8] ser ut til å være et fenomen å merke seg. Dette blir bl.a. beskrevet i CrowdStrikes *2024 Global Threat report* [15].

Det er meget sannsynlig at trusselaktører publiserer uriktige påstander om lekkede data på lekkasjesider. Antallet virksomheter som får sine data publisert på lekkasjesider øker (se f.eks. rapportene fra Group-IB[29] og Crowdstrike[15]). KraftCERT har observert falske og overdrevne påstander om lekkede data: forsøk på utpressing uten at det faktisk er lekket og publisert data. Det er derfor viktig å grundig undersøke påstander om lekkede data før man reagerer på disse.

[8] Faketivisme: begrep brukt for å beskrive handlinger gjort under dekke av å være ideologisk motivert aktivisme, men som i virkeligheten er gjort av statlige eller andre «profesjonelle» organisasjoner.

7 Trusler mot kontrollsystemer

Følgeskader fra opportunistiske angrep er den mest sannsylige trusselen for kontrollsystemer, mens det er driftsforstyrrelser som er den mest sannsynlige konsekvensen av angrep. Den mest alvorlige trusselen på lang sikt er angrep fra ressurssterke statlige aktører som har som mål å svekke forsvarsviljen i befolkningen. Slike angrep vil kunne ha både ødeleggende og driftsforstyrrende konsekvenser.

7.1 Driftsforstyrrelser

> En driftsforstyrrelse er at leveransene stanser midlertidig, enten helt eller delvis. Det kan være strømutfall eller -avbrudd, stans i produksjonen eller leveransen, eller feil ved leveranse eller med produktet. Et eksempel på det siste er feil på vannkvalitet for vannverk.
>
> I dagligtale blant cybersikkerhetspersonell brukes gjerne driftsforstyrrelse og disruptiv om hverandre, men disruptiv kan gi assosiasjoner til større konsekvenser.

Det er sannsynlig at virksomheter i våre sektorer utsettes for angrep som har driftsforstyrrende effekt. Ved angrep som har driftsforstyrrelse som mål, er det meget sannsynlig at en trusselaktør vil utnytte avhengigheter i funksjonalitet mellom kontrollsystemsonene og IT-sonene eller eksterne tjenester og skytjenester. Slike avhengigheter blir flere og viktigere for drift og leveranse. Eksterne koblinger gjør at angrepsflaten utvides utenfor det som tradisjonelt har vært kontrollsystemsonen. Kontrollsystemet må kunne segregeres og driftes autonomt. For å ivareta denne integriten krever det uavhengighet til andre funksjoner. En målrettet angriper kan dermed utnytte at funksjoner for drift er spredt ut av kontrollsystemsonen til å gjennomføre disruptive angrep.

Eksterne koblinger og funksjonsavhengighet

Det blir flere sammenkoblinger mellom kontrollsystem og utenforliggende system på grunn av behov for datautveksling, og virksomhetenes operations/drift blir mer avhengig av disse sammenkoblingene. Funksjoner som tidligere lå innenfor kontrollsystemsonen, eller som tidligere ikke var nødvendig for drift, blir plassert i soner med ulik kritikalitet eller sikkerhetsnivå.[a].

For eksempel har utviklinga av det nordiske kraftmarkedet ført til krav om kortere tidsforsinkelse i regulering av balansen mellom produksjon og forbruk, raskere enn manuell regulering klarer. Dette presser frem nye koblinger mellom det som tradisjonelt har vært separate virksomheter og kontrollsystemer. Dette gjøres også over Internett, som fører til at man er avhengig av infrastruktur som er internettvendt, og som utgjør en forstørret angrepsflate. Totalt utgjør dette en driftsavhengighet som har stor risiko for å bli utnyttet av angripere som ønsker å forstyrre kraftforsyningen.

I praksis betyr sammenkoblingen mellom kontrollsystem og utenforliggende system at systemene utenfor kontrollsystemsonen har samme kritikalitet, slik at klassisk øydrift blir en utilstrekkelig metode for å opprettholde normaldrift også i ekstraordinære situasjoner. Dette gir en utfordring for virksomheter som i dag har krav om øvelse på øydrift, og krav til oversikt over hvilke funksjoner som faller bort og hvor lenge man kan produsere eller levere.

[a] https://en.wikipedia.org/wiki/IEC_62443#Security_Level

Ved direkte angrep på perimeter til kontrollsystemer vil trusselaktører sannsynligvis utnytte fjerntilkobling og integrasjoner mot IT-systemer. Angripere vil utnytte sårbarheter i utstyr eller bruke stjålet tilgangsinformasjon mot internettvendte tjenester ved direkte angrep på kontrollsystemer. Sammen med manglende autentisering av trafikk inne i kontrollsystemsonen kan disse sårbarhetene gi en økt mulighet for vellykkede angrep.

Dette gjelder også internt i virksomheters nettverk. Systemer som kontrollsystemet utveksler informasjon med er ofte mer utsatt for kompromittering enn kontrollsystemet selv, og kan dermed benyttes som springbrett hvis knytningen ikke er tilstrekkelig sikret, eller det finnes sårbarheter i kontrollsystemet.

Bruken av fjerntilkobling er økende på grunn av effektivisering av drift og mangel på personell, og pga. mer omfattende driftsavtaler hvor leverandører tar større del av ansvaret for utstyret/enhetene. Dette fører til at interessen for stjålne innloggingsdetaljer er økende, og KraftCERT vurderer at det er sannsynlig at slike detaljer for fjerntilgang til industrikontrollsystemer vil bli brukt i angrep.

Driftsforstyrrende effekt kan også være en følge av andre typer angrep. Manglende oversikt over funksjonsavhengigheter kan gjøre at virksomheten preventivt stenger en driftsavhengig funksjon, f.eks. ved et opportunistisk utressingsangrep. Et angrep som forstyrrer IT kan forårsake at virksomheten stenger OT-funksjoner[9] som et føre-var-tiltak [14, s.9].

For kontrollsystemer er følgeskader fra utpressingsangrep den mest sannsynlige trusselen. Kontrollsystemer er blir sjelden angrepet av kriminelle med økonomisk vinningsmotiv. Å kompromittere kontrollsystemer krever normalt ekstra innsats, siden kontrollsystemer som hovedregel er mer beskyttet enn IT-tjenester. I tillegg kan det være nødvendig med spesialkompetanse som det vanligvis ikke er behov for ved

9 Operasjonell teknologi (OT)

angrep på støttesystemer[10] i IT-nettverk. Angrep med mål om styring og kontroll krever at angriperen har spesialisert kunnskap om kontrollsystemer. Sammen gjør dette det sannsynlig at opportunistiske angripere heller vil søke å angripe enklere mål innenfor virksomhetene.

KraftCERT er kjent med at det finnes kode som kan installere krypteringsskadevare på kontrollere. I tillegg kan plansystem, overordnet kontrollsystem [11], og interne støttesystemer være utsatt for generisk krypteringsskadevare. Samtidig har driftsorganisasjonene ofte bedre rutiner for gjenoppretting av drift, noe som kan ha betydning for viljen til å betale løsepenger.

Hvis en angriper, under et angrep, finner kontrollsystemet uten å forstå systemets funksjon, kan dette føre til at angrepet får større konsekvenser enn tilsiktet. Dersom kontrollsystemet ikke er tilstrekkelig adskilt fra IT- nettverkene kan en angriper spre skadevare videre fra IT-nettverket uten å vite at de angriper kontrollsystemet.

Alle angrep hvor offeret blir kjent med at de er angrepet vil også kunne føre til aksjoner og reaksjoner som vil påvirke kontrollsystemene negativt. En hendelse vil kunne spre usikkerhet slik at offeret stenger ned eller separerer nettverk som får konsekvenser for funksjoner med avhengigheter mellom soner.

Utpressingsangrep er den angrepsformen det er mest sannsynlig at KraftCERTs medlemmer kan bli direkte utsatt for. Det er ingen forskjell mellom IT-systemer i virksomheter med og uten kontrollsystemer. De er like avhengige av kontorsystemer, CRM-systemer, varelagersystemer, mm. De er dermed utsatt for de samme truslene som andre. Trendene viser at det er utpressingsangrep som er det mest vanlige kjente angrepsformen.

KraftCERT mener at manglende grunnsikring av IT-infrastruktur skaper muligheter for vellykkede angrep med konsekvenser for kontrollsystemer. Opportunistiske angripere går etter det som er mest regningssvarende. Akkurat som andre kriminelle vil de ha mest mulig inntjening, ikke ulikt lovlydige virksomheter. Hvis det er kjente sårbarheter eller muligheter for angrep som ikke trenger spesialisert kunnskap hos virksomheter vil kriminelle aktører velge å angripe disse fremfor de med bedre forsvarsevne. Mange kriminelle angriper også bredt, men blindt, og blir stoppet av overvåking og forsvarsevne.

Det utvikles samtidig stadig ny skadevare og disse utnyttes av flere aktører til opportunistiske angrep. Dette fører til at virksomheter må ha grunnsikring på plass for å kunne forsvare seg mot nye angrep.

7.2 Destruktive angrep

Det er svært lite sannsynlig at vi på kort sikt får se vellykkede destruktive angrep mot KraftCERTs sektorer. Dette har ikke endret seg siden *Trusselvurdering 2023*[10]. Angrep som har til hensikt å skade mennesker eller anlegg er svært ressurskrevende å gjennomføre. Det krever at man samtidig angriper både kontrollsystem og safetysystem. I angrepene mot Ukrainske energiselskap har trusselaktørene oppnådd driftsforstyrrelser, men ikke ødeleggende effekter. Ukraina har riktignok kunnet forberede seg i flere år (siden før 2014), og håndtert flere angrep mot kontrollsystem det siste tiåret.

Det er meget sannsynlig at statlige og oppdragsstyrte aktører jobber kontinuerlig for å utvikle destruktive angrep. KraftCERT forutsetter at flere aktører har et ønske om å bygge evne til destruktive angrep, og det er sannsynlig at virksomhetenes sårbarheter gir muligheter for gjennomføring. Det er dermed et spørsmål om planlegging, kapasitet, tidspunkt og ikke minst informasjon om målet.

Driftsforstyrrende angrep er i seg selv enklere å få til, siden de kun krever at at man angriper en funksjon en virksomhet er avhengig av for leveranse. Det kan være nok med en mistanke om kompromittering for at

[10] Systemer som er nødvendig for drift, men ikke er i kontrollsystemsonen
[11] Supervisory control and data acquisition (SCADA)

man tar ned slike systemer for å være føre var. Dersom en aktør ønsker å signalisere at det er mulig å lamme energiforsyningen i form av kraft- eller olje- og gassleveranser er driftsforstyrrelse et mulig angrepsmål.

Målsetninger ved angrep mot kontrollsystemer
Ulike målsetninger for angrep i stigende vanskelighetsgrad.

Tilgang (Access)
Tilgangsangrep er når trusselaktører har til hensikt å skaffe tilgang til virksomhetens nettverk, enten for å selge tilgangen videre via IABer eller for å skaffe seg fotfeste til videre angrep.

Datatyveri (Data theft)
Angrep som har til hensikt å hente ut informasjon om virksomhetens produkter, leveranser, strategier, systemer og nettverk, og/eller kontrollsystem. Det kan også være en forberedelse for senere angrep.

Driftsforstyrrelse (Disruption)
Angrep som har som mål å forstyrre virksomhetens leveranse. Dette kan gjøres direkte ved angrep på kontrollsystem, eller indirekte ved å angripe støttesystemer man er avhengig av for drift. Også kalt «Disruptive angrep».

Ødeleggelse (Destruction)
Angrep med mål om å ødelegge utstyr, forårsake ytre ødeleggelser (miljø) eller ta liv. De er vanskelige og ressurskrevende å gjennomføre fordi man ofte må inn på kontrollsystem samtidig som man slår av funksjoner i safetysystem. Også kalt «Destruktive angrep».

Kontroll (Control)
Angrep for å ta kontroll over og styre prosesser i kontrollsystemer er de vanskeligste. Selv om man ikke trenger å angripe både kontrollsystem og safetysystem, krever et slikt angrep både god domene- og lokalkunnskap om systemet og den underliggende infrastrukturen for å lykkes, og for å kunne styre prosessen. Ved å ha full kontroll på kontrollsystemet kan være mulig å lage situasjoner som omgår safetysystemet.

Driftsforstyrrende angrep har langt større mulighet for å lykkes enn destruktive angrep, selv i krig. Ukrainakrigen er et godt eksempel på dette. Krigen har vart i over ti år, og det er kun ett kjent angrep som faktisk har hatt ødeleggende effekt: Angrepet på Viasat/KA-SAT-modemene [31] som satte dem varig ut av spill. De resterende har hatt disruptive effekter, inkludert angrepene i 2015 og 2016 som resulterte i strømutfall i store områder i Ukrainske byer. Skadevaren som har vært brukt i disse angrepene direkte mot kontrollsystemene har variert over tid, fra skadevare med standard IT-funksjonalitet til de med funksjonalitet for å angripe kontrollsystemers egne protokoller.

Skadevare i kontrollsystem er under stadig utvikling, men kontrollsystemskadevare som har vært brukt i angrep har blitt mindre komplekse over tid, sannsynligvis på grunn av ressursbegrensningene en krig medfører. [32]

Det er sannsynlig at målrettede oppdragsstyrte trusselaktører vil fortsette å utvikle ny skadevare som har til hensikt å angripe kontrollsystemer. Det er i de senere årene kommet flere nye skadevarer (Industroyer2, PIPEDREAM/ INCONTROLLER). To eksempler på ny skadevare med kontrollsystemfunksjonalitet ble brukt i Ukraina i 2022 og 2023, hvor russiske statlige aktører har brukt ny skadevare på et MicroSCADA-system [33] i angrep på kraftsystemet. CosmicEnergy ble observert lastet opp til en åpen

skadevareskanner, og er laget for forstyrre enheter i elkraft ved bruk av IEC-104[12] [34]. Dette viser at trusselaktører evner å utvikle skadevare selv om de er sterkt presset på både tid og ressurser.

KraftCERT mener også at det er sannsynlig at statlige oppdragsstyrte trusselaktører vil kjøpe eller sette ut utvikling av skadevare for å angripe kontrollsystemer. Se også kapittel 6 på side 13 om aktørutvikling. For eksempel mistenker Mandiant at skadevaren CosmicEnergy[34] er utviklet av penetrasjonstestere i Rostelecom-Solar.

I Ukrainakrigen virker det som om russiske trusselaktører har gjort en dreining i ICS-skadevaren de har brukt, fra store, komplekse og modulære systemer med flere innebygde funksjoner og protokoller til mindre, enklere verktøy med spesifikke funksjoner og hardkodet konfigurasjon. Det er sannsynlig at dette er på grunn av at angriperne ikke lenger har tid til å utvikle modulær skadevare med mange muligheter pga. krigen.

Adresseringsinformasjon: hvorfor er dette så viktig for trusselbildet?

Adresseringsinformasjon er tilstrekkelig grunnlag for å kommunisere med adresserte enheter etter kompromittering av perimeter til kontrollsystemet. Adresseringsinformasjonen gir også muligheter for styring, som igjen gir muligheter for avbrudd og kontroll. For en angriper vil adresseringsinformasjon forenkle kommunikasjon med kontrollsystemenheter uten å lage unødvendig støy som kan oppstå ved rekognosering. Rekognosering av kontrollsystemet er dermed redusert til simpelt databasetyveri, som kan gjøres i en tidligere fase, eller av andre. Adresseringsinformasjon om kontrollsystemet kan finnes mange steder med svært ulikt sikringsnivå, blant annet:

- redundant system
- nøddriftsystem
- test- og utviklingssystem
- digital tvilling
- leverandørers støttesystem
- sikkerhetskopier
- dokumentasjon om konfigurasjoner og sikkerhetsgjennomganger
- systemer for prosessering av driftsdata i sky

Det er meget sannsynlig at oppdragsstyrte trusselaktører vil samle og strukturere topologidata og adresseringsinformasjon, for å kunne bygge skadevare og angrepsteknikk. Mange typer data, fra for eksempel åpne kilder, fagsystemer, prosjektplaner, og IoT-enheter, vil være mulig og nyttig for en angriper i langsiktige forberedelser av angrep. Data kan anskaffes ved tyveri eller ved kjøp fra andre aktører. Slike data vil kunne forenkle angrepene, siden man kan bygge angrep som er mer spesifikt rettet mot kontrollsystemet. Uten slike data vil angriper være nødt til å rekognosere for å skaffe seg denne informasjonen eller ha funksjonalitet for rekognosering i skadevaren som skal benyttes. Det er derfor viktig å hindre trusselaktørers tilgang til slike data, spesielt om data befinner seg utenfor kontrollsystemsonen.

Det er meget sannsynlig at KI vil bli brukt til å forenkle arbeidet med sammenstilling av adresseringinformasjon og topologidata med annen informasjon for å kunne bygge angrepsteknikk. Det vil likevel kreve menneskelig kunnskap om kontrollsystemet både generelt og spesifikt. KI kan ikke selv forstå hvilken informasjon som er nyttig eller avgjørende for angrepsbygging, men vil sammen med kyndig personell kunne samle informasjon og finne mangler raskere enn tradisjonell etterretning og analyse.

[12] IEC 61850-5-104

Ved angrep på kontrollsystemer er det meget sannsynlig at en trusselaktør vil utnytte manglende autentisering av kontrolltrafikk mot SCADA eller kontrollere. De fleste kontrollsystemer har i dag ikke støtte for autentisering av trafikk til kontrollsystemet utenfra, eller mellom SCADA[13]/DCS[14]-system og PLC[15]/RTU[16]. Dette gjør det mulig for angripere å forfalske avsenderinformasjon slik at det ser ut som trafikken kommer fra f.eks. redundante systemer. Enkle og vanlige mottiltak på kontrollere eller nettverksutstyr, som f.eks. aksesslister eller enkel brannmurfunksjonalitet, kan omgås.

13 SCADA
14 Distributed Control System (DCS)
15 Programmable Logic Controller (PLC)
16 Remote Terminal Unit (RTU)

8 Trusselbildet er både lokalt og felles

Det er aktører i verden som ønsker å angripe våre sektorer, mange av økonomiske, men noen av sikkerhetspolitiske grunner. KraftCERT mener at god trusselforståelse krever nyansering.

Driftsforstyrrende angrep med f.eks kortvarig stans i produksjon er sannsynlig. Dette bør ikke blandes sammen med destruktive angrep med skade på mennesker eller varig skade på utstyr, som er meget lite sannsynlig. Forskjellen bør kommuniseres til alle interessenter.

KraftCERT oppfordrer sine medlemmer til å gjøre egne vurderinger, og ikke ukritisk legge til grunn informasjon eller påstander fra hverken kommersielle selskap eller myndigheter. Trusselbildet må ses i sammenheng med den enkelte virksomhets verdier og sårbarheter.

Det er viktig at medlemmer deler informasjon med KraftCERT, slik at vi kan bidra til et felles og mest mulig korrekt og oppdatert trusselbilde.

Referanser

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

[2] Etteretningstjenesten. *Fokus 2024*. 9. feb. 2024. URL: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2024%20-%20NO%20-%20Weboppslag%20v2.pdf.

[3] PST. *Nasjonal trusselvurdering 2024*. 12. feb. 2024. URL: https://pst.no/globalassets/2024/ntv2024/nasjonal-trusselvurdering-2024_uuweb.pdf.

[4] Kripos. *Cyberkriminalitet 2024*. 24. apr. 2024. URL: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf.

[5] Politiet. *Politiets trusselvurdering 2024*. 4. mar. 2024. URL: https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2024.pdf.

[6] Orange Cyberdefense. *Security Navigator 2024*. 11. jan. 2024. URL: https://www4.orangecyberdefense.com/security-navigator-2024.

[7] Microsoft Security. *Microsoft Digital Defense Report 2023*. 6. okt. 2023. URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[8] Global Resilience Federation. *Semi annual Ransomware Report H2 2023*. 28. feb. 2024. URL: https://static1.squarespace.com/static/60ccb2c6d4292542967cece7/t/65df77b189e978590077e1cd/1709143989084/Semiannual+Ransomware+Report+-+H2+2023+Final.pdf.

[9] ODNI. *Annual Threat Assessment of the U.S. Intelligence Community*. 8. mar. 2024. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[10] KraftCERT/InfraCERT. *Trusselvurdering 2023*. 6. jul. 2023.

[11] Inc Dragos. *OT CYBERSECURITY THE 2023 YEAR IN REVIEW FEBRUARY 2024*. 19. feb. 2024. URL: https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf.

[12] Palo Alto. *Incident Response Report 2024*. 16. feb. 2024. URL: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf.

[13] Artic Wolf. *2024 Threat Report*. 20. feb. 2024. URL: https://arcticwolf.com/resource/2024-threat-report-lp/arctic-wolf-labs-2024-threat-report.

[14] Waterfall. *2024 Threat Report: OT cyberattacks with Physical Consequences*. 1. apr. 2024. URL: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-ot-cyberattacks-with-physical-consequences/.

[15] Crowdstrike. *2024 Global Threat Report*. 6. mar. 2024. URL: https://go.crowdstrike.com/global-threat-report-2024.html.

[16] IBM Security. *Threat Intelligence Index 2024*. 13. mai 2024. URL: https://www.ibm.com/downloads/cas/L0GKXDWJ.

[17] ENISA. *ENISA THREAT LANDSCAPE 2023*. 19. okt. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.

[18] Environmental Protection Agency. *EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water*. 20. mai 2024. URL: https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect.

[19] Nasjonal sikkerhetsmyndighet. *Nasjonalt digitalt risikobilde 2023*. 19. okt. 2023. URL: https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf.

[20] Betina Slagnes. *FFI-RAPPORT 23/00546 Hva vet vi om innsiderisiko?* 6. mar. 2023. URL: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3155/23-00546.pdf.

[21] Daniel Frank. *Threat Assessment: BianLian*. 19. jan. 2024. URL: https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment.

[22] CISA. *Exploitation of Unitronics PLCs used in Water and Wastewater Systems*. 28. nov. 2023. URL: https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems.

[23] National Cyber Security Centre. *The near-term impact of AI on the cyber threat*. 24. jan. 2024. URL: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

[24] Microsoft Threat Intelligence. *Staying ahead of threat actors in the age of AI*. 14. feb. 2024. URL: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai.

[25] Security Intelligence. *AI vs. human deceit: Unravelling the new age of phishing tactics*. 24. okt. 2023. URL: https://securityintelligence.com/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics.

[26] Nathaniel Raymond. *Major Energy Company Targeted in Large QR Code Campaign*. 20. sep. 2023. URL: https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign.

[27] Google Cloud. *Insights for future planningCybersecurity Forecast 2024*. 9. nov. 2023. URL: https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf.

[28] CISA. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. 7. feb. 2024. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[29] Group-IB. *HI-TECH CRIME TRENDS REPORT 2023/2024 - EUROPEAN CYBER THREAT LANDSCAPE*. 28. feb. 2024. URL: https://www.group-ib.com/landing/hi-tech-crime-trends-2023-2024/.

[30] Trend Micro. *LockBit Attempts to Stay Afloat with a New Version*. 22. feb. 2024. URL: https://www.trendmicro.com/en_us/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html.

[31] Viasat. *KA-SAT Network cyber attack overview*. 31. mar. 2022. URL: https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview.

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

[33] Mandiant. *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*. 10. nov. 2023. URL: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

[34] Mandiant. *COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises*. 25. mai 2023. URL: https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response.

Tillegg

A Om KraftCERT

KraftCERT optimaliserer sikring av prosesskontrollsystemer for kraftbransjen. Vi oppdaterer våre medlemmer om relevante sårbarheter og trusler, slik at de vil være i stand til å detektere og motvirke digitale angrep.

KraftCERT er et ISAC (Information Sharing and Analysis Center) og et IRT (Incident Response Team) for sin målgruppe, og KraftCERT jobber for god, sikker og effektiv hendelseshåndtering og informasjonsdeling mellom relevante selskaper nasjonalt og internasjonalt.

KraftCERT er sektor-cyberresponsmiljø for sektorene kraft og petroleum, og ellers består målgruppen av prosessindustri, vann- og avløpssektoren samt energigjenvinning. KraftCERT er med i den nasjonale beredskapsorganisasjonen.

KraftCERT er et uavhengig non-profit selskap, men har varslingsansvar til myndighetene for kraft- og petroleumssektorene i Norge ved alvorlige cyberhendelser. KraftCERT bistår også til den nasjonale trusselvurderingen via innspill til myndighetene.

KraftCERT er del av det norske sektorresponsmiljøet, er medlem av Forum of Incident Response and Security Teams (FIRST) og er et sertifisert incident response team i Trusted Introducer. KraftCERT har medlemmer både i Norge og på Island.

Les mer om våre tjenester på https://www.kraftcert.no/

Varsle KraftCERT om hendelse: https://varsling.infracert.no/

Kontaktinformasjon:

- cert@kraftcert.no (Hendelser/incidents)
- postmottak@kraftcert.no (Administrative henvendelser)
- Tlf: +47 940 32 443 (Vakt, betjent 08-16 hverdager)

B Ordliste

CRM *Customer relationship management*. Systemer som brukes til å håndetre kunderelasjoner. Side 16.

DCS *Distributed Control System*. Kontrollsystem med stor grad av autonomi ved anlegg. Har ofte overordnet overvåking. Side 19.

HMI *Human-Machine Interface*. Grensesnitt mellom menneske og maskin, gjerne i form av skjerm og knapper/taster. Side 24.

IAB *Initial Access Broker*. Tilgangsmegler. Side 13, 17, *se også* Tilgangsmegler.

ICS *Industrial Control Systems*. Systemer for styring og kontroll av industrielle prosesser. Inkluderer begreper som HMI, PLC, PLS. Side 18.

IoT *Internet of Things*. Tingenes internett – utstyr (sensorer, brytere, osv) koplet i nettverk. Side 18.

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 12.

OT *Operasjonell teknologi*. Prosessteknologi. Side 15.

PLC *Programmable Logic Controller*. Spesialisert datamaskin som kan styre industrielle prosesser. Side 19, 24.

PLS Programmerbar Logisk Styring. Side 24, *se også* PLC.

RTU *Remote Terminal Unit*. Terminalenhet for å konvertere digitale og analoge signaler mellom sensorer og aktuatorer og kontrollsystemet. Side 19.

SCADA *Supervisory control and data acquisition*. Systemer for styring og overvåking av automasjons- eller styringssystemer. Side 16, 19.

Tilgangsmegler Aktør som videreselger stjålne tilganger til systemer. Side 13.