Rapport

Leverandørkjedesikkerhet

Relevante krav for nettselskapers innkjøpsprosesser

Forfattere:

Martin Gilje Jaatun, Hanne Sæle

Rapportnummer:

2023:00121 - Åpen

Oppdragsgiver:

Norges vassdrags- og energidirektorat

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Leverandørkjedesikkerhet

Relevante krav for nettselskapers innkjøpsprosesser

EMNEORD
Leverandørkjede
Sikkerhet
Anskaffelsesprosess

VERSJON
1.0

DATO
2023-02-20

FORFATTER(E)
Martin Gilje Jaatun, Hanne Sæle

OPPDRAGSGIVER(E)
Norges vassdrags- og energidirektorat

OPPDRAGSGIVERS REFERANSE
Janne Merete Hagen

PROSJEKTNUMMER
102028038

ANTALL SIDER OG VEDLEGG
24 + 3s vedlegg

SAMMENDRAG
Denne rapporten presenterer resultater fra gjennomgang av tidligere NVE-rapporter rundt temaet leverandørkjedesikkerhet, supplert med et litteratursøk blant nyere akademisk litteratur og diskusjoner med et lite utvalg av bransjeaktører, og anbefaler basert på dette, et sett med anbefalinger til krav knyttet til anskaffelse av IT og OT, med spesielt fokus på leverandørkjede.

Det er utarbeidet anbefalinger til må- og bør-krav, rettet spesielt mot små og mellomstore nettselskap til bruk i anskaffelsesprosesser.

UTARBEIDET AV
Martin Gilje Jaatun

SIGNATUR
Martin G. Jaatun
Martin G. Jaatun (Feb 20, 2023 15:32 GMT+1)

KONTROLLERT AV
Karin Bernsmed

SIGNATUR
Karin Bernsmed (Feb 20, 2023 15:45 GMT+1)

GODKJENT AV
Aida Omerovic

SIGNATUR
Aida Omerovic
Aida Omerovic (Feb 20, 2023 20:17 GMT+1)

RAPPORT NR. 2023:00121

ISBN 978-82-14-07944-9

GRADERING Åpen

GRADERING DENNE SIDE Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2023-02-20	Første versjon

Innholdsfortegnelse

1 Introduksjon

Målsettingen med dette arbeidet er å utarbeide en rapport om leverandørkjede-sikkerhet for å identifisere god praksis på kravsetting relatert til IKT-sikkerhet i anbudsdokumenter på anskaffelse av IT og OT[1], og hvordan dette kan følges opp i drift. Dette vil også være relevant f.eks. for anskaffelse av driftskontrollsystemer, men dette har ikke vært behandlet spesielt.

Det finnes i dag allerede et samarbeid kalt SELLIHCA kvalifikasjonsordning[2] som brukes "for å skaffe tilveie […] informasjonen i utvelgelsen av leverandører ved forespørsler av varer, tjenester og entrepriser". Krav og anbefalinger vi spesifiserer i det følgende kommer i tillegg til det som dekkes av SELLIHCA, og kommer også i tillegg til det som dekkes av anskaffelsesloven [1].

For nettselskaper er det sannsynligvis de konkrete anbefalingene i kapittel 5 som vil ha størst umiddelbar interesse.

2 Metode

I forbindelse med prosjektet har vi gått gjennom og vurdert anbefalinger fra rapporter og akademisk litteratur som er relevante for oppdraget. Det gjelder i første omgang følgende rapporter:

- Elisabeth Kirkebø, Mathias Ljøsne, IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen, NVE Rapport 90:2018. [2]
- Maren Maal, Katrine Krogedal og Arthur Gjengstø, IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen - sjekkliste, NVE- Rapport nr. 1/2020 [3]
- Veiledning til kraftberedskapsforskriften [4]
- Sigrid Haug Selnes, Sina Rebekka Moen, Siyang Emily Ji og Ove Njå, Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder, NVE-Eksternrapport 18:2021 [5]

Videre har vi gjennomført et litteratursøk i Scopus, som beskrevet i kapittel 3. Dessuten har vi gjennomført et lite antall uformelle intervjuer med aktører i kraftbransjen, for å få tilbakemeldinger på foreløpige resultater og nye innspill.

[1] IT = Informasjonsteknologi, OT = Operasjonell teknologi, https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id6-premisser-for-digitalisering-og-integrasjon-it-ot_sintef-rapportnr-2021-00057-feb--signert.pdf

[2] http://www.achilles.no/services/sellihca/downloads/rights_and_duties.pdf

3 Litteratursøk

Vi har brukt en forenklet utgave av retningslinjene for systematisk litteraturanalyse [6], hvor vi først sorterer på tittel, deretter på abstract, og til slutt på hele artikkelen. Dette er illustrert i Figur 1: Søkestrategi i prosjektet.

Figur 1: Søkestrategi i prosjektet

3.1 Søk fra tilbud

I tilbudet anga vi følgende eksempel på søkestreng: på " TITLE-ABS-KEY (digital AND supply AND chain AND security)", som ga 714 resultater. Dette er åpenbart for mange resultater, og en kjapp stikkprøve viste at det var mange av disse som ikke var relevante. Det var derfor behov for ytterligere avgrensning, som beskrives under.

3.2 Søkekriterier

Selnes og kolleger [5] angir eksempler på søkestrenger, men det er ikke åpenbart hvordan disse er knyttet sammen, ettersom de sier at "Søkene har resultert i et relativt lite antall treff". Hvis vi avgrenser søket angitt i tilbudet til artikler publisert etter 2020, får vi 322 treff, noe som fortsatt er for mange for vårt formål.

Vi valgte derfor å tilnærme oss søket til Selnes og kolleger. Ved å søke i Scopus med kriteriene (*"supply chain risk management"* OR *"supplychain energy power supply"* OR *"supply chain attack"*) AND *"cybersecurity"* AND (LIMIT-TO (PUBYEAR , *2022*) OR LIMIT-TO (PUBYEAR , *2021*)) får vi 227 treff.

Scopus gir muligheten til å avgrense søket innen fagområder ("subject areas"). Ved stikkprøver fant vi at hvis vi avgrenser søket til sosialvitenskap, forretning, og beslutningsvitenskap, er resultatene i stor grad irrelevante for vårt formål, og ved å i stedet ekskludere disse kommer vi ned i 119 treff[3]:

[3] Det er mulig at dette kriteriet er for strengt; med bedre tid tilgjengelig burde man verifisert at ingen relevante artikler er utelatt

("supply chain risk management" OR "supplychain energy power supply" OR "supply chain attack") AND "cybersecurity" AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021)) AND (EXCLUDE (SUBJAREA , "BUSI") OR EXCLUDE (SUBJAREA , "DECI") OR EXCLUDE (SUBJAREA , "SOCI"))

Etter gjennomgang av alle titler, får vi redusert antallet til 31. Vi har her også ekskludert alle artikler som omhandler bruk av blokkjeder, ettersom vi ikke anser dette som moden teknologi.

Vi har så vurdert abstract til de 31 artiklene. Oppdragsgiver har kommunisert at et viktig resultat vil være anbefalinger og/eller god praksis som kan bedre leverandørkjedesikkerhet for små og mellomstore aktører, og vi har tatt hensyn til dette ved vurdering av sammendraget til de utvalgte artiklene.

3.3 Resultat fra søk

Blant de 31 artiklene som var relevante basert på tittel, har vi vurdert 4 som relevante og ytterlige 9 som kanskje relevante for arbeidet som beskrives i denne rapporten. På grunn av den begrensede tiden tilgjengelig, har vi i første omgang kun sett nærmere på de 4 artiklene vi vurderte til å være relevante. En fullstendig oversikt over de 31 artiklene finnes i vedlegg A.

3.3.1 Viega og Michael [7]

J. Viega and J. B. Michael, 'Struggling with Supply-Chain Security', Computer, vol. 54, no. 7, pp. 98–104, 2021

Viega og Michael fremhever at det viktigste verktøyet for leverandørkjedesikkerhet fremstår som et standardisert spørreskjema/sjekkliste for leverandører, og peker på Vendor Security Alliance[4] som et godt eksempel. De fremhever at det store utvalget av tjenestebaserte løsninger representerer en utfordring for leverandørkjedesikkerhet.

De anbefaler å bruke en risikorangering av leverandører, og så sørge for at de med størst risiko blir vurdert på nytt med en høyere frekvens (f.eks. årlig). Imidlertid påpeker de at å be leverandører om selv-evaluering har betydelige utfordringer; de rapporterer om egne opplevelser hvor leverandører har blitt tatt i blank løgn om sine sikkerhetsløsninger[5]. Det motiverer et ønske om mer automatiserte løsninger or overvåking av en leverandørs løsninger, for å kunne verifisere at levert sikkerhetsnivå harmonerer med påstått sikkerhetsnivå. Dette kan også omfatte f.eks. at kunden kan foreta monitorering av nettforum hvor sikkerhetslekkasjer deles, for å oppdage sikkerhetshendelser før de er varslet gjennom offisielle kanaler.

3.3.2 Wang [8]

X. Wang, 'On the Feasibility of Detecting Software Supply Chain Attacks', presented at the IEEE Military Communications Conference MILCOM, November 2021, pp. 458–463.

Beskriver en eksperimentell metode for detektering av leverandørkjedeangrep, men bidrar ikke med noe som kan brukes til å stille krav til bestillere eller leverandører.

3.3.3 Nygård og Katsikas [9]

A. R. Nygård and S. Katsikas, 'SoK: Combating threats in the digital supply chain', presented at the 2022 ARES conference

Systematisk gjennomgang av litteratur med søkebegrep: (Cybersecurity OR security) AND supply AND chain). Søkeresultatene er ytterligere raffinert I flere omganger ved å bruke nøkkelord som "attack" OR "vulnerability" OR "trojans" OR "trust."

[4] vendorsecurityalliance.org
[5] Dette er også bekreftet av norske aktører vi har pratet med.

Artikkelen nevner råd fra NIST, men få som kan brukes til å sette krav til leverandører. Ett unntak: "Implement a documented vulnerability management program."

3.3.4 Yang, Lee og McDonald [10]

J. Yang, Y. Lee, and A. P. McDonald, SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies, presented at SNPD 2021: Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SCI vol. 1012, 2022, p. 58.

Artikkelen beskriver et spesifikt tilfelle, hvor leverandøren SolarWinds som utviklet et populært administrasjonsverktøy, Orion, ble kompromittert av en gruppe som fikk tilgang til kildekoden til produktet, og fikk lagt inn en bakdør (kjent som SunBurst) som i neste omgang ble distribuert av leverandøren som en gyldig oppdatering.

Forfatterne diskuterer årsaker og konsekvenser for SolarWinds og deres kunder, og identifiserer et antall faktorer med forslag til løsninger. Disse er oppsummert i tabellen under, med våre kommentarer.

Problem	**Løsning**	**Vår kommentar**
Markedet har intensiver for profitt, ikke sikkerhet	• Staten bør angi minimum sikkerhetsstandarder for utvikling og distribusjon av programvare • Forbedring av statens innkjøpsprosesser slik at firma sørger for sikkerhet • Innføring av ansvar for programvareselskaper	Vi er skeptiske til om dette vil ha ønsket virkning – vil være en fordyrende prosess, og til slutt vil store firma med mange advokater uansett kunne gjøre som de vil
"Additiv" sikkerhet tilfører nye verktøy som potensielt lager nye sårbarheter	"Reduktiv" sikkerhet som fjerne unødvendige tjenester, biblioteker, etc.	Dette er i praksis det som kalles "herding", og er noe som kan anbefales generelt
Må oppdatere til neste versjon	La være å oppdatere hvis oppdatering er unødvendig	Potensielt en farlig anbefaling, ettersom oppdateringer ofte korrigerer oppdagede sikkerhetsfeil
Kunder stoler på digitalt signerte oppdateringer	Lag verktøy for å enkelt vurdere sikkerhet til oppdateringer	Naiv tilnærming som kunne vært dekkende for akkurat dette tilfellet, men i det generelle tilfellet må man kunne stole på signerte oppdateringer. På samme måte som at dagens antivirusverktøy ikke er 100% nøyaktige, vil ikke et slikt verktøy forfatterne anbefaler kunne være det.
For mye vekt legges på brannmurer og antivirus og konfidensialitetskrav til offentlig nettsky	• Bruk sterk kryptering overalt • Flytt rundt på data som lagres i skyen	Her virker det som om forfatterne ikke vet hva de snakker om

Stor utfordring å gjennomføre skadevurdering, og deteksjon av modifiserte komponenter	Bruk AI til å detektere rekognosering, kommando og kontroll, og andre tegn på kompromittering	Dette er i praksis en anbefaling om å bruke inntrengnings-deteksjonsystemer (IDS)

Forfatterne har ytterligere anbefalinger som går på å oppdage sårbarheter i avhengigheter til åpen kildekode, noe som harmonerer med andres anbefalinger om å bruke Software Bill of Materials (SBOM).

4 Gjennomgang av relevante NVE-rapporter

Basert på gjennomgang av de relevante rapportene nevnt i kap. 2 er det beskrevet viktige momenter knyttet til hvordan virksomheter kan ivareta sikkerhet. Dette oppsummeres deretter for hva dette betyr for leverandørkjeden.

4.1 IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen, NVE 90/2018 [2]

NVE-rapporten 90/2018 [2] om informasjonssikkerhetstilstanden i energiforsyningen viser hvor avhengige energibransjen er til sine leverandører, bl.a. knyttet til økt bruk av skytjenester og utkontraktering, og spesialisert tjenestekjøp bl.a. knyttet til sikkerhet, som kan gi lange digitale verdikjeder.

NVE-rapporten "Regulering av IKT-sikkerhet"[11] som nevnes, gir en vurdering av tjenesteutsetting, leverandørkjeder og fjernaksess, og nevner at informasjonssikkerhet bør være en del av det helhetlige arbeidet med forebyggende sikkerhet og beredskap i energiforsyningen. Den generelle sikringsplikten mot uønskede hendelser og handlinger bør tydeliggjøres i dagens krav.

Virksomhet og leverandør må bli enige om en IKT-driftsmodell, som bl.a. omfatter:

- Adgangskontroll og overvåking av systemer ved fysisk service eller fjerntilgang
- Hvilken type data som skal lagres eller behandles, og hvor i verden disse lagres
- Sikring av mobile enheter og rettighetsstyring ved utvikling av mobile applikasjoner med kobling til sentrale tjenester, der bruker får tilgang via internett

Det er i dag strenge krav til beskyttelse av kraftsensitiv og taushetsbelagt informasjon, men det er ikke eksplisitte krav knyttet til bruk av skytjenester eller utsetting av IKT-drift.

NVE-rapporten "Informasjonssikkerhetstilstanden i energiforsyningen"[12] beskriver sårbarheter som er avdekket (i penetrasjonstester), og som kunne vært unngått dersom virksomheten hadde hatt bedre leverandørkontroll. Det viser at sikkerhet ikke er tilstrekkelig ivaretatt i forbindelse med kjøp og utsetting av IT-tjenester til leverandører. Rapporten presiserer viktigheten i å ta inn over seg hvor avhengig virksomheter er av sine leverandører, og at dette tas hensyn til både for forebyggende sikkerhet og beredskap. Rapporten anbefales at det foretas risikovurderinger, utføres sikkerhetstester av systemene før tjenester blir satt ut, sjekker sikkerhetstilstanden regelmessige (også etter at tjeneste er satt ut), og involverer leverandører i utvikling og øving av beredskapsplaner.

Det anbefales å integrere sikkerhet i anskaffelsesprosessen, fra start til slutt. Sikkerhetskrav bør ikke bare begrenses til selve produktet, men også dekke forhold som funksjonalitet, analysekapasitet, overvåkbarhet, styring og integrasjon, herunder samsvar med virksomhetens sikkerhetsarkitektur. Det bør velges en leverandør der virksomheten kan stole på leverandørkjeden og tjenestene som leveres gjennom hele livsløpet til produktet eller tjenesten, og at underleverandører inkluderes som en del av hendelsesteamet der det kan være nødvendig, også inkludert i øvelser.

For å ivareta IKT-sikkerhet, er det oppsummert fem sikkerhetsfaglige anbefalinger:

- Oversikt og kontroll på hele livsløpet – Forberedende, anskaffelse, forvaltning, opphør
- God bestillerkompetanse – Virksomhetskompetanse, sikkerhetskompetanse, integrasjonskompetanse, kompetanse på anskaffelser, juridisk kompetanse
- Gode risikovurderinger for å kunne ta riktig beslutning – faktorer som kan påvirke risikobilder (komplekse verdikjeder, tap av intern kompetanse, landrisikovurderinger)

- Riktige og gode krav til IKT-tjenesten og til leverandør
- Riktig beslutning på riktig nivå

Rapporten 90/2018 beskriver resultater fra en intervjustudie, og viktige elementer knyttet til leverandør-kjedesikkerhet (som danner grunnlag for anbefalinger til krav) er bl.a.:

- Det viktig med god oversikt over leverandørkjeden, dvs. oppdatert informasjon om leverandører og dens underleverandører. Tilsvarende er det nettselskapenes sitt ansvar å kjenne egen IKT-infrastruktur, og følge opp leverandørene i forhold til dette.
- Krav om hvor det er lov å lagre data (Landvurdering (Nato, EU, EØS)).
- Krav om hvor arbeidskraft hos leverandør og underleverandør kan sitte (Landvurdering (Nato, EU, EØS))
- Krav til hvilke endringer leverandører skal rapportere om, f.eks. omfang av endringer i programvare eller evt. endring i teknologi
- Jevnlig rapportering av hvor mange som har tilgang fra leverandør/underleverandør og hvilke tilganger dette gjelder
- Stole på store leverandører (vanskelig å få detaljert informasjon om sikkerhetsrutiner), aktuelt å gjennomgå sikkerhetsrutiner hos mindre leverandører
- Risikobilde endrer seg i løpet av livssyklus av et system, og det kan/vil bli behov for revidering av sikkerhet underveis. Det bør også være mulig å endre kontrakt underveis i livsløpet hvis risikobildet endrer seg. Elementer som bør inkluderes i kontrakt ved anskaffelse er f.eks.
    - Avtalefeste årlige revisjonsrapporter fra leverandøren
    - Varsling fra KraftCERT om sårbarheter i eget system
    - Lov å gjennomføre sikkerhetstester
    - Jevnlige møter med leverandør, med bl.a. sikkerhet som tema
    - Revidering av sikkerhet ved endringer (ny funksjonalitet)
- Kriterier knyttet til planer for hvordan håndtere ulike hendelser som kan påvirke sikkerhet
- Behov for bestillerkompetanse knyttet til IKT-sikkerhet. Tverrfaglig kompetanse trengs for å gjøre gode bestillinger – innen business, IKT og jus (Virksomhetskompetanse, sikkerhetskompetanse, integrasjonskompetanse, kompetanse om anskaffelser og juridisk kompetanse)
- Krav til at virksomhet kan gjennomføre tilsyn hos leverandører. (Det å kontraktsfeste rett til tilsyn av store leverandører kan være vanskelig).

4.2 IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen, NVE- Rapport nr. 1/2020 [3]

NVE-rapporten 1/2020 [3] er en sjekkliste for anskaffelser og tjenesteutsetting i energisektoren, bl.a. med utgangspunkt i at økt digitalisering påvirker risikobildet for energibransjen. Sjekklisten beskriver viktige punkter knyttet til forberedende fase, anskaffelsesfasen, implementering og forvaltningsfasen, og opphørsfasen. Momenter som er relevante for leverandørkjedesikkerhet, er oppsummert nedenfor.

Forberedende fase

For å oppnå et godt sikkerhetsnivå, må virksomheten vurdere hvordan tjenesten som settes ut/ anskaffelsen skal integreres med virksomhetens øvrige IKT-systemer.

- Risikovurdering av tjenesteutsetting og anskaffelse
- Vurdering av egne ferdigheter/forutsetninger og virksomhetens kontekst (Forretningsprosess, Informasjonsflyt, Kompetanse innen sikkerhet, anskaffelser, m.m.)
- Etterlevelse av krav (Lovkrav og retningslinjer som gjelder ved anskaffelser/tjenesteutsetting, interne sikkerhets- og beredskapsbehov og krav, kravspesifikasjon for krav til sikkerhet)
- Beslutning om tjenesteutsetting og anskaffelse (involvering av øverste ledelse)

Anskaffelsesfasen
Virksomheten skal være i stand til å vurdere kvaliteten av tilbudene fra ulike tilbydere i selve anskaffelsesfasen.

- Vurdering av ulike typer risikoer i anskaffelsesprosessen (Kompetanse, Landrisikovurdering)
    - Det er avgjørende at kontrakten stiller tydelige krav til leverandør og sikrer tydelig plassert ansvar med hensyn til IKT-sikkerhet.
- Krav til leverandør i forkant av anbud (Informasjonssikkerhetsavtale, krav om å følge alle relevante bestemmelser i kraftberedskapsforskriften, oppetid, krav til å iverksette tiltak dersom avvik fra leveransekravene oppdages, deteksjon, varsling og håndtering av sikkerhetstruende hendelser hos leverandør, krav til exit-strategi – f.eks. hvis leverandør kjøpes opp, går konkurs eller hvis tjenestetilbudet endres)
- Sikkerhetskrav (revisjonsrapport, bakgrunnssjekk, tilgangsstyring til systemer, Informere/orientere om skifte av underleverandører, sikkerhetsovervåking, godkjenningsprosedyrer for bruk av underleverandører)
- Anbudskriterier (leveransekrav, varighet på anskaffelsen)
- Evaluering og valg av leverandør (bakgrunnssjekk av leverandør og nøkkelpersonell hos leverandør, etablert eget team med nødvendig kompetanse, etterlevelse av internasjonale standarder for skytjenester)
- Kontraktsforhandling (gjennomgå sammen med leverandør)

Implementering og forvaltningsfasen
Omfatter implementering, integreringer og forvaltning av tjenesten som settes ut.

- Leverandørsamarbeid, kontroll og revisjon (avvikslogg, beredskapsøvelser)
- Kontinuerlig risikohåndtering og kvalitetsoppfølging (kontroll av endringer og hvorvidt de bør medføre krav til leverandørens tjenester)

Opphørsfasen
Perioden der leverandørforholdet skal avvikles og kontrakten skal avsluttes (f.eks. på grunn av tap av anbud, kontraktsbrudd, konkurs eller endrede uakseptable forhold ved vertslandet og/eller leverandør).

- Sikre kompetanseoverføring in-house, eller fra gammel til ny leverandør
- Plan for tilbakeføring av tjeneste til virksomheten (in-sourcing)

4.3 IKT-sikkerhetstilstanden i kraftforsyningen 2021, NVE 19/2021 [13]

NVE-rapporten 19/2021 [13] dokumenterer en spørreundersøkelse om IKT-sikkerhetstilstanden i kraftforsyningen for perioden 2020-2021, som bl.a. viser at 80% av virksomhetene har en IKT-sikkerhetsstrategi, men kun 35% har styringssystem for informasjonssikkerhet. Basert på spørreunder-søkelsen, er det 8% av virksomhetene som har hatt alvorlige IKT-hendelser i adm. IKT-systemer med konsekvenser for virksomhetens drift og 3% har hatt hendelser i driftskontrollsystemet med kortvarig konsekvens for funksjonen i driftskontrollsystemet. Ingen av disse hendelsene skylder cyberangrep.

I mai 2021 ble Volue rammet av et cyberangrep klassifisert som ransomware, dvs. et angrep designet for å ødelegge tilgang til tiler på maskiner og servere ved å kryptere dem, og kreve betaling for å få tilgang til dekrypteringsnøkkelen. God beredskapsplan og -forberedelse bidro til at virksomheten klarte å handle raskt mot angrepet. Viktige læringspunkter knyttet til mulige tiltak som kunne forhindret hendelsen:

- **Utvidet bruk av tofaktor-autentisering** både hos kundesystemer og egne interne systemer kunne bidratt til å forhindre hendelsen.

- **Døgnkontinuerlig respons på overvåkning av sikkerhetsvarsler** kunne bidratt til tidlig respons og reduksjon av konsekvenser
- Utelat muligheten for å betale ransom (løspenger) bidro til å sette søkelys på å forstå angrepet og hvordan reetablere normal drift raskere.
- **Revisjon av all backup** kan sikre at backup inkluderer alle kritiske systemer og data.
- **Forbedret forståelse av kundedata**, hvor de er lagret og konsekvenser ved tap av tilgang til data.

Rapporten viser at det er viktig å rette søkelyset mot å beskytte administrative IKT-systemer i tillegg til driftskontrollsystemet.

Resultater fra spørreundersøkelsen som beskrives i [13], viser at hendelser hos leverandør eller tredjepart er den vanligste årsaken til IKT-sikkerhetshendelser hos virksomheter i kraftforsyningen, der hendelsen har konsekvenser for virksomhetens drift eller driftskontrollsystemets funksjon.

En kjent sårbarhet er manglende oversikt over verdikjeder og avhengigheter av leverandører på tvers av landegrenser. Det observeres et økende omfang av tredjepartsangrep og epost-angrep gjennom leverandører, partnere og kunder, og det er grunn til å tro at risikoen for angrep vil øke ved bruk av IIoT (Industrial Internet Of Things) dersom underleverandørene har svak kontroll på egen verdikjede.

Gjennom overvåkning av nettverkstrafikken i driftskontrollsystemet er det mulig å oppdage unormal trafikk og om en trusselaktør forsøker å trenge seg inn i systemet. Undersøkelsen som presenteres i [13], viser at 60% av de virksomhetene som besvarte undersøkelsen, har monitorering/overvåkning av datanettverkstrafikken, mens 30% ikke har det, og 10% vet ikke. Virksomheters manglende eller begrensede mulighet for å undersøke hendelser i driftskontrollsystemene avdekker svakheter ved de aktuelle virksomhetenes sikkerhet.

God beredskap forutsetter at det foreligger gode rutiner for hendelseshåndtering som er trent på i forkant av hendelsen, bl.a. gjennom øvelser. For å ha en god beredskap mot uønskede digitale hendelser og krisesituasjoner er det viktig med et godt samarbeid med leverandørene.

Spørreundersøkelsen viser også hvorvidt virksomhetene mener selv de oppfyller NSMs grunnprinsipper for IKT-sikkerhet. Totalt er det 118 tiltak, som er prioritert ut fra 1 (grunnleggende), 2 og 3 (gi ytterligere sikkerhet). Spørreundersøkelsen fokuserte på 35 tiltak med prioritet 1 og 2, dvs. tiltak som virksomheter bør prioritere først. En oversikt over tiltak for IKT-sikkerhet, basert på NSMs grunnprinsipper, som kan være relevant grunnlag for utarbeidelse av krav til leverandørkjedesikkerhet, er vist i tabell 4.1

Tabell 4.1 Tiltak for å ivareta IKT-sikkerhet, basert på NSMs grunnprinsipper (Basert på [13])

Hovedkategorier NSMs grunnprinsipper	**Prioritet 1-tiltak**	**Prioritet 2-tiltak**
Identifisere og kartlegge *(Opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere)*	• Kartlegging av enheter og programvare – for å få oversikt over IKT-infrastrukturen • Det er mindre oversikt over programvare enn over fysiske enheter	• Manglende styringsstrukturer og prosesser for risikovurdering kan føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens sikkerhetsarbeid. • Ledelsen må fastsette hvilke grenser for risiko virksomheten aksepterer, hva som er

Hovedkategorier NSMs grunnprinsipper	Prioritet 1-tiltak	Prioritet 2-tiltak
		uakseptabel risiko og etablere kriterier for hvordan man evaluerer risiko sett opp mot virksomhetenes sikkerhetsmål.
Beskytte og opprettholde *(Ivareta en forsvarlig sikring av IKT-miljøet og opprettholde den sikre tilstanden over tid og ved endringer)*	• konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Etablerte rutiner for sporing, rapportering og korrigering av sikkerhets-konfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse. • Sikkerheten økes betraktelig dersom virksomheten har god kontroll på tillatt programvare.	• Beskytte data og systemer og opprettholde et sikkerhetsnivå. • Bygge en god sikkerhetsarkitektur med god styring på tilgangs-rettigheter fra ulike brukere og dataflyt.
Oppdage *(Løsninger for å oppdage sikkerhetstruende hendelser)*	• Analyse og innsamling av sikkerhetsrelevant data kan bidra til å forstå hendelsesforløpet og oppdage sikkerhetshendelser tidlig. • Sikkerhetsbrudd og uautoriserte handlinger bør oppdages så tidlig som mulig slik at skaden kan minimeres og aller helst forhindres. • Identifisere kritiske systemer og data og beslutte hvilke data som er sikkerhetsrelevante og skal samles inn	• Sikkerhetsbrudd og uautoriserte handlinger bør oppdages så tidlig som mulig slik at skaden kan minimeres og aller helst forhindres. For at hendelser skal oppdages raskt, er det nødvendig å kartlegge sårbarheter (Sårbarhetskartlegging). • Viktig å etablere tilstrekkelig sikkerhetsovervåking
Håndtere og gjenopprette *(Håndtere sikkerhetstruende hendelser effektivt)*	• Plan og en prosess for hendelses-håndtering for å begrense skaden og gjenopprette normal-tilstanden.	• Tydelig rolle- og ansvars-beskrivelser for personale som skal bidra i hendelses-håndteringen. • Hendelseshåndtering inkluderer: deteksjon, skadevurdering (triage), tiltak for skademini-mering, sikring av bevis ved angrep og gjenoppretting av integriteten til systemer og IT-nettverk.

4.4 Kraftbransjens leverandørkjeder, NVE nr. 18/2021 [5]

NVE-rapporten 18/2021 [5] beskriver en studie av leverandørkjedesårbarhet og sikkerhet som ble gjennomført sommeren 2021, og er basert på intervjuer med ressurspersoner i kraftforsyningen, litteraturstudier og spørreundersøkelser.

For å kunne forbedre arbeidet med leverandørkjedesikkerhet, må virksomhetene ha en oversikt over hva sårbarhetene i leverandørkjedene er. Digitale sårbarheter relatert til leverandørkjedeangrep (identifisert via taksonomien til ENISA) er kompleksitet, oversikt, avhengighet, tillit, bestillerkompetanse, resiliens og sikkerhetskultur.

Rapporten gir anbefalinger til hvordan bransjen kan forstå digital sårbarhet i leverandørkjedene, og hvordan virksomhetene kan jobbe med å redusere sårbarhetene. Punkter som er relevant underlag for utarbeidelse av krav knyttet til leverandørkjedesikkerhet, oppsummeres her.

Faktorer med betydning for IKT-sikkerhet som er viktige karakteristikker ved leverandørkjedesårbarheten:

- **Økonomisk globalisering** innebærer ulike former for avhengighet mellom aktører. Modulære verdikjeder gjør at virksomheter forholder seg til færre leverandører, som de har tettere relasjoner til. Leverandøren har da ansvaret for teknologien og produksjonsutstyret, men samtidig krever leverandører at kjøpere av produkter (f.eks. produkter som krever IT-støtte) har et ansvar for at disse brukes riktig (bl.a. ansvarlig for å oppdatere programvare på produktene)

Nedenfor er det gitt eksempler på utfordringer i leverandørkjeder (som muligens kan danne grunnlag for krav ved anskaffelse).

Oversikt

Oversikt og innsikt i egne systemer er viktig i styring av risiko og sikkerhet, men oversikt utfordres av kompleksitet og mangel på transparens, og ikke minst lange digitale verdikjeder[6]. Kontrakten inngås mellom kjøper og hovedleverandør, og ansvaret for underleverandørene ligger dermed hos hovedleverandøren og ikke kjøperen. Leverandører i andre land er underlagt nasjonalt lovverk og andre sikkerhetskrav, og de er ikke nødvendigvis villige til å dele sine interne dokumenter eller gi innsyn til virksomheter i andre land.

Markedsdominans og mangel på redundans

Redundans er et viktig virkemiddel som øker sikkerheten gjennom eksempelvis duplikasjoner, overlapp og reservesystemer som kan kompensere for eventuelle feil

Bestillerkompetanse

Dette innebærer å ha tilstrekkelig forståelse av virksomhetens behov, kvalitet på produktene som skal kjøpes, regelverk og IKT-sikkerhet i anskaffelsen. Innkjøpere må ha kompetanse til å stille de riktige spørsmålene slik at de tenker sikkerhet hele tiden. I følge rapporten stilles det sjeldent strenge krav til IT-sikkerhet når det gjøres innkjøp. NSMs landvurdering er også viktig å ta i betraktning når det gjøres anskaffelser.

[6] NVE Rapport (90/2018) [2] om IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen, beskriver energiselskapers leverandører sin plikt til å holde full oversikt over sine underleverandører.

Risikostyring og sikkerhetskultur

Kraftberedskapsforskriften[7] skal sikre forsvarlige beredskapsmessige hensyn for at kraftforsyningen skal kunne opprettholde sin funksjonalitet under ekstraordinære påkjenninger. § 6-9 i forskriften stiller særskilte krav til sikring og risikovurdering av digitale informasjonssystemer.

Risikostyring handler om virkemidlene som kan benyttes for å kontrollere risiko, og arbeidet med å redusere risiko og sårbarheter i digitale verdikjeder må inngå i de ordinære risikostyringsprosessene til virksomheten.

Sikkerhetskultur handler om hvordan sikkerhet prioriteres i organisasjoner, og holdningsskapende arbeid gjøres også på IKT-sikkerhet, men rapporten påpeker at kompetanse om leverandør-kjedesikkerhet er en utfordring. Cybersikkerhetsvurderinger og tiltak må bygges inn i design- og distribusjonsfaser, bl.a. for å forankre sikkerhetsarbeidet i virksomheten.

Rapporten avslutter med å gi noen anbefalinger til virksomheter i kraftforsyningen, knyttet til digitale sårbarheter i leverandørkjeden. Flere momenter er relevante knyttet til hvilke krav til sikkerhet som skal settes ved anskaffelse av IT-/OT-systemer, og det gjelder for eksempel:

- Det er viktig at virksomheter i kraftforsyningen *overvåker leverandørkjedene av viktig infrastruktur* for virksomhetens systemer og funksjoner, slik at beredskapsløsninger kan planlegges og iverksettes ved kritiske endringer i kjeden.
- Ved anskaffelse bør det *vurderes om det innebærer en risiko å sette ut tjenester til utlandet*.
    - NSM anbefaler at landvurderinger bør være en del av risikovurderingen ved tjenesteutsetting, og derfor utarbeidet følgende fire kriterier som bør inngå i den totale risikovurderingen ved tjenesteutsetting, og vektlegges med utgangspunkt i virksomhetens behov:
        - 1. Statlige styringsindikatorer.
        - 2. Cybersikkerhetstilstanden.
        - 3. IKT-infrastruktur og kompetanse.
        - 4. Forretningsstabilitet
    - I tillegg til disse indikatorene, bør også trusselvurderingene fra etterretningstjenesten og PST vurderes.
- DSB anbefaler å bruke tenkningen i *NS-ISO 31000* i modell for risikostyring knyttet til digitale verdikjeder. Modellen vil være nyttig i anskaffelser, så vel som under drift og vedlikehold av virksomhetenes systemer
- Det anbefales mer *samarbeid mellom IKT-avdeling og innkjøpsavdeling* for å få et helhetlig bilde på hva som faktisk skal kjøpes og hva anskaffelsen krever av sikkerhetstiltak.
    - Hvis sikkerhet inkluderes hver gang det gjøres anskaffelser, kan virksomheter sikre seg bedre.
- Det er ikke realistisk å detaljert følge opp leveranser og produksjon av *maskinvare*, og løsningen er heller å gjennomføre *hyppigere stikkprøver av produktene* som blir levert.
- Risikostyring
- Ifølge kraftberedskapsforskriften, skal ikke tjenesteutsetting redusere sikkerheten, og NSM påpeker at virksomhetene selv må ta ansvar for virksomhetens sikkerhet ved tjenesteutsetting. Dette innebærer følgende [5]:
    - Å ha *oversikt og kontroll* på hele livsløpet til tjenesten(e) som skal settes ut.
    - Å ivareta behovet for *bestillerkompetanse* gjennom hele livsløpet til tjenesteutsettingen.
    - Gjennomføre *gode risikovurderinger* som inkluderer IKT og hensyntar hele livsløpet.

[7] https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

- Utarbeide et *kravdokument for alle faser av tjenesteutsettingen* hvor krav kan verifiseres.
- *Avtaler om tjenesteutsetting* av IKT-tjenester og endringer i slike avtaler skal behandles i henhold til virksomhetens fullmaktsstruktur.
- Det bør sjekkes at *leverandøren har utviklingsplaner* for fremtidig sikkerhetsfunksjonalitet i tjenestene i tråd med utvikling i teknologi og trusselbildet over tid.

- Kompleksitet krever sterkere systemorientering, men det kan være vanskelig å gjennomføre i praksis. Viktige punkter er:
  - Virksomhetene må kjenne til og ta ansvar for egne systemer.
  - Virksomhetene må vite grensene til omgivelsene.
  - Virksomhetene må være i stand til å kontrollere og korrigere viktige prosesser.
  - Avhengighetene til leverandørkjedene må avklares.
  - Systemtenkning handler om kommunikasjon og kontroll.

5 Anbefalinger til krav knyttet til anskaffelse av IT og OT, med spesielt fokus på leverandørkjede

Vi vil i det følgende gi krav til leverandører, delt inn i "må-krav" og ytterligere anbefalinger.

Kravene er vurdert som "må" og "ytterligere anbefalinger" ut fra følgende kriterier:

- Må-krav: Kravene er basert på krav i gjeldende regelverk (forskriftskrav). Legg imidlertid merke til at vi tolker dette videre enn kun NVEs myndighetsområde, slik at f.eks. krav som kommer fra GDPR også kommer til anvendelse her. Legg også merke til at Kraftberedskapsforskriftens §6.9 [14] legger relativt brede føringer for "sikr[ing] av digitale informasjonssystemer".
- "Ytterligere anbefalinger": Basert på anbefalinger fra et begrenset antall intervjuer med aktører i kraftbransjen, anbefalinger fra tidligere NVE-rapporter, og anbefalinger fra fagfellevurdert litteratur fra de to siste årene (NSMs grunnprinsipper, …)

Kravene slik de er presentert, må anses som et første utkast, og vi anbefaler at det gjennomføres en større "høringsrunde" med nettselskaper og leverandører for å innhente tilbakemeldinger før NVE eventuelt formaliserer kravene.

Et nettselskap står fritt til å oppgradere "bør"-krav til "må"-krav i et konkret anbud.

5.1 Forutsetninger for nettselskapene

En viktig forutsetning for å lykkes med innkjøp av varer og tjenester, er å ha tilstrekkelig bestiller-kompetanse [15]. Bestillerkompetanse er et vidt begrep, og omfatter generell virksomhetskompetanse, IKT-sikkerhetskompetanse, integrasjonskompetanse, kompetanse om anskaffelser og juridisk kompetanse. For å gjøre gode bestillinger, trenger man altså tverrfaglig kompetanse. I følge NSM [15] trenger man virksomhetskompetanse for å kunne definere behov og stille relevante krav, og IKT-sikkerhetskompetanse trengs følgelig for å kunne stille fornuftige sikkerhetskrav. Kjennskap til virksomheten er også viktig for å kunne vurdere hvordan det man bestiller kan integreres i eksiterende systemer, og det er nødvendig med kjennskap til eksisterende APIer, protokoller og andre grensesnitt. Dersom eksisterende systemer f.eks. kommuniserer med et gitt sett av protokoller, kan det bli katastrofalt dersom det bestilles noe som forutsetter helt andre protokoller – dette har vi sett flere eksempler på i senere tid. Generell kunnskap om anskaffelsesprosesser i virksomheten er viktig for å sørge for at anskaffelser passer inn i etablerte mønster og rutiner (se også i sammenheng med virksomhetsforståelse).

Det er imidlertid vanskelig å formulere allmenngyldige krav om dette, og dette er også vanskelig å måle. Store nettselskaper vil typisk ha bedre tilgang på bestillerkompetanse enn små nettselskaper. Det vil være viktig med et samarbeid mellom de som er ansvarlige for drift av IT/OT og innkjøpsavdeling. I forbindelse med utrullingen av smarte målere i Norge, gikk mange mindre nettselskap sammen i allianser for å kunne dekke opp kompetansekravene i anskaffelsesprosessen

5.2 Må-krav

Følgende krav **må** oppfylles av alle leverandører til kraftbransjen.

5.2.1 Periodisk risikovurdering

Leverandører må omfattes av periodisk risikovurdering slik at nettselskaper kan oppfylle sin sikringsplikt [4]. Nettselskapet kan benytte sjekklister (se 4.2).

5.2.2 Kartlegge hvordan leverandør kan bistå i en akutt situasjon

Leverandøren må dokumentere hvordan den kan bistå kunden i en akutt situasjon som involverer leverandørens produkter eller tjenester, herunder hendelseshåndtering. Dette skal spesifiseres i leverandørkontrakten eller tilsvarende avtale.

5.2.3 Øvelser

Leverandører må involveres i beredskapsøvelser som berører deres produkter og/eller tjenester [13], iht. det som er avdekket i 5.2.2. Dette skal angis i leverandørkontrakten eller tilsvarende avtale.

Dette er ikke ment å tolkes dithen at det ikke skal være mulig å arrangere øvelser uten å involvere alle leverandører dersom nettselskapet anser det som hensiktsmessig å også gjennomføre mer avgrensede beredskapsøvelser.

5.2.4 Plassering av servere

Dersom tjenesten som leveres skal behandle sensitiv informasjon (personopplysninger), må servere som benyttes av tjenesten være plassert i et land som tilfredsstiller til enhver tid gjeldende regler for servere og personopplysninger som GDPR-lovverket krever, noe som p.t. er EU/EØS [2]. Dette gjelder også forskjellige former for skyløsninger [16].

5.2.5 Kraftsensitiv informasjon

Dersom tjenesten som leveres skal behandle kraftsensitiv informasjon, må servere som benyttes av tjenesten være plassert i et land som tilfredsstiller krav til anskaffelse av driftskontrollsystem for klasse 2 og høyere [4], [14].

5.2.6 Plassering av ansatte

Dersom tjenesten som leveres skal behandle sensitiv informasjon, må leverandørens ansatte som får tilgang til slik informasjon fysisk befinne seg i EU/EØS [2].

Utover dette kravet, må leverandører også gjøre ytterligere vurdering av nasjonalitet, avhengig av type oppgaver som skal utføres, også når det ikke er behov for sikkerhetsklarering. Strategiske/ledende roller skal ikke fylles av ansatte med nasjonalitet fra land vi ikke har sikkerhetspolitisk samarbeid med.

5.2.7 Eierskap til data

For tjenester som innebærer at leverandøren behandler nettselskapets data i leverandørens infrastruktur, må det eksplisitt angis i leverandørkontrakten at eierskapet til slike data beholdes av nettselskapet.

5.3 Ytterligere anbefalinger

Følgende krav **bør** oppfylles dersom det er mulig, og begrunnelse skal gis i de tilfellene man velger å se bort fra dem.

5.3.1 Software Bill of Materials

All programvare bør ha en mekanisme for å kunne spore de forskjellige delene av programvaren tilbake til opphav, og for å holde styr på hvilke versjoner av programvarebiblioteker osv. som er benyttet, slik at man kan avgjøre om oppdatering er nødvendig når nye sårbarheter oppdages. Dette kan være i form av en Software Bill of Materials (SBOM) [17] eller tilsvarende løsning. Leverandøren er ansvarlig for å vedlikeholde en oversikt for den versjonen som kunden til enhver tid bruker, men dette medfører ikke at kunden skal ha sanntids innsikt i detaljer i leverandørens løsning (f.eks. i en SaaS løsning). Når en ny

sårbarhet blir offentlig kjent, bør leverandøren umiddelbart kunne svare på om tjenesten/produktet er berørt av sårbarheten. Dette betyr også at nettselskapet bør ha mulighet til å føre kontroll av endringer i produkter og/eller tjenester.

5.3.2 NSM grunnprinsipper eller tilsvarende

Leverandører bør dokumentere i hvilken grad de tilfredsstiller NSMs Grunnprinsipper for IKT-sikkerhet [18] (nivå 1&2) eller tilsvarende rammeverk, som f.eks. ISO/IEC 27001 [19] eller NIST CSF [20]. Disse to er eksempler på ledelsesstandarder/retningslinjer som i stor grad har fungert som inspirasjon for NSMs grunnprinsipper. Det finnes også mer teknologiorienterte systemstandarder som IEC 62443 [21] som kan være relevante .

5.3.3 VSA sjekkliste

Nye leverandører bør dokumentere sin leveranse iht. sjekklisten fra Vendor Security Alliance[8] . Litteraturen bekrefter at løsninger som spørreskjemaer til leverandørene er blant de primære verktøyene som brukes [7]. Sjekklisten fra VSA oppdateres med jevne mellomrom.

Sjekklisten fra VSA kan lastes ned gratis hvis man registrerer seg på deres nettside. Det finnes en utvidet versjon og en kjerneversjon, sistnevnte består av et regneark med 9 fliker:

- Introduksjon til sjekklisten
- Introduksjon til tjenesten som skal leveres
- Dataoversikt
- Sikkerhetskontroller
- Introduksjon til personvern
- USA personvern
- GDPR personvern
- Definisjoner
- Juridiske begrep

Dataoversikten brukes for å avklare hvilke typer data leverandøren samler inn fra sine brukere, f.eks.:

- Alder
- Adresse
- Utdannelse
- Epostadresse
- …

Under sikkerhetskontroller er det spørsmål som:

- Hvordan krypterer dere kundedata (i transitt, i ro)?
- Hvilke grupper av ansatte (faste og innleide) har tilgang til personlig og sensitiv informasjon om kunder?
- Har dere et dedikert informasjonssikkerhetsteam? Hvordan er det i så fall satt sammen, og hvilken rapportstruktur er på plass?
- Må alt personell undertegne en taushetserklæring?
- Hvordan evalueres jevnlige oppdateringer for deres infrastruktur?
- Beskriv deres hendelseshåndteringsprogram.

[8] https://www.vendorsecurityalliance.org/

5.3.4 Prosess for håndtering av sårbarheter

Leverandøren bør ha en dokumentert prosess for håndtering av sårbarheter iht. god praksis, inkludert en mekanisme for å distribuere hurtigoppdateringer (patches) [22].

5.3.5 Redundans mellom underleverandører

Leverandører bør sørge for redundans slik at alternative underleverandører kan benyttes ved bortfall av en underleverandør.

5.3.6 Overføring av data og konfigurasjon ved terminering av kontrakt

Leverandørkontrakten bør spesifisere hvordan leverandøren skal bistå med overføring av data og konfigurasjon til en ny leverandør ved terminering av kontrakt.

5.3.7 Oversikt over verdikjeder

Leverandører bør kunne dokumentere den fullstendige underleverandørkjeden for sitt produkt eller tjeneste, spesielt over landegrenser. NSMs anbefalinger om landvurdering bør tas med i betraktning når man vurderer den totale verdikjeden.

5.3.8 Automatisert monitorering av tjenester

Det vil være gunstig om leverandøren kan legge til rette for automatisert monitorering av den tilbudte tjenesten for å godtgjøre at den til en enhver tid tilfredsstiller de avtalte sikkerhetskravene [7]. Dette kan også omfatte innsyn i tredjeparts revisjonsrapporter. Tilsyn hos leverandør bør kunne gjøres av nettselskap og/eller NVE.

5.3.9 Sikker utvikling

Det vil være gunstig om leverandøren kan dokumentere en prosess for sikker utvikling iht. god praksis [22], [23], f.eks. som angitt i IEC 62443 [24]. Prosessen må være hensiktsmessig for det aktuelle produktet eller tjenesten.

5.3.10 Herding av løsninger

Det vil være gunstig om produkter og tjenester som leveres er "herdet" ved å fjerne alle komponenter og delsystemer som ikke er strengt nødvendige [10].

5.3.11 Separasjon mellom kunder

Det vil være gunstig om leverandøren kan dokumentere hvordan den ivaretar separasjon mellom kunder, både teknisk og med hensyn til i hvilken grad personell har tilgang til data for flere kunder.

6 Konklusjon og videre arbeid

Denne rapporten presenterer resultater fra gjennomgang av tidligere NVE-rapporter rundt temaet leverandørkjedesikkerhet, supplert med et litteratursøk blant nyere akademisk litteratur og diskusjoner med et lite utvalg av bransjeaktører, og anbefaler basert på dette et sett med anbefalinger til krav knyttet til anskaffelse av IT og OT, med spesielt fokus på leverandørkjede.

Det er utarbeidet krav og anbefalinger (må- og bør-krav), rettet mot spesielt mot små og mellomstore nettselskap til bruk i anskaffelsesprosesser. Kravene som er utarbeidet og presentert i kap. 5, må anses som et første utkast, og vi anbefaler at det gjennomføres en større "høringsrunde" med nettselskaper og leverandører for å innhente tilbakemeldinger før NVE eventuelt formaliserer kravene.

For mer utdypende krav, bør det gjøres et større arbeid knyttet til mer empiri og dialog med ulike aktører i bransjen – av ulik størrelse. Vi ser at det er et behov for mer koordinering av innkjøpsprosesser, og sannsynligvis må det finne sted en samling i bransjen i form av innkjøpsallianser eller lignende for å kunne møte utfordringene rundt å stille krav til de store leverandørene.

Krav og anbefalinger bør ikke bare basere seg på historiske erfaringer, men også inkludere vurderinger basert på ulike scenarioer og mer proaktive tiltak for å ivareta leverandørkjedesikkerhet.

7 Referanser

[1] *Lov om offentlige anskaffelser (anskaffelsesloven)*, vol. LOV-2016-06-17-73. 2017. Accessed: Jan. 29, 2023. [Online]. Available: https://lovdata.no/dokument/NL/lov/2016-06-17-73

[2] E. Kirkebø and M. Ljøsne, 'IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen', NVE, Nr. 90/2018, Oct. 2018. [Online]. Available: https://publikasjoner.nve.no/rapport/2018/rapport2018_90.pdf

[3] M. Maal, K. Krogedal, and A. Gjengstø, 'IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen - sjekkliste', NVE, Nr. 1/2020, Jan. 2020. [Online]. Available: https://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf

[4] 'Veiledning til kraftberedskapsforskriften'. NVE. [Online]. Available: https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/

[5] S. H. Selnes, S. R. Moen, S. E. Ji, and O. Njå, 'Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder', NVE, 2021:18. Accessed: Sep. 26, 2022. [Online]. Available: https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_18.pdf

[6] B. A. Kitchenham, 'Systematic review in software engineering: where we are and where we should be going', in *Proceedings of the 2nd international workshop on Evidential assessment of software technologies*, 2012, pp. 1–2.

[7] J. Viega and J. B. Michael, 'Struggling with Supply-Chain Security', *Computer*, vol. 54, no. 7, pp. 98–104, 2021, doi: 10.1109/MC.2021.3075412.

[8] X. Wang, 'On the Feasibility of Detecting Software Supply Chain Attacks', presented at the Proceedings - IEEE Military Communications Conference MILCOM, 2021, vol. 2021-November, pp. 458–463. doi: 10.1109/MILCOM52596.2021.9652901.

[9] A. R. Nygård and S. Katsikas, 'SoK: Combating threats in the digital supply chain', in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna, Austria, 2022. doi: 10.1145/3538969.3544421.

[10] J. Yang, Y. Lee, and A. P. McDonald, 'SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies', presented at the SNPD 2021: Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2022, vol. 1012 SCI, p. 58. doi: 10.1007/978-3-030-92317-4_4.

[11] J. Hagen, O. Hermansen, Ø. Toftegård, J.-M. Pettersen, R. Steen, and S. L. Paulen, 'Regulering av IKT-sikkerhet', NVE, NVE rapport 26–2017, Mar. 2017. [Online]. Available: http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

[12] 'Informasjonssikkerhetstilstanden i energiforsyningen', NVE, NVE Rapport 90–2017. [Online]. Available: http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

[13] F. K. Tøien, J. Fagermyr, G. Treider, and H. Remvang, 'IKT-sikkerhetstilstanden i kraftforsyningen 2021', NVE, Nr. 19/2021, Desember 2021. [Online]. Available: https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf

[14] *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)*. 2019. Accessed: Jan. 25, 2023. [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

[15] 'Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester'. NSM, Jul. 01, 2020. [Online]. Available: https://nsm.no/getfile.php/133998-1593590999/NSM/Filer/Dokumenter/Rapporter/2020-07-01%20-%20Temarapport%20-%20Tjenesteutsetting.pdf

[16] 'Cybersecurity — Supplier relationships — Part 4: Guidelines for security of cloud services'. ISO/IEC, 2016. [Online]. Available: https://www.iso.org/standard/59689.html

[17] É. Ó. Muirí, 'Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)'. NTIA, Nov. 12, 2019. [Online]. Available: https://ntia.gov/files/ntia/publications/framingsbom_20191112.pdf
[18] 'Grunnprinsipper for IKT-sikkerhet 2.0'. Nasjonal sikkerhetsmyndighet, Jun. 05, 2020. Accessed: Jan. 29, 2023. [Online]. Available: https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf
[19] ISO, 'ISO/IEC 27001:2013', Standard. Accessed: Mar. 22, 2022. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html
[20] M. G. Jaatun, E. Wille, K. Bernsmed, and S. S. Kilskar, 'Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer', SINTEF Digital, Trondheim, SINTEF rapport 2021:00055, 2021. Accessed: Jan. 29, 2023. [Online]. Available: https://sintef.brage.unit.no/sintef-xmlui/handle/11250/2835081
[21] 'IEC 62443: Industrial communication networks - Network and system security'. IEC. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443
[22] 'Threat Landscape for Supply Chain Attacks', Report/Study, Jul. 2021. Accessed: Jan. 05, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[23] CISA, 'Defending Against Software Supply Chain Attacks'. Cybersecurity and Infrastructure Security Agency, Apr. 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[24] 'IEC 62443-2-4:2015 | Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers'. IEC, 2015. Accessed: Jan. 25, 2023. [Online]. Available: https://webstore.iec.ch/publication/22810

A Oversikt over artikler fra søk

I det følgende presenteres en liste av artikler funnet ved litteratursøk som beskrevet i kapittel 3, og som ble vurdert som muligens relevante etter vurdering av tittel. Kolonnen "Relevant?" angir om artikkelen ble ansett som relevant etter vurdering av abstract.

Nr	Tittel	Forfatter(e)	Relevant?
1	Cyberattack Ontology: A Knowledge Representation for Cyber Supply Chain Security	Yeboah-Ofori, A., Ismail, U.M., Swidurski, T., Opoku-Boateng, F.	Nei
2	On the Feasibility of Detecting Software Supply Chain Attacks	Wang, X.	Ja
3	Struggling with Supply-Chain Security	Viega, J., Michael, J.B.	Ja
4	Information Security Assessment and Certification within Supply Chains	Santos, H., Oliveira, A., Soares, L., Satis, A., Santos, A.	Nei
5	SoK: Combating threats in the digital supply chain	Nygård, A.R., Katsikas, S.	Ja
6	Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study	Martínez, J., Durán, J.M.	Kanskje
7	Cybersecurity Certification Requirements for Supply Chain Services	Kyranoud, P., Kalogeraki, E.-M., Michota, A., Polemi, N.	Kanskje
8	Economics of Supply Chain Cyberattacks	Kshetri, N.	Nei
9	Analytic hierarchy process (ahp) for supply chain 4.0 risks management	Zekhnini, K., Cherrafi, A., Bouhaddou, I., Benghabrit, Y.	Kanskje
10	SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies	Yang, J., Lee, Y., McDonald, A.P.	Ja
11	Risk Indicators and Data Analytics in Supply Chain Risk Monitoring	Stampe, L., Hellingrath, B.	Nei
12	IoT and Supply Chain Security	Kieras, T., Farooq, J., Zhu, Q.	Nei

13	Applying NIST SP 800-161 in supply chain processes empowered by artificial intelligence	Al-Alawi, L., R. Al-Busaidi, and S. Ali.	Nei
14	Energy Resilience Impact of Supply Chain Network Disruption to Military Microgrids	Anuat, E., D.L. Van Bossuyt, and A. Pollman.	Kanskje
15	Alice in (Software Supply) Chains: Risk Identification and Evaluation.	Benedetti, G., L. Verderame, and A. Merlo.	Kanskje
16	Integrating Zero Trust in the Cyber Supply Chain Security	Do Amaral, T.M.S., and J.J.C. Gondim	Kanskje
17	Cyber Supply Chain Risk Management and Performance in Industry 4.0 Era: Information System Security Practices in Malaysia	Fernando, Y., M.-L. Tseng, I.S. Wahyuni-Td, A.B.L. de Sousa Jabbour, C.J. Chiappetta Jabbour, and C. Foropon	Kanskje
18	Supply Chain Flows and Stocks as Entry Points for Cyber-Risks	Filho, N.G., N. Rego, and J. Claro.	Kanskje
19	Functional Requirements and Supply Chain Digitalization in Industry 4.0	Han, L., H. Hou, Z.M. Bi, J. Yang, and X. Zheng.	Nei
20	A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures	Hassija, V., V. Chamola, V. Gupta, S. Jain, and N. Guizani	Nei
21	I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions	Kieras, T., J. Farooq, and Q. Zhu.	Kanskje
22	A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities	Pitney, A.M., S. Penrod, M. Foraker, and S. Bhunia	Nei
23	Internet of Things in Supply Chain Management: A Systematic Review Using the Paradigm Funnel Approach	Rajabzadeh, M., S. Elahi, A. Hasanzadeh, and M. Mehraeen.	Nei

24	A Taxonomy for Threat Actors' Delivery Techniques	Villalón-Huerta, A., I. Ripoll-Ripoll, and H. Marco-Gisbert	Nei
25	A Data Processing Pipeline for Cyber-Physical Risk Assessments of Municipal Supply Chains	Weaver, G.A. Yeboah-Ofori, A., S. Islam, S.W. Lee, Z.U. Shamszaman, K. Muhammad, M. Altaf, and M.S. Al-	Nei
26	Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security	Rakhami.	Nei
27	Supply Chain 4.0 Risk Management: Bibliometric Analysis and a Proposed Framework	Zekhnini, K., A. Cherrafi, I. Bouhaddou, and Y. Benghabrit	Nei
28	On the Impact of Security Vulnerabilities in the Npm and RubyGems Dependency Networks	Zerouali, A., T. Mens, A. Decan, and C. De Roover	Nei
29	Cyber-Security Risk Management and Control of Electric Power Enterprise Key Information Infrastructure	Zhang, G., Y. Xu, Y. Hou, L. Cui, and Q. Wang.	Nei
30	Summary of Risk Warning of Electric Power Material Supply Chain	Zhang, Z., S. Feng, and T. Hu.	Nei
31	Evaluation Indicators for Open-Source Software: A Review	Zhao, Y., R. Liang, X. Chen, and J. Zou.	Nei