DNV·GL

IKT-SIKKERHET – ROBUSTHET I PETROLEUMSSEKTOREN

Resiliens mot cyberhendelser og kan blokkjede bidra?

Petroleumstilsynet

Rapport nr.: 2019-0825, Rev. 0
Dato: 2020-02-21

Prosjekt navn:	IKT-sikkerhet – Robusthet i petroleumssektoren	DNV GL AS
Rapport tittel:	Resiliens mot cyberhendelser og kan blokkjede bidra?	Digital solutions Postboks 300
Kunde:	Petroleumstilsynet, P.O. Box 599 4003 Stavanger Norway	1322 Høvik Norway
Kontaktperson:	Arne Halvor Embergsrud	
Dato:	2020-02-21	
Prosjekt nr.:	101572712	
Organisation unit:	Cyber Security Services	
Rapport nr.:	2019-0825 Rev. 0	
Dokument nr.:		

Kontrakt for leveranse av denne rapport:

Kontrakt 06677 IKT-sikkerhet – Robusthet i petroleumssektoren - Prosjekt 992709

Hensikt: DNV GL har fått i oppdrag av Ptil å vurdere hvordan metoder for å bygge resiliens, kan anvendes for å gjøre IKT-sikkerhet knyttet til industrielle IKT systemer mer robust. DNV GL har også vurdert hvordan prinsipper for IKT-sikkerhet kan anvendes i relasjon til blokkjedeteknologi og hvordan sikkerheten kan ivaretas og eventuelt styrkes ved implementering av blokkjede.

Utarbeidet av:

Rolf Lervik
Senior Principal Consultant

Elisabet Line Haugsbø
Senior Engineer

Egil Wille
Senior Engineer

Håvard Grindheim
Principal Consultant

Verifisert av:

Boye Tranum
Associate Director

Kenneth Kvinnesland
Senior Principal Consultant

Tor Helge Kristiansen
Principal Consultant

Jon Jerre
Senior Principal Consultant

Godkjent av:

Trond Solberg
Head of Section, Cyber Security Services

DNV GL Distribution:

☒ Unrestricted distribution (internal and external)
☐ Unrestricted distribution within DNV GL
☐ Limited distribution within DNV GL after 3 years
☐ No distribution (confidential)
☐ Secret

Keywords:

Cybersecurity, Digitalisation, Oil & Gas, Resilience, Blockchain

Rev. nr.	Dato	Formål	Utarbeidet av	Verifisert av	Godkjent av
0	21.2.2020	Første utgave	RLER	BOTRA	TROSOL

INNHOLD

1 SAMMENDRAG

Petroleumstilsynet (Ptil) har gitt DNV GL oppdrag å vurdere hvordan metoder for å bygge resiliens, kan anvendes for å gjøre IKT-sikkerhet knyttet til industrielle IKT systemer mer robust. DNV GL har også vurdert hvordan prinsipper for IKT-sikkerhet kan anvendes i relasjon til blokkjedeteknologi og hvordan sikkerheten kan ivaretas og eventuelt styrkes ved implementering av blokkjede. Denne rapporten utgjør en delleveranse i prosjektet, IKT-sikkerhet – robusthet i petroleumssektoren.

Anvendelse av ny teknologi og stadig mer digitalisering i petroleumsnæringen bidrar til besparelser og økt produktivitet, men skaper også en større angrepsflate for IKT-sikkerhetstrusler. Det er ikke lenger bare generelle IT-systemer som utsettes for dataangrep, nå har også industrielle IKT-systemer blitt attraktive mål. Driftsoperatører og annet teknisk personell har på kort tid gått fra å jobbe med isolerte systemer til å være en sentral del av virksomhetens cyber-forsvar, fordi de industrielle IKT-systemene blir stadig mer eksponerte.

For å ivareta effektiv, sikker og pålitelig drift, er det viktig at ikke bare teknologi, men også personell og organisasjon er forberedt på å håndtere uønskede hendelser. God IKT-sikkerhet vil i økende grad være et konkurransefortrinn.

Cyber-resiliens er mer enn å forhindre eller å respondere på en hendelse – cyber-resiliens handler også om evnen til å opprettholde helt eller delvis operasjon mens hendelsen pågår. I tillegg handler cyber-resiliens om å tilpasse forsvaret etter dagens risikobilde, samt evnen til å komme seg tilbake i normal drift, så fort som mulig, etter en cyber-hendelse. Det viktigste her er barrieretankegang og å følge det gamle speidermotto om å være beredt. Gode beredskapsplaner, testing, trening og øvelser på ulike scenarier er viktige ingredienser for å sikre cyber-resiliens.

Like viktig er det å følge med på endringer i risikobildet i form av nye trusler og sårbarheter. Arbeidet med cyber-resiliens blir aldri ferdig. Her, som mange steder ellers, gjelder kontinuerlig forbedring.

Digitalisering og ny teknologi skaper nye muligheter, men kan også føre til nye sårbarheter. Hvis man for eksempel ønsker å eksportere måledata fra produksjonen og foreta beregninger i skyen, for så å sende resultatet tilbake for å endre parametere for optimalisering av produksjonen, er det en utfordring å gjøre dette på en sikker måte. Denne problematikken kunne vært gjenstand for en egen studie.

Blokkjede bidrar til sikkerhet og resiliens i form av at denne teknologien sikrer sporbarhet av data og transaksjoner og er «tamper-proof», dvs. man kan stole på det som er lagret. Imidlertid er man ikke garantert 100 % sikkerhet, da fortsatt noen av de vanlige sårbarhetene (for eksempel svake passord) ligger i «endene» av blokkjeden.

Blokkjede har noen anvendelsesområder som den er godt skikket for. Det synes å være særlig to generiske tilfeller hvor blokkjedeteknologien vil kunne bidra i positiv retning, både når det gjelder effektivisering og resiliens: 1) effektivisere og øke sikkerheten i eksisterende prosesser mellom flere aktører der det ikke er en sentral motpart, for eksempel styring av leveransekjeder og 2) bidra til helt nye måter å gjøre ting på, for eksempel smarte kontrakter.

I blokkjedeteknologi er det gjennomgående stort behov for lagringsplass og kommunikasjon mellom nodene. Noen løsninger har stort energibehov. Skalering er en utfordring. I tillegg er blokkjede foreløpig en umoden teknologi og det er usikkert hvilke typer blokkjeder som vil bli foretrukket og markedsledende. Noen av de eksemplene vi har sett på mulig bruk av blokkjede kan i dag enklere og på en nesten like sikker måte, implementeres ved hjelp av vanlige, sentrale databaser. På den annen side er teknologien i rivende utvikling, så en sannhet i dag er ikke nødvendigvis en sannhet i morgen.

2 ENGLISH SUMMARY

The Petroleum Safety Authority Norway (PSA) has given DNV GL the task of evaluating how methods for building resilience can be used to improve cybersecurity for industrial control systems (ICS). DNV GL has also evaluated how principles for cybersecurity can be used in relation to blockchain technology and how security can be maintained and potentially strengthened by implementation of blockchain. This report is a partial delivery in the project, Cyber security – robustness in the petroleum sector.

Use of new technology and accelerated digitalisation in the petroleum industry contribute to savings and improved productivity, but also represent a larger cyberattack surface. There are no longer only general IT-systems that are exposed to cyberattacks, in later years ICS have also become increasingly attractive targets. Operators and other technical personnel have in a short time span gone from working with isolated system, to becoming a central part of the organisation's cyber defence, because the industrial control systems are becoming more exposed.

To ensure efficient, secure and reliable operations, it is important that not only technology but also the personnel and organisation are prepared to handle unwanted events. Good cyber security will be an increasingly important competitive advantage.

Cyber-resilience is more than preventing and responding to an incident – cyber-resilience is also concerned with the ability to continue operations fully or partly, while the incident is still developing. In addition, cyber-resilience is to adapt the defence according to today's risk picture, and the ability to recover to normal operations, as soon as possible, after a cyber-attack. The most important elements in this respect are the barrier philosophy and to follow the old motto about being prepared. Good preparedness, plans, testing, training and exercises on different scenarios are important elements for assuring cyber-resilience.

It is of equal importance to follow-up on changes in the risk picture in terms of new threats and vulnerabilities. Here, as in many other places, continuous improvement is what matters.

Digitalisation and new technology create new opportunities but may also represent new vulnerabilities. In case someone wants to export measurement data from the production environment and perform cloud computing and returning the result to change parameters for production optimisation, it is a challenge to do this in a secure way. This problem could be subject for a separate study.

Blockchain contributes to security and resilience by securing traceability of data and transactions and is tamper-proof, so one can trust what has been stored. However, one is not guaranteed 100 % security as some of the usual vulnerabilities (as for instance weak passwords) are sitting at the "ends" of the blockchain.

Blockchain has some applications that it is well suited for. There seems to be two generic occurrences where blockchain may contribute in a positive way, both for efficiency and resilience; 1) improve efficiency and security in existing processes between actors where there is no central counterpart, for instance management of supply chains; and 2) contribute to new ways of doing business, for instance smart contracts.

In blockchain technology there is generally a large need for storage space and communication between the nodes. Some solutions demand a lot of energy. Scalability is a challenge. In addition, blockchain is still an immature technology and it is uncertain which type of blockchain will be the preferred one. Some of the use cases where we have looked on the possibility of using blockchain may, in an almost equally secure way, be implemented by use of ordinary central databases. On the other hand, the technology is developing fast, so a truth today may not necessarily be a truth tomorrow.

3 INNLEDNING

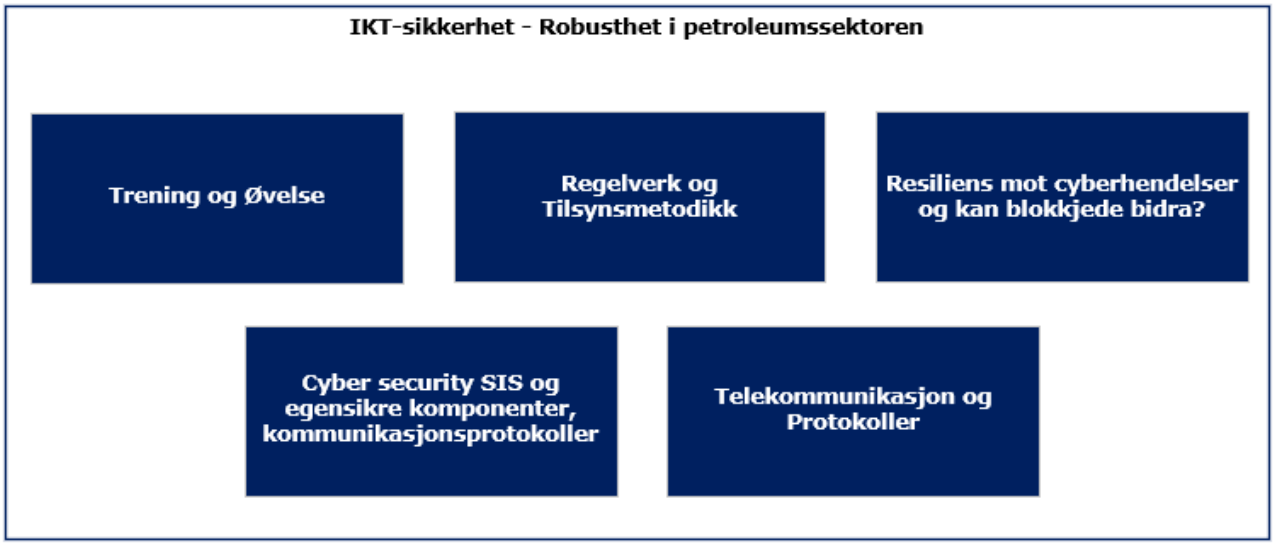
3.1 Bakgrunn

Digitalisering i olje- og gass-sektoren åpner opp for effektivisering, men gjør også sektoren mer sårbar for IKT-sikkerhetshendelser. Olje- og gass-sektoren er et mål for trusselaktører både på grunn av de store verdier sektoren representerer, og for aktivister med idealistisk eller politisk motivasjon.

Utvinning, transport og distribusjon av hydrokarboner medfører en risiko for ulykker med konsekvenser for liv og helse, miljø og materielle verdier. For å redusere risiko for slike ulykker, er det installert en rekke sikkerhetssystemer. Mange av disse sikkerhetssystemene benytter IKT-teknologi og kan være sårbare for IKT-sikkerhetshendelser. Manglende eller feil funksjonalitet i sikkerhetssystemene kan få katastrofale konsekvenser. Det er et mål at IKT-sikkerhetshendelser ikke skal påvirke sikkerhetssystemene.

Petroleumstilsynet gjennomfører en satsing på IKT-sikkerhet i perioden 2018-2021. Målet er å gå i dybden på en del viktige områder, innhente kunnskap om den teknologiske utviklingen og vurdere hvordan dette påvirker risikobildet. Nylig er det publisert rapporter innen temaene «Kunnskap IKT-sikkerhet og CERT» og «Fjernarbeid og HMS». Videre pågår det en utredning om «Industriell IKT og IIoT».

Petroleumstilsynet utlyste en konkurranse for å utrede «IKT-sikkerhet – Robusthet i petroleumssektoren», som inneholder flere arbeidspakker og delleveranser, som illustrert i figuren under. Dette oppdraget ble tildelt DNV GL. Alle arbeidspakker har gjennomført intervjuer og innhentet informasjon fra aktørene i bransjen, samt innhentet erfaringer med tilsyn av IKT-sikkerhet i andre sektorer.



Figur 3-1 Delleveranser i prosjektet

Anvendelse av ny teknologi og stadig mer digitalisering i olje- og gass-sektoren åpner ikke bare opp for effektivisering, men skaper også en større angrepsflate for cyber-trusler. Industrielle kontrollsystemer har gått fra å være helt eller delvis isolerte, til å bli bestanddeler av komplekse, integrerte løsninger, med grensesnitt mot prosesser, andre kontrollsystemer, bedriftens IT-systemer og internett.

Fordi industrielle IKT-systemer styrer fysiske og ofte sikkerhetskritiske prosesser, har hendelser stort skadepotensial. Et vellykket cyber-angrep på et slikt system vil derfor kunne ha store og umiddelbare konsekvenser. Ytterste konsekvens vil kunne være langvarig produksjonsstans, tap av eiendeler, miljøkatastrofer eller dødsfall. De alvorlige utfallene ved kompromittering kombinert med den økende eksponeringen mot eksterne systemer og -nettverk gjør at industrielle IKT-systemer bør prioriteres på likt nivå med IT-systemer når virksomheter bygger cyber-resiliens. Selv om fokuset på cyber-sikring, også av industrielle IKT-systemer, er økende, er det fortsatt en prominent skjevfordeling på krav til sikring av hardware kontra sikring av software for industrielle IKT-systemer.

Foruten å påse at alle komponenter er operative hver for seg, er det stadig viktigere å sikre kommunikasjonen mellom forskjellige systemer og delsystemer. Teknologi som CCTV-kameraer, ROV-er, droner, posisjoneringssystemer og smarte sensorer legger til rette for automatiserte prosesser og til slutt ubemannede installasjoner, men for at slike løsninger skal ha tilstrekkelig pålitelighet kreves ikke bare toppmoderne teknologi, men også sikker kommunikasjon.

Hvordan kan man være sikker på at kommunikasjonen mellom systemer, sensorer eller mennesker er sikker? Hvordan kan man være trygg på at driften ivaretas dersom kommunikasjonen faller fra, eller verre, noen har tatt seg inn i systemene og dette resulterer i stans av (eller integritetsproblemer med) kritiske prosesser i driften?

Blokkjede («Blockchain» eller «Distributed Ledger Technology» - DLT på engelsk) er en forholdsvis ny type teknologi for databehandling som det er skapt store forventninger til. Mange forbinder blokkjede med kryptovaluta (Bitcoin) som var den opprinnelige applikasjonen, men blokkjede kan også ha andre anvendelsesområder som går langt utover dette. Blokker i kjeden skal ikke kunne forfalskes uten at det blir oppdaget. En blokkjede skal derfor være «tamper-proof». Det er derfor flere industrier, deriblant oljeindustrien, som ser på muligheter for å bruke blokkjedeteknologi til å få en sikrere samhandling og kommunikasjon mellom aktører.

For å legge til rette for at dagens og fremtidens drift på norsk sokkel skal fungere optimalt, er det avgjørende at IKT-sikkerhet blir ivaretatt, også ved bruk av ny teknologi (så som blokkjede). HMS og effektivitet har høy prioritet, men etter hvert som flere og flere systemer kobles til hverandre og til internett, må IKT-sikkerhet og resiliens få økt oppmerksomhet, da dårlig praksis på nettopp dette området kan true sikker og velfungerende drift.

3.2 Hensikt

DNV GL har fått i oppdrag av Ptil å vurdere hvordan resiliens, med tilhørende metoder, kan anvendes for å gjøre IKT-sikkerhet knyttet til industrielle IKT systemer mer robust. DNV GL vil også vurdere hvordan prinsipper for IKT-sikkerhet kan anvendes i relasjon til blokkjedeteknologi og hvordan sikkerheten kan ivaretas og eventuelt styrkes ved implementering av blokkjede.

Hovedmål for utredningen er å dele kunnskap og ekspertise (fra DNV GL og fra intervjuobjekter) innen cyber-resiliens og blokkjede, og hvordan dette kan bygges opp og opprettholdes for å gjøre fremtidens drift på norsk sokkel trygg, effektiv og moderne.

I vurderingen vil menneskelige, tekniske og organisatoriske forhold ligge som et bakteppe for all jobbing med IKT-sikkerhet og cyber-resiliens. I arbeidet med resiliens legges det spesielt vekt på å også kunne håndtere hendelser som har blitt vurdert til å ha svært liten sannsynlighet, men ha svært stor konsekvens, såkalt sorte svaner /1/. Videre vil viktigheten og fremgangsmåten for segregering mellom kontornett og tekniske nett forklares kort, mens barrieremetodikker og andre arbeidsmetoder for oppbygging og kontinuerlig utbedring av industriell IKT-sikkerhet og resiliens vil få mest fokus.

Det diskuteres også, på bakgrunn av dagens informasjon og tilgjengelig forskning, om blokkjede kan bidra positivt til oppbygging av resiliens og muliggjøre nye metoder for å fremme cyber-sikkerhet knyttet til industrielle IKT-systemer (OT) og i skjæringspunktet mellom IT og OT.

3.3 Metodikk

For å utrede prinsipper for industriell IKT-sikkerhet og hvordan disse kan anvendes i relasjon til blokkjedeteknologi, er det utført litteraturstudier og innhentet erfaringer. Som et ledd i vurderingen har DNV GL gjennomført intervjuer både internt og med aktører i sektoren. Det har også vært møter med aktører innen energi og luftfart. Vi har hatt møter med følgende eksterne aktører: Aker BP, Avinor, ConocoPhillips, Equinor, Lundin, Norske Shell, NVE, Statnett og Vår Energi.

Særlig innen blokkjede har vi i stor grad basert oss på litteraturstudier, interne eksperter og søk på nettet, da det i de fleste selskap har vært begrenset erfaring med dette tema blant dem vi har intervjuet.

Drøftinger, analyser og rapportskriving er basert på det innhentede materiale. Fakta for å belyse drøftingene og analysene, samt sitater, er tatt med i egne faktabokser i rapporten.

3.4 Forkortelser og definisjoner

B2C	Business to consumer
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CSIRT	Cyber Security Incident Response Team (synonymt begrep med CERT)
DDOS	Distributed Denial of Service (distribuert tjenestenektangrep)
DLT	Distributed Ledger Technology/Distribuert hovedbokteknologi
DMZ	Demilitarized Zone
ESD	Emergency shutdown / nødavstengning
FFI	Forsvarets forskningsinstitutt
IATA	International Air Transport Association
ICS	Industrial Control System
IDS	Intrusion Detection System
IioT	Industrial Internet of Things
IKT	Informasjon- og kommunikasjonsteknologi
IoT	Internet of Tings – Tingenes internett
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
IT	Informasjonsteknologi
MSS	Managed Security Services. Dette er å tilby SOC som tjeneste
MTO	Man Technology Organisation (Menneske Teknologi Organisering)
NIST	National Institute of Standards and Technology
NOROG	Norsk olje og gass
NSM	Nasjonal Sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OT	Operasjonell Teknologi
PLS/PLC	Programmerbar Logisk Styring/Programmable Logic Controller
PoA	Proof of Authority, valideringsmekanisme typisk brukt i private blokkjeder
PoS	Proof of Stake, valideringsmekanisme benyttet i offentlige blokkjeder
PoW	Proof of Work, valideringsmekanisme benyttet i offentlige blokkjeder
Ptil	Petroleumstilsynet
ROV	Remotely Operated Vehicle
SAS	Safety Automation System
SCADA	Supervisory Control and Data Acquisition

SIEM	Security Information and Event Management
SIS	Safety Instrumented System
SOC/ISOC	(Information) security operation centre
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network

Blokkjedebegreper (engelsk-norsk)

Blockchain	Blokkjede
Digital asset	Digital eiendel
Ledger	Hovedbok
Miner	Graver
Private/permissioned DLT	Tilgangsstyrt DLT / Tilgangsstyrt blokkjede
Public DLT	Offentlig DLT / Ikke-tilgangsstyrt blokkjede
Side chain	Sidekjede
Smart contracts	Smarte kontrakter

Definisjoner

Barriere	En barriere i IKT-sikkerhetssammenheng er et tiltak, enten i form av teknologi, prosess eller menneske, som har til formål å gjøre det vanskeligere for en aktør å trenge inn i systemer eller begrense konsekvensen av et angrep.
Digital Sikkerhetskultur	Digital sikkerhetskultur kan forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til informasjonsverdier. Digital sikkerhetskultur er derfor et sett med handlingsmønstre, og et sett med idéer, holdninger og kunnskaper /18/.
Edge computing	Dette innebærer å ha regnekraft så nær rådata som mulig, i stedet for å gjøre beregninger i en sentral datamaskin eller i «skyen». Edge computing er et begrep som benyttes blant annet i forbindelse med 5G (neste generasjons mobilnett) der noen anvendelser krever svært rask responstid.
Malware/Skadevare	Malware (fra engelsk malicious software) eller skadelig programvare (skadevare) er programvare som er designet for å utføre «ondsinnede» oppgaver. Det kan også gjerne kalles «skadevare» eller «skadeprogrammer». Eksempler på malware er datavirus, ormer, trojanere, spyware, adware, ransomware, backdoors, rootkit og keyloggere.
Pentest	Penetrasjonstest eller inntrengningstest. En test hvor noen forsøker med de samme midler som datakriminelle å bryte seg inn i et system. Dette kan gjøres mot et virkelig system for å avdekke sårbarheter.
Phishing	Phishing er en teknikk innen social engineering / sosial manipulering. Phishing er utsendelse av en epost som har som mål å lure mottageren til å klikke på en link, åpne et dokument og/eller gi i fra seg sensitiv informasjon som brukernavn og passord.

Red team – blue team	En cyberøvelse hvor man har et team med angripere (red) og et team med forsvarere (blue).
Resiliens	Det engelske begrepet «resilience» innbefatter noe mer enn bare motstandsdyktighet eller robusthet. Resiliens er evnen til å forberede seg, respondere på og forbedre seg etter en utfordrende situasjon eller hendelse.
Risikoanalyse	Risikoanalyse er en prosess som gjøres for å avdekke risiko knyttet til en virksomhet/aktivitet/situasjon. I korte trekk handler det om å få oversikt over tenkelige uønskede hendelser som kan inntreffe, hva sannsynligheten er for at de inntreffer, og hva konsekvensene vil være dersom de inntreffer.
Social Engineering/sosial manipulering	"Social engineering" eller sosial manipulering, er en måte å manipulere eller lure mennesker til å oppgi sensitiv informasjon eller gjøre noe de vanligvis ikke ville gjort.
Zero-day sårbarhet	En Zero-day eller 0-day sårbarhet er en sårbarhet som ennå ikke er oppdaget, eller nyoppdaget, og derfor ennå ikke er adressert av utgiver/eier av softwaren. Navnet kommer av at utgiver/eier av softwaren ikke har hatt noen dager til å fikse sårbarheten på. Når utgiver/eier har utviklet en oppdatering (patch) for å tette/fikse sårbarheten vil den ikke lenger være en 0-day sårbarhet.

3.5 Omfang

Petroleumstilsynets myndighetsansvar favner sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på norsk kontinentalsokkel. Dette omfatter innretninger til havs og installasjoner på land.

Denne rapporten omfatter betraktninger rundt cyber resiliens og blokkjedeteknologi, primært i skjeringsfeltet mellom IT og OT-området.

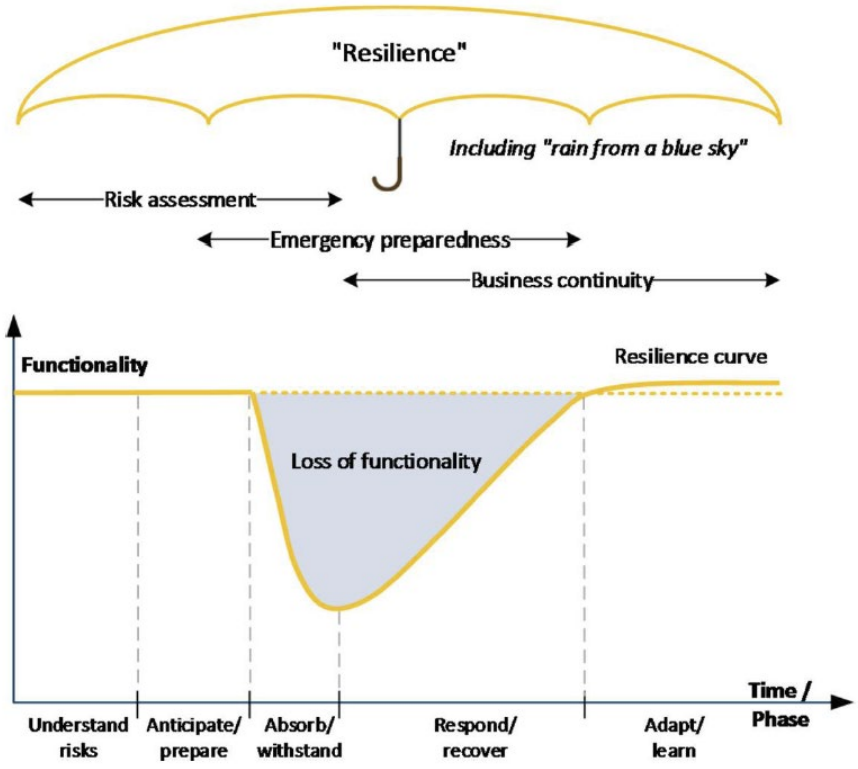
For blokkjedeteknologi har det vært vanskelig å finne gode eksempler på anvendelser innen OT-området.

4 CYBER-RESILIENS I INDUSTRIELLE IKT-SYSTEMER

4.1 Cyber-resiliens

Hva er cyber-resiliens og hvorfor er dette viktig?

Det snakkes ofte om motstandsdyktighet eller robusthet når cyber-sikkerhet i industrielle og vanlige IKT systemer blir diskutert. Det engelske begrepet «resilience» derimot, innbefatter noe mer enn bare motstandsdyktighet eller robusthet. Derfor følger vi FFIs anbefaling (ref. /3/) og bruker det fornorskete begrepet resiliens. På engelsk ble begrepet «resilience» opprinnelig brukt om egenskapen til en ting – et materiale – som utsettes for en påkjenning, og som etterpå kan gå tilbake til sin opprinnelige form uten å ha blitt deformert. I senere tid har begrepet også fått utvidet betydning – at noe er blitt sterkere etter at det har blitt utsatt for en påkjenning. Eksempelvis blir muskler sterkere etter påkjenning i form av trening. Nassim Nicholas Taleb omtaler dette som «Antifragile», i boken med samme navn /10/. Innen IKT kan analogien være at en organisasjon som har opplevd en cyber-hendelse og lært av den, i ettertid vil være bedre rustet til å takle nye cyber relaterte hendelser på en bedre måte. I arbeidet med resiliens står nettopp fokuset på konsekvensen av hendelsen, ikke om hendelsen i seg selv er utløst av tilfeldigheter eller målrettede angrep.



Figur 4-1 - Illustrasjon av resiliens slik det er drøftet i FFIs rapport /3/. Merk at resiliens-kurven ligger på et høyere nivå etter hendelsen

Cyber-resiliens er mer enn å forhindre eller å respondere på en hendelse – cyber-resiliens handler også om evnen til å opprettholde helt eller delvis operasjon mens hendelsen pågår. I tillegg handler cyber-resiliens om å tilpasse forsvaret etter dagens risikobilde, samt evnen til å komme seg tilbake i normal drift, så fort som mulig, etter en cyber-hendelse. Dette omfatter også evnen til ytterste konsekvens å kunne gjennomføre en nødavstengning på forsvarlig måte. Om dette ikke er utfordrende nok alene, så må en aktør som har vært utsatt for en cyber-hendelse være sikker på at situasjonen er under kontroll før systemene kan friskmeldes og normal drift kan gjenopprettes. Inntrengere vil svært ofte etablere en

eller flere ekstra innganger til systemet de har kompromittert, såkalte bakdører. Dersom en eller flere bakdører ikke blir oppdaget under oppryddingen, vil angriperen fortsatt kunne komme seg tilbake i systemene etter at den opprinnelige tilgangen har blitt fjernet. Erfaring tilsier at inntrengerne kommer seg inn igjen i systemene i rundt halvparten av tilfellene etter at tilgangen deres er blitt fjernet fra systemet første gang (ref. GIAC-kurs – Global Industrial Cybersecurity Professional, SANS Institute). Et annet problem, enten det er en eller gjentatte inntrengninger, er at mye av utstyret i bruk på plattformer og installasjoner (f.eks. PLSer og andre logiske enheter) vil være sensitivt for kommunikasjonsfeil, strømbrudd og andre forstyrrelser, og i mange tilfeller så kan utilsiktet skade være vel så fatalt for systemet som den tilsiktede aktiviteten.

Dette understreker at risikovurdering av utfallet av hendelser bør vektlegges i større grad enn vurderingen av sannsynligheten for at hendelsen skal inntreffe /1/. Samtidig advarer NSM i sin rapport Risiko 2019 /5/, at mange virksomheter har et ufullstendig risikobilde og manglende egenskaper til å kartlegge avhengigheter både internt i sine systemer og mellom virksomheter. Forutsetningen en bedrift har for å kunne oppnå god cyber-resiliens med et ufullstendig risikobilde er derfor dårlig.

Resiliens er, som beskrevet over, en sammensatt aktivitet og handler om å inneha god organisatorisk oversikt, teknisk modenhet og samtidig evne kontinuerlig læring og forbedring. God resiliens krever dermed en mer proaktiv tankegang i arbeidet med cyber-sikkerhet, heller enn en reaktiv tilnærming etter at «noe» har skjedd.

I påfølgende delkapitler vil ulike barrieremetodikker og arbeidsmetoder for oppbygging og kontinuerlig utbedring av IKT-sikkerhet og resiliens gjennomgås mer detaljert. Begrepet IKT-sikkerhet omfatter i denne rapporten både vanlig IT og OT/industriell IKT. Der vi klart ønsker å skille mellom IT og OT/industriell IKT benytter vi disse begrepene eksplisitt.

4.2 Prinsipper for IKT-sikkerhet

Det finnes mange definisjoner av prinsipper for å jobbe med IKT-sikkerhet. NIST sitt rammeverk /2/ følges av mange og trekkes frem som et godt utarbeidet og oversiktlig rammeverk. I tillegg til Norsk olje og gass sine «104 retningslinjer for industriell IKT-sikkerhet» /16/, viser også NSM sin anbefaling, «Grunnprinsipper for IKT-sikkerhet» /7/, tilbake til NISTs oppdeling av tiltak. DNV GL har også utgitt anbefalinger for hvordan bedrifter kan jobbe med IKT-sikkerhet basert på IEC 62443 i sine «recommended practices» for Olje og Gass /15/ og Maritim sektor /14/. I de følgende avsnittene vil noen av prinsippene gjennomgås der hovedformålet er å beskrive en god måte å jobbe med industriell IKT-sikkerhet for å kunne oppnå god resiliens mot cyber-hendelser.

Figur 4-2 – Det gyldne triangelet (MTO) beskriver tre viktige forhold å jobbe med for å inneha god IKT-sikkerhet; Menneskelige, Teknologiske og Organisatoriske forhold. Det er ikke tilstrekkelig å kun fokusere på ett eller to av elementene i MTO-triangelet, man må fokusere på alle tre elementene i parallell for å kunne oppnå god IKT-sikkerhet. For eksempel hjelper det lite med brannmur, antivirus, etc. hvis en ansatt gir fra seg brukernavn/passord til noen med uærlige hensikter. Det vil være like vanskelig eller umulig å ha god IKT-sikkerhet dersom et eller flere av forholdene i modellen under ikke er tilstrekkelig forankret i bedriften.

Figur 4-2 – Det gyldne triangelet (MTO)

Menneskelig

Mange omtaler mennesker eller personell som «the weakest link»[1] fordi det er mennesker som lar seg lure av phishing eposter, bruker USB eller andre bærbare lagringsenheter uten å påse at de er «rene» eller opptrer godtroende ovenfor andre mennesker. Med rett type trening og oppfølging kan det motsatte argumenteres. De ansatte er den første forsvarslinjen i mange tilfeller og kan også være den viktigste årsaken til at hendelser kan oppdages, varsles og stoppes på et tidlig tidspunkt. Trening og kompetansebygging er veldig viktig for å øke årvåkenheten blant ansatte. De må vite hva de skal se etter, de må kunne ha kompetanse og selvsikkerhet nok til å kunne gjenkjenne f.eks. en phishing epost. Deretter må de vite hvilken prosedyre de skal bruke, f.eks. hvem skal varsles dersom en mistenkelig epost er blitt oppdaget, eller hvem skal varsles dersom en mistenkelig person er observert i kontorlokalene. Det hjelper lite å ha prosedyrene i orden dersom ingen har lest dem eller fått innføring i hvordan de skal brukes.

Teknologisk

Tradisjonelt sett har sikkerhetsbarrierer vært av teknisk eller fysisk karakter og mange tenker kanskje fortsatt først på slike tradisjonelle barrierer når det snakkes om IKT-sikkerhet eller annen sikring av kritisk infrastruktur. I MTO-modellen utgjør det tekniske forholdet bare en av de tre viktige forholdene, men oppleves kanskje som den mest dominerende fordi teknologien stadig er i endring. Mange av verktøyene som brukes i løpet av en arbeidsdag er digitale eller innehar elementer av software. All software vil ha sårbarheter, men dersom softwaren ikke er oppdatert så vil den ha mange kjente sårbarheter i tillegg til de som kanskje ikke er oppdaget enda, såkalt zero-day sårbarheter. Problemet med å ha mange kjente sårbarheter i systemene er at disse også har kjente verktøy for å kunne utnyttes. Teknologi-elementet i triangelet over omfatter også nettverks-sikkerhetsdesign, som diskuteres mer i seksjon 4.3.2.1, og segregering.

1 "According to data from the Notifiable Data Breaches Scheme, human error is the cause of 67% of data breaches, with some reports citing human error as the cause of over 90% of data breaches" https://www.cso.com.au/article/667214/human-factor-cyber-security/

Når IKT-sikkerhet diskuteres så er teknologi ofte det første som nevnes. Utdaterte systemer utpekes fort som hovedsynderen til de fleste cyber-hendelser, men ofte så er bildet mer sammensatt.

Organisatorisk

Begrepet organisatoriske forhold omfatter en mengde temaer og har sterke linker over til menneskelige og tekniske forhold, også illustrert i modellen over. Et av temaene som står sentralt i en organisasjon, og spesielt en organisasjon med høyt fokus på sikkerhet (i betydningen «safety»), er prosedyrer. Prosedyrer legger grunnlaget for at prosesser kan gjøres på lik måte, av ulike mennesker, hver gang. De muliggjør også at prosesser og handlinger gjennomføres på en trygg og effektiv måte. I lys av det menneskelige forholdet beskrevet over så må opplæring av ansatte og utvikling av organisatoriske forhold gå hånd i hånd. Prosesser og prosedyrer for IKT-sikkerhet vil måtte være i konstant utvikling for å henge med i trusselbildet som stadig er i endring, ref. tekniske forhold. Sikkerhetskultur og dermed også digital sikkerhetskultur springer ofte ut av gode prosedyrer og solid forankring hos ledelsen og de ansatte, men kultur er også mye mer /18/. Gode organisatoriske forhold spiller en viktig rolle i å forankre IKT-sikkerhetstankegang i bedriftskulturen.

Det er altså flere «hull og mangler» som kan utnyttes for å skape eller forårsake en cyber-hendelse. Et eksempel kan være at en aktør sender phishing eposter med et vedlegg som inneholder en eller annen type skadevare, til mange selskaper. Eposten inneholder som regel elementer som spiller på menneskelige triggere (f.eks. følelse av press med hensyn på tid, viktighet, belønning eller utnytting av tillitsforhold). Dette fører til at noen ansatte blir lurt til å åpne vedlegg og/eller å klikke på linken. Aktøren utnytter dermed først det menneskelige og organisatoriske aspektet, men det tredje elementet (teknologi) må også være mangelfull for at et slikt tenkt scenario skal forårsake en hendelse og i dette eksempelet at skadevare blir installert på en eller flere maskiner i bedriften. Nå er det imidlertid ikke slik at det går an å basere seg kun på sikring via teknologi, fordi teknologi alltid vil inneholde sikkerhetshull eller andre mangler. Dette illustrerer dermed viktigheten av å ta med alle tre elementene (MTO) når det jobbes med IKT-sikkerhet og resiliens. Elementene er komplementære og vil ikke gi god sikkerhet enkeltvis.

4.3 Arbeidsmetoder for IKT-sikkerhet og resiliens

For å jobbe vellykket med IKT-sikkerhet kreves det strukturert kartlegging av hele trusselbildet og identifisering og prioritering av tilhørende arbeidsmetoder. Dette kan oppnås med å bruke tilgjengelige rammeverk og metodikker. Eksempler på noen relevante rammeverk og standarder er NIST Cybersecurity Framework, IEC 62443 og ISO/IEC 27001, og disse ligger også til grunn for denne leveransen. Felles for alle rammeverk er at de ikke er ment å erstatte organisasjonens egne styringsprosesser og virksomhetsplaner, men utviklet for å støtte oppunder og styrke organisasjonen sine egenutviklede prosesser og programmer. Dersom organisasjonen på gitt tidspunkt ikke har slike egenutviklede prosesser og planer er direkte bruk av rammeverkene selvsagt en god start.

NIST Cybersecurity framework[2] opererer med fem hovedfunksjoner, illustrert i figuren under.

[2] Mye av det samme inngår i NSMs rammeverk og i IEC 62443, men inndeling og terminologi kan være noe forskjellig.

Figur 4-3 – Hovedfunksjoner i NIST rammeverk for IKT-sikkerhet

Gjennom de fem punktene over, vil en organisasjon kunne:

- Finne nåværende status for Industriell IKT- og IKT-sikkerhet
- Sette fremtidig mål og delmål for Industriell IKT- og IKT-sikkerhet i organisasjonen
- Identifisere og prioritere oppfølging og kontinuerlig forbedring av Industriell IKT- og IKT-sikkerhet
- Kontinuerlig vurdere og følge fremgangen mot mål og delmål fra kulepunkt 2
- Kommunisere status for industriell IKT- og IKT-sikkerhet til interne og eksterne interessenter

I de påfølgende delkapitlene vil denne rapporten gjennomgå de fem stegene illustrert i Figur 4-3 med noen utvalgte arbeidsmetoder for hvert steg, samt råd og diskusjon rundt bruken av arbeidsmetodene.

4.3.1 Identifisering og kartlegging (Identify)

4.3.1.1 Risikoanalyse

Å velge hensiktsmessige tiltak for å bygge resiliens forutsetter at man har god oversikt over tenkelige hendelser, samt årsaker og konsekvenser som kan knyttes til disse tenkte hendelsene. En slik oversikt kalles gjerne for et risikobilde, og fås ved å foreta en risikoanalyse. I risikoanalysen identifiserer man relevante uønskede hendelser som kan inntreffe, basert på kunnskap om det foreliggende systemet og lignende systemer.

Det finnes riktignok mange eksempler på historiske hendelser som ingen greide å forutse, på tross av omfattende risikoanalyser. Disse kalles gjerne sorte svaner /1/, og kjennetegnes enten ved at de ikke har blitt vurdert som tenkelig hendelse eller at den tenkte hendelsen har blitt ansett for å være en umulighet. Når man jobber med risikohåndtering er det imidlertid en grense for hvor utenkelige/usannsynlige hendelser man kan vurdere, før risikoanalysen mister sin verdi. Derfor gjør man "så godt man kan", ut ifra den kunnskap man til enhver tid sitter inne med. En sort svane som har inntruffet en gang bør brukes for å øke kunnskapsnivået slik at den vil bli vurdert ved senere risikoanalyser.

Når relevante tenkelige hendelser har blitt identifisert, vurderer man sannsynlighetene[3] for, og konsekvensene av, disse hendelsene. Kombinasjonen av sannsynlighet og konsekvens for en gitt hendelse gjør det mulig å anslå hvor mye risiko som er knyttet til hendelsen - risikonivået. De forskjellige tenkte hendelsene og deres risikonivå utgjør til sammen et risikobilde, som er essensielt å ha for at man skal kunne identifisere og prioritere tiltak for å redusere risiko.

Et risikobilde påvirkes av diverse faktorer, både interne og eksterne. Sikkerhetsoppdateringer, nye prosedyrer, nye funksjoner og konfigurasjonsendringer er eksempler på interne faktorer, mens politiske forhold og teknologiutvikling blant datakriminelle er eksempler på eksterne faktorer. Dette gjør at risikobildet må anses som dynamisk, slik at konklusjonene fra en risikoanalyse er ferskvare. Noen risikoer kan reduseres over tid ved hjelp av sikkerhetsoppdateringer og andre tiltak, samtidig som andre risikoer kan øke eller oppstå. Eksempelvis kan nye angrepsmetoder og -verktøy føre til at en trussel/risiko som tidligere ble ansett for å være minimal, plutselig blir betydelig.

For å holde tritt med endringene i risikobildet er det derfor anbefalt å gjøre regelmessige risikoanalyser. Innen IKT er det stadig utvikling i trusselbildet, så selv om et system forblir relativt uendret kan det skje betydelige endringer i risiko og sårbarhet. Hvor ofte risikovurdering bør gjøres kan variere, de fleste anbefalingene ligger på mellom annethvert år og to ganger pr år[4]. I tillegg anbefales «ekstraordinær» risikovurdering ved spesielle omstendigheter, slik som ved større oppgraderinger/endringer, etter en cyber-hendelse, etc.

Det finnes diverse metoder og verktøy for risikovurdering, med det til felles at de bidrar til å skaffe oversikt og tilrettelegger for risikohåndtering. Denne rapporten diskuterer ikke hvilke metoder som er best, ettersom forskjellige aktører kan ha forskjellige preferanser. Det viktigste er å finne en metode man er komfortabel med, og at man gjennomfører regelmessige risikovurderinger og følger opp resultatene kontinuerlig, slik at risiko reduseres over tid. Vi vil se nærmere på sløyfeanalyse, som er en av de mer utbredte metodene for risikovurdering.

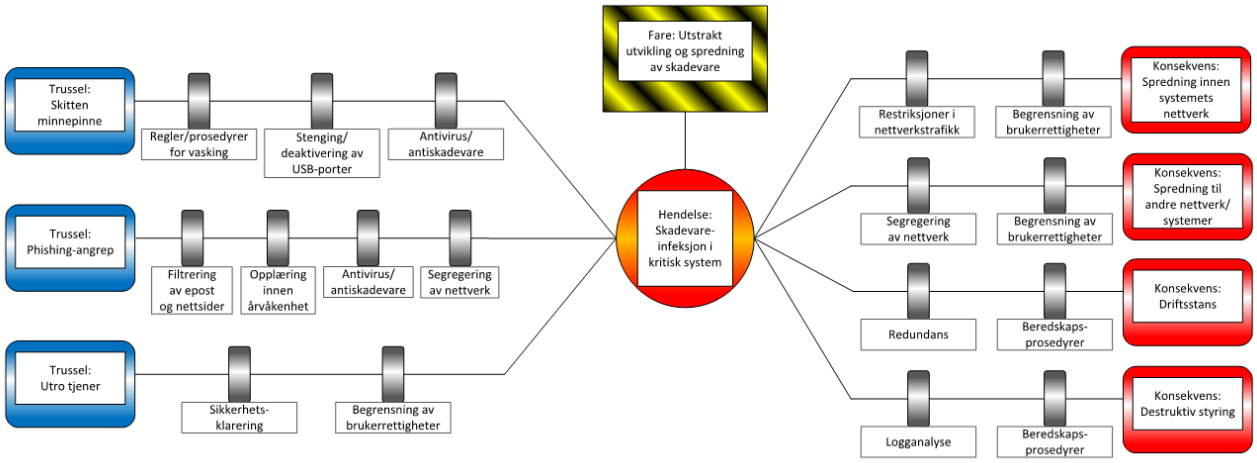
4.3.1.2 Sløyfeanalyse og barrieremetodikk

Sløyfeanalyse (på engelsk «bow tie») er en spesiell teknikk for risikoanalyse som gir en grafisk fremstilling av omstendighetene rundt en tenkt hendelse. Sløyfefiguren tar utgangspunkt i en konkret tenkt hendelse, og viser forskjellige årsaker som kan utløse en slik hendelse. I tillegg vises spesifikke konsekvenser som den tenkte hendelsen kan føre til dersom den inntreffer. Hendelsen i midten kalles en *topphendelse*, og beskrivelsen av denne er ganske generell. En faktisk hendelse (dersom den inntreffer) vil være mer spesifikk ved at den følger en konkret «sti» fra årsak, til venstre i modellen, via topphendelse og til konsekvens, til høyre i modellen.

Mellom topphendelsen og dens årsaker og konsekvenser vises de forskjellige *barrierene*, altså tiltak eller omstendigheter som reduserer risiko. Barrierer til venstre for topphendelsen reduserer sannsynlighet og barrierer til høyre for topphendelsen reduserer konsekvens.

[3] Det er delte oppfatninger om man skal benytte sannsynlighet for villede handlinger.

[4] NVEs Kraftberedskapsforskrift (Kbf) krever at kritiske systemer er gjenstand for risikoanalyse årlig. Kbf angir i § 2-3: Vurderingene skal minimum gjennomgås årlig og oppdateres ved behov. Og i § 6-9: Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.



Figur 4-4 – Eksempel på sløyfediagram

Årsaker til hendelser og tilhørende konsekvenser bør bekjempes med flere barrierer, i tilfelle en barriere svikter eller blir omgått. Det er også viktig å ha barrierer både mot tilfeldige og tilsiktede hendelser slik at systemet er robust mot angrep så vel som komponentsvikt.

Noen eksempler på konkrete barrierer:

- Opplæring av personell for å bevisstgjøre og unngå menneskelige feil
- Trening og øvelser i håndtering av cyberhendelser
- Antivirus/antiskadevare for å blokkere mot inntrenging
- Brannmurer for å tillate/blokkere nettverkstrafikk og segmentere mellom soner
- Systemer for å detektere/bekjempe inntrengning (IDS/IPS)
- Redundans av systemer med høyt krav til tilgjengelighet
- Mulighet for å gjennomføre ESD ved å kutte strømmen (siste utvei)
- To-faktor- eller multifaktorautentisering (f.eks. engangskode i tillegg til passord)
- Begrensning i brukerrettigheter
- Prosedyrer/regler for passord
- Prosedyrer for oppdatering av programvare (patching)
- Prosedyrer/regler for bruk av minnepinne

Gjennom regelmessige risikoanalyser og kontinuerlig arbeid med å opprette/forbedre barrierer, vil man redusere risiko og få et system som er bedre rustet mot angrep så vel som tilfeldige tekniske problemer. Sløyfediagrammene for de forskjellige topphendelsene gir en god indikasjon på hvor systemet er robust og hvor det er sårbart, slik at det blir lettere å prioritere fremtidige tiltak for å bygge resiliens.

4.3.1.3 Deling av kunnskap og erfaring

Resiliens gjennom kunnskapsdeling

En kollektiv svakhet i flere industrier er at aktørene av forskjellige årsaker ikke deler kunnskap og erfaring rundt IKT-sikkerhet /20/. Uten slik utveksling er det vanskelig for aktørene å lære av hverandres sårbarheter og tiltak, og de blir som gruppe mer utsatt for angrep. På grunn av likheter i de forskjellige aktørenes virksomheter og systemer, er det sannsynlig at mange av sårbarhetene eksisterer hos flere aktører og på flere fartøy/installasjoner. Hvis en av aktørene rammes av et angrep som utnytter en bestemt sårbarhet, og det ikke er kommunikasjon/samarbeid mellom aktørene, så kan angriperne bruke de samme metodene mot øvrige aktører med god uttelling. De kriminelle deler flittig både informasjon og verktøy og utgjør til sammen en enorm trussel fordi de bygger videre på hverandres bragder.

Cyber-kriminalitet er sterkt økende og i 2018 ble inntektene fra slik kriminalitet estimert til ca. 14 000 milliarder NOK på verdensbasis /23/, men majoriteten av angrep er fortsatt ikke målrettede, de er ment å ramme bredt for å øke sjansen for «suksess». Det finnes selvsagt flere tilfeller av målrettede angrep, også i olje og gass industrien, men de fleste angrep er ikke direkte målrettede og bygger på sårbarheter og svakheter som er kjente og har vært utnyttet før.

Deling og samarbeid gir store fordeler uansett hvilken side man er på. Redelige aktører som ønsker å styrke sitt cyber-forsvar anbefales å ta del i relevante allianser for å dra nytte av andres kunnskap og erfaringer. Jo flinkere aktørene er til å dele og lære av relevant og nyttig kunnskap og erfaring, jo vanskeligere blir det for datakriminelle å lykkes.

Delingsforum for utveksling av informasjon og erfaringer innen cyber-sikkerhet kalles ofte ISAC (Information Sharing and Analysis Center). Det finnes en rekke slike ISAC, som grupperes ut ifra bransje/næring og geografi. Noen konkrete eksempler er beskrevet i /20/. I tillegg til fora for deling finnes det allianser/miljøer som også innehar kapasitet til å respondere på hendelser. Disse kalles CERT[5] (computer emergency response team) og beskrives nærmere i avsnittet om beredskapsplanlegging.

En del, da spesielt små og mellomstore aktører, oppgir manglende økonomiske ressurser som grunn for å ikke ta del i et CERT /20/. Det finnes derimot alternativer som ikke trenger å koste mye eller noe, men da får en heller ikke tilgang til f.eks. et beredskapsteam (slik som et CERT medlemskap gjør). Slike alternativer er såkalte «lukkede» delingsforum der deltagerne kan dele alt fra angrep de har hatt/opplevd, tiltak de har gjort, hva som var utfordrende, hva var mindre utfordrende og dermed lære av hverandre. Slike fora er helt tillitsbasert og avhenger av at noen tør å begynne å dele.

Med godt samarbeid gjennom delingsforum/allianser/responsmiljøer kan aktører dele erfaringer og lære av hverandres sårbarheter slik at de lettere kan identifisere trusler og håndtere risiko. Det vil igjen føre til at det blir vanskelig for kriminelle å gjøre «samme angrep» mange steder.

4.3.2 Beskytte (Protect)

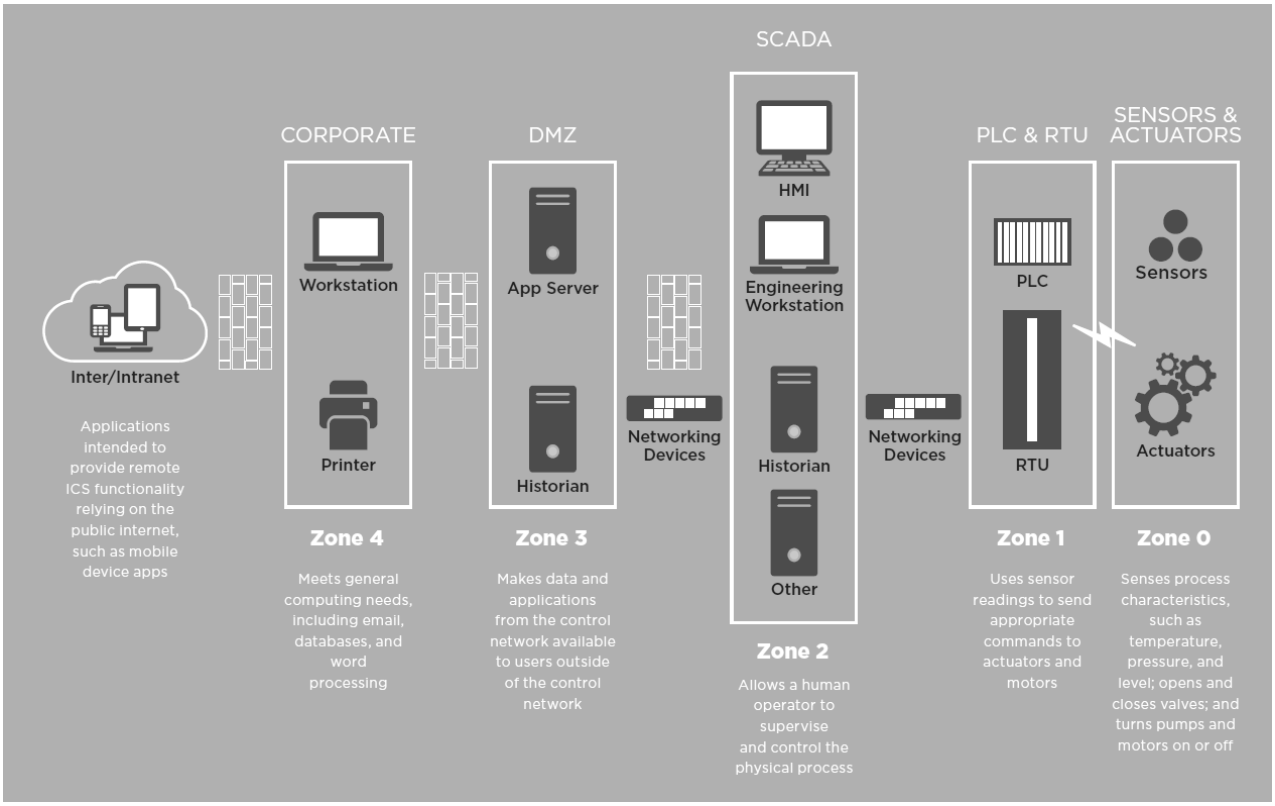
Mange av de konkrete barrierene nevnt i diskusjonen om sløyfeanalyse og barriermetodikk i 4.3.1.2 går ut på å beskytte. I tillegg ønsker vi i her spesielt å diskutere segregering mellom soner som en beskyttelsesmekanisme for å forhindre at et cyberangrep sprer seg.

[5] CERT er et registrert varemerke, og det er spesifikke krav til de organisasjoner som ønsker å være CERT. CSIRT er også en betegnelse som benyttes.

4.3.2.1 Segregering mellom IT og OT

Industrielle IKT-systemer (OT) har tradisjonelt sett vært mer eller mindre fullstendig isolert fra administrative nett og andre systemer, noe som i seg selv er et sikkerhetstiltak, slik at behovet for (IKT-) sikkerhet i slike systemer har vært begrenset. OT-systemenes isolerte tilværelse har ført til at funksjonalitet har blitt prioritert fremfor sikkerhet, med det resultat at mange OT-systemer ikke er robuste nok til å bli eksponert for andre nettverk og systemer. Selv normal datatrafikk i et moderne IT-nettverk kan fungere som ødeleggende støy om den samme informasjonen skulle vært sendt i et OT-nettverk. Mange OT-komponenter er ikke utviklet for å håndtere uventet datatrafikk og vil i verste fall krasje på grunn av manglende evne til å filtrere bort «støyen».

Som nevnt i /17/ har det i senere tid utviklet seg et økende behov for å koble sammen nettopp IT og OT, blant annet for å få tilgang til produksjonsdata og for å muliggjøre fjernvedlikehold. For å gjøre OT-systemer tilgjengelige «fra utsiden» uten å måtte akseptere høy risiko eller gjøre store investeringer i å «herde» systemet, har det blitt vanlig å etablere en egen logisk «sone» som beskytter OT-systemet ved å regulere all kommunikasjon mellom OT-systemet og andre systemer. Denne sonen kalles ofte DMZ (demilitarisert sone). De tekniske detaljene for hvordan DMZ implementeres og konfigureres kan variere, men det fungerer i hovedsak som en brannmur for å hindre at uønsket datatrafikk når inn til og ut av teknisk nett (OT), samtidig som det fungerer som et grensesnitt mellom IT og OT ved å tillate begrenset datatrafikk mellom utvalgte komponenter. Behovet for kommunikasjon mellom IT og OT er ofte begrenset både i mengde og tid, slik at DMZ kan konfigureres til å kun tillate små dataoverføringer i avgrensede tidsrom.



Figur 4-5 – Sonemodell med IT i sone 4, DMZ i sone 3, og OT i sone 2, 1 og 0 (kilde: FireEye)

Segregeringen mellom IT og OT, enten ved hjelp av DMZ eller ved å ha fullstendig isolasjon, vil kunne beskytte OT-systemene både under normal drift og i tilfelle cyber-hendelse i IT-systemet. Dette er

imidlertid ikke det fulle bilde. Direkte hacking via IT-domenet er en risiko som reduseres med DMZ-løsninger og brannmurer, men det er flere veier å få skadevare inn i OT-systemene. Det kan bli introdusert skadevare ved leveranse av system, gjennom vedlikehold, gjennom uautorisert tilkobling til OT-systemer (USB, mobiltelefon, etc.). Ofte er denne veien («the slow way in») den vanskeligste å ha gode barrierer for, fordi den er veldig personavhengig.

Det er ille nok om angripere trenger inn i IT-systemene og utfører destruktive handlinger i det digitale rom, slik som kryptering av data, uthenting av sensitiv informasjon etc. Om angriperne i tillegg får tilgang til å påvirke/styre fysiske prosesser, vil man også kunne få store fysiske konsekvenser, som i verste fall kan medføre ulykke, forurensning eller fare for liv og helse. Det er eksempler på angrep rettet spesielt mot safety-systemer (SIS).[6]

4.3.3 Oppdage (Detect) og Opprettholde

Hvordan kan en organisasjon best mulig legge til rette for å evne å oppdage en cyber-hendelse på et tidlig tidspunkt? Dersom MTO-modellen, vist i Figur 4-2, legges til grunn, er det flere aspekter og tiltak som kan brukes for å få til et godt deteksjonssystem.

De ansatte ble omtalt som den første forsvarslinjen i delkapittel 4.2 og menneskene spiller uten tvil en viktig rolle i å kunne gjenkjenne ting som er «utenom det vanlige», men som kanskje ikke skiller seg nok ut til at dagens teknologi greier å plukke det opp. Hvordan dette håndteres i den daglige driften vil måtte bli individuelt i henhold til hvordan driften gjøres på hver lokasjon og/eller i hver organisasjon.

Noen organisasjoner har opprettet et eget SOC (Security Operations Centre) som har som oppgave å overvåke aktiviteten i de relevante nettverkene og maskinene/enhetene. Dataene som samles inn aggregeres og vurderes over en tidsperiode slik at SOC kan finne en definisjon av hva som er «normaltilstand» for det overordnede systemet. Hvis det kommer inn data som avviker fra de definerte normalverdiene, vil dette undersøkes nærmere for å avgjøre om det er uønsket aktivitet (angrep/innbrudd) i systemet, eller om aktiviteten er akseptabel/forventet og kan brukes til å oppdatere/justere normaldefinisjonen. En SOC-tjeneste kan også leies/kjøpes fra eksterne tilbydere. I den sammenhengen kalles det ofte MSS (managed security services).

Rent teknisk kan et SOC være basert på et IDS (og noen ganger IPS). SOC kan også være basert på et mer avansert SIEM-system (Security Information and Event Management), der dataene som hentes inn kommer fra kilder som nettverksskanning, databaseskanning, IDS, IPS[7], innsamling av diverse logger, antivirusprogrammer og brannmurer, for å nevne noen. De individuelle hendelsene som logges innehar i seg selv for lite informasjon til å dra konklusjoner, men når dataene kommer inn i stort volum kan de settes i system ved hjelp av regnekraft (maskinlæring), slik at interessant/avvikende aktivitet flagges mens vanlig aktivitet ignoreres. Ytelsen/treffsikkerheten til SIEM vil gjerne øke i takt med mengden «erfaring» systemet har. Hvis det gjøres større endringer i et system, vil SOC kunne få litt ekstra arbeid i en periode, frem til nye «normalverdier» er bedre definert.

---

6 Triton (også kalt Trisis) er en skadevare utviklet for å angripe Triconex Safety Instrumented System (SIS) kontrollere fra Schneider Electric. Denne skadevaren ble brukt i 2017 i et angrep som førte til en «emergency shut down» i en petrokjemisk fabrikk i Saudi Arabia. Triton/Trisis var antakelig den første kjente hendelsen hvor et SIS ble angrepet. https://www.darkreading.com/vulnerabilities---threats/triton-trisis-attacks-another-victim/d/d-id/1334388

7 NB. IPS, Intrusion prevention system, kan være nyttig i et kontornett (IT) for å avverge angrep, men i et OT-miljø kan det få store uønskete konsekvenser hvis IPS automatisk stopper mistenkelig nettverkstrafikk. I OT-miljø er det best å nøye seg med et IDS, Intrusion Detection System, som passivt oppdager og rapporterer om mistenkelig trafikk i nettet.

Et av målene med tidlig deteksjon av cyber-hendelser er at opprettholdelse av driften og produksjonen skal være mulig. I en organisasjon må alle trenes og bevisstgjøres på hvordan oppdage mistenkelige hendelser, og hva de skal gjøre hvis en slik hendelse inntreffer.

Hvis et cyberangrep rammer IT-systemer på land – når skal man kutte forbindelsen til innretninger til havs, og vet man konsekvensen? Man må ha kriterier for når en cyberhendelse skal eskaleres til en beredskapshendelse og dermed må håndteres på tilsvarende måte som andre fare- og ulykkessituasjoner. Når skal man trykke på den store knappen? Siste utvei er nødavstengning (ESD).

4.3.4 Håndtere (respond) og gjenopprette (recover)

4.3.4.1 Beredskapsplanlegging

Det bør lages planer for hvordan man skal håndtere og gjenopprette i forbindelse med cyber-relaterte hendelser. NIST har guidelines for beredskapsplanlegging, ref. /21/. Det anbefales også å teste og øve på cyber-hendelser.

I Ptils forskrifter omhandler blant annet følgende paragrafer forhold rundt beredskap (Ref. DNV GL-rapport /27/):

- Aktivitetsforskriften § 76, Beredskapsplaner. «Det skal utarbeides beredskapsplaner som til enhver tid beskriver beredskapen og inneholder aksjonsplaner for de definerte fare- og ulykkessituasjonene.» Cybersikkerhetshendelser bør utgjøre noen av de definerte situasjonene/scenariene med tilhørende aksjonsplaner.
- Aktivitetsforskriften § 77, Håndtering av fare- og ulykkessituasjoner.
  Også alvorlige cyberhendelser bør håndteres som en farlig situasjon og integreres i krisehåndteringen.

Innen IT beredskap skiller man mellom aktivitetene «business continuity» og «disaster recovery». Business continuity går ut på å holde produksjonen i gang (hvis mulig) og å håndtere krisen er en jobb for selskapets/installasjonens ledelse, mens det å undersøke og respondere på hva som skjer og gjenopprette drift av IT-systemene (disaster recovery) håndteres av IKT-organisasjonen, ofte med support fra leverandører. Det overordnete målet er at selv om man blir utsatt for et cyberangrep bør installasjonen være i stand til å opprettholde sikker produksjon. Om man lykkes med dette er en annen sak:

- Dersom data-angrepet også innbefatter OT-systemer så som driftskontrollsystemer og i verste fall safety-systemer, er ikke dette mulig. I noen tilfeller kan det være mulig å ha noe redusert drift med manuelle prosesser, men dette kommer an på situasjonen.
- Selv om angrepet kun rammer IT-systemene i kontornettet, kan produksjonen være så avhengig av noen av disse systemene slik at normal drift i praksis ikke er mulig.

IKT-hendelser er derfor viktige scenarier som må inn i installasjonens beredskapsplan, med tilhørende aksjonsplaner. Man bør ha tenkt igjennom noen scenarier, basert på risikoer med høy konsekvens, men også ta høyde for at noe totalt uventet skjer (en «svart svane»).

Et såkalt CERT (Computer Emergency Response Team) som har ekspertkompetanse fra diverse medlemmer vil også kunne bidra med rask og effektiv hjelp hvis en hendelse oppstår, slik at konsekvensene begrenses. Det finnes diverse CERT, noen av disse beskrives i Sintef-rapport /20/ og i DNV GL-rapport /27/. Et CERT kan også advare/informere andre aktører om et angrep som er under oppseiling, slik at de får tatt sine forholdsregler.

En utfordring er også å vite hva man skal gjøre for å opprettholde sikkerheten (i betydningen «safety») under en hendelse som omfatter OT-systemer. Dette kan være noe forskjellig fra anlegg til anlegg.

Gjenoppretting eller «disaster recovery» går ut på å få IKT-systemene (gjelder enten IT eller OT) tilbake i normal drift etter en hendelse. Avhengig av hva som forårsaket hendelsen må systemer renses for eventuell skadevare, programvare må reinstalleres, rene (ukorrupte) data må hentes inn fra backup, hardware som har feilet må erstattes, osv. Det bør derfor være detaljerte «disaster recovery» planer for hvordan gjenopprette hvert system. Det bør også være en overordnet plan for rekkefølgen av gjenoppretting og oppstart. Denne bør ta hensyn til to forhold:

1. Avhengigheter mellom systemer – hvilke systemer som er grunnleggende for at andre skal virke
2. Kritikaliteten av systemene – hva som er viktigst fra et operativt synspunkt

Det er viktig å kartlegge dette på forhånd, slik at man unngår at unødig tid går med til prøving og feiling i en kritisk og stresset situasjon.

Etter en alvorlig IKT-hendelse bør man finne ut hva som har skjedd, innhente beviser (logger, filer, disker, etc.), hvorfor det har skjedd (rotårsak), analysere hvordan hendelsen ble håndtert, og hva som kan gjøres for å være bedre rustet mot lignende hendelser i fremtiden. På denne måten vil organisasjonen også ha styrket sin resiliens (ref. Figur 4-1).

4.3.4.2 Testing, trening og øvelser

Risikovurdering, beredskapsplanlegging og trening/opplæring bidrar til bedre forståelse, oversikt og kunnskap om mulige uønskede hendelser og hvordan disse bør håndteres. Men for å oppnå god mestringsevne er det ikke tilstrekkelig med kun teorikunnskap. Som i de fleste andre situasjoner hvor det er viktig å prestere under krevende forhold, er det nødvendig med øvelse for å oppnå ønsket beredskap.

Begrepene trening og øvelse beskrives nærmere i /26/, men kort oppsummert kan vi si at trening går ut på å øke kunnskap og ferdigheter på individnivå for å gjøre hver enkelt skikket til å utfylle sin rolle, mens øvelse handler om å utvikle organisasjonens evne til å håndtere en hendelse. Øvelse omhandler ikke bare «selve øvelsen», men også forberedelser/planlegging i forkant og evaluering/oppfølging i etterkant.

For å oppnå resiliens er det nødvendig å utvikle ferdigheter både på individnivå (trening) og organisasjonsnivå (øvelse). Samtidig er det viktig å ha god kjennskap til den tekniske delen av cyber-forsvaret. Man kan ikke alltid være sikker på at systemene fungerer akkurat som planlagt/spesifisert, derfor bør de tekniske løsningene testes, slik at man «vet hva man har» og kan forbedre de sårbare delene av systemet.

For å kunne trene på håndtering av cyber-hendelser kan organisasjonen gjennomføre simulering av angrep gjennom f.eks. å arrangere en pentest med såkalte blue-team og red-team der øvelsen også hensyntar et eventuelt forsvar under en pentest. Dette bør helst skje på et backup/testsystem da f.eks. en pentest kan kjøre systemet ned. Andre vanlige øvelser kan for eksempel være enkle phishingangrep eller større øvelser som cyber drill.

NVE har laget en veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen /24/. Den inneholder flere eksempler på IKT-øvelser som også kan være relevant å øve på innen olje & gass:

- Enkel IKT-øvelse, anonym trussel

- Middels krevende IKT-øvelse, hacking
- Middels krevende IKT-øvelse, tyveri av sensitiv informasjon
- Krevende IKT-øvelse: Angrep på SCADA-system

I tillegg inneholder rapporten også relevante øvelser av typen brann i driftskontrollrom, varsling, pandemi, terrortrussel, osv. Øvelsene er tilpasset kraftsektoren, men det burde også være mulig å tilpasse dem til olje & gass-sektoren. I det minste kan man her finne inspirasjon til scenarier å øve på.

For mer detaljer rundt trening og øvelser, se DNV GL rapport /26/).

4.3.5 Kontinuerlig forbedring

Systemet kan sies å modnes/herdes etter hvert som risikoreduserende tiltak implementeres. I tillegg må man stadig følge med på endringer i risikobildet i form av nye trusler og sårbarheter. Hendelser som rammer andre i samme bransje eller i andre industrier vil også kunne være en vekker om at noe kan forbedres.

De nye mulighetene som økt digitalisering og ny teknologi medfører, vil også kunne føre til ny risiko som gir behov for nye tiltak og barrierer. Det er mange nye teknologier som er i vinden for tiden og som det er store forventninger til. For å nevne noen: Stordata (Big Data), blokkjede (blockchain), kunstig intelligens (AI), maskinlæring, tingenes internett (IoT og IIoT), 5G. Mye av teorien rundt for eksempel maskinlæring har vært kjent i mange år, men det er først i våre dager at man kan gjøre noe effektivt i praksis på grunn av mye raskere prosessering og større tilfang av lærings- og testdata.

5 CYBERSIKKERHET I RELASJON TIL BLOKKJEDE-TEKNOLOGI

I dette kapitlet ser vi på om blokkjedeteknologi kan brukes for å øke cyber-resiliens. I forbindelse med cyber-resiliens er det spesielt interessant at en blokkjede tar vare på integritet ved at den er såkalt «tamper-proof» - det er i utgangspunktet umulig å tukle med data lagret i blokkjeden. I tillegg til at transaksjoner lagres i blokker som er kjedet sammen er blokkjeden lagret på alle noder (servere) som deltar. Dette utgjør en desentral database. Nedenfor gir vi en generell introduksjon til blokkjedeteknologi og drøfter om dette også gir verdi for bedre sikring av OT eller sikring av grensesnittet mellom IT og OT.

5.1 Bakgrunn for blokkjede

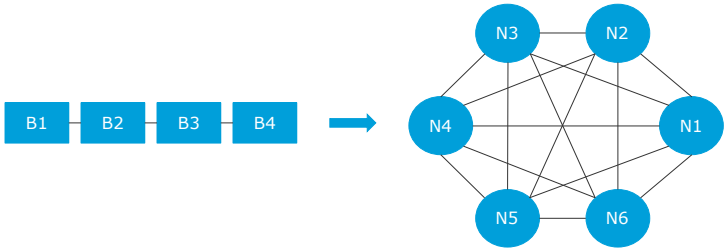
Blokkjede («Blockchain» eller «Distributed Ledger Technology» - DLT på engelsk) er en forholdsvis ny type teknologi for databehandling som det er skapt store forventninger til. Det er mange sider på internett som inneholder ett eller annet med blokkjede. For eksempel kom det i november 2019 opp 259 millioner treff[8], ved et enkelt søk på ordet «blockchain» i Google.

Mange forbinder blokkjede med kryptovaluta (Bitcoin) som var den opprinnelige applikasjonen, men blokkjede kan også ha andre anvendelsesområder som går langt utover dette.

*Vitalik Buterin (grunnlegger av Ethereum)**: "**One of the big things that needs to be communicated is the fact that five years ago the blockchain was just about bitcoin, but now it's much bigger than just bitcoin. It's split off into separate spaces that have a lot of different visions."*

https://www.thestar.com/business/2019/08/19/ethereums-vitalik-buterin-on-reducing-cryptocurrencys-risks.html

En blokkjede er et nettverk av distribuerte databaser. I grove trekk går dette ut på at mange noder (servere) i et nettverk benyttes for å lagre og behandle data i et desentralt register («ledger» eller hovedbok). Flere eller alle noder i nettverket må godkjenne transaksjonen ut ifra et konsensusregelverk. Disse reglene kan være forskjellig avhengig av type blokkjede, hvor mange noder som må godkjenne, osv. Data om transaksjoner pakkes inn i blokker og kjedes sammen – derav navnet blokkjede. En blokk inneholder transaksjonsdata og blant annet et tidsstempel samt hash-verdien[9] til forrige blokk og hash-verdien til seg selv.



Figur 5-1 – En blokkjede bestående av fire blokker er lagret på seks noder som alle kan kommunisere med hverandre

Transaksjonsdata er autentisert med digitale signaturer (asymmetriske kryptografiske nøkler). Blokker i kjeden skal ikke kunne forfalskes uten at det blir oppdaget. En blokkjede skal derfor være «tamper-proof». Alle blokker lagres på alle noder. Noen omtaler derfor blokkjede som «distribuert sannhet» (ref. /8/).

8 Et tilsvarende søk i januar 2018 ga 60 millioner treff, ref. /13/. Dette må sies å være en kraftig økning på nesten to år. Søk med «blockchain» som søkeord var imidlertid på det høyeste i desember 2017 og har senere gått noe ned. Til sammenligning har søk etter Bitcoin hele tiden vært ca. 10 ganger høyere enn søk etter blockchain (Google trends).

9 Enkelt forklart er en hashing-algoritme en matematisk «enveisoperasjon» som med utgangspunkt i et gitt datasett genererer et tall med fast lengde. Dette tallet kalles en hash-verdi. Egenskapene er slik at ved den minste endring i datasettet (bare ett tegn) vil hash-verdien endres radikalt. I tillegg er det (nesten) umulig at to ulike datasett får samme hash-verdi – dette kalles kollisjonsfrihet. Det samme datasettet vil alltid gi den samme hash-verdien. Derfor kan to uavhengige noder se at de har de samme data.

Typiske applikasjoner hvor blokkjede kan være spesielt egnet er hvor det er store krav til sikkerhet/autentisitet av transaksjoner, hvor det ikke er en betrodd tredjepart, og hvor sporbarhet er viktig.

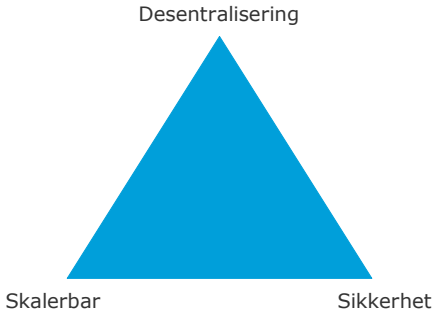
Det finnes i hovedsak to typer blokkjeder:

1. Ikke-tilgangsstyrt blokkjede («permissionless»)
2. Tilgangsstyrt blokkjede («permissioned»)

Den første typen kalles ofte offentlig («public») blokkjede og hvem som helst som har den riktige programvaren har tilgang (eksempel Bitcoin), i den andre typen må brukere gis tillatelse og rettigheter fra eieren eller eierne av blokkjeden. Dette kalles ofte også privat eller konsortium blokkjede. Privat/konsortium blokkjede er spesielt populært innen banker, handel, shipping og telekom. Disse blokkjedeløsningene er typisk mer sentraliserte, i og med at det er færre noder som validerer transaksjoner og genererer blokker. Det er også mulig å kjøre blokkjeder i lukkede nett.
(Ref. https://thenextweb.com/hardfork/2018/11/05/permissioned-permissionless-blockchains/)

Ulike varianter av blokkjeder kan ha ulike krav til desentralisering, sikkerhet og skalerbarhet, hvor det er vanskelig/umulig å oppnå maksimal verdi av alle tre egenskaper. Vitalik Buterin har kalt dette et blokkjede-trilemma:

- Sikkerhet og desentralisering medfører redusert skalerbarhet (hastighet, ytelse, antall brukere)
- Sikkerhet og skalerbarhet nødvendiggjør redusert desentralisering (økt sentralisering)
- Skalerbarhet og desentralisering medfører redusert sikkerhet.



Figur 5-2 – Trilemma-trekant for blokkjede (valg av to egenskaper går på bekostning av den tredje), tilpasset fra ref. /9/

Utdrag fra intervju med Vitalik Buterin, The Star, 19.8.2019:
How do you improve scalability?
VB: *The main problem with the current blockchain is this idea that every computer has to verify every transaction. If we can move to networks where every computer on average verifies only a small portion of transactions then it can be done better.*
Can that be done without sacrificing security?
VB: *There would be a sacrifice but it would be fairly modest.*
Would scalability bring costs down?
VB: *By a lot — by a factor of over 100 for every transaction.*

https://www.thestar.com/business/2019/08/19/ethereums-vitalik-buterin-on-reducing-cryptocurrencys-risks.html

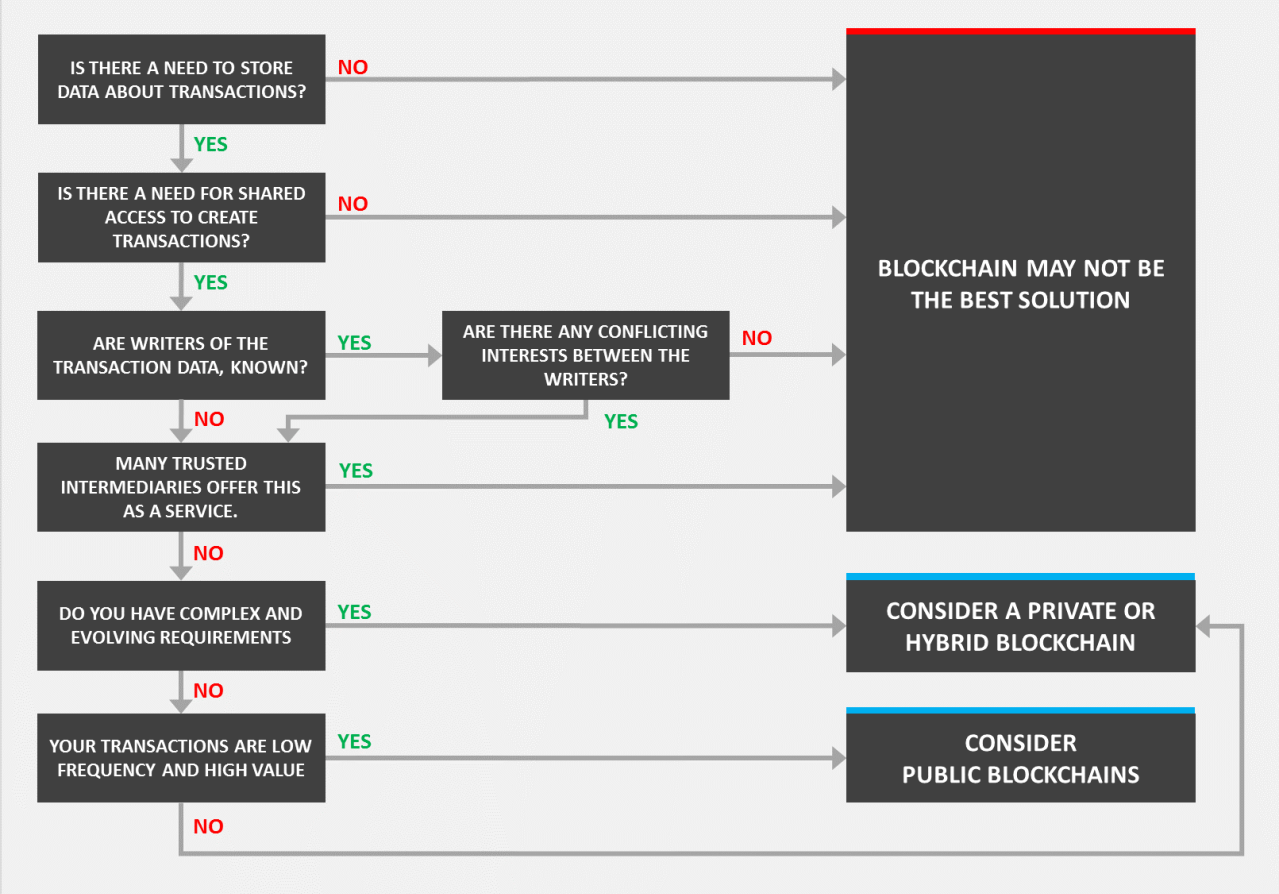
5.2 "To blockchain or not to blockchain – that's the question"

Når er blokkjedeteknologi relevant og når er den mindre hensiktsmessig? Flere kilder har laget lignende flytskjema som det vi har gjengitt i Figur 5-3. Hovedbudskapet er at man må først bestemme seg for hvilket problem man skal forsøke å løse og deretter finne ut om blokkjede er veien å gå.

IATA skriver følgende i et whitepaper om blokkjede i luftfart /6/:

"While the value of Blockchain is concrete in certain use cases, the approach should start with a specific problem and remain solution oriented throughout the process to avoid Blockchain becoming a solution that is looking for problem to solve. When there is a use case for Blockchain, all design options (e.g. public versus private, permissioned versus permissionless) should be carefully analyzed to arrive at the most suitable solution."

Nedenfor gjengis deres flytskjema for å velge om man skal bruke blokkjede, og i så fall hvilken type som passer best.



Figur 5-3 – Flytskjema for valg av blokkjede eller ikke blokkjede, IATA /6/

Som man ser av flytskjemaet over er det i mange tilfeller ikke opplagt at blokkjede er den optimale løsningen, men at heller en sentral database-løsning kan være å foretrekke.

Følgende tabell gir en oversikt over egenskaper forbundet med to typer blokkjeder sammenlignet med en sentral database.

Tabell 5-1 – Sammenligning av to typer blokkjede og en sentral database

Egenskap	Ikke-tilgangsstyrt blokkjede	Tilgangsstyrt blokkjede	Sentral database
Ytelse (throughput)	Lav	Høy	Svært høy
Antall med lesetilgang	Høy	Høy	Høy
Antall med skrivetilgang	Høy	Lav	Høy
Antall upålitelige skrivere	Høy	Lav	Ingen
Sentralt styrt	Nei	Ja	Ja

Tabellen er oversatt og tilpasset fra tilsvarende tabell i Wüst, Gervais (2017), Do you need a blockchain? /11/.

Det er ikke alle typer data som egner seg å lagre i blokkjede på grunn av lovreguleringer. Egenskapen uforanderlighet (dvs. at blokker ikke kan slettes) kan bryte med prinsipper som at noen kan be om at visse typer data skal kunne slettes, eller at data bare skal lagres i et visst antall måneder – for deretter å slettes. Man må derfor grundig tenke igjennom slike forhold før man starter med å implementere blokkjedeløsning. Deloitte har drøftet dette i sin rapport til regjeringen /8/.

Ett tiltak kan være å lagre transaksjoner om status av prosessen i en blokkjede, men holde selve dataene lagret i en sentral database. Dette er filosofien i enterprise-blokkjeden som det nystartete blokkjede-utviklingsselskapet Vakt er i ferd med å utvikle for oljeindustrien. Blokkjeden er bare en del av løsningen, 80 % av innsatsen går med til «business as usual» applikasjonsutvikling og infrastruktur, ref. whitepaper fra ThoughtWorks, Vakt /12/.

Det er mange andre forhold rundt blokkjeder som vi ikke kommer inn på i denne rapporten, så som hvilke verifikasjons- eller konsensusmekanismer som benyttes (Proof of Work, Proof of Elapsed Time, Proof of Stake, Proof of Authority, Byzantine Fault-Tolerant), ulike filosofier for DLT som «chain» versus «tangle», osv. Det er også etter hvert blitt en del implementasjoner av blokkjedeteknologi, så som Ethereum, Hyperledger, Iota, for å nevne noen. Vi tar ikke stilling til egnethet av disse, eller hva som er best. Blokkjedeteknologien synes ennå å ikke være helt moden og mye kan endre seg i løpet av få år. Vi fokuserer derfor mer på bruken av blokkjede enn alle ulike varianter og implementeringer.

"Every enterprise needs special features and modifications to help a blockchain achieve its intended purpose. Since different organizations have different needs, there will never be one single, standard blockchain. Instead, we expect to see many blockchains with different features that provide a wide range of solutions across many industries."

An Introduction to Hyperledger, August 2018, https://www.ibm.com/downloads/cas/0XMOQJNP

5.3 Blokkjede bidrag til sikkerhet og resiliens

De viktigste egenskapene ved blokkjede er at den ivaretar integriteten av data som er lagret og at data er lagret flere steder. Mer spesifikt bidrar blokkjede til sikkerhet og resiliens gjennom følgende egenskaper:

- Desentralisering
- Uforanderlighet («immutability»)
- Transparens
- Håndhevet ansvarlighet («enforced accountability»)
- Beskyttelse av kritisk infrastruktur

Nedenfor går vi igjennom hver av disse egenskapene i mer detalj.

5.3.1 Desentralisering

Et desentralisert system er svært feiltolerant. Hvis en node krasjer i blokkjede-nettverket, medfører ikke det at hele systemet går ned, siden det er andre noder i nettverket som fortsatt er oppe. Desentralisering gir også mer sikkerhet siden informasjonen som er lagret på en datamaskin må kopieres til alle noder i nettverket. Dette betyr at hvis en node blir kompromittert, må en hacker være nødt til å endre informasjonen på andre noder for å kunne manipulere dataene. Dette er en barriere som kan bidra til å avskrekke angrep mot systemet.

I den distribuerte løsningen signeres transaksjoner digitalt med asymmetrisk kryptering (offentlige og private nøkler), og dette sammen med hash-algoritmen gjør blokkjeden sikrere mot angrep.

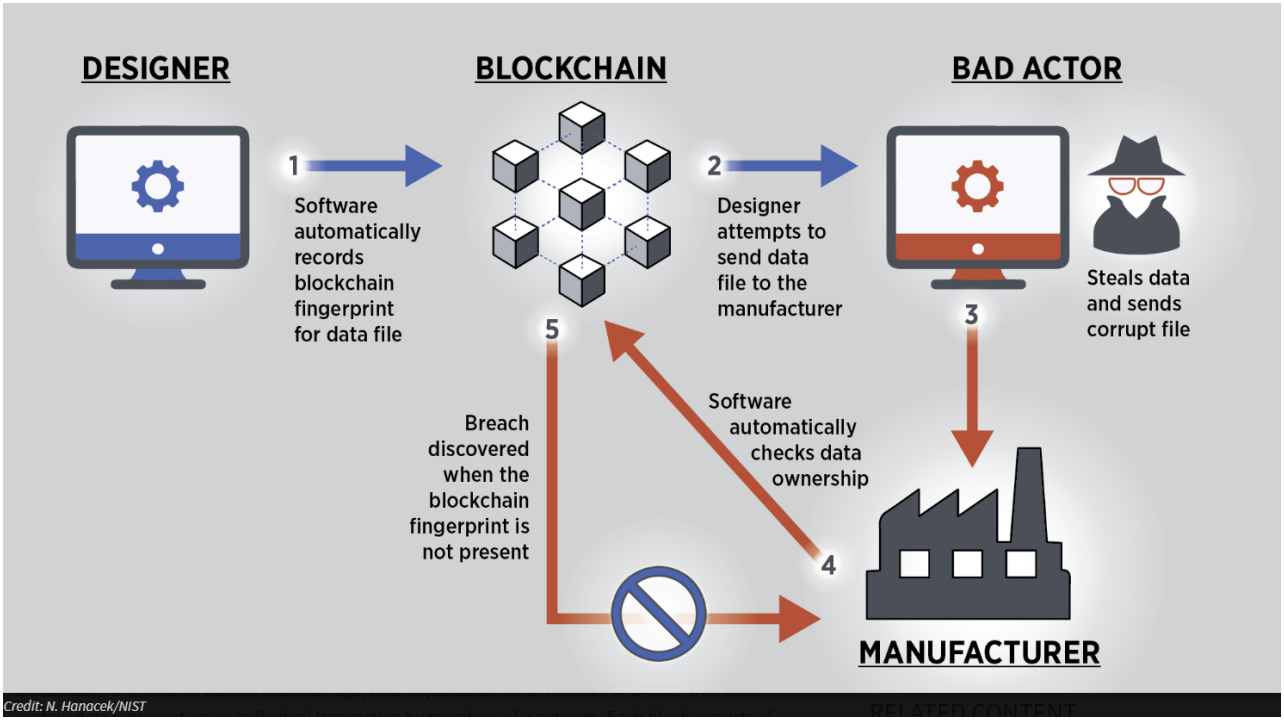
Offentlige blokkjeder med mange noder bidrar til å dempe konsekvensen av DDoS-angrep i og med at det er vanskelig å treffe alle noder. For en privat eller konsortium blokkjede vil det typisk være færre noder, slik at denne ikke er like motstandsdyktig mot et slikt angrep.

Hvis vi sammenligner med en sentral database, kan denne dubleres i en såkalt «high-availability» løsning. Kritiske applikasjoner kan ha en reservelokasjon med servere, og data kan i tillegg speiles til en tredje lokasjon for sikkerhetskopi. Det finnes også skyløsninger der prosesseringen foregår på flere servere. Dette sikrer mot hardware-feil, men ikke mot logiske feil eller dataangrep, som lett vil kunne spre seg mellom redundante databaseservere. Nå er riktignok ikke blokkjeder sikre mot logiske feil heller, da for eksempel smarte kontrakter kan inneholde feil i koden.

5.3.2 Uforanderlighet («immutability»)

En blokkjede lagrer informasjon som blir uforanderlig, noe som betyr at den ikke kan endres når en blokk er blitt validert. Dette gjør den også motstandsdyktig mot manipulering fordi informasjonen er lagt inn i en digital hovedbok som er lagret på mange noder. For å kunne endre historiske blokker må en potensiell angriper ha kontroll over flertallet av noder. Dette kalles et 51 % angrep. Dette gjør at et slikt angrep blir veldig krevende.

Følgende illustrasjon fra NIST viser hvordan forsøk på å endre data vil bli oppdaget:



Figur 5-4 – Illustrasjon av hvordan blokkjede sikrer data mot manipulering.
https://www.nist.gov/el/systems-integration-division-73400/blockchain-industrial-applications-community-interest

5.3.3 Transparens

Et sentralt trekk ved blokkjede er transparens. Informasjon om en transaksjon kan ikke skjules, så dette skaper mer tillit og gir økt verdi. Dette gir sporbarhet og mulighet for innsyn/kontroll av alle transaksjoner. For eksempel kan en utro tjener på innsiden ha store vanskeligheter med å fjerne spor etter uautoriserte handlinger. Transparens betyr ikke nødvendigvis at alle data i transaksjonen ligger åpent. Data kan være kryptert. En annen måte å løse dette på er å lagre slike data utenfor blokkjeden («off-chain»), og kun beholde data i kjeden som sikrer sporbarhet av selve transaksjonen.

5.3.4 Håndhevet ansvarlighet

Blokkjeden med sin distribuerte hovedbokarkitektur gjør det til et godt verktøy for de som ønsker å ha revisjonsstøtte for sikkerhet og infrastrukturstyring. Siden det er svært vanskelig eller umulig å forfalske data lagret i blokkjeden, er det faktisk mye enklere å gjøre jobben i henhold til et regelverk enn det er å svindle. Man vil derfor kunne ha høy tillit til data som ligger i en blokkjede, og som sjekkes ved revisjon eller tilsyn.

5.3.5 Beskyttelse av kritisk infrastruktur

Blokkjede kan bidra til sikring av kritisk infrastruktur ved hjelp av to egenskaper, verifikasjon av endringer og transparens av transaksjoner. Det er langt vanskeligere å skjule noen form for skadevare på et system når det er oversikt over enhver endring, og vanskeligere å gjøre ulovlige endringer når autoriteten til å gjøre en endring må verifiseres av flere noder i et distribuert system.

5.4 Blokkjede-sårbarheter

Selv om blokkjedeteknologi er laget for å være sikker, er det ikke dermed sagt at det ikke er sårbarheter. Dette skyldes som oftest forhold på "utsiden" eller i endene av selve blokkjeden. Nedenfor er noen betraktninger:

"For all systems, the theft of passwords or other access devices through various forms of attack is a common and recurring problem. Blockchains are no different. The majority of attacks related to blockchains have been designed to steal cryptographic keys, not necessarily attack the blockchain itself."
https://digitalchamber.org/wp-content/uploads/2018/03/Blockchain-Cyber-Security_WhitePaper_Single-Page_Linked.pdf

"If your bitcoin exchange gets hacked, you lose all of your money. If your bitcoin wallet gets hacked, you lose all of your money. If you forget your login credentials, you lose all of your money. If there's a bug in the code of your smart contract, you lose all of your money. If someone successfully hacks the blockchain security, you lose all of your money."
https://www.bloomberg.com/opinion/articles/2019-05-03/blockchain-hype-missed-the-mark-and-not-by-a-little

Kryptovalutabørser synes å være spesielt populære angrepsmål. Det er ikke selve blokkjedene som blir hacket, men børsene hvor det er mulig å få ut virkelige penger. Nedenfor er overskrifter fra to hendelser i juli 2019:

BITCOIN NORGE HACKET

Norsk bitcoinbørs hacket: – Jeg har mistet alle sparepengene mine, sier sjokkert kunde

Digi.no, 2.7.2019, https://www.digi.no/artikler/norsk-bitcoin-bors-hacket-jeg-har-mistet-alle-sparepengene-mine-og-er-i-veldig-darlig-form-sier-sjokkert-kunde/469007

Kryptobørs i Japan hacket for 275 millioner

Den japanske kryptobørsen Bitpoint, med lisens fra det japanske finanstilsynet, ble torsdag hacket og skal ha mistet kontrollen for kryptovaluta verdt over 275 millioner kroner.

E24.no, 12.7.2019, https://e24.no/boers-og-finans/bitcoin/kryptoboers-i-japan-hacket-for-275-millioner/24657026

5.4.1 Et utvalg av sårbarheter

51 % angrep

Blokkjeder kan angripes ved et såkalt 51 % angrep hvor noen av deltakerne konspirerer mot resten for å svindle. I 2018 ble flere kryptovalutaer så som ZenCash, Verge og Ethereum Classic angrepet på denne måten. Totalt fikk angriperne med seg 20 millioner dollar. https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security-issues-in-2019

Skalerbarhet og desentralisering

Ifølge trilemmatrekanten (ref. Figur 5-2) vil det å fokusere på desentralisert blokkjede kombinert med høye krav til skalerbarhet kunne gå på bekostning av sikkerhet. En rask konsensusmekanisme med få noder involvert, kan være mindre sikker enn en som involverer alle noder. En måte å sikre dette på, i en privat eller konsortium blokkjede, kan være å kjøre i et lukket nettverk.

Ikke alle noder er like sikre

Ved bruk av konsortium blokkjede kan det være en utfordring at ikke alle deltagende organisasjoner har like god kontroll på sikkerhet i sine egne systemer. De kan derfor utgjøre en større flate for eksternt angrep. NIST /2/ deler inn organisasjoner i ulike nivåer fra Tier 1 (minst sikker) til Tier 4 (mest sikker). Det kan derfor være krav til en organisasjon om et visst minimum av sikkerhet for å kunne delta i et konsortium eller få tilgang til en privat blokkjede. Dette gjelder spesielt for organisasjoner som skal ha skriveaksess, godkjenne transaksjoner og generere blokker, mens for de som kun skal ha leseaksess er ikke dette like viktig.

Manglende test i full skala

Mange blokkjeder er ikke testet i full skala, og det er usikkert hvordan skalerbarheten er. De offentlige, ikke-tilgangsstyrte blokkjedene Bitcoin og Ethereum er så langt de eneste som er satt på skikkelig prøve, og status i dag er at Bitcoin er veldig treg, og Ethereum er i ferd med å nærme seg maksimal størrelse. Dette er uutforsket terreng og skalerbarhet er et problem.

Ikke alle data egner seg

Som vi var inne på i kapittel 5.2 er det ikke alle typer data som egner seg å lagre i blokkjede på grunn av lovreguleringer. En sårbarhet er derfor at det uforvarende lagres data i blokkjeden som slett ikke skulle vært lagt der. En måte å håndtere dette på som nevnt tidligere, er å lagre slike data utenfor blokkjeden, og kun beholde data om selve transaksjonen i kjeden.

Leverandørsikkerhet

Hvis tredjepartsleverandører utvikler blokkjedeplattformen og tilhørende applikasjoner, så er sikkerheten også avhengig av hvor troverdig og dyktig leverandøren er. For offentlige, ikke-tilgangsstyrte blokkjeder, er det i praksis softwareutviklerne som eier blokkjeden.

Feil i applikasjoner

Applikasjoner oppå blokkjeden kan inneholde sårbarheter – for eksempel smarte kontrakter. Smarte kontrakter drøftes nærmere i kapittel 5.6.7.

De vanlige sårbarhetene gjelder også her

Andre sårbarheter så som sosial manipulering, phishing, osv., gjelder også i forbindelse med blokkjede. Det hjelper ikke hvor «tamper-proof» en blokkjede er dersom noen kan utnytte sårbarheter på utsiden av blokkjeden.

Datakvalitet

Og sist, men ikke minst, dårlig datakvalitet vil fortsatt gi «garbage in → garbage out». Blokkjede løser på ingen måte det problemet. Så selv om noen omtaler blokkjede som «distribuert sannhet», så behøver ikke dette å stemme med de fysiske realiteter som ligger bak dataene.

5.4.2 Manglende standardisering og regelverk

Manglende standardisering og regelverk kan gjøre det vanskelig å implementere gode løsninger på tvers av organisasjoner. Interoperabilitet mellom ulike typer blokkjeder virker også å være et uutforsket tema. Man kan risikere lock-in til én leverandør, og/eller at man har valgt feil, og må foreta et dyrt bytte på et senere tidspunkt. Og det er ikke garantert at den eller de beste løsningen(e) vinner. Noen har sammenlignet dette med forrige århundres strid mellom videoformatene VHS og BetaMax, hvor mange mener at det dårligste produktet vant, og sluttresultatet var at de som hadde kjøpt BetaMax måtte kaste utstyret sitt.

5.4.3 Stort energiforbruk

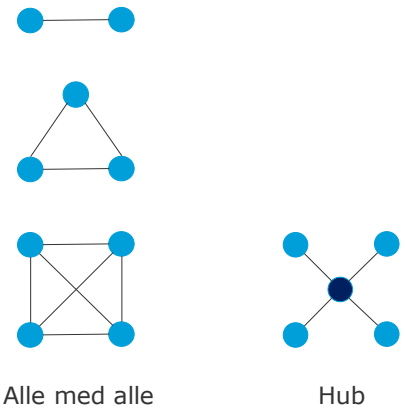
Til slutt vil vi nevne en annen bekymring med blokkjede, som ikke har med IKT-sikkerhet å gjøre, men med bærekraft. Dette er et aspekt som særlig gjelder offentlige blokkjeder med svært mange noder. Det å spre prosessering og data på mange noder fører til stort behov for lagringsplass, datakraft og kommunikasjonsbåndbredde. Dette fører igjen til stort strømforbruk og tilhørende CO_2 fotavtrykk. Særlig er Bitcoin med minering og sin spesielle konsensusmekanisme en versting i så måte.

"Bitcoin's electricity usage is enormous. In November, the power consumed by the entire bitcoin network was estimated to be higher than that of the Republic of Ireland. Since then, its demands have only grown. It's now on pace to use just over 42TWh of electricity in a year, placing it ahead of New Zealand and Hungary and just behind Peru, according to estimates from Digiconomist. That's commensurate with CO2 emissions of 20 megatonnes – or roughly 1m transatlantic flights."

The Guardian, 17. januar 2018, https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

Til sammenligning var Norges brutto elektrisitetsforbruk på 134,1 TWh i 2017. Ref. Teknisk Ukeblad, 8. februar 2018, https://www.tu.no/artikler/norge-brukte-rekordmye-strom-i-fjor/430005.

I blokkjedeteknologi skal et stort antall noder kommunisere med hverandre. Figuren nedenfor gir en sammenligning av antall logiske kommunikasjonsmuligheter der alle kommuniserer med alle, versus en datahub eller sentral database.



Alle N noder kommuniserer med alle:
Antall forbindelser: 1 + 2 + 3 + … + N-1 = N(N-1)/2

Datahub:
Antall forbindelser = N

Eksempel N = 100,
N(N-1)/2 = 100 x 99/2 = 4 950

Hvis N ≥ 4, har en datahub færre forbindelser, enn hvis alle skal kommunisere med alle.

Figur 5-5 – Sammenligning av antall kommunikasjonsveier der alle kommuniserer med alle, versus en datahub.

Dette illustrerer at mens kommunikasjonsbehovet for en datahub øker lineært med antall noder N, vil kommunikasjonsbehovet for blokkjedeteknologi øke kvadratisk som N^2. For det samme antall noder vil blokkjede være mye mer kommunikasjonskrevende enn en datahub. Erfaring har vist at ved størrelsesorden 10 noder som må kommunisere med hverandre, vil det kunne det lønne seg å implementere en sentral datahub. På den annen side vil en datahub være «single-point-of-failure» og hvis denne blir utsatt for noe, vil hele nettverket rammes[10]. Derfor er en blokkjede med mange noder sikrere ut fra et desentraliseringssynspunkt (ref. kap. 5.3.1), men har mye større kommunikasjonsbehov, og derav tregere prosessering enn en sentral datahub.

Det finnes private blokkjeder i lukkete nettverk med få noder uten avansert validering, som synes å kunne kombinere fra begge verdener. Det finnes også tilgangsstyrte nettverk der bare noen få noder validerer (Proof-of-Authority). Energyweb.org har ca. 1000 deltakere og 25 noder som validerer /25/. Denne har ifølge dem selv en kapasitet på ca. 30 x Ethereum eller ca. 600-750 transaksjoner per sekund (rundt 3000-3750 transaksjoner på 5 sekunder).

10 For å gjøre dette på en sikker måte må en datahub lages som en high availability løsning med dublering av servere, databaser og reservelokasjon.

5.5 Hvordan sikre blokkjeder

Det er startet arbeid med hvordan sikre systemer basert på blokkjeder. I USA har Government Blockchain Association (GBA) Cyber Security Working Group begynt å diskutere hvordan man kan benytte NIST SP 800-serien for å vurdere sikkerheten av en blokkjedeløsning.

De har utgitt et whitepaper «Assessment and Authorization of Blockchain Systems» /19/ hvor dette blir gjennomgått. I USA må et offentlig føderalt IT-system igjennom en A&A (Assessment & Authorization) før det kan settes i produksjon. De går særlig inn på spørsmål som[11]:

- *Hvem «eier» blokkjeden?*
- *Hvem er ansvarlig for overordnet sikkerhet av blokkjeden eller applikasjonen?*
- *Hvem er ansvarlig for å bestemme om en node tillates å inngå i blokkjeden?*
- *Hvem er ansvarlig for oppsyn/kontroll for å sikre vedvarende overensstemmelse?*
- *Hvem har autoritet til å autorisere en blokkjedeløsning?*
- *Hvordan evaluere smarte kontrakter før de blir lagt på en blokkjede?*
- *Hvem er ansvarlig for å styre konsensusmekanismen?*

Videre går de i mer detalj gjennom RMF (Risk Management Framework) kontroll-familier fra NIST SP 800-53 og hvordan disse kontrollene er anvendelig for en blokkjede. RMF kontroll-familier er for eksempel Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), osv. Innen hver familie stiller de spørsmål som kan være relevant for blokkjede.

Chamber of Digital Commerce og Microsoft anbefaler at tilsvarende prinsipper fra NIST følges i finanssektoren, ref. whitepaper /28/.

5.6 Eksempler på mulige bruksområder

Det er blitt hevdet at blokkjede kan brukes til nær sagt hva som helst, men i mange tilfeller er nok dette å overdrive. Det synes å være særlig to generiske tilfeller hvor blokkjedeteknologien vil kunne bidra i positiv retning, både når det gjelder effektivisering og resiliens:

1. Blokkjede kan bidra til å effektivisere og øke sikkerheten i eksisterende prosesser
2. Blokkjede kan muliggjøre helt nye måter å gjøre ting på, som ikke ville vært mulig før

> *"With blockchains, many existing business processes in many industries can be streamlined to save time, save money, and reduce risk. And many entirely new processes—perhaps even whole new industries—can be invented."*
>
> An Introduction to Hyperledger, August 2018, https://www.ibm.com/downloads/cas/0XMOQJNP

Nedenfor er noen eksempler på mulig bruk av blokkjedeteknologi. De fleste av blokkjede-bruksområdene vi har behandlet går direkte på å sikre integritet, autentisitet og tilgjengelighet og derigjennom bidra til cyber resiliens. Imidlertid er det ikke alle blokkjede-bruksområdene som er like lette å gjennomføre. Kun de tre første bruksområdene har med OT eller grensesnittet mellom IT og OT å gjøre. Dette gjelder 5.6.1,

[11] Oversatt av DNV GL.

5.6.2 og særlig 5.6.3, hvor dette med digital tvilling er en aktuell problemstilling. Resten av bruksområdene er mer generell IT. Flere av eksemplene ligner på hverandre i og med at de benytter blokkjedeteknologi på samme måte, men applikasjonen kan være forskjellig.

I noen tilfeller er det referanse til prosjekter og implementeringer som er iverksatt. I andre tilfeller er dette mer på idé-stadiet. De fleste kildene er fra 2018 og 2019. Ut ifra kildene er det ikke alltid like lett å bedømme hvor modent det enkelte eksemplet er[12].

5.6.1 Integritetssjekk av konfigurasjonslogger

En plattform eller annen innretning består typisk av mange systemer satt sammen av flere leverandører. Det kan være en utfordring til enhver tid å vite status på konfigurasjonen. En blokkjedeløsning av konfigurasjonsloggen vil kunne sikre integritet, og at ingen kan slette eller endre deler av en logg. En utfordring her er å sikre innrapporteringskanalen, at det til enhver tid registreres faktisk konfigurering. Leverandørene må derfor ha direkte tilgang og blokkjeden må automatisk oppdateres hver gang en konfigurasjonsendring gjøres. Den opplagte fordelen her er at hvis noe uforutsett skjer, kan man dokumentere nøyaktig hvordan konfigurasjonen var på det angitte tidspunkt. Utfordringen er å kunne implementere dette med en stor samling leverandører, underleverandører og andre aktører. En privat eller konsortium blokkjede synes å være mest aktuelt.

Logganalyseverktøyet Splunk har begynt å bruke blokkjede for å gjøre logger sikrere mot manipulering, ref. https://www.splunk.com/blog/2018/09/24/the-newest-data-attack.html

5.6.2 Effektivisering/integritetskontroll av dokumentsystem og sertifikater

DNV GL har laget en privat blokkjedeløsning for å sikre at alle kan se at sertifikatene er ekte («non-repudiation») og at de ikke er endret (integritet).

> *"DNV GL has transferred all its 90 000 certificates to a private blockchain, being the first in the certification industry to leverage on this technology. Every certificate is digitally tagged, traceable and stored in a private blockchain. The technology blocks counterfeit certificates, allowing companies to communicate their certification in a transparent and secure way."*
>
> https://www2.deloitte.com/ie/en/pages/about-deloitte/articles/Deloitte_DNV_GL_first_blockchain_solution_certification_industry.html

Det kreves ofte at et firma eller en operatør har gyldige sertifikater som dekker forskjellige områder. Det er vanskelig å finne en samlet oversikt. I Norge har http://www.kvalex.no/ en oversikt over noen typer sertifikater, men dette gjelder neppe alle relevante sertifikater innenfor olje & gass. Ideelt sett hadde det vært best å ha en slik oversikt fra alle relevante sertifiseringsorganer innenfor et område om status på sertifikater. En konsortium-blokkjedeløsning på tvers av disse sertifiseringsorganene kunne være en måte å løse dette på, men det er kanskje ikke så enkelt å få til dette i praksis. Da må i så fall konkurrenter måtte samarbeide om en felles løsning.

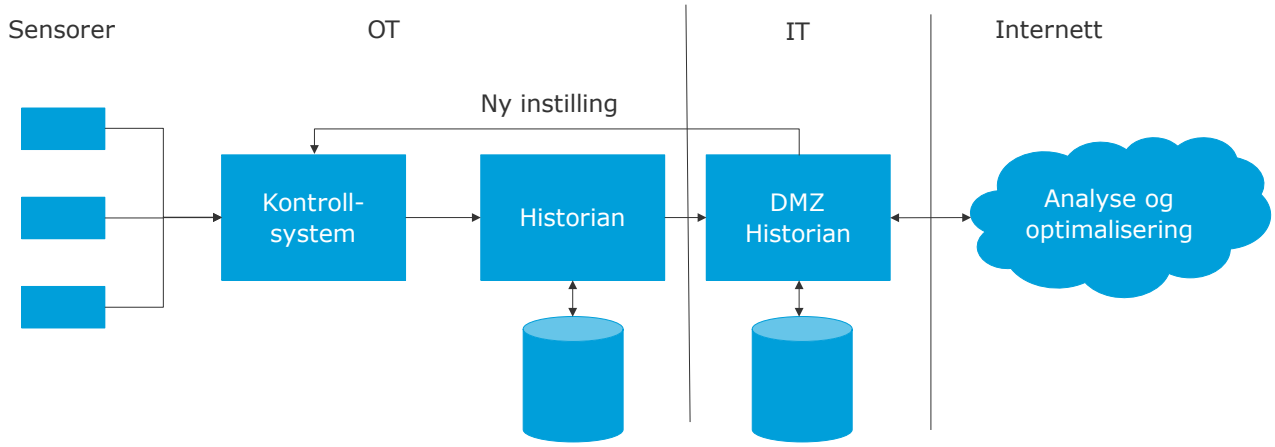
En annen anvendelse er at en operatør kan lage et register for hver installasjon (plattform, landanlegg, etc.) med opplysninger om godkjenninger eller sertifikater på deler som inngår. Sertifikatene kan komme fra ulike kilder. Ved å legge alle sertifikater i en blokkjedeløsning når de blir utstedt, kan alle interessenter som har tilgang, få tak i sertifikatene uten unødig forsinkelse, og være sikret at de er aktuelle og gyldige. Da kan man se hvor ting kommer fra, prosessen de har vært igjennom, osv. Dette

[12] Erfaringsvis er det ikke sjelden at noen går ut og annonserer en satsing på ny teknologi, og gjerne at man har kommet litt lenger enn det man faktisk er. Hvis prosjektet senere mislykkes, kan det være vanskelig å finne opplysninger om det på nettet.

ligner også på det som er drøftet i kapittel 5.6.1 om integritetssjekk av logger og konfigureringer, og kapittel 5.6.4 om sikring og garanti av opprinnelse.

5.6.3 Sikring av informasjonskjede for prosessoptimalisering

Dersom innstillinger i et kontrollsystem skal endres av analyse- og optimaliseringsløsninger, er man avhengig av tillit og sporbarhet. Dette foregår i skjæringspunktet mellom OT og IT. La oss anta at rådata fra sensorer (IoT) eller fra en DMZ Historian (som står på utsiden av kontrollsystemet) sendes til en skyløsning for avanserte beregninger, kanskje ved bruk av maskinlæringsalgoritmer («digital tvilling»). Resultatet fra beregningen skal sendes tilbake til kontrollsystemet for automatisk å justere relevante innstillinger. Dette krever toveiskommunikasjon mellom IT og OT, noe som bryter med sonemodell (e.g. Purdue). Her er det behov for autentisering, kryptering og integritetsbeskyttelse, slik at man er sikker på at ingen har «tuklet» med dataene. I et slikt scenario kan en blokkjede-løsning bidra til økt sikkerhet.



Figur 5-6 – Illustrasjon av logisk dataflyt i eksempelet

Dersom beregningene og interaksjonen skal foregå i tilnærmet sanntid, må løsningen være skalerbar med liten forsinkelse. Dette tyder på at man ikke kan bruke en offentlig blokkjede-løsning med omfattende og tidkrevende konsensusmekanisme. Hvis man ønsker sikkerhet og skalerbarhet, må dette gå på bekostning av desentralisering. En operatør DNV GL har intervjuet har vurdert en slik blokkjedeløsning, men gått bort fra det fordi de har funnet at blokkjedeteknologi er for umoden. De var også bekymret for kvalitet på data.

Et alternativ til å beregne i skyen er, hvis mulig, å la beregningene foregå i kraftige servere innenfor sikker sone. Dette er mer i retning av «edge computing». Da er det mindre behov for ekstra sikkerhet i form av blokkjede eller kryptering. En annen fordel er at man er nærmere rådata og også nærmere korrekt rekkefølge av meldinger, noe som kan være viktig for resultatet av slike beregninger. Man har likevel noen utfordringer med å hente inn eventuelle data på en sikker måte fra eksterne kilder, hvis slike data inngår i beregningsalgoritmen.

Uansett, en kanskje vel så viktig utfordring i dette scenariet er om operatøren våger å stole på beregningene som blir gjort («garbage in → garbage out»), og tillate automatiske justeringer av innstillinger i kontrollsystemet. Dersom justeringen fører til at man kjører utenfor operasjonsvinduet definert i sikkerhetssystemet, vil sikkerhetssystemet stenge ned produksjonen automatisk.

5.6.4 Sikring og garanti av opprinnelse

I noen bransjer er garanti for opprinnelsen til en vare svært viktig, at man kan dokumentere helt sikkert hvor et produkt kommer fra, hvilke prosesser det har vært igjennom, etc. I denne forbindelsen kan en blokkjede-løsning bidra til å garantere for ektheten. Man bør imidlertid være klar over at dette kan saboteres av uærlige aktører[13]. Man må derfor ha tilsyn med at prosessen følges.

Et eksempel på dette er My Story fra DNV GL som blant annet er brukt for å garantere opprinnelsen til vin produsert i Italia. En konsument kan lett kontrollere opprinnelsen til vinen på flasken ved å skanne QR-koden.

"My Story™ as a service will help companies with:

- *Data collection*
- *Access to product information for consumers*
- *Enterprise and product ID issued*
- *Product story shared in the My Story™ dAPP*
- *Verification of activities and data (DNV GL)*
- *Stored on blockchain (VeChain)"*

Merk at noen (DNV GL) er inne og verifiserer aktiviteter og data. En blokkjedeløsning alene er ikke nok. Det må også kontrolleres at ting går riktig for seg.

https://www.dnvgl.com/mystory/index.html

Et annet eksempel er en blokkjede-løsning for LNG fra VeChain:

"The blockchain-based LNG solution can be used to keep track of the core data generated during the transportation, storage, and online-transaction of LNG. The data collected will be stored on the VeChainThor Blockchain, thus making it possible for data to be shared by the suppliers and users. The solution handles the quality assurance process including classification standards, weighing practices, and transportation process for different types of natural gas. All information will be uploaded to the VeChainThor Blockchain to establish credible industry standards per government mandates."

https://www.vechain.com/solution/gas

5.6.5 "On-demand" leveransekjeder

Det er flere initiativer som går ut på å bruke blokkjedeteknologi for å sikre at en reservedel som lages «on-demand» ute i felten ved hjelp av 3D-skrivere er autentisk og identisk med originaldelen. Dette bidrar til sikkerhet i begge betydninger av ordet, både «security» og «safety», i og med at opphavsrettigheter sikres og at kvaliteten er like god som originaldelen. 3D-print bransjen generelt er opptatt av dette og anbefaler blokkjede som medisin.

The Value of Blockchain for Securing 3D Printed Intellectual Property

"Plagiarism is always a concern in the 3D printing world. For makers, this is an annoyance, albeit a sizable one. But when it comes to things like medical devices and aerospace components, plagiarism becomes a serious danger."

https://3dprint.com/224165/blockchain-3d-printed-ip/

13 Eksempel: I stedet for å måle temperaturen i et lasterom hvor det skal være kjølig, plasseres temperatursensoren i et lite kjøleskap i lasterommet. Da vil sensoren måle +4 grader uansett hva temperaturen i lasterommet er.

Eksemplet nedenfor gjelder reservedeler til militærfly.

"For example, the U.S. Department of Defense envisions using on-demand 3D printing to quickly make needed parts for planes. Military agencies could use proprietary designs from suppliers like Boeing that are stored in a blockchain but are transferred to 3D-printing machines using a key code at the machine.

No one outside of Boeing would be able to touch the design data as it moves digitally to the machine. This way, the designs are always available but not exposed, and the military can fix planes and pay for parts without waiting for Boeing to produce them."

Siemens: https://community.plm.automation.siemens.com/t5/Digital-Transformations/Planning-for-the-future-of-blockchain-in-manufacturing/ba-p/538076

Fieldmade er et selskap som jobber med «additive manufacturing» basert på 3D-skriving og bruk av blokkjede. De er del av Equinors Techstars incubator program. http://fieldmade.no/

Det finnes også andre eksempler på 3D-printing innen ulike industrier i Norge, men bruk av blokkjede eller andre måter å sikre autentisitet er ikke nevnt i noen av disse referansene:

Forsvaret: I Norge har FFI eksperimentert med 3D-printing av reservedeler ute i felten (28.09.2016): https://www.ffi.no/no/Aktuelle-tema/videocaster/Sider/Korleis-kan-Forsvaret-bruke-3D-printarar.aspx

Et eksempel fra shipping:
«Norske Espen Sivertsen spesialiserer seg på 3D-printing av reservedeler til shipping-industrien – fra hjertet av Silicon Valley. … I fremtiden ser man for seg at skipsverksteder og andre kan motta en datafil med spesifikasjoner for en reservedel og så produsere lokalt med 3d-printing. Ivaldi Group er allerede i gang med å teste dette i markedet i Singapore.»
Sparebanken Vest, 21.2.2018, https://www.spvnyheter.no/teknologi/3d-printing-kan-bli-en-disruptiv-teknologi/

Et eksempel fra olje og gass:
«I Tronrud Engineerings lokaler i Hønefoss 3D-printes titandeler til Equinors nye oljefelt i Barentshavet. Interessen for teknologien tar av og vil fundamentalt endre flere bransjer, tror både Equinor og HP»

«For første gang har oljeselskapet fått serieprodusert en del med bruk av 3D-printing. Det er snakk om 29 såkalte svanehalser i titan til bruk i brannslangetromler.»
E24.no, 15.1.2019, https://e24.no/digital/equinor/e24-podden-naa-tar-3d-printing-av-og-inntar-norsk-sokkel/24540630

5.6.6 Styring av leveransekjeder

Ofte er det en lang kjede fra produksjonssted til forbruker, og det kan være mye papirarbeid og ulike systemer for å holde rede på prosessen fra A til B til C til D. Feil kan oppstå og prosessen er ikke strømlinjeformet. Et begrep som benyttes, er at det er mye friksjon. I et slikt scenario kan en blokkjede-løsning bidra til økt effektivitet, sporbarhet og integritet.

Det er blant annet gjort forsøk med blokkjedeløsninger for konnossement[14] (engelsk: Bill of lading). Ref. https://cerasis.com/blockchain-for-bill-of-lading/. Konnossement er et dokument, et slags fraktbrev, som følger med lasten på et skip og har tre hovedfunksjoner:

[14] Bill of lading (engelsk) = Konnossement (norsk), ref. https://snl.no/konnossement

1. Kvittering på lasten
2. Dokument på eierskap
3. Bevis på transportavtalen

(ref. https://transporteca.no/konnossement/). Et konnossement kan følge med varene fra skip til tog til fly. Varene kan også videreselges mens de er i transitt. Det at konnossementet er dokument på eierskap gjør dette mulig. Det er derfor viktig at opplysningene i konnossementet er korrekte og «tamper-free». En blokkjede vil kunne lagre alle transaksjonene, og skulle noe være galt med leveransen er hele kjeden fra produsent til endelig sluttkunde sporbar og dokumentert.

Maersk og IBM har siden januar 2018 samarbeidet om en blokkjede for Bill of lading/konnossement:

Maersk and IBM Introduce TradeLens Blockchain Shipping Solution
"Industry-wide collaboration announced in January advances as more than 90 organizations participate in the global trade solution.
More than 154 million events captured on the platform and growing by one million per day."

"In a follow up to their January announcement, A.P. Moller –Maersk and IBM today announced the creation of TradeLens, jointly developed by the two companies to apply blockchain to the world's global supply chain. TradeLens is the result of a collaboration agreement between Maersk and IBM, a blockchain-enabled shipping solution designed to promote more efficient and secure global trade, bringing together various parties to support information sharing and transparency, and spur industry-wide innovation."

"During the 12-month trial, Maersk and IBM worked with dozens of ecosystem partners to identify opportunities to prevent delays caused by documentation errors, information delays, and other impediments. One example demonstrated how TradeLens can reduce the transit time of a shipment of packaging materials to a production line in the United States by 40 percent, avoiding thousands of dollars in cost. Through better visibility and more efficient means of communicating, some supply chain participants estimate they could reduce the steps taken to answer basic operational questions such as "where is my container" from 10 steps and five people to, with TradeLens, one step and one person."

https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution

Denne måten å gjøre det på er overførbart til andre leveransekjeder, f.eks. olje og gassleveranser. IoT kan også sørge for at sensorer overvåker lasten underveis, slik at det dokumenteres om den utsettes for påkjenninger som kan forringe kvaliteten. Dette kan gjøres ved en trigger som sørger for at verdier utenfor grenseområdene blir registrert.

5.6.7 Smarte kontrakter

Konseptet med smarte kontrakter ble lansert i 1996, mens implementasjon ble først mulig rundt 2015 med å bruke blokkjeder som var egnet for dette (Ethereum og Hyperledger).

Enkelt fortalt er en smart kontrakt et program som går på toppen av en blokkjede, og som inneholder et sett med regler som partene er enige om. Hvis og når betingelsene for disse reglene er oppfylt vil kontrakten automatisk tre i kraft. Programmet inneholder derfor logikk av typen «Hvis A så B».

Et eksempel fra forsikringsbransjen illustrerer dette. AXA har en spesiell forsikring mot forsinkelse som innebærer at hvis et fly er mer enn to timer forsinket, har passasjerer rett på kompensasjon. Dette er laget som en smart kontrakt-applikasjon oppå en Ethereum blokkjede. Programmet sjekker mot en

global database som inneholder trafikkdata for fly, og hvis det er registrert en forsinkelse på mer enn to timer, sørger det straks for automatisk kompensasjon til passasjerene som har slik forsikring. (Ref. https://dolare.com/blog/post/8-smart-contracts-use-cases)

Smarte kontrakter kan også inngå i leveransekjeder som beskrevet over i kapitlene 5.6.5 og 5.6.6, og sørge for automatisk betaling for de ulike transaksjonene. Smarte kontrakter inngår også i blokkjedeløsningen til Maersk og IBM:

> *"Using blockchain smart contracts, TradeLens enables digital collaboration across the multiple parties involved in international trade. The trade document module, released under a beta program and called ClearWay, enables importers/exporters, customs brokers, trusted third parties such as Customs, other government agencies, and NGOs to collaborate in cross-organizational business processes and information exchanges, all backed by a secure, non-repudiable audit trail."*
>
> https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution

I oljebransjen er det også lignende initiativer. Her er et presseoppslag fra november 2018:

> ***New Vakt Blockchain Energy Commodity Trading Platform Has Backing of BP, Shell, Equinor and Major Banks***
>
> *"BP, Shell, and Equinor are some of the biggest names in oil, and they decided to make a change in their industry. Together, they are working with trading houses and major banks in an effort to launch a new platform for energy commodity trading, which they have decided to call "Vakt." The news of the launch was reported by S&P Global Platts on November 12th."*
>
> https://www.vakt.com/new-vakt-blockchain-energy-commodity-trading-platform-has-backing-of-bp-shell-equinor-and-major-banks/

Her er man imidlertid mer skeptisk til å bruke smarte kontrakter. Dette er utdrag fra et «white paper» fra ThoughtWorks og Vakt, ref. /12/:

> *"The use of smart contracts tends to polarise opinion. We lean towards the view that they should be used sparingly and only where it makes complete sense to do so. While it is possible to build an entire distributed application with smart contracts it is not necessarily desirable because of the difficulty of management of contract versions, security concerns and complexity in implementing simple business logic. We recommend that you carefully consider what logic you place in smart contracts. At VAKT we are moving more towards using smart contracts only to store state."*

Vi skal nedenfor undersøke noen sårbarheter forbundet med smarte kontrakter. I denne sammenheng er det betimelig å minne om Hyppönens lov[15]: *"Whenever an appliance is described as being "smart", it is vulnerable."*

- En opplagt bekymring er kvaliteten på programvaren som inngår i den smarte kontrakten. Hvis det er komplisert forretningslogikk som ligger til grunn, vil nødvendigvis programmet være tilsvarende komplisert, vanskelig å verifisere, og med stor sannsynlighet inneholde feil, som kan gi ubehagelige overraskelser for dem som har inngått kontrakten. Det er dessuten en utfordring å lage kode som eksekveres på en desentral plattform, i stedet for på en lokal maskin.

[15] Se for eksempel https://en.wikipedia.org/wiki/Mikko_Hyppönen eller https://blog.f-secure.com/hypponens-law-smart-vulnerable/

- Hvis det er noe galt med data fra en sensor eller database utenfor blokkjeden, og som har betydning for beslutningsalgoritmen i den smarte kontrakten, kan den smarte kontrakten begynne å oppføre seg merkelig. En hacker behøver derfor ikke angripe blokkjeden direkte, men kan konsentrere seg om de omkringliggende nodene.
- En annen bekymring er hvis smarte kontrakter benyttes på tvers av landegrenser. Hva med lover og regler som gjelder i ulike land? Husk at smarte kontrakter eksekveres automatisk basert på logikken i programmet. Ingen tredjepart er involvert.
- Det har vært eksempler på at hackere har utnyttet sårbarheter i smarte kontrakter, se for eksempel følgende blogginnlegg fra januar 2019: https://hackernoon.com/smart-contract-vulnerabilities-remain-a-clear-and-present-danger-59acaf82213f.

5.6.8 Sammenligning av de ulike bruksområdene

De fleste av blokkjede-bruksområdene vi har behandlet går direkte på å sikre integritet, autentisitet og tilgjengelighet og derigjennom bidra til cyber resiliens. Imidlertid er det ikke alle blokkjede-bruksområdene som er like lette å gjennomføre. Kun de tre første bruksområdene har med OT eller grensesnittet mellom IT og OT å gjøre. Resten er mer generell IT.

Nedenfor er en tabell som oppsummerer fordeler og ulemper med bruk av blokkjede innen de ulike bruksområdene. Her tenker vi først og fremst på nytteverdi og gjennomførbarhet.

Tabell 5-2 – Fordeler og ulemper ved anvendelse av blokkjede innen ulike bruksområder

Bruksområde	Fordeler	Ulemper	Kommentarer
Integritetssjekk av konfigurasjonslogger	En blokkjedeløsning av konfigurasjonsloggen vil kunne sikre integritet, og at ingen kan slette eller endre deler av en logg. Hvis noe uforutsett skjer, kan man dokumentere nøyaktig hvordan konfigurasjonen var på det angitte tidspunkt.	Utfordringen er å kunne implementere dette med en stor samling leverandører, underleverandører og andre aktører.	
Effektivisering/ integritetskontroll av dokumentsystem og sertifikater	Vil sikre ektheten av dokumentasjon rundt deler som inngår og hvilke prosesser det har vært igjennom		Det er kun den digitale eiendel som er uforanderlig. Blokkjede alene er ikke nok. I tillegg kreves sertifisering.
Sikring av informasjonskjede for prosessoptimalisering	Det er behov for autentisering, kryptering og integritetsbeskyttelse, slik at man er sikker på at ingen har «tuklet» med dataene. I et slikt scenario kan en blokkjede-løsning bidra til økt sikkerhet.	Dersom beregningene og interaksjonen skal foregå i tilnærmet sanntid, må løsningen være skalerbar med liten forsinkelse.	Bryter med prinsipper for sonemodell. Kan også løses på andre måter.
Sikring og garanti av opprinnelse	Man kan dokumentere hvor et produkt kommer fra, hvilke prosesser det har vært igjennom, etc. I denne forbindelsen kan en blokkjede-løsning bidra til å garantere for ektheten.	Dette kan saboteres av leverandør. Det er «innpakningen» som dokumenteres, ikke nødvendigvis det fysiske innholdet.	Blokkjede alene er ikke nok. Det bør i tillegg være tilsyn/revisjon av at prosessen følges.

Bruksområde	Fordeler	Ulemper	Kommentarer
«On-demand» leveransekjeder (3D-print av reservedeler)	Blokkjede bidrar til sikkerhet i begge betydninger av ordet, både «security» og «safety», i og med at opphavs-rettigheter sikres og at kvaliteten er like god som originaldelen.		3D-print-bransjen anbefaler blokkjede.
Styring av leveransekjeder	Blokkjede-løsning kan bidra til økt effektivitet, sporbarhet og integritet.	Det kan bli mange aktører involvert, noe som krever koordinering	
Smarte kontrakter	Smarte kontrakter kan gjøre transaksjoner mellom kunde og leverandør mye enklere, sikre integritet og minimere behandlingstiden.	Jo mer komplisert kontrakt (forretningslogikk), jo mer sannsynlig at koden inneholder feil. Mange parter og mange typer kontrakter kompliserer ytterligere.	Kan se ut til å ha mest for seg i et B2C forhold, med forholdsvis enkle avtaler (ref. eksemplet med forsikring mot flyforsinkelse).

6 DISKUSJON OG OPPSUMMERING

Cyber-resiliens er mer enn å forhindre eller å respondere på en hendelse – cyber-resiliens handler også om evnen til å opprettholde helt eller delvis operasjon mens hendelsen pågår. I tillegg handler cyber-resiliens om å tilpasse forsvaret etter dagens risiko og trusler, samt evnen til å komme seg tilbake i normal drift, så fort som mulig, etter en cyber-hendelse. Det viktigste her er barrieretankegang og å følge det gamle speidermotto om å være beredt. Gode beredskapsplaner, testing, trening og øvelser på ulike scenarier er viktige ingredienser for å sikre cyber-resiliens.

Like viktig er det å følge med på endringer i risikobildet i form av nye trusler og sårbarheter. Arbeidet med cyber-resiliens blir aldri ferdig. Her, som mange steder ellers, gjelder kontinuerlig forbedring.

Digitalisering og ny teknologi skaper nye muligheter, men kan også føre til nye sårbarheter. Hvis man for eksempel ønsker å eksportere måledata fra produksjonen og foreta beregninger i skyen, for så å sende resultatet tilbake for å endre parametere for optimalisering av produksjonen, er det en utfordring å gjøre dette på en sikker måte. Denne problematikken kunne vært gjenstand for en egen studie.

Blokkjede bidrar til sikkerhet og resiliens i form av at denne teknologien sikrer sporbarhet av data og transaksjoner og er «tamper-proof», dvs. man kan stole på det som er lagret. Imidlertid er man ikke garantert 100 % sikkerhet, da fortsatt noen av de vanlige sårbarhetene (for eksempel svake passord) ligger i «endene» av blokkjeden.

Blokkjede har noen anvendelsesområder som den er godt skikket for. Det synes å være særlig to generiske tilfeller hvor blokkjedeteknologien vil kunne bidra i positiv retning, både når det gjelder effektivisering og resiliens: 1) effektivisere og øke sikkerheten i eksisterende prosesser mellom aktører der det ikke er en sentral motpart, for eksempel styring av leveransekjeder og 2) bidra til helt nye måter å gjøre ting på, for eksempel smarte kontrakter.

På den annen side er ikke blokkjede løsningen på «alt». Det er stort behov for lagringsplass og kommunikasjon mellom noder. Noen løsninger har stort energibehov. Skalering er en utfordring. I tillegg er blokkjede foreløpig en umoden teknologi og det er usikkert hvilke typer blokkjeder som vil bli foretrukket og markedsledende. Det er mye «hype» og store forventninger. Mange ser store potensialer for å få innpass i et nytt marked, enten det gjelder software, rådgivning eller for den saks skyld hardware og infrastruktur. Et sitat fra et intervju:

> *«Mye rundt blokkjeder er i dag en kombinasjon av hype og pyramidespill»*

Noen av de eksemplene vi har sett på mulig bruk av blokkjede kan i dag enklere og på en nesten like sikker måte, implementeres ved hjelp av vanlige, sentrale databaser. Dette gjelder særlig der det er høye krav til rask prosessering. På den annen side er teknologien i rivende utvikling, så en sannhet i dag er ikke nødvendigvis en sannhet i morgen.

Nedenfor gis noen anbefalinger om resiliens og blokkjede. Det må påpekes at det er vanskelig å gi gode råd om blokkjede, da denne teknologien ennå er ny og umoden. Vi har likevel dristet oss til å gi noen få overordnede anbefalinger.

Tabell 6-1 – Anbefalinger

Nr.	Anbefaling	Referanse til kapitler
	Resiliens	
1.	**Deling av kunnskap og erfaring.** Med godt samarbeid gjennom delingsforum/allianser/responsmiljøer kan aktører dele erfaringer og lære av hverandres sårbarheter slik at de lettere kan identifisere trusler og håndtere risiko. Det vil igjen føre til at det blir vanskelig for kriminelle å gjøre «samme angrep» mange steder.	Se kapittel 4.3.1 Identifisering og kartlegging (Identify)
2.	Regelmessige **risikoanalyser**. Man må til enhver tid kjenne risikobildet. Tydelig definerte barrierer er viktige med tanke på å minske sannsynligheten for, eller mildne konsekvensen av cyberhendelser.	Se kapittel 4.3.1 Identifisering og kartlegging (Identify) og 4.3.2 Beskytte (Protect)
3.	**Vær beredt**. Selv om man tror man har sikret seg 100 % mot at en cyberhendelse skal kunne inntreffe, må man likevel være forberedt på at det vil kunne skje. Det er like viktig å være forberedt på recovery som å forhindre at en hendelse inntreffer.	Se kapittel 4.3.3 Oppdage (Detect) og Opprettholde, og kapittel 4.3.4 Håndtere (respond) og gjenopprette (recover)
4.	Ikke glem det **menneskelige** aspektet. Mange omtaler mennesker eller personell som det svakeste leddet fordi det er mennesker som lar seg lure. Cyber bevisstgjøringstrening er viktig.	Se kapittel 4.3.4 Håndtere (respond) og gjenopprette (recover)
5.	Gode **beredskapsplaner**, **trening** og **øvelser** er viktig. Dette kan gjøres for å trene enkeltpersoner, organisasjonen, eller for å øve på teknikk, f.eks. restore av en database.	Se kapittel 4.3.4 Håndtere (respond) og gjenopprette (recover)
6.	Arbeidet med cyber-resiliens blir **aldri ferdig**. Kontinuerlig forbedring krever innsats.	Se kapittel 4.3.5 Kontinuerlig forbedring
	Blokkjede	
7.	La **problemet man ønsker å løse** være utslagsgivende for om man skal velge blokkjedeløsning eller en annen løsning. Man må ikke implementere «alt» ved hjelp av blokkjede, selv om dette er en teknologi som er i vinden.	Se kapittel 5.2 "To blockchain or not to blockchain – that's the question"
8.	Blokkjede **sikrer integritet av data** og transaksjoner (den digitale eiendel), men ikke glem å verifisere (eller få verifisert) den fysiske realiteten bak de data som er registrert.	Se kapittel 5.4.1 om Datakvalitet og kapittel 5.6.4 Sikring og garanti av opprinnelse
9.	Ikke glem de **vanlige sårbarhetene** som ligger i endepunktene av en blokkjede. Disse må sikres på en hensiktsmessig måte.	Se kapittel 5.4 Blokkjede-sårbarheter og spesielt om De vanlige sårbarhetene gjelder også her

Nr.	Anbefaling	Referanse til kapitler
10.	Ved implementering av **smarte kontrakter** er verifikasjon og validering av programvaren som inngår alfa og omega.	Se kapittel 5.6.7 Smarte kontrakter
11.	Vær forberedt på at det første blokkjede-prosjektet ikke nødvendigvis blir 100 % vellykket. **Start i det små**, med enkle problemstillinger og vær forberedt på at teknikken er umoden og at type blokkjedeteknologi kanskje må skiftes ut.	Se kapittel 5.4.2 Manglende standardisering og regelverk, og kapittel 5.6 Eksempler på mulige bruksområder
12.	**Optimalisering av produksjon.** Hvis man ønsker å eksportere måledata fra produksjonen og foreta beregninger i skyen, for så å sende resultatet tilbake for å endre parametere for optimalisering av produksjonen, er det en utfordring å gjøre dette på en sikker måte. Denne problematikken kunne vært gjenstand for en egen studie. (Vi har i denne rapporten diskutert dette som en mulig anvendelse av blokkjede, men det behøver ikke bli løst på den måten.)	Se kapittel 5.6.3, Sikring av informasjonskjede for prosessoptimalisering, og kapittel 5.6.8, Sammenligning av de ulike bruksområdene

7 REFERANSER

/1/ Norsk Olje & Gass: Sorte Svaner – Et utvidet perspektiv på risiko
https://www.norskoljeoggass.no/drift/storulykkerisiko/sorte-svaner--et-utvidet-perspektiv-pa-risiko/

/2/ NIST: Framework for Improving Critical Infrastructure Cybersecurity
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

/3/ FFI-Rapport 19/00363: Brynhild Stavland, Janita Andreassen Bruvoll,
Resiliens – hva er det og hvordan kan det integreres i risikostyring?, Mars 2019
https://www.ffi.no/no/Rapporter/19-00363.pdf

/4/ NKOM: EkomROS 2019: Den digitale grunnmuren
https://www.nkom.no/aktuelt/nyheter/_attachment/42430?_ts=16b4a976ad8

/5/ NSM: Risiko 2019 – Krafttak for et sikrere Norge
https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

/6/ IATA: Blockchain In Aviation - Exploring the Fundamentals, Use Cases, And Industry Initiatives. White Paper, October 2018
https://www.iata.org/publications/Documents/blockchain-in-aviation-white-paper.pdf

/7/ NSM: NSMs Grunnprinsipper for IKT-sikkerhet, versjon 1.1, november 2018
https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

/8/ Deloitte: Distribuert sannhet – Potensial og barrierer for blokkjeder i norsk offentlig sektor, mars 2018
https://www.regjeringen.no/contentassets/f5db1086d5324ec786f440afcb5cde52/blokkjeder_offentlig_sektor_deloitte.pdf

/9/ Louise Hagström, Olivia Dahlquist, Scaling blockchain for the energy sector, Masteroppgave fra Uppsala Universitet, Juni 2017
https://uu.diva-portal.org/smash/get/diva2:1118117/FULLTEXT01.pdf

/10/ Nassim Nicholas Taleb, Antifragile. Things that gain from disorder, Penguin, 2013

/11/ Wüst, Gervais (2017), Do you need a blockchain?
https://eprint.iacr.org/2017/375.pdf

/12/ ThoughtWorks, Vakt, From PoC to Production: Implementing an enterprise blockchain solution, 2019
https://www.vakt.com/wp-content/uploads/2019/07/VAKT-TW-POC-TO-PRODUCTION.pdf

/13/ DNV GL, Blockchain i kraftsystemet, Teknologianalyse for Statnett, Rapportnr.: 2018-0577, rev. 2, 31.5.2018
http://195.18.187.202/Global/FoU/Blockchain%20i%20kraftsystemet.pdf

/14/ DNV GL, DNVGL-RP-0496 - CS resilience management or ships and mobile offshore units in operation, rev September 2019
https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

/15/ DNV GL, DNVGL-RP-G108 Cyber security in the oil and gas industry based on IEC 62443, rev September 2017
http://rules.dnvgl.com/docs/pdf/DNVGL/RP/2017-09/DNVGL-RP-G108.pdf

/16/ Norsk Olje og Gass, 104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems, Rev 6, 2016-12-05

/17/ DNV GL, Industriell IKT og IioT, Infrastruktur innen industrielle kontroll- og sikkerhetssystemer, Rapportnr.: CyberSecurity/J-24/25154785/DNV, Rev. 1, 2019-06-21

/18/ NorSIS, Nordmenn og Digital Sikkerhetskultur 2018, publisert 5.november 2018

/19/ Government Blockchain Association (GBA) Cyber Security Working Group, Assessment and Authorisation of Blockchain Systems, 2018,
https://www.gbaglobal.org/resources/listing/assessment-and-authorization-of-blockchain-systems

/20/ Sintef: Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhets- systemer i petroleumsvirksomheten, 2018-05-29
https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf

/21/ NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, rev. 1, May 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

/22/ NSM, Rammeverk for håndtering av IKT-sikkerhetshendelser, 7.12.2017
https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

/23/ Into the web of profit – understanding the growth of the cybercrime economy by Dr. Michael McGuire, April 2018
https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

/24/ NVE Rapport 2015/39, Øvelser -
En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen
http://publikasjoner.nve.no/rapport/2015/rapport2015_39.pdf

/25/ Energy Web Foundation, The Energy Web Chain, Version 2.0, July 2019
https://www.energyweb.org/wp-content/uploads/2019/05/EWF-Paper-TheEnergyWebChain-v2-201907-FINAL.pdf

https://energyweb.atlassian.net/wiki/spaces/EWF/pages/717881446/Proof+of+Authority+Consensus

/26/ DNV GL rapport 2019-0823, Trening og øvelse

/27/ DNV GL rapport 2019-0824, Regelverk og tilsynsmetodikk

/28/ Chamber of Digital Commerce / Microsoft, Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry
https://digitalchamber.org/microsoft-whitepaper/

Om DNV GL

DNV GL er et internasjonalt selskap innen kvalitetssikring og risikohåndtering. Siden 1864 har vårt formål vært å sikre liv, verdier og miljøet. Vi bistår våre kunder med å forbedre deres virksomhet på en sikker og bærekraftig måte.

Vi leverer klassifisering, sertifisering, teknisk risiko- og pålitelighetsanalyse sammen med programvare, datahåndtering og uavhengig ekspertrådgivning til maritim sektor, til olje- og gass-sektoren, og til energibedrifter. Med 80,000 bedriftskunder på tvers av alle industrisektorer er vi også verdensledende innen sertifisering av ledelsessystemer.

Med høyt utdannede ansatte i 100 land, jobber vi sammen med våre kunder om å gjøre verden sikrere, smartere og grønnere.