CYBERSIKKERHED

I FORBINDELSE MED TEKNISKE INSTALLATIONER OG INDUSTRIPRODUKTER

Januar 2020

TEKNIQ ARBEJDSGIVERNE

Indhold

Forord

Rammevilkårene for installations- og industribranchen gennemgår i disse år voldsomme forandringer, der er foranlediget af blandt andet den teknologiske udvikling, ændret kundeadfærd samt forandrede samfundsmæssige rammevilkår og forventninger. Disse ændringer er fra TEKNIQ Arbejdsgiverne tidligere blevet belyst i forhold til installationsbranchen i rapporterne "Nye muligheder i installationsbranchen" og "Elbranchens Vision 2025".

En stor del af den udvikling, der sker i branchen, er drevet af en stadig accelererende teknologisk udvikling, som har intelligente løsninger og digitalisering som omdrejningspunkt.

Installationsbranchen har længe anvendt digitale løsninger, men i forhold til tidligere bliver løsningerne i dag baseret på standardteknologier og koblet til internettet. Denne udvikling giver slutbrugerne en lang række nye muligheder for blandt andet bedre brugervenlighed, højere komfort og økonomiske gevinster ved billigere og mere effektive løsninger. For de professionelle slutbrugere giver udviklingen mulighed for en mere effektiv produktion, højere effektivitet og en bedre kundeservice.

På industriområdet har man ligeledes længe anvendt forskellige former for automationsløsninger i produktionen, og også her bliver løsninger i dag digitaliseret og koblet sammen med andre it-systemer i virksomheden til bl.a. optimering, planlægning og styring af produktionen. De traditionelle automationsløsninger bliver desuden suppleret med en lang række nye avancerede teknologier, bl.a. robotter og kunstig intelligens ofte understøttet af big data, augmented reality (AR) og cloud-løsninger. Ofte betegnes denne udvikling også som Industri 4.0, som er en samlet betegnelse for integrationen mellem digitale løsninger og fysisk produktion i intelligente, sammenhængende netværk, der kan kontrollere udstyr og elementer i hele den industrielle værdikæde.

Udviklingen i installations- og industribranchen er identisk med den udvikling, som ses ved digitalisering i det øvrige samfund, men rammer langt bredere end når digitalisering normalt behandles. Den stigende digitalisering har nemlig en bagside i form af en større potentiel eksponering for forskellige former for cyberangreb, der kan medføre forstyrrelser, nedbrud eller tab af data eller kontrol. Installations- og industribranchen er i den forbindelse i en særlig situation, da en lang række af de digitale løsninger, der arbejdes med, også har en forbindelse til den fysiske verden. Derved vil et cyberangreb potentielt kunne have omfattende konsekvenser og forårsage uheld og skader i den fysiske verden i form af voldsomme materielle skader, personskade eller i yderste konsekvens dødsfald.

Mange intelligente og digitale løsninger er baseret på sensorer, der løbende foretager dataopsamling fra omgivelserne bl.a. om folks handlinger og dermed potentielt opsamler data om personlig adfærd og rutiner. Denne form for oplysninger er ofte personoplysninger. Det betyder, at behandlingen skal ske med passende sikkerhed, ligesom evt. brud på sikkerheden omkring persondata vil være omfattet af EU's persondataforordning (GDPR).

Denne rapport sætter fokus på de særlige udfordringer, den teknologiske udvikling medfører i forhold til cybersikkerhed, og hvilke udfordringer og muligheder dette giver for installations- og industribranchen.

Kort om analysen

For at afdække udfordringer og muligheder i forbindelse med intelligente og opkoblede produkter har TEKNIQ Arbejdsgiverne bedt it-sikkerhedsspecialister fra Dubex om at udarbejde en rapport, der beskriver den aktuelle bevidsthed i branchen og gennemgår de cybersikkerhedsmæssige konsekvenser og udfordringer ved brugen af de nye teknologier.

I forlængelse af undersøgelsen er Dubex blevet bedt om at komme med konkrete anvisninger og anbefalinger til, hvordan medlemmerne og branchen kan arbejde med cybersikkerhed fremadrettet, samt belyse de forretningsmæssige muligheder det giver.

Formålet med analysen er at skabe et overblik over området, der kan fungere som udgangspunkt for TEKNIQ Arbejdsgivernes videre arbejde omkring cybersikkerhed. Analysen omfatter derfor de områder, som medlemmerne af TEKNIQ Arbejdsgiverne generelt arbejder med, herunder både el og vvs, samt industriautomatiseringsløsninger.

Alle vurderinger og anbefalinger i denne rapport er baseret på Dubex' analysearbejde, der inkluderer et baggrundsstudie, workshops med en række repræsentanter blandt TEKNIQ Arbejdsgivernes medlemmer og samarbejdspartnere, samt dialog med TEKNIQ Arbejdsgiverne. Der er ikke gennemført tekniske undersøgelser.

Kombinationen af baggrundsstudiet og de enkelte workshops har gjort det muligt for Dubex at sammenholde de generelle udfordringer i branchen med de observationer, som repræsentanterne bidrog med. Derudover har Dubex været i tæt dialog med TEKNIQ Arbejdsgiverne for at sikre, at al viden med relevans for analysen, herunder relevante standarder og kendskab til medlemmernes arbejde, blev afdækket.

Formålet med rapporten

Dubex er blevet bedt om at

- Afdække udviklingen på området for digitale løsninger
- Afdække og synliggøre de cybersikkerhedsmæssige konsekvenser og udfordringer ved digitale løsninger
- Afdække forretningsmæssige muligheder ved digitale løsninger
- Afdække den aktuelle tilgang til cybersikkerhed i installations- og industribranchen

Med afsæt i dette samler Dubex en række anbefalinger til branchens arbejde med cybersikkerhed samt vurderer ansvarsfordelingen i forhold til cybersikkerhed mellem de enkelte installatører, der etablerer de digitale og intelligente løsninger, og f.eks. it-branchen og slutkunderne.

Ledelsesresumé

Installationsbranchen og industrien rammes i disse år af en omfattende digitalisering, der teknologisk rammer alt lige fra de produkter og enheder, der anvendes, og den måde installationer skal udføres på, til den måde der kommunikeres med kunder og samarbejdspartnere.

Digitaliseringen er et naturligt resultat af den hastige teknologiske udvikling, der blandt andet gør det muligt at automatisere og effektivisere processer, som før var manuelle og tidskrævende. Den digitalisering, der ses i installationsbranchen og industrien, er parallel med det, som opleves i det øvrige samfund, og medfører på samme måde forandringer af forretnings- og samarbejdsmodeller. Digitaliseringen har imidlertid også medført en voldsom vækst i antallet og omfanget af cyberangreb.

De digitaliserede løsninger bliver mere kritiske for os, når de udfører væsentlige opgaver og indeholder værdifulde informationer. Dette gør dem til værdifulde mål for cyberkriminelle og efterretningstjenester, der kan kaste mange ressourcer i at gennemføre angreb. Og den stigende digitalisering medfører en øget eksponering i forhold til cyberangreb.

Indenfor installationsbranchen og industrien betyder digitaliseringen, at enheder, der før var isoleret og betjent lokalt, nu er baseret på it-systemer og ofte kan tilgås via internettet. I takt med, at flere og flere systemer integreres og forbindes på kryds og tværs, bliver it-miljøet mere komplekst. Samtidig bliver eksponeringen større, fordi enheder, der før var isoleret til ét område, nu berører flere områder og dermed kan "overføre" sårbarheder fra ét område til et andet. Enhederne har ofte en meget lang levetid og derfor kobles gammelt udstyr med gammel teknologi og mangel på basale sikkerhedsfunktioner sammen med nye digitale løsninger.

I takt med at enheder, der er koblet til internettet, styrer fysiske enheder, bliver der risiko for, at hændelser i det digitale domæne kan medføre omfattende fysiske ødelæggelser og i værste fald tab af menneskeliv.

En forudsætning for udbredelsen af digitale løsninger er tillid til, at de fungerer, og at de data, de opbevarer og behandler, er troværdige. Cyber- og informationssikkerhed er derfor en absolut nødvendighed, hvis digitaliseringen skal blive en succes.

I forbindelse med den foreliggende analyse har Dubex observeret, at der indenfor installations- og industribranchen er en udbredt manglende bevidsthed i forhold til cyber- og informationssikkerhed. Dette skyldes bl.a., at tekniske løsninger ikke betragtes som it-systemer, der kan være sårbare, og at sikkerhed ikke altid tænkes ordentlig ind fra starten. Generelt er awareness og erkendelse omkring cybersikkerhed blevet bedre, men da der kun har været få kendte hændelser, har området ikke fået meget opmærksomhed.

Slutbrugernes bevidsthed og dermed interesse i cybersikkerhed er stadig begrænset, og blandt andet derfor bliver cybersikkerhed ikke opfattet som kommercielt interessant. Området har derfor ikke den store interesse for installatørerne, og kun ganske få installatører arbejder systematisk med cybersikkerhed, herunder prøver at bruge cybersikkerhed som forretningsenabler. Installatørerne mener således, at cybersikkerhed er kundens ansvar.

Rent kommercielt bliver stadig mere avancerede løsninger solgt som almindelige forbrugerprodukter. Det betyder, at installatørernes løsningssalg bliver udfordret af simple kommercielle løsninger, som slutbrugeren selv kan konfigurere. Det vurderes, at producenterne på sigt vil gå mere direkte til slutkunderne. Hvis installatørerne fremadrettet skal sælge avancerede løsninger, kræves således et salgsmæssigt fokus på løsningssalg fra installatørerne – kunderne køber ikke løsningerne af sig selv.

En anden observation er, at ansvaret for cybersikkerhed ikke er klart placeret. Slutkunden er ansvarlig i sidste ende, men er ofte uvidende og har ikke erkendt opgaverne og ansvaret. I forlængelse heraf er der observeret en stor forskel på modenhed hos henholdsvis professionelle slutkunder eller privatpersoner. Tilgangen fra mange installatører er at betragte alt, der har med it at gøre, som kundens ansvar, men der er samtidig nogen bekymring blandt installatørerne i forhold til, om de kan ifalde erstatningsansvar for manglende cybersikkerhed. Blandt producenterne er der stor forskel på fokus i forhold til cybersikkerhed i deres produkter, men de større og seriøse producenter virker alle til at tage området seriøst.

En sidste observation er, at der mangler cybersikkerhedskompetencer hos medarbejderne. It- og cybersikkerhed er ikke et element på grunduddannelserne, og uddannelse er en omkostning, der kan være svær at forsvare, når der ikke er et klart udbytte. Det er vigtigt at understrege, at der er en udfordring med både tekniske og kommercielle kompetencer indenfor cybersikkerhed.

Indenfor industrien er der en række særlige forhold i forbindelse med automatisering af produktionen, blandt andet er der ofte manglende vidensudveksling med den normale it-organisation, ligesom der ofte mangler indsigt og kompetencer i forhold til cybersikkerhed. Indenfor industrien prioriteters tilgængelighed og oppetid højt, hvorfor stabilitet vægtes højt. Dette fungerer dårligt i forhold til opretholdelse af cybersikkerhed, hvor opdatering af software er væsentlig – særligt med det stigende fokus på OT/ICS-sikkerhed, der medfører, at der bliver fundet mange flere sårbarheder i de anvendte enheder og løsninger. Endelig findes der mange løsninger, som ikke er designet og implementeret med fokus på sikkerhed, ligesom basale processer i forhold til sikkerhedsovervågning og beredskab ofte ikke er på plads.

På baggrund af den gennemførte analyse har Dubex en række anbefalinger, som efter Dubex' opfattelse kan medvirke til at sætte det nødvendige fokus på cybersikkerhed – og i øvrigt medvirke til udvikle branchen og skabe en række nye forretningsmuligheder:

- Det er nødvendigt at erkende, at cyber- og informationssikkerhed er en væsentlig forudsætning for digitaliseringen, hvis de digitale løsninger skal være robuste og troværdige. Det kræver, at aktører i branchen søger indsigt i cybersikkerhedsområdet og forstår problemstillingerne.

- De generelle digitale kompetencer skal underbygges med cyber- og informationssikkerhedskompetencer, hvilket kræver et generelt kompetenceløft og fokus på uddannelse og efteruddannelse af medarbejdere. Uddannelsen skal omfatte både tekniske og kommercielle kompetencer, ligesom virksomhederne bør overveje ansættelse af andre typer medarbejdere med relevante kompetencer, der kan medvirke til en højere værdiskabelse.

- Det er vigtigt at erkende, at opgaven og ansvaret for cybersikkerhed skal løftes i et samarbejde mellem alle interessenter – og at cybersikkerhed skal være en del af den samlede livscyklus for løsningerne. Det kræver, at installationsvirksomhederne identificerer, hvor de arbejder med cybersikkerhed, og sikrer at dette sker på en passende måde. Dette omfatter blandt andet, at de samarbejder med leverandørerne om sikre produkter og har en dialog med slutkunderne omkring cybersikkerhed. Det er vigtigt, at installatørerne er tydelige i deres kommunikation med slutkunderne, så slutkunderne forstår den løsning, de har fået overdraget.

- Digitalisering og cybersikkerhed giver mulighed for nye eller ændrede forretningsmodeller, da cybersikkerhed blandt andet kræver vedligeholdelse. Det medfører en mulighed for etablering af en serviceforretning. Det anbefales, at installatørerne overvejer, hvordan der kan udvikles nye forretningsmodeller, evt. i et tættere samarbejde med producenter og distributører, med henblik på at kunne markedsføre og sælge de mere avancerede og værdiskabende samlede digitale løsninger

- Indenfor industrien anbefales det at gennemgå organisationen og identificere brugen af OT/ICS-løsninger og de personer, der har ansvaret for disse. På baggrund af dette skal der udarbejdes en plan for risikovurdering af ICS/OT-anvendelsen. Desuden er det vigtigt at etablere de organisatoriske og proceduremæssige rammer til håndtering af de identificerede risici og korrigerende handlinger samt de nødvendige cybersikkerhedskontroller. Endelig er det vigtigt, at der etableres et samarbejde mellem IT- og OT-området.

Hvorfor er cybersikkerhed vigtigt?

Produkter og løsninger inden for el, vvs og industriautomatisering bliver i stigende grad digitalt intelligente og opkoblede.

Digitalisering er en naturlig udvikling, som også ses i alle andre brancher og samfundet generelt. Men det er ikke uden udfordringer. Udviklingen betyder nemlig, at produkter og løsninger, som f.eks. bygningsinstallationer, der tidligere var mekanisk og elektroteknisk simple og kun kunne betjenes lokalt, nu er baseret på it-systemer og er koblet op til internettet. Dermed kommer de i berøring med et større og for mange ukendt område i form af det offentlige internet.

Det er i grænsefladen mellem den fysiske verden og de digitale løsninger, at særlige udfordringer opstår, når sikkerhed i den fysiske verden bliver afhængig af sikkerheden i digitale løsninger. Ofte sker denne ændring ubevidst og uden egentlig opmærksomhed og er derfor sjældent ordentlig gennemtænkt.

I traditionelle installationer har man normalt haft mulighed for at teste sikkerhed i løsningen, og derefter ville løsningen have de samme sikkerhedsegenskaber i al fremtid.

Det samme er ikke tilfældet med de intelligente og digitalt opkoblede løsninger, der – ligesom alle andre former for forbundet it-udstyr – er eksponeret for en række trusler i form af f.eks. hacking, malware, ransomware, botnets, overbelastningsangreb (Denial-of-Service) og kompromittering af information (se oversigt over cyberangreb). Ofte benyttes alment tilgængelige standardkomponenter og software, hvor dokumentation er frit tilgængelig.

En særlig udfordring er således software og softwarekomponenter, som på udviklings- og testtidspunktet betragtes og fastslås til at være sikre og leverer den ønskede funktionalitet og sikkerhed, men hvor der på et senere tidspunkt konstateres sårbarheder, der kan misbruges. Da denne information ofte distribueres og er frit tilgængelig – eller kan være fundet i en udbredt standardkomponent, som løsningen anvender – betyder det, at produktet eller løsningen pludselig kan blive potentielt sårbar. Det gør også, at løsningerne kan blive angrebet af ondsindede eksterne aktører, der har et specifikt kendskab til, hvordan den pågældende løsning eller produkt kan kompromitteres.

Cyberangreb i Danmark?!

Cyberbegrebet fylder mere og mere i mediebilledet, men er det overhovedet relevant i et dansk perspektiv?

Svaret er ja.

Ifølge den seneste trusselsvurdering fra Center for Cybersikkerhed[1] (CFCS) er truslen fra cyberspionage og cyberkriminalitet mod danske virksomheder, myndigheder og borgere angivet som "Meget høj". Det betyder, at der er en specifik trussel, og at et angreb eller skadevoldende aktivitet er meget sandsynlig.

I trusselsvurderingen fremgår det, at Internet of Things (IoT)-enheder i dag er blandt den type af enheder, der bliver udsat for flest cyberangreb, og udviklingen indenfor IoT betyder, at hackernes angrebsflade udvides. I takt med at enheder, der er koblet til internettet, styrer fysiske enheder, øges risikoen desuden for, at et cyberangreb kan medføre fysiske ødelæggelser. IoT-begrebet uddybes i afsnittet "Hvad er Internet of Things?".

PwC's Cybercrime Survey 2018[2] viser, at 44 % af de danske virksomheder i undersøgelsen i 2018 har været udsat for en sikkerhedshændelse. Undersøgelsen viser samtidig, at 49 % har haft øgede udgifter til udbedring og efterforskning af sikkerhedshændelser i forhold til 2017.

1 https://fe-ddis.dk/cfcs/nyheder/arkiv/2019/Pages/Cybertruslen-2019.aspx

2 https://www.pwc.dk/da/publikationer/2018/cybercrime-survey-2018.pdf

Et af de mest omtalte eksempler er det omfattende angreb, der ramte A.P. Møller – Mærsk i 2017[3]. Angrebet var formentlig et russisk destruktivt cyberangreb oprindelig målrettet virksomheder i Ukraine, men det kom ud af kontrol og blev spredt til flere lande og ramte en bred vifte af virksomheder verden over[4]. Hos Mærsk gik skærmene i sort, og for at forhindre virussen i at sprede sig yderligere, blev it-systemerne lukket ned[5]. Det resulterede i, at flere containerhavne effektivt blev lukket, og at kunderne ikke vidste, hvor deres forsendelser var. Det tog 10 dage at reinstallere hele it-infrastrukturen, og omkostningerne er estimeret til at være i størrelsesorden 1,3-1,9 milliarder danske kroner[6]. Selve angrebet var kamufleret som et ransomware-angreb, så det så ud som om, at kriminelle stod bag, men det var i virkeligheden en del af et cyberangreb på Ukraine, hvor Mærsk blev tilfældigt ramt.

Et vigtigt element i beskyttelsen mod disse angreb er viden om cybertruslen, herunder hvem angriberne er, hvilke motiver de har, og hvilke metoder de bruger. Med denne viden er det nemlig muligt at tage en række forholdsregler.

3 https://www.maersk.com/news/2017/10/09/maersk-line-high-tea

4 https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/

5 http://investor.maersk.com/da/news-releases/news-release-details/cyber-attack-update

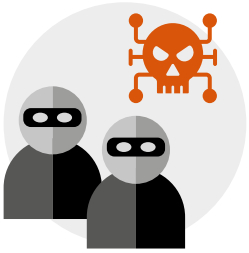
6 https://www.version2.dk/artikel/notpetya-cyberangreb-koster-maersk-milliardbeloeb-1079124

Cyberangreb – hvordan?

Gennemførelsen af et cyberangreb kræver, at tre faktorer er tilstede: Angriber, metode og mulighed.

På nuværende tidspunkt vurderes de væsentligste angrebsaktører at være:

- Cyberkriminelle
- Stater
- Aktivister
- Terrorister
- Insidere



På overordnet plan kan man sige, at angribernes motiver varierer fra økonomisk vinding til spionage, terror og bevidst ødelæggelse af andres ejendom/forretning.

Selvom nogle angrebsaktører er mere motiveret af f.eks. spionage, er der ikke en entydig sammenhæng mellem motiverne og bestemte typer af angribere.

Cyberangreb kan være målrettede og tilfældige. I langt de fleste tilfælde er der tale om tilfældige angreb, hvor bagmændene udnytter en sårbarhed til at skyde med sprede-hagl, f.eks. i håbet om at gøre mest mulig skade eller at ofrene betaler en løsesum. I andre tilfælde kompromitterer en hacker en enhed og bruger den som springbræt til at komme videre ind i et netværk og få adgang til systemer og data.

Eksempler på forskellige typer af cyberangreb med små forklaringer

Botnet
En bot er en fjernstyret software-robot, der automatisk kan afvikle scripts på internettet. En bot er typisk en enhed, der er blevet hacket og har fået installeret noget malware. Et botnet består af mange internetforbundne enheder, som er knyttet sammen og fjernstyres fra den samme command and control-server. Botnets bruges ofte til at afvikle DoS og DDoS-angreb (overbelastningsangreb), udsende spammail og søge efter sårbare enheder. Det er også muligt for en hacker at udnytte en bot til at få adgang til en enhed, eller det netværksenheden er forbundet til, og stjæle data.

DoS og DDoS-angreb
Et Denial of Service (DoS)-angreb er et angreb, der gør en service utilgængelig ved f.eks. at "oversvømme" et netværk med trafik, så netværket bryder sammen. Ved et Distributed Denial of Service (DDoS)-angreb kommer trafikken fra flere kilder, typisk kompromitterede maskiner spredt på internettet (botnets), hvilket gør det vanskeligt at blokere.

Malware
Malware står for "malicious software" og er en betegnelse for ondsindet programkode, der gør skadelige eller uønskede ting.

Phishing
Phishing er en metode, hvor hackeren forsøger at "fiske" oplysninger ved at snyde modtageren af en e-mail til at indtaste brugernavn og kodeord, trykke på et link eller downloade en fil, der indeholder skadelig kode (malware).

Ransomware
Ransomware er en type malware, der krypterer den inficerede enhed og/eller data. I forbindelse med krypteringen fremsættes typisk et krav om en løsesum, før adgangen til data (måske) genetableres.

Man-in-the-Middle-angreb
Et angreb, hvor angriberen sætter sig imellem to kommunikerende enheder som et usynligt mellem-/bindeled. Giver mulighed for at "lytte med" og manipulere på kommunikationen og opsnappe f.eks. passwords, kreditkortinformationer eller andre oplysninger, samt manipulere i det som transmitteres.

Case

Target

Den amerikanske butikskæde Target blev i 2013 udsat for et cyberangreb, hvor det viste sig, at hackernes indfaldsvinkel var en ekstern tredjepartsleverandør til Targets HVAC-anlæg. Tredjepartsfirmaet havde fjernadgang til Targets netværk, som herefter blev overtaget og misbrugt af hackere. Hackerne misbrugte herefter HVAC-anlægget som springbræt til at tilgå det netværk, der anvendes af kassesystemerne. Hackerne var således i stand til at udnytte HVAC-virksomhedens eksterne adgang til at angribe Targets betalingssystemnetværk. Her installerede de malware, der stjal kreditkortoplysninger. Hændelsen kostede både Targets sikkerhedsansvarlige og den administrerende direktør jobbet.

Hvad er trusler, sårbarheder og risiko?

Indenfor cybersikkerhed er en **sårbarhed** (engelsk: vulnerability) en svaghed eller fejl, som kan udnyttes af en trusselsaktør, såsom en cyberkriminel eller ondsindet hacker, til at udføre uautoriserede handlinger i et computersystem.

For at **udnytte** en sårbarhed skal en hacker have mindst ét relevant værktøj eller teknik (engelsk: exploit), der kan udnytte sårbarheden. Dette kaldes også en trussel. De potentielle sårbarheder, som en angriber eller en trussel kan nå, kaldes **angrebsoverfladen**.

En sårbarhed med et eller flere kendte og fuldt implementerede angrebsmetoder klassificeres som en **udnyttelig sårbarhed** (engelsk: exploitable vulnerability). **Sårbarhedsvinduet** (engelsk: window of vulnerability) er den periode, der går fra sikkerhedshullet bliver introduceret til tidspunktet, hvor muligheden for udnyttelse er fjernet – enten med implementering af en sikkerhedsrettelse eller anden form for blokering af mulige angreb. Sårbarheder, som bliver udnyttet før en producent bliver opmærksom på dem, og som det derfor ikke er muligt at lukke via en opdatering, kaldes **dag-0 sårbarheder** (engelsk: zeroday vulnabilities).

Sårbarhedsstyring er den systematiske og gentagne proces med at identificere, klassificere, udbedre og afbøde sårbarheder i computersystemer og henviser generelt til softwaresårbarheder, men kan godt være mere bredt.

Når en trussel udnytter en sårbarhed, medfører det en **hændelse** (engelsk: incident). En hændelse kan have nogle **konsekvenser**, der kan være mere eller mindre kritiske alt efter, hvor alvorlig hændelsen er.

Risikoen er udtryk for konsekvenserne ved en hændelse set i forhold til sandsynligheden for, at hændelsen indtræffer.

Risikovurdering er den systematiske proces, hvor man identificerer organisationens aktiver, dvs. alle de kritiske informationer og processer, og vurderer risikoen i forhold til dem. Risikovurderingen er et nødvendigt værktøj for at sikre et overblik over, hvor risikoen er størst, så sikkerhedsforanstaltningerne kan prioriteres og gennemføres, hvor de har den største værdi.

Andre gange udnytter hackeren en kompromitteret enhed, i kombination med andre kompromitterede enheder, til at lave et overbelastningsangreb (Distributed Denial of Service) mod f.eks. en hjemmeside. I nogle tilfælde kan angrebet være så omfattende, at det skader den angrebne enhed så meget, at den skal udskiftes eller geninstalleres for at komme i drift igen.

Trusselsbilledet er i konstant udvikling, hvilket skyldes, at angriberne hele tiden udvikler deres evner og kompetencer, blandt andet gennem en øget udveksling af viden og værktøjer. Det betyder, at avancerede metoder, der tidligere var forbeholdt statsaktører, nu også bruges af cyberkriminelle og terrorister. Derudover stiller cyberkriminelle ofte deres værktøjer til rådighed eller salg online, så aktører uden særlige kompetencer til cyberangreb nemt kan bestille relativt avancerede angreb via internettet.

Ændringerne i trusselsbilledet sker typisk evolutionært og ikke revolutionært. Det betyder, at man med passende opmærksomhed som regel vil kunne forberede sig på potentielt kommende trusler. Derfor er det også vigtigt at vide, hvilke sårbarheder der gør det muligt for en angriber at gennemføre et angreb.

Her er det især vigtigt at vide, at installatøren og hans medarbejdere selv spiller en rolle. For hvis en intelligent enhed ikke tilkobles og konfigureres korrekt, kan det resultere i f.eks. datalækager eller datatab, uautoriseret modificering af enheden eller kompromittering af det netværk, som enheden er koblet til. Dermed er vejen banet for et muligt angreb.

Konsekvenser ved angreb

Konsekvenserne ved et angreb kan være mange og af både individuel og samfundsmæssig karakter. For eksempel vil en hacker, der overtager en installation eller et HVAC-system i en bolig med Smart Home-installation, en bygning med bygningsautomatik eller en industrivirksomhed med et SCADA-anlæg, ofte kunne ødelægge systemet ved at tænde/slukke for motorer og kompressorer på en måde, der er udover, hvad de kan tåle, og dermed potentielt skabe en sikkerhedsrisiko. Det gælder enhver type udstyr med bevægelige dele, der kan manipuleres via IoT, f.eks. aircondition-kompressorer, varmeanlæg, dørlåse, industrielt udstyr og pumper. IoT-kontrollerede skodder/persienner vil man potentielt kunne få til at overophede eller bryde i brand, hvis de over en længere periode presses udover deres tolerancer.

"Smarte" bygninger kan være sårbare overfor potentielle cyberhændelser forårsaget af en række forskellige typer cyberangreb. Der kan f.eks. være tale om:

1. Afbrydelse af opvarmning eller afkøling på følsomme steder, såsom i den farmaceutiske industri eller på fødevareforarbejdningsanlæg

2. Manipulering af køleindstillinger på et HVAC-system i en virksomhedsbygning, hvilket skaber betydelig forretningsforstyrrelse og mistet produktivitet

3. Afbrydelse af køle- eller strømstyringsfunktioner til et datacenter, der ødelægger it-udstyr og tager forretningskritiske applikationer offline

4. Uautoriseret adgang til intelligente højtalere udstyret med mikrofon muliggør aflytning og dermed industrispionage eller krænkelse af personer

5. Uautoriseret adgang til et internetforbundet fysisk sikkerhedssystem (videoovervågning og adgangsstyring) muliggør et fysisk indbrud eller anden form for angreb

Jo flere af denne type hændelser vi ser, jo mindre tillid vil slutkunderne have til de digitaliserede løsninger. Det betyder, at kunderne går glip af de muligheder, løsningerne giver, og at vi samfundsmæssigt mister en stor potentiel effektivisering og vækst i vores samfund. Men producenter og installatører går ligeledes glip af en potentielt givtig forretning.

I et samfundsmæssigt perspektiv kan et angreb, der rammer flere enheder, desuden være af enorm betydning. Hvis et angreb f.eks. rammer el-distributionsnetværket, hvor den samme type it-systemer anvendes bredt, kan det have stor betydning for elforsyningssikkerheden.

Case

Angreb mod el-produktionen i Ukraine

I december 2015 var der et russisk angreb på el-produktionen i Ukraine, der betød, at dele af landet var uden strøm i flere timer.

Tre elproduktionsfirmaer var blevet ramt af et cyberangreb med malwaren "BlackEnergy". Malwaren har været kendt siden 2007 og er løbende blevet opdateret med nye funktioner.

Malwaren kom ind via en phishing-mail og fandt herefter vej til forsyningssystemerne. Forsyningssystemerne havde en række sårbarheder, der gjorde det muligt for angriberne at skaffe sig adgang til loginoplysningerne til kontrolsystemet, hvorfra de forårsagede et strømnedbrud flere steder i Ukraine. Samtidig blev firmaernes callcentre angrebet, hvilket gjorde det umuligt for kunderne at komme i kontakt med firmaerne.

Hvad er Internet of Things (IoT)?

Internet of Things er et system med indbyrdes forbundne computerenheder, mekaniske og digitale enheder, objekter, dyr eller mennesker, der har mulighed for at overføre data over et netværk uden at kræve menneske-til-menneske eller menneske-til-computer interaktion.

Definitionen af IoT har udviklet sig på grund af konvergensen af flere teknologier, realtidsanalyse, maskinlæring, sensorer og indlejrede systemer. Traditionelle områder med indlejrede systemer, trådløse sensornetværk, kontrolsystemer, automatisering (inklusive hjemme- og bygningsautomatisering) og andre bidrager alle til at muliggøre IoT.

I forbrugermarkedet er IoT-teknologi mest synonymt med produkter, som vedrører begrebet "smarte hjem", der dækker enheder og apparater (såsom belysningsarmaturer, termostater, sikkerhedssystemer til hjemmet og kameraer og andre husholdningsapparater), der understøtter et eller flere almindelige økosystemer og kan styres via enheder, der er tilknyttet disse økosystemer, f.eks. smartphones og smarte højttalere.

Typisk kobles IoT-produkter op til forbrugerens netværk via enten Bluetooth eller wireless LAN, og meget ofte benyttes en eller anden form for cloudtjeneste.

I en professionel sammenhæng tales ofte om Industrial Internet of Things (IIoT), der henviser til sammenkoblede sensorer, instrumenter og andre enheder, der er koblet sammen med systemer til industriel styring og overvågning. Denne sammenkobling giver mulighed for dataindsamling, udveksling og analyse, der potentielt kan forbedre produktivitet og effektivitet samt give en række andre økonomiske fordele.

Forskellige typer IoT-udstyr

Indenfor IoT/IIoT-området findes der forskellige klasser1 af enheder karakteriseret efter bl.a. deres energiforbrug, processorkraft, hukommelse og muligheder for opkobling til netværk.

De helt enkle IoT-enheder er typisk meget simple sensorer eller lignende, der på grund af stærkt begrænsede ressourcer ikke har mulighed for afvikling af en fuld internet-protokolstak og derfor typisk er forbundet til en eller anden form for proxy eller gateway, der står for den egentlige netværkskommunikation. Disse enheder er typisk så simple, at de ikke har mulighed for basale sikkerhedsfunktioner som kryptering og autentifikation.

De lidt mere avancerede IoT-enheder har typisk flere muligheder, herunder bedre mulighed for opkobling via standardiserede netværksteknologier som Bluetooth og wireless LAN. Eksempler på denne type enheder er forbundne lyskilder og smarte låse. De kan have enkelte simple funktioner, men har sjældent de store muligheder for avancerede sikkerhedsfunktioner.

Derudover findes en klasse af avancerede IoT-enheder med væsentlig flere ressourcer og muligheder, eksempelvis i form af husholdningsapparater og smarte termostater. Disse enheder vil typisk have kapacitet til fuld selvstændig internetopkobling og afvikling af mere avancerede sikkerhedsfunktioner som f.eks. kryptering.

Endelig findes der en klasse af high-end IoT-enheder, som blandt andet omfatter f.eks. netværksforbundne harddiske (NAS-enheder), gateway-produkter og routere. Disse har ressourcer til afvikling af udvidede sikkerhedsfunktioner og kan bl.a. medvirke til at koble simplere enheder sammen med det egentlige netværk/Internettet samt understøtte sikkerheden på simplere enheder.

1 Yderligere information omkring systematisk kategorisering af IoT-enheder kan eksempelvis findes i RFC7228 "Terminology for Constrained-Node Networks" se evt. https://tools.ietf.org/html/rfc7228

Der er en række alvorlige bekymringer om farer i væksten af IoT, især inden for områderne privatliv og sikkerhed, hvilket har sat gang i en lang række initiativer fra leverandørerne af IoT-produkter og lovgivere med henblik på at adressere bekymringerne.

Der sker en konstant udvikling indenfor komponent- og processorområdet, hvilket gør, at integrerede kredsløb bliver billigere, hurtigere, mindre og bruger mindre strøm. Denne udvikling har to konsekvenser på IoT-området: For det første bliver de eksisterende anvendelser mere avancerede, da man får mere avancerede funktioner. For det andet bliver komponenter med samme muligheder som i dag billigere, mindre og anvender mindre strøm, hvilket medfører stadig flere nye anvendelsesmuligheder.

I dag er det muligt at få en chip, som er et enkeltintegreret kredsløb indeholdende en relativ kraftig fuld computer, inklusiv hukommelse og mulighed for trådløs opkobling via Bluetooth og WiFi for under 10 kroner. Det betyder, at alle og enhver kan IoT-enable deres produkt for en ganske beskeden merpris, hvilket er baggrunden for en stadig udvikling med flere og flere forskellige IoT-enablede produkter.

Endelig sker der også en konstant udvikling indenfor mulighederne for trådløs opkobling af IoT-enheder, herunder fremkomsten af en række standarder og teknologier målrettet anvendelse i forbindelse med IoT-løsninger. Dette drejer sig blandt andet om standarder i forbindelse med fjernaflæsning af målere som Wireless M-Bus (anvendes bl.a. af Kamstrup til deres målere), Narrowband Internet of Things (NB-IoT) og LoRaWan. Til automatisering på kortere distancer findes blandt andet standarder som ZigBee, samt naturligvis Bluetooth. Desuden forventes det kommende 5G-netværk at have en stor rolle i forbindelse med IoT-udstyr, da det tilbyder bedre forbindelser med højere båndbredde, mindre forsinkelse og er billigere.

Generelt bliver de trådløse teknologier, der understøtter IoT, konstant hurtigere og billigere, hvorfor det må forventes, at stadig flere IoT-enheder bliver forbundet trådløst.

En væsentlig forskel på "almindeligt" it-udstyr og Internet of Things (IoT)-enheder er, at it-udstyret typisk er designet til at blive koblet på nettet fra starten, mens mange IoT-produkter og -løsninger ikke er udviklet og produceret med digital sikkerhed for øje. I stedet forsøges sikkerhedsfunktioner tilføjet efterfølgende i forbindelse med at udstyret forsynes med et digitalt interface.

Ofte har hardwaren i IoT-enheder ikke ressourcer til mere avancerede sikkerhedsfunktioner som kryptering til beskyttelse af data. Samtidig er softwaren i enhederne typisk baseret på standardkomponenter, det vil sige alment tilgængelige operativsystemer og softwarebiblioteker. Det betyder, at når der findes sårbarheder i disse standardkomponenter, vil tilsvarende sårbarheder også være tilstede i IoT-produktet. Det stiller krav til, at softwaren løbende vedligeholdes, så nye sårbarheder lukkes.

Producenterne af IoT-enheder har ofte ikke en veldefineret politik for vedligeholdelse af deres produkter i hele produktets levetid. Mange af løsningerne er således ikke designet til at modtage sikkerhedsopdateringer automatisk eller bliver slet ikke opdateret fra producenten. Det betyder, at brugerne anskaffer en IoT-løsning, som ofte allerede på købstidspunktet har sårbarheder. Derudover oplyses det kun sjældent, hvor længe producenten forventer at vedligeholde produktet, herunder hvor længe de retter sårbarheder og frigiver nye software versioner.

Typiske fejl og sårbarheder i IoT-udstyr

- **Passwords, der er svage, lette at gætte eller gemt i klartekst**
- **Usikre netværkstjenester**
- **Usikre brugerinterface**
- **Manglende funktion til sikker opdatering**
- **Brug af usikre og forældede komponenter**
- **Manglende eller utilstrækkelig beskyttelse af persondata**
- **Usikker dataoverførsel og -opbevaring**
- **Manglende styring af enheden**
- **Usikre defaultindstillinger**
- **Manglende fysisk hærdning**

Baseret på OWASP TOP 20

Case

Best Buy stopper service på deres produkter

Den 6. november 2019 stoppede Best Buy service på deres Insignia Connect linje af smart home produkter. Serien inkluderer konvertible kølefryseskabe, smart plugs, smart light switches og kameraer, der kan kobles på Wi-Fi. Servicestoppet betød, at mange af produkterne mistede den funktionalitet, som mange forbrugere havde købt dem på baggrund af.

Som forbruger indgår man en serviceaftale med producenten, der står for vedligeholdelse af software. Det betyder, at man som forbruger skal satse på, at producenten bliver ved med at vedligeholde produktet. Best Buy tilbød kunderne delvise gavekort og ikke fuld tilbagebetaling. Derudover svarede de ikke på de mange henvendelser fra forbrugerne om situationen.

Mange IoT-produkter er produceret med usikre standardindstillinger, typisk for at gøre dem let tilgængelige for slutbrugeren ("it's not a bug – it's a feature"). Det betyder, at hvis de personer, der anskaffer, installerer og anvender produkterne, ikke er bevidste om cybersikkerhed og får ændret standardindstillingerne, vil produktet ofte være sårbart for angreb. Typiske eksempler på dette er manglende skift af standardpasswordet eller utilsigtede åbninger fra internettet.

En særlig udfordring med IoT-udstyr er, at det ofte er eksponeret eller tilgængeligt eksternt samtidig med, at det er koblet på virksomhedens interne netværk. Da IoT-udstyret ofte mangler basale sikkerhedsfunktioner, ofte ikke bliver overvåget og ofte er fejlkonfigureret, er det et oplagt og simpelt springbræt ind i virksomhedens øvrige systemer.

Case

Cyberangreb mod varme- og airconditionanlæg

I 2012 blev et firma i New Jersey ramt af et cyberangreb, der var rettet mod firmaets varme- og aircondition enheder[1]. Hackeren fik adgang til systemet via en bagdør i den anvendte software. Via denne var det muligt at omgå loginsystemet og få adgang med administratorrettigheder. Her fik hackeren adgang til en GUI med overblik over kontorets grundplan, som blandt andet indeholdt tydelige markeringer af områder og navne på ansatte. Den udnyttede software er et meget udbredt stykke software, der blandt andet bruges i lignende systemer hos statslige myndigheder som Pentagon og FBI samt større virksomheder som Google[2] mv. Systemet var tilsluttet direkte til internettet, uden en firewall, og kunne tilgås eksternt fra.

1 https://arstechnica.com/information-technology/2012/12/intruders-hack-industrial-control-system-using-backdoor-exploit/

2 https://www.wired.com/2013/05/googles-control-system-hacked/

Andre former for misbrug kan f.eks. være, at enhederne udnyttes til at gennemføre Man-in-the-Middle-angreb eller datatyveri.

Case

Ransomware i en IoT sammenhæng – Seedorf Hotel

I januar 2017 blev Romantik Seehotel Jäegerwirt, et 4-stjernet Superior-hotel i Østrig, ramt af ransomware, der blandt andet ramte systemet til styring og administration af nøglekort. Dette betød, at flere hundrede gæster blev låst ud af deres værelser. Ransomwaren inficerede systemerne på hotellet, og dets ledelse valgte at betale løsepenge for at gendanne systemerne. Hotellet oplyser, at de har betalt 1.500 € i Bitcoin for at gendanne det elektroniske nøglekortsystem, der blev kompromitteret af ransomware[1].

1 http://securityaffairs.co/wordpress/55790/cyber-crime/ransomware-luxury-hotel.html

Udviklingen i digitale løsninger

Ligesom stort set alle andre brancher bliver industri- og installationsbranchen i disse år ramt af nogle tendenser, der ændrer de teknologiske og markedsmæssige rammevilkår.

Den teknologiske og digitale udvikling ændrer den måde, som virksomheder løser centrale opgaver på og deres muligheder. Samtidig får private forbrugere en lang række muligheder for nye smarte produkter. Udviklingen har fået en række prædikater, blandt andet "den fjerde industrielle revolution" eller industri 4.0, SmartHome, SmartCity.

Denne udvikling bliver drevet frem af udviklingen på en lang række forskellige områder, der også har nogle potentielle risici i forhold til cybersikkerhed.

Område	Anvendelse	Cybersikkerhedsrisici
Billigt hardware	Prisen på digitalt hardware falder konstant, og i dag er det f.eks. muligt at få integrerede kredsløb med processor, hukommelse og indbygget mulighed for Bluetooth og WiFi for langt under 10 kroner. Det betyder, at barrieren for, hvilket udstyr der med rimelighed kan gøres digitalt, i praksis er væk. Alt udstyr må efterhånden forventes at blive digitaliseret med mulighed for opkobling – alene fordi det ikke kan betale sig at lade være.	Udviklingen betyder, at vi kommer til at se langt flere digitale enheder, både i anvendelsesområder og antal, hvilket medfører langt flere forskellige steder, der kan angribes. Forskellige enheder anvender som oftest forskelligt software og håndteres på forskellige vis. Det betyder, at der vil være mange forskellige systemer, vi skal forholde os til. Endelig viser erfaringen, at jo billigere og simplere en enhed er, jo mindre fokus er der på kvalitet og dermed cybersikkerhed. Dette medfører, at mange enheder kommer med usikkert software, og at producenten ofte ikke har fokus på at levere opdateringer, når der bliver fundet sikkerhedshuller.
5G	Der findes allerede i dag en række forskellige netværksløsninger, der anvendes til opkobling af IoT-udstyr, bl.a. baseret på LoRaWan gateways og eksisterende 3G/4G mobilnetværk. Med udbredelsen af 5G-teknologien, der bl.a. er målrettet netop IoT og Machine to Machine (M2M)-kommunikation, forventes det, at rigtig meget udstyr i fremtiden vil være født med 5G-forbindelse. Dette vil gøre det simplere for mange flere typer af udstyr at blive opkoblet. Nogle af de anvendelsesmuligheder, der er i spil i forhold til det kommende 5G-netværk, er hele IoT-området, hvor der bliver åbnet nye muligheder for automatisering ligesom 5G netværket betragtes som en enabler for selvkørende biler, fjernstyrede operationer m.m. De første 5G-tests er blevet gennemført fra alle danske mobilselskaber i løber af 2019, og det er annonceret, at TDC forventer at være klar med landsdækkende 5G-service i slutningen af 2020.	Udbredelsen af 5G kommer til at betyde, at meget udstyr vil blive leveret opkoblet. Det vil sige, at det er forbundet pr. default. På 5G-netværket er alle enheder i princippet frit eksponeret med en egen offentlig adresse. Når udstyret er konstant opkoblet, er det i princippet også konstant eksponeret for angreb. Det betyder, at udstyret har en væsentlig større risiko for at blive angrebet, fordi evt. sårbarheder er væsentlig mere eksponeret. Da sårbarhederne er mere eksponeret og vil blive forsøgt hurtigere udnyttet, bliver løbende sikkerhedsopdateringer yderst vigtige for at opretholde sikkerheden. Når kommunikationen ikke sker via virksomhedens netværk, vil det være umuligt for virksomheden at styre og overvåge kommunikationen, da denne sker via teleudbyderens netværk.

Område	Anvendelse	Cybersikkerhedsrisici
Mobile enheder	Brugerne har et ønske om stor fleksibilitet og brugervenlighed. Derfor bliver mange løsninger i dag udviklet som "mobile first", hvilket betyder, at udgangspunktet er betjening via en app.	Mobilapplikationer har længe været en særlig udfordring i forhold til sikkerhed, da mobile enheder er vanskelige at kontrollere. En lang række problemer skyldes sårbarheder i applikationerne og den cloud-baserede backend, som applikationerne bruger. Der er ligeledes gentagende eksempler på uautoriseret dataopsamling. En anden udfordring er brugervalideringen, som der ofte bliver gået på kompromis med, fordi det skal være nemt at tilgå løsningen.
Smart Home / IoT	Stadig flere produkter som f.eks. hårde hvidevarer og lyskilder (smart light) bliver digitaliserede. Samtidig anvendes talegenkendelse og kunstig intelligens flere og flere steder i hverdagen. Der er typisk tale om simple løsninger, der kobles sammen i forskellige økosystemer og som konfigureres af slutbrugerne selv.	I sidste ende er det slutbrugeren, der har ansvaret for den enhed, der installeres i hjemmet. De mange forskellige løsninger og teknologier medfører, at it-miljøet i hjemmet bliver stadig mere komplekst. Det stiller krav til brugernes viden om sikkerhed og trusler. Når slutbrugerne selv konfigurerer løsningerne, er det nemt ubevidst at kompromittere sikkerheden på grund af fejlkonfiguration, eller fordi udstyret er koblet på husets almindelige netværk i stedet for et selvstændigt.
Grøn omstilling	Der er en forventning om, at den grønne omstilling vil medføre, at hovedparten af energiforsyningen elektrificeres. Desuden vil store dele af elproduktionen blive baseret på variable kilder, som f.eks. vindmøller og solceller. Det forventes derfor, at der i et vist omfang bliver behov for at kunne styre forbruget decentralt. På den måde kan man eksempelvis styre, at opvarmning af vand og opladning af elektriske biler ikke sker samtidig med, at der i øvrigt er lav produktionskapacitet. En anden overvejelse er muligheden for at benytte decentral opbevaring af energi, f.eks. ved at batterierne i elektriske biler kan levere strøm til elnettet, når der i øvrigt er strømmangel. For at dette kan lade sig gøre, kræves digitale løsninger til gradueret overvågning og styring af det elektriske energiforbrug decentralt.	Der er i dag mange digitale løsninger, som medvirker ved styring af energiforbrug mv. Hvis sådanne løsninger kompromitteres, er der risiko for decentrale afbrydelser og forstyrrelser og dermed risiko for strømafbrydelser, lukning af varmeforsyning m.m. Derudover er der også risiko for, at en kompromittering af løsningerne kan påvirke den samlede energiforsyning. Det kan f.eks. ske ved at forbruget hos mange forbrugere forstyrres og medfører, at der sendes transiente overspændinger ud i elnettet med risiko for alvorlig ødelæggelse og beskadigelse af udstyr.
Integration	En væsentlig del af værdien ved digitaliseringen er muligheden for, at forskellige systemer kan integreres på kryds og tværs med henblik på blandt andet styring og dataudveksling. Dette ses f.eks. i bygningsautomatisering, hvor der kan være et ønske om at sammenkoble adgangsstyringen med virksomhedens HR-system, i industrien hvor ERP-systemet kobles sammen med produktionen, og i SmartHome-løsninger hvor intelligent belysning ønskes sammenkoblet med Smart hubs, digitale taleassistenter og cloud løsninger.	Den øgede integration medfører flere potentielt sårbare grænseflader og øger samtidig kompleksiteten i it-miljøerne, hvilket gør det svært at overskue den faktiske sikkerhed. Derudover er der risiko for, at problemer i én løsning kan påvirke andre løsninger.
Industri 4.0	Industri 4.0 er en samlet betegnelse for integrationen mellem digitale løsninger og fysisk produktion i intelligente, sammenhængende netværk, der kan kontrollere udstyr og elementer i hele den industrielle værdikæde. Baggrunden for udviklingen mod industri 4.0 er et ønske om bedre og mere effektiv styring af produktion, herunder gennem dataopsamling.	Sammenkoblingen af nye og gamle teknologier udgør en sårbarhed, fordi de gamle teknologier ikke nødvendigvis er bygget til integration med nyere og digitalt opkoblede teknologier. Hvis et produktionsanlæg kompromitteres, kan det have alvorlige økonomiske, fysiske såvel som menneskelige konsekvenser ved afbrydelser og forstyrrelser.

Område	Anvendelse	Cybersikkerhedsrisici
Cloud-løsninger	Stadig flere produkter er baseret på cloud-services til dataopsamling og kontrol. Cloud-løsninger anvendes især med henblik på at reducere omkostninger ved selv at hoste en løsning, eller fordi det er nemmere for slutbrugerne at anvende en plug'n'play-løsning til f.eks. opbevaring af billeder eller håndtering af kundedatabaser og økonomisystemer. Cloud-løsninger gør det typisk også væsentlig simplere at udvikle applikationer, hvilket betyder, at barriererne for at udvikle software er væsentlig længere.	Brugerne er ikke altid bevidste om, at løsningen/produktet bruger en cloud-løsning. Det betyder, at de ikke aktivt har overvejet, hvilke data der overføres til cloud-løsningen, og hvordan de er beskyttet, herunder hvem der har adgang til løsningen og dermed data. Det er især en udfordring, når der er tale om personoplysninger, men i lige så høj grad, når der er tale om fortrolige eller virksomhedskritiske oplysninger. Cloud-løsninger er ofte komplekse forstået på den måde, at man kan have en leverandør, der varetager selve infrastrukturen, mens en anden leverandør leverer applikationen. Ved anvendelse af cloud-løsninger er det vigtigt at være opmærksom på den model for delt ansvar, som cloudtjenesten benytter sig af. Dette for, at man ved, hvilke forhold leverandøren varetager, og hvilke områder man selv er ansvarlig for. Al erfaring viser, at de store seriøse cloud-infrastrukturleverandører har styr på deres del af sikkerheden, og at alle brud i praksis opstår på grund af sårbarheder i applikationerne eller dårlig kontrol og styring hos slutbrugere. Det er særligt et problem ved mindre seriøse, forbrugerorienterede produkter. Endelig er der en risiko for, at en hændelse i en cloud-løsning vil betyde, at mange produkter og kunder rammes på samme tid. Det er dog vigtigt at understrege, at cloud-løsninger ofte er væsentlig mere sikre end andre løsninger, fordi der ofte er flere ressourcer til at have fokus på sikkerhed.
Kunstig intelligens (AI)	Kunstig intelligens (engelsk: Artificial Intelligence) anvendes i stigende grad til at øge effektivitet og inkluderes i forskellige former for smarte løsninger. Kendte eksempler på anvendelsen af AI i hverdagen er Apples Siri og Googles Alexa, men den kunstige intelligens bruges også i mange andre sammenhænge, f.eks. i forbindelse med sikkerhed, hvor den kan være med til at opdage ukendte trusler eller forbedre sikkerhedsløsningernes evne til at opdage sikkerhedstrusler. Andre områder hvor AI vinder indpas er f.eks. brugen af ansigtsgenkendelse.	Brugen af kunstig intelligens stiller krav til sikkerheden på en række forskellige områder. AI-løsninger er som regel baseret på, at de lærer på baggrund af (meget store) indsamlede datasæt. Disse datasæt kan ofte indeholde følsomme data. Det betyder blandt andet, at man skal være opmærksom på, hvem der har adgang til de indsamlede data, så regler omkring privacy ikke overtrædes. Det er også vigtigt, at data er ordentlig repræsentative, da AI-systemet ellers trænes på baggrund af et forkert grundlag. AI giver en lang række muligheder, men samtidig kan det være svært helt at gennemskue, hvad systemet rent faktisk reagerer på. Det kan medføre en manglende tillid til, at systemet er til at stole på.
Konvergens	Der findes en lang række forskellige standarder og protokoller til automatisering og styring. I forhold til intelligente installationer og bygningsstyring anvendes f.eks. LON og KNX, mens der i industrien anvendes standarder som Profinet/Profibus, Modbus, DNP3 med flere. Alle disse protokoller er som udgangspunkt standardiserede, men også proprietære i forhold til standard ip-baseret internetkommunikation. I dag er der imidlertid et stort ønske og behov for at kunne integrere gamle løsninger baseret på disse protokoller med moderne ip-baserede løsninger. Det har medført, at der findes forskellige former for "gateways", som gør det muligt at koble udstyr baseret på gamle protokoller på standard ip-netværk.	Mange af de anvendte protokoller er oprindeligt udviklet til brug i lukkede og isolerede miljøer, hvor man antog, at netværket var sikkert. Det betyder, at de mangler basale sikkerhedsfunktioner til bl.a. autentifikation og kryptering. Når disse protokoller bliver "internet enabled", sker det ofte ved en simpel indpakning i internettrafik uden tilføjelse af basale sikkerhedsfunktioner. Det betyder, at protokollerne nemt kan misbruges af en angriber, der har tilegnet sig adgang til netværket.

Den accelererede teknologiske udvikling har stor betydning for markedet. Producenterne har ikke lang tid til at få deres nye løsninger og teknologier skubbet ud i markedet, før nyere løsninger fra konkurrenterne kommer til. Time-to-market er således afgørende for at klare sig og få succes. Nye online kanaler skaber nemt en kortere vej mellem producent og forbruger, hvilket gør det nemmere for producenten at komme tæt på kunden og etablere en kommerciel kontakt.

Samtidig bliver selv komplekse produkter stadig mere simple at konfigurere, og kunderne/slutbrugerne bliver mere teknisk kompetente. Det giver plads i markedet til de såkaldte "prosumer"-produkter, der er produkter af en kvalitet og funktionalitet, der tidligere var målrettet professionel anvendelse, men nu kan købes og installeres af private eller professionelle slutbrugere. Dette bliver hurtigt attraktivt for slutbrugeren i det omfang, at der ikke er en tydelig merværdi ved at bruge en installatør til at levere en løsning baseret på produktet.

På mange områder er slutkunder og markedet ved at være tilvænnet forskellige former for leje, leasing eller serviceløsninger, hvor der ikke sker en kapitalbinding og investering i produkter, men at disse i stedet leveres som en service fra en producent. Indenfor bygningsområdet ses det eksempelvis ved forskellige former for facility management-løsninger. Ofte medfører dette også, at producenten har ansvaret for vedligeholdelsen af produktet eller løsningen i en "as-a-service"-leverancemodel. I forhold til cybersikkerhed kan dette både være en fordel og en ulempe. En fordel i det omfang at leverandøren på kvalificeret vis påtager sig ansvaret for opdatering og sikring af løsningen. En ulempe i det omfang at leverandøren påtager sig ansvaret, men ikke løser opgaven på en kvalificeret måde.

I det omfang at produkter leveres via en "as-a-service"-leverancemodel direkte fra en producent, kan det potentielt medføre, at det kommercielle forhold også etableres direkte mellem producent og slutkunde. Mange løsninger er i dag baseret på forskellige online cloud-løsninger fra producenten, som gør, at producenten har en direkte kanal til slutbrugeren. Ofte vil producenten kunne benytte denne kommercielt f.eks. i forbindelse med forlængelse af aftaler, hvorved mellemmanden dvs. distributør og leverandør forsvinder. Samtidig er slutkundernes prioritering blevet mere kommercielt og løsningsorienteret, dvs., at de har fokus på den værdi, der leveres i løsningen, fremfor teknologien, og hvor og af hvem det købes. Altså samme udvikling som ses andre steder med faldende kundeloyalitet. Slutkundernes prioritering og lavere kundeloyalitet kombineret med muligheden for direkte kommercielle forbindelser mellem producent og slutkunde betyder, at installatøren risikerer at forsvinde fra værdikæden og dermed miste forretning. Hvis dét ikke skal ske, er installatøren nødt til at bidrage tydeligt med værdi overfor slutkunden.

Ofte er mange løsninger udviklet udelukkende med funktionalitet for øje, mens alt der har med sikkerhed at gøre ikke er indarbejdet som del af løsningen. Således er det fortsat muligt at finde produkter uden passende og tidssvarende sikkerhedsfunktioner, primært fra mindre seriøse producenter, hvor det primære fokus er på prisbillige og simple løsninger. De store og seriøse producenter af udstyr er de senere år generelt begyndt at tage cybersikkerhed seriøst, og fornuftige sikkerhedsfunktioner er i dag en integreret del af de fleste nye løsninger. Ligeledes arbejder de ud fra principper om "security by design" og "security by default", hvilket betyder, at løsningerne som udgangspunkt er designet og konfigureret, så de er sikre.

Men at et produkt er designet med fokus på sikkerhed, betyder nødvendigvis ikke, at det er sikkert og vedbliver med at være sikkert. Der kan stadig være eller blive konstateret sårbarheder i de anvendte komponenter, der gør at produktet er sårbart og dermed usikkert, indtil den pågældende sårbarhed er blevet udbedret.

Ligeledes er der ikke altid en entydig sammenhæng mellem pris på produktet og sikkerhedsniveauet. Her er det afgørende at have fokus på producenten bag produktet og deres tilgang og arbejde med sikkerhed, eksempelvis deres politik omkring produktlivscyklus og håndtering af sårbarheder og frigivelse af nye softwareversioner.

Samtidig bliver løsningerne stadig mere integrerede, og det bliver vanskeligere at trække grænsen for, hvornår noget er en komponent til en løsning, og hvornår det er selvstændig IoT-enhed.

Regulering og standarder

Den teknologiske udvikling har også betydning for arbejdet med regulering og standarder, hvor cybersikkerhed i stigende grad begynder at fylde mere og mere.

Industri- og installationsbrancen er vant til at arbejde ud fra standarder i flere sammenhænge. Således findes der på de fleste områder en standard, der – hvis den følges – sikrer, at installatøren lever op til lovgivningen. Det gælder eksempelvis elsikkerhedsloven og installationsbekendtgørelsen, hvor relaterede standarder er samlet i DS/HD 60364-serien, og maskindirektivet, hvor der er en række standarder, der tager udgangspunkt i direktivets krav.

Der ses på nuværende tidspunkt en tendens til, at flere direktiver ændres fra direktiver til forordninger. Forskellen på direktiver og forordninger er, at direktiver skal implementeres i de enkelte EU-landes lovgivning gennem bekendtgørelser, mens forordninger har direkte retsvirkning i alle EU-lande.

Et af de direktiver, der er planer om at ændre, er maskindirektivet. I forbindelse med en planlagt opdatering overvejer EU-Kommissionen samtidig at inkludere risici, der er relateret til nye digitale teknologier. Det gælder blandt andet cybersikkerhed, Internet of Things (IoT) og kunstig intelligens (AI)[1].

Fællesregulativet er i sommeren 2019 blevet opdateret på baggrund af en række EU-forordninger og elforsyningsloven. En af de største ændringer vedrører forbrugsenheder som varmepumper, el-radiatorer, køleanlæg og vindmøller. Installatører skal nu tilmelde større forbrugsgenstande, der producerer eller forbruger energi, til det lokale netselskab[2].

Cybersikkerhed bliver også relevant i relation til bygningsreglementet, hvor der er et funktionskrav om, at en bygning ikke må bidrage til, at mennesker slås ihjel eller kommer til skade. Det stiller krav til sikring af IoT-løsninger, der anvendes i relation til f.eks. elevatorer eller brandtekniske installationer, er tilstrækkeligt adskilt fra øvrige netværk.

Cybersikkerhed er ligeledes tænkt ind i IEC 62443-standarden, der forholder sig til sikring af industrielle automations- og kontrolsystemer, herunder også de cybersikkerhedsmæssige aspekter. Kendskabet til standarden er endnu ikke så udbredt, men det ventes, at standarden vil vinde større og større indpas.

Også i USA ser vi tendenser til, at cybersikkerhed fylder mere og mere i lovgivningen. Californien har som den første stat vedtaget en lovgivning, der forholder sig til Internet of Things. Fra 1. januar 2020 skal produkter, der direkte eller indirekte kan kobles på internettet, være udstyret med tilstrækkelige sikkerhedsforanstaltninger og designet til at beskytte mod uautoriseret adgang, ændring eller afsløring af informationer. Hvis udstyret kan tilgås fra et eksternt netværk, skal udstyret enten have et unikt password, eller brugerne skal tvinges til at ændre password, første gang udstyret kobles på netværket. Selvom der er delte meninger om lovgivningens tilgang til sikkerhed, er det en start og hjælper med at hæve grundniveauet.

Derudover findes der en række initiativer med henblik på etablering af retningslinjer, vejledninger og standarder fra blandt andet Global Cybersecurity Alliance (GCA).

På industriområdet er International Society of Automation (ISA) aktiv, blandt andet med udgivelsen af ISA 62433-standarden, som særlig er anvendelig i industrien.

Glem ikke persondata

Det er ikke kun standarder for selve installationen eller sikringen af denne, der skal tages højde for. EU-persondataforordningen (GDPR) betyder, at installatører også skal være opmærksomme på, hvilke af de data der indsamles og sendes via IoT-enheder, der er persondata og dermed skal beskyttes mod misbrug og uvedkommendes adgang.

Et eksempel er anvendelsen af kameraovervågning med ansigtsgenkendelse, der f.eks. kan bruges til adgangskontrol. Her skal man være opmærksom på, at GDPR stiller skrappe krav til nødvendigheden af at behandle data og omfanget af de data, der behandles. Det er derfor ikke muligt at lave vilkårlig indsamling af ansigter. I skrivende stund er Brøndby IF den eneste private aktør, der har fået tilladelse til at anvende ansigtsgenkendelse med det formål at holde karantænedømte fans ude[3].

1 https://www.sik.dk/erhverv/produkter/vejledninger/maskiner/nyheder/eu-kommissionen-vil-aendre-maskindirektivet

2 https://www.danskenergi.dk/sites/danskenergi.dk/files/media/dokumenter/2019-07/F%C3%A6llesregulativet%202019.pdf

3 https://ipaper.ipapercms.dk/tekniq/electra-2019/august-2019-electra/?page=14

Case

Opsamling af persondata ved adgangskontrol

I oktober 2018 fik Arbejdernes Andels Boligforening (AAB) installeret et nyt låsesystem med nøglebrikker, der skulle give adgang til opgange, vaskerum og andre fællesarealer. I forbindelse med dette blev der udsendt et brev til beboerne. Heri stod der, at låsesystemet logger, hvor nøglerne bliver brugt, og at beboerne har mulighed for at få indsigt i deres log. I januar 2019 blev der indsendt en klage til Datatilsynet over det nye låsesystem, og at logningen foregik uden at beboerne havde givet samtykke, og uden at de blev informeret om behandlingen af data. AAB forklarede herefter, at det var ID, hændelseskode og tidsstempel, der blev logget, og at formålet var at spare beboerne for den daglige drift med udskiftning og vedligeholdelse af låsesystemet. Datatilsynet afgjorde, at der var foretaget en tilnærmelsesvis overvågning af beboerne og dermed et ulovligt indgreb på beboernes privatliv. AAB er efterfølgende holdt op med at logge disse data [1] [2].

1 https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/aug/logning-af-beboeres-noeglebrikker/

2 https://www.version2.dk/artikel/boligselskab-overvaagede-ulovligt-beboeres-faerden-gennem-noeglebrikker-1089087

Cybersikkerhed i bygningers installationer og HVAC

Hovedparten af alle nye bygninger etableres som smarte bygninger, hvor man søger at udnytte bygningsdata for at optimere driften og mindske omkostningerne, mens det øger sikkerheden og bæredygtigheden. Smarte bygninger tilpasser sig udnyttelsen i realtid, mens de optimerer energiforbruget så meget som muligt. De forbinder ofte interne systemer – HVAC-kontroller (Heating, Ventilation and Air Conditioning), datanetværk, strømstyring osv. – med eksterne netværk for mere effektivt at overvåge og styre bygningsoperationer.

Alarm- og sikringsområdet er en særlig udfordring, da der sker en sammenkobling mellem virksomhedens fysiske sikringssystemer og digitale løsninger. Det betyder, at cyberhændelser vil kunne have konsekvenser også for den fysiske adgangssikkerhed.

Videoovervågning opsamler persondata, hvilket betyder, at behandling og opbevaring af disse data er underlagt kravene fra EU-persondataforordningen (GDPR). Det er således ikke kun lov om tv-overvågning, der skal tages hensyn til, når der opsættes overvågningskameraer. Det understreger en dom fra Østrig, hvor et forkert opsat overvågningskamera medførte en bøde på 4800 EUR. Lignende sager er ikke utænkelige i Danmark.

Case

Bøde i forbindelse med tv-overvågning

I 2018 blev et Østrigsk iværksætterfirma tildelt en bøde på 4800 EUR for overtrædelse af TV-overvågningsloven og GDPR. Overtrædelsen gik ud på, at firmaet havde sat et overvågningskamera op ude foran sin bygning. Problematikken ved dette var, at kameraet ikke alene overvågede firmaets private grund, men også en stor del af fortovet. Fortov defineres som offentligt område, hvilket medfører flere overtrædelser. Først og fremmest blev der ikke tilstrækkeligt informeret om overvågningen, personerne, der blev overvåget, gav ikke deres samtykke, og der blev behandlet for mange persondata i forhold til, hvad der var nødvendigt [1 2].

1 https://serop.dk/de-foerste-boeder-er-allerede-kommet/

2 https://synchlaw.se/da/datatilsynet-i-oestrig-boede-til-oestrigsk-virksomhed-paa-4-800-eur/

Inden for HVAC-området er det løsninger som smarte termostater, tilsluttede varmesystemer, tjenesteudbydere, fjernovervågning, kølesystemer m.fl. Løsningerne giver en lang række muligheder for bedre komfort, mere effektiv og økonomisk energiudnyttelse. Samtidig forventes intelligente løsninger på HVAC-området at blive et vigtigt element i forbindelse med den grønne omstilling, da man blandt andet vil kunne styre og fordele energiforbruget på en mere hensigtsmæssig måde.

Stadig flere af løsningerne bliver IoT-enablet og digitaliseret, hvorved det bliver nødvendigt at håndtere cybersikkerheden.

Case

Las Vegas Casino

I 2017 blev et unavngivet amerikansk kasino udsat for et cyberangreb, hvor hackerne fik adgang til kasinoets netværk gennem et termometer i akvariet i kasinoets lobby. Termometeret gjorde det muligt at regulere miljøet i akvariet. Selvom der var installeret firewall og andre sikkerhedsmekanismer, havde termostaten nogle sårbarheder, der gjorde det muligt for udefrakommende at opnå adgang til netværket. På netværket fik hackerne adgang til databasen med oplysninger om de højst profilerede spillere. 10 Gigabyte data blev sendt til Finland, før det lykkedes at opdage og stoppe angrebet [1 2].

1 https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=US&IR=T

2 https://thehackernews.com/2018/04/iot-hacking-thermometer.html

Produkterne og løsningerne er ofte forbundet til kundens netværk og kan potentielt give adgang til disse netværk. Dermed kan systemer og andre enheder blive kompromitteret. Der findes lang række eksempler, også fra Danmark, på forskellige typer HVAC-systemer, der har været eksponeret direkte på internettet ofte med standardbrugernavne og adgangskoder. Adgangen til HVAC-systemerne kan herefter misbruges til at manipulere med styringen, ligesom HVAC-systemet ofte har adgang til andre netværk og dermed kan anvendes til at stjæle data og true andre systemers sikkerhed.

Cybersikkerhed i industriautomatisering

Digitalisering i industrien – også beskrevet som rejsen mod Industri 4.0, den fjerde industrielle revolution, Smart Manufacturing eller Industrial Internet of Things (IIoT) – har et kæmpe potentiale til at blive katalysator for massiv økonomisk vækst og nye innovative produkter og services. Industri 4.0 bygger på interoperabilitet, autonomi, informationsudveksling, teknologiske løsninger og distribueret digitalisering.

Traditionelt har produktionsprocessen været baseret på en hardwarebaseret struktur. Det har ændret sig med den teknologiske udvikling, der giver mulighed for en ændring til en mere decentral produktion.

Med indførelsen af Industri 4.0 bliver der mulighed for mere intelligent og digitaliseret produktion, fordi produktionsprocessen bliver en integreret del af et samlet netværk og baseret på fleksible, software-styrede systemer, hvor maskinerne kommunikerer med hinanden og produktionen kan baseres på information og data.

Risikoen, når disse sårbarheder udnyttes, er ikke kun digitale skader, men også skader i den fysiske verden på produkter, mennesker og udstyr.

Vejledningen Håndtering af industrikontrolsystemer fra Center for Cybersikkerhed (CFCS) beskriver syv skridt til at opnå tryghed og sikring af industrielle kontrolsystemer.

Begreber – industriautomatisering og industri 4.0

ICS står for Industrial Control Systems. ICS betegner flere forskellige typer af kontrolsystemer og dertil knyttede værktøjer, der bruges til industriel proceskontrol.

OT står for Operational Technology eller på dansk operationel teknik. Betegnelsen bruges om hardware og software, der monitorerer, hvordan fysiske enheder fungerer.

SCADA står for Supervisory Control and Data Acquisition. Betegnelsen bruges om systemer, der samler og analyserer data i realtid. Bruges typisk til at overvåge og kontrollere et produktionsanlæg.

IIoT står for Industrial Internet of Things (IIoT) og dækker over internetforbundne enheder i industrien, eksempelvis sensorer. Sikkerhedsudfordringerne omkring IIoT er de samme, som kendes fra IoT. Konsekvenserne, hvis noget går galt i industrien er dog typisk væsentligt større.

Betegnelserne ICS, OT og SCADA dækker typisk over det samme og er bredt anvendt på tværs af industrier og brancher. Oprindeligt var disse systemer ikke koblet på netværket, men i dag bliver enheder imidlertid koblet til netværket og integreret med administrative it-systemer, hvilket stiller krav til sikkerheden.

Observationer i relation til cybersikkerhed i installationsbranchen

Strukturen i installationsbranchen

Branchen består af en række aktører med forskellige roller:

- Rådgivere
- Producenter
- Grossister/Distributører
- Installatører
- Slutbrugere

Denne struktur med mange interessenter, der ofte har forskelligt fokus, forskellige kompetencer og forskellige interesser, giver et meget varierende fokus, som er med til at komplicere arbejdet med cybersikkerhed.

I forbindelse med de afholdte workshops blev der observeret en meget stor spredning i fokus og særligt digitale kompetencer, hvor nogle virksomheder har valgt at fokusere på avancerede digitale løsninger, mens andre virksomheder ikke har et særligt fokus på digitalisering.

Installationsbranchen er præget af en relativ hård kommerciel konkurrence. Mange – og særligt de større – sager vindes gennem udbud, hvor pris som regel ender med at være den afgørende parameter.

Generelt er det indtrykket fra de afholdte workshops, at cybersikkerhed på nuværende tidspunkt ikke fylder så meget i hverken udbud eller dialogen med kunder. Dette vurderes at skyldes, at cybersikkerhed er et ganske komplekst område, som det kræver særlige kompetencer og indsigt at itale- og værdisætte, hvilket særligt tilgangen til udbud ikke er fremmende for. Cybersikkerhed bliver derfor ofte sparet væk, eller slet ikke medtaget, for derved at være konkurrencedygtig og vinde opgaven.

RÅDGIVERE

PRODUCENTER

GROSSISTER/
DISTRIBUTØRER

INSTALLATØRER

SLUTBRUGERE

Så længe pris er den vigtigste faktor, og det findes svært og besværligt at italesætte værdien af cybersikkerhed på såvel den korte som den lange bane, vil cybersikkerhed ikke blive prioriteret, da det udelukkende betragtes som en yderligere omkostning, som det er svært at retfærdiggøre og tjene på.

Særligt i større og komplekse sager og udbud er rådgiveren kontaktpunktet mellem kunde og installatør. Det er typisk rådgiveren, der står for udformning af kravspecifikation og udbudsmaterialet på større opgaver. Rådgiveren har typisk heller ikke fokus på cybersikkerhed, og rådgivningen er meget rettet mod funktionalitet.

De store producenter har efterhånden alle sammen et rimeligt fokus på cybersikkerhed, og der findes således produkter med fornuftige sikkerhedsegenskaber. Ofte har producenterne dog kun begrænsede kompetencer og ressourcer til cybersikkerhed lokalt i Danmark. Samtidig er produkter med gode cybersikkerhedsfunktioner typisk lidt dyrere, hvorfor de i mange situationer fravælges.

Grossisterne og distributørerne er dem, der har den primære kontakt med, og er agenter for, producenterne. Installatørerne læner sig i vidt omfang op ad distributørernes viden omkring produkter og løsninger. Dette betyder, at der er et stykke vej mellem producenterne og installatører og slutbrugere, hvilket gør, at viden om cybersikkerhed i produkterne kun langsomt udbredes.

Erkendelse af behovet for cybersikkerhed

Der er generelt en udbredt manglende bevidsthed i forhold til cyber- og informationssikkerhed, som går igen i forbindelse med alle former for digitaliseringsinitiativer. Denne manglende bevidsthed og awareness observeres også i installationsbranchen og i industrien.

Det er i denne forbindelse vigtigt at være opmærksom på, at cybersikkerhed er en forudsætning for digitalisering. Uden et passende niveau af cybersikkerhed vil digitaliseringen fejle pga. manglende robusthed i løsningerne og manglede tillid fra brugerne. Det er vigtigt, at der er fokus på cybersikkerhed, så digitaliseringen bliver vellykket, og risikoen for cyberangreb ikke hæmmer innovationen. Dette kræver, at der sker en ændring i opfattelsen af cybersikkerhed, så investeringerne i cybersikkerhed ikke blot betragtes som en ekstra omkostning, men i stedet som en faktor, der understøtter og muliggør en effektiv og hurtig digitalisering samtidig med, at den digitale investering beskyttes.

Der er en særlig udfordring på installationsområdet, da mange ikke betragter de indlejrede tekniske løsninger som egentlige it-systemer og derfor ikke er opmærksomme på, at de kan være sårbare overfor cyberangreb. Dette skyldes blandt andet, at der indtil nu har været relativt få sager, og at de faktiske hændelser med få undtagelser kun har fået begrænset opmærksomhed. Dette betyder, at der som regel ikke er noget fokus på enhedernes livscyklus, og hvornår de ikke længere opdateres fra producenten.

I industrien har digitaliseringen et kæmpe potentiale til at blive katalysator for massiv økonomisk vækst og nye innovative produkter og services. Imidlertid medfører det også, at løsningerne baseres på standard it-komponenter og en voldsom vækst i antallet af forbundne enheder samt forbindelser til internettet og forretningssystemer. Men flere OT-relaterede forbindelser til fremmede systemer gør også systemerne langt mere sårbare ikke bare i forhold til enheds- og operatør fejl, men også målrettede angreb og tilfældig malware. Disse angreb medfører ikke kun digitale skader, men øger også risikoen for skader på produkter, mennesker og udstyr i den fysiske verden. Det er vigtigt, at disse udfordringer erkendes, og cybersikkerhed bliver tænkt ind som en del af fundamentet i digitalisering i industrien.

Producenterne bag de løsninger og produkter, der kommer på markedet, vurderes aktuelt at være de mest aktive på cybersikkerhedsområdet. Især de større europæiske producenter beskrives som dem med størst fokus på sikkerhed, mens der er en tendens til, at særligt mange billigere IoT-produkter – primært til private – mangler basale sikkerhedsfunktioner. De fleste producenter vil naturligt nok hævde, at deres produkter er sikre, og at de har styr på sikkerheden, men dette dækker over store faktiske forskelle.

Distributørerne er ofte også ansvarlige for at videreformidle produktviden til de installatører, der køber produkter fra dem. Det er observationen, at distributørerne er opmærksomme på udfordringerne i forhold til cybersikkerhed og forsøger at videreformidle budskaberne, men de oplever ofte, at installatørerne ikke har interesse i cybersikkerhed, da de ikke vurderer, at det har nogen kommerciel værdi.

Rådgiveren er ofte kontaktpunktet mellem kunde og installatør. Det er umiddelbart indtrykket, at det manglende fokus på cybersikkerhed hos rådgiverne skyldes en kombination af manglende viden og kompetencer på området, samt at kunderne ikke stiller krav til cybersikkerhed.

Grundlæggende er installatørerne afventende, og så længe kunderne ikke direkte kræver sikkerhed i deres løsninger, har installatørerne heller ikke fokus på dét, fordi det ikke har nogen kommerciel værdi. Såvel det professionelle og forbrugermarkedet er drevet af et fokus på pris og funktionalitet. Det er dog vurderingen, at der er kommet en stigende awareness på sikkerhed blandt slutkunder, hvilket formodentlig vil øge efterspørgslen på sikre løsninger. Det er oplevelsen fra de afholdte workshops, at der er stor forskel på installatørernes indstilling i forhold til cybersikkerhed, og at de installatører, der arbejder mest med digitale løsninger, også har det største fokus på cybersikkerhed.

Det skal understreges, at den generelle bevidsthed omkring cyber- og informationssikkerhed har udviklet sig meget gennem de sidste 3-5 år blandt andet på grund af de mange ransomware-angreb, det store cyberangreb på Mærsk i 2017, fokus omkring ikrafttræden af EU's persondataforordning (GDPR), samt den nationale strategi for cyber- og informationssikkerhed fra 2018. Denne generelle større opmærksomhed ifht. cybersikkerhed gør også, at der er en voksende forståelse for vigtigheden af at prioritere cybersikkerhed.

Ansvaret for cybersikkerhed

Ansvaret for cybersikkerhed i de etablerede løsninger fremstår ikke klart placeret, og det virker som om, alle parter forventer, at nogle andre påtager sig ansvaret for cybersikkerheden.

Producenterne søger at fremstille produkter med indbyggede sikkerhedsfunktioner, men mener at ansvaret for, at de bliver anvendt korrekt, ligger hos enten installatørerne eller slutbrugerne.

Det betragtes ikke som et ansvar hos installatørerne at forholde sig til cybersikkerhed omkring installationerne, og i mange situationer er det først, når kunderne begynder at stiller krav, at installatørerne rent faktisk begynder at forholde sig til cybersikkerhed. Baseret på de afholdte workshops kan det virke som om, nogle installatører mener, at det er producenternes ansvar at levere produkter og løsninger, der er sikre, og når installationen er gennemført, er det i øvrigt slutkunden, der overtager ansvaret. I nogle situationer søger installatørerne at interagere med slutbrugerne omkring cybersikkerhed, men de oplever ofte, at dette er besværligt og derfor er dialogen begrænset.

Slutkunderne er ofte slet ikke opmærksomme på, at cybersikkerhed er et potentielt problem i forbindelse med f.eks. bygningsinstallationer, hvorfor dette område ofte ikke indgår i virksomhedernes risikostyring i forhold til cyber- og informationssikkerhed i øvrigt. Slutkunderne har desuden den opfattelse og forventning, at de produkter og løsninger, de får leveret og installeret, er sikre.

Hos flere aktører gives der udtryk for en stigende bekymring for og opmærksomhed på, at banker og forsikringsselskaber fremadrettet vil undersøge, hvem der er skyld i et angreb eller lækage, og at det i sidste ende vil medføre erstatningsansvar for installatøren.

Hvis installatøren kun er ansvarlig for selve installationen, skal installatøren sikre, at løsningen etableres i overensstemmelse med best-practice for cybersikkerhed. Det involverer f.eks., at passwords er skiftet fra defaultværdier, at der ikke er uhensigtsmæssige åbninger fra internettet, og at løsningen er opdateret med seneste softwareversioner. Dernæst er det vigtigt, at installatøren overdrager løsningen til slutkunden på en måde, så slutkunden er opmærksom på sikkerheden.

Det er desuden vigtigt at være opmærksom på, at der er stor forskel på, hvorvidt der arbejdes med professionelle slutkunder eller privatpersoner. De professionelle slutkunder køber typisk væsentlig større løsninger og besidder i mange situationer en god indsigt i den løsning, der anskaffes. Private slutkunder har sjældent den store faglige indsigt, dvs. deres primære fokus er som regel funktionalitet frem for cybersikkerhed.

Det er en udbredt opfattelse, bl.a. diskuteret på de afholdte workshops, at cybersikkerhed anses som et it-problem, der skal løses af slutkunden, og at der er ikke meget dialog omkring udfordringerne i den forbindelse. Det samme gør sig gældende i erhvervssammenhæng, hvor sikkerhed typisk betragtes som et problem for slutkundens it-afdeling.

En af grundene er manglende bevidsthed om udfordringerne, og samtidig kan der være udfordringer, når kunder, installatører, rådgivere og it-afdeling skal tale sammen. Ofte kommer de til dialogen med hvert deres udgangspunkt og referencerammer, herunder deres egen fagterminologi. Når dialogen sker med forskelligt udgangspunkt, kan det være svært at ramme en faktisk fælles forståelse.

Da slutkundens it-afdeling ofte betragtes som besværlig og forsinkende, bliver de ikke nødvendigvis involveret i et installationsprojekt. Dog er der især på området for industri-automatisering et udtrykt ønske fra installatørerne om at samarbejde med it-afdelingen. Her har it-afdelingen dog ikke altid forståelse for, at de ikke skal have ejerskabet over udstyret.

I sidste ende vil det altid være slutbrugeren, der har ansvaret for den købte løsning. Fremadrettet vil ansvaret for f.eks. softwareopdatering ligge hos slutbrugerne, mens installatøren typisk har stået for det i forbindelse med installationen.

Når installationen er færdiggjort, vælger nogle kunder at give installatøren mulighed for remote support. Selvom nogle installatører går i dialog med kunderne om risikoen ved dette og en eventuel meromkostning ved at gøre det på en sikker måde, vægtes funktionalitet og bekvemmeligheden i de fleste tilfælde højere hos kunden. Ofte ses også, at åbninger, der er er lavet ad hoc under en installation, ikke bliver lukket, når løsningen overdrages til slutkunden. Derudover antages det ofte, at de løsninger, som producenterne stiller til rådighed, er tilstrækkeligt sikre.

I lyset af at kunder og installatører formoder, at de udbudte løsninger er sikre – og at dette er en forudsætning for etablering af sikre løsninger – har producenterne en central rolle i forhold til cybersikkerhed. Det er således kritisk, at producenterne har fokus på en ordentlig proces for produkternes livscyklus, så der er fastsat en klar levetid, og at produktet i denne levetid bliver forsynet med opdateringer, som adresserer de sårbarheder, der bliver fundet.

Tilgangen til cybersikkerhed varierer imidlertid meget fra producent til producent.

Ikke alle producenter vælger at prioritere arbejdet med cybersikkerhed. En af årsagerne til det manglende fokus er, at producenternes forretningsmodel er baseret på engangssalg. De har således ikke tradition for at levere produkter med lang levetid, og derfor vedligeholder de ikke produkterne – en problemstilling der særligt ses i forbrugersegmentet. Når der samtidig ikke er noget krav fra slutbrugerne, er der intet økonomisk eller praktisk incitament til at fokusere på cybersikkerhed.

Det skal bemærkes, at alle de større og seriøse udbydere specielt af professionelle løsninger i dag har et stort fokus på cybersikkerhed og fremstiller produkter med fornuftige

sikkerhedsfunktioner, mens produkter med dårlig sikkerhed primært kommer fra mindre producenter, der laver simple produkter rettet mod privatmarkedet.

Det er indtrykket, at de store producenter ønsker at fremstille sikre produkter, blandt andet for at beskytte deres varemærke og renomme. Desuden er det opfattelsen, at stadig flere producenter anser cybersikkerhed som en potentiel konkurrenceparameter.

Forretningsmodeller i branchen

Installatørerne oplever ikke, at kunderne efterspørger mere intelligente digitale løsninger – og set fra installatørernes side er disse løsninger ofte mere til besvær, da de er mere komplekse og dermed øger omkostningerne. Ganske få installatører gør en systematisk og aktiv indsats for at promovere digitale løsninger til slutkunderne. Enkelte nicheinstallatører arbejder aktivt med digitale løsninger som grundlaget for deres forretning og værdiskabelse. Hovedparten af installatørerne arbejder dog stadig med et analogt mindset og anser den digitale del af løsningerne, som noget slutkunden eller dennes it-leverandør selv må varetage. Enkelte installatører giver dog udtryk for, at de i forbindelse med opsætning af digitale løsninger foretager nogle simple sikkerhedsforanstaltninger jf. best practice, blandt andet i form af ændring af standard-passwords samt rådgivning af kunderne om skift af disse.

Producenterne laver i dag både teknisk meget avancerede løsninger, der kræver professionel hjælp, samt "plug'n'play"-løsninger, som kunderne selv kan installere. Sidstnævnte løsninger markedsføres bredt fra forskellige online og detailbutikker som smarthome-produkter til intelligent styring af hjemmet. Mange af løsningerne supplerer eksisterende installationer eller fungerer ovenpå, f.eks. ved at tilbyde intelligent styring af lys og varme samt integration med eksempelvis stemmestyring og remote kontrol via en mobilapp. Alt dette kan etableres af forbrugeren selv, uden at der er behov for besøg af en installatør.

På nuværende tidspunkt er der plads til begge løsningstyper, men på sigt vil producenterne formodentlig satse på det, der er mest rentabelt for dem. Her har installatørerne et valg: Vil installatøren fortsat nøjes med at arbejde analogt, eller vil installatøren være en aktiv medspiller, der er med til at levere løsningen, skabe værdi for kunden og dermed sikre en god forretning?

Der fornemmes en vis frustration hos producenterne over, at deres nye og innovative løsninger ikke bliver præsenteret for kunderne og markedet. Hvis distributører og installatører ikke tager nye løsninger hurtigt nok til sig, vil reaktionen fra producenterne formodentlig være, at de begynder at markedsføre og sælge deres løsninger direkte til kunderne.

Dette er blandt andet muligt, fordi online kanaler nemt skaber en kortere vej mellem producent og forbruger.

Skal der være et marked til de mere avancerede løsninger, der kræver en installatør, kræver det, at kunderne kender disse muligheder og oplever en tilstrækkelig høj værdi ved dem.

Dét kræver, at der bliver investeret i uddannelse, så videns- og kompetenceniveauet hos installatørerne øges. Dernæst er det nødvendigt at gå i dialog med kunderne om de løsninger, der skaber værdi for dem, og italesætte værdien af den professionelle installatørs arbejde i den forbindelse. I forlængelse af dét, vil det formodentlig være de installatører, der formår at opbygge en serviceforretning, der er bedst rustet til den digitaliserede fremtid.

Her er det vigtigt at forstå, at arbejdet med cybersikkerhed bygger ovenpå arbejdet med digitale løsninger generelt. Cybersikkerhed er en forudsætning for digitalisering, og uden en basal forståelse for digitalisering er det ikke muligt at arbejde med cybersikkerhed. Digitaliseringen medfører således et behov for at arbejde på tværs af fagområder for at udnytte viden. I installationsbranchen kunne det f.eks. ske ved, at man hyrer it-folk ind, der kan berige forretningen med den nødvendige viden om it- og cybersikkerhed.

Kompetencer

It- og cybersikkerhed er ikke et element på grunduddannelserne, og der mangler efter- og videreuddannelse på området. Det betyder, at der på nuværende tidspunkt er en arbejdsstyrke, der ikke altid har forståelse for, hvilke konsekvenser deres arbejde kan have.

Der er et stort udbud af efter- og videreuddannelse i branchen, men dette er primært baseret på specifikke produkter eller producenter og er ikke generelt teknologiorienteret.

Der er igangsat flere initiativer i forhold til uddannelse. Ønsket er at basere mest muligt på standarder, som det er tilfældet mange andre steder i branchen.

Udbuddet af og efterspørgslen på uddannelse er et spørgsmål om økonomi; det koster at udvikle en uddannelse, og branchen skal se meningen med uddannelsen for at sende medarbejderne på den.

Et andet niveau af kompetencer er de kommunikative og kommercielle kompetencer til at formidle budskaber omkring cybersikkerhed til slutbrugerne på en effektiv og værdibaseret måde, så slutbrugerne forstår og anerkender behovet for cybersikkerhed. Hvis installatørerne ikke kan formidle budskabet omkring cybersikkerhed til slutkunderne, kommer der ikke til at ske meget på området. Der er ikke identificeret nogen undervisningsinitiativer eller lignende, der adresserer dette behov.

Teknologisk arv

Den digitale udvikling og omstilling i installationsbranchen er hæmmet og udfordret af, at løsningernes levetider er ganske lang. Ofte kan en el- eller vvs-installation leve i årtier. Et eksempel er de gamle elinstallationer baseret på stofledninger, som stadig findes i mange gamle lejligheder og huse.

Det medfører, at mange digitaliseringsløsninger etableres sammen med gamle installationer, som på ingen måde er designet til at være en del af en digitaliseret intelligent installation. I mange situationer er dette ikke et problem, men ofte kan gamle styringssystemer ikke sikres tilstrækkeligt til, at de kan digitaliseres på en sikker måde.

Mange af de tidlige kommunikationsprotokoller til intelligente installationer, som f.eks. traditionel KNX, har ingen eller stærkt mangelfulde sikkerhedsfunktioner og er sårbare overfor en lang række angreb som f.eks. aflytning og genafspilning af kommunikationen, manglende kryptering af kommunikationen m.m. Sikkerhed er således ikke tænkt ind i de gamle protokoller, da sikkerhed ikke var et væsentligt problem, da de blev udviklet.

Mange moderne løsninger er fortsat baseret på eller understøtter de gamle kommunikationsprotokoller. I forhold til f.eks. KNX er standarden i dag suppleret med KNXnet/IP Secure, der adresserer mange af de oprindelige svagheder i protokollen. Men selv disse nye versioner har svagheder. Desuden kan en protokol som KNXnet/IP Secure kun anvendes sammen med nyere udstyr, der understøtter den, hvorfor nyt udstyr alligevel ofte anvender den gamle usikre KNX-protokol for at være kompatibelt med gammelt udstyr.

Dette illustrerer nogle af de udfordringer, som installationsbranchen har og kommer til at have med hensyn til den fremtidige levetid på digitale løsninger. Følgende citat fra "KNX Systems Specification" illustrerer, hvordan sikkerhed er baseret på en række uholdbare antagelser: "For KNX, security is a minor concern, as any breach of security requires local access to the network". I dag må det desværre antages, at netværk kan blive kompromitteret, hvorfor antagelsen ikke holder.

Cybersikkerhed i industrien

De personer, der er involveret i implementeringen af nye løsninger i industrien, har normalt kun kendskab til enten IT- eller OT-området og mangler tværgående viden og kompetence. Dertil kommer, at der ofte mangler tilstrækkelig ekspertise og opmærksomhed i forhold til cyber- og informationssikkerhed. Det sinker etableringen af passende og nødvendige cybersikkerhedsforanstaltninger.

Etablering af cybersikkerhed i forhold til Industri 4.0 kræver kompetence på en række områder, blandt andet netværkssikkerhed, indlejrede systemer, og samspillet mellem OT og IT-sikkerhed. Det er vanskeligt at finde kvalificerede specialister indenfor it-sikkerhed og specifikt på OT-området.

Ofte kommer digitale løsninger i industrien "snigende", det vil sige uden, at de er en del af en bevidst og planlagt strategi. Dét betyder, at der ikke bliver fastlagt og vedtaget stringente processer og politikker i forhold til etablering, implementering og vedligeholdelse af løsningerne. OT-syste-

met bliver af ledelsen ofte opfattet som et isoleret system, hvorfor der ikke er fokus på det i forhold til it-sikkerheden generelt.

Der er generelt kommet et stigende fokus på OT/ICS-sikkerhed, hvilket medfører, at der aktuelt bliver fundet mange flere sårbarheder i OT- og IIoT-produkter end tidligere. Dermed har potentielle angribere langt flere metoder, de potentielt kan anvende i et angreb. Det betyder, at det er nødvendigt med et større fokus på opdateringer end tidligere – eller at sårbarhederne håndteres på anden vis.

Ansvaret for cybersikkerhed i industrien er langt fra altid klart placeret i organisationen. Observationen er, at de ansvarlige for produktionen ofte har den opfattelse, at cybersikkerhed håndteres af it-afdelingen, mens it-afdelingen ikke ved noget om OT-systemer og derfor ikke mener, at det kan være deres ansvar. Denne problemstilling ses desværre ofte ved introduktionen af ny teknologi i krydsfeltet mellem forskellige ansvarsområder.

Mange steder mangler OT-sikkerheden at blive forankret ordentligt. Det betyder, at væsentlige elementer i forhold til sikkerhed, blandt andet overvågning i forhold til sikkerhedshændelser, evnerne og beredskabet i forhold til hændelseshåndtering samt det generelle beredskab, ofte ikke er ordentlig på plads og gennemtestet.

Cybersikkerhed i industrien er udfordret af, at der ikke findes entydige regler, standarder og retningslinjer for, hvordan sikkerhed skal implementeres. Der findes således en lang række forskellige anbefalinger i forhold til såvel udvikling af produkter og applikationer som implementering af løsningerne. Det medfører, at det kan være vanskeligt og uoverskueligt at finde ud af, hvilke baselines, vejledninger, standarder og tjeklister, man skal anvende.

Hvad er sikkerhed?

Sikkerhed beskriver både den situation, hvor man er uden for fare, men også de forholdsregler man kan tage for at undgå at ende i en faretruende situation.

I it-sammenhæng har målet med sikkerhed traditionelt været at sikre fortrolighed, integritet og tilgængelighed. Målet opnås gennem en afbalanceret kombination af teknologi, processer og mennesker.

Hidtil har it-sikkerhed primært haft fokus på beskyttelsen af kontor-it-systemer, men med udbredelsen af blandt andet IoT er det nødvendigt også at fokusere på alle de forbundne og intelligente systemer, der på en eller anden måde har forbindelse til den fysiske verden. Dette gør, at målet med sikkerhed udvides fra at sikre fortrolighed, integritet og tilgængelighed til også at omfatte beskyttelse mod fysiske skader på materiel og personer.

En lang række af de alvorlige brud på sikkerheden vi har set gennem de senere år, skyldes en kombination mellem uhensigtsmæssig adfærd fra brugerne og sårbar teknologi. Årsagen er, at selvom løsninger forsøges bygget så robuste som muligt, vil det i praksis oftest være umuligt at bygge systemer, der kan håndtere alle former for uhensigtsmæssig adfærd. Derfor skal sikkerhed etableres i en sammenhæng mellem mennesker og teknologi, samtidig med at der bygges en sikker forbindelse mellem den digitale og fysiske verden, således at der etableres teknologiske løsninger med passende robusthed og tillid.

Hvad skal man gøre?

Der findes en række forskellige mulige tiltag i forhold til cyber- og informationssikkerhed. En række tiltag er generelle, mens der også findes en række særlige tiltag, der adresser nogle af de specifikke sikkerhedsmæssige udfordringer i forhold til forbundne intelligente enheder.

Når man betragter forbundne intelligente produkter, kan de sikkerhedsmæssige tiltag betragtes på tre forskellige stadier:

- Udvikling: Når produktet udvikles og fremstilles
- Installation: Når produktet installeres og integreres
- Anvendelse: Når produktet anvendes

Bemærk, at nedenstående tiltag primært er medtaget for at eksemplificere nogle af de best-practice anbefalinger, der findes. Det er ikke en komplet liste over mulige og/eller nødvendige tiltag i forhold til cyber- og informationssikkerhed i forbundne intelligente enheder.

Stadie	Behov i relation til cybersikkerhed	Tjekliste
Udvikling	**Udviklingsproces**. Sikkerhed skal være en integreret del af designprocessen for alle netværksforbundne enheder. Løsningen på sikkerhedsproblemerne designes i de tidlige faser af produktets eller servicens livscyklus. Som en generel regel skal sikkerhedsarkitekturen for en løsning defineres og dokumenteres tidligt. Dette er den praktiske implementering af "Security by Design" fremgangsmåden. **Hardware og software**. Når man skal udvikle en sikker enhed, er der en række standardkrav og funktioner, som skal være understøttet i den valgte hardware og software.	**Sikkerhed i udviklingsprocessen** • Designfase • Udviklingsfase • Testfase **Sikkerhedsfunktioner i hardware og software** • Sikkerhedsaudit • Beskyttelse af kommunikation • Kryptering • Databeskyttelse • Identifikation, autentificering og autorisation • Selvbeskyttelse
Anskaffelse	**Sikkerhedskrav**. Krav til cybersikkerhed skal inkluderes i kravspecifikationsprocessen fra starten. Samarbejd med leverandører og sikkerhedspartnere for at få prioriteret sikkerhed som en integreret del af enhver løsning. Som en del af anskaffelsen skal det defineres, hvordan leverandøren skal integrere til eksisterende netværk, f.eks. ved at bruge separate netværkssegmenter. Vær opmærksom på, at der skal være afsat budget til håndtering af sikkerhed i hele løsningens livscyklus. **Vurdering af løsning**. Der skal etableres en konsistent metode til evaluering af sikkerhedsleverandører og deres løsninger. Foretrukne leverandører bør være dem, der har et livscyklusprogram, implementerer sikkert design og kodningspraksis, samt har en moden proces til sårbarhedsstyring, så det sikres, at produktsårbarheder opdages, afhjælpes og rettes rettidigt. Accepter, at forretningsmæssige prioriteringer – som omkostninger – kan medføre, at man vælger ikke-optimale løsninger. Der skal etableres en metode, der evaluerer sikkerhedsmæssige implikationer og integrationer mellem ældre og nye systemer, men giver fleksibilitet til ekstra sikkerhedskontroller, som kan anvendes for at minimere identificerede risici.	**Sikkerhedskrav** • Sikkerhedspolitik • Compliance • Planlægning & design **Vurdering af løsning** • Risikostyring ift. tredjepart • Risikovurderinger
Installation	**Indbygget sikkerhed**. Forstå leverandøranbefalinger for, hvordan enheden installeres og implementeres sikkert, og samarbejd med it-sikkerhedsafdeling for at følge disse retningslinjer. Overvej også, hvordan yderligere kontroller ud over leverandøranbefalinger kan tilføjes baseret på de identificerede sikkerhedskrav. De indbyggede sikkerhedsfunktioner er vigtige, men hvordan en løsning installeres og implementeres – især i forhold til netværksdesign og fjernadgangsfunktioner – er afgørende for minimering af risikoen.	**Indbygget sikkerhed** • Netværkssikkerhed • Sikkerhedsgateway • Netværkssegmentering • Beskyttet infrastruktur • Sikker parring og forbindelse • Fjernadgang
Anvendelse	**Regelmæssig opdatering**. Sørg for at have en vedligeholdelsesaftale på softwaren og gerne en proaktiv serviceaftale med din integrator, så dine enheder anvender de seneste softwarerevisioner. Vær desuden opmærksom på, hvor længe leverandøren vil frigive sikkerhedsopdateringer og support til enhederne, og sørg for, at du har en strategi til udskiftning af enheden, inden supporten stopper og enheden går end-of-life. **Test, overvågning og response**. Kend din risiko. Oprethold et overblik over, hvilke enheder der er forbundet. Få udviklet og implementeret en metode til vurdering af alle løsninger. Test regelmæssigt sikkerheden og de tekniske sårbarheder. Overvåg kontinuerligt enheden for tegn på kompromittering og foretag evt. nødvendigt incident response arbejde.	**Beskyttelse af dataudveksling** • Autentifikation • Sikre adgangsrettigheder • Sikkerhedsgateway • Kryptering **Operationel sikkerhed** • Sårbarhedsscanning • Sikkerhedsopdateringer • Beskyttelse af API Interfaces • Værktøjer til styring af sikkerheden • Asset Management • Sikkerhedsovervågning • Test af sikkerheden (Red Team-øvelser) • Threat Intelligence • Hændelseshåndtering – Incident Response • Træning og øvelser **Kontrol af brugerdata** • Sikker backup • Sletning af data

Konklusion og anbefalinger

Som beskrevet ovenfor er der en lang række udfordringer i forhold til arbejdet med cybersikkerhed. Ingen af disse udfordringer er simple problemstillinger, der umiddelbart kan løses med enkle midler, men kræver derimod en langsigtet og strategisk indsats hos installationsbranchen.

Det er vigtigt at understrege, at cybersikkerhed er en nødvendig forudsætning for at kunne levere robuste digitaliserede løsninger, og at cybersikkerhed derfor skal ses i forbindelse med sådanne.

Cybersikkerhed er et komplekst område og har kun en værdi, når det indgår som en integreret del i samlede, avancerede digitale løsninger.

Nødvendig erkendelse af at sikkerhed er forudsætningen for digitalisering

Som beskrevet tidligere i rapporten bliver tekniske løsninger i installationsbranchen og industrien i stadig stigende grad digitaliseret. En nøgleforudsætning for denne udvikling er, at de digitale løsninger er robuste, og at der er tillid til dem. Krav til cyber- og informationssikkerhed er derfor uundgåelige i relation til de digitale løsninger. Hvis ikke sikkerheden er på plads, vil digitaliseringen mislykkes.

Heldigvis er der en generelt stigende opmærksomhed på vigtigheden af cyber- og informationssikkerhed som et nøgleelement i digitaliseringen. Der er imidlertid stadig mange situationer, hvor der mangler forståelse eller erkendelse, og de sikkerhedsmæssige udfordringer derfor ikke bliver håndteret i tilstrækkeligt omfang.

Det er vigtigt at understrege, at hvis ikke det lykkes at løfte sikkerhedsudfordringerne, vil det ikke være muligt at høste alle gevinsterne ved digitaliseringen.

Nogle af aktørerne i installationsbranchen har allerede fokus på cyber- og informationssikkerhed, men der er desværre mange installationsvirksomheder, der endnu ikke har erkendt behovet. Det er nødvendigt, at alle involverede interessenter erkender behovet, da det ellers ikke er muligt at sikre, at de digitale løsninger har et passende sikkerhedsniveau hele vejen igennem fra planlægning, over implementering og i drift.

Første led i at løfte niveauet i forhold til cyber- og informationssikkerhed er således en erkendelse af udfordringerne, og at alle involverede interessenter forstår problemstillingen. Dette kræver et konstant fokus på en kontinuerlig informations- og oplysningsindsats rettet mod såvel producenter, distributører, installatører og slutkunder.

Erkendelsen er nødt til at starte og være forankret hos virksomhedernes ledelser. Det er ledelsen, der er ansvarlig for prioriteringen og skabelsen af en kultur, hvor der er fokus på cybersikkerhed. Ledelserne er derfor nødt til strategisk at beslutte, at der skal være fokus på cybersikkerhed.

Bestyrelsesforeningens Center for Cyberkompetencer har udarbejdet en række vejledninger, der har til formål at øge opmærksomheden over for cyberrisiko og at styrke kompetencerne inden for cybersikkerhed i danske bestyrelser og direktioner.

På baggrund af dette har Dubex følgende understøttende anbefalinger og bemærkninger:

- Dubex anbefaler, at ledelserne hos installationsvirksomhederne investerer tid og ressourcer i at sætte sig ind i og forstå udfordringerne omkring cybersikkerhed, herunder forstå hvor problemstillingen er relevant for den enkelte virksomhed og den type opgaver og projekter, som virksomheden gennemfører.

- Dubex anbefaler, at installationsvirksomhederne, evt. sammen med deres komponentleverandører, gennemgår de forskellige digitale løsninger, som virksomheden allerede i dag arbejder med, og vurderer, hvor der kan være problemstillinger i forhold til cybersikkerhed, som bør håndteres.

- Dubex anbefaler, at installationsvirksomhederne fremadrettet prioriterer og holder fokus på cybersikkerhed som en del af de kompetencer, virksomheden skal have.

- Dubex foreslår, at TEKNIQ Arbejdsgiverne iværksætter en række informationsinitiativer overfor deres medlemmer, hvor der sættes fokus på de ændringer, som digitaliseringen medfører, og nødvendigheden af at fokusere på cybersikkerhed. Initiativerne kan f.eks. være afholdelse

af konferencer og gå-hjem-møder, kommunikation i medlemsblade, udgivelse af vejledninger mv. Det er vigtigt, at aktiviteterne rammer bredt, så de installationsvirksomhederne, der i dag ikke arbejder med cybersikkerhed, får det sat på agendaen.

- Dubex foreslår, at TEKNIQ Arbejdsgiverne indgår i samarbejde med relevante myndigheder og andre organisationer, der kan være med til at fremme det overordnede budskab.

Ansvarsfordeling

Det diskuteres meget, hvem der har ansvaret for cyber- og informationssikkerhed indenfor installationsområdet. Det er således indtrykket, at ingen aktører ønsker at have ansvaret for cybersikkerhed, hvilket er ganske forståligt, når behovet og kravene til cyber- og informationssikkerhed ikke er mere bredt erkendt og forankret – og cybersikkerhed i øvrigt anses som dyrt og besværligt.

Det vurderes ikke, at ansvaret for cyber- og informationssikkerhed kan placeres ét enkelt sted. Ansvaret skal derimod løftes i et samarbejde mellem alle interessenter i branchen. Således har producenter, distributører, installatører og slutbrugere alle et ansvar for deres del af området.

Sikkerhed skal først og fremmes være indbygget i produkter og løsninger fra starten. Det er ikke en feature, der kan tilføjes efterfølgende, men et element der skal være en del af hele produktets livscyklus. Producenterne har således et ansvar for, at sikkerhed er en indbygget og integreret del af deres produkter. Dette ansvar skal løftes i hele produktets levetid, hvor det er vigtigt, at produktet vedligeholdes, således at nye sårbarheder og fejl rettes.

Distributører og installatører har også et ansvar for, at produkterne de vælger har passende cybersikkerhedsniveau og en veldefineret livscyklus. De skal samtidig fravælge de usikre produkter for derigennem at skabe et kommercielt pres for de mest sikre løsninger.

Installatøren har også et ansvar i forhold til at sikre, at de løsninger, der etableres hos slutkunderne, er etableret med fokus på sikkerhed, og at de sikkerhedsfunktioner, der er i produkterne, rent faktisk bliver udnyttet.

I sidste ende overtager slutbrugeren ansvaret for den købte løsning. Dét stiller krav til, at slutbrugernes viden er up-to-date. Her er det altafgørende, at slutkunden forstår, at de har overtaget ansvaret og har tillid til installatøren og dennes viden og kompetencer. Det betyder, at installatøren skal være i stand til at tage dialogen med kunden og evt. tilbyde en service, der fremadrettet sikrer et højt cybersikkerhedsniveau.

På baggrund af dette har Dubex følgende understøttende anbefalinger og bemærkninger:

- Dubex anbefaler, at installationsvirksomhederne gennemgår de digitale løsninger, der arbejdes med, med henblik på at sikre, at den installation og opsætning, der foretages, sker med passende viden om og fokus på cybersikkerhed.

- Dubex anbefaler, at installationsvirksomhederne i deres overdragelse til slutkunden sikrer, at der sker en tydelig overdragelse i forhold til cybersikkerhed. Det vil sige, at slutkunden gøres opmærksom på de potentielle sikkerhedsudfordringer, samt at ansvaret herefter ligger hos dem. Dette kan f.eks. ske ved, at der udfærdiges et overdragelsesdokument.

- Dubex anbefaler, at TEKNIQ Arbejdsgiverne medvirker til at synliggøre, hvordan ansvaret for cybersikkerhed er fordelt på tværs af branchen. Dette kan f.eks. ske ved udgivelse af en simpel pjece, som illustrerer placering af opgaver og ansvar, og som medlemsvirksomhederne kan bruge i forhold til kommunikationen med deres slutkunder.

- Dubex anbefaler, at TEKNIQ Arbejdsgiverne udarbejder tjeklister/skemaer, som medlemmerne kan bruge ved afslutning og overdragelse af installationsopgaver, der indeholder digitale løsninger, så der sker en synlig og konsistent overdragelse af ansvar til slutkunden.

- Dubex anbefaler, at TEKNIQ Arbejdsgiverne medvirker til at facilitere et bredere samarbejde på tværs i branchen med fokus på informationsudveksling omkring cybersikkerhed for at tydeliggøre, hvad de enkelte aktører bidrager med.

Forretningsmodeller

Kravene om cyber- og informationssikkerhed giver også anledning til overvejelse af mulighederne for nye eller ændrede forretningsmodeller.

Som installatør er man derfor nødt til at have fokus på de muligheder, som slutkunderne ikke umiddelbart kan få andre steder. Dette er primært de mere avancerede og integrerede løsninger, som ikke kan købes som simple forbruger-"plug-and-play"-produkter.

Den lette adgang til prosumer-produkter betyder, at branchen skal være bedre til at værdisætte sig selv overfor kunderne for at forblive synlige og relevante. Privatkunderne vurderes i stigende grad at gøre brug af "plug-and-play"-løsninger, hvilket langt hen ad vejen kan gøres uden hjælp fra en installatør. Installatørerne bør overveje, med hvad og hvordan de kan være relevante overfor privatkunderne.

Som installatør bør fokus også være på erhvervskunderne og rådgivning om valg af produkter samt etablering af sammenhængende løsninger med fokus på blandt andet cybersikkerhed.

Da cybersikkerhed er en proces, og løbende vedligeholdelse er en nødvendig del af processen, kan det med fordel overvejes, om installatøren kan tilføje merværdi til leverancen i form af f.eks. serviceaftaler, som blandt andet omfatter cybersikkerhedsydelser.

Salg og leverance af avancerede løsninger kræver mere af installationsvirksomhederne, da slutkunderne ikke blot køber ind på denne type løsninger. Det betyder, at installationsvirksomhederne er nødt til at kunne udarbejde og designe sådanne løsninger og forklare og formidle værdien til slutkunderne.

Af andre forretningsmodeller, der kan overvejes, er leverance af løsninger på en "as-a-service"-model, hvor overvågning, fjernadministration, vedligehold og regelmæssige gennemgange leveres som en del af en samlet servicepakke, mens slutbrugeren blot betaler et samlet "abonnement" på løsningen.

På baggrund af dette har Dubex følgende understøttende anbefalinger og bemærkninger:

- Dubex anbefaler, at installationsvirksomhederne indgår i en rådgiverdialog med deres kunder omkring cybersikkerhed i forbindelse med digitaliserede løsninger, og bruger cybersikkerhed som et værktøj til at værdisætte deres leverancer og kompetencer og dermed komme tættere på kunderne.

- Dubex anbefaler, at installationsvirksomhederne, i forbindelse med tiltag omkring system- og løsningssalg, hvor digitalisering indgår, gennemgår, hvordan cybersikkerhed kan gøres til en integreret og værdisat bestanddel af løsningen.

- Dubex foreslår, at installationsvirksomhederne forfølger mulighederne for at udbygge deres nuværende serviceforretning med ydelser omkring vedligeholdelse af digitale løsninger med henblik på at holde cybersikkerheden vedlige.

- Dubex foreslår, at installationsvirksomhederne søger et tættere samarbejde med producenter og distributører for i samarbejde med dem at kunne markedsføre og sælge avancerede og værdiskabende samlede digitale systemløsninger

- Dubex foreslår, at TEKNIQ Arbejdsgiverne overvejer, hvordan de bedst kan understøtte deres medlemmer i forbindelse med ændrede forretningsmodeller, som i højere grad er baseret på salg af services. Dette kan f.eks. ske i forlængelse af de foreslåede initialiver omkring cybersikkerhedsanbefalinger til slutbrugere, hvor løbende vedligeholdelse kunne indgå.

Kompetencer

Efterhånden som de løsninger, installationsbranchen arbejder med, bliver digitaliserede, ændres værdiskabelsen, og det bliver i stadig højere grad de digitale løsninger, som skaber værdi for kunderne. De digitale løsninger bliver også i stigende omfang selve løsningen, dvs. det er er den funktion, som den digitale løsning giver, slutkunden rent faktisk vælger.

For fortsat at være en relevant interessent for slutkunden er installationsbranchen nødt til at tilegne sig de digitale kompetencer, der er nødvendige for etableringen af digitale løsninger. Som nævnt tidligere er cyber- og informationssikkerhed et krav i denne forbindelse, hvorfor generelle digitale kompetencer skal understøttes af cyber- og informationssikkerhedskompetencer.

Cyber- og informationssikkerhed kan blive meget kompliceret, da det udover den lokale installation også kan involvere f.eks. netværk, cloud-løsninger, mobilapps, komplekse integrationer mv., som alt sammen stiller krav til installatørens viden på området. Installatørerne er derfor nødt til at sikre sig adgang til disse kompetencer, hvilket enten kan ske via uddannelse af egne medarbejdere, ansættelse af medarbejdere med rette kompetencer eller samarbejder.

Et evt. samarbejde fritager ikke installatørerne fra at have en grundlæggende og tilstrækkelig viden omkring cyber- og informationssikkerhed. Derfor er der behov for et generelt kompetenceløft i installationsbranchen både uddannelsesmæssigt i grunduddannelserne og indenfor efter- og videreuddannelsesområdet samt via rekruttering af andre typer medarbejdere med disse kompetencer.

Den enkelte virksomhed har et ansvar for at sikre, at deres ansatte har den nødvendige viden og kompetencer til at udføre de opgaver og projekter, som virksomheden gennemfører. Det betyder blandt andet, at virksomhederne har et ansvar i forhold til at sikre passende efteruddannelse af deres medarbejdere, herunder også i relation til cybersikkerhed.

Endelig er det nødvendigt, at installationsvirksomhederne styrker deres rådgivningskompetencer, så de bliver i stand til at italesætte og værdisætte cybersikkerhed som en del af løsningssalget, da det ikke kan forventes, at kunderne automatisk efterspørger digitale løsninger og herunder cybersikkerhed.

Det bemærkes, at det ikke er realistisk, at installationsvirksomhederne bliver cybersikkerhedseksperter, og det forventes, at der stadig vil være brug for egentlige sikkerhedsspecialister. Der er imidlertid behov for en basal forståelse for cybersikkerhed, så installatøren kan lave en simpel installation, der lever op til minimumskrav i forhold til cybersikkerhed.

På baggrund af dette har Dubex følgende understøttende anbefalinger og bemærkninger:

- Dubex anbefaler, at installationsvirksomhederne gennemgår kompetencerne hos deres nuværende medarbejdere og derefter laver en plan for et evt. nødvendigt kompetenceløft på tekniske kompetencer indenfor digitalisering og cybersikkerhed.

- Dubex anbefaler, at installationsvirksomhederne også styrker deres kommercielle kompetencer i forhold til system- og løsningssalg – og herunder cybersikkerhed – så installationsvirksomhederne bliver i stand til at tage en kvalificeret rådgivningsbaseret dialog med kunderne.

- Dubex anbefaler, at installationsvirksomhederne overvejer at ansætte medarbejdere med andre kompetencer, f.eks. fra it-branchen, for på den måde at styrke system- og løsningssalget.

- Dubex anbefaler, at TEKNIQ Arbejdsgiverne medvirker til etablering af passende efteruddannelsestilbud til deres medlemsvirksomheder. Det anbefales, at det overvejes, hvordan der kan tilbydes efteruddannelse på både kommercielt og teknisk niveau.

- Dubex anbefaler, at TEKNIQ Arbejdsgiverne hjælper med at sætte fokus på, hvordan andre medarbejderprofiler kan medvirke til en højere værdiskabelse.

Cybersikkerhed i industrien

Beskyttelse af de digitale løsninger indenfor Industri 4.0 og IIoT-området er en kompleks opgave, der kræver en kombination af forskellige tiltag og initiativer indenfor områderne mennesker, processer og teknologi.

De følgende anbefalinger omfatter de overordnede forhold i forbindelse med etablering af rammerne omkring cybersikkerhed i industrien.

En grundlæggende forudsætning for etablering af cybersikkerhed i industrien er erkendelsen af behovet for cybersikkerhed. De relevante aktører er nødt til at få en forståelse for de potentielle trusler, de særlige sikkerhedsmæssige udfordringer i forhold til produktion samt de metoder og forudsætninger, der skal til for at etablere et passende niveau af cybersikkerhed.

Behovet for personer med sikkerhedskompetencer i forhold til industrien og forståelse for de særlige udfordringer indenfor industrien omfatter både de medarbejdere, der står for de tekniske løsninger, og awareness hos ledelserne. Det er således vigtigt, at der sker en bred kompetenceudvikling, som med fordel kan understøttes, blandt andet af passende uddannelses- og undervisningsinitiativer. Initiativerne bør ramme bredt, så der tilbydes relevant industrirettet uddannelse i cybersikkerhed – både som elementer i tilbudt grunduddannelse og som del af mulighederne for efteruddannelse.

Derudover er det vigtigt, at der etableres samarbejde og vidensdeling på tværs af IT- og OT-områderne. Almindelige it-systemer og systemer til industriautomatisering bliver i stigende omfang integreret og er baseret på samme teknologier. Mange af de trusler, der eksisterer i forhold til industrien, stammer fra og/eller er identiske med truslerne i forhold til normale it-systemer. Etablering af cybersikkerhed skal derfor ske på tværs af systemerne, hvis det skal være effektivt.

Udgangspunktet for investeringer i cybersikkerhed bør være den forretningsmæssige understøttelse af virksomhedens mål og ikke et ensidigt fokus på kun at forebygge tab. Det er først, når investeringerne bliver sammenkædet med forretningen, at man kan foretage en passende og korrekte prioritering af investeringerne omkring cybersikkerhed.

I betragtning af kompleksiteten og omfanget af industriautomatisering er der ingen løsning, der passer til alle virksomheder i forhold til IoT og Industri 4.0-sikkerhed. Det er et spørgsmål om at kombinere løsninger og sikre, at der bliver taget højde for fleksibilitet, brugervenlighed og udvidelsesmuligheder uden at gå på kompromis med sikkerheden.

På baggrund af dette har Dubex følgende understøttende anbefalinger og bemærkninger:

- Det er vigtigt, at cybersikkerhed i industrien sker på baggrund af en struktureret proces, der blandt andet indeholder følgende aktiviteter:
  - Gennemgang og identifikation af organisationens brug af OT
  - Identifikation af hvem der er ansvarlig for risikostyring for de områder, hvor der anvendes OT
  - Udarbejdelse af en samlet plan for en sammenhængende risikovurdering af både OT- og IT-anvendelsen
  - Gennemførelse af en OT/IT-risikovurdering
  - Etablering af de organisatoriske og proceduremæssige rammer til at håndtere identificerede risici og korrigerende handlinger
  - Fokus på IT/OT-konvergens – strategisk og operationelt
  - Etablering af cybersikkerheds-framework baseret på risikovurderingen

- Det anbefales, at arbejdet med cybersikkerhed tilrettelægges efter et veldefineret framework, som f.eks. NIST. Dette indebærer, at sikkerhed anskues som en række forskellige discipliner, der indbefatter:
  - Risikostyring af aktiverne (Predict & Identify)
  - Beskyttelse af systemerne (Prevent & Protect)
  - Detektering af en kompromittering (Detect)
  - Reaktion og brandslukning (Respond)
  - Genetablering (Recover)

Overblik over sikkerhedsdisciplinerne

Sikkerhedsarbejdet skal understøtte og håndtere de forskellige discipliner med værktøjer og processer. I det følgende beskrives kort, hvad de enkelte discipliner dækker over.

Predict & Identify
Første disciplin er at skaffe et overblik over virksomhedens aktiver og risici, altså få overblik over komponenter, sårbarheder og trusler, samt konsekvenserne hvis noget går galt. Dette bruges til at udforme en risikovurdering, der herefter er udgangspunktet for at kunne prioritere sikkerhedsindsatsen. Herigennem sikres det, at ressourcerne bruges på at beskytte virksomhedens største værdier.

Prevent & Protect
Det er fortsat meget relevant at have styr på den fundamentale sikkerhed, dvs. etablering af et fornuftigt design og ordentlig beskyttelse af systemerne med firewalls, antivirus osv. Her er det vigtigt, at der er fokus på at holde kontrollerne ordentlig opdateret, så de er tilpasset det aktuelle trusselsbillede. Et eksempel på dette er beskyttelse mod malware, hvor antivirus i mange år har været løsningen. Malware-truslen er imidlertid blevet så dynamisk, at man må supplere med løsninger som program white-listing og sandbox emulering.

Detect
I dag er det essentielt at overvåge, hvad der sker i systemerne. Det gøres ved at indsamle logfiler fra netværksudstyr, servere, firewalls osv. og kombinere disse med en aktiv trafikovervågning. I kombination med den rette viden om aktuelle angrebsmønstre og trusler får man derved mulighed for hurtigt at opdage, når nogen prøver at trænge ind i systemerne. Hvis det lykkes for uvedkommende at trænge ind i systemet, har man også fuldt overblik over, hvad der er sket, så man kan reagere målrettet og effektivt på hændelsen.

Respond
Det er ikke længere et spørgsmål, *om* man bliver kompromitteret, men *hvornår*. Derfor er det vigtigt at vide præcis, hvordan der skal reageres, når en hændelse indtræffer, så systemet hurtigst muligt kan komme tilbage til normaltilstanden, hvor der er fuld kontrol over, hvad der foregår. Det kræver blandt andet, at man har en veldefineret tilgang til hele processen omkring Incident Response, så der er et veldefineret beredskab på plads.

Recover
Når en sikkerhedshændelse er indtruffet og incident response er gennemført, skal forretningen genetableres. Det omfatter blandt andet, at systemerne skal genetableres og bringes tilbage til normal funktion hurtigst muligt, så tabene reduceres mest muligt. Genetablering omfatter blandt andet gennemførelsen af passende beredskabsplanlægning, og at man løbende tester, at ens beredskab fungerer, som det skal.

Ordliste

Botnet er en fjernstyret software-robot, der automatisk kan afvikle scripts på Internettet. En bot er typisk en enhed, der er blevet hacket og har fået installeret noget malware. Et botnet består af mange internetforbundne enheder, som er knyttet sammen og fjernstyres fra den samme command and control-server. Botnets bruges ofte til at afvikle DoS og DDoS-angreb (overbelastningsangreb), udsende spammail og søge efter sårbare enheder. Det er også muligt for en hacker at udnytte en bot til at få adgang til en enhed, eller det netværk enheden er forbundet til, og stjæle data.

Dag-0-angreb
Et angreb, der følger opdagelsen af en dag-0-sårbarhed. Angriberen injicerer malware, før sårbarheden er patchet.

Dag-0-malware
Nyt og ukendt malware, der endnu ikke fanges af antivirus-software.

Dag-0-sårbarhed
Sårbarhed, der endnu ikke er offentligt kendt, og derfor kan udnyttes i det skjulte, fordi der ikke er et patch.

DoS og DDoS-angreb
Et Denial of Service (DoS)-angreb er et angreb, der gør en service utilgængelig eksempelvis ved at "oversvømme" et netværk med trafik, så netværket bryder sammen. Ved et Distributed Denial of Service (DDoS)-angreb kommer trafikken fra flere kilder, typisk kompromitterede maskiner spredt på internettet, hvilket gør det vanskelligt at blokere.

KNX er en standardiseret (EN 50090, ISO / IEC 14543), OSI-baseret netværkskommunikationsprotokol til bygningsautomation. KNX er efterfølgeren og konvergensen af tre tidligere standarder: European Home Systems Protocol (EHS), BatiBUS og European Installation Bus (EIB eller Instabus). KNX-standarden administreres af KNX Association.

Kryptering
Kryptering er en sikringsforanstaltning, hvor data kodes på en måde, så kun autoriserede personer/enheder med adgang til den korrekte nøgle kan tilgå data.

Kryptering bruges også i forbindelse med ransomware til at afpresse offeret for en løsesum. Se under ransomware.

Malware
Malware står for "malicious software" og er en betegnelse for ondsindet programkode, der gør skadelige eller uønskede ting.

Man-in-the-Middle-angreb
Et angreb, hvor angriberen sætter sig imellem to kommunikerende enheder som et usynligt mellem-/bindeled. Giver mulighed for at "lytte med" og manipulere på kommunikationen og opsnappe eksempelvis passwords, kreditkortinformationer eller andre oplysninger, samt manipulere i det som transmitteres.

Principle of Least Privilege (PoLP)
Et begreb, der dækker over brugere, programmer og processer, der udelukkende har de rettigheder, som er nødvendige for at kunne udføre deres funktion/opgave. Bruges til at reducere angrebsoverfladen og dermed risikoen for, at en angriber får adgang til kritiske systemer.

Ransomware
Ransomware er en type malware, der krypterer den inficerede enhed og/eller data. I forbindelse med krypteringen fremsættes typisk et krav om en løsesum før adgangen til data (måske) genetableres.

Security-by-Default
Et begreb der bruges om produkter, der frigives med de strengest mulige sikkerhedsindstillinger. Indstillingerne kræver intet manuelt input fra brugeren og er ikke altid specielt brugervenlige. En indstilling i dette er f.eks., at persondata kun opbevares i det nødvendige tidsrum som default.

Security-by-Design
Begrebet dækker over, at løsningerne fra starten er designet til at være sikre. Det vil sige, at det forudsættes, at løsningerne vil blive forsøgt kompromitteret af ondsindede angribere, hvorfor der gøres mest muligt for at gøre løsningerne modstandsdygtige og robuste for derved at mindske konsekvenserne. Endvidere antages det, at en mulig angriber kender til designet af løsningen, som også i denne situation skal være sikker.

Risiko er udtryk for konsekvenserne ved en hændelse set i forhold til sandsynligheden for at hændelsen indtræffer.

Sårbarhed er en svaghed eller fejl, som kan udnyttes af en trusselsaktør, såsom en cyberkriminel eller ondsindet hacker, til at udføre uautoriserede handlinger i et computersystem.

Vejledninger – Sådan gør du!

Sådan kommer du som installatør i gang med at arbejde med cybersikkerhed:

- Få overblik over de mest almindelige former for cyberangreb. Det kan f.eks. ske via denne rapport, deltagelse på konferencer og seminarer om cybersikkerhed eller via information på www.sikkerdigital.dk.
- Forstå hvilke løsninger, der findes på dit område, og stil spørgsmål til dine leverandører og producenter, så du forstår cybersikkerhed i deres løsninger.
- Vælg produkter baseret på deres sikkerhedsfunktioner, bl.a. security og privacy by design/default.
- Skaf et overblik over de aktuelle digitale kompetencer – og særligt med fokus på cybersikkerhed – i virksomheden, find ud af, hvad der mangler, og læg en plan for forbedring.
- Sørg for videreuddannelse af personalet i forhold til planen – husk fokus på både kommercielle og tekniske kompetencer.
- Vær ikke bange for at gå i dialog med kunderne om cybersikkerhed og få dem til at forstå, at de skal afsætte penge i budgettet til cybersikkerhed.
- Gennemgå leveranceprocessen, og hvordan cybersikkerhed kan blive en værdifuld del af jeres leverancer. Overvej, om eksempelvis servicekontrakter kan være en mulighed.
- Lær af erfaringerne – hvad virker, og hvad virker ikke?
- Gør cybersikkerhed til en del af organisationens DNA. God cybersikkerhed kræver en kultur med fokus på sikkerhed (awareness).

HUSK at cybersikkerhed er en forudsætning for, og understøtter, digitalisering!

Det skal der være fokus på ved valg af produkter:

- Har producenten en kommunikeret og tydelig tilgang til sikkerhed i udviklingsprocessen, f.eks. "Security by design", "Security by default" og "Principle of Least Privilege", samt en proces med review af kode og sårbarhedstest af deres produkter?
- Har producenten en kommunikeret "End-of-Life"-politik, der beskriver, hvor længe deres produkter og enheder bliver vedligeholdt med ny software?
- Har producenten klare vejledninger omkring sikkerheden i deres produkter, og hvordan de konfigureres korrekt?
- Har producenten en politik og klare retningslinjer for rapportering og håndtering af sårbarheder?
- Er produkterne certificeret efter nogen standarder? (Dette er ikke nødvendigvis et krav, men en god indikation af, at producenten arbejder seriøst med sikkerhed).
- Har producenten klare retningslinjer omkring privacy, herunder en tydelig beskrivelse af eventuelle data som enheden eller produktet opsamler?
- Anvender produktet kryptering af data – både når det transmitteres over netværket, og når det opbevares på enheden?
- Er enheden beskyttet med hensyn til platformsintegritet, det vil sige mod manipulation af software, f.eks. via anvendelse af Secure boot og code signing?
- Anvendes der et hærdet operativsystem, som er begrænset til de nødvendige funktioner, dvs. med en så lille angrebsoverflade som muligt?
- Understøtter enheden regelmæssige softwareopdateringer, f.eks. gennem en automatiseret proces, hvis det ønskes?
- Understøtter enheden stærk autentifikation, evt. at man kan bruge en ekstern autentifikationsplatform?

Som installatør skal du bl.a. være opmærksom på:

- Hjælp kunderne med at lave en risikoanalyse, så der er klarhed over, hvor risikoen er størst, og hvor fokus skal være.

- Skift default-kodeord og opret unikke kodeord på alle enheder i installationen. I princippet skal hver kunde og hver enkelt enhed have sit eget unikke kodeord, som er anderledes end standardkodeordet fra producenten.

- Alle steder, hvor det er muligt, skal 2-faktor autentifikation slås til. Dette er bl.a. muligt på mange af de mest udbredte cloud-løsninger.

- Sørg for, at alle enheder er opdateret og installeret med nyeste software uden kendte sårbarheder.

- Netværkssikkerhed. Det er blandt andet vigtigt, at udstyret placeres på et separat netværk, der ikke har direkte forbindelse til kundens interne netværk. Desuden bør det overvejes, om der skal bruges NAC (eller som mindre sikkert alternativ MAC-filtrering) til at sikre, hvilke enheder der kan komme på netværket.

- Firewall. Firewallen bruges til at beskytte forskellige netværk mod hinanden og bruges f.eks. mellem det interne netværk og det offentlige internet. Det er vigtigt, at firewallen konfigureres rigtigt, så der ikke er for mange åbninger. Det er nemt at fejlkonfigurere en firewall, så det er vigtigt at have den nødvendige viden.

- At udstyret så vidt muligt placeres, så fysisk adgang ikke er mulig. Kan det ikke lade sig gøre, så sørg for, at der kommer en alarm, hvis der "pilles" ved udstyret.

- Husk at anvende kryptering alle de steder, hvor det er muligt. Det er især vigtigt de steder, hvor der ikke er kontrol over enhederne og netværket. Netværkstrafik kan f.eks. krypteres ved hjælp af VPN eller en https-forbindelse.

- Hvis installatøren er ansvarlig for driften, f.eks. via en serviceaftale, skal enhederne kontrolleres regelmæssigt, blandt andet via gennemgang af logfiler og opdatering af software.

- Når installationen er gennemført, er det vigtigt, at den overdrages ordentlig til kunden, så kunden forstår, hvilken løsning de har overtaget og deres ansvar i den forbindelse.

TEKNIQ Arbejdsgiverne
Paul Bergsøes Vej 6
2600 Glostrup

Magnoliavej 2-4
5250 Odense SV

Telefon: +45 4343 6000
www.tekniq.dk
tekniq@tekniq.dk

TEKNIQ ARBEJDSGIVERNE