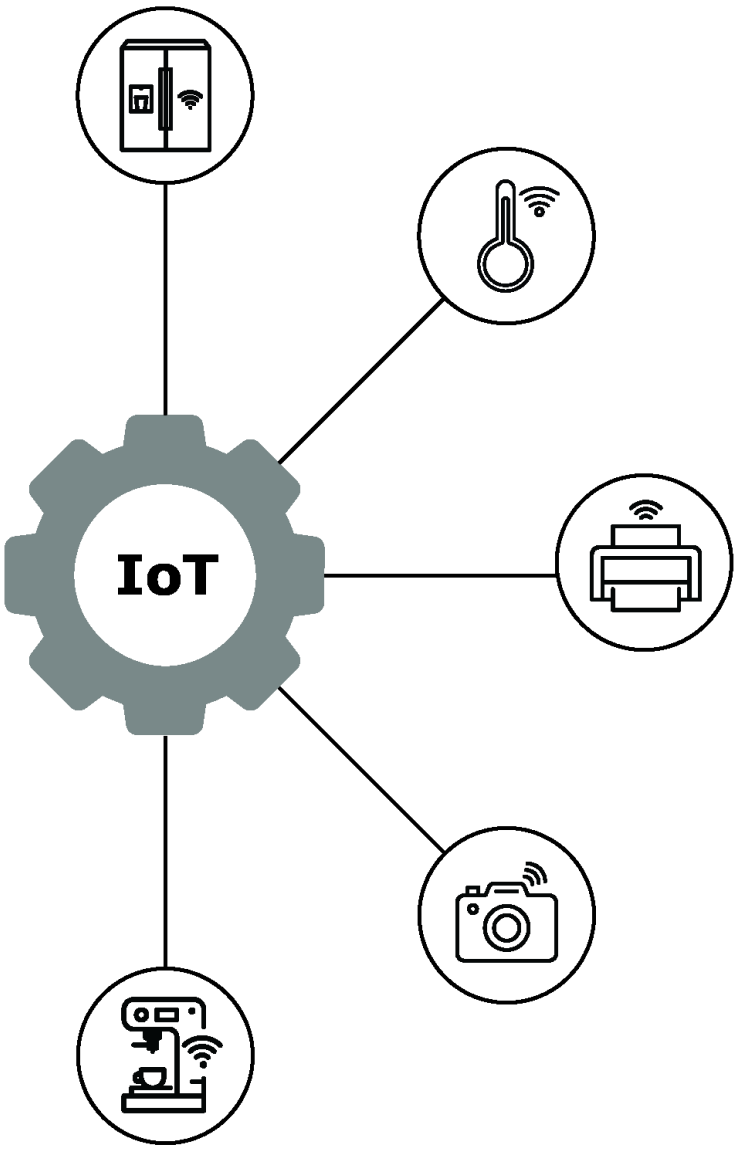
CENTER FOR CYBERSIKKERHED

Beskyt IoT-enheder

Vejledning til best practice-beskyttelse



Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave oktober 2023

Indledning

Antallet af forskellige enheder, der kan forbinde og udveksle data med andre enheder og systemer over internettet, er eksploderet de seneste år. Enhederne, også kaldet Internet of Things eller IoT-enheder, kan være alt lige fra ladestandere og termostater til overvågningskameraer. IoT-enhederne giver en lang række fordele, da de kan automatisere og effektivisere opgaver, men de skal løbende sikres for at undgå, at de forringer organisationens cybersikkerhed.

I trusselsvurderingen *Cybertruslen mod IoT-enheder* (2023) vurderer CFCS, at truslen fra cyberangreb mod IoT-enheder er **MEGET HØJ**. Truslen bliver understreget af, at IoT-enheder i Danmark løbende er udsat for forsøg på cyberangreb, og at det er meget sandsynligt, at det vil fortsætte på lang sigt. IoT-enheder er generelt attraktive mål, da de typisk er dårligere beskyttede end almindelige computere og dermed nemmere at hacke. Særligt udsatte er IoT-enheder med kendte sårbarheder, som ikke beskyttes ordentligt (Center for Cybersikkerhed 2023a).

Denne vejledning kommer derfor med konkrete anbefalinger til, hvordan organisationer kan beskytte IoT-enheder efter best practice.

Vejledningen er relevant for alle organisationer, der har IoT-enheder på arbejdspladsen, uanset om enhederne har en væsentlig rolle, såsom ladestandere til firmabilerne eller stemmestyrede højtalere, som spiller musik i frokostpausen. Vejledningen supplerer de grundlæggende cybersikkerhedsprincipper i CFCS' vejledning *"Cyberforsvar der virker"* (Center for Cybersikkerhed 2023b).

Ikke alle IoT-enheder og IoT-leverandører kan leve op til alle anbefalinger, som er nævnt i denne vejledning. Det skyldes, at mange IoT-enheder er meget simple i opbygningen. Hensigten med vejledningen er at præsentere best practice beskyttelse, og få organisationer til at tage bevidste valg om organisationens brug af IoT-enheder, og undgå enheder der ikke kan sikres.

Organisationen skal på baggrund af egen risikovurdering tage stilling til, hvilke sikkerhedskrav de stiller til deres IoT-enheder, og hvilke foranstaltninger de skal implementere. Organisationens sikkerhedskrav kan betyde, at organisationen må fravælge nogle IoT-enheder, der i funktionalitet ikke kan leve op til kravene.

Trusselsvurderingen "Cybertruslen mod IoT-enheder" og denne vejledning samt IoT-kort guide er udarbejdet i dialog med Dansk Erhverv og Rådet for Digital Sikkerhed i rammen af "Aftale om et styrket cyberforsvar", og indholdet har bl.a. været drøftet med medlemmer af Dansk Erhvervs it-sikkerhedsnetværk. CFCS takker Dansk Erhverv, Rådet for Digital sikkerhed samt medlemmer af Dansk Erhvervs it-sikkerhedsnetværk for samarbejdet omkring udgivelserne.

Målgruppe
Vejledningen indeholder anbefalinger til to målgrupper: forretnings- og it-ledelsen samt drift og implementering. I hvert kapitel er det angivet med ikoner, hvem anbefalingerne er rettet mod.

Forretnings- og it-ledelsen
I denne vejledning er forretnings- og it-ledelsen den del af organisationen, som har til opgave at kende trusler mod og potentielle sårbarheder ved IoT-enheder, vurdere risikoen og på den baggrund udarbejde en IoT-politik. Det er også it-ledelsens ansvar, at IoT-politikken implementeres og formidles til relevante interessenter. IoT-politikken skal være i overensstemmelse med organisationens risikovurdering, lovgivning og organisationens målsætninger.

Drift og implementering
Drift og implementering er i denne vejledning den del af organisationen, der har ansvaret for indkøb, herunder at stille krav til leverandør, opsætte, drifte og bortskaffe IoT-enheder. De skal også give input til forretning- og it-ledelsen om, hvordan drift og implementering af IoT-enheder fungerer i organisationen.

Hvad er en IoT-enhed?
IoT er en samlebetegnelse for alle enheder, der forbindes til internettet med henblik på bl.a. fjernstyring. Eksempelvis et kamera, der kan identificere biler ud fra nummerplader og tage betaling for parkering eller en printer, som hurtigt ordnes af en it-leverandør via fjernadgang. Begrebet dækker i denne vejledning ikke over almindelige computere, servere eller telefoner samt operationelle teknologier som f.eks. industrielle kontrolsystemer.

Overordnede anbefalinger

Organisationen skal medtænke sikkerhed i hele livscyklussen for IoT-enheder. Både ved indkøb, opsætning og drift, samt ved bortskaffelse. Denne vejledning vedrører alle stadier i IoT-enheders livscyklus. Oversigten nedenfor viser vejledningens overordnede anbefalinger, samt hvilke anbefalinger, der tilhører hvilket stadie. Enhver organisation bør ved sikring af IoT-enheder tage afsæt i sin egen risikovurdering.

Ved indkøb

CFCS anbefaler, at organisationen:

- har en politik for IoT-sikkerhed
- stiller krav til leverandører af IoT-enheder og -systemer
- har tekniske krav til IoT-enhederne. I denne vejledning bliver tekniske krav til IoT-enheder behandlet i de forskellige kapitler. Bilag 1 samler derfor en oversigt over de krav, CFCS anbefaler, at virksomheden er særligt opmærksom på ved anskaffelse af nye IoT-enheder

Opsætning og drift

CFCS anbefaler, at organisationen:

- udfører hærdning af IoT-enheder og -systemer
- har oversigt over IoT-enheder og -systemer
- har kontrol over adgang til IoT-enheder
- segmenterer IoT-enheder fra resten af organisationens netværk
- har processer for opdateringer og behandling af sårbarheder på IoT-enheder og -systemer
- monitorerer og logger tilstande (states), hændelser og netværkstrafik fra IoT-enheder og -systemer
- krypterer kommunikation af data
- har processer for behandling og sletning af data på IoT-enheder og -systemer

Bortskaffelse

CFCS anbefaler, at organisationen:

- har processer for genbrug og bortskaffelse af IoT-enheder og -systemer

Politik for IoT-sikkerhed

Organisationen bør have en politik for IoT-sikkerhed. Formålet er at sikre en kontinuerlig, sammenhængende og passende sikkerhed for brug af IoT-enheder. IoT-politikken skal sikre ensartethed for, at brugen af IoT er i tråd med organisationens målsætninger og strategier, regler på området og kontraktlige krav. Ledelsen har ansvaret for at sætte de overordnede rammer for organisationens sikkerhed, herunder sikkerheden for IoT-enheder. Det er it-ledelsens ansvar at forstå trusler og sårbarheder ved brug af IoT-enheder, vurdere hvad et acceptabelt risikoniveau er ved brug af IoT-enheder og på grundlag heraf udarbejde en intern politik for brug af IoT i organisationen. Det er også it-ledelsens ansvar, at politikken implementeres og formidles til de relevante medarbejdere.

Politikken skal sørge for, at der er processer på plads, som sikrer, at der ikke er IoT-enheder, der er misligholdt, ukorrekt opsat eller behandler data forkert. Politikken skal også sørge for at fastlægge, hvem der skal vurdere og godkende nye IoT-enheder, samt sikre at enhederne bliver integreret og opdateret i det eksisterende system. Det kræver, at alle relevante medarbejdergrupper og personer i organisationen kender deres roller og ansvarsområder. De skal også kende deres rolle og ansvar i en beredskabssituation, hvor IoT-enheder er involveret. Roller og ansvar skal beskrives i IoT-politikken.

Politikken bør opliste organisationens krav til data til og fra IoT-enheder, herunder hvilke data enhederne må indsamle. Nogle IoT-enheder indsamler sensitive data, som kun relevante personer må have adgang til. Det er organisationens opgave at vurdere, hvilke data der er sensitive med afsæt i organisationens risikovurdering og eventuel lovmæssige forpligtelser på området. For nogle organisationer er data fra kameraovervågningen af deres produktionsplatform sensitive data, mens personoplysninger af de fleste organisationer betragtes som særligt beskyttelsesværdige.

Organisationen skal også tage stilling til, hvor data må opbevares og transmitteres. Hvis data bliver transmitteret ubeskyttet mellem en IoT-enhed og bagvedliggende systemer, eksempelvis hos leverandøren, er der risiko for, at uvedkommende kan få adgang til dataene.

Data fra nogle IoT-enheder kan derudover blive behandlet i lande, hvor organisationen ikke kan kontrollere, hvem der har adgang til deres data. Virksomheder fra visse lande er underlagt lovgivning, der giver landets statslige myndigheder beføjelser til at indsamle oplysninger fra selskaber i landet. Organisationen skal vurdere, om databehandling i lande med sådan lovgivning kan udgøre en risiko for organisationen.

Organisationen skal have styr på, om der gælder særlige love, myndighedskrav eller standarder, som kan have betydning for de sikkerhedskrav, organisationen skal stille til IoT-enheder. Det kan for eksempel være særlige krav til certificeringer på udstyr, der skal bruges i et specifikt forretningsområde.

IoT-politikken skal være ledelsesgodkendt og dokumenteret for at verificere, at den er i overensstemmelse med ledelsens retning og organisationens mål.

CFCS anbefaler, at organisationen har en politik for IoT-sikkerhed. Politikken bør være ledelsesgodkendt og dokumenteret. Organisationens politik for IoT-sikkerhed bør tage udgangspunkt i organisationens risikovurdering. Politikken bør indeholde:

Organisationens krav til data fra IoT-enheder

- Hvilken type data IoT-enheder må indsamle
- Hvor data fra IoT-enheder må opbevares
- Hvordan data fra IoT-enheder skal beskyttes, når de overføres
- I hvilke lande organisationens data fra IoT-enheder må behandles

Organisationens sikkerhedskrav til IoT-enheder

Organisationens krav til IoT-leverandør

Organisationens fordeling af roller og ansvar for

- vurdering, godkendelse og brug af IoT-enheder og -systemer
- adgang til data på og fra IoT-enheder
- organisationens beredskab i forbindelse med en hændelse, hvor IoT-enheder er involveret

Organisationens politik for IoT-sikkerhed bør evalueres og revurderes af ledelsen mindst en gang om året, eller hvis der sker væsentlige ændringer.

Krav til leverandør

Organisationen bør stille sikkerhedskrav til leverandør af IoT-enheder og -systemer og løbende sikre, at kravene bliver efterlevet. Ved at stille krav til leverandøren og tilse, at de bliver efterlevet, sikrer organisationen, at leverandøren opfylder organisationens sikkerhedskrav. Det er afgørende for, at organisationen kan forhindre potentielle sikkerhedsbrud i organisationens eget system.

CFCS anbefaler, at IoT-leverandøren kan dokumentere en række oplysninger, blandt andet hvor længe IoT-enheden modtager sikkerhedsopdateringer, leverandørens politik for sikkerhedstest, og hvilke data leverandøren indsamler. Informationerne er med til at give organisationen viden om sikkerhedsniveauet hos leverandøren og gøre organisationen i stand til at vælge en leverandør, som lever op til organisationens sikkerhedskrav.

Organisationen bør sikre sig, at leverandører sikkerhedstester og opdaterer deres produkter, herunder både hardware og software, når de bliver bekendt med sårbarheder. Organisationen bør undersøge, om leverandørens sikkerhedstest er passende i forhold til det sikkerhedsbehov, som organisationen har, herunder i forhold til grundighed og, hvor ofte leverandøren sikkerhedstester. Organisationen bør også undersøge, om den tidsramme leverandøren har, fra de erkender en sårbarhed, til de reagerer på dem, er passende i forhold til organisationens risikovurdering.

I tilfælde af at der gælder særlige love, myndighedskrav eller standarder på det forretningsområde, hvor en IoT-enhed skal anvendes, skal organisationen sikre, at leverandøren kan leve op til kravene.

Leverandører bør som udgangspunkt ikke have ubegrænset adgang til organisationens data fra IoT-enheder. Undtagelser bør kræve et ledelsesgodkendt, forretningsmæssigt behov og skal bero på organisationens risikovurdering.

Ved valg af IoT-enheder kan det være væsentligt at undersøge, om enhederne er fremstillet af en Original Equipment Manufacturer (OEM) og indgår i forskellige produkter eller sælges under forskellige varemærker. Hvis dette er tilfældet, kan samme teknologi og eventuelle sårbarheder findes i forskellige IoT-enheder (IPVM 2022).

CFCS anbefaler, at IoT-leverandøren kan dokumentere oprindelsesland på komponenter i udstyr, samt den geografiske placering af den opbevaringsplatform, som data bliver opbevaret på udenfor organisationen. Disse krav er relevante for organisationer, der i deres politik for IoT-sikkerhed har udvalgt, hvilke lande deres data må behandles i. Komponenter skal her ses som både hardware og software samt komponenter, der indeholder firmware.

Endvidere bør organisationen være opmærksom på, om en leverandør af en IoT-enhed er omfattet af andre landes eksportregler. Dette kan påvirke leverandørens mulighed for leverance, support og opdatering af produktet. Udfordringen kan for eksempel opstå, hvis en leverandør er registreret på USA's Bureau of Industry and Security (BIS) såkaldte Entity List[1] (BIS 2023). Entitylisten er en liste over amerikanske handelsrestriktioner mod blandt andet leverandører. En leverandør, der er på denne liste, kan potentielt have IoT-enheder

[1] Entity List er en liste over amerikanske handelsrestriktioner mod de såkaldte entiteter, dvs. udenlandske personer, forskningsinstitutter, regeringer, private organisationer, virksomheder og andre typer juridiske personer. Restriktionerne kan betyde, at amerikanske virksomheder ikke må eksportere hverken servicesydelser eller produkter til eller fra entiteter angivet på Entity-listen.

med chips og software, som er købt i USA inden de amerikanske handelsrestriktioner trådte i kraft, men som på grund af handelsrestriktionerne ikke længere er mulige at opdatere.

Det er vigtigt, at organisationen har en formaliseret proces for håndtering af dialog med leverandøren af IoT-enheder, som både omfatter den daglige dialog og kommunikation samt ansvarsfordeling i tilfælde af sikkerhedshændelser og i en beredskabssituation. En formaliseret proces er med til at sikre, at det er klart for både organisationen og leverandøren, hvilke forpligtelser og handlinger parterne hver især skal udføre i tilfælde af hændelser.

CFCS anbefaler, at organisationen stiller sikkerhedskrav til leverandøren af IoT-enheder og -systemer. Organisationen bør sikre, at leverandøren af IoT-enheder og -systemer dokumenterer:

- oprindelsesland af komponenter i udstyret
- hvor data opbevares, hvis det opbevares uden for organisationen. Hvis organisationens politik for IoT-sikkerhed stiller krav om lande, som data ikke må behandles i, så skal leverandøren informere om den geografiske placering på opbevaringsplatformen
- hvilke interfaces og interaktionsmekanismer, der er til stede på IoT-enheden[2]
- den anvendte kryptografi i IoT-enheden
- IoT-enhedens model og version
- hvor længe IoT-enheden understøttes
- leverandørens politik for sikkerhedstest
- leverandørens politik for sårbarheder, herunder tidsramme fra opdaget sårbarhed til kommunikation med kunder
- opdateringer, og hvor de kan hentes
- hvilke data IoT-enheden indsamler, opbevarer og kommunikerer ud

Leverandør af IoT-enheder og -systemer bør:

- ikke have adgang til organisationens IoT-enheder uden organisationens viden
- foretage løbende sikkerhedstest af softwaren og hardwaren i sine produkter
- kommunikere ved udgivelse af nye sikkerhedsopdateringer
- udgive tilstrækkelige anvisninger om installation af sikkerhedsopdateringer
- håndtere erkendte sårbarheder
- etablere en sikker distributionsmetode for sikkerhedsopdateringer

Organisationen bør vælge leverandører, som kan leve op til de sikkerhedskrav, der stilles til håndtering af data fra IoT-enheder i organisations IoT-politik.

Organisationen bør have en formaliseret proces for håndtering af dialog og ansvars-fordeling med leverandør af IoT-enheder i tilfælde af sikkerhedshændelser og i en beredskabssituation.

[2] Interfaces dækker både over logiske interfaces, eksempelvis VLAN, og fysiske interfaces såsom USB.

Organisationen bør løbende tilse, at organisationens sikkerhedskrav til leverandøren bliver efterlevet

For yderligere information om leverandørstyring, læs "Vejledning om leverandørforhold" (Center for Cybersikkerhed og Digitaliseringsstyrelsen 2022).

Hærdning af IoT-enheder

Når organisationen har anskaffet en IoT-enhed, bør organisationen udføre hærdning af enheden. Formålet med hærdning af enheden er at formindske enhedens potentielle angrebsflade. Hærdning er en proces, som indeholder en række sikkerheds-foranstaltninger, der alle er med til at gøre enheden mere robust overfor angreb. Det kan bl.a. udføres ved at deaktivere netværksprotokoller, som ikke skal benyttes, eksempelvis telnet-protokollen[3], som i nogle tilfælde kan anvendes til at udføre cyberangreb mod IoT-enheder.

Før indkøb skal organisationen have taget stilling til, om det er vigtigt, at IoT-enheden skal forbindes til internettet. Det gør enheden meget mere sikker ikke at være internetforbunden. CFCS anbefaler, at alle unødvendige interfaces, protokoller, funktioner, hardware og software slås fra. Det gælder også enheder, som er offline.
Dette er en måde at reducere risikoen for, at sårbarheder udnyttes.

Det er også vigtigt, at de fysiske interfaces kun kan tilgås, hvis det er nødvendigt. Eksempelvis kan en organisation have et overvågningskamera, der overvåger en offentlig tilgængelig foyer. Hvis organisationen ikke skal benytte den USB-port, som er i kameraet, så skal den deaktiveres. En åben, ubenyttet USB-port kan give uønsket adgang til organisationens netværk, for eksempel ved at indsætte en USB-nøgle inficeret med malware i kameraet.

En vigtig måde at beskytte IoT-enheder på er ved at begrænse mængden af informationer, der kan indhentes fra enhederne. Der findes værktøjer, der kan scanne og indsamle metadata fra alle internetopkoblede enheder, og som stiller data offentligt tilgængeligt på hjemmesider. Disse lettilgængelige metadata kan afsløre sårbarheder, såsom forældede softwareversioner.

Organisationen skal være opmærksom på, om de protokoller, som kører på IoT-enhederne, er forældede. Årsagen til dette er, at netværksscanning-teknologi er blevet moden nok til, at den kan informere om, hvilke services der har sårbarheder. Nogle services kan acceptere brug af TLS-version 1.0, 1.1 og 1.2. Her er det væsentligt at konfigurere IoT-enheden, så den som minimum kun accepterer TLS 1.2. I samme omgang kan organisationen undersøge, om enheden i en opdatering understøtter TLS-version 1.3. Hvis organisationen har IoT-enheder, som eksempelvis kun understøtter TLS-version 1.0 eller WiFi-forbindelse med WEP, så skal organisationen lave en vurdering af, om det er risikoen værd at koble enheden til organisationens netværk, eller om IoT-enheden skal isoleres eller udskiftes.

Hærdning af IoT-enheder kan både foretages af organisationen eller leverandøren af enheden, hvis det ikke er muligt for organisationen at tilgå eksempelvis software eller protokoller.

IoT-enheder kan ejes af en ekstern virksomhed, eksempelvis et vagtfirma, som opsætter og overvåger overvågningsudstyr på organisationens lokation. Hvis dette er tilfældet, skal organisationen sikre, at organisationen krav til hærdning af IoT-enheder følges af den eksterne IoT-ejer.

[3] Telnet er en netværksprotokol, der anvendes på netværk til tovejs datakommunikation.

CFCS anbefaler, at:

- alle interfaces og protokoller, der ikke bliver brugt, slås fra. Interfaces dækker både over logiske interfaces, såsom VLAN, og fysiske interfaces, såsom USB
- alle funktioner, hardware og software, som ikke er nødvendige, slås fra, deaktiveres eller afinstalleres. Hvis det er nødvendigt at forbinde enheden til internettet, så tag stilling til, om fjernadgang skal være mulig
- hvis IoT-enheden forbindes via WiFi, slås WEP og WPA fra. Benyt WPA2 eller WPA3
- fysiske interfaces kun tilbyder den tiltænkte funktionalitet
- begrænse mængden af information, der kan indhentes fra enheden, når man ikke er logget på. Følgende bør ikke kunne indhentes:
    - Informationer om IoT-enhedens opsætning
    - Informationer om IoT-enhedens operativsystem, herunder kernen (kernel)[4]
    - Informationer om IoT-enhedens softwareversion
- slå automatisk opdatering til, hvis risikovurderingen tillader det
- software afvikles med færrest mulige rettigheder
- alle usikre adgange forhindres, f.eks. telnet og http, medmindre andre sikkerhedstiltag kan implementeres, f.eks. SSH og https

[4] En kerne er en del af et styresystem. En kerne forbinder software med hardware, allokerer hukommelse, styrer processor og kontrollerer også sikkerhed gennem eksempelvis adgangskontrol.

Oversigt over IoT-enheder

Organisationen bør fastholde en fuldkommen oversigt over IoT-enhederne. Forsømte IoT-enheder udgør en sikkerhedsrisiko for organisationen, idet de uden organisationens kendskab kan udgøre sårbare angrebsflader, hvis ikke de er beskyttet korrekt. Derfor er en fyldestgørende dokumentation af enhederne vigtig.

Oversigten er med til at sikre, at der er udpeget en ejer af hver enhed, at enheder bliver opdateret, og at der er et samlet overblik over alle enheder. Oversigten er eksempelvis relevant, når IoT-enheder skal bortskaffes på en sikker måde, afhængigt af hvilke data enheden har behandlet[5].

Mangelfuld dokumentation kan lede til situationer, hvor organisationen ikke er klar over, at der er en IoT-enhed, som ikke længere opdateres, eller hvor fabrikanten for længst er stoppet med at understøtte enheden. En glemt enhed kan være sårbar overfor angreb og dermed gøre det muligt for hackere at få adgang til enhedens data og organisationens øvrige netværk.

Hvis organisationen har slået automatisk opdatering til på en IoT-enhed, kan versions-overblikket bruges til at undersøge, om der rent faktisk er blevet udført opdateringer. Oversigten bør gennemgås mindst én gang om året. Leverandøren vil kunne informere om, hvilken version enheden kører på.

Hvis IoT-enheder ejes af en ekstern virksomhed, så skal organisationen stadig have enheden dokumenteret.

CFCS anbefaler, at organisationen dokumenterer informationer om alle IoT-enheder, herunder:

- navn og model på hver IoT-enhed
- IoT-enhedens unikke ID
- opsætningsdato
- eventuel MAC-adresse på IoT-enheden
- IoT-enhedens fysiske placering
- IoT-enhedens logiske placering i organisationens netværk
- firmware og anden software, der er installeret på IoT-enheden, herunder versioner
- dato for seneste opdatering
- fabrikantens garanterede periode for vedligeholdelse
- eventuelle interne supportrutiner eller supportaftaler med leverandør
- fabriksindstillinger for den enkelte enhed og system
- hvilke data der behandles af IoT-enheden
- systemejere af IoT-enheder og bagvedliggende IoT- systemer, herunder hvis enheden ejes af en ekstern virksomhed

Organisationen bør sikre, at dokumentationen er aktuel og præcis, og bliver opdateret mindst én gang om året eller ved omfattende ændringer.

[5] Behandling kan være indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Organisationen bør dokumentere datastrømme til og fra IoT-systemer, herunder hvilke andre systemer, netværk og adgange IoT-enhederne benytter sig af.

Adgangskontrol

Det er vigtigt at beskytte adgangen til IoT-enheder, og organisationen bør have kontrol over adgangen. Adgangskontrollen sikrer, at kun autoriserede ansatte kan tilgå enhederne og de bagvedliggende systemer.

IoT-enheder med svag adgangsstyring kan eksempelvis være IoT-enheder med svage passwords. Svage passwords udgør en stor risiko, da hackere lettere vil kunne bryde dem ved hjælp af brute force-angreb. Et brute force-angreb er et angreb, hvor hackeren gentagne gange forsøger at gætte et password ved at kombinere alle mulige bogstaver, tal og tegn, der kan indgå i et password. Dette kan et computerprogram gøre meget hurtigt, hvis ikke passwordet er langt nok. For at gøre det sværere at gætte passwords, anbefaler CFCS lange passwords på minimum 15 tegn, samt flerfaktor-autentifikation når det er muligt (Center for Cybersikkerhed 2023d). Hvis organisationen ønsker at sikre passwords yderligere mod brute force-angreb, kan organisationen med fordel have alfanumeriske tegn, altså både tal, bogstaver, grafiske tegn og specialtegn, i passwordet.

En anden måde, hackere kan få adgang til IoT-enheder, er, hvis enheden har prædefinerede loginoplysninger, som ikke kan ændres. Hackere har derved mulighed for at slå loginoplysningerne op på internettet og forsøge sig frem med standardlogin. Eksempelvis har mange hjemmeroutere et standardlogin, hvor både brugernavn og password er ”admin”. Derfor anbefaler CFCS, at organisationer ikke anskaffer sig IoT-enheder, som har prædefinerede loginoplysninger, der ikke kan ændres.

Udover den digitale adgang skal organisationen overveje, hvordan den fysiske adgang til IoT-enheden skal sikres. Det er for at sikre, at kun relevante personer kan tilgå displays og interaktionsmekanismer. Med display og interaktionsmekanismer menes der henholdsvis en skærm, hvorpå information vises, og mekanismer, hvor en bruger kan interagere med IoT-enheden. Det kan være knapper, berøringsfølsomme skærme eller lignende. Displays og interaktionsmekanismer kan eksempelvis sikres ved at afskærme dem fysisk eller ved passwordbeskyttelse. Ved IoT-enheder, hvor displays og interaktionsmekanismer benyttes af mange brugere, såsom dørtelefoner, skal organisationen sikre, at kun relevante personer kan foretage administrative ændringer gennem displays og interaktionsmekanismer.

Hvis IoT-enheder ejes af en ekstern virksomhed, så skal organisationen sikre, at enhedens adgangskontrol lever op til organisationens krav til adgangskontrol.

CFCS anbefaler, at:

- adgangsrettigheder til IoT-enheder kun gives til relevante personer og systemer, hvis roller beskrives i politik for IoT-sikkerhed
- IoT-enheder ikke har prædefinerede loginoplysninger, der ikke kan ændres
- IoT-enhedernes passwords ændres ved opsætning
- flerfaktor-autentifikation slås til hvor det er muligt
- brugeradgange til IoT-enheder har unikke passwords
- brugeradgange ikke deles med andre brugere
- passwords til IoT-enheder er på minimum 15 tegn
- eventuel fjernadgang til IoT-enheder sker via en sikker forbindelse
- IoT-enheder og bagvedliggende systemer tidsbegrænser loginforsøg efter 3 mislykkede forsøg med minimumsværdierne 5, 15, og 30 minutter imellem eller efter det antal forsøg, som vurderes tilstrækkelig på baggrund af risikovurderinger af enhederne
- IoT-enheder låses for adgang efter 12 mislykkede forsøg eller efter det antal forsøg, som vurderes tilstrækkelig på baggrund af organisationens risikovurdering

IoT-enheder sikres fysisk[6]:

- Organisationen skal overveje, om der bør være fysisk beskyttelse på IoT-enheder, herunder adgang til netværks- og USB-stik, og i så fald hvilken beskyttelse der skal være
- Det bør kun være muligt for relevante personer at foretage administrative ændringer gennem IoT-enheders display og interaktionsmekanismer, eksempelvis ved fysisk og/eller password beskyttelse

For yderligere information om passwordsikkerhed læs CFCS' vejledning om passwordsikkerhed (Center for Cybersikkerhed 2023d).

[6] Anbefalingerne til fysisk sikring er udarbejdet i samarbejde med PET.

Segmentering af netværk

Organisationen bør så vidt muligt segmentere IoT-enheder fra resten af organisationens netværk. Ved at segmentere netværk mindsker organisationen sandsynligheden for, at et eventuelt angreb kan sprede sig, og segmenteringen kan gøre det lettere at monitorere og reagere på afvigelser i normalbilledet.

Segmenteringen i mindre isolerede delnetværk øger sikkerheden, da man kan have netværk med forskellige sikkerhedsforanstaltninger. Det kan eksempelvis være regler for, hvilke udstyr der må kobles på de enkelte netværk, og særskilte adgangsrettigheder til hvem der må tilgå hvilke netværkssegmenter.

CFCS anbefaler, at organisationen har sit netværk kortlagt og dokumenteret, eksempelvis gennem et dataflowdiagram. Kortlægningen er blandt andet med til at skabe overblik over, hvilke data der løber igennem hvilke systemer. Overblikket gør det lettere at adskille IoT-enheder og systemer, der behandler sensitive data, fra de øvrige IoT-enheder og -systemer. Det bidrager til at beskytte de sensitive data.

Ved at segmentere IoT-enheder fra resten af organisationens netværk og konfigurere firewalls kan organisationen begrænse muligheden for, at malware spreder sig i netværket, eller at uvedkommende får adgang til sensitive data eller forretningskritiske systemer.

CFCS anbefaler, at organisationen:

- har sit netværk kortlagt og dokumenteret
- separerer netværkssegmenter til IoT-enheder og -systemer fra øvrige netværk
- adskiller IoT-enheder og -systemer, der behandler sensitive data, fra de øvrige IoT-enheder og -systemer
- sikrer sig, at kun IoT-enheder eller andet relevant udstyr er koblet til de dedikerede netværkssegmenter
- konfigurerer firewall, så unødvendig intern og ekstern trafik blokeres

Opdateringer og håndtering af sårbarheder

Al software, inklusive firmware, vil løbende have fejl og sårbarheder, som potentielt åbner døren
for hackere. Manglende opdateringer på IoT-enheder gør disse sårbare. Derfor bør organisationen sikre, at IoT-enheder er opdaterede, og at sårbarheder håndteres.

Opdateringer til IoT-enheder kan benyttes til at rette fejl i enhedens software eller tilføje ny funktionalitet. Den vigtigste type af opdatering for en organisation vil dog typisk være sikkerhedsopdateringer. En sikkerhedsopdatering kan blive udstedt på baggrund af en fejl fundet i en kildekode, en fejl i bagvedliggende softwarebiblioteker, en ny protokolversion med det formål at sikre IoT-enheden, eller hvis leverandøren selv enten har modtaget eller opdaget en sikkerhedsbrist i en enhed. Organisationen bør også sikre, at al firmware på IoT-enheder er den nyeste version.

Når det er muligt, anbefaler CFCS, at organisationer slår automatisk opdatering til. De IoT-enheder, som vurderes egnede til automatisk opdatering, skal prioritere sikkerheds-opdateringer, mens feature opdateringer er valgfrie.

Ikke alle sårbarheder kan håndteres med det samme. Det kan være en sårbarhed så kompliceret, at opdateringen ikke kommer hurtigt nok. Det kan også ske, at der er en fejl i opbygningen af IoT-enheden, der gør, at sårbarheden ikke kan udbedres. Organisationen skal derfor have retningslinjer for, hvornår en opdatering senest skal installeres, og hvornår en sårbarhed senest skal håndteres. Retningslinjerne skal beskrive en procedure for, hvad organisationen skal gøre, hvis ikke opdateringen kommer hurtigt nok. Det kan eksempelvis være ved at afkoble enheden fra internettet, indtil sikkerhedsopdateringen kommer, eller ved at fjerne eller udskifte IoT-enheden. Alle relevante medarbejdere skal også kende deres roller og ansvar i en beredskabssituation, hvor sårbarheder skal håndteres, jævnfør organisationens politik for IoT-sikkerhed.

For at sikre effektiv håndtering af sårbarheder og opdateringer til IoT-enheder er det vigtigt, at organisationen har et centralt sted, hvorfra disse kan modtages og handles på. Det kan eksempelvis være en patch management-ansvarlig i it-driften. Dette er for at sikre, at alle IoT-enheder bliver løbende opdateret.

CFCS anbefaler, at organisationen:

- har et centralt sted for modtagelse af informationer om sårbarheder eller opdateringer
- sikrer, at alle relevante medarbejdere kender deres rolle og ansvar i en beredskabssituation, hvor sårbarheder skal håndteres
- slår automatisk opdatering til, hvis risikovurderingen tillader det
- sikrer manuel installation af softwareopdateringer, herunder firmwareopdateringer, hvis automatisk installation fejler
- sikrer, at opdateringer er legitime, eksempelvis via certifikater eller betroede serviceleverandører
- sikrer, at IoT-enheder, der ikke kan opdateres eller konstateres sårbare, enten udskiftes eller isoleres fuldstændig fra det øvrige netværk
- sikrer, at opdateringer, der foretages via netværk, sker gennem krypterede kanaler
- har retningslinjer for, hvornår opdateringer til IoT-enheder senest skal installeres
- har retningslinjer for, hvornår sårbarheder i IoT-enheder senest skal håndteres

Logning og monitorering

Monitorering og logning af IoT-enheder og -systemer gør organisationen i stand til at opdage, følge og analysere anomalier i og hændelser på IoT-enheder og -systemer. Monitorering er organisationens mulighed for at iagttage aktivitet på netværk, IoT-systemer og -enheder med henblik på at opdage mulige sikkerhedshændelser og agere på dem. Logning er organisationens mulighed for at registrere hændelser på netværk, systemer og IoT-enheder for senere at undersøge hændelserne. Organisationen bør logge tilstande (states), hændelser og netværkstrafik fra IoT-enheder og -systemer.

CFCS ser ofte, at organisationer, der har været ude for it-hændelser, ikke har opbevaret logs længe nok. Logning og monitorering af logs fra netværk, systemer og IoT-enheder i organisationens infrastruktur er afgørende for dens evne til at opdage et cyberangreb, stoppe angrebet og effektivt afdække hændelsesforløbet efterfølgende. Logning kan afsløre hackeres mål, metoder og de teknikker, som de anvender. Logs kan også hjælpe med at afdække, hvor hackere kom ind i organisationens it-infrastruktur, hvilket kan gøre det muligt for organisationen at udbedre sine sårbarheder. Organisationen kan også se, om hackere har bevæget sig rundt i organisationens øvrige infrastruktur, og hvilke handlinger, der er foretaget. På den måde kan organisationen også afdække, om der er risiko for flere it-sikkerhedshændelser.

CFCS anbefaler at monitorere, om grænseværdier overskrides på sensor- eller aktuator-enheder. Det kan eksempelvis være fysiske sensorer, der alarmerer på bestemte temperaturer. CFCS anbefaler også at monitorere anomal aktivitet. Anomal aktivitet er al aktivitet, der afviger fra normalbilledet uden grund, for eksempel et input, der normalt kun modtager tal, men hvor bogstaver begynder at optræde.

CFCS anbefaler, at organisationen logger følgende på IoT-enheder:

- bruger-id og enheders unikke id
- ændringer i enheders og systemers konfiguration
- netværkstrafikken, herunder særligt
  - tid
  - protokol
  - eventuelle IP-adresser på afsender og modtager
  - access logs
  - systemlogs
- brugernavn på autentifikationsforsøg
- processer- og RAM-forbrug

Logs bør opbevares i mindst 13 måneder.

CFCS anbefaler, at organisationen monitorerer følgende på IoT-enheder:

- udfald på enheder eller systemer
- netværkstrafik
- om grænseværdier overskrides på sensor- eller aktuator-enheder
- anormal aktivitet på systemer og enheder, herunder forskellige Indicators of Compromise (IoC)

For yderligere information, læs CFCS' vejledning om logning (Center for Cybersikkerhed 2023e).

Kryptografi og kommunikation i brug af IoT-enheder

Organisationen bør kryptere IoT-enheders kommunikation, da det er med til at sikre korrekt og effektiv beskyttelse af organisationens data. Det gælder både i trafikken til og fra enhederne, og tilsvarende for alle de andre services, som man kan tilgå enhederne gennem. Kryptering beskytter data mod uautoriseret adgang og læsning. Dette er afgørende for at forhindre eksponering af sensitive data.

Hvis hackere har adgang til autentifikationsmekanismernes nøgler, kan de skaffe sig en tilsyneladende legitim adgang til IoT-enheder. Derfor anbefaler CFCS, at der benyttes unikke nøgler, der beskyttes med kryptografi.

Kryptografiske algoritmer kan med tiden blive forældede, hvormed krypteringen kan brydes. Derfor skal det være muligt at opdatere eksempelvis kryptografiske algoritmer og nøgler.

CFCS anbefaler, at:

- autentifikationsmekanismer bør benytte unikke nøgler for hver enkel IoT-enhed
- nøgler beskyttes med kryptografi
- kryptografiske funktioner bør kunne opdateres
- kryptografiske funktioner, der benyttes i IoT-enheder, benytter sig af standardimplementeringer af velafprøvede kryptografiske biblioteker
- trafik krypteres og autentificeres
- IoT-enheder, som ikke har tilstrækkelig kryptering, udskiftes eller isoleres fuldstændig fra det øvrige netværk

Behandling og sletning af data

Organisationen bør sikre, at behandling af data på en IoT-enhed og system sker på forsvarlig vis, og at det er let at slette data. Dette er vigtigt for at beskytte organisationens data.

IoT-enheder har typisk et lavt energiforbrug, fordi de som regel ikke selv foretager databehandling. I stedet overfører IoT-enheder det meste data fra sensorer, eksempelvis videofeeds fra kameralinsen eller temperaturmålinger fra termometeret, til et system, der håndterer behandlingen. Organisationen bør foretage en risikovurdering af, hvilke konsekvenser det kan have, hvis andre end godkendte medarbejdere kan behandle eller have adgang til de data. Det er vigtigt, at eventuelle behandlere har systemejers tilladelse til at behandle data eller har den tilladelse, som organisationen vurderer nødvendig på baggrund af sin risikovurdering.

Organisationen bør have et fuldstændig overblik over, hvilke data der gemmes og hvor samt et overblik over datastrømme i IoT-enheder og -systemer. Opbevaring og transmission af data på en IoT-enhed eller et tilhørende system skal ske på forsvarlig vis, og det bør være let for organisationen at slette data, der ikke længere er nødvendige. Hvis det ikke er tilfældet, risikerer organisationen, at sensitive data opbevares på systemer, som ikke er egnet til den slags datahåndtering og derfor er ekstra sårbare.

Organisationen skal være opmærksom på, at det kan være lovmæssigt påkrævet at slette visse typer data efter en vis periode for at overholde reglerne om databehandling og opbevaring. Ved spørgsmål om GDPR henviser CFCS til Datatilsynet.

CFCS anbefaler, at organisationen:

- kan redegøre for, hvem der behandler hvilke data på organisationens IoT-enheder og -systemer, og på hvilken måde det foregår
- sikrer sig, at der er indhentet de fornødne tilladelser til behandling af data på organisationens IoT-enheder og -systemer
- er i stand til at slette udvalgte data fra organisationens IoT-enheder og -systemer

Bortskaffelse og genbrug af IoT-enheder

Når IoT-enheder ikke længere benyttes, bør organisationen tage stilling til, om enhederne skal destrueres eller genbruges i eller udenfor organisationen. Organisationen bør tage stilling til, hvilke data enheden har behandlet og sikre, at bortskaffelse først sker efter sikker sletning af enhedens data. I tilfælde af, at data ikke slettes sikkert, kan organisationen risikere, at uvedkommende kan få adgang til data fra tidligere brug, som med forskellige teknikker (forensics) kan blive genskabt og kopieret.

CFCS deler i denne anbefaling data op i to kategorier: ikke-sensitive og sensitive. Organisationen skal selv vurdere, hvilke data der er sensitive for dem. Nogle myndigheder er lovmæssigt forpligtet til at klassificere information efter Justitsministeriets sikkerhedscirkulære.

Data deles op i kategorier, da forskellige typer data kræver forskellig behandling. Hvis en IoT-enhed har opsamlet og behandlet ikke-sensitive data, kan enheden genbruges eller bortskaffes ved at blive nulstillet eller renset for al data. Hvis enheden derimod har håndteret sensitive data, må den ikke forlade organisationen intakt. Den skal i stedet destrueres. Hvis IoT-enheder skal destrueres, skal organisationen sikre, at al data bliver destrueret på korrekt vis. Eksempelvis kan magnetfelter destruere data på magnetiske lagrings-typer, men ikke på transistorer i Solid State Drives. Hvis organisationen ønsker at makulere datalagring, er det vigtigt, at enheden bliver revet i tilpas små stykker for at sikre, at selv små flash chips bliver destrueret.

Hvis en IoT-enhed nulstilles, skal organisationen være opmærksom på, at nulstilling af enhed (factory reset) oftest kun sletter data på den lokale hukommelse. Det vil sige, at nulstillingen ikke fjerner data på systemer eller på andre lagerenheder, der er tilkoblet IoT-enheden, såsom USB-nøgler eller SD-kort.

Anbefalingerne forholder sig ikke til behandling af personoplysninger. Ved spørgsmål om GDPR henviser CFCS til Datatilsynet.

Organisationen skal være opmærksom på, om den er omfattet af særlige krav til bortskaffelse og genbrug af IoT-enheder, eksempelvis særlige destruktionskrav til enheder, der har behandlet klassificeret data.

CFCS anbefaler, at organisationen sikrer, at bortskaffelse og genbrug af IoT-enheder sker efter sikker sletning af data.

Organisationen bør være opmærksom på, hvilken type data IoT-enheden har behandlet, da det har betydning for, hvordan enheden skal behandles. Behandlingen bør være ledelsesgodkendt. Hvis organisationen renser en enhed, bør rensningen efterfølgende verificeres.

For IoT-enheder, der ikke har behandlet sensitive data:

- Enheder, der genbruges i organisationen, bør nulstilles (factory reset)
- Enheder, der ikke skal genbruges, bør renses for data på alle hukommelseslagre Det kan ske ved sletning af krypteringsnøglen (cryptographic erase) eller ved at overskrive data tre gange med tilfældige data. Hvis sletning eller overskrivning ikke er mulig, skal enheden destrueres

For IoT-enheder, der har behandlet sensitive data, som andre ikke skal have adgang til:

- Enheder, der genbruges i organisationen, bør renses for data på alle hukommelseslagre på enheden. Det kan ske ved sletning af krypteringsnøglen (cryptographic erase) eller ved at overskrive data tre gange med tilfældige data. Enhedernes firmware bør geninstalleres
- Enheder, der ikke skal genbruges, bør destrueres

Referenceliste

Bureau of Industry and Security. (2023). *Supplement No. 4 to Part 744 of the Export Administration Regulations.* https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

Center for Cybersikkerhed. (2023a). *Trusselsvurdering: Cybertruslen mod IoT-enheder* https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-iot-enheder/

Center for Cybersikkerhed. (2023b). Cyberforsvar der virker. https://www.cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

Center for Cybersikkerhed. (2023d). *Passwordsikkerhed - Passwordvejledning til it-brugere, -udviklere, -driftsfolk og ledelsen.* https://www.cfcs.dk/da/forebyggelse/vejledninger/passwords/

Center for Cybersikkerhed. (2023e). Logning – en del af et godt cyberforsvar https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/

Center for Cybersikkerhed og Digitaliseringsstyrelsen. (2022). *Cybersikkerhed i leverandørforhold.* https://www.cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

DS/ISO/IEC 27400:2022 Cybersecurity – IoT security and privacy – Guidelines

DS/EN ISO/IEC 27002:2022 *Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Foranstaltninger til informationssikkerhed*

ETSI EN 303 645:2020 *Cyber Security for Consumer Internet of Things: Baseline Requirements*

GSMA 2020 *IoT Security Guideline for Endpoint Ecosystems*

Forbes. (2017). *Criminals Hacked A Fish Tank To Steal Data From A Casino*. http://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/

IPVM. (2022). *Hikvision OEM Directory*. https://ipvm.com/reports/hik-oems-dir

ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

ISO/IEC DIS 27402:2022 *Cybersecurity – IoT security and privacy – Device baseline requirements*

NIST IR 8228 *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

NIST SP 800-213 *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Reequipments*

NIST SP 800-88 *Guidelines for Media Sanitization*

Swanson, Steven. (2011). *Destroying Flash Memory-Based Storage Devices.* UC San Diego: Department of Computer Science & Engineering. https://escholarship.org/uc/item/0f02d3bm

Bilag 1

Bilag 1 beskriver de tekniske krav til IoT-enheder, som er blevet behandlet i forskellige kapitler i vejledningen. Bilaget indeholder en oversigt over de tekniske krav, som CFCS anbefaler, at virksomheden skal være særligt opmærksom på ved anskaffelse af nye IoT-enheder. CFCS anbefaler, at organisationen stiller kravene, uanset om enheden anskaffes direkte eller via en leverandør.

CFCS anbefaler, at IoT-enheder lever op til følgende tekniske krav:

- Det skal være muligt at udføre den hærdning af IoT-enheder, som er krævet i forhold til organisationens sikkerhedskrav til enheder (se afsnittene Politik for IoT-sikkerhed og Hærdning af IoT-enheder)
- IoT-enheder må ikke have prædefinerede (hardcodede) loginoplysninger, som ikke kan ændres (se afsnittet Adgangskontrol)
- Det skal være muligt at lave passwords med minimum 15 tegn (se afsnittet Adgangskontrol)
- Der skal foretages løbende opdateringer af IoT-enheden (se afsnittet Opdateringer og håndtering af sårbarheder)
- Det skal være muligt at kryptere data (se afsnittet Kryptografi og kommunikation)
- Organisationen skal være i stand til at slette udvalgte data fra IoT-enheder og -systemer (se afsnittet Behandling og sletning af data)