CENTER FOR CYBERSIKKERHED

Kom i gang med at beskytte IoT

Dette er en kort guide til, hvordan organisationer kan komme i gang med at beskytte IoT-enheder. **CFCS vurderer, at truslen mod IoT-enheder er meget høj**. Guiden fremhæver en række værdifulde sikkerhedstiltag, men organisationer bør orientere sig i vejledningen "Beskyt IoT-enheder" for at arbejde i dybden med emnet.

IoT-enheder
(Internet of Things) er en samlet betegnelse for internetforbundne enheder og kan f.eks. være overvågningskameraer, printere eller ladestandere. IoT-enheder omfatter i denne sammenhæng ikke almindelige computere, servere eller telefoner samt operationelle teknologier i industrien, f.eks. industrielle kontrolsystemer.

Før anskaffelsen af en IoT-enhed

- **Tag stilling til, om IoT-enheden skal kobles til internettet.** Hvis I ikke har brug for, at enheden kobles til internettet, så lad være. Det gør brugen af enheden meget mere sikker. Husk at undersøge, om I kan opsætte og anvende enheden uden internetforbindelse.

Undersøg og beslut, hvilken leverandør af IoT-enheder I vil bruge:

- **Find ud af, hvilken data leverandøren indsamler, og hvordan leverandøren anvender de data.** Svaret står ofte på leverandørens hjemmeside eller i deres privatlivspolitik.
- **Overvej jeres behov for at kunne kontrollere, hvem der har adgang til jeres data.** Virksomheder fra visse lande, inkl. Kina, er underlagt lovgivning, der giver landets statslige myndighederne beføjelse til at indsamle oplysninger fra selskaber i landet.
- **Tag stilling til, om I vil dele jeres data med leverandøren.** Overvej bl.a., om der er tale om sensitive data, altså data I ikke vil eller må dele med andre.

Ved køb af en IoT-enhed, bør enheden leve op til følgende tekniske krav:

- **Der skal være løbende opdateringer af IoT-enheden.** Al software vil løbende have fejl og sårbarheder. Løbende opdateringer sikrer dog, at sikkerhedsfejl og sårbarheder udbedres.
- **Det skal være muligt at ændre standardlogin på IoT-enheden.** Hvis udstyret leveres med producentens standardlogin, skal I kunne ændre det, for standardlogins kan findes på internettet.

Efter anskaffelsen af en IoT-enhed

Hvis IoT-enheden kobles til internettet, så øg enhedens robusthed således:

- **Start med at ændre standardloginoplysninger og lav et password på minimum 15 tegn.** Derved kan I begrænse adgangen til enhederne.
- **Slå funktioner fra, som I ikke skal bruge.** Gå i enhedens Indstillinger og luk porte (USB, porte til netværkskabler, Bluetooth), og deaktiver funktioner, som I ikke skal bruge.
- **Undgå at koble IoT-enheder direkte til internettet med en offentlig IP-adresse.** Hav eksempelvis et særskilt netværk til IoT-enheder, der er beskyttet med firewall.
- **Segmentér (opdel) organisationens netværk til mindre delnetværk** for at beskytte jeres systemer og data.
- **Hold enheden løbende opdateret.** Slå eventuelt automatisk opdatering til, hvis det er muligt.

Hold styr på jeres enheder i hele deres levetid:

- **Lav en oversigt over, hvilke IoT-enheder I har.** Opdater oversigten mindst én gang om året, og aftal, hvem der har ansvar for hvilke enheder. Ved at have overblik over enheder og ansvarsområder undgår I usikre IoT-enheder, som kan udgøre en sikkerhedsrisiko for jeres organisation
- **Skil jer af med gamle enheder.** Når leverandøren stopper med at opdatere IoT-enheden, så skil jer af med enheden. Er det ikke muligt, bør I som minimum afkoble enhederne fra internettet.

Sikkerhedstiltagene er baseret på CFCS' vejledning til at beskytte IoT-enheder, der sammen med en trusselsvurdering af IoT-enheder (2023) ligger på www.cfcs.dk.