IoT-tjekliste til virksomheder

Dette dokument indeholder en “før og efter”-tjekliste med 16 punkter, der guider virksomheder til køb og sikker brug af IoT-enheder.

Hvad er IoT?
IoT er en forkortelse af Internet Of Things. Det er teknologier, der sammenkobler produkter og systemer via internettet, så produkterne er i stand til at sende eller modtage data. Det er fx overvågningskameraer, pumper eller varmesensorer, der kan fjernstyres.

Hvorfor beskytte IoT-enheder?
Hvis virksomheden ikke beskytter sine IoT-enheder, kan hackere få adgang til de data, som enheden genererer, og styre eller bruge dem som springbræt til at få adgang til virksomhedens øvrige computernetværk. Det kan fx betyde, at virksomhedens produktion går i stå, eller at it-kriminelle kan udføre ransomware-angreb eller lække virksomhedens data.

Hvem kan bruge tjeklisten?
Tjeklisten henvender sig både til virksomheder, der endnu ikke har IoT-enheder, og virksomheder, der allerede har investeret i IoT.

Hvordan bruges tjeklisten?
Tjeklisten indeholder fire råd, som virksomheder bør følge, før de køber en IoT-enhed. Når hvert råd er dækket tilfredsstillende, kan I sætte et hak. Hvis I ikke kan sætte hak ved alle fire, så bør I overveje, om det er bedre for virksomheden at investere i et andet produkt.

Når virksomheden har valgt en enhed og taget den i brug, er der 12 råd, I bør følge. Det er måske ikke alle, der er relevante for netop jeres virksomhed, men det er en god huskeliste, hvis I vil beskytte jeres virksomhed.

IoT-tjekliste til virksomheder

		✓
Før køb	**1. Overvej om det er risikoen værd at koble enheden på nettet?** Hver gang man sætter en enhed på nettet, øger man risikoen for, at virksomheden kan blive angrebet. Derfor er det vigtigt at veje fordele og ulemper ved at anvende enheden.	
	2. Gå efter kvalitet og sikkerhed Vælg anerkendte leverandører og se efter standarder, certificeringer og mærkningsordninger som fx den europæiske ETSI EN 303 645-standard, UL-2900-1 og IEC 62443. Bemærk, at disse standarder er nye og derfor endnu ikke så udbredte.	
	3. Tal med din it-leverandør - stil følgende spørgsmål: **Adgangskoder:** Kan man selv ændre adgangskoder, og kan de laves stærke nok? Hvis man ikke kan ændre adgangskoder, er det tegn på, at producenten ikke har prioriteret sikkerheden. **Opdatering:** Kan enheden opdateres, og forventer producenten at opdatere? Der opdages løbende nye sikkerhedshuller, og en enhed, der ikke (kan) opdateres, er ikke beskyttet mod de huller. Giver producenten garantier for at holde enheden opdateret? **Data:** Opsamler enheden data, og sender den data ud af virksomheden? Tænk over, hvilke data enheden opsamler. Jo mere kritiske data, jo vigtigere er det at have styr på, hvor data bliver gemt. **Kryptering:** Hvordan gemmes data i produktet, og hvordan sendes data? Hvis data ikke er krypteret, kan de lettere opsnappes og bruges mod virksomheden. Det kan både gælde for adgangskoder og de data, som produktet er i berøring med.	
	4. Beslut om I vil købe produktet eller ej Foretag en vurdering på baggrund af snakken med it-leverandøren. Forstod I både de risici og muligheder, der er for at beskytte IoT-enheden, og er I trygge ved, at enheden lever op til virksomhedens sikkerhedskrav?	

IoT-tjekliste til virksomheder

		✓
Efter køb	**1. Skift adgangskoder og brugernavne** Mange IoT-enheder har standardadgangskoder og brugernavne, der kan være kendt af hackere. Hvis muligt, så lav unikke adgangskoder på minimum 12 tegn og suppler med to-faktor-godkendelse.	
	2. Hold software opdateret Slå automatisk opdatering til, når det er muligt.	
	3. Sluk udstyr, når det ikke er i brug	
	4. Tjek IoT-enhedernes indstillinger, hvis det er muligt I bør vide, hvad indstillingerne dækker over, så I kan indstille dem korrekt og med størst mulig sikkerhed for øje.	
	5. Sæt produktet til at bruge kryptering - normalt WPA2 (ikke kun WEP) En IoT-enhed, der ikke er sikret, kan anvendes af hackere til at få adgang til virksomhedens øvrige systemer.	
	6. Slå Universal Plug and Play (UPnP) fra Det kan misbruges til at skaffe adgang til dit netværk.	
	7. Husk at nulstille produktet/slette data, når produktet smides ud Der kan ligge personlige oplysninger som fx personlige billeder fra et kamera.	
	8. Hav overblik over, hvad I har af IoT-enheder Sørg for at it-afdelingen eller den it-ansvarlige er involveret i alle indkøb af produkter, der kan gå på nettet eller bruge wifi.	
	9. Undersøg hvad konsekvensen er, hvis det net, som IoT-enheden er koblet på, bliver hacket Hvilke data og systemer får hackeren adgang til?	
	10. Indfør segmentering (opdeling) af netværk, så adgang til kritiske netværk og ressourcer begrænses Det kan fx være relevante medarbejdere på ét netværk, IoT-enheder på et andet og gæster til virksomheden på et tredje.	
	11. Få ekstern hjælp til at implementere udstyr på sikker vis, så du er sikker på, at alle forholdsregler er taget Husk, at ansvaret i sidste ende altid vil ligge i virksomheden.	
	12. Husk fysisk sikkerhed Beskyt IoT-enheden mod fysisk adgang og hav overblik over, om enheden kan misbruges, hvis der er fysisk adgang til den.	

Rådet for Digital Sikkerhed
Erhvervsstyrelsen