

Eksperternes gode råd

Ingen forsyningskæde er stærkere end det svageste led.

Din virksomhed kan også blive ramt af et cyberangreb, og derfor har vi samlet gode råd til, hvordan du løfter sikkerheden.

Læs mere på cybersikrefødevarer.dk



1.

Værdikæden er vigtig, men start med at feje for egen dør



2.

Sikkerhed handler om mennesker, ikke teknologi



3.

Stil krav til virksomhedens leverandører



4.

Find gode kilder



1

Værdikæden er vigtig, men start med at feje for egen dør

Skab internt overblik og forståelse: Det bliver nemmere at arbejde med sikkerhed for eksterne aktører i jeres værdikæde, når I forstår jeres egen situation.

Det handler om at vide hvor, I er (mest) sårbare: Hvilke er de mest kritiske data og systemer, som bør beskyttes?

Overvej fx:

- Hvad koster 'nedetid' hos jer i form af penge, tid og omdømme?
- Hvad koster fejl eller mangler i et batch?
- Hvem har ansvaret for og budgettet til at arbejde med cybersikkerhed?
- Hvordan opdager I eventuelle hackerangreb?

Det er ledelses og bestyrelsens ansvar at vide, hvad der er digitalt kritisk for virksomheden, og at der er **strategier, politikker og testede planer** på plads for beskyttelse af vigtige digitale aktiver og aktiviteter.



2

Sikkerhed handler om mennesker, ikke teknologi

Undgå "vi skal bare købe noget software der løser det for os"-mentaliteten.

Fokuser på at identificere de rette individer og at afstemme **roller og ansvar**.

Sæt milepæle og hold hinanden ansvarlige. Sæt også gerne ambitionsniveau: NIS2 minimumskrav, D-mærke, ISO, noget helt fjerde?

Sørg også for, at alle medarbejdere er trænet i og har en god it-praksis:

- Opdater programmer løbende
- Køb antivirus og firewall
- Tag backup
- Lær at spotte mistænkelige mails
- Lav stærke adgangskoder



3

Stil krav til virksomhedens leverandører



Ingen forsyningskæde er stærkere end det svageste led, derfor skal du også stille krav til alle - fra underleverandører, it-leverandører, serviceteknikere mv.

Vær forberedt på at dine kunder måske også stiller større krav til **din** virksomheds cybersikkerhed – og dokumentationen heraf – som en del af det kommende NIS2-direktiv.

4

Find gode kilder



Der er god hjælp at hente fra D-mærkets kriterier (d-maerket.dk) og på sikkerdigital.dk.

På D-mærket kan virksomheder gennemføre en gratis selvevaluering, der kommer hele vejen omkring virksomheden og giver et fælles sprog at tale cybersikkerhed ud fra.

D-mærket kan samtidig bruges som et hjælpeværktøj, når virksomheden skal forberede sig på de kommende NIS2-krav, der vil påvirke hele branchen, uanset om man er direkte omfattet af direktivet eller ej.