USER IT

...din ven i IT

IT-SIKKERHED forklaret for dig, der træffer beslutninger

En kort guide til ledere om ansvar, strategi og sikkerhedskultur.

INDHOLD

Hvorfor IT-sikkerhed er et ledelsesansvar

En stærk sikkerhedskultur kan være afgørende for, hvordan I som virksomhed står, når cybertrusler rammer.

Men den kultur opstår ikke af sig selv - den skal forankres og drives fra toppen. **Det vil sige, af dig som leder.**

IT-sikkerhed er med andre ord ikke kun et teknisk ansvar.
Det er et strategisk ledelsesansvar, og der forventes i stigende grad, at du som beslutningstager kan identificere risici, prioritere investeringer og sikre, at virksomheden har de rette processer og kompetencer på plads.

Det kan virke uoverskueligt, men tillad os at præsentere det for dig med andre øjne:

Det er billigere at tage ansvar nu end at stå til ansvar senere.

Cyberangreb kan lamme driften, skade jeres omdømme og koste dyrt - både økonomisk og juridisk. Derfor er det afgørende, at ledelsen tager aktivt ansvar for at:

- **Skabe en sikkerhedskultur**, hvor medarbejdere ved, hvordan de skal agere.
- **Sætte IT-sikkerhed på dagsordenen** i strategiske beslutninger.
- **Stille krav til leverandører og samarbejdspartnere**.
- **Følge op på rapportering og hændelser** – og lære af dem.

Men hvad betyder det egentlig? Det ser vi nærmere på nu.

Hvad du kan lære af NIS2

- også selvom du ikke er omfattet

NIS2 er et EU-direktiv, der skal gøre virksomheder og myndigheder bedre til at beskytte sig mod cyberangreb. Den gælder for alle, der arbejder med kritisk infrastruktur - fx energi, sundhed, transport osv.

De fleste virksomheder er ikke direkte omfattet af NIS2 endnu, men mange er indirekte omfattet ved fx at have kunder eller samarbejdspartnere, der er direkte omfattet. Det betyder altså, at selv virksomheder uden direkte lovkrav stadig kan blive mødt med strenge sikkerhedskrav fra deres kunder eller samarbejdspartnere.

Derfor er det relevant at kende til NIS2 - ikke som en juridisk pligt, men som en løftestang for bedre cybersikkerhed. Direktivet er udviklet med et formål: at skabe mere robuste og modstandsdygtige virksomheder. Det er noget, alle kan lære af.

Som sikkerhedsekspert Steffen Friis fra 3 udtrykker det:

"Faktisk burde NIS2 gælde alle virksomheder"

Han understreger også, at NIS2 tydeliggør, at ledelsen har det endelige ansvar for sikkerheden. Og det gør en kæmpe forskel for den prioritering, IT tidligere har haft i budgettet.

Med andre ord:
NIS2 lægger et stort ansvar på ledelsen. Hvis der sker et databrud, og der var et kendt kritisk problem, som ikke er blevet håndteret, så vil ansvaret i sidste ende ligge hos ledelsen.

5 spørgsmål du bør stille din IT-leverandør

Når du vælger en IT-partner, vælger du ikke bare teknik - du vælger sikkerhed, gennemsigtighed og fremtidssikring.
Derfor er det vigtigt, at du som leder stiller de rigtige spørgsmål.

Ikke kun for at sikre compliance, men for at sikre, at din virksomhed er modstandsdygtig og klar til at håndtere digitale trusler.

Her er fem centrale spørgsmål, du bør stille din IT-leverandør:

1

Er i D-mærket eller certificeret på anden vis?
Et kvalitetsstempel som D-mærket viser, at leverandøren arbejder ansvarligt med data og cybersikkerhed. Det er en indikator for, at de har styr på både processer og dokumentation.

2

Er vores backup beskyttet mod ransomware - og gemt på et sekundært site?
En backup er kun god, hvis den virker, når uheldet er ude. Spørg ind til, hvordan backuppen er beskyttet, hvor den ligger, og hvordan den testes. En god leverandør har en plan for worst-case-scenarier.

3

Får vi løbende opdateringer om nye trusler og sikkerhedstendenser?

En proaktiv partner deler viden, for at forebygge eventuelle trusler. Du bør forvente, at din leverandør holder dig opdateret og hjælper dig med at forstå, hvad der er relevant for netop din branche.

4

Har vi et overblik over, hvem der har adgang til hvad - og hvorfor?

Adgangsstyring er afgørende for både sikkerhed og GDPR-compliance. Spørg ind til, hvordan leverandøren håndterer roller, rettigheder og dokumentation af adgang.

5

Er vores løsninger skalerbare, så de kan følge med vores vækst?

Din IT-infrastruktur skal kunne vokse med din forretning.

Disse spørgsmål er ikke kun relevante for virksomheder, der er omfattes af NIS2.

De er relevante for alle, der ønsker at tage ansvar for deres IT-sikkerhed - og som vil sikre, at deres leverandører gør det samme.

Og har i en intern IT-afdeling?

Så gælder spørgsmålene stadig.

Det handler ikke om, hvem der udfører opgaven - men om, at du som leder tager ansvar for, at den bliver udført ordentligt.

Husk:
Du kan outsource opgaven,
men ikke ansvaret.

Praktiske råd til hvordan du som leder kan styrke *sikkerhedskulturen*

Som nævnt i første afsnit, starter en **stærk sikkerhedskultur** med dig som leder. Det er dig, der sætter retningen, prioriterer indsatsen og viser, at IT-sikkerhed er vigtigt - ikke kun når noget går galt, men som en del af den daglige drift.

Her er fem skridt du kan tage:

Gå forrest
Vis med dine beslutninger og kommunikation, at sikkerhed er en prioritet.

Skab tydelige rammer
Sørg for at have klare retningslinjer og politikker, som alle forstår.

Gør det trygt at tale om sikkerhed
Opfordr til spørgsmål og åbenhed, også når noget går galt.

Prioritér awareness-træning
Både for dig selv og dine medarbejdere. Menneskelige fejl er den største sårbarhed.

Følg op og mål udviklingen
Få rapporter, lav statusmøder og sæt mål for sikkerhedskulturen.

Du behøver ikke være IT-ekspert for at tage ansvar.

Du skal blot stille de rigtige spørgsmål, tage de første skridt - og vælge de rigtige samarbejdspartnere.

Det er en strategisk ledelsesopgave, og det starter med dig.

Og du har nu fået indsigt i, hvordan du som leder kan:

- **Forstå dit ansvar**
- **Lære af NIS2 – også selvom du ikke er omfattet**
- **Stille de rigtige spørgsmål til jeres IT-ansvarlige eller leverandører**
- **Skabe en stærk sikkerhedskultur**

Hvis du er i tvivl om, hvor din virksomhed står, eller hvordan du kommer i gang, så tag fat i os.

Vi hjælper gerne med en uforpligtende samtale om jeres IT-sikkerhed og hvordan I kan tage de første skridt.