Appendiks 5. Leverandørsikkerhed (IT-leverandører)

Supply chain

At have styr på sine IT-leverandører er et væsentlig element i arbejdet med virksomhedens cybersikkerhed og arbejdet med at forebygge supply chain-angreb. IT-leverandører er attraktive mål for alle cyberkriminelle. Hardware og softwareprodukter kan udstyres med bagdøre og sårbarheder, og en IT-leverandør kan derfor udnyttes af de kriminelle til at skaffe sig adgang til mange virksomheder på en gang.

Bestyrelsens rolle

Bestyrelsen har det overordnede ansvar for sikkerheden i de IT-løsninger og IT-services virksomheden anvender, og skal være bevidste om, at sikkerhedshændelser hos virksomhedens leverandører kan have alvorlige konsekvenser for virksomheden selv, da den f.eks. selv kan kompromitteres, få driftsforstyrrelser og miste data.

Due diligence

Sikkerhed og krav til sikkerhed bør være en del af dialogen allerede ved anskaffelsen, da det ofte er dyrt og besværligt at stille sikkerhedskrav senere. Sikkerhedskravene skal afspejle, hvor kritiske systemerne er for virksomheden, da IT-leverandørerne normalt kræver yderligere betaling for bedre IT-sikkerhed.

Ansvaret for sikkerheden kan ikke delegeres, og derfor bør virksomheden som led i sin due diligence altid stille følgende spørgsmål til sine IT-leverandører:

1. Hvad gør IT-leverandøren for at beskytte mod uønsket adgang?
2. Hvad gør IT-leverandøren for at sikre tilgængelighed og høj oppetid?
3. Hvad gør IT-leverandøren for at dokumentere egen sikkerhed?
4. Hvad gør IT-leverandøren for at passe på persondata (GDPR)?
5. Hvordan aftales den konkrete ansvarsfordeling mellem virksomheden og leverandøren?

På sikkerdigital.dk ligger et spørgeskema inkl. vejledning, der kan hjælpe de IT-, indkøbs- og kontraktansvarlige med dialogen på disse områder.

Generelle emner, bestyrelsen bør føre kontrol med i relation til leverandørsikkerhed:

- **Overblik over it-aktiver og leverandører**: At virksomheden har et overblik over alle sine IT-leverandører og de løsninger og services de hver især leverer til virksomheden. Overblikket skal dække data og forretningsprocesser håndteret af de enkelte leverandører (se også vejledningen s. 10). Uden dette er det svært at stille de relevante sikkerhedskrav.

- **Drøftelse af konsekvenser ved hændelser**: At virksomheden har lavet en business impact analyse, BIA, der kortlægger, hvor afhængig kerneforretningen er af de forskellige IT-leverandører, og at sikkerhedskravene er tilsvarende høje, hvis konsekvenserne ved nedbrud / utilgængelighed som følge af et angreb er store.

- **Ressourceforbrug og kompetencer**: At virksomheden forstår hvilke krav sikker anvendelse af de leverede it-løsninger stiller til virksomheden. Særligt IT-løsninger, der installeres lokalt i virksomheden (on-premise løsninger) kan stille større krav til virksomhedens egen IT-sikkerhed og øvrige håndtering.

- **Kontrakt og forpligtelser**: At virksomheden i aftaler med IT-leverandørerne har fastlagt en klar ansvars- og risikofordeling i forhold til de services og den tilgængelighed, leverandørerne er ansvarlige for at levere, at der er rapporteringskrav ved sårbarheder og evt. cyberangreb, samt at lovkrav er opfyldt (GPDR, outsourcingkrav for den finansielle sektor, NIS-krav for regulerede sektorer m.v.).

- **Certificeringer**: Om virksomheden stiller krav til, at dens IT-leverandører følger eller er certificeret efter, en eller flere standarder eller rammeværk indenfor IT-sikkerhed (f.eks. ISO27001), og om virksomheden bruger disse til kontrollere, at IT-leverandøren lever op til aftalte krav.

- **Opfølgning**: At virksomheden minimum én gang om året følger op på, at IT-leverandørerne opfylder de aftalte sikkerhedskrav, og at disse krav er passende ift. en aktuel og opdateret risikovurdering.

- **Overvågning**: At virksomheden overvåger sine IT-leverandører (i det omfang det er muligt), især i tilfælde hvor IT-leverandøren har adgang til virksomhedens øvrige IT-systemer.

- **Beredskab**: At beredskabsplanen er forberedt på hændelser hos de forskellige IT-leverandører.