Ny vejledning fra Rådet for Digital Sikkerhed sætter fokus på cybersikkerhed og informationssikkerhed i SMV'er

"Mindre og mellemstore virksomheder er særligt udfordrede, når det kommer til sikkerhedstiltag, fordi man ofte ikke har mange ressourcer at dedikere til området, og fordi området kan være vanskeligt at sætte sig ind i (...) Der er behov for, at danske virksomheder beskytter deres forretning og data mod de trusler, som digitaliseringen fører med sig".[1]

Dette er bl.a. ordene fra Rådet for Digital Sikkerheds faggruppe, som netop har offentliggjort en ny brugervenlig vejledning, hvori de oplister en række gode råd og links, med hvilke man som SMV kan kvalitetstjekke sin egen informationssikkerhed og cyberrobusthed.

Vejledningen opstiller blandt andet følgende gode råd:

0-10 ansatte

- Få overblik over hvilke systemer, tjenester, data og leverandører du er afhængig af

- Opdater softwareprogrammer, så sårbarheder fjernes
- Sørg for, at du har antivirus og firewall på dit udstyr
- Tag backup af data og systemer (også de data, der er i skyen) og sørg for, at den er beskyttet og udenfor virksomhedens almindelige rækkevidde (airgapped / off-line)
- Øv restore af din backup
- Lær at spotte mistænkelige mails og links
- Brug to-faktor autentifikation og hvis ikke muligt, så brug kodehusker med lange og unikke adgangskoder
- Lav en plan for hvem der gør hvad, når uheldet er ude (beredskabsplan)
- Overvej cyberforsikring

11-50 ansatte

- Implementer de forudgående råd
- Udpeg en ansvarlig for it-sikkerhed (kan være en person, som har andre roller i forvejen)
- Sørg for medarbejderes awareness
- Sørg for at styre, hvilke brugere du har og hvilke rettigheder, de har
- Hvis du bruger fjernarbejdspladser, skal disse beskyttes med VPN, to-faktor autentifikation og kryptering af harddiske
- Sørg for en passende fysisk sikkerhed (aflåsning, afskærmning, overvågning m.v.)
- Sørg for dokumenterbar compliance med lovgivning og kundekrav (databeskyttelse, dataetik, NIS2, mv.) Vurder hvilke risici du står overfor og lad det være udgangspunktet for din beredskabsplan
- Test din beredskabsplan
- Hav fokus på de personoplysninger du behandler og sørg for, at de er beskyttet godt nok
- Se på din virksomhed udefra og tænk over, hvad du eksponerer, og tag stilling til om det er hensigten

51-250 ansatte

- Implementer de forudgående råd
- Sørg for at have en dokumenteret proces for risikostyring
- Skanning efter sårbarheder

- Hvis du har produktion, automatiseret lager eller tilsvarende, skal du også sørge for god beskyttelse af dette (OT). Vælg en egnet standard til dette formål.
- Netværkssegmentering
- Logopsamling og loganalyse (SIEM)
- Begræns og beskyt administrative rettigheder
- Konfigurationsstyring
- Hvis du udvikler kode, så stil krav til sikkerheden i kodeudviklingen og kontroller at kravene er opfyldt. Vælg en egnet standard til dette formål.
- Sørg for at opsamle, godkende og dokumentere ændringer på en systematisk måde.
- Sørg for at have styr på dine informationsaktiver ved anskaffelse, vedligeholdelse og bortskaffelse
- Sørg for at du har en veludviklet, opdateret og gennemtestet beredskabsplan. Planen skal være godkendt af ledelsen.
- Træn jeres medarbejdere, så de har kendskab til sikkerhedspolitikker, deres roller og ansvar
- Hændelseskommunikation til omverden, til jeres kunder og til myndighederne
- Opret en online kanal for at 3. parter kan rapportere sårbarheder på jeres produkter.

Du kan læse den fulde vejledning her: Microsoft Word - 202402 Vejledning - informationssikkerhed (digitalsikkerhed.dk)

[1] Microsoft Word - 202402 Vejledning - informationssikkerhed (digitalsikkerhed.dk), s. 2

<

Jesper Lynge Thomsen
Management Consultant
75 62 99 99 · jt@roesgaard.dk