Digital sikkerhed

Hvad kan du som rådgiver gøre, for at styrke it-sikkerheden i de virksomheder, du rådgiver?

For at styrke små og mellemstore virksomheders robusthed over for it-nedbrud eller angreb fra it-kriminelle, skal it-sikkerhed tænkes ind som en naturlig del af den digitale omstilling. It-sikkerhed er relevant for alle dele af den digitale omstilling, uanset om det omhandler cykelsmedens kundedatabase eller servicevirksomhedens lønsystem.

Det er derfor vigtigt, at du som rådgiver har fokus på digital sikkerhed, når du rådgiver små og mellemstore virksomheder i deres digitale omstilling. Denne oversigt har til formål at give et overblik over, hvordan it-sikkerhed kan indtænkes i dit rådgivningsarbejde.

Vejledning om it-sikkerhed bør altid tage udgangspunkt i virksomhedens forhold: Hvor digital er virksomheden, arbejder man aktivt med it-sikkerhed allerede, eller skal det basale på plads? Erhvervsstyrelsen har en række værktøjer og vejledninger, der kan anvendes, enten af virksomheden selv eller som en del af rådgivningsarbejdet. Det vil komme an på en konkret vurdering, hvilke værktøjer, det er relevant at bruge:

- Sikkerhedstjekket: Få overblik over virksomhedens risikoprofil og mulige indsatspunkter. Relevant for alle, og især virksomheder der i begrænset omfang arbejder med it-sikkerhed
- Fem gode råd: De fem gode råd på sikkerdigital.dk er relevante at gennemgå for alle virksomheder.
- Stil krav til it-leverandøren: Relevant for virksomheder, der har udliciteret deres it – og dermed også en del af deres it-sikkerhed – til en leverandør.
- Andre værktøjer på sikkerdigital.dk: Fx skabelon til risikovurdering og it-sikkerhedspolitik. Relevant for virksomheder, der er i gang med at opbygge deres it-sikkerhed.
- Mere avanceret rådgivning: For virksomheder, der er længere i deres it-sikkerhedsarbejde, kan det være relevant at foretage fx en sårbarhedsscanning, penetrationstest eller lignende. Det kræver formentlig inddragelse af rådgivere med særlig ekspertise på området.

Læs mere om de forskellige værktøjer nedenfor.

Sikkerhedstjekket
Sikkerhedstjekket er et digitalt redskab for særligt små og mellemstore virksomheder. Tjekket gør det nemt for virksomhederne at få viden om deres it-sikkerhed ved at besvare en række grundlæggende spørgsmål, og kan bruges til at skabe et øget fokus på it-sikkerhedsarbejde.

Sikkerhedstjekket er et værktøj tilpasset virksomheder og tager udgangspunkt i, at alle virksomheder har brug for sikkerhed, men at ikke alle har brug for (eller mulighed for) samme modenhedsniveau. Værktøjet tager afsæt i den internationale sikkerhedsstandard ISO27001 og favner således også kategorier som organisation, ledelse og processer.

Sikkerhedstjekket vil skabe en større forståelse for vigtigheden af it-sikkerhed for virksomhedens forretning. Når virksomheden har gennemført det, får de en række konkrete anbefalinger, der er tilpasset risikoprofil og andre forhold. Anbefalingerne fra sikkerhedstjekket kan fx tydeliggøre, hvad ledelsen bør gøre for at forankre it-sikkerheden i virksomheden.

Det kan evt. være relevant at drøfte anbefalingerne fra Sikkerhedstjekket med virksomheden og lægge en handlingsplan for at gå videre med dem.

Sikkerhedstjekket kan findes her: https://startvaekst.virk.dk/sikkerhedstjekket

Fem gode råd der kan gennemgås med virksomheden for at øge it-sikkerheden

De fem gode råd er konkrete råd til, hvordan virksomheden kan påbegynde og forbedre arbejdet med it-sikkerhed. De er udarbejdet på baggrund af ekspertviden fra branchen og relevante myndigheder. Som rådgiver kan du kan gennemgå dem med virksomheden og få dem til at fokusere på eventuelle huller. Du kan læse mere om de gode råd på sikkerdigital.dk: https://sikkerdigital.dk/virksomhed/fem-gode-raad-der-styrker-din-virksomheds-it-sikkerhed/

1. *Få overblik over de vigtigste data og systemer:* Når virksomheden skal styrke it-sikkerhedsniveauet er det vigtigt at få overblik over virksomhedens vigtigste data og de systemer/personer, der håndterer dem. Eksempler på vigtigt data er informationer, der er afgørende for at holde virksomhedens produktion og drift i gang, kundeinformationer, patenter, økonomiske nøgletal. Derfor er det vigtigt, at du som rådgiver sætter fokus på kritisk data og systemer.
2. *Opdatér systemerne:* It-kriminelle misbruger huller i computersystemerne, og formår på denne måde at angribe virksomhederne. Hvis virksomhederne husker at opdatere deres systemer og programmer, lukker de hullerne. Som rådgiver kan du eksempelvis opfordre virksomheden til at slå automatiske opdateringer til.
3. *Invester i backup:* Manglende backup eller mangelfuld backup er en af de mest almindelige årsager til, at virksomheder mister deres kritiske data. Udover at opfordre virksomheden til at få overblik over de vigtigste data, kan du som rådgiver opfordre virksomheden til at tage backup af deres kritiske data - gerne med jævne mellemrum. Backuppen skal ligeledes opbevares sikkert, enten via en cloudløsning eller et separat fysisk sted end i virksomheden, idet der er en risiko for indbrud, brand eller vandskade.
4. *Få gode digitale vaner:* Mange it-sikkerhedsbrud sker på grund af manglende viden og fejl blandt medarbejdere. De kan fx blive narret til at klikke på inficerede links eller til at overføre penge. Det er vigtigt, at du som rådgiver opfordrer virksomheden til at gøre medarbejderne opmærksomme på trusler, og at medarbejderne har stærke kodeord mv.
5. *Stil krav til sikkerheden hos it-leverandøren:* Særligt små og mellemstore virksomheder outsourcer it-driften til eksterne leverandører. Som rådgiver kan du opfordre virksomheden til at stille krav til disse leverandører, så de fx tager backup af data eller opbevarer deres data sikkert.

Stil krav til it-leverandøren
Fordi mange virksomheder outsourcer deres it-drift, kan du være med til at gøre dem opmærksomme på at stille sikkerhedskrav til leverandøren. Leverandører skal gerne leve op til de fem gode råd samt andre it-sikkerhedsforanstaltninger.

Virksomheder bør derfor stille følgende krav til deres leverandører:

- Krav til opbevaring af data både fysisk og virtuelt. Eksempelvis er det vigtigt, at der tages backup samt at data ikke ligger frit tilgængeligt hos leverandørens medarbejdere.

- Krav til kontroller såsom logning af netværk, firewall mv.

Du kan finde flere krav på sikkerdigial.dk: https://sikkerdigital.dk/virksomhed/fem-gode-raad-der-styrker-din-virksomheds-it-sikkerhed/stil-krav-til-sikkkerheden-hos-it-leverandoeren/

Andre værktøjer på sikkerdigital.dk
På sikkerdigital.dk kan du finde flere værktøjer, som virksomheder kan anvende undervejs i deres arbejde med it-sikkerhed. Der er eksempelvis værktøjer til risikovurderinger, til at sætte fokus på it-sikkerhed overfor ledelsen, skabeloner til it-sikkerhedspolitikker mv:
https://sikkerdigital.dk/virksomhed/saadan-beskytter-du-din-virksomhed/skabeloner-og-vaerktoejer/

Mere avanceret rådgivning
Hvis virksomheden har arbejdet med it-sikkerhed længe og ikke har brug for sikkerhedstjekket eller værktøjerne på sikkerdigital.dk, kan det evt. være relevant med mere avanceret it-sikkerhedsrådgivning. Det kan fx være en sårbarhedsscanning af virksomhedens systemer eller en penetrationstest. Det vil formentlig kræve specialiseret it-sikkerhedsrådgivning. Der arbejdes løbende på at udbygge listen over rådgivere inden for digital sikkerhed på SMV:Digital's rådgiverdatabase.