Er din virksomhed it-sikker?

”Det sker ikke for mig” kan ikke bruges mere

Truslen fra cyberkriminalitet kategoriseres af Center for Cybersikkerhed som MEGET HØJ
Undersøgelser viser, at mange danske virksomheder ikke tænker nok over deres egen informationssikkerhed – **gør I?**

Det kan medføre store økonomiske tab samt tab af tillid til din virksomhed, hvis de cyberkriminelle eksempelvis får adgang til data eller informationer fra virksomheden, låser disse eller forstyrrer virksomhedens drift.

Små og mellemstore virksomheder er særligt udsatte. Det skyldes, at de bliver anset for at være nemme mål, fordi de ofte ikke investerer i informationssikkerhed – **gør I?**

HVOR SKAL DU STARTE?

Sikkerhedsforanstaltninger virksomheden kan benytte og implementere

Kritisk

Benytter:

- Firewall
- Antivirus

Implementerer:

- **Systematisk opdatering** af softwareprogrammer og styresystemer
- **Stærke og varierede adgangskoder**
- **Adgangskoder** på trådløse netværk

Basal

Benytter yderligere:

- Backup
- Password manager

Implementerer yderligere:

- **Risiko- og trusselsvurdering**
- **Informationssikkerhedspolitik:** Ledelsesinvolvering, tager stilling til ønsket sikkerhedsniveau
- **Funktionsadskillelse:** Begrænsning af adgange til data og systemer til kun det mest nødvendige

Godt

Benytter yderligere:

- Spamfilter, fx frasortering af phishingmails
- Overblik over vigtigste data og systemer
- To-trins-beskyttelse

Implementerer yderligere:

- **Hændelseshåndtering** og beredskabsplan
- **Løbende test** af at informationssikkerheden fungerer, inkl. test af backup
- **Uddannelse og træning** af medarbejdere, fx i at spotte mistænkelige mails

Kilder til anbefalinger: Center for Cybersikkerhed, Erhvervsstyrelsen og Digitaliseringsstyrelsen
Henvisninger: *National strategi for cyber- og informationssikkerhed* og *Styrk virksomhedens digitale sikkerhed* og *Sikkerhedstrappen*

DANSKE REVISORER FSR

LØSESUM 22.000 KR. – ØVRIGE OMKOSTNINGER 1 MIO. KR.

Undersøgelser fra den amerikanske it-virksomhed Datto viser, at de cyberkriminelle i gennemsnit kræver 22.000 kr. i løsesum for at frigive virksomhedens data, men at det koster over 1 mio. kr. at genskabe de øvrige data, som de cyberkriminelle får ødelagt i deres søgen efter bytte.

Har du råd til eksempelvis at miste adgangen til dit ordremodul, miste en måneds omsætning eller bruge tid og penge på at genskabe din virksomheds data? Kan det ultimativt betyde, at din virksomhed må dreje nøglen om?

Erhvervsstyrelsen – 40 procent af de danske SMV'er har et lavt digitalt sikkerhedsniveau
I en analyse fra Erhvervsstyrelsen svarer 33 procent af virksomhederne, at de ikke føler sig i risikozonen for cyberangreb. 46 procent af virksomhederne mener ikke, at deres data har særlig værdi for de cyberkriminelle. Men har data værdi for dig, har de også værdi for de cyberkriminelle!

5 TYPISKE METODER, DE CYBERKRIMINELLE – ENKELTVIS ELLER I KOMBINATION – BRUGER TIL AT ANGRIBE DIN VIRKSOMHED

1. **DDoS – Distributed Denial of Service**: Den cyberkriminelle overbelaster virksomhedens hjemmeside(r) med det mål at gøre virksomhedens online platforme utilgængelige.
2. **Phishing:** Den cyberkriminelle forklæder sig i en mail som en genkendelig kilde, eksempelvis en leverandør, for at franarre medarbejdere deres oplysninger.
3. **CEO-fraud:** Den cyberkriminelle udgiver sig for at være direktør i virksomheden og forsøger at få en medarbejder til at betale falske fakturaer eller overføre et beløb.
4. **Ransomware:** Den cyberkriminelle krypterer virksomhedens data og kræver løsesum for at dekryptere igen.
5. **Social engineering:** Den cyberkriminelle indsamler offentligt tilgængelige oplysninger fra eksempelvis sociale medier og forsøger ud fra disse oplysninger at gætte dine adgangskoder.

DET MENNESKELIGE ASPEKT

Mange sikkerhedsbrud sker desværre på grund af fejl og manglende viden blandt medarbejderne, som eksempelvis kan blive narret af phishing-mails til at klikke på usikre links, udlevere adgangskoder eller benytte sig af hackede eller genbrugte adgangskoder. Der bliver dagligt sendt over 3,2 mia. phishing-mails!

På **sikkerdigital.dk** finder du relevant materiale, som du kan tage udgangspunkt i, fx en præsentation til fællesmøder, print-selv-plakater, vejledninger og mange flere gode råd.

sikkerdigital.dk
Gør dine medarbejdere klogere på sikker digital adfærd

— Det er vigtigt, at dine medarbejdere får uddannelse i gode digitale vaner og forstår vigtigheden af god informationssikkerhed.

NÅR SKADEN ER SKET

På **sikkerdigital.dk** har myndighederne samlet vigtig viden om informationssikkerhed til virksomhederne – blandt andet om, hvad I bør gøre, før og når informationssikkerheden er brudt.

sikkerdigital.dk
Når skaden er sket

ANBEFALEDE SIKKERHEDSTILTAG

Et passende informationssikkerhedsniveau afhænger af din virksomheds risikoprofil. Der er ikke ét fælles niveau af sikkerhedsforanstaltninger, som dækker alle danske virksomheder. Virksomhederne varierer blandt andet i størrelse, forretningsmodel, teknologianvendelse mv. – og dermed varierer behovet for sikkerhedsforanstaltninger.

Skab et overblik over de mest kritiske informationer og systemer i din virksomhed, som du bør beskytte.

Utilstrækkelig og uafprøvet backup er en af de hyppigst forekommende årsager til, at virksomheder ikke kan reetablere deres informationer og systemer.

Bliv klogere på din virksomheds risikoprofil på **startvaekst.virk.dk/sikkerhedstjekket**

"Er din virksomhed it-sikker?" er udarbejdet af FSR – danske revisorer i samarbejde med Uniqkey A/S. FSR – danske revisorer er brancheorganisationen for godkendte revisorer i Danmark. Foreningen varetager revisorernes interesser fagligt og politisk. Uniqkey er en privat leverandør af markedsledende teknologier og software inden for adgangs- og identitetsstyring til virksomheder.

Læs mere på **fsr.dk** og **uniqkey.eu**