Rådet for
Digital Sikkerhed

INFORMATIONSSIKKERHED I DANSKE VIRKSOMHEDER

Med gode råd til SMV'er

Vejledning, overblik og relevante links

Februar 2024

Informationssikkerhed i danske virksomheder

Der er behov for, at danske virksomheder beskytter deres forretning og data mod de trusler som digitaliseringen fører med sig. Forskellige virksomheder står overfor forskellige trusler. Ingen kan sige sig fri, fordi der er penge i det for de kriminelle bagmænd. Derfor er det vigtigt, at danske virksomheder beskytter sig i overensstemmelse med de trusler, de står overfor, og de sårbarheder i organisationen, som kan udnyttes.

Det vil altid bero på et konkret skøn, hvilke tiltag man skal iværksætte. Rådet for Digital Sikkerhed har samlet en række gode råd til virksomheder i forskellige størrelser, der kan bruges som et pejlemærke for, hvad der som minimum bør iværksættes af tiltag. Desuden har Rådet skrevet en række mere specialiserede vejledninger på udvalgte områder, ligesom vi har samlet en række gode kilder, hvor man kan gøre sig klogere.

1. Gode råd til 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. Følger man nedenstående råd, er man nogenlunde klædt på til at beskytte sig.

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

2. Rådets egne faglige vejledninger om cybersikkerhed

- Introduktion sikkerhedsstandarden – ISO/IEC 27002 https://www.digitalsikkerhed.dk/introduktion-til-sikkerhedsstandarden-27002/
- Overblik over implikationer af NIS2 https://www.digitalsikkerhed.dk/overblik-over-implikationer-af-nis2/

3. Henvisninger til råd fra andre aktører

En række aktører har lavet gode vejledninger til virksomheder om cybersikkerhed. RfDS har samlet nogle af de bedste i nedenstående link-samling.

Sikkerdigital, https://sikkerdigital.dk/virksomhed/

På sikkerdigital.dk har Digitaliseringsstyrelsen i samarbejde med andre myndigheder og organisationer samlet vigtig viden om informationssikkerhed. Du finder råd og vejledning af både generel og specifik karakter.

- Cyberhotline med konkret vejledning, 3337 0037
- Sikkerhedstjekket som er et konkret værktøj til at arbejde med sikkerhed, https://startvaekst.virk.dk/sikkerhedstjekket
- It-risikovurderingsværktøj, https://sikkerdigital.dk/myndighed/iso-27001-implementering/risikostyring
- Gode råd hvis du er blevet angrebet, https://sikkerdigital.dk/virksomhed/naar-skaden-er-sket
- Gode råd ved valg af leverandører, https://sikkerdigital.dk/virksomhed/leder/leverandoerpakken
- Beskyt det fysiske produktionsapparat mod cyberangreb: https://sikkerdigital.dk/virksomhed/it-sikkerhedsansvarlig/ot-sikkerhed-beskyt-det-fysiske-produktionsapparat-mod-cyberangreb-
- IoT-tjekliste, https://www.digitalsikkerhed.dk/iot-tjekliste-2/
- Standarder – et systematisk redskab til cyber- og informationssikkerhed, https://sikkerdigital.dk/virksomhed/leder/standarder-et-systematisk-redskab-til-cyber-og-informationssikkerhed-

Center for Cybersikkerhed, https://www.cfcs.dk/da/

Center for Cybersikkerhed skriver en række trusselsvurderinger og tekniske vejledninger og hjælper myndigheder og virksomheder indenfor kritisk infrastruktur med at ruste sig mod angreb.

- CFCS, trusselsvurderinger, https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/

- CFCS, temaartikler, https://www.cfcs.dk/da/temasider/
- CFCS, vejledninger, https://www.cfcs.dk/da/forebyggelse/vejledninger/

Datatilsynet, https://www.datatilsynet.dk/

Sikkerhed og databeskyttelse hænder tæt sammen og Datatilsynet har lavet række vejledninger og værktøjer, som giver indsigt i, hvordan man arbejder med sikkerhedsforanstaltninger rettet mod personoplysninger.

- Datatilsynets vejledninger om sikkerhed, https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed
- Datatilsynets GDPR-univers for små virksomheder, https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/gdpr-univers-for-smaa-virksomheder
- Datatilsynets katalog over sikkerhedsforanstaltninger, https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed/katalog-over-foranstaltninger.

Rigspolitiet, https://politi.dk/da

Rigspolitiet har lavet gode råd til at beskytte sig mod truslerne hacking og DDoS-angreb. På dette site kan man også anmelde kriminalitet.

- Vejledning og anmeldelse, https://politi.dk/hacking
- Anmeldelse af et brede spektrum af it-relaterede kriminalitetsformer, https://politi.dk/oekonomisk-svindel-paa-nettet/anmeld-oekonomisk-svindel-paa-nettet/forening-eller-virksomhed

Det Kriminalpræventive råd, https://dkr.dk/

Det Kriminalpræventive Råd har lavet en række gode råd til virksomheder med særlig fokus på de helt små virksomheder.

- Forebyggelse for SMV, https://dkr.dk/it/it-sikkerhed-i-smaa-virksomheder

Lovpligtig anmeldelse af sikkerhedshændelser

En række sikkerhedshændelser er det lovpligtigt at anmelde – bl.a. hvis virksomheden er udsat for en hændelse, der kan udgøre en trussel for de registrerede.

- Lovpligtig anmeldelse, https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/

SektorCert, https://sektorcert.dk/

SektorCERT (tidligere EnergiCERT) er de kritiske sektorers cybersikkerhedscenter. Via SektorCERTs sensornetværk monitoreres internettrafikken med henblik på at opdage cyberangreb mod dansk kritisk infrastruktur. Herudover vedligeholder SektorCERT en sektorspecifik trusselsvurdering baseret på efterretninger fra internationale aktører, og udarbejder vejledninger, som er relevante for det brede erhvervsliv.

- Publikationer, https://sektorcert.dk/publikationer/

Bestyrelsesforeningen, https://bcfc.dk/

IT-sikkerhed kan være nørdet. Man får omvendt ikke succes med sit arbejde med IT-sikkerhed, hvis man ikke har ledelsesopbakning. Derfor er det relevant med vejledning rettet mod ledelsen, som er let tilgængelig.

- Bestyrelsesforeningens vejledninger og anbefalinger, https://bcfc.dk/vejledning-og-anbefalinger/

D-mærket, https://d-maerket.dk/

Det er både vigtigt, at man kommer hele vejen rundt om alle relevante sikkerhedskrav, og at man kan signalere sit gode arbejde til omverdenen, så der er tillid til ens organisation. Dette kan man opnå ved at tage D-mærket, som er en mærkningsordning for virksomheder, der vil adressere IT-sikkerhed, databeskyttelse og dataetik. D-mærket skalerer efter virksomhedsstørrelse og sektor, og der er desuden auditorer tilknyttet, som hjælper virksomhederne på vej med at forbedre sikkerheden og bevæge sig mod certificeringen.

Kriterier for D-mærket, https://d-maerket.dk/kriterier/

Dansk Standard, https://www.ds.dk/da/fagomraader/it-og-digitalisering

Standarder er den ultimative vej til god sikkerhed. Standarder sikrer at man arbejder systematisk med cyber- og informationssikkerhed og kommer hele vejen rundt om alle aspekter. Der er mange forskellige standarder alt efter om det er IT-sikkerhed, databeskyttelse,

OT-sikkerhed eller sikre produkter man har fokus på. Overblikket over og introduktionen til arbejdet med standarder findes hos Dansk Standard.

- Informationsside om ISO/IEC 27001: https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed
- Informationsside om ISO/IEC 27002: https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed/iso-27002-foranstaltninger
- Informationsside om ISO/IEC 27005: https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed/iso-27005-risikostyring
- Informationsside om ISO/IEC 27701: https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27701-privatlivsbeskyttelse
- Informationsside om SoA-dokument: https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed/soa-dokument
- Informationsside om NIS2-direktivet: https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder/nis2-direktivet
- Overblik over de mest anvendte standarder for privatlivsbeskyttelse og cyber- og informationssikkerhed: https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder
- Risikovurdering for SMV, https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder/guide-til-risikostyring
- Diverse guides og whitepapers om cyber- og informationssikkerhed og kunstig intelligens: https://www.ds.dk/da/download#t=it