Cyberforsikring

I en verden i forandring skal alle virksomheder - små som store - sørge for, at IT-sikkerhed og procedurer i virksomhedens IT-systemer er tilstrækkeligt robuste til at kunne beskytte virksomhedens værdier mod angreb fra IT-kriminelle.

Med en cyberforsikring er din virksomhed sikret, hvis den bliver udsat for hackerangreb, virus eller anden slags datakriminalitet. Med forsikringen får virksomheden ikke bare erstatning for tabt fortjeneste, men også hjælp fra IT-eksperter til at minimere følgerne af et dataangreb.

- Hackere afsøger konstant internettet for udstyr med sårbarheder, de kan udnytte til at skade virksomheden
- Hackere skader sårbare fjernadgange og sælger dem videre til andre kriminelle, som udnytter dem til målrettede ransomwareangreb. Det vil sige en type skadelig software eller malware, som truer et offer med at ødelægge eller blokere adgang til vigtig data eller systemer, indtil der er betalt en løsesum
- Kommunikation via e-mails anvendes primært af alle myndigheder, virksomheder og borgere i Danmark, og e-mails kan uden større teknisk kompetence misbruges af hackere til at beskadige en virksomhed

Hvad dækker forsikringen:

- Teknisk bistand og kriseassistance ved cyberangreb
- Rekonstruktionsomkostninger
- Driftstab
- Ansvar for tredjemand
- Kriminalitet
- Netbanksindbrud
- Rådgivning ved ID-tyveri
- Varsling ved tab af personoplysninger

Hvad dækker forsikringen ikke:

- Forbedringer af systemer
- Videregående ansvar som virksomheden f.eks. ved kontrakt har forpligtet sig til
- Indirekte tab, som ikke betragtes som driftstab
- Krænkelse af immaterielle rettigheder
- Bøder
- Kryptovaluta
- Betaling af løsepenge

Ovenstående lister, vedrørende hvad forsikringen dækker eller ikke dækker, er ikke udtømmende. Det fulde overblik findes i Gjensidiges forsikringsbetingelser 3504191/R407241 Cyberforsikring.

Sikkerhedsforholdsregler

- Alle dataenheder skal til enhver tid have et opdateret operativt system samt aktivt antivirus-program og aktiv firewall
- Alle smarttelefoner og øvrige mobile enheder skal til enhver tid have et opdateret operativt system
- Alle dataenheder, smarttelefoner, mobile enheder og andet udstyr koblet til internet skal være password beskyttet
- Standardpassword skal ændres umiddelbart efter en enhed er taget i brug
- Der skal dagligt tages sikkerhedskopi (backup) af alle virksomhedens data
- Sikkerhedskopien skal opbevares adskilt fra originaldata sådan, at de ikke kan skades ved samme hændelse, som rammer originaldata (fx i cloud eller i et IT system, som ikke er tilkoblet samme system som originaldata)
- Verificering af data på sikkerhedskopier skal foretages mindst 1 gang om måneden

Ved henvisning via Middelfart Sparekasse opnås op til 10% rabat på præmien for cyberforsikringen.

MIDDELFART SPAREKASSE

Gjensidige