Vejledning til SMV om cyberforsikringer

Rådet for Digital Sikkerhed

DI

Forsikring & Pension

Rådet for Digital Sikkerhed · DI · Forsikring & Pension

Oktober 2020

Vejledning til SMV'er om cyberforsikringer

Med virksomhedernes stigende afhængighed af digital teknologi og data følger risici i forhold til IT-nedbrud og angreb fra IT-kriminelle. Cybersikkerhedshændelser kan derfor have store økonomiske konsekvenser for den enkelte virksomhed. Rådet for Digital Sikkerhed, Dansk Industri og Forsikring & Pension giver her et overblik over, hvad virksomhederne skal være opmærksomme på, hvis de skal købe en cyberforsikring.

Cyberkriminalitet er stigende – flere virksomheder rammes

Virksomheder er i stigende grad afhængige af digital infrastruktur, cloudløsninger etc., og mange har en stadig større kompleksitet i deres IT-portefølje. De genererer, håndterer og opbevarer meget store mængder data, og dermed bliver behovet for databeskyttelse større. Digitaliseringen generelt udfordres af trusler om spionage og kriminalitet fra ondsindede aktører, og samtidig kan cyberangreb udføres let og billigt.

Center for Cybersikkerhed vurderer truslen fra cyberkriminalitet som meget høj[1]. I 2018 svarer to ud af tre virksomheder, at de har været udsat for cyberangreb[2], mens der er sket en stigning på 7 pct. i antallet af sikkerhedshændelser fra 2018 til 2019[3]. Det voksende antal sikkerhedshændelser kan være medvirkende til, at 40 pct. af danske topledere oplever cybertrusler som meget bekymrende[4], og at 76 pct. i nogen eller høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed[5].

Man kan som virksomhed gøre meget for at beskytte sig mod cyberkriminalitet, og det bør man også. Du kan læse mere om, hvordan du får styr på den mest basale IT-sikkerhed senere i vejledningen. Uanset hvor meget du gør, kan der ikke stilles garantier, når man taler om cybersikkerhed. Selvom din virksomhed har gjort, hvad der kan forventes, kan I alligevel blive ramt af et skadeligt cyberangreb – sandsynligheden er dog mindre. Virksomheder kan derfor vælge at investere i en cyberforsikring, som kan være med til at sikre mod store økonomiske tab, hvis uheldet er ude. Det er dog vigtigt at forstå, at en cyberforsikring forudsætter, at man forholder sig til IT-sikkerhedsforanstaltninger i sin virksomhed. En cyberforsikring kan dække økonomiske tab som følge af et cyberangreb, men kun hvis din virksomhed har gjort, hvad man kan forvente for at beskytte sig mod cyberangreb.

Denne vejledning gennemgår de typiske krav til virksomheder der ønsker at tegne en cyberforsikring, og den giver anbefalinger til, hvorledes du får styr på den basale sikkerhed i din virksomhed. Vejledningen beskriver forskellige typer af cyberforsikringer og kommer med 7 konkrete trin du kan følge, inden du eventuelt investerer i en cyberforsikring, og endelig foreslår den en række spørgsmål, som du kan stille dit forsikringsselskab.

Cybersikkerhed – de væsentligste sikkerhedshændelser

Cybersikkerhedshændelser er karakteriseret ved, at de berører en virksomheds systemer eller data.

---

[1] https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf
[2] Rambøll for IDA-IT og FSR: https://ida.dk/om-ida/cyberangreb-hagler-mod-danske-virksomheder
[3] https://www.pwc.dk/da/publikationer/2019/cybercrime-survey-2019.pdf
[4] PwC CEO Survey 2018
[5] https://www.pwc.dk/da/publikationer/2019/cybercrime-survey-2019.pdf

Eksempler på hændelser er:

- **Onlinesvindel og falske e-mails, fx phishing.** Svindlere benytter sig af falske mails eller beskeder til at franarre brugere eller virksomheder (person)oplysninger eller til at få gennemført falske pengeoverførsler.
- **Virus, malware og anden ondsindet digital kode.** Dækker over software, som har til formål at skade virksomhedens programmer og data.
- **Online-afpresning af din virksomhed.** Det sker via ransomware, der er en form for malware, som IT-kriminelle anvender til at få adgang til virksomheders data eller systemer. Malwaren kan låse denne adgang gennem kryptering for derefter at bruge dette til at afpresse virksomheder økonomisk.
- **Overbelastningsangreb på din virksomheds hjemmeside.** Et såkaldt DDoS-angreb er et digitalt angreb, hvor en person spammer IP-adressen på en hjemmeside, og derved overbelaster den, så den bryder sammen.
- **Insidere – bevidste og ubevidste cybertrusler.** Der findes medarbejdere, som bevidst går efter at misbruge deres adgang til virksomhedens systemer eller data. Men det kan også være manglende viden om god digital adfærd blandt medarbejdere, som kan resultere i sikkerhedsbrud i virksomheden. CFCS og PET vurderer, at ubevidste insidere er involveret i op mod halvdelen af sikkerhedshændelserne i en organisation[6].
- **Cyberspionage.** Cyberspionage kan fx foregå ved, at hackere infiltrerer computere eller netværk med software, som i al hemmelighed trækker oplysninger og værdifulde data fra virksomhedens systemer.
- **Faktura-bedrageri og CEO-fraud.** Hvis din organisation er mål for fakturaer fra falske afsendere, fx via mail, kan I svindles til at betale fakturaer til de kriminelles konti i stedet for jeres kreditorer. Ved CEO-fraud udgiver svindleren sig for at være direktør i virksomheden med målet om at narre medarbejderne til at gennemføre betalinger, som viser sig at være til de IT-kriminelle.

Typiske krav til din virksomhed, inden du kan tegne en cyberforsikring

Manglen på data og den evige foranderlighed, som kendetegner cybertruslen, gør det vanskeligt for forsikringsselskaber at udvikle modeller, som i tilfredsstillende grad kan forudsige potentielle tab som følge af cybersikkerhedshændelser. Derfor opstiller forsikringsselskaberne typisk en række krav til din virksomhed, hvis du ønsker at tegne en forsikring. Kravene er aftalebestemt, og kan bl.a. omfatte:

- **Antivirus-program/firewall:** Der skal være installeret antivirusprogrammer og firewalls på virksomhedens IT-systemer.
- **Back up:** Virksomheden skal lave backup af data (regelmæssigheden heraf er forskellig) og opbevare den på en sikker fysisk lokation.
- **Opdatering og vedligeholdelse af IT-udstyr og systemer**: Virksomheden skal sikkerhedsopdatere og vedligeholde IT-udstyr, herunder hardware og software. Nødvendig udskiftning til nyere og sikrere alternativer kan være et krav.

[6] https://www.pet.dk/Nyheder/2019/~/media/Files/20190219Truslenfrabevidsteogubevidsteinsiderepdf.ashx

- **Medarbejder-awareness**: Virksomheden skal have klare regler for, hvordan medarbejdere kan afværge skade og tab – fx procedurer for at bortskaffe og destruere hardware og papirudskrifter med henblik på at beskytte data.
- **Kryptering af mobile enheder:** Mobile enheder, som bruges i virksomheden eller håndterer virksomhedens information, skal være hardwarekrypteret**.**
- **Efterlevelse af PCI-DSS:** Tilbyder virksomheden betaling via konto- eller kreditkort, skal virksomheden opfylde krav i dennes kontrakt, som regulerer håndtering af kreditkortoplysninger.

Rådet for Digital Sikkerheds anbefaling til foranstaltninger

Hvis din virksomhed skal investere i en cyberforsikring, er det dermed vigtigt, at I har styr på den basale IT-sikkerhed, da forsikringsselskaberne stiller krav til jeres digitale sikkerhedsniveau. Derfor opfordrer vi til, at din virksomhed følger følgende anbefalinger.

Sådan får du styr på den mest basale sikkerhed

- Få overblik over de vigtigste data og systemer:
  - Hvilke data gemmer I, og hvad bruges de til?
  - Hvilke systemer er jeres virksomhed afhængige af i den daglige drift?
  - Hvor er jeres systemer og data placeret? Hos jer selv? Hos leverandører?
- Opdatér programmer og styresystemer:
  - Hvem har ansvaret for, at programmer og styresystemer holdes opdateret?
  - Hvem vurderer, hvilke programmer, som skal opdateres, og hvornår det skal gøres?
- Investér i en IT-sikkerhedspakke med backup:
  - Hvad er virksomhedens behov?
  - Hvilke løsninger findes der på markedet?
- Få gode digitale vaner:
  - I mange tilfælde kan hackere forhindres i at få adgang til virksomheders data og systemer, hvis medarbejderne er bevidste om IT-sikkerhed.
- Stil krav til sikkerheden hos IT-leverandøren:
  - Selvom virksomhedens IT-drift er outsourcet, er det stadig virksomhedens ansvar at sikre, at der er styr på IT-sikkerheden.
  - Tal med IT-leverandøren om IT-sikkerhed og spørg ind til, hvordan de sikrer, at din virksomheds systemer og data er sikret mod hackere?

Læs mere om myndighedernes anbefalinger til at styrke IT-sikkerheden her.

Hvad dækker en cyberforsikring?

Hvis din virksomhed vælger at investere i en forsikringsdækning, som fx kan indeholde dækning for teknisk bistand ved cybersikkerhedshændelser og dækning for det efterfølgende økonomiske tab, anbefaler vi, at I i forvejen skaber et godt overblik over, hvilke behov jeres forsikring skal dække.

Antallet af cyberforsikringsprodukter på markedet er støt stigende, men forsikringsdækningen kan variere markant. Nogle forsikringsselskaber tilbyder én samlet løsning, hvor der både er dækning for cybersikkerhedshændelser, virksomhedskriminalitet og netbankindbrud, mens andre tilbyder dækning for dette i separate produkter.

Forsikring for cybersikkerhedshændelser forudsætter dialog mellem virksomhed og forsikringsselskab for at sikre den optimale dækning. Først og fremmest er det vigtigt, at I har et overblik over virksomhedens vigtigste data og systemer, så I kan vurdere, hvad der er behov for, at en cyberforsikring skal dække. Det er en god ide at tage udgangspunkt i virksomhedens risikovurdering. Du kan læse mere om og få hjælp til, hvordan I laver en risikovurdering for jeres virksomhed her[7].

Som udgangspunkt bør virksomheden overveje sit behov i forhold til følgende dækninger:

Dækning af omkostninger

- Dækning af adgang til IT-konsulenter, der kan bistå med undersøgelse af cyberhændelsen, fx om der er tale om brud på datasikkerheden eller andre sikkerhedstrusler
- Omkostninger til at genetablere data og netværk
- Assistance ved cyberafpresning
- Driftstab som følge af cyberangreb, herunder dækning for tabt indtjening
- Omkostninger forbundet med krisekommunikation og genopretning af virksomhedens omdømme
- Omkostninger forbundet med eventuel retssag (kan også være dækket af en erhvervsretshjælpsforsikring)
- Erstatningsansvar (se nedenfor)
- Dækning af omkostninger ved sikkerhedshændelser hos IT-leverandøren (se nedenfor).

Dækning af Erstatningsansvar

Virksomheder skal være opmærksomme på deres behov for at forsikre sig for et eventuelt erstatningsansvar. For eksempel kan I stå over for et erstatningsansvar, hvis din virksomhed overfører virus eller andre former for malware til jeres kunder. Forsikring for et evt. erstatningsansvar kan deles op i to:

- Dækning for sagsomkostninger og erstatningskrav i forbindelse med erstatningskrav fra tredjemand, fx vedrørende tab af data samt utilsigtet videresendelse af virus, malware og lignende. Vær opmærksom på, at rene IT-virksomheder bør tegne ansvarsforsikring med særlige udvidelser (specielt, hvis der er tale om hosting).
- Dækning for databrud, herunder uberettiget offentliggørelse af persondata, som samtidig er et brud på databeskyttelsesreglerne (GDPR) og som ikke nødvendigvis er betinget af, at virksomheden har handlet ansvarspådragende.

[7] https://sikkerdigital.dk/virksomhed/saadan-beskytter-du-din-virksomhed/skabeloner-og-vaerktoejer/

Dækning af outsourcing-partner /IT-leverandør

70 pct. af SMV'er udliciterede hele eller dele af deres IT-sikkerhed til en ekstern leverandør i 2019[8]. Derudover benytter mange virksomheder sig af tredjepartssoftware, fx cloudservices eller complianceprogrammer. Sikkerhedshændelser, som påvirker din leverandør, kan have konsekvenser for din virksomhed, lige fra tabt profit til databrud. Det er vigtigt at være opmærksom på, om forsikringen dækker, hvis sikkerhedshændelser finder sted hos din leverandør, og det påvirker din virksomhed.

Hvordan adskiller cyber-, kriminalitets- og netbankforsikring sig fra hinanden?

Ovenstående forsikringer tilpasses de enkelte virksomheders behov, og derfor er dialogen med forsikringsselskabet vigtig. Produkternes dækninger varierer, ligesom virksomhedernes forudsætninger er forskellige.

Det kan være vanskeligt at skelne imellem de forskellige forsikringsprodukter, hvorfor nedenstående illustrerer de generelle forskelle. Bemærk dog, at forsikringsselskaberne kan tilbyde produkter, som indeholder flere af dækningerne i ét samlet produkt:

Begivenhed	Netbankforsikring	Kriminalitetsforsikring	Cyberforsikring
Indbrud i netbank	Dækker 🟢	Kan dække 🟡	Kan dække 🟡
Ansattes bedrageri, underslæb, mandatsvig	Dækker ikke 🔴	Dækker 🟢	Dækker ikke 🔴
Kriminalitet (formuetab) begået af tredjemand mod virksomheden (fx CEO-fraud/fakturasvindel)	Dækker ikke 🔴	Dækker 🟢	Dækker ikke 🔴
Elektronisk afpresning	Dækker ikke 🔴	Dækker ikke 🔴	Dækker 🟢
Tab af data (genetableringsomkostninger)	Dækker ikke 🔴	Dækker ikke 🔴	Dækker 🟢
Tab af data (erstatningsansvar + advokatomkostninger)	Dækker ikke 🔴	Dækker ikke 🔴	Dækker 🟢
Fjernelse af virus, malware, kryptering og genetablering af netværk	Dækker ikke 🔴	Dækker ikke 🔴	Dækker 🟢
Driftstab / meromkostninger	Dækker ikke 🔴	Dækker ikke 🔴	Dækker 🟢
Omkostninger til eller bistand fra IT-konsulenter	Dækker ikke 🔴	Dækker ikke 🔴	Dækker 🟢

Oplysninger i tabellen er fra Willis Towers Watson

[8] Danmarks Statistik, VITA

Anbefaling

Når du som virksomhed køber en forsikring, skal du sørge for at indhente flere tilbud og sammenligne disse. Ligeledes er det afgørende, at du har en grundig dialog med forsikringsselskabet om din virksomheds konkrete udfordringer og behov. Det er også nødvendigt, at du forstår præcis, hvad der er dækket og ikke dækket. Før du vælger og investerer i en cyberforsikring, kan det derfor være en god ide at følge følgende trin:

7 trin du kan følge, inden du investerer i en cyberforsikring:

1. Skab et overblik over din virksomheds vigtigste data og systemer, og hvor de er placeret. Tag gerne udgangspunkt i virksomhedens risikovurdering.
2. Kortlæg hvilke sikkerhedsforanstaltninger I allerede har implementeret, og hvilke I mangler at implementere, så I kan opfylde kravene fra forsikringsselskabet.
3. Udarbejd en IT-beredskabsplan, så I har styr på den nødvendige forberedelse og konkrete beredskabsinstruktioner i tilfælde af, at I er udsat for en cybersikkerhedshændelse.
4. Overvej om virksomheden har nogen ansatte, der er uddannet til at afhjælpe en potentiel sikkerhedshændelse, eller om virksomheden har brug for eksterne sikkerhedsspecialister?
5. Klarlæg din virksomheds udfordringer, behov og risici i forhold til IT-sikkerhed, så I ved, hvad jeres cyberforsikring skal dække.
6. Indhent tilbud og sammenlign forskellige cyberforsikringstilbud.
7. Skab en dialog med forsikringsselskaberne og spørg ind til, hvad de forskellige forsikringsprodukter dækker og ikke dækker.

Gode spørgsmål at stille til forsikringsselskabet

For at du kan have en kvalificeret dialog med forsikringsselskabet om, hvad deres forsikringsprodukter dækker og ikke dækker, kan du tage udgangspunkt i følgende spørgsmål. På den måde kan I få et bedre overblik over, hvorvidt forsikringsproduktet lever op til virksomhedens behov.

Gode spørgsmål at stille til forsikringsselskabet
Hvad dækker forsikringsproduktet, og hvad dækker den ikke?
Dækkes erstatningskrav fra tredjepart i tilfælde af et cyberangreb, eller hvis personlige data går tabt som et resultat af et databrud i min virksomhed?
Dækkes systemer og software, som er under udvikling?
Dækkes omkostninger, hvis en medarbejder stjæler data i ledtog med en tredjemand?
Dækkes tab, der skyldes en sikkerhedshændelse hos min IT-leverandør?
Dækkes tab af data og systemer, som er leveret af en tredjeparts tjenesteudbyder? Fx på cloudservices?
Dækkes tab af omsætning og mistede indtægter under forretningsafbrydelser, der direkte skyldes cyberangreb (fx DDoS-angreb)?

Dækkes omkostninger forbundet med skade af min virksomheds omdømme?
Dækkes fysiske tab af materielle ting?
Dækkes cyberangreb på baggrund af Social Engineering – fx at en medarbejder er blevet manipuleret til at videresende fortrolige data?
Er det kun tidspunktet under en netværksafbrydelse, der dækkes, eller dækkes den samlede forretningsforstyrrelse på længere sigt?
Hvilke services leverer forsikringsselskabet i det øjeblik, en potentiel sikkerhedshændelse opstår? Hjælper I min virksomhed med fx at forbedre modstandsdygtigheden og styre genopretningen? Er det muligt at få hjælp fra sin egen IT-sikkerhedsleverandør, eller skal man bruge forsikringsselskabet, hvis man har været udsat for et cyberangreb?
Praktikaliteter
Hvor ofte skal forsikringen evalueres? Årligt?
Hvor stor en forsikringssum dækkes?
Hvor høj er selvrisikoen?
Stiller forsikringsselskabet krav om brug af tredjepart til udbedring af skaden?