Kriminalitetsforsikring

Hvorfor etablere en kriminalitetsforsikring?
HDI Danmark tilbyder kriminalitetsforsikring, der dækker risikoen for det formuetab, en virksomhed kan få, hvis de ansatte eller en tredjemand – begår kriminalitet mod virksomheden.

De fleste virksomheder har indført kontrol-foranstaltninger for at begrænse risikoen, men det er ikke muligt at forbygge kriminalitet fuldstændigt. Mange gange foregår det kriminelle forhold over en længere periode, og det gør det sværere at opdage. Derfor bliver det kriminelle forhold ofte kun opdaget ved et tilfælde eller ved udskiftning af personale.

De kriminelle handlinger kan foregå på mange måder, men særligt er virksomhedens bogholderi, varelager og it-systemer udsat for angreb.

Ét er det økonomiske tab, som i værste fald kan true virksomhedens fortsatte eksistens. Noget andet er virksomhedens omdømme, som kan lide et knæk, hvis det kriminelle forhold bliver kendt.

Hvad dækker kriminalitetsforsikringen?
Forsikringen dækker som standard fire væsentlige elementer:

- Direkte formuetab som følge af ansattes kriminelle handlinger.
- Virksomhedens erstatningsansvar som følge af ansattes kriminelle handlinger.
- Direkte formuetab som følge af it-kriminalitet, herunder indbrud i virksomhedens netbank, uanset om det er begået af ansatte eller tredjemand.
- Meromkostninger til rekonstruktion af data tabt som følge af databedrageri eller et dækket indbrud i netbanken.

De fuldstændige forsikringsbetingelser fås ved henvendelse til HDI Danmark.

Eksempler på dækkede skader:

- Underslæb begået af en bogholder, der uberettiget udbetaler penge til sig selv.
- ”Ompostering” af lønninger af en it-medarbejder.
- Hackerindbrud i virksomhedens danske netbankkonti, uanset gerningsmandens geografiske placering.
- Databedrageri, hvor nogen uberettiget har ændret eller slettet data for at opnå vinding og påføre virksomheden et formuetab.

Sammenblanding af roller øger risikoen
Særligt i mindre virksomheder har en bogholder eller regnskabsansvarlig mulighed for selv at anvise et beløb til udbetaling og foretage den faktiske udbetaling. Sammenblanding af roller øger således risikoen for svindel.

Hacker- og virusangreb et stigende problem
Virksomhedens it-systemer bliver stadigt mere komplekse og kræver særlig teknisk indsigt at kunne betjene og vedligeholde, og da hacker- og virusangreb er et stigende problem, risikerer alle virksomheder at blive udsat for angreb, fx mod netbankkonti.

I forbindelse med et angreb mod virksomhedens it-systemer eller netbankkonti dækker forsikringen også omkostninger forbundet med at genetablere tabte data, så virksomhedens drift kan fortsætte med mindst mulig gene efter angrebet.

Forsikringen kan udvides med dækning mod cyberkriminalitet på følgende områder:

- Distribution af ondsindet programkode (malware) – erstatningsansvar over for tredjemand til genopretning af data, hvis I utilsigtet videregiver ondsindet programkode, fx vira, orme, trojanske heste mv. fra jeres it-systemer.
- Notifikation – omkostninger til at notificere jeres kunder om, at et databedrageri rettet mod jer har kompromitteret deres data, samt etablere kreditovervågning (Identity Theft Services).
- Trusler – betaling af løsepenge og omkostninger til afværgelse af trusler om at beskadige eller offentliggøre fortrolige data.
- Genopretning af renommé – omkostninger til ekstern konsulentbistand med henblik på at genetablere virksomhedens renommé efter en dækningsberettiget hændelse.
- Driftstab – nedgang i omsætning af varer og tjenesteydelser efter en dækningsberettiget hændelse.

Distribution af ondsindet programkode
Når I agerer på internettet eller blot har forbindelse til det via jeres intranet, er der risiko for, at kriminelle udnytter sikkerhedsbrister i jeres it-systemer til at installere spionprogrammer, som de kan anvende til at få adgang til fortrolige informationer, fx kundedata, bankoplysninger m.v.

Hvis I på grund af manglende sikkerhedstiltag utilsigtet videredistribuerer sådan ondsindet programkode (malware), risikerer I, at modtagerne af malwaren vil rejse erstatningskrav imod jer, fordi I er blevet ”distributøren” af malwaren.

- ✓ Vores forsikring dækker jeres erstatningsansvar for genopretning af data – ikke det beløb, som dataene udgør.

HDI– Indiakaj 6, 1. – 2100 København Ø – Tlf. 3336 9595 – E-mail: info-dk@hdi-specialty.com

Notifikation
Som mange virksomheder ligger I måske også inde med fortrolige oplysninger om jeres kunder, fx kreditkortoplysninger, bank- og forsikringsoplysninger, helbredsoplysninger og forretningshemmeligheder. Bliver jeres netværk hacket, er der risiko for, at disse oplysninger kan blive misbrugt. Det kan resultere i utilfredse kunder, der i bedste fald ikke længere ønsker at være kunder hos jer. Det kan også betyde, at de ramte kunder vil rejse krav om erstatning for det tab, de har lidt som følge af, at I er blevet hacket.

I en lang række lande, fx USA, Australien og Storbritannien, er der allerede nu krav om, at kunder, hvis data er blevet kompromitteret, skal notificeres. Også i EU er der lovgivning på vej i form af et direktivforslag om samme emne med henblik på at iværksætte tiltag, der mindsker misbrug og reducerer effekten.

- ✓ Vores forsikring dækker udgifter, der afholdes til at notificere jeres kunder efter et databedrageri og etablere kreditovervågning (Identity Theft Services).

Trusler
Det er ikke vanskeligt at forestille sig, at en hacker, der er kommet i besiddelse af fx forretningshemmeligheder, vil kræve at få en løsesum for ikke at offentliggøre fx vitale forretningshemmeligheder. Hackeren kan også true med at gøre netværk og/eller data uanvendelige, hvilket er kritisk for virksomheder, der har brug for at kommunikere og agere med deres kunder via internettet.

- ✓ Vores forsikring dækker såvel løsepenge som omkostninger til afværgelse af truslen.

Genopretning af renommé
Kriminelle handlinger foretaget af en virksomheds ansatte stiller ofte virksomheden selv i et dårligt lys. For at tage vare på virksomhedens renommé kan kriminalitetsforsikringen derfor udvides med dækning af omkostninger til ekstern konsulentbistand. Denne dækning er uden selvrisiko.

Driftstab
Særligt ved it-kriminalitet er der en øget risiko for, at virksomheden efter at være blevet udsat for et angreb vil ligge stille. Det kan tage tid at retablere it-systemerne og sikre, at der er renset ud i alle elementer, som kan være inficerede.

- ✓ Med driftstabsdækningen dækker vi nedgangen i omsætningen, indtil driften er retableret til samme niveau som før skaden, dog højst i 12 måneder.

Hvad koster kriminalitetsforsikringen?
Ved at henvende dig til din sædvanlige betjener af dine forsikringer eller HDI Danmark, kan du få et spørgeskema, som danner baggrund for, at vi kan give dig et tilbud på kriminalitetsforsikringen.

Prisen fastsætter vi ud fra spørgeskemaet og din virksomheds økonomiske forhold. Skemaet indeholder blandt andet spørgsmål om, hvorvidt I har installeret firewalls og antivirusprogrammer, samt hvilke procedurer I har for pengeoverførsler og ansættelse af nyt personale.

Netbankforsikring
I modsætning til hvad der gælder for private forbrugere, dækker pengeinstitutterne i Danmark ikke, hvis en virksomheds netbank bliver udsat for et hackerangreb. Derfor tilbyder HDI Danmark også en netbankforsikring, der alene dækker ved indbrud i virksomhedens netbankkonti – og dermed er det billige alternativ til de virksomheder, der ikke har behov for den mere omfattende kriminalitetsforsikring.

Yderligere information fås ved at kontakte:

HDI
Louise Dam Christiansen
Louise.christiansen@hdi-specialty.com
Tel +45 3142 3184