Bedriftens ansvar
Sikkerhetsforskriftene sier hva bedriften selv skal gjøre for å begrense eller forebygge skader. Dersom disse ikke overholdes, kan erstatningen bli redusert eller falle bort. I tillegg beskrives bedriftens plikter som å melde fra om risiko endres. Dere finner også andre bestemmelser om bedriftens ansvar som det r viktig at dere setter dere inn i. Disse reglene finnes kun i forsikringsbeviset og de er en del av forsikringsavtalen.

Forutsetninger for cyberforsikring - Sikkerhetsforskrift FB038

Forskrift av 01.01.2024. Avløser forskrift av 01.01.2021

1. Forutsetning for rett til erstatning

Retten til erstatning er betinget av at virksomheten:

1.1. Beskytter seg mot skadelig epost

Som sikkerhet mot uønskede og skadelige e-poster skal virksomheten bruke oppdatert
- brannmur som beskytter forsikringstakers nettverk
- antivirusprogram
- aktivt spamfilter.

1.2. Sikkerhetskopierer alle data

Alle data skal sikkerhetskopieres minst hver 5. dag. Hvis forsikringstaker selv tar sikkerhetskopi av lokale medier, må data lagres i en separat låst bygning eller låst databrann- eller sikkerhetsskap. Hvis sikkerhetskopiering gjøres via en online leverandør, må forbindelsen mellom forsikringstaker og leverandør være kryptert.

1.3. Krever passord

- Datamaskiner, computere og nettverk skal beskyttes med et sterkt passord på minst 8 tegn. Passordet skal minimum bestå av en kombinasjon av store og små bokstaver og tall

- Mobile enheter og nettbrett må beskyttes med flerfaktor-autentisering ved ekstern pålogging (MFA*)
- Det skal ikke bruke standard passord eller standard bruker-id på virksomhetens systemer.

1.4. Fysisk sikring

Tilgang til nettverk og IT-utstyr er fysisk sikret mot uautorisert tilgang.

1.5. Krypterer eksterne tilkoblinger

Eksterne tilkoblinger til virksomhetens nettverk er sikret via en sikker, kryptert tilkobling.

1.6. Jevnlig sikkerhetsoppdaterer

- Operativ-/styresystemer som er brukes skal være understøttet og supportert av produsenten med løpende sikkerhetsoppdateringer

- Internettprogram, inkludert 3. parts programmer (for eksempel Java, Adobe Reader, Flash Player og internettsøkemotor) skal kontinuerlig oppdateres til den nyeste versjonen, med mindre det ikke er mulig på grunn av funksjonaliteten til annen programvare.

1.7. Krav til datastyrte produksjons- og prosesseringsmaskiner

Hvis virksomheten bruker datastyrte produksjons-, bearbeidingsmaskiner (prosesseringsmaksiner) e.l., skal disse være koblet til et nettverk som er atskilt fra virksomhetens øvrige IT-nettverk.

1.8. Krav ved bruk av kortbetalingsløsninger

Oppfyller krav som er beskrevet i gjeldende kontrakt med kortinnløser vedrørende håndtering av kredittkortopplysninger (PCI-DSS) dersom virksomheten mottar betalinger via konto-, kreditt- eller debetkort.

1.9. EDR

Bedrifter som produserer programvare, applikasjoner, spill e.l. må ha installert EDR* (Endpoint Detection and Responce).

2. Følgene ved brudd på sikkerhetsforskriftene

Ved overtredelse av sikkerhetskravene skal Tryg være helt uten ansvar, jf. FAL paragraf 4-8.