FÖRKÖPSINFORMATION

Dataintrångsförsäkring

2026-10-01

svedea

Förköpsinformation Dataintrångsförsäkring

Dataintrångsförsäkringen ger specialisthjälp och ersättning om ditt företag utsatts för ett dataintrång, exempelvis en hackerattack eller ett virus, eller genom ett dataintrång inträffat informationsläckage.

Vår dataintrångsförsäkring omfattar

UTREDNINGS- OCH ÅTERSTÄLLANDEKOSTNADER
Kostnader för att vid dataintrång utreda orsak och omfattning samt återställa eller återskapa information eller programvara.

KOSTNADER VID INFORMATIONSLÄCKAGE
Kostnader för krishantering som uppkommer till följd av dataintrång och därigenom inträffat informationsläckage. Det kan vara kostnader för juridiskt biträde och notifiering eller PR-kostnader.

AVBROTTSFÖRSÄKRING
Avbrott som uppkommer i den försäkrade rörelsen till följd av ett ersättningsbart dataintrång. Ansvarstiden, det vill säga den tidsperiod under vilken ersättning kan lämnas, är 120 dagar.

ANSVARSFÖRSÄKRING
Skadeståndsskyldighet för ren förmögenhetsskada och kränkning enligt allmänna skadeståndsrättsliga regler vid skadeståndskrav till följd av ett dataintrång eller informationsläckage som omfattas av försäkringen.

Viktiga undantag och begränsningar

I försäkringen finns undantag när försäkringen inte gäller. De viktigaste undantagen som försäkringen inte omfattar eller gäller för är

- vissa verksamheter som pornografisk verksamhet och vuxenunderhållning, hantering av virtuella valutor, flyg- eller luftfartsverksamhet, onlinespel eller spel om pengar, betalningsförmedling eller verksamhet som samlar data/personuppgifter i syfte att analysera och vidareförmedla dessa
- skada till följd av
  - fel (elektronisk eller tekniskt), avbrott eller störningar i eller på elnätet, allmännyttiga tjänster eller externa telekommunikationstjänster som inte står under den försäkrades direkta operativa kontroll
  - brand, översvämning, jordbävning, vulkanutbrott, explosion, blixtnedslag, storm, hagel, flodvåg, jordskred eller annan naturskada
- skada som orsakas genom intrång i patent, varumärke eller upphovsrätt och inte heller för röjande av icke offentlig känslig företagsinformation eller affärshemlighet
- skada vars uppkomst eller omfattning direkt eller indirekt orsakats av eller står i samband med cyberkrigföring
- ekonomisk förlust/skada eller det belopp (lösensumma) som utges till följd av cyberutpressning
- sak- eller personskada.

Observera även att försäkringen endast omfattar skador som har samband med den verksamhet som är angiven i försäkringsbrevet/-beviset.

Försäkringsbelopp, självrisk och karens

Försäkringsbelopp, självrisk och avbrottsförsäkringens karens framgår av ditt försäkringsbrev. Du betalar endast självrisk om ett dataintrång identifieras.

Säkerhetsföreskrifter

För att minska risken för skada gäller försäkringen med vissa säkerhetsföreskrifter.

Om föreskrifterna inte följs och det inträffar en skada betalas ersättning endast i den utsträckning skadan kan antas ha inträffat även om föreskriften hade följts. Vid allvarlig försummelse kan avdrag göras med upp till 100 %.

De viktigaste säkerhetsföreskrifterna är:

- System och nätverk ska vara skyddade av ett aktivt och professionellt antivirusprogram och en aktiv och professionell hårdvaru- eller mjukvarubrandvägg.
- Säkerhetskopiering (backup) ska göras varje arbetsdag eller med den högre frekvens som vanligen tillämpas inom verksamhetsområdet.
- Datorer och nätverk ska skyddas med ett starkt och unikt lösenord bestående av minst 8 tecken och smartphones och andra mobila enheter ska skyddas med lösenord eller pinkod.
- Datorer, smartphones och andra mobila enheter ska alltid ha ett uppdaterat operativsystem.
- Vid betalning genom konto- eller kreditkort ska tillses att man efterlever det regelverk som reglerar hanteringen av kreditkortsuppgifter, PCI DSS (Payment Card Industry Data Security Standard).
- Anlitas leverantör för exempelvis datasystem- och hostingtjänster eller bearbetning, underhåll eller lagring av elektronisk data, ska det finnas skriftliga avtal som säkerställer att ställda krav är uppfyllda.
- Datorstyrda produktions- och bearbetningsmaskiner ska vara anslutna till ett nätverk som separerats från företagets övriga nätverk.

Vad gör jag om jag misstänker att ett dataintrång inträffat?

Behöver du rådgivning och hjälp ring snarast möjligt vår samarbetspartner PocketSafe. De har öppet dygnet runt. Telefonnumret hittar du på ditt försäkringsbrev eller på vår hemsida Svedea.se.