

MODERNA RISKER KRÄVER ETT MODERNT SKYDD

Cyberförsäkring



Cyberförsäkring

Vad är Söderberg & Partners cyberförsäkring?

Söderberg & Partners har genom noggranna villkorsanalyser och ett nära samarbete med RSG tagit fram en cyberförsäkring som är utformad för att ge ett brett skydd mot de vanligaste cyberriskerna.

Varför teckna en cyberförsäkring?

I dagens digitaliserade samhälle är cyberangrepp ett av de största hoten som företagen står inför. Dessa angrepp blir allt vanligare samtidigt som angreppen blir allt mer sofistikerade och svårare att skydda sig mot. Cyberförsäkringen hjälper er bland annat med en rad åtgärder för att minimera skadan av ett angrepp samtidigt som den ersätter förluster vid eventuella verksamhetsavbrott. Försäkringen skyddar även vid misstag i samband med drift, underhåll eller uppgradering av ert nätverk eller vid andra typer av funktionsstörningar eller funktionsstopp.

I Söderberg & Partners cyberförsäkring erbjuds konsulter ett utökat skydd som, förutom grundomfattningen ersätter skadestånd och försvarskostnader vid krav från tredje man som grundas på vårdslös handling, misstag eller underlåtenhet i samband med konsulttjänster.

Vilka företag bör försäkra sig?

Alla bolag som är beroende av ett fungerande nätverk bör teckna en cyberförsäkring. Har man en omfattande ansvarsexponering, exempelvis genom att man hanterar andra bolags IT-infrastruktur eller personuppgifter är det extra viktigt.

Vad finns det för hot?

Ett cyberangrepp kan uppstå när en angripare sänder ett mail med ett skadligt program till en anställd som av misstag för in viruset i företagets datasystem. Det kan också röra sig om cyberbrott, det vil säga intrång i och spridning av konfidentiell information. Om tredje man lider skada av detta kan ett omfattande skadestånd bli aktuellt. Dessutom kan ett läckage av känslig information skada företagets renommé bland allmänheten. Konsekvenserna av ett angrepp kan alltså bli allvarliga och resultera i omfattande kostnader för företaget.

Exempel på cyberrisker

DDos	Angrepp mot en dator, ett datasystem eller en webbtjänst som hindrar användning genom att överbelasta datasystemet med stora mängder trafik.
Malware	Skadlig kod som förstör eller bereder åtkomst till information eller datasystem.
Cyberutpressning	Skadlig programvara som hindrar åtkomst till datainformation. Utpressaren kräver lösesumma för att användaren ska återfå tillgång till systemet.
ID-kapning	Angriparen utger sig för att vara exempelvis en bank för att få tillgång till personlig information så som kreditkortsuppgifter.
Identitetsbedrägeri	Angriparen utger sig för att vara exempelvis en leverantör för att förmå en behörig person på företaget att föra över pengar eller andra tillgångar.

Försäkringens omfattning

Egna skador

Vid en cyberincident kan företaget drabbas av en rad förluster och skador. Till att börja med är det ofta komplicerat att hitta felet och utreda dess omfattning. För att minimera skadorna är det därför viktigt med en snabb och effektiv incidenthantering. Söderberg & Partners cyberförsäkring erbjuder en omfattande beredskap som hjälper dig med anlitan av IT-specialister, juridiska rådgivare och PR-konsulter för att snabbt hjälpa till med hanteringen av ett intrång, ett utpressningskrav, ett avbrott eller någon annan funktionsstörning samt vid en personuppgiftsincident.

I samband med en cyberincident är det även stor risk för att verksamheten ligger nere under en tid. Cyberförsäkringen täcker ekonomiska förluster som uppstår under denna tid. En stor fördel med lösningen är att avbrottet inte bara täcks vid dataintrång utan även vid avbrott som beror på vårdslöshet, misstag, programmeringsfel eller andra funktionsstörningar. Dessutom täcks avbrott som beror på att någon av ovan nämnda händelser sker hos en IT-leverantör som bolaget anlitar.

En cyberincident kan naturligtvis leda till att datainformation eller programvara skadas eller går förlorad. Cyberförsäkringen täcker både återställandekostnader och utgifter för uppgradering eller byte av programvara eller datorutrustning.

I de fall företaget obehörigt har röjt personuppgifter eller spridit skadlig kod finns risk för att bolaget lider en renomméskada. Cyberförsäkringen täcker de väsentliga förluster som beror på en värdeminskning av företagets verksamhet, varumärke eller kundförluster.

En annan stor cyberrisk för företagen är att drabbas av olika typer av cyberbedrägerier. Det kan handla om att någon utomstående förmår någon på företaget att föra över pengar genom att antingen ta sig in i företagets nätverk eller genom att uppge sig för att vara en kund eller liknande. Sådana förluster täcks även av cyberförsäkringen.

Försäkringens omfattning - Egna skador

Nätverksincident	Kostnader för att hantera ett intrång, avbrott eller en funktionsstörning i bolagets nätverk.
Personuppgiftsincident	Kostnader för att hantera ett obehörigt röjande av eller åtkomst till personlig eller sekretessbelagd information.
Utpressning	Kostnader för att hantera ett utpressningskrav som hotar att leda till spridning eller förstörelse av data och/eller skador på bolagets nätverk.
Verksamhetsavbrott	Täcker ekonomiska förluster, samt kostnader för att minimera dessa, i upp till 90 dagar vid avbrott. Orsaken till avbrottet kan vara såväl cyberangrepp som handhavandefel eller misstag vid underhåll av företagets nätverk.
Återställande av data och programvara	Täcker utgifter för att reparera eller återställa information eller programvara och potentiellt även uppgradera eller ersätta påverkad programvara eller datorutrustning.
Renomméskada	Täcker förluster när företagets varumärke eller verksamhet lider skada på grund av att allmänheten fått vetskap om att företaget obehörigen röjt personuppgifter eller spridit skadlig kod.
Dator- och identitetsbedrägeri	Förluster som beror på felaktiga överföringar av pengar genom obehörig tillgång till nätverket eller genom avsiktligt vilseledande. Det här skyddet täcker även förluster som beror på att tredje part genom uppsåt berett sig tillgång till bolagets telekommunikationssystem.

Se försäkringsvillkor för fullständig information om omfattning och begränsningar.

Försäkringens omfattning

Ansvar för tredje parts skador

Vid cyberincidenter drabbas ofta tredje part av skador som på olika sätt kan drabba företaget som ansvarar för skadan. Det kan exempelvis handla om försvarskostnader och skadestånd som beror på att företaget obehörigt röjt personuppgifter eller datainformation. Sådana kostnader kan även drabba företaget om de spridit skadlig kod eller om de inte kunnat hålla sina avtalsförpliktelser gentemot tredje part på grund av ett verksamhetsavbrott.

En annan risk för bolaget är att skada tredje part genom publicering i media. Cyberförsäkringen täcker skadestånd och försvarskostnader vid exempelvis förtal, integritetskränkning, illojal konkurrens eller immateriella intrång som uppkommer inom ramen för företagets publicering av digital media.

En ytterligare risk för bolaget är att drabbas av kostnader i samband med utredningar av tillsynsmyndighet. Det kan handla om kostnader för att bistå tillsynsmyndigheten under deras undersökning, försvarskostnader samt eventuella sanktionsavgifter och andra avgifter som kan ådömas bolaget.

Styrelse och ledning

En cyberincident kan även medföra att ledande befattningshavare i bolaget drabbas av personliga kostnader. Dessa kostnader kan exempelvis bero på intrång i deras personliga datorutrustning eller bankkonton. Cyberförsäkringen ersätter skäliga och nödvändiga kostnader med anledning av sådana händelser.

Vid tredjepartsskador som beror på personuppgiftsincidenter eller spridning av exempelvis datavirus kan ledande personer även drabbas av personligt ansvar. Försäkringen ersätter försvarskostnader och skadestånd som har samband med sådana skador.

Försäkringens omfattning - Tredje parts skador

Behandling av personuppgifter	Försvarskostnader och skadestånd som beror på obehörigt röjande av eller åtkomst till personuppgifter eller affärshemligheter.
Behandling av datainformation	Försvarskostnader och skadestånd som beror på obehörig tillgång eller förhindrad behörig tillgång till datainformation.
Nätverkssäkerhet	Försvarskostnader och skadestånd som beror på cyberincidenter som t.ex. spridning av skadlig kod eller oavsiktliga avtalsbrott till följd av ett verksamhetsavbrott.
Ansvar för digital media	Krav baserade på förtal, ärekränkning, integritetskränkning m.m. som begåtts vid företagets publicering av digital media.
Ansvar för immateriella rättigheter	Krav baserade på oavsiktligt intrång i upphovsrätt, piratkopiering, renomménlytning m.m. vid publicering av digital media.
Tillsynsförfaranden	Utgifter för hantering vid myndighetsutredning samt tillhörande försvarskostnader och sanktionsavgifter.
Tillsynsåtgärder	Kostnader för juridiska rådgivare och IT-specialister för att upprätta en plan kring de åtgärder som krävs för att efterkomma tillsynsmyndighets verkställighetsmeddelande.

Försäkringens omfattning - Styrelse och ledning

Ledningspersons-incident	Utgifter, förluster och försvarskostnader som drabbar en angiven ledningsperson med anledning av en händelse som täcks av skyddet för incidentåtgärder, utpressning, återställande, ansvar för personuppgiftsbehandling och identitetsbedrägeri.
Ledningspersons-ansvar	Täcker personliga försvarskostnader och skadestånd som en angiven ledningsperson kan bli skyldig att betala vid ett krav gällande en personuppgifts- eller spridningsincident.

Se försäkringsvillkor för fullständig information om omfattning och begränsningar.

Digitaliseringens baksida

Sedan en tid tillbaka har reglerna för hantering av data blivit allt mer strikta. Den verksamhet som behandlar person- och företagsuppgifter har ett ansvar att uppgifterna behandlas och lagras i enlighet med gällande lag. I samband med implementeringen av EU:s nya dataskyddsförordning GDPR har kraven på verksamheter som behandlar dessa uppgifter att ökat. Ett av kraven innebär en skyldighet att anmäla en personuppgiftsincident till tillsynsmyndigheten inom 72 timmar.

Cyberbrott blir även ett allt vanligare fenomen runt om i världen. I USA visades en undersökning från 2013 att nästan 50% av alla bolag utsattes för minst ett cyberbrott, och mörkertalet anses vara stort. Detta har medfört ett uppvaknande hos försäkringsbolagen. Enligt försäkringsbolaget Allianz är cyberincidenter den näst största risken som bolag står inför under 2019.



soderbergpartners.se

OM SÖDERBERG & PARTNERS

Söderberg & Partners grundades 2004 och är en av Sveriges ledande fristående rådgivare och förmedlare av försäkringar och finansiella produkter med en av Nordens största fristående analysavdelningar. Företaget har en mängd olika verksamheter inom fyra affärsområden: Insurance Consulting, Securities & Asset Management, Financial Technology, Payroll & Benefits.