Forsikringsavtalen består av forsikringsbevis og forsikringsvilkår. Beviset gjelder foran vilkårene. Beviset viser hvilke dekninger som er valgt og hva som er bedriftens ansvar. Vilkårene sier hva forsikringen dekker, hvilke unntak som gjelder og hvordan erstatningen beregnes. Bestemmelser som gjelder alle deler av forsikringen kommer først. Deretter kommer bestemmelser for hver dekning. I tillegg gjelder Generelle vilkår (vilkårsnummer BGE90080) for alle våre forsikringer.

Cyberforsikring Ekstra - Vilkår BNLJC918

Vilkår av 01.01.2024. Avløser vilkår av 01.02.2023

Denne forsikringsavtalen består av:
- Forsikringsbevis
- Forsikringsvilkår
- Generelle vilkår BGE90080, med unntak av kapittel 15
- Forsikringsavtaleloven

1. Behandling av personopplysninger og samtykke
På www.tryg.no/sikkerhet-og-personvern/personvern.html kan du lese mer om hvordan vi behandler dine personopplysninger. Her finner du blant annet informasjon om til hvilket formål vi behandler informasjon om deg, hvor opplysningene blir registrert, og hvem opplysningene eventuelt blir gitt videre til. Du kan alltid kontakte oss, hvis du ønsker å vite mer.

2. Hvis det skjer en skade
Skal det straks meldes på telefon 915 04040.
Du er forpliktet til å følge den veiledning og anvisning som du mottar fra oss og våre samarbeidspartnere.

1. Hvem forsikringen gjelder til fordel for

Forsikringen gjelder til fordel for forsikringstaker (sikrede).

Forsikringen gjelder også for datterselskaper som forsikringstaker overtar eller etablerer i løpet av forsikringstiden innen Norge, Sverige eller Danmark når omsetningen i datterselskapet ikke overstiger 20% av morselskapets omsetning per år.

2. Hvor forsikringen gjelder

Forsikringen gjelder i Norge, Danmark og Sverige og på reise og under midlertidig opphold i EU/EØS-området i inntil 3 måneder.

3. Hva forsikringen omfatter

3.1. Undersøkelses-, rekonstruksjons- og utbedringskostnader
3.1.1. Hendelser som er omfattet av forsikringen

Forsikringen dekker nødvendige, rimelige og dokumenterte kostnader til gjenoppbygging (rekonstruksjon) av forsikringstakers IT-systemer, nettverk, programvare og data* som er kryptert, slettet, fjernet eller skadet som følge av et direkte, ondsinnet angrep av skadelig kode, for eksempel:

- Virus*
- Ransomware*
- Hacking
- DDoS-angrep*
- Website hijacking*
- Website defacement*

Forsikringen dekker kostnader som påløper i opptil seks måneder etter at forsikringstaker har konstatert en erstatningsmessig skade eller et erstatningsmessig tap.

3.2. Datatap
3.2.1. Forsikringen omfatter tredjeparts personopplysninger

Ved mistanke om eller konstatering av utilsiktet videresendelse av tredjeparts personopplysninger* fra sikrede eller sikredes databehandler dekker forsikringen nødvendige, rimelige og dokumenterte kostnader til informasjon og rådgivning om gjeldende regler, inkludert rådgivning om hvordan situasjonen skal håndteres

- for å vurdere behov for, og yte, eksperthjelp for å utrede om mistanken om brudd er berettiget eller om det har skjedd et brudd
- for å vurdere rapporterings- og varslingsplikt til myndighetene i henhold til gjeldende lover og berørte parter (de registrerte)
- til rapportering og varsling, jf. strekpunkt ovenfor.

3.2.2. Forutsetninger for dekning
Det er en forutsetning for forsikringen at årsaken til videresendelse av tredjeparts personopplysninger* er utilsiktet, og ikke skyldes forsikringstakers egne forsettlige handlinger eller at forsikringstager har utvist grov uaktsomhet. Det er også en forutsetning at forsikringstaker, ved bruk av databehandler*, benytter skriftlige avtaler, slik at begge parter er kjent med de offentlige krav, som loven stiller vedrørende behandling av personopplysninger*, jf. den til enhver tid gjeldende lovgivning.

3.3. Uten særskilt avtale svarer selskapet ikke for skade eller tap som følge av
- driftsavbrudd
- erstatningsansvar overfor tredjepart som følge av utilsiktet videreformidling av personopplysninger, se punkt 3.2.

4. Når forsikringen gjelder

4.1. Konstatert skade
Forsikringen dekker skade eller tap som konstateres av forsikringstaker i forsikringstiden. Skade eller tap anses for konstatert på det tidspunkt forsikringstaker første gang blir oppmerksom på, eller får mistanke om, at skade eller tap har funnet sted.

4.2. Serieskader
Alle skader som skyldes samme utløsende forhold eller som har sin årsak i en sammenhengende kjede av hendelser, regnes som ett skadetilfelle. Skadetilfellet regnes som konstatert på det tidspunkt første skade konstateres og reguleres av vilkårene på det tidspunkt da første skade konstateres. Har flere sikrede medvirket til en skade, regnes også dette som ett skadetilfelle.

4.3. Etteranmeldelse
Erstatningskrav som er reist mot forsikringstakeren i forsikringsperioden, men som rapporteres til selskapet senere enn tre måneder etter forsikringens slutt, dekkes ikke.

5. Begrensninger som gjelder

5.1. Forsikringen omfatter ikke skade som er en direkte følge av
- naturskade*

- krig, krigslignende handlinger, NBCR-terrorskader (terror-handlinger hvor det anvendes atom, biologiske, kjemiske eller radioaktive våpen), terrorisme*, nøytralitetskrenkelse, borgerkrig, opprør eller borgerlige uroligheter

- beslagleggelse, nasjonalisering eller revolusjon.

5.2. Videre omfatter forsikringen ikke
- indirekte kostnader eller tap, driftstap, renter, bøter, tap av goodwill eller tap som følger av at data* om fordringer, tilgodehavende og fakturabeløp er gått tapt

- direkte eller indirekte økonomisk tap

- kostnader til utskifting av betalingskort, ID-papirer og lignende

- tyveri eller misbruk forårsaket av ansatte* eller andre personer som virksomheten har gitt tillatelse til å benytte virksomhetens identitet

- betaling som er gjort av virksomheten i den tro at betalingsanmodningen var fremsatt av virksomhetens ledelse eller av en særlig betrodd ansatt (CEO-Fraud*/direktørsvindel)

- bøter eller tilsvarende, uansett om de tilfaller en privat eller en offentlig myndighet

- angrep, skade eller tyveri forårsaket av person som eier mer enn 5 prosent av virksomhetens aksjer eller andeler, eller som har vært medlem av forsikringstakers styre eller ledelse/faktisk ledelse, eller som utfører eller har utført arbeide for forsikringstaker i egenskap av selvstendig revisor eller advokat. Dette gjelder uansett om den det gjelder handler alene eller står i ledtog med andre

- kostnader som fabrikant, leverandør eller reparatør er ansvarlig for ifølge kontrakt, lov eller rettspraksis, med mindre denne er gått konkurs, er under suspensjon av betalinger eller er under konkurslignende forhold

- begivenheter som fant sted før forsikringen trådte i kraft, herunder programvare eller data* som var tapt eller skadet innen forsikringen trådte i kraft

- fysisk skade på, herunder tyveri, ran, skadeverk og tap, av forsikringstakers IT-utstyr, IT-system eller nettverk

- kostnader med å fjerne programvarefeil, med mindre feilen er en direkte følge av en ellers erstatningsberettiget skade

- noen form for avtale eller forlik med, eller betaling til, den eller de personer som har utført eller på annen måte medvirket til angrepet, tyveriet eller misbruket

- kostnader som medfører at forsikringstaker blir bedre stilt enn før den dekningsberettigede hendelsen fant sted, inkludert oppgraderinger eller forbedringer av programvare eller data*

- kostnader eller tap som følge av angrep mot forsikringstakers bankkonto, verdipapirdepot eller lignende

- kostnader som skyldes svikt i elektrisitets-, gass- eller annen form for energiforsyning

- ansvar overfor tredjemann som går ut over det som er omfattet under dekningen «Rettslig ansvar ved datatap».

Indirekte følger av angrep som ikke er rettet mot forsikringstaker, for eksempel følger av angrep rettet mot internett-leverandører

- forsikringstakers egne kostnader for oppgjør av erstatningskrav eller for konstatering, eller sannsynliggjøre, en dekningsberettiget hendelse

- saker om immaterielle rettigheter, herunder tvister om rettigheter til navn, design, varemerker, opphavsrett, patenter og domener.

5.3. Forbehold om bortfall eller nedsettelse av erstatningen ved endring av risiko

5.3.1. Hvis forsikringstakers opplysninger om virksomhet og driftsinntekter endrer seg slik at det betinger en høyere premie, vil erstatningen bli redusert forholdsmessig, jf. FAL paragraf 4-7.

5.3.2. Gjelder endringen et forhold av vesentlig betydning for risikoen, skal selskapet være helt uten ansvar, jf. FAL paragraf 4-6.

6. Sikkerhetsforskrifter

Retten til erstatning er betinget av at virksomheten:

6.1. 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.

6.2. 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 databranneller sikkerhetsskap. Hvis sikkerhetskopiering gjøres via en online leverandør, må forbindelsen mellom forsikringstaker og leverandør være kryptert.

6.3. 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.

6.4. Fysisk sikring

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

6.5. Krypterer eksterne tilkoblinger

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

6.6. 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.

6.7. 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.

6.8. 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.

6.9. EDR

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

6.10. Følgende ved brudd på sikkerhetsforskriftene

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

7. Selskapets plikter

7.1. Skadebehandling

Tryg benytter eksterne samarbeidspartnere i skadebehandlingen, som er spesialister på behandling av skader som er omfattet av denne forsikringen.

Tryg utpeker spesialister som skal:

- sikre rekonstruksjon av forsikringstagers IT-systemer, nettverk, programvare eller data*
- foreta juridisk rådgivning i forbindelse ved tap av data/brudd på personlovgivning
- gjennomføre nødvendig rapportering og varsling i forbindelse ved tap av data

med mindre annet er skriftlig avtalt med Tryg.

Tryg videreformidler de nødvendige opplysninger om virksomheten til den eller de spesialister, som er utpekt, slik at spesialistene er i stand til at behandle virksomhetens skade.

Spesialistene vil være selvstendige dataansvarlig for de opplysninger som ekspertene samler inn og registrerer om forsikringstaker. Forsikringstaker skal ta kontakt med den eller de eksperter som Tryg har utpekt, hvis forsikringstaker vil benytte retten til innsikt, har innvendinger mot behandlingen eller korrigere forsikringstakers personlige opplysninger hos den eller de utpekte eksperter.

Forsikringstaker plikter å følge de instrukser fra de utpekte spesialister, bistå med nødvendig dokumentasjon og opplysninger til bruk for sakens behandling, samt samarbeide med Tryg med hensikt å begrense kostnadens størrelse. Tryg kan allikevel i noen tilfeller godkjenne at sikredes vanlige IT-leverandør står for utbedringen.

Forsikringstaker er forpliktet til for egen regning å holde utgifter til dokumentasjon av et erstatningskrav i form av revisjonsuttalelse, -oppgjør eller lignende dersom Tryg krever dette.

7.2. Krav mot tredjepart

I det omfang Tryg har betalt erstatning for skade eller tap som en tredjepart kan holdes ansvarlig for, trer Tryg i Forsikringstakerens krav mot tredjepart.

7.3. Merverdiavgift

Merverdiavgift erstattes når det er dokumentert at avgiften er betalt.

Avgift som kan fradragsføres i merverdiavgiftsregnskapet erstattes ikke.

8. Forsikring i annet selskap

Hvis det er tegnet forsikring for samme type skade i et annet forsikringsselskap, foreligger det dobbeltforsikring, og skaden skal meldes til begge selskap.

Tryg betaler ikke erstatning for skader som det er utbetalt full dekning for hos et annet forsikringsselskap. Har det andre selskapet begrenset dekning i tilfelle med dobbeltforsikring, gjelder de samme begrensninger i denne forsikring. Dermed er Tryg og det andre forsikringsselskapet forpliktet til å betale forholdsmessig erstatning når skaden er dekket av forsikringen.

9. Ordforklaringer

Der det i teksten er vist en * er emnet utdypet i følgende ordforklaring:

Passord
Med tilstrekkelig sikkert passord menes en kode, som inneholder minst 8 tegn, med en kombinasjon av både store og små bokstaver samt tall, og at denne skiftes minimum hver 3 måned. Et passord skal ikke inneholde navn på virksomheten, og skal ikke være identisk med brukernavn eller passord som benyttes i andre sammenhenger i virksomheten.

Ansatte
Enhver lønnet person, herunder trainees og konsulenter som arbeider under en kontrakt i forsikredes tjeneste.

CEO-Fraud/direktørsvindel
Et CEO-Fraud foregår typisk ved at svindleren utgir seg for å være toppsjef som sender en mail ut til en medarbeider i virksomheten. I mailen blir medarbeideren for eksempel bedt om at betale falske regninger, gjøre overførsler til banker i utlandet eller kjøpe produkter i virksomhetens navn.

Data
Data og programmer som kan lastes inn på en datamaskin, som programvare systemoppsettinger. Men data i lukket (ikke-redigerbart) elektroniske kretsløp (IC-krets) regnes ikke som data. Data som forsikringstaker har lagret på eksterne servere, inkludert sky- eller hosting, regnes som forsikringstakers data.

Databehandler
Med en databehandler forstås en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller et annet organ som behandler personopplysninger på den dataansvarliges vegne.

Datterselskap
Som datterselskap regnes juridiske personer (selskaper) hvor forsikringstakeren selv, eller sammen med andre sikrede, eier mer enn 50 % av stemmerettighetene.

Distributed Denial of Service (DDoS)/Denial of Service (DOS)
Angrep utført med forsett til å overbelaste en internettserver i en slik grad at rettmessige forespørsler til serveren ikke kan besvares i tide.

EDR
Endpoint Detection and Responce er en IT-sikkerhetsløsning som installeres på PC/Mac/tablet. EDR detekterer og responderer på trusler og angrep og forhindrer derved virus å spre seg.

Flerfaktor-autentisering
Flerfaktor-autentisering (multi-factor authentication, MFA) er en metode for tilgangskontroll hvor en bruker kun gis adgang etter å ha presentert to eller flere separate bevis for sin identitet ved pålogging. MFA brukes ved ekstern pålogging (f.eks. nettbank).

Forsvarskostnader
Forsvarskostnader defineres som kostnader og utgifter til undersøkelse, avgjørelse eller forsvar av et erstatningskrav, som reises overfor sikrede. Det er en forutsetning for dekningen at det er inngått skriftlig avtale om dette med Tryg.

Fysisk har sikret adgangen
Ved at sikrede fysisk har sikret adgangen menes at virksomhetens IT-utstyr herunder datamaskiner, servere, routere mv. som minimum skal befinne seg i avlåst bygning og lokale utenfor virksomhetens åpningstid.

Hackerangrep
En ulovlig inntrenging i IT-systemet (se også under «Virus»).

Nettverk
Omfatter mobile enheter, USB-nøkler, virksomhetens nettverk og andre databærende medier.

Ransomware
Angrep utført med formål å infisere virksomhetens PC'er og kryptere brukernes filer og dokumenter. Deretter krever hackerne løsepenger for å frigi filene og dokumentene.

Regelmessig (bytte av passord)
Med regelmessig menes at adgangskoden skal endres hver 3. måned. På den måten minimeres sannsynligheten for at det passordet som en kriminell får fatt i, faktisk fungerer. Jo oftere passordet skiftes, desto mindre sannsynlighet er det for at det passordet en hacker har fått fatt i er det nyeste.

Personopplysninger
Med personopplysninger forstås enhver form for informasjon som kan tilbakeføres/tilskrives til bestemte personer, eksempelvis personnummer, bilder, registreringsnummer eller lignende.

Sikker, kryptert tilkobling
Med en sikker, kryptert tilkobling menes en forbindelse som er sikret med kryptering, for eksempel en kryptert VPN-tilkobling (Virtual Private Network).

Naturskade
Skade som direkte skyldes naturulykke ved skred, storm, flom, stormflo, jordskjelv eller vulkanutbrudd, se naturskadeforsikringsloven.

Terrorisme
Med terrorisme menes en handling, herunder - men ikke begrenset til - vold eller trussel om anvendelse av vold, foretatt av en person eller flere personer uavhengig av om de handler på egen hånd eller i forbindelse med en eller flere organisasjoner og/eller myndigheter, begått med politisk, religiøst, ideologisk eller etnisk formål eller begrunnelse, herunder med den hensikt at påvirke en regjering og/eller å spre frykt i offentligheten eller deler av offentligheten.
For at karakterisere handlingen som terrorisme forutsettes, at handlingen er egnet til at påvirke en regjering og/eller spre frykt i offentligheten eller deler av den.

Virus
Med virus menes et program som er utviklet til å spre seg selv med hensikt å påvirke eller skade innholdet i andre programmer, som ofte dermed ødelegges. Et virusangrep er således forårsaket av en automatisk prosess som er initiert for eksempel ved at en i virksomheten har klikket på for eksempel en link i en mail, klikket på en link på en hjemmeside mv.

Website defacement
Ved website defacement-angrep får en hacker adgang til en hjemmeside, og legger sine egne sider inn på den.

Website hijacking
Ondsinnet/uautorisert overtakelse av virksomhetens hjemmeside eller programmer som installeres på din datamaskin via virus*, med mål om å overta kontrollen på hjemmesiden.