

Cyberforsikring 2022, Bedriftens beskyttelse i nye tider

Ingen Amedia-aviser i trykken etter alvorlig dataangrep

Natt til tirsdag ble flere av Amedias sentrale datasystemer angrepet, og personopplysninger kan være på avveie. Onsdag kommer ingen av papiravisene ut.



Nortura sliter fremdeles etter dataangrepet

Selskapet og samarbeidspartnerne har jobbet igjennom helligdagene for å kunne komme opp i normal drift igjen. Men de vet ikke når det kan skje.



NATIONEN

Norsvin etter dataangrepet: – En kostbar og arbeidsom prosess

Avlsselskapet brukte over én måned på å få i gang igjen sine viktigste IT-systemer.



Norsk bilforhandlerkjede hardt rammet av cyberangrep

Minst 30 bilbutikker står uten fungerende IT-system.



Hvorfor cyberforsikring?

- Etter hvert som virksomhetenes aktiviteter blir stadig mer digitaliserte og dermed avhengige av IT og deres digitale nettverk – og i de fleste situasjoner også Internett – øker risikoen for at selskapet er negativt påvirket av en såkalt cyberhendelse. Listen over IT / Cyberrelaterte risikoer som truer bedriftens aktiviteter er lange og kan være både tredjeparts og ansatte som forårsaket cyberhendelsen.
- Cyberrisiko er relevant for alle selskaper – uansett størrelse.
- Nedenfor er noen spørsmål til vurdering av eksponeringen mot cyberhendelser:
 - Hva gjør vi hvis vi ikke har tilgang til e-post?
 - Hva om ordreboken plutselig er utilgjengelig?
 - Hva gjør vi dersom personopplysninger lekkes?
 - Hva gjør vi om alle IT-systemer plutselig er kryptert?

Trygs cyberforsikring - Modulbasert

Utvidet modul for
«**Erstatning for driftstap**»
Dekker: Driftstap som følge av dataangrep

Utvidet modul for «**Ansvar ved datatap**» dekker:

- Rettslig erstatningsansvar som skyldes brudd på personopplysningsloven eller andre brudd på juridisk forpliktelse til å holde tredjeparts opplysninger fortrolige
- Utgifter til gjenoppretting av renommé

Grunnmodul «**Beredskap og eksperthjelp 24/7**» dekker:

- Utgifter for å stoppe et angrep, vurdere skadeomfang og gjenoppbygging av kundens IT-systemer, nettverk, programvare og data
- Gjenoppbygging av programvare og data som følge av funksjonsfeil, feil bruk/tilpasning/konfigurerings eller handlinger begått av egne ansatte når intensjon er å skade data
- Ved tap av 3. manns data omfattes:
 - Vurdere omfang hvis tap av 3. manns data – kan det komme på avveie
 - Informasjon og rådgivning om gjeldende regler og håndtering av situasjonen
 - Rapportering til myndighetene ved behov



Hva dekker forsikringen?

- ✓ Teknisk bistand og rådgivning for å kartlegge omfang av dataangrep
- ✓ Gjenoppbygging av skadet IT-system og nettverk
- ✓ Gjenoppbygging av programvare og data som følge av dataangrep
- ✓ Gjenoppbygging av program og data etter funksjonsfeil
- ✓ Gjenoppbygging av program og data etter dataangrep utført av egne ansatte
- ✓ Angrep mot data i sky-/hostingløsninger
- ✓ Kostnader til informasjon og rådgivning ved tap av personopplysninger
- ✓ Vurdere og utføre rapporterings- og varslingsplikt i forbindelse med tap av tredjemanns data

Forsikringen kan utvides til å omfatte

- ✓ Rettslig erstatningsansvar som følge av brudd på personopplysningsloven
- ✓ Gjenoppretting av renommé
- ✓ Driftstap som følge av et dataangrep



Hva dekker forsikringen ikke?

Her er noen eksempler på hva forsikringen ikke dekker. Vær oppmerksom på at listen ikke er fullstendig. Hele oversikten finnes i vilkårene.

- ✗ Oppgradering eller andre forbedringer av skadet utstyr/nettverk/program
- ✗ Direkte, eller indirekte, økonomisk tap
- ✗ Direktørsvindel
- ✗ Immaterielle rettigheter
- ✗ Fysisk skade på IT-utstyr eller nettverk
- ✗ Utpressing, trusler og lignende
- ✗ Goodwill



Begrensninger i forsikringen

Listen viser noen eksempler hvor rett til utbetaling ved skade kan reduseres eller falle bort

- ! Nettverk og programvare er beskyttet med brannmurer og antivirusprogram
- ! Data blir sikkerhetskopiert jevnlig
- ! At det benyttes unike og sterke passord på mobilt og fast utstyr

Hva dekker cyberforsikringen?

- Kostnader til undersøkelser/ utredning av hendelsen
- Utbedring av skaden/gjenoppretting
- Avbruddstap
- Utpressing, kostnader til å overvinne cyberangrepet
- Kostnader til
 - å beskytte og gjenopprette omdømme
 - juridisk rådgiving og representasjon
 - varsling/notifikasjon
- Ansvar

Dekker ikke

- Fysiske skader
 - Eiendomsforsikring
- Finansielle midler (penger)
 - Kriminalitetsforsikring

IT-leverandør vs. cyberforsikring

	«IT a/s»	Utvidet beredskap med Trygs Cyberforsikring
Teknisk bistand • Undersøke/utrede • Rekonstruksjon av data/programvare • Minimere driftsavbrudd	 Eksperthjelp • Tilgjengelighet? • Kostnad?	 Beredskap og eksperthjelp • 24/7 • Kostnad = egenandel
Avbruddstap		 Økonomisk tap ved drifts-avbrudd, inntil 120 dager
Omdømmebeskyttelse		 Medierådgivning ved spredning av sensitive personopplysninger
Erstatningskrav		 Erstatning for 3. parts tap ved tap av data, brudd på personvernlovgivning osv.
Juridisk bistand		 Advokatutgifter dekkes ved erstatningskrav fra tredjemann
Notifikasjon		 Bistand til lovpålagt varslings av offentlige myndigheter

Ved skade:

Meld fra til Tryg så raskt som mulig gjennom

Arkitektbedriftenes medlemsportal:

Viktig informasjon:

- Hvilken forstyrrelse er det forsikringstaker opplever (ransomware, hacking, virus etc.)?
- Når skjedde det?
- Hvor stort er omfanget av hendelsen?
- Kontaktopplysninger hos forsikringstaker.
- Kan det sendes et skjermbilde av hendelsen?
- Foreligger brudd på GDPR?
- Hvem er påvirket av hendelsen?
- Har hendelsen påvirkning på driften hos forsikringstaker?
- Hvilke lokasjoner er berørte?
- Hvilke tiltak er utført for å minimere omfanget av hendelsen?

Ønsker dere tilbud på cyberforsikring?

Ta kontakt med
Arkitektbedriftenes
Forsikringskontor.

post@arkitektbedriftene.no

Oppgi ønsket forsikringssum:

- Alt. 1: 1 mill
- Alt. 2: 3 mill
- Alt. 3: 5 mill

Oppgi bedriftens driftsinntekter
siste regnskapsår.