# Cyberforsikring
# Bedriftens beskyttelse i nye tider

# Ta kontroll over bedriftens svakeste ledd

**Cyberangrep mot bedrifters pcer, skytjenester og mobile enheter er sterkt økende. Ikke bare store bedrifter rammes, også små bedrifter er i faresonen. Mer enn 90 % av alle bedrifter har vært rammet av et cyberangrep med datainntrengning som resultat. Angrepene blir stadig mer sofistikerte og et omfattende dataangrep kan bli kostbart for bedriften.**
**Med Trygs Cyberforsikring får bedriften en beskyttelse og en beredskap for å håndtere et cyberangrep. I denne brosjyren får du vite mer om hva et cyberangrep er, og hvordan en cyberforsikring kan styrke din bedrift.**

Cyberangrep er en ekstern trussel som har til hensikt å skade, forstyrre eller overbelaste datasystemet. Det kan for eksempel oppstå når en ansatt klikker på en annonse eller åpner et infisert bilag i en mail, som resulterer i at et skadelig program aktiveres i bedriftens datamiljø.

Vanlige konsekvenser av et cyberangrep er at datasystem ikke lenger virker etter sin hensikt eller slutter helt å virke, og avbrudd med økonomisk tap kan oppstå. Kostbare tiltak må iverksettes, ofte med hjelp fra eksterne konsulenter som utreder, gjenoppretter og igangsetter datasystemene som har blitt rammet. Angrepene kan også føre til at kunders data (personopplysninger og annen følsom informasjon) spres ulovlig noe som kan få konsekvenser for bedriftens renomme.

Mange bedrifter har ikke den nødvendige beredskap som kreves for å håndtere et alvorlig angrep. Dersom en bedrift rammes er det viktig at håndteringen er rask slik at konsekvensene blir minimale.

## Særlig utsatte bransjer

- produksjon
- detaljhandel
- e-handel
- publishing
- transportbedrifter
- restauranter
- bokføring
- reklame
- utdanning
- hotell

# Vanlige cyberangrep

### Malware
Skadelige koder som er designet for å få tilgang til eller skade en pc uten at eier oppdager dette. Den skadelige koden installeres for eksempel når en ansatt klikker på en link i en e-post. Malware kan brukes for å samle informasjon om brukeren, som kan anvendes til ulike formål som for eksempel markedsføring.

### Ransomware
En variant av malware som hindrer tilgang til et datasystem. Brukeren kan ikke benytte systemet på normal måte. Det kreves ofte løsepenger for å oppheve hindringen.

### Datavirus
Datavirus er en skadelig programkode som er skapt for å infisere program og filter, og spres gjerne videre i nettverket.

### Distributed Denial of Service (DDoS)
Et DDoS angrep er et forsøk på å gjøre en pc, et nettverk eller en onlinetjeneste utilgjengelig ved å overbelaste den med trafikk fra mange datakilder.

# Sterk bedrift med Trygs Cyberforsikring

### Hjelp mot både eksterne angrep og interne hendelser

Utover eksterne angrep dekker forsikringen også uoversiktlige forhold i bedriftens datamiljø. Dersom det er feil i nyinstallert programvare og dette fører til systemhavari, så kan bedriften få hjelp via forsikringen til å finne årsak, opprette normal drift og få erstattet et eventuelt avbrudd i virksomheten.

### Beredskap døgnet rundt, året rundt

Oppdager dere at bedriften er utsatt for et cyberangrep har dere mulighet til å ringe vår vakttelefon der Charles Taylor vil besvare henvendelsen. Hjelp tilbys 24/7/365.

### Global skadekunnskap – lokal eksperthjelp

Hver skade er unik og krever ulike tiltak. Med Trygs Cyberforsikring håndteres skadene av Charles Taylor, et globalt selskap med tilgang til et nettverk av eksperter med ulike kompetanseområder på lokalt nivå.

# Eksempel på hjelp
# ved angrep og hendelser

### E-handelsbedrift blir utsatt for trussel om et DDos-angrep

En e-handelsbedrift selger varer på Internet og daglig leder mottar en trussel om at hjemmesiden kommer til å bli utsatt for et overbelastningsangrep om bedriften ikke betaler løsepenger innen 24 timer.

### Løsning

Ettersom bedriften har cyberforsikring i Tryg kontaktes Charles Taylor som undersøker og forsøker å avverge trusselen.

### Stålverket får produksjonsstopp

Et selskap som produserer stål har maskiner med programvare. Plutselig slutter maskinene å fungere og produksjonen stopper. Ingen materielle skader inntreffer.

### Løsning

Ettersom bedriften har cyberforsikring i Tryg kontaktes Charles Taylor som koordinerer og sender ut en IT-ekspert for å undersøke hendelsen. Det viser seg at programvaren har blitt infisert av datavirus i forbindelse med programoppdatering. Programvaren gjenopprettes og produksjonen kommer i gang igjen. Avhengig av produksjonsstansens lengde erstattes det økonomiske tapet systemavbruddet har forårsaket.

### Ina åpner feil e-post

Ina får en e-post fra en avsender som utgir seg for å være hennes kollega. I e-posten finnes et vedlegg som kollegaen ber Ina kikke på. Ina klikker på vedlegget og svarer på e-posten. Uten at Ina har merket det har det blitt installert programvare i hennes pc, og en hacker får adgang til personopplysninger tilhørende kunder som deretter spres på en hjemmeside.

### Løsning

Via Trygs Cyberforsikring får bedriften tilgang på juridisk bistand samt en PR-ekspert som vurderer om hendelsen har påvirket bedriftens renomme. Videre kan forsikringen dekke kostnader som påløper for å varsle de personene som har blitt rammet av lekkasjen.

# Overblikk

## Dette inngår i forsikringen

### Beredskap og eksperthjelp

Dersom bedriftens data infiseres, skades eller ødelegges i forbindelse med et cyberangrep får dere hjelp til å undersøke og analysere skadens omfang, hjelp til gjenopprette systemene og gjenskape tapt informasjon for å minimere et eventuelt avbrudd i driften.

### Erstatning ved avbrudd i inntil 120 dager

Ved avbrudd i bedriftens virksomhet på grunn av et cyberangrep dekker forsikringen økonomisk tap i inntil 120 dager.

### Bistand ved erstatningskrav

Har bedriftens kundedata eller annen tredjemannsdata blitt feilbehandlet som følge av et cyberangrep dekker forsikringen erstatningskrav som fremmes mot bedriften som følge av feilbehandlingen.

### Utpressing

Dersom bedriften utsettes for trussel om cyberangrep og det kreves løsepenger for at angrepet skal utebli, dekker forsikringen kostnader for å avverge trusselen.

### Beskyttelse av data i skyen

Dersom bedriften lagrer data hos en skyleverandør dekker forsikringen også datainntrengning som skjer i skytjenesten.

### Omdømme

Dersom kundedata eller annen følsom informasjon stjeles eller spres ulovlig i forbindelse med et cyberangrep, kan dette skade bedriftens omdømme. Forsikringen dekker kostnader til medierådgivning for å beskytte bedriftens omdømme.

## ID- og kredittovervåkingstjenester

Dersom bedriften ulovlig har spredt kunders kredittopplysninger eller personopplysninger som følge av et cyberangrep, dekker forsikringen kostnader ved å overvåke om opplysningene misbrukes.

## Varslingskostnader

Dersom et cyberangrep forårsaker en informasjonslekkasje og det er viktig at kunder eller andre berørte blir informert, dekker forsikringen kostnadene til nødvendig varsling.

## Forsikringen gjelder blant annet ikke ved:

- Konsulentoppdrag og rådgivende virksomhet
- Cyberangrep som forårsaker person- eller tingskade
- Cyberangrep som forårsaker stopp i tilførselen av el-, tele-, tv- og datakommunikasjon
- Cyberangrep som forårsaker formuestap
- Cyberangrep som forårsaker brudd på patentrettigheter

# Skadehåndtering via Charles Taylor
## Global rekkevidde – lokal eksperthjelp

Ved et cyberangrep er det avgjørende at din bedrift får profesjonell skadehåndtering så raskt som mulig. Derfor har Tryg valgt å samarbeide med Charles Taylor som er et selskap som er spesialist på cyberskader. Charles Taylor avgjør hvilke tiltak som skal iverksettes for å finne en løsning. Dere får tilgang til et globalt nettverk av eksperter innen ulike områder som avpasser håndteringen etter skadens karakter.

## Slik håndteres din skade:

1

### Kontakt med Charles Taylor

Mistenker dere at bedriften har blitt utsatt for et angrep kontakter dere Charles Taylor umiddelbart. En koordinator vil innhente nødvendig informasjon og avgjøre hvilke tiltak som skal iverksettes.

2


### Eksperter kobles inn

På bakgrunn av de opplysningene som gis ved melding av skaden instruerer koordinatoren eksperter (IT-konsulenter, jurister, revisorer, PR-konsulenter m.m) som vil undersøke hendelsen. Koordinatoren har lang erfaring med ulike typer skader og vurderer nøye hvilke ressurser som kreves.

3

### Skadehåndtering

Målet er å lokalisere kilden til datainntrengningen innen 48 timer etter at skaden er meldt. Skadens karakter avgjør den etterfølgende skadehåndteringen.

Charles Taylor

# Fordeler med skadehåndtering via Charles Taylor

- Tilgjengelighet 24 timer i døgnet – 365 dager i året
- Eksperter og kriseberedskap på lokalt nivå
- Global skadehåndtering
- Skreddersydd skadehåndtering tilpasset bedriftens behov

# Forutsetninger
# for å tegne Trygs Cyberforsikring

1

### Rutiner ved sikkerhetskopiering

Bedriften skal foreta sikkerhetskopiering minst hver femte arbeidsdag eller oftere dersom dette er vanlig i den aktuelle bransje. Sørg for at sikkerhetskopieringen er komplett og funksjonsdyktig.

2

### Benytt antivirus og brannvegger

Det skal være installert profesjonelle antivirusprogram og profesjonelle softvarebrannvegger for å beskytte bedriftens system og nettverk. Påse at antivirusprogram og brannvegger oppdateres med den høyeste frekvens driften tillater.

3

### Kryptere bedriftens mobile enheter

Mobile enheter som bærbare pcer, mobiltelefoner, lesebrett og liknende skal være hardvarekryptert.

4

### Sørg for å ta imot betaling på riktig måte

Tar bedriften imot betaling ved konto- eller kredittkort? Påse da at regelverket for håndtering av kredittkortopplysninger – PCI-DSS (Payment Card Industry – Data Security Standard) følges.

**Interessert i å tegne Trygs Cyberforsikring?**
Kontakt:
Arkitektbedriftene Forsikringsservice!

**Spørsmål om cyberforsikring?**

Tryg Forsikring
915 04040
www.tryg.no

**Ved mistanke om cyberangrep**

**Charles Taylor Adjusting**
**55172030**