# Det skal du vide om cybersikkerhed

- De bedste sikkerhedsråd til virksomheden
- De farligste og mest udbredte cybertrusler
- De svageste punkter som hackerne leder efter

GlobalConnect

eGuide

# Indhold



GlobalConnect

”Værdien af data har oversteget værdien af råstoffer som guld og olie”

”Moderne cyberkriminelle er professionelle og velorganiserede”

”Truslerne er både alvorlige og reelle”

”Tag ikke fejl. Hackerne er ofte et skridt foran”

# Cyberkriminalitet er en reel forretningsrisiko

Hackerangreb koster danske virksomheder milliarder af kroner om året. Konsulentfirmaet PwC har regnet sig frem til et gennemsnitligt cirkatal for en virksomhed: 1,8 mio. kr. i ekstra udgifter som følge af et vellykket angreb.

Deloitte vurderer, at den private sektor i Danmark samlet set bruger 2 mia. kr. om året på at sikre sig mod digitale trusler. Og truslerne er både alvorlige og reelle. Ved fx at bruge ransomware kan hackerne tage hele jeres it-infrastruktur som ‘gidsel’ ved at lamme den. Først når I betaler en løsesum, er der igen adgang til servere, netværk, databaser og arbejdsstationer.

I en tid, hvor værdien af data har oversteget værdien af råstoffer som guld og olie, er hackerne også på jagt efter forretningskritisk information. Det kan være viden om jeres kunder, strategien for hvordan forretningen skal vækste, forskningsresultater og patenter. Altså, ren og skær industrispionage. Har I overvejet, hvilken værdi jeres forretningshemmeligheder har for virksomheden?

Moderne cyberkriminelle er professionelle og velorganiserede. De arbejder struktureret ud fra klare angrebsstrategier. Sammen med deres hackerkolleger udvikler de avancerede koder og metoder, som kan give adgang til virksomheders data og lamme kritisk infrastruktur.

I mange tilfælde er der tale om state sponsored hacking med nærmest ubegrænsede ressourcer i ryggen. Dét er en svær fjende at bekæmpe ene virksomhed. Og tag ikke fejl. Hackerne er ofte et skridt foran. Og det kan være fatalt for forretningen, hvis I ikke følger med.

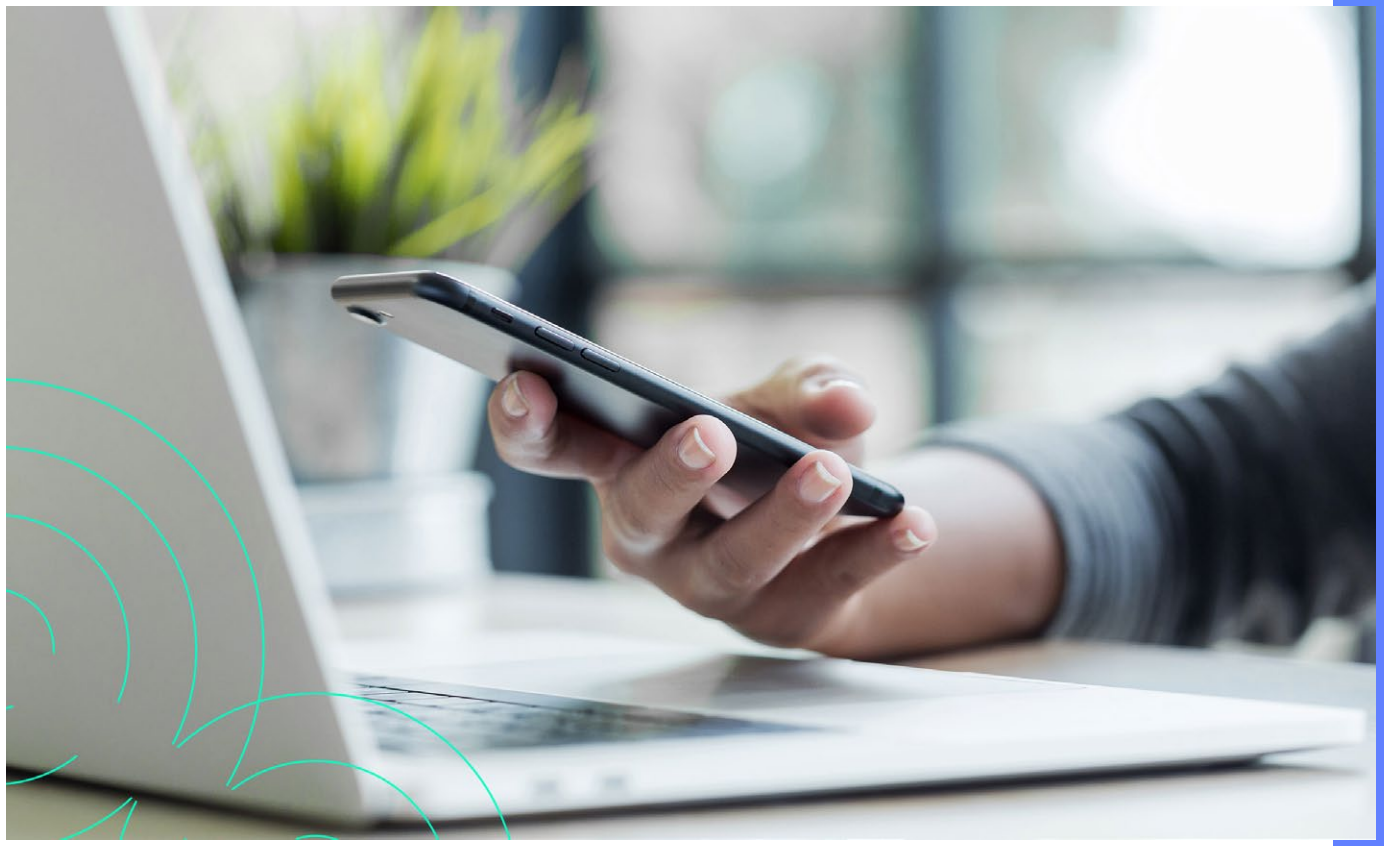
Heldigvis er der forskellige muligheder for at sikre virksomhedens data, beskytte forretningen og skabe tryghed i hverdagen. Det er dem, du kan læse mere om i denne guide.

God læselyst

# Kender du de farligste og mest udbredte cybertrusler?

De cyberkriminelle opfinder konstant nye måder at angribe virksomheder og organisationer på.

På næste side kan du se, hvilke typer af cyberangreb, som er de mest udbredte for tiden, og som I derfor skal være særligt opmærksomme på at sikre jer imod, når I lægger strategien for cybersikkerhed.



- Malware
- Phishing
- MitM-angreb
- DDoS-angreb

## Malware

Malware er en overordnet betegnelse for ondsindet (malicious) software, som fx kan lamme jeres infrastruktur eller tappe vigtig information fra jeres server.

De mest udbredte former for malware er:
- **Spyware,** som stjæler data og information
- **Ransomware,** som låse jeres systemer, indtil I betaler en løsesum
- **Virus og orme,** som spreder sig og nedbryder/ødelægger infrastrukturen

Typisk slipper malware ind i virksomheden, fordi en medarbejder klikker på et farligt link eller en fil i en e-mail. Men der kan også være andre sprækker jeres IT-infrastruktur, hvor hackerne kan finde en vej ind.

## Phishing

Phishing er en metode til at lokke følsomme informationer og data ud af personer og virksomheder.

Phishing bliver mere og mere udbredt. Typisk foregår det via en falsk e-mail, som til forveksling ligner en henvendelse fra jeres bank, fra en samarbejdspartner eller fra en offentlig myndighed.

I mailen bliver modtageren fx opfordret til at videregive kreditkortoplysninger eller login-informationer til virksomhedens datacenter.

Phishing kan også have det formål at skabe en indgang til at installere malware på virksomhedens server.

## MitM-angreb

MitM er en forkortelse for Man-in-the-Middle.

Et MitM-angreb er en moderne form for aflytning, hvor hackere skaffer sig adgang til at placere sig mellem parterne i en samtale eller transaktion.

Så snart hackerne er 'med på linjen', kan de stjæle information og data fra de to parter.

Hackerne får typisk adgang via offentligt tilgængelige netværk, som er uden helt kode eller ikke er sikret med tilstrækkeligt stærke passwords.

## DDoS-angreb

DDoS-angreb (Distributed-Denial-of-service) handler om at overbelaste en virksomheds system, så det ikke kan gennemføre andre transaktioner og handlinger. Hackeren får en koordinerede enheder til at sende utallige forespørgsler mod virksomhedens netværk, så kapaciteten bliver maksimalt belastet, og systemet lukker ned.

# Derfor bliver de cyberkriminelle ved med at hærge

Man kan undre sig over, hvordan hackere og cyberkriminelle stadig har relativt let ved at få adgang til mange virksomheders netværk.

Der har jo været globalt fokus på cybersikkerhed i årevis, og der investeres mange milliarder i sikkerhedsløsninger.

Udover stadigt mere sofistikerede metoder fra hackernes side, er en vigtig del af forklaringen, at den største sikkerhedstrussel ofte er medarbejdernes digitale adfærd.

Og så hjælper det selvfølgelig heller ikke, hvis helt banale sikkerhedsregler ikke bliver overholdt, fx med hensyn til passwords eller fysisk adgang til forskellige områder.

Mange virksomheder har ikke formuleret en intern sikkerhedspolitik. Og hvis de har, er den ikke altid kommunikeret godt nok til virksomhedens ansatte.

Mere skal der faktisk ikke til for at lægge virksomhedens IT-infrastruktur ned med store økonomiske tab til følge.

På næste side kan du se nogle af de yndlingsindgange, ubudne gæster typisk benytter, når de har held til at snige sig ind på jeres netværk.

## Her er hackernes yndlingsindgange

- Wi-fi gæstenetværket
- Netværkskabler
- Spam/E-mails
- IoT - Internet of Things

## Wi-fi gæstenetværket

Alle vil jo gerne gøre det nemt og bekvemt for deres gæster. Men hvis der ingen kode er på gæstenetværket, eller måske bare en nem (og dermed svag) kode, kan en hacker logge sig på udefra, fx fra en bil uskyldigt udseende på parkeringspladsen.

Det er heller ikke usædvanligt, at koden til gæstenetværket er synlig på et skilt, der kan ses fra vinduet. Og så er der jo fri adgang for uvedkommende gæster.

PS. Har I i øvrigt sikret jer, at det ikke er muligt at komme dybt ind i system og netværk, bare fordi man er logget på wi-fien som gæst?

## Netværkskabler

I de fleste virksomheder er der fuld IP-adgang (altså du adgang til hele netværket) via alle netværksporte. Ofte gælder det også for printerporte.

Her behøver hacker ikke engang en kode. Det er nok at skaffe sig fysisk adgang, fx ved at give sig ud for håndværker eller måske leverandør af den daglige frokost.

Derefter skal den ubudne gæst blot have 20-30 sekunder alene i et mødelokale, printerrummet eller et andet sted med en netværksport - så er der fri adgang.

## Spam/E-mails

Et klik på et link eller download af en vedhæftet fil fra en ukendt eller maskeret afsender i en svindelmail, kan lukke hackere ind på jeres netværk.

For få år siden, var den slags mails nemmere at gennemskue (Fx Nigeria-mails på dårligt Google Translate english), men i dag fremstår de langt mere raffinerede og professionelle i både design og sprog.

Svindelmails kan ligne en henvendelse fra en myndighed, eller fra virksomhedens CFO, der hurtigt skal bruge nogle login-oplysninger.

## IoT - Internet of Things

Det bliver mere og mere udbredt at have nye typer af fysiske enheder på netværket, fx voice assistants, smart lysstyring, Smart Tv's eller produktionsmaskiner med internetforbindelse.

Datatrafikken fra enhederne ind i (og ud af!) jeres netværk er svært at få overblik over. Mange af enhederne hører og gør meget mere, end det er nødvendigt og forsvarligt i forhold til datasikkerhed.

Derfor bør I være meget kritiske over for, og bevidste om, hvad I forbinder med netværket. Der kan strømme overraskende meget data til og fra jeres IoT-enheder.

# Invester i cybersikkerhed.
## Det betaler sig

Det giver ikke meget mening at spørge om det kan betale sig at investere i professionel og tidssvarende cybersikkerhed.

Det gode spørgsmål er, om I har råd til at lade være? At investere i sikkerhedsløsninger, der kan forhindre cyberkriminalitet og redde forretningskritiske data (også på grund af uheld eller menneskelige fejl) svarer til at købe en hvilken som helst anden forsikring, som skaber tryghed og sikkerhed omkring forretningen. Hvem ville fx undlade at have en brandforsikring eller en forsikring mod indbrud? Ingen.

Skal man tro den aktuelle trusselsvurdering fra Center for Cybersikkerhed, er risikoen for, at en virksomhed brænder ned, statistisk set mange gange mindre end risikoen for, at I bliver udsat for et angreb, hvor hackere enten kidnapper jeres data og kræver løsesum. Eller simpelthen ødelægger, hvad de kan bare fordi de kan.

Udover de økonomiske tab kan vellykkede cyberangreb og sløset sikkerhed skade jeres anseelse alvorligt. Især hvis I opererer indenfor en branche, hvor sikkerhed omkring data og information er afgørende for kunders og samarbejdspartneres tillid til virksomhed.

Worst-case-scenariet er det samme, uanset om der er tale om hændelige uheld, ærgerlige fejl eller ren cyberkriminalitet: Virksomheden kan ende med at bukke under og lukke helt.

> "It-kriminelle bruger stadig flere og mere avancerede teknikker, når de hacker sig ind i systemer, og det gør truslen større. "
>
> Center for Cybersikkerhed

# De 5 gode råd der kan øge sikkerheden i dagligdagen

## 1

### Bliv del af et globalt sikkerhedsnetværk

Tiden, hvor en Firewall og lidt hjemmelavet integration var nok, er forbi. I dag er det stort set umuligt at beskytte mod stadigt mere sofistikerede sikkerhedstrusler alene. Der skal professionel hjælp til. Jeres sikkerhedsløsning bør være forbundet med globale leverandører af cybersikkerhed, så al software automatisk bliver opdateret og er beskyttet mod nye trusler. Mange IT-leverandører tilbyder færdige sikkerhedspakker, som kan indgå i en samlet løsning med internetadgang.

## 2

### Hold styr på hvem der har adgang til hvad

Skab regler og begrænsninger, som bygger på sund fornuft, altså klare regler for hvem der kan bruge hvilke IT-enheder til hvad og hvor på netværket. Fx at en laptop i bogholderiet kun må tilsluttes fra regnskabsafdelingen og bruge 5 udvalgte programmer. På den måde kan jeres sikkerhedssystem med det samme se, hvis der foregår noget unormalt på - og reagere hurtigt på det.

## 3

### Inddel jeres netværk i sikkerhedszoner

Inddel jeres fysiske og virtuelle netværk i forskellige sikkerhedsniveauer. Alle bør ikke have adgang til alt. I bør definere, hvilke enheder og brugere, der har adgang til hvilke servere og datacentre. I bør også sikre kabler og tilslutningsporte, så alt ikke giver adgang til hele netværket. Hvis I har særligt følsomme områder, bør medarbejdernetværket være fysisk adskilt fra de dele af netværket, der ikke har noget med deres dagli-ge arbejde.

## 4

### Hav to-trins-godkendelser ved log-on

Der er en rigtig god grund til, at bruge to-trins-godkendelse (Fx MS Authenticator eller lignende) som del af sikkerhedsløsningen: Det virker!
En nøglekode på en smartphone eller en anden fysisk enhed, i kombination med en kode, som kun den enkelte bruger kan og skal huske i hovedet, gør er det betydeligt sværere for hackere at skaffe sig log-on-adgang til netværket.

## 5

### Definer automatiske sikkerhedsprocesser

Hvis der opstår et sikkerhedsproblem i virksomhedens netværk, er reaktionshastigheden ofte afgørende for, hvor store skader der kan ske på data og infrastruktur. Der bør være forskellige niveauer for automatiske advarsler og reaktioner, så hele netværket ikke lukker ned, hver gang der er 'et hår i suppen', men samtidig er i stand til at gøre det hurtigt, når der er tegn på en alvorlig trussel. Sikkerhedsprocesserne kan fastlægges sammen med en professionel IT-samarbejdspartner.

# Den direkte vej til større cybersikkerhed

GlobalConnect er et førende teknologi- og datakommunikationsselskab i Nordeuropa.

Vi leverer helhedsløsninger fra jord til sky baseret på egen infrastruktur, der består af 74.500 km fibernetværk og 27.000 kvadratmeter datacenter i Danmark, Sverige, Norge Finland og det nordlige Tyskland.

## Vælg os som professionel IT-partner, når I skal sikre jeres forretningskritiske data.

Jo mere I arbejder og kommunikerer digitalt, jo mere forretningskritisk er det at beskytte jeres data mod uheld, nedbrud og cyberkriminalitet. Fordi det er afgørende for forretningen at sikre uhindret og sikker adgang til lager, kundeoplysninger, logistik, webshop og andre vigtige salgskanaler.

I kan sikre forretningen via intelligente netværksløsninger, tidssvarende backup og effektiv beskyttelse mod hackerangreb med GlobalConnect som professionel IT-samarbejdspartner.

# Vil du vide mere om vores stærke sikkerhedsløsninger?

Ring til os på 7730 3050, læs mere eller kontakt os her

# SmartFiber

## Helt sikkert. Helt enkelt.

SmartFiber fra GlobalConnect er en sikker, lynhurtig og komplet netværksløsning med internet, firewall, wifi og 4G backup.
Perfekt til mindre virksomheder. Helt enkelt.


## Vælg ekstra sikkerhed til din SmartFiber-løsning

Hjemme

**Extended Security**
Ekstra automatisk opdateret sikkerhed på virksomhedens eget netværk med Next Generation Firewall

Ude

**Extended Remote Work**
Log sikkert på virksomhedens netværk udefra, fx ved kundebesøg eller fra hjemmekontoret.

GlobalConnect