KROMANN
REUMERT

# IT-SIKKERHED
## skal op på ledelsesniveau

Januar 2017

**Torben Waage**
Partner

Mobil: +45 40 61 08 86
Direkte: +45 38 77 45 60
tw@kromannreumert.com

# IT-SIKKERHED SKAL OP PÅ LEDELSESNIVEAU

**Hvert år bliver der brugt milliarder af kroner på at beskytte digitale aktiver, så fortrolige informationer undgår at finde vej til offentligheden. Alligevel sker der oftere og oftere sikkerhedsbrud, der potentielt kan true dit forretningsgrundlag. Det er derfor nødvendigt at beskytte sin virksomhed gennem en strategisk tilgang til cyber security, der imødekommer fremtidens skærpede lovkrav og involverer ledelsen i, hvordan ansvaret for IT-sikkerheden skal placeres.**

I Danmark har hackersagen hos CSC, hvor millioner af danske CPR-numre og andre personfølsomme data blev stjålet, medført, at både private og offentlige virksomheder oplever øget kritik for ikke at have styr på IT-sikkerheden. CSC-sagen er blot ét af mange eksempler på et alvorligt brud på IT-sikkerheden. Engang var IT-sikkerhed et anliggende for IT-afdelingen, men i dag er det nødvendigt at udarbejde nye strategiske tiltag, der kan afværge trusler om ulovlig indtrængning i det digitale univers, før det er for sent.

## Sæt strategisk IT-sikkerhed på dagsordenen

Kromann Reumert oplever en stigende efterspørgsel på rådgivning inden for IT-sikkerhed. Vores anbefaling er, at virksomhedens ledelse tager initiativ til at arbejde aktivt med følgende strategiske spørgsmål om IT-sikkerhed:

**1) Hvilke krav skal i leve op til på nuværende tidspunkt?**
Kortlæg først hvilke data, virksomheden opbevarer, og identificér de mest kritiske i forhold til forretningen, kunderne osv. Undersøg hvilke lovgivningsmæssige krav virksomheden er underlagt på nuværende tidspunkt, og hvorvidt I overholder dem. Hvordan håndterer I f.eks. dataopbevaring i kontrakter og leverandøraftaler?

**2) Hvordan er jeres organisation omkring IT-sikkerhed?**
Identificér hvilke procedurer virksomheden har for at sikre data og eventuelle sikkerhedsrisici. Hvad gør I for at forbedre virksomhedens sikkerhed? Er der en egentlig politik for IT-sikkerhed? Er jeres sikkerhedsopdateringer blevet installeret korrekt, og bliver der løbende ført tilsyn med dem? Og hvem har administratorrettigheder?

**3) Hvilke strategiske tiltag kan sikre virksomheden bedre?**
Orientér jer om fremtidig lovgivning og hvorvidt I overholder den. Tag stilling til, om der skal igangsættes projekter, der sikrer, at virksomheden overholder reglerne på området. Læg en plan for, hvordan I håndterer eventuelle brud på sikkerheden.

Når I har udarbejdet en strategi for jeres virksomheds IT-sikkerhed, bør den præsenteres for den øverste ledelse. Alle skal være klar over virksomhedens sikkerhedsmæssige risici og behov for eventuelle nødvendige investeringer for at forbedre sikkerheden.

## Manglende ledelsesfokus øger risiko for cyberangreb

En undersøgelse foretaget af analysehuset IDC i 2014 viste, at der i 149 adspurgte danske firmaer med over 10 ansatte er en bred anerkendelse af, at de udsættes for cyberangreb, eller at uautoriserede brugere opnår uberettiget adgang til data.

Virksomhedernes svækkede IT-sikkerhed udspringer blandt andet af, at virksomhederne ikke har tilstrækkelig fokus på IT-sikkerheden på ledelsesplan. De har ofte heller ikke en egentlig politik for, hvordan de skal sikre virksomhedens IT-sikkerhed og håndtere eventuelle brud. Og det gør dem sårbare. For med en haltende IT-sikkerhed følger store økonomiske og forretningsmæssige omkostninger og risici.

## Brud på IT-sikkerhed har konsekvenser for økonomi og omdømme

Når der sker brud på datasikkerheden, kan det få alvorlige økonomiske og forretningsmæssige konsekvenser.

Det gælder ikke kun i forhold til bødestraf fra myndigheder og omkostninger relateret til at reetablere IT-systemer mv. Virksomhederne betaler også dyrt med negativ omtale, tab af kunder, omsætning og eventuelle sagsanlæg. For nogle virksomheder betyder det også et fald i aktiekursen.

En strategisk tilgang til IT-sikkerhed medfører blandt andet, at eventuelle erstatningskrav ikke kan baseres på virksomhedens passivitet – og at omkostningerne i forhold til at begrænse skaderne samtidigt holdes nede, hvis der fra start har været styr på sikkerheden.

I 2016 oplevede virksomheder verden over en stigning i antallet af ransomware-angreb, der kendetegner sig ved at tage data som gidsel gennem kryptering. En undersøgelse foretaget af cyber security-firmaet Malwarebytes i 2016 viser, at 40 % af de adspurgte virksomheder i England, USA, Canada og Tyskland har oplevet ransomware-angreb inden for det seneste år. Udviklingen forventes at fortsætte ind i 2017 og det forventes, at angrebene vil blive mere sofistikerede og målrettede for at opnå det største udbytte for bagmændene.

Med så omfattende konsekvenser på spil er det nødvendigt, at I sætter IT-sikkerhed højt på ledelsens dagsorden. Det er vigtigt lige nu – men også for at I er ordentligt forberedt til fremtidens skærpede krav.

## Det betaler sig at have styr på IT-sikkerheden

Det betaler sig at have styr på IT-sikkerheden, inden bruddet opstår. Det indebærer, at ledelsen forholder sig konkret til jeres nuværende sikkerhedsprocedurer, og hvad der skal gøres, hvis et brud opstår.

Der kan, ud over de nævnte og mere direkte konsekvenser, også være indirekte konsekvenser ved ikke at have styr på datasikkerheden. Det kan f.eks. være den indvirkning, en manglende IT-sikkerhed kan have på en eventuel salgsproces af en virksomhed.

Købers due diligence bør inkludere undersøgelser af målvirksomhedens opbevaring og beskyttelse af data, ledelsens engagement i IT-sikkerhed, og om der er udarbejdet klare retningslinjer og procedurer for databehandling og eventuelle brud på sikkerheden. Viser det

sig i løbet af en due diligence-fase, at målvirksomheden ikke har fuldt styr på disse forhold, vil dette direkte kunne afspejle sig i den pris, som køber er villig til at give – eller i de garantier, som køber vil forlange af sælger for at minimere risikoen for IT-brud efter overtagelse af den købte virksomhed.

## Forbered jer på skærpede krav i fremtiden

De største investeringer inden for IT-sikkerhed bruges på at overholde gældende regler for behandling og opbevaring af data. Og de krav, som stilles til virksomheder, der behandler data, vil blive væsentligt skærpet, når den ny persondataforordning træder i kraft den 25. maj 2018.

To nye krav i persondataforordningen er principperne om data protection by design og data protection by default. Data protection by design kræver, at design af systemer, der skal håndtere persondata, fremadrettet er særligt indrettet til at tage højde for databeskyttelse, mens data protection by default indeholder et princip om, at de mest begrænsende standardindstillinger skal anvendes som udgangspunkt for håndtering af persondata.

Persondataforordningen medfører ikke kun nye og strammere regler, men medfører også, at de virksomheder, der ikke overholder reglerne for behandling af persondata, risikerer meget større bøder end hidtil.

Bødeudregningen under den nye persondataforordning er baseret på virksomhedens omsætning, som man kender det fra bødeudregning i forbindelse med overtrædelse af konkurrenceretlige regler. Dermed vil en strategisk tilgang til cyber security blot blive endnu mere forretningskritisk for din virksomhed.

[Du kan læse mere om den nye persondataforordning i vores Insight herom: https://www.kromannreumert.com/Insights/2016/Den-nye-persondataforordning

## Vurder hvilke tiltag, der bedst sikrer jer mod IT-sikkerhedsbrud

Datatilsynet har udgivet en række tekster, der beskriver nogle af de problemstillinger, som dataansvarlige- og behandlere bør tage i betragtning.

Teksterne kan fungere som udmærket inspiration, men de er dog langt fra dækkende og ofte meget operationelle. Skal der for alvor styr på IT-sikkerheden, må der andre mere strategiske greb til.

Én måde at gardere jer imod visse konsekvenser af et brud på datasikkerhed er at tegne særlige forsikringsprodukter, der dækker brud på datasikkerhed. Der er, særligt i USA, set en række forskellige produkter, der blandt andet forsikrer virksomheder mod skade forårsaget af hackere eller udgifter til brug for udbedring af et sikkerhedsbrud. Usikkerhed omkring omfanget af dækningen har dog gjort, at forsikringer mod cyberangreb endnu ikke er blevet særlig udbredt.

Kromann Reumert ser grundig strategisk forberedelse som den bedste måde at sikre sig som virksomhed. Dette vil blandt andet medføre, at jeres virksomhed, i tilfælde af brud på IT-sikkerheden, vil spare omkostninger til håndtering af bruddet, fordi en proaktiv indsats vil gøre det nemmere at inddæmme konsekvenserne af bruddet. Samtidig undgår I at skulle bruge store summer på at udvikle en plan, efter at skaden er sket, idet dette er sket under rolige forhold, længe inden bruddet sker.

## Vær på forkant og undgå brud på IT-sikkerheden

- Afklar hvilke lovgivningsmæssige krav virksomheden er underlagt, og hvorvidt I overholder dem.
- Identificér virksomhedens procedurer, i forhold til sikring af data og eventuelle sikkerhedsrisici.
- Orientér jer om fremtidig lovgivning/regulering, og hvorvidt I overholder den.
- Tag stilling til, om der er projekter, som I bør sætte i gang allerede nu, for at sikre at I fortsat overholder reglerne på området.
- Vurder hvilke tiltag, der bedst muligt sikrer jeres virksomhed mod IT-sikkerhedsbrud.
- Inddrag ledelsen i strategien for jeres virksomheds IT-sikkerhed, og afklar, hvor ansvaret for eventuelle brud på IT-sikkerheden skal placeres.

# Kromann Reumerts rådgivning

Kromann Reumert har indsigt i både eksisterende og fremtidig lovgivning, og kan hjælpe virksomheder med at udarbejde konkrete skridt til at imødegå IT-sikkerhedsbrud, herunder udarbejde retningslinjer der medfører overholdelse af de gældende regler eller gennemgå allerede eksisterende systemer og retningslinjer.

**KROMANN REUMERT**

*Kromann Reumerts vision er "Vi sætter standarden". Vi vil ikke nøjes med at være gode - vi vil være de bedste. Vi leverer værdiskabende løsninger og rådgivning med engagement og nærvær. Det opnår vi med fokus på værdierne kvalitet, forretningsforståelse, samarbejdsglæde og troværdighed. Vi er Danmarks førende advokatvirksomhed med kontorer i København, Aarhus og London.*


**KØBENHAVN**

SUNDKROGSGADE 5

DK-2100 KØBENHAVN Ø

**AARHUS**

RÅDHUSPLADSEN 3

DK-8000 AARHUS C

**LONDON**

65 ST. PAUL'S CHURCHYARD

LONDON EC4M 8AB

**ADVOKATFIRMA**

WWW.KROMANNREUMERT.COM

TLF +45 70 12 12 11