IDA OG FSR – DANSKE REVISORER

# ANALYSE AF DATA- OG CYBERSIKKERHED

## DELRAPPORT 2: CYBERSIKKERHED

**VERSION 1.0 19/3-2018**

RAMBØLL

# IDA OG FSR – DANSKE REVISORER
# VERSION 1.0 19/3-2018

| | |
|---|---|
| Revision | **1.0** |
| Dato | **19/03/2018** |

Rambøll
Hannemanns Allé 53
DK-2300 København S
T +45 5161 1000
F +45 5161 1001
www.ramboll.dk

# INDHOLD

# 1. INDLEDNING

Formålet med denne undersøgelse er at tage temperaturen på, hvor langt danske virksomheder er med at gøre sig klar til den nye persondataforordning, der træder i kraft i maj 2018, og hvordan det står til med beredskabet i forhold til cybersikkerhed.

Hovedfokus i undersøgelsen er IDA's medlemmer i offentlige og private virksomheder. Derudover er et mindre antal kommunalt ansatte og lidt over 100 it-ansvarlige i offentlige og private virksomheder blevet spurgt.

Undersøgelsens af status på cybersikkerhed fokuserer på medarbejdernes viden, kompetencer og adfærd.

# 2. KONKLUSIONER

- Det **står generelt ganske godt til, når det handler om medarbejdernes "beredskab" i forhold til cybersikkerhed.**
- Medarbejderne er generelt **godt klædt på til at takle cyberangreb eller misbrug på egen computer.**
- De er i vidt omfang **klar over, hvad de skal passe på med, når de bevæger sig rundt på nettet eller bruger e-mail**.
- De har i det store og hele **en fornuftig adfærd, når det drejer sig om fx backups, omgang med USB-sticks og offentlige WIFI-hotspots, brug af passwords etc**.
- **Hver femte medarbejder er dog ikke uddannet i at minimere risikoen for at inficere virksomhedens it-systemer med virus eller malware**.
- **Kun godt hver tiende medarbejder har deltaget i en eller flere cyber- og datasikkerhedsøvelser,** hvor beredskabet er blevet testet.
- **Mere end to tredjedele af de it-ansvarliges virksomheder har været udsat for hacking eller anden form for ti-angreb i løbet af dette seneste år** – langt størstedelen af angrebene som ransomware. Lang de fleste af angrebene blev stoppet, men under en tredjedel blev anmeldt til politiet eller andre myndigheder.

Selvom det generelle billede er positivt, er kæden ikke stærkere end det svageste led, der skal kun en medarbejder med uhensigtsmæssig adfærd til at lukke malware ind i systemerne. Derfor er det også her vigtigt med en flerlags-strategi, hvor adfærd understøttes af procedurer og systemer, og hvor systemerne så vidt muligt fungerer som bagstoppere for de fejl, mennesker uundgåeligt begår.

Hvor der kan være grund til bekymring, når det drejer sig om paratheden i forhold til persondatabeskyttelse, står det generelt ganske godt til, når det drejer sig om medarbejdernes viden og adfærd i forhold til cybersikkerhed. Her er kæden dog ikke stærkere end det svageste led, og det er derfor også her vigtigt med en flerlags-strategi, hvor adfærd understøttes af procedurer og systemer, og hvor systemerne så vidt muligt fungerer som bagstoppere for de fejl, mennesker uundgåeligt begår. Det er dog også vigtigt at huske, at den overvældende del af respondenterne i undersøgelsen er ingeniører. Alt andet lige kunne man forvente, at ingeniører vil være mere tilbøjelige til at have styr på cybersikkerhed end andre medarbejdergrupper.

# 3. DATAGRUNDLAG

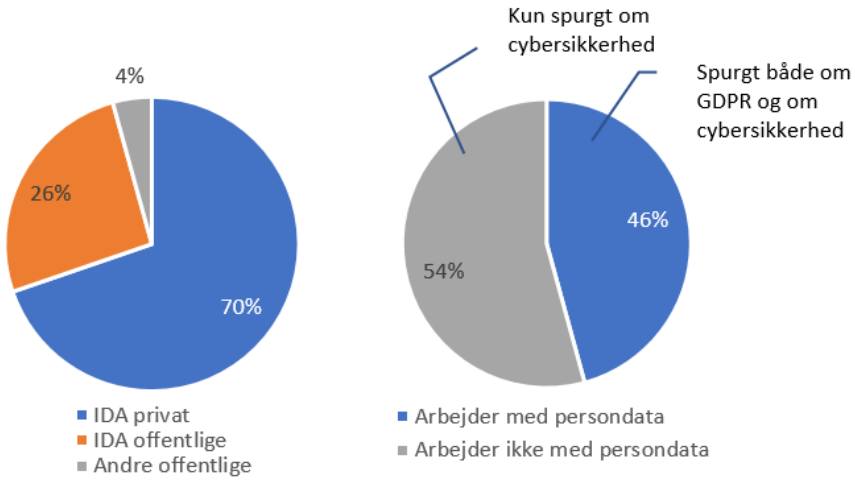
Datagrundlaget for denne rapport er en spørgeskemaundersøgelse henvendt henholdsvis til it-ansvarlige og til medarbejdere i danske offentlige og private virksomheder.

Datagrundlaget for det strategiske niveau består af 113 it-ansvarlige respondenter, hvoraf 89 er fra den private sektor, og 24 er fra den offentlige sektor.

*Det lille antal respondenter betyder, at data fra det strategiske niveau kun kan bruges til at give nogle forsigtige indikationer om tingene tilstand.*

Datagrundlaget for det operationelle niveau består af 1.215 medarbejdere, hvoraf 849 respondenter er ansat i det private, og 366 respondenter er ansat i den offentlige sektor. Langt størstedelen af respondenterne på det operationelle niveau er hentet i IDA's medlemsbase og er derfor ingeniører. Der er altså tale om en særlig – og må det antages – som udgangspunkt relativt teknisk minded målgruppe. Undersøgelsens resultater kan derfor ikke uden videre tages til indtægt for alle medarbejdere.

Spørgsmålene til det operationelle niveau i Datasikkerheds- eller GDPR-delen af undersøgelsen er dog kun stillet til respondenter, der har angivet, at de arbejder med persondata i deres job. Det gælder 555 respondenter, hvoraf 289 er fra private virksomheder, og 266 fra det offentlige.




For yderligere information om datagrundlaget og undersøgelsens metode henvises til Bilag 1: Metode.

## 3.1 Profil af deltagerne

Dette afsnit indeholder en række tabeller, der beskriver fordelingen af respondenter på geografi, virksomhedsstørrelse og kommunestørrelse. Tabellerne giver en indikation af datagrundlaget og dermed de "stemmer", der er hørt i undersøgelsen.

### 3.1.1 Fordeling af respondenter på geografi (i pct. af det samlede antal deltagere i kategorierne)

Vi har respondenter fra hele landet. Region Nord og Region Sjælland er antageligt noget underrepræsenteret i undersøgelsen. Men da vi ikke har data om, hvor i landet de IDA-medlemmer, vi har spurgt, bor, er det vanskeligt at sige noget præcist om den geografiske repræsentativitet.

(Tabel på næste side).

| Regioner | | | Nord | Midt | Syd | Sjælland | Hovedstaden | I alt |
|---|---|---|---|---|---|---|---|---|
| Strategisk | Offentlig | n | 1 | 8 | 4 | 2 | 9 | 24 |
| | | % | 4% | 33% | 17% | 8% | 38% | 100% |
| | Privat | n | 2 | 22 | 17 | 4 | 44 | 89 |
| | | % | 2% | 25% | 19% | 4% | 49% | 100% |
| | I alt | n | 3 | 30 | 21 | 6 | 53 | 113 |
| | | % | 3% | 27% | 19% | 5% | 47% | 100% |
| Operationelt | Offentlig (IDA-medlemmer) | n | 47 | 74 | 74 | 32 | 88 | 315 |
| | | % | 15% | 23% | 23% | 10% | 28% | 100% |
| | Offentlig (via Fagchefer) | n | 3 | 10 | 21 | 15 | 3 | 52 |
| | | % | 6% | 19% | 40% | 29% | 6% | 100% |
| | Privat (IDA-medlemmer) | n | 48 | 169 | 114 | 41 | 474 | 846 |
| | | % | 6% | 20% | 13% | 5% | 56% | 100% |
| | I alt | n | 98 | 253 | 209 | 88 | 565 | 1.213 |
| | | % | 8% | 21% | 17% | 7% | 47% | 100% |

### 3.1.2 Fordeling af offentlige respondenter på kommunestørrelse

Langt de fleste deltagere i den operationelle undersøgelse har svaret på spørgsmålet om kommunestørrelse og arbejder derfor antageligt i en kommune*. Der er her en ret ligelig fordeling mellem stor og små kommuner.

| Kommunestørrelse (målt på antal borgere) | | Små | Mellemstor | Store | I alt |
|---|---|---|---|---|---|
| Strategisk | n | 3 | 4 | 11 | 24 |
| | % | 17% | 22% | 61% | 100% |
| Operationelt | n | 133 | 113 | 106 | 366 |
| | % | 38% | 32% | 30% | 100% |
| I alt | n | 136 | 117 | 117 | 390 |
| | % | 37% | 32% | 32% | 100% |

Procentsatsen viser andelen af respondenter fra små, mellemstore og store kommuner for henholdsvis strategisk niveau, operationelt niveau og i alt.

*Oprindeligt blev dette spørgsmål stillet til alle på den "offentlige" liste, uanset om de arbejdede i en kommune eller ej. Antagelig er der en del, der har svaret på spørgsmålet alene for at kunne komme videre i undersøgelsen – også selvom de evt. ikke arbejdede i en kommune. Det blev dog ret hurtigt rettet, så man kun skulle svare, hvis man arbejdede i en kommune.

### 3.1.3 Fordeling af private respondenter på virksomhedsstørrelse

Medarbejdere fra store virksomheder er overrepræsenterede i undersøgelsen, mens medarbejdere i små virksomheder er underrepræsenterede. Dette kan dog skyldes frekvensen af ingeniører, som antageligt er større i store end i små virksomheder. Undersøgelsen kan derfor stadig godt være repræsentativ for virksomhedsstørrelse i forhold til ingeniørerne.

| Virksomhedsstørrelser | Antal ansatte |
|---|---|
| Små | 1-50 |
| Mellemstore | 51-250 |
| Store | 251+ |

(Tabel på næste side).

| Virksomhedstørrelse (målt på ansatte) | | Små 0-50 | Mellemstor 51-250 | Store 250+ | I alt |
|---|---|---|---|---|---|
| Population | % af alle DK-virksomheder | 97,4% | 2,1% | 0,5% | 165.667 |
| | % af medarbejder i all DK-virksomheder | 31% | 16% | 53% | 2.195.576 |
| Strategisk | N | 7 | 24 | 58 | 89 |
| | % | 8% | 27% | 65% | 100% |
| Operationelt | N | 151 | 181 | 515 | 849 |
| | % | 18% | 21% | 61% | 100% |
| I alt | N | 158 | 205 | 573 | 938 |
| | % | 17% | 22% | 61% | 100% |

Procentsatsen viser andelen af respondenter fra små, mellemstore og store virksomheder for henholdsvis strategisk niveau, operationelt niveau og i alt.

### 3.1.4 Fordeling af respondenter på branche (operationel del)

| **Branche** | Fremstilling | Forsyning | Handel/ service | Offentlig | Finans | It og tele | Bygge og anlæg | Andet |
|---|---|---|---|---|---|---|---|---|
| n | 315 | 87 | 158 | 27 | 12 | 121 | 84 | 45 |
| Fordeling | 37% | 10% | 19% | 3% | 1% | 14% | 10% | 5% |

Procentsatsen viser andelen respondenter fordelt på forskellige brancher.

### 3.1.5 Fordeling af respondenter på roller i forhold til data- og cybersikkerhed

Respondenterne er alt overvejende medarbejdere, der ikke har data- eller cybersikkerhed som en selvstændig del af deres arbejde. Deres svar kan altså betragtes som værende repræsentative for "almindelige" medarbejdere (eller rettet "almindelige" ingeniører).

| Hvad er din rolle i forhold til virksomhedens cyber- og datasikkerhed? | | Jeg arbejder med cyber- og datasikkerhed som den vigtigste del af mit job | Jeg arbejder med cyber- og datasikkerhed som en del af mit job | Jeg arbejder i it-afdelingen, men har ikke så meget med cyber- og datasikkerhed at gøre | Jeg arbejder i andre dele af virksomheden og arbejder ikke med cyber- og datasikkerhed som en selvstændig del af mit arbejde | Andet | N |
|---|---|---|---|---|---|---|---|
| | Privat | 1% | 9% | 6% | 84% | 1% | 849 |
| | Offentlig | 1% | 7% | 1% | 89% | 2% | 367 |
| | **Alle** | **1%** | **8%** | **5%** | **85%** | **1%** | **1216** |

Procentsatsen viser fordelingen af respondenterne set i forhold til, hvordan de arbejder med cybersikkerhed.

# 4. ANALYSE

## 4.1 Introduktion

I takt med stigende digitalisering af produkter, processer og services er cybersikkerhed mere relevant end nogensinde før. Flere og flere processer håndteres digitalt, hvilket øger antallet af steder og it-systemer, hvor virksomheder kan udsættes for angreb.

Dette kapitel beskriver virksomhedernes håndtering af og udfordringer med cybersikkerhed, herunder medarbejdernes adfærd på digitale medier og viden om, hvordan deres digitale adfærd kan påvirke risikoen for angreb eller misbrug af arbejdscomputere og virksomhedens it-systemer.

## 4.2 Temaer

Tabeller med data fra undersøgelsen blandt IDA's medlemmer er markeret med en grøn header. Data fra undersøgelsen blandt kommunale ledere er markeret med en blå header.

### 4.2.1 Medarbejdernes viden og kompetencer

Dette tema beskriver medarbejdernes (selvrapporterede) viden og kompetencer i relation til cybersikkerhed.

**Medarbejderne er generelt godt klædt på til at takle cyberangreb eller misbrug af egen computer**

Medarbejderne er generelt godt rustet til at håndtere cyberangreb eller misbrug af egen computer. 85 % angiver således, at de ved, hvad de skal gøre, hvis deres arbejdscomputer udsættes for angreb eller misbrug.

| Cybersikkerhed | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg ved, hvad jeg skal gøre, hvis min arbejdscomputer udsættes for angreb eller misbrug | Privat | 6% | 8% | 85% | 1% | 849 |
| | Offentlig | 5% | 10% | 84% | 1% | 367 |
| | **Alle** | **5%** | **9%** | **85%** | **1%** | **1216** |

Medarbejdere i små (79 %) og mellemstore (77 %) private virksomheder angiver i høj grad, at de ved, hvad de skal gøre, hvis deres computer udsættes for angreb, men medarbejdere i store virksomheder er endnu bedre beredt. Her angiver 89 % af medarbejderne, at de ved, hvad de skal gøre i tilfælde af angreb eller misbrug af deres computer.

**Omtrent hver femte medarbejder er ikke uddannet i at minimere risikoen for at inficere virksomhedens it-systemer med virus eller malware**

Omtrent 20 % fortæller, at de ikke har modtaget uddannelse i at mindske risikoen for inficering af virksomhedens it-systemer med virus eller malware. Stort set alle medarbejdere arbejder med computer og har internet, og er dermed i praksis udsat for potentielle angreb og bør derfor introduceres til, hvordan risikoen for inficering af it-systemer kan minimeres.

| Cybersikkerhed | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg er blevet uddannet i, hvordan jeg i praksis kan mindske risikoen for, at virksomhedens it-systemer inficeres af virus eller anden skadelig kode (malware). | Privat | 20% | 16% | 64% | 1% | 849 |
| | Offentlig | 23% | 17% | 57% | 2% | 367 |
| | **Alle** | **21%** | **16%** | **62%** | **1%** | **1216** |

**Store virksomheder uddanner i højere grad medarbejderne i at minimere risikoen for at inficere virksomhedens it-systemer med virus eller malware**

Halvdelen af medarbejdere i små og mellemstore virksomheder angiver, at de har modtaget uddannelse i, hvordan de i praksis kan mindske risikoen for, at virksomhedens it-systemer inficeres af virus eller anden skadelig kode (malware). Dette tal stiger til lige knap trefjerdedele, når vi spørger medarbejderne i store virksomheder. Denne uddannelses indsats kan bidrage til at forklare, hvorfor flere medarbejdere i store virksomheder ved, hvad de skal gøre i tilfælde af angreb eller misbrug af deres arbejdscomputer.

| Cybersikkerhed | Privat | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg er blevet uddannet i, hvordan jeg i praksis kan mindske risikoen for, at virksomhedens it-systemer inficeres af virus eller anden skadelig kode (malware). | Små | 31% | 16% | 51% | 2% | 151 |
| | Mellemstore | 29% | 20% | 50% | 1% | 181 |
| | Store | 13% | 14% | 72% | 1% | 515 |
| | **Privat i alt** | 20% | 16% | 64% | 1% | 849 |

### Under halvdelen af respondenterne modtager regelmæssig opdatering af deres viden om virksomhedens cyber- og datasikkerhed

Det er langt fra alle medarbejdere, der oplever, at deres viden om cyber- og datasikkerhed jævnligt opdateres.

| Cybersikkerhed | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Min viden om virksomhedens cyber- og datasikkerhed genopfriskes og opdateres jævnligt | Privat | 31% | 23% | 44% | 2% | 849 |
| | Offentlig | 34% | 23% | 40% | 3% | 367 |
| | **Alle** | **32%** | **23%** | **43%** | **2%** | **1216** |

### Flere medarbejdere i store virksomheder oplever regelmæssig opdatering af deres viden om cyber- og datasikkerhed

Ser vi udelukkende på medarbejderne i de store private virksomheder, angiver halvdelen (51 %), at deres viden opdateres jævnligt. Det gælder 32 % af respondenterne i små virksomheder og 35 % i mellemstore virksomheder.

### Kun godt hver tiende medarbejder har deltaget i en eller flere cyber- og datasikkerhedsøvelser, hvor beredskabet er blevet testet

Sådanne øvelser kan være komplicerede at tilrettelægge, og det vil derfor ofte være vanskeligt særligt for små virksomheder at arrangere dem. Men at kun 11 % har været igennem en sådan øvelse er alligevel problematisk. Dette gælder 7 % af medarbejderne fra små private virksomheder, 8% fra mellemstore virksomheder og 14 % fra de store virksomheder.

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg har deltaget i en eller flere cyber- og datasikkerhedsøvelser, hvor beredskabet er blevet testet | Privat | 77% | 8% | 13% | 2% | 849 |
| | Offentlig | 78% | 11% | 7% | 3% | 367 |
| | **Alle** | **77%** | **9%** | **11%** | **2%** | **1216** |

### Medarbejderne er i vidt omfang klar over, hvad de skal passe på med, når de bevæger sig rundt på nettet eller bruger e-mail

Lang de fleste medarbejdere ved, hvad de skal være opmærksomme på, når de bevæger sig rundt på nettet eller bruger mail. Da netop mail og browsing er de mest udbredte angrebsveje, er dette meget positivt. Spørgsmålet er så bare, om det er tilstrækkeligt – der skal jo kun et uheldigt klik til, før der potentielt er åbnet for et angreb. Man når aldrig 100 %, men man skal nok endnu højere op end 84%.

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg ved, hvad jeg skal være opmærksom på, når jeg fx klikker på link eller vedhæftede filer, eller besøger hjemmesider for at undgå at bringe virksomhedens data eller systemer i fare. | Privat | 5% | 8% | 86% | 1% | 849 |
| | Offentlig | 8% | 12% | 79% | 1% | 367 |
| | **Alle** | **6%** | **9%** | **84%** | **1%** | **1216** |

## 4.2.2 Medarbejder adfærd

Dette tema beskriver medarbejdernes (selvrapporterede) adfærd i relation til cybersikkerhed.

Medarbejderne har i vidt omfang en sund og hensigtsmæssig adfærd, når det drejer sig om at beskytte mod uautoriseret adgang til systemer og data og om at sikre muligheden for genetablering af data ved hjælp af backups. Kun i forhold til omgangen med passwords er adfærden lidt mindre hensigtsmæssig, særligt i forhold til genbrug og deling af passwords.

Når det er sagt, er der for de øvrige – ikke password-relaterede spørgsmål, mellem 7 og 9 % af deltagerne, der har en uhensigtsmæssig adfærd, og det kan i den virkelige verden være tilstrækkeligt til, at en angriber kan finde et hul.

**Langt de fleste har sat deres enheder op til at låse automatisk**

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Min computer og andre enheder (fx tablets og mobil) er sat op således, at de låser efter kort tid (fx 5 minutter), hvis jeg ikke bruger dem. | Privat | 8% | 7% | 83% | 2% | 849 |
| | Offentlig | 5% | 5% | 88% | 2% | 367 |
| | **Alle** | **7%** | **6%** | **85%** | **2%** | **1216** |

**Langt de fleste sikrer også backup af deres arbejdsrelaterede filer**

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg laver jævnligt backup af mine arbejdsfiler (eller opbevarer dem i systemer/på drev, der backes up centralt). | Privat | 8% | 5% | 86% | 2% | 849 |
| | Offentlig | 11% | 7% | 78% | 4% | 367 |
| | **Alle** | **9%** | **6%** | **83%** | **2%** | **1216** |

**De fleste er opmærksomme på risikoen ved at bruge USB-sticks og andre flytbare medier**

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg er opmærksom på risikoen ved brug af USB-sticks og andre flytbare medier. | Privat | 7% | 11% | 81% | 1% | 849 |
| | Offentlig | 9% | 17% | 72% | 2% | 367 |
| | **Alle** | **8%** | **13%** | **78%** | **1%** | **1216** |

**De fleste er også opmærksomme på risikoen ved at bruge offentlige WIFI-hotspots**

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg er opmærksom på risikoen ved brug af offentlige WIFI hotspots. | Privat | 10% | 13% | 76% | 1% | 849 |
| | Offentlig | 17% | 14% | 64% | 4% | 367 |
| | **Alle** | **12%** | **14%** | **72%** | **2%** | **1216** |

**Kun lidt under halvdelen genbruger ikke deres password/kodeord flere steder**

| | Sektor | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|---|
| Jeg genbruger mit password/kodeord flere steder. | Privat | 45% | 19% | 36% | 1% | 849 |
| | Offentlig | 46% | 25% | 29% | 1% | 367 |
| | **Alle** | **45%** | **21%** | **34%** | **1%** | **1216** |

**Langt de fleste undgår at dele deres password med andre**

| | | Aldrig | En gang i mellem | Ofte | Ved ikke | n |
|---|---|---|---|---|---|---|
| Jeg har delt mit password til virksomhedens it-systemer med andre ansatte (uden for it-afdelingen). | Privat | 88% | 11% | 1% | 0% | 849 |
| | Offentlig | 83% | 17% | 0% | 0% | 367 |
| | **Alle** | **87%** | **13%** | **0%** | **0%** | **1216** |

**Godt en femtedel har skrevet deres password ned hvis de skulle glemme det**

| | | Ja | Nej | Ved ikke | n |
|---|---|---|---|---|---|
| Jeg har skrevet mit password ned (fx på mobilen eller på en seddel), hvis jeg skulle komme til at glemme det. | Privat | 19% | 81% | 0% | 849 |
| | Offentlig | 28% | 72% | 0% | 367 |
| | **Alle** | **21%** | **78%** | **0%** | **1216** |

### 4.2.3 Beredskab

På en række områder er beredskabet i forhold til cybersikkerhed for lavt hos de 113 virksomheder, der har besvaret undersøgelsen. De fleste foretager løbende risikovurderinger, og der er styr

på den formelle ansvarsfordeling i organisationen, men når det drejer sig om kommunikation til medarbejdere, kunder og leverandører, afholdelse af cybersikkerhedsøvelser og den enkelte medarbejders egen rolle har kun mellem en tredjedel og godt halvdelen et tilstrækkeligt beredskab.

| **Beredskab** | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|
| Virksomheden foretager løbende risikovurderinger med hensyn til cyber- og datasikkerhed | 10% | 17% | 73% | 1% | **113** |
| Virksomheden har udarbejdet en beredskabsplan med hensyn til cyber- og datasikkerhed med en fastlagt plan for, hvem der gør hvad i tilfælde af forskellige former for it-nedbrud eller angreb | 19% | 15% | 65% | 1% | **113** |
| Virksomhedens ansatte kender deres egen rolle i beredskabsplanen | 27% | 15% | 57% | 2% | **113** |
| Der er en klar ansvarsfordeling på it-området. Ansvaret for sikkerhed på de enkelte it-services er uddelegeret til konkrete personer? (Fx mail-service, registre m.m.) | 8% | 19% | 72% | 2% | **113** |
| Virksomheden har en kommunikationsplan til medarbejdere i tilfælde af et cyberangreb | 33% | 20% | 42% | 4% | **113** |
| Virksomheden har en kommunikationsplan til kunder og leverandører i tilfælde af et cyberangreb | 41% | 19% | 35% | 4% | **113** |
| Virksomheden afholder jævnligt cybersikkerhedsøvelser, hvor beredskabet testes | 42% | 19% | 35% | 4% | **113** |

### 4.2.4 Sikkerhed

Virksomhederne i undersøgelsen ser ud til i det store og hele at have de nødvendige sikkerhedsprocedurer på plads. Dog er der 18 %, der ikke logger aktiviteter i it-systemerne, og 17 %, der ikke bruger kryptering. Hvorvidt dette er et problem afhænger dog i høj grad af naturen af virksomhedens aktiviteter.

| **Sikkerhed** | 1+2 | 3 | 4+5 | v. ikke | n |
|---|---|---|---|---|---|
| Virksomheden har de nødvendige advarselsværktøjer, så man kan opdage angreb mod virksomhedens it-systemer | 8% | 22% | 66% | 4% | **113** |
| Virksomheden har de nødvendige værktøjer, så man kan stoppe angreb mod virksomhedens it-systemer | 7% | 17% | 72% | 4% | **113** |
| Virksomheden logger aktivitet i it-systemerne og har redskaberne til at opdage uregelmæssigheder | 18% | 19% | 59% | 4% | **113** |
| Virksomheden har en proces for vedligeholdelse af brugerrettigheder, så brugerne kun har adgang til det, de aktuelt har brug for | 11% | 14% | 74% | 1% | **113** |
| Virksomheden bruger kryptering af data for at øge datasikkerheden | 17% | 24% | 56% | 4% | **113** |
| Virksomheden foretager systematisk backup | 0% | 2% | 98% | 0% | **113** |
| Virksomheden har begrænsninger for eksekvering af "farlige" filtyper | 6% | 10% | 77% | 7% | **113** |
| Virksomheden har begrænset netværksadgang for eksterne parter | 2% | 5% | 92% | 1% | **113** |

### 4.2.5 Udfordringer og barrierer (Strategisk niveau)

Den væsentligste udfordring for de 113 virksomhedernes indsats i forhold til data- og cybersikkerhed er ifølge de it-ansvarlige manglende ressourcer, at reglerne for håndtering af persondata er svære at forstå, og at reglerne er svære at leve op til i det daglige.

| **Udfordringer og barrierer (offentlig og privat)** | 1+2 | 3 | 4+5 | Ved ikke | n |
|---|---|---|---|---|---|
| Virksomheden mangler ressourcer til at løfte opgaven | **39%** | **25%** | **35%** | **2%** | **113** |
| Virksomheden mangler kompetencer til at løfte opgaven | **52%** | **21%** | **25%** | **2%** | **113** |
| Virksomhedens øverste ledelse prioriterer ikke opgaven højt nok | **65%** | **19%** | **14%** | **2%** | **113** |
| Virksomhedens ansattes daglige adfærd udgør en risiko mht. sikkerhed i forhold til cyber- og datasikkerhed | **45%** | **32%** | **22%** | **1%** | **113** |
| Virksomhedens ansatte er utilstrækkeligt uddannede og har en for lav awareness over for cyber- og datasikkerhed | **53%** | **32%** | **14%** | **1%** | **113** |
| Det er uoverskueligt at være up-to-date med hensyn til advarsels- og forsvarsværktøjer, der forhindrer angreb | **54%** | **26%** | **17%** | **4%** | **113** |
| Reglerne for håndtering af persondata er meget svære at leve op til i det daglige | **30%** | **36%** | **31%** | **3%** | **113** |
| Reglerne for håndtering af persondata er meget svære at forstå | **42%** | **29%** | **26%** | **3%** | **113** |
| Vi har vanskeligt ved at rekruttere kvalificerede medarbejdere, der kan løfte opgaven med virksomhedens cyber- og datasikkerhed | **35%** | **24%** | **16%** | **26%** | **113** |

### 4.2.6 Trusselsbillede (Strategisk niveau)

68 % af de 113 virksomheder i undersøgelsen har været udsat for hacking eller anden form for it-angreb i løbet af dette senest år. Af dem der blev angrebet, fik 87 % angrebet stoppet, og 31 % anmeldte angrebet til politiet eller andre myndigheder. Den mest udbredte type angreb var ransomware, som 80 % af deltagerne har oplevet.

| | Nej | Ja, blev stoppet | Ja, blev ikke stoppet | Ved ikke | Ønsker ikke at oplyse | n |
|---|---|---|---|---|---|---|
| Er du bekendt med, om din virksomhed har været udsat for hacking eller anden form for it-angreb indenfor det seneste år? | 23% | 59% | 9% | 2% | 7% | 113 |
| % af dem der blev angrebet | | 87% | 13% | | | |

| | Forsøg på at trænge ind i netværket og kopiere data | Ransomware | DDoS-angreb | Ved ikke | Andet | n |
|---|---|---|---|---|---|---|
| Hvilken type angreb var der tale om? | 22% | 80% | 21% | 12% | 17% | 76 |

| | Nej | Ja, til politiet | Ja, til andre myndigheder | Ved ikke | n |
|---|---|---|---|---|---|
| Har virksomheden indberettet angrebet? | 64% | 18% | 13% | 11% | 76 |

OBS. Det var muligt at vælge flere valgmuligheder til de to sidste spørgsmål. Herudover er det udelukkede respondenter, der har svaret, at de er bekendte med, at deres virksomheder har været udsat for angreb, der er blevet stillet de to sidste spørgsmål.

# 5. ORGANISERING (STRATEGISK NIVEAU)

Ansvaret for cybersikkerhed er tilsyneladende mere spredt. It-afdelingen har her en mindre fremtrædende rolle og topledelsen en mere fremtrædende. Dette kunne betyde, at cybersikkerhed i højere grad ses som et strategisk anliggende, mens databeskyttelse mere ses som et operationelt anliggende.

| **Ansvarsplacering, Cybersikkerhed** | | It-afdelingen | I topledelsen | Flere afdelinger | Flere geografiske enheder | Datasikkerhedsansvarlig * | Eksterne konsulenter | Andet | n |
|---|---|---|---|---|---|---|---|---|---|
| Alle | n | 49 | 64 | 27 | 8 | 25 | 7 | 17 | 113 |
| | % | 43% | 57% | 24% | 7% | 22% | 6% | 15% | |

OBS. Det var muligt at vælge flere valgmuligheder til dette spørgsmål.

*Der er ved en fejl spurgt ind til det samme som i forrige spørgsmål.

| **Ansvar forankret i topledelsen** | | Ja | Nej | Ved ikke | I alt |
|---|---|---|---|---|---|
| Alle | n | 93 | 15 | 5 | 113 |
| | % | 82% | 13% | 4% | 100% |

# BILAG 1: METODE

Rapporten er baseret på en spørgeskemaundersøgelse, foretaget i perioden januar 2018-februar 2018. Rambøll Management Consulting (herefter Rambøll) har i samarbejde med IDA og FSR – danske revisorer udarbejdet nærværende rapport. Rambøll har været udførende i udarbejdelse af spørgeramme, dataindsamling og analyse.

## 5.1 Målgruppe

Undersøgelsen har til formål at undersøge udrulningen af procedurer, beredskab og awareness om cybersikkerhed og overholdelse af databeskyttelsesforordningen i den offentlige og private sektor. Med henblik på at afdække dette undersøgelsesfelt er følgende fire målgrupper defineret:

Strategisk niveau

1. It-ansvarlige i den offentlige sektor
2. It-ansvarlige i den private sektor

Operationelt niveau

3. Medarbejdere i den offentlige sektor
4. Medarbejdere i den private sektor.

## 5.2 Spørgeskema

Spørgeskemaet er delt i to afsnit; et, der handler om databeskyttelsesforordningen (GDPR), og et, der handler om cybersikkerhed.

### 5.2.1 Databeskyttelsesforordningen

På det operationelle niveau er det udelukkende personer, der i spørgeskemaet har angivet, at de arbejder med persondata, der er blevet stillet spørgsmålene omhandlende databeskyttelsesforordningen og de her tilhørende regler og procedurer.

Spørgsmålene er forsøgt stillet således, at kompleksiteten i databeskyttelsesforordningen på den ene side rummes, og at spørgsmålet på den anden side stadig er forståeligt for en almen medarbejder, der arbejder med persondata.

På det strategiske niveau spørges ind til udbredelse af viden om og træning i procedurer relaterede til databeskyttelsesforordningen, medarbejdernes kunnen samt virksomhedens it-systemers evne til at understøtte processerne.

### 5.2.2 Cybersikkerhed

Samtlige medarbejdere på det operationelle niveau er stillet spørgsmålene relateret til cybersikkerhed, eftersom det kan argumenteres, at alle der arbejder med en pc eller mobil enhed, der er på nettet, er udsat for cyberangreb. Der spørges i høj grad ind til medarbejdernes egen rolle og kendskab, hvordan de kan mindske risikoen for angreb.

På det strategiske niveau spørges der i højere grad ind til virksomheden forudsætninger for at modstå angreb samt udfordringer og barrierer for at beskytte sig imod angreb.

### 5.2.3 Justeringer i spørgeskemaet

Der er foretaget to mindre justeringer i spørgeskemaerne, der kan have en lille effekt på besvarelserne, og dette er taget in mente undervejs i analysen. I det store hele antages disse små ændringer at have influeret undersøgelsen i meget lav grad.

Spørgsmålet "hvor mange indbyggere er der i den kommune, hvor du er ansat?" blev ændret til "hvis du er ansat i en kommune, hvor mange indbyggere er der så i kommunen, hvor du er ansat?", eftersom nogle af respondenterne ikke var sikre på, hvordan det første spørgsmål skulle forstås. Yderligere blev der også tilføjet en kategori mere til dette spørgsmål "jeg er ikke ansat i en kommune", eftersom nogle af respondenterne ikke var ansat i en kommune.

Ændringen blev foretaget den 18. januar, hvor følgende antal respondenter havde besvaret spørgeskemaet indeholdende det konkrete spørgsmål.

| Respondent | Antal |
|---|---|
| Strategisk niveau i det offentlige | 12 |
| Forsyningsvirksomheder | 5 |
| Operationelt niveau i det private | 354 |

Yderligere blev der den 17. januar foretaget en ændring i det strategiske niveau i det private spørgeskema, hvor der ved spørgsmålet "har virksomheden indberettet angrebet?" blev tilføjet en mulighed for at afkrydse flere svarmuligheder. Ændringen blev foretaget, da der var 58 respondenter på det strategiske niveau i det private, der havde svaret på spørgeskemaet.

## 5.3 Dataindsamling

Undersøgelsen er sendt ud via mail til de fire målgrupper, som angivet i nedenstående tabel:

| Respondenter | Antal respondenter | Antal besvarelser | Besvarelses procent |
|---|---|---|---|
| Strategisk niveau | | | |
| It-ansvarlige i kommunerne | 125 | 24 | 19,2% |
| It-ansvarlige i den private sektor | 859 | 89 | 10,3% |
| Operationelt niveau | | | |
| Medarbejdere i den offentlige sektor | 3018 | 370 | 12,3% |
| Medarbejdere i den private sektor | 4995 | 850 | 17,0% |

Dataindsamlingen startede d. 4. januar, hvorefter der er fulgt to opfølgningsmails. Desuden er der taget direkte kontakt via telefon til respondenter i den offentlige sektor, hvor det har været muligt. Undersøgelsen blev afsluttet den 9. februar med ovenstående resultater.

Der er ikke anvendt vægtning.

For yderligere information om datagrundlaget henvises til afsnit 3. Datagrundlag, hvor selve rapportens datagrundlag beskrives.

### 5.3.1 Frafald af respondenter

Frafald i undersøgelsen kan kategoriseres som inaktive mails (hvor modtager ikke længere har den anvendte mailadresse), generiske svarmails (vedrørende personer, der er syge/på barsel/netop gået på pension eller skiftet job) samt personer, der ikke ønsker at deltage i undersøgelsen.

| Respondentgruppe | Frafaldsårsag | Antal |
|---|---|---|
| Strategisk niveau | | |
| Offentlige respondenter | Inaktiv mail | 12 |
| | Automatiske svarmails | 10 |
| | Ønsker ikke at deltage | 1 |
| Private respondenter | Inaktiv mail | 69 |
| | Automatiske svarmails | 55 |
| | Ønsker ikke at deltage | 13 |
| Operationelt niveau | | |
| Offentlige og private respondenter | Inaktiv mail | 69 |
| | Automatiske svarmails | 55 |
| | Ønsker ikke at deltage | 13 |