ERHVERVSSTYRELSEN

# Indberetninger i 2018 og 1. halvår 2019 af brud på persondatasikkerhed på området for elektronisk kommunikation

## Reglerne om persondatasikkerhed på området for elektronisk kommunikation

Erhvervsstyrelsen er tilsynsmyndighed for de særlige regler om persondatasikkerhed inden for elektronisk kommunikation.

Der er tale om sektorspecifikke regler, der træder i stedet for den generelle databeskyttelsesforordning (GDPR), når det handler om beskyttelse af persondata inden for elektronisk kommunikation.

Reglerne findes i bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og i Kommissionens forordning nr. 611/2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden.

I medfør af disse regler skal udbydere af offentlige elektroniske kommunikationstjenester overholde forskellige krav for at sikre persondatasikkerheden i forbindelse med deres udbud af elektroniske kommunikationstjenester (fx telefoni- og internettjenester). Det vil i praksis sige teleselskaber på det danske marked.

Udbyderne skal løbende træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden. Foranstaltningerne skal sikre et sikkerhedsniveau, der, under hensyn til teknologiens aktuelle stade og omkostningerne ved at gennemføre foranstaltningerne, står i forhold til risici.

Hvis der sker et brud på persondatasikkerheden, skal udbyderne underrette Erhvervsstyrelsen herom, ligesom de personer, der er berørt af bruddet, som hovedregel skal underrettes.

Udbydere af offentlige elektroniske kommunikationstjenester skal underrette Erhvervsstyrelsen om alle brud på persondatasikkerheden. Efter GDPR skal et brud på persondatasikkerheden ikke indberettes til Datatilsynet, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. En sådan undtagelse findes ikke i telelovgivningen. En udbyder skal alene underrette Erhvervsstyrelsen, og ikke (også) Datatilsynet, når der er tale om et brud på persondatasikkerheden, der relaterer sig til udbuddet af en offentligt tilgængelig elektronisk kommunikationstjeneste. Det omfatter fx uautoriseret adgang eller utilsigtet videregivelse af oplysninger om abonnenter, men eksempelvis ikke brud på oplysninger om udbyderens egne ansatte (HR-data o.lign.). I sidstnævnte tilfælde er det de almindelige regler efter GDPR, der gælder.

Udbydere af offentlige elektroniske kommunikationstjenester skal indberette et brud på persondatasikkerheden senest 24 timer efter påvisning af bruddet. Også på dette punkt adskiller reglerne om indberetning sig fra reglerne efter GDPR, hvor fristen er 72 timer. Der kan efterfølgende foretages en uddybende underretning senest tre dage efter den indledende underretning, i fald oplysninger udestod eller skal ajourføres.

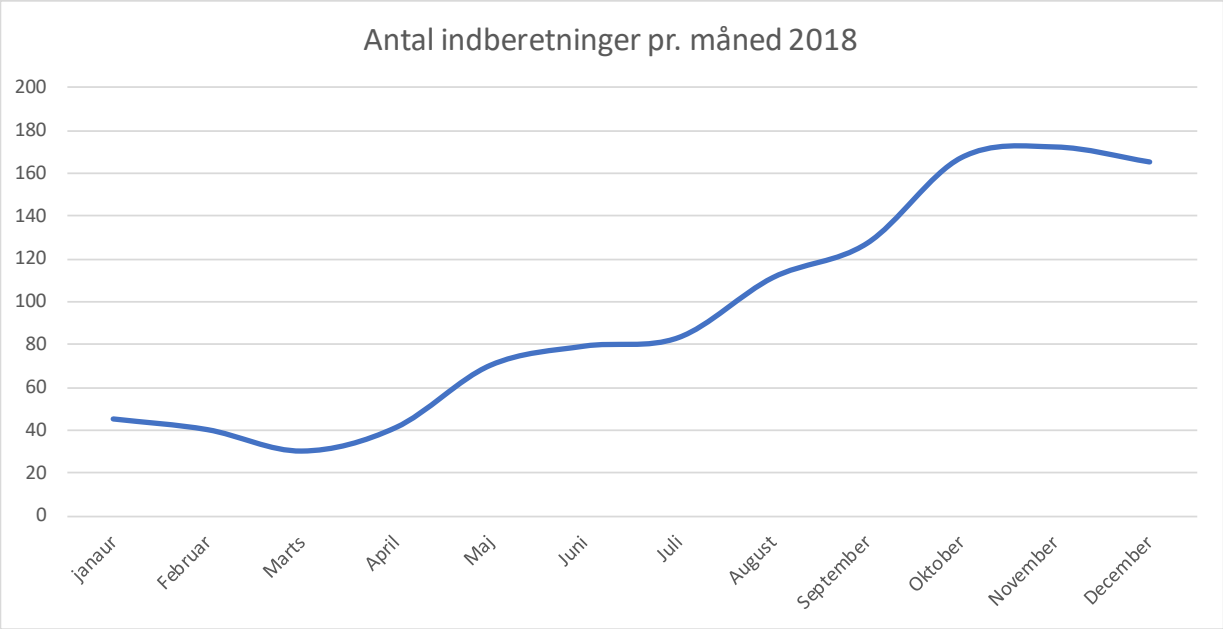
Indberetning af brud sker via den fælles offentlige indberetningsplatform, der kan findes på virk.dk.

Erhvervsstyrelsen behandler løbende de indberetninger om brud på persondatasikkerheden, som styrelsen modtager fra udbydere af offentlige elektroniske kommunikationstjenester. Erhvervsstyrelsen har bl.a. fokus på udbydernes identifikation, håndtering og løsning af hændelserne samt læring heraf, herunder eventuel iværksættelse af foranstaltninger for fremadrettet af undgå tilsvarende hændelser. Endvidere fokuseres på overholdelse af kravene om underretning af tilsynsmyndigheden og af de berørte personer.

# Indberetninger 2018

Erhvervsstyrelsen har, som det fremgår af figur 1, i 2018 modtaget 1131 indberetninger fra udbydere af offentlige elektroniske kommunikationstjenester om brud på persondatasikkerheden.

Figur 1: Antal indberetninger pr. måned 2018




Figur 1 viser, at antallet af indberetninger i løbet af 2018 steg betydeligt. Det kan konstateres, at antallet af indberetninger steg omkring maj, hvor GDPR fik virkning. I fjerde kvartal stagnerede antallet af indberetninger dog. Udviklingen tyder på, at det øgede fokus på persondatabeskyttelse generelt tillige har haft indflydelse på teleselskabernes opmærksomhed på persondatasikkerhed inden for elektronisk kommunikation.

## Typer af persondata, der er berørt at brud på persondatasikkerheden

Udbydere af elektroniske kommunikationstjenester håndterer data såsom navn, adresse, telefonnummer (som evt. kan være hemmeligt eller udeladt), e-mailadresse, abonnementsoplysninger, betalingsoplysninger, kundenummer eller kontonummer hos udbyderen. Brud på persondatasikkerheden, der sker hos udbydere af offentlige elektroniske kommunikationstjenester, omfatter oftest eksponering af en eller flere af ovenstående typer data. Det gælder, uanset om der er tale om manuelle fejl, systemfejl eller andet.

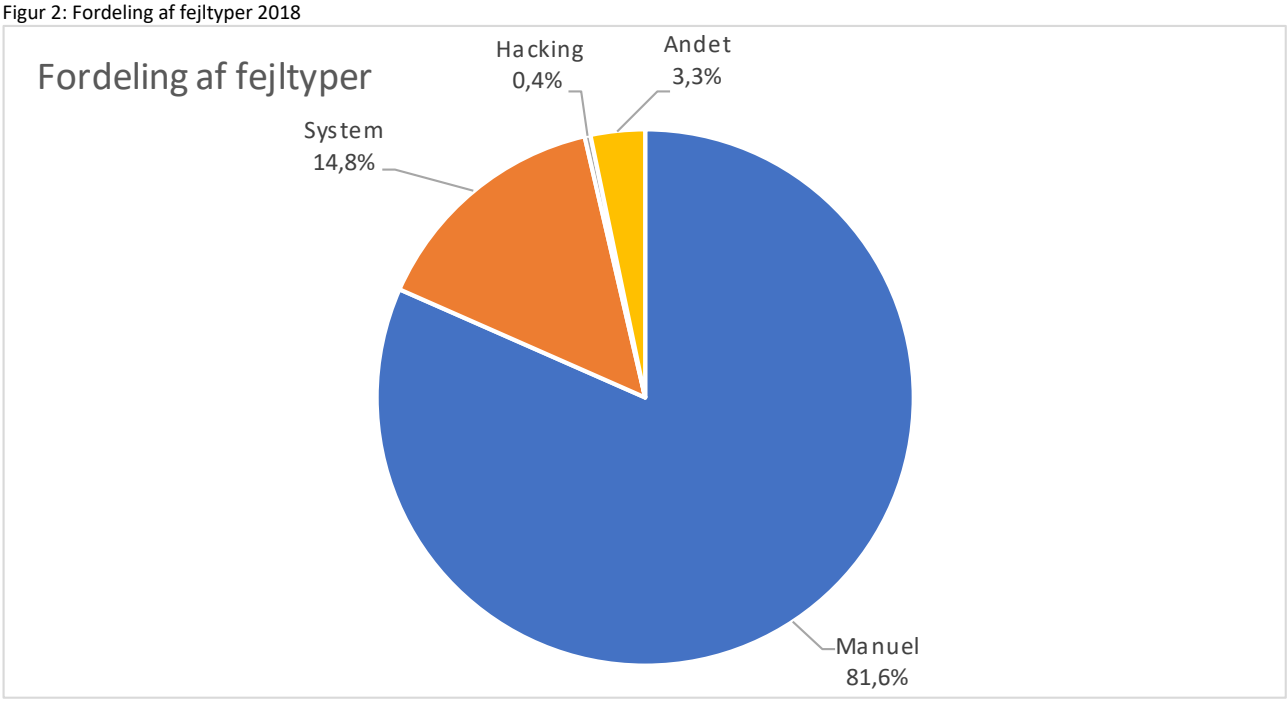
Ved manuelle fejl såvel som systemfejl ses eksempler på hændelser, der fører til eksponering af 'hemmelige' og 'udeladte' nummeroplysningsdata (navn, adresse og telefonnummer), som må anses for at være særligt alvorligt i forbindelse med teleselskabers håndtering af kundedata.

Typisk berører de enkelte brud på persondatasikkerheden ganske få personer. I forbindelse med fx større systemmigreringer ses der dog brud, hvor en større gruppe er berørt af hændelsen - dette uddybes nærmere nedenfor.

## Fordeling af fejltyper

Indberetningerne fordeler sig i en række hovedgrupper. Manuelle fejl er den primære fejltype og udgør ca. 82 % af indberetningerne. Det drejer sig om menneskelige fejl, hvor fx en medarbejder taster data forkert. Ca. 15 % af indberetningerne skyldes systemfejl og er relateret til it-løsninger, mens godt 3 % vedrører andre fejltyper. Sidstnævnte dækker bl.a. over svindel, tyveri samt tilfælde, hvor det på tidspunktet for indberetningen endnu var uklart, hvad fejlen skyldtes. Slutteligt vedrørte en ganske lille del af indberetningerne sikkerhedsbrud som følge af hacking. Figur 2 illustrerer fordelingen af fejltyper.

Figur 2: Fordeling af fejltyper 2018




## Manuelle fejl

Udbydere af offentlige elektroniske kommunikationstjenester har i sagens natur megen kundekontakt (bl.a. gennem kundeservicecentre og butikker), og stort set samtlige personer og virksomheder i Danmark har enten ét eller flere abonnementer hos et teleselskab. Det er som oftest i kundeservice, at manuelle fejl sker. Af de manuelle fejl udgør tastefejl 59 %. Tastefejl vedrører oftest fejltastning af nummer, e-mail eller CPR-nummer. Fejltastning kan medføre, at en mail eller sms, der indeholder personoplysninger, sendes til en forkert modtager. CPR-numre, der tastes forkert ved oprettelse af et kundeforhold, kan medføre, at en kontrakt indeholder forkert navn og adresse, uden at selve CPR-nummeret dog eksponeres.

Ca. 4 % af de indberettede brud skyldes tastefejl fra *kundens* side.

Andre manuelle fejl handler om, at data om en kunde indtastes i en andens kundes kundeprofil. Det kan fx ske, hvis et "systemvindue" i forbindelse med kundeekspedition ikke er blevet lukket ned efter afsluttet ekspedition (fx ved ændring og tilpasning af abonnement, eller lignende), eller fx hvis der sker et fejlopslag i udbyderens kundedatabase i forbindelse med en kundeekspedition.

Brug af fiktive mails er ligeledes en årsag til manuelle fejl. Sådanne fejl opstår typisk som følge af, at systemet "kræver", at der skal angives en mailadresse, når der oprettes et kundeforhold eller afsendes et tilbud, men kunden enten ikke ønsker at oplyse sin mail eller slet ikke har en mailadresse. I sådanne situationer sker det, at en kundeservicemedarbejder i stedet anvender en angiveligt fiktiv mailadresse – fx "mangler@mail.dk". Hvis denne adresse viser sig faktisk at tilhøre en person og dermed ikke er fiktiv, vil ejeren af den "fiktive" mailadresse modtage ordrebekræftelser og lign. med fx andre personers navn og kontaktoplysninger.

Når der er tale om manuelle fejl, er det oftest 1-2 personer, der er berørt af det enkelte brud på persondatasikkerheden. Der kan dog også ske manuelle fejl, der bevirker, at et stort antal personer bliver berørt. Således er set hændelser, hvor en menneskelig fejl i forbindelse med en migrering af kundeoplysninger fra et it-system til et andet it-system medførte, at et stort antal 'hemmelige' navne og adresser blev gjort offentligt tilgængelige.

## Systemfejl

Særligt i den første del af 2018 var der i forbindelse med implementeringen af databeskyttelses-forordningen tilsyneladende et stort fokus blandt teleselskaber på at optimere og tilpasse de it-systemer, der indeholder persondata. Det medførte, at man i flere tilfælde opdagede fejl i systemerne, som blev indberettet til Erhvervsstyrelsen, hvis det havde ført til et brud på persondatasikkerheden. Mod slutningen af 2018 har styrelsen noteret et fald i antallet af indberetninger af brud på persondatasikkerheden, der beror på systemfejl.

I 2018 modtog Erhvervsstyrelsen en række indberetninger om brud på persondatasikkerheden, der specifikt relaterede sig til migrering af data til nye it-systemer. Bruddet skyldes i disse sager, at kunders data er blandet sammen, hvilket fx resulterer i forkerte oplysninger på regninger. Migreringsfejl kan imidlertid også føre til større og mere alvorlige brud på persondatasikkerheden. Sådanne brud har bl.a. vedrørt eksponering af 'hemmelige' og 'udeladte' telefonnumre og adresser.

Omtrent en tredjedel af de indberettede brud, der skyldes systemfejl, relaterer sig til selskabernes selvbetjeningssystemer, hvor kunderne opretter og ændre abonnementer, tv-pakker osv. Sådanne fejl opstår ofte ved systemopdateringer eller -migreringer, hvor data ikke overføres korrekt fx på grund af fejl i indstillinger, design, kode eller kompatibilitet. Dette kan blandt andet medføre, at kunder "blandes sammen", således at én kunde kan se en anden kundes oplysninger på sin egen selvbetjeningsløsning.

Der er også eksempler, hvor en kunde har fået adgang til en anden kundes mailkonto via selvbetjeningsløsningen. Dette kan igen skyldes sammenblanding af kunders data, men kan ligeledes opstå, hvis tidligere konti ikke er blevet lukket korrekt i systemet, og nye kunder får tildelt samme kontonumre som de tidligere kunder, og derved får adgang til deres selvbetjening.

Der er også eksempler, hvor en kunde, der har glemt sit brugernavn/adgangskode til selvbetjeningsløsningen, via en funktion til nulstilling af kodeord får adgang til en anden kundes selvbetjening. Dette kan fx ske ved, at et opsagt nummer ved en fejl stadig er lagret i systemet, således at en ny kunde, der overtager det tidligere opsagte telefonnummer, får genoprettet brugernavn/adgangskode til den tidligere ejeres selvbetjening i stedet for sin egen.

## Andre

Denne kategori udgør (som vist i figur 2) ca. 3 % af de indberettede hændelser, og vedrører bl.a. svindel, tyveri samt tilfælde, hvor det på tidspunktet for indberetningen endnu var uklart, hvad fejlen skyldtes. Underretning til Erhvervsstyrelsen skal ske senest 24 timer efter påvisning af bruddet på persondatasikkerheden, hvorfor hændelsesforløb i større eller mindre grad kan være uafklaret på tidspunktet for indberetningen.

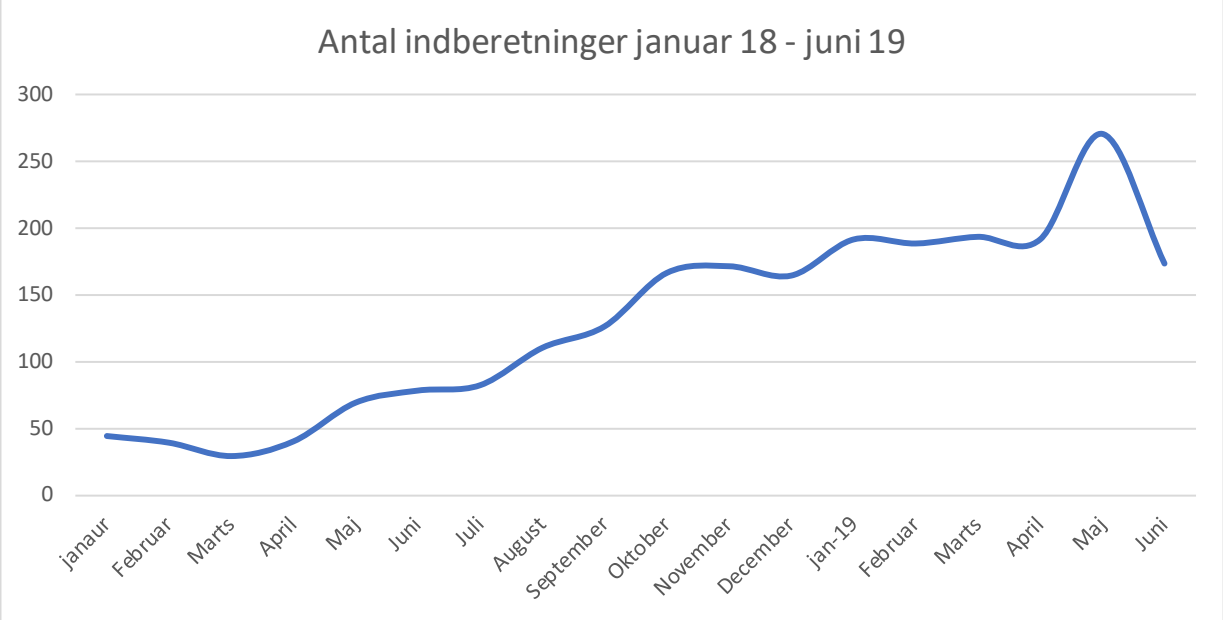
## Hacking

Der har været et mindre antal indberetninger vedrørende hacking af selvbetjeningssystemer. Der er typisk tale om hacking af login-oplysninger, der fx giver adgang til information om kunders tv-pakker og online streamingtjenester. Uautoriseret adgang opnås fx ved brug af lister med brugernavne/e-mailadresser og passwords, der hidrører fra hacking af andre større platforme (fx Facebook og LinkedIn). Hackerne køber listerne på Internettet. Hackere tester disse lister af på selvbetjeningssystemerne, og hvis en bruger har anvendt samme brugernavn og adgangskode flere steder, kan det lykkes hackerne at skaffe sig uautoriseret adgang. Antal berørte varierer, men der er – med enkelte undtagelser – oftest tale om ganske få personer.

# Tendenser for første halvår 2019

Erhvervsstyrelsen har, som det fremgår af figur 3, modtaget 1212 indberetninger om brud på persondatasikkerheden i perioden 1. januar til 30. juni 2019.
I første kvartal 2019 har styrelsen modtaget 575 indberetninger og i andet kvartal 2019 637 indberetninger.

Figur 3: Antal indberetninger pr. måned januar 2018 - 1. halvår 2019




Antallet af indberetninger har for den første halvdel af 2019 ligget forholdsvis stabilt med en mindre stigning i maj måned. Sammenlignet med det sidste kvartal af 2018, kan det konstateres, at udviklingen fra det sidste kvartal i 2018 er fortsat over i 2019. Det gennemsnitlige antal indberetninger modtaget i 2019 ligger således på samme niveau som for 4. kvartal i 2018. Det vurderes, at faldet af indberetninger, som ses omkring maj og juni måned 2019 bl.a. kan tilskrives ferie.

## Fordeling af fejltyper

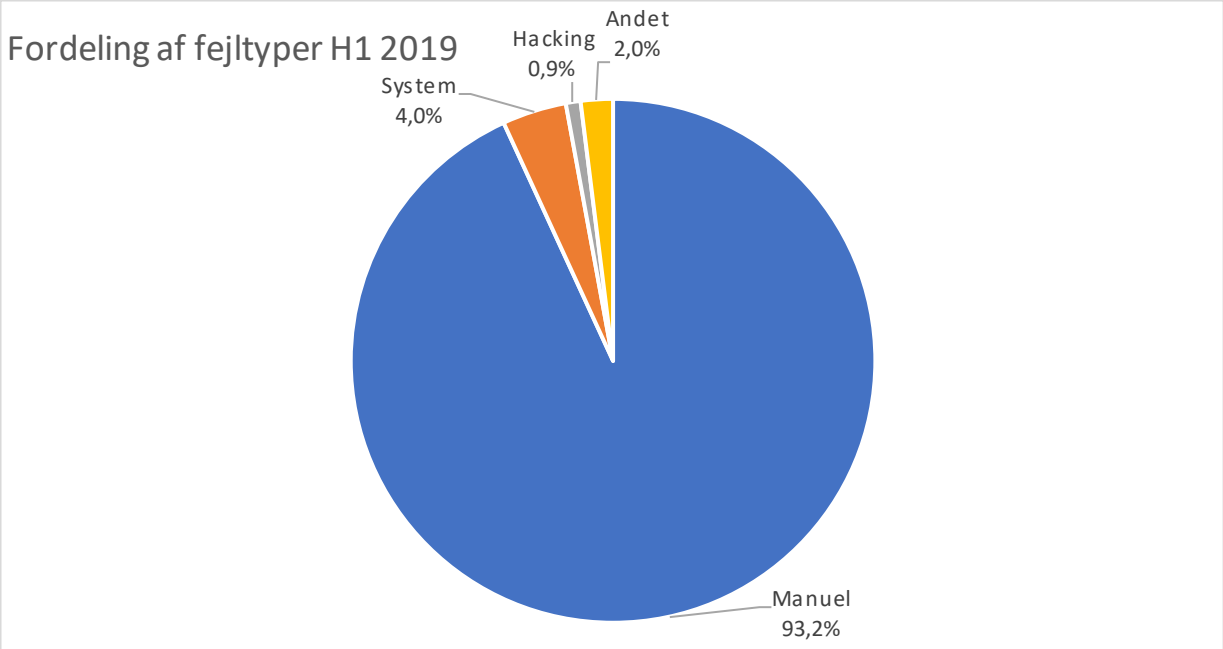
Som vist i figur 4 nedenfor, er manuelle fejl fortsat den kategori, som størstedelen af indberetningerne falder i. 93 % af indberetningerne om brud på persondatasikkerheden i første halvår 2019 omhandler manuelle fejl. Manuelle fejl dækker som tidligere nævnt over menneskelige fejl, hvor fx en medarbejder taster data forkert. Manuelle fejl inkluderer også kundefejl, hvor kunder fx har tastet e-mail forkert. Kundefejlene udgør 8 % af de manuelle fejl. 95 % af de indberettede brud, der skyldes manuelle fejl, vedrører hændelser, hvor 1-2 person er berørt af bruddet.

4 % af indberetningerne vedrører systemfejl og er relateret til it-løsninger. 68 % af de indberettede brud, som skyldes systemfejl, vedrører hændelser, hvor 1-2 personer er berørt af bruddet.

2 % af indberetningerne beror på andre fejltyper (kategorien 'andet'). Denne dækker bl.a. over svindel, tyveri samt tilfælde, hvor det på tidspunktet for indberetningen endnu var uklart, hvad fejlen skyldtes. Alle disse indberetninger vedrører brud, hvor 1-2 personer er berørt af hændelsen.

En ganske lille del af indberetningerne (0,9%) vedrørte sikkerhedsbrud som følge af hacking, hvor udefrakommende har testet "lækkede" passwords fra andre sider mod brugeres loginoplysninger til deres teleudbyder. Antal berørte varierer her, men i 63 % af tilfældene er der tale om 1-9 berørte.

Figur 4: Fordeling af fejltyper H1 2019




Overordnet set kan det siges, at tendenser i fejltyper fra 2018 går igen i 2019.

Manuelle fejl er fortsat den kategori langt størstedelen af indberetningerne vedrører. Der har i det første halve år af 2019 været et fald i antallet af systemfejl sammenlignet med 2018. Dette afspejler tendensen fra 2018, hvor Erhvervsstyrelsen mod slutningen af året havde noteret sig et fald i antal indberetninger, der vedrørte systemfejl. Kategorierne 'hacking' og 'andet' har oplevet en lille stigning.

# Læringspunkter

- Skab opmærksomhed om persondatasikkerhed i hele organisationen - fra ledelsen til kundeservice og hos databehandlere - således at evt. brud på persondatasikkerheden bliver identificeret og indberettet til Erhvervsstyrelsen.
- Sørg for en positiv indberetningskultur i organisationen.
- Ved telefonopkald anbefales det, at kundeservicemedarbejdere guider kunden til i videst muligt omfang at bruge selvbetjening, så kunden selv indtastet sine oplysninger, fremfor at kundeservicemedarbejderen skal taste kundes oplysninger med de risici for fejl, det medfører.
- Der bør ikke anvende "fiktive" e-mails fx ved abonnementsoprettelse.
- Overvej, hvilke persondata der behøver at indgå i beskeder til kunder. Sendes en sms om opdateringer eller lignende, kan dette gøres med et "Hej" i stedet for navn i sms'en.
- I forbindelse med ændringer i it-systemer og migrering af data, er det vigtigt, at der gennemføres grundige tests af systemændringerne forud for lancering, således at brud på persondatasikkerheden kan undgås.
- Sørg for et hurtigt beredskab i organisationen, således at brud på persondatasikkerheden bliver indberettet til Erhvervsstyrelsen inden for 24 timer.