Digitaliseringstyrelsen
KL
Danske Regioner
DKCERT
DelC

Danskernes informationssikkerhed

December 2018

2018

DANSKERNES INFORMATIONSSIKKERHED

Digitaliseringsstyrelsen, KL, Danske Regioner og DKCERT, DeiC
Redaktion: Henrik Larsen, Torben B. Sørensen og Nicolai Devantier
Design: Kiberg & Gormsen

DKCERT, DeIC
DTU, Asmussens Allé, Bygning 305
2800 Kgs. Lyngby

Indhold

1.
Resume

1. Resume

Rapporten dækker oplevelser med og kendskab til informationssikkerhed hos offentligt ansatte og borgere.

Denne rapport bygger på en undersøgelse, som Danmarks Statistik har gennemført i foråret 2018 for Digitaliseringsstyrelsen, KL, Danske Regioner og DKCERT. Rapporten er udarbejdet som led i initiativ 9.3 i den fællesoffentlige digitaliseringsstrategi. Undersøgelsen dækker oplevelser med og kendskab til informationssikkerhed hos to befolkningsgrupper: Offentligt ansatte og borgere.

DKCERT har gennemført undersøgelser vedr. borgernes informationssikkerhed i 2013, 2014, 2015, 2016 og igen her i 2018. De offentligt ansatte blev indlemmet i undersøgelsen i 2016.

1.1. Trusler

Det konkrete sikkerhedsbillede blandt borgere og de offentligt ansatte fordeler sig således:

En ud af tre borgere har enheder, der har været inficeret med virus eller lignende, og fem procent har fået misbrugt personoplysninger på nettet. Otte procent af borgerne har desuden mistet penge som følge af onlinesvindel eller afpresning og 17 procent har mistet data som følge af et computernedbrud eller softwarenedbrud.

Samlet har 44 procent af borgerne været udsat for mindst et af fire sikkerhedsproblemer: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data. Det er en stigning fra 34 procent i 2016. Som noget nyt har vi også spurgt, om borgerne har oplevet mindst en af fire trusler mod informationssikkerheden på deres telefon eller tablet-computer. Her svarer 23 procent ja.

Det er bemærkelsesværdigt, at en ud af tre af offentligt ansatte ikke tager sikkerhedskopier af data på computeren, og at 55 procent ikke tager sikkerhedskopier af data på telefon eller tablet-computer. Otte procent har da også oplevet datatab som følge af manglende backup. Kun fire ud af ti af borgerne tager jævnligt sikkerhedskopi af data på deres computer.

37 procent af de offentligt ansatte bruger de samme passwords til flere systemer. Det øger risikoen forbundet med hackerangreb på de systemer, de anvender. Hvis hackere får fat i blot ét sæt brugernavn og password, kan de forsøge at genbruge dem til andre systemer. 37 procent af borgerne anvender samme adgangskode til flere online-tjenester. I 2016 var det 66 procent, og der er således sket en stor forbedring.

Knap seks ud af ti offentligt ansatte oplyser, at de har sat sig ind i informationssikkerhedspolitikken for deres arbejdsplads. I 2016 var det knap fem ud af 10, hvilket viser en klar forbedring. Otte procent undlader dog nogle gange at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet. Af dem oplyser 15 procent, at det forekommer hver dag.

Borgerne viser stor usikkerhed over for trusler i hverdagen. Knap fire ud af ti borgere mener nemlig ikke, at de er godt klædt på til at beskytte sig mod cybertrusler. Det kan både skyldes manglende viden og/eller mediernes fokus på dramatiske episoder forbundet med cyber- og informationssikkerhed. Det viser også, at borgerne er bevidste om, at det er nødvendigt at forholde sig til problemet.

1.2. Konsekvenser

Stort set alle borgere og offentligt ansatte, der har været udsat for sikkerhedsproblemer, ændrede adfærd. Den hyppigste ændring var, at de holdt op med at åbne e-mails, der kom fra ukendte afsendere. Det gjorde 88 procent af borgerne og 82 procent af de offentligt ansatte.

Derudover var det også udbredt blandt de fleste at installere eller opgradere sikkerhedssoftware. Det gjorde halvdelen af de offentligt ansatte og 73 procent af borgerne. Andre tiltag er at undlade at besøge bestemte websider. Det gjorde 66 procent af borgerne og 55 procent af de offentligt ansatte. En anden svarmulighed har været at spørge arbejdspladsens it-funktion. Det gjorde 59 procent. Det er en stigning på seks procentpoint i forhold til 2016.

1.3. Foranstaltninger

Ni ud af ti af de offentligt ansatte beskytter deres computer med sikkerhedssoftware. Det samme gælder seks ud af ti af borgerne.

70 procent af de ansatte og 32 procent af borgerne har sikkerhedssoftware på deres smartphone eller tablet-computer. I 2016 var det tal på godt halvdelen af de ansatte og 26 procent af borgerne.

Seks procent af borgerne har været ramt af ransomware, og 17 procent af disse oplyser, at de ikke fik deres data tilbage. Problemet er ikke så udbredt, men bliver man ramt, er konsekvenserne store.

41 procent af borgerne tager jævnligt sikkerhedskopier af computeren, og cloud-tjenesterne bliver benyttet mere og mere. 55 procent af de ansatte oplyser, at der bliver taget sikkerhedskopi af de data, som de bruger i deres arbejde. Over halvdelen tager ikke sikkerhedskopi af telefonen eller tablet-computeren.

2.
Indledning

2. Indledning

Denne rapport belyser informationssikkerheden hos offentligt ansatte og borgere. Rapporten afdækker, hvilke sikkerhedshændelser de bliver udsat for og belyser deres viden om informationssikkerhed og deres evne til at beskytte sig mod udbredte trusler.

Formålet med undersøgelsen er at afdække, dels hvilke trusler mod informationssikkerheden deltagerne oplever, dels hvad de ved om informationssikkerhed og deres mulighed for at beskytte sig.

Rapporten bygger på en undersøgelse, som Danmarks Statistik foretog for Digitaliseringsstyrelsen og DKCERT i foråret 2018. Undersøgelsen stillede en række spørgsmål til et repræsentativt udvalg af den voksne danske befolkning om deres erfaringer med informationssikkerhed. Undersøgelsen bygger på svar fra 1.505 personer i alderen 18-74 år.

Der regnes ud fra en samlet population på 995.475[1] offentligt ansatte og 3.155.504 borgere i alderen 18-74 år. Heraf oplyser 88 procent svarende til 2.775.790, at de har adgang til en computer til privat brug, mens 87 procent svarende til 2.757.155 har adgang til smartphone eller tabletcomputer til privat brug. For at nå frem til antallet af personer i forbindelse med de enkelte spørgsmål har Danmarks Statistik foretaget en vægtning ud fra antallet af besvarelser. I rapporten anvendes som oftest procentangivelsen, men enkelte steder er det samlede antal trukket frem.

Der blev stillet spørgsmål ud fra to forskellige spørgeskemaer målrettet til henholdsvis offentligt ansatte og borgere i deres egenskab af privatpersoner. Deltagerne var fordelt således:

- 777 offentligt ansatte
- 728 borgere

Størrelsen af grupperne medfører, at små svarprocenter bygger på ret få personer. Det betyder også, at der ikke har været svar nok i alle kategorier til at give et statistisk grundlag for en konklusion. Det gør sig gældende i forbindelse med kategorierne ransomware, spørgsmålet om falsk teknisk support og direktørsvindel.

Danmarks Statistik udførte lignende undersøgelser for Digitaliseringsstyrelsen og DKCERT i 2013, 2014, 2015 og 2016. I alle årene har borgerne været genstand for undersøgelsen. I 2016 blev offentligt og privat ansatte indlemmet i undersøgelsen, mens det kun er borgere og offentligt ansatte i 2018. Resultaterne fra de tidligere undersøgelser indgår i denne rapport under de punkter, hvor det er muligt og relevant at foretage en sammenligning. Som hovedregel anvendes søjlediagrammer, hvis der kan sammenlignes med tidligere år, mens lagkagediagrammer anvendes, når der ikke kan sammenlignes. Hvis der ikke kan sammenlignes med tidligere år, skyldes det, der er tale om et nyt eller væsentligt ændret spørgsmål.

[1] I denne undersøgelse omfatter offentligt ansatte i stat, regioner, kommuner og offentlige virksomheder. Der afgrænses primært ud fra e-indkomst og bevægelser inden for et kvartal.

3.
Definitioner

3. Definitioner

I rapporten indgår en række udbredte trusler og begreber inden for informationssikkerhed. De defineres kort i dette kapitel.

3.1. Skadelige programmer

Skadelige programmer eller malware (malicious software) er programmer, der ændrer i eller sletter brugerens data, forhindrer adgang til applikationer eller tjenester, eller på anden måde er generende eller skadelige. Virus er skadelige programmer, der spreder sig ved at kopiere sig ind i andre programfiler. Orme er skadelige programmer, der spredes via netværk.

De fleste skadelige programmer er trojanske heste, der giver sig ud for at være tilforladelige programmer, men som i virkeligheden er skadelige. Ofte henter den trojanske hest flere skadelige programmer og installerer dem på computeren.

Man kan beskytte sig mod skadelige programmer såsom virus med antivirusprogrammer. Firewalls beskytter mod angreb fra orme.

3.2. Botnet

En bot (forkortelse af robot) er en computer, som er blevet inficeret med et skadeligt program, der giver angriberen mulighed for at tage kontrollen over computeren. Når det sker, kan en computer udføre opgaver over internettet, uden at computerens ejer ved det. De inficerede computere samles i store netværk, kaldet botnet, der bl.a. kan anvendes af kriminelle til at udføre overbelastningsangreb, såkaldte Distributed Denial-of-Service (DDoS) angreb.

3.3. Ransomware

Ransomware er skadelige programmer, der spærrer for brugerens adgang til data eller systemer. Bagmændene kræver betaling af en løsesum for at give brugeren adgang igen. Ofte krypterer bagmændene offerets data, så man skal betale for at få udleveret den nøgle, der kan dekryptere dem (læs om kryptering i afsnit 3.8).

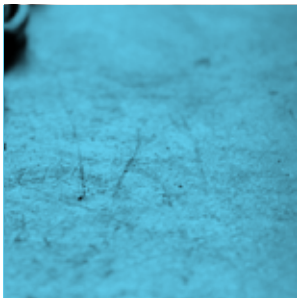
3.4. Beskeder med links

It-kriminelle udsender mails og andre former for digitale beskeder, der indeholder links til websider. Hvis offeret klikker på linket, åbnes en skadelig webside. Den kan indeholde software, der automatisk afprøver, om den besøgende browser har en eller flere kendte sårbarheder. Hvis det er tilfældet, udnyttes sårbarhederne til at installere skadelig software på offerets computer.

Et link kan også føre til et forfalsket websted som led i phishing-svindel, se afsnit 3.5.

3.5. Mails med phishing

Phishing er en form for svindel, hvor svindlerne forsøger at narre fortrolige oplysninger fra offeret. Et typisk phishing-angreb har to komponenter: en indledende e-mail og et forfalsket websted.



I den e-mail, som offeret modtager, forsøger afsenderen at lokke vedkommende til at gå ind på en bestemt webside. I mailen kan der fx stå, at modtagerens bankkonto er blevet spærret, og at man skal gå ind på websiden og indtaste brugernavn og password for at åbne kontoen igen.

Hvis offeret klikker på linket i mailen, vises en webside, der giver sig ud for at være den tjeneste, mailen henviser til. Her er der indtastningsfelter, som offeret kan udfylde med de oplysninger, bagmændene er interesserede i.

Hvis offeret falder for svindelnummeret, får uvedkommende adgang til fortrolige oplysninger. Det kan fx være password eller betalingskortoplysninger.

3.6. Direktørsvindel

Ved direktørsvindel (CEO-fraud) giver it-kriminelle sig ud for at være en ledende medarbejder i offerets virksomhed. Offeret vil typisk være ansat i bogholderiet eller en anden funktion med adgang til at overføre penge.

Bagmændene sender en mail, der ser ud til at komme fra en ledende medarbejder. Vedkommende beder modtageren sørge for hurtigst muligt at overføre et beløb til en ny udenlandsk samarbejdspartner. Hastværket bliver brugt som begrundelse for, at medarbejderen ikke skal bruge tid på at gå gennem de normale kanaler og kontrolprocedurer.

Hvis offeret falder for svindlen, får bagmændene de penge, der bliver overført.

3.7. Falsk teknisk support

Svindlere ringer til potentielle ofre og udgiver sig for at være fra fx Microsoft eller andre former for teknisk support. De siger, at der er sikkerhedsproblemer med offerets computer. Formålet er at narre offeret til at åbne for fjernstyring af pc'en, så de kan overtage den, eller installere skadelig software.

3.8. Kryptering

Kryptering er kodning af information ved hjælp af en nøgle. Kun indehaveren af nøglen kan bryde koden og få adgang til informationerne. Ved asymmetrisk kryptering anvendes to nøgler, en offentlig og en privat nøgle.

Hvis man ønsker at sende en krypteret e-mail, skal afsenderen kende modtagerens offentlige nøgle. Afsenderen krypterer beskeden med modtagerens offentlige nøgle. Modtageren dekrypterer den med sin private nøgle.

Det er muligt at få et nøglesæt med en offentlig og en privat nøgle via NemID. Det kræver en vis teknisk viden at installere og bruge dem i et mailprogram. Brugere uden den fornødne tekniske viden kan få hjælp og vejledning på nettet samt via telefonsupport.

Hvis kommunikationen mellem en browser og et websted er krypteret, begynder web-adressen med HTTPS i stedet for HTTP.

3.9. VPN (virtuelt privat netværk)

Et virtuelt privat netværk (VPN) udnytter kryptering til at beskytte information, der sendes over internettet. Et VPN kan udgøre en form for tunnel gennem internettet fra brugerens pc til serveren på vedkommendes arbejdsplads. Dermed er man beskyttet mod aflytning, selvom det skulle lykkes angribere at opsnappe de datapakker, der indgår i kommunikationen.

3.10. Trådløse netværk

Trådløse netværk sender data som radiobølger. Derfor kan enhver, der er inden for senderens rækkevidde, opsnappe signalerne. Til at beskytte kommunikationen kan man anvende kryptering, der typisk følger standarden WPA2 (Wi-Fi Protected Access). Så er det kun brugere, der har password til nettet, der kan se data på det.

Hvis et trådløst netværk kan bruges, uden at man indtaster en adgangskode, er det ikke beskyttet med kryptering. Dermed kan de øvrige brugere på nettet potentielt se de data, brugeren sender og modtager. Angribere kan fx udføre man-in-the-middle-angreb, hvor alle data fra offerets pc sendes gennem angriberens computer, før de sendes videre.

Hvis netværket er beskyttet med en adgangskode, som alle deles om, kan andre brugere på nettet også få adgang til ens data. Man kan beskytte sig mod aflytning på trådløse netværk ved at anvende et VPN (virtuelt privat netværk, se definitionen i afsnit 3.9).

3.11. Passwords

Adgangen til mange it-systemer er beskyttet af kombinationen af et brugernavn og et password (også kaldet kodeord). It-kriminelle kan angribe passwords ved hjælp af programmer, der systematisk afprøver en lang række mulige koder. Disse koder hentes fra ordbøger og andre ordlister. Et password, der kan findes i en ordliste eller en liste over ofte anvendte koder, er derfor ikke sikkert.

Et sikkert password skal være unikt og skal være mindst 12 tegn langt. Man kan med fordel følge anvisningerne i Passwordvejledning fra Center for Cybersikkerhed.

Hvis man bruger det samme password til flere tjenester, udsætter man sig for en risiko. Hvis blot en af tjenesternes sikkerhed bliver kompromitteret, får angribere fat i ens brugernavn og password. De kan derefter afprøve, om den samme kombination giver adgang til andre tjenester. Derfor anbefales det at bruge unikke passwords til alle tjenester.

3.12. To-trinsbekræftelse

To-trinsbekræftelse, også kaldet to-trinslogin, to-faktorsikkerhed eller to-faktorautentifikation, er en metode til at øge sikkerheden ved systemer, der er beskyttet med brugernavn og password. Her suppleres passwordet med et ekstra element, som brugeren skal anvende for at få adgang. Det kan fx være et nøglekort, som det kendes fra NemID: Her skal brugeren først indtaste brugernavn og adgangskode. Derefter skal der indtastes en engangskode, som står på det udleverede kort. Dermed kan hackere ikke misbruge et brugernavn og password, selvom de har fundet frem til dem, hvis de ikke har det tilhørende nøglekort.

Andre eksempler på to-trinsbekræftelse er engangskoder, der tilsendes via sms eller genereres af en app på en smartphone.

3.13. Lagring af passwords

Det kan være vanskeligt at huske unikke passwords til alle de tjenester, man anvender. En passwordmanager er et program, der opbevarer alle brugerens passwords beskyttet med kryptering. For at få adgang til databasen over passwords skal man indtaste et masterpassword. Derefter kan man kopiere og indsætte passwords i de tjenester, de tilhører.

En fordel ved passwordmanagers er, at de letter administrationen af sikre passwords. En ulempe er, at hvis angribere får fat i databasen og knækker masterpasswordet, har de adgang til alle brugerens passwords.

De fleste browsere giver mulighed for at gemme brugernavn og passwords til web-tjenester. Hvis brugeren gør det, og en angriber får fat i vedkommendes computer, kan angriberen benytte de lagrede oplysninger til at få adgang til tjenesterne. I nogle tilfælde beskytter browseren passwords ved at lagre dem krypteret. Nogle browsere giver mulighed for at beskytte adgangen med et password, som brugeren skal indtaste, før der er adgang til at bruge de lagrede passwords.

Nogle browsere giver mulighed for at synkronisere lagrede passwords på tværs af enheder. Dermed skal en angriber kun få fat i en enkelt enhed for at få adgang til alle de lagrede passwords.

Lagring af passwords i browsere udgør en sikkerhedsrisiko, der er størst, hvis angriberen får fysisk adgang til enheden.

3.14. Single sign-on

Single sign-on (SSO) er en teknologi, der lader brugere logge ind på flere systemer med det samme sæt brugernavn og password. Som regel anvender systemerne i virkeligheden forskellige passwords, men SSO-løsningen sørger for at sende det korrekte brugernavn og password til de enkelte systemer, uden at brugeren bliver involveret.

Single sign-on er et centraliseret alternativ til password managers (se definitionen i afsnit 3.13). Det løser problemet med at holde styr på mange sikre passwords for de systemer, der er omfattet af det. Svagheden er også den samme som ved password managers: Hvis en angriber får fat i brugerens password, kan vedkommende potentielt få adgang til alle tjenester, brugeren har adgang til.

3.15. Deling af passwords

En medarbejder bør aldrig dele sine passwords med andre. Men i en it-afdeling kan der stadig være systemer, som flere systemadministratorer og andre tekniske medarbejdere har brug for at tilgå. Det kan være centrale servere, routere, administrative servere og lignende. Ofte skal man logge ind som én bestemt bruger. Derfor kender alle de betroede medarbejdere brugernavn og adgangskoder til disse systemer. Her deles flere medarbejdere altså om et password, der giver adgang til systemer, som kan være afgørende for organisationens drift. Det er en praksis, der ikke er i overensstemmelse med moderne sikkerhedsstandarder, og som bør undgås.

Det medfører især sikkerhedsmæssige udfordringer i forbindelse med udskiftning af personale. Når en medarbejder forlader en stilling, bør alle delte passwords udskiftes, så vedkommende ikke fortsat kan tilgå systemerne. Endvidere kan man beskytte sin organsiation mod misbrug ved at begrænse, hvorfra det er muligt at logge ind på systemerne. Det kan ske via fysisk adgangskontrol eller krav om, at brugerne skal anvende et særligt VPN (se definitionen i afsnit 3.9). I sidstnævnte tilfælde skal medarbejderens konto på VPN'et blot lukkes for at spærre for adgangen til systemerne med delte passwords.

Der findes også systemer, der gør det muligt at styre adgangen til delte systemer, uden at medarbejderne deler passwords til dem. Det indebærer også den fordel, at man efterfølgende kan identificere, hvem der har været logget på systemet på et bestemt tidspunkt.

3.16. Opdatering af programmer

Mange angreb udnytter sårbarheder i de programmer, ofrene anvender. En sårbarhed kan fx være en programmeringsfejl, der giver uvedkommende adgang til at køre skadelig software på systemet. Når softwareproducenterne opdager sårbarheder i deres produkter, udsender de opdateringer, der lukker sikkerhedshullerne. Det er derfor afgørende for sikkerheden, at software holdes opdateret. Sårbarheder forsøges ofte massivt udnyttet i den nærmeste tid efter udsendelse af en opdatering. Det skyldes, at angriberne satser på, der går nogen tid, før brugerne får opdateret deres systemer.

Alle moderne styresystemer har indbyggede funktioner til at installere opdateringer automatisk. Brugerne har dog mulighed for at slå funktionen fra.

Applikationer har varierende grader af automatisering, når det gælder opdatering. Nogle browsere opdateres automatisk. Det kræver kun, at brugeren lukker programmet og starter det igen. Udvidelsesprogrammer til browsere som Adobe Flash Player og Java kan sættes til at opdatere automatisk.

Automatisk opdatering af styresystemer og applikationer øger sikkerheden, men skal suppleres med manuel opdatering af de programmer, der ikke kan opdateres automatisk.

3.17. Sikkerhedskopiering

For at sikre data mod at gå tabt eller blive ændret kan man tage kopi af dem. En sikkerhedskopi kan blandt andet sikre, at offeret kan få adgang til sine data efter et angreb med ransomware. I stedet for at betale løsesummen kan offeret indlæse den seneste sikkerhedskopi. Dermed mister man kun de data, der er dannet, efter sikkerhedskopien blev taget. Af samme grund er det en fordel at tage hyppige sikkerhedskopier.

Sikkerhedskopier kan tages på bånd, brændbare cd'er/dvd'er, flytbare diske eller servere på netværket. Endvidere er der også cloud-udbydere, der tilbyder sikkerhedskopiering. Her kører der et program på brugerens computer, der løbende kopierer ændrede filer over på en server på internettet.

En fordel ved cloud-baseret sikkerhedskopiering er, at kopien altid er opdateret. Det kan dog også være en ulempe: Hvis et ransomware-program krypterer brugerens filer, bliver de krypterede filer straks sikkerhedskopieret. Dermed kan brugeren kun gendanne data, hvis cloud-tjenesten giver mulighed for at lagre data i flere versioner, så en tidligere, ukrypteret version kan gendannes.

4.
Offentligt ansattes informationssikkerhed

4. Offentligt ansattes informationssikkerhed

Dette kapitel belyser den aktuelle status for informationssikkerhed hos offentligt ansatte.

I dette afsnit gennemgår vi de konkrete tal, som Danmarks Statistik har indsamlet, og sammenligner resultaterne med tallene fra 2016, hvor det er muligt. I afsnit 4.9 kan du finde en analyse af tallene og en forklaring på, hvorfor de ser ud som de gør.

Undersøgelsen blandt de offentligt ansatte stødte på den udfordring, at nogle medarbejdere ikke har en computer til deres personlige brug. I stedet deles de om afdelingscomputere. Det gælder eksempelvis for nogle ansatte i sundhedssektoren. De vil derfor sjældent vide noget om, hvorvidt en bestemt computer har været inficeret med virus.

For at undgå det problem er nogle spørgsmål kun stillet til medarbejdere, der har fået stillet en computer, smartphone eller tablet til rådighed til eget brug. Mere generelle spørgsmål er stillet til alle.

Deltagerne fik at vide, at spørgsmålene udelukkende handlede om deres brug af computer på arbejdet. De skulle altså ikke svare ud fra, hvad de oplever uden for arbejdssituationen.

4.1. Oplevede trusler

De oplevede trusler på offentligt ansattes computere fordelt på fire forskellige trusler mod deres informationssikkerhed ser således ud (se Figur 1).

a) 11 procent har været ude for, at computeren har været inficeret med virus eller andre typer skadelige programmer.
b) To procent har mistet data som følge af et angreb.
c) Otte procent har mistet data som følge af manglende backup.
d) En procent har oplevet, at uvedkommende har fået fat i data, de har ansvaret for.

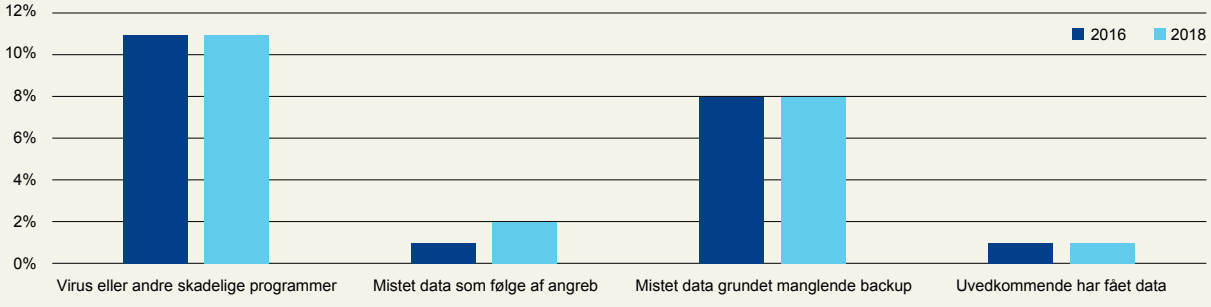
51 procent anmeldte sikkerhedsproblemet til it-funktionen på deres arbejdsplads, hvilket er lidt færre end i 2016 (57 procent).

Kun godt to procent har downloadet en skadelig app eller andet skadeligt indhold til deres smartphone eller tablet-computer, hvilket ligger på niveau med 2016.

Figur 1

Oplevede informationssikkerhedsproblemer

Sikkerhedsproblemerne ser ret konstante ud mellem 2016 og 2018.



4.2. Konsekvenser som følge af truslerne

De medarbejdere, der havde oplevet en eller flere af de fire sikkerhedstrusler, blev spurgt, hvilke konsekvenser hændelsen havde for deres adfærd (se Figur 2).

a) 55 procent har undladt at besøge bestemte websteder.
b) 15 procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv Erhverv, digital post eller borger.dk).
c) 51 procent har installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 67 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 59 procent har fået arbejdspladsens it-funktion til at hjælpe sig med at beskytte data og computer.
f) 82 procent har undladt at åbne mail, der kommer fra ukendte.

Vi spurgte også de medarbejdere, der ikke havde oplevet sikkerhedsproblemer, om de havde foretaget nogle af de samme handlinger for at forebygge problemer. Også her havde stort set alle foretaget en eller flere ændringer i adfærd. Dette ligger lidt højere eller på niveau med 2016.

a) 56 procent har undladt at besøge bestemte websteder.
b) 26 procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv Erhverv, digital post eller borger.dk).
c) 40 procent har installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 67 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 51 procent har fået arbejdspladsens it-funktion til at hjælpe sig med at beskytte data og computer.
f) 80 procent har undladt at åbne mail, der kommer fra ukendte.

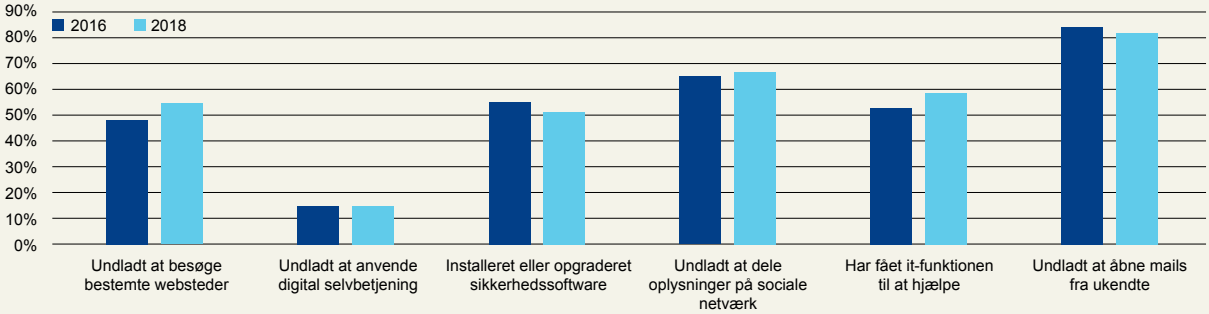
Adfærden og handlingerne foretaget af de to grupper indikerer, at der er en bred forståelse af, hvordan man skal sikre sig, både hvis man har været ramt af et sikkerhedsproblem eller ikke har.

Ransomware har været et meget omtalt sikkerhedsproblem i de seneste år. To procent oplyser, at de faktisk har været ramt af ransomware, 96 procent oplyser, at de ikke har været ramt, mens to procent ikke er klar over det. I 2016 var antallet af ramte på seks procent, så der er sket en nedgang i antallet.

De, der var ramt af ransomware, blev spurgt, hvad de selv eller arbejdspladsens it-funktion gjorde for at få adgang til data igen. Der har dog været for få observationer til at give en valid konklusion.

Figur 2

Handlinger for at forbedre sikkerheden
Der er kommet mindre fokus på sikkerhedssoftware i forhold til sidste undersøgelse.



4.3. Ondsindede digitale beskeder og phishing

Mange trusler ankommer i form af digitale beskeder: E-mail, sms'er, chat-beskeder eller indlæg på sociale netværk. Ofte er et klik på et link første skridt på vej mod sikkerhedsproblemer.

65 procent oplyser, at de undersøger, hvor et link i en mail eller sms fører hen, før de klikker på det. Dermed kan de undgå at lande på farlige websteder.

Vi har spurgt, om medarbejderne har modtaget tre former for beskeder med risikabelt indhold via e-mail, sms eller chat.

Den første type er en besked med et link, som modtageren opfordres til at klikke på. Resultatet kan være, at der installeres skadelig software på computeren, eller at brugeren føres til en forfalsket webside.

48 procent har modtaget sådan en mail. De reagerede på forskellig vis (se Figur 3).

a) To procent klikkede på linket.
b) En procent førte musen over linket for at se, hvor det førte hen. De klikkede på det, da det så ud til at være i orden.
c) 32 procent førte musen over linket for at se, hvor det førte hen. De klikkede ikke på det, da det virkede mistænkeligt.
d) 28 procent orienterede arbejdspladsens it-funktion.
e) 37 procent gjorde noget andet.

Den anden type skadelig besked, vi spurgte til, er phishing (se definitionen i afsnit 3.5). 25 procent havde modtaget en phishing-besked. En procent ved ikke. Her spurgte vi også til, hvilken handling, der blev foretaget (se Figur 4).

a) 58 procent klikkede ikke på linket.
b) Fire procent klikkede på linket, men indtastede ikke de ønskede oplysninger.
c) Godt to procent klikkede på linket og indtastede de ønskede oplysninger.
d) 16 procent orienterede arbejdspladsens it-funktion.
e) 20 procent gjorde noget andet.

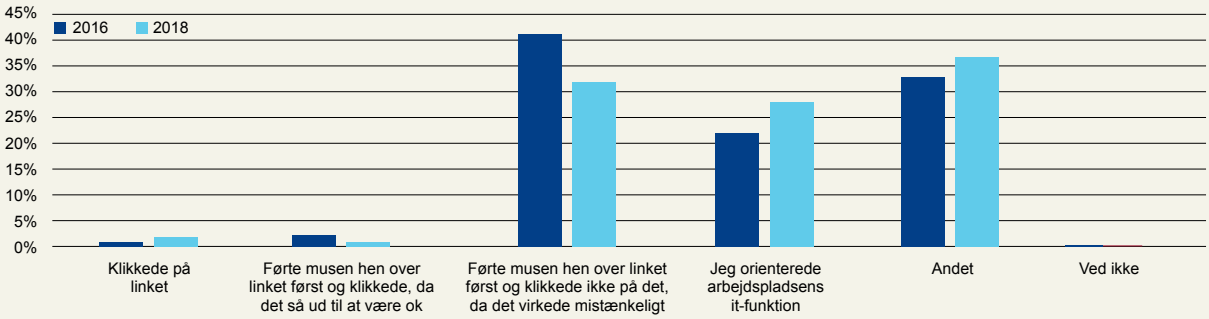
Endelig spurgte vi til direktørsvindel (se definitionen i afsnit 3.6). Fire procent havde modtaget en eller flere beskeder med direktørsvindel, mens 96 ikke har oplever problemet. I 2016 oplevede syv procent at modtage en mail med direktørsvindel. Disse fup-beskeder udsendes ofte i bølger, hvilket kan være en forklaring på forskellen.

Ni procent har været ude for opkald fra falsk teknisk support (se definitionen i afsnit 3.7). Det er samme antal som i 2016.

Figur 3

Handlinger ved mail med tvivlsomt link

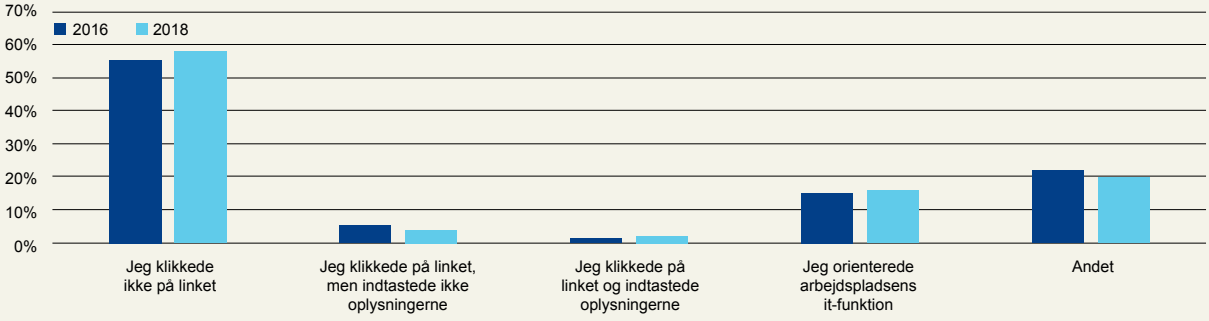
De færreste klikker på mistænkelige links, de får tilsendt uopfordret.



Figur 4

Handlinger ved phishing-mail

Kun få falder for phishing-svindel.



4.4. De offentligt ansattes adfærd

Vi har i 2018 stillet en række nye spørgsmål om, hvordan brugerne opfører sig i hverdagen. Svarene afspejler, i hvor høj grad brugerne udviser sikker adfærd.

Grundlæggende er det altid arbejdspladsens ledelse, der via informationssikkerhedspolitikken udstikker retningslinjer for medarbejdernes adfærd. De nye spørgsmål, vi har stillet i forbindelse med denne undersøgelse afspejler dog, hvad der er god praksis i håndtering af fortrolige oplysninger.

Det er derfor bekymrende, hvis medarbejderne sender fortrolige oplysninger ukrypteret via åben mail (se Figur 5). Men det kan bero på manglende viden om, at åbne mails er ubeskyttede, eller hvad reglerne er. Kryptering er en teknisk disciplin, der måske kan afskrække medarbejdere, der ikke har teknisk forståelse. Her kan ledelsen med fordel sætte ind med information.

30 procent har sendt et cpr-nummer eller andre personlige oplysninger i en e-mail til andre offentlige instanser, mens 69 procent ikke har gjort det og en procent ikke ved det. Af dem, der sendte cpr-numre, oplyser 77 procent, at der er anvendt krypteret e-mail. 21 procent (svarende til 6,3 procent af de offentligt ansatte) har anvendt åben mail (se Figur 6).

Vi har som noget nyt i denne undersøgelse spurgt om respondentens adfærd kan have medført, at uvedkommende kan have fået adgang til fortrolige data. Det kan eksempelvis være sket ved en mistet USB-nøgle eller mobiltelefon.

Fire procent svarer, at uvedkommende kan have fået adgang til personlige data, mens 95 procent svarer nej. En procent ved ikke (se Figur 7).

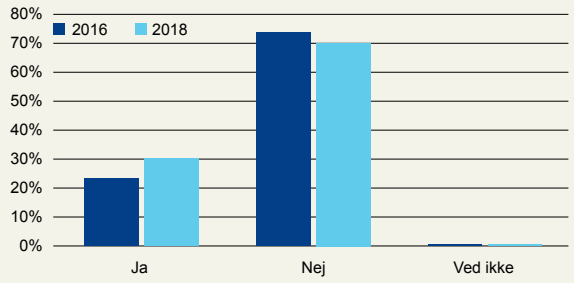
83 procent låser deres pc, når de forlader den, så andre ikke kan bruge den i deres fravær. 17 procent gør ikke (se Figur 8). Det er på niveau med 2016.

49 procent af deltagerne har mulighed for at tilgå arbejdspladsens systemer hjemmefra. Tre ud af fire af dem anvender VPN (virtuelt privat netværk) til at beskytte kommunikationen (se definitionen i afsnit 3.9).

Figur 5

Har du sendt cpr eller personlige oplysninger via mail?

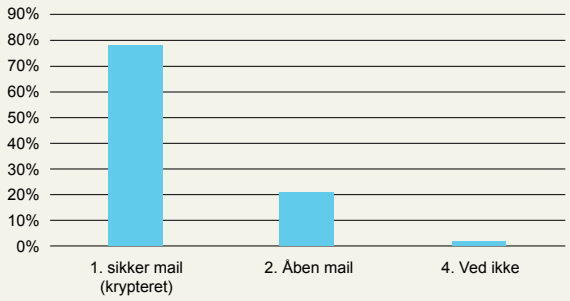
30 procent har sendt cpr-nummer vi e-mail.



Figur 6

Sendes oplysninger via krypteret eller åben mail?

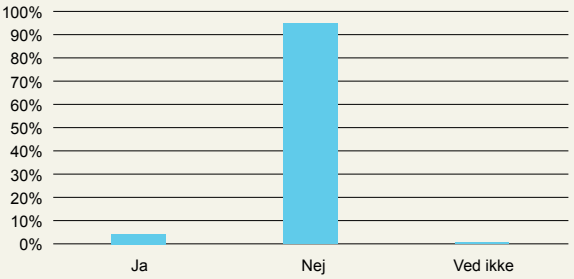
Hele 21 procent oplyser, at de har sendt cpr-nummer via mail uden kryptering.



Figur 7

Kan andre have fået adgang til disse data?

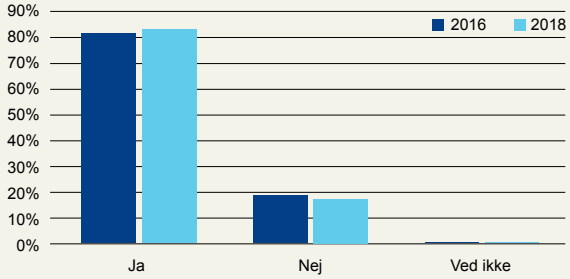
Langt hovedparten er ret sikre på, at uvedkommende ikke kan have fået adgang til deres data.



Figur 8

Låser du pc når den forlades?

17 procent låser ikke deres pc. I 2016 var tallet 18 procent.



4.5. Beskyttelse af enheder

92 procent har installeret sikkerhedsprogrammer, såsom antivirus og firewall, på arbejds-pc'en. Fem procent svarer nej, tre procent ved det ikke. Det er på niveau med 2016 (se Figur 9).

70 procent har sikkerhedsprogrammer på den smartphone eller tablet-computer, de bruger på jobbet. 23 procent har det ikke, seks procent ved det ikke eller har ikke svaret (se Figur 10).

Nok så væsentlig er det, om de installerede sikkerhedsprogrammer opdateres. 93 procent holder programmer på deres computer opdateret (se omtalen af softwareopdatering i afsnit 3.16). Der kan svares i flere kategorier. Svarene fordeler sig således (se Figur 11).

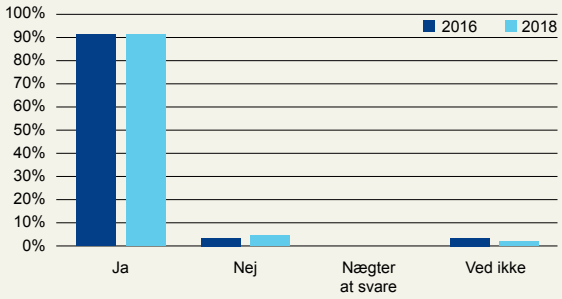
a) Hos 86 procent sørger arbejdspladsens it-funktion for det.
b) 14 procent har slået automatisk opdatering til.
c) Seks procent opdaterer nogle programmer manuelt.

I forhold til 2016 er der en svag stigning i, at arbejdspladsens it-funktion opdaterer, mens medarbejderen i mindre grad gør det selv.

Figur 9

Har du sikkerhedssoftware på din arbejds-pc?

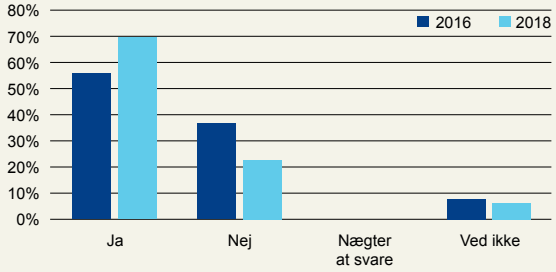
Der er fem procent, der ikke har sikkerhedssoftware på deres arbejds-pc.



Figur 10

Har installeret sikkerhedssoftware på mobil/tablet fra arbejdspladsen.

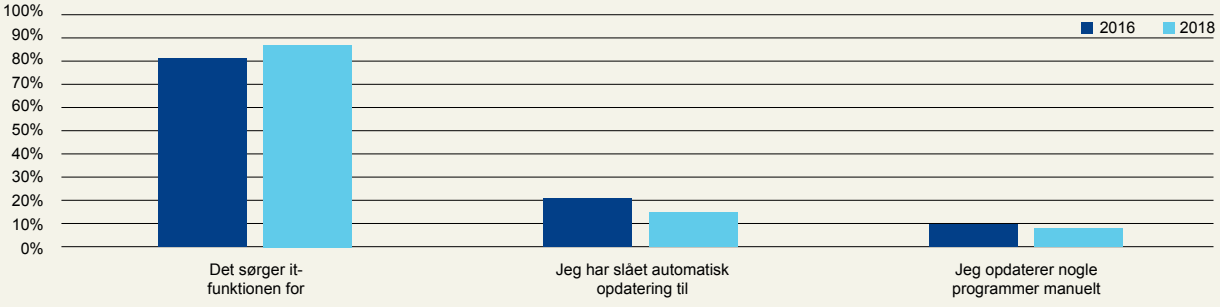
På tablet-computer og telefon er det 23 procent, der ikke har installeret sikkerhedssoftware.



Figur 11

Sådan holdes software opdateret.

Hovedparten overlader opdateringer til arbejdspladsen.



4.6. Trådløse netværk

Ni ud af ti oplyser, at der er et trådløst netværk på arbejdspladsen.

80 procent af brugerne af trådløst netværk på arbejdspladsen skal indtaste en adgangskode for at få adgang til netværket. Det er ofte tegn på, at forbindelsen er krypteret, men er det ikke altid (se omtalen af trådløse netværk i afsnit 3.10).

45 procent anvender trådløse netværk, når de er væk fra arbejdspladsen (se Figur 12). Ud af dem anvender 26 procent også netværk, der ikke kræver en adgangskode og dermed er ukrypterede og usikre (se Figur 13).

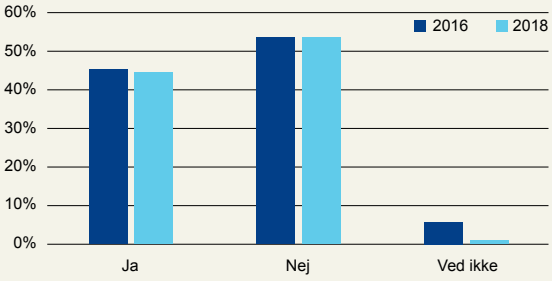
26 procent anvender trådløse netværk, hvor alle bruger samme adgangskode, fx på caféer og lignende. Det er et fald fra 34 procent i 2016. Grunden til faldet kan skyldes, at der er kommet en bedre forståelse af, at trådløse net uden kryptering giver en sikkerhedsrisiko.

Halvdelen anvender VPN (se definitionen i afsnit 3.9) til kommunikationen med arbejdet, når de bruger trådløse netværk uden for arbejdspladsen. 48 procent gør ikke, mens tre procent ikke ved det. I 2016 benyttede 46 procent VPN, hvilket giver en lille stigning i antallet (se Figur 14).

Figur 12

Anvendes trådløst netværk udenfor arbejdspladsen?

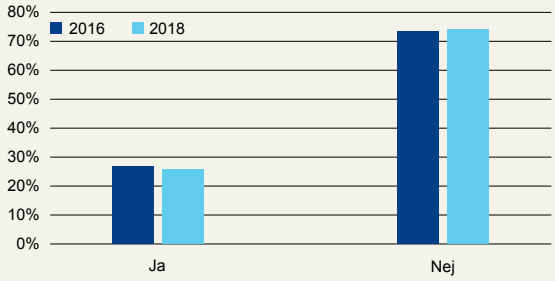
Knap halvdelen anvender trådløst netværk uden for arbejdspladsen.



Figur 13

Anvendes trådløst netværk uden adgangskode?

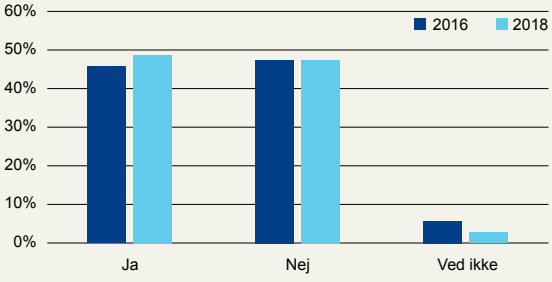
Godt en fjerdedel af dem, der anvender trådløst netværk uden for arbejdspladsen, benytter netværk uden kode.



Figur 14

Anvendes VPN?

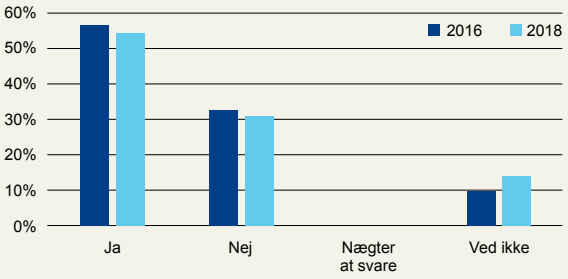
VPN til kommunikation med arbejdet bruges af halvdelen.



Figur 15

Bliver der taget sikkerhedskopi af dine data?

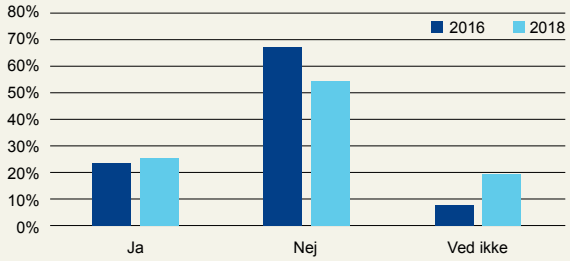
Hele 31 procent svarer, at der ikke tages sikkerhedskopi af arbejdsdata.



Figur 16

Bliver der taget sikkerhedskopi af telefon eller tablet?

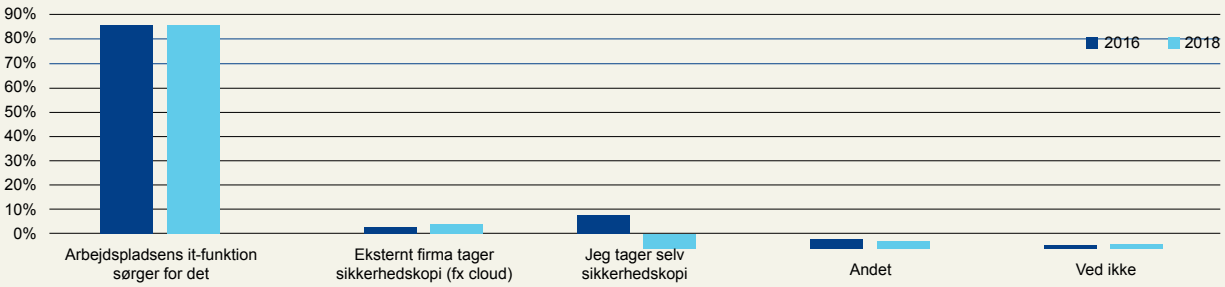
Over 50 procent har ikke en sikkerhedskopi af telefon eller tablet-computer.



Figur 17

Sikkerhedskopiering af data

Hos de fleste sørger it-funktionen for at sikkerhedskopiere data.



4.7. Sikkerhedskopiering

55 procent oplyser, at der bliver taget sikkerhedskopi af de data, vedkommende bruger i sit arbejde (se omtalen af sikkerhedskopiering i afsnit 3.17). 31 procent svarer nej, mens 14 procent ikke ved det (se Figur 15). Det er et lille fald i forhold til 2016.

Sikkerhedskopiering af arbejdsdata bliver varetaget på disse måder (se Figur 17).

a) Hos 85 procent sørger arbejdspladsens it-funktion for det.
b) Hos fire procent tager et eksternt firma sikkerhedskopi (fx med en cloud-løsning).
c) Seks procent tager selv sikkerhedskopi.
d) Tre procent svarer ”Andet”.
e) To procent ved det ikke.

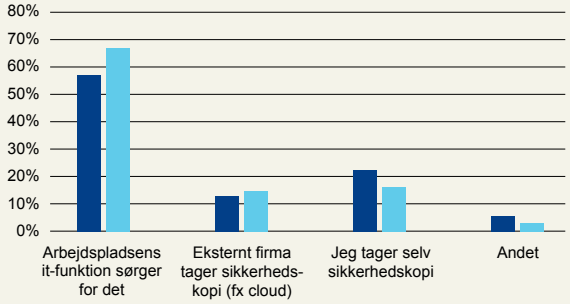
Fire ud af ti får taget sikkerhedskopi af data på smartphone eller tablet. 55 procent svarer nej til spørgsmålet, 20 procent ved det ikke (se Figur 16). Af dem, der får taget sikkerhedskopi, er metoderne fordelt således (se Figur 18).

a) Hos 67 procent sørger arbejdspladsens it-funktion for det.
b) Hos 15 procent tager et eksternt firma sikkerhedskopi (fx med en cloud-løsning).
c) 16 procent tager selv sikkerhedskopi.
d) Tre procent svarer ”Andet”.

Figur 18

Sikkerhedskopiering af smartphone/tablet

Lidt flere anvender cloud-tjenester til sikkerhedskopi, når det gælder telefon og tablet-computer.



37 procent bruger samme adgangskode til flere systemer eller tjenester på arbejdet i 2016 var det 33 procent (se omtalen af passwordsikkerhed i afsnit 3.11-3.15). 28 procent har kun ét sæt brugernavn og password (se Figur 19).

Godt halvdelen (54 procent) af dem, der bruger samme password til flere systemer, gør det også til systemer, der behandler følsomme data (se Figur 20). Det er en stigning i forhold til 2016.

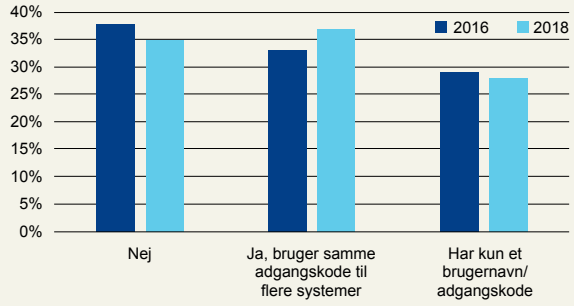
Endvidere oplyser én ud af ti, at de er flere medarbejdere, der deles om samme passwords til fælles it-systemer eller databaser. Det er samme niveau som i 2016 (se definitionen af delte passwords i afsnit 3.15) (se Figur 21).

Vi har spurgt, om arbejdspladserne tilbyder single sign-on (se definitionen i afsnit 3.14). Det gør de hos 36 procent af medarbejderne, mens 40 procent har forskellige login. 14 procent har ikke brug for det, da de kun har ét system, de skal logge ind på (se Figur 22).

Af de respondenter, der anvender flere systemer, oplyser 76 procent, at de selv har valgt at benytte det samme password til flere systemer.

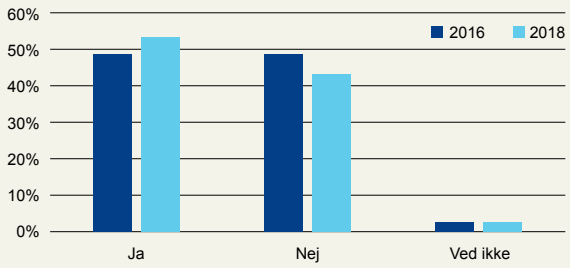
Figur 19

Har du samme adgangskode til flere systemer?
Mere end hver tredje bruger samme adgangskode til flere systemer/tjenester.



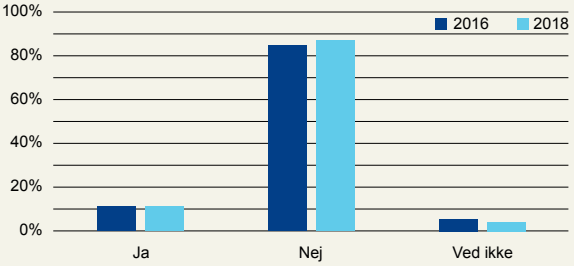
Figur 20

Benyttes samme kode til følsomme systemer?
54 procent af dem, der bruger samme password til flere systemer, gør det også til systemer, som behandler følsomme data.



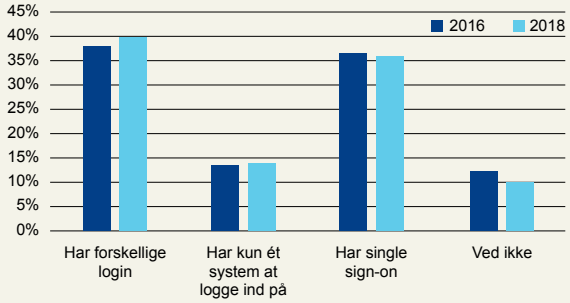
Figur 21

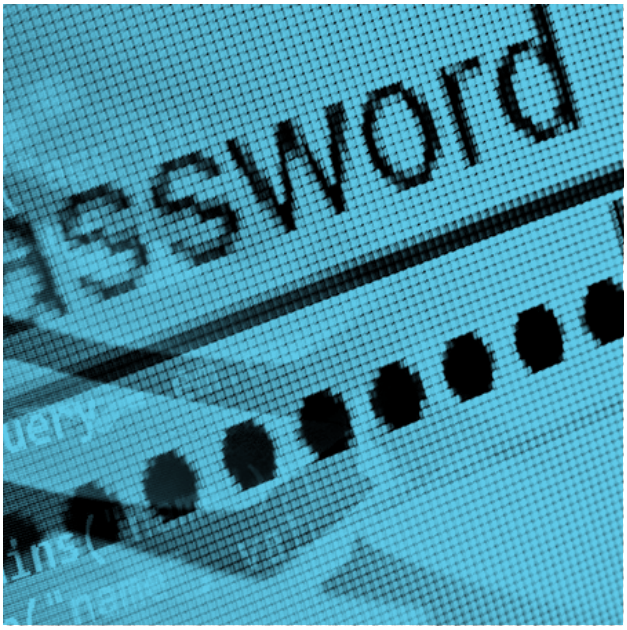
Er I flere medarbejdere om samme password?
11 procent deler adgangskode med flere.



Figur 22

Forskellige login eller single-on?
En tredjedel af medarbejderne har et single sign-on-system, der styrer adgangen til systemerne.





27 procent (se Figur 23) lader deres browser lagre passwords (se definitionen i afsnit 3.13). 62 procent af dem oplyser, at disse passwords er beskyttet med en adgangskode, der skal indtastes, før man får adgang til dem.

Af dem, der gemmer password i browseren beretter 33 procent, at de ikke er beskyttet med en adgangskode. 62 procent fortæller, at de benytter adgangskode til browserens gemte password. I 2016 sagde 25 procent ja og 74 procent sagde nej.

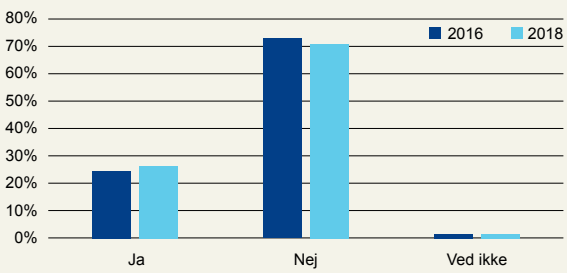
Syv procent anvender en passwordmanager til at opbevare og holde styr på passwords (se definitionen i afsnit 3.13). 74 procent af dem bruger en password manager, hvor data lagres krypteret og beskyttes med adgangskode.

60 procent har en metode til at huske sikre passwords med. I sidste rapport var det halvdelen. Mediernes mange historier om stjålne password og informationskampagner om vigtigheden af stærke adgangskoder, der ikke anvendes på tværs af tjenester, kan have haft en afsmittende effekt.

Figur 23

Lader du browseren huske dit password?

27 procent gemmer adgangskoder i browseren. I 2016 var det 25 procent.



4.8. Sikkerhedsregler, kendskab og efterlevelse

57 procent oplyser, at de har sat sig ind i informationssikkerhedspolitikken for deres arbejdsplads. I 2016 var tallet 48 procent (se Figur 24).

Samtidig kan 63 procent oplyse, at de er blevet informeret om arbejdspladsens informationssikkerhedspolitik eller opdateringer til den. 35 procent er ikke og 2 procent ved det ikke (se Figur 25).

Men hele otte procent undlader nogle gange at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet.

I 2016 var tallet på seks procent. Det er en ikke uvæsentlig stigning på et område, der ellers burde være faldende (se Figur 26).

Vi spurgte dem, der indimellem ikke efterlever sikkerhedspolitikken, hvor ofte det sker (se Figur 27).

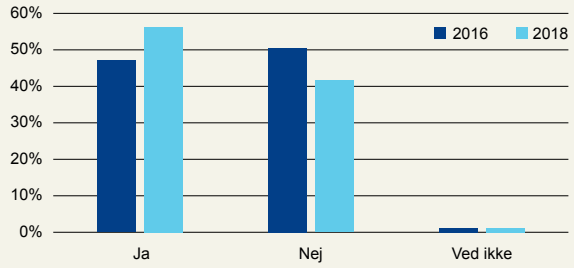
a) 15 procent omgår reglerne hver dag.
b) 18 procent omgår reglerne mindst en gang om ugen.
c) 19 procent gør det mindst en gang om måneden.
d) Hos 49 procent sker det sjældnere end en gang om måneden.

Det indebærer, at 2,64 procent i den offentlige sektor bryder sikkerhedsreglerne dagligt eller ugentligt, hvilket er en bemærkelsesværdig stigning i forhold til 2016.

Figur 24

Kender du sikkerhedspolitikken på arbejdet?

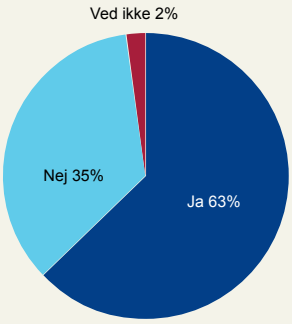
57 procent har sat sig ind i arbejdspladsens informationssikkerhedspolitik.



Figur 25

Er du blevet informeret om sikkerhedspolitikken?

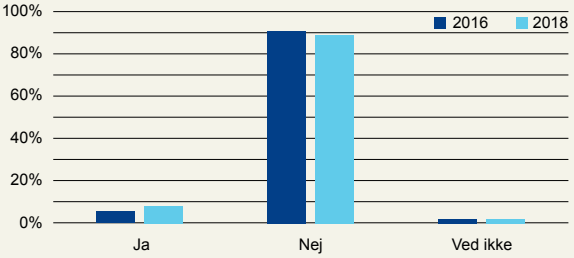
Det er langt fra alle arbejdsgivere, der har informeret om deres informationssikkerhedspolitik. Dette er et nyt spørgsmål i forhold til 2016, hvor vi spurgte om medarbejderne havde været på kursus i it-sikkerhed. Det havde 12 procent. Da der er ændret grundlæggende ved spørgsmålet, har vi ikke sammenfattet udviklingen i en graf.



Figur 26

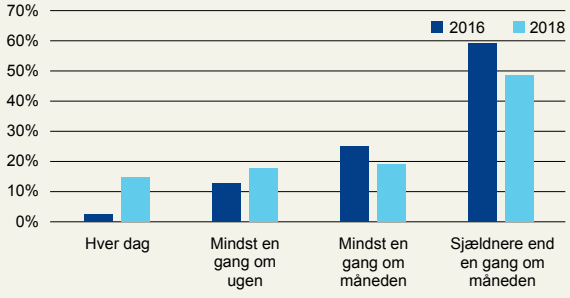
Undlader du nogle gange at følge sikkerhedsreglerne på arbejdspladsen?

Hele otte procent undlader nogle gange at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet.



Figur 27

Hvor ofte undlader du at følge sikkerhedsreglerne?



4.9. Delkonklusion om offentligt ansattes informationssikkerhed

4.10. Trusler

De offentligt ansatte i undersøgelsen oplever ikke alvorlige sikkerhedsproblemer i hverdagen. Der synes at være generelt godt styr på sikkerheden i den offentlige sektor.

I 2016 havde 16 procent af de offentligt ansatte været udsat for mindst en af fire trusler mod informationssikkerheden: Infektion med skadelig software, tab af data efter et angreb, tab af data grundet manglende backup, eller at uvedkommende fik adgang til data, vedkommende havde ansvaret for. I denne undersøgelse er tallet steget til 18 procent. Der er således sket en lille stigning på to procentpoint.

Der er dog stadig områder, hvor der er plads til forbedringer. Det gælder eksempelvis disse fire punkter:

1. De ansattes manglende efterlevelse af sikkerhedspolitikken.
2. Manglende backup.
3. Manglende kryptering af mails med følsomme oplysninger.
4. Genbrug af adgangskoder.

Blandt de offentligt ansatte oplyser 11 procent, at de har oplevet en infektion med virus eller anden type skadelige programmer. To procent oplyser, at de har mistet data som følge af et angreb. Det tyder på, at arbejdspladserne har styr på de grundlæggende discipliner såsom antivirus og mail-filtrering.

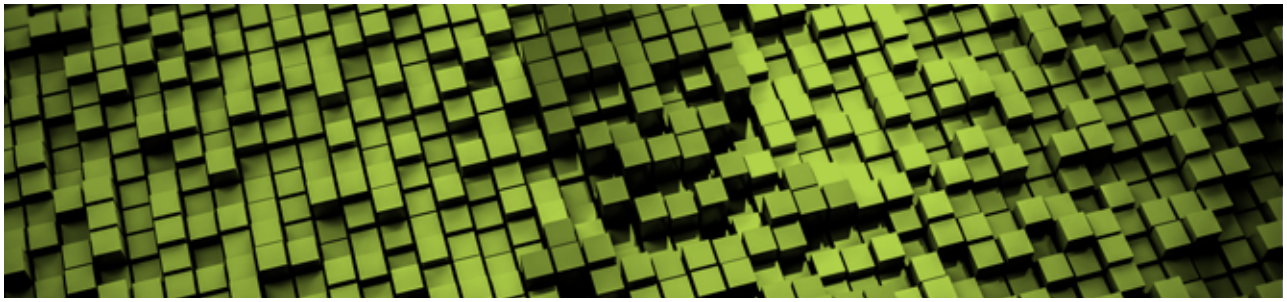
Otte procent oplyser, at de har oplevet datatab som følge af manglende backup, mens en procent har oplevet, at uvedkommende har fået fat i de data, de har ansvaret for. En bedre sikkerhedskopiering vil give højere produktivitet, hvilket ledelsen opfordres til at implementere.

To procent har downloadet en skadelig app til telefonen eller tablet-computeren. Ligeledes oplyser to procent, at de har været ramt af ransomware. Halvdelen af de offentligt ansatte har modtaget en mail med et tvivlsomt link, de blev opfordret til at klikke på. Det var dog kun to procent, der klikkede på linket. Der er ikke tale om alarmerende tal, men ondsindede udsendelser kommer typisk i bølger, så en fortsat oplysningsindsats og sikkerhedspolitik kan være med til at holde antallet nede. Ligeledes vil de mobile platforme i stigende grad blive mål for phishing o.l.

Fire procent har modtaget beskeder med direktørsvindel og ni procent har fået opkald fra en falsk teknisk supportenhed. Der er ingen tendens til nye problemer med ransomware på computeren. Problemet kræver dog stadig opmærksomhed, af samme grund som beskrevet ovenfor.

En ud af tre har sendt cpr-nummer eller andre personlige oplysninger via mail. 21 procent af dem i åbne mails uden kryptering. Det tyder på, at reglerne i Sikkerhedsbekendtgørelsen fra maj 2000 ikke har været implementeret korrekt, eller informationen omkring reglerne har været mangelfuld. Som følge af persondataforordningens implementering burde arbejdspladserne også være mere opmærksomme på reglerne.

31 procent oplyser, at der ikke tages sikkerhedskopier af data på computeren. 55 procent tager ikke sikkerhedskopier af data på telefon eller tablet-computer. Det tyder på, at nogle offentlige arbejdspladser ikke får taget sikkerhedskopi af alle data. En årsag kan være, at nogle medarbejdere lagrer data på deres egen computer eller mobile enhed, mens kun data på netværksdrev bliver sikkerhedskopieret. Ligeledes er alle måske ikke klar over, at der tages backup.



37 procent bruger de samme passwords til flere systemer. Det øger risikoen forbundet med hackerangreb på de systemer, de anvender: Hvis hackere får fat i blot ét sæt brugernavn og password, kan de forsøge at genbruge dem til andre systemer. En opstramning af password-sikkerheden vil styrke organisationens sikkerhedsniveau.

45 procent af de offentligt ansatte anvender offentligt tilgængelige trådløse netværk. Af dem anvender 26 procent netværk uden kryptering. Det medfører risiko for, at uvedkommende får adgang til data og systemer. Halvdelen anvender sikker VPN-forbindelse til arbejdet. Det burde være standard på arbejdspladser, der behandler følsomme oplysninger.

57 procent oplyser, at de har sat sig ind i informationssikkerhedspolitikken for deres arbejdsplads. I 2016 var tallet 48 procent. Otte procent undlader dog nogle gange at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet. Det lyder ikke af meget, men i betragtning af, at tallet i 2016 var på seks procent, så er der tale om en voldsom stigning på 30 procent. Af dem oplyser 15 procent, at det forekommer hver dag og yderligere 18 procent, at det forekommer mindst en gang om ugen.

Ledelsen bør følge op på dette og undersøge, om det er regler, praksis og/eller holdninger, der skal bearbejdes. Ledelsen kan passende starte med at oplyse medarbejderne om informationssikkerhedspolitikken. 63 svarer ja på spørgsmålet om, hvorvidt de har fået information om sikkerhedspolitikken, mens 35 procent svarer nej. Det er ubetinget en ledelsesopgave at udbrede kendskabet til sikkerhedspolitikken, og det er samtidig forudsætningen for, at medarbejderne kan agere sikkert og i henhold til det valgte sikkerhedsniveau.

Den mobile hverdag medfører nye sikkerhedsrisici. Hver fjerde af de medarbejdere, der bruger trådløst netværk i arbejdssammenhæng, når de er væk fra arbejdspladsen, anvender usikre netværk (se omtalen af sikkerhed ved trådløse netværk i afsnit 3.10). Omkring halvdelen benytter sig af VPN (se definitionen i afsnit 3.9), når de anvender trådløse netværk uden for arbejdspladsen.

Den usikre brug af trådløse netværk medfører en risiko for, at uvedkommende kan få adgang til fortrolige data, når medarbejderne er væk fra arbejdspladsen.

Det samlede prioriterede trusselsbillede for offentlige ansatte ser således ud:

1. Skadelig software inficerer computere.
2. Uvedkommende får adgang til fortrolige data eller inficerer computere ved hjælp af phishing og andre former for skadelige mails.
3. Sikkerhedspolitikken overholdes ikke altid, hvilket potentielt åbner arbejdspladsens data for uvedkommende.
4. Risiko for at følsomme data kompromitteres, hvis de sendes eksempelvis via mail.
5. Uvedkommende får adgang til fortrolige data ved at udnytte usikre trådløse netværk.
6. Uvedkommende får adgang til fortrolige data og it-systemer, fordi medarbejdere genbruger og deler passwords.
7. Medarbejdere mister data som følge af manglende backup.

4.11. Konsekvenser

De konkrete konsekvenser er, at 82 procent af dem, der har været udsat for sikkerhedsproblemer, har undladt at åbne mail, der kom fra ukendte afsendere. 55 procent har undladt at besøge bestemte websider.

To ud af tre har undladt at dele oplysninger om sig selv på sociale netværk. Seks ud af 10 har fået hjælp fra it-funktionen på deres arbejdsplads til at beskytte deres data og computer.

Tallene er nogenlunde de samme for de medarbejdere, der ikke har været udsat for sikkerhedsproblemer. Det tyder på, at det ikke gør den store forskel for medarbejdernes indstilling til informationssikkerhed, om de har oplevet sikkerhedsproblemer eller ej. Det viser, at der er en bred forståelse af, at sikkerhed på en arbejdsplads er essentielt.

4.12. Foranstaltninger - adfærd

4.12.1. Beskyttelse af enheder

Ni ud af ti har sikkerhedsprogrammer på deres computer. Når det gælder smartphones og tablet-computere, er tallet på 70 procent af medarbejderne, hvilket er en fremgang i forhold til 2016. 83 procent husker at låse computeren, når den forlades. Generelt er medarbejderne opmærksomme på, at det er vigtigt at holde software på enhederne opdateret.

4.12.2. Forsvar mod svindel

De offentligt ansatte har generelt sunde vaner, når det gælder svindel. De klikker ikke på et vilkårligt link, de får tilsendt i en mail eller sms. De kontrollerer, hvor et link fører hen, før de klikker. Og de lader sig ikke narre af engelsktalende, falske supportteknikere eller mails med ønske om at overføre store beløb til udlandet, også kaldet direktørsvindel. Kun to procent har downloadet en skadelig app til mobil eller tablet-computer.

4.12.3. Brug af passwords

Et område, hvor der er plads til forbedring, er adgangskoder: En ud af tre bruger det samme password til flere tjenester (se afsnit 3.11 om risikoen ved genbrug af passwords). Over halvdelen af dem, der bruger samme password til flere systemer, gør det også til systemer, der behandler følsomme data. En årsag til genbrug kan være, at det er vanskeligt at huske mange komplicerede passwords. Det problem kan løses med SSO (Single Sign-On, se definitionen i afsnit 3.14) eller en password manager (se definitionen i afsnit 3.13). Begge dele anvendes kun i begrænset omfang og er på niveau med 2016.

4.12.4. Brug af trådløse netværk

Ni ud af ti bruger trådløse netværk på arbejdspladsen. Heraf oplyser 80 procent, at man skal bruge kode. Det reelle tal kan være højere, hvis medarbejderen har sat sin enhed til at huske koden til nettet og derefter har glemt, at der oprin-delig blev indtastet en kode. Hver fjerde af de medarbejdere, der anvender trådløse netværk uden for arbejdspladsen, gør det også, selvom netværket ikke er krypteret. Dermed udsæt-ter de sig for risiko for aflytning. Dog bruger halvdelen VPN, der krypterer kommunikationen mellem deres computer og arbejdspladsens netværk.

4.12.5. Sikkerhedskopiering

Hele 31 procent svarer, at der ikke bliver taget sikkerhedskopi af deres data på computeren, hvilket er et lille fald på 2 pro-centpoint fra 2016. Og kun hver fjerde får taget sikkerheds-kopi af data på smartphone eller tablet-computer. Det er pri-mært arbejdspladsen, der tager backup og cloud-løsningerne bliver også anvendt mere. En bedre backup-politik vil give hø-jere produktivitet, da data hurtigt kan genskabes.

4.12.6. Informationssikkerhed på arbejdspladsen

Informationssikkerhed er altid et kompromis mellem ønsket om sikkerhed på arbejdspladsen og brugernes behov for at kunne udføre deres daglige arbejdsopgaver. Den balance ser det ud til, mange arbejdspladser opnår, men der er også en gruppe på otte procent, der til tider undlader at følge sikkerhedsreglerne for at udføre deres arbejde. 15 procent af dem gør det dagligt og 18 procent ugentligt. Det er uheldigt, når medarbejderne ser bort fra sikkerheden. Det åbner for problemer i hele organisationen, som ikke nødvendigvis kommer til udtryk i form af sikkerhedshændelser med det samme, men som kan medvirke til at undergrave borgernes tillid til den offentlige sektor.

57 procent oplyser, at de har sat sig ind i informationssikkerhedspolitikken for deres arbejdsplads. I 2016 var tallet 48 procent, så det går fremad. 63 procent oplyser, at de har fået information om informationssikkerhedspolitikken, mens 35 procent svarer nej. I 2016 stillede vi spørgsmålet, om offentligt ansatte havde været på kursus i it-sikkerhed, det betyder, at tallene ikke umiddelbart kan sammenlignes.

Der er stadig problemer med kryptering i forbindelse med følsomme data, der sendes via mail.

5.
Borgernes informationssikkerhed

5. Borgernes informationssikkerhed

Dette kapitel belyser den aktuelle status for informationssikkerhed hos danske borgere.

Spørgsmålene i dette kapitel er stillet til borgere i deres egenskab af privatpersoner. Her fortæller de om deres oplevelser med og kendskab til informationssikkerhed uden for arbejdstid. Nogle af spørgsmålene blev også stillet i de foregående undersøgelser af borgernes informationssikkerhed. Hvor det er relevant og muligt, sammenligner vi med svar fra de tidligere år for at vise udviklingen. Du kan finde vurderinger og analyser af tallene i afsnit 5.13.

5.1. Oplevede trusler

34 procent af borgerne fortæller, at deres enheder har været inficeret med virus eller skadelig kode (se definition afsnit 3.1), mens 17 procent har mistet data. De fire specifikke trusler mod deres informationssikkerhed, som vi har spurgt til, fordeler sig således (se Figur 28).

a) 34 procent har oplevet, at computeren var inficeret med virus eller andre typer skadelige programmer (948.000 borgere).
b) Fem procent har været ude for, at nogen har misbrugt deres personoplysninger på nettet (143.000 borgere).
c) Otte procent har mistet penge som følge af et informationssikkerhedsproblem (212.000 borgere).
d) 17 procent har mistet data som følge af et it-sikkerhedsproblem (fx et computernedbrud) hos dem selv eller hos en tjeneste på nettet (461.000 borgere).

Tre områder adskiller sig fra 2016. Flere har oplevet virusproblemer, flere har oplevet økonomiske tab, og så er mængden af datatab vokset betydeligt. Her kan ransomware og/eller manglende sikkerhedskopiering være medvirkende årsager, se afsnit 5.2.

I år har vi som noget nyt spurgt specifikt til sikkerhedstrusler på smartphone og tabletcomputer. Her er tendensen den samme, men færre er ramt. Otte procent oplyser, at deres smartphone eller tablet-computer har været inficeret med virus eller skadelige programmer.

Tre procent har fået misbrugt personoplysninger, og fire procent har mistet penge ved online-svindel eller afpresning.

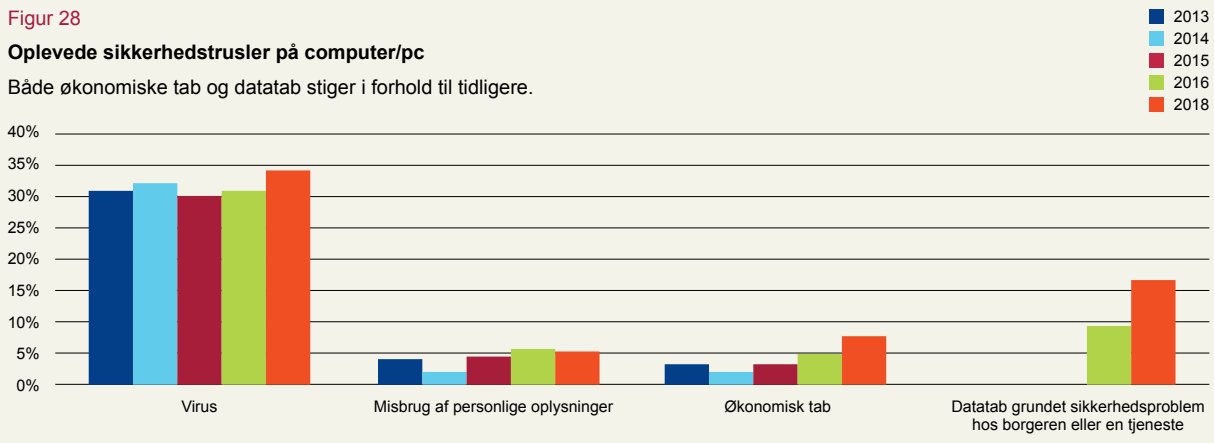
14 procent har mistet data, fordi deres telefon eller tabletcomputer er gået i stykker, og tre procent har mistet data/penge/personoplysninger, fordi de har mistet eller fået stjålet deres smartphone eller tablet-computer.

De borgere, der havde oplevet en eller flere af de fire sikkerhedstrusler, blev spurgt, hvilke konsekvenser hændelsen havde for deres adfærd. Stort set alle af disse havde gjort et eller flere tiltag for at mindske risikoen for yderligere problemer.

Figur 28

Oplevede sikkerhedstrusler på computer/pc

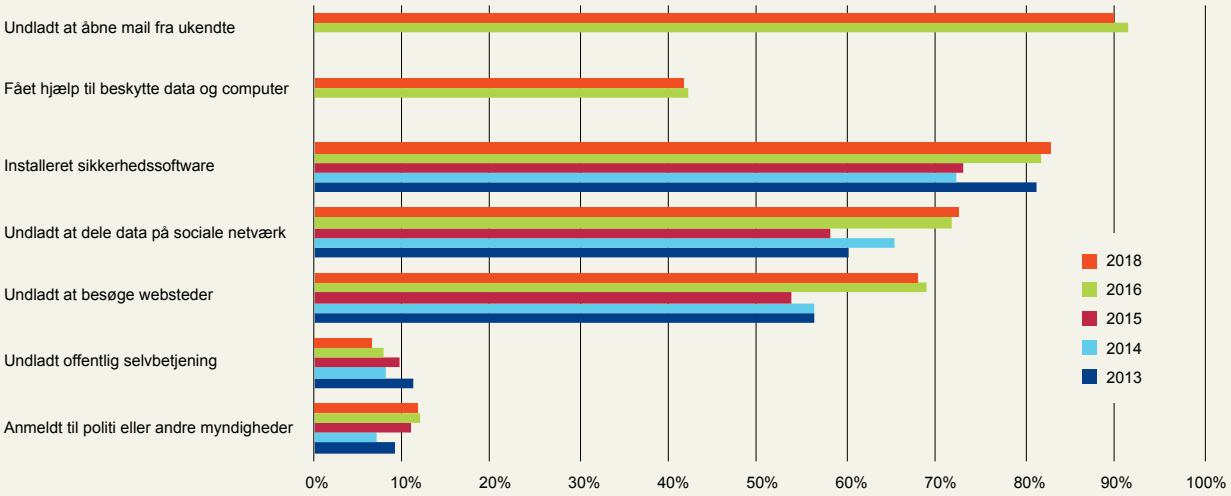
Både økonomiske tab og datatab stiger i forhold til tidligere.



Figur 29

Handlinger som følge af sikkerhedsproblemer

Mønstret i handlinger, som følge af sikkerhedsproblemer, ligger ret konstant ift. 2016.



I forbindelse med anvendelse af de digitale selvbetjeningstjenester er der sket et fald fra otte procent i 2016 til seks procent (se Figur 29).

a) 90 procent har undladt at åbne mail, der kommer fra ukendte.
b) 41 procent har fået nogen til at hjælpe sig med at beskytte sine data og computer.
c) 83 procent har installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 72 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 68 procent har undladt at besøge bestemte websteder.
f) Seks procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv, melde flytning, digital post eller borger.dk).
g) 12 procent har anmeldt sikkerhedsproblemet til politi eller andre.

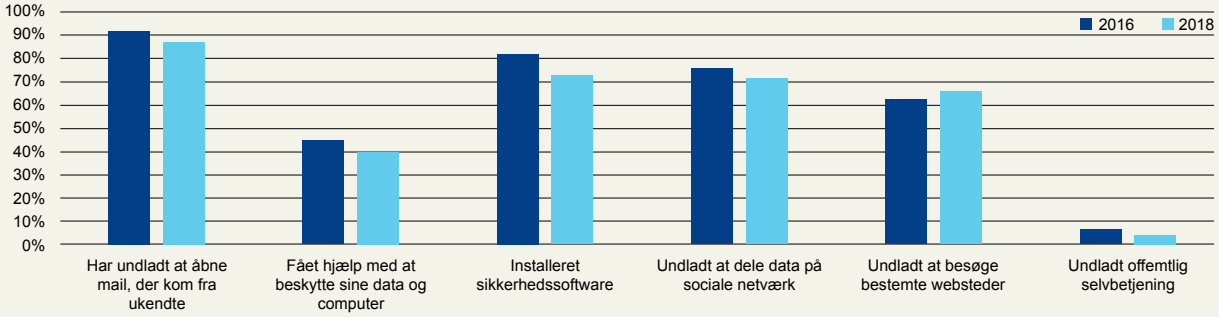
Vi spurgte også deltagere i undersøgelsen, der ikke havde oplevet sikkerhedsproblemer, om de havde foretaget nogle af de samme handlinger for at forebygge problemer.

Tallene fordeler sig således (se Figur 30):

a) 88 procent har undladt at åbne mail, der kommer fra ukendte.
b) 40 procent har fået nogen til at hjælpe sig med at beskytte sine data og computer.
c) 73 procent har installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 72 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 66 procent har undladt at besøge bestemte websteder.
f) Fire procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv, melde flytning, digital post eller borger.dk).

Figur 30

Handlinger i gruppen, der ikke har oplevet sikkerhedsproblemer



Som noget nyt i forhold til de tidligere år har vi spurgt om, i hvilken grad borgeren er opmærksom på trusler mod sine personlige informationer på nettet fx data, billeder, identitetsoplysninger, adgang til sociale medier mv.

79 procent af danskerne i alderen 18-74 år har en profil på et socialt medie, svarende til knap 2,5 millioner. Af disse er 49 procent ekstremt opmærksomme eller meget opmærksomme på problemet. 36 procent er gennemsnitligt opmærksomme, mens 13 procent er lidt opmærksom eller slet ikke opmærksom (se Figur 31).

64 procent oplyser, at de efter egen opfattelse er klædt godt på til at beskytte sig mod truslerne mod personlige informationer på nettet. 34 procent mener ikke, at de er. Det tyder på, at der er behov for at øge læringsindsatsen for at klæde borgerne på til at kunne beskytte sig mod truslerne.

I år har vi desuden spurgt om, i hvilken grad borgeren er opmærksom på trusler mod egen computer, tablet-computer eller smartphone fra nettet (se Figur 32), altså de trusler der kan ramme eget udstyr. Her svarer:

a) Ekstremt opmærksom: 13%
b) Meget opmærksom: 36%
c) Gennemsnitligt opmærksom: 36%
d) Kun lidt opmærksom: 9%
e) Slet ikke opmærksom: 4%
f) Ved ikke: 1%

Borgerne er dog ikke sikre på, at de kan beskytte sig mod cybertrusler. Fire ud af 10 svarer nej til spørgsmålet, om de efter egen opfattelse er godt klædt på til at beskytte sig mod truslerne. På spørgsmålet: ”Er du efter din egen opfattelse godt klædt på til at beskytte dig mod disse trusler?” svarer 61 procent ja og 37 procent nej.

Borgerne er i dog stort omfang bevidste om, at truslerne er der, og at de truer forskellige elementer ved informationssikkerhed. Det kan man se af besvarelserne på spørgsmålet: ”Er du klar over, at dårlig beskyttelse af dine enheder og risikobetonet adfærd på nettet, kan medføre følgende risici?”

Svarene på spørgsmålet fordeler sig således (det er muligt at give flere svar):

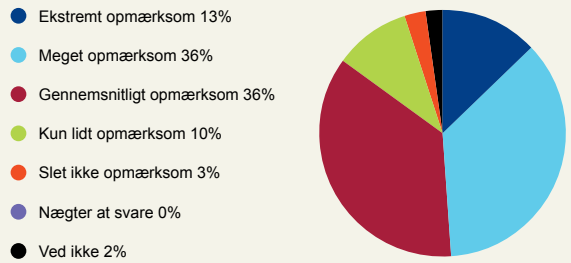
a) 94 procent svarede ja til identitetstyveri.
b) 87 procent svarede ja til tab af adgang til fx sociale medier, mailkonti mv.
c) 90 procent ja til tab af data.
d) 91 procent svarede ja til tab af penge.
e) 74 svarede ja til at deres enheder kan bruges til cyberangreb mod andre.

Tallene viser, at hovedparten af borgerne kender de primære risici, dog ved én ud af fire ikke, at deres enheder kan anvendes i forbindelse med cyberangreb, eksempelvis hvis deres enheder er blevet en del af et botnet.

Figur 31

I hvilken grad er du opmærksom på trusler mod dine personlige informationer på nettet?

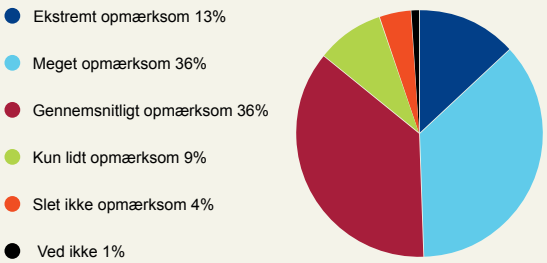
49 procent er ekstremt opmærksom eller meget opmærksom på trusler mod personlige informationer.



Figur 32

I hvilken grad er du opmærksom på trusler mod din computer, tablet-computer eller smartphone?

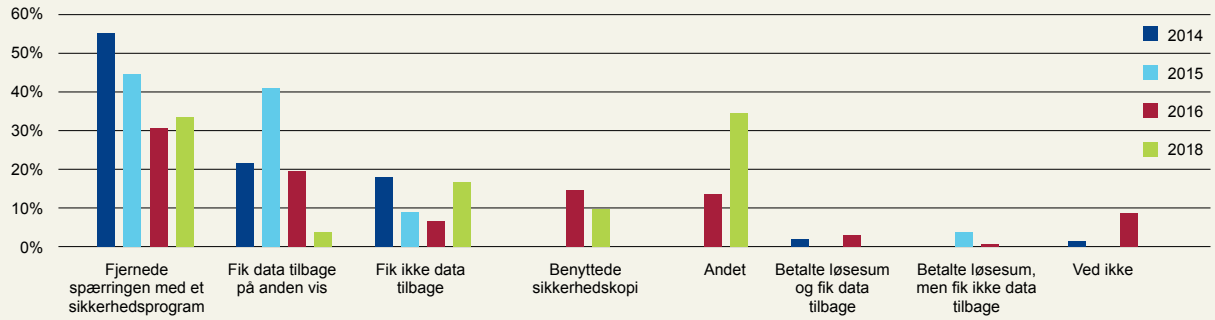
13 procent er kun lidt eller slet ikke opmærksom på trusler mod enheder.



Figur 33

Hvad gjorde du for at få data tilbage?

17 procent fik ikke deres data tilbage efter at have været offer for ransomware.



5.2. Ransomware

Seks procent har været ramt af ransomware på deres pc (se definitionen i afsnit 3.3). Det er en smule lavere end i 2016, hvor ransomware ramte otte procent. 93 procent har ikke været ramt, mens en procent ikke ved det.

17 procent af de seks procent fik ikke data tilbage efter at være blevet ramt af ransomware. Det er mere end en fordobling i forhold til 2016, hvor det tal var godt otte procent. Der er således en relativ stor risiko for, at man ikke ser sine data igen, hvis man bliver ramt af ransomware. Det er ikke mange, men for den enkelte kan det være et alvorligt problem at miste adgang til sine data. En løsning på det er at tage jævnlig backup af data, der kan genskabe systemet. Vi har spurgt om, hvad borgerne har gjort for at få data tilbage (se Figur 33).

a) 34 procent fjernede spærringen med et sikkerhedsprogram og fik data tilbage.
b) Fire procent fik data tilbage på anden vis.
c) 17 procent fik ikke data tilbage.
d) 10 procent benyttede sikkerhedskopi.
e) 35 procent gjorde noget andet.
f) Nul procent betalte løsesum og fik data tilbage.
g) Nul procent betalte løsesum, men fik ikke data tilbage.

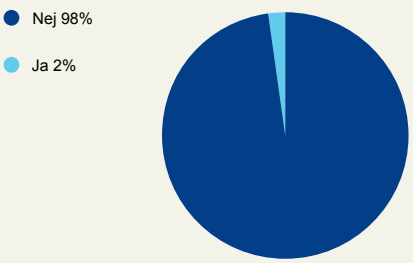
Ransomware på telefon eller tablet-computer er et begrænset problem. Kun to procent kunne svare, at de har oplevet det (se Figur 34).

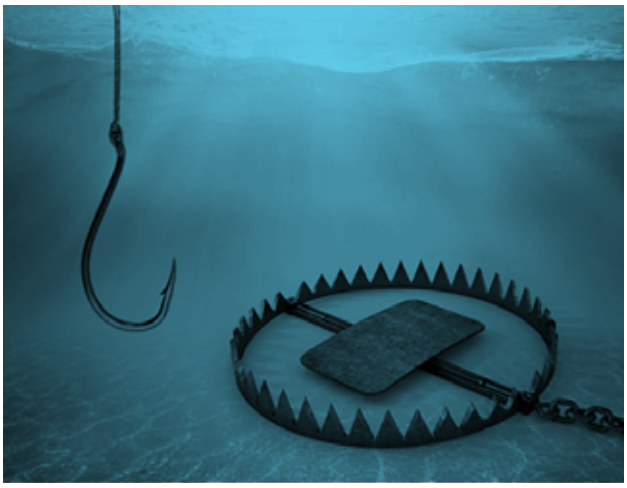
Hele 42 procent af dem fik dog ikke deres data tilbage.

Figur 34

Har du oplevet ransomware på telefon eller tablet?

Det er heldigvis langt hovedparten, der ikke har mødt ransomware på telefon eller tablet-computer.





5.3. Ondsindede beskeder – phishing

51 procent har modtaget e-mails med forsøg på phishing (se definitionen i afsnit 3.5). Det er lidt færre end i 2016, hvor 58 procent modtog en phishingmail (se Figur 35). Der er ligeledes sket et fald, fra 5 til 2 procent, der indsender de ønskede oplysninger.

Hvis man modtager en mail med et link, kan man føre musemarkøren hen over det uden at klikke. Så viser browseren den adresse, et klik på linket vil føre til. Den metode anvender 56 procent af borgerne til at kontrollere links, før de klikker. Samme tal som i rapporten fra 2016.

28 procent har sendt cpr-nummer eller andre personlige oplysninger i e-mail til det offentlige. I 2016 var det 26 procent. Det er usandsynligt, at de har anvendt krypteret e-mail. Det er ganske vist muligt at sende krypteret e-mail ved hjælp af NemID, men det er kompliceret at sætte op. Hvis data sendes ukrypteret, er der risiko for, at uvedkommende får fat i dem. Risikoen er størst, hvis mailen ydermere er sendt over et usikkert netværk, fx et trådløst netværk uden kryptering.

To procent svarer, at de har taget et foto af deres NemID og sendt det til andre.

5.4. Nethandel

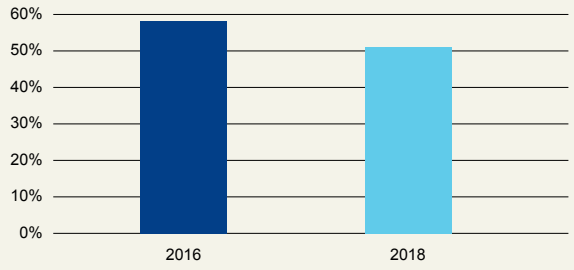
I denne undersøgelse har vi spurgt til nethandel. 85 procent kan berette, at de foretager køb via internettet (se Figur 36).

Af dem kan 68 procent oplyse, at de forsøger at sikre sig mod fup-butikker. 31 procent gør det ikke, mens en procent ikke ved det. Metoderne til beskyttelse fordeler sig således (se Figur 37).

Figur 35

Har du modtaget phishing-mail?

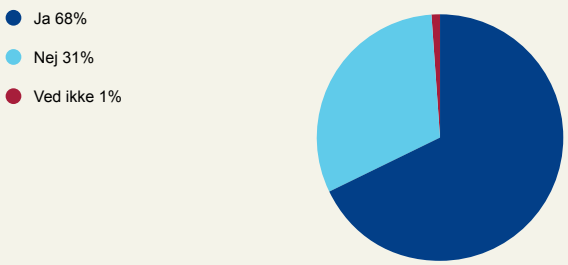
Der er sket en nedgang i antallet af modtagede phishing-mail. Der foreligger ikke data på det spørgsmål tidligere end 2016.



Figur 36

Gør du noget for at sikre dig mod fupbutikker?

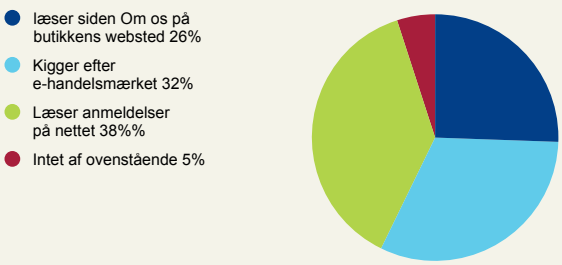
68 procent oplyser, at de forsøger at sikre sig mod fup-butikker. Vi har ikke tidligere stillet spørgsmål om borgernes anvendelse af e-handel.



Figur 37

Hvad gør du for at sikre dig mod fup-butikker?

Af de danskere, der sikrer sig mod fupbutikker, læser de fleste anmeldelser på nettet.



5.5. Hjælp til børn

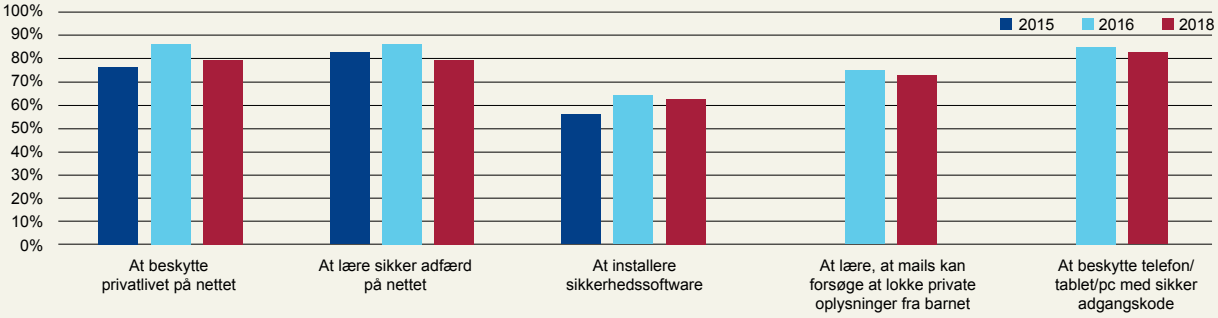
Et flertal af de borgere, dog med et lille fald i forhold til 2016, der har børn i alderen 5-16 år, hjælper deres børn med at få bedre informationssikkerhed (se Figur 38). Det er muligt at afgive flere svar:

a) 80 procent hjælper barnet med at beskytte dets privatliv på nettet (fx ved ikke at lægge private billeder ud offentligt).
b) 80 procent hjælper barnet med at lære sikker adfærd på nettet (fx ved ikke at indgå aftaler med fremmede uden at spørge forælderen først).
c) 63 procent hjælper barnet med at installere sikkerhedssoftware (fx antivirus).
d) 74 procent hjælper barnet med at lære, at nogle mails forsøger at lokke private oplysninger ud af barnet.
e) 83 procent hjælper barnet med at beskytte telefon, tablet eller pc med en sikker adgangskode.

Figur 38

Hjælper du dit barn med....

De fleste forældre oplyser, at de hjælper deres børn med informationssikkerhed.



5.6. Beskyttelse af enheder

Næsten tre ud af fire beskytter computeren med en adgangskode (se Figur 39).

59 procent beskytter deres pc med sikkerhedsprogrammer såsom antivirus og firewall. I 2016 var det 66 procent. 25 procent oplyser, at de ikke beskytter computeren og 16 procent ved det ikke. Beskyttelsen med sikkerhedsprogrammer såsom antivirus og firewall er således gået ned i forhold til 2016. (se Figur 40).

29 procent af brugerne af sikkerhedsprogrammer anvender den software, som fulgte med, da de købte computeren. 37 procent har selv købt sikkerhedssoftware, mens 29 procent bruger gratis programmer. Seks procent ved det ikke (se Figur 41). Der er således sket en stigning i andelen, der anvender det sikkerhedsprogram, der fulgte med pc'en.

88 procent beskytter deres telefon eller tablet-computer med en kode, fingeraftryk eller lignende.

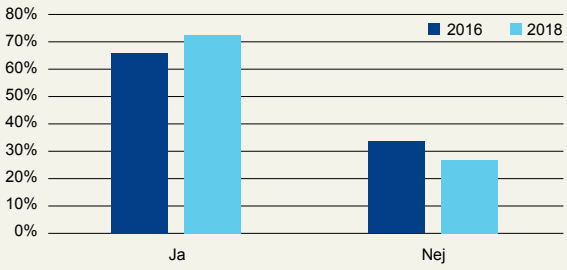
32 procent beskytter deres smartphone og/eller tablet-computer med sikkerhedsprogrammer såsom antivirus. I 2016 var det 26 procent.

40 procent oplyser, at de ikke beskytter enheden og data på den. I 2016 var det 53 procent. I 2013 og 2014 var det 32 og 34 procent. 19 procent ved ikke, om de har sikkerhedssoftware på enheden.

Figur 39

Anvendes adgangskode til computeren?

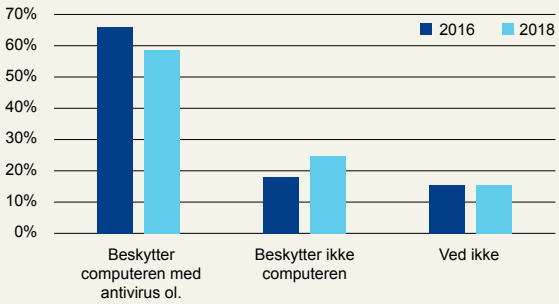
Cirka en fjerdedel anvender ikke adgangskode til computeren.



Figur 40

Hvordan beskytter du din private computer og data?

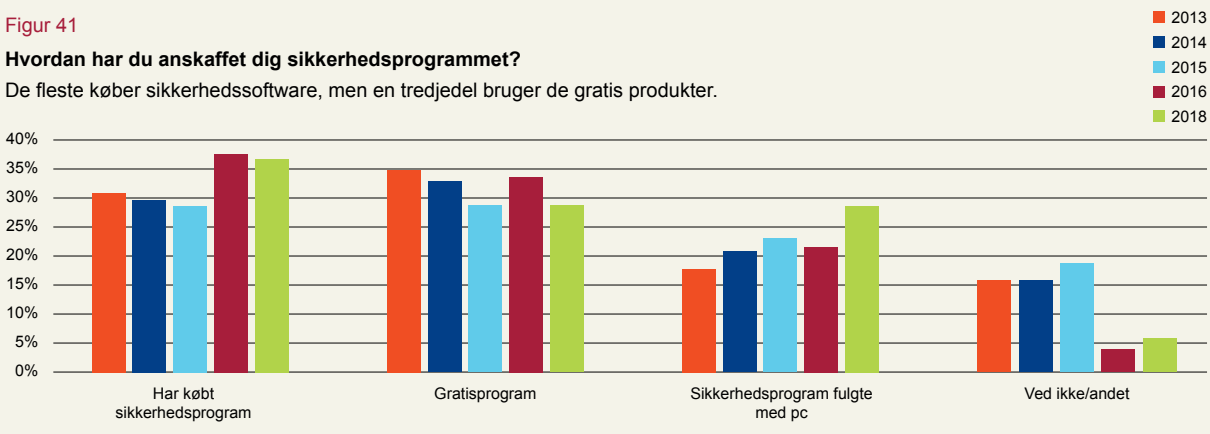
Beskyttelsen med sikkerhedsprogrammer såsom antivirus og firewall er gået ned i forhold til 2016.



Figur 41

Hvordan har du anskaffet dig sikkerhedsprogrammet?

De fleste køber sikkerhedssoftware, men en tredjedel bruger de gratis produkter.



Sikkerhedssoftware til smartphone/tablet-computer er fordelt med 14 procent gratis software, 32 procent købeprogrammer og 49 procent software, der fulgte med ved køb af enheden.

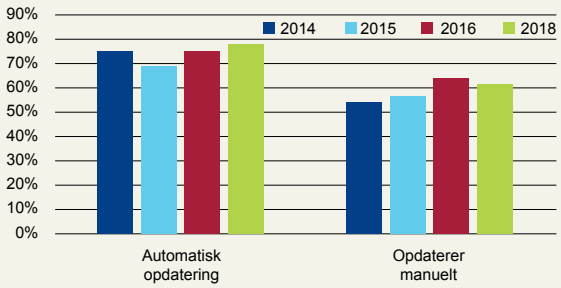
87 procent holder programmer på deres computer opdateret (se omtalen af softwareopdatering i afsnit 3.16). Det er muligt at afgive flere svar.

a) 78 procent har slået automatisk opdatering til.
b) 62 procent opdaterer nogle programmer manuelt.

Tallene ligger nogenlunde på niveau med tidligere år (se Figur 42).

Figur 42

Hvordan holder du software på pc opdateret?
Knap 80 procent bruger automatisk opdatering.



5.7. Trådløse netværk

94 procent oplyser, at de har trådløst netværk i hjemmet.

Af disse skal 94 procent af brugerne af trådløst netværk i hjemmet skal indtaste en adgangskode for at få adgang til netværket (se omtalen af trådløse netværk i afsnit 3.10). Der har været en stigende andel af sikrede trådløse net i de undersøgelser, vi har stillet spørgsmålet. (se Figur 43).

54 procent af borgerne, der bruger adgangskode, har selv lavet adgangskoden til nettet, mens 46 procent anvender den kode, der var indkodet, da de fik udstyret.

Det kan være et sikkerhedsproblem, hvis systemet er leveret med en usikker standardkode. Mange internetudbydere leverer dog i dag deres routere med koder, der er forskellige for hver kunde.

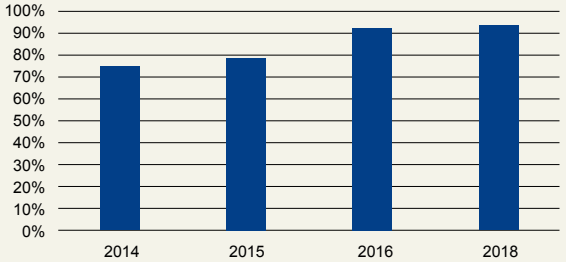
68 procent anvender trådløse netværk uden for hjemmet. Ud af dem anvender 49 procent netværk, der ikke kræver en adgangskode og dermed er ukrypterede og usikre (se Figur 44).

61 procent af dem bruger trådløse netværk, hvor alle bruger den samme adgangskode fx på en café. Tallene har næsten ikke ændret sig siden sidste rapport.

I 2016 anvendte 25 procent VPN (se definitionen i afsnit 3.9), når de brugte trådløse netværk uden for hjemmet. Det antal er faldet til 13 procent i 2018. 64 procent anvender ikke VPN og godt 24 procent ved det ikke. Årsagen til forskellen kan ikke aflæses ud af svarene på spørgsmålet. Der kan skyldes uklarhed om, hvad VPN er.

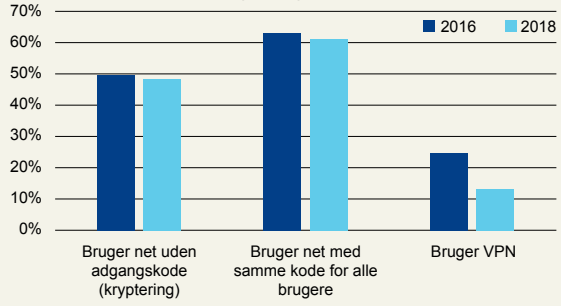
Figur 43

Trådløs net med adgandskode i hjemmet
Næsten alle anvender sikre trådløse netværk i hjemmet.



Figur 44

Brugere af trådløse net uden for hjemmet
13 procent bruger af trådløse netværk uden for hjemmet anvender et VPN (virtuelt privat netværk) til at sikre kommunikationen. I 2016 var tallet på 25 procent.



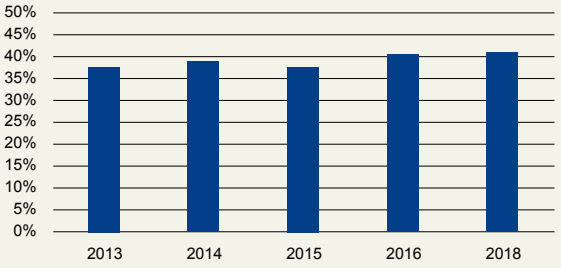
5.8. Sikkerhedskopiering

41 procent tager jævnligt sikkerhedskopi af data på deres computer. Det er næsten identisk med 2016 (se Figur 45).

Figur 45

Tager sikkerhedskopi af data på pc

Fire ud af ti borgere tager jævnligt sikkerhedskopi af deres data i 2018.



De borgere, der tager sikkerhedskopi af pc, anvender disse metoder (se Figur 46).

a) 66 procent tager backup på nettet (cloud).
b) Fire procent brænder data på cd/dvd.
c) 68 procent tager kopi til ekstern harddisk/USB-nøgle.
d) 15 procent svarer "Andet".

Den største udvikling er på cloud-siden, hvor andelen er forøget. Ligeledes ser det ud til at cd/dvd og harddisk/USB-nøgler er på retur. Tallene giver sammenlagt mere end 100 procent, fordi nogle brugere kombinerer flere backup-metoder.

I 2016 tog 30 procent sikkerhedskopi af data på deres smartphone eller tablet. Det tal er steget til 41 procent i år. 58 procent tager stadig ikke kopier af telefon eller tablet-computer.

De, der tager backup, anvender disse metoder. Flere svar er muligt (se Figur 47).

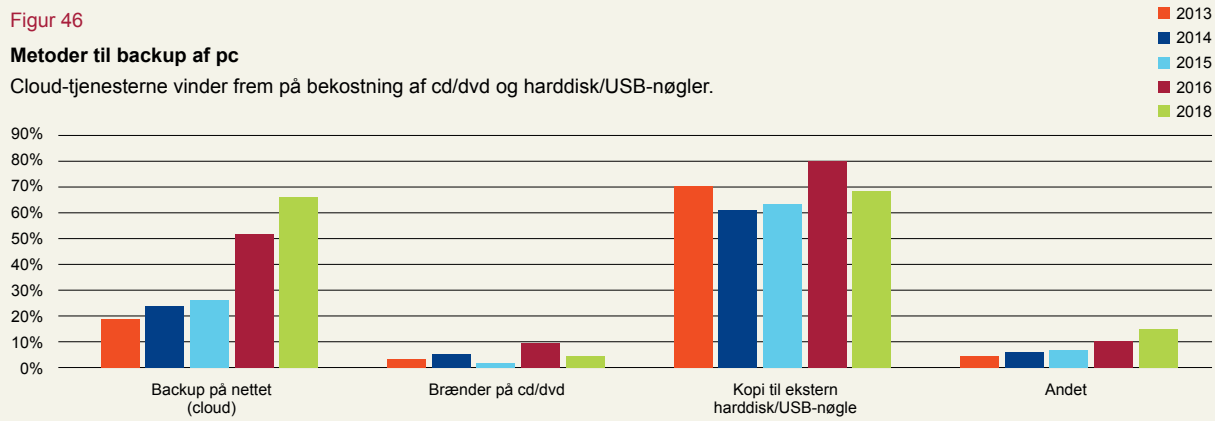
a) 82 procent tager backup på nettet (cloud)
b) 38 procent tager kopi til en computer
c) 27 procent tager kopi til ekstern harddisk/USB-nøgle
d) Tre procent brænder data på cd/dvd
e) Ni procent svarer "Andet".

Igen er der en tendens i retning af cloud-baseret lagring af data.

Figur 46

Metoder til backup af pc

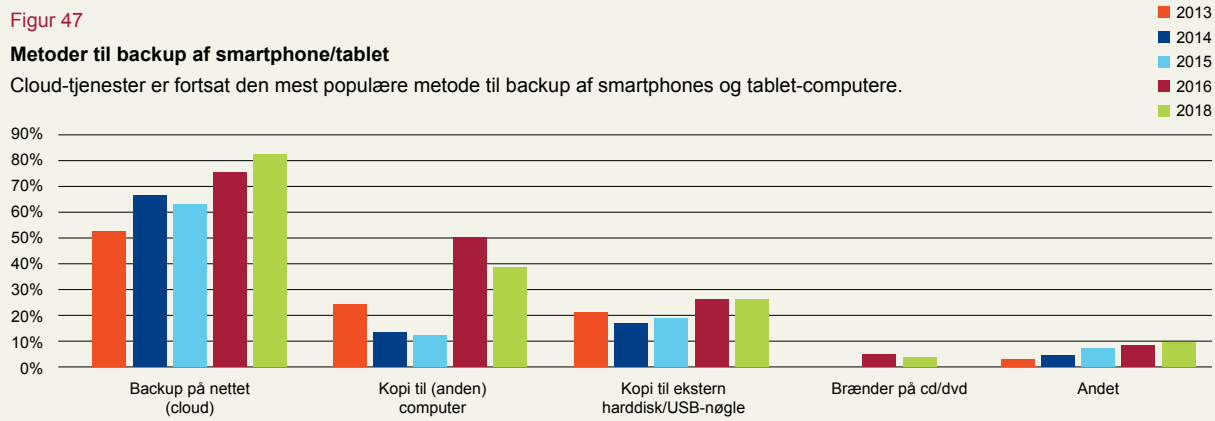
Cloud-tjenesterne vinder frem på bekostning af cd/dvd og harddisk/USB-nøgler.



Figur 47

Metoder til backup af smartphone/tablet

Cloud-tjenester er fortsat den mest populære metode til backup af smartphones og tablet-computere.



5.9. Sociale medier

79 procent har en profil på et eller flere sociale medier såsom Facebook, LinkedIn, Twitter, Instagram og lignende.

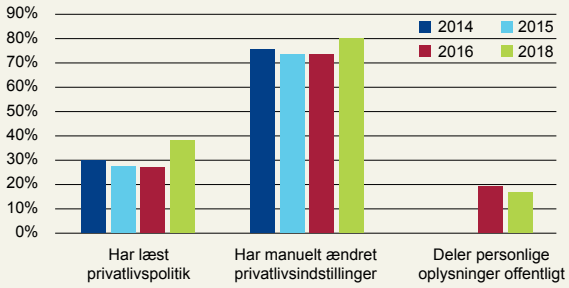
38 procent af dem, der har en profil, har læst privatlivspolitikken for det sociale medie. I 2016 var tallet på 27 procent. Fremgangen kan skyldes det øgede fokus i medierne, eksempelvis i forbindelse med indførelsen af GDPR, der trådte i kraft tidligere i år. Otte ud af ti har manuelt indstillet privatlivsindstillingerne. Denne andel er ligeledes steget i forhold til tidligere år (se Figur 48).

17 procent deler personlige oplysninger på den åbne del af mediet – for eksempel ved at gøre opslag offentligt tilgængelige. Det er et lille fald fra sidste rapport. 82 procent gør det ikke.

Figur 48

Brugere af sociale medier

Flere læser privatlivspolitikken, og 80 procent ændrer aktivt privatlivsindstillingerne på sociale medier.



5.10. Passwordsikkerhed

37 procent (se Figur 49) anvender samme adgangskode til flere online-tjenester. 24 procent svarer dog, at det kun er til tjenester, der ikke håndterer følsomme data.

I sidste rapport anvendte 66 procent samme password til flere tjenester, der er altså sket et markant fald, hvilket er positivt (se omtalen af passwords i afsnit 3.11). 75 procent har en adgangskode på mellem seks og ti tegn. 18 procent har over 11 tegn, mens kun fire procent anvender mellem et og fem tegn (se Figur 50). Vi har ændret svarmuligheden i forhold til 2016, fordi anbefalingerne til et godt password er ændret.

41 procent lader deres browser lagre passwords (se definitionen i afsnit 3.13). 57 procent af dem oplyser, at disse passwords er beskyttet med en adgangskode, der skal indtastes, før man får adgang til dem. I 2016 var tallene henholdsvis 45 og 48 procent.

Ti procent bruger en password manager (se definitionen i afsnit 3.13) til at opbevare og holde styr på passwords. 80 procent af dem bruger et program, hvor data lagres krypteret og beskyttes med adgangskode. 61 procent har en metode til at huske sikre passwords med. I 2016 var det tal på 47 procent.

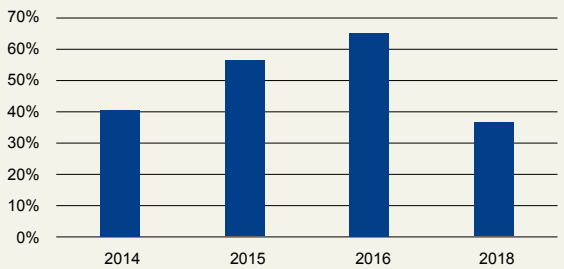
Nogle tjenester er sikret med password, men tilbyder også supplerende sikkerhed i form af to-faktorbekræftelse. Det sker i form af engangskoder, man får tilsendt via sms eller fra en app. Derfor har vi for første gang spurgt borgerne, om de anvender den type sikkerhedsfunktion til en eller flere tjenester (her ses bort fra login med NemID-nøglekort). 52 procent anvender denne to-faktor sikkerhed, 45 procent gør ikke.To-faktor sikkerhed anvendes følgende steder (det er muligt for respondenten at svare i flere kategorier):

a) Sociale medier: 34 procent.
b) E-mail-tjenester: 47 procent.
c) Datalagring i cloud: 28 procent.
d) E-handelsplatforme: 61 procent.

Figur 49

Benytter samme password til flere online-tjenester

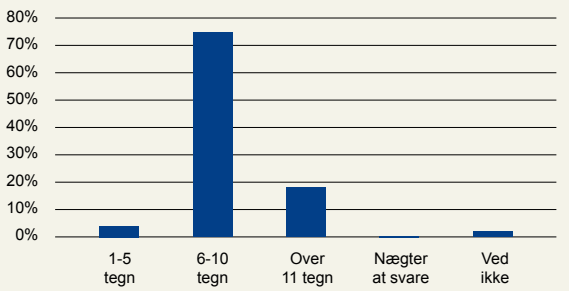
Genbrugen af adgangskoder til online-tjenester er faldet.



Figur 50

Hvor langt er dit password?

Tre ud af fire danskere bruger en adgangskode på mellem seks og 10 tegn.



5.11. Indsamling af viden om informationssikkerhed

Denne gang har vi spurgt brugerne, hvor de finder frem til deres viden om informationssikkerhed. Det er interessant i forbindelse med oplysning eller kampagner, der skal højne borgernes viden om området. Det er muligt at give flere svar:

a) Nyhedsmedier: 72 procent.
b) Sociale medier: 38 procent.
c) Forbrugerrådet Tænks app Mit digitale selvforsvar: Syv procent.
d) Nyhedsbreve: 14 procent
e) Venner og bekendte: 52 procent.
f) Offentlige websider: 21 procent
g) Arbejdsplads/uddannelsesinstitution: 28 procent.

Når det handler om mediet, der foretrækkes til formidling af informationssikkerhed, fordeler svarene sig således. Flere svar er muligt:

a) Tekst: 73 procent.
b) Video: 27 procent.
c) Video med grafik: 20 procent.
d) Test/quiz: fem procent.
e) Spil: tre procent.
f) Reklamespots i fjernsynet: syv procent.
g) Sociale medier: 21 procent.

Hvis en borger søger vejledning om at få højere informationssikkerhed, så søges efter følgende områder. Flere svar er muligt:

a) Vejledning i at beskytte data: 55 procent.
b) Vejledning i at agere sikkert på nettet: 32 procent.
c) Vejledning i at beskytte enheder (computere, smartphones eller tablet-computere): 52 procent.

Disse tal viser, at beskyttelse af data og enheder står højt på dagsordenen hos borgerne.

5.12. Tillid til offentlige digitale tjenester

86 procent bruger offentlige digitale tjenester som fx Skat TastSelv, løsninger til at melde flytning eller opskrivning til børnepasning. Af dem har 86 procent tillid til, at myndighederne håndterer deres personlige oplysninger med den nødvendige fortrolighed og sikkerhed. Graden af tillid fordeler sig således (se Figur 51).

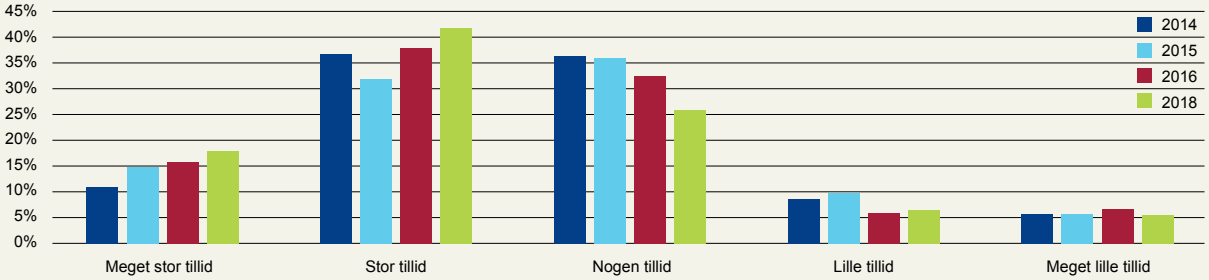
a) 18 procent har meget stor tillid.
b) 42 procent har stor tillid.
c) 26 procent har nogen tillid.
d) Seks procent har lille tillid.
e) Seks procent har meget lille tillid.

Andelene viser, at der er en stigende tendens til højere tillid.

Figur 51

Tillid til offentlige digitale tjenester

Flere borgere har tillid til, at det offentlige håndterer personlige oplysninger sikkert og fortroligt.



5.13. Delkonklusion om borgernes informationssikkerhed

5.14. Trusler

Virus og skadelige programmer er den hyppigste trussel, borgerne er udsat for. 34 procent oplyser, at de har haft infektioner med skadelig software. Det er en lille stigning i forhold til 2016 og faktisk helt tilbage fra 2013, hvor tallet har ligget nogenlunde stabilt. Dog er der samlet set en stor stigning i andelen af borgere, der bliver ramt af mindst en af fire sikkerhedstrusler.

Nettrusler har printet sig ind i borgernes bevidsthed, hvilket sandsynligvis skyldes det meget mediemæssige fokus, der har været på området. 37 procent af borgerne mener ikke, at de er godt klædt på til at beskytte sig mod cybertrusler. Næsten lige så mange (34 procent) føler sig ikke godt nok klædt på til at beskytte sig mod trusler mod personlige oplysninger. Dette er et nyt tal i forhold til tidligere år, og vi har således ikke haft mulighed for at se en udvikling. Men der er ingen tvivl om, at det er et fokusområde hos borgerne – og det vil næppe falde i de kommende år. Der er således en stor gruppe, der kan få gavn af saglig information, råd og vejledning om sikker adfærd på nettet.

I vores undersøgelse er det fem procent, svarende til knap 143.000 danskere, der har fået misbrugt personoplysninger. Men risikoen for misbrug kan være større, da hele 28 procent af danskerne har sendt cpr-nummer eller andre personlige oplysninger i en e-mail til det offentlige. Otte procent, godt 212.000 danskere, har mistet penge ved online-svindel eller afpresning. Seks procent har været ramt af ransomware, hvilket er lidt mindre end i 2016.

17 procent (svarende til 461.000) har desuden mistet data som følge af et it-sikkerhedsproblem (fx et computernedbrud) hos dem selv eller hos en tjeneste på nettet. En markant stigning i forhold til 2016, hvor det var ni procent. I de tidligere undersøgelser har vi ikke stillet spørgsmålet. En del af tallet kan dække over tab som følge af manglende sikkerhedskopiering, et område, hvor der er god plads til forbedring. Kun 41 procent af borgerne tager jævnligt sikkerhedskopi af data på deres computer, svarende til knap 1.150.000 Det betyder, at omkring 60 procent (1.610.000) i alderen 18-74 år udsætter sig selv for risikoen for ransomwareangreb. Det er et tal, der stort set ikke har ændret sig i de år, vi har gennemført undersøgelserne.

Fire ud af ti anvender samme adgangskode til flere online-tjenester. 24 procent svarer dog, at det kun er til tjenester, der ikke håndterer følsomme data. I sidste rapport anvendte 66 procent samme password til flere tjenester, der er altså heldigvis sket et markant fald. Anbefalingen er, at man ikke bruger det samme password til flere tjenester.

Halvdelen af dem, der bruger trådløse netværk uden for hjemmet, bruger usikre netværk. Dog beskytter 13 procent sig med VPN (virtuelt privat netværk). I 2016 var det en ud af fire. Forskellen i tallene kan skyldes, at der næppe i den brede befolkning er bevidsthed om, hvad VPN i det hele taget er. Det samlede prioriterede trusselsbillede for borgerne ser således ud:

1. Skadelig software inficerer computere.
2. Borgerne mister data som følge af et it-sikkerhedsproblem/manglende backup.
3. Uvedkommende får adgang til fortrolige data ved at udnytte usikre trådløse netværk.
4. Borgerne genbruger passwords til flere tjenester, hvilket giver risiko for uvedkommende adgang til systemer og data.

5.15. Konsekvenser

Næsten alle de borgere, der oplevede sikkerhedsproblemer, ændrede adfærd.

Ni ud af ti er holdt op med at åbne mails, der kommer fra ukendte, efter at de var udsat for et sikkerhedsproblem. Dermed er det den hyppigste handling som konsekvens af sikkerhedsproblemer. Næstmest hyppigt er at installere eller opgradere sikkerhedssoftware, det gjorde 83 procent. Syv ud af ti undlod at dele oplysninger om sig selv på sociale medier og samme antal holder sig væk fra bestemte websteder. Tallene minder om 2016-resultatet.

5.16. Foranstaltninger - adfærd

5.16.1. Beskyttelse af enheder

Tre ud af fire beskytter computeren med en adgangskode. 88 procent beskytter deres telefon eller tablet-computer med en kode, fingeraftryk eller lignende. En tredjedel beskytter deres smartphone og/eller tablet-computer med sikkerhedsprogrammer såsom antivirus. I 2016 var det 26 procent. Der er altså tale om en pæn stigning.

Seks ud af ti beskytter deres pc med sikkerhedsprogrammer såsom antivirus og firewall. I 2016 var det 66 procent. Hver fjerde oplyser, at de ikke beskytter computeren og 16 procent ved det ikke. 87 procent holder programmerne på computeren opdateret, hvilket er glædeligt, da det er en af de vigtigste sikkerhedsregler. Dette tal er en smule højere end i 2016, hvor tallet var på 82 procent. Knap 80 slår automatisk opdatering til, hvilket er en lille stigning i forhold til tidligere.

5.16.2. Forsvar mod svindel

Halvdelen har modtaget e-mails med forsøg på phishing, men kun to procent af dem indsendte de ønskede oplysninger. Et lavt antal, men stadig et område, der skal holdes øje med. Phishing kommer i bølger og har været et permanent problem gennem flere år.

Syv ud af ti af dem, der har handlet på nettet, oplyser, at de forsøger at sikre sig mod fup-butikker. Anmeldelser på nettet er den primære kilde til information. Det er en god metode til at komme fup til livs.

5.16.3. Brug af passwords

37 procent anvender samme adgangskode til flere online-tjenester, hvilket kan give adgang til flere konti, hvis adgangskoden udnyttes af tredjepart.

Borgerne har desuden for korte adgangskoder. Tre ud af fire har en adgangskode på mellem seks og 10 tegn, 18 procent har over 11 tegn, mens fire procent anvender mellem et og fem tegn. Anbefalingen er, at lange passwords – mindst 12 karakterer - betyder bedre sikkerhed. Det betyder mindre om de indeholder specialtegn, store bogstaver ol. Borgerne har metoder til at huske adgangskoder, men anvender næsten ikke password manager-programmer (ti procent). Til gengæld er de rimelig flittige med to-faktorsikkerheden. Halvdelen oplyser, at de anvender to-trinsbekræftelse. En række tjenester anvender dog kun to-trinsbekræftelse til visse typer af transaktioner. I de tilfælde er et langt og unikt password stadig nødvendigt for at beskytte adgang til data.

5.16.4. Brug af trådløse netværk

94 procent beskytter deres trådløse netværk i hjemmet med kryptering. Tallet er steget løbende gennem de fire år, vi har spurgt til emnet; det var tre ud af fire i 2014. Halvdelen af borgerne har selv lavet adgangskoden til nettet, mens 46 procent anvender den kode, der var indkodet, da de fik udstyret. Det kan være et sikkerhedsproblem, hvis systemet er leveret med en usikker standardkode. Mange internetudbydere leverer dog i dag deres routere med koder, der er forskellige for hver kunde.

5.16.5. Sikkerhedskopiering

Sikkerhedskopiering har været en udfordring i alle de år, vi har gennemført undersøgelsen. I år var der en forbedring på et enkelt procentpoint, idet 41 procent jævnligt tager backup af data på deres pc. Men seks ud af ti danskere må forvente at miste data, hvis deres pc går i stykker eller bliver overtaget af ransomware. Cloud-tjenesterne bliver i stigende grad anvendt til sikkerhedskopiering. Det skyldes sandsynligvis, at borgerne har opdaget, at det er en enkelt metode at sikre løbende backup. Alternativt – fx backup på anden pc, usb-stick eller cd/rom – kræver en systematisk og en disciplineret indsats.

5.16.6. Sikkerhedskultur

De fleste borgere hjælper deres børn med at lære om informationssikkerhed, og hvordan de beskytter sig mod trusler. Men i takt med, at der kommer flere og flere digitale enheder ind i familien, kan det være en kompleks opgave at følge med.

Et punkt er dog steget markant. 38 procent af brugerne har i dag læst privatlivspolitikken for det sociale medie. I 2016 var tallet på 27 procent. Ligeledes har 80 procent manuelt indstillet privatlivsindstillingerne. Debatten om sikkerhed på sociale medier kan være en medvirkende årsag.

Borgerne har høj tillid til offentlige digitale tjenester, der er blevet dagligdag for næsten alle danskere.

6.
Perspektivering

6. Perspektivering

Dette afsnit sammenligner undersøgelsens resultater med data fra andre danske og internationale sikkerhedsundersøgelser.

6.1. Skadelig software

Danskerne er langt mere udsatte for skadelig software i hjemmet end på arbejdspladsen. Blandt offentligt ansatte har én ud af ti været ude for et virusangreb, hvor andelen er mere end tre ud af ti for borgerne. I vores undersøgelse mangler 25 procent af de private borgere, svarende til knap 700.000, at sikre computeren med sikkerhedssoftware.

I Microsofts løbende analyser på området kan man se, at 91,7 procent af computerne i landet var beskyttet med antivirus i 2017. Det er et lille fald i forhold til 2016, hvor 92,3 procent var beskyttet[2]. De to grundregler for digital sikkerhed er at benytte sikkerhedssoftware og at opdatere sine programmer med de nyeste rettelser fra producenterne. Microsofts opgørelser viser dog, at andelen er stigende over tid. For tre år siden var Microsofts tal på 79,8 procent. Anbefalingen er, at alle installerer sikkerhedssoftware på systemerne.

6.2. Phishing

Ifølge vores undersøgelse er danskerne generelt gode til at genkende og undgå phishing-svindel. To-faktorsikkerhed i form af NemID og ikke mindst den nye NemID-app, der til dels sender nøglekortet på pension, giver høj sikkerhed. Tal fra FinansDanmark viser, at en del danskere falder for svindelnumrene fra it-kriminelle[3]. I 2017 registrerede FinansDanmark 792 forsøg på phishing. 341 af forsøgene lykkedes og medførte økonomisk tab. Det samlede tab på grund af phishing beløb sig i 2017 til 5.694.756 kroner. Tabet på netbankindbrud er til sammenligning på 5.283.861 kroner. (Se Figur 52). Phishing står således for en større andel af tabene end digitale bankrøverier.

[2] Microsoft Security Intelligence Report Volume 23, Denmark, https://www.microsoft.com/sir

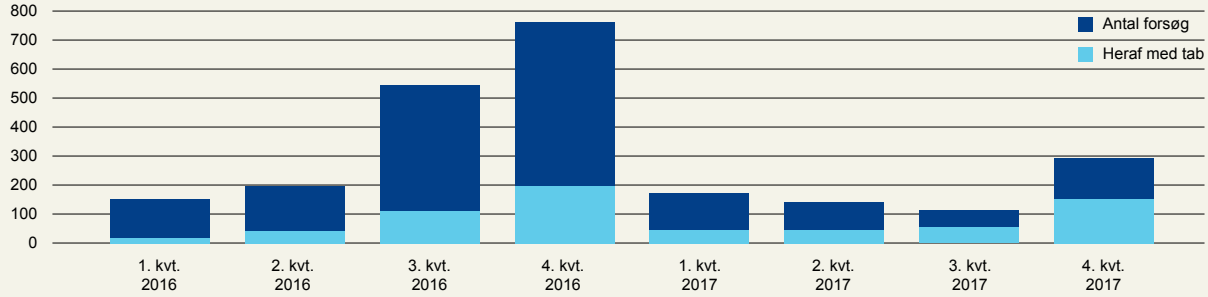
[3] Finans Danmark: Netbankindbrud og phishing, http://finansdanmark.dk/toerre-tal/institutter-filialer-ansatte/kriminalitet/netbankindbrud-og-phishing/

Figur 52

Social engineering/phishing

Antal phishing-forsøg samt heraf med tab. Registreringen startede i 2016, derfor er der ikke tal før dette år.

Kilde: FinansDanmark.



6.3. Sikkerhed på mobile enheder

Sikkerheden på de mobile platforme er ikke så prioriteret som på computeren, men dog stigende. Blandt de offentligt ansatte har 70 procent sikkerhedsprogrammer på den smartphone eller tablet-computer, de bruger på jobbet. I undersøgelsen fra 2016 var andelen af mobile enheder med sikkerhedssoftware på 56 procent. I befolkningen er tallet noget lavere, men tendensen den samme. 32 procent beskytter deres smartphone og/eller tablet-computer med sikkerhedsprogrammer såsom antivirus. I 2016 var det 26 procent. Anbefalingen er, at man anvender antivirus på alle mobile enheder.

Mængden af skadelig software rettet mod mobile enheder har været stigende de senere år. Men vi har ikke set en tilsvarende stor mængde infektioner af smartphones og tablet-computere. Otte procent af borgerne oplyser, at deres smartphone eller tablet-computer har været inficeret med virus eller skadelige programmer. I 2016 var tallet på seks procent.

De lave tal kan være tegn på, at danskerne primært henter apps fra de officielle app stores og ikke fra alternative kilder, hvor der er større risiko for infektioner. To procent af de offentligt ansatte oplyser, at de har hentet en skadelig app. Den lave grad af infektion kan også forklare, hvorfor færre installerer antivirus på deres mobile enheder i forhold til computerne. Sikkerhedssoftware til mobile enheder hentes via de officielle app-tjenester. Der findes både betalingsversioner og gratis programmer. På websiden AV-Comparatives.org kan du finde uafhængige test af sikkerhedssoftware til både mobile enheder og pc'er.

6.4. Ransomware

De senere år er en ny type skadelig software dukket op: Ransomware. Vores tidligere undersøgelser har vist, at denne angrebsform i gennemsnit rammer 7-8 procent af borgerne. I denne undersøgelse er tallet på seks procent. Ransomware ser ud til at være lidt på retur, også ifølge sikkerhedsfirmaet McAfee. Firmaet oplyser, at ransomware-angreb faldt 32 procent fra fjerde kvartal 2017 til første kvartal 2018, mens andre sikkerhedsproblemer som 'cryptocoin mining' steg med 1.189 procent i årets første kvartal[4].

Europol regner dog ransomware blandt de vigtigste trusler[5]. Også Center for Cybersikkerhed melder om et ikke uvæsentligt antal angreb mod både private, virksomheder og myndigheder[6].

6.5. Sikkerhedskopiering

55 procent af de offentligt ansatte oplyser, at der bliver taget sikkerhedskopi af de data, de bruger på jobbet. 31 procent svarer nej til spørgsmålet. Dette høje tal kan enten skyldes manglende backup i organisationen eller brugerens manglende viden om, at it-afdelingen faktisk tager backup, der ofte foregår automatisk. Otte procent har mistet data som følge af manglende backup og to procent har mistet data som følge af angreb. Center for Cybersikkerheds vejledning om at reducere risikoen for ransomware betegner systematisk sikkerhedskopiering af alle kritiske informationer som absolut påkrævet. Ligeledes kan en sikkerhedskopi genskabe data ved nedbrud ol.

6.6. Sikkerhedspolitik

Kun 57 procent af de offentligt ansatte har sat sig ind i sikkerhedspolitikken på deres arbejdsplads, hvilket dog er en stigning fra 2016, hvor tallet var 49 pct. Otte procent af de offentligt ansatte undlader indimellem at overholde reglerne. Af denne gruppe omgår 15 procent reglerne dagligt og 18 procent mindst en gang om ugen og tendensen har været stigende, hvilket bør tænde en advarselslampe hos ledelserne i offentlige myndigheder.

6.7. Sikkerhed er ledelsens ansvar

Informationssikkerhed er ledelsens ansvar. Derfor har ledelsen ansvaret for, at de nødvendige værktøjer stilles til rådighed. Ledelsen har også ansvaret for, at medarbejderne kender sikkerhedspolitikken og bør derfor sætte ind for at oplyse de ansatte om både politikken og de mere konkrete retningslinjer, som en organisation har til håndtering af data og informationer. Op mod en tredjedel er ikke oplyst om politikken. Ligeledes skal organisationens procedurer og forretningsgange indrettes på en måde, så informationssikkerheden indgår. Sikkerhedspolitikker og retningslinjer bør udformes således, at medarbejderne ikke føler, det er nødvendigt at bryde dem for at kunne udføre deres job.

[4] McAfee details rise in blockchain threats, cryptocurrency attacks, https://searchsecurity.techtarget.com/news/252443993/McAfee-details-rise-in-blockchain-threats-cryptocurrency-attacks

[5] Europol: 2017 Internet Organised Crime Threat Assessment, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

[6] Center for Cybersikkerhed: Reducér risikoen for ransomware, maj 2016, https://feddis.dk/cfcs/nyheder/arkiv/2016/Pages/ransomware.aspx

7.
Samlede konklusioner

7. Samlede konklusioner

Ud fra undersøgelsens resultater konkluderer DKCERT, at der er generelt godt styr på sikkerheden i den offentlige sektor, men flere borgere bliver udsat for sikkerhedshændelser.

Ud fra undersøgelsens resultater konkluderer DKCERT, at den offentlige sektor fortsat har behov for at skabe mere opmærksomhed om sikker adfærd blandt medarbejderne, selvom det relativt lave antal af hændelser tyder på, at der er styr på den basale sikkerhed. Men der er adfærdsmæssige udfordringer blandt medarbejderne med blandt andet:

- genbrug af passwords,
- anvendelse af ukrypteret e-mail til fortrolige oplysninger,
- kendskab og overholdelse af sikkerhedspolitikker,
- anvendelse af usikre trådløse netværk og
- manglende sikkerhedskopiering.

Særligt med anvendelse af e-mail til fortrolige oplysninger bør ledelsen i offentlige institutioner sætte ind med oplysning om organisationens regler på området. At man ikke overholder sikkerhedspolitikker og retningslinjer kan måske ikke mærkes i første omgang, men kan medføre hændelser på længere sigt og skade borgernes tillid til den offentlige sektor.

Bemærkelsesværdigt er det, at markant flere borgere bliver udsat for en sikkerhedshændelse, der truer deres data. Ifølge undersøgelsen har 44 procent af danskerne oplevet mindst et af fire brud på informationssikkerheden: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data.

Nye spørgsmål i 2018 viser, at borgerne generelt er opmærksomme på truslerne, men det afsløres også, at der med fordel kan gøres en indsats for at støtte borgerne i at beskytte sig mod truslerne. Ikke kun fordi så mange flere bliver ramt af hændelser, men også fordi over en tredjedel ikke føler sig godt klædt på til at beskytte sig mod truslerne. Andelen af borgere med tillid til de offentlige, digitale tjenester er intakt i forhold til tidligere, og der er en tendens til, at tilliden øges.

7.1. Trusler

Trusselsniveauet mod borgerne er voksende – dels som følge af et generelt øget trusselsniveau, dels fordi over 44 procent af borgerne i 2018 havde oplevet mindst en af fire trusler mod informationssikkerheden på deres pc. Det svarer til, at over 1,2 millioner danskere har oplevet brud på informationssikkerheden. Det er en stigning fra 34 procent i 2016.

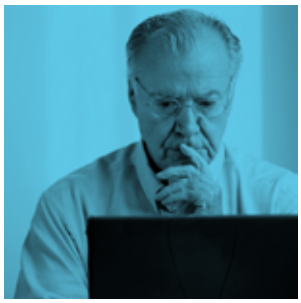
Truslerne har også forplantet sig til telefon eller tablet, hvor 23 procent, svarende til 630.000 borgere, har været berørt af et informationssikkerhedsproblem på en mobil enhed.

Økonomisk tab som følge af trusler er steget siden 2013, og der har været en fordobling fra fire til otte procent. Også datatab på grund af et sikkerhedsproblem hos borgeren eller en tjeneste er næsten fordoblet siden 2016 (fra ni til 17 procent), hvor vi for første gang stillede spørgsmålet. Fem procent har været ude for misbrug af deres personlysninger på nettet. Det er store tal, som dels kan skyldes et øget trusselsniveau, dels en øget opmærksomhed på problemerne.

Over en tredjedel svarer, at de ikke føler sig godt nok klædt på til at beskytte sig, ligesom op mod en fjerdedel af befolkningen ikke er bevidste om, at usikker adfærd på nettet kan medføre, at deres enheder kan blive anvendt til cyberangreb mod andre. Endelig mangler en fjerdedel af borgerne at sikre deres pc med sikkerhedssoftware.

I den offentlige sektor synes der derimod ud fra andelen af offentligt ansatte, der har været inficeret med virus eller skadelig kode, at være godt styr på den basale sikkerhed. (se Figur 1: Sikkerhedsproblemerne ser ret konstante ud mellem 2016 og 2018). Ikke mindst i betragtning af de store mængder skadelige programmer, der cirkulerer.

Men mange sikkerhedshændelser opdages ikke altid, og konsekvenserne af inficerede systemer i en organisation kan være store og dyre. Derfor er det vigtigt fortsat at have fokus på forebyggende tiltag som eksempelvis sikkerhedskopiering, password og god adfærd i forhold til omgang med følsomme oplysninger.



7.2. Konsekvenser

Næsten alle ændrer adfærd, efter at de har været udsat for en sikkerhedshændelse. Det mest almindelige er at undlade at åbne e-mails fra ukendte afsendere, hvilket 90 procent svarer ja til (se Figur 29: Mønstret i handlinger, som følge af sikkerhedsproblemer, ligger ret konstant ift. 2016). Derudover er det også udbredt at installere eller opgradere sikkerhedssoftware (82 procent).

Ligeledes undlader mange (ca 2/3) at besøge bestemte websider og dele oplysninger om sig selv på de sociale medier. Det er fornuftige og sikre handlinger, der ligger stort set på samme niveau som i 2016, men dog markant højere end i 2015. Tallene fra 2018 bekræfter dermed en tendens, vi har set siden 2013. Borgeren ændrer adfærd og tager således en læring med sig, når de har været ude for en sikkerhedshændelse.

7.3. Foranstaltninger - adfærd

7.3.1. Beskyttelse af enheder

Kun 59 procent af borgerne beskytter deres pc med sikkerhedsprogrammer såsom antivirus og firewall. Henover årene er den andel faldet fra over 80 procent i 2013. Der er dermed sket et markant fald i borgernes anvendelse af sikkerhedssoftware. Samme tendens ser vi på de mobile enheder, hvor kun 40 procent af borgerne (i 2016 var det 53 procent) oplyser, at de ikke beskytter deres smartphone og/eller tabletcomputer med sikkerhedsprogrammer såsom antivirus.

Det er bekymrende, fordi ubeskyttede enheder er i stor risiko for at blive ramt af malware. Den relativt lave andel med sikkerhedsprogrammer kan skyldes, at ikke alle er klar over, at deres enhed kan være beskyttet, eksempelvis med et program der fulgte med, da de købte enheden. Til gengæld holder hele 87 procent af borgerne deres software på pc'erne opdateret, de fleste har slået automatisk opdatering til (se figur 42: Knap 80 procent bruger automatisk opdatering).

For den offentlige sektor oplyser ni ud af ti offentligt ansatte, at de har sikkerhedsprogrammer på deres computer, mens 70 procent har sikkerhedsprogrammer på den smartphone eller tablet-computer, de bruger på jobbet. Det er på niveau med 2016.

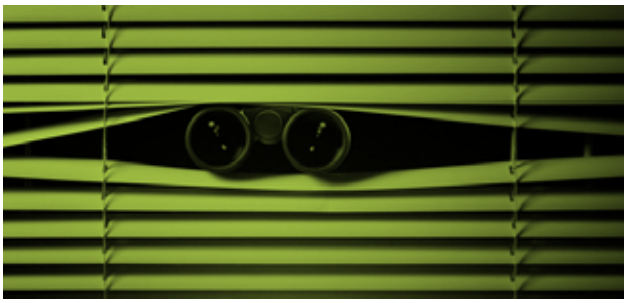
Tre ud af fire borgere beskytter computeren med en adgangskode, hvilket er en stigning fra 2016, hvor tallet var på 66 procent. Ni ud af ti af borgerne beskytter deres telefon eller tablet-computer med en kode, fingeraftryk eller lignende.

83 procent offentligt ansatte låser deres computer, når de forlader den, hvilket er en lille stigning fra 82 procent i 2016.

7.3.2. Forsvar mod svindel

De færreste falder for direktør-, phishing-svindel og andre former for svindelforsøg over nettet (se Figur 35: Der er sket en nedgang i antallet af modtagede phishing-mail). Det gælder både borgere og offentligt ansatte.

Det er glædelige tal, ikke mindst fordi fire procent af de offentligt ansatte svarer, at de har modtaget mails, hvor afsenderen giver sig ud for at være en ledende medarbejder på arbejdspladsen, der beder modtageren om at overføre penge til udlandet. Medierne har haft stor fokus på problemet, og det kan have medvirket til, at emnet er blevet bredere kendt i offentligheden – ligesom ledelserne kan have gået



procedurerne efter i sømmene. Det har medført øget opmærksomhed hos medarbejderne og information til borgerne, hvilket i sig selv har en positiv effekt.

7.3.3. Brug af passwords

Efterhånden som vi bruger mere tid på nettet, ligger vores data hos en lang række tjenester. De er som minimum beskyttet med et brugernavn og en adgangskode. Men hvis en kriminel får fat i brugernavne og passwords til blot en af dem, kan vedkommende let afprøve samme kombination på andre tjenester. Der er i de seneste år set store tyverier af brugernavne og passwords, som sælges i vidt omfang via kriminelle fora på nettet.

Et middel til at begrænse den type angreb er to-trinsbekræftelse, hvor passwordet suppleres med en anden information, typisk i form af en engangskode. Derudover kan man øge sin sikkerhed ved at bruge unikke passwords til alle tjenester.

På arbejdspladser kan en del af problemet med de mange passwords løses med single sign-on-systemer (se Figur 22: En tredjedel af medarbejderne har et single sign-on-system, der styrer adgangen til systemerne.). Det er positivt, at en tredjedel af de offentligt ansatte bruger den type løsning. Her overtager it-funktionen besværet med passwords, så medarbejderne kun skal huske et enkelt.

Fire ud af ti ansatte bruger imidlertid samme adgangskode til flere systemer eller tjenester på arbejdet, hvilket er en stigning fra 33 procent i 2016 (se Figur 19: Mere end hver tredje bruger samme adgangskode til flere systemer/tjenester.).

Godt halvdelen af dem, der bruger samme password til flere systemer, gør det også til systemer, der behandler følsomme data (se Figur 20: 54 procent af dem, der bruger samme password til flere systemer, gør det også til systemer, som behandler følsomme data.). Det svarer til, at over 200.000 offentligt ansatte genbruger passwords til følsomme systemer.

Hos borgerne er der en tendens til et fald i genbrug af passwords. 37 procent anvender samme adgangskode til flere online-tjenester, hvor det i 2016 var 66 procent. Faldet er således markant på genbrug af passwords, men styrken af passwords kan stadig forbedres. 75 procent har en adgangskode på mellem seks og ti tegn. Kun 18 procent har over 11 tegn. Det er for korte passwords i forhold til anbefalingen om lange passwords på mindst 12 tegn og derover.

Der er således et behov for at øge kendskabet til anbefalingen om lange passwords og de offentligt ansattes kendskab til genanvendelse af passwords. Det er en opgave for ledelserne i de offentlige virksomheder.

7.3.4. Brug af trådløse netværk

Omkring halvdelen af de offentligt ansatte (se Figur 14: VPN til kommunikation med arbejdet bruges af halvdelen.) og 13 procent af de borgere, der bruger usikre trådløse netværk, beskytter sig med VPN. I 2016 var antallet af borgere, der anvendte VPN på 25 procent. Det er et markant fald, som kan skyldes, at respondenterne ikke er klar over, hvad VPN er. Tallet fra dette års undersøgelse lyder mere sandsynligt end det fra 2016. Det er DKCERTs opfattelse, at VPN ikke er så udbredt blandt private, fordi det kræver en del opsætning og i mange tilfælde også betaling. Der er dog begyndt at dukke enklere løsninger op eksempelvis indbygget i en browser eller i antivirusprogrammet.

7.3.5. Sikkerhedskopiering

Hvis man løbende tager sikkerhedskopi af sine data, betyder det i princippet intet, om man eksempelvis rammes af ransomware-angreb og mister adgangen til sine dokumenter. Kun godt 40 procent af borgerne tager sikkerhedskopi, hvilket er på niveau med 2016, men det bekræfter dog en lille stigning, vi har set siden 2013, hvor tallet var på godt 37 procent (se Figur 45: Fire ud af ti borgere tager jævnligt sikkerhedskopi af deres data i 2018.).

Med cloud-tjenesternes indmarch er det blevet langt lettere for private at tage en automatisk backup (se Figur 47: Cloud-tjenester er fortsat den mest populære metode til backup af

smartphones og tablet-computere.). Man skal dog være opmærksom på, at cloud-løsninger ikke i alle tilfælde giver den tilstrækkelige beskyttelse mod ransomware-angreb (beskrevet i afsnit 2.16).

På arbejdspladserne er det vigtigt at gemme sine dokumenter rigtigt, og it-afdelingen bør oplyse om hvilke mapper, der sikkerhedskopieres, så brugerne kan placere data de rigtige steder.

I den offentlige sektor fortæller tre ud af ti af de offentligt ansatte, at der ikke tages sikkerhedskopi af data på pc, og 55 procent svarer, at der ikke tages kopi af data på telefon eller tablet-computer. Der tages dog det forbehold, at ikke alle nødvendigvis har kendskab til, om der tages automatisk backup af data på arbejdspladsernes computere og mobile enheder.

Der er fortsat et behov for en øget indsats for information om sikkerhedskopiens potentiale i forbindelse med tab af data, nedbrud eller angreb som eksempelvis ransomware.

7.3.6. Sikkerhedskultur i hjemmet og på arbejde

I takt med at digitalisering fylder mere og mere både i den offentlige sektor og hos borgeren, træder betydningen af god og sikker adfærd frem. Betydningen af sikkerhedskultur både i hjemmet og på arbejdspladsen bliver vigtigere og vigtigere for at man kan imødekomme et øget trusselsbillede.

På arbejdspladserne er det ledelsens opgave at udbrede sikkerhedspolitikkerne og sikre, at medarbejderne kender den. Fire ud af ti medarbejdere har ikke sat sig ind i reglerne om informationssikkerhed på deres arbejdsplads og otte procent undlader nogle gange at følge sikkerhedsreglerne (seks procent i 2016), selvom de kender den.

Af dem oplyser 33 procent, svarende til omkring 25.000, at de undlader at følge reglerne dagligt eller mindst en gang om ugen. Det kan synes som et lille tal i forhold til antallet af offentligt ansatte, men der er faktisk tale om fordobling i forhold til 2016, hvor tallet var 16 procent.

En uomgængelig regel for offentligt ansatte er, at man ikke må sende personfølsomme oplysninger i ukrypterede e-mails. 30 procent har alligevel gjort det i mails, og af disse oplyser 21 procent, at der ikke har været anvendt kryptering, hvilket svarer til omkring 60.000 offentligt ansatte (se Figur 6: Hele 21 procent oplyser, at de har sendt cpr-nummer via mail uden kryptering.). Fire procent svarende til ca. 40.000 oplyser, at uvedkommende kan have fået adgang til fortrolige oplysninger som følge af deres adfærd. Det vil sige, at der potentielt kunne have været 40.000 hændelser med kompromittering af fortrolige oplysninger.

Det er uheldig adfærd blandt offentligt ansatte, der har en særlig forpligtelse til at beskytte borgernes personfølsomme oplysninger. Også her bør ledelsen indskærpe, at sikkerhedspolitikkerne og retningslinjerne skal efterleves. I det hele taget er det en ledelsesopgave at oplyse de ansatte om informationssikkerhedspolitikken, hvilket 35 procent af de offentligt ansatte oplyser, at de *ikke* har modtaget oplysning om (se Figur 25: Det er langt fra alle arbejdsgiverne, der har informeret om deres informationssikkerhedspolitik.).

I hjemmet er borgerne generelt gode til at hjælpe deres børn/unge med informationssikkerhed, men hver femte hjælper ikke sit barn (se Figur 38: De fleste forældre oplyser, at de hjælper deres børn med informationssikkerhed.). Alligevel er der sket et fald fra 88 procent i 2016 til 80 procent i 2018. Faldet kan skyldes, at der kommer flere og flere enheder i hjemmet, og at det kan opleves som en mere og mere komplekst opgave at holde styr på de mange enheder.

Privatlivsbeskyttelse har været meget i vælten i de senere år, blandt andet som følge af implementeringen af databeskyttelsesforordningen i maj 2018, ligesom sociale medier også har haft øget fokus på det. Det kan muligvis være årsagen til, at otte ud af ti borgere nu manuelt har indstillet egne privatlivsindstillinger. Det er en stigning fra 72 procent i 2016. Der er også fremgang i andelen af borgere, der læser privatlivspolitikken på et socialt medie. En stigning til 38 procent fra 27 procent.

Og otte ud af ti hjælper med at beskytte barnets privatliv på nettet. Dette er på niveau med de tre år, vi har stillet spørgsmålet.

8.
Anbefalinger til ledelsen

8. Anbefalinger til ledelsen

Ud fra resultaterne af undersøgelsen har DKCERT udarbejdet disse anbefalinger for at øge informationssikkerheden blandt offentligt ansatte.

Informationssikkerhed er ledelsens ansvar. Hvis medarbejdere ikke handler sikkerhedsmæssigt fornuftigt i hverdagen, kan det skyldes, at der ikke er nok ledelsesmæssig fokus på informationssikkerhed i virksomheden. En indsats for øget informationssikkerhed kan fx tage udgangspunkt i en analyse af organisationens sikkerhedskultur og de holdninger til sikkerhed, der udgår fra ledelsen. Ledelsen bør altid sikre, at der kommunikeres i et klart, tydeligt og forståeligt sprog, så der ikke er tvivl om, hvordan medarbejderen skal håndtere informationssikkerheden. Fremfor alt bør ledelsen være synlig i sin kommunikation af betydningen af informationssikkerhed og sætte fokus på at udbrede kendskabet til informationssikkerhedspolitikken.

8.1. Indsats mod netbaseret svindel

Rigtig mange ansatte oplever, at der er enten en mail med et risikabelt link eller en phishing-mail i indbakken. Heldigvis klikker kun ganske få på links og udfylder felterne på phishing-sider. For at mindske risikoen bør medarbejderne dog uddannes i at genkende tvivlsomme mails. Endvidere bør arbejdspladsen indføre tekniske kontroller i form af mailfiltrering og teknologier som DMARC (Domain-based Message Authentication, Reporting & Conformance), der gør det vanskeligt for svindlerne af angive en forfalsket afsenderadresse.

8.2. Indsats mod tab af data

Skadelig software har ramt 11 procent af de offentligt ansatte. To procent har været ramt af ransomware, otte procent har mistet data som følge af manglende backup og to procent som følge af angreb. Det kan afhjælpes ved at øge indsatsen mod skadelig software og kontrollere rutinerne for sikkerhedskopiering af data. Især mobile enheder synes at mangle sikkerhedskopiering. I den forbindelse anbefales det, at dette understøttes teknisk eksempelvis med opsætning af automatisk backup.

8.3. Indsats mod uvedkommendes adgang til data

Genbrug af adgangskoder giver risiko for, at hackere kan få adgang til data og systemer, hvis blot et af systemerne får kompromitteret sikkerheden. Genbrug kan mindskes med brug af single sign-on og password managers. Endvidere kan risikoen mindskes med to-trinsbekræftelse, hvor det er muligt.

Brug af usikre trådløse netværk på cafeer og hoteller medfører også en risiko for, at uvedkommende får adgang til fortrolige data. Hver fjerde, der anvender netværk uden for arbejdspladsen, bruger ukrypterede netværk, og kun halvdelen af dem anvender VPN. Det kan forbedres ved at øge kendskabet til risici ved anvendelse af usikre, trådløse netværk. Informationssikkerhedspolitikken bør også adressere sikker anvendelse af enhederne uden for arbejdspladsen fx ved hjælp af VPN. En højere andel af VPN-brugere vil styrke sikkerheden markant.

8.4. Råd til medarbejderne

Ledelsen kan bruge følgende råd til medarbejdere som udgangspunkt i en oplysningsindsats, der bør være målrettet den enkelte organisation.

1. Sæt dig ind i arbejdspladsens regler for informationssikkerhed og følg dem, selv om det kan være besværligt.
2. Brug stærke passwords: Et password bør være mindst 12 tegn langt og unikt, dvs. det bør ikke genbruges på tværs af tjenester.
3. Brug forskellige passwords til forskellige tjenester og systemer. Bed om at få systemer som single sign-on eller password manager stillet til rådighed. Benyt to-faktorbekræftelse, hvis det er muligt.
4. Undlad at klikke på links eller vedhæftede filer i e-mails, du får tilsendt uopfordret.
5. Vær kritisk over for henvendelser, der beder dig gøre noget, du ikke plejer at gøre som led i dit arbejde. Eksempelvis pengeoverførsler.
6. Undgå at sende følsomme data over åbne trådløse netværk (netværk uden kryptering) eller via ukrypteret e-mail.
7. Pas på med flytbare medier såsom USB-nøgler, cd'er og transportable harddiske, de kan være inficeret med skadelig kode.
8. Læg ikke følsomme oplysninger på flytbare medier, med mindre de er beskyttet med kryptering eller et password.
9. Brug din sunde fornuft – og bed om hjælp, hvis du er i tvivl.
10. Stil spørgsmål og kom med forslag, der kan øge informationssikkerheden på din arbejdsplads.

9.
Anbefalinger til borgerne

9. Anbefalinger til borgerne

Ud fra resultaterne af undersøgelsen har DKCERT udarbejdet disse anbefalinger, der skal hjælpe borgerne til at øge deres informationssikkerhed.

Medarbejdere i den offentlige sektor har som regel professionelle it-folk eller en ledelse, som de kan støtte sig til, når det gælder informationssikkerhed. Sådan er det ikke for borgere. De står ofte alene med problemerne. Samtidig har de ikke nødvendigvis fået en uddannelse i de sikkerhedsmæssige aspekter af det it-udstyr, de har købt. Derfor er det ikke overraskende, at sikkerhedsproblemerne, eksempelvis antallet af virusinfektioner, blandt de private borgere er større end blandt de ansatte.

DKCERT anbefaler, at borgere især sætter ind på følgende områder:

9.1. Beskyttelse mod skadelig software

Hver tredje borger i undersøgelsen har været udsat for infektioner med skadelig software. Sikkerhedssoftware og opdatering af programmer er nogle af de vigtigste faktorer for god sikkerhed. En øget brug vil give bedre sikkerhed for alle, da it-problemerne spredes via sårbare systemer. Brug derfor altid antivirus og firewall. Husk at opdatere programmer med de nyeste rettelser fra producenterne.

9.2. Indsats mod netbaseret svindel

Rigtigt mange af borgerne har modtaget en phishing-mail. Kun to procent faldt for svindlen. Det er en forbedring på tre procentpoint i forhold til 2016. Alle bør være kritiske over for mails, der kommer fra ukendte afsendere. Ligeledes bør man se på indholdet, hvor man ofte vil genkende fup-mails ud fra dårligt dansk sprog, tilbud, der er for gode til at være sande, samt kontrollere, hvor et link fører hen.

Borgerne søger oftest deres viden om informationssikkerhed via nyhedsmedier, venner og bekendte samt sociale medier. Det anbefales, at man følger med i de aktuelle sikkerhedstrusler, gerne via medier, der har specialiseret sig i informationssikkerhed. På den måde kan man være på forkant med eksempelvis spam-kampagner eller konkrete sikkerhedstrusler.

9.3. Øget sikkerhedskopiering

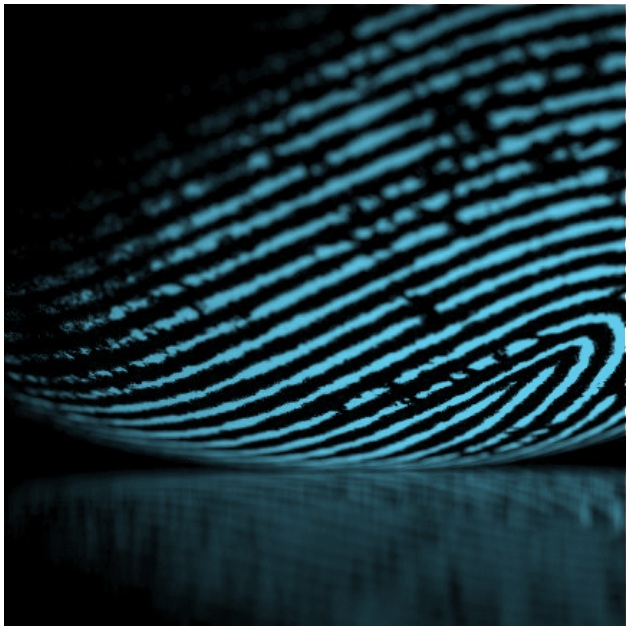
Jævnlige sikkerhedskopier vil mindske risikoen for tab af data ved computernedbrud, tyveri eller ransomware-angreb. Det samme gør sig gældende for mobile enheder. Tag en backup og gerne en ekstra, der er placeret på en enhed, eksempelvis ekstern harddisk, der ikke er koblet på internettet.

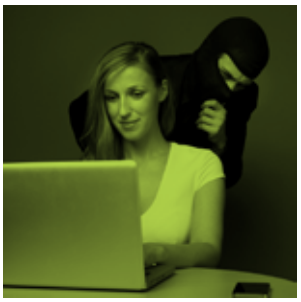
9.4. Stop for genbrug af passwords

Anvend altid stærke adgangskoder og aldrig det samme password til flere tjenester. Det giver risiko for misbrug af personlige oplysninger. Benyt også to-trinslogin, hvis det er muligt. Hvis man har svært ved at huske de lange adgangskoder, kan man anvende en password manager, der er et program, beregnet til at hjælpe med at holde styr koderne.

9.5. Sikker brug af trådløse netværk

Hvis du anvender trådløse netværk uden kryptering, eksempelvis på en kaffebar, så sæt dit system op til at 'glemme' netværket, når du kobler af det. På den måde har du styr på, hvornår og hvor du er online. Hvis du udveksler følsomme data, anbefales det, at du anvender en krypteret VPN-tunnel. Det sikrer dine data effektivt.





9.6. Råd til borgere

1. Brug sikkerhedssoftware som antivirus og firewall.
2. Hold altid dine programmer opdateret med den nyeste software fra producenten.
3. Tag sikkerhedskopi af dine data og opbevar flere kopier, helst forskellige steder.
4. Undlad at klikke på links eller vedhæftede filer i e-mails, du får tilsendt uopfordret.
5. Undersøg adressen på et websted, før du udfylder formularer med fortrolige oplysninger. Oplys generelt kun fortrolige oplysninger på netsteder, du har tillid til. Kontroller, at links til sider med fortrolig information begynder med teksten ”https:”.
6. Beskyt dit trådløse netværk med en unik adgangskode.
7. Pas på flytbare medier såsom USB-nøgler, cd’er og transportable harddiske, de kan være inficeret med skadelig kode.
8. Undgå at sende følsomme data over åbne trådløse netværk (netværk uden kryptering) eller via ukrypteret e-mail.
9. Brug VPN (virtuelt privat netværk), hvis du bruger åbne trådløse netværk. Et VPN er software, der danner en sikret tunnel mellem din computer og fx din arbejdsplads.
10. Hvis du har brugt et åbent eller fremmed trådløst netværk, så sæt din telefon/computer til at glemme det bagefter. Ellers kan hackere senere narre din enhed til at koble sig op på deres netværk.
11. Brug stærke passwords: Et password bør være mindst 12 tegn langt og unikt, dvs. det bør ikke genbruges på tværs af tjenester.Brug forskellige passwords til alle tjenester. Du kan holde styr på dine passwords med et password manager-program.
12. Brug to-trins bekræftelse, hvor det er muligt. Det er et supplement til passwords, som kan bestå af engangskoder, du modtager via sms, på et nøglekort eller med en app.
13. Indstil privatlivsindstillingerne på sociale netværk, så de opfylder dine behov for privatlivsbeskyttelse i det omfang, det er muligt.
14. Oplys ikke fortrolige og personlige oplysninger på sociale netsteder, debatsider og chatrum.
15. Hjælp dine børn med at lære sikker adfærd i den digitale verden.

DIGITALISERINGSSTYRELSEN

KL

DANSKE REGIONER

DKCERT

DeiC

sikkerdigital.dk