DIGITALISERINGSSTYRELSEN

DKCERT

DeiC DANISH e-INFRASTRUCTURE COOPERATION

Borgernes informationssikkerhed 2015

Januar 2016

1. Indledning

Denne rapport belyser danskernes informationssikkerhed ud fra to perspektiver: Den afdækker, hvilke sikkerhedshændelser borgerne bliver udsat for, og den belyser borgernes viden om informationssikkerhed og deres evne til at beskytte sig mod udbredte trusler.

Rapporten bygger på en undersøgelse, som Danmarks Statistik foretog for Digitaliseringsstyrelsen og DKCERT i efteråret 2015. Undersøgelsen stillede en række spørgsmål til et repræsentativt udvalg af den voksne danske befolkning om deres erfaringer med informationssikkerhed. Undersøgelsen bygger på svar fra 851 personer i alderen 16-74 år.

Danmarks Statistik udførte lignende undersøgelser for Digitaliseringsstyrelsen og DKCERT i 2013 og 2014. Resultaterne fra de tidligere undersøgelser indgår i denne rapport under de punkter, hvor det er muligt og relevant at foretage en sammenligning.

Som noget nyt har årets undersøgelse spurgt til, hvordan borgerne hjælper deres børn med at håndtere de udfordringer med sikkerhed og privatlivsbeskyttelse, som det digitale liv giver børnene.

BORGERNES INFORMATIONSSIKKERHED 2015

Digitaliseringsstyrelsen og DKCERT, DeIC
Redaktion: Henrik Larsen og Torben B. Sørensen
Design: Kiberg & Gormsen

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

DeIC-journalnummer: JS 2015-4

2. Danskernes informationssikkerhed

Statistisk undersøgelse af konkrete trusler mod danskernes informationssikkerhed og borgernes kendskab til området.

I dette kapitel belyser vi den aktuelle status for danskernes informationssikkerhed ud fra svarene i undersøgelsen.

2.1. Oplevede trusler

Vi har spurgt deltagerne, om de har oplevet tre specifikke trusler mod deres informationssikkerhed: Virus, misbrug af personlige data og økonomisk tab som følge af en sikkerhedshændelse.

30 procent har været udsat for virus eller andre skadelige programmer. 4 procent har oplevet misbrug af deres personoplysninger på nettet. Det kan fx være oplysninger om betalingskort, som svindlere udnytter til at købe varer på offerets regning. Knap 3 procent har lidt økonomisk tab som følge af it-sikkerhedsproblemer.

Tallene ligger på niveau med svarene fra de tidligere år. Dog er der dobbelt så mange, der har oplevet misbrug af personlige data i forhold til 2014, mens tallet var på samme niveau i 2013.

Tallene viser kun, hvilke sikkerhedstrusler borgerne selv har observeret. Det er derfor muligt, at flere kan have været udsat for fx virusinfektioner eller misbrug af fortrolige data, uden at de har opdaget det.

2.2. Konsekvenser som følge af truslerne

De borgere, der havde oplevet en eller flere af de tre sikkerhedstrusler, blev spurgt, hvilke konsekvenser hændelsen havde for deres adfærd. De fik fem valgmuligheder:

Har du som følge af de oplevede it-sikkerhedsproblemer:

- undladt at besøge bestemte websteder?
- undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat Tastselv, melde flytning)?
- installeret eller opgraderet sikkerhedssoftware (fx antivirus)?
- undladt at dele oplysninger om dig selv på sociale netværk?
- anmeldt sikkerhedsproblemet til politi eller andre?

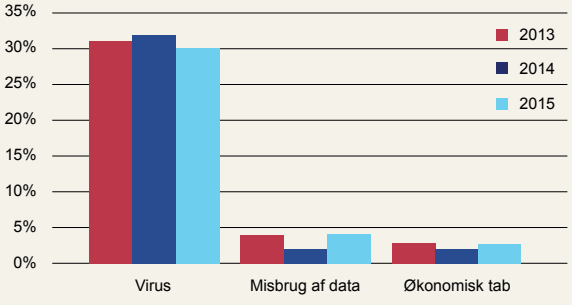
Den hyppigste reaktion er at installere sikkerhedssoftware, det gjorde 73 procent. Det stemmer godt overens med, at virus er den hyppigst oplevede sikkerhedstrussel.

58 procent blev mere tilbageholdende med at dele data på sociale netværk, og 54 procent undlod at besøge bestemte websteder efter sikkerhedshændelsen.

Derimod er det kun henholdsvis 11 og 10 procent, der har anmeldt hændelsen til politiet eller undladt at bruge digitale selvbetjeningsløsninger fra det offentlige.

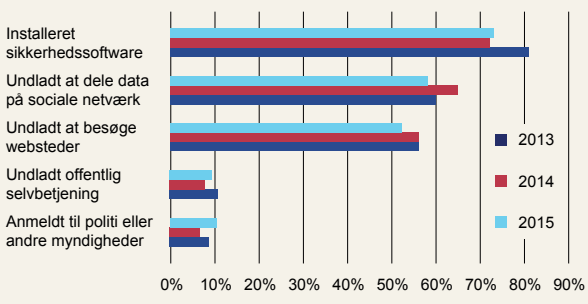
Figur 1

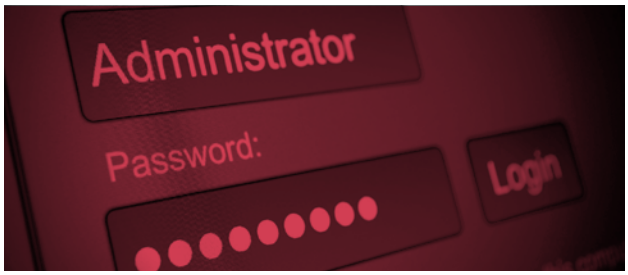
Borgernes oplevede sikkerhedstrusler



Figur 2

Handlinger som reaktion på sikkerhedshændelser





2.3. Kommunikation med det offentlige

E-mail er som udgangspunkt ukrypteret. Hvis nogen opfanger en e-mail på vej fra afsender til modtager, kan vedkommende læse indholdet. Derfor er det også et krav, at når offentlige myndigheder sender e-mails med fortrolige oplysninger, skal de krypteres.

21 procent har sendt et cpr-nummer eller andre personlige oplysninger i en e-mail til det offentlige. Det er lidt færre end de 25 procent i 2014.

I undersøgelsen blev deltagerne spurgt, om de vidste, at e-mail er en usikker metode til at sende fortrolige oplysninger med. De fik disse svarmuligheder:

- Ja, ved at det er usikkert.
- Nej, ved ikke det er usikkert.
- Ja, derfor sender jeg oplysningerne med krypteret e-mail.
- Nej, det er en sikker metode, når der sendes krypteret.

Tre ud af fire er klar over, at e-mail er usikkert. 19 procent ved ikke, at e-mail er usikkert. Kun fire procent oplyser, at de bruger krypteret e-mail.

2.4. Tillid til det offentliges datahåndtering

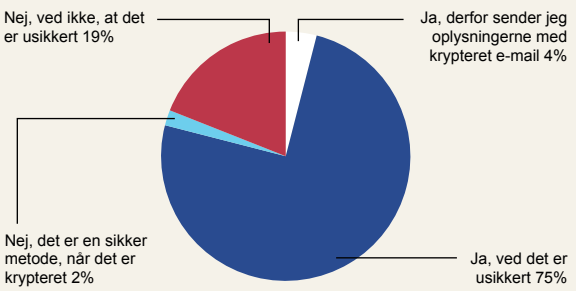
83 procent af deltagerne i undersøgelsen anvender offentlige digitale tjenester. Det kan fx være indberetning til Skat, anmeldelse af flytning eller opskrivning til børnepasning. De blev spurgt om, hvor høj grad af tillid de har til, at myndighederne håndterer deres personlige oplysninger sikkert og fortroligt.

Det er også 83 procent af deltagerne, der har fra nogen tillid til meget stor tillid til, at det offentlige har styr på fortrolighed og sikkerhed. 16 procent har lille eller meget lille tillid.

Borgernes tillid er stort set uændret i forhold til undersøgelsen fra 2014. Dog udtrykker lidt flere meget stor tillid, mens lidt færre svarer ”Stor tillid”.

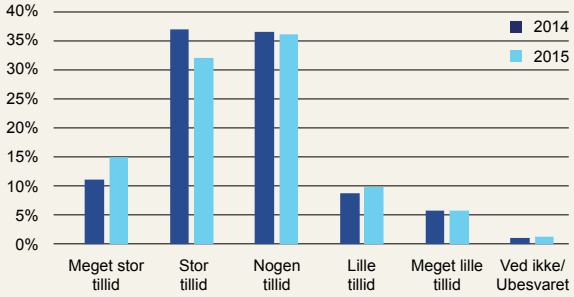
Figur 3

Ved du, at e-mail er en usikker metode til at sende fortrolige pålysninger med?



Figur 4

De fleste har tillid til, at det offentlige har styr på sikkerhed og fortrolighed, når det gælder følsomme persondata.



2.5. Hjælp til børns adfærd på nettet

25 procent af deltagerne havde børn i alderen 5-16 år. De blev stillet tre spørgsmål om, hvorvidt de hjælper deres barn med:

- at beskytte dets privatliv på nettet?
- at lære sikker adfærd på nettet?
- at installere sikkerhedssoftware?

De fleste svarede ja til de to første spørgsmål. 56 procent hjalp deres barn med at installere sikkerhedssoftware.

2.6. Privatlivsbeskyttelse på sociale medier

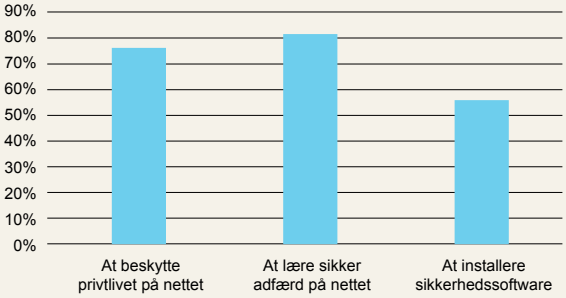
Stadig flere borgere har profiler på sociale netværk som Facebook, LinkedIn og Twitter. Hvor andelen i 2014 var 72 procent, var den i 2015 oppe på 75 procent. Disse tjenester er gratis, men virksomhederne bag dem kan tjene penge på at udnytte de oplysninger, brugerne deler på dem.

28 procent oplyser, at de har læst privatlivspolitikken for de sociale netværk, de anvender. 74 procent har manuelt været inde og ændre i privatlivsindstillingerne. En tilsvarende andel er klar over, at de ofte fraskriver sig rettighederne til de billeder, de lægger op på tjenesten.

Svarene ligner dem, der kom i undersøgelsen i 2014. Andelen af borgere, der kender til rettighederne til billeder, er vokset lidt. Men det kan hænge sammen med, at spørgsmålet var formuleret anderledes i 2014-undersøgelsen. Dengang lød det: ”Ved du, hvem der ejer rettighederne til de billeder, du lægger op?”

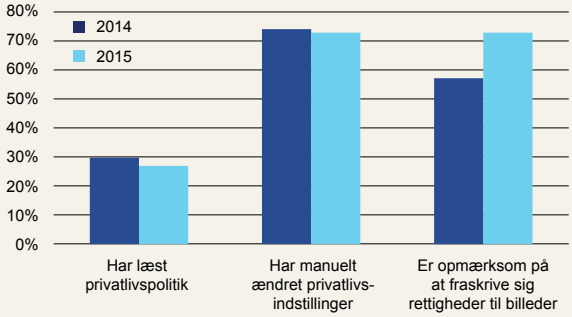
Figur 5

De fleste forældre hjælper deres børn med at lære, hvordan man agerer sikkert på nettet.



Figur 6

Brugere af sociale netværks kendskab til privatlivsbeskyttelsen



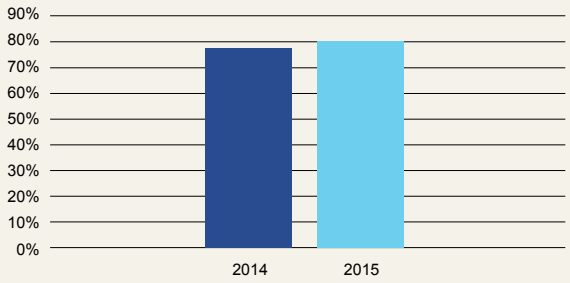
2.7. Cookies

En cookie er data, som et websted kan lagre i brugerens browser. Dermed kan webstedet genkende brugeren ved det næste besøg. Opmærksomheden på cookies er øget de senere år, efter at et EU-direktiv krævede, at brugere skal informeres om cookies og have mulighed for at vælge dem fra.

80 procent af borgerne svarer, at de ved, hvad en cookie er. Ud af de 80 procent er 85 procent opmærksomme på, hvad det medfører, når de siger ja til cookies fra en hjemmeside. Selvom borgerne selv mener, at de ved, hvad en cookie er, kan de tage fejl. En undersøgelse fra Kommunikationsbureauet Bjerg K fra september 2015 viste således, at kun 10,5 procent af borgerne forstår ordet cookie. 40 procent forstår det delvis.

Figur 7

Borgere der kender begrebet cookie



2.8. Beskyttelse mod skadelig software

Vi har spurgt borgerne, hvordan de beskytter deres computer og smartphone eller tablet mod skadelig software og andre angrebsformer. 29 procent anvender gratis sikkerhedsprogrammer, andre 29 procent bruger programmer, de selv har betalt. 23 procent bruger sikkerhedssoftware, der fulgte med, da de købte pc'en. I forhold til de foregående år er der et lille fald i andelen, der anvender gratis sikkerhedsprogrammer. I alt svarer 81 procent, at de bruger en form for sikkerhedssoftware.

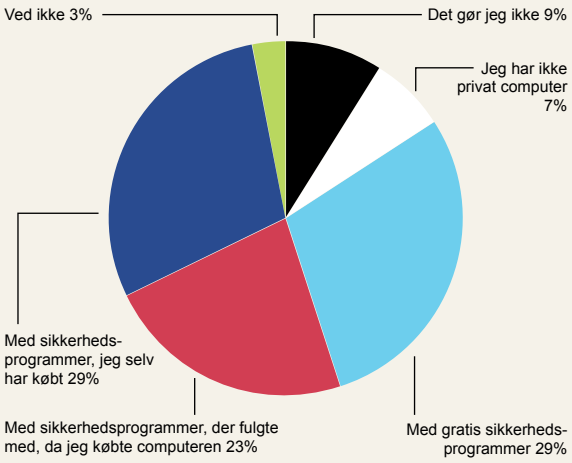
Billedet er meget anderledes, når det gælder smartphones og tablets. Hele 39 procent svarer, at de ikke beskytter enheden med sikkerhedssoftware. Det en stigning i forhold til 34 procent i 2014 og 32 procent i 2013. Samtidig er mængden af enheder i stigning, kun 15 procent har ikke en smartphone eller tablet mod 26 procent i 2013.

Hos dem, der beskytter deres enhed, er den hyppigste løsning at bruge programmer, der blev leveret sammen med den.

Manglen på sikkerhedssoftware til smartphones og tablets kan måske forklares med, at brugerne ikke oplever et behov for at beskytte sig. Kun 4 procent har downloadet en app eller andet indhold til smartphone eller tablet, som viste sig at være skadeligt. Det er dog muligt, at nogle borgere har fået inficeret deres enhed uden at opdage det. Tallet er i øvrigt på niveau med 2014.

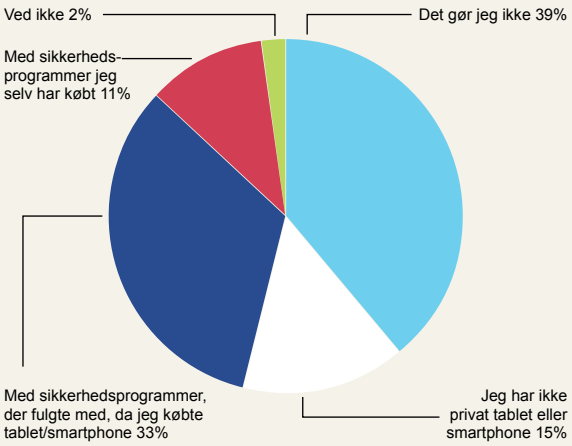
Figur 8

Hvordan beskytter du din private computer og data på den?



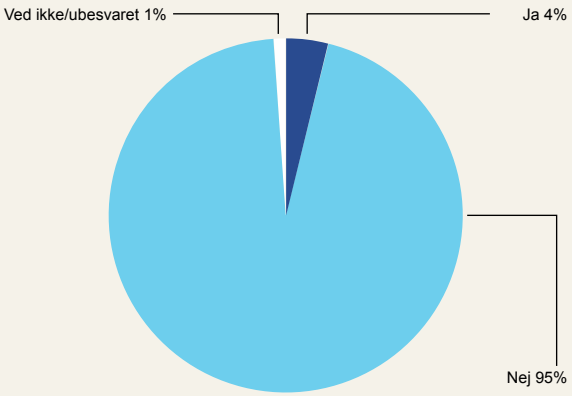
Figur 9

Hvordan beskytter du din smartphone eller tablet?



Figur 10

Har du prøvet at downloade en app eller andet indhold til din smartphone eller tablet, som viste sig at være skadeligt?



2.9. Opdatering af software

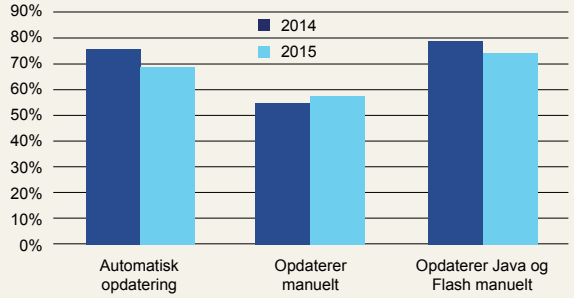
Gamle versioner af software udgør en væsentlig sikkerhedsrisiko: De kan indeholde sikkerhedshuller, som angribere kan udnytte. Derfor er det vigtigt for sikkerheden, at programmer så vidt muligt holdes opdateret til nyeste version.

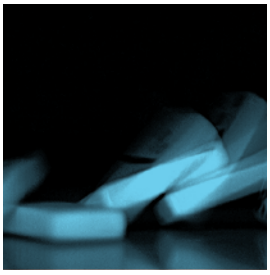
85 procent af borgerne oplyser, at de holder programmerne på deres computer opdateret. 69 procent bruger automatisk opdatering, 57 procent opdaterer manuelt. Overlapningen skyldes, at man godt kan opdatere nogle programmer manuelt, mens andre opdateres automatisk.

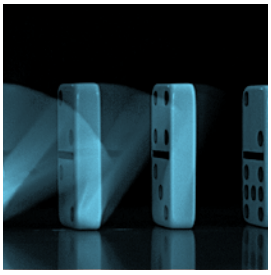
To af de mest sårbare programmer er Java og Adobe Flash Player. Derfor er det særlig vigtigt, at de holdes opdateret. 74 procent oplyser, at de opdaterer disse programmer manuelt. Faldet fra 79 procent i 2014 kan skyldes, at flere har slået automatisk opdatering til for disse to programmer.

Figur 11

Brugere der holder programmerne på deres pc opdateret.

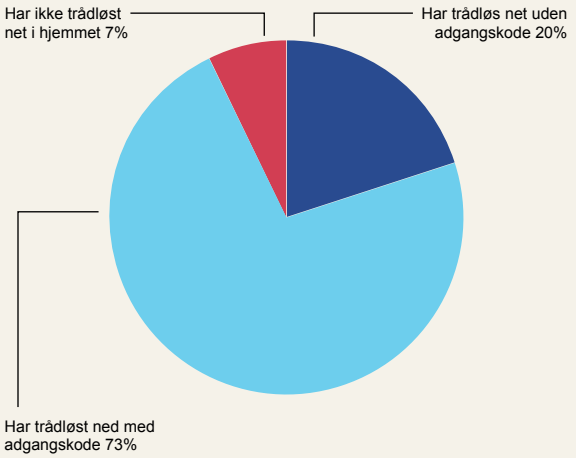






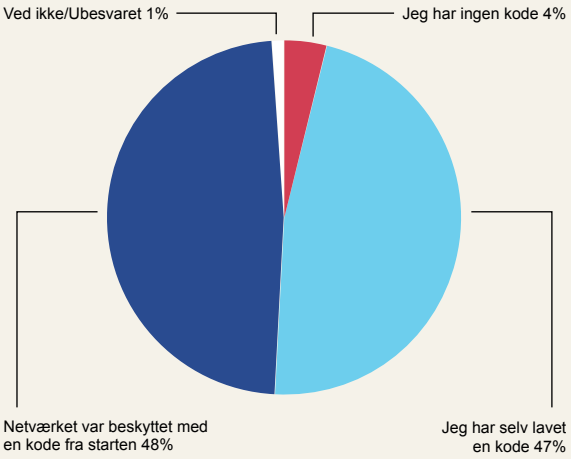
Figur 12

20 procent har usikre trådløse netværk i deres hjem



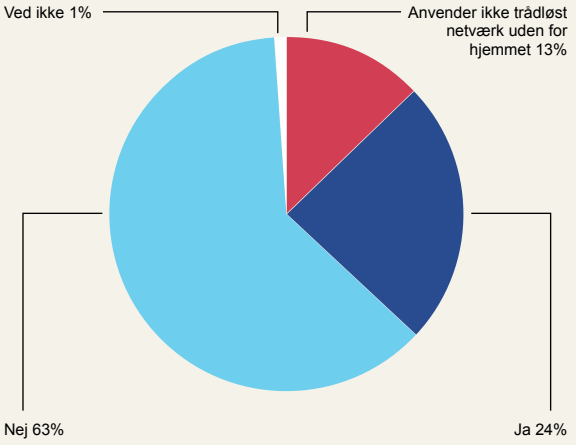
Figur 13

Hvordan er adgangskoden til dit trådløse netværk i hjemmet sat op?



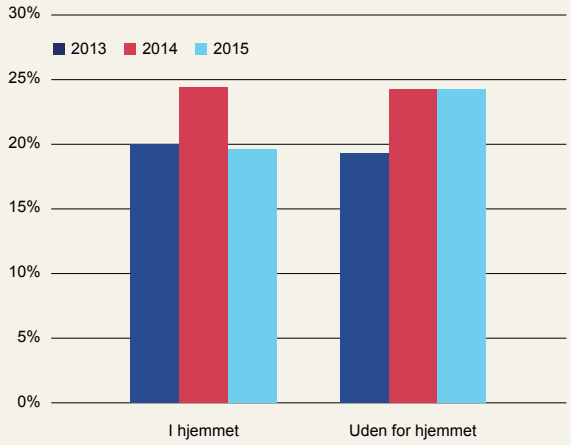
Figur 14

Bruger du trådløse netværk uden adgangskode uden for hjemmet?



Figur 15

Brugen af usikre trådløse netværk er stort set uændret



2.10. Sikkerhed på trådløse netværk

Trådløse netværk kommunikerer via radiobølger. Enhver, der er inden for netværkets senderækkevidde, kan opfange data fra det. Derfor er det vigtigt for sikkerheden, at alle data sendes krypteret. Hvis et trådløst netværk kræver en adgangskode, før det kan bruges, er det som regel tegn på, at det er krypteret.

20 procent af borgerne har i deres hjem et trådløst netværk, der ikke kræver adgangskode. Disse netværk må formodes at være uden kryptering. I 2014 var andelen 24 procent.

Hos de borgere, der har beskyttet deres netværk med en adgangskode, har halvdelen selv sat koden op. De øvrige bruger den kode, som udstyret blev leveret med.

Sikkerhedsmæssigt kan den sidste løsning både være god og dårlig. Hvis der er tale om en standardkode fra fabrikken, som alle apparater er udstyret med, er den usikker. Kommer koden derimod fra internetudbyderen, og er der forskellige koder til alle kunder, kan den være sikkerhedsmæssigt forsvarlig.

Når det gælder trådløse netværk uden for hjemmet, oplyser 24 procent, at de bruger netværk, som ikke kræver en adgangskode. Andelen er uændret i forhold til 2014.

2.11. Sikkerhed på onlinetjenester

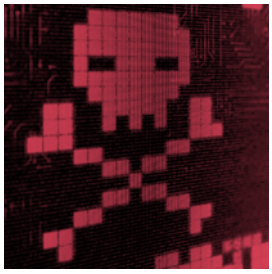
Det udgør en sikkerhedsrisiko, hvis borgerne anvender den samme adgangskode til flere web-tjenester. Hvis hackere får fat i passwords fra blot en af tjenesterne, kan de afprøve dem på en række andre tjenester. Er der gevinst, risikerer borgeren at miste data på alle tjenesterne eller fx få sin profil på et socialt medie overtaget af andre.

Derfor er det sikrest at have unikke passwords til alle tjenester. Men det er i praksis umuligt for de fleste at huske så mange koder. En løsning er at opbevare adgangskoderne i et særligt program, der er beskyttet med en masterkode. Så skal borgeren kun huske masterkoden for at få adgang til alle sine passwords.

En anden metode går ud på at opdele websteder efter, hvor vigtige oplysninger de opbevarer. Så kan borgeren bruge samme password til alle websteder med mindre følsomme oplysninger, mens adgangen til fx netbank eller digitale selvbetjeningsløsninger via NemID bliver beskyttet med stærke og unikke passwords.

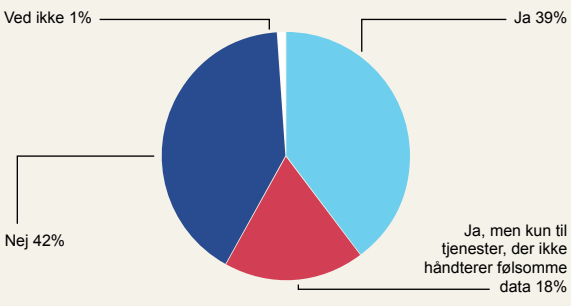
57 procent bruger samme password til flere tjenester. Men 18 procent anvender den graduerede løsning, hvor de kun bruger samme kode til tjenester, der ikke håndterer følsomme data.

I 2014 svarede 41 procent ja til at bruge samme password til flere tjenester. Dermed er mængden, der anvender samme password, steget. Tallene er dog ikke helt sammenlignelige, da deltagerne i 2013 og 2014 kun havde to svarmuligheder: ”Bruger du samme adgangskode til flere onlinetjenester, ja eller nej?” I 2015 fik de mulighed for at graduere det med svaret ”Ja, men kun til tjenester, der ikke håndterer følsomme data.”



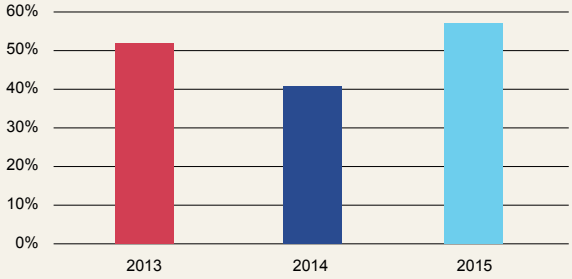
Figur 16

Bruger du samme adgangskode til flere onlinetjenester?



Figur 17

Bruger samme adgangskode til flere onlinetjenester



2.12. Sikkerhedskopiering

Hvis data forsvinder, er det altafgørende at have en kopi af dem. En sikkerhedskopi er nødvendig, når en computer bliver stjålet, går i stykker, går tabt i en brand – eller bliver udsat for ransomware, der gør data ulæselige. Læs mere om ransomware i afsnit 2.14.

38 procent tager jævnligt sikkerhedskopi af data på deres computer. 31 procent sikkerhedskopierer data fra deres smartphone eller tablet.

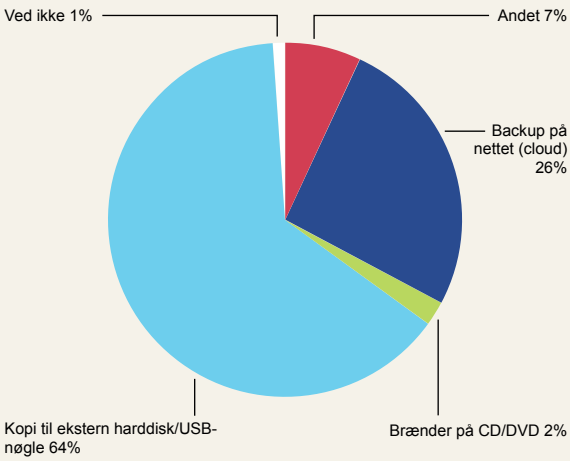
På computeren er en ekstern disk stadig den mest populære metode. Det gør 64 procent af dem, der tager backup. På andenpladsen kommer kopiering over nettet via cloudtjenester med 26 procent. Den andel har været stigende siden 2013, hvor det var 19 procent.

På smartphone og tablet er kopiering til en server i skyen derimod langt den mest udbredte metode med 62 procent. 19 procent anvender en ekstern disk eller USB-nøgle.

De forskellige aldersgrupper er stort set lige gode til at tage sikkerhedskopi af deres pc'er. Men på de mobile enheder er det tydeligt, at de yngre har bedst styr på backup-proceduren. Kun 14 procent af borgere over 65 år tager sikkerhedskopi af deres smartphone eller tablet, hvor gennemsnittet på tværs af aldersgrupper er 31 procent.

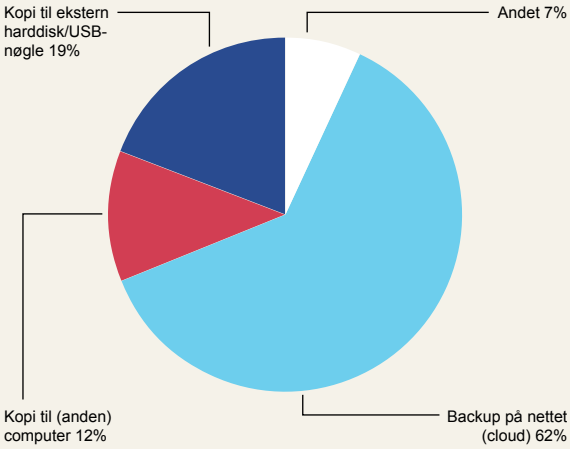
Figur 18

Metoder til sikkerhedskopiering af computer



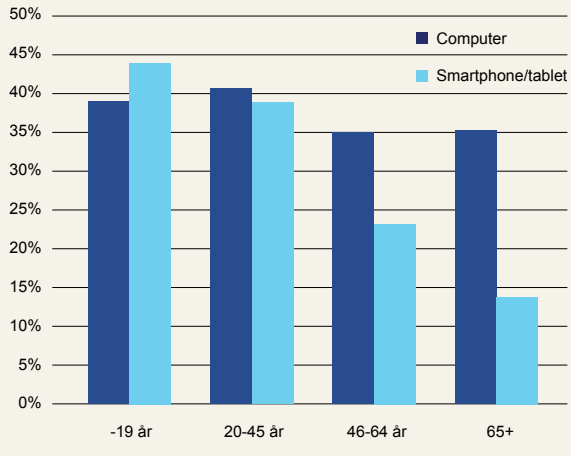
Figur 19

Metoder til sikkerhedskopiering af smartphone/tablet



Figur 20

Sikkerhedskopiering fordelt på aldersgrupper



2.13. Evnen til at beskytte sig

De fleste borgere mener, at de er i stand til at beskytte sig mod udbredte trusler som virus og e-mails med vedhæftede filer eller links. Derimod mener kun 29 procent, at de kan beskytte sig mod phishing. En mulig årsag kan være, at de ikke kender begrebet. Phishing er forsøg på at lokke fortrolige oplysninger fra ofrene, hvor angriberen fx giver sig ud for at være borgerens bank. Digitaliseringsstyrelsen kørte en landsdækkende informationskampagne om blandt andet phishing fra 20. oktober til 10. november 2015, men det var således efter, at denne undersøgelse var gennemført. Derfor kan undersøgelsen ikke vise et eventuelt øget kendskab til phishing som følge af kampagnen.

Tallene er stort set uændrede over årene bortset fra en stigning fra 2013, når det gælder virus og andre skadelige programmer.

2.14. Angreb med ransomware

Ransomware er skadelige programmer, der spærrer for adgangen til data og/eller programmer. Offeret får besked om, at der skal betales en løsesum for at få data tilbage.

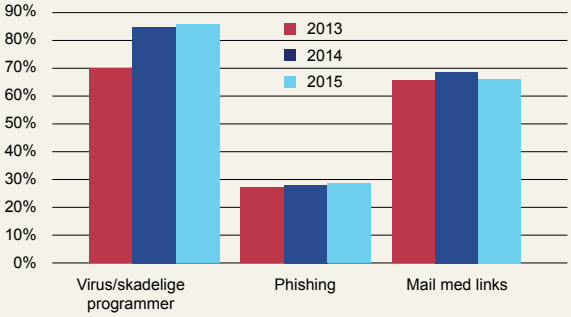
7 procent af borgerne har oplevet ransomware. I 2014 var det 8 procent.

13 procent af de ramte fik aldrig deres data tilbage – 4 procent endda, selvom de betalte løsesummen til bagmændene. De øvrige 87 procent fik deres data tilbage, de fleste ved hjælp af sikkerhedsprogrammer.

Ingen svarede, at de betalte løsesummen og fik deres data tilbage.

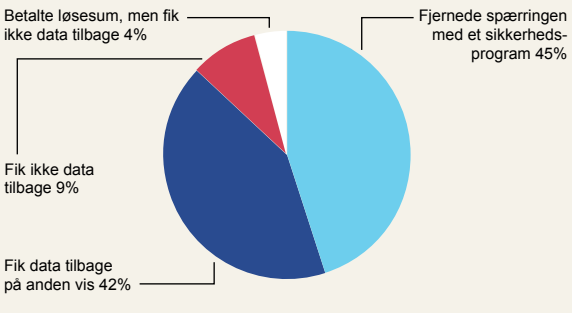
Figur 21

Borgere, der kan beskytte sig mod bestemte trusler.



Figur 22

Metoder til at få data tilbage efter angreb med ransomware



3. Konklusioner

Ud fra undersøgelsens resultater konkluderer Digitaliseringsstyrelsen og DKCERT, at borgerne på mange områder er godt dækket ind, når det gælder informationssikkerhed.

3.1. Sikkerhed på pc'en

Langt de fleste danskere holder programmerne på deres computere opdateret. De har også installeret sikkerhedssoftware i form af antivirus eller lignende. Dermed har de godt styr på nogle af de grundlæggende metoder til at begrænse risikoen.

Men på et enkelt område udsætter borgerne sig for en stor risiko: 61 procent tager ikke jævnligt sikkerhedskopi af data på deres computer. Dermed risikerer de at miste indscannede kvitteringer, familiefotos og e-mails, hvis computeren går ned eller bliver stjålet. Sikkerhedskopiering beskytter også mod tab som følge af brand, hvis sikkerhedskopien opbevares et andet sted end den computer, der går tabt i branden. Endvidere er sikkerhedskopiering den bedste beskyttelse mod konsekvenserne ved at være udsat for ransomware, se afsnit 3.5.

Andelen, der ikke tager backup, er uændret i forhold til de to tidligere år.

3.2. Sikkerhed på trådløse netværk

72 procent har beskyttet deres trådløse netværk i hjemmet med en adgangskode. Det er godt for sikkerheden – især hvis koden ikke er nem at gætte. Derfor kan det være udmærket, at halvdelen bruger den kode, de har fået udleveret fra deres internetudbyder. Det kræver blot, at udbyderne uddeler forskellige koder til kunderne og holder dem hemmelige.

Det kan være en sikkerhedsrisiko, når en fjerdedel anvender usikre trådløse netværk uden for hjemmet. Det er dog muligt, at nogle af borgerne bruger et VPN (virtuelt privat netværk), så kommunikationen alligevel bliver krypteret.

3.3. Sikkerhed på smartphones

Automatisk opdatering af apps er indbygget i smartphones og er typisk slået til som standard. Borgeren kan dog vælge at slå funktionen fra, og der er også situationer, hvor borgeren skal tage stilling til en foreslået opdatering. Alligevel er der kun lille risiko for, at angribere kan udnytte sårbarheder i apps, hvis brugeren ikke har opdateret dem.

Derimod er opdateringer til Android-operativsystemet en stor udfordring. Det skyldes, at det er op til de enkelte producenter at opdatere deres versioner af styresystemet. Så der kan gå måneder eller år, fra en rettelse til Android er tilgængelig, til den når ud til brugernes smartphones. I nogle tilfælde sker det aldrig. Det er et problem, som borgerne ikke kan gøre noget ved – ud over at vælge apparater fra producenter, der lægger vægt på at opdatere hurtigt.

39 procent har ikke installeret sikkerhedssoftware på deres smartphone. Det kan være et sikkerhedsproblem, men mængden af skadelig software til de mobile enheder er endnu begrænset.

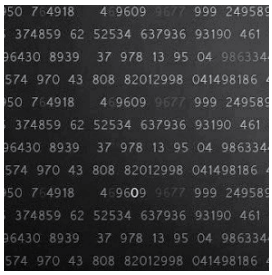
Et større problem ligger i, at 68 procent ikke tager sikkerhedskopi af data på deres smartphone. Efterhånden som en stadig større del af vores liv foregår på smartphones, er det store mængder data, vi risikerer at miste. Dog vil mange data i praksis befinde sig på cloud-systemer, som de forskellige apps kommunikerer med. Så selvom borgeren ikke selv tager backup, vil der ofte være adgang til data, hvis enheden går tabt.

3.4. Privatlivsbeskyttelse og datasikkerhed

83 procent af borgerne har tillid til, at det offentlige behandler deres fortrolige oplysninger sikkert og fortroligt. Andelen er uændret i forhold til 2014.

Andelen af borgere med tillid til behandlingen af data svarer i øvrigt til den andel, der anvender digitale selvbetjeningsløsninger.

Næsten hver femte borger (19 procent) er ikke klar over, at det er usikkert at sende data som e-mail. Det passer godt sammen med, at 21 procent har sendt deres cpr-nummer eller andre fortrolige oplysninger med ukrypteret e-mail.



3.5. Ransomware

Ransomware er fortsat en udbredt trussel, som har ramt 7 procent af de adspurgte. Ud fra svarene kan man konkludere, at det ikke kan betale sig at betale løsesummen: Ingen svarer, at de har fået deres data retur efter at have betalt. 4 procent af ofrene betalte, men fik intet ud af det.

Der er ét effektivt middel mod ransomware: Sikkerhedskopiering. Hvis man har en sikkerhedskopi, kan man gendanne de data, som ransomwaren har krypteret. Det understreger det kritiske problem, som borgernes manglende sikkerhedskopiering udgør.

Undersøgelsen underbygger også rådet om, at offeret under ingen omstændigheder bør betale den påkrævede løsesum. Det er kun med til at understøtte bagmændenes forretning, men er ingen garanti for, at man får sine data retur.

3.6. Den kommende generation

Borgerne er opmærksomme på, at deres børn har brug for hjælp til at lære at agere sikkert i den digitale hverdag. 82 procent lærer deres barn sikker adfærd på nettet, og 77 procent lærer barnet at beskytte personlige oplysninger.

Når opgaven bliver mere teknisk konkret, er andelen lidt mindre: 56 procent hjælper deres barn med at installere sikkerhedssoftware.

Det er meget positivt, at danskerne er blevet opmærksomme på behovet for at lære deres børn sikker adfærd og beskyttelse af privatlivet på nettet. Det kan være med til at gøre de kommende generationer mere sikre og trygge i deres digitale liv. Undersøgelsen tyder på, at mange forældre er opmærksomme på de holdningsmæssige aspekter, mens færre er i stand til at hjælpe med de mere teknisk krævende discipliner.

3.7. Opsamling

Overordnet set viser undersøgelsen ingen væsentlige ændringer i forhold til sidste års undersøgelse. Det store smertensbarn er stadig sikkerhedskopieringen.

En anden udfordring ligger i passwords. I takt med at stadig mere af borgernes liv finder sted på nettet, bliver der flere steder, hvor de opretter sig med brugernavn og adgangskode. Her er det sikkerhedsmæssigt uheldigt, når 57 procent bruger samme password til flere tjenester.

Ganske vist svarer 18 procent, at de kun bruger den samme kode til tjenester, som ikke opbevarer følsomme oplysninger. Men i praksis kan den skillelinje ændre sig – måske opfattede man ikke Facebook som en kritisk tjeneste, da man i sin tid tilmeldte sig, men siden da kan man have lagt fortrolige oplysninger ind, man kun ønsker at dele med sine venner.

Et godt supplement til passwords er to-faktor-autentifikation, hvor brugernavn og password suppleres med en engangskode. Det kan være i form af nøglekort, som det kendes fra NemID, eller engangskoder sendt som sms eller genereret af en app. Koden skal typisk anvendes, hver gang man forsøger at logge ind på en tjeneste fra en computer eller smartphone, man ikke før har brugt til den. Dermed kan det begrænse misbrug, hvor hackere har fået fat i eller gættet brugernavn og password.

Trods svaghederne inden for sikkerhedskopiering og passwordhåndtering har borgerne generelt et tilfredsstillende niveau inden for informationssikkerhed. De anvender sikkerhedssoftware, holder deres programmer opdateret og er klar over risikoen ved at klikke på links i mails, de får tilsendt uopfordret. De er også opmærksomme på konsekvenserne ved cookies og deling af informationer på sociale netværk.

Endelig kan man glæde sig over, at borgere med børn lægger sikker adfærd og beskyttelse af privatlivet på nettet ind som en del af opdragelsen.

4. Anbefalinger til borgerne

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

1. Brug sikkerhedssoftware som antivirus og firewall.
2. Hold programmer opdateret.
3. Tag sikkerhedskopi af dine data.
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.
6. Beskyt dit trådløse netværk med adgangskode.
7. Undgå at sende følsomme data over åbne trådløse netværk (netværk uden kryptering) eller via ukrypteret e-mail.
8. Brug VPN (virtuelt privat netværk), hvis du bruger åbne trådløse netværk.
9. Hvis du har brugt et åbent trådløst netværk, så sæt din telefon/computer til at glemme det bagefter.
10. Brug forskellige passwords til alle tjenester. Du kan evt. holde styr på dine passwords med et password manager-program.
11. Slå to-faktor-autentifikation til.
12. Indstil privatlivsindstillingerne på sociale netværk, så de passer til dine krav.
13. Oplys ikke fortrolige og personlige oplysninger på sociale netsteder, debatsider og chatrum.
14. Hjælp dine børn med at lære sikker adfærd i den digitale verden.

5. Kilder

Bjerg K: Det offentliges digitale overvågning 2015. Danskernes forståelse, holdninger og reaktioner.
http://bjergk.dk/det-offentliges-digitale-overvagning.pdf

DIGITALISERINGSSTYRELSEN

DKCERT

DeiC DANISH e-INFRASTRUCTURE COOPERATION