Digitaliseringstyrelsen
DKCERT
DeIC

Danskernes informationssikkerhed

Marts 2017

2016

DANSKERNES INFORMATIONSSIKKERHED

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

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

Copyright ©DeIC 2017

Indhold

Indhold

Indhold

1.
Resume

1. Resume

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

Denne rapport bygger på en undersøgelse, som Danmarks Statistik har gennemført i efteråret 2016 for Digitaliseringsstyrelsen og DKCERT. Undersøgelsen dækkede oplevelser med og kendskab til informationssikkerhed hos tre befolkningsgrupper: Offentligt ansatte, privatansatte og borgere.

1.1. Trusler

16 procent af de offentligt ansatte og 17 procent af de privatansatte har 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.

34 procent af borgerne havde oplevet mindst en af fire trusler mod informationssikkerheden: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data.

51 procent af de offentligt ansatte og 59 procent af de privatansatte har modtaget en mail med et tvivlsomt link, de blev opfordret til at klikke på.

33 procent af de offentligt ansatte, 28 procent af de privatansatte og 66 procent af borgerne 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.

27 procent af de offentligt ansatte, 33 procent af de privatansatte og 50 procent af borgerne anvender offentligt tilgængelige trådløse netværk uden kryptering. Det medfører risiko for, at uvedkommende får adgang til data og systemer.

1.2. Konsekvenser

96 procent af de offentligt ansatte, 98 procent af de privatansatte og 99 procent af de borgere, der var udsat for sikkerhedsproblemer, ændrede adfærd. Den hyppigste ændring var, at de holdt op med at åbne e-mails, der kom fra ukendte afsendere.

Derudover var det også udbredt at installere eller opgradere sikkerhedssoftware. Det gjorde 55 procent af de offentligt ansatte, 74 procent af de privatansatte og 82 procent af borgerne.

1.3. Foranstaltninger

Ni ud af ti offentligt ansatte beskytter deres computer med sikkerhedssoftware. Det samme gælder for to ud af tre borgere. Kun lidt over halvdelen af de offentligt ansatte og 26 procent af borgerne har sikkerhedssoftware på deres smartphone eller tablet-computer.

Kun ganske få af de ansatte falder for svindelforsøg såsom phishing. Fem procent af borgere lader sig narre af den type svindel.

28 procent af de privatansatte og 36 procent af de offentligt ansatte har adgang til single sign-on på deres arbejdsplads. Det letter brugen af sikre passwords. Derimod er brugen af password managers begrænset – det gælder også for borgerne.

33 procent af de offentligt ansatte og 60 procent af borgerne oplyser, at der ikke bliver taget sikkerhedskopi af deres data. Halvdelen af medarbejderne har sat sig ind i reglerne om informationssikkerhed på deres arbejdsplads. Seks procent af de offentligt ansatte og ni procent af de privatansatte undlader indimellem at overholde reglerne, fordi de opfattes som en hindring for at udføre arbejdet.

2.
Indledning

2. Indledning

Denne rapport belyser informationssikkerheden hos privatansatte, 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.

Rapporten bygger på en undersøgelse, som Danmarks Statistik foretog for Digitaliseringsstyrelsen og DKCERT i efteråret 2016. Undersøgelsen stillede en række spørgsmål til et repræsentativt udvalg af den voksne danske befolkning om deres erfaringer med informationssikkerhed. Undersøgelsen bygger på svar fra 2.284 personer i alderen 18-74 år.

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

- 669 offentligt ansatte
- 630 privatansatte
- 985 borgere

Størrelsen af grupperne medfører, at små svarprocenter bygger på ret få personer. Fx betyder en svar-andel på seks procent af de privatansatte, at 37 personer har givet det pågældende svar.

Danmarks Statistik udførte lignende undersøgelser for Digitaliseringsstyrelsen og DKCERT i 2013, 2014 og 2015. Disse undersøgelser handlede kun om borgerne som privatpersoner. Resultaterne fra de tidligere undersøgelser indgår i denne rapport under de punkter, hvor det er muligt og relevant at foretage en sammenligning.

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

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. 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 3.7).

3.3. 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 3.4.

3.4. 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.

3.5. 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.

3.6. 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.

3.7. 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.

3.8. 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.

3.9. 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[1].

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 3.8).

3.10. Passwords

Adgangen til mange it-systemer er beskyttet af kombinationen af et brugernavn og et password. 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 gerne sammensat af store og små bogstaver, tal og specialtegn. Det skal være mindst 12 tegn langt. Man kan med fordel følge anvisningerne i Passwordvejledning fra Center for Cybersikkerhed[2].

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 er det mere sikkert at bruge unikke passwords til alle tjenester.

1 Kent Lawson: Why Public WiFi Hotspots Are Trouble Spots for Users, http://blog.productcentral.aol.com/2013/03/10/public-wifi-hotspot-security/

2 Center for Cybersikkerhed: Passwordvejledning, https://fe-ddis.dk/cfcs/CFCSDocuments/Passwordvejledning_22092016.pdf

3.11. To-trinsbekræftelse

To-trinsbekræftelse 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 kende 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.

3.12. Lagring af passwords

Det kan være vanskeligt at huske unikke passwords til alle de tjenester, man anvender. En password manager 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 password managers 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.

3.13. 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. I nogle tilfælde 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 3.12). 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.

3.14. 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 en 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 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 3.8). 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.

3.15. 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.

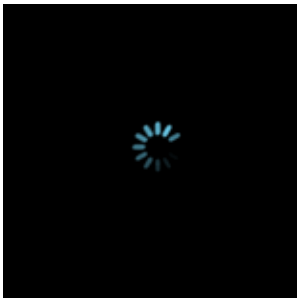
Automatisk opdatering af styresystemer og applikationer øger sikkerheden, men skal suppleres med manuel opdatering af de programmer, der ikke kan opdateres automatisk.

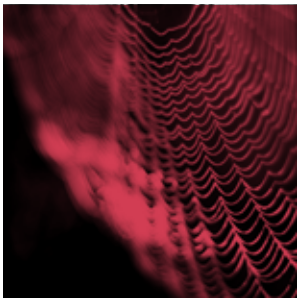
3.16. Sikkerhedskopiering

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 ransomwareprogram 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.

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 fx for nogle ansatte i sundhedssektoren. De vil derfor fx 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

16 procent har oplevet mindst en af fire trusler mod deres informationssikkerhed (se Figur 1):

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

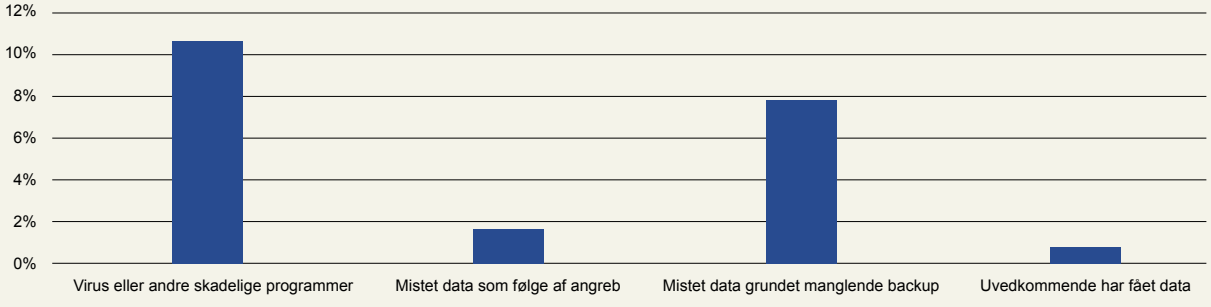
57 procent anmeldte sikkerhedsproblemet til it-funktionen på deres arbejdsplads.

Kun godt to procent har downloadet en skadelig app eller andet skadeligt indhold til deres smartphone eller tablet-computer.

Figur 1

Oplevede it-sikkerhedsproblemer

16 procent har oplevet mindst et af de fire sikkerhedsproblemer.



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. 96 procent havde foretaget et eller flere af følgende tiltag (se Figur 2):

a) 49 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) 55 procent har installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 66 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 53 procent har fået arbejdspladsens it-funktion til at hjælpe sig med at beskytte data og computer.
f) 85 procent har undladt at åbne mail, der kommer fra ukendte.

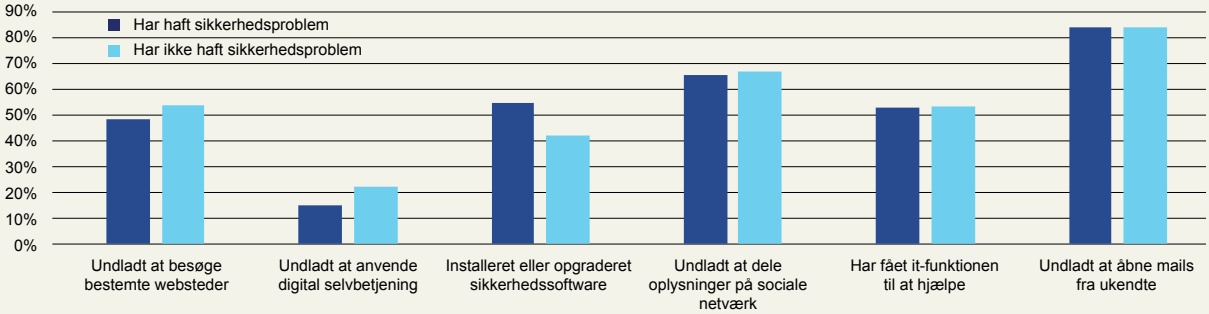
Vi spurgte også de medarbejdere, der ikke havde oplevet sikkerhedsproblemer, om de havde foretaget nogle af de samme handlinger for at forebygge problemer. Også her havde 96 procent foretaget tiltag.

a) 54 procent har undladt at besøge bestemte websteder.
b) 23 procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv Erhverv, digital post eller borger.dk).
c) 42 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) 53 procent har fået arbejdspladsens it-funktion til at hjælpe sig med at beskytte data og computer.
f) 84 procent har undladt at åbne mail, der kommer fra ukendte.

Figur 2

Handlinger for at forbedre sikkerheden

Både de, der var ramt af sikkerhedsproblemer, og de øvrige deltagere har foretaget handlinger for at forebygge sikkerhedsproblemer.



4.3. Ransomware

Seks procent af deltagerne var ramt af ransomware. De der var ramt af ransomware, blev spurgt, hvad de selv eller arbejdspladsens it-funktion gjorde for at få adgang til data igen (se Figur 3):

a) 33 procent fjernede spærringen med et sikkerhedsprogram og fik data tilbage.
b) 12 procent benyttede en sikkerhedskopi til at gendanne data.
c) 14 procent fik data tilbage på anden vis.
d) Syv procent fik ikke data tilbage.

Ingen svarede, at de har betalt den løsesum, som bagmændene krævede.

4.4. Ondsindede digitale beskeder - phishing

Mange trusler ankommer i form af digitale beskeder: E-mails, sms'er, chatbeskeder eller indlæg på sociale netværk. Ofte er et klik på et link første skridt på vej mod sikkerhedsproblemer. 68 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.

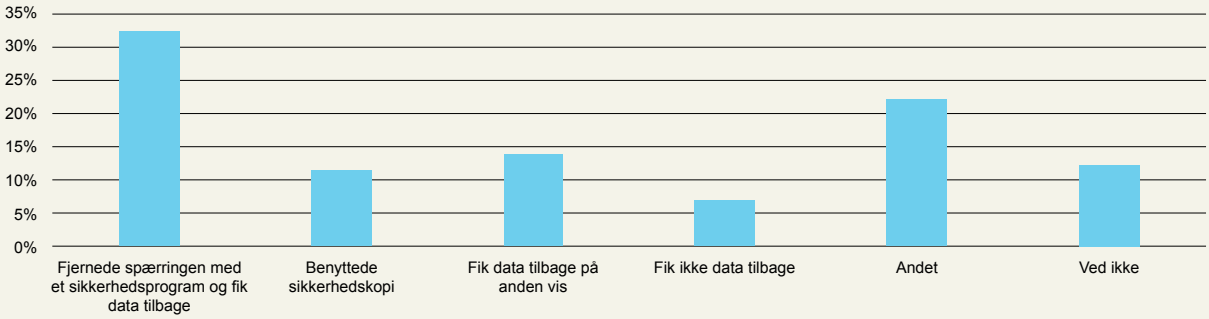
51 procent har modtaget sådan en mail. De reagerede på forskellig vis (se Figur 4):

a) En procent klikkede på linket.
b) To procent førte musen hen over linket for at se, hvor det førte hen. De klikkede på det, da det så ud til at være i orden.
c) 41 procent førte musen hen over linket for at se, hvor det førte hen. De klikkede ikke på det, da det virkede mistænkeligt.
d) 22 procent orienterede arbejdspladsens it-funktion.
e) 33 procent gjorde noget andetsendt uopfordret.

Figur 3

Metoder til at få data tilbage efter ransomwareangreb

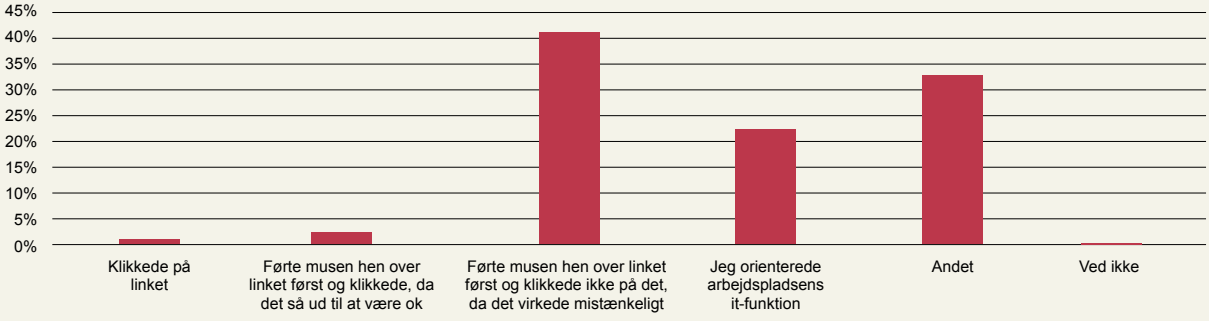
Kun syv procent af ofrene for ransomware får aldrig deres data tilbage.



Figur 4

Handlinger ved mail med tvivlsomt link

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



Den anden type skadelig besked, vi spurgte til, er phishing (se definitionen i afsnit 3.4).

32 procent havde modtaget en phishing-besked (se Figur 5).

a) 56 procent klikkede ikke på linket.
b) Fem procent klikkede på linket, men indtastede ikke de ønskede oplysninger.
c) Godt en procent klikkede på linket og indtastede de ønskede oplysninger.
d) 15 procent orienterede arbejdspladsens it-funktion.
e) 22 procent gjorde noget andet.

Figur 5

Handlinger ved phishing-mail

Kun få falder for phishing-svindel.

Endelig spurgte vi til direktørsvindel (se definitionen i afsnit 3.5). Syv procent havde modtaget en eller flere beskeder med direktørsvindel. De reagerede således (se Figur 6):

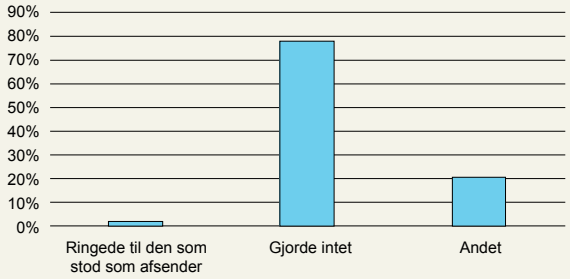
a) Knap to procent ringede til den, der stod som afsender, for at få bekræftet overførslen.
b) 78 procent gjorde intet.
c) 20 procent svarede ”Andet”.

Ingen svarede, at de overførte pengene. Heller ingen oplyste, at de gik i gang, men at overførslen blev standset.

Figur 6

Handlinger ved direktørsvindel.

Ingen af deltagerne faldt for direktørsvindel, hvor en falsk direktør prøvede at narre dem til at overføre penge til en konto i udlandet.



4.5. Falsk teknisk support

Ni procent har været ude for opkald fra falsk teknisk support (se definitionen i afsnit 3.6).

Modtagerne af opkald fra falsk teknisk support blev spurgt, hvordan de håndterede det (se Figur 7):

a) Tre procent begyndte at følge personens anvisninger, men blev mistænksomme og lagde på.
b) 84 procent afbrød samtalen og lagde på med det samme.
c) To procent stillede personen om til firmaets it-funktion.
d) Ni procent svarede "Andet".

Ingen svarede, at de fulgte personens anvisninger.

4.6. Brugernes adfærd

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

26 procent har sendt et cpr-nummer eller andre personlige oplysninger i e-mail til andre offentlige instanser. Det kan være et brud på persondataloven, da cpr-numre og andre fortrolige oplysninger skal krypteres. Det fremgår dog ikke af svarene, om der anvendes krypteret e-mail.

82 procent låser deres pc, når de forlader den, så andre ikke kan bruge den i deres fravær.

47 procent af deltagerne har mulighed for at tilgå arbejdspladsens systemer hjemmefra. 73 procent af dem anvender VPN (virtuelt privat netværk) til at beskytte kommunikationen (se definitionen i afsnit 3.8).

4.7. Beskyttelse af enheder

92 procent har sikkerhedsprogrammer såsom antivirus og firewall på arbejds-pc'en. Fire procent svarer nej, fire procent ved det ikke.

56 procent har sikkerhedsprogrammer på den smartphone eller tablet, de bruger på jobbet. 37 procent har det ikke, otte procent ved det ikke eller har ikke svaret.

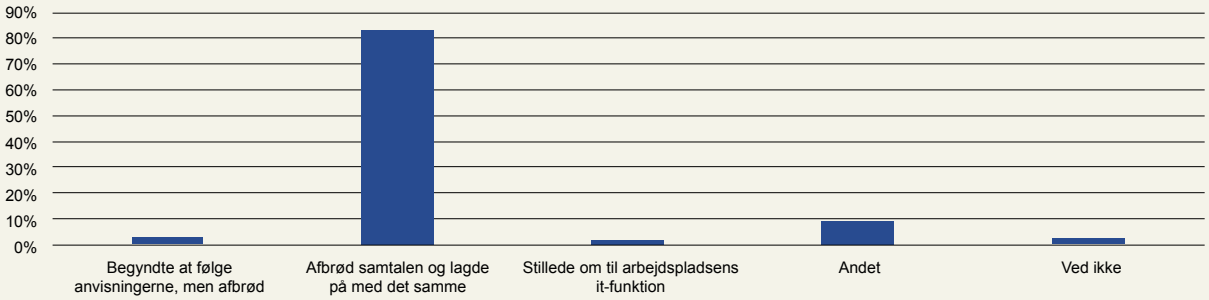
94 procent holder programmer på deres computer opdateret (se omtalen af softwareopdatering i afsnit 3.15). Det gør de således (se Figur 8):

a) Hos 83 procent sørger arbejdspladsens it-funktion for det.
b) 18 procent har slået automatisk opdatering til.
c) Otte procent opdaterer nogle programmer manuelt.
d) Otte procent opdaterer Java og Flash manuelt.

Figur 7

Handlinger ved falsk teknisk support-opkald.

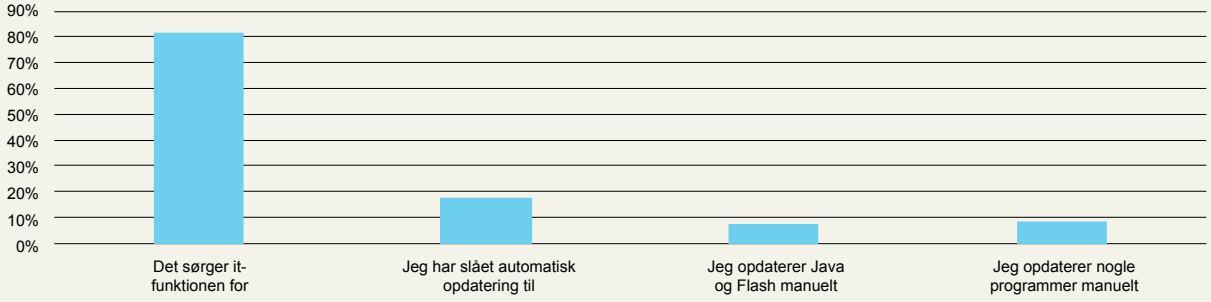
Otte ud af ti lægger røret på, når en falsk supporttekniker ringer op.



Figur 8

Sådan holdes software opdateret.

De fleste overlader det til it-funktionen at holde programmer på computere opdateret.



4.8. Trådløse netværk

82 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 3.9).

46 procent anvender trådløse netværk, når de er væk fra arbejdspladsen. Ud af dem anvender 27 procent også netværk, der ikke kræver en adgangskode og dermed er ukrypterede og usikre.

34 procent anvender trådløse netværk, hvor alle bruger samme adgangskode, fx på caféer og lignende.

46 procent anvender VPN (se definitionen i afsnit 3.8) til kommunikationen med arbejdet, når de bruger trådløse netværk uden for arbejdspladsen.

4.9. Sikkerhedskopiering

57 procent oplyser, at der bliver taget sikkerhedskopi af de data, vedkommende bruger i sit arbejde (se omtalen af sikkerhedskopiering i afsnit 3.16). 33 procent svarer nej, mens 10 procent ikke ved det.

Sikkerhedskopiering bliver varetaget på disse måder (se Figur 9):

a) Hos 85 procent sørger arbejdspladsens it-funktion for det.
b) Hos knap tre procent tager et eksternt firma sikkerhedskopi (fx med en cloud-løsning).
c) Syv procent tager selv sikkerhedskopi.
a) Fire procent svarer ”Andet”.

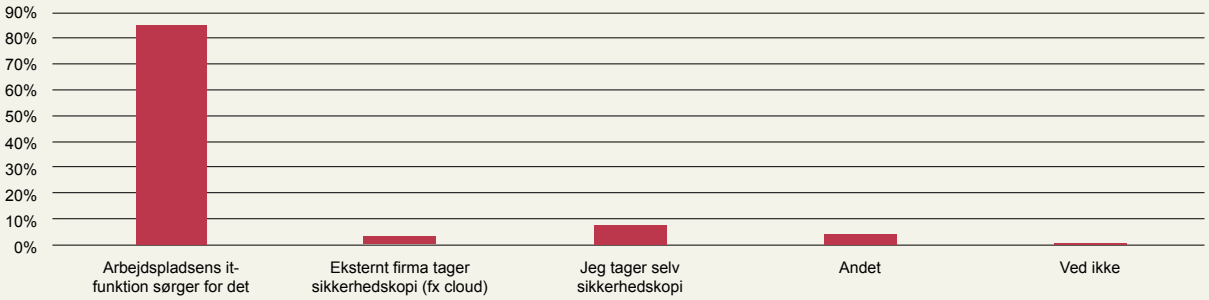
24 procent får taget sikkerhedskopi af data på smartphone eller tablet. 68 procent svarer nej, otte procent ved det ikke. Af dem der får taget sikkerhedskopi er metoderne fordelt således (se Figur 10):

a) Hos 58 procent sørger arbejdspladsens it-funktion for det.
b) Hos 14 procent tager et eksternt firma sikkerhedskopi (fx med en cloud-løsning).
c) 23 procent tager selv sikkerhedskopi.
b) Seks procent svarer ”Andet”.

Figur 9

Sikkerhedskopering

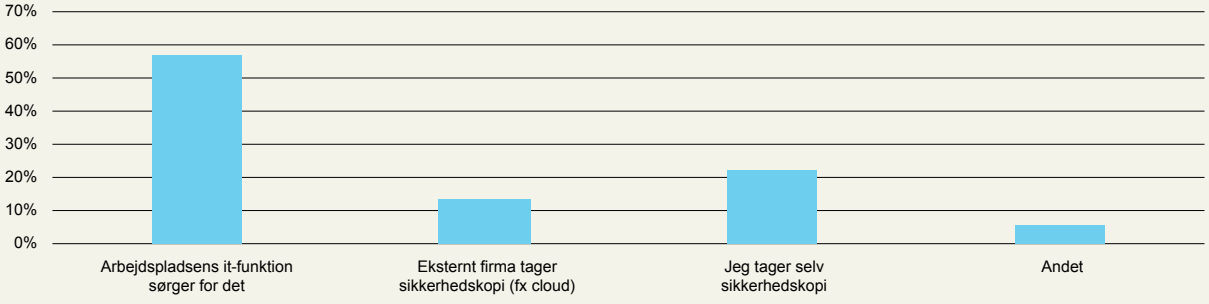
Hos de fleste sørger it-funktionen for at sikkerhedskopiere data.



Figur 10

Sikkerhedskopiering af smartphone/tablet

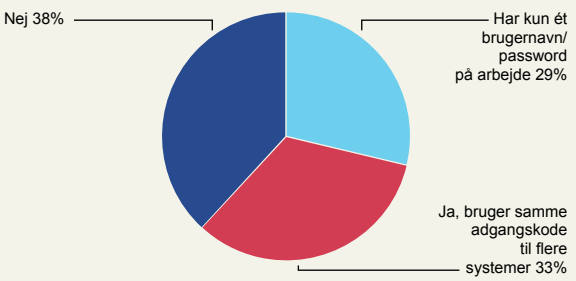
Kun hver fjerde medarbejder får taget sikkerhedskopi af data på smartphone/tablet-computer.



Figur 11

Samme adgangskode til flere systemer?

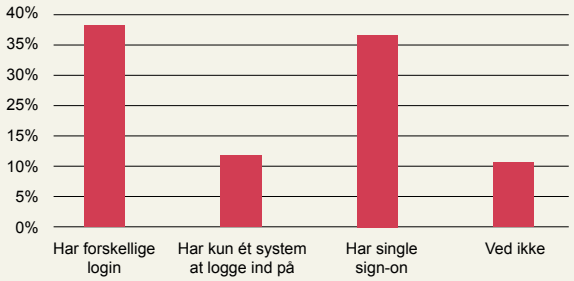
Hver tredje bruger samme adgangskode til flere systemer.



Figur 12

Single sign-on

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



4.10. Passwordsikkerhed

33 procent bruger samme adgangskode til flere systemer eller tjenester på arbejdet (se omtalen af passwordsikkerhed i afsnit 3.10-3.14). 29 procent har kun ét sæt brugernavn og password (se Figur 11).

Halvdelen af dem, der bruger samme password til flere systemer, gør det også ved systemer, der behandler følsomme data.

Endvidere oplyser 11 procent, at de er flere medarbejdere, der deles om samme passwords til fælles IT-systemer eller databaser (se definitionen af delte passwords i afsnit 3.14).

Vi har spurgt, om arbejdspladserne tilbyder single sign-on (se definitionen i afsnit 3.13). Det gør de hos 36 procent af medarbejderne, mens 38 procent har forskellige login. 13 procent har ikke brug for det, da de kun har et system, de skal logge ind på (se Figur 12).

25 procent lader deres browser lagre passwords (se definitionen i afsnit 3.12). 47 procent af dem oplyser, at disse passwords er beskyttet med en adgangskode, der skal indtastes, før man får adgang til dem.

Seks procent bruger en password manager til at opbevare og holde styr på passwords (se definitionen i afsnit 3.12). 59 procent af dem bruger en password manager, hvor data lagres krypteret og beskyttet med adgangskode.

29 procent bruger pinkode (et firecifret tal) til NemID i stedet for et password.

51 procent har en metode til at huske sikre passwords med.

Vi præsenterede deltagerne for en række forslag til passwords og spurgte, hvilket af dem der kan være sikkert:

a) pASSW0RD
b) 12345678
c) tuborg
d) sdli11ekk,Nheds0d (kan huskes som se den lille kattekilling, Nej hvor er den sød)

82 procent svarede d, som er det rigtige svar.

4.11. Sikkerhedsregler, kendskab og efterlevelse

48 procent har sat sig ind i it-sikkerhedspolitikken for deres arbejdsplads. 12 procent har været på kursus i it-sikkerhed.

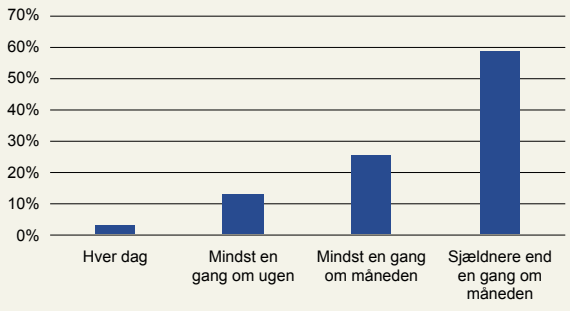
Men seks procent undlader nogle gange at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet. Vi spurgte dem, der indimellem gør det, hvor ofte det sker (se Figur 13):

a) Tre procent gør det hver dag.
b) 13 procent omgår reglerne mindst en gang om ugen.
c) 25 procent gør det mindst en gang om måneden.
d) Hos 59 procent sker det sjældnere end en gang om måneden.

Figur 13

Hvor ofte undlader du at følge sikkerhedsregler?

Seks procent af de offentligt ansatte føler sig indimellem nødsaget til at omgå sikkerhedsreglerne.



4.12. Delkonklusion om offentligt ansattes informationssikkerhed

4.13. Trusler

De offentligt ansatte i undersøgelsen oplever ikke alvorlige sikkerhedsproblemer i hverdagen. Kun 16 procent har været udsat for en af de fire trusler, vi har spurgt ind til. Her er topscoreren infektion med skadelige programmer, som 11 procent har været ramt af. Det tyder på, at arbejdspladserne har styr på de grundlæggende discipliner såsom antivirus og mailfiltrering.

Seks procent har været ramt af ransomware. Ingen af de ramte har betalt løsesum for at få adgang til data igen.

Otte procent har mistet data som følge af manglende backup. 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.

Hver tredje genbruger passwords, og 11 procent deles om passwords til bestemte systemer med deres kolleger.

51 procent har modtaget en mail med et mistænkeligt link. 32 procent har modtaget phishing-mails.

Den mobile hverdag medfører nye sikkerhedsrisici. Hver fjerde af de medarbejdere, der bruger trådløst netværk i embeds medfør, når de er væk fra arbejdspladsen, anvender usikre netværk (se omtalen af sikkerhed ved trådløse netværk i afsnit 3.9). Under halvdelen benytter sig af VPN (se definitionen i afsnit 3.8), 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. Uvedkommende får adgang til fortrolige data ved at udnytte usikre trådløse netværk.
4. Uvedkommende får adgang til fortrolige data og it-systemer, fordi medarbejdere genbruger og deler passwords.
5. Medarbejdere mister data som følge af manglende backup.

4.14. Konsekvenser

96 procent af dem, der har været udsat for et sikkerhedsproblem, har ændret adfærd.

85 procent har undladt at åbne mail, der kom fra ukendte afsendere. To ud af tre har undladt at dele oplysninger om sig selv på sociale netværk. Godt halvdelen har fået hjælp fra it-funktionen på deres arbejdsplads til at beskytte deres data og computer.

Tallene er næsten 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.

4.15. Foranstaltninger - adfærd

4.15.1. Beskyttelse af enheder

Ni ud af ti har sikkerhedsprogrammer på deres computer. Men når det gælder smartphones og tablet-computere, gælder det kun lidt over halvdelen af medarbejderne.

Generelt er medarbejderne opmærksomme på, at det er vigtigt at holde software på enhederne opdateret.

4.15.2. Forsvar mod svindel

De offentligt ansatte har generelt sunde vaner, når det gælder informationssikkerhed. De klikker ikke på et vilkårligt link, de får tilsendt i en mail eller sms. De tjekker, 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. Otte ud af ti husker også at låse computeren, når de går fra den.

4.15.3. Brug af passwords

På et område har medarbejderne dårlige vaner: En ud af tre bruger det samme password til flere tjenester (se afsnit 3.10 om risikoen ved genbrug af passwords).

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 3.13) eller en password manager (se definitionen i afsnit 3.12). Kun seks procent bruger en password manager – og knap halvdelen anvender øjensynlig en usikker version, der ikke krypterer de lagrede data.

4.15.4. Brug af trådløse netværk

Otte ud af ti bruger trådløse netværk på arbejdspladsen, der er sikret med kryptering. Det reelle tal kan være højere, hvis medarbejderen har sat sin enhed til at huske koden til nettet og derefter har glemt, at der oprindelig 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 udsætter de sig for risiko for aflytning. Dog bruger 46 procent VPN, der krypterer kommunikationen mellem deres computer og arbejdspladsens netværk.

4.15.5. Sikkerhedskopiering

33 procent svarer, at der ikke bliver taget sikkerhedskopi af deres data på computeren. Og kun hver fjerde bruger får taget sikkerhedskopi af data på smartphone/tablet.

4.15.6. Sikkerhedskultur

Informationssikkerhed er et kompromis mellem ønsket om sikkerhed og brugernes behov for at kunne udføre deres daglige arbejdsopgaver. Den balance ser det ud til, mange arbejdspladser opnår. Imidlertid føler seks procent af deltagerne sig nødsaget til indimellem at bryde reglerne for at gøre deres arbejde. De fleste af dem gør det dog kun sjældent.

5.
Privatansattes informationssikkerhed

5. Privatansattes informationssikkerhed

Dette kapitel belyser den aktuelle status for informationssikkerhed hos ansatte i det private erhvervsliv.

Ansatte i private virksomheder overlader typisk en del af ansvaret for informationssikkerhed til virksomhedens it-funktion. Derfor er der emner, det ikke giver mening at spørge dem om. Det gælder tekniske detaljer om installation af antivirus, firewall og backupsystemer. I stedet har vi fokuseret spørgsmålene på de områder, hvor medarbejderens adfærd kan forventes at have en betydning for sikkerheden.

Deltagerne i undersøgelsen blev instrueret i udelukkende at svare ud fra deres oplevelser på jobbet og ikke inddrage noget, der foregår uden for arbejdstiden.

5.1. Oplevede trusler

17 procent af de ansatte i det private erhvervsliv havde været ude for en eller flere af fire trusler mod deres informationssikkerhed (se Figur 14):

a) 11 procent har været ude for, at computeren var inficeret med virus eller andre typer skadelige programmer.
b) Fire procent har mistet data (fx filer, mails eller registerdata) som følge af et angreb.
c) Otte procent har mistet data som følge af manglende backup.
d) En procent har oplevet, at uvedkommende fik fat i data, vedkommende havde ansvaret for.

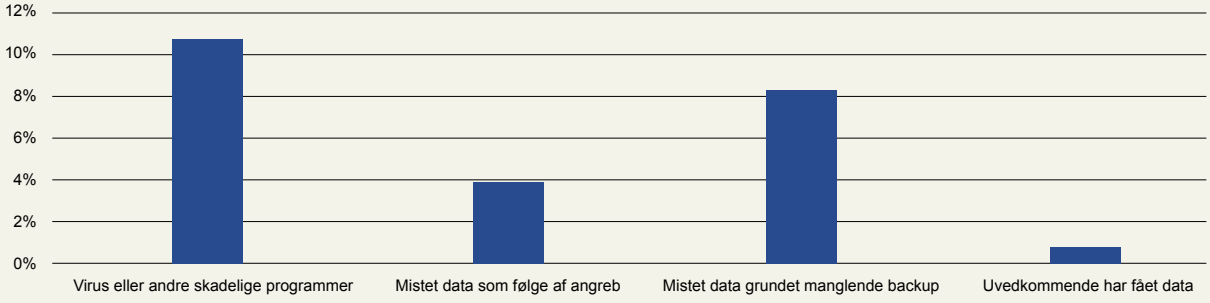
49 procent af dem, der havde været udsat for en af truslerne, anmeldte sikkerhedsproblemet til virksomhedens it-funktion.

Kun to procent har downloadet en skadelig app eller andet indhold til smartphone eller tablet-computer.

Figur 14

Oplevede it-sikkerhedsproblemer

17 procent har oplevet mindst et af de fire sikkerhedsproblemer.



5.2. Konsekvenser som følge af truslerne

Hos 98 procent af de ramte har sikkerhedstruslen haft konsekvenser for deres adfærd:

a) 63 procent har undladt at besøge bestemte websteder.
b) 21 procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv Erhverv, digital post eller borger.dk).
c) 74 procent har fået installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 69 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 55 procent har fået virksomhedens it-funktion til at hjælpe med at beskytte data og computer.
f) 86 procent har undladt at åbne mail, der kommer fra ukendte.

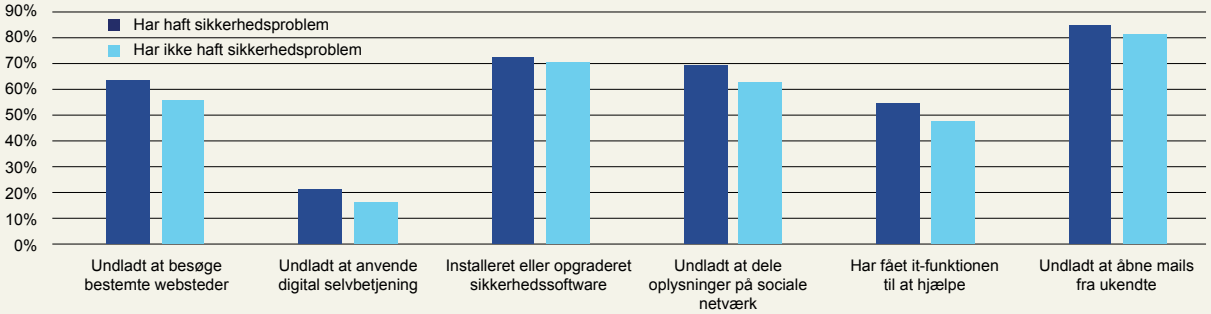
De samme spørgsmål blev stillet til alle medarbejdere, hvad enten de har oplevet et sikkerhedsproblem eller ej. 96 procent af dem har gjort et eller flere forebyggende tiltag for at forbedre it-sikkerheden (se Figur 15):

a) 56 procent har undladt at besøge bestemte websteder.
b) 16 procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv Erhverv, digital post eller borger.dk).
c) 71 procent har fået installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
d) 63 procent har undladt at dele oplysninger om sig selv på sociale netværk.
e) 47 procent har fået virksomhedens it-funktion til at hjælpe med at beskytte data og computer.
f) 82 procent har undladt at åbne mail, der kommer fra ukendte.

Figur 15

Handlinger for at forbedre sikkerheden

De medarbejdere der har været ramt af et sikkerhedsproblem er en smule mere forsigtige end hele gruppen af privatansatte.



5.3. Ransomware

Seks procent har været ramt af ransomware (se definitionen i afsnit 3.2). De der var ramt af ransomware, blev spurgt, hvad de selv eller arbejdspladsens it-funktion gjorde for at få adgang til data igen (se Figur 16):

a) 34 procent fjernede spærringen med et sikkerhedsprogram og fik data tilbage.
b) 32 procent benyttede en sikkerhedskopi til at gendanne data.
c) 10 procent fik data tilbage på anden vis.
d) Seks procent fik ikke data tilbage.
e) 13 procent svarede ”Andet”.
f) Fem procent ved ikke.

Ingen oplyste, at de havde betalt løsesummen.

5.4. Farlige beskeder

Ansatte i det private erhvervsliv modtager jævnligt digitale meddelelser med potentielt skadeligt indhold. Vi har spurgt om tre former for beskeder, man kan modtage via e-mail, sms eller chat.

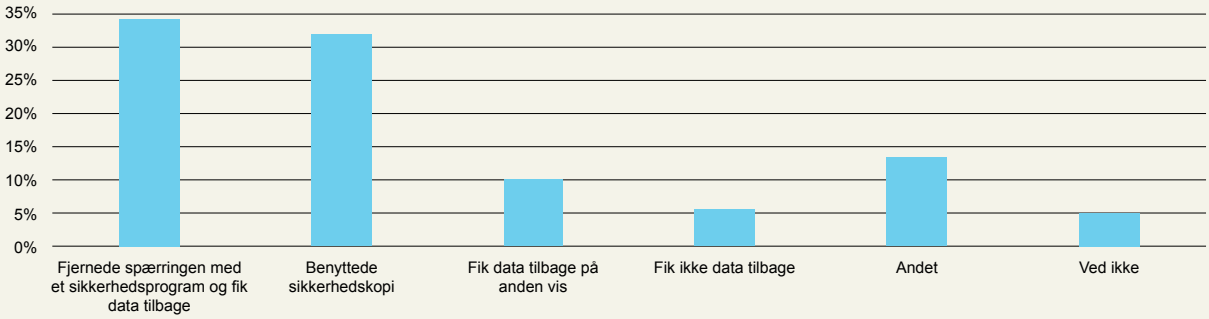
59 procent har modtaget en besked med et link, som modtageren opfordres til at klikke på. Modtagerne reagerede således (se Figur 17):

a) Tre procent klikkede på linket.
b) Tre procent førte musen hen over linket for at se, hvor det førte hen. De klikkede på det, da det så ud til at være i orden.
c) 39 procent førte musen hen over linket for at se, hvor det førte hen. De klikkede ikke på det, da det virkede mistænkeligt.
d) 23 procent orienterede arbejdspladsens it-funktion.
e) 32 procent svarede ”Andet”.

Figur 16

Metoder til at få data tilbage efter ransomwareangreb

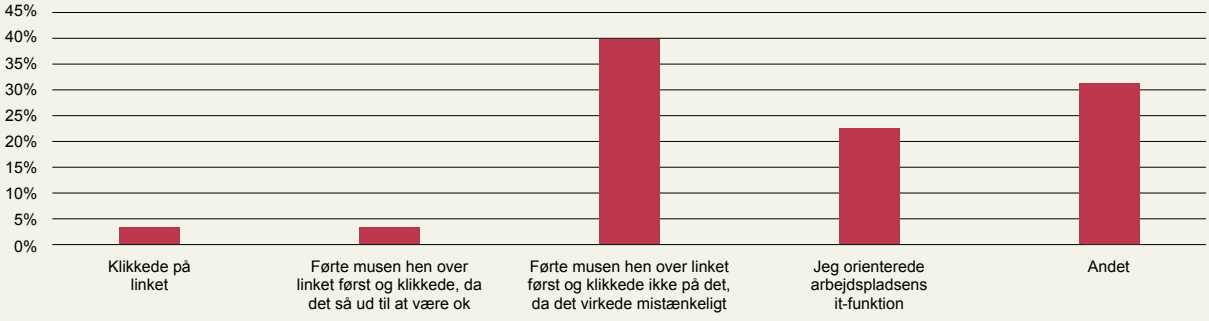
Mindst seks procent af ofrene for ransomware fik ikke data tilbage.



Figur 17

Handlinger ved mail med tvivlsomt link

De færreste klikker på links, de får tilsendt uopfordret.



Figur 18

Handlinger ved phishing-mail

Under en halv procent af modtagerne af phishing-mails afgav de oplysninger, svindlerne bad om.

40 procent har modtaget beskeder med forsøg på phishing (se definitionen i afsnit 3.4 samt Figur 18).

a) 50 procent klikkede ikke på linket.
b) Fem procent klikkede på linket, men indtastede ikke de ønskede oplysninger.
c) Næsten ingen klikkede på linket og indtastede de ønskede oplysninger.
d) 17 procent orienterede arbejdspladsens it-funktion.
e) 27 procent svarede ”Andet”.

Ni procent har været udsat for direktørsvindel (se definitionen i afsnit 3.5 og Figur 19).

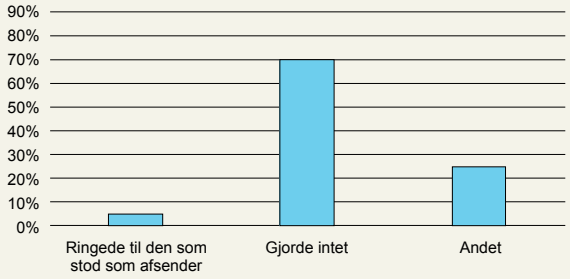
a) Fem procent ringede til den, der stod som afsender, for at få bekræftet overførslen.
b) 70 procent gjorde intet.
c) 24 procent svarede ”Andet”.

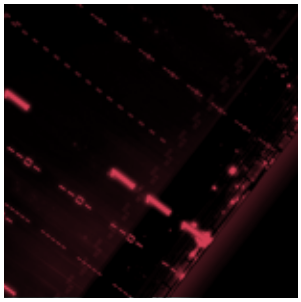
Ingen af deltagerne gik i gang med eller gennemførte pengeoverførslen.

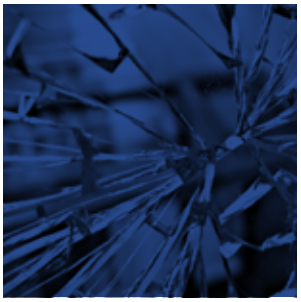
Figur 19

Handlinger ved direktørsvindel.

De fleste ignorerer forsøg på at narre dem til at overføre penge, selvom mailen ser ud til at komme fra en ledende medarbejder.








5.5. Falsk teknisk support

17 procent har været udsat for opkald fra falsk teknisk support (se definitionen i afsnit 3.6 og Figur 20).

Modtagerne af opkald fra falsk teknisk support håndterede det således:

a) 84 procent afbrød samtalen og lagde på med det samme.
b) To procent begyndte at følge personens anvisninger, men blev mistænksom og lagde på.
c) To procent stillede personen om til arbejdspladsens it-funktion.
d) 12 procent svarede "Andet".

Ingen fulgte svindlerens anvisninger helt igennem.

5.6. Brugernes adfærd

De ansattes adfærd i hverdagen har betydning for deres egen og virksomhedens informationssikkerhed. Derfor har vi stillet en række spørgsmål om, hvordan brugerne opfører sig i hverdagen.

15 procent har sendt et cpr-nummer eller andre personlige oplysninger i e-mail til offentlige instanser. Hvis det sker i en ukrypteret e-mail, kan det være et brud på persondataloven, da cpr-numre og andre fortrolige oplysninger skal krypteres.

69 procent låser deres pc, når de forlader den, så andre ikke kan bruge den i deres fravær.

53 procent kan tilgå systemerne på deres arbejdsplads hjemmefra. Hos 73 procent af dem er forbindelsen beskyttet med VPN (se definitionen i afsnit 3.8).

5.7. Trådløse netværk

84 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 sikkerhed i trådløse netværk i afsnit 3.9).

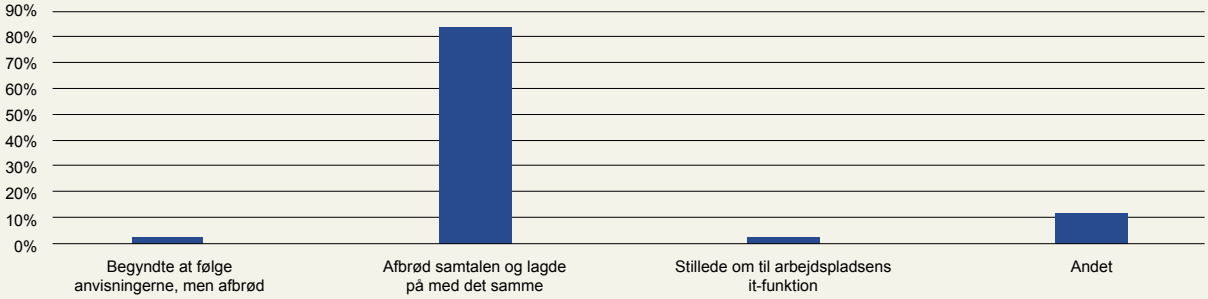
51 procent anvender trådløse netværk, når de er væk fra arbejdspladsen. Ud af dem anvender 33 procent også netværk, der ikke kræver en adgangskode og dermed er ukrypterede og usikre. 41 procent af dem anvender trådløse netværk, hvor alle bruger den samme adgangskode (fx på en café).

46 procent af dem, der bruger trådløse netværk uden for arbejdspladsen, anvender VPN (virtuelt privat netværk).

Figur 20

Handlinger ved falsk teknisk support-opkald.

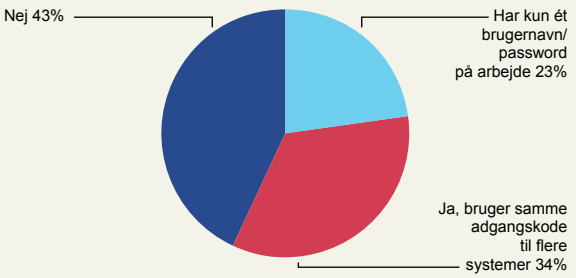
De fleste lægger straks røret på, når svindlere ringer til dem med besked om, at der er sikkerhedsproblemer med deres pc.



Figur 21

Samme adgangskode til flere systemer?

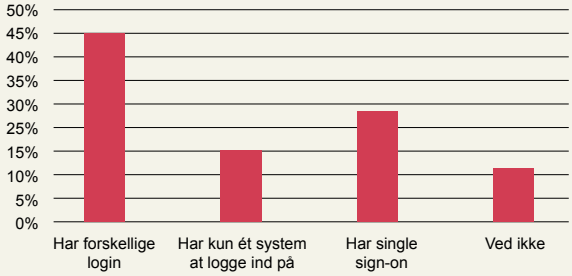
En tredjedel genbruger passwords.



Figur 22

Single sign-on

28 procent har et single sign-on-system, så de kun skal logge ind ét sted.



5.8. Passwordsikkerhed

34 procent bruger samme password til flere tjenester eller it-systemer (se omtalen af passwordsikkerhed i afsnit 3.10). 23 procent har ikke brug for det, da de kun har et sæt brugernavn og password på deres job (se Figur 21).

28 procent oplyser imidlertid, at de har single sign-on (se definitionen i afsnit 3.13) på arbejdspladsen (se Figur 22). De anvender altså sandsynligvis en sikker metode til genbrug af passwords. Hvis de ikke regnes med i dem, der genbruger passwords, er det 28 procent af de privatansatte, der genbruger passwords på en usikker måde.

Blandt dem der genbruger passwords, gør 36 procent det også til systemer, der indeholder data, som er følsomme for virksomheden.

22 procent oplyser, at de er flere medarbejdere, der deles om de samme passwords til fælles it-systemer eller databaser (se definitionen i afsnit 3.14).

Otte procent bruger en password manager (se definitionen i afsnit 3.12) til at opbevare og holde styr på passwords. 61 procent af dem bruger et program, hvor data lagres krypteret og beskyttet med adgangskode.

50 procent har en metode til at huske sikre passwords med.

5.9. Sikkerhedsregler, kendskab og efterlevelse

57 procent har sat sig ind i it-sikkerhedspolitikken for deres arbejdsplads. 14 procent har været på kursus i it-sikkerhed.

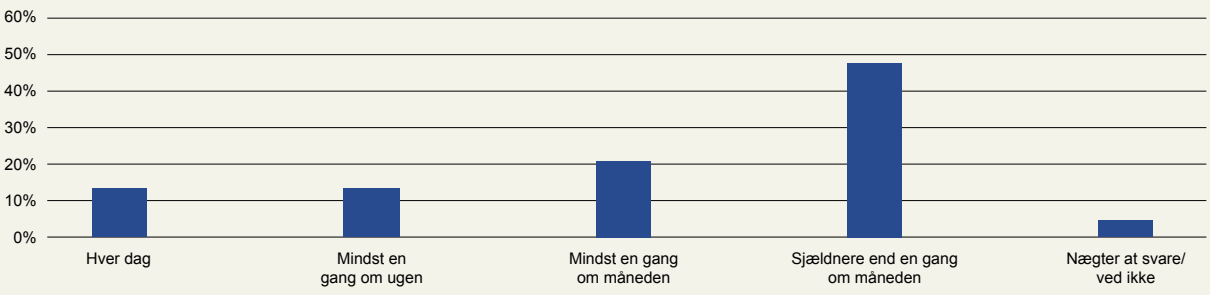
Men ni procent undlader nogle gange at følge sikkerhedsreglerne, fordi de gør det besværligt at udføre arbejdet. Vi spurgte, hvor ofte det sker (se Figur 23):

a) 13 procent gør det hver dag.
b) 13 procent omgår reglerne mindst en gang om ugen.
c) 21 procent gør det mindst en gang om måneden.
d) Hos 48 procent sker det sjældnere end en gang om måneden.

Figur 23

Hvor ofte undlader du at følge sikkerhedsregler?

Ni procent af ansatte i det private erhvervsliv omgår indimellem sikkerhedsreglerne.



5.10. Delkonklusion om privatansattes informationssikkerhed

5.11. Trusler

17 procent af de ansatte i det private erhvervsliv er udsat for sikkerhedsproblemer på arbejdspladsen. Skadelige programmer er den hyppigste trussel, de har ramt 11 procent. Seks procent har været ramt af ransomware, men ingen har betalt den krævede løsesum.

Otte procent har mistet data som følge af manglende backup.

28 procent genbruger passwords på en usikker måde. Oven i købet gør hver tredje af dem det også på systemer, der indeholder følsomme data.

22 procent deler passwords til visse systemer med deres kolleger. Det er især en risiko i forbindelse med medarbejdere, der forlader arbejdspladsen, men som fortsat kan få adgang til systemerne.

59 procent har modtaget mails med mistænkelige links, 40 procent har modtaget phishing-mails.

En tredjedel af brugerne af trådløse netværk uden for arbejdspladsen anvender usikre netværk. Sikkerhedsrisikoen her kan mindskes ved brug af VPN, men det bruger kun knap halvdelen.

Det samlede prioriterede trusselsbillede for privatansatte 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. Uvedkommende får adgang til fortrolige data ved at udnytte usikre trådløse netværk.
4. Uvedkommende får adgang til fortrolige data og it-systemer, fordi medarbejdere genbruger og deler passwords.
5. Medarbejdere mister data som følge af manglende backup.

5.12. Konsekvenser

98 procent af de medarbejdere, der har været ramt af sikkerhedsproblemer, har ændret adfærd som følge af oplevelsen.

Den hyppigste handling som konsekvens af et sikkerhedsproblem er at undlade at åbne mails fra ukendte afsendere. Tre ud af fire har også fået installeret eller opgraderet sikkerhedssoftware. 63 procent undlader at besøge bestemte websteder.

Tallene er på niveau med dem for alle medarbejdere, uanset om de har oplevet sikkerhedsproblemer.

5.13. Foranstaltninger - adfærd

5.13.1. Forsvar mod svindel

Medarbejderne kender til metoder til at beskytte sig mod udbredte former for svindel. De er klar over, at de skal være forsigtige med links i mails, de får tilsendt uden at have bedt om det. De færreste falder for phishing-svindel eller falske teknisk support-opkald.

5.13.2. Brug af passwords

28 procent anvender single sign-on-løsninger. Kun otte procent bruger en password manager.

5.13.3. Brug af trådløse netværk

Størstedelen af de trådløse netværk, medarbejderne har adgang til på arbejdspladsen, er beskyttet med kryptering. Men hver tredje af de medarbejdere, der bruger trådløse netværk uden for arbejdspladsen, anvender også usikre netværk. Dog beskytter knap halvdelen deres forbindelse med VPN.

5.13.4. Sikkerhedskultur

Lidt over halvdelen af medarbejderne har sat sig ind i reglerne om informationssikkerhed på deres arbejdsplads. Ni procent af medarbejderne føler sig imidlertid indimellem nødsaget til at bryde reglerne, fordi de gør det vanskeligt at udføre arbejdsopgaverne.

6.
Borgernes informationssikkerhed

6. 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 arbejdstiden. Nogle af spørgsmålene blev også stillet i de tre foregående undersøgelser af borgernes informationssikkerhed. Hvor det er relevant, sammenligner vi med svar fra de tidligere år for at vise udviklingen.

6.1. Oplevede trusler

34 procent af borgerne har oplevet en eller flere af fire specifikke trusler mod deres informationssikkerhed (se Figur 24):

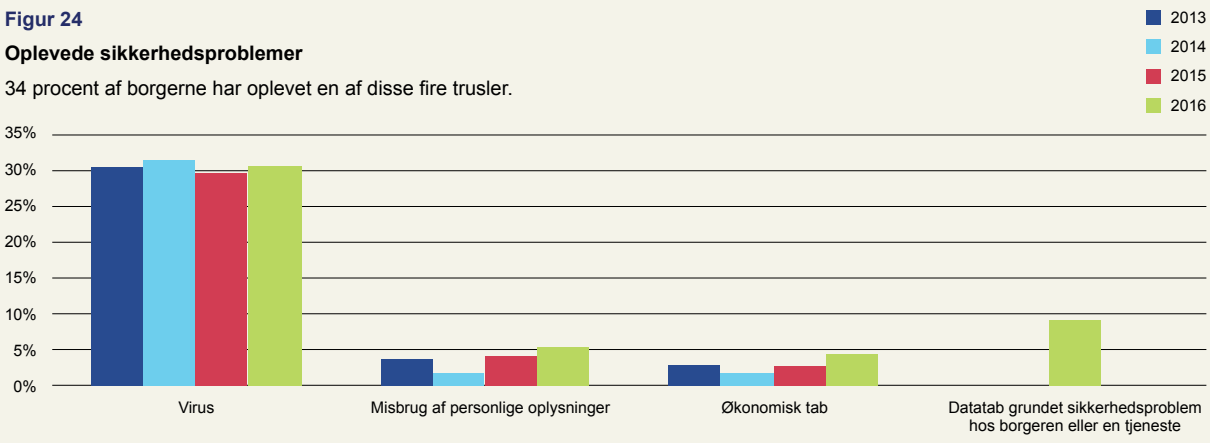
a) 31 procent har oplevet, at computeren var inficeret med virus eller andre typer skadelige programmer.
b) Seks procent har været ude for, at nogen har misbrugt deres personoplysninger på nettet.
c) Fem procent har mistet penge som følge af et it-sikkerhedsproblem.
d) Ni procent har mistet data som følge af et it-sikkerhedsproblem (fx et computernedbrud) hos dem selv eller hos en tjeneste på nettet.

Tallene ligner dem fra tidligere år, dog er der en lille stigning i økonomisk tab og misbrug af personlige oplysninger. Her kan ransomware være en medvirkende årsag, se afsnit 6.2. Vi har ikke tidligere spurgt om tab af data som følge af sikkerhedsproblemer.

Figur 24

Oplevede sikkerhedsproblemer

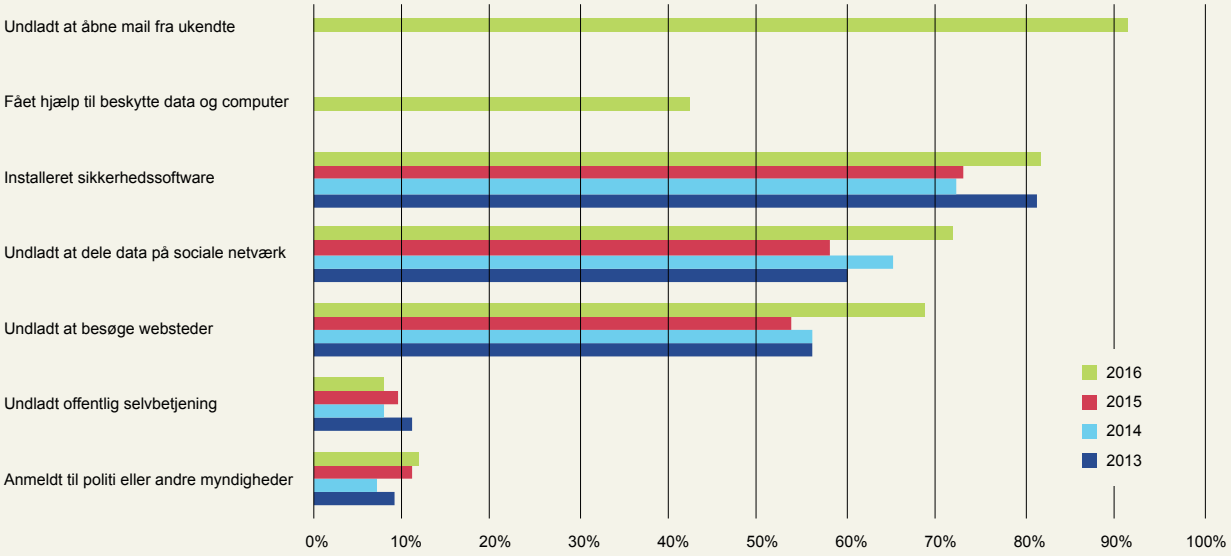
34 procent af borgerne har oplevet en af disse fire trusler.



Figur 25

Handlinger som følge af angreb

I forhold til tidligere års undersøgelser har vi tilføjet to mulige handlinger som følge af, at man har haft et sikkerhedsproblem: At undlade at åbne mails fra ukendte og at få hjælp fra andre.



De borgere, der havde oplevet en eller flere af de fire sikkerhedstrusler, blev spurgt, hvilke konsekvenser hændelsen havde for deres adfærd. 99 procent af dem havde gjort et eller flere tiltag for at mindske risikoen for yderligere problemer (se Figur 25).

a) 69 procent har undladt at besøge bestemte websteder.
b) Otte procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv, melde flytning, digital post eller borger.dk).
c) 82 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) 12 procent har anmeldt sikkerhedsproblemet til politi eller andre.
f) 42 procent har fået nogen til at hjælpe sig med at beskytte sine data og computer.
g) 91 procent har undladt at åbne mail, der kommer fra ukendte.

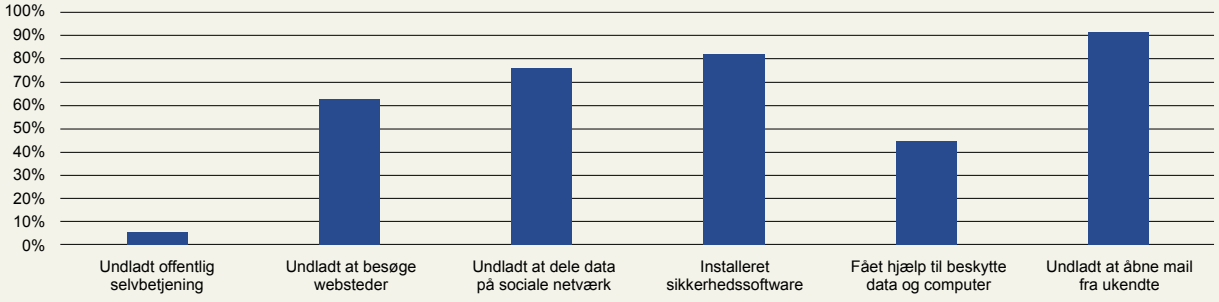
Vi spurgte også alle deltagere i undersøgelsen inklusive dem, der ikke havde oplevet sikkerhedsproblemer, om de havde foretaget nogle af de samme handlinger for at forebygge problemer. Det havde 56 procent (se Figur 26).

a) Seks procent har undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat TastSelv, melde flytning, digital post eller borger.dk).
b) 63 procent har undladt at besøge bestemte websteder.
c) 76 procent har undladt at dele oplysninger om sig selv på sociale netværk.
d) 82 procent har installeret eller opgraderet sikkerhedssoftware (fx antivirus eller firewall).
e) 45 procent har fået nogen til at hjælpe sig med at beskytte sine data og computer.
f) 92 procent har undladt at åbne mail, der kommer fra ukendte.

Figur 26

Forebyggelse af it-sikkerhedsproblemer

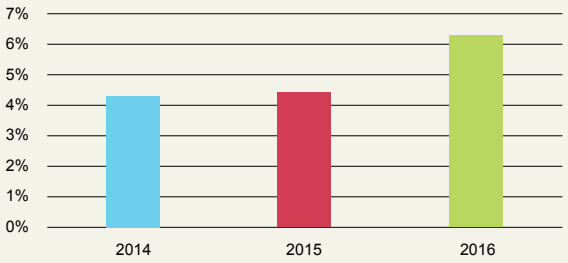
Borgerne er forsigtige med at åbne e-mails fra ukendte afsendere.



Figur 27

Har downloadet skadeligt indhold til smartphone/tablet

Lidt flere møder trusler på deres smartphone eller tablet-computer.



Seks procent har downloadet en skadelig app eller andet skadeligt indhold til deres smartphone eller tablet-computer. Det er en lille stigning i forhold til tidligere år (se Figur 27).

6.2. Ransomware

Otte procent har været ramt af ransomware (se definitionen i afsnit 3.2). Det er på niveau med 2015, hvor ransomware ramte syv procent.

Mindst otte procent af de ramte fik ikke deres data tilbage (se Figur 28). Tre procent betalte løsesummen og fik data tilbage – mens knap en procent betalte løsesummen uden at få data tilbage. I 2015 var det fire procent, der betalte uden at få frigivet deres data.

6.3. Ondsindede beskeder – phishing

58 procent har modtaget e-mails med forsøg på phishing (se definitionen i afsnit 3.4). Men kun fem procent af dem indsendte de ønskede oplysninger.

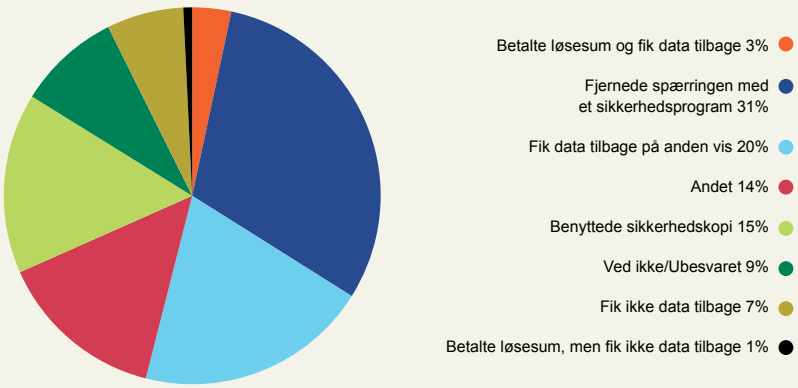
Hvis man modtager en mail med et link, kan man føre musemarkøren hen over det uden at klikke. Så viser browseren den adresse, et klik på linket vil føre til. Den metode anvender 56 procent af borgerne til at tjekke links, før de klikker.

27 procent har sendt cpr-nummer eller andre personlige oplysninger i e-mail til det offentlige. 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.

Figur 28

Ofre for ransomware

Mindst otte procent af ofrene for ransomware fik ikke deres data tilbage.



6.4. Hjælp til børn

Et flertal af de borgere, der har børn i alderen 5-16 år, hjælper deres børn med at få bedre informationssikkerhed (se Figur 29). For de tre spørgsmåls vedkommende, som vi også stillede i 2015, er der tale om en lille stigning.

a) 87 procent hjælper barnet med at beskytte dets privatliv på nettet (fx ved ikke at lægge private billeder ud offentligt).
b) 86 procent hjælper barnet med at lære sikker adfærd på nettet (fx ved ikke at indgå aftaler med fremmede uden at spørge forælderen først).
c) 64 procent hjælper barnet med at installere sikkerhedssoftware (fx antivirus).
d) 75 procent hjælper barnet med at lære, at nogle mails forsøger at lokke private oplysninger ud af barnet.
e) 86 procent hjælper barnet med at beskytte telefon, tablet eller pc med en sikker adgangskode.

6.5. Beskyttelse af enheder

66 procent låser deres pc, når de forlader den, så andre ikke kan bruge den i deres fravær.

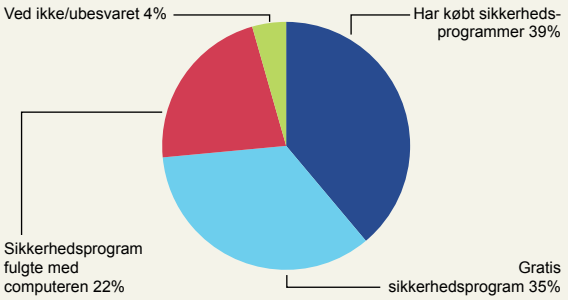
66 procent beskytter deres pc med sikkerhedsprogrammer såsom antivirus og firewall. 16 procent har ikke besvaret spørgsmålet eller ved ikke, om de har sikkerhedssoftware på deres pc.

22 procent af brugerne af sikkerhedsprogrammer anvender den software, som fulgte med, da de købte computeren. 39 procent har selv købt sikkerhedssoftware, mens 35 procent bruger gratis programmer (se Figur 30).

Figur 30

Hvordan har du anskaffet dit sikkerhedsprogram?

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



26 procent beskytter deres smartphone og/eller tablet-computer med sikkerhedsprogrammer såsom antivirus. 53 procent oplyser, at de ikke beskytter enheden og data på den. 21 procent ved ikke, om de har sikkerhedssoftware på enheden.

Sikkerhedssoftware til smartphone/tablet-computer er fordelt med 33 procent gratis software, 32 procent købeprogrammer og 31 procent software, der fulgte med ved køb af enheden.

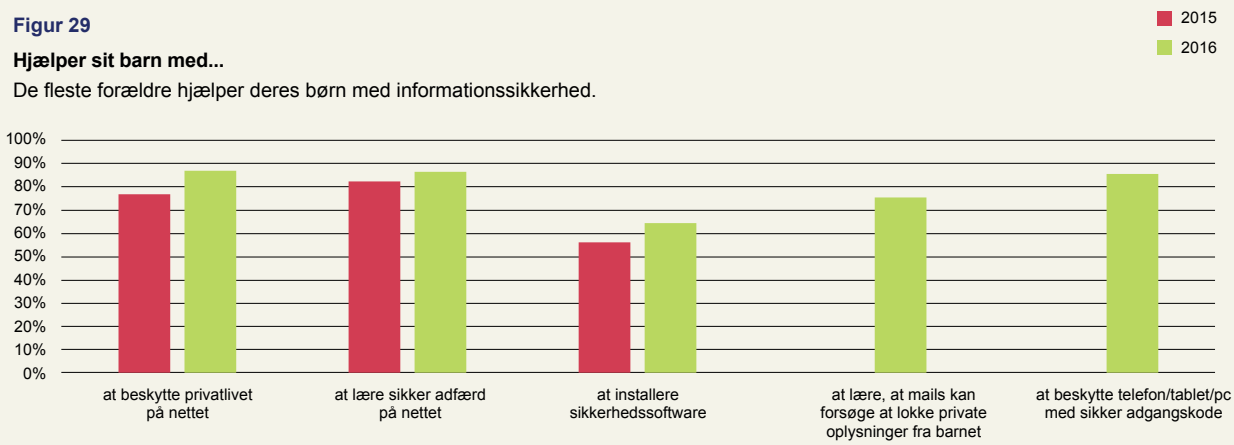
89 procent holder programmer på deres computer opdateret (se omtalen af softwareopdatering i afsnit 3.15). Det gør de således:

a) 76 procent har slået automatisk opdatering til.
b) 65 procent opdaterer nogle programmer manuelt.
c) 61 procent opdaterer Java og Flash manuelt.

Figur 29

Hjælper sit barn med...

De fleste forældre hjælper deres børn med informationssikkerhed.

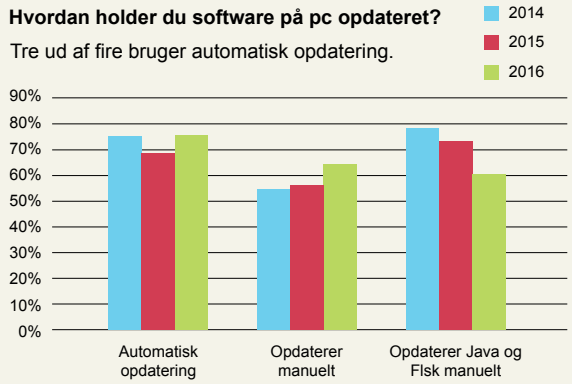


Tallene ligger på niveau med tidligere år (se Figur 31). Dog er der færre, der svarer, at de opdaterer Java og Flash manuelt. Til dette spørgsmål svarede 14 procent ved ikke. Det er muligt, at færre anvender Java og Flash, blandt andet fordi NemID ikke længere kræver Java.

Figur 31

Hvordan holder du software på pc opdateret?

Tre ud af fire bruger automatisk opdatering.



6.6. Trådløse netværk

93 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 3.9). Der har været en stigende andel af sikrede trådløse net i de tre år, vi har stillet spørgsmålet (se Figur 32).

Halvdelen af borgerne har selv lavet adgangskoden til nettet, mens den anden halvdel bruger 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.

66 procent anvender trådløse netværk uden for hjemmet. Ud af dem anvender 50 procent netværk, der ikke kræver en adgangskode og dermed er ukrypterede og usikre (se Figur 33).

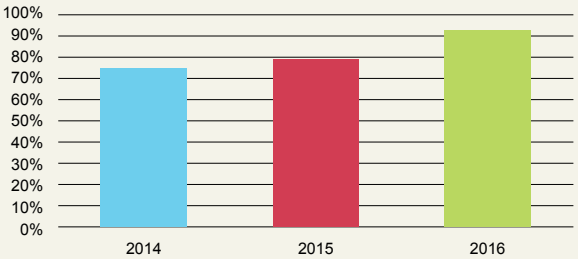
58 procent af dem bruger trådløse netværk, hvor alle bruger den samme adgangskode (fx på en café).

25 procent anvender VPN (se definitionen i afsnit 3.8), når de bruger trådløse netværk uden for hjemmet.

Figur 32

Trådløs net med adgangskode i hjemmet

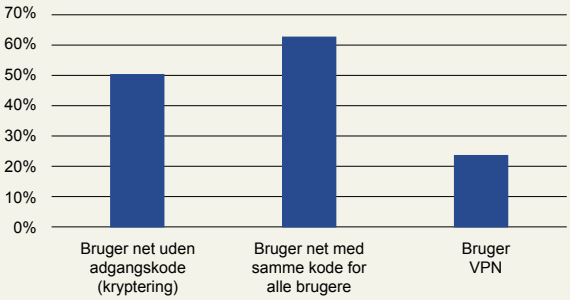
Ni ud af ti anvender sikre trådløse netværk i hjemmet.



Figur 33

Brugere af trådløse net uden for hjemmet

Hver fjerde bruger af trådløse netværk uden for hjemmet anvender et VPN (virtuelt privat netværk) til at sikre kommunikationen.



6.7. Sikkerhedskopiering

40 procent tager jævnligt sikkerhedskopi af data på deres computer. Det er en lille stigning i forhold til tidligere år (se omtalen af sikkerhedskopiering i afsnit 3.16 og Figur 34).

De borgere, der tager sikkerhedskopi, anvender disse metoder (se Figur 35):

a) 80 procent tager kopi til ekstern harddisk/USB-nøgle.
b) 52 procent tager backup på nettet (cloud).
c) Otte procent brænder data på cd/dvd.
d) 10 procent svarer "Andet".

Den største udvikling her er på cloud-siden, hvor andelen er fordoblet på et år. Tallene giver sammenlagt mere end 100 procent, fordi nogle brugere kombinerer flere backupmetoder.

30 procent tager sikkerhedskopi af data på deres smartphone eller tablet. Det er uændret i forhold til tidligere år.

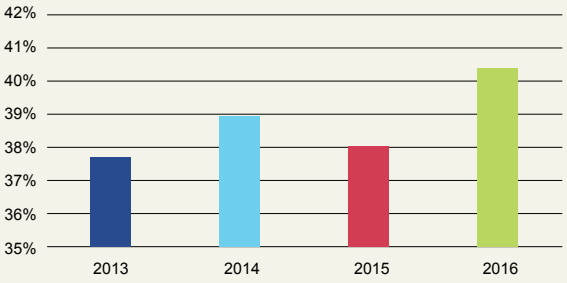
De der tager backup, anvender disse metoder (se Figur 36):

a) 27 procent tager kopi til ekstern harddisk/USB-nøgle
b) 75 procent tager backup på nettet (cloud)
c) Fire procent brænder data på cd/dvd
d) 50 procent tager kopi til en computer
e) Otte procent svarer "Andet".

Figur 34

Tager sikkerhedskopi af data på pc

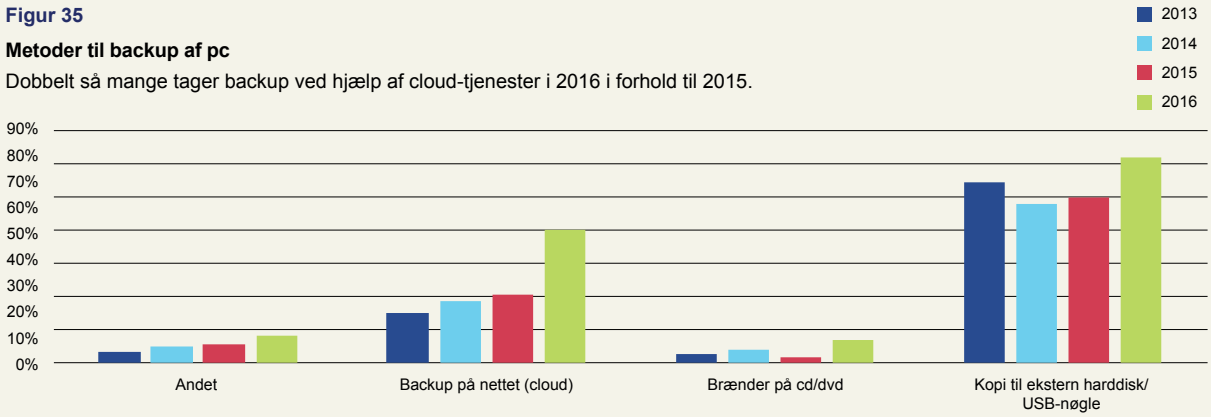
Fire ud af ti borgere tager jævnligt sikkerhedskopi af deres data.



Figur 35

Metoder til backup af pc

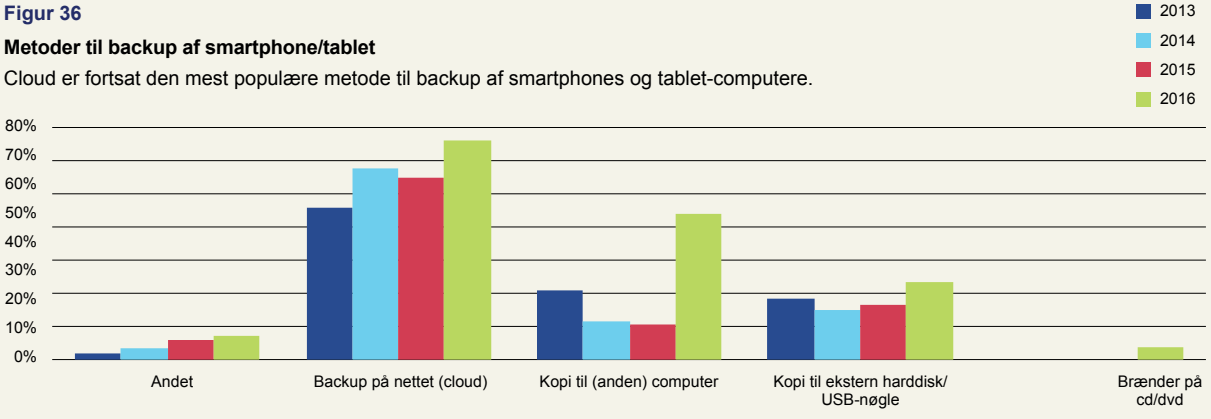
Dobbelt så mange tager backup ved hjælp af cloud-tjenester i 2016 i forhold til 2015.



Figur 36

Metoder til backup af smartphone/tablet

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



6.8. Sociale medier

77 procent har en profil på et eller flere sociale medier såsom Facebook, LinkedIn, Twitter, Instagram og lignende. 27 procent af brugerne har læst privatlivspolitikken for det sociale medie. 74 procent har manuelt indstillet privatlivsindstillingerne. Disse andele er uændrede i forhold til tidligere år (se Figur 37).

18 procent deler personlige oplysninger på den åbne del af mediet – for eksempel ved at gøre opslag offentligt tilgængelige. Der er ikke tal fra tidligere år at sammenligne med.

6.9. Passwordsikkerhed

66 procent anvender samme adgangskode til flere tjenester (se omtalen af passwords i afsnit 3.10). 22 procent svarer dog, at de kun gør det for tjenester, der ikke håndterer følsomme data (se Figur 38). Mængden af borgere der anvender samme adgangskode er steget siden 2015, især fordi flere kun gør det til tjenester, de ikke mener håndterer følsomme data.

45 procent lader deres browser lagre passwords (se definitionen i afsnit 3.12). 48 procent af dem oplyser, at disse passwords er beskyttet med en adgangskode, der skal indtastes, før man får adgang til dem.

Ti procent bruger en password manager (se definitionen i afsnit 3.12) til at opbevare og holde styr på passwords. 68 procent af dem bruger et program, hvor data lagres krypteret og beskyttet med adgangskode.

75 procent bruger pinkode (et firecifret tal) til NemID i stedet for et password.

47 procent har en metode til at huske sikre passwords med.

Vi præsenterede deltagerne for en række forslag til passwords og spurgte, hvilket af dem der kan være sikkert:

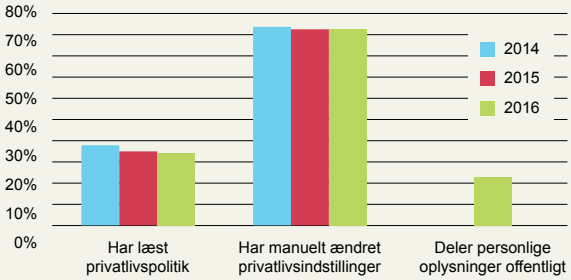
a) pASSW0RD
b) 12.345.678
c) tuborg
d) Fo!85_XcQ4

85 procent svarede d, som er det rigtige svar.

Figur 37

Brugere af sociale medier

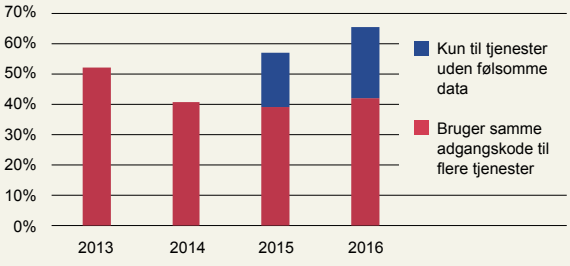
Få læser privatlivspolitikken, men tre ud af fire ændrer aktivt privatlivsindstillingerne på sociale medier.



Figur 38

Bruger samme adgangskode til flere tjenester

To ud af tre borgere bruger den samme adgangskode til flere systemer eller tjenester.



6.10. 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 87 procent tillid til, at myndighederne håndterer deres personlige oplysninger med den nødvendige fortrolighed og sikkerhed. Graden af tillid fordeler sig således (se Figur 39):

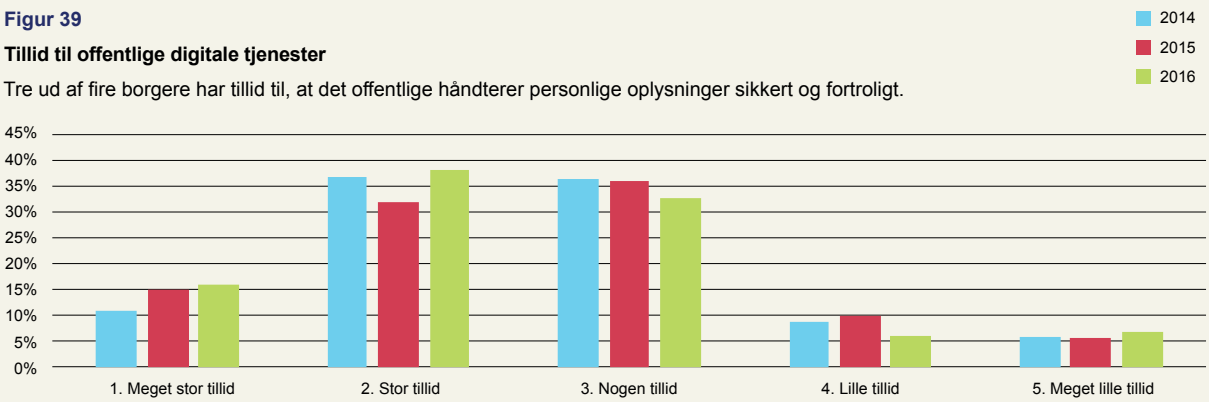
a) 16 procent har meget stor tillid.
b) 38 procent har stor tillid.
c) 33 procent har nogen tillid.
d) Seks procent har lille tillid.
e) Syv procent har meget lille tillid.

Andelene er stort set uændrede i forhold til 2015.

Figur 39

Tillid til offentlige digitale tjenester

Tre ud af fire borgere har tillid til, at det offentlige håndterer personlige oplysninger sikkert og fortroligt.



6.11. Delkonklusion om borgernes informationssikkerhed

6.12. Trusler

Virus og lignende skadelige programmer er den hyppigste trussel, borgerne er udsat for. Det er uændret i forhold til tidligere år. Knap hver tredje har haft infektioner med skadelig software.

Seks procent har haft skadeligt indhold på deres smartphone eller tablet-computer, det er lidt flere end i de foregående år.

Ransomware ramte otte procent, det er på niveau med tidligere år.

58 procent har modtaget e-mails med forsøg på phishing-svindel, men kun fem procent af dem faldt for svindlen.

Ni procent har mistet data som følge et sikkerhedsproblem hos dem selv eller en tjeneste på nettet. En del af tallet kan dække over tab som følge af manglende sikkerhedskopiering.

Over halvdelen bruger samme password til flere tjenester. Dermed udsætter de sig for en sikkerhedsrisiko, hvis hackere får adgang til en af tjenesterne.

Halvdelen af dem, der bruger trådløse netværk uden for hjemmet, bruger usikre netværk. Dog beskytter 25 procent sig med VPN (virtuelt privat netværk).

Det samlede prioriterede trusselsbillede for borgerne ser således ud:

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

6.13. Konsekvenser

99 procent af de borgere, der oplevede sikkerhedsproblemer, ændrede adfærd.

91 procent 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 hyppig var at installere eller opgradere sikkerhedssoftware, det gjorde 82 procent.

72 procent undlod at dele oplysninger om sig selv på sociale medier, og 69 procent holdt sig væk fra bestemte websteder. Tallene er typisk lidt højere end i tidligere år.

6.14. Foranstaltninger - adfærd

6.14.1. Beskyttelse af enheder

To ud af tre låser deres pc, når de forlader den. En tilsvarende andel beskytter computeren med sikkerhedssoftware.

Derimod er det kun 26 procent, der har sikkerhedssoftware på deres smartphone eller tablet-computer.

89 procent holder programmerne på computeren opdateret.

6.14.2. Forsvar mod svindel

Tre ud af fire er klar over, hvordan de kan se, hvor et link fører hen, før de klikker på det. Selvom mange modtager e-mails med forsøg på phishing-svindel, er det kun fire procent af dem, der falder for svindlen og indsender de ønskede oplysninger.

6.14.3. Brug af passwords

De fleste kan genkende et stærkt password, når de ser det. Men de er mindre gode til at bruge unikke passwords til alle tjenester. En del af forklaringen kan være, at programmer af typen password manager er meget lidt udbredte. Kun otte procent bruger en password manager.

En anden mulig forklaring kan være, at brugerne har så stor tillid til systemer, der tilbyder to-trinsbekræftelse, at de bruger samme password til flere tjenester. Det kunne være ud fra en ide om, at engangskoden på nøglekortet eller via sms'en alligevel er unik. En række tjenester anvender dog kun to-trinsbekræftelse til visse typer af transaktioner. I de tilfælde er et unikt password stadig nødvendigt for at beskytte adgang til data.

6.14.4. Brug af trådløse netværk

93 procent beskytter deres trådløse netværk i hjemmet med kryptering. Tallet er steget løbende gennem de tre år, vi har spurgt til emnet, det var 75 procent i 2014.

6.14.5. Sikkerhedskopiering

Sikkerhedskopiering har været en udfordring i alle de år, vi har gennemført undersøgelsen. I år var der en forbedring på et par procentpoint, idet 40 procent tager backup af data på deres pc. Så seks ud af ti danskere må forvente at miste data, hvis deres pc går i stykker eller bliver overtaget af ransomware.

6.14.6. Sikkerhedskultur

De fleste borgere hjælper deres børn med at lære om it-sikkerhed og hvordan de beskytter sig mod trusler.

7.
Perspektivering

7. Perspektivering

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

7.1. Skadelig software

Danskerne er mere udsatte for skadelig software i hjemmet end på arbejdspladsen. Både blandt offentligt ansatte og privatansatte har 11 procent været ude for et virusangreb, hvor andelen er 31 procent af borgerne.

Internationale undersøgelser af skadelig software viser, at Danmark generelt ligger i den gode ende. Således fandt Microsofts månedlige sikkerhedstjek skadelig software på kun 3,1 promille af computerne i Danmark i andet kvartal 2016[3]. På verdensplan var gennemsnittet 8,8 promille. 92,3 procent af computerne i Danmark er ifølge Microsofts data beskyttet med antivirus. Andelen er stigende, for to år siden var det 79,8 procent.

7.2. Phishing

Ifølge vores undersøgelse er danskerne generelt gode til at genkende og undgå phishing-svindel. Men tal fra Finansrådet viser, at en del danskere alligevel falder for svindelnumrene og udleverer deres NemID-engangskoder til it-kriminelle[4]. I de første tre kvartaler af 2016 registrerede Finansrådet 972 forsøg på phishing og lignende. 203 af forsøgene lykkedes og medførte økonomisk tab.

Udviklingen i 2016 viste også, at angreb med skadelig software på netbanker er faldet kraftigt, mens tab på phishing er i stigning (se Figur 40).

7.3. Deling af fortrolige oplysninger

Undersøgelsens spørgsmål om, hvorvidt deltagerne har delt fortrolige oplysninger på nettet, kan suppleres med rapporten It-anvendelse i befolkningen 2016 fra Danmarks Statistik[5]. Her fremgår det, at 68 procent har oplyst deres kontaktinformation på internettet. 58 procent har oplyst personlige data såsom navn, fødselsdato eller cpr-nummer (se Figur 41). 53 procent har angivet bankoplysninger – det kan fx være et kreditkortnummer i forbindelse med et køb. Undersøgelsen viser også, at 49 procent af danskerne tjekker om en hjemmeside er sikker, før de angiver personlige oplysninger.

[3] Microsoft Security Intelligence Report Volume 21, https://www.microsoft.com/sir

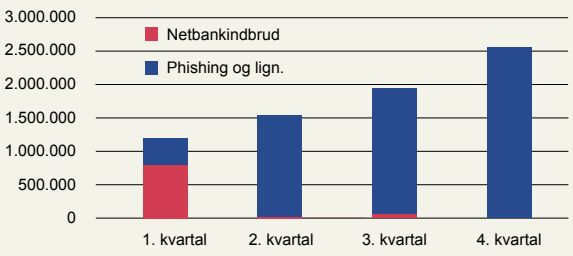
[4] Finansrådet: Netbankindbrud, http://www.finansraadet.dk/tal--fakta/Pages/statistik-og-tal/netbankindbrud---statistik.aspx

[5] Danmarks Statistik: It-anvendelse i befolkningen 2016, http://www.dst.dk/da/Statistik/Publikationer/VisPub?cid=20738

Figur 40

Tab på netbankindbrud og phishing

Tab på indbrud i netbanker og phishing i 2016.

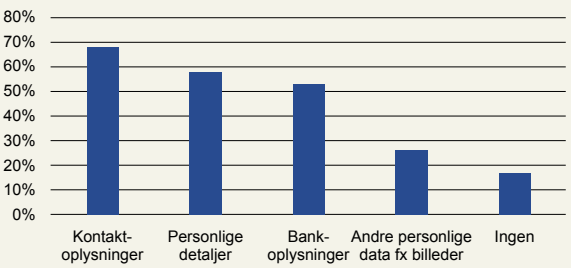


Kilde: Finansrådet.

Figur 41

Personlige data oplyst på internettet

Hvilke personlige oplysninger har du angivet på internettet de sidste 12 måneder?



Kilde: Danmark Statistik, It-anvendelse i befolkningen.



7.4. Sikkerhed på mobile enheder

Ifølge It-anvendelse i befolkningen 2016 bruger 39 procent sikkerhedssoftware på deres mobiltelefon. I vores undersøgelse er det kun 26 procent. Forskellen her skyldes sandsynligvis, at 21 procent svarede ved ikke i vores undersøgelse mod kun en procent i It-anvendelse i befolkningen.

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. I år var der en lille stigning fra fire til seks procent hos borgerne, mens tallet hos medarbejdere var omkring to procent. I It-anvendelse i befolkningen er tallet fire 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. Den lave grad af infektion kan også forklare, hvorfor færre installerer antivirus på deres mobile enheder i forhold til computerne.

7.5. Ransomware

De senere år er en ny type skadelig software dukket op: Ransomware. Den rammer i snit 7-8 procent af borgerne, viser tal fra vores undersøgelser de sidste tre år. Her følger Danmark tilsyneladende ikke med den internationale tendens, hvor der de seneste år har været et stigende antal infektioner med ransomware. Europol regner således i dag ransomware blandt de vigtigste trusler[6]. Også Center for Cybersikkerhed melder om et stigende antal angreb mod både private, virksomheder og myndigheder[7], men det fremgår altså ikke af svarene i denne undersøgelse.

7.6. Sikkerhedskopiering

57 procent af de offentligt ansatte oplyser, at der bliver taget sikkerhedskopi af de data, de bruger på jobbet. Otte procent af både offentligt og privat ansatte har mistet data som følge af manglende backup. Center for Cybersikkerheds vejledning om at reducere risikoen for ransomware betegner systematisk sikkerhedskopiering af alle kritiske informationer som absolut påkrævet.

7.7. Sikkerhedspolitik

Omkring halvdelen af de offentligt ansatte har sat sig ind i sikkerhedspolitikken på deres arbejdsplads. Hos de privatansatte er det 57 procent. Seks procent af de offentligt ansatte undlader indimellem at overholde reglerne, men over halvdelen af dem gør det sjældnere end en gang om måneden.

For de privatansattes vedkommende er det ni procent, der indimellem ikke overholder reglerne. 26 procent af dem gør det mindst en gang om ugen eller dagligt.

7.8. Sikkerhed er ledelsens ansvar

I forbindelse med sikkerheden for de offentligt ansatte og privatansatte medarbejdere skal det understreges, at informationssikkerhed er ledelsens ansvar. Derfor har ledelsen ansvaret for, at de nødvendige værktøjer stilles til rådighed. Ligeledes skal organisationens procedurer og forretningsgange indrettes på en måde, så informationssikkerheden indgår. Sikkerhedspolitikker bør udformes således, at medarbejderne ikke føler, det er nødvendigt at bryde dem for at kunne udføre deres job.

6 Europol: 2016 Internet Organised Crime Threat Assessment, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
7 Center for Cybersikkerhed: Reducér risikoen for ransomware, maj 2016, https://fe-ddis.dk/cfcs/nyheder/arkiv/2016/Pages/ransomware.aspx

8.
Samlede konklusioner

8. Samlede konklusioner

Ud fra undersøgelsens resultater konkluderer DKCERT, at der generelt er godt styr på sikkerheden, men at der er problemer med genbrug af passwords og manglende sikkerhedskopiering.

8.1. Trusler

16 procent af de offentligt ansatte og 17 procent af de privatansatte har været udsat for mindst en af de trusler, vi har spurgt til. For borgerne er tallet 34 procent.

I betragtning af de store mængder skadelige programmer, der cirkulerer, er mængden af infektioner på arbejdscomputerne på et rimeligt niveau med 11 procent. Værre ser det ud på hjemmefronten, hvor 31 procent er ramt.

Ransomware ramte seks procent af de ansatte og otte procent af borgerne. Det er en lille andel i forhold til det trusselsbillede, internationale undersøgelser tegner. Mest overraskende er, at mængden af ransomware-infektioner ikke er vokset gennem tre år.

Otte procent af de ansatte har mistet data som følge af manglende backup. Samme spørgsmål er ikke stillet til borgerne, men her har ni procent mistet data som følge et sikkerhedsproblem hos dem selv eller en tjeneste på nettet – det kan i nogle tilfælde skyldes manglende sikkerhedskopiering.

Hver fjerde offentligt ansatte, hver tredje privatansatte og hver anden borger anvender usikre trådløse netværk. Det giver risiko for, at uvedkommende får adgang til deres data.

Knap en tredjedel af de ansatte genbruger passwords på tværs af systemer. Over halvdelen af borgerne gør det.

8.2. Konsekvenser

Næsten alle ændrer adfærd, efter de har været udsat for et sikkerhedsproblem. Det mest almindelige er at undlade at åbne e-mails fra ukendte afsendere. Derudover er det også udbredt at installere eller opgradere sikkerhedssoftware. Det gør 55 procent af de offentligt ansatte, 74 procent af de privatansatte og 82 procent af borgerne.

Vi spurgte også de deltagere, der ikke havde været ude for sikkerhedsproblemer, om de havde foretaget nogle af de samme tiltag som dem, der var ramt. For de ansatte var andelen næsten den samme. Men for borgerne var det kun 56 procent af dem, der ikke var ramt, der havde foretaget nogle af tiltagene.

8.3. Foranstaltninger - adfærd

8.3.1. Beskyttelse af enheder

Ni ud af ti offentligt ansatte har sikkerhedsprogrammer på deres pc. Det samme gælder for to ud af tre borgere.

Kun halvdelen af de offentligt ansatte og hver fjerde borger har sikkerhedssoftware på deres smartphone eller tabletcomputer.

8.3.2. Forsvar mod svindel

De færreste falder for phishing-svindel og andre former for svindelforsøg over nettet. Tre ud af fire borgere ved, hvordan de kan se, hvor et link fører hen, før de klikker på det.

8.3.3. Brug af passwords

De fleste kan genkende et stærkt password. 28 procent af de privatansatte og 36 procent af de offentligt ansatte har adgang til single sign-on på deres arbejdsplads. Derimod er brugen af password managers begrænset – det gælder også for borgerne.

8.3.4. Brug af trådløse netværk

Omkring halvdelen af de ansatte og hver fjerde af de borgere, der bruger usikre trådløse netværk, beskytter sig med VPN (virtuelt privat netværk).

8.3.5. Sikkerhedskopiering

33 procent af de offentligt ansatte oplyser, at der ikke bliver taget sikkerhedskopi af deres data. For borgerne er tallet omkring 60 procent. Det er en lille stigning i forhold til tidligere. Stigningen ser ud til især at komme på de cloudbaserede tjenester, der imidlertid ikke nødvendigvis giver den tilstrækkelige beskyttelse mod ransomwareangreb (beskrevet i afsnit 2.16).

Da otte procent af både de offentligt ansatte og de privatansatte har mistet data som følge af manglende sikkerhedskopier, kan der også her være behov for en øget indsats.

8.3.6. Sikkerhedskultur

Typisk sætter omkring halvdelen af medarbejderne sig ind i reglerne om informationssikkerhed på deres arbejdsplads. Seks procent af de offentligt ansatte og ni procent af de privatansatte undlader indimellem at overholde reglerne, fordi de opfattes som en hindring for at udføre arbejdet.

8.3.7. Sikkerhed på smartphones

Smartphones og tablet-computere er ikke voldsomt plaget af skadelig software. En større sikkerhedsmæssig udfordring ligger her i, at mange ikke får taget sikkerhedskopi af de data, der ligger på de mobile enheder.

8.4. Metoder til øget passwordsikkerhed

Efterhånden som vi lever stadig mere af vores liv på nettet, ligger vores data hos en lang række tjenester. De er som minimum beskyttet med et brugernavn og en adgangskode. Det er blevet kutyme at bruge mailadressen som brugernavn. Hvis brugeren anvender samme password til flere tjenester, og en hacker 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 løbende set store tyverier af brugernavne og passwords. De stjålne brugeroplysninger sælges i vidt omfang i 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. Det kender vi fx fra NemID. Flere tjenester, fx mange af de populære cloud-tjenester, tilbyder to-trinsbekræftelse enten via sms eller særlige apps, der danner engangskoder.

Derudover kan man øge sin sikkerhed ved at bruge unikke passwords til alle tjenester. Det er i praksis umuligt at huske så mange komplicerede koder. Det problem kan løses med et password manager-program. Når en tredjedel af både offentligt ansatte og privatansatte medarbejdere og to tredjedele af borgerne genbruger passwords på tværs af tjenester, kan årsagen være, at password managers ikke er udbredte: Kun seks-otte procent af de ansatte og ti procent af borgerne anvender en password manager.

På arbejdspladser kan en del af problemet med de mange passwords løses med single sign-on-systemer. Det er positivt, at en tredjedel af de offentligt ansatte og lidt færre i det private erhvervsliv bruger den løsning. Her overtager it-funktionen besværet med passwords, så medarbejderne kun skal huske et enkelt.

9.
Anbefalinger til ledelsen

9. Anbefalinger til ledelsen

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

Informationssikkerhed er ledelsens ansvar. Hvis medarbejdere ikke handler sikkerhedsmæssigt fornuftigt i hverdagen, kan det skyldes en manglende sikkerhedskultur i organisationen. Derfor bør en indsats for øget informationssikkerhed tage udgangspunkt i en analyse af organisationens sikkerhedskultur og de holdninger til sikkerhed, der udgår fra ledelsen.

Da truslerne for offentligt ansatte og privatansatte ligner hinanden meget, har vi udarbejdet følgende anbefalinger, der gælder for begge grupper. Procentsatserne i teksten gælder for de offentligt ansatte.

9.1. Indsats mod netbaseret svindel

51 procent af de ansatte har modtaget en mail med et risikabelt link, 32 procent har fået phishing-mails. Kun få klikker på links og udfylder felterne på phishing-sider. For at mindske risikoen bør medarbejderne uddannes i at genkende tvivlsomme mails. Endvidere kan 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.

9.2. Indsats mod tab af data

Skadelig software ramte 11 procent. Seks procent har været ramt af ransomware, og otte procent har mistet data som følge af manglende backup. Det kan afhjælpes ved at øge indsatsen mod skadelig software og kontrollere rutinerne for sikkerhedskopiering. Især smartphones og tablet-computere savner sikkerhedskopiering.

9.3. Indsats mod uvedkommendes adgang til data

Hver tredje genbruger passwords. Det 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 ved genbrugte passwords mindskes med to-trinsautentifikation.

Brug af usikre trådløse netværk på cafeer og hoteller medfører også en risiko for, at uvedkommende får adgang til fortrolige data. Hver fjerde bruger ukrypterede netværk, og kun halvdelen af dem anvender VPN. Det kan forbedres ved at øge kendskabet til VPN og sikre, at den nødvendige software er installeret på brugernes enheder.

51 procent har modtaget en mail med et mistænkeligt link, 32 procent har fået en phishing-mail. Det medfører også risiko for, at angribere får fat i fortrolige data eller får kontrol over brugerens computer.

9.4. Råd til medarbejderne

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

1. Sæt dig ind i arbejdspladsens regler for informationssikkerhed og følg dem.
2. Brug stærke passwords: Et password skal være mindst 12 tegn langt, bestå af store og små bogstaver, tal og specialtegn, og må ikke optræde i ordlister.
3. Brug forskellige passwords til forskellige tjenester og systemer. Bed om at få systemer som single sign-on eller password manager stillet til rådighed.
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.
6. Undgå at sende følsomme data over åbne trådløse netværk (netværk uden kryptering) eller via ukrypteret e-mail.
7. Pas på flytbare medier såsom USB-nøgler, cd'er og transportable harddiske, de kan være inficeret med skadelig kode.
8. Brug din sunde fornuft – og bed om hjælp, hvis du er i tvivl.
9. Stil spørgsmål og kom med forslag, der kan øge informationssikkerheden på din arbejdsplads.

10.
Anbefalinger til borgerne

10. Anbefalinger til borgerne

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

Medarbejdere har som regel en it-afdeling eller en chef, 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 blandt de private borgere er større end blandt de ansatte.

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

10.1. Beskyttelse mod skadelig software

Hver tredje borger i undersøgelsen har været udsat for infektioner med skadelig software. Derfor er der brug for en øget indsats i form af sikkerhedssoftware. Den kan suppleres med uddannelse, så færre borgere klikker på tvivlsomme links og på den måde inficerer deres enheder.

10.2. Indsats mod netbaseret svindel

58 procent af borgerne har modtaget en phishing-mail. Kun fem procent faldt for svindlen. En indsats med uddannelse i, hvordan man genkender fup-mails og ser, hvor et link fører hen, kan bringe tallet længere ned.

10.3. Øget sikkerhedskopiering

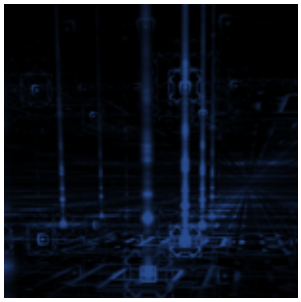
Ni procent har mistet data som følge et sikkerhedsproblem hos dem selv eller en tjeneste på nettet. En del heraf kan skyldes, at der ikke er taget backup. Kun 40 procent tager regelmæssigt sikkerhedskopi af data på computeren. For smartphones og tablet-computere er tallet 30 procent. En øget andel vil mindske risikoen for tab af data ved computernedbrud, tyveri eller ransomwareangreb.

10.4. Stop for genbrug af passwords

To ud af tre borgere anvender det samme password til flere tjenester. Det giver risiko for misbrug af deres personlige oplysninger. Den risiko kan mindskes ved brug af to-trinsbekræftelse, hvor det er muligt. Endvidere kan borgerne anvende password managers til at holde styr på de mange passwords.

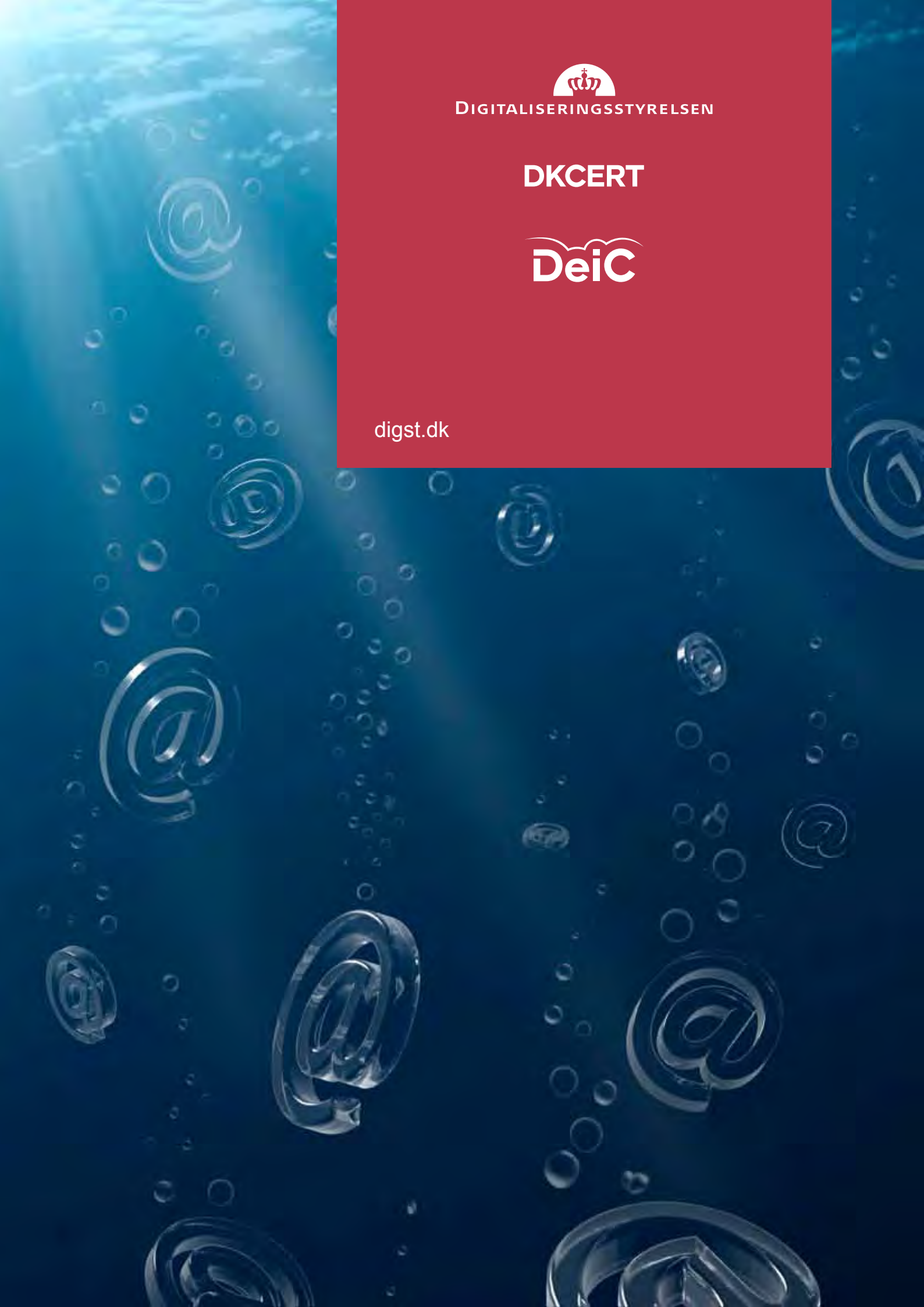
10.5. Sikker brug af trådløse netværk

Halvdelen af de borgere, der bruger trådløse netværk uden for hjemmet, anvender usikre netværk uden kryptering. Dog bruger 25 procent VPN til at beskytte kommunikationen. Sikkerheden kan øges, hvis flere anvender VPN eller undlader at bruge usikre netværk.



10.6. Råd til borgere

1. Brug sikkerhedssoftware som antivirus og firewall.
2. Hold dine programmer opdateret.
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. Tjek, at links til sider med fortrolig information begynder med teksten "https:".
6. Beskyt dit trådløse netværk med 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 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 skal være mindst 12 tegn langt, bestå af store og små bogstaver, tal og specialtegn, og må ikke optræde i ordlister.
12. Brug forskellige passwords til alle tjenester. Du kan holde styr på dine passwords med et password manager-program.
13. Brug to-trinsbekræftelse, 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.
14. Indstil privatlivsindstillingerne på sociale netværk, så de passer til dine krav.
15. Oplys ikke fortrolige og personlige oplysninger på sociale netsteder, debatsider og chatrum.
16. Brug din sunde fornuft – og bed om hjælp, hvis du er i tvivl.
17. Hjælp dine børn med at lære sikker adfærd i den digitale verden.



DIGITALISERINGSSTYRELSEN

DKCERT

DeiC

digst.dk