Udvalget for Digitalisering og It 2022-23 (2. samling)
DIU Alm.del - Bilag 61
Offentligt

CENTER FOR CYBERSIKKERHED

Håndbog i sikkerhed for mobile enheder

For ministre, departementschefer, særlige rådgivere og udvalgte medarbejdere i ministerierne

1. udgave februar 2023

Forord

Den generelle trussel fra fremmede staters efterretningsvirksomhed i Danmark vurderes at være specifik og vedvarende, og truslen fra cyberspionage vurderes at være meget høj. Blandt de oplagte mål for spionage er ministre og centrale embedsmænd.

Mobiltelefoner og tablets er nødvendige redskaber i de flestes dagligdag, men de er også sårbare over for, at uvedkommende skaffer sig uberettiget adgang. Samtaler, beskeder og datatrafik kan eksempelvis relativt simpelt indhentes og aflyttes, medmindre der er taget særlige beskyttelsesforanstaltninger som f.eks. brug af stærk kryptering.

Der kan også være tale om fysisk kompromittering, f.eks. hvis en person får fysisk adgang til dine mobile enheder eller fysisk har mulighed for at følge med i, hvad du laver på din enhed. Eller det kan dreje sig om digital kompromittering, hvor uvedkommende kan få delvis eller fuld kontrol over din mobile enhed. Dette kan f.eks. ske gennem phishing, hacking, skadelige apps eller malware. En sådan kompromittering betyder, at uvedkommende kan aflytte dine samtaler eller få adgang til dine beskeder, fotos mv.

Den nuværende opsætning af mobile enheder i staten modsvarer ikke dette trusselsbillede. Der implementeres derfor nu en række tiltag, som skal sikkerhedshærde de mobile enheder og derved reducere deres sårbarhed over for spionage.

Ved sikkerhedshærdningen indstilles de mobile enheder på en måde, der begrænser anvendelsen af en række funktioner såsom Bluetooth, Wi-Fi og lokalitetstjenester. Samtidig vil kun et begrænset antal apps kunne anvendes på telefonen.[1] Der installeres tillige krypteringsapps, som giver en stærk beskyttelse af samtaler og beskeder mod aflytning. Husk ***ikke*** at ændre i indstillingerne på din tjenestetelefon eller tablet, når hærdningen er foretaget. Hvis du ændrer indstillinger eller installerer apps, der ikke er på listen, svækker du sikkerheden på dine mobile enheder.

Sikkerhedshærdningen reducerer dine mobile enheders sårbarheder, men fjerner ikke risikoen ved at anvende dem. Sikker adfærd er derfor fortsat vigtig for at imødegå spionagetruslen. F.eks. vil informationer klassificeret FORTROLIGT[2] eller højere som hidtil skulle håndteres via særligt sikkerhedsgodkendte systemer som REGNEM eller Tiger-telefoner, der er godkendt til HEMMELIGT.

Mange brugere vil formentlig opleve behov for en privat telefon for at kunne anvende funktioner og apps, der ikke er tilgængelige på den sikkerhedshærdede tjenestetelefon. Der må ikke udleveres og anvendes tjenestetelefoner og tablets, som ikke er sikkerhedshærdede.[3]

I denne håndbog kan du læse mere om indstillingerne på din sikkerhedshærdede tjenestetelefon. Håndbogen er udarbejdet i overensstemmelse med Justitsministeriets foreløbige retningslinjer for statslige myndigheders opbevaring af SMS-beskeder mv., gældende sikkerhedsinstrukser[4] og eksisterende vejledninger om sikkerhed på mobile enheder.

[1] Oversigten over tilladte apps fremgår af bilag 4.
[2] Definitionen af klassifikationsgrader fremgår af bilag 1.
[3] Der gælder undtagelser ifm. rejser til visse lande, hvor det af sikkerhedshensyn kan være nødvendigt at medtage særlige rejsetelefoner mm.
[4] Gældende sikkerhedsinstrukser og retningslinjer fremgår af bilag 2.

Sikkerhedshærdet tjenestetelefon

Sikkerhedshærdning[5] af tjenestetelefon og eventuel tablet øger sikkerheden, men vil medføre visse begrænsninger af enhedens funktionalitet. Sikkerhedshærdning af tjenestetelefon og tablet vil tage ca. 30 minutter og vil blive udført on-site. Det er som udgangspunkt din eksisterende tjenestetelefon og evt. tablet, der bliver sikkerhedshærdet.

Tjenestetelefonen vil løbende få foretaget backup af beskeder, jf. Justitsministeriets foreløbige retningslinjer for statslige myndigheders opbevaring af SMS-beskeder mv., og Statens It vil i den forbindelse i samarbejde med hvert enkelt ministeriums IT-kontor/sikkerhedsorganisation foretage scanning for visse typer malware samt kontrol med sikkerhedshærdningen af tjenestetelefonen og evt. tablet.

Under den jævnlige scanning mv. vil apps installeret på din tjenestetelefon blive efterset. Fremgår de ikke på listen over tilladte apps, vil de skulle slettes i dialog med brugeren.

Selvom hærdningen reducerer sårbarhederne, vil der altid være en vis risiko, når man kommunikerer over en mobiltelefon eller en tablet. Sikker brugeradfærd er derfor også vigtig bl.a. i forhold til anvendelse af f.eks. apps til sociale medier. På side 5 findes en række konkrete råd i afsnittet Adfærd – sikkerhedsmæssige fokuspunkter.

Brugerkonto og cloudbackup på tjenestetelefonen

Bl.a. for at kunne hente apps i producenternes appbutikker er det nødvendigt at tilknytte en brugerkonto til tjenestetelefonen. Brugeren vil ved udlevering af tjenestetelefonen få oprettet en statslig brugerkonto, hvor brugerens arbejdsmailadresse og arbejdstelefonnummer benyttes til oprettelsen.

Beskrivelse og opsætning af tjenestetelefon og tablet

- Tjenestetelefonen er en smartphone[6].
- Lokalitetstjenester, Wi-Fi, stemmestyring, cloudbackup og Bluetooth er slået fra.
- Der udleveres et headset med ledning.
- Adgangskode på minimum 10 cifre, eventuelt med ansigtsgenkendelse eller fingeraftryk.
- Indholdet af notifikationer skjules på låseskærmen.
- En række standard-apps er præinstalleret – mail, kalender, kontakter, statens sikkerhedsgodkendte krypteringsapp SMART-2 samt appen Signal.

Myndighedens egen sikkerhedsorganisation opretter og nedlægger brugerkonti. Man kan således ikke benytte sin private brugerkonto på tjenestetelefonen, og cloud må ikke anvendes til dataopbevaring og backup mv. Det bemærkes, at cloudbackup som led i sikkerhedshærdningen slås fra – for at undgå utilsigtet overførsel af data – og ikke må slås til efterfølgende.

Den statslige brugerkonto låses op ved, at brugeren ved ansættelsesophør udleverer kodeordet til kontoen, eller – hvis brugeren ikke har gjort dette – at organisationen nulstiller kodeordet via mail eller telefonnummer.

[5] Se bilag 3 for oversigt over tiltag i sikkerhedshærdningen.
[6] Det bemærkes, at anvendelsen af statens sikkerhedsgodkendte krypteringsapp skal understøttes på tjenestetelefoner, som skal indkøbes på rammeaftaler for tjenestetelefoner.

Samtaler og beskeder på tjenestetelefonen

Stærk kryptering er et helt nødvendigt og grundlæggende tiltag for at beskytte tjenestetelefonen mod aflytning af samtaler og beskeder. Derfor er der installeret to krypteringsapps på telefonen, som kan benyttes til samtaler, beskeder og video-samtaler. SMART-2 er udviklet og anskaffet af Forsvarsministeriet og er statens sikkerhedsgodkendte krypteringsapp til samtaler og beskeder, der er klassificeret TIL TJENESTEBRUG. Signal har en stærk kryptering, men er dog ikke godkendt til klassificeret kommunikation.

Tjenestetelefonens almindelige samtale- og beskedfunktion er sårbar over for aflytning. Du kan fortsat benytte telefonens almindelige samtale- og beskedfunktion, men når du kommunikerer med personer i danske myndigheder, og der er behov for at beskytte kommunikationen mod aflytning, bør du som udgangspunkt anvende SMART-2 eller Signal, hvis SMART-2 ikke kan benyttes.

SMART-2 app

SMART-2 har en meget stærk kryptering og yder meget god beskyttelse mod aflytning.

SMART-2 kan anvendes af personer i danske myndigheder.

SMART-2 er sikkerhedsgodkendt og må anvendes til kommunikation, der er klassificeret TIL TJENESTEBRUG.

Der kan ikke kommunikeres via SMART-2 med personer, der ikke er oprettet som brugere på SMART-2 eller kompatible systemer.

Der kan pt. ikke laves backup af beskeder i SMART-2, men beskeder lagres lokalt på telefonen. Der er dialog med producenten af SMART-2 om udvikling af en backup-funktion.

Signal app

Er kommunikation med SMART-2 ikke mulig, kan du i stedet bruge Signal.

Signal kan for eksempel benyttes til kommunikation med udenlandske samarbejdspartnere.

Signal har en stærk kryptering og yder god beskyttelse mod aflytning.

Signal er dog ikke sikkerhedsgodkendt og må ikke bruges til klassificeret kommunikation.

Brug af Signal forudsætter, at modtager har accepteret opkald og beskeder fra afsender.

Der kan foretages backup af Signal-beskeder ved skærmprint eller tilsvarende. Der arbejdes på en mere automatiseret backup-proces.

Opkald og SMS mv.

Tjenestetelefonens almindelige samtale- og beskedfunktioner har begrænset eller ingen beskyttelse i form af kryptering.

Der findes desuden metoder til at angribe og kompromittere disse almindelige tjenester.

Det må derfor antages, at kommunikation via telefonens almindelige samtale- og beskedfunktion er sårbar over for aflytning.

Der kan foretages backup af SMS-beskeder mv. ved hjælp af den SIT-understøttede løsning.

HØJ SIKKERHED — **LAV SIKKERHED**

Apps på tjenestetelefonen

For at begrænse angrebsfladen på din tjenestetelefon og tablet begrænses også mængden af apps, du kan benytte. Jo færre apps på din enhed, jo færre potentielle sårbarheder og softwarefejl, som kan udgøre en sikkerhedsrisiko.

Du skal være opmærksom på følgende i forhold til apps på din tjenestetelefon og tablet:

- Din tjenestetelefon og tablet er udstyret med en række apps til primært arbejdsmæssige opgaver.
- Du må installere en række yderligere apps, der opfylder et arbejdsbetinget behov, som på forhånd er udvalgt og fremgår af en liste.
- Du må ikke installere apps, der ikke er på listen.

Det fremgår af bilag 4, hvilke apps du må installere på din tjenestetelefon og tablet[7].

Listen med apps er udarbejdet med fokus på arbejdsrelevante behov, hvem der er udvikleren eller udgiveren af appen, samt de funktioner på telefonen, som appen har behov for, for at fungere korrekt.

Hvis der opstår tjenstligt behov for en app med funktionalitet, som ikke kan opfyldes af en eksisterende app på listen, kan den sikkerhedsansvarlige ved myndigheden anmode om at få den pågældende app optaget på listen ved mail til VKM@Statens-it.dk[8]. Statens It og Center for Cybersikkerhed vil sammen vurdere, om app'en kan blive optaget på listen.

Den sikkerhedshærdede tjenestetelefon og tablet kan benyttes til privat brug under forudsætning af, at der ikke ændres i indstillingerne eller installeres apps, der ikke fremgår af bilag 4, samt at det sker inden for de gældende rammer, herunder lokale aftaler samt beskatningsregler. Hvis du har privat behov for funktionaliteter eller apps ud over dem, der stilles til rådighed på den sikkerhedshærdede tjenestetelefon, vil du skulle anvende en anden telefon.

Eksempler på tilladte apps

- Mail, kalender og kontakter
- SMART-2 (telefon)
- Signal
- Google Maps
- MitID/NemID
- Facebook, Instagram og LinkedIn

Eksempler på ikke tilladte apps

- Fildelingstjenester, såsom DropBox
- Nogle sociale medier, såsom TikTok og Snapchat
- Motionsapps, såsom Strava

[7] Der kan desuden i forbindelse med sikkerhedsopdateringer automatisk blive installeret andre apps på telefonen og evt. tablet.
[8] Udenrigsministeriet og Forsvarsministeriet varetager administrationen af mobile enheder selv og følger en lignende intern procedure.

Adfærd – sikkerhedsmæssige fokuspunkter

Selvom din tjenestetelefon bliver sikkerhedshærdet, kan hærdningen ikke stå alene. Der vil altid være et behov for, at brugerens adfærd understøtter sikkerhedstiltagene, og derfor skal du stadig selv være på vagt.

Du skal være opmærksom på følgende:

- Vær opmærksom på, at sikkerheden på din telefon og tablet også er dit eget ansvar.
- Tænk over omgivelserne og indholdet, når du taler. Det kan for eksempel være i bilen, i lufthavnen, i flyet eller i toget, hvor uvedkommende kan lytte med.
- Hvis du taler uden at overveje sensitivitet eller klassifikation, øger du risikoen for, at information kommer til uvedkommendes kendskab. Overvej derfor altid, om den information, du skal til at kommunikere, egner sig til at blive delt, på den måde, du har tænkt dig.
- Du skal ***ikke*** ændre i sikkerhedsopsætningen på tjenestetelefonen f.eks. ved at slå Bluetooth, Wi-Fi, lokalitetstjenester, cloudbackup eller lignende til. Ved at ændre på indstillingerne øger du risikoen for, at telefonens sikkerhed reduceres.

Du kan komme i en situation, hvor du midlertidigt er nødt til at slå eksempelvis lokalitetstjenester eller Wi-Fi til på din tjenestetelefon. Det kan for eksempel være på tjenesterejser i lande eller ved sikkerhedsopdatering, hvor der ikke kan anvendes mobilnetværk. Hvis du i en sådan ekstraordinær situation aktiverer funktionen, så husk altid at slå den fra igen, når du ikke længere bruger den. Nærmere retningslinjer for håndtering af bl.a. sådanne situationer under rejser er under udarbejdelse i et kommende rejsekoncept.

Brug af private enheder på arbejdet

Idet din tjenestetelefon er sikkerhedshærdet, kan din private telefon, smartwatch eller tablet nu muligvis udgøre det sikkerhedsmæssigt svageste punkt. Kompromittering af din privattelefon kan udgøre en trussel mod informationssikkerheden, f.eks hvis hackere har fået adgang til privattelefonens mikrofon eller kamera. Dette udgør også en yderligere risiko, da din privattelefon, smartwatch eller tablet muligvis kan kompromittere din tjenestetelefon.

Du må derfor som det klare udgangspunkt ikke benytte din privattelefon til at udføre tjenstlige opgaver.

Husk, at du altid kan få hjælp til at sætte din privattelefon op på en sikker måde af din organisations supportfunktion.

Do's and don'ts på privattelefonen

Tag privattelefonen og andre mobile enheder ud af kontoret og medbring dem ikke til tjenstlige møder, hvis der skal tales om forhold, der er klassificeret højere end TIL TJENESTEBRUG.

Brug privattelefon til eventuelle apps, som ikke er på listen over apps til tjenestetelefonen. Eksempelvis apps til spil, underholdning, navigation, indkøb og sportsaktiviteter mm.

Brug af mobile enheder i hjemmet
I kraft af den øgede globale digitalisering er der kommet mange nye enheder til for at gøre vores dagligdag lettere. Mange af disse er dog udstyret med mikrofoner og kameraer, og derfor skal du holde nogle risici for øje, når du arbejder i hjemmet. Du skal for eksempel være opmærksom på følgende:

- Smarthøjttalere, Smart-tv og digitale assistenter (f.eks. Echos, Alexa, Google Assistant) er ofte udstyret med mikrofon, kamera og Wi-Fi.
- Derudover er de også ofte designet til at lytte og reagere på nøgleord fra deres brugere.
- Smart-enheder er ofte forbundet til private netværk via eksempelvis Wi-Fi. Derfor kan de også bruges som adgangsvej for en hacker til at komme ind på dit private netværk og derfra skaffe sig adgang til andre enheder eller opsnappe datapakker.

Hvis du skal tale i tjenestetelefon i hjemmet, bør du gennemføre samtalen i et rum uden smarthøjttalere og digitale assistenter mv. Hvis dette ikke er muligt, bør du sikre dig, at smarthøjttalere og digitale assistenter mv. i rummet er slukket og ikke aktiveres af din samtale.

Hjælp til din mobiltelefon
Kontakt din sikkerhedsofficer eller sekretær, hvis du har brug for hjælp til din mobiltelefon.

BILAG 1

Klassifikation af informationer

HEMMELIGT
(NATO SECRET, SECRET UE/EU SECRET)

Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO eller EU alvorlig skade.

FORTROLIGT
(NATO CONFIDENTIAL, CONFIDENTIEL UE/EU CONFIDENTIAL)

Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO eller EU skade.

TIL TJENESTEBRUG
(NATO RESTRICTED, RESTREINT UE/EU RESTRICTED)

Denne klassifikationsgrad skal anvendes om informationer, der ikke må offentliggøres eller komme til uvedkommendes kendskab.

Supplerende informationer for klassifikation af informationer TIL TJENESTEBRUG

SMART-2 er sikkerhedsgodkendt og må anvendes til kommunikation, der er klassificeret TIL TJENESTEBRUG.

Når det skal vurderes, om informationer skal klassificeres TIL TJENESTEBRUG, bør der anvendes et bredt sikkerhedsperspektiv med fokus på skadevirkningen ved en kompromittering af informationerne med udgangspunkt i følgende sikkerhedsinteresser:

- De øverste statsorganers virksomhed, sikkerhed og handlefrihed.
- Danmarks forsvar, sikkerhed og beredskab.
- Forholdet til andre stater og internationale organisationer.
- Danmarks økonomiske stabilitet og handlefrihed.
- Samfundets grundlæggende funktionalitet.
- Befolkningens grundlæggende sikkerhed, tryghed og tillid til staten.
- Enkeltpersoners og virksomheders væsentlige økonomiske og erhvervsmæssige interesser.

Følgende informationstyper vil eksempelvis være relevante at overveje at klassificere TIL TJENESTEBRUG:

- Visse informationer i relation til regeringens virke, eksempelvis informationer til regeringsudvalg, interne høringer, lovforberedende arbejde mv.
- Visse informationer vedrørende organisationers beredskab og sikkerhed, eksempelvis beredskabsplaner, sårbarhedsanalyser, interne procedurer mv.
- Følsomme informationer om særlige lokaliteter og offentlig kritisk infrastruktur, eksempelvis it-systemers tekniske tilstand, risikovirksomheder mv.
- Visse informationer til og fra samt internt i udenrigstjenesten, Forsvaret, politiet og efterretningstjenesterne, eksempelvis konkrete oplysninger om ansatte, indkøb af materiel mv.
- Visse informationer i relation til Danmarks internationale relationer, eksempelvis informationer om forhandlingspositioner og -oplæg.
- Visse sektorspecifikke informationer i relation til virksomheder og borgere, der anvendes internt i og mellem myndigheder, eksempelvis tilsynsrapporter, klagesager mv.

Fortsætter næste side

Med sikkerhedshærdningen af de mobile enheder, herunder installation af SMART-2, samt udrulningen af TTJ-platformen i staten, bliver det lettere at håndtere materiale klassificeret TIL TJENESTEBRUG. Det er positivt for sikkerheden i staten, men medfører også en øget risiko for, at sager, der bør klassificeres FORTROLIGT eller højere, i stedet klassificeres TIL TJENESTEBRUG. En sådan "underklassificering" vil medføre en utilstrækkelig beskyttelse.

Klassificering skal altid ske ud fra en konkret vurdering af materialet og dets potentielle skadesvirkninger. Er du i tvivl om klassificering af en information, kan du kontakte din organisations sikkerhedsofficer.

PET bistår gerne sikkerhedsofficerer med råd og vejledning om klassificering samt håndtering af klassificerede oplysninger.

BILAG 2

Gældende sikkerhedsinstruks og retningslinjer

Den gældende sikkerhedsinstruks for sikkerhedsministerierne fastsætter, at ministerierne generelt skal benytte mulighederne for at anvende kommunikationsmidler og informationssystemer, der har et højt sikkerhedsniveau. Personer med adgang til REGNEM-telefoner skal i videst muligt omfang anvende disse til tjenstlige telefonsamtaler, ikke kun hvor der er tale om klassificeret indhold, men også hvor samtalen indeholder beskyttelsesværdige informationer.

Ministeriernes handleplaner for anvendelse af kommunikationsmidler og informationssystemer skal sikre, at risikoen for kompromittering af ejer og informationer mindskes. Handleplaner skal udarbejdes under inddragelse af CFCS' vejledninger – herunder vejledninger udarbejdet i samarbejde med PET – på området mhp. at opnå et passende højt sikkerhedsniveau.

Sikkerhedsinstruksen fastslår endvidere, at personer, der arbejder med klassificerede informationer eller besidder en sensitiv stilling, kan have et øget behov for at adskille arbejde og privatliv og for at have et generelt højere sikkerhedsniveau for tjenstlig mobiltelefoni.

Relevante personer i ministerierne skal derfor have udleveret mobiltelefoner med Forsvarsministeriets krypterede og sikkerhedsgodkendte mobilapplikation "SMART" installeret. SMART er sikkerhedsgodkendt til tale op til klassifikationsgraden TIL TJENESTEBRUG og skal generelt anvendes af disse personer til tjenstlige mobilsamtaler.

Den seneste version (SMART-2) har endvidere krypteret og sikkerhedsgodkendt besked- og videosamtalefunktion. SMART-2 har aktuelt ikke en automatisk og brugeruafhængig backup-funktion, men dette indebærer ikke, at den statslige myndighed skal begrænse brugen af denne beskedtjeneste, i den udstrækning informationssikkerhedsmæssige hensyn tilsiger, at den anvendes.[8] For så vidt angår beskeder i SMART-appen, som alene lagres lokalt på tjenestetelefonen, kan opbevaringen i praksis eksempelvis ske ved, at tjenestetelefonen opbevares i aflåst skab uden at blive nulstillet og således, at myndigheden er i besiddelse af adgangskode til telefonen.

For at fremtidssikre retningslinjerne omfatter Justitsministeriets foreløbige retningslinjer for statslige myndigheders opbevaring af SMS-beskeder mv. opbevaring af SMS-beskeder og andre lignende beskedtjenester (eksempelvis, iMessage, Whatsapp, Signal o.lign). Benyttes andre beskedtjenester end SMS, iMessage og Whatsapp, vil opbevaring i praksis eksempelvis kunne ske ved, at en lokal kopi af arbejdsrelaterede beskeder sikres ved et skærmprint af de enkelte beskeder. Den statslige myndighed kan – af praktiske og ressourcemæssige årsager – overveje at begrænse brugen af andre beskedtjenester til situationer, hvor det er særligt velbegrundet, f.eks. i forbindelse med kommunikation i eller med modtagere i andre lande, eller hvor spionagetruslen i øvrigt må antages at være udtalt.

[9] Justitsministeriets foreløbige retningslinjer for statslige myndigheders opbevaring af SMS-beskeder mv., side 7.

BILAG 3

Oversigt over tiltag i sikkerhedshærdningen

Tiltag	Begrundelse
0. Skift af brugerkonto til statslig brugerkonto	For at undgå at data forlader myndigheden. Udføres kun i de tilfælde, hvor der ikke er tilknyttet en statslig brugerkonto til tjenestetelefonen. Hvis punktet udføres på et senere tidspunkt, skal punkt 13 gennemgås igen.
1. Deaktivering af Wi-Fi	Wi-Fi-netværk, herunder specielt åbne netværk, kan benyttes til at opsnappe information, hvorved kommunikationen kompromitteres. Derfor frakobles Wi-Fi.
2. Deaktivering af Bluetooth	Bluetooth har en lang rækkevidde og søger ofte efter andre enheder. Bluetooth bliver deaktiveret for at sikre, at det ikke kan anvendes til sporing eller kompromittering.
3. Deaktivering af lokalitetstjenester	Lokalitetstjenester bruges til at identificere din geografiske placering. Dette kan anvendes som værktøj til at spore, hvor du er og eksempelvis identificere, hvem du er sammen med.
4. Deaktivering af reklamer	Risiko for målrettet indsamling og efterfølgende misbrug af oplysninger om din anvendelse af telefonen og internettet.
5. Skjul indhold af notifikationer på låseskærm	For at undgå at uvedkommende kan tilgå telefonens beskeder, mens den eventuelt er lagt væk, skjuler telefonen indholdet af notifikationer, indtil den er låst op.
6. 10-cifret låsekode	4- og 6-cifrede låsekoder kan brydes af moderne software. Derfor skal du benytte 10-cifret låsekode. Benyt gerne biometri til at få nemmere adgang.
7. Deaktivering af udsendelse af diagnostik-informationer	Udsendelse af diagnostik-informationer udgør en risiko for målrettet indsamling og misbrug af oplysninger om din brug af telefonen og internettet. Derfor slås dette fra.

Tiltag	Begrundelse
8. Ingen sporing på tværs af apps	Sammenfletning af oplysninger kan resultere i, at hackere kan indsamle informationer om for eksempel din omgangskreds, vaner og placeringer mv. Derfor bliver sporing på tværs af apps slået fra.
9. Deaktivering af stemmestyring	Stemmestyringsfunktionen er slået fra for at reducere datamængden, der sendes til smartphone-leverandøren. Du kan stadig benytte "Speech-text"-funktionen.
10. Ændring af enhedens navn	Enhedens navn bør af sikkerhedsmæssige årsager ikke være personhenførbar eller indeholde oplysninger om telefonmodel eller type. Derfor sikres det, at enhedens navn ikke indeholder disse oplysninger.
11. Ændring af søgemaskine	Browserens søgemaskine indstilles til DuckDuckGo i stedet for f.eks. Google. Dette sker for at minimere dataindsamling.
12. Aktivering af automatiske opdateringer af apps	Hvis en app er sårbar, vil en udvikler typisk udrulle en sikkerhedsopdatering. Automatiske opdateringer af apps sørger for, at du er på den nyeste version og derfor mindre sårbar.
13. Deaktivering af cloudbackup	For at undgå utilsigtet overførsel af data deaktiveres backup og dataopbevaring i cloud. Såfremt enheden har været tilknyttet en privat brugerkonto, skal brugeren og sikkerhedsorganisationen være opmærksom på, hvilken data der er blevet overført til cloud. Sikkerhedsorganisationen har en vejledning i sletning af data i cloud og kan hjælpe med dette.
14. Installation af krypterede kommunikationsapps	Beskeder og almindelige telefonopkald er sårbare overfor aflytning. Derfor er der installeret statens sikkerhedsgodkendte krypteringsapp SMART-2 samt appen Signal, som fungerer som krypterede kommunikationskanaler.

Fortsætter næste side

Oversigt over tiltag i sikkerhedshærdningen

Tiltag	Begrundelse
15. Lockdown mode (iPhone)	Indbygget sikkerhedshærdning i iPhone, der reducerer risikoen for spyware. Lockdown omfatter bl.a., at visse filer og links i beskeder blokeres. Der vil endvidere være en større sikkerhed ifm. webbrowsing, men enkelte web-sider indlæses langsommere som følge heraf. Desuden skal iPhonen låses op, når denne tilsluttes andre enheder. Tilsvarende funktionalitet findes ikke på Android-enheder.
16. Kræv låsekode	Indstilling ændres til "Straks". Telefonen vil herefter kræve adgangskode eller biometri med det samme, når skærmen går i dvale.
17. Skærm & lysstyrke automatisk lås	Automatisk lås ændres til 30 sekunder. Telefonens skærm vil herefter gå i dvale efter 30 sekunder.
18. Montering af privacy filter	Hvis enheden ikke har påmonteret privacy filter, vil det blive monteret.

BILAG 4

Oversigt over tilgængelige apps[10]

Bank og betaling		Fly		
Bank Norwegian	SparKron - Mobilbank	Air France	SWISS	Instagram
Corporate Card	Spendwise	Austrian	Thai Airways	LinkedIn
Dit Guldkort	Sydbanks Mobilbank Privat	Book Flight Tickets by Pegasus	Turkish Airlines: Book Flights	Messenger
Eurocard	WeShare	British Airways	United Airlines	Twitter
Eurocard Pro	Western Union DK Send Penge	Brussels Airlines	Vueling Airlines-Cheap Flights	WhatsApp
Jyske Bank		CPH Airport	Wizz Air	**Møde apps**
Jyske Mastercard Expense Mate	**Transport**	easyJet: Travel App	**Rejseplanlægning**	GoToMeeting
Lunar	APCOA FLOW | Mobile Parking	EGYPTAIR	DB Navigator	GoToWebinar
Mine Kort fra Jyske Bank	Bolt: Fast, Affordable Rides	Emirates	Google Maps	Jitsi Meet
Mobilbank DK - Danske Bank	Brobizz	Eurowings	Google Translate	Pexip
Mobilbank Lån & Spar Bank	EasyPark - find & pay parking	Finnair	Hotels.com: Book Hotels & More	Saba Meeting
MobilePay	EasyPark - Parking made easy	Flightradar24 | Flight Tracker	Kiwi.com: Cheap Flights	Skype
Nordea Business DK	FREE NOW	Fly Delta	MAPS.ME: Offline Maps, GPS Nav	Skype for Business
Nordea ID	GoMore - car sharing	Flyr	Momondo: Flights, Hotels, Cars	Teams
Nordea Mobile - Danmark	GreenMobility	Icelandair	My CWT	Webex Meetings
Nordea Mobile - Denmark	Midttrafik	KLM	Mytrip.com	Zoom
Nordea Wallet	MOLSLINJEN	LATAM Airlines	Rejseklar	Zulip
Ny MitNykredit	Q8	Lufthansa	Rejseplanen	**Offentlige apps**
Revolut Business	Q-Park	Norwegian Travel Assistant	Rejseplanen til iPad	Akuthjælp
SAS EuroBonus World Mastercard	SHARE NOW (car2go & DriveNow)	Paris Aéroport - Official	RejsUd - Ibistic	Digital Post
SEB Corporate Card	Skyhost Booking	Planes Live - Flight Radar	Scandic Hotels	eBoks
Spar Nord	Skyhost GPS	Priority Pass™	Skyscanner - travel deals	Kørekort
Spar Nord Mobilbank Erhverv	Sydtrafik	Qatar Airways	Travellink - Flights, Hotels	MitID
Sparekassen Danmark Mobilbank	Viggo - book a ride	Ryanair	Tripadvisor: Plan & Book Trips	NemID
Sparekassen Kronjylland		SAS - Scandinavian Airlines	**Sociale Medier**	Rejseklar
Sparekassen Sjælland-Fyn		Schiphol Amsterdam Airport	Facebook	Sundhedskortet
				Fortsætter næste side

[10]Smartphone og tablet leveres med en række præinstallerede apps fra producenten, som ikke fremgår af bilag 4.

Oversigt over tilgængelige apps

MIA apps (Statens IT)			
360° eManager	BBC News	Nyhedskiosken app	
360° eWorker	BBC World Service	Politiken app og e-avis	
Citrix Files	Berlingske app og e-avis	Reuters News	
Citrix SSO	Berlingske Business app	Ritzau Nyheder	
Driftsstatus	Bornholms Tidende app	Sjællandske Medier – aviser app	
F2 Manager	Børsen app og e-avis	Skive Folkeblad app	
F2 Touch	CBC News	The New York Times	
Filkassen	CNN: Breaking US & World News	TV fra Folketinget	
FreeOTP	Licitationen E-avis	TV2 Nyheder	
KMD Workzone	DR LYD	TV2 Play	
My Workplace (Coor)	DR Nyheder	UN News Reader	
Office	Ekstra Bladet app og e-avis	Weekendavisen app og e-avis	
Pages	Financial Times	**Andre apps**	
Secure Hub	DRTV	Microsoft Authenticator	
Secure Mail	Finans - Danmarks erhvervsavis		
Secure Web	Folketidende app		
Signal	Frihedsbrevet		
Skype for Business	Infomedia Mobile News		
SMART-2	Information app og e-avis		
TDC Erhverv	Ingeniøren app		
Kontor apps	ITWatch		
Office	Jyllands-Posten app og e-avis		
Outlook	Jyllands-Postens Lokalaviser app		
Onenote	Kristeligt Dagblad app		
Nyheder	Midtjyllands Avis app		
B.T. Online app og e-avis	Nordjyske app		

Alle apps, der installeres, skal have et tjenstligt formål og må alene installeres fra producenternes appbutikker.

Mængden af apps øger angrebsfladen, så installer så få apps som muligt. Listen er dynamisk og opdateres løbende i takt med udviklingen.

Er du i tvivl, om du må installere en app på din tjenestetelefon, så spørg din sikkerhedsofficer eller installer eventuelt app'en på en anden telefon.