Bekendtgørelse om oplysnings- og underretningspligter vedrørende ~~net- og informations~~sikkerhed i net og tjenester[1)]

I medfør af § 4, § 7, § 11, stk. 2, og § 14, stk. 2, i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed, som ændret ved lov nr. 1831 af 8. december 2020, fastsættes:

Definitioner

§ 1. I denne bekendtgørelse forstås ved:

1) Kritiske netkomponenter, systemer og værktøjer: Operations support systemer, network management systemer og business support systemer, der kan benyttes til at aflæse, ændre indhold af eller dirigere data, som relaterer sig til slutbrugere, samt hardware, firmware og software, der anvendes i eller i forbindelse med core-net i mobilnet, fastnet og internet, eller i centrale routere og servere i backbonenettene eller i kontrolenheder, som anvendes til styring i mobilnettenes radionet.
2) Slutbruger: En bruger af elektroniske kommunikationsnet og -tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.
3) Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikations-net og -tjenester:
   a) Udbydere af elektroniske kommunikationsnet, hvor disse net anvendes af mere end 50.000 slutbrugere. Ved opgørelsen medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder. Radio- og tv-stationer, der er udbydere af net, er kun omfattet, såfremt de har landsdækkende public service-forpligtelser.
   b) Udbydere, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheder og institutioners egne slutbrugere.
4) Beredskabsaktører: Myndigheder, institutioner og virksomheder, som skal bidrage til opretholdelse af samfundet funktioner i beredskabssituationer og i andre ekstraordinære situationer.
5) Beredskabssituationer og andre ekstraordinære situationer: Større ulykker, katastrofer eller hændelser, hvor det kan være nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at kunne opretholde samfundets funktioner.

Afgivelse af oplysninger til Center for Cybersikkerhed

§ 2. Center for Cybersikkerhed kan udstede påbud om, at erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skriftligt til centeret skal afgive oplysninger om væsentlige dele af udbydernes net og tjenester eller varetagelsen af driften heraf.

Stk. 2. Påbud efter stk. 1 kan omfatte oplysninger om hardware, firmware og softwares fabrikat, konfiguration, typebetegnelse, serienummer, antal og tilsvarende, oplysninger om netarkitektur og -design, eventuelle leverandører, herunder driftsleverandører, samt den geografiske placering af udbydernes og relevante leverandørers hardware og drifts- og supportcentre.

Stk. 3. Center for Cybersikkerhed kan fastsætte en tidsfrist for udbydernes afgivelse af oplysninger. Tidsfristen skal være på mindst fire uger.

Stk. 4. Center for Cybersikkerhed kan stille krav om, at oplysningerne afgives elektronisk.

Underretning af Center for Cybersikkerhed om aftaleforhandlinger

§ 3. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal skriftligt underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger om aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf.

Stk. 2. Udbyderne skal skriftligt underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger om tillæg til eksisterende aftaler, som vedrører eller grundet tillægget vil komme til at vedrøre kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf.

§ 4. Underretninger efter § 3 skal indeholde oplysninger om:

1) Hvilke kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som aftalen påtænkes at omfatte.
2) Aftalens påtænkte omfang.
3) Eventuel placering af opgaver uden for Danmark.
4) Eventuelle leverandører, der påtænkes inddraget i aftaleforhandlingerne.
5) Overordnet tidsplan for aftaleforhandlingerne.
6) Aftalens påtænkte varighed.

§ 5. Center for Cybersikkerhed kan udstede påbud om, at det endelige udkast til en aftale, der er omfattet af § 3, skal fremsendes til Center for Cybersikkerhed forud for indgåelse af den endelige aftale.

Stk. 2. Den endelige aftale vil herefter først kunne indgås, når udbyderen har modtaget en tilbagemelding fra Center for Cybersikkerhed. Tilbagemeldingen vil blive givet hurtigst muligt og senest 10 arbejdsdage fra Center for Cybersikkerheds modtagelse af aftaleudkastet.

Stk. 3. Såfremt indholdet af et aftaleudkast, som en udbyder har fremsendt til Center for Cybersikkerhed på baggrund af et påbud efter stk. 1, efterfølgende ændres, skal det ændrede aftaleudkast fremsendes til Center for Cybersikkerhed, hvorefter stk. 2 atter finder anvendelse. Dette gælder dog ikke, hvis ændringerne i aftaleudkastet alene er foretaget på baggrund af Center for Cybersikkerheds tilbagemelding efter stk. 2.

§ 6. Center for Cybersikkerhed kan udstede påbud om, at endelige aftaler, der er omfattet af § 3, skal fremsendes til Center for Cybersikkerhed til orientering senest 10 arbejdsdage efter aftaleindgåelsen.

Underretning af Center for Cybersikkerhed ved ~~brud på informations~~sikkerhed~~en~~hændelser

§ 7. Udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal underrette Center for Cybersikkerhed ved ~~brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester, jf. § 8.~~sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester i form af skade på tilgængeligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester, jf. § 8.

Stk. 2. Udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal underrette Center for Cybersikkerhed ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester i form af en begivenhed, der har haft en faktisk negativ indvirkning på net og tjenesters evne til at modstå handlinger, der er til skade for fortroligheden, integriteten eller autenticiteten af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester, jf. § 9.

Stk. 3. Underretningspligten efter stk. 1 og 2 indtræder, når udbyderen bliver bekendt med, at sikkerhedshændelsen har haft væsentlig indvirkning på driften af net eller tjenester, jf. § 8 eller § 9. Underretningen skal foretages uden unødigt ophold gennem den fælles digitale løsning for indberetning til offentlige myndigheder på www.virk.dk.

§ 8. Væsentlig indvirkning på driften af net eller tjenester i form af skade på tilgængeligheden efter § 7, stk. 1, foreligger, når berørte brugertimer overstiger en af de nedennævnte grænseværdier, jf. nr.

1-6, jf. dog stk. 5. Ved berørte brugertimer forstås varigheden af den pågældende sikkerhedshændelse multipliceret med antallet af slutbrugere, der har været berørt af sikkerhedshændelsen.

1) For mobiltelefoni 35.000 brugertimer.
2) For fastnettelefoni 10.000 brugertimer.
3) For internetacces 10.000 brugertimer.
4) For tv- og radiotransmission af landsdækkende public service tv og radio 55.000 brugertimer.
5) For NUIK-tjenester 50.000 brugertimer.
6) For øvrige tjenester, som ikke er omfattet af nr. 1-5, 5.000 brugertimer.

Stk. 2. Hvis varigheden af sikkerhedshændelsen ikke kan opgøres efter stk. 1, betragtes indvirkningen som væsentlig for driften af net eller tjenester, når antallet af berørte slutbrugere overstiger en af følgende grænseværdier:

1) For mobiltelefoni 35.000 slutbrugere.
2) For fastnettelefoni 10.000 slutbrugere.
3) For internetacces 10.000 slutbrugere.
4) For tv- og radiotransmission af landsdækkende public service tv og radio 55.000 slutbrugere.
5) For NUIK-tjenester 50.000 slutbrugere.
6) For øvrige tjenester, som ikke er omfattet af nr. 1-5, 5.000 slutbrugere.

Stk. 3. Hvis antallet af berørte slutbrugere ikke kan opgøres med sikkerhed, skal udbyderne anlægge et kvalificeret skøn ved opgørelsen heraf.

Stk. 4. Indvirkningen på driften af net eller tjenester betragtes endvidere som væsentlig, jf. dog stk. 5, når:

1) Mere end 200 slutbrugere hos forsvar, politi eller beredskabsaktører har været berørt.
2) Net og tjenester til brug for beredskabssituationer eller ekstraordinære situationer har været berørt på regionalt eller nationalt serviceniveau.
3) Trafik via net og tjenester til et eller flere andre lande end Danmark ikke er mulig.
4) Mere end 50% af kapaciteten hos en udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester på en ikke brofast ø med mere end 1500 beboere har været berørt.

Stk. 5. Uanset stk. 1 og 4 foreligger der ikke væsentlig indvirkning på driften af net eller tjenester, hvis sikkerhedshændelsen har en varighed på under en time.

§ 9. Væsentlig indvirkning på driften af net eller tjenester efter § 7, stk. 2, foreligger, når den pågældende sikkerhedshændelse har berørt mere end 1.000 slutbrugere.

~~§ 8. Væsentlige følger for driften af net og tjenester efter § 7 foreligger, når antallet af berørte brugertimer overstiger en af de i stk. 2 nævnte grænseværdier, jf. dog stk. 3 og 4. Ved berørte brugertimer forstås varigheden af bruddet på informationssikkerheden multipliceret med antallet af slutbrugere, der har været berørt af det pågældende brud.~~

~~Stk. 2. Grænseværdierne efter stk. 1 udgør:~~
~~1) For mobiltelefoni 35.000 brugertimer.~~
~~2) For fastnettelefoni 10.000 brugertimer.~~
~~3) For internetacces 10.000 brugertimer.~~
~~4) For tv- og radiotransmission af landsdækkende public service tv og radio 55.000 brugertimer.~~
~~5) For øvrige tjenester, som ikke er omfattet af nr. 1-4, 5.000 brugertimer.~~

~~Stk. 3. Uanset stk. 1 foreligger der ikke væsentlige følger for driften af net og tjenester, såfremt bruddet på informationssikkerheden har en varighed på under en time.~~

~~Stk. 4. Såfremt følgerne af et brud på informationssikkerheden ikke kan opgøres tidsmæssigt, betragtes følgerne som væsentlige for driften af net og tjenester, når antallet af berørte slutbrugere overstiger en af følgende grænseværdier:~~

~~1) For mobiltelefoni 35.000 slutbrugere.~~
~~2) For fastnettelefoni 10.000 slutbrugere.~~
~~3) For internetacces 10.000 slutbrugere.~~
~~4) For tv- og radiotransmission af landsdækkende public service tv og radio 55.000 slutbrugere.~~
~~5) For øvrige tjenester, som ikke er omfattet af nr. 1-4, 5.000 slutbrugere.~~
~~Stk. 5. Såfremt antallet af berørte slutbrugere ikke kan opgøres med sikkerhed, skal udbyderne anlægge et kvalificeret skøn ved opgørelsen heraf.~~

§ 10~~9~~. Udbydere af offentligt tilgængelige elektroniske kommunikationsnet skal i nødvendigt omfang indhente oplysninger fra tjenesteudbydere, der benytter udbydernes net, med henblik på at kunne foretage underretning i medfør af § 7, herunder opgørelse efter § 8 og 9.

~~**§ 10.** Underretning i medfør af § 7 skal ske senest 14 dage efter, at det er konstateret, at bruddet på informationssikkerheden har fået væsentlige følger for driften af net og tjenester, jf. § 8.~~
~~*Stk. 2.* Underretningen skal ske gennem den fælles digitale løsning for indberetning til offentlige myndigheder på www.virk.dk.~~

§ 11. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at underrette offentligheden om en ~~brud på informations~~sikkerhedshændelse~~en~~, der har haft væsentlig~~e~~ indvirkning~~følger for~~ på ~~de udbudte~~ på driften af net eller~~og~~ tjenester, ~~såfremt~~ hvis det er i offentlighedens interesse, at sikkerhedshændelsen~~bruddet~~ offentliggøres.

§ 12. Center for Cybersikkerhed kan i særlige tilfælde underrette offentligheden om ~~brud på informationsen~~ sikkerhedshændelse~~en~~, der har haft væsentlig~~e~~ indvirkning på ~~følger for~~ driften af net eller~~og~~ tjenester, hvis~~såfremt~~ offentlighedens interesse ikke i tilstrækkelig grad tilgodeses efter § 11.
Stk. 2. Center for Cybersikkerheds underretning af offentligheden efter stk. 1 må ikke indeholde
1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el. lign., for så vidt det er af væsentlig økonomisk betydning for den udbyder, som oplysningerne angår,
2) oplysninger, ~~der~~ hvis hemmeligholdelse er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer, eller
4) oplysninger om enkeltpersoners forhold.

§ 13. Udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal informere deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe, når udbyderne bliver bekendt med en særlig og betydelig trussel om en sikkerhedshændelse i deres net eller tjenester, herunder trussel om:
1) Et BGP-hijack (border gateway protocol-hijack) mod udbyderen, hvorved data fra udbyderens netværk omdirigeres til et ondsindet netværk eller en falsk hjemmeside.
2) En kompromittering af udbyderens DNS (Domain Name Server), hvorved internettrafik dirigeres til falske og skadelige hjemmesider.
3) Kompromittering af brugeres konti eller selvbetjeningsløsninger.
4) Kompromittering af udbyderens mailsystem således, at der sendes phishingmails til brugere.
5) Scanninger mod en kendt og fortsat gældende sårbarhed i udbyderens hjemmeroutere.
6) Ondsindet SS7-trafik målrettet en eller flere kunder. Dette kan f.eks. være forsøg på opsnapning af SMS/2-faktor autentifikationskoder, indhentning af positionsoplysninger eller omdirigering af talesamtaler.
7) At driftsleverandører er kompromitteret, så kunderelaterede tjenester eller data risikerer at blive kompromitteret på tilgængelighed, fortrolighed, integritet eller autenticitet.

Stk. 2. Center for Cybersikkerhed kan på baggrund af en konkret vurdering af truslen stille krav om, at de pågældende udbydere skal informere deres brugere om selve truslen.

Aktindsigt

§ 14~~3~~. Oplysninger og underretninger modtaget af Center for Cybersikkerhed i medfør af §§ 2 og 3, § 5, stk. 1 og 3, § 6 og § 7 er i deres helhed undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Straffebestemmelser

§ 15~~4~~. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der

1) overtræder §§ 3 og 4, § 5, stk. 2 og 3, §§ 7, ~~§ 9~~ og ~~§~~ 10 og § 13, stk. 1, eller
2) undlader at efterkomme et påbud efter § 2, stk. 1, § 5, stk. 1, § 6 og § 11, eller et krav efter § 13, stk. 2.

Stk. 2. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Ikrafttrædelse

§ 16~~5~~. Bekendtgørelsen træder i kraft den xxx ~~1. januar 2020~~.

Stk. 2. §§ 3-6 finder ikke anvendelse på aftaleforhandlinger, der er indledt før den 1. juli 2016.

Stk. 3. Bekendtgørelse nr. 1256~~566~~ af 27~~1~~. november~~juni~~ 2019~~6~~ om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed ophæves.

Center for Cybersikkerhed, den xx. xx 2021

Thomas Lund-Sørensen

/ Anette Arnsted

1) Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36~~2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), EU-Tidende 2002, nr. L 108, side 33, som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009~~.