Lovtidende A

2016

Udgivet den 3. juni 2016

1. juni 2016. Nr. 566.

Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed[1)]

I medfør af § 4, § 7 og § 14, stk. 2, i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed 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 corenet 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 net og tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.
3) Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester:
   a) Udbydere af net, 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.

Afgivelse af oplysninger til Center for Cybersikkerhed

§ 2. Center for Cybersikkerhed kan udstede påbud om, at erhvervsmæssige udbydere af offentligt tilgængelige net 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 net 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

[1)] Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 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.

AG000719

Forsvarsmin.,
Center for Cybersikkerhed, j.nr. 2015/002263

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 informationssikkerheden

§ 7. Udbydere af offentligt tilgængelige net og tjenester skal underrette Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester, jf. § 8.

§ 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.

§ 9. Udbydere af offentligt tilgængelige net 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.

§ 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 være skriftlig og indeholde de i bilag 1 angivne oplysninger.

§ 11. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige net og tjenester at underrette offentligheden om brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester, såfremt det er i offentlighedens interesse, at bruddet offentliggøres.

§ 12. Center for Cybersikkerhed kan i særlige tilfælde underrette offentligheden om brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester, 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 er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer, eller
4) oplysninger om enkeltpersoners forhold.

Aktindsigt

§ 13. 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

§ 14. 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, eller
2) undlader at efterkomme et påbud efter § 2, stk. 1, § 5, stk. 1, § 6 og § 11.

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

Ikrafttrædelse

§ 15. Bekendtgørelsen træder i kraft den 1. juli 2016.

Stk. 2. §§ 3-6 finder ikke anvendelse på aftaleforhandlinger, der er indledt før bekendtgørelsens ikrafttræden.

Center for Cybersikkerhed, den 1. juni 2016

THOMAS LUND-SØRENSEN

/ Jon Bach Holm

Bilag 1

Skema til brug for underretning ved brud på informationssikkerheden, jf. § 10, stk. 2

1. Virksomhed og kontaktoplysninger vedrørende denne underretning:
2. Tidspunkt for og varighed af hændelsen: *(Hvis hændelsen ikke er afsluttet, angives dette)*
3. Beskrivelse af hændelsen:
4. Hvor har hændelsen fundet sted? :
5. Hvilke net og tjenester har været berørt? :
6. Hvor mange slutbrugere har været berørt? :
7. Hvilke geografiske områder har været berørt? :
8. Hvilke tiltag er blevet iværksat? :
9. Er de berørte net og tjenester blevet retableret? Hvis nej, hvornår forventes dette at ske? :
10. Er de berørte brugere (evt. andre) blevet informeret og hvordan? :
11. Andre oplysninger af betydning: *(Der kan evt. oplyses yderligere om hændelsens konsekvenser, herunder om hændelsen berører samfundsvigtige funktioner, beredskabsmyndigheder m.m.)*

12. Udfærdiget af og udfærdigelsestidspunkt:

Underretningen sendes til teletilsyn@cfcs.dk. Såfremt underretningen indeholder sensitive oplysninger, kan der ved henvendelse til Center for Cybersikkerhed træffes nærmere aftale om fremsendelse af underretningen.