

U d k a s t

Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

I medfør af § 3, stk. 5, i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, som ændret ved lov nr. xx af xx, fastsættes:

Aftale om tilslutning

§ 1. Tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste sker for regioner og kommuner samt virksomheder, der har samfundsvigtig karakter, jf. § 3, stk. 3, i lov om Center for Cybersikkerhed, ved indgåelse af aftale med Center for Cybersikkerhed, jf. dog § 2.

Stk. 2. Tilslutningsaftalen med Center for Cybersikkerhed kan omfatte:

- 1) Opsætning og drift af en eller flere alarmerheder,
- 2) installation og drift af sikkerhedssoftware på lokale enheder, og
- 3) løbende overførsel af logoplysninger og oplysninger om konstaterede og mulige sikkerhedshændelser fra eget sikkerhedssystem, herunder ved opsætning og drift af udstyr fra Center for Cybersikkerhed til håndtering af den løbende dataoverførsel.

Stk. 3. Det skal af tilslutningsaftalen fremgå, om data hidrørende fra den tilsluttede virksomhed, region eller kommune er omfattet af sletterreglerne i § 17, stk. 2, nr. 2, i lov om Center for Cybersikkerhed.

Påbud om tilslutning

§ 2. Center for Cybersikkerhed kan i særlige tilfælde påbyde virksomheder, der har særligt samfundsvigtig karakter, samt regioner og kommuner at blive tilsluttet netsikkerhedstjenesten med henblik på monitorering af netværkskommunikation, jf. § 3, stk. 4, i lov om Center for Cybersikkerhed. Påbuddet kan kun omfatte de dele af virksomheden, regionen eller kommunen, der har en væsentlig betydning for Danmarks kritiske infrastruktur.

Stk. 2. Ved vurderingen af, om en virksomhed, region eller kommune er omfattet af stk. 1, skal Center for Cybersikkerhed lægge vægt på, om virksomheden, regionen eller kommunen beskæftiger sig med aktiviteter eller råder over informationssystemer og digital infrastruktur af en sådan betydning, at en sikkerhedshændelse vil kunne medføre konsekvenser for nationale sikkerhedsinteresser, jf. stk. 3.

Stk. 3. Ved nationale sikkerhedsinteresser, jf. stk. 2, forstås i denne bekendtgørelse landets suverænitet, territoriale integritet og demokratiske styreform samt interesser knyttet til:

- 1) De øverste statsorganers virksomhed, sikkerhed og handlefrihed,
- 2) forsvar, sikkerhed og beredskab,
- 3) forholdet til andre stater og internationale organisationer,

- 4) landets økonomiske stabilitet og handlefrihed, og
- 5) befolkningens grundlæggende sikkerhed og velfærd.

Stk. 4. Påbud kan kun meddeles, såfremt mindre indgribende midler ikke er tilstrækkelige, og påbuddet ikke står i misforhold til tilslutningens betydning for sikringen af Danmarks kritiske infrastruktur. Påbuddet må ikke gå videre end det, der er nødvendigt af hensyn til formålet med påbuddet.

Stk. 5. Afgørelse om påbud forudsætter enighed mellem Center for Cybersikkerhed og tilsynsmyndigheden i den relevante sektor.

Stk. 6. Påbud omfatter netsikkerhedstjenestens monitorering gennem opsætning og drift af en eller flere alarmerheder, jf. § 1, stk. 2, nr. 1.

Stk. 7. Afgørelsen om påbud skal mindst indeholde:

- 1) En begrundelse med henvisning til de retsregler, i henhold til hvilke afgørelsen er truffet, og angivelse af de hovedhensyn, der har været bestemmende for skønsudøvelsen, samt en redegørelse for de oplysninger vedrørende sagens faktiske omstændigheder, som er tillagt betydning for afgørelsen, jf. principperne i forvaltningslovens §§ 22 og 24.
- 2) En vejledning om klageadgang med angivelse af klageinstans og oplysning om fremgangsmåden ved indgivelse af klage, jf. principperne i forvaltningslovens § 25.
- 3) Oplysning om, hvorvidt data hidrørende fra den pågældende virksomhed, region eller kommune er omfattet af slettereglerne i § 17, stk. 2, nr. 2, i lov om Center for Cybersikkerhed.
- 4) En standardbeskrivelse af Center for Cybersikkerheds behandling af personoplysninger, som virksomheden, regionen eller kommunen kan anvende til at informere organisationens medarbejdere.

Stk. 8. Center for Cybersikkerhed skal løbende vurdere, om forudsætningerne for et meddelt påbud fortsat er tilstede. Hvis det ikke er tilfældet, skal påbuddet tilbagekaldes eller justeres uden unødigt ophold. Center for Cybersikkerhed skal uanset 1. og 2. pkt. mindst hvert halve år vurdere, om et meddelt påbud skal opretholdes, jf. § 3, stk. 4, i lov om Center for Cybersikkerhed.

§ 3. En virksomhed, region eller kommune, der er meddelt et påbud i medfør af § 2, skal loyalt medvirke til netsikkerhedstjenestens opsætning og drift af en eller flere alarmerheder. Opsætning, konfiguration, drift og nedtagning af alarmerheder foretages af netsikkerhedstjenesten på virksomhedens, regionens eller kommunens lokaliteter.

Stk. 2. En virksomhed, region eller kommune, der er meddelt et påbud, skal efter anmodning fra Center for Cybersikkerhed stille de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten til brug for opsætning og drift af alarmerheder, herunder:

- 1) Oversigt over netarkitektur og segmentering.
- 2) Liste over netværkssystemer og infrastrukturkomponenter, herunder type og funktion.
- 3) Liste over ip-adresser, der håndterer netværksbaserede tjenester, og allokering af disse.
- 4) Angivelse af, hvilke dele af driften af den digitale infrastruktur, der varetages af eventuelle driftsleverandører.

Stk. 3. Det påhviler herudover den virksomhed, region eller kommune, der er meddelt et påbud:

- 1) At stille den nødvendige fysiske, tekniske og netværksmæssige understøttelse til rådighed.
- 2) At sikre, at der ikke foretages fysiske, tekniske og netværksmæssige ændringer, som kan påvirke driften af alarmerhederne, med mindre dette på forhånd er aftalt med netsikkerhedstjenesten.

3) At sikre, at der er etableret passende sikkerhedsforanstaltninger for adgang til netsikkerhedstjenestens alarmerheder og tilhørende udstyr.

Stk. 4. Den virksomhed, region eller kommune, der er meddelt et påbud, skal endvidere angive kontaktoplysninger til medarbejdere, herunder medarbejdere hos eventuelle driftsleverandører, der kan kontaktes i forbindelse med opsætning og drift af alarmerheder, herunder i forbindelse med eventuelle sikkerhedshændelser.

Stk. 5. Den virksomhed, region eller kommune, der er meddelt et påbud, skal sikre, at netsikkerhedstjenesten uden unødigt ophold informeres om ændringer i oplysninger omfattet af stk. 2.

Stk. 6. Den virksomhed, region eller kommune, der er meddelt et påbud, skal sikre, at eventuelle driftsleverandører i nødvendigt omfang medvirker til opsætning og drift af alarmerhederne i overensstemmelse med stk. 1, samt stiller de nødvendige oplysninger omfattet af stk. 2 til rådighed for virksomheden, regionen eller kommunen.

Ansvarsforhold

§ 4. Den eller de alarmerheder, som opsættes i medfør af tilslutningsaftalen, jf. § 1, stk. 2, nr. 1, eller i medfør af § 2, stk. 6, er Center for Cybersikkerheds ejendom, og centeret er at betragte som dataansvarlig for data, der indsamles og i øvrigt behandles i forbindelse med driften af alarmerheden.

Stk. 2. Ved installation og drift af sikkerhedssoftware på lokale enheder, jf. § 1, stk. 2, nr. 2, er Center for Cybersikkerhed at betragte som dataansvarlig for den behandling, der foretages ved hjælp af sikkerhedssoftwaren.

Stk. 3. Ved løbende overførsel af oplysninger fra eget sikkerhedssystem til Center for Cybersikkerhed, jf. § 1, stk. 2, nr. 3, er Center for Cybersikkerhed at betragte som dataansvarlig for data, når data er videregivet til centeret, herunder til eventuelt installeret udstyr tilhørende centeret.

Straffebestemmelser

§ 5. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der overtræder § 3.

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

Ikrafttrædelse

§ 6. Bekendtgørelsen træder i kraft den 1. juli 2019.

Stk. 2. Bekendtgørelse nr. 1599 af 14. december 2018 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste ophæves.