FORSVARETS EFTERRETNINGSTJENESTE

NOTAT

Erfaringsnotat vedrørende net- og informationssikkerhedsloven

Center for Cybersikkerheds generelle erfaringer med net- og informationssikkerhedsloven

Dato: 3. december 2019

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 66
E-mail: fe@fe-mail.dk
www.fe-ddis.dk

I dette notat beskrives de erfaringer, som Center for Cybersikkerhed har indhøstet ved anvendelse af lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed (net- og informationssikkerhedsloven).

I forbindelse med udvalgsbehandlingen af lovforslaget til loven besvarede forsvarsministeren den 17. november 2015 spørgsmål nr. 2, hvoraf fremgår, at ministeren er indstillet på, at der udarbejdes en rapport med erfaringerne med loven, som oversendes til Folketinget tre år efter lovens ikrafttræden. Til brug for rapporten indhentes bidrag fra Center for Cybersikkerhed og Tilsynet med Efterretningstjenesterne. Dette notat udgør Center for Cybersikkerheds bidrag.

Det er Center for Cybersikkerheds erfaring, at loven har skabt konstruktive rammer og incitamentsstrukturer, der har sikret, at samarbejdet omkring teleudbydernes sikkerhedsmæssige indsats har været tilfredsstillende. Teleudbyderne har således generelt medvirket positivt og konstruktivt til at fremme net- og informationssikkerheden i samfundet. Center for Cybersikkerhed er også af den klare opfattelse, at de tilsyns- og påbudsmuligheder, der fremgår af loven, er meget væsentlige for at fastholde det konstruktive samarbejde mellem tilsynsmyndigheden (Center for Cybersikkerhed) og teleudbyderne.

Det er Center for Cybersikkerheds erfaring, at loven gennem dens krav til udbyderne har medvirket til at opfylde lovens formål om at fremme net- og informationssikkerheden i samfundet, og at der således ikke er et aktuelt behov for ændringer af loven.

Risikobaseret tilgang til informationssikkerhed
Loven har sikret en regelmæssig dialog mellem Center for Cybersikkerhed og de danske udbydere med henblik på at sikre, at udbyderne gennemfører en risikobaseret tilgang til tekniske, processuelle og organisatoriske foranstaltninger med henblik på at opretholde et passende informationssikkerhedsniveau i deres net og tjenester.

Oplysning og underretning
Oplysningspligterne har styrket Center for Cybersikkerheds overblik over udbydernes infrastruktur, herunder hvilke produkter og leveran-

dører der anvendes. Det er erfaringen fra dialogen med teleudbyderne, at disse generelt har inddraget nærmere angivne trusler mod informationssikkerheden i deres risikostyring.

Derudover skal væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester 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.

Denne oplysningspligt har givet Center for Cybersikkerhed mulighed for, hvor det efter centerets skøn har været af væsentlig samfundsmæssig betydning, at indgå i en teknisk dialog med udbyderen om implementering af konkrete informationssikkerhedsforanstaltninger i det endelige kontraktudkast. Som eksempel kan nævnes de eksisterende og kommende aftaler om 5G-leverancer til de danske teleudbydere.

De væsentlige erhvervsmæssige udbydere har generelt efterlevet kravet og så betids, at det ikke indtil nu har været nødvendigt at udnytte CFCS' mulighed for at iværksætte en 10-arbejdsdages "standstill-periode", som loven giver mulighed for, før den endelige aftale kan indgås.

De tilfælde, hvor Center for Cybersikkerhed har indgået i dialog med udbyderne inden indgåelse af kontrakt, er Center for Cybersikkerheds ønsker til specifikke sikkerhedskrav i alle tilfælde imødekommet i det endelige aftaleudkast. Center for Cybersikkerhed har derfor ikke haft anledning til at anvende muligheden for at udstede påbud til udbyderne om at træffe konkrete foranstaltninger.

Det er dog fortsat Center for Cybersikkerheds vurdering, at eksistensen af standstill-perioden og påbudsmulighederne medvirker til at sikre det fornødne incitament hos ovennævnte udbydere til at påbegynde en tidlig dialog med Center for Cybersikkerhed om kommende leverancekontrakter.

Som andet element påhviler der udbydere en underretningspligt der har sikret, at Center for Cybersikkerhed løbende er blevet orienteret om driftsproblemer i den danske teleinfrastruktur, hvilket især er nødvendigt, hvis en krisesituation kræver national koordinering.

Beredskabssituationer

Krav om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer, har efter Center for Cybersikkerheds erfaring styrket beredskabsarbejdet hos udbyderne. Det er Center for Cybersikkerheds erfaring, at specielt erhvervsmæssige og væsentlige erhvervsmæssige udbydere har fået udarbejdet beredskabsplaner, som i et omfang, det ikke har været tilfældet tidligere, nu er baseret på en dokumenteret og ledelsesforankret risikostyringsproces.

Der har i lovens levetid ikke været en beredskabssituation eller anden ekstraordinær situation, hvor Center for Cybersikkerhed har haft behov for efter lovens § 5, stk. 3, at koordinere og prioritere beredskabsaktørers behov for samfundsvigtig elektronisk kommunikation.

Aktindsigt
Enkelte udbydere har i dialogen med CFCS udtrykt ønske om, at en straksrapportering i forbindelse med aktivering og deaktivering af teleudbyderens interne beredskab fritages for aktindsigt i sin helhed.

Tilsyn
Center for Cybersikkerhed har gennem lovens hidtidige levetid udført en række tilsyn om efterlevelse af loven og tilhørende bekendtgørelser.

Det er Center for Cybersikkerheds erfaring, at hvor disse tilsyn har afdækket mangler eller uhensigtsmæssigheder i forhold til lovgivningen, har berørte udbydere i dialog med Center for Cybersikkerhed efterfølgende justeret deres praksis i overensstemmelse med lovgivningens hensigt.

Der var i forbindelse med lovens vedtagelse en i diskussion om Center for Cybersikkerheds mulighed for som tilsynsmyndighed uden retskendelse at få adgang til udbydernes og udbydernes samarbejdspartneres forretningslokaler med henblik på at påse overholdelse af loven.

I lovens endelige udformning blev det i § 9, stk. 6 og 7, fastsat, at en sådan adgang kun kunne ske efter et skriftligt varsel på mindst 7 arbejdsdage.

Det er Center for Cybersikkerheds erfaring, at disse bestemmelser ikke har givet anledning til praktiske problemer. Center for Cybersikkerhed har de gange, hvor centeret i forbindelse med tilsyn har haft behov for at få adgang til udbydernes eller udbydernes samarbejdspartneres forretningslokaler, fået sikret en sådan adgang gennem dialog med udbyderne og typisk med en kortere frist end de 7 dage.

Det har i praksis vist sig, at i de tilfælde, hvor en udbyder har outsourcet dele af nettet eller driften heraf til udlandet, har udbyderen, efter råd fra Center for Cybersikkerhed, samtidig kontraktmæssigt sikret sig, at Center for Cybersikkerhed har mulighed for at assistere og rådgive udbyderen i dennes tilsyn med samarbejdspartneren i udlandet.

Konklusion
Det er Center for Cybersikkerheds erfaring, at loven gennem dens krav til udbyderne har medvirket til at opfylde lovens formål om at fremme net- og informationssikkerheden i samfundet, og at der således ikke er et aktuelt behov for ændringer af loven.