PROSA
Forbundet af It-professionelle

Association of IT Professionals
Vester Farimagsgade 37A
1606 København V

Søren Frichs Vej 38K
8230 Åbyhøj

Overgade 54
5000 Odense

prosa.dk
+45 33 36 4141

Forsvarsministeriet
Holmens Kanal 9
1060 København K
fmn@fmn.dk
Cc: tbl@fmn.dk, sbu@fmn.dk

København, 4. februar 2019

Høringssvar om *Initiativer til styrkelse af cybersikkerheden (2018/006599)*

Forsvarsministeriet har udsendt udkast til ændring af lov om Center for Cybersikkerhed (CfCS). PROSA – Forbundet af It-professionelle er blevet inviteret til at udtale sig om udkastet.

Test af sikkerhed

Lovforslaget lægger op til at teste de tilsluttede organisationers sikkerhed.

Ligesom det er en god idé at tjekke, at fødevarereglerne overholdes, så er det også en god idé at teste, at organisationerne lever op til de IT-forskrifter, som de har forpligtet sig til.

Det skal naturligvis ske på en ansvarlig måde: Det giver ikke mening at lave en penetrationstest på en organisation, hvor ledelsen ikke har prioriteret at leve op til forskrifterne. Ledelsen bør jævnligt afholde beredskabsøvelser, hvor sikkerheden testes, og CfCS kunne være med til at afholde disse.

Vi betragter grundlæggende IT-sikkerhed på linje med GDPR som et ledelsesansvar, hvorfor vi som udgangspunkt mener, at evt. sanktioner i forbindelse med test af IT-sikkerhed skal lægges på ledelsen. En undtagelse kan være, hvis en medarbejder handler i ond tro, hvilket vi mener, eksisterende lovgivning dækker fint.

I øvrigt finder PROSA det bekymrende, at en statslig myndighed skal have mulighed for at optræde under fordækte identiteter, anspore ansatte til ulovligheder, få dén medarbejder, hvis identitet de har overtaget, til at "reagere hensigtsmæssigt", hvis den berørte medarbejder henvender sig, og dermed er med til at kompromittere en kollega og i det hele taget, at det skal være nødvendigt med dén slags beføjelser for at sikre et fornuftigt sikkerhedsniveau i danske virksomheder og institutioner.

Stor udvidelse af beføjelser

Lovforslaget lægger op til en drastisk udvidelse af CfCS' beføjelser. Således vil CfCS installere sikkerhedssoftware på såvel servere som klienter. Dette er for at kunne monitorere data, der sendes krypteret. Sikkerhedssoftware vil også kunne tilgå harddiskene på disse maskiner.

Det betyder i princippet, at CfCS vil kunne læse:

- Alle data, der flyder ind og ud af organisationen
- Alle data, der ligger på alle harddiskene

Oven i dette vil CfCS kunne tvinge organisationer til at tilslutte sig.

Dette er væsentligt udvidede beføjelser til CfCS virke. Forventeligt vil CfCS ikke misbruge disse beføjelser og vil næppe heller kræve udrulning af sikkerhedssoftwaren på alle maskiner hos alle tilsluttede, men loven giver disse beføjelser, hvilket i sig selv er problematisk.

Alle æg i én kurv

Der findes ikke 100 % sikkerhed. Det tilbyder CfCS da heller ikke. Derfor bør man overveje, hvad der vil ske, hvis CfCS bliver kompromitteret – det kan f.eks. ske via et digitalt angreb eller via medarbejdere, som bliver afpresset.

Et velkendt eksempel er Stuxnet, som var en virus, der blev udviklet til at angribe iranske uranberigelsescentrifuger, og som det lykkedes at få ind i berigelsesanlægget på trods af de skrappe sikkerhedsforanstaltninger, der helt sikkert har været. Et succesfuldt angreb er derfor ingenlunde et utænkeligt scenarie. Med de muligheder, som sikkerhedssoftwaren giver, vil muligheden for at kunne få adgang til at fjernstyre sikkerhedssoftwaren være et meget værdifuldt mål, som man sagtens kunne forestille sig, at organisationer med budget som nationalstater ville prioritere. PROSA er bekymret for, at ved at putte alle æg i én kurv, så udsætter man sig for en unødig risiko.

En bedre løsning vil være at gøre, som vi gør med bankerne: Her er der ikke én enkelt organisation, der har adgang til alle bankers data. Derimod er der skarpt opdelte organisationer, så hvis én bank bliver kompromitteret, så vil det ikke betyde, at alle andre banker samtidigt er kompromitterede.

CfCS's rolle kunne da være at hjælpe med at sikre de forskellige organisationer, uden at CfCS selv ville få adgang til udstyret.

Mangel på transparens

CfCS ligger under Forsvarets Efterretningstjeneste (FE). Det er helt naturligt, at der nødvendigvis må være et center under FE, som kan udveksle hemmeligt stemplede informationer med udenlandske efterretningstjenester. Det er fuldt forståeligt, at befolkningen ikke kan få adgang til visse informationer, som efterretningstjenesterne indhenter.

Men centerets virke bør være begrænset til de elementer, som *kun* kan varetages af en efterretningstjeneste – de elementer, der kan varetages af et ikke-militært center, bør ligge i en civil del, der ikke er underlagt samme begrænsninger i indsigt.

Rollen som Danmarks nationale IT-sikkerhedsmyndighed og nationalt kompetencecenter mener PROSA bedre ville kunne varetages uden for efterretningstjenesterne (f.eks. som et center under Indenrigsministeriet). Derved kan borgerne få indsigt i omfanget af centerets virke – en indsigt som borgerne er frataget ved at lægge centeret under FE.

PROSA foreslår derfor, at man, i stedet for at give CfCS meget vidtgående beføjelser, opdeler CfCS i et civilt CfCS (f.eks. under Indenrigsministeriet) og i et militært CfCS (som forbliver under FE). Det civile center vil da kunne blive det nationale kompetencecenter, der hjælper myndigheder og virksomheder med at sikre deres IT-infrastruktur. En udveksling af viden mellem de to centre vil selvfølgelig være en naturlig del, men vi ser ingen grund til, at de dele, der er uproblematiske at give befolkningen indsigt i, tilbageholdes med henvisning til, at centeret hører under FE.

Opsummering

Det er PROSAs opfattelse, at frem for at udstyre CfCS med så omfattende beføjelser i en organisation uden nævneværdig demokratisk kontrol bør centerets opgave være at opstille sikkerhedskriterier og niveauer for de virksomheder og institutioner, som arbejder med samfundskritiske opgaver. Herudover kunne der være en opgave med at kontrollere, at de pågældende sikkerhedsforskrifter overholdes, evt. gennem et samarbejde med virksomheder, som udbyder digitale sikkerhedsløsninger. Herved undgås, at der sker en centralisering af data med en øget sårbarhed til følge, og det giver de enkelte virksomheder og institutioner mulighed for selv at vælge, hvilke sikkerhedssystemer der passer til deres forretning.

Venlig hilsen

Niels Bertelsen

Formand