Konsekvenserne af lovforslaget om Center for Cybersikkerhed

/ C-cure

Mette Nikander, Direktør

Det er positivt….

- at man ønsker at fokusere i langt højere grad på vores IT Sikkerhed og digitale integritet.
- at der søges et lovgrundlag for CFCS virke.
- at man tager udgangspunkt i ”Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.”
- at analysen af de pakkedata som CFCS' prober opsamler i civile netværk, kun må "finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen”.

Sikkerhedshændelse

Man tager i lovforslaget flere steder udgangspunkt i sikkerhedshændelser.

En sikkerhedshændelse er beskrevet, som en hændelse der negativt påvirker, eller **vurderes** at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester

Det at der er tale om en *vurdering*, kan åbne for en vid fortolkning, fordi det i princippet ud fra en masse øvrige hændelser på andre "områder", kan vurderes at være nødvendigt eller passende at foretage overvågning, på et nyt "område".

Vi risikerer med andre ord at der uberettiget vurderes associerede interesser mellem parter, til begrundelse for periodisk systematisk overvågning.

Placering

CFCS placering under FE, undtager CFCS for persondataloven. **Men CFCS skal udføre civile opgaver.**

Det foreslås derfor, at CFCS i det hele adskilles fra FE og lægges i en separat forvaltningsmyndighed beskyttet af persondataloven.

Insisterer man på en placering under FE, så bør CFCS, **som minimum placeres i en, separat IT sikkerhedsafdeling underlagt persondataloven**, men selvfølgelig således at der der tages nødvendige mindre forbehold i forhold til, at det skal ligge under FE.

Forvaltningsmyndigheden, der skal spore, overvåge og hindre cyberangreb, **skal være underlagt almindelige forvaltningsretlige principper** for indsigt, åbenhed og kontrol, samt retsplejelovens krav om retskendelse ved indgreb i meddelelseshemmeligheden.

Placering

Da persondataloven i lovforslaget ikke gælder for CFCS, er der derfor givet **retningslinjer** ud for behandling af personoplysninger**, men det er kun retningslinjer, der fastsætter en række bestemmelser. Det er ikke en eksakt lovgivning.**

Det at man vil lave retningslinjer i loven for at kompensere for det "tab" af retslighed virksomheder og personer i modsat fald vil bevare, er ikke godt nok.

Retningslinier kan ikke bruges ved en domstol, men kun ved tjenestelige sager.

Desuden bør **CFCS aktiviteter** tilrettelægges således, at netsikkerhedstjenesten **i mindst muligt omfang konkurrerer med private udbydere** af sammenlignelige services. Hvilket der ellers åbnes for under lovforslagets §6 og §7. Netsikkerhedstjenestens tilsluttede virksomheder bør være så få (i øvrigt offentliggjorte) virksomheder som muligt.

Meddelelseshemmelighed

GovCert har lige nu adgang til betydelige dele af kommunikationen mellem borgere/virksomhederne og staten og **CFCS vil på sigt få endnu bredere adgang ,også til kommunikationen med øvrige offentlige myndigheder.**

Man påtænker endda at få lov til at bryde krypteret kommunikation, men hvis det er for at hindre kriminalitet, så vil de kriminelle jo blot finde andre kommunikationsveje end gennem Nettjenestens tilsluttede virksomheder.

Der gribes derved ind i Grundlovens passus om **meddelelseshemmelighed** og i retten til privatlivets fred, men også i borgernes og virksomhedernes retssikkerhed, som de beskyttes af i persondataloven.

Brud på kryptering bør kun ske, hvis der ligger en retskendelse og at Tilsynet informeres forinden.

En nødlem

Kapitel 4, Indgreb i meddelelseshemmeligheden
Dette kapitel kan i princippet være en nødlem for Center for Cybersikkerhed, der kan refereres til under andre paragraffer, hvilket der også gøres flere steder.
Man kan uden retskendelse behandle pakke og trafikdata hidrørende fra netværk hos tilsluttede myndigheder, også Forsvarets område,- og virksomheder**. Og meget vil være efter vurdering om nødvendighed…derfor bliver et effektivt tilsyn vigtigt.**

Der henvises f.eks. i §11 og §12 til kapitel 4, når der tales om, at der ikke må behandles, videregives og analyseres personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og personoplysninger om helbredsmæssige og seksuelle forhold eller strafbare forhold **med mindre behandlingen er nødvendig for varetagelsen af CFCS opgaver, er til beskyttelse** af væsentlige hensyn til statens sikkerhed eller rigets forsvar **eller at behandlingen vedrører personoplysninger der er omfattet af kapitel 4**

Kapitel 9, Tilsyn med behandling af personoplysninger
§21, **Den væsentligste nødlem - Stk.3, CFCS kan undtagelsesvist beslutte ikke at følge en henstilling fra Tilsynet og skal da blot underrette Tilsynet herom og uden unødigt ophold forelægge sagen for forsvarsministeren til afgørelse.**

Behandling af personoplysninger

Vedr. kapitel 6 , Behandling af personoplysninger i CFCS

Det er kritisabelt at det i §9 indikeres at indsamling af personoplysninger ikke anses uforenelige med senere formål, som at indsamle historiske, statistiske eller videnskabelige øjemed. Indsamling bør udelukkende være af sikkerhedsmæssig karakter.

I §10 om behandling af personoplysninger og i §12 om videregivelse af disse, angives at de da kun må finde sted hvis;

6)Behandlingen er nødvendig for at CFCS eller **den tredjemand til hvem oplysningerne videregives, kan forfølge en berettiget interesse** og hensynet til den pågældende person ikke overstiger denne interesse.

Vil Tilsynet være med til at vurdere dette grundigt nok, eller kun ved stikprøver involveres?

Databehandling og deling

I lov om Politiets Efterretningstjeneste, og Lov for Forsvarets Efterretningstjeneste, åbnes der for indsamling , analyse, bearbejdning m.m. af data, som også kan udveksles under rammer af et etableret gensidigt samarbejde med udenlandske myndigheder….**CFCS /GOVCERT bør kun dele data med disse myndigheder efter Tilsynets og ministeriets vurdering og forudgående accept**.

Pakkedata bør slettes efter 1 måned også hvis de er videregivet til udlandet.

Vi bør nuanceret forholde os til andre landes lovgivning og efterretningstjenester der til tider er er meget åbne for indsigt i data og åbne for industrispionage.
I enhver henseende at data deles med tredje part bør Tilsynet samtykke forinden!

Tilsyn

Lovforslaget angiver at CFCS skal træffe passende tekniske og organisatoriske foranstaltninger mod oplysninger tabes forringes, misbruges eller kommer uvedkommende i hænde.

Med reference til de nylige sager med NETS, IBM, Se og Hør etc. Hvor f.eks. Finanstilsynet og Datatilsynet ikke har udfyldt sin rolle tilfredsstillende**, er det vigtigt at Tilsynet hyppigt og effektivt tilsikrer, at dette også sker, som ønsket og løbende overholdes.**

§23 Tilsynets virksomhed er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens §13
Det fordrer stor tillid til Tilsynet og at der ikke må kunne opstå interessekonflikter i Tilsynet.

Der skal nedsættes et Tilsyn udenfor "Tilsynet med Efterretningtjenesterne". Tilsynet skal have omfattende it-revisionsmæssige og tekniske sagkundskaber og stærke juridiske kompetencer, før at man kan tilsikre at borgernes og virksomhedernes rettigheder overholdes.

Loven om CFCS, når den er vedtaget, bør revideres efter 2 år, for at vi derved har mulighed for at korrigere og indrette loven, efter den teknologiske udvikling, menneskerettighedshensyn, konkurrencehensyn, behov for videndeling m.m.

Tak for Jeres tid

Mette Nikander: mn@c-cure.dk
Tlf. 45 41 14 46
www.c-cure.dk