TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Center for Cybersikkerhed

Sendt pr. e-mail til
fe@fe-mail.dk
fe-4418@feddis.

Sagsnr.: 2020/001583.

4. februar 2021

Høring over udkast til bekendtgørelser om sikkerhed i net og tjenester

Teleindustrien (TI) har noteret sig, at Center for Cybersikkerhed den 7. januar 2021 har sendt udkast til 4 reviderede bekendtgørelser om sikkerhed i net og tjenester i høring med frist den 4. februar 2021, kl. 12.

En velfungerende og sikker teleinfrastruktur er afgørende for det danske samfund, teleselskabernes kunder og naturligvis også branchen selv. Med det afsæt har branchen over de seneste 10 år investeret 70 mia. kr. i at udbygge den digitale infrastruktur i Danmark med fokus på både kapacitet og sikkerhed. Udbygningen er sket i tæt dialog med danske myndigheder, herunder særligt Center for Cybersikkerhed.

TI har forståelse for, at bekendtgørelserne opdateres som følge af de ændringer, der er gennemført ved lov nr. 1831 af 8. december 2020 om ændring af lov om net- og informationssikkerhed, med henblik på implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation (Koden) herunder, at anvendelsesområdet udstrækkes til at omfatte udbydere af nummeruafhængig interpersonelle kommunikationstjenester (NUIK-tjenester).

TI har dog også noteret sig, at nogle af bekendtgørelserne indeholder yderligere skærpende ændringer, end der er nødvendige i forhold at sikre en EU-konform implementering af Koden. CFCS har ikke begrundet, hvorfor disse ændringer er nødvendige, og TI finder ikke, at der er tilstrækkeligt grundlag for at foretage sådanne skærpelser over for teleselskaberne. TI skal i den forbindelse henvise til, at Forsvarsministeren den 12. november 2020 i en besvarelse til Folketingets Forsvarsudvalg udtalte følgende:

> *"I forhold til de traditionelle teleudbydere vil lovforslaget som udgangspunkt kun indebære, at der foretages mindre justeringer af de eksisterende rammer i lov om net- og informations-*

sikkerhed. Lov om net- og informationssikkerhed er en rammelov, som i dag er udmøntet i fire bekendtgørelser.

Lovforslaget ændrer ikke ved lovens grundlæggende struktur. Strukturen, hvor den detaljerede regulering sker i bekendtgørelser, er valgt for at give mulighed for, at reglerne løbende kan tilpasses den hastige udvikling i teknologi, best practices og trusselsbilledet. Samtidig giver strukturen den bedste mulighed for at tage højde for anbefalinger fra EU's Agentur for Cybersikkerhed (ENISA), der bl.a. har til opgave at fremme medlemsstaternes samordning på området."

TI skal derfor anmode CFCS om nærmere at redegøre for, hvorfor de skærpede regler anses for at være nødvendige, henset til ministerens udtalelse.

På den baggrund har TI i det følgende kommenteret på ændringerne i bekendtgørelserne.

Generelt skal TI opfordre CFCS til at udarbejde **vejledninger** til de enkelte bekendtgørelser, så det bliver lettere for udbyderne at efterleve reglerne, herunder få en bedre forståelse af CFCS' praksis og fortolkning af de enkelte regler. Fx vil det være nyttigt at få en nærmere forståelse af, hvilke typer af tjenester der omfattes af definitionen "NUIK-tjenester".

Ud over ovennævnte bemærkninger har TI ikke yderligere bemærkninger til **bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv**.

Til **bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet for sikkerhed i net og tjenester** har TI følgende bemærkninger:

TI foreslår, at det tydeliggøres, hvilke medarbejdere som skal sikkerhedsgodkendes, om godkendelsen skal ske til PET-HEM eller FE-HEM, samt hvilket udstyr der er omfattet af følgende "adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden". Efter TI's opfattelse bør de pågældende systemer afgrænses til de særlige systemer, hvor det kan identificeres, at der foretages et konkret indgreb.

Til **bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og Informationssikkerhed i net og tjenester** har TI følgende bemærkninger:

§1: Definition af, hvad der er "Kritiske netkomponenter", er ikke ændret. TI har dog tidligere i forbindelse med vedtagelsen af første udgave af bekendtgørelsen og i forbindelse med høringen over lovforslag til lov om leverandørsikkerhed peget på, at definitionen i prak-

sis er meget bred og også rammer systemer og komponenter, der ud fra en sikkerhedsfaglig vurdering ikke er kritiske.

De anvendte begreber som fx "operations support systemer" og "business support systemer" udgør ikke nogen entydig branchemæssig forståelse, hvorved stort set alle IT-systemer, der anvendes i en teleudbyders forretning, herunder tjenesteudbydere, der ikke har eget netværk, men anvender egne support-systemer, bliver omfattet. Det er også uklart, hvad der forstås ved "centrale routere og servere i backbonenettet". Der er ingen afgrænsning af, hvad der er "centrale" og "ikke-centrale" routere. Udbyderne er således overladt til Center for Cybersikkerheds uforudsigelige vurdering af, om et netværkselement er omfattet.

Det er tilsvarende uklart, hvad der menes med "hardware […], der anvendes i core-net". Det er uklart, om det også betyder, at fx passive dele som fiberkablerne i et core-net omfattes, selvom et fiberkabel vanskeligt kan indeholde aflytningsudstyr eller kan kompromitteres af leverandøren.

TI skal opfodre til, at definitionen tilrettes, så de dele af udbydernes infrastruktur, der omfattes, afgrænses til kun at gælde det absolut mest nødvendige og fremstår entydig for den enkelte udbyder. Det kunne fx ske ved, at "Kritiske netkomponenter" defineres ud fra den sikkerhedsmæssige vurdering, udbyderen har foretaget af sit netværk, eller som CFCS ved en gennemgang af udbyderens netværk har identificeret som kritiske. Dermed undgår udbyderne fx at skulle anmelde aftaler og forhandlinger om systemkomponenter, som i praksis ikke udgør en sikkerhedsmæssig risiko.

§3 og §5: Udbyderens pligt til at underrette CFCS om aftaleforhandlinger og CFCS's mulighed for at udstede påbud om, at en endelig aftale skal indsendes til CFCS, er ikke nye. Der er dog ikke efter de gældende bestemmelser fastsat nogen frist for, hvornår Center for Cybersikkerhed skal give et påbud om at få det færdigt udkast til aftale indsendt. Erfaringerne har vist, at teleudbyderne har oplevet, at centeret ikke har reageret eller forholdt sig passiv i lang tid. Udbyderne kan dermed have indrette sine forhandlinger på, at aftalen kan indgås uden anmærkninger fra Center for Cybersikkerhed. Med de kommende regler om leverandørsikkerhed skærpes behovet for, at udbyderne hurtigt får klarhed, om der udstedes et påbud. TI skal derfor foreslå, at der i § 5 indsættes en frist således, at Center for Cybersikkerhed senest 20 arbejdsdage efter, underretning er foretaget, skal afgøre, om der er behov for at udstede et påbud om at indsende det endelige udkast til aftale til CFCS.

Der henvises i øvrigt herom til TI's høringssvar af 4. januar 2021 vedrørende lov om leverandørsikkerhed.[1]

[1] http://www.teleindu.dk/wp-content/uploads/2021/01/4-januar-2021-h%C3%B8ringssvar-vedr-leverand%C3%B8rsikkerhed.pdf

§ 7, stk. 2 og § 9: Ud over grænseværdien for, hvornår en hændelse skal indberettes efter § 7, stk. 2, er lavere, jf. § 9, end ved hændelser efter § 7, stk. 1, jf. § 8, så er det uklart, hvilke hændelser der er omfattet af § 7, stk. 2. TI skal derfor anmode CFCS om nærmere at redegøre for begrundelsen for den skærpede indberetningspligt efter § 7, stk. 2, herunder hvad der forstås ved "en begivenhed, der faktisk har haft væsentlig negativ indvirkning på net og tjenesters evne til at modstå handlinger, der er til skade for fortroligheden, integriteten eller autenticiteten…"

Der ønskes i øvrigt en særlig præcisering af, hvad der i bestemmelsen forstås ved "handlinger der er til skade for.. autenticiteten".

Der ønskes endelig en nærmere begrundelse for, hvorfor grænseværdien for indberetning efter 7, skt. 2, er sat til 1000 slutbrugere, jf. § 9, hvilket TI anser for at være en væsentlig skærpelse i forhold til den gældende indberetningspligt.

§7, stk 3: Fristen for underretning af sikkerhedshændelser er efter de gældende regler 14 dage (jf. den gældende § 10). Med den ændrede tekst i § 7, stk. 3, ændres underretningspligten til "uden unødigt ophold". Dette er en alvorlig skærpelse. Man vil ofte skulle undersøge en hændelse grundig, inden man i praksis vil kunne underrette om, hvad der rent faktisk er sket, hvor mange slutbrugere der er berørt og lign. Ændringen vil potentielt medføre indberetning af hændelser, før de er analyseret. Det vil potentielt betyde indberetning af hændelser, som ved nærmere analyse ikke er væsentlige eller løbende vil ændre sig efterhånden, som fejlundersøgelse pågår.

TI finder denne skærpelse ubegrundet og finder, at det vil være rimeligt med en frist på ikke mindre end 72 timer efter, udbyderen bliver bekendt med, at sikkerhedshændelsen har haft væsentlig indvirkning på driften.

En frist på mindst 72 timer vil sikre;

- at udbyderen kan holde fokus på kritisk udbedring og mitigering af den samfundsmæssige risiko
- en mere præcis og korrekt indrapportering til de offentlige myndigheder
- adgang til de nødvendige kompetencer og bemyndigede personer, hvis sikkerhedshændelsen sker uden for normal arbejdstid, f.eks. i weekenden eller påsken
- at indberetningspligten vil svare til den, der også gælder efter GDPR ved brud på persondatasikkerheden. Det vil således være ske en ensrettet håndtering ved indberetning af sikkerhedshændelser.

§8: De gældende grænseværdier for vurdering af, hvornår en hændelse anses for at have væsentlig indvirkning på driften af net og tjenester, er i det væsentlige opretholdt, dog er der indført en ny kate-

gori for NUIK-tjenester, og der er i § 8, stk. 4, indføjede nye kategorier.

TI ønsker en afklaring af, hvorfor der er forskel i grænseværdierne, herunder hvilke overvejelser har CFCS gjort i forbindelse med fastlæggelsen af grænseværdierne. TI finder det uklart, hvordan værdierne er opgjort og henstiller derfor til, at der foretages en ensretning af grænseværdierne. Dette vil skabe transparens, og TI kan ikke se, hvorfor der skal være forskel på mobilabonnementer og NUIK-tjenester. TI ønsker en ensretning af f.eks. de 35.000 brugertimer for mobilabonnementer og 50.000 brugertimer for NUIK-tjenester – dette bør ensrettes til 50.000 brugertimer.

Det er uklart, hvad kategorien ”øvrige tjenester” dækker over, og som ikke allerede er dækket af de andre nævnte tjenester, herunder hvorfor grænsen for ”øvrige tjenester” er sat væsentlig lavere end de andre anførte tjenester, som må anses at være de væsentligste tjenester på telemarkedet.

TI savner en nærmere begrundelse for indførsel af de nye kategorier, som er anført i stk. 4. Udbyderne har ikke systemer til at identificere præcist

- om mere end 200 slutbrugere indenfor forsvar, politi eller beredskab er berørt. Udbyderne har ikke nødvendigvis viden om, hvor slutbrugerne er ansat, eller hvilket formål kommunikationstjenesten anvendes til.
- hvilke tjenester beredskabsmyndighederne vælger at anvende til beredskabssituationer, eller hvad der i øvrigt forstås ved ”ekstraordinære situationer”.
- hvilke dele af udbyderens kapacitet, der dækker ikke-brofaste øer.

TI skal anbefale, at der indledes en dialog med branchen, inden der fastsættes nye kategorier, således at der findes kan underrettes på forhold, som udbyderne er i stand til at monitorere.

§13: Der indføres en ny skærpende informationspligt, hvorefter udbydere skal informere deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe, når udbyderne bliver bekendt med en særlig og betydelig trussel om en sikkerhedshændelse i deres net eller tjenester.

Den foreslåede bestemmelse pålægger udbyderne et stort ansvar samt en ressourcemæssig byrde.

Der er tale om en helt ny og detaljeret forpligtelse, som det ikke indenfor høringsfristen er muligt fuldt ud at afklare virkninger af, herunder om det er muligt i praksis at efterleve forpligtelsen.

TI mener derfor, at § 13 skal udgå og indtænkes i sektorens cyberstrategi som generel awareness overfor brugerne.

Bestemmelsen indeholder en række uklarheder i forhold til fx, hvordan og hvad der konkret skal informeres om. I værste fald kan udbyderne blive forpligtet til at "overinformere", hvorved kundernes opmærksomhed på de alvorlige trusler helt udebliver.

Det er i øvrigt uklart, om det er udbyderen af et net eller udbyderen af en tjeneste, der har forpligtelsen til at informere. Denne afklaring er særlig relevant, når netejer og tjenesteudbyder ikke er samme selskab.

TI finder betegnelsen 'potentielt berørte brugere' for vidtgående. 'Potentielt berørte brugere' indebærer, at der ikke længere er noget råderum for udbyderne til at vurdere, hvorvidt det er nødvendigt at involvere og underrette kunderne. Der er således ikke mulighed for at vurdere underretningen af de potentielle berørte brugere ift. den risiko, der reelt har eksisteret. TI skal derfor anbefale, at betegnelsen kvalificeres til alene at omfatte 'berørte brugere'.

TI forstår i øvrigt, at hændelserne som udgangspunkt kan kommunikeres til brugerne via generel driftsinformation, f.eks. på udbyderens hjemmeside.

I forhold til de i bestemmelsen anførte trusler (§ 13, stk. 1, nr. 1-7) har TI følgende bemærkninger:

Nr.1 og 2: Det er ikke sikkert, at udbyderne præcist har alle oplysninger om, hvem der fx benytter en DNS-løsning. Det samme gælder i forbindelse med BGP hijack, hvor alle slutbrugere anvender det pågældende IP-net. Sådanne trusler egner sig således bedst til information via fx udbyderes hjemmeside.

Nr. 2: Visse udbydere har det, man kalder rekursive DNS servere, hvor kompromittering kan kun identificeres to måder. Enten ved at en bruger henvender sig, eller ved at miljøet er ustabilt. Udbyderne foretager typisk ikke selv opdateringer, idet disse arves fra overliggende nationale servere – fx når www.dr.dk skifter IP-adresse, så kommer informationen automatisk til udbyderne fra de overliggende nationale servere. Informationspligten bør således ikke ligge på udbyderne, men på udbyderne af de nationale servere.

Nr. 3: Kompromittering af en brugers konto kan ofte være, at brugeren selv der har givet kontooplysninger videre på uheldig vis, dvs. noget, som udbyderne ikke er herre over. Sådanne situationer bør udbyderne ikke være forpligtet til at informere den enkelte slutbruger om.

Nr. 6: Efter TI's opfattelse er beskrivelsen af "ondsindet SS7-trafik" ikke realistisk, da der i praksis ses meget 'signalerings støj' fra fejlkonfigureret netværkselementer i fremmed netværk, og desuden ses der løbende sårbarhedsscanninger (pen-tests) fra mange forskellige

udenlandske aktører, som jævnligt scanner (pen-tester) med byger af forskellig SS7 angrebsmønstrer rettet mod tilfældige SIM/IMSI mhp. profilering af nettes sårbarhedsprofil og som forberedelse til evt. kommende spydspidsangreb.

I denne henseende kan støjen på SS7 nettet ses som analog til støjen på Internet, hvor der også er et konstant støjloft og vedvarende scanninger. Forskellen med SS7 støjen er, at der indgår et IMSI (en kunde) ifm. de alle støjende SS7 beskeder.

En stor andel af denne type støj vil subjektivt kunne tolkes eller fejltolkes som ondsindet forsøg på positionsindhentning, idet der i forskellige angrebsmønstre er SS7 MAP kommandoer, der kan relateres til position.

TI skal derfor anbefale, at nr. 6 præcises og ændres til:

> *"Identificeret vellykket ondsindet SS7-angreb målrettet en eller flere kunder, hvor det er lykkes at kompromittere kunden, og hvor det skønnes at have almenhedens interesse. Dette kan f.eks. være opsnapning af SMS/2-faktor autentifikationskoder, indhentning af positionsoplysninger eller omdirigering af talesamtaler."*

Til **Bekendtgørelse om sikkerhed og beredskab i net og tjenester** har TI følgende bemærkninger:

§ 2: TI skal anmode om, at begreberne defineres, herunder begrebet "autenticitet".

§3, §5 og § 6: I de gældende bestemmelser stod der, at udbyderne skulle styre informationssikkerheden, udarbejde en informationssikkerhedspolitik og foretage risikostyring "med udgangspunkt i en international standard", fx ISO27001. Med den foreslåede ændring fremgår det nu, at disse skal udarbejdes "efter en international standard". Det er uklart, om der med den pågældende ændring er tiltænkt en indholdsmæssig ændring.

Hvis det betyder, at man skal følge en bestemt international standard slavisk, vil det ikke medføre nogen sikkerhedsmæssig styrkelse af infrastrukturerne. For de fleste operatører er der en klar værdi i at selektere og inddrage brugbare vejledninger, modeller o.l. fra andre anerkendte standarder end ISO/IEC 27001; f.eks. NIST's Cybersecurity Framework og ISF's "Standard of Good Practice".

Der fremgår i øvrigt af lovbemærkningerne til § 3 i lov om sikkerhed i net og tjenester[2], at:

> *"Der kan således administrativt stilles krav om, at processerne skal fastlægges og gennemføres med udgangspunkt i en rele-*

[2] https://www.retsinformation.dk/eli/ft/201512L00010

vant og anerkendt international standard eller tilsvarende." (TI's understregning)

For at undgå fortolkningstvivl, skal TI opfodre til, at bestemmelserne ikke ændres, og at der fastholdes en tekstnær formulering svarende til rammerne i hjemmelsbestemmelsen.

§§11-15: TI finder det ubegrundet, at der er forskel på, hvordan NU-IK-tjenester og elektroniske kommunikationstjenester skal håndteres.

§ 26 og 27: Med de foreslåede bestemmelser gives CFCS som noget nyt mulighed for at påbyde udbyderne at foretage en risikovurdering under særlige ikke-afgrænsede omstændigheder.

TI mener, at bestemmelsen er for vidtgående og giver CFCS bred bemyndigelse til at indføre indgribende foranstaltninger på udbyderne. Bestemmelsen synes ikke at tage højde for, at der er nødt til at være proportionalitet i de iværksatte foranstaltninger, som kan pålægges i forhold til truslen. Myndighederne kan reelt pålægge ret omfattende foranstaltninger uden at tage højde for omkostningerne forbundet hermed, og der synes at mangle en form for afvejning af truslen og de pågældende foranstaltninger.

CFCS kan benytte bemyndigelsen, når der foreligger en "betydelig trussel", men det er ikke defineret nærmere og er et meget løst begreb. Der savnes også en sondring af, hvordan begreberne "betydelig trussel" i §§ 26 og 27 og "væsentlig samfundsmæssig betydning" i § 28 skal forstås. I den forbindelse skal TI anmode om, at der nærmere redegøres for, hvorfor foranstaltningerne efter § 28 ikke anses for at være tilstrækkelige.

TI finder det også uklart, hvordan processen vil være, hvis CFCS udsteder et påbud, herunder hvilken information CFCS er forpligtet til at forsyne udbyderen med, herunder om udbyderne skal udlevere risikovurderingen til CFCS, og hvordan skal der følges op på disse risikovurderinger.

De udvidede beføjelser kan medføre krav om yderligere foranstaltninger, hvilket vil medføre omkostninger for udbyderne. Særligt nedenstående bestemmelsens (§ 27, nr. 3-5) sætter store krav til udbyderne, hvis de umiddelbart skal kunne implementeres:

> *3) Sikring af sporbarhed eller logning af fysisk eller logisk adgang til nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder krav om analyse af logfiler.*
>
> *4) Iværksættelse af kryptering efter internationale anerkendte standarder eller best practice på kritiske netkomponenter, systemer og værktøjer.*
>
> *5) Sikring af, at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i den pågældende udbyders net og tjenester, undersøges for sårbarheder.*

Eksempelvis er det udefineret, hvad § 27, nr. 5, indebærer og kan i praksis være meget omfattende. I praksis kan det måske være helt umuligt at gennemføre fx en sourcekode review.

TI skal derfor henstille til, at §§ 26, 27 og 28 ændres, således at ansvaret for at definere, hvilke præcise passende foranstaltninger, der skal implementeres ved en betydelig trussel, ligger hos udbyderne. TI mener udbyderne kender deres virksomhederne bedst og således bedst kan vurdere, hvad der er passende foranstaltninger.

Med venlig hilsen

Jakob Willer
Direktør