EUROPEISKA
KOMMISSIONEN

Bryssel den 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Maximalt utnyttjande av it-säkerhetsdirektivet – mot ett effektivt genomförande av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

SV

Inledning

Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen[1] (nedan kallat *direktivet*), som antogs den 6 juli 2016, är den första övergripande EU-lagstiftningen som behandlar cybersäkerhetsproblem. Direktivet ändrar radikalt förutsättningarna för cybersäkerhetsresiliens och -samarbete i Europa.

Direktivets huvudmål är att

- förbättra den nationell cybersäkerhetskapaciteten,
- bygga upp samarbete på EU-nivå, och
- främja en kultur av riskhantering och incidentrapportering hos centrala ekonomiska aktörer, i synnerhet leverantörer som tillhandahåller tjänster som är samhällskritiska och behövs för ekonomisk och samhällelig verksamhet samt leverantörer av digitala tjänster.

Direktivet är en hörnsten i EU:s svar på de ökande cyberhot och utmaningar som följer på ekonomins och samhällslivets digitalisering. Genomförandet av direktivet är därför en viktig del av det cybersäkerhetspaket som lades fram den 13 september 2017. EU:s åtgärder kan inte få fullt genomslag förrän direktivet helt införlivats i alla EU-medlemsstater. Detta erkändes också som en avgörande punkt i kommissionens meddelande *Stärka Europas system för cyberresiliens* från 2016[2].

Mot bakgrund av det nytänkande som präglar direktivet och det faktum att det brådskar att angripa de föränderliga cyberhoten måste vi vara mycket uppmärksamma på alla aktörers utmaningar när det gäller att säkerställa ett snabbt och framgångsrikt införlivande av direktivet. Tidsfristen för införlivandet går ut den 9 maj 2018 och tidsfristen för att identifiera leverantörer av samhällsviktiga tjänster är den 9 november 2018, och därför har kommissionen stött medlemsstaternas införlivandeprocesser och deras arbete i samarbetsgruppen.

Detta meddelande och dess bilaga baseras på kommissionens förberedande arbete och analys av genomförandet av direktivet fram till nu, på bidrag från Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) samt på diskussioner med medlemsstaterna i samband med införlivandet av direktivet, bl.a. i samarbetsgruppen[3]. Meddelandet kompletterar de stora insatser som redan har gjorts, i följande sammanhang:

- Det intensiva arbetet i samarbetsgruppen, som har antagit en arbetsplan som huvudsakligen fokuseras på införlivandet av direktivet, bl.a. frågan om identifiering av leverantörer av samhällsviktiga tjänster och deras skyldigheter vad gäller säkerhetskrav och rapportering av incidenter. Direktivet ger medlemsstaterna viss

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Direktivet trädde i kraft den 8 augusti 2016.
[2] COM(2016) 410 final.
[3] En mekanism för strategiskt samarbete mellan medlemsstaterna enligt artikel 11 i direktivet.

frihet vid införlivandet av de bestämmelser som rör leverantörer av samhällsviktiga tjänster, men de har konstaterat att det är viktigt med ett harmoniserat tillvägagångssätt[4].

- Inrättande av ett nätverk av CSIRT-enheter (enheter för hantering av it-säkerhetsincidenter), som snabbt ska inleda sin verksamhet, i enlighet med artikel 12.1 i direktivet. Detta nätverk har börjat lägga grunden för ett strukturerat operativt samarbete på europeisk nivå.

På både politisk och operativ nivå, som representeras av dessa två strukturer, krävs ett totalt engagemang från alla medlemsstater för att uppnå målet, som är en hög gemensam säkerhetsnivå för nät- och informationssystem i hela unionen.

Meddelandet och dess bilaga kommer att stärka dessa insatser genom att sammanställa och jämföra goda arbetsmetoder från medlemsstaterna av relevans för genomförandet av direktivet, genom att ge ytterligare vägledning om hur direktivet bör genomföras och genom mer ingående förklaringar av specifika bestämmelser. Det övergripande målet är att stödja medlemsstaterna för att uppnå ett effektivt och harmoniserat genomförande av direktivet i hela EU.

Meddelandet kommer att kompletteras av kommissionens kommande genomförandeförordning, som ytterligare specificerar aspekter och parametrar kopplade till säkerhets- och incidentrapporteringskraven för leverantörer av digitala tjänster enligt artikel 16.8 i direktivet. Genomförandeförordningen kommer att främja genomförandet av direktivet när det gäller skyldigheter för leverantörer av digitala tjänster[5].

I meddelandet redogörs för de viktigaste slutsatserna av analysen av de frågor som ses som viktiga referenspunkter och potentiell inspiration när det gäller införlivandet med nationell lagstiftning. Här ligger fokus i första hand på bestämmelser som rör medlemsstaternas kapacitet och skyldigheter när det gäller enheter som omfattas av direktivet. Bilagan innehåller en mer ingående granskning av de områden där kommissionen ser största värde av att ge praktisk vägledning till införlivandet genom att förklara och tolka vissa av direktivets bestämmelser och beskriva goda arbetsmetoder och den samlade hittillsvarande erfarenheten av direktivet.

Mot ett praktiskt genomförande av direktivet

Direktivets syfte är att uppnå en hög gemensam säkerhetsnivå för nät- och informationssystem i EU. Det innebär att man förbättrar säkerheten för internet och de privata nät- och informationssystem som behövs för att vårt samhälle och vår ekonomi ska fungera.

[4] Samarbetsgruppen håller för närvarande på att utarbeta vägledande referensdokument avseende bl.a. följande: Kriterier för att fastställa om en leverantör är samhällsviktig i enlighet med artikel 5.2 i direktivet. Under vilka omständigheter som leverantörer av samhällsviktiga tjänster måste rapportera incidenter baserat på artikel 14.7 i direktivet. Säkerhetskraven för leverantörer av samhällsviktiga tjänster, i linje med artikel 14.1 och 14.2.

[5] Utkastet till genomförandeförordningen har lagts ut för offentligt samråd på https://ec.europa.eu/info/law/better-regulation/have-your-say_en.

Den första viktiga aspekten när det gäller detta är att medlemsstaternas beredskap måste säkerställas genom nationella cybersäkerhetsstrategier, såsom föreskrivs i direktivet, genom CSIRT-enheternas arbete och genom verksamheten hos de behöriga nationella myndigheterna.

De nationella strategiernas omfattning

Det är viktigt att medlemsstaterna i samband med införlivandet av direktivet utnyttjar möjligheten att se över sin nationella cybersäkerhetsstrategi mot bakgrund av luckor, goda arbetsmetoder och nya utmaningar som tas upp i bilagan.

Direktivet fokuserar förståeligt nog på de företag och tjänster som är av särskild stor betydelse, men det är cybersäkerheten för ekonomin och samhället i stort som måste hanteras konsekvent och med ett helhetsgrepp, med tanke på vårt allt större behov av informations- och kommunikationsteknik. Därmed kan antagandet av övergripande nationella strategier som går längre än minimikraven enligt direktivet (och t.ex. omfattar fler sektorer och tjänster än de som förtecknas i bilagorna II och III) höja den totala säkerhetsnivån för nät- och informationssystem.

I och med att cybersäkerhet är ett relativt nytt och snabbt växande område inom samhällspolitiken, måste man i de flesta fall göra nya investeringar, även om den allmänna situationen i de offentliga finanserna föranleder nedskärningar och besparingar. Ambitiösa beslut för att säkra de finansiella resurser och personalresurser som behövs för ett effektivt genomförande av nationella strategier, inklusive tillräckliga resurser till nationella behöriga myndigheter och CSIRT-enheter, är därmed en förutsättning för att direktivets mål ska kunna uppnås.

Effektivitet i genomförandet och kontrollen av efterlevnaden

I artikel 8 i direktivet beskrivs behovet av att utse respektive nationella behöriga myndigheter och gemensamma kontaktpunkter, vilket är viktigt för ett effektivt genomförande av direktivet och för samarbetet över gränserna. Här har både mer centraliserade och mer decentraliserade tillvägagångssätt utvecklats i medlemsstaterna. När medlemsstater använder ett mer decentraliserat tillvägagångssätt i samband med utseendet av nationella behöriga myndigheter har det visat sig viktigt att de säkerställer starka samarbetsstrukturer mellan de olika myndigheterna och den gemensamma kontaktpunkten (*se tabell 1 i avsnitt 3.2 i bilagan*). Detta kan effektivisera genomförandet och underlätta kontrollen av efterlevnaden.

De erfarenheter som gjorts i samband med skydd av kritisk informationsinfrastruktur kan vara till hjälp i arbetet med att utforma en optimal styrelsemodell för medlemsstaterna, som säkrar både ett effektivt genomförande av direktivet i olika sektorer och ett sammanhängande horisontellt tillvägagångssätt (*se avsnitt 3.1 i bilagan*).

Förbättrad nationell CSIRT-kapacitet

Utan effektiva nationella CSIRT-enheter med tillräckliga resurser i hela EU, såsom anges i artikel 9 i direktivet, kommer EU att förbli sårbart för gränsöverskridande cyberhot. Medlemsstaterna skulle därför kunna överväga att utvidga räckvidden för CSIRT-enheterna till att omfatta sektorer och tjänster utanför direktivets tillämpningsområde (*se avsnitt 3.3 i bilagan*). Detta skulle göra det möjligt för nationella CSIRT-enheter att ge operativt stöd vid cyberincidenter som inträffar hos företag och organisationer som inte omfattas av direktivet men som också är viktiga för samhället och ekonomin. Medlemsstaterna skulle också kunna utnyttja alla kompletterande finansieringsmöjligheter som erbjuds genom programmet för infrastruktur för digitala tjänster inom Fonden för ett sammanlänkat Europa, som utformats för att öka de nationella CSIRT-enheternas kapacitet och främja samarbete mellan dem (*se avsnitt 3.5 i bilagan*).

Konsekvent förfarande för identifiering av leverantörer av samhällsviktiga tjänster

Enligt artikel 5 i direktivet ska medlemsstaterna senast den 9 november 2018 identifiera de enheter som ska anses som leverantörer av samhällsviktiga tjänster. Medlemsstaterna kan då överväga att konsekvent använda de definitioner och den vägledning som finns i detta meddelande för att säkerställa att liknande typer av enheter som spelar en liknande roll på den inre marknaden konsekvent identifieras som leverantörer av samhällsviktiga tjänster i andra medlemsstater. Medlemsstaterna kan också överväga att utvidga direktivets tillämpningsområde till offentliga förvaltningar, med tanke på den betydelse som dessa har för samhället och ekonomin som helhet (*se avsnitt 2.1 och 4.1.3 i bilagan*).

Det är vettigt om de nationella tillvägagångssätten för att identifiera leverantörer av samhällsviktiga tjänster anpassas till varandra så mycket som möjligt med hjälp av den vägledning som tagits fram av samarbetsgruppen (*se avsnitt 4.1.2 i bilagan*), eftersom det kan leda till en mer harmoniserad tillämpning av direktivets bestämmelser och därmed minska risken för fragmentering av marknaden. I de fall då leverantörer av samhällsviktiga tjänster tillhandahåller sådana i två eller fler medlemsstater är det viktigt att sträva efter att uppnå enighet mellan dessa (genom samrådsprocessen enligt 5.4) om en konsekvent identifiering av enheter (*se avsnitt 4.1.7 i bilagan*), eftersom det motverkar att samma enhet behandlas olika inom olika medlemsstaters jurisdiktioner.

Inlämnande till kommissionen av uppgifter om identifiering av leverantörer av samhällsviktiga tjänster

Enligt artikel 5.7 ska medlemsstaterna informera kommissionen om nationella åtgärder som gör det möjligt att identifiera leverantörer av samhällsviktiga tjänster samt förteckningen över samhällsviktiga tjänster, antalet identifierade leverantörer av samhällsviktiga tjänster och dessa leverantörers betydelse för sektorn. Medlemsstaterna ska också ange eventuella trösklar som används i identifieringsförfarandet för att fastställa relevant försörjningsnivå eller en viss leverantörs betydelse för upprätthållandet av en tillräcklig försörjningsnivå. Medlemsstaterna

kan också överväga att överlämna förteckningen över identifierade leverantörer till kommissionen, om nödvändigt på konfidentiell grund, eftersom det skulle bidra till att göra kommissionens bedömning mer exakt och kvalitativ.

Enhetliga tillvägagångssätt avseende säkerhet och rapportering av incidenter för leverantörer av samhällsviktiga tjänster

När det gäller de skyldigheter som avser säkerhetskrav och incidentrapportering för leverantörer av samhällsviktiga tjänster (artikel 14.1, 14.2 och 14.3) kan ett mer enhetligt tillvägagångssätt, som gör det lättare för leverantörer av samhällsviktiga tjänster att uppfylla kraven även över medlemsstaternas gränser, främja största möjliga effekt på den inre marknaden. Referensen är även här samarbetsgruppens arbete med ett vägledande dokument (*se avsnitt 4.2 och 4.3 i bilagan*).

Vid storskaliga cyberincidenter som påverkar flera medlemsstater är det sannolikt att en obligatorisk incidentrapportering görs av en leverantör av samhällsviktiga tjänster eller en leverantör av digitala tjänster i enlighet med artiklarna 14.3 och 16.3 eller av en annan enhet som inte omfattas av direktivet på frivillig grund enligt artikel 20.1. I enlighet med kommissionens rekommendation om samordnade insatser vid storskaliga gränsöverskridande cyberincidenter och -kriser kan medlemsstaterna överväga att anpassa sina nationella tillvägagångssätt till varandra så att de, snarast möjligt, kan lämna relevant information baserad på dessa rapporter till de behöriga myndigheterna eller till CSIRT-enheten i den andra berörda medlemsstaten. Tillförlitlig information som kan ligga till grund för åtgärder kan vara avgörande för att minska antalet ”infektioner” eller åtgärda brister innan de utnyttjas.

För att maximera direktivets effekter avser kommissionen i en anda av partnerskap att utvidga stödet inom Fonden för ett sammanlänkat Europa till att omfatta alla aktörer som berörs av denna lagstiftning. Fokus har hittills legat på CSIRT-kapacitetsuppbyggnad och på en plattform för snabbt och effektivt operativt samarbete, för att på så sätt stärka nätverket av CSIRT-enheter, men kommissionen kommer nu att undersöka hur finansiering genom Fonden för ett sammanlänkat Europa också kan gagna nationella behöriga myndigheter, leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster.

Slutsats

Mot bakgrund av att tidsfristen för att införliva direktivet med nationell lagstiftning går ut den 9 maj 2018 och att tidsfristen för identifiering av leverantörer av samhällsviktiga tjänster går ut den 9 november 2018, bör medlemsstaterna vidta de åtgärder som behövs för att säkerställa att direktivets bestämmelser och samarbetsmodeller kan tillhandahålla bästa tänkbara verktyg på EU-nivå för att uppnå en hög säkerhetsnivå för nät- och informationssystem i hela unionen. Kommissionen uppmanar medlemsstaterna att i samband med denna process beakta informationen, vägledningen och rekommendationerna i detta meddelande.

Detta meddelande kan också kompletteras av andra åtgärder, t.ex. åtgärder som tas fram inom ramen för det pågående arbetet i samarbetsgruppen.