Europeiska unionens råd

Bryssel den 18 december 2020
(OR. en)

14150/20
ADD 3

Interinstitutionellt ärende:
2020/0359(COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	16 december 2020
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2020) 344 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN Följedokument till Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148

För delegationerna bifogas dokument – SWD(2020) 344 final.

Bilaga: SWD(2020) 344 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 16.12.2020
SWD(2020) 344 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN

Följedokument till

Förslag till Europaparlamentets och rådets direktiv

om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Sammanfattning

Konsekvensbedömning av *översynen av 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 (nedan kallat NIS-direktivet)*

A. Behov av åtgärder

Vad är problemet och varför är det ett problem på EU-nivå?

Trots dess betydande framsteg har NIS-direktivet, som banade väg för en betydande förändring i fråga om attityder och den institutionella och lagstiftningsmässiga strategin för cybersäkerhet i många medlemsstater, nu också visat sina begränsningar. Den digitala omvandlingen av samhället (som trappats upp på grund av covid-19-krisen) har expanderat hotbilden och medför nya utmaningar som kräver anpassade och innovativa svarsåtgärder. Antalet cyberattacker fortsätter att öka, och de alltmer sofistikerade attackerna kommer från ett brett spektrum av källor i och utanför EU.

På grundval av utvärderingen av NIS-direktivets funktion identifierades följande problem i konsekvensbedömningen: den låga nivån av cyberresiliens hos företag som är verksamma i EU, bristen på enhetlig resiliens mellan medlemsstater och sektorer, den låga graden av gemensam situationsmedvetenhet och avsaknaden av gemensam krishantering. Som exempel kan nämnas att till följd av vissa av dessa problem och faktorer finns det situationer där vissa större sjukhus i en medlemsstat inte ingår i NIS-direktivets tillämpningsområde och därför inte är skyldiga att genomföra direktivets säkerhetsåtgärder, medan i en annan medlemsstat nästan varenda sjukhus i landet omfattas av NIS-direktivets säkerhetskrav.

Vad vill man uppnå?

Översynen av NIS-direktivet har tre allmänna mål:

1. **Att öka cyberresiliensen hos ett stort antal företag med verksamhet i EU inom alla relevanta sektorer,** genom att införa regler som säkerställer att alla offentliga och privata entiteter på hela den inre marknaden som fyller viktiga funktioner för ekonomin och samhället som helhet blir skyldiga att vidta lämpliga cybersäkerhetsåtgärder.
2. **Att minska bristen på enhetlighet hos motståndskraften på den inre marknaden inom de sektorer som redan omfattas av direktivet,** genom att ytterligare justera 1) det faktiska tillämpningsområdet, 2) säkerhets- och incidentrapporteringskraven, 3) bestämmelserna om nationell tillsyn och efterlevnadskontroll och 4) kapaciteten hos medlemsstaternas behöriga myndigheter.
3. **Att förbättra den gemensamma situationsmedvetenheten och den kollektiva förmågan att ha beredskap och reagera,** genom att vidta åtgärder för att öka förtroendet mellan behöriga myndigheter, utbyta mer information och fastställa regler och förfaranden i händelse av en storskalig incident eller kris.

Vad är mervärdet med åtgärder på EU-nivå (subsidiaritet)?

Det kan inte finnas en effektiv motståndskraft mot cyberhot i unionen om frågan hanteras på olika sätt genom ett nationellt eller regionalt silotänkande. NIS-direktivet kom till för att åtgärda detta problem genom att fastställa en ram för säkerhet i nätverks- och informationssystem på nationell nivå och unionsnivå. Införlivandet och genomförandet av direktivet visade dock också på inneboende brister i vissa bestämmelser eller strategier, såsom den oklara avgränsningen av NIS-direktivets tillämpningsområde.

Sedan covid-19-krisen startade har den europeiska ekonomin dessutom blivit mer beroende av nätverks- och informationssystem än någonsin förr och olika sektorer och tjänster blir alltmer sammankopplade. Den första periodiska översynen av NIS-direktivet gav därför möjlighet till ytterligare EU-åtgärder. Insatser på EU-nivå utöver NIS-direktivets nuvarande åtgärder motiveras främst av i) att problemet har gränsöverskridande karaktär, ii) att åtgärder på EU-nivå har potential att förbättra och underlätta ändamålsenliga nationella strategier och iii) att samordnade och samarbetsinriktade nät- och informationssäkerhetspolitiska åtgärder kan bidra till ett effektivt skydd av personuppgifter och integritet.

B. Lösningar

Vilka alternativ finns för att nå målen? Finns det ett rekommenderat alternativ? Om inte, varför?

I konsekvensbedömningen analyserades fyra alternativ: 0) ett bibehållande av status quo, 1) andra åtgärder än lagstiftning för att anpassa införlivandet, 2) begränsade ändringar av NIS-direktivet för att uppnå ytterligare harmonisering och 3) systemförändringar och strukturella förändringar av NIS-direktivet. Alternativ 1 förkastades i ett tidigt skede eftersom det inte avviker avsevärt från status quo. I konsekvensbedömningen dras slutsatsen att det **rekommenderade alternativet** är alternativ 3 (dvs. **systemförändringar och strukturella förändringar av NIS-ramen**), eftersom det skulle innebära ett mer grundläggande strategiskifte mot att täcka ett bredare segment av unionens ekonomier, dock med en mer fokuserad tillsyn inriktad på proportionellt stora och centrala företag, samtidigt som tillämpningsområdet fastställs tydligt. Det skulle också rationalisera och ytterligare harmonisera de säkerhetsrelaterade skyldigheterna för företag, skapa en mer ändamålsenlig ram för operativa aspekter och en tydlig grund för delat ansvar och ansvarsutkrävande med avseende på relevanta aktörer och ge incitament till informationsutbyte.

Vad anser de berörda parterna? Vem stöder vilka alternativ?

En majoritet av de behöriga myndigheterna och företagen stödde en översyn av NIS-direktivet. Under flera samråd framförde de att ett reviderat NIS-direktiv borde täcka ytterligare (del)sektorer och anpassa eller rationalisera ytterligare säkerhetsåtgärder och rapporteringsskyldigheter. Berörda parter stödde också nya koncept eller policyrelaterade åtgärder som endast ingår i det rekommenderade alternativet (t.ex. strategier för säkerhet i leveranskedjan och institutionalisering av en operativ EU-ram för krishantering).

C. Det rekommenderade alternativets konsekvenser

Vad är nyttan med det rekommenderade alternativet (om ett sådant finns, annars för huvudsakliga alternativ)?

Det rekommenderade alternativet skulle medföra betydande fördelar: uppskattningar som gjorts på grundval av en ekonomisk modell som tagits fram i en undersökning till stöd för översynen av NIS-direktivet visar att det rekommenderade alternativet kan leda till en minskning av kostnaderna för cyberincidenter med 11,3 miljarder euro.

Det sektoriella tillämpningsområdet skulle utvidgas avsevärt inom NIS-ramen, men utöver ovannämnda fördelar skulle den börda som kan skapas av nät- och informationssäkerhetskraven, särskilt ur tillsynssynpunkt, också bli balanserad för både de nya entiteter som ska omfattas och de behöriga myndigheterna. Detta beror på att den nya NIS-ramen skulle inrätta en tvåstegsstrategi, med fokus på stora och centrala entiteter och en differentiering av tillsynen som endast medger tillsyn i efterhand (dvs. en tillsyn som är reaktiv och utan någon allmän skyldighet att systematiskt dokumentera fullgörandet) för ett stort antal av dessa entiteter, särskilt de som anses vara ”viktiga” men inte ”väsentliga”.

På det hela taget skulle det rekommenderade alternativet leda till effektiva kompromisser och synergier,

med den bästa potentialen av alla analyserade politiska alternativ för att säkerställa en ökad och konsekvent nivå av cyberresiliens hos centrala entiteter i hela unionen som så småningom skulle leda till kostnadsbesparingar för både företag och samhället.

Vad är kostnaderna för det rekommenderade alternativet (om ett sådant finns, annars för huvudsakliga alternativ)?

Det rekommenderade alternativet skulle leda till vissa fullgörande- och efterlevnadskontrollkostnader för de berörda myndigheterna i medlemsstaterna (en total ökning på cirka 20–30 % av medlen uppskattades). Den nya ramen skulle dock också medföra betydande fördelar genom en bättre överblick över och bättre samverkan med centrala företag, ett förbättrat gränsöverskridande operativt samarbete samt mekanismer för ömsesidigt bistånd och sakkunnigbedömningar. Detta skulle leda till en generell ökning av cybersäkerhetskapaciteten i alla medlemsstater.

De företag som skulle omfattas av NIS-ramen uppskattas behöva öka sina nuvarande utgifter för IKT-säkerhet med högst 22 % under de första åren efter införandet av den nya NIS-ramen (12 % för företag som redan omfattas av det nuvarande NIS-direktivet). Denna genomsnittliga ökning av utgifterna för IKT-säkerhet skulle dock leda till en proportionell nytta av sådana investeringar, särskilt på grund av en betydande minskning av kostnaderna för cyberincidenter (uppskattningsvis 11,3 miljarder euro under tio år).

Hur påverkas små och medelstora företag och konkurrenskraften?

Små företag och mikroföretag skulle inte omfattas av NIS-ramen enligt det rekommenderade alternativet. För medelstora företag kan man förvänta sig en ökning av utgifterna för IKT-säkerhet under de första åren efter införandet av den nya NIS-ramen. Samtidigt skulle en höjning av säkerhetskraven för dessa entiteter också stimulera deras cybersäkerhetskapacitet och bidra till att förbättra deras IKT-riskhantering.

Påverkas medlemsstaternas budgetar och förvaltningar i betydande grad?

Medlemsstaternas budgetar och förvaltningar skulle påverkas på följande vis: En beräknad ökning på cirka 20–30 % av medlen förväntas på kort och medellång sikt.

Uppstår andra betydande konsekvenser?

Inga andra betydande negativa konsekvenser förväntas. Det rekommenderade alternativet förväntas leda till en mer robust cybersäkerhetskapacitet och skulle följaktligen ha en mer betydande dämpande effekt på antalet incidenter och deras allvarlighetsgrad, inbegripet för dataintrång. Det kommer sannolikt också att ha en positiv inverkan på säkerställandet av lika villkor i medlemsstaterna för alla entiteter som ingår i NIS-direktivets tillämpningsområde och minska asymmetrierna i fråga om information om cybersäkerhet.

Proportionalitetsprincipen

Det rekommenderade alternativet går inte utöver vad som är nödvändigt för att i tillräckligt hög grad uppnå de särskilda målen. Den planerade anpassningen och rationaliseringen av säkerhetsåtgärder och rapporteringsskyldigheter har samband med medlemsstaternas och företagens önskemål om en förbättring av den nuvarande ramen.

D. Uppföljning

När kommer åtgärderna att ses över?

Den första översynen skulle äga rum 54 månader efter det att rättsakten trätt i kraft. Kommissionen skulle lägga fram en rapport om dess översyn för Europaparlamentet och rådet. Översynen skulle göras med stöd av Enisa och samarbetsgruppen.