Europeiska unionens råd

Bryssel den 16 september 2022
(OR. en)

12429/22
ADD 6

Interinstitutionellt ärende:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	15 september 2022
till:	Rådets generalsekretariat
Komm. dok. nr:	SWD(2022) 283 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN om cyberresiliensakten Följedokument till förslag till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

För delegationerna bifogas dokument – SWD(2022) 283 final.

Bilaga: SWD(2022) 283 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 15.9.2022
SWD(2022) 283 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN

om cyberresiliensakten

Följedokument till

förslag till Europaparlamentets och rådets förordning

om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Sammanfattning (högst 2 sidor)

Konsekvensbedömning av cyberresiliensakten

A. Behov av åtgärder

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

Hårdvaru- och mjukvaruprodukter utsätts ofta för framgångsrika cyberattacker, som beräknas medföra en global årlig kostnad för cyberbrottslighet på 5,5 biljoner EUR 2021. Dessa produkter har två stora problem som ökar kostnaderna för användarna och samhället: 1) en låg cybersäkerhetsnivå, vilket återspeglas av utbredda sårbarheter och ett otillräckligt och inkonsekvent tillhandahållande av säkerhetsuppdateringar för att åtgärda dessa sårbarheter, och 2) användarnas bristfälliga förståelse och tillgång till information, som hindrar dem från att välja produkter med lämpliga cybersäkerhetsegenskaper eller använda dem på ett säkert sätt.

Cybersäkerheten för produkter med digitala element har en stark gränsöverskridande dimension, eftersom produkter som tillverkas i ett land ofta används på hela den inre marknaden. På bara några minuter kan incidenter, som först påverkar en enda enhet eller enda medlemsstat, ofta sprida sig på hela den inre marknaden.

Den befintliga inremarknadslagstiftningen omfattar vissa produkter med digitala element, men de flesta hårdvaru- och mjukvaruprodukter omfattas i dagsläget inte av någon EU-lagstiftning om cybersäkerhet. Den nuvarande rättsliga EU-ramen omfattar i synnerhet inte cybersäkerheten för icke-inbyggd mjukvara, trots att cybersäkerhetsattacker allt oftare riktas mot sårbarheter i sådana produkter, vilket medför betydande samhällskostnader och ekonomiska kostnader. Några färska exempel är Pegasus-spionprogrammet, som utnyttjade sårbarheter i mobiltelefoner, och gisslanmasken WannaCry, som utnyttjade en sårbarhet i Windows, vilket påverkade datorer i hela världen.

Vad vill man uppnå?

Två huvudmål identifierades för att säkerställa en korrekt fungerande inre marknad: 1) Skapa förutsättningar för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under hela produktens livscykel, och 2) skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element. Fyra särskilda mål fastställdes**:** i) att säkerställa att tillverkarna förbättrar säkerheten för produkter med digitala element från utformnings- och utvecklingsfasen och genom hela produktens livscykel, ii) att säkerställa en sammanhängande cybersäkerhetsram, som främjar överensstämmelse för hårdvaru- och programvarutillverkare, iii) att förbättra transparensen när det gäller säkerhetsegenskaperna hos produkter med digitala element, och iv) att möjliggöra en säker användning av produkter med digitala element för företag och konsumenter.

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

Cybersäkerhetens starka gränsöverskridande dimension och det ökande antalet incidenter med spridningseffekter över gränser och mellan sektorer och produkter innebär att målen inte kan uppnås på ett effektivt sätt av medlemsstaterna på egen hand. Eftersom marknaderna för produkter med digitala element är globala möter alla medlemsstater på sina territorier samma risker för samma produkter med digitala element. En framväxande fragmenterad ram bestående av potentiellt olika nationella regler riskerar att stå i vägen för en öppen och konkurrenspräglad inre marknad för produkter med digitala element. Det krävs alltså gemensamma åtgärder på EU-nivå för att öka förtroendet hos användarna och stärka

dragningskraften för produkter med digitala element på EU-marknaden. Detta skulle också gagna den digitala inre marknaden genom att skapa rättssäkerhet och lika spelregler för alla tillverkare av produkter med digitala element.

B. Lösningar

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

Följande fyra politiska alternativ och underalternativ analyserades vilka gick utöver den rådande situationen: 1) Ett ”icke-bindande” tillvägagångssätt och frivilliga åtgärder. 2) Produktspecifika ad hoc-regleringsåtgärder för cybersäkerhet för fysiska produkter med digitala element respektive inbyggd programvara. 3) Ett blandat tillvägagångssätt, som innefattar övergripande obligatoriska krav för cybersäkerheten för produkter med digitala element och respektive inbyggd programvara, och ett stegvist tillvägagångssätt för icke-inbyggd programvara, med två underalternativ för bedömning av överensstämmelse. 4) En övergripande regleringsåtgärd som omfattar cybersäkerhetskrav för ett brett spektrum av produkter med digitala element, inklusive icke-inbyggd programvara, med underalternativ avseende omfattningen av bedömningen av överensstämmelse.

Slutsatsen var att alternativ 4 var det **rekommenderade alternativet**. Det omfattar alla produkter med digitala element och en obligatorisk tredjepartsbedömning för kritiska produkter. Detta baserades på effektiviteten i förhållande till de särskilda målen och vad gäller kostnader och nytta, samt samstämmigheten.

Vad anser de berörda parterna? Vem stöder vilka alternativ?

Deltagarna ombads rangordna de olika åtgärdernas effektivitet och de var eniga om att alternativ 4 skulle vara den mest ändamålsenliga åtgärden (4,08 på en skala från 1 till 5). Detta innefattar konsumentorganisationer (5,00), deltagare som identifierar sig som användare (4,22), anmälda organ (4,17), marknadskontrollmyndigheter (5,00) och tillverkare av produkter med digitala element (3,85), inbegripet tillverkare som är små och medelstora företag (4,05).

C. Det rekommenderade alternativets konsekvenser

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

Det rekommenderade alternativet skulle innebära betydande fördelar för de olika intressenterna. För företagen skulle det förhindra att olikartade säkerhetsregler gäller för produkter med digitala element, och det skulle sänka kostnaderna för uppfyllande av kraven i cybersäkerhetslagstiftningen. Det skulle minska antalet cyberincidenter, kostnaden för incidenthantering och risken för skadat anseende. För EU som helhet beräknas att initiativet kan minska kostnaderna för incidenter som påverkar företag med i storleksordningen 180–290 miljarder euro per år. Det skulle också leda till ökad omsättning tack vare en ökad efterfrågan på produkter med digitala element. Det skulle förbättra företagens globala anseende och leda till en ökad efterfrågan också utanför EU. För slutanvändarna skulle det rekommenderade alternativet öka transparensen för säkerhetsegenskaper och underlätta användningen av produkter med digitala element. Konsumenter och medborgare skulle också gagnas av ett bättre skydd för sina grundläggande rättigheter, såsom personlig integritet och skydd av personuppgifter.

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

Det rekommenderade alternativet skulle medföra kostnader för överensstämmelse och kontroll av

efterlevnad för företag, anmälda organ och offentliga myndigheter, inbegripet anmälande myndigheter och ackrediterings- och marknadskontrollmyndigheter. För programvaruutvecklare och hårdvarutillverkare kommer det att öka de direkta kostnaderna för uppfyllandet av nya cybersäkerhetskrav, bedömning av överensstämmelse, dokumentation och rapporteringsskyldigheter, uppgående till sammanlagt omkring 29 miljarder EUR för ett beräknat marknadsvärde för produkter med digitala element på upp till 1 485 miljarder EUR i omsättning. Slutanvändare, såsom slutanvändare som är företag, konsumenter och medborgare, kan drabbas av högre priser på produkter med digitala element. Detta bör dock ses mot bakgrund av de betydande fördelar som beskrivs ovan. För anmälda organ väntas merkostnaderna täckas genom en ökad omsättning.

Hur påverkas små och medelstora företag och konkurrenskraften?

Små och medelstora företag kommer att påverkas av de nya kraven som både tillverkare och slutanvändare. När det gäller kostnaderna för att uppfylla kraven skulle de små och medelstora företagen i princip påverkas mer än större företag, som normalt har skalfördelar och större cybersäkerhetsmedvetenhet. Små och medelstora företag skulle dock få stora fördelar av initiativet eftersom cybersäkerhet som är inbyggd i produkter med digitala element skulle medföra betydande kostnadsbesparingar för dessa företag. Som tillverkare skulle små och medelstora företag gagnas av ökat förtroende hos slutanvändarna och nya kunder. En sömlös tillgång till den inre marknaden och minskad marknadsfragmentering är faktorer som kan vara ännu mer fördelaktiga för små och medelstora företag, eftersom de har sämre förutsättningar för att hantera en mångfald av regleringskrav. De små och medelstora företagen betonade behovet av en proportionell strategi och stödåtgärder, men stödde generellt tanken på lika spelregler för alla företag och trodde inte att de skulle missgynnas jämfört med större företag i ett scenario med övergripande obligatoriska krav.

Påverkas medlemsstaternas budgetar och förvaltningar i betydande grad?

Initiativet kommer att påverka nationella myndigheter, däribland nationella anmälande myndigheter, ackrediteringsmyndigheter och marknadskontrollmyndigheter som har ansvaret för att övervaka och kontrollera efterlevnaden av de föreslagna åtgärderna. Dessa myndigheter kommer att få merkostnader för anpassning (t.ex. utbildning och personalresurser) och kontroll av efterlevnaden till följd av de nya kraven. De resurser som används av ackrediteringsorganen kompenseras dock och bärs huvudsakligen av organ för bedömning av överensstämmelse genom en upphandling av ackrediteringstjänster.

Uppstår andra betydande konsekvenser?

Inga andra betydande negativa konsekvenser förväntas. Det rekommenderade alternativet skulle bidra till att minska antalet incidenter och incidenternas allvarlighetsgrad, inbegripet när det gäller personuppgiftsincidenter, och skulle ha positiva sociala effekter, såsom minskad cyberbrottslighet. Efterfrågan på säkerhetspersonal kommer sannolikt att öka och asymmetrierna i fråga om cybersäkerhetsinformation kommer att minska.

Proportionalitetsprincipen

Det rekommenderade alternativet går inte utöver vad som är nödvändigt för att i tillräckligt hög grad uppnå de särskilda målen. Åtgärden skulle säkerställa att produkter med digitala element är säkra under hela sin livscykel och den skulle stå i proportion till de berörda riskerna.

D. Uppföljning

När kommer åtgärderna att ses över?

Kommissionen ska senast [36 månader efter den dag då initiativet börjar tillämpas] och därefter vart fjärde år, överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet.