EUROPA-
KOMMISSIONEN

Bruxelles, den 15.9.2022
SWD(2022) 283 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF RAPPORTEN OM KONSEKVENSANALYSEN

om retsakten om cyberrobusthed

Ledsagedokument til

Forslag til Europa-Parlamentets og Rådets forordning

om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020

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

Resumé (maks. 2 sider)

Konsekvensanalyse af retsakten om cyberrobusthed

A. Behov for handling

Hvad er problemet, og hvorfor udgør det et problem på EU-plan?

Hardware- og softwareprodukter udsættes ofte for vellykkede cyberangreb, og de samlede årlige omkostninger ved cyberkriminalitet beløb sig således til 5,5 mia. EUR i 2021. Der er to store problemer forbundet med disse produkter, som øger omkostningerne for brugerne og samfundet: 1) et lavt cybersikkerhedsniveau, der afspejles i udbredte sårbarheder og utilstrækkelig og inkonsekvent levering af sikkerhedsopdateringer til håndtering heraf, og 2) brugernes utilstrækkelige forståelse af og adgang til oplysninger, hvilket forhindrer dem i at vælge produkter med passende cybersikkerhedsfunktioner eller at anvende dem på en sikker måde.

Cybersikkerheden for produkter med digitale elementer har en stærk grænseoverskridende dimension, da produkter fremstillet i ét land ofte anvendes i hele det indre marked. Hændelser, der i første omgang berører en enkelt enhed eller en enkelt medlemsstat, spreder sig desuden ofte inden for få minutter i hele det indre marked.

Selv om den eksisterende lovgivning om det indre marked finder anvendelse på visse produkter med digitale elementer, er de fleste hardware- og softwareprodukter i øjeblikket ikke omfattet af EU-lovgivning om cybersikkerhed. EU's nuværende retlige ramme indeholder navnlig ikke bestemmelser om cybersikkerheden for ikkeindlejrede softwareprodukter, selv om cyberangreb i stigende grad er rettet mod sårbarheder i disse produkter, hvilket medfører betydelige samfundsmæssige og økonomiske omkostninger. Nylige eksempler herpå er Pegasus-spyware, som udnyttede sårbarheder i mobiltelefoner, eller WannaCry ransomware-ormen, som udnyttede en Windows-sårbarhed og ramte computere i hele verden.

Hvilke resultater skal der opnås?

Der blev udpeget to hovedmål, som skal sikre et velfungerende indre marked: 1) skabe betingelser for udvikling af sikre produkter med digitale elementer ved at sikre, at hardware- og softwareprodukter bringes i omsætning med færre sårbarheder, og at fabrikanterne tager sikkerheden alvorligt i hele et produkts livscyklus og 2) skabe betingelser, der gør det muligt for brugerne at tage hensyn til cybersikkerhed, når de udvælger og anvender produkter med digitale elementer. Der blev fastsat fire specifikke mål: i) sikre, at fabrikanterne forbedrer sikkerheden af produkter med digitale elementer lige fra design- og udviklingsfasen og i hele livscyklussen, ii) sikre en sammenhængende ramme for cybersikkerhed, der letter hardware- og softwarefabrikanternes overholdelse af kravene, iii) øge gennemsigtigheden med hensyn til sikkerhedsegenskaber ved produkter med digitale elementer og iv) gøre det muligt for virksomheder og forbrugere at anvende produkter med digitale elementer på en sikker måde.

Hvad er merværdien ved at handle på EU-plan (nærhedsprincippet)?

Den stærke grænseoverskridende karakter af cybersikkerhed og det stigende antal hændelser med afsmittende virkninger på tværs af grænser, sektorer og produkter betyder, at målene ikke kan opfyldes effektivt af medlemsstaterne alene. I betragtning af den globale karakter af markederne for produkter med digitale elementer står medlemsstaterne over for de samme risici i forbindelse med det samme produkt med digitale elementer på deres område. Et kludetæppe af potentielt divergerende nationale regler risikerer også at forhindre et åbent og konkurrencedygtigt indre marked for produkter med digitale

elementer. En fælles indsats på EU-plan er derfor nødvendig for at øge tilliden blandt brugerne og gøre produkter med digitale elementer mere attraktive på EU-markedet. Det vil også gavne det indre marked ved at sikre retssikkerhed og lige vilkår for fabrikanter af produkter med digitale elementer.

B. Løsninger

Hvilke løsninger er der overvejet for at nå målene? Foretrækkes en bestemt løsning frem for andre? Hvis ikke, hvorfor?

Fire løsninger og relaterede delløsninger blev analyseret ud over status quo: 1) en tilgang med blød lovgivning og frivillige foranstaltninger, 2) et produktspecifikt ad hoc-reguleringstiltag i forbindelse med cybersikkerhed for håndgribelige produkter med digitale elementer og indlejret software, 3) en blandet tilgang, herunder horisontale obligatoriske regler for cybersikkerhed for håndgribelige produkter med digitale elementer og indlejret software og en trinvis tilgang til ikkeindlejret software med to delløsninger for overensstemmelsesvurdering og 4) et horisontalt reguleringstiltag med indførelse af cybersikkerhedskrav til en bred vifte af produkter med digitale elementer, herunder ikkeindlejret software, med delløsninger for anvendelsesområdet og overensstemmelsesvurdering.

I konsekvensanalysen blev det konkluderet, at den **foretrukne løsning** er løsning 4, der omfatter alle produkter med digitale elementer og indebærer obligatorisk tredjepartsvurdering af kritiske produkter baseret på en vurdering af effektiviteten i forhold til de specifikke mål, omkostningseffektiviteten og sammenhængen.

Hvad er de forskellige interessenters synspunkter? Hvem støtter hvilken løsning?

Da respondenterne i den offentlige høring blev bedt om at vurdere effektiviteten af de politiske tiltag, var de enige i, at løsning 4 ville være den mest effektive foranstaltning (4,08 på en skala fra 1 til 5). Dette omfatter forbrugerorganisationer (5,00), respondenter, der angav sig som brugere (4,22), bemyndigede organer (4,17), markedsovervågningsmyndigheder (5,00) og fabrikanter af produkter med digitale elementer (3,85), herunder små og mellemstore fabrikanter (4,05).

C. Den foretrukne løsnings virkninger

Hvilke fordele er der ved den foretrukne løsning (hvis en bestemt løsning foretrækkes — ellers fordelene ved de vigtigste af de mulige løsninger)?

Den foretrukne løsning vil medføre betydelige fordele for de forskellige interessenter. For virksomhederne vil det forhindre divergerende sikkerhedsregler for produkter med digitale elementer og mindske omkostningerne til overholdelse af relateret lovgivning om cybersikkerhed. Det vil reducere antallet af cyberhændelser, omkostningerne til håndtering af hændelser og skade på omdømme. For hele EU anslås det, at initiativet kan føre til en omkostningsreduktion som følge af hændelser, der påvirker virksomheder, på ca. 180-290 mia. EUR om året. Initiativet vil desuden føre til en øget omsætning som følge af øget efterspørgsel efter produkter med digitale elementer. Det vil også forbedre virksomhedernes globale omdømme og føre til øget efterspørgsel uden for EU. For slutbrugerne vil den foretrukne løsning øge gennemsigtigheden med hensyn til sikkerhedsegenskaberne og lette anvendelsen af produkter med digitale elementer. Forbrugere og borgere vil også få en bedre beskyttelse af deres grundlæggende rettigheder såsom privatlivets fred og databeskyttelse.

Hvilke omkostninger er der ved den foretrukne løsning (hvis en bestemt løsning foretrækkes — ellers omkostningerne ved de vigtigste af de mulige løsninger)?

Den foretrukne løsning vil medføre yderligere overholdelses- og håndhævelsesomkostninger for

virksomheder, bemyndigede organer og offentlige myndigheder, herunder bemyndigende myndigheder og akkrediterings- og markedsovervågningsmyndigheder. For softwareudviklere og hardwarefabrikanter vil den øge de direkte overholdelsesomkostninger forbundet med nye cybersikkerhedskrav, overensstemmelsesvurdering og dokumentations- og rapporteringsforpligtelser, hvilket vil bringe de samlede overholdelsesomkostninger på op til ca. 29 mia. EUR for en anslået markedsværdi af produkter med digitale elementer på op til 1 485 mia. EUR i omsætning. Slutbrugere, herunder erhvervsbrugere, forbrugere og borgere, vil kunne opleve højere priser på produkter med digitale elementer. Disse skal dog ses på baggrund af de betydelige fordele, der er beskrevet ovenfor. For bemyndigede organer forventes meromkostningerne at blive opvejet af en stigning i omsætningen.

Hvordan påvirker den foretrukne løsning SMV'er og konkurrenceevnen?

SMV'er vil blive påvirket af de nye krav både som fabrikanter og slutbrugere. Med hensyn til overholdelsesomkostninger vil SMV'er i princippet blive hårdere ramt end store virksomheder, som typisk har større stordriftsfordele og større bevidsthed om cybersikkerhed. SMV'er vil dog drage stor fordel af initiativet, da cybersikkerhed indbygget i produkter med digitale elementer vil medføre en betydelig omkostningsbesparelse for SMV'er som brugere. Som fabrikanter vil SMV'er drage fordel af slutbrugernes større tillid og nye kunder. En gnidningsløs adgang til det indre marked og en mindskelse af markedsfragmenteringen kan være endnu mere gavnlig for SMV'er, da de er mindre rustet til at håndtere forskellige lovkrav. SMV'erne understregede behovet for en forholdsmæssig tilgang og støtteforanstaltninger, men støttede generelt lige vilkår for alle virksomheder og mente ikke, at de ville blive stillet ringere end større virksomheder i et scenarie med horisontale obligatoriske krav.

Vil den foretrukne løsning få væsentlige virkninger for de nationale budgetter og myndigheder?

Initiativet vil påvirke nationale myndigheder såsom nationale bemyndigende myndigheder, akkrediteringsmyndigheder og markedsovervågningsmyndigheder med ansvar for overvågning og håndhævelse af de foreslåede foranstaltninger. Disse myndigheder vil blive pålagt yderligere tilpasningsomkostninger (f.eks. uddannelse og menneskelige ressourcer) og håndhævelsesomkostninger for at tage hensyn til de nye krav. De ressourcer, som akkrediteringsorganerne kommer til at bruge, vil imidlertid i vid udstrækning blive opvejet og dækket af overensstemmelsesvurderingsorganerne gennem indkøb af akkrediteringstjenester.

Vil den foretrukne løsning få andre væsentlige virkninger?

Der forventes ingen andre væsentlige eller negative virkninger. Den foretrukne løsning vil bidrage til at reducere antallet og alvoren af hændelser, herunder brud på persondatasikkerheden, og vil have positive sociale virkninger såsom et lavere niveau af cyberkriminalitet. Efterspørgslen efter sikkerhedsspecialister vil sandsynligvis vokse, og asymmetrierne i cybersikkerhedsoplysninger vil blive reduceret.

Proportionalitet?

Den foretrukne løsning går ikke ud over, hvad der er nødvendigt for at opfylde de specifikke mål på tilfredsstillende vis. Tiltaget vil sikre, at produkter med digitale elementer sikres i hele deres livscyklus på en måde, der står i et rimeligt forhold til de pågældende risici.

D. Opfølgning

Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?

Senest [36 måneder] efter datoen for dette initiativs anvendelse og hvert fjerde år derefter forelægger

Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af dette initiativ.