Vijeće
Europske unije

**Bruxelles, 16. rujna 2022.**
**(OR. en)**

**12429/22**
**ADD 6**

**Međuinstitucijski predmet:**
**2022/0272(COD)**

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

**POPRATNA BILJEŠKA**

| | |
|---|---|
| Od: | Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ |
| Datum primitka: | 15. rujna 2022. |
| Za: | Glavno tajništvo Vijeća |
| Br. dok. Kom.: | SWD(2022) 283 final |
| Predmet: | RADNI DOKUMENT SLUŽBI KOMISIJE SAŽETAK IZVJEŠĆA O PROCJENI UČINKA Akta o kiberotpornosti priložen dokumentu Prijedlog uredbe Europskog parlamenta i Vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020 |

Za delegacije se u prilogu nalazi dokument SWD(2022) 283 final.

Priloženo: SWD(2022) 283 final

EUROPSKA
KOMISIJA

Bruxelles, 15.9.2022.
SWD(2022) 283 final

**RADNI DOKUMENT SLUŽBI KOMISIJE**

**SAŽETAK IZVJEŠĆA O PROCJENI UČINKA**

**Akta o kiberotpornosti**

***priložen dokumentu***

**Prijedlog uredbe Europskog parlamenta i Vijeća**

**o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020**

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

**Sažetak (najviše dvije stranice)**

Procjena učinka Akta o kiberotpornosti

**A. Potreba za djelovanjem**

**O čemu je riječ? Zašto je to problem na razini EU-a?**

Hardverski i softverski proizvodi često su izloženi uspješnim kibernapadima te se procjenjuje da je do 2021. godišnja šteta od kiberkriminaliteta bila 5,5 bilijuna EUR. Dva su glavna problema zbog kojih ti proizvodi stvaraju troškove korisnicima i društvu: 1. imaju nisku razinu kibersigurnosti, čemu su dokaz raširene ranjivosti te nedovoljna i neredovita sigurnosna ažuriranja za njihovo otklanjanje, i 2. korisnici nemaju dovoljno znanja ni informacija, pa ne mogu odabrati proizvode s odgovarajućim kibersigurnosnim obilježjima ili ih rabiti na siguran način.

Kibersigurnost proizvoda s digitalnim elementima ima snažnu prekograničnu dimenziju jer se proizvodi proizvedeni u jednoj zemlji često rabe na cijelom unutarnjem tržištu. Usto, incidenti koji isprva pogode jedan subjekt ili samo jednu državu članicu često se veoma brzo prošire na cijelo unutarnje tržište.

Premda se postojeće zakonodavstvo o unutarnjem tržištu primjenjuje na određene proizvode s digitalnim elementima, većina hardverskih i softverskih proizvoda trenutačno nije obuhvaćena nijednim propisom EU-a koji se odnosi na njihovu kibersigurnost. Točnije, postojećim se pravnim okvirom EU-a ne uređuje pitanje kibersigurnosti neugrađenog softvera iako su kibernapadi sve češće usmjereni na ranjivosti tih proizvoda, što uzrokuje znatne društvene i gospodarske troškove. Nedavni su primjeri špijunski softver Pegasus, kojim su se iskorištavale ranjivosti mobilnih telefona, ili ucjenjivački crv WannaCry, koji je iskoristio ranjivost Windowsa i zarazio računala u cijelom svijetu.

**Što bi trebalo postići?**

Utvrđena su dva glavna cilja kako bi se osiguralo pravilno funkcioniranje unutarnjeg tržišta: 1. stvoriti uvjete za razvoj sigurnih proizvoda s digitalnim elementima tako što će se urediti da se hardverski i softverski proizvodi stavljaju na tržište s manje ranjivosti i da proizvođači ozbiljno shvaćaju sigurnost tijekom cijelog životnog ciklusa proizvoda; i 2. stvoriti uvjete koji korisnicima omogućuju da proizvode s digitalnim elementima odabiru i rabe vodeći računa o kibersigurnosti. Utvrđena su četiri posebna cilja: i. pobrinuti se da proizvođači poboljšaju sigurnost proizvoda s digitalnim elementima od faze projektiranja i razvoja te tijekom cijelog životnog ciklusa; ii. stvoriti usklađen okvir za kibersigurnost kako bi ga se proizvođači hardvera i softvera lakše pridržavali; iii. povećati transparentnost sigurnosnih svojstava proizvoda s digitalnim elementima i iv. poduzećima i potrošačima omogućiti sigurnu upotrebu proizvoda s digitalnim elementima.

**Koja je dodana vrijednost djelovanja na razini EU-a (supsidijarnost)?**

Zbog izrazite prekogranične prirode kibersigurnosti i sve češćih incidenata čiji se učinci prelijevaju preko granica te na druge sektore i proizvode države članice ne mogu same učinkovito ostvariti ciljeve. Zbog globalne prirode tržišta proizvoda s digitalnim elementima isti proizvod s digitalnim elementima ima iste sigurnosne rizike na državnim područjima različitih država članica. Rascjepkan okvir potencijalno različitih nacionalnih pravila kakav se počeo pojavljivati mogao bi i ugroziti otvoreno i konkurentno jedinstveno tržište proizvoda s digitalnim elementima. Dakle, zajedničko djelovanje na razini EU-a potrebno je radi povećanja povjerenja korisnika i privlačnosti proizvoda s digitalnim elementima koji se stavljaju na tržište EU-a. To bi pogodovalo i unutarnjem tržištu zbog stvaranja pravne sigurnosti i jednakih uvjeta za proizvođače proizvoda s digitalnim elementima.

**B. Rješenja**

**Koje su različite opcije za ostvarenje ciljeva? Postoji li najpoželjnija opcija? Ako ne, zašto?**

Analizirane su četiri opcije politike i povezane podopcije koje nadilaze *status quo*: 1. pravno neobvezujuće i dobrovoljne mjere; 2. *ad hoc* regulatorna intervencija za pojedine proizvode radi kibersigurnosti materijalnih proizvoda s digitalnim elementima i odgovarajućeg ugrađenog softvera; 3. mješoviti pristup, uključujući horizontalna obvezna pravila za kibersigurnost materijalnih proizvoda s digitalnim elementima i odgovarajućim ugrađenim softverom te postupni pristup za neugrađeni softver, uz dvije podopcije za ocjenjivanje sukladnosti; i 4. horizontalna regulatorna intervencija kojom se uvode kibersigurnosni zahtjevi za širok raspon proizvoda s digitalnim elementima, uključujući neugrađeni softver, s podopcijama u pogledu područja primjene i o ocjenjivanju sukladnosti.

U procjeni učinka zaključeno je da je **najpoželjnija** četvrta opcija, koja se odnosi na sve proizvode s digitalnim elementima i kojom se predviđa obvezno ocjenjivanje rizičnih proizvoda koje provodi treća strana na temelju procjene djelotvornosti u odnosu na posebne ciljeve, učinkovitost troškova u odnosu na koristi te usklađenosti.

**Koja su stajališta različitih dionika? Tko podržava koju opciju?**

Upitani da ocijene djelotvornost intervencija politike, sudionici javnog savjetovanja složili su se da bi četvrta opcija bila najdjelotvornija mjera (4,08 na ljestvici od 1 do 5). Među njima su organizacije potrošača (5,00), sudionici koji su se identificirali kao korisnici (4,22), prijavljena tijela (4,17), tijela za nadzor tržišta (5,00) i proizvođači proizvoda s digitalnim elementima (3,85), uključujući male i srednje proizvođače (4,05).

**C. Učinci najpoželjnije opcije**

**Koje su prednosti najpoželjnije opcije (ako postoji, inače prednosti glavnih opcija)?**

Najpoželjnija opcija donijela bi znatne koristi različitim dionicima. Kad je riječ o poduzećima, spriječila bi pojavu različitih sigurnosnih pravila za proizvode s digitalnim elementima i smanjila troškove usklađivanja s povezanim zakonodavstvom o kibersigurnosti. Time bi se smanjili broj kiberincidenata, troškovi rješavanja incidenata i šteta za ugled. Procjenjuje se da bi inicijativa cijelom EU-u mogla smanjiti troškove od incidenata koji pogađaju poduzeća za otprilike 180 do 290 milijardi EUR godišnje. Nadalje, dovela bi do povećanja prometa zbog veće prihvaćenosti proizvoda s digitalnim elementima. Povećala bi i globalni ugled poduzeća, pa bi potražnja porasla i izvan EU-a. Krajnjim bi korisnicima najpoželjnija opcija povećala transparentnost sigurnosnih svojstava i olakšala uporabu proizvoda s digitalnim elementima. Potrošači i građani koristi bi imali i od bolje zaštite temeljnih prava kao što su privatnost i zaštita podataka.

**Koji su troškovi najpoželjnije opcije (ako postoji, inače troškovi glavnih opcija)?**

Najpoželjnijom opcijom dodali bi se troškovi usklađivanja i provedbe za poduzeća, prijavljena tijela i javna tijela, uključujući tijela koja provode prijavljivanje, akreditacijska tijela i tijela za nadzor tržišta. Programerima softvera i proizvođačima hardvera povećat će izravne troškove usklađivanja za nove kibersigurnosne zahtjeve, ocjenjivanje sukladnosti, dokumentiranje i obveze izvješćivanja, pa će ukupni troškovi usklađivanja iznositi otprilike 29 milijardi EUR za procijenjenu tržišnu vrijednost proizvoda s digitalnim elementima u iznosu do 1 485 milijardi EUR prometa. Krajnji korisnici, uključujući poslovne krajnje korisnike, potrošače i građane, možda će se suočiti s višim cijenama proizvoda s digitalnim elementima. To, međutim, treba promatrati u kontekstu prethodno opisanih znatnih koristi. Za prijavljena

| |
|---|
| tijela očekuje se da će se dodatni troškovi nadoknaditi povećanjem prometa. |
| **Koji su učinci na MSP-ove i konkurentnost?** |
| Novi će zahtjevi MSP-ove zahvatiti i kao proizvođače i kao krajnje korisnike. Kad je riječ o troškovima usklađivanja, na MSP-ove bi u načelu utjecaj bio veći nego na velika poduzeća, koja obično imaju bolju ekonomiju razmjera i više znanja o kibersigurnosti. MSP-ovi bi, međutim, imali veliku korist od inicijative jer bi im kibersigurnost ugrađena u proizvode s digitalnim elementima donijela znatne uštede kao korisnicima. Kao proizvođači bi pak imali koristi od većeg povjerenja krajnjih korisnika i novih kupaca. Još bi veću korist mogli imati od neometanog pristupa unutarnjem tržištu i smanjenja rascjepkanosti tržišta s obzirom na to da im je teže ispunjavati različite regulatorne zahtjeve. Premda su istaknuli potrebu za proporcionalnim pristupom i mjerama potpore, MSP-ovi su općenito podržali jednake uvjete za sva poduzeća i nisu smatrali da bi ih horizontalni obvezni zahtjevi stavili u nepovoljan položaj u odnosu na veća poduzeća. |
| **Hoće li to bitno utjecati na državne proračune i uprave?** |
| Inicijativa će utjecati na nacionalna tijela, primjerice nacionalna tijela koja provode prijavljivanje, akreditacijska tijela i tijela za nadzor tržišta koja su odgovorna za praćenje i provedbu predloženih mjera. Ta će tijela snositi dodatne troškove prilagodbe (npr. osposobljavanje i ljudski resursi) i provedbe zbog novih zahtjeva. Međutim, sredstva koja utroše akreditacijska tijela uglavnom će nadoknaditi tijela za ocjenjivanje sukladnosti kupnjom akreditacijskih usluga. |
| **Hoće li biti drugih bitnih učinaka?** |
| Ne očekuju se drugi znatni negativni učinci. Najpoželjnija opcija politike pridonijela bi smanjenju broja i težine incidenata, uključujući povrede osobnih podataka, te bi imala pozitivne društvene učinke kao što je smanjenje kiberkriminaliteta. Potražnja za stručnjacima za sigurnost vjerojatno će rasti, a asimetričnost kibersigurnosnih informacija bi se smanjila. |
| **Proporcionalnost?** |
| Najpoželjnija opcija ne prelazi ono što je potrebno za zadovoljavajuće ispunjenje posebnih ciljeva. Intervencijom bi postiglo da su proizvodi s digitalnim elementima zaštićeni u cijelom životnom ciklusu razmjerno rizicima kojima su izloženi. |
| **D. Daljnje mjere** |
| **Kad će se predložene mjere preispitati?** |
| Najkasnije [36 mjeseci] nakon datuma početka primjene inicijative i svake četiri godine nakon toga Komisija Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju inicijative. |