Svet
Evropske unije

Bruselj, 16. september 2022
(OR. en)

Medinstitucionalna zadeva:
2022/0272 (COD)

12429/22
ADD 6

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

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	15. september 2022
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	SWD(2022) 283 final - ANNEX
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK POROČILA O OCENI UČINKA o aktu o kibernetski odpornosti Spremni dokument Predlog uredbe Evropskega parlamenta in Sveta o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020

Delegacije prejmejo priloženi dokument SWD(2022) 283 final - ANNEX.

Priloga: SWD(2022) 283 final - ANNEX

EVROPSKA
KOMISIJA

Bruselj, 15.9.2022
SWD(2022) 283 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK POROČILA O OCENI UČINKA

o aktu o kibernetski odpornosti

Spremni dokument

Predlog uredbe Evropskega parlamenta in Sveta

o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020

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

Povzetek (največ 2 strani)

Ocena učinka o aktu o kibernetski odpornosti

A. Nujnost ukrepanja

V čem je težava in zakaj je to težava na ravni EU?

Izdelki strojne in programske opreme so pogosto tarča uspešnih kibernetskih napadov, zaradi katerih so letni stroški kibernetske kriminalitete na svetovni ravni do leta 2021 po ocenah znašali 5,5 bilijona EUR. Pri takih izdelkih obstajata dve glavni težavi, zaradi katerih imajo uporabniki in družba dodatne stroške: (1) nizka raven kibernetske varnosti, ki se odraža v splošno razširjenih ranljivostih ter nezadostnem in nedoslednem zagotavljanju varnostnih posodobitev za njihovo odpravljanje, ter (2) nezadostno razumevanje in nezadosten dostop uporabnikov do informacij, ki preprečujeta izbiro izdelkov z ustreznimi lastnostmi kibernetske varnosti ali njihovo varno uporabo.

Kibernetska varnost izdelkov z digitalnimi elementi ima jasno čezmejno razsežnost, saj se izdelki, izdelani v eni državi, pogosto uporabljajo na celotnem notranjem trgu. Poleg tega se incidenti, ki prvotno prizadenejo posamezen subjekt ali državo članico, pogosto v nekaj minutah razširijo na celotni notranji trg.

Čeprav se sedanja zakonodaja o notranjem trgu uporablja za nekatere izdelke z digitalnimi elementi, večina izdelkov strojne in programske opreme trenutno ni vključenih v nobeno zakonodajo EU, ki bi obravnavala njihovo kibernetsko varnost. Zlasti sedanji pravni okvir EU ne obravnava kibernetske varnosti nevgrajene programske opreme, čeprav so kibernetski napadi čedalje pogosteje usmerjeni v ranljivosti teh izdelkov ter povzročajo precejšnje družbene in ekonomske stroške. Nedavna primera sta vohunsko programje Pegasus, ki je izkoriščalo ranljivosti v mobilnih telefonih, in črv izsiljevalskega programja WannaCry, ki je izrabil ranljivost v operacijskem sistemu Windows ter s tem prizadel računalnike po vsem svetu.

Kaj bi bilo treba doseči?

Določena sta bila dva glavna cilja za zagotovitev ustreznega delovanja notranjega trga: (1) ustvariti pogoje za razvoj varnih izdelkov z digitalnimi elementi z zagotavljanjem, da se na trg dajejo izdelki strojne in programske opreme z manj ranljivostmi in da proizvajalci v celotnem življenjskem ciklu izdelka resno obravnavajo vprašanje varnosti, ter (2) ustvariti pogoje, ki uporabnikom omogočajo upoštevanje kibernetske varnosti pri izbiri in uporabi izdelkov z digitalnimi elementi. Oblikovani so bili štirje specifični cilji: (i) zagotoviti, da proizvajalci izboljšujejo varnost izdelkov z digitalnimi elementi že od faze zasnove in razvoja ter v celotnem življenjskem ciklu izdelka; (ii) zagotoviti skladen okvir kibernetske varnosti, s čimer se olajša zagotavljanje skladnosti za proizvajalce strojne in programske opreme; (iii) izboljšati preglednost varnostnih lastnosti izdelkov z digitalnimi elementi ter (iv) podjetjem in potrošnikom omogočiti varno uporabo izdelkov z digitalnimi elementi.

Kakšna je dodana vrednost ukrepanja na ravni EU (subsidiarnost)?

Očitno čezmejna narava kibernetske varnosti in vse večje število incidentov, katerih učinki segajo čez meje, v razne sektorje in izdelke, pomeni, da države članice ne morejo same učinkovito doseči navedenih ciljev. Glede na globalno naravo trgov izdelkov z digitalnimi elementi se države članice na svojih ozemljih spoprijemajo z istimi tveganji glede istih izdelkov z digitalnimi elementi. Nastajajoči neenotni okvir potencialno različnih nacionalnih pravil lahko tudi ogrozi odprt in konkurenčen enotni trg izdelkov z digitalnimi elementi. Zato je potrebno skupno ukrepanje na ravni EU, da se povečata zaupanje med uporabniki in privlačnost izdelkov z digitalnimi elementi, danih na trg EU. To bi tudi koristilo notranjemu

trgu, saj bi zagotavljalo pravno varnost in enake konkurenčne pogoje za proizvajalce izdelkov z digitalnimi elementi.

B. Rešitve

Katere so različne možnosti za dosego ciljev? Ali ima katera od njih prednost? Če ne, zakaj ne?

Analizirane so bile štiri možnosti politike in z njimi povezane podmožnosti, ki presegajo sedanje stanje: (1) pristop mehkega prava in prostovoljni ukrepi; (2) izdelkom prilagojeno *ad hoc* regulativno posredovanje za kibernetsko varnost materialnih izdelkov z digitalnimi elementi in zadevne vgrajene programske opreme; (3) mešani pristop, vključno s horizontalnimi obveznimi pravili za kibernetsko varnost materialnih izdelkov z digitalnimi elementi in zadevne vgrajene programske opreme ter postopnim pristopom za nevgrajeno programsko opremo, z dvema podmožnostima glede ugotavljanja skladnosti, ter (4) horizontalno regulativno posredovanje, na podlagi katerega bi se uvedle zahteve glede kibernetske varnosti za širok nabor izdelkov z digitalnimi elementi, vključno z nevgrajeno programsko opremo, s podmožnostmi glede področja uporabe in ugotavljanja skladnosti.

Iz ocene učinka izhaja, da je na podlagi ocene uspešnosti glede na specifične cilje, stroškovne učinkovitosti glede na koristi in skladnosti **prednostna možnost** možnost 4, ki se nanaša na vse izdelke z digitalnimi elementi in predvideva obvezno ugotavljanje skladnosti kritičnih izdelkov, ki ga opravi tretja oseba.

Kakšna so stališča različnih deležnikov? Kdo podpira katero možnost?

Kar zadeva oceno uspešnosti ukrepov politike, so se anketiranci v javnem posvetovanju strinjali, da bi bila možnost 4 najuspešnejši ukrep (na lestvici od 1 do 5 je bila ocenjena s 4,08). Med anketiranci so bili potrošniške organizacije (5,00), anketiranci, ki so se opredelili za uporabnike (4,22), priglašeni organi (4,17), organi za nadzor trga (5,00) in proizvajalci izdelkov z digitalnimi elementi (3,85), vključno z malimi in srednjimi (4,05).

C. Učinki prednostne možnosti

Kakšne so koristi prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Prednostna možnost bi imela pomembne koristi za različne deležnike. Za podjetja bi preprečila različna varnostna pravila glede izdelkov z digitalnimi elementi in znižala stroške zagotavljanja skladnosti z zadevno zakonodajo o kibernetski varnosti. Zmanjšala bi število kibernetskih incidentov, znižala stroške obvladovanja incidentov in zmanjšala škodo za ugled. Za celotno EU se ocenjuje, da bi se lahko zaradi pobude stroški zaradi incidentov, ki prizadenejo podjetja, znižali za približno 180–290 milijard EUR na leto. Nadalje, s pobudo bi se povečal promet zaradi večjega povpraševanja po izdelkih z digitalnimi elementi. Izboljšal bi se tudi globalni ugled podjetij, zaradi česar bi se povečalo povpraševanje tudi zunaj EU. Za končne uporabnike bi prednostna možnost izboljšala preglednost varnostnih lastnosti in olajšala uporabo izdelkov z digitalnimi elementi. Potrošniki in državljani bi imeli tudi koristi zaradi boljše zaščite svojih temeljnih pravic, kot sta zasebnost in varstvo podatkov.

Kakšni so stroški prednostne možnosti (če obstaja, sicer glavnih možnosti)?

S prednostno možnostjo bi se povišali stroški zagotavljanja skladnosti in izvrševanja za podjetja, priglašene organe in javne organe, vključno s priglasitvenimi organi, akreditacijskimi organi in organi za nadzor trga. Za razvijalce programske opreme in proizvajalce strojne opreme se bodo zvišali neposredni stroški zagotavljanja skladnosti zaradi novih zahtev glede kibernetske varnosti, ugotavljanja skladnosti, zagotavljanja dokumentacije in obveznosti poročanja, zaradi česar bodo skupni stroški zagotavljanja

skladnosti dosegli približno 29 milijard EUR glede na ocenjeno tržno vrednost izdelkov z digitalnimi elementi v višini 1 485 milijard EUR prometa. Za končne uporabnike, vključno s poslovnimi končnimi uporabniki, potrošniki in državljani, bo to morda pomenilo višje cene izdelkov z digitalnimi elementi. Vendar pa bi bilo treba te presojati glede na pomembne koristi, opisane zgoraj. Glede priglašenih organov se predvideva, da bo dodatne stroške odtehtalo povečanje prometa.

Kakšen bo vpliv na MSP in konkurenčnost?

Nove zahteve bodo vplivale na MSP kot proizvajalce in končne uporabnike. Glede stroškov zagotavljanja skladnosti bo vpliv na MSP načeloma večji kot vpliv na večja podjetja, ki imajo običajno boljšo ekonomijo obsega in so bolj ozaveščena glede kibernetske varnosti. Vendar pa bodo MSP imela veliko koristi zaradi pobude, saj bo kibernetska varnost, vgrajena v izdelke z digitalnimi elementi, pomenila pomemben prihranek stroškov MSP kot uporabnikov. Kot proizvajalci bodo MSP uživala več zaupanja končnih uporabnikov in novih strank. Nemoten dostop do notranjega trga in zmanjšanje tržne razdrobljenosti lahko pomeni še večjo korist za MSP, ki so slabše opremljena za spoprijemanje z različnimi regulativnimi zahtevami. Ob poudarjanju potrebe po sorazmernem pristopu in podpornih ukrepih so MSP na splošno podprla enake konkurenčne pogoje med vsemi podjetji in menila, da v primeru uporabe scenarija horizontalnih obveznih zahtev ne bodo v slabšem položaju kot večja podjetja.

Ali bo prišlo do znatnih učinkov na nacionalne proračune in uprave?

Pobuda bo imela učinek na nacionalne organe, kot so nacionalni priglasitveni organi, akreditacijski organi in organi za nadzor trga, ki so odgovorni za spremljanje in izvrševanje predlaganih ukrepov. Ti organi bodo imeli zaradi upoštevanja novih dodatne stroške prilagajanja (npr. usposabljanje in človeški viri) ter izvrševanja. Vire, ki jih bodo porabili akreditacijski organi, pa bodo večinoma odtehtali organi za ugotavljanje skladnosti z nakupom akreditacijskih storitev.

Bo imela pobuda druge pomembnejše učinke?

Drugi pomembnejši negativni učinki se ne pričakujejo. Prednostna možnost politike bi pripomogla k zmanjšanju števila in resnosti incidentov, vključno s kršitvami varnosti osebnih podatkov, in bi imela pozitivne družbene učinke, kot je zmanjšanje kibernetske kriminalitete. Pričakuje se povečanje povpraševanja po strokovnjakih s področja varnosti, prav tako bi se zmanjšale asimetrije informacij o kibernetski varnosti.

Sorazmernost?

Prednostna možnost ne presega tistega, kar je potrebno za zadovoljivo doseganje specifičnih ciljev. S posredovanjem bi se zagotovila varnost izdelkov z digitalnimi elementi v njihovem celotnem življenjskem ciklu in sorazmerno s tveganji.

D. Spremljanje

Kdaj se bo politika pregledala?

Komisija v [36 mesecih] po datumu začetka uporabe pobude ter nato vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu pobude.