Rada
Európskej únie

V Bruseli 18. januára 2021
(OR. en)

Medziinštitucionálny spis:
2020/0359(COD)

14150/20
ADD 3

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

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	16. januára 2021
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	SWD(2020) 344 final
Predmet:	PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU Sprievodný dokument Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii a o zrušení smernice (EÚ) 2016/1148

Delegáciám v prílohe zasielame dokument SWD(2020) 344 final.

Príloha: SWD(2020) 344 final

EURÓPSKA
KOMISIA

V Bruseli 16. 12. 2020
SWD(2020) 344 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU

Sprievodný dokument

Návrh smernice Európskeho parlamentu a Rady

o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii a o zrušení smernice (EÚ) 2016/1148

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

Súhrnný prehľad

Posúdenie vplyvu v súvislosti s *preskúmaním smernice (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“)*

A. Potreba konať

V čom spočíva problém a prečo ide o problém na úrovni EÚ?

Smernica NIS, ktorá viedla k významnej zmene v zmýšľaní o kybernetickej bezpečnosti, ako aj v inštitucionálnom a regulačnom prístupe ku kybernetickej bezpečnosti v mnohých členských štátoch, aj napriek svojim významným výsledkom už ukázala svoje obmedzenia. Digitálna transformácia spoločnosti (posilnená krízou spôsobenou pandémiou COVID-19) rozšírila panorámu hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôsobené a inovačné reakcie. Počet kybernetických útokov naďalej narastá, pričom tieto útoky sú čoraz dômyselnejšie a pochádzajú zo širokej škály zdrojov v rámci EÚ aj mimo nej.

Na základe hodnotenia fungovania smernice NIS sa v rámci posúdenia vplyvu identifikovali tieto problémy: nízka úroveň kybernetickej odolnosti podnikov pôsobiacich v EÚ, nejednotná úroveň odolnosti v jednotlivých členských štátoch a odvetviach a nízka úroveň spoločnej situačnej informovanosti a nedostatočná spoločná reakcia na krízu. Dôsledkom niektorých týchto problémov a faktorov napríklad vznikajú situácie, v rámci ktorých veľké nemocnice v jednom členskom štáte nepatria do rozsahu pôsobnosti smernice NIS, a preto sa od nich nevyžaduje, aby vykonávali z nej vyplývajúce bezpečnostné opatrenia, zatiaľ čo v inom členskom štáte sa na takmer každú jednu nemocnicu v krajine vzťahujú bezpečnostné požiadavky smernice NIS.

Čo by sa malo dosiahnuť?

V rámci preskúmania smernice NIS sa majú dosiahnuť tieto tri všeobecné ciele:

1. **Zvýšiť úroveň kybernetickej odolnosti komplexného súboru podnikov pôsobiacich v Európskej únii vo všetkých príslušných odvetviach,** a to prostredníctvom zavedenia pravidiel, ktoré zabezpečia, aby všetky verejné a súkromné subjekty v rámci vnútorného trhu plniace dôležité funkcie pre hospodárstvo a spoločnosť ako celok boli povinné prijať vhodné opatrenia v oblasti kybernetickej bezpečnosti.
2. **Znížiť mieru nezrovnalostí, pokiaľ ide o odolnosť na vnútornom trhu v odvetviach, na ktoré sa už smernica vzťahuje**, a to prostredníctvom väčšieho zosúladenia 1. rozsahu pôsobnosti *de facto*, 2. bezpečnostných požiadaviek a požiadaviek na oznamovanie incidentov, 3. ustanovení upravujúcich vnútroštátny systém dohľadu a presadzovanie predpisov a 4. spôsobilostí príslušných orgánov v členských štátoch.
3. **Zlepšiť úroveň spoločnej situačnej informovanosti a spoločnej spôsobilosti na prípravu a reakciu,** a to prijatím opatrení na zvýšenie úrovne dôvery medzi príslušnými orgánmi, zdieľaním väčšieho objemu informácií a stanovením pravidiel a postupov v prípade rozsiahleho incidentu alebo krízy.

Aká je pridaná hodnota opatrení na úrovni EÚ (subsidiarita)?

Kybernetická odolnosť v rámci Únie nemôže byť účinná, ak sa k nej prostredníctvom vnútroštátnych alebo regionálnych dátových síl pristupuje odlišným spôsobom. Cieľom smernice NIS bolo napraviť tento nedostatok stanovením rámca pre bezpečnosť sietí a informačných systémov na vnútroštátnej úrovni a úrovni Únie. Jej transpozícia a vykonávanie však takisto odhalili charakteristické nedostatky istých

ustanovení alebo prístupov, ako je napríklad nejasné vymedzenie rozsahu pôsobnosti smernice NIS. Okrem toho je od začiatku krízy spôsobenej pandémiou COVID-19 európske hospodárstvo viac ako kedykoľvek predtým závislé od sietí a informačných systémov a odvetvia a služby sú čoraz viac prepojené. Prvé pravidelné preskúmanie smernice NIS preto vytvorilo príležitosť pre ďalšie opatrenia na úrovni EÚ. Intervenciu EÚ nad rámec súčasných opatrení smernice NIS možno odôvodniť najmä týmito skutočnosťami: i) cezhraničný charakter problému; ii) potenciál opatrenia EÚ zlepšiť a uľahčiť účinné vnútroštátne politiky; iii) príspevok zosúladeného postupu založeného na spolupráci v oblasti politických opatrení NIS k účinnej ochrane údajov a súkromia.

B. Riešenia

Aké sú rôzne možnosti na dosiahnutie týchto cieľov? Existuje uprednostňovaná možnosť? Ak nie, prečo?

V posúdení vplyvu sa analyzovali štyri možnosti politiky: 0. zachovanie súčasného stavu; 1. nelegislatívne opatrenia na zosúladenie transpozície; 2. obmedzené zmeny smernice NIS na ďalšiu harmonizáciu; 3. systémové a štrukturálne zmeny smernice NIS. Možnosť 1 bola v prvotnom štádiu vylúčená, keďže sa od súčasného stavu podstatne neodchyľuje. Z posúdenia vplyvu vyplýva, že **uprednostňovaná je možnosť** 3 (t. j. **systémové a štrukturálne zmeny rámca NIS**), keďže sa v nej počíta so zásadnejšou zmenou prístupu, a to v podobe zahrnutia širšej oblasti hospodárstiev v Únii, ale zároveň s cielenejším dohľadom zameraným na pomerne veľké a kľúčové spoločnosti s jasným stanovením rozsahu uplatňovania. Takisto by sa tým zefektívnili a ďalej harmonizovali povinnosti spoločností týkajúce sa bezpečnosti, vytvorilo by sa účinnejšie nastavenie prevádzkových aspektov a takisto by vznikol jasný základ pre spoločnú zodpovednosť a zodpovednosť príslušných aktérov a podnietila by sa výmena informácií.

Aké sú názory jednotlivých zainteresovaných strán? Kto podporuje ktorú možnosť?

Väčšina príslušných orgánov a podnikov vyjadrila podporu revízii smernice NIS. Počas niekoľkých konzultácií naznačili, že preskúmaná smernica NIS by mala zahŕňať dodatočné (pod-)odvetvia, mala by zosúladiť bezpečnostné opatrenia a oznamovacie povinnosti alebo ich viac zefektívniť. Zainteresované strany takisto vyjadrili podporu novým koncepciám alebo opatreniam súvisiacim s politikou, ktoré tvoria len časť uprednostňovanej možnosti (napr. politiky týkajúce sa bezpečnosti dodávateľského reťazca, inštitucionalizácia operačného rámca EÚ pre krízové riadenie).

C. Vplyvy uprednostňovanej možnosti

Aké sú výhody uprednostňovanej možnosti (prípadne hlavných možností, ak sa žiadna konkrétna možnosť neuprednostňuje)?

Uprednostňovaná možnosť by priniesla významné výhody: odhady založené na hospodárskom modelovaní vypracovanom v rámci podpornej štúdie o preskúmaní smernice NIS naznačujú, že uprednostňovaná možnosť môže viesť k zníženiu nákladov na kybernetickobezpečnostné incidenty o 11,3 miliardy EUR.

V rámci NIS by sa značne rozšíril odvetvový rozsah pôsobnosti, ale popri uvedených výhodách by sa pre nové subjekty, na ktoré sa má rámec vzťahovať, ako aj pre príslušné orgány vyvážilo zaťaženie, ktoré môže vzniknúť na základe požiadaviek smernice NIS, najmä z pohľadu dohľadu. Je to z toho dôvodu, že v novom rámci NIS by sa zaviedol dvojúrovňový prístup s dôrazom na veľké a kľúčové subjekty a rozlišovanie režimu dohľadu, ktorý umožňuje len dohľad *ex post* (t. j. reaktívny a bez všeobecnej povinnosti systematicky preukazovať súlad) pre veľký počet týchto subjektov, a to najmä pre tie, ktoré sa považujú za „dôležité“, ale nie „kľúčové“.

Uprednostňovaná možnosť politiky by celkovo viedla k efektívnym kompromisom a synergiám, pričom má najlepší potenciál zo všetkých analyzovaných možností politiky na zabezpečenie zvýšenej a konzistentnej úrovne kybernetickej odolnosti kľúčových subjektov v Únii, čo by v konečnom dôsledku viedlo k úspore nákladov pre podniky aj spoločnosť.
Aké sú náklady na uprednostňovanú možnosť (prípadne na hlavné možnosti, ak sa žiadna konkrétna možnosť neuprednostňuje)?
Uprednostňovaná možnosť politiky by viedla k istým nákladom na zabezpečenie súladu a presadzovanie predpisov pre príslušné orgány členských štátov (odhaduje sa celkový nárast o približne 20 – 30 % zdrojov). Nový rámec by však priniesol aj značné výhody, a to prostredníctvom lepšieho prehľadu o kľúčových podnikoch a lepšej interakcie s nimi, posilnenú cezhraničnú operačnú spoluprácu, ako aj vzájomnú pomoc a mechanizmy partnerského preskúmania. To by viedlo k celkovému posilneniu spôsobilostí v oblasti kybernetickej bezpečnosti v členských štátoch. Pokiaľ ide o spoločnosti, ktoré by patrili do rozsahu pôsobnosti rámca NIS, odhaduje sa, že by potrebovali zvýšenie o maximálne 22 % svojich súčasných výdavkov v oblasti bezpečnosti IKT v prvých rokoch po zavedení nového rámca NIS (to predstavuje 12 % pre spoločnosti, ktoré už do rozsahu pôsobnosti súčasnej smernice NIS patria). Tento priemerný nárast výdavkov v oblasti bezpečnosti IKT by však viedol k pomernému úžitku z takých investícií, najmä z dôvodu výrazného zníženia nákladov kybernetickobezpečnostných incidentov (odhadom 11,3 miliardy EUR za desať rokov).
Aký je vplyv na MSP a konkurencieschopnosť?
Z rozsahu pôsobnosti rámca NIS by boli podľa uprednostňovanej možnosti vyňaté malé podniky a mikropodniky. Pokiaľ ide o stredné podniky, očakávať možno nárast úrovne výdavkov v oblasti bezpečnosti IKT v prvých rokoch po zavedení nového rámca NIS. Zvyšovanie úrovne bezpečnostných požiadaviek pre tieto subjekty by zároveň aj stimulovalo ich spôsobilosti v oblasti kybernetickej bezpečnosti a pomohlo im zlepšiť ich riadenie rizík v oblasti IKT.
Očakáva sa významný vplyv na štátne rozpočty a verejnú správu?
Malo by to vplyv na štátne rozpočty a verejnú správu: v krátkodobom a strednodobom horizonte sa očakáva nárast približne o 20 – 30 % zdrojov.
Očakávajú sa iné významné vplyvy?
Neočakávajú sa žiadne ďalšie významné negatívne vplyvy. Očakáva sa, že uprednostňovaná možnosť politiky bude viesť k stabilnejším spôsobilostiam v oblasti kybernetickej bezpečnosti a následne bude mať významnejší zmierňujúci vplyv na počet a závažnosť incidentov vrátane porušenia ochrany údajov. Takisto je pravdepodobné, že bude mať pozitívny vplyv na zabezpečenie rovnakých podmienok v členských štátoch pre všetky subjekty, ktoré patria do rozsahu pôsobnosti smernice NIS, a zníži informačné asymetrie v oblasti kybernetickej bezpečnosti.
Proporcionalita?
Uprednostňovaná možnosť neprekračuje rámec nevyhnutný na uspokojivé plnenie špecifických cieľov. Plánované zosúladenie a zefektívnenie bezpečnostných opatrení a oznamovacích povinností sa týka požiadaviek členských štátov a podnikov na zlepšenie súčasného rámca.
D. Následné opatrenia

Kedy sa táto politika preskúma?
Prvé preskúmanie by sa uskutočnilo 54 mesiacov od nadobudnutia účinnosti právneho nástroja. Komisia by poskytla správu o preskúmaní Európskemu parlamentu a Rade. Preskúmanie sa pripraví s podporou agentúry ENISA a skupiny pre spoluprácu.