Rada
Evropské unie

Brusel 18. ledna 2021
(OR. en)

Interinstitucionální spis:
2020/0359(COD)

14150/20
ADD 3

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

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	16. ledna 2021
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	SWD(2020) 344 final
Předmět:	PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ Průvodní dokument k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

Delegace naleznou v příloze dokument SWD(2020) 344 final.

Příloha: SWD(2020) 344 final

EVROPSKÁ
KOMISE

V Bruselu dne 16.12.2020
SWD(2020) 344 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ

Průvodní dokument k

návrhu směrnice Evropského parlamentu a Rady

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

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

Souhrnný přehled

Posouzení dopadů týkající se *přezkumu směrnice (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „směrnice o bezpečnosti sítí a informací“)*

A. Potřeba opatření

V čem spočívá problém a proč se jedná o problém na úrovni EU?

Navzdory svým pozoruhodným úspěchům směrnice o bezpečnosti sítí a informací, která v mnoha členských státech připravila cestu k významné změně ve způsobu uvažování o kybernetické bezpečnosti a v institucionálním a regulačním přístupu k ní, nyní ukazuje i svá omezení. Digitální transformace společnosti (zintenzivněná krizí COVID-19) rozšířila škálu hrozeb a přináší nové výzvy, které vyžadují odpovídající a inovativní reakci. Počet kybernetických útoků stále roste, přičemž z celé řady zdrojů v EU i mimo ni přicházejí neustále sofistikovanější útoky.

Na základě hodnocení fungování směrnice o bezpečnosti sítí a informací byly v posouzení dopadů zjištěny následující problémy: nízká úroveň kybernetické odolnosti podniků působících v EU; kolísavá odolnost členských států a odvětví a nízká úroveň společného přehledu o situaci a nedostatečná společná reakce na krizi. V důsledku některých z těchto problémů a hybných sil například nastávají situace, kdy velké nemocnice v členském státě nespadají do oblasti působnosti směrnice o bezpečnosti sítí a informací, a proto nejsou povinny zavádět z ní vyplývající bezpečnostní opatření, zatímco v jiném členském státě se bezpečnostní požadavky směrnice o bezpečnosti sítí a informací vztahují téměř na každou nemocnici v zemi.

Čeho by mělo být dosaženo?

Přezkum směrnice o bezpečnosti sítí a informací má tři obecné cíle:

1. **Zvýšit úroveň kybernetické odolnosti komplexního souboru podniků působících v Evropské unii napříč všemi příslušnými odvětvími**, a to zavedením pravidel, která zajistí, aby všechny veřejné a soukromé subjekty na vnitřním trhu, které plní důležité funkce pro hospodářství a společnost jako celek, byly povinny přijmout odpovídající opatření v oblasti kybernetické bezpečnosti.
2. **Omezit nesrovnalosti v odolnosti na vnitřním trhu v odvětvích, na která se směrnice již vztahuje,** a to dalším sladěním 1) skutečné oblasti působnosti, 2) požadavků na bezpečnost a hlášení incidentů, 3) ustanovení upravujících vnitrostátní dohled a prosazování práva a 4) schopností příslušných orgánů v členských státech.
3. **Zlepšit úroveň společného přehledu o situaci a kolektivní schopnosti připravit se a reagovat** přijetím opatření ke zvýšení úrovně důvěry mezi příslušnými orgány, sdílením více informací a stanovením pravidel a postupů v případě rozsáhlého incidentu nebo krize.

Jakou přidanou hodnotu budou mít tato opatření na úrovni EU (subsidiarita)?

Kybernetická bezpečnost napříč Unií nemůže být účinná, pokud se k ní bude přistupovat nesourodým způsobem prostřednictvím izolovaných vnitrostátních nebo regionálních koncepcí. Směrnice o bezpečnosti sítí a informací začala tento nedostatek řešit stanovením rámce pro bezpečnost sítí a informačních systémů na vnitrostátní a unijní úrovni. Její provádění však také odhalilo podstatné nedostatky některých ustanovení nebo přístupů, například nejasné vymezení oblasti její působnosti. Od krize COVID-19 navíc evropské hospodářství závisí na sítích a informačních systémech více než kdy

předtím a průmysl a služby jsou stále provázanější. První pravidelný přezkum směrnice o bezpečnosti sítí a informací proto vytvořil příležitost pro další opatření na úrovni EU. Zásah EU, který jde nad rámec současných opatření směrnice o bezpečnosti sítí a informací, je odůvodněn zejména: i) přeshraniční povahou tohoto problému; ii) potenciálem opatření EU ke zlepšení a usnadnění účinných vnitrostátních politik; iii) podílem koordinovaných a společných politických opatření v oblasti sítí a informačních systémů na účinné ochraně údajů a soukromí.

B. Řešení

Prostřednictvím kterých možností lze cílů dosáhnout? Je některá možnost upřednostňována? Pokud ne, proč?

Posouzení dopadů zkoumalo čtyři možnosti politiky: 0) zachovat *status quo*; 1) nelegislativní opatření ke sladění provedení; 2) omezené změny směrnice o bezpečnosti sítí a informací pro účely další harmonizace; 3) systémové a strukturální změny směrnice o bezpečnosti sítí a informací. Možnost 1 byla vyloučena již v rané fázi, jelikož se příliš neodlišuje od *statu quo*. Posouzení dopadů dospělo k závěru, že **upřednostňovanou možností** je možnost č. 3 (tj. **systémové a strukturální změny rámce směrnice o bezpečnosti sítí a informací**), jelikož ta by předjímala zásadnější posun v přístupu k pokrytí širšího segmentu hospodářství v celé Unii, avšak s cílenějším dohledem zaměřeným na poměrně velké a klíčové společnosti, přičemž by jasně určila rozsah uplatnění. Rovněž by zefektivnila a dále harmonizovala povinnosti společností související s bezpečností, vytvořila by účinnější prostředí pro provozní aspekty a také stanovila jasný základ pro sdílené povinnosti a odpovědnost příslušných aktérů a stimulovala by sdílení informací.

Jaké jsou názory jednotlivých zúčastněných stran? Kdo podporuje kterou možnost?

Podporu revizi směrnice o bezpečnosti sítí a informací vyjádřila většina příslušných orgánů a podniků. Ty v průběhu několika konzultací signalizovaly, že přezkoumaná směrnice o bezpečnosti sítí a informací by měla zahrnovat další (pod)odvětví a sladit nebo zefektivnit další bezpečnostní opatření a oznamovací povinnosti. Zúčastněné strany rovněž vyjádřily podporu novým koncepcím nebo opatřením souvisejícím s politikou, která jsou součástí výhradně upřednostňované možnosti (např. bezpečnostní politiky dodavatelských řetězců, institucionalizace provozního rámce krizového řízení EU).

C. Dopady upřednostňované možnosti

Jaké jsou výhody upřednostňované možnosti (je-li nějaká doporučena, jinak uveďte výhody hlavních možností)?

Upřednostňovaná možnost by měla významné výhody: odhady založené na ekonomickém modelování vypracovaném v rámci podpůrné studie k přezkumu směrnice o bezpečnosti sítí a informací naznačují, že upřednostňovaná možnost může vést ke snížení nákladů na incidenty související s kybernetickou bezpečností o 11,3 miliardy EUR.

Odvětvová působnost by se podle rámce směrnice o bezpečnosti sítí a informací značně rozšířila, ale vedle výše uvedených výhod by zátěž, kterou by mohly požadavky směrnice o bezpečnosti sítí a informací způsobit, zejména z perspektivy dohledu, byla vyvážená jak pro nové subjekty, na které se má směrnice vztahovat, tak pro příslušné orgány. Je tomu tak proto, že nový rámec směrnice o bezpečnosti sítí a informací by zavedl dvouúrovňový přístup se zaměřením na velké a klíčové subjekty a diferenciaci režimu dohledu, který u řady z nich umožňuje pouze dohled *ex post* (tj. reaktivní a bez obecné povinnosti systematicky dokumentovat dodržování předpisů), zejména u těch, které jsou považovány za „důležité“, nikoli však za „základní“.

Celkově by upřednostňovaná možnost politiky vedla k účinným kompromisům a součinnostem a měla by největší potenciál ze všech analyzovaných možností politiky zajistit zvýšenou a stálou úroveň kybernetické odolnosti klíčových subjektů v celé Unii, přičemž by nakonec vedla k úsporám nákladů pro podniky i společnost.

Jaké jsou náklady na upřednostňovanou možnost (je-li nějaká doporučena, jinak uveďte náklady na hlavní možnosti)?

Upřednostňovaná možnost politiky by vedla k určitým nákladům na dodržování předpisů a prosazování práva pro příslušné orgány členských států (odhadovalo se celkové zvýšení přibližně o 20–30 % zdrojů). Nový rámec by však také přinesl značné výhody díky lepšímu přehledu o klíčových podnicích a lepší interakci s nimi, díky větší přeshraniční operativní spolupráci, jakož i díky mechanismům vzájemné pomoci a vzájemného hodnocení. To by vedlo k celkovému zlepšení schopností v oblasti kybernetické bezpečnosti ve všech členských státech.

V případě společností, které by spadaly do působnosti rámce směrnice o bezpečnosti sítí a informací, se odhaduje, že by v prvních letech po zavedení nového rámce směrnice o bezpečnosti sítí a informací potřebovaly své současné výdaje na bezpečnost IKT zvýšit maximálně o 22 % (v případě společností, které do oblasti působnosti současné směrnice o bezpečnosti sítí a informací již spadají, by to bylo 12 %). Investice spočívající v tomto průměrném zvýšení výdajů na bezpečnost IKT by však měly přiměřený přínos, zejména by se výrazně snížily náklady na incidenty v oblasti kybernetické bezpečnosti (odhadem o 11,3 miliardy EUR během deseti let).

Jaké budou dopady na malé a střední podniky a na konkurenceschopnost?

Malé podniky a mikropodniky by byly v upřednostňované možnosti z oblasti působnosti rámce směrnice o bezpečnosti sítí a informací vyňaty. U středních podniků lze očekávat, že v prvních letech po zavedení nového rámce směrnice o bezpečnosti sítí a informací by došlo ke zvýšení úrovně výdajů na bezpečnost IKT. Současně by zvýšení úrovně bezpečnostních požadavků na tyto subjekty také stimulovalo jejich schopnosti v oblasti kybernetické bezpečnosti a pomohlo by zlepšit jejich řízení rizik v oblasti IKT.

Očekávají se významné dopady na vnitrostátní rozpočty a správní orgány?

Opatření by mělo dopad na vnitrostátní rozpočty a správní orgány: v krátkodobém a střednědobém horizontu se odhaduje zvýšení zdrojů přibližně o 20–30 %.

Očekávají se jiné významné dopady?

Neočekávají se žádné jiné významné negativní dopady. Předpokládá se, že upřednostňovaná možnost politiky zlepší schopnosti v oblasti kybernetické bezpečnosti, a v důsledku toho bude mít výrazněji zmírňující dopad na počet a závažnost incidentů, včetně narušení zabezpečení údajů. Je také pravděpodobné, že bude mít pozitivní dopad na zajištění rovných podmínek všech subjektů spadajících do oblasti působnosti směrnice o bezpečnosti sítí a informací ve všech členských státech a na snížení informační asymetrie v oblasti kybernetické bezpečnosti.

Proporcionalita?

Upřednostňovaná možnost nepřekračuje rámec toho, co je nezbytné pro uspokojivé splnění konkrétních cílů. Předpokládané sladění a zefektivnění bezpečnostních opatření a povinností podávat hlášení souvisí s požadavky členských států a podniků na zlepšení stávajícího rámce.

D. Návazná opatření
Kdy bude tato politika přezkoumána?
První přezkum by proběhl 54 měsíců po vstupu právního aktu v platnost. Komise by o svém přezkumu podala zprávu Evropskému parlamentu a Radě. Přezkum by byl vyhotoven za podpory agentury ENISA a skupiny pro spolupráci v oblasti bezpečnosti sítí a informací.