EVROPSKÁ
KOMISE

V Bruselu dne 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Maximální využití směrnice o bezpečnosti sítí a informací – účinné provedení směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

CS

Úvod

Směrnice (EU) 2016/1148 o bezpečnosti sítí a informačních systémů v Unii[1] (dále jen „směrnice o bezpečnosti sítí a informací“ nebo „směrnice“) přijatá dne 6. července 2016 je první horizontální právní předpis EU, který řeší výzvy oblasti kybernetické bezpečnosti a přináší skutečnou změnu z hlediska odolnosti vůči bezpečnostním hrozbám a spolupráce v Evropě.

Má tři hlavní cíle:

- zlepšení vnitrostátních schopností v oblasti kybernetické bezpečnosti,
- rozvíjení spolupráce na úrovni EU a
- podporu kultury řízení rizik a hlášení incidentů mezi klíčovými hospodářskými subjekty, zejména provozovateli poskytujícími základní služby pro zachování hospodářských a sociálních činností a poskytovateli digitálních služeb.

Směrnice o bezpečnosti sítí a informací je základním kamenem reakce EU na stále závažnější kybernetické hrozby a výzvy spojené s digitalizací našeho hospodářského a společenského života, a její provádění je tedy zásadní součástí kybernetického balíčku předloženého dne 13. září 2017. Účinnost reakce EU zůstává oslabena, dokud nebude směrnice o bezpečnosti sítí a informací plně provedena ve všech členských státech EU. Tato skutečnost byla též označena za kritický bod ve sdělení Komise o posílení evropského systému kybernetické odolnosti[2] z roku 2016.

V důsledku změn, které směrnice o bezpečnosti sítí a informací přináší, a naléhavé potřeby řešit rychle se vyvíjející situaci v oblasti kybernetických hrozeb, je vhodné věnovat zvláštní pozornost problémům, se kterými se setkávají všichni aktéři při zajišťování včasného a úspěšného provedení této směrnice. Vzhledem ke lhůtě pro její provedení ve vnitrostátním právu (9. května 2018) a lhůtě pro určení provozovatelů základních služeb (9. listopadu 2018) Komise podporuje proces provedení v členských státech a jejich činnost ve skupině pro spolupráci.

Toto sdělení a jeho příloha vychází z přípravné činnosti a analýzy Komise týkající se dosavadního provádění směrnice o bezpečnosti sítí a informací, z informací poskytnutých Agenturou Evropské unie pro bezpečnost sítí a informací (ENISA) a z rozhovorů s členskými státy v rámci fáze provádění směrnice, zejména ve skupině pro spolupráci[3]. Sdělení doplňuje značné dosavadní úsilí dosažené zejména prostřednictvím:

- intenzivní činnosti skupiny pro spolupráci, která se dohodla na pracovním plánu zaměřeném převážně na provedení směrnice o bezpečnosti sítí a informací a zejména

[1] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Směrnice vstoupila v platnost dne 8. srpna 2016.
[2] COM(2016) 410 final.
[3] Mechanismus pro strategickou spolupráci mezi členskými státy ve smyslu článku 11 směrnice o bezpečnosti sítí a informací.

na otázku určení provozovatelů základních služeb a jejich povinností z hlediska bezpečnostních požadavků a hlášení incidentů. Třebaže směrnice ponechává určitou volnost při provádění ustanovení týkajících se provozovatelů základních služeb, členské státy uznaly význam harmonizovaného přístupu v tomto ohledu[4],

- zřízení a rychlého zprovoznění sítě tvořené bezpečnostními týmy CSIRT v souladu s čl. 12 odst. 1 směrnice. Poté již tato síť začala budovat základy strukturované operativní spolupráce na evropské úrovni.

K dosažení cíle vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii na politické i operativní úrovni, které obě tyto struktury představují, je nezbytné plné zapojení všech členských států.

Toto sdělení s přílohou posílí tyto snahy tím, že na jednom místě prezentuje a srovnává osvědčené postupy z členských států, které jsou relevantní pro provedení směrnice, poskytuje další pokyny ohledně toho, jak by směrnice měla být provedena, a podrobněji vysvětluje konkrétní ustanovení. Zastřešujícím cílem je podpořit úsilí členských států o účinné a harmonizované provedení směrnice o bezpečnosti sítí a informací v celé EU.

Toto sdělení bude dále doplněno připravovaným prováděcím nařízením Komise, které blíže upřesní prvky a parametry týkající se požadavků ohledně bezpečnosti a hlášení incidentů pro poskytovatele digitálních služeb podle čl. 16 odst. 8 směrnice o bezpečnosti sítí a informací. Prováděcí nařízení usnadní provedení směrnice, pokud jde o povinnosti týkající se poskytovatelů digitálních služeb[5].

Sdělení představuje hlavní závěry analýzy otázek, které jsou považovány za důležité referenční body a možnou inspiraci z hlediska provedení ve vnitrostátním právu. Zaměřuje se především na ustanovení týkající se schopností a povinností členských států, pokud jde o subjekty, které spadají do oblasti působnosti směrnice. Jeho příloha podrobně zkoumá oblasti, kde Komise spatřuje největší hodnotu v poskytování praktických pokynů k provedení tím, že vysvětluje a vykládá některá ustanovení směrnice a prezentuje osvědčené postupy a dosavadní zkušenosti se směrnicí.

Účinné provedení směrnice o bezpečnosti sítí a informací

Cílem směrnice o bezpečnosti sítí a informací je zajistit vysoký stupeň bezpečnosti sítí a informačních systémů v EU. To znamená zvýšit bezpečnost internetu a soukromých sítí a informačních systémů, na nichž je postaveno fungování naší společnosti a hospodářství. Prvním důležitým prvkem v tomto ohledu je připravenost členských států, která by měla být

[4] Skupina pro spolupráci v současnosti pracuje na referenčních pokynech, které se týkají mimo jiné: kritérií pro určení kritičnosti služeb provozovatele podle čl. 5 odst. 2 směrnice; okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty podle čl. 14 odst. 7 směrnice a bezpečnostních požadavků na provozovatele základních služeb v souladu s čl. 14 odst. 1 a 2.

[5] Návrh prováděcího nařízení je k dispozici k veřejné konzultaci na adrese https://ec.europa.eu/info/law/better-regulation/have-your-say_en.

zajištěna zavedením národních strategií kybernetické bezpečnosti, jak je popsáno ve směrnici, činností bezpečnostních týmů typu CSIRT a příslušných vnitrostátních orgánů.

Komplexnost národních strategií

Je důležité, aby členské státy využily příležitosti provedení směrnice o bezpečnosti sítí a informací k přezkumu svých národních strategií kybernetické bezpečnosti z hlediska případných nedostatků, osvědčených postupů a nových výzev, o nichž pojednává příloha.

Ačkoli se směrnice samozřejmě zaměřuje na ty podniky a služby, které mají klíčový význam, je třeba se uceleně a konsistentně věnovat kybernetické bezpečnosti hospodářství a společnosti jako celku, neboť jsou stále více závislé na IKT. Přijetí komplexních národních strategií, které jdou nad rámec minimálních požadavků směrnice o bezpečnosti sítí a informací (tj. jejich rozšíření nad rámec odvětví a služeb uvedených v přílohách II a III směrnice) by tedy posílilo celkovou úroveň bezpečnosti sítí a informačních systémů.

Vzhledem k tomu, že kybernetická bezpečnost je stále poměrně novou a rychle se rozvíjející oblastí veřejné politiky, je ve většině případů zapotřebí nových investic, přestože celková situace veřejných financí vyžaduje škrty a úspory. Pro dosažení cílů směrnice je proto nutno učinit odvážná rozhodnutí k zajištění odpovídajících finančních a lidských zdrojů, jež jsou nezbytné pro účinné provádění národních strategií, včetně dostatečných zdrojů pro vnitrostátní příslušné orgány a týmy CSIRT.

Účinnost provádění a prosazování

Potřeba určit odpovídající vnitrostátní příslušné orgány a jednotná kontaktní místa je stanovena v článku 8 směrnice a je klíčovým prvkem k zajištění účinného provedení směrnice o bezpečnosti sítí a informací a přeshraniční spolupráce. Zde se v členských státech objevily centralizovanější i méně centralizované přístupy. Tam, kde členské státy přistupují k otázce určení příslušných vnitrostátních orgánů centralizovanějším způsobem, se jako klíčové ukázalo zajištění účinných mechanismů spolupráce mezi četnými orgány a jednotným kontaktním místem (*viz tabulka 1 v bodu 3.2 přílohy*). Tím by se zvýšila účinnost provádění a usnadnilo prosazování.

Dosavadní zkušenosti s ochranou kritické informační infrastruktury (CIIP) mohou pomoci členským státům vytvořit optimální model řízení a zajistit jak účinné odvětvové provádění směrnice o bezpečnosti sítí a informací, tak i jednotný horizontální přístup (*viz bod 3.1 přílohy)*.

Posílení schopností vnitrostátních bezpečnostních týmů typu CSIRT

Bez účinných vnitrostátních týmů CSIRT s odpovídajícími zdroji po celé EU stanovených v článku 9 směrnice o bezpečnosti sítí a informací bude EU i nadále příliš zranitelná vůči přeshraničním kybernetickým hrozbám. Členské státy by proto mohly zvážit rozšíření oblasti působnosti týmů CSIRT nad rámec odvětví a služeb zahrnutých do oblasti působnosti směrnice (*viz bod 3.3 přílohy*). To by vnitrostátním týmům CSIRT umožnilo poskytovat

operativní podporu při kybernetických incidentech, ke kterým dochází v podnicích a organizacích, které do oblasti působnosti směrnice nespadají, avšak jsou pro společnost a hospodářství rovněž důležité. Kromě toho by členské státy mohly plně využít možnosti dodatečného financování, které nabízí program pro infrastrukturu digitálních služeb v oblasti kybernetické bezpečnosti v rámci Nástroje pro propojení Evropy (CEF) určený k posílení schopností vnitrostátních týmů CSIRT a jejich vzájemné spolupráce (*viz bod 3.5 přílohy*).

Konzistentnost procesu určování provozovatelů základních služeb

Podle článku 5 směrnice o bezpečnosti sítí a informací jsou členské státy povinny určit do 9. listopadu 2018 subjekty, které budou považovány za provozovatele základních služeb. V souvislosti s tímto úkolem by členské státy mohly zvážit konsistentní používání definic a pokynů uvedených v tomto sdělení, aby bylo zajištěno, že podobné subjekty, které v rámci vnitřního trhu sehrávají podobnou roli, byly za provozovatele základních služeb konzistentně označovány i v ostatních členských státech. Kromě toho by členské státy mohly zvážit rozšíření oblasti působnosti směrnice o bezpečnosti sítí a informací na orgány veřejné správy, vzhledem k úloze, kterou sehrávají pro společnost a hospodářství jako celek (*viz body 2.1 a 4.1.3 přílohy*).

Velmi užitečné by bylo co největší sladění přístupů jednotlivých členských států k určování provozovatelů základních služeb, zejména dodržováním pokynů vypracovaných skupinou pro spolupráci (*viz bod 4.1.2 přílohy*), jelikož by vedlo k harmonizovanějšímu provádění ustanovení směrnice, a tedy ke zmírnění rizika roztříštěnosti trhu. Pokud provozovatelé základních služeb poskytují základní služby ve dvou či více členských státech, je důležité, aby členské státy usilovaly o dosažení dohody (v rámci konzultačního procesu podle čl. 5 odst. 4) na konsistentním určení subjektů (*viz bod 4.1.7 přílohy*), neboť by se tak zamezilo odlišnému regulačnímu zacházení s týmž subjektem v jurisdikcích různých členských států.

Předkládání informací o určení provozovatelů základních služeb Komisi

Podle čl. 5 odst. 7 se od členských států požaduje, aby Komisi poskytly informace o vnitrostátních opatřeních umožňujících určení provozovatelů základních služeb, seznamu základních služeb, počtu určených provozovatelů základních služeb a významu těchto provozovatelů pro dané odvětví. Kromě toho se od členských států požaduje, aby uvedly případné mezní hodnoty používané v procesu určení ke stanovení příslušné úrovně poskytování služeb nebo významu konkrétního provozovatele pro zachování dostatečné nabídky. Členské státy by rovněž mohly zvážit, že by, v případě potřeby důvěrně, poskytly Komisi seznam určených provozovatelů základních služeb, neboť by to pomohlo zlepšit přesnost a kvalitu posouzení ze strany Komise (*viz body 4.1.5 a 4.1.6 přílohy)*.

Harmonizované přístupy týkající se požadavků kladených na provozovatele základních služeb ohledně bezpečnosti a hlášení incidentů

V souvislosti s povinnostmi provozovatelů základních služeb z hlediska bezpečnostních požadavků a hlášení incidentů (čl. 14 odst. 1, 2 a 3) by harmonizovaný přístup k požadavkům na bezpečnost a hlášení incidentů za účelem snadnějšího dodržování požadavků ze strany

provozovatelů základních služeb přes hranice členských států v co nejvyšší míře podpořil účinek jednotného trhu. I nadále se zde odkazuje na práci na pokynech skupiny pro spolupráci (*viz body 4.2 a 4.3 přílohy*).

V případě rozsáhlého kybernetického bezpečnostního incidentu s dopadem v několika členských státech je velmi pravděpodobné, že provozovatel základních služeb nebo poskytovatel digitálních služeb předloží povinné hlášení o incidentu podle čl. 14 odst. 3 nebo čl. 16 odst. 3, nebo že tak dobrovolně učiní jiný subjekt, který nespadá do oblasti působnosti směrnice, podle čl. 20 odst. 1. V souladu s doporučením Komise o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize by členské státy mohly zvážit harmonizaci svých vnitrostátních přístupů, aby mohly na základě těchto hlášení co nejdříve poskytnout relevantní informace příslušným orgánům nebo týmům CSIRT v ostatních dotčených členských státech. Přesné a užitečné informace by byly klíčové ke snížení počtu případů infekcí nebo k řešení zranitelností dříve, než dojde k jejich zneužití.

V duchu partnerství a s cílem využít směrnici o bezpečnosti sítí a informací co nejlépe hodlá Komise rozšířit podporu z Nástroje pro propojení Evropy na všechny příslušné zúčastněné strany, na které se tento právní předpis vztahuje. Zatímco dosud byl kladen důraz na budování schopností týmů CSIRT a vytvoření platformy pro rychlou a účinnou operativní spolupráci vedoucí k posílení sítě CSIRT, nyní Komise posoudí, jak mohou být finanční prostředky z Nástroje pro propojení Evropy přínosné i pro příslušné vnitrostátní orgány, jakož i pro provozovatele základních služeb a poskytovatele digitálních služeb.

Závěr

S ohledem na blížící se konec lhůty pro provedení směrnice o bezpečnosti sítí a informačních systémů ve vnitrostátním právu (9. května 2018) a lhůty pro určení provozovatelů základních služeb (9. listopadu 2018) by členské státy měly přijmout vhodná opatření pro zajištění toho, aby ustanovení a modely spolupráce uvedené ve směrnici o bezpečnosti sítí a informací přinesly co nejlepší nástroje na úrovni EU k dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů v celé Unii. Komise vyzývá členské státy, aby v tomto procesu zvážily příslušné informace, pokyny a doporučení uvedené v tomto sdělení.

Toto sdělení může být doplněno dalšími opatřeními, včetně těch, která přinese probíhající činnost v rámci skupiny pro spolupráci.