EURÓPSKA
KOMISIA

V Bruseli 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

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Čo najlepšie využívanie sietí a informačných systémov - smerom k účinnej implementácii smernice 2016/1148/EÚ, pokiaľ ide o opatrenia na dosiahnutie vysokej všeobecnej úrovne bezpečnosti sietí a informačných systémov v EÚ

SK

Úvod

Smernica (EÚ) 2016/1148 zo 6. júla 2016 o bezpečnosti sietí a informačných systémov v Únii[1] (ďalej len „smernica NIS“ alebo „smernica“) je prvým horizontálnym právnym predpisom EÚ na riešenie výziev kybernetickej bezpečnosti, ktorý prináša skutočnú zmenu z hľadiska odolnosti a európskej spolupráce v oblasti kybernetickej bezpečnosti.

Smernica má tri hlavné ciele:

- zlepšenie vnútroštátnych spôsobilostí z hľadiska kybernetickej bezpečnosti,
- budovanie spolupráce na úrovni EÚ a
- podpora kultúry riadenia rizík a oznamovania incidentov medzi kľúčovými hospodárskymi subjektmi – najmä prevádzkovateľmi základných služieb pre zachovanie hospodárskych a spoločenských činností (PZS), ale aj poskytovateľmi digitálnych služieb (PDS).

Smernica NIS je základným pilierom reakcie EÚ na čoraz závažnejšie kybernetické hrozby a výzvy spojené s digitalizáciou nášho hospodárskeho a spoločenského života, a jej vykonávanie je teda esenciálnou súčasťou kybernetického balíka predstaveného 13. septembra 2017. Účinnosť reakcie EÚ je oslabená, kým nebude smernica NIS plne transponovaná vo všetkých členských štátoch EÚ. Za kľúčovú otázku to označuje aj oznámenie Komisie z roku 2016 o posilnení odolnosti európskeho kybernetického systému[2].

Zmena, ktorú smernica NIS prináša, ako aj naliehavosť potreby čeliť dynamickej panoráme kybernetických hrozieb si vyžadujú zameranie osobitnej pozornosti na výzvy pre všetkých aktérov pri zaisťovaní včasnej a úspešnej transpozície danej smernice. Keďže termín transpozície je 9. máj 2018 a termín na identifikáciu prevádzkovateľov základných služieb je 9. november 2018, Komisia podporuje transpozičný proces v členských štátoch, ako aj ich súvisiacu činnosť v skupine pre spoluprácu.

Toto oznámenie spolu s prílohou vychádza z prípravných prác Komisie a analýz doterajšieho vykonávania smernice NIS, z podnetov Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), ako aj z diskusií s členskými štátmi vo fáze transpozície smernice, najmä v skupine pre spoluprácu[3]. Oznámenie dopĺňa doterajšie nezanedbateľné úsilie, a to najmä:

- intenzívnu činnosť skupiny pre spoluprácu, ktorá sa dohodla na pracovnom pláne so zameraním predovšetkým na transpozíciu smernice NIS, a najmä na problém identifikácie prevádzkovateľov základných služieb a ich povinností z hľadiska bezpečnostných požiadaviek a oznamovania incidentov. Hoci smernica ponecháva pri

[1] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Smernica nadobudla účinnosť 8. augusta 2016.
[2] COM(2016) 410 final.
[3] Mechanizmus strategickej spolupráce medzi členskými štátmi v zmysle článku 11 smernice NIS.

transpozícii ustanovení o prevádzkovateľoch základných služieb určitú voľnosť, členské štáty uznali význam harmonizovaného prístupu v tomto smere[4],

- zriadenie a promptné sfunkčnenie siete jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT) v súlade s článkom 12 ods. 1 smernice. Táto sieť už začala budovať základy štruktúrovanej operačnej spolupráce na európskej úrovni.

Na dosiahnutie cieľa vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii je nevyhnutné úplné angažovanie všetkých členských štátov na politickej i operačnej úrovni, ktoré tieto dve štruktúry reprezentujú.

Toto oznámenie vrátane prílohy posilní uvedené snahy vďaka zhromaždeniu a porovnaniu osvedčených postupov členských štátov, ktoré sú relevantné pre vykonávanie smernice, bližšiemu usmerneniu k tomu, ako by sa mala smernica vykonať, a podrobnejším vysvetlením konkrétnych ustanovení. Konečným cieľom je podporiť členské štáty v účinnom a zosúladenom vykonávaní smernice NIS v celej EÚ.

Toto oznámenie bude ďalej doplnené pripravovaným vykonávacím nariadením Komisie o bližšej špecifikácii prvkov a parametrov súvisiacich s požiadavkami na poskytovateľov digitálnych služieb v oblasti bezpečnosti a oznamovania incidentov v zmysle článku 16 ods. 8 smernice NIS. Uvedené vykonávacie nariadenie uľahčí vykonávanie smernice z hľadiska povinností poskytovateľov digitálnych služieb[5].

V tomto oznámení sa predstavujú kľúčové závery analýzy problémov, ktoré sa považujú za významnú referenciu a možnú inšpiráciu z hľadiska transpozície do vnútroštátnych legislatív. Primárne sa zameriava na ustanovenia, ktoré sa týkajú spôsobilostí a povinností členských štátov z hľadiska subjektov, ktoré spadajú do rozsahu pôsobnosti smernice. V prílohe sa podrobnejšie skúmajú oblasti, v ktorých Komisia vidí najvyšší potenciál praktického usmernenia z hľadiska transpozície, pričom uvádza vysvetlenie a svoj výklad niektorých ustanovení smernice, a zároveň prezentuje osvedčené postupy a doterajšie skúsenosti so smernicou.

Účinné vykonávanie smernice NIS

Cieľom smernice NIS je vysoká spoločná úroveň bezpečnosti sietí a informačných systémov v celej EÚ. Znamená to posilnenie zabezpečenia internetu a súkromných sietí a informačných systémov, o ktoré sa opiera fungovanie našej spoločnosti a hospodárstva. Prvým dôležitým prvkom v tomto smere je pripravenosť členských štátov, ktorá by sa mala zabezpečiť

[4] Skupina pre spoluprácu momentálne pracuje na referenčných usmerneniach, ktoré sa týkajú okrem iného: kritérií na identifikáciu toho, či prevádzkovateľ poskytuje základné služby, v zmysle článku 5 ods. 2 smernice; okolností, za ktorých musia prevádzkovatelia základných služieb oznamovať incidenty v zmysle článku 14 ods. 7 smernice a bezpečnostných požiadaviek na prevádzkovateľov základných služieb v súlade s článkom 14 ods. 1 a 2.

[5] Návrh vykonávacieho nariadenia je sprístupnený na verejnú konzultáciu na adrese https://ec.europa.eu/info/law/better-regulation/have-your-say_sk.

zavedením národných stratégií kybernetickej bezpečnosti (ako sa opisuje v smernici), ako aj prácou jednotiek CSIRT a príslušných vnútroštátnych orgánov.

Robustnosť národných stratégií

Je dôležité, aby členské štáty poňali transpozíciu smernice NIS ako príležitosť na prehodnotenie svojich národných stratégií kybernetickej bezpečnosti z hľadiska prípadných medzier, osvedčených postupov a nových výziev, ktorým sa venuje príloha.

Hoci smernica sa pochopiteľne zameriava na tie spoločnosti a služby, ktoré majú osobitný kľúčový význam, holisticky a konzistentne sa treba zamerať na kybernetickú bezpečnosť hospodárstva a spoločnosti ako celku, keďže tie sa čoraz viac opierajú o IKT. Prijatie robustných národných stratégií nad rámec minimálnych požiadaviek smernice NIS (t. j. ich rozšírenie nad rámec odvetví a služieb uvedených v prílohách II, resp. III k smernici) by teda posilnilo celkovú úroveň bezpečnosti sietí a informačných systémov.

Keďže kybernetická bezpečnosť je stále relatívne novou a rýchlo sa rozvíjajúcou oblasťou verejnej politiky, vo väčšine prípadov budú potrebné nové investície, aj keď si celková situácia verejných financií vyžaduje škrty a úspory. Dosiahnutie cieľov smernice si preto nevyhnutne vyžaduje ambiciózne rozhodnutia o zaistení primeraných finančných a ľudských zdrojov, ktoré sú nevyhnutné na účinnú implementáciu národných stratégií, vrátane dostatočných zdrojov príslušných vnútroštátnych orgánov a jednotiek CSIRT.

Účinnosť vykonávania a presadzovania

Potrebe určiť vnútroštátne príslušné orgány a jednotné kontaktné miesta sa venuje článok 8 smernice, pričom ide o kľúčový prvok na zaistenie účinného vykonávania smernice NIS a cezhraničnej spolupráce. Tu sa v členských štátoch objavili centralizovanejšie i menej centralizované prístupy. Tam, kde členské štáty pristupujú k otázke určenia vnútroštátnych príslušných orgánov decentralizovanejšie, sa ako kľúčová ukázala potreba účinných mechanizmov spolupráce medzi jednotlivými orgánmi a jednotným kontaktným miestom (*pozri tabuľku 1 v oddiele 3.2 prílohy*). Posilní sa tým účinnosť vykonávania a uľahčí presadzovanie.

Doterajšie skúsenosti s ochranou kritických informačných infraštruktúr (CIIP) môžu členským štátom pomôcť pri návrhu optimálneho modelu riadenia a zaistiť účinnú sektorovú implementáciu smernice NIS, ako aj zosúladený horizontálny prístup (*pozri oddiel 3.1 prílohy*).

Posilnenie spôsobilostí vnútroštátnych jednotiek CSIRT

Bez účinných vnútroštátnych jednotiek CSIRT s dostatočnými zdrojmi po celej EÚ v zmysle článku 9 smernice NIS bude Únia príliš zraniteľná voči cezhraničným kybernetickým hrozbám. Členské štáty by preto mohli zvážiť rozšírenie rozsahu pôsobnosti jednotiek CSIRT nad rámec odvetví a služieb, ktoré upravuje smernica (*pozri oddiel 3.3 prílohy*). Vnútroštátne jednotky CSIRT tak budú môcť poskytovať operačnú podporu pri kybernetických

incidentoch, ku ktorým dôjde v spoločnostiach a organizáciách, ktoré síce nespadajú do rozsahu pôsobnosti smernice, no tiež sú pre spoločnosť a hospodárstvo dôležité. Okrem toho by členské štáty mohli plne využiť možnosti dodatočného financovania, ktoré ponúka program kybernetickej bezpečnosti infraštruktúr digitálnych služieb (DSI) v rámci nástroja na prepájanie Európy (NPE) určený na posilnenie spôsobilostí vnútroštátnych jednotiek CSIRT a ich vzájomnej spolupráce (*pozri oddiel 3.5 prílohy*).

Konzistentnosť procesu identifikácie PZS

V súlade s článkom 5 smernice NIS sa od členských štátov vyžaduje, aby do 9. novembra 2018 identifikovali subjekty, ktoré sa budú považovať za prevádzkovateľov základných služieb. V kontexte tejto úlohy by členské štáty mohli zohľadniť konzistentné použitie vymedzení a usmernení uvedených v tomto odporúčaní, aby sa zaistilo, že podobné subjekty, ktoré zohrávajú na vnútornom trhu podobné roly, sa konzistentne označia za prevádzkovateľov základných služieb aj v ďalších členských štátoch. Členské štáty by okrem toho mohli zvážiť aj rozšírenie pôsobnosti smernice NIS na verejné správy vzhľadom na ich úlohu v spoločnosti a hospodárstve ako celku (*pozri oddiely 2.1 a 4.1.3 prílohy*).

Maximálne možné zosúladenie vnútroštátnych prístupov k identifikácii prevádzkovateľov základných služieb – najmä dodržiavaním usmernení skupiny pre spoluprácu (*pozri oddiel 4.1.2 prílohy*) – by bolo veľmi užitočné, keďže by viedlo k harmonizovanejšiemu uplatňovaniu ustanovení smernice, a tak zmiernilo riziko fragmentácie trhu. Ak prevádzkovatelia základných služieb poskytujú základné služby v dvoch alebo viacerých členských štátoch, je kľúčové, aby sa členské štáty usilovali o dohodu v kontexte konzultačného procesu podľa článku 5 ods. 4 na jednotnej identifikácii týchto subjektov (*pozri oddiel 4.1.7 prílohy*), keďže by sa tak zabránilo odlišnému regulačnému zaobchádzaniu s daným subjektom v rámci kompetencií rôznych členských štátov.

Informovanie Komisie o identifikácii PZS

V súlade s článkom 5 ods. 7 sa od členských štátov žiada, aby Komisii poskytli informácie o vnútroštátnych opatreniach, ktoré umožnia identifikáciu PZS, zoznamu základných služieb, počtu identifikovaných PZS a relevantnosti týchto prevádzkovateľov v danom odvetví. Okrem toho sa od členských štátov žiada, aby uviedli prípadné prahové hodnoty, ktoré v procese identifikácie používajú pri určovaní príslušnej úrovne poskytovania služieb či významu daného prevádzkovateľa z hľadiska udržania dostatočnej úrovne poskytovania služieb. Členské štáty by takisto mohli zvážiť, že by Komisii poskytli zoznamy identifikovaných prevádzkovateľov základných služieb (podľa potreby dôverne), keďže by to pomohlo spresniť a skvalitniť posúdenie Komisie (*pozri oddiely 4.1.5 a 4.1.6 prílohy*).

Zosúladené prístupy v oblasti požiadaviek na PZS z hľadiska bezpečnosti a oznamovania incidentov

V súvislosti s povinnosťami prevádzkovateľov základných služieb z hľadiska bezpečnostných požiadaviek a oznamovania incidentov (článok 14 ods. 1, 2 a 3) by zosúladený prístup k bezpečnostným požiadavkám a oznamovaniu incidentov, ktorý by PZS uľahčil dodržiavanie

požiadaviek vo viacerých členských štátoch EÚ, v maximálnej možnej miere podporil efekt jednotného trhu. Aj v tomto smere je referenciou práca na usmernení v rámci skupiny pre spoluprácu (*pozri oddiely 4.2 a 4.3 prílohy*).

V prípade rozsiahleho kybernetického incidentu s dosahom vo viacerých členských štátoch je veľmi pravdepodobné, že niektorý PZS alebo PDS predloží povinné oznámenie o incidente podľa článku 14 ods. 3, resp. článku 16 ods. 3, alebo že toto oznámenie dobrovoľne predloží iný subjekt, ktorý nespadá do pôsobnosti smernice, v zmysle článku 20 ods. 1. V súlade s odporúčaním Komisie ku koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu by členské štáty mohli zvážiť zosúladenie svojich vnútroštátnych prístupov, aby na základe týchto oznámení dokázali čo najskôr poskytnúť relevantné informácie príslušným orgánom alebo jednotkám CSIRT v ostatných dotknutých členských štátoch. Presné a užitočné informácie sú kľúčové na obmedzenie počtu prípadov infikovania či na riešenie zraniteľných miest skôr, než ich niekto zneužije.

V duchu partnerstva a snahe využiť smernicu NIS čo najlepšie plánuje Komisia rozšíriť podporu z Nástroja na prepájanie Európy na všetky zainteresované subjekty, ktorých sa dotýka tento právny predpis. Zatiaľ čo doposiaľ sa kládol dôraz na budovanie kapacít jednotiek CSIRT a sprevádzkovanie platformy rýchlej a účinnej operačnej spolupráce, čím sa sieť CSIRT posilnila, Komisia teraz preskúma, ako môžu financovanie z Nástroja na prepájanie Európy využiť aj vnútroštátne príslušné orgány, prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb.

Záver

Vzhľadom na blížiaci sa termín transpozície smernice NIS do vnútroštátneho práva (9. máj 2018) a termín na identifikáciu prevádzkovateľov základných služieb (9. november 2018) by mali členské štáty prijať vhodné opatrenia na zaistenie toho, aby ustanovenia a modely spolupráce uvedené v smernici NIS priniesli na úrovni EÚ čo najlepšie nástroje na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v celej Únii. Komisia vyzýva členské štáty, aby v tomto procese zohľadnili relevantné informácie, usmernenia a odporúčania uvedené v tomto oznámení.

Toto oznámenie môže byť doplnené o ďalšie opatrenia vrátane tých, ktoré prinesie prebiehajúca činnosť skupiny pre spoluprácu.