EURÓPSKA
KOMISIA

V Bruseli 13. 9. 2017
COM(2017) 474 final

SPRÁVA KOMISIE EURÓPSKEMU PARLAMENTU A RADE

o posúdení rozsahu, v akom členské štáty prijali opatrenia, ktoré sú nevyhnutné na dosiahnutie súladu so smernicou 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV

Obsah

Obsah ... 2
1. Úvod ... 3
1.1. Ciele a rozsah pôsobnosti smernice ... 3
1.2 Účel a metodika správy ... 5
2. Transpozičné opatrenia ... 6
2.1 Právne vymedzenie pojmov (článok 2 smernice) ... 6
a) Informačný systém ... 6
b) Počítačové údaje ... 6
c) Právnická osoba ... 6
d) Bez oprávnenia ... 6
2.2 Konkrétne trestné činy (články 3 až 7 smernice) ... 7
a) Protiprávny prístup do informačných systémov ... 7
b) Protiprávny zásah do systému ... 7
c) Protiprávny zásah do údajov ... 7
d) Protiprávne zachytávanie údajov ... 7
e) Nástroje na spáchanie trestných činov ... 8
2.3 Všeobecné pravidlá týkajúce sa uvedených trestných činov (články 8 až 12 smernice) .. 8
a) Navádzanie, pomoc a podnecovanie ... 8
b) Pokus ... 8
c) Sankcie ... 8
d) Zodpovednosť právnických osôb ... 10
e) Sankcie voči právnickým osobám ... 10
f) Súdna právomoc ... 11
2.2 Funkčné otázky (články 13 a 14 smernice) ... 11
a) Ustanovenie týkajúce sa funkčného vnútroštátneho kontaktného miesta ... 11
b) Informácie o zriadených funkčných vnútroštátnych kontaktných miestach ... 12
c) Oznamovacie kanály ... 12
d) Zber štatistických údajov ... 12
e) Zasielanie štatistických údajov Komisii ... 12
3. Záver a ďalšie kroky ... 12

1. Úvod

Podľa hodnotenia hrozieb internetovej organizovanej trestnej činnosti za rok 2016, ktoré vypracoval Europol, je počítačová kriminalita čoraz agresívnejšia a konfrontačnejšia. Dokazujú to rôzne formy počítačovej kriminality, vrátane útokov na informačné systémy[1]. Medzi vážnymi formami útokov, ktoré Europol spomína, je používanie škodlivého softvéru a sociálne inžinierstvo s cieľom preniknúť do informačných systémov a prevziať nad nimi kontrolu alebo zachytávať informácie, ako aj spúšťanie rozsiahlych sieťových útokov, namierených aj na kritickú infraštruktúru. Tieto útoky sa považujú za kľúčové hrozby pre našu spoločnosť.

Keďže sa čoraz viac informácií ukladá v cloudoch a informácie a páchatelia sú dnes vysoko mobilní, cezhraničná spolupráca orgánov presadzovania práva sa stala nevyhnutnou pri väčšine vyšetrovaní počítačovej kriminality.

Aby mohli členské štáty účinne bojovať proti tejto kriminalite, je potrebné spoločne vymedziť, ktoré činy sa budú považovať za útoky na informačné systémy. Ďalej je potrebné aproximovať úrovne sankcií a funkčné prostriedky na hlásenie trestných činov a výmenu informácií medzi orgánmi. S týmto cieľom 12. augusta 2013 Európsky parlament a Rada prijali smernicu 2013/40/EU o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (ďalej len „smernica“).[2]

1.1. Ciele a rozsah pôsobnosti smernice

Ciele tejto smernice sú aproximácia trestného práva členských štátov[3] v oblasti útokov na informačné systémy, ako aj zlepšenie spolupráce medzi príslušnými orgánmi. Dosiahne sa to ustanovením minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a príslušných sankcií v oblasti útokov na informačné systémy ako aj požiadavkou funkčných kontaktných miest, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni.

Vymedzenia relevantných pojmov sa v smernici uplatňujú takto:

- „informačný systém“ v článku 2 písm. a)[4]. Vymedzenie pojmu je podobné ako vymedzenie počítačového systému v článku 1 písm. a) Dohovoru Rady Európy o počítačovej kriminalite z 23. novembra 2001 („Budapeštiansky dohovor“), avšak v smernici sa výslovne vzťahuje aj na samotné počítačové údaje.
- „počítačové údaje“ v článku 2 písm. b). Vymedzenie pojmu vychádza z článku 1 písm. b) Budapeštianskeho dohovoru, avšak namiesto počítačového systému sa uvádza informačný systém.

[1] Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2016, ktoré vypracoval Europol, je dostupné na https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:sk:PDF

[3] Odteraz sa pojem „členské štáty“ alebo „všetky členské štáty“, pokiaľ nie je výslovne uvedené inak, vzťahuje na členské štáty, ktoré sú viazané smernicou, t. j. všetky členské štáty EÚ okrem Dánska, ktoré sa nezúčastnilo na prijatí smernice v súlade s článkami 1 a 2 Protokolu o postavení Dánska, ktorý je pripojený k Zmluve o Európskej únii a Zmluve o fungovaní Európskej únie. V súlade s článkom 3 Protokolu (č. 21) o postavení Spojeného kráľovstva a Írska sa oba štáty zúčastnili na prijatí smernice a sú ňou viazané.

[4] Všetky spomenuté články sú článkami smernice, pokiaľ nie je uvedené inak.

- „právnická osoba“ v článku 2 písm. c). Vymedzenie pojmu má za cieľ zabezpečiť zodpovednosť fyzických aj právnických osôb, a zároveň z nej vylúčiť štáty, verejnoprávne subjekty a verejnoprávne medzinárodné organizácie.
- „bez oprávnenia“ v článku 2 písm. d). Vymedzenie pojmu sa týka všeobecnej zásady trestného práva a jeho cieľom je vylúčiť trestnú zodpovednosť osoby, ktorá koná buď v súlade s vnútroštátnym právom alebo s povolením vlastníka či iného držiteľa práv na informačný systém alebo jeho časť.

Vymedzujú sa **konkrétne trestné činy**, a to:

- protiprávny prístup do informačných systémov ako taký (článok 3);
- protiprávny zásah do systému (článok 4), ktorý zahŕňa akýkoľvek protiprávny vstup do informačného systému, ktorý závažne zabráni fungovaniu informačného systému alebo fungovanie preruší;
- protiprávny zásah do údajov (článok 5), ktorý sa týka akéhokoľvek neoprávneného zásahu do počítačových údajov, ktorý naruší ich integritu a dostupnosť;
- protiprávne zachytávanie (článok 6) neverejného prenosu počítačových údajov a elektromagnetického vysielania z informačného systému nesúceho takéto údaje;
- protiprávne poskytovanie nástrojov na spáchanie spomínaných trestných činov (článok 7). V tejto súvislosti môže byť takýmto nástrojom počítačový program, počítačové heslo alebo iný údaj, ktorý poskytne prístup do informačného systému.

V smernici sa navyše **rozširuje trestná zodpovednosť** na navádzanie, pomoc a podnecovanie na spáchanie trestných činov uvedených vyššie fyzickými a/alebo právnickými osobami a na ich pokus o spáchanie takýchto trestných činov (článok 8). Navádzanie, pomoc a podnecovanie sa týkajú všetkých trestných činov uvedených v článkoch 3 až 7, pokus sa týka iba činov uvedených v článkoch 4 a 5.

Dolné hranice najvyšších **sankcií** za trestné činy uvedené v smernici sa stanovujú v článku 9:

- Ako základ je horná hranica trestu odňatia slobody stanovená najmenej na dva roky za všetky trestné činy okrem tých, ktoré sú uvedené v článku 8 (článok 9 ods. 2).
- Najvyšší trest odňatia slobody za trestné činy uvedené v článkoch 4 a 5 je stanovený najmenej na tri roky v prípade, že bolo postihnuté veľké množstvo informačných systémov (vo všeobecnosti označované ako trestné činy vytvárania botnetov; článok 9 ods. 3).
- Najvyšší trest odňatia slobody stanovený najmenej na päť rokov sa vyžaduje za trestné činy uvedené v článkoch 4 a 5 spáchané v rámci zločineckej organizácie [článok 9 ods. 4 písm. a)], ktoré spôsobili závažnú škodu [článok 9 ods. 4 písm. b)] alebo boli spáchané na informačnom systéme kritickej infraštruktúry [článok 9 ods. 4 písm. c)].
- V prípade, že je trestný čin podľa článkov 4 a 5 spáchaný prostredníctvom zneužitia osobných údajov inej osoby, členské štáty by mali zabezpečiť, aby sa to mohlo považovať za priťažujúce okolnosti, pokiaľ tieto okolnosti už nepatria pod iný trestný čin (článok 9 ods. 5).

V nasledujúcich článkoch sa stanovujú minimálne podmienky **zodpovednosti právnických osôb** (článok 10) a poskytujú sa príklady sankcií, ktoré je možné právnickým osobám uložiť (článok 11).

Keďže uvedené trestné činy môžu byť spáchané (v zmysle „vykonané“) v mieste, kde páchateľ reálne koná, pričom ich účinky na napádaný informačný systém sa môžu prejaviť na

inom mieste, v článku 12 sa vymedzujú povinnosti pri stanovení **súdnej právomoci,** pričom sa rozlišuje:

- miesto, kde bol páchateľ fyzicky prítomný, keď bol trestný čin spáchaný,
- umiestnenie napadnutého informačného systému,
- štátna príslušnosť páchateľa,
- miesto obvyklého pobytu páchateľa a
- sídlo právnickej osoby, v ktorej prospech bol trestný čin spáchaný.

Pokiaľ ide o výmenu informácií, v článku 13 ods. 1 sa stanovuje povinnosť členských štátov zabezpečiť, aby mali funkčné **vnútroštátne kontaktné miesto**, ktoré bude k dispozícii 24 hodín denne a sedem dní v týždni, aby mohli odpovedať na naliehavé žiadosti zo zahraničia do 8 hodín.

Ďalej musia členské štáty prijať potrebné opatrenia na **uľahčenie ohlasovania** trestných činov uvedených vyššie príslušným vnútroštátnym orgánom (článok 13 ods. 3) a na zber a spoločné využívanie minimálneho množstva **štatistických údajov** o týchto činoch (článok 14).

1.2 Účel a metodika správy

V článku 16 smernice sa stanovuje povinnosť členských štátov uviesť do účinnosti zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu so smernicou najneskôr do 4. septembra 2015 a oznámiť ich Komisii.

Komisia touto správou spĺňa požiadavku podľa článku 17 smernice, aby predložila Európskemu parlamentu a Rade správu, v ktorej posúdi rozsah, v akom členské štáty prijali opatrenia nevyhnutné na dosiahnutie súladu so smernicou. Účelom správy je poskytnúť stručný a informatívny prehľad hlavných transpozičných opatrení, ktoré členské štáty prijali.

Transpozícia členskými štátmi zahŕňala zber informácií o príslušných právnych predpisoch a správnych opatreniach, ich analýzu a navrhnutie nových právnych predpisov alebo — vo väčšine prípadov — zmenu existujúcich zákonov a bola zavŕšená prijatím právnych predpisov a podaním správy Komisii.

Do uplynutia lehoty na transpozíciu 22 členských štátov oznámilo Komisii, že dokončilo transpozíciu smernice v plnom rozsahu. V novembri 2015 Komisia začala postupy v prípade nesplnenia povinnosti v súvislosti s neoznámením vnútroštátnych transpozičných opatrení proti zvyšným piatim členským štátom: BE, BG, EL, IE a SI[5]. K 31. máju 2017 postupy v prípade nesplnenia povinnosti v súvislosti s neoznámením vnútroštátnych transpozičných opatrení proti BE, BG a IE ešte prebiehali.[6]

[5] Členské štáty sa v tomto dokumente uvádzajú skratkami podľa : http://publications.europa.eu/code/sk/sk-5000600.htm.

[6] Informácie o rozhodnutiach Komisie o postupoch v prípade nesplnenia povinnosti nájdete na: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=sk.

Opis a analýza v tejto správe vychádzajú z informácií, ktoré členské štáty poskytli do 31. mája 2017.[7] Oznámenia prijaté po uvedenom dátume neboli zohľadnené. Zohľadnili sa všetky oznámené opatrenia týkajúce sa vnútroštátnych právnych predpisov, ako aj rozhodnutia súdov a v prípadoch, kedy to bolo vhodné, aj spoločná právna teória. V priebehu analýzy Komisia navyše kontaktovala členské štáty priamo, keď bolo potrebné alebo vhodné získať doplňujúce informácie alebo objasnenie. V analýze sa zohľadnili všetky získané informácie.

Okrem problémov identifikovaných v tejto správe môžu existovať ďalšie výzvy spojené s transpozičnými a inými ustanoveniami, ktoré neboli oznámené Komisii, alebo ďalší legislatívny alebo nelegislatívny vývoj. Táto správa preto Komisii nebráni v ďalšom hodnotení určitých ustanovení s cieľom podporiť členské štáty pri transpozícii a uplatňovaní smernice.

2. Transpozičné opatrenia

2.1 Právne vymedzenie pojmov (článok 2 smernice)

V článku 2 smernice sú právne vymedzené pojmy „informačný systém“ [písm. a)], „počítačové údaje“ [písm. b)], „právnická osoba“ [písm. c)] a „bez oprávnenia“ [písm. d)]. Iba CY a UK (Gibraltár) zaviedli právne predpisy týkajúce sa všetkých aspektov týchto vymedzených pojmov. Podrobne to znamená:

a) Informačný systém

Pojem vymedzený v smernici vychádza z vymedzenia pojmu „počítačový systém“ v článku 1 písm. a) Budapeštianskeho dohovoru, pričom počítačové údaje boli doplnené ako súčasť informačného systému. CY, EL, IE, FI, HR, MT, PT a UK (Gibraltár) prijali právne predpisy s vymedzením pojmu informačný systém, pričom informácie poskytnuté DE, ES, FR, LU, LV, PL, SE a SK neboli presvedčivé. V prípade zvyšných členských štátov, t.j. AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI a UK (s výnimkou Gibraltáru), v príslušnom právnom vymedzení pojmov sa konkrétne neuvádza „počítačové údaje“. Z toho vyplýva odkaz na článok 1 písm. a) Budapeštianskeho dohovoru s rovnakým rozsahom vymedzenia pojmu počítačový systém.

b) Počítačové údaje

Pojem „počítačové údaje“ sa stanovuje v právnych predpisoch AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO a UK (Gibraltár), zatiaľ čo informácie poskytnuté ES, FR, IT, LU, LV, PL, SE, SK a UK (s výnimkou Gibraltáru) neboli presvedčivé. V prípade SE je vymedzenie tohto pojmu zbytočné vzhľadom na konkrétnu formuláciu predmetných článkov. Čo sa týka zvyšných členských štátov, HU uvádza definíciu počítačových údajov iba pre trestné činy opísané v článkoch 4 a 5 smernice, zatiaľ čo v právnych predpisoch BE a SI nie je vo vymedzení pojmu počítačové údaje zahrnutý „program, ktorý zabezpečí, aby informačný systém vykonal funkciu“.

c) Právnická osoba

S výnimkou LU, ktoré poskytlo nepresvedčivé informácie o transpozícii článku 2 písm. c), transpozícia pojmu právnická osoba nespôsobila žiadne problémy. Je to preto, že vo všeobecnosti sa už nachádza v ustanoveniach občianskeho alebo obchodného práva väčšiny členských štátov. Iba CY prijal osobitné ustanovenie v rámci opatrení na transpozíciu smernice.

[7] IE oznámilo úplnú transpozíciu smernice 31. mája 2017.

d) Bez oprávnenia
Transpozíciu vymedzenia pojmu „bez oprávnenia“ v článku 2 písm. d) oznámili iba CY, IE, RO a UK (Gibraltár), pričom 23 členských štátov neprijalo žiadne transpozičné opatrenia, pokiaľ ide o tento pojem. Treba však poznamenať, že vo všetkých členských štátoch platí všeobecný princíp, že trestná zodpovednosť sa nevyvodzuje za akékoľvek činy spáchané s príslušným oprávnením.

2.2 Konkrétne trestné činy (články 3 až 7 smernice)

a) Protiprávny prístup do informačných systémov
Protiprávny prístup do informačného systému, ako je vymedzený v článku 3 smernice, pokrývajú vnútroštátne právne predpisy AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE a SK.

V prípade ostatných členských štátov, teda BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI a UK, príslušný vnútroštátny opis trestného činu nerozlišuje medzi získaním vstupu do celého informačného systému alebo iba do jeho časti, napriek tomu, že v smernici je toto výslovne stanovené. V transpozícii DE nie je pokrytý samotný prístup do počítačového hardvéru, AT a LU prijali doplňujúce ustanovenia týkajúce sa osobitného zámeru (zámer získať vedomosti, spôsobiť nevýhodu alebo podvodný úmysel) a LV prijalo doplňujúce ustanovenie týkajúce sa spôsobenia závažnej ujmy. V prípade BE, BG, FR, HR, LU, MT, PT, RO, SI a UK je rozsah pôsobnosti vnútroštátnych ustanovení širší ako v smernici, keďže tieto ustanovenia pri stanovovaní trestnej zodpovednosti nevyžadujú obídenie žiadnych bezpečnostných opatrení. Zvyšné členské štáty buď doslovne odkazujú na trestný čin spáchaný porušením bezpečnostného opatrenia (CY, EL a SK), alebo používajú podobnú terminológiu na opis tohto aspektu (AT, CZ, DE, EE, ES, FI, HU, IT, LT, LV, NL, PL a SE).

b) Protiprávny zásah do systému
V článku 4 smernice sa hovorí o protiprávnom zásahu do systému. V smernici je vymenovaných 8 možných činov (vloženie počítačových údajov, prenos, poškodenie, vymazanie, zhoršenie, pozmenenie alebo potlačenie takýchto údajov alebo ich zneprístupnenie a 2 možné výsledky týchto činov (závažné bránenie fungovaniu informačného systému alebo prerušenie jeho fungovania). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE a UK (s výnimkou Gibraltáru) prijali zodpovedajúce právne predpisy. BG hovorí iba o vložení vírusu, zatiaľ čo ostatné členské štáty (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK a UK) konkrétne neuvádzajú 1 až 4 možné činy. V tejto súvislosti možno konštatovať, že najviac problémov vzniklo v súvislosti s výrazmi „zhoršenie“ (chýba v 8 prípadoch) a „zneprístupnenie“ (chýba v 9 prípadoch).

c) Protiprávny zásah do údajov
V článku 5 smernice sa vymedzuje protiprávny zásah do údajov a vymenovaných je týchto 6 možných činov: vymazanie, poškodenie, zhoršenie, pozmenenie, potlačenie údajov alebo zneprístupnenie takýchto údajov. CY, EL, IE a MT doslovne transponovali toto ustanovenie; BE, CZ, LT, PT a SE použili všeobecnejšie výrazy s cieľom zahrnúť všetky možné činy. Transpozičné opatrenia ostatných členských štátov sa nevzťahujú na všetky možnosti, ale týkajú sa iba 5 alternatív (FI a SK) alebo menej (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL , RO, SI a UK). Väčšina problémov súvisela s výrazom „poškodenie“ (chýba 8-krát), „zhoršenie“ (13-krát), „potlačenie údajov“ (11-krát) a „zneprístupnenie takýchto údajov“ (13-krát). Nad rámec znenia smernice FI vyžaduje „úmysel spôsobiť škodu alebo finančnú stratu“, aby sa mohla vyvodiť trestná zodpovednosť, zatiaľ čo LT a LV vyžadujú, aby „čin spôsobil veľkú škodu alebo závažnú ujmu“.

d) Protiprávne zachytávanie údajov
V článku 6 sa hovorí o protiprávnom zachytávaní prostredníctvom neverejného prenosu počítačových údajov a elektromagnetického vysielania z informačného systému nesúceho takéto údaje. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK a UK (Gibraltár) zaviedli právne predpisy, ktoré v plnej miere pokrývajú článok 6. Všeobecný rozsah pôsobnosti smernice týkajúci sa zachytávania počítačových údajov sa obmedzuje na správy (AT a BG), pozorovanie osoby (EE) alebo korešpondenciu (FR a HU). Okrem toho sa transpozičné opatrenia týchto členských štátov nevzťahujú na zachytávanie elektromagnetického vysielania: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI a UK (s výnimkou Gibraltáru). Niektoré členské štáty navyše vyžadujú osobitný úmysel (ako napr. získať vedomosti, ekonomický zisk, spôsobiť nevýhodu — pozri AT, EL, HU) alebo konkrétne ďalšie činy (napr. zaznamenávanie alebo oboznámenie sa so zachyteným obsahom – pozri BG a HU).

e) Nástroje na spáchanie trestných činov
V článku 7 sa kriminalizujú niektoré činy, súvisiace s nástrojmi, ako sú počítačové programy alebo prístupové kódy na spáchanie trestných činov uvedených v článkoch 3 až 6: výroba takýchto nástrojov, predaj, obstarávanie na použitie, dovoz, distribúcia alebo akékoľvek sprístupnenie nástrojov. AT, BE, CY, DE, EL, IE a SK zaviedli zodpovedajúce vnútroštátne právne predpisy. Niektoré členské štáty nezahrnuli všetky uvedené trestné činy (EE, IT, MT, PL a SI). Niektoré nerozlišujú páchateľa v zmysle článku 7 od páchateľa trestných činov uvedených v článkoch 3 až 6 (CZ a SI). Niektoré vyžadujú konkrétny úmysel (spôsobiť škodu alebo konať podvodným spôsobom — pozri FI, IT a LU), a konkrétny výsledok, napr. porušenie tajomstva (BG) alebo aspoň úroveň pripravenosti uvedených trestných činov (SE). A napokon, nezrovnalosti medzi článkom 7 a vnútroštátnymi opatreniami je možné nájsť v nedostatočnej transpozícii všetkých uvedených činov. To platí pre BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI a UK. Spomedzi nich právne predpisy LU osobitne uvádzajú päť alebo šesť možných činov uvedených v smernici, zatiaľ čo ostatné členské štáty výslovne uvádzajú iba štyri alebo menej.

Iba ES transponovalo alternatívu obstarania na použitie.

2.3 Všeobecné pravidlá týkajúce sa uvedených trestných činov (články 8 až 12 smernice)

a) Navádzanie, pomoc a podnecovanie
V článku 8 ods. 1 sa vyžaduje, aby členské štáty zabezpečili, aby navádzanie alebo pomoc a podnecovanie na spáchanie trestného činu uvedeného v článkoch 3 až 7 boli sankcionované ako trestný čin. Všetky členské štáty transponovali toto ustanovenie.

b) Pokus
Podľa článku 8 ods. 2 musí byť pokus o spáchanie trestných činov uvedených v článkoch 4 a 5 sankcionovaný ako trestný čin. Zatiaľ čo PT neuvádza všetky typy pokusov o spáchanie trestných činov uvedených v článku 4 a SE chýba trestná zodpovednosť za pokus o spáchanie trestného činu „porušenia komunikačného tajomstva“, všetky ostatné členské štáty zaviedli právne predpisy, ktorými sa toto ustanovenie transponuje.

c) Sankcie
aa) Všeobecné ustanovenia
V článku 9 ods. 1 sa všeobecne vyžaduje, aby členské štáty stanovili účinné, primerané a odrádzajúce trestné sankcie za trestné činy uvedené v smernici. Hoci sa predpokladá, že takmer všetky členské štáty toto vykonali, AT, BE, BG, IT, PT, SE a SI nesplňajú dolné hranice najvyšších sankcií stanovené v článku 9 ods. 2 (pozri časť 1.1 vyššie) vo všetkých prípadoch. Toto ovplyvňuje transpozíciu článku 9 ods. 1, keďže možno konštatovať, že

minimálne požiadavky uvedené v článku 9 ods. 2 sú minimálnymi požiadavkami pre prijatie účinných, primeraných a odrádzajúcich trestných sankcií.

bb) Všeobecná dolná hranica najvyššej sankcie

Podľa článku 9 ods. 2, dolná hranica najvyššej sankcie za štandardné trestné činy uvedené v článkoch 3 až 7 je trest odňatia slobody v dĺžke najmenej 2 roky. Väčšina členských štátov dosahuje súlad s týmto ustanovením. Iba 6 členských štátov vykazuje odlišnosti: AT (horná hranica trestu odňatia slobody 6 mesiacov), BG (horná hranica trestu odňatia slobody 1 rok za všetky trestné činy okrem neoprávneného zachytávania), IT [horná hranica trestu odňatia slobody 1 rok za trestný čin uvedený v článku 7 písm. b)], PT (horná hranica trestu odňatia slobody 1 rok za trestný čin uvedený v článku 3), SE (horná hranica trestu odňatia slobody 1 rok za trestný čin „spôsobenia škody“ a SI (horná hranica trestu odňatia slobody 1 rok za trestné činy uvedené v článkoch 3, 6 a 7): V prípade BE sa dolná hranica najvyššej sankcie za trestné činy uvedené v článkoch 3, 6 a 7 uplatňuje iba pri trestných činoch spáchaných s podvodným úmyslom.

cc) Postihnutie veľkého množstva informačných systémov

V článku 9 ods. 3 sa dolná hranica hornej sadzby trestu odňatia slobody zvyšuje na tri roky ak bolo postihnuté veľké množstvo informačných systémov trestnými činmi uvedenými v článkoch 4 a 5. Vo všeobecnosti členské štáty zaviedli zodpovedajúce právne predpisy, DE zahrnulo iba informačné systémy, „ktoré majú závažný význam pre iné“, FI požaduje posúdenie trestného činu „ako celku“ pre uplatnenie vyššej sadzby trestu a LV neodkazuje na veľké množstvo informačných systémov (alebo podobného znenia), ale iba na spôsobenie „závažnej ujmy“. Informácie, ktoré poskytli BG a SI, neboli presvedčivé.

dd) Zločinecké organizácie

Podľa článku 9 ods. 4 písm. a) sa dolná hranica najvyššej sadzby trestu odňatia slobody stanovená na 5 rokov uplatňuje za trestné činy uvedené v článkoch 4 a 5, keď boli spáchané zločineckou organizáciou, ako je vymedzená v rámcovom rozhodnutí Rady 2008/841/SVV. Väčšina členských štátov dosahuje súlad s ustanovením článku 9 ods. 4 písm. a). V súlade s trestným právom LU a SI, ustanovenia týkajúce sa trestných činov spáchaných zločineckou organizáciou sa nevzťahujú na počítačovú kriminalitu. Právne predpisy BE stanovujú hornú sadzbu trestu odňatia slobody na 3 roky za trestné činy uvedené v článku 5, podľa právnych predpisov DE sa za obete týchto trestných činov nepovažujú fyzické osoby, právne predpisy FI vyžaduje dodatočné posúdenie trestného činu „ako celku“ a právne predpisy SE stanovujú najvyššiu sadzbu trestu odňatia slobody na 4 roky za „hrubé poškodenie“.

ee) Spôsobenie závažnej škody

V článku 9 ods. 4 písm. b) sa stanovuje 5 rokov ako dolná hranica najvyššej sadzby trestu odňatia slobody za trestné činy uvedené v článkoch 4 a 5, ak bola spôsobená závažná škoda. Hoci sa nevymedzuje, čo by sa malo považovať za závažnú škodu, všetky členské štáty okrem BG, DE, FI, HU, LU a SE prijali právne predpisy zodpovedajúce smernici. Informácie, ktoré poskytlo HU, neboli presvedčivé. V prípade BG dolná hranica najvyššej sadzby trestu nedosahuje 5 rokov, zatiaľ čo LU uvádza všeobecné ustanovenie týkajúce sa sankcií za spôsobenie závažnej škody, ktoré sa nevzťahuje na počítačovú kriminalitu. Menšie nezrovnalosti sa vyskytujú pri DE (nezahrnutie fyzických osôb ako obetí trestných činov), FI (vyššia sankcia vyžaduje doplňujúce posúdenie trestného činu ako celku) a SE (horná hranica trestu odňatia slobody za „hrubé poškodenie“).

ff) Informačné systémy kritickej infraštruktúry

Pri trestných činoch uvedených v článkoch 4 a 5 spáchaných na informačnom systéme kritickej infraštruktúry sa takisto uplatňuje dolná hranica najmenej 5 rokov v rámci najvyššej sadzby trestu odňatia slobody, ako je uvedené v článku 9 ods. 4.
Väčšina členských štátov dosiahla súlad s týmto ustanovením, pričom BG neposkytlo konkrétne informácie o transpozícii. BE stanovilo najvyššiu sadzbu trestu za trestné činy uvedené v článku 5 na 3 roky. DE neuvádza fyzické osoby ako obete. FI vyžaduje doplňujúce posúdenie trestných činov „ako celku“, IT vyžaduje skutočné spôsobenie „zničenia“, PT vyžaduje útok „ťažkým a trvalým spôsobom“, a nevzťahuje sa na článok 5 a SE spĺňa požiadavky smernice iba pri trestných činoch „hrubej sabotáže“.

gg) Krádež identity a iné trestné činy súvisiace s identitou

V článku 9 ods. 5 sa vyžaduje, aby členské štáty zabezpečili, aby sa prípad, keď je akýkoľvek trestný čin uvedený v článkoch 4 a 5 spáchaný prostredníctvom zneužitia osobných údajov inej osoby s cieľom získať dôveru tretej strany a tým spôsobiť škodu právoplatnému nositeľovi identity, mohol považovať za priťažujúce okolnosti, pokiaľ tieto okolnosti už nepatria pod iný trestný čin. Veľká miera voľnosti viedla k širokému rozsahu transpozičných opatrení členských štátov. BE a EL neoznámili žiadnu transpozíciu a trestnoprávne predpisy CZ neobsahujú konkrétne ustanovenie. AT, CY, ES, IE, MT, PT a SE sa rozhodli uplatňovať priťažujúce okolnosti, pričom posledný z menovaných odkazuje na okolnosť „osobitného plánovania“), zatiaľ čo všetky ostatné členské štáty odkazujú na zvláštne ustanovenia týkajúce sa konkrétneho trestného činu. Pri členských štátoch, ktoré odkazujú na osobitné ustanovenia, možno otázky transpozície zhrnúť takto: BG a NL vyžadujú osobitný úmysel („získať výhodu“ a „s cieľom zamaskovať alebo zneužiť identitu“), DE uvádza iba „osobné údaje, ktoré nie sú bežne prístupné“, FR uvádza iba meno osoby a žiadne iné osobné údaje, LV vyžaduje spôsobenie „závažnej ujmy“, RO pokrýva iba použitie „dokumentu“ a vyžaduje spáchanie podvodu.

d) Zodpovednosť právnických osôb

aa) Všeobecne

V článku 10 ods. 1 sa vyžaduje, aby sa určila zodpovednosť právnických osôb za trestné činy zahrnuté v článkoch 3 až 8, ak má páchateľ právomoci zastupovať právnickú osobu a), oprávnenie prijímať rozhodnutia v mene právnickej osoby b) alebo oprávnenie vykonávať kontrolu v rámci právnickej osoby c). Všetky členské štáty prijali právne predpisy zodpovedajúce tomuto článku, iba s týmito drobnými nedostatkami: BG nezahrnulo trestný čin podľa článku 6 a HR neuviedlo páchateľa s právomocou vykonávať kontrolu v rámci tejto právnickej osoby [článok 10 ods. 1 písm. c)].

bb) V dôsledku nedostatočného dozoru alebo kontroly

V článku 10 ods. 2 sa vyžaduje, aby členské štáty zaviedli zodpovednosť právnických osôb, ak nedostatočný dozor alebo kontrola vykonávaná osobou uvedenou v odseku 1 umožnili spáchanie niektorého z trestných činov uvedených v článkoch 3 až 8 (článok 10 ods. 1). Zatiaľ čo takmer všetky členské štáty dosahujú súlad s týmto ustanovením, informácie poskytnuté LU nie sú presvedčivé a BG neuvádza spáchanie trestného činu, ktorý spadá pod článok 6.

e) Sankcie voči právnickým osobám

aa) Povinné sankcie

V článku 11 ods. 1 smernice sa vyžaduje, aby členské štáty zabezpečili účinné, primerané a odrádzajúce sankcie, ktoré zahŕňajú trestnoprávne alebo iné ako trestnoprávne pokuty pre právnické osoby. Všetky členské štáty okrem IE a UK oznámili zosúladenie vnútroštátnych opatrení. V týchto dvoch krajinách nie je určená horná sadzba možných pokút v súvislosti

s nedostatkom konkrétnych právnych ustanovení. Z tohto dôvodu nie je možné posúdiť, či sú príslušné pokuty účinné, primerané a odrádzajúce.

bb) Nepovinné sankcie

V článku 11 ods. 1 je uvedený zoznam možných ďalších sankcií pre právnické osoby. Takýmito sú: vylúčenie z nároku na štátne dávky alebo pomoc (ES, HR, HU, LU, MT, PL, PT a SK), dočasný alebo trvalý zákaz výkonu obchodnej činnosti (AT, BE, CY, CZ, EL, ES FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI a SK), nariadenie súdneho dohľadu (CY, ES, FR, MT, PT and RO), súdne rozhodnutie o zrušení (CY, CZ, EL, ES, FR, HR, HU,LT, LU, LV, MT, PT, RO, SI a SK) a dočasné alebo trvalé zatvorenie prevádzok, ktoré sa použili na spáchanie trestného činu (BE, CY, WS, FR, LT, MT, PT and RO). BG, DE, EE, IE, FI, NL a UK si nevybrali žiadnu z možností.

cc) Sankcie za opomenutie

Podľa článku 11 ods. 2 členské štáty musia zabezpečiť, aby sa na právnické osoby, ktoré sú zodpovedné za omisívne trestné činy, uvedené v článku 10 ods. 2, uplatňovali účinné, primerané a odrádzajúce sankcie. Informácie, ktoré poskytlo LU, neboli presvedčivé. Ostatné členské štáty, s výnimkou IE a UK, zaviedli zodpovedajúce právne predpisy. V prípade IE a UK rovnaký problém nastal aj pri článku 11 ods. 1: [pozri bod aa) vyššie].

f) Súdna právomoc

aa) Požadované kritéria právomoci

V článku 12 ods. 2 a 3 smernice sa vyžaduje, aby členské štáty stanovili svoju súdnu právomoc pre trestné činy uvedené v článkoch 3 až 8, ak boli trestné činy spáchané úplne alebo čiastočne na ich území, ak tam bol páchateľ fyzicky prítomný v čase spáchania trestného činu alebo ak bol trestný čin spáchaný na informačnom systéme na území daného členského štátu alebo ak bol trestný čin spáchaný v zahraničí príslušníkom daného členského štátu. Väčšina členských štátov prijala zodpovedajúce vnútroštátne právne predpisy, právne predpisy IT nestanovujú súdnu právomoc pre ich príslušníkov v zahraničí pre prípady základných trestných činov, právne predpisy LV a ST uvádzajú nejasné ustanovenia ohľadom územných aspektov, súdna právomoc podľa právnych predpisov MT za činy spáchané čiastočne na ich území je nejasná a predpisy UK sa vzťahujú na počítačový a nie na informačný systém.

bb) Ďalšie kritériá právomoci

V článku 12 ods. 3 sa vyžaduje, aby členský štát informoval Komisiu, ak sa rozhodne rozšíriť súdnu právomoc aj na trestný čin spáchaný v mieste obvyklého pobytu páchateľa (AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE a SK) alebo bol trestný čin spáchaný v prospech právnickej osoby so sídlom na jeho území (CY, CZ, LV, PT, RO a SK).

2.2 Funkčné otázky (články 13 a 14 smernice)

a) Ustanovenie týkajúce sa funkčného vnútroštátneho kontaktného miesta

V článku 13 ods. 1 sa vyzývajú členské štáty, aby zriadili funkčné vnútroštátne kontaktné miesta na účely výmeny informácií, ktoré sa týkajú trestných činov uvedených v článkoch 3 až 8. Na základe tohto ustanovenia je potrebné, aby členské štáty zabezpečili, aby mali k dispozícii postupy, ktorými v prípade naliehavých žiadostí o pomoc príslušné orgány mohli do 8 hodín odpovedať. Podľa poskytnutých informácií väčšina členských štátov požadovanú infraštruktúru zriadila. IE a RO oznámili, že príslušné kontaktné miesta sú k dispozícii obmedzený počet hodín denne, čo by neumožnilo orgánom odpovedať do 8 hodín na žiadosť v každom jednom prípade. Niektoré členské štáty uviedli, že používajú existujúcu sieť

funkčných kontaktných miest G7, zriadenú v súlade s Budapeštianskym dohovorom Rady Európy o počítačovej kriminalite.

b) Informácie o zriadených funkčných vnútroštátnych kontaktných miestach
V súlade s článkom 13 ods. 2 členské štáty sú povinné oznámiť kontaktné údaje svojich kontaktných miest Komisii, ktorá tieto informácie podá ostatným členským štátom. Všetky členské štáty poskytli potrebné informácie.

c) Oznamovacie kanály
Podľa článku 13 ods. 3 sú členské štáty povinné sprístupniť primerané oznamovacie kanály s cieľom uľahčiť bezodkladné ohlasovanie trestných činov uvedených v článkoch 3 až 6 príslušným vnútroštátnym orgánom. Informácie, ktoré poskytli HR, IT, IE a PT neboli presvedčivé. Zvyšné členské štáty zvolili rôzne spôsoby realizácie oznamovacích kanálov. Väčšina členských štátov (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK a UK) oznámila opatrenia na zabezpečenie kanálov, ktoré majú za cieľ zjednodušiť oznamovanie pre osobu alebo organizáciu, ktorá ako prvá hlási trestný čin, napr. pre obeť počítačového útoku (pričom informácie o samotných oznamovacích kanáloch LV sú nepresvedčivé). Avšak ostatné členské štáty (AT, ES a LU) poskytli rovnaké informácie o vykonávaní článku 13 ods. 1 a ods. 2, čo vedie k záveru, že ich opatrenia uľahčia komunikáciu najmä medzi orgánmi.

d) Zber štatistických údajov
Podľa článku 14 ods. 1 a 2 musia členské štáty zabezpečiť, aby bol zavedený systém na zaznamenávanie, vytváranie a poskytovanie štatistických údajov, minimálne o počte trestných činov uvedených v článkoch 3 až 7, ktoré boli zaevidované členskými štátmi, a počte osôb, ktoré sú stíhané a odsúdené za tieto trestné činy. Na základe poskytnutých oznámení sa zdá, že väčšina členských štátov uskutočnila právne aj správne opatrenia s cieľom zabezpečiť zber informácií, a to zvyčajne formou všeobecného vnútroštátneho elektronického systému. Viaceré členské štáty poskytli nepresvedčivé informácie [EL, IE, UK (Gibraltár, Severné Írsko a Škótsko)]. Jedným z dôvodov je, že informácie o konkrétnych trestných činoch uvedených v smernici nie je možné zbierať osobitne (BE, DE a SE) alebo zhromaždené informácie sa netýkajú všetkých trestných činov uvedených v smernici (RO).

e) Zasielanie štatistických údajov Komisii
V článku 14 ods. 3 sa vyzývajú členské štáty, aby zasielali príslušné štatistické údaje Komisii. Všetky členské štáty, ktoré poskytli informácie o opatreniach, okrem UK (Gibraltár, Severné Írsko a Škótsko) a HU, potvrdili prijatie právnych alebo správnych opatrení alebo oboch druhov opatrení, aby zabezpečili splnenie tejto povinnosti. V prípade EL, ES, LU a SI neboli poskytnuté informácie presvedčivé.

3. Záver a ďalšie kroky

Smernica viedla k podstatnému pokroku v oblasti kriminalizácie počítačových útokov na porovnateľnej úrovni v členských štátoch, čo uľahčuje cezhraničnú spoluprácu orgánov presadzovania práva, ktoré vyšetrujú tento typ trestných činov. Členské štáty zmenili trestné zákony a iné relevantné právne predpisy, zosúladili postupy a zriadili alebo zlepšili systémy spolupráce. Komisia oceňuje veľké úsilie členských štátov o transpozíciu smernice.

Stále však existuje značný priestor na využitie plného potenciálu smernice, ak by členské štáty v plnej miere vykonávali všetky jej ustanovenia. Z doterajšej analýzy vyplýva, že niektoré z hlavných zlepšení, ktoré môžu členské štáty dosiahnuť, zahŕňajú použitie vymedzených pojmov (článok 2), ktoré má vplyv na rozsah trestných činov vymedzených

vnútroštátnymi právnymi predpismi na základe smernice. Okrem toho sa zdá, že pre členské štáty bolo náročné zahrnúť všetky možnosti, ktoré vymedzujú skutky v súvislosti s trestnými činmi (články 3 až 7) a zaviesť spoločné štandardy pre sankcie za počítačové útoky (článok 9). Ďalšie problémy sa týkajú vykonávania správnych opatrení týkajúcich sa vhodných oznamovacích kanálov (článok 13 ods. 3) a monitorovania a štatistiky trestných činov uvedených v smernici (článok 14).

Komisia bude naďalej poskytovať podporu členským štátom pri vykonávaní smernice. Z hľadiska potenciálneho prínosu k cezhraničnej spolupráci ide najmä o funkčné ustanovenia smernice o výmene informácií (článok 13 ods. 1 a ods. 2), oznamovacie kanály (článok 13 ods. 3) a monitorovanie a štatistiku (článok 14). V tejto súvislosti Komisia poskytne členským štátom ďalšie príležitosti identifikovať a vymeniť si najlepšie postupy v druhej polovici roku 2017.

Komisia v súčasnosti nevidí potrebu navrhnúť zmeny smernice. V tejto súvislosti, a to aj v záujme podpory trestného vyšetrovania útokov na informačné systémy, trestných činov páchaných prostriedkami digitálnej povahy a iných druhov trestnej činnosti, zvažuje Komisia opatrenia na zlepšenie cezhraničného prístupu k elektronickým dôkazom pri vyšetrovaní trestných činov vrátane navrhnutia legislatívnych opatrení do začiatku roka 2018[8] Komisia tiež zvažuje úlohu šifrovania v trestnom vyšetrovaní a do októbra 2017 podá správu o svojich zisteniach.[9]

Komisia sa zameria na zabezpečenie toho, aby bola transpozícia dokončená v celej EÚ a aby boli ustanovenia vykonané správne. To zahŕňa monitorovanie toho, či sú vnútroštátne opatrenia v súlade so zodpovedajúcimi ustanoveniami smernice. Komisia v prípade potreby využije svoju právomoc presadzovania podľa zmlúv prostredníctvom postupov v prípade nesplnenia povinnosti.

[8] Úvodné posúdenie vplyvu zlepšenia cezhraničného prístupu k elektronickým dôkazom zo 4. augusta 2017 je dostupné na ec.europa.eu.

[9] Oznámenie o ôsmej správe o pokroku na ceste k účinnej a skutočnej bezpečnostnej únii, COM(2017) 354 final.