Rada
Európskej únie

V Bruseli 9. októbra 2017
(OR. en)

12711/1/17
REV 1

GENVAL 79
CYBER 136
CATS 98
JAI 855

POZNÁMKA K BODU I/A

Od:	Generálny sekretariát Rady
Komu:	Výbor stálych predstaviteľov/Rada
Č. predch. dok.:	9986/2/17 REV 2
Predmet:	Záverečná správa o 7. kole vzájomných hodnotení s názvom „Praktické vykonávanie a uplatňovanie európskych politík v oblasti predchádzania počítačovej kriminalite a boja proti nej – informácia pre Radu

Pracovná skupina pre všeobecné záležitosti vrátane hodnotenia (GENVAL) rozhodla 3. októbra 2013 v súlade s článkom 2 jednotnej akcie 97/827/SVV z 5. decembra 1997[1], že siedme kolo vzájomných hodnotení sa bude týkať praktického vykonávania a uplatňovania európskych politík v oblasti predchádzania počítačovej kriminalite a boja proti nej.

[1] Jednotná akcia 97/827/SVV z decembra 1997 prijatá Radou na základe článku K.3 Zmluvy o Európskej únii, ktorou sa stanovuje mechanizmus na hodnotenie uplatňovania a vykonávania medzinárodných záväzkov v boji proti organizovanému zločinu na národnej úrovni (Ú. v. ES L 344, 15.12.1997).

Návrh záverečnej správy uvedený v dokumente 9986/17, ktorý vypracoval Generálny sekretariát Rady a ktorý obsahuje zhrnuté závery a odporúčania uvedené v skôr prijatých správach pre jednotlivé členské štáty, sa predložil na zasadnutí pracovnej skupiny GENVAL 13. júna 2017 na predbežnú výmenu názorov.

Delegácie sa vyzvali, aby do 3. júla 2017 predložili písomné pripomienky k návrhu záverečnej správy.
Revidovaná verzia správy uvedená v dokumente 9986/1/17 REV 1 sa predložila horizontálnej pracovnej skupine pre kybernetické otázky na jej zasadnutí 4. septembra 2017.

Na základe pripomienok jednej delegácie sa návrh správy mierne upravil tak, ako sa uvádza v prílohe k dokumentu 9986/2/17 REV 2, pričom výbor CATS ho schválil na zasadnutí 22. septembra 2017.

COREPER rozhodol 4. októbra 2017, že predloží záverečnú správu o siedmom kole vzájomného hodnotenia uvedenú v prílohe k dokumentu 12711/17 na informačné účely Rade, aby vzala na vedomie výsledky tohto hodnotenia. V konečnej verzii správy uvedenej v prílohe sa vykonalo zopár redakčných zásahov.

V súlade s článkom 8 ods. 4 uvedenej jednotnej akcie sa záverečná správa pošle na informačné účely aj Európskemu parlamentu.

PRÍLOHA

Záverečná správa o siedmom kole vzájomných hodnotení s názvom „Praktické vykonávanie a uplatňovanie európskych politík v oblasti predchádzania počítačovej kriminalite a boja proti nej“

OBSAH

I. ÚVOD

V nadväznosti na prijatie jednotnej akcie 97/827/SVV z 5. decembra 1997, ktorou sa stanovuje mechanizmus na hodnotenie uplatňovania a vykonávania medzinárodných záväzkov v boji proti organizovanému zločinu na národnej úrovni, je cieľom tejto správy zhrnúť zistenia a odporúčania a vyvodiť závery, pokiaľ ide o siedme kolo vzájomného hodnotenia.

Pracovná skupina pre všeobecné záležitosti vrátane hodnotenia (GENVAL) rozhodla 3. októbra 2013 v súlade s článkom 2 uvedenej jednotnej akcie, že siedme kolo vzájomných hodnotení sa bude týkať praktického vykonávania a uplatňovania európskych politík v oblasti predchádzania počítačovej kriminalite a boja proti nej.

Členské štáty výber počítačovej kriminality za predmet siedmeho kola vzájomného hodnotenia uvítali. Vzhľadom na širokú škálu trestných činov, na ktorú sa pojem počítačovej kriminality vzťahuje, sa však dohodlo, že hodnotenie sa zameria na tie trestné činy, ktoré si podľa členských štátov vyžadujú osobitnú pozornosť. Preto sa hodnotenie týkalo týchto oblastí: počítačové útoky, online sexuálne zneužívanie detí/detská pornografia a online podvody s bankovými/kreditnými kartami, pričom ponúklo komplexné preskúmanie právnych a operačných aspektov boja proti počítačovej kriminalite, cezhraničnej spolupráce a spolupráce s príslušnými agentúrami EÚ. V tomto kontexte je obzvlášť dôležitá smernica 2011/92/EÚ o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii[2] (dátum transpozície: 18. decembra 2013) a smernica 2013/40/EÚ[3] o útokoch na informačné systémy (dátum transpozície: 4. septembra 2015).

[2] Ú. v. EÚ L 335, 17.12.2011, s. 1.
[3] Ú. v. EÚ L 218, 14.8.2013, s. 8.

Pracovná skupina GENVAL rokovala o dotazníku pre siedme kolo vzájomných hodnotení 27. novembra 2013 a 22. januára 2014 a následne ho prijala zjednodušeným písomným postupom 31. januára 2014. Poradie návštev s výhradou určitých úprav a zloženie hodnotiacich tímov vo vzťahu k pozorovateľom schválila pracovná skupina GENVAL 1. apríla 2014.

V súlade s článkom 3 jednotnej akcie 97/827/SVV a na základe písomnej žiadosti vedúceho odboru DGD 2B Generálneho sekretariátu Rady z 28. januára 2014 určenej delegáciám nominovali členské štáty expertov s významnými praktickými znalosťami v danej oblasti. Pri každej návšteve sa na hodnotení zúčastnili traja národní experti. Na niektorých hodnotiacich návštevách sa ako pozorovatelia zúčastnili ďalší experti z Komisie, Eurojustu, Europolu a z agentúry ENISA. Generálny sekretariát Rady tieto návštevy koordinoval a zúčastňoval sa na nich prostredníctvom jedného alebo dvoch zamestnancov na každom hodnotení, pripravil príslušné postupy a pomáhal expertom.

Prvá hodnotiaca návšteva sa konala vo Francúzsku od 28. do 31. októbra 2014. Posledná hodnotiaca návšteva sa uskutočnila vo Švédsku od 27. do 30. septembra 2016. Všetkých 28 hodnotiacich návštev viedlo k podrobným správam o jednotlivých členských štátoch. O týchto hodnotiacich správach sa následne rokovalo v pracovnej skupine GENVAL, ktorá ich prijala[4]. Väčšina z nich je dostupná na webovej stránke Rady a sú verejne prístupné.

[4] Francúzsko (7588/2/15 REV 1 DCL 1); Holandsko (7587/15 DCL 1); Spojené kráľovstvo (10952/2/15 REV 2 DCL 1); Rumunsko (13022/1/15 REV 1 DCL 1); Slovensko (9761/1/15 REV 1 DCL 1); Estónsko (10953/15 DCL 1); Slovinsko (14586/1/16 REV 1 DCL 1); Taliansko (9955/1/16 REV 1 DCL 1); Španielsko (6289/1/16 REV 1 DCL 1); Bulharsko (5156/1/16 REV 1 DCL 1); Litva (6520/1/16 REV 1 DCL 1); Malta (7696/1/16 REV 1 DCL 1); Grécko (14584/1/16 REV 1 DCL 1); Chorvátsko (5250/1/17 REV 1 DCL 1); Portugalsko (10905/1/16 REV 1 DCL 1); Cyprus (9892/1/16 REV 1 DCL 1); Poľsko (14585/1/16 REV 1 DCL 1); Česká republika (13203/1/16 REV 1 DCL 1); Maďarsko (14583/1/16 REV 1 DCL 1); Lotyšsko (5387/1/17 REV 1 DCL 1); Dánsko (13204/1/16 REV 1 DCL 1 + COR 1); Belgicko (8212/1/17 REV 1); Rakúsko (8185/1/17 REV 1); Nemecko (7159/1/17 REV 1 DCL 1); Luxembursko (7162/1/17 REV 1 DCL 1); Írsko (7160/1/17 REV 1 DCL 1); Fínsko (8178/17); Švédsko (8188/17 REV 1).

V tomto dokumente sa odzrkadľujú závery a odporúčania uvedené v skôr vypracovaných osobitných správach pre jednotlivé členské štáty[5]. Je však potrebné poznamenať, že vzhľadom na dlhodobú povahu hodnotenia nemusia správy týkajúce sa jednotlivých krajín úplne odrážať aktuálny stav.

[5] Správy o jednotlivých krajinách sa vypracovali bezprostredne po návštevách v členských štátoch. Následne mohlo dôjsť k zmenám, ktoré sa v správach o jednotlivých krajinách neodrážajú, napr. k dokončeniu vykonávania právnych predpisov. Tieto zmeny by sa mali zachytiť v správach nadväzujúcich na hodnotiace správy, ktoré sa vypracúvajú 18 mesiacov po prijatí hodnotiacich správ. V čase rokovaní o tejto správe v pracovnej skupine GENVAL členské štáty často oznamovali (budúce) zmeny, prostredníctvom ktorých mali v úmysle plniť odporúčania uvedené vo svojej individuálnej správe.

II – ZHRNUTIE

- V dôsledku častejšieho využívania internetu sa počítačová kriminalita rozširuje a vznikajú nové trendy a *mody operandi* trestnej činnosti; ide o počítačovú kriminalitu *stricto sensu*, ktorá je z právneho hľadiska definovaná ako trestné činy, ktoré si vyžadujú použitie počítačového systému, ako aj o trestné činy umožnené informačnými technológiami, ktoré sú tradičnými trestnými činmi spáchanými s použitím informačných a komunikačných technológií (IKT). Pokrok v boji proti počítačovej kriminalite si preto vo všetkých krajinách vyžaduje vysoký stupeň politickej vôle, rozpočtové úsilie a veľké investície do ľudských a technických zdrojov.

- Z hodnotenia vyplynulo, že všetky členské štáty berú boj proti počítačovej kriminalite vážne a na tento účel zriadili štruktúry, vyhradili zdroje a prijali opatrenia. Miera odhodlania a efektívnosti v jednotlivých členských štátoch sa však líši a v niektorých prípadoch existuje priestor na zlepšenie v súvislosti s niektorými aspektmi celkového prístupu k boju proti počítačovej kriminalite. Zároveň sa identifikovali aj niektoré spoločné problémy a výzvy.

- V čase hodnotenia už väčšina členských štátov prijala národnú stratégiu kybernetickej bezpečnosti, ktorá poskytuje rámec na stanovenie vnútroštátnych priorít, ako aj kľúčové koordinačné štruktúry na strategickej a operačnej úrovni s cieľom bojovať proti počítačovej kriminalite a zabezpečiť kybernetickú odolnosť, pričom niektoré členské štáty takúto stratégiu práve prijímali. Niektoré členské štáty prijali na vykonávanie svojej národnej stratégie kybernetickej bezpečnosti akčný plán.

- V čase hodnotenia už väčšina členských štátov podpísala a ratifikovala Budapeštiansky dohovor Rady Európy o počítačovej kriminalite z roku 2001 a väčšina z nich aj jeho dodatkový protokol týkajúci sa kriminalizácie skutkov rasistického a xenofóbneho pôvodu páchaných prostredníctvom počítačových systémov. Členské štáty, ktoré tak ešte neurobili, sa nabádajú, aby tieto nástroje podpísali a ratifikovali.

- Jeden z hlavných zistených nedostatkov sa týka zhromažďovania samostatných štatistických údajov o počítačovej kriminalite a počítačovej bezpečnosti, pretože tie, ktoré sú k dispozícii, nie sú dostatočné, sú roztrieštené a neumožňujú porovnanie medzi jednotlivými regiónmi v rámci jedného členského štátu a medzi rôznymi členskými štátmi. Spoľahlivé štatistiky sú potrebné na to, aby sa zabezpečil prehľad o počítačovej kriminalite a monitorovanie a analyzovanie trendov a vývoja v tejto oblasti, a to s cieľom prijímať primerané opatrenia a posudzovať účinnosť právnych systémov v boji proti tejto forme trestnej činnosti. Členským štátom sa preto odporúča, aby zbierali konkrétne a vyčerpávajúce štatistické údaje v oblasti počítačovej kriminality v jednotlivých fázach konania na základe štandardizovaného prístupu.

- Vzhľadom na rýchly rozvoj IKT s čoraz rafinovanejšími metódami, ako aj zložitosť počítačovej kriminality je mimoriadne dôležitý vysoký stupeň špecializácie odborníkov pracujúcich v tejto oblasti. Podľa zistení predmetného hodnotenia je úroveň špecializácie vo všeobecnosti dostatočná alebo uspokojivá, pokiaľ ide o orgány presadzovania práva, ale priestor na zlepšenie existuje v justičnom sektore, keďže v niekoľkých členských štátoch sa počítačovou kriminalitou zaoberajú všeobecné prokuratúry a všeobecné trestné súdy. Členským štátom sa preto odporúča, aby zvýšili úroveň špecializácie justičného personálu, ktorý sa zaoberá prípadmi počítačovej kriminality.

- Z rovnakých dôvodov sa v hodnotení zdôraznil význam poskytovania pravidelnej a nepretržitej špecializovanej odbornej prípravy v oblasti počítačovej kriminality pre orgány presadzovania práva aj pre justíciu vrátane čo najlepšieho využívania možností odbornej prípravy, ktoré v súlade so svojimi mandátmi poskytujú orgány EÚ, ako sú napríklad EC3/Europol, ECTEG, Eurojust, OLAF, CEPOL, alebo ku ktorým tieto orgány prispievajú.

- V hodnotení sa zdôraznilo, že úzka a efektívna medziinštitucionálna koordinácia a spolupráca založená na prístupe pozostávajúcom z práce viacerých agentúr na strategickej a operačnej úrovni medzi všetkými príslušnými verejnými a súkromnými zainteresovanými stranami zapojenými do boja proti počítačovej kriminalite a zaisťovania kybernetickej bezpečnosti je kľúčovým prvkom v záujme účinného boja proti počítačovej kriminalite a zabezpečenia dobrej úrovne odolnosti národných systémov kybernetickej bezpečnosti proti počítačovým hrozbám. V niektorých členských štátoch sa však takáto spolupráca ešte dostatočne nerozvinula alebo sa môže ďalej zlepšovať.

- Na tento účel sa členské štáty taktiež vyzvali, aby zvážili možnosť zriadenia ústredného orgánu/subjektu, ktorý by zastupoval verejný aj súkromný sektor a koordinoval činnosti v tejto oblasti.

- V tejto súvislosti má kľúčový význam úzka spolupráca medzi verejným a súkromným sektorom – finančnými/bankovými inštitúciami, telekomunikačnými spoločnosťami, poskytovateľmi internetových služieb, mimovládnymi organizáciami, akademickou obcou, podnikmi, profesijnými združeniami atď. –, keďže ich odborné znalosti predstavujú veľkú pridanú hodnotu pre úspech vyšetrovaní počítačovej kriminality a pre úspech opatrení, ktorými sa reaguje na kybernetické incidenty. Najrozvinutejšie formy spolupráce so súkromným sektorom sú inštitucionalizované zriadením vhodných orgánov/pracovných skupín. Za dôležitý nástroj pre dobrú spoluprácu medzi orgánmi presadzovania práva a súkromným sektorom označili hodnotitelia verejno-súkromné partnerstvá.

- Niektoré členské štáty majú priamy kontakt s poskytovateľmi internetových služieb v zahraničí, a to najmä v USA, ale osud žiadostí nie je vzhľadom na dobrovoľnosť spolupráce úplne jasný; pre EÚ a jej členské štáty by teda bolo prospešné, aby vymedzili jasné pravidlá určujúce, ako môžu orgány presadzovania práva získať údaje, ktoré sú v držbe zahraničných poskytovateľov internetových služieb.

- V niektorých členských štátoch umožňujú vnútroštátne právne predpisy získať základné informácie o zákazníkoch priamo od zahraničných poskytovateľov služieb, zatiaľ čo v iných členských štátoch je potrebné uplatňovať postupy vzájomnej právnej pomoci, ktorá by mala byť rýchlejšia a účinnejšia. Členské štáty sa vyzvali, aby zabezpečili, že ich vnútroštátne právne predpisy budú dostatočne pružné na to, aby uľahčovali prípustnosť elektronických dôkazov vrátane elektronických dôkazov získaných z inej krajiny alebo priamo od poskytovateľov služieb.

- Čoraz väčšou výzvou pre orgány presadzovania práva a spravodajské služby vo všetkých členských štátoch je rastúce využívanie šifrovania s čoraz dokonalejšími metódami, pretože sťažuje alebo úplne znemožňuje získať prístup k relevantným informáciám o počítačovej kriminalite. Ak je dešifrovanie vôbec možné, je to prostredníctvom vysokokapacitného špecializovaného hardvéru a softvéru, pričom hodnotenie ukázalo, že pri riešení bezchybného šifrovania sa dosahujú len čiastočné úspechy. Mnohé členské štáty využívajú dešifrovaciu platformu Európskeho centra boja proti počítačovej kriminalite v rámci Europolu (EC3). Podľa zistení z hodnotenia by výzvy, ktoré predstavuje šifrovanie, mohlo čiastočne zneutralizovať zintenzívnenie výskumu a vývoja a rozvoj nových metód, ako aj dobrá spolupráca medzi rôznymi zainteresovanými orgánmi. Členským štátom a inštitúciám EÚ sa takisto odporučilo, aby zvážili spoločné riešenia so súkromným sektorom a aby s ním posilnili otvorený dialóg.

- Z povahy elektronických dôkazov môžu vyplývať problémy, pokiaľ ide o ich prípustnosť, ktoré nevznikajú pri iných druhoch dôkazov; Preto sa v niektorých členských štátoch uplatňujú osobitné požiadavky na zhromažďovanie elektronických dôkazov, aby sa zabezpečila ich prípustnosť na súde. Z hodnotenia však vyplynulo, že vo väčšine členských štátov je procesné právo prevažne technologicky neutrálne, čo znamená, že sa uplatňujú všeobecné pravidlá a zásady zhromažďovania dôkazov a že procesný systém neobsahuje žiadne osobitné formálne pravidlá prípustnosti a hodnotenia elektronických dôkazov.

- V hodnotení sa zdôrazňuje, že počítačová kriminalita, ktorej súčasťou sú údaje uložené v „cloude“, všeobecne predstavuje problémy z hľadiska vyšetrovania a stíhania, pretože orgány presadzovania práva nemôžu informácie v „cloude“ ľahko lokalizovať a pristupovať ku nim. V závislosti od konkrétneho prípadu sa na elektronické dôkazy môže vzťahovať právomoc jedného alebo viacerých členských štátov, a niekedy súčasne aj právomoc tretích štátov. Môže preto dochádzať k sporom o právomoc; v takýchto prípadoch možno žiadať o pomoc Eurojust a EJS. V hodnotení sa zdôrazňuje význam riešenia tohto problému na úrovni EÚ a medzinárodnej úrovni.

- Hodnotenie potvrdilo obavy členských štátov v súvislosti s absenciou spoločného právneho rámca pre uchovávanie údajov na úrovni EÚ. Táto skutočnosť má vplyv na účinnosť vyšetrovania trestných činov a stíhania ich páchateľov, najmä pokiaľ ide o zhromažďovanie údajov z elektronických komunikácií, ktoré sa majú použiť ako dôkazy na súdoch, ako aj na cezhraničnú justičnú spoluprácu. V hodnotení sa zdôraznila potreba spoločného prístupu na úrovni EÚ. V súčasnosti prebieha spoločný proces úvah, do ktorého sú zapojené inštitúcie EÚ a členské štáty a ktorým sa skúma problém uchovávania údajov s cieľom identifikovať právne a praktické riešenia výziev, ktoré vyplývajú z judikatúry Súdneho dvora.

- V posledných rokoch sa výrazne zvýšilo sexuálne zneužívanie detí na internete v rôznych podobách. V záujme účinného boja proti týmto formám trestnej činnosti sa v členských štátoch v rôznom rozsahu vykonáva široká škála preventívnych (napr. odborná príprava a informačné kampane zamerané na zvyšovanie povedomia) a donucovacích opatrení (blokovanie prístupu alebo odstraňovanie nezákonného obsahu), do ktorých sa zapája verejný aj súkromný sektor. Z hodnotenia vyplynulo, že národnú databázu na identifikáciu obetí v rámci boja proti sexuálnemu zneužívaniu detí má iba niekoľko členských štátov; ostatným členským štátom, ktoré používajú iba medzinárodnú databázu sexuálneho vykorisťovania detí (ICSE-DB) v rámci Interpolu, sa odporučilo, aby takéto vnútroštátne databázy zriadili. Viaceré členské štáty zaviedli opatrenia na predchádzanie opakovanej viktimizácii detí, v niektorých prípadoch vrátane ochrany svedkov a obetí sexuálneho zneužívania detí počas trestného konania. Ako dôležitý prvok boja proti tejto forme trestnej činnosti sa identifikovala dobrá spolupráca medzi všetkými príslušnými zainteresovanými stranami, konkrétne orgánmi presadzovania práva, horúcimi linkami, mimovládnymi organizáciami a poskytovateľmi internetových služieb (ISP).

- Pokiaľ ide o kybernetickú bezpečnosť, kľúčovú úlohu v oblasti monitorovania kybernetických incidentov a reakcií na ne zohrávajú vnútroštátne jednotky CSIRT, ktoré vytvorila už väčšina členských štátov. Okrem toho musia členské štáty vo svojom vnútroštátnom práve zaviesť pre poskytovateľov základných služieb povinnosť bezodkladne oznamovať príslušným orgánom alebo jednotkám CSIRT kybernetické incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb. Obe otázky sú upravené v smernici o bezpečnosti sietí a informačných systémov a musia sa zrealizovať do 9. mája 2018.

- Keďže vyšetrovania počítačovej kriminality „*stricto sensu*“ a trestných činov umožnených informačnými technológiami často zahŕňajú viac než jeden členský štát, prioritou je spolupráca s agentúrami EÚ – Europolom/EC3, Eurojustom, EJS, EJCN a agentúrou ENISA – , poskytovanie informácií týmto agentúram a v náležitých prípadoch aj získavanie informácií od nich. Z rovnakého dôvodu sa odporúčalo aj širšie využívanie spoločných vyšetrovacích tímov ako účinný nástroj pri cezhraničných vyšetrovaniach.

- Keďže Internet nepozná hranice, bezproblémová a riadne fungujúca medzinárodná spolupráca je preto v efektívnom boji proti počítačovej kriminalite zásadná. Ako sa však zdôraznilo v hodnotení, postupy vzájomnej právnej pomoci sú často pomalé, časovo náročné a neefektívne, čo má negatívny vplyv na vyšetrovania, pretože elektronické dôkazy sú nestabilné, a preto treba ich získavať rýchlo. Následne je v súvislosti s vyšetrovaniami počítačovej kriminality potrebné urýchliť vybavovanie žiadostí o vzájomnú právnu pomoc. Členské štáty sa navyše nabádajú, aby okrem iného častejšie využívali nástroje Europolu, Eurojustu a EJS a aby rozvíjali neformálne kontakty s príslušnými zahraničnými orgánmi

III – NÁRODNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI

HLAVNÉ ZISTENIA A ZÁVERY

- V čase hodnotenia už väčšina členských štátov prijala národnú stratégiu kybernetickej bezpečnosti, niektoré z nich aj akčný plán jej vykonávania, zatiaľ čo v zopár členských štátoch sa tento proces práve odohrával.

- Po vypracovaní národnej stratégie kybernetickej bezpečnosti a prípadného akčného plánu je nevyhnutné zabezpečiť prijatie vhodných nadväzujúcich opatrení a pozorne monitorovať vykonávanie národnej stratégie.

- Vzhľadom na rýchly vývoj informačných a komunikačných technológií (IKT) aj nových typov trestných činov, ktorých predmetom sú informačné technológie, je potrebné neustále aktualizovať opatrenia a prostriedky, ktoré sa zaviedli na účinný boj proti počítačovej kriminalite, z čoho vyplýva aj potreba zabezpečiť včasné preskúmanie národnej stratégie kybernetickej bezpečnosti podľa potrieb.

- Zriadenie jediného subjektu s koordinačnými funkciami na vykonávanie národnej stratégie kybernetickej bezpečnosti, ako je to v niektorých členských štátoch, sa môže považovať za osvedčený postup, ktorý by mali ostatné členské štáty nasledovať.

- Prijatie národnej stratégie v oblasti bezpečnosti sietí a informačných systémov sa predpokladá v nedávno prijatej smernici 2016/1148/(„smernica NIS“) s cieľom vymedziť strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne bezpečnosti sietí a informačných systémov (článok 7).

ODPORÚČANIA

- ***Členské štáty, ktoré zatiaľ národnú stratégiu kybernetickej bezpečnosti neprijali, sa vyzývajú, aby tak urobili v čo najkratšej lehote a zvážili aj prijatie akčného plánu; tie, ktoré stratégiu prijali, by mali zabezpečiť jej riadne vykonávanie a prípadné pridelenie koordinačných funkcií na tento účel jedinému subjektu/orgánu.***

- ***Členské štáty by mali svoje národné stratégie kybernetickej bezpečnosti aktualizovať vždy, keď je to potrebné, a to v súlade s príslušným vývojom v oblasti IKT, ako aj s trendmi v oblasti počítačovej kriminality.***

IV – BUDAPEŠTIANSKY DOHOVOR

HLAVNÉ ZISTENIA A ZÁVERY

- Budapeštiansky dohovor Rady Európy o počítačovej kriminalite z roku 2001 je prvým a jediným medzinárodným dohovorom, ktorého cieľom je presadzovanie spoločnej politiky v oblasti boja proti trestnej činnosti zameranej na ochranu spoločnosti proti počítačovej kriminalite, a to najmä prijímaním príslušných právnych predpisov a posilnením medzinárodnej spolupráce.

- Budapeštianskym dohovorom sa vymedzujú trestné činy proti dôvernosti, celistvosti a dostupnosti počítačových údajov a systémov, falšovania počítačových údajov a počítačových podvodov, detskej pornografie a porušenia autorských práv.

- Takisto sa ním ustanovuje súbor právomocí a postupov, ako napríklad urýchlené uchovanie a sprístupnenie údajov, príkazy na predloženie, prehliadka počítačových sietí a zákonné odpočúvanie telekomunikačnej prevádzky.

- V článku 35 sa ustanovuje medzinárodná sieť 24/7 na poskytovanie okamžitej pomoci na účely vyšetrovania alebo konania, ktorá umožňuje zmrazenie údajov, čím sa umožňuje zachovať elektronické dôkazy. Sieť 24/7 je dôležitý nástroj, pretože predstavuje rýchlu možnosť uchovať elektronické dôkazy ešte pred zaslaním žiadosti o vzájomnú právnu pomoc.

- Budapeštiansky dohovor dopĺňa dodatkový protokol týkajúci sa kriminalizácie skutkov rasistickej a xenofóbnej povahy páchaných prostredníctvom počítačových systémov, a pokiaľ ide o ochranu detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním, dopĺňa ho dohovor z Lanzarote.
- Hoci v čase hodnotenia už väčšina členských štátov tieto nástroje podpísala a ratifikovala, niekoľko členských štátov tak ešte stále neurobilo. V záveroch Rady o zlepšení trestnej justície v kybernetickom priestore z 9. júna 2016 sa zopakovala výzva ostávajúcim členským štátom, aby ratifikovali a plne vykonali Dohovor o počítačovej kriminalite a jeho dodatkový protokol.

ODPORÚČANIA

- ***Členské štáty, ktoré tak ešte neurobili, sa nabádajú, aby podpísali a ratifikovali Budapeštiansky dohovor Rady Európy z roku 2001 o počítačovej kriminalite a jej dodatkový protokol a plne tieto nástroje vykonali.***

V – ŠTATISTIKA

HLAVNÉ ZISTENIA A ZÁVERY

- Z analýzy právnych predpisov EÚ vyplýva jasná potreba zbierať štatistické údaje v oblasti počítačovej kriminality. Podľa článku 14 ods. 1 smernice 2013/40/EÚ o útokoch na informačné systémy členské štáty zabezpečia, aby bol zavedený systém na zaznamenávanie, vytváranie a poskytovanie štatistických údajov o trestných činoch uvedených v článkoch 3 až 7.

- Podľa článku 14 ods. 2 uvedenej smernice štatistické údaje uvedené v odseku 1 zahŕňajú minimálne existujúce údaje o počte trestných činov uvedených v článkoch 3 až 7, ktoré boli zaevidované členskými štátmi, a počte osôb, ktoré sú stíhané a odsúdené za trestné činy uvedené v článkoch 3 až 7.

- Okrem toho, podľa odôvodnenia 44 smernice 2011/93/EÚ o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii sa členské štáty nabádajú na to, aby s cieľom sledovať a vyhodnocovať jav sexuálneho zneužívania a sexuálneho vykorisťovania detí vytvorili na štátnej alebo miestnej úrovni a v spolupráci s občianskou spoločnosťou mechanizmy alebo koordinačné strediská na zber údajov.

- Okrem toho potreba zbierať štatistické údaje na vnútroštátnej úrovni *in principio* vyplýva z vnútroštátneho práva alebo iných nariadení členských štátov.

- Štatistické údaje o počítačovej kriminalite sú mimoriadne dôležité. Na jednej strane umožňujú podrobnú analýzu a prehľad o rozsahu nových vznikajúcich trendov v rámci tejto rozširujúcej sa formy trestnej činnosti, čím sa umožňuje vytvorenie realistickej predstavy o rozšírenosti počítačovej kriminality, ktorá je skreslená nedostatočným oznamovaním takýchto trestných činov, a sledovanie jej vývoja, aby sa mohli prijímať primerané opatrenia; na druhej strane umožňujú posúdiť efektívnosť právneho systému a primeranosť právnych predpisov v oblasti boja proti počítačovej kriminalite a ochrany záujmov občanov, ktorí sa stali jej obeťou.

- Komplexné štatistiky by sa mali týkať všetkých fáz konania: vyšetrovania, trestného stíhania, súdneho konania, pričom by sa mal uviesť druh trestnej činnosti a konkrétne vyšetrovacie úkony, počet nahlásených trestných činov, počet vykonaných vyšetrovaní a rozhodnutia nevyšetrovať určité druhy počítačovej kriminality, počet obetí a počet trestných oznámení obetí, počet stíhaných osôb a osôb odsúdených za rôzne druhy počítačovej kriminality, počet cezhraničných prípadov, výsledky žiadostí o vzájomnú právnu pomoc a dĺžka trvania konania.

- Avšak jeden z hlavných nedostatkov, ktoré sa identifikovali v rámci 7. kola hodnotenia vo väčšine členských štátov, sa týka zberu samostatných štatistických údajov o počítačovej kriminalite *stricto sensu*, trestných činoch umožnených informačnými technológiami a o kybernetických bezpečnostných incidentoch. Údaje, ktoré sú k dispozícii, sú vo väčšine členských štátov nedostatočné, roztrieštené a nemožno ich porovnávať.

- Okrem toho nemajú mnohé členské štáty vnútroštátne vymedzenie počítačovej kriminality *stricto sensu* a trestných činov umožnených informačnými technológiami na štatistické účely. V mnohých členských štátoch nie je možné určiť podiel počítačovej kriminality na celkovej trestnej činnosti a iné členské štáty, ktoré zberajú konkrétne štatistické údaje o počítačovej kriminalite, generujú štatistiky s jedinou hodnotou; v dôsledku toho nie je možné rozdeliť ich do kategórií a rozlišovať medzi prípadmi, ktoré sa týkajú počítačovej kriminality *stricto sensu*, a trestnými činmi umožnenými informačnými technológiami. Nie všetky členské štáty zostavujú pravidelné štatistické správy o počítačovej kriminalite.

- Vo väčšine členských štátov sú justičné štatistiky oddelené od štatistík orgánov presadzovania práva. Keďže sa štatistické systémy často výrazne líšia od jedného príslušného orgánu k druhému a každý orgán zbiera údaje z rôznych zdrojov, rozdielnymi metódami a spravuje ich na základe odlišných kritérií a/alebo používa rôzne databázy bez interoperability, počítačovú kriminalitu nie je možné sledovať v jedinom štatistického systéme.

- V mnohých členských štátoch je počet údajov o počítačovej kriminalite zadávaných do príslušných štatistických systémov veľmi nízky. V týchto prípadoch môžu vzniknúť otázky o účinnosti odhaľovania, stíhania a trestania počítačovej kriminality a o presnosti štatistických záznamov.

ODPORÚČANIA

- ***Členské štáty, ktoré čelia problémom súvisiacim s nedostatočným spoločným vymedzením alebo spoločným chápaním počítačovej kriminality, sa vyzývajú, aby vypracovali jednotné vnútroštátne vymedzenie (alebo chápanie) počítačovej kriminality, ktoré budú uplatňovať všetky zainteresované strany, ktoré sa podieľajú na boji proti počítačovej kriminalite, a ktoré sa bude používať na účel zostavovania štatistík.***

- ***Členské štáty sa nabádajú, aby zhromažďovali konkrétne a samostatné štatistické údaje o počítačovej kriminalite stricto sensu, trestných činoch umožnených informačnými technológiami a o kybernetických bezpečnostných incidentoch, umožňujúce overenie celkového objemu počítačovej kriminality a určenie podielu počítačovej kriminality na všetkých spáchaných trestných činoch.***

- ***Členské štáty sa nabádajú, aby vytvorili štandardizovaný prístup k zberu komplexných štatistických údajov vo všetkých rôznych fázach trestného konania, rozčlenených na konkrétne oblasti počítačovej kriminality, prednostne tie, ktoré sú vymedzené na úrovni EÚ, t. j. online sexuálne zneužívanie detí, online podvody s bankovými/kreditnými kartami a kybernetické útoky.***

- ***Členské štáty by mali zvážiť riešenia, ktoré umožňujú interoperabilitu rôznych databáz obsahujúcich údaje o počítačovej kriminalite s cieľom rýchlo dosiahnuť možnosť identifikovať páchateľov, kvantifikovať prípady a porovnávať ich.***

- ***Členské štáty by mali uľahčovať výmenu štatistických údajov medzi rôznymi vnútroštátnymi orgánmi zapojenými do boja proti počítačovej kriminalite, najmä medzi orgánmi presadzovania práva a súdnymi orgánmi.***

VI – ŠTRUKTÚRY – SÚDNICTVO

HLAVNÉ ZISTENIA A ZÁVERY

- Štruktúra a organizácia súdnictva sa v jednotlivých členských štátoch líšia, a to vrátane rozdelenia právomocí v oblasti počítačovej kriminality.

- Vzhľadom na rýchly vývoj IKT a komplexnosť a čoraz väčšiu rafinovanosť počítačovej kriminality závisí úspech vyšetrovaní, stíhaní a odsúdení v prípadoch počítačovej kriminality vo veľkej miere od zručnosti a skúseností orgánov zodpovedných za vyšetrovanie a súdne konanie. Preto je v tejto oblasti mimoriadne dôležitá vysoká úroveň chápania problematiky a znalostí, ako aj špecializácie zamestnancov súdnych orgánov.

- Podľa zistení vzájomného hodnotenia však nie je úroveň špecializácie a konkrétnych znalostí prokurátorov a sudcov, ktorí sa zaoberajú počítačovou kriminalitou a súvisiacimi trestnými činmi, vždy uspokojivá.

- V značnom počte členských štátov sa počítačovou kriminalitou zaoberajú všeobecné prokuratúry a v žiadnom z členských štátoch neexistujú špecializované súdy alebo sudcovia vymenovaní na skúmanie prípadov počítačovej kriminality a rozhodovanie o nich. Niektoré členské štáty však majú špecializovaných prokurátorov alebo špecializované štruktúry v rámci prokuratúr, ktoré sa zaoberajú počítačovou kriminalitou. V zopár členských štátoch zodpovedajú *de facto* za takéto trestné činy špecializovaní prokurátori a sudcovia, ktorí absolvovali odbornú prípravu alebo majú skúsenosti v oblasti počítačovej kriminality.

- V niektorých členských štátoch existujú národné siete „kybernetických prokurátorov“ so špecializáciou na počítačovú kriminalitu, čo možno považovať za osvedčený postup, pretože umožňujú vzájomnú výmenu znalostí a skúseností a podporujú šírenie najlepších postupov medzi odborníkmi pracujúcimi v oblasti práva.

- Hodnotitelia odporučili, aby členské štáty s podporou Eurojustu uľahčili vytvorenie európskej siete sudcov, ktorí sa špecializujú na boj proti počítačovej kriminalite, so zameraním na zlepšenie a uľahčenie justičnej spolupráce v tejto oblasti. Tento cieľ sa medzičasom dosiahol v júni 2016 zriadením Európskej justičnej siete na boj proti počítačovej kriminalite (EJCN) na základe záverov Rady, pričom táto sieť už začala pracovať. Výmena odborných znalostí a skúseností v rámci danej siete môže prispieť k zvýšeniu úrovne špecializácie justície v členských štátoch.

ODPORÚČANIA

- ***Členské štáty by mali zvýšiť úroveň špecializácie svojho justičného sektora s cieľom účinne stíhať a sankcionovať počítačovú kriminalitu stricto sensu a trestné činy umožnené informačnými technológiami. Na tento účel by mali zvážiť zriadenie špecializovaných úradov alebo vnútorných štruktúr/jednotiek a/alebo vymenovať na riešenie takýchto prípadov špecializovaných prokurátorov a sudcov s vysokou mierou chápania problematiky a vedomostí o počítačovej kriminalite.***

- ***Členské štáty by mali zvážiť vytvorenie siete prokurátorov a sudcov špecializovaných na počítačovú kriminalitu na vnútroštátnej úrovni ako dodatočný nástroj na zlepšenie účinnosti boja proti tomuto druhu trestnej činnosti.***

VII – ŠTRUKTÚRY – ORGÁNY PRESADZOVANIA PRÁVA (OPP)

HLAVNÉ ZISTENIA A ZÁVERY

- Štruktúra a organizácia orgánov presadzovania práva (OPP) sa v jednotlivých členských štátoch významne líši, aj pokiaľ ide o rozdelenie právomoci v oblasti počítačovej kriminality. V niektorých členských štátoch pracujú špecializované jednotky na základe zastrešujúceho prístupu, ktorý zahŕňa strategické plánovanie aj operačné činnosti, zatiaľ čo v iných členských štátoch tieto funkcie vykonávajú samostatne iné úrady a orgány.

- Kľúčovými prvkami v boji proti počítačovej kriminalite sú účinná organizácia, medzinárodná integrácia a odborná spôsobilosť OPP zapojených do vyšetrovania tohto druhu trestnej činnosti. Pre účinný boj proti tejto komplexnej a rafinovanej forme trestnej činnosti je nevyhnutná aj vysoká úroveň znalostí a špecializácie OPP, ktorá sa z rovnakých dôvodov zdôrazňuje v justičnom sektore.

- Zo vzájomného hodnotenia vo všeobecnosti vyplýva, že úroveň špecializácie OPP je vyššia ako v justícii, ale v mnohých prípadoch ju možno zlepšiť.

- Vo väčšine členských štátov existujú v rámci ministerstva vnútra a/alebo polície špecializované ústredné štruktúry alebo jednotky zodpovedné za predchádzanie počítačovej kriminalite a boj proti nej na národnej úrovni, čím sa zabezpečuje koordinácia vyšetrovania počítačovej kriminality v celej krajine s vysokou úrovňou špecializácie v tejto oblasti. Uľahčuje sa tým aj komunikácia medzi políciou a prokurátormi. Vo viacerých členských štátoch existujú aj decentralizované špecializované jednotky na miestnej a/alebo regionálnej úrovni, ktoré sa zaoberajú špecificky vyšetrovaniami počítačovej kriminality.

- Niektorým členským štátom sa odporúča, aby zreorganizovali políciu a prijali príslušné kroky, pokiaľ ide o zvyšovanie počtu ľudských zdrojov, zabezpečenie účinnejšej a intenzívnejšej odbornej prípravy polície a dostatočné technické vybavenie určené na boj proti počítačovej kriminalite. Okrem toho sa zariadenia a zdroje OPP musia neustále aktualizovať s cieľom zvládnuť konštantný vývoj a diverzifikáciu *modu operandi* počítačovej kriminality.

- Hlavné prekážky úspešného vyšetrovania počítačovej kriminality sú, okrem iného, rýchly rozvoj technológie a nový zložitý *modus operandi*, zvyšujúca sa profesionalizácia a úroveň odbornosti páchateľov počítačovej kriminality, skutočnosť, že na počítačovú kriminalitu sa často vzťahujú právomoci viacerých krajín, ťažkosti pri získavaní prístupu k elektronickým dôkazom v súvislosti s počítačovou kriminalitou a výzvy súvisiace s použitím šifrovania, siete TOR a anonymizácie.

ODPORÚČANIA

- ***Členské štáty by mali zachovať a v relevantných prípadoch zvýšiť úroveň špecializácie OPP, ktoré sa zaoberajú vyšetrovaniami počítačovej kriminality. Členské štáty, ktoré tak ešte neurobili, by mali zvážiť zriadenie špecializovaných jednotiek v rámci OPP na účinnejší boj proti počítačovej kriminalite, a to aj na regionálnej/miestnej úrovni.***

- ***Členské štáty by mali zvážiť vytvorenie siete príslušníkov polície špecializovaných na počítačovú kriminalitu na národnej úrovni, ktorá by tiež mohla pomôcť udržiavať komunikačný kanál medzi verejným a súkromným sektorom a políciou.***

- ***Členské štáty by mali zvážiť posilnenie netechnického policajného personálu v krajských a regionálnych štruktúrach a zabezpečenie dostatočného technického vybavenia podľa jeho potrieb.***

VIII – SPOLUPRÁCA A KOORDINÁCIA NA VNÚTROŠTÁTNEJ ÚROVNI

HLAVNÉ ZISTENIA A ZÁVERY

- Keďže počítačová kriminalita má prierezový charakter a zodpovednosť za bezpečnosť kybernetického priestoru na vnútroštátnej úrovni vo všeobecnosti nesú spoločne rôzni aktéri, ktorí majú rôzne právomoci a spôsobilosti, či už ide o verejných alebo súkromných, vojenských alebo civilných, kolektívnych alebo individuálnych aktérov, kľúčovým faktorom pre účinné predchádzanie a boj proti počítačovej kriminalite a zabezpečenie kybernetickej odolnosti je multidisciplinárny prístup.

- V tejto súvislosti má zásadný význam úzka a efektívna medziinštitucionálna koordinácia a spolupráca medzi rôznymi orgánmi verejnej moci a subjektmi verejného sektora na operačnej a strategickej úrovni, ako aj medzi ústrednými a miestnymi/regionálnymi orgánmi s cieľom koordinovať iniciatívy a posilňovať výmenu údajov, technickú podporu a vyšetrovacie techniky.

- Spolupráca v boji proti počítačovej kriminalite medzi políciou, prokuratúrou a národnými spravodajskými službami môže byť v rámci prísneho rozdelenia funkcií a právomocí týchto inštitúcií, ako si to vyžadujú niektoré členské štáty, prospešná z hľadiska získania podpory z technického hľadiska (odpočúvania, odborné poradenstvo atď.) alebo spravodajských informácií v rámci vyšetrovania a stíhania trestných činov, najmä pokiaľ ide o získavanie a spracúvanie elektronických dôkazov.

- Spolupráca medzi verejným a súkromným sektorom má takisto zásadný význam z hľadiska úspešného vyšetrovania, stíhania a odsudzovania páchateľov počítačovej kriminality *stricto sensu* a trestných činov umožnených informačnými technológiami, ako aj z hľadiska reakcie na kybernetické hrozby a kybernetické útoky (pre podrobnejšie informácie pozri nasledujúcu kapitolu).

- Spolu s právnym rámcom pre spoluprácu medzi agentúrami, ak je vymedzený, sa zvyčajne prostredníctvom národnej stratégie kybernetickej bezpečnosti a akčného plánu na jej realizáciu, ak existuje, vytvára všeobecný rámec pre koordináciu a spoluprácu medzi všetkými verejnými inštitúciami a orgánmi s právomocami v oblasti kybernetickej bezpečnosti a so súkromným sektorom s cieľom zabezpečiť, aby vymedzili úlohy a povinnosti.

- Riadne vykonávanie národnej stratégie kybernetickej bezpečnosti je preto kľúčovým prvkom zabezpečenia synergií a maximalizácie pripravenosti, ako aj reakčnej spôsobilosti v boji proti počítačovej kriminalite a pri posilňovaní kybernetickej bezpečnosti.

- Podľa zistení z hodnotení sa podoby, spôsoby a úrovne spolupráce a koordinácie medzi príslušnými zainteresovanými stranami, ktoré sa podieľajú na boji proti počítačovej kriminalite a zaisťovaní kybernetickej bezpečnosti, v jednotlivých členských štátoch líšia. V niekoľkých členských štátoch neexistuje žiadny právny rámec spolupráce medzi agentúrami v prípadoch týkajúcich sa počítačovej kriminality a orgány zapojené do boja proti počítačovej kriminalite spolupracujú neformálnym spôsobom. Niektoré členské štáty vytvorili modernejšie a účinnejšie formy interakcie, ktoré sa v jednotlivých správach označili za osvedčené postupy.

- Najlepším spôsobom, ako zabezpečiť riadne fungovanie systému, je štruktúrovaný mechanizmus, najmä pokiaľ sa koordinačné funkcie otázok týkajúcich sa kybernetickej bezpečnosti a politiky boja proti počítačovej kriminalite zveria jedinej inštitúcii (t. j. ministerstvu alebo úradom v jeho organizačnej štruktúre) alebo jedinému *ad hoc* orgánu alebo subjektu. Takáto jediná inštitúcia alebo orgán, ktorý zabezpečuje inštitucionálny rámec pre spoluprácu zahŕňajúci verejné aj súkromné strany zainteresované v boji proti počítačovej kriminalite a v oblasti zaisťovania kybernetickej bezpečnosti, už v niektorých členských štátoch existujú, pričom iné členské štáty v čase hodnotenia zvažovali ich zriadenie.

- Niektoré členské štáty, v ktorých sa v súvislosti so vzájomným hodnotením zistili nedostatky, vynakladajú úsilie na posilnenie existujúcich štruktúr a procesov spolupráce a koordinácie s cieľom účinnejšie predchádzať počítačovej kriminalite a bojovať proti nej.

ODPORÚČANIA

- ***Členské štáty by mali priorizovať inštitucionálnu koordináciu a spoluprácu medzi všetkými príslušnými zainteresovanými stranami zapojenými do predchádzania počítačovej kriminalite a boja proti nej a do zaisťovania kybernetickej bezpečnosti založenú na multidisciplinárnom prístupe s cieľom vytvárať synergie, ako aj maximalizovať pripravenosť a reakčnú spôsobilosť.***

- ***Na tento účel sa členské štáty nabádajú predovšetkým k tomu, aby zaviedli alebo posilnili štruktúrovaný rámec spolupráce a prípadne zriadili ústredný orgán/subjekt alebo platformu, v ktorej bude zastúpený verejný aj súkromný sektor a ktorý bude mať koordinačné funkcie a právomoc odporúčať riešenia zistených problémov.***

IX – SPOLUPRÁCA MEDZI VEREJNÝM A SÚKROMNÝM SEKTOROM

HLAVNÉ ZISTENIA A ZÁVERY

- Úzka spolupráca medzi verejným a súkromným sektorom má zásadný význam, keďže boj proti počítačovej kriminalite je veľmi zložitý, čo znamená, že OPP nemôžu úspešne bojovať proti tejto trestnej činnosti bez spolupráce súkromného sektora (finančných/bankových inštitúcií, telekomunikačných spoločností, poskytovateľov internetových služieb, mimovládnych organizácií, akademickej obce, obchodných a profesijných združení atď.).

- Takáto spolupráca by mohla fungovať v prospech oboch sektorov, pretože vytvára príležitosť na to, aby sa do spolupráce zapojilo širokého spektrum subjektov a aby sa zabezpečili synergie medzi nimi, čím by sa prispelo k zvýšeniu úrovne kybernetickej bezpečnosti.

- Príspevok súkromných zainteresovaných strán z hľadiska odborných znalostí, technickej podpory a výmeny informácií o kybernetických hrozbách a trendoch v oblasti kybernetickej bezpečnosti má veľký prínos pre úspech vyšetrovaní a opatrení zameraných na riešenie kybernetických incidentov. Do stykov so súkromným sektorom je tiež vhodné zapojiť prokurátorov, aby sa zabezpečilo, že dôkazy sa budú zhromažďovať v súlade s platnými právnymi predpismi a budú prípustné v súdnom konaní.

- Podľa zistení hodnotenia sa úroveň spolupráce medzi verejným a súkromným sektorom v jednotlivých členských štátoch líši a vo všeobecnosti je rozvinutejšia a účinnejšia, ak je štruktúrovanejšia a prebieha v dôvernom a spoľahlivom prostredí. V hodnotení sa identifikovali osvedčené postupy v niektorých členských štátoch, zatiaľ čo v prípade iných sa zdôraznila potreba zlepšenia takejto spolupráce.

- V niektorých členských štátoch je využívanie verejno-súkromných partnerstiev súčasťou národnej stratégie kybernetickej bezpečnosti, ale niekedy je obmedzené na osobitné oblasti. Môže sa zakladať na memorandách o porozumení alebo podobných formálnych dohodách.

- Nie všetky členské štáty však už vypracovali formálny rámec pre verejno-súkromné partnerstvá a v niektorých z nich sa spolupráca, stretnutia a výmeny informácií o incidentoch, trendoch a vývoji so súkromným sektorom odohrávajú neformálne, a nie na právnom základe.

- Najpokročilejšie formy spolupráce so súkromným sektorom sa identifikovali v niektorých členských štátoch, kde je takáto spolupráca inštitucionalizovaná zriadením vhodných inštitúcií/pracovných skupín pre spoluprácu medzi súkromným sektorom a orgánmi verejnej správy alebo orgánmi presadzovania práva.

- Podľa zistení vyplývajúcich z hodnotenia identifikovali hodnotitelia verejno-súkromné partnerstvá ako dôležitý nástroj pre dobrú spoluprácu medzi orgánmi presadzovania práva a súkromným sektorom, najmä s poskytovateľmi internetových služieb, finančným sektorom, konkrétne s bankami, ale aj s mimovládnymi organizáciami, jednotkami CSIRT a prevádzkovateľmi kritických infraštruktúr. Môžu byť užitočné, pokiaľ ide o odstraňovanie nezákonného obsahu, dešifrovanie, boj proti počítačovým útokom atď.

- Spolupráca s poskytovateľmi služieb je obzvlášť užitočná na to, aby sa mohli zúžitkovať ich odborné znalosti aj aby sa získal prístup k základným informáciám o používateľoch. Poskytovatelia elektronických komunikačných sietí a služieb môžu prostredníctvom posudzovania rizík, vhodných bezpečnostných opatrení a uplatňovania štruktúrovanej bezpečnostnej politiky nielen zabrániť výskytu určitých druhov počítačovej kriminality, ale aj pomáhať OPP s poskytovaním dôkazov.

- Podľa zistení vyplývajúcich z hodnotenia je potrebné nájsť riešenia pre jasný a primeraný rámec upravujúci vzťahy justičných orgánov s poskytovateľmi internetových služieb v celej EÚ. Na tento účel by bolo možné zlepšiť túto spoluprácu postupmi, ktoré by mohli orgánom umožniť, aby dostávali odpovede na svoje žiadosti včas, a ktorými by sa zaviedol systém sankcií pre prípady neplnenia príslušných povinností (správne alebo poriadkové pokuty).

- Dialóg s hlavnými prevádzkovateľmi internetu, hostiteľskými spoločnosťami a poskytovateľmi pripojenia na internet a poskytovateľmi služieb na úrovni EÚ i na medzinárodnej úrovni by mohol posilniť ich spoluprácu v rámci vyšetrovaní trestných činov.

- V oblasti boja proti podvodom s kartami, pri ktorých karta nie je fyzicky prítomná, a iným druhom online podvodov je nevyhnutná aj účinná spolupráca medzi OPP na jednej strane a finančnými inštitúciami a komerčnými bankami na druhej strane s cieľom identifikovať takéto podvody, aktualizovať situáciu v súkromnom sektore vzhľadom na nové trendy a identifikovať preventívne opatrenia.

- V niektorých členských štátoch túto spoluprácu uľahčujú špecializované združenia bánk alebo medzibankové výbory zriadené na boj proti podvodom v oblasti platobných systémov a platobných prostriedkov, ktoré organizujú pravidelné stretnutia, aj s účasťou polície. V jednom členskom štáte hodnotitelia označili za osvedčený postup účasť polície v poradnom orgáne národného združenia bánk.

- V iných členských štátoch je spolupráca medzi OPP a bankovými a finančnými inštitúciami menej štruktúrovaná a obmedzuje sa na styk a/alebo stretnutia s cieľom zabezpečiť spoluprácu a výmenu informácií o otázkach týkajúcich sa počítačovej kriminality.

- V niektorých členských štátoch existuje pre súkromný sektor v súvislosti s počítačovou kriminalitou oznamovacia povinnosť, zatiaľ čo iné členské štáty takéto oznamovanie neustanovili ako povinné, alebo je obmedzené na špecifické odvetvia súkromného sektora alebo na určitý typ počítačovej kriminality.

- V určitých prípadoch funguje oznamovanie počítačovej kriminality na dobrovoľnom základe. Avšak podľa zistení vyplývajúcich z hodnotenia sa finančné a úverové inštitúcie a poskytovatelia internetových služieb v niektorých členských štátoch zdráhajú oznamovať počítačovú kriminalitu a podporovať trestné konanie s cieľom určiť trestnú zodpovednosť páchateľa. Majú väčší záujem na čo najrýchlejšom odstránení škôd, ktoré by mohli vzniknúť z dôvodu zverejňovania a mediálneho pokrytia, čo nie je dobré pre ich dôveryhodnosť a povesť.

- Podľa niektorých správ o jednotlivých krajinách je spolupráca s OPP zvyčajne dobrá, keď je súkromný sektor obeťou alebo poškodenou stranou, pretože sa usiluje o uchovanie dôkazov, ich výklad a poskytnutie OPP.

- Súkromný sektor zohráva dôležitú úlohu, aj pokiaľ ide o ochranu detí a pri činnostiach zameraných na prevenciu a zvyšovanie informovanosti v tejto oblasti; súkromné združenia a mimovládne organizácie pôsobiace v tejto oblasti, ktoré spolupracujú s OPP zapojenými do boja proti online sexuálnemu zneužívaniu, prispievajú zásadným spôsobom – oznamovaním prípadov zneužívania.

- Podľa záverov hodnotenia by dialóg so súkromným sektorom, ktorý by šiel nad rámec požiadaviek povinného oznamovania, v každom prípade umožnil lepšie výsledky boja proti počítačovej kriminalite.

- Verejné orgány by tiež mali spolupracovať, ako sa už deje v niekoľkých členských štátoch, s akademickou obcou, vzdelávacími inštitúciami, so sociálnymi službami, s podnikateľskými a profesijnými združeniami, médiami a inými organizáciami a podnikmi s cieľom predchádzať nepriaznivým dôsledkom počítačovej kriminality *stricto sensu* a trestných činov umožnených počítačmi na bezpečnosť informácií v krajine a zmierňovať ich. Z hľadiska zvyšovania informovanosti, odbornej prípravy a výskumu a vývoja je veľmi dôležitá najmä spolupráca s akademickou obcou.

ODPORÚČANIA

- ***Členské štáty a inštitúcie EÚ by mali naďalej uvažovať o metodikách na udržiavanie a posilňovanie spolupráce medzi verejným a súkromným sektorom (banky, telekomunikačné spoločnosti a poskytovatelia služieb), a to aj vrátane prokurátorov a možno aj sudcov.***

- ***Členské štáty by mali využívať štruktúrované verejno-súkromné partnerstvá s cieľom zabezpečiť jasný rámec pre spoluprácu medzi verejným a súkromným sektorom s jasnými pravidlami a povinnosťami, pričom by možno mali rozlišovať medzi preventívnymi opatreniami na jednej strane a vyšetrovaním a trestným stíhaním na strane druhej.***

- ***Členské štáty by mali nabádať súkromný sektor, aby si vymieňal informácie s orgánmi verejnej moci, a ak je to vhodné, stanoviť pre súkromný sektor vo vnútroštátnom práve povinnosť oznamovať kybernetické bezpečnostné incidenty, najmä pokiaľ ide o úverové inštitúcie a iné kritické infraštruktúry, aby bezodkladne oznamovali kybernetické incidenty zamerané na nich a/alebo ich zákazníkov.***

- ***Európska únia a jej členské štáty by mali naďalej uvažovať, akým spôsobom sa dá zlepšiť spolupráca medzi OPP členských štátov a poskytovateľmi služieb vrátane možnosti pre EÚ uzatvárať dohody s niektorými z nich s cieľom posilniť spoluprácu v oblasti justičných vyšetrovaní.***

X – VYŠETROVACIE TECHNIKY

HLAVNÉ ZISTENIA A ZÁVERY

- Vzhľadom na veľkú rozmanitosť počítačovej kriminality nemôžu existovať žiadne všeobecne odskúšané a overené postupy alebo metódy vyšetrovania takýchto trestných činov. Každé vyšetrovanie a prístup závisí od konkrétnych okolností a vyšetrovacie postupy a metódy sa musia prispôsobiť konkrétnemu prípadu.

- V oblasti počítačovej kriminality sa najmä neustále a v krátkych intervaloch mení používaný *modus operandi*, softvér a nástroje. Vyšetrovacie techniky sa preto musia neustále aktualizovať (napr. špeciálnym vyšetrovacím počítačovým softvérom) v súlade s vývojom počítačovej kriminality.

- Na vyšetrovanie prípadov počítačovej kriminality sa okrem bežných techník vyšetrovania používajú aj osobitné techniky. Existuje mnoho možností: najčastejšie sa používajú osobitné vyšetrovacie techniky, ktoré sú mimoriadne účinnými pracovnými nástrojmi najmä pri riešení prípadov týkajúcich sa sexuálneho vykorisťovania detí, ako je odpočúvanie, uchovávanie údajov a utajené vyšetrovanie.
  Utajené vyšetrovanie, ktoré je užitočné najmä vtedy, ak vyšetrovanie nemožno vykonať pomocou technických prostriedkov, uskutočňujú agenti, ktorí vyšetrujú na diskusných fórach. Vyšetrovania tohto druhu však spravidla prinášajú uspokojivé výsledky, len ak sa vykonávajú dlhodobo.

- Ďalšie osobitné vyšetrovacie techniky sú založené na nových technických možnostiach v oblasti online boja proti počítačovej kriminalite, ako je napríklad online monitorovanie, alebo iných technológiách, ako sú napr. blokovanie prístupu k hardvéru a špeciálne aplikácie na kopírovanie na úrovni bitov („bit-copier“), prehliadky a zaisťovanie na diaľku (napr. ak OPP získajú priamy prístup do podozrivého počítača, namiesto toho, aby sa ho zmocnili fyzicky), sledovanie IP adresy, prehľadávanie otvorených zdrojov na internete, zálohovanie údajov z nosičov dát a z internetu (webové stránky, protokolové súbory). Osobitné techniky sa používajú aj pre mobilné zariadenia (napr. UFED).

- Nie vždy však vnútroštátne právne predpisy členských štátov využívanie osobitných vyšetrovacích techník umožňujú. V niektorých členských štátoch je na tento účel potrebný súdny príkaz.

ODPORÚČANIA

- ***Členské štáty, ktoré tak ešte neurobili, sa vyzývajú, aby vo svojich vnútroštátnych právnych predpisoch ustanovili možnosť využívať osobitné vyšetrovacie techniky s cieľom uľahčiť vyšetrovanie prípadov počítačovej kriminality.***

XI – ŠIFROVANIE

HLAVNÉ ZISTENIA A ZÁVERY

- Zvýšenou dostupnosťou a využívaním bezpečných a dôveryhodných šifrovacích technológií sa zaisťuje bezpečnosť, zabezpečený prenos a dôvernosť počítačových údajov, a tým aj ochrana súkromia občanov a účinná ochrana údajov v kybernetickom priestore.

- Rastúce využívanie šifrovania pri ukladaní údajov a v internetovej komunikácii s čoraz dokonalejšími metódami však spôsobuje, že je čím ďalej ťažšie, ak nie takmer nemožné šifrovanie prelomiť, čo predstavuje rastúci problém vo všetkých členských štátoch.

- Šifrovanie často využívajú zločinci na ochranu nelegálnych materiálov vo svojej držbe a svoju komunikáciu, čo vyšetrovanie počítačovej kriminality značne sťažuje. Keďže šifrovanie je štandardne nastavené v mnohých aplikáciách, OPP sa často stretávajú s problémami pri získavaní dôkazov v zašifrovanej forme.

- Šifrovanie sťažuje alebo úplne znemožňuje získať prístup k príslušným informáciám o počítačovej kriminalite, najmä pokiaľ ide o identifikáciu komunikácie alebo počítačových údajov v držbe podozrivých alebo páchateľov, a to nielen počas forenzného skúmania, ale aj počas všetkých ostatných druhov vyšetrovaní. Okrem toho odpočúvanie alebo výklad materiálu komplikuje používanie úplného šifrovania medzi koncovými zariadeniami, ktoré využíva čoraz väčší počet poskytovateľov služieb.

- Pre šifrované údaje ani šifrovanú komunikáciu neexistuje žiadne štandardné riešenie. Po preskúmaní individuálneho prípadu možno použiť cielené opatrenia, ako sú osobitné opatrenia na sledovanie telekomunikácie alebo dešifrovacie opatrenia.

- V tejto súvislosti prvá výzva spočíva v tom, aby sa potrebným vybavením odhalil zašifrovaný obsah a forma zašifrovania. Najväčším problémom je však dešifrovanie samotné, ktoré si nevyhnutne vyžaduje vysokovýkonný špecializovaný hardvér a softvér, čo predstavuje vysoké investície a značné náklady.

- V záujme riešenia týchto problémov sú potrebné znalosti súčasného stavu technológie šifrovania a štúdium nedostatkov v algoritmoch a implementácii, a to aj s cieľom využiť prípadné chyby.

- Hodnotenie ukázalo, že určitý úspech sa zvyčajne dosiahne pri veľmi jednoduchých šifrovacích metódach, a že ku kľúčom je možné dospieť alebo ich spätne vypočítať pomocou príslušného softvéru, čo následne umožní dešifrovanie. Jednoduché heslá možno prelomiť použitím vhodného hardvéru a nástrojov.

- Vyšetrovacie orgány môžu významne prispieť k úspešnému prelomeniu hesla, ak dokážu forenzným počítačovým odborníkom poskytnúť informácie týkajúce sa samotného hesla (možné heslové frázy, ich fragmenty, znaková sada, dĺžka hesla atď.) a všetky elektronické dôkazy alebo zariadenia. Nie vždy to však funguje.

- Podľa zistení vyplývajúcich z hodnotenia sa v niektorých prípadoch zložitejšie šifrovanie úspešne dešifrovalo použitím hrubej sily – vyskúšali sa všetky možné kódy alebo sa použili slovníkové útoky – t. j. zoznam pojmov vytvorený na účely prelamovania hesiel – alebo ak podozrivý poskytol heslo alebo frázu potrebnú na prelomenie šifrovania, pretože súhlasil so spoluprácou. Dotknuté osoby však nie sú vždy ochotné spolupracovať s orgánmi a neexistujú žiadne prostriedky donútiť ich, aby spolupracovali.

- Ak sú súbory chránené silným šifrovaním (archívy šifrované cez AES-256) alebo ak je šifrovaný celý disk (TrueCrypt, BitLocker, FileVault2, WinRar alebo PGP), môže byť dešifrovanie pomocou hrubej sily alebo slovníkových útokov časovo nesmierne náročné (mesiace, v niektorých prípadoch dokonca roky) a vyžaduje si veľa výpočtovej kapacity (špecializovaný komerčný softvér a infraštruktúra zosieťovaných klastrov). Šifrovaciu ochranu sa aj tak nemusí podariť prelomiť v prípadoch, keď páchatelia využívajú technicky pokročilé heslá alebo zložité algoritmy; v niektorých prípadoch sa proces dešifrovania musí zastaviť.

- V niektorých členských štátoch sa dešifrovanie vykonáva v spolupráci so súkromnými spoločnosťami, ktorých odborné znalosti sú užitočné, najmä ak ide o veľmi rafinované metódy šifrovania. Vo viacerých členských štátoch súkromné spoločnosti naopak nie sú zapojené do dešifrovania v rámci trestného vyšetrovania, ktoré je vyhradené pre vnútroštátne forenzné inštitúty.

- Zdroje a služby Europolu, najmä jeho Európske centrum boja proti počítačovej kriminalite (EC3), ponúkajú dešifrovaciu platformu a niektoré členské štáty túto možnosť využívajú.

- Podľa zistení hodnotenia možno na výzvy, ktoré prináša šifrovanie, čiastočne reagovať zintenzívnením výskumu a rozvíjaním nových metód vrátane inteligentnejších analýz vzorcov, ktoré páchatelia využívajú na tvorbu hesla, a dynamickou agregáciou výkonu počítačov.

- Nevyhnutná je aj kvalitná spolupráca medzi rôznymi dotknutými orgánmi, najmä OPP, prokurátormi a forenznými IT odborníkmi, a to aj preto, že nie každé oddelenie alebo orgán si môže dovoliť nákup hardvéru a softvéru na prelamovanie hesiel vzhľadom na súvisiace náklady.

- Spolupráca medzi členskými štátmi v oblasti dešifrovania sa zabezpečuje prostredníctvom spoločného využívania zdrojov a skúseností a účasťou na spoločných operáciách. Ak je potrebné postúpiť dôkazy iným orgánom na dešifrovanie, je to možné uskutočniť prostredníctvom kanálov Europolu a Interpolu.

ODPORÚČANIA

- ***Členské štáty by mali investovať do špecializovaného softvéru a hardvéru s primeranou výpočtovou kapacitou a do zamestnancov, ktorí sú primerane vyškolení, s cieľom zabezpečiť dešifrovanie aj v zložitých prípadoch šifrovaných súborov a komunikácií.***

- ***Členské štáty by mali zabezpečiť spoluprácu medzi všetkými príslušnými zainteresovanými stranami – prípadne vrátane súkromných spoločností – s cieľom zvýšiť dešifrovacie schopnosti príslušných orgánov.***

- ***Členské štáty by mali urýchliť výskum a vývoj s cieľom rozvíjať nové a efektívnejšie metódy dešifrovania a využívať zariadenia Europolu, konkrétne dešifrovaciu platformu Európskeho centra boja proti počítačovej kriminalite (EC3), na komplikovanejšie prípady šifrovania.***

- ***Členským štátom a inštitúciám EÚ sa takisto odporúča, aby zvážili spoločné riešenia so súkromným sektorom aby s ním posilnili otvorený dialóg.***

XII – ELEKTRONICKÉ DÔKAZY

HLAVNÉ ZISTENIA A ZÁVERY

- Značný počet členských štátov nemá vo svojich vnútroštátnych právnych predpisoch vymedzený pojem elektronické dôkazy. Ako referencia slúžia pojmy použité v Budapeštianskom dohovore Rady Európy o počítačovej kriminalite a v smernici 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy.

- V praxi sa vo všeobecnosti elektronické dôkazy chápu ako akékoľvek informácie vytvorené, uložené alebo prenášané prostredníctvom elektronických zariadení, na základe ktorých možno skonštatovať existenciu alebo neexistenciu trestného činu, identifikovať osobu, ktorá spáchala takýto trestný čin, a určiť okolnosti potrebné na urovnanie sporu.

- Zahŕňajú okrem iného informácie z registra, históriu surfovania na internete, dáta tvoriace obsah, obrázky, adresy IP, emaily, elektronické dokumenty, digitálne video súbory, audio súbory a obrázky, databázy, cookies, údaje z tabuliek, výstupy z tlačiarne, elektronické účtovníctvo, geolokalizačné údaje z GPS, záznamy o bankových operáciách atď.

- Zhromažďovanie, analýza a využívanie elektronických dôkazov v trestnom konaní sú čoraz dôležitejšie nielen v súvislosti s počítačovou kriminalitou, ale aj vo vzťahu k akémukoľvek inému trestnému činu, ktorý môže zahŕňať elektronické dôkazy.

- Z povahy elektronických dôkazov a ľahkosti, s akou s nimi možno manipulovať alebo ich falšovať, môžu vyplývať problémy, pokiaľ ide o ich prípustnosť, ktoré nevznikajú pri iných druhoch dôkazov.
  Preto sa v niektorých členských štátoch uplatňujú osobitné požiadavky na zhromažďovanie elektronických dôkazov, aby sa zabezpečila ich prípustnosť na súde. Napríklad si to môže vyžadovať, aby zhromažďovanie vykonal odborník s technickými znalosťami v záujme zachovania integrity elektronických dôkazov alebo kvalitného zdokumentovania reťazca dôkazov, pokiaľ ide o spôsob, akým sa tieto dôkazy pôvodne získali, kto a ako s nimi manipuloval vrátane toho, či boli akokoľvek pozmenené.

- Niektoré členské štáty na účely zhromažďovania elektronických dôkazov postupujú v súlade s najlepšími postupmi v oblasti digitálnej forenznej vedy stanovenými v Dohovore Rady Európy o počítačovej kriminalite alebo v medzinárodných usmerneniach, ako sú usmernenia združenia prezidentov policajných zborov (ACPO), ktoré sa vzťahujú aj na ukladanie a prenos elektronických dôkazov.

- Z hodnotenia však vyplynulo, že vo väčšine členských štátov je procesné právo technologicky neutrálne, čo znamená, že sa uplatňujú všeobecné pravidlá a zásady zhromažďovania dôkazov a že procesné právo neobsahuje žiadne osobitné pravidlá prípustnosti a hodnotenia elektronických dôkazov; tieto podliehajú rovnakým podmienkam ako akýkoľvek iný dôkaz a sudcovia ich vyhodnocujú v súlade so všeobecným trestným poriadkom.

- Preto sú elektronické dôkazy v trestnom konaní vo všeobecnosti prípustné, ak sa získali zákonným spôsobom a sú pre príslušné konanie relevantné. Vzťahuje sa to aj na elektronické dôkazy získané mimo štátu spoluprácou s členskými štátmi prostredníctvom medzinárodnej vzájomnej právnej pomoci alebo priamou spoluprácou s poskytovateľmi internetových služieb.

- Neexistencia právnych predpisov týkajúcich sa metodiky na zhromažďovanie elektronických dôkazov a ich predkladanie pred súdom, ako sa uvádza v jednej individuálnej správe, by v zásade nemala brániť v účinnom stíhaní prípadov počítačovej kriminality, keďže prípustnosť elektronických dôkazov patrí do pôsobnosti všeobecných právnych predpisov o dôkazoch.

- V niekoľkých členských štátoch sú elektronické dôkazy rovnako ako väčšina tradičných dôkazov prípustné na súde a vyhodnocované sudcom v súlade so zásadou slobodného hodnotenia dôkazov. To znamená, že všetko, čo môže slúžiť ako dôkaz v konaní, možno v zásade predložiť súdu, ktorý v každom jednotlivom prípade rozhodne, akú hodnotu má daný dôkaz. Podľa záverov hodnotenia to možno považovať za osvedčený postup.

- Ak sú naopak pravidlá prípustnosti dôkazov dosť prísne, môže to vytvárať prekážky pre elektronické dôkazy, najmä ak sa získali z inej krajiny, napr. prostredníctvom žiadostí o vzájomnú právnu pomoc.

- Polícia môže mať, často na základe povolenia od sudcu, v súlade s konkrétnymi medzinárodnými zmluvami prístup k údajom uloženým na mieste prehliadky, ako aj k vzdialeným údajom alebo údajom nachádzajúcich sa v zahraničí. Ak si objasnenie skutkových okolností relevantných z hľadiska trestného konania vyžaduje uchovanie uložených počítačových údajov, ktoré sa majú zapísať do trestných spisov, vrátane prevádzkových údajov uložených prostredníctvom počítačového systému alebo na akomkoľvek nosiči údajov, (napr. CD, DVD nosiče, mobilné telefóny), dané predmety sa zvyčajne zaistia na základe príslušných pravidiel trestného poriadku členských štátov.

- Ak sa elektronický dôkaz nachádza na internete, alebo je v držbe poskytovateľov služieb, je priama spolupráca s nimi dôležitá, aby sa získali potrebné údaje a prijali opatrenia, ktorých cieľom je zabrániť strate, zničeniu alebo zmene údajov. Nie všetky členské štáty však majú možnosť priameho prístupu k elektronickým dôkazom nachádzajúcim sa v inej krajine alebo v cloude, a preto by mali v takýchto prípadoch dodržiavať postupy vzájomnej právnej pomoci.

- Podľa záverov hodnotenia by súčasné postupy vzájomnej právnej pomoci mali byť rýchlejšie a účinnejšie s cieľom riešiť tieto problémy, pričom orgány, ktoré vedú vyšetrovanie, musia mať možnosť posielať žiadosti veľmi rýchlo a do mnohých rôznych krajín.

- V niektorých členských štátoch umožňujú vnútroštátne právne predpisy získať informácie priamo od zahraničných poskytovateľov, ak je to povolené aj podľa práva štátu, v ktorom je poskytovateľ usadený. Spoločný rámec na výmenu údajov o používateľoch a nové prístupy na úrovni EÚ k právomoci presadzovať právo sú, okrem iného, predmetom práve prebiehajúcej činnosti na úrovni EÚ, ktorá sa vykonáva na základe záverov Rady o zlepšení trestnej justície v kybernetickom priestore z 9. júna 2016.

- Postupy a podoby sprístupnenia elektronických dôkazov zaistených v rámci vyšetrovania ako súčasť spisu v podobe, ktorou sa umožní preskúmanie zo strany prokurátorov a sudcov, sa v jednotlivých členských štátoch odlišujú.

- Zdá sa, že zaistenie počítačového hardvéru, ktorý obsahuje elektronické dôkazy, nie je najlepšou možnosťou, keďže môže byť problematické, aby obeť počítačovej kriminality akceptovala stratu svojho digitálneho zariadenia počas vyšetrovania.

- V záujme zabezpečenia elektronických dôkazov však možno uložené údaje skopírovať (vyhotoviť presnú kópiu) na iné pamäťové médium (napríklad DVD, pevný disk) a sprístupniť v tejto podobe, pričom čitateľné údaje (napríklad textové správy) alebo obrazové súbory možno vytlačiť a sprístupniť aj v papierovej podobe.

- Ten istý postup sa zvyčajne používa pre elektronické dôkazy zhromaždené zo zahraničia. Ak však krajina, ktorá pomohla získať dôkazy, stanoví osobitné podmienky, polícia a prokurátori ich budú musieť dodržiavať.

- Ak prokurátor a sudcovia, ktorí musia narábať s elektronickými dôkazmi v súdnych konaniach, dostanú tieto dôkazy v podobe, ktorá si na účely ich sprístupnenia a vyhodnotenia vyžaduje použitie IT zariadení, a preto vyvstane potreba špecifických odborných znalostí, a to aj na účely analýzy pravosti elektronických dôkazov, možno o radu požiadať forenzného experta.

- Podľa zistení vyplývajúcich z hodnotenia by špeciálny vyspelý hardvér a softvér na lepšiu identifikáciu a získavanie elektronických dôkazov umožnil orgánom členských štátov pracovať a spolupracovať s porovnateľnými elektronickými dôkazmi.

ODPORÚČANIA

- ***Členské štáty by mali mať k dispozícii primeraný vyspelý hardvér a softvér na identifikáciu a získavanie elektronických dôkazov, ktoré orgánom členských štátov umožnia, aby pracovali a spolupracovali s porovnateľnými elektronickými dôkazmi.***

- ***Členské štáty by mali zabezpečiť, aby ich vnútroštátne procedurálne právne predpisy boli dostatočne pružné na to, aby uľahčovali prípustnosť elektronických dôkazov vrátane dôkazov získaných z inej krajiny, napríklad prostredníctvom postupov vzájomnej právnej pomoci.***

- ***Členské štáty by mali zvážiť nadviazanie a udržiavanie neustáleho dialógu so súkromným sektorom, za prípadnej účasti Eurojustu a Európskej justičnej siete na boj proti počítačovej kriminalite, a prediskutovanie metodík na zabezpečenie, aby sa zhromažďovanie elektronických dôkazov uskutočňovalo tak, aby boli prípustné na súdoch.***

- ***EÚ a jej členské štáty by mali v dôsledku prebiehajúceho expertného procesu v oblasti prístupu k elektronickým dôkazom zvážiť vytvorenie rámca EÚ, ktorým sa stanovia pravidlá prístupu k údajom v držbe poskytovateľov služieb na účely presadzovania práva. Takýmto rámcom s jasnými pravidlami a povinnosťami by sa mali upraviť vzťahy medzi OPP a poskytovateľmi internetových služieb.***

XIII – „CLOUD COMPUTING“

HLAVNÉ ZISTENIA A ZÁVERY

- Veľký počet členských štátov označil za oblasť, ktorá je problematická z hľadiska vyšetrovania a stíhania, počítačovú kriminalitu, ktorej súčasťou sú údaje „v cloude“.

- Niektoré členské štáty nemali v čase hodnotenia žiadne skúsenosti s vyšetrovaním počítačovej kriminality tohto druhu, a preto sa otázka právomoci v oblasti ukladania údajov v cloude ešte pred vnútroštátnymi súdmi neotestovala, čo by mohlo znamenať, že isté množstvo počítačových trestných činov zostáva v praxi nestíhané; uznali však, že takýmto situáciám budú v budúcnosti nevyhnutne čeliť.

- Tento jav môže v budúcnosti viesť k závažným problémom, pretože riešenia v cloude sú čoraz populárnejšie a používanie cloudu na ukladanie dát a poskytovanie služieb sa čoraz viac stáva bežnou praxou nielen u právnických a fyzických osôb, ale aj u páchateľov.

- Vzhľadom na používané technológie a úložnú kapacitu serverov, ako aj úspory z rozsahu, ktoré s tým súvisia, sa údaje neustále pohybujú po celom svete a môžu byť fragmentované, pričom sa spoja len pri ich získaní. Osobitným problémom pri riešení trestných činov týkajúcich sa cloudu je preto stanoviť skutočné fyzické miesto, kde sa trestný čin spáchal, a zistiť to môže byť ťažké, veľmi komplikované a zdĺhavé. OPP preto nemôžu ľahko nájsť informácie a servery, na ktorých sú uložené údaje, v cloude a získať k nim prístup.

- Nedostatok informácií spôsobuje, že vyšetrovatelia nemôžu objavovať digitálne stopy, a môže sťažiť identifikáciu páchateľa, času a miesta spáchania trestného činu a nástrojov, prostredníctvom ktorých bol trestný čin spáchaný, v dôsledku čoho môže počítačová kriminalita zostať nepotrestaná, pričom situácie, v ktorých sa ľudia stali obeťami, sa môžu opakovať znova a znova.

- Aj poskytovatelia cloudových úložísk môžu mať problémy pri hľadaní skutočného (územného) umiestnenia údajov; dokonca ani vlastníci údajov často nevedia, kde sa nachádzajú.

- Keďže na trestné činy týkajúce sa údajov v cloude sa môže vzťahovať právomoc niekoľkých členských štátov alebo aj právomoc tretej krajiny, cloud computing predstavuje vzhľadom na zvrchovanosť štátov a zásadu teritoriality problém nielen na vnútroštátnej, ale aj na medzinárodnej úrovni.

- Aj v prípade, že sa zistí lokalita, vnútroštátne právne predpisy v niektorých členských štátoch neumožňujú extrateritoriálnu právomoc alebo počítačové trestné činy, ktorých súčasťou sú údaje uložené v cloude možno stíhať len vtedy, ak sú takéto údaje dostupné z dotknutých členských štátov.

- V prípade, keď právomoc vo veci konštatujú dva alebo viac členských štátov, môže dôjsť ku sporu o právomoc, pokiaľ ide o vydávanie príkazov na zaistenie elektronických dôkazov; v takýchto prípadoch môžu členské štáty vyriešiť takéto konflikty tým, že využijú služby Eurojustu a spoločných vyšetrovacích tímov.

- V hodnotení sa uznávajú dve základné možnosti, ako získať údaje uložené v cloude: priamy prístup k obsahu takýchto profilov a pamäťových zariadení možno jednak získať prostredníctvom súhlasu používateľa/majiteľa profilu alebo konta. Alebo, ak možno identifikovať miesto, kde sa informácie nachádzajú, môžu sa použiť aj postupy vzájomnej právnej pomoci, ktoré sú však často zdĺhavé a neefektívne.

- Ďalšia možnosť, ktorou je nariadiť priamo poskytovateľom, aby poskytli určité informácie, sa často v praxi ukáže ako veľmi problematická, keďže existujú poskytovatelia, ktorí nespolupracujú so zahraničnými OPP a neodpovedajú na každú žiadosť.

- S cieľom prekonať tieto ťažkosti sa v hodnotení zdôrazňuje, že by sa mohli zaviesť osobitné pravidlá s niektorými poskytovateľmi cloudových služieb (napr. Google, Yahoo atď.) na skrátenie lehôt a získavanie informácií vo formátoch, ktoré sú prípustné na súde. Určité opatrenia na prekonanie tohto problému sa v súčasnosti posudzujú na úrovni EÚ v rámci prebiehajúceho expertného procesu v oblasti elektronických dôkazov, ako napríklad jednotné kontaktné miesta na strane členských štátov aj poskytovateľov služieb a právny rámec EÚ na vyšetrovacie opatrenia adresované poskytovateľom služieb, ktoré orgánom umožňujú požiadať poskytovateľa služieb v inom členskom štáte o zverejnenie informácie o používateľovi atď. („žiadosť o predloženie“) alebo ho k tomu prinútiť („príkaz na predloženie“).

- Podľa Dohovoru o počítačovej kriminalite sú úkony na cezhraničnej úrovni možné len vo veľmi obmedzenom počte prípadov, napr. so zákonným súhlasu osoby, ktorá má zákonnú právomoc zverejňovať údaje, v prípade, keď právomoc je známa. V prípadoch, keď sú údaje umiestnené mimo územia zmluvných strán, nie sú tieto ustanovenia uplatniteľné.

- Vzhľadom na uvedené skutočnosti nebolo zatiaľ možné vyriešiť problém cloudových úložísk primerane. Rôzne možnosti konať nezávisle alebo prostredníctvom vzájomnej právnej pomoci, ktoré poskytuje medzinárodné právo, sa ukázali pri vyšetrovaní počítačovej kriminality, ktorej súčasťou sú údaje v cloude, ako obmedzené.

- Podľa záverov hodnotenia by sa malo zvážiť, ako zlepšiť prax so zámerom zabezpečiť účinné vyšetrovanie a stíhanie počítačovej kriminality, ktorej súčasťou sú údaje v cloude, a zároveň zohľadniť ťažkosti, ktoré vyplývajú z prípadných pozitívnych kompetenčných sporov.

- Na tento účel by mohlo byť užitočné zvážiť riešenie existujúcich príslušných právnych rámcov a/alebo vyšetrovacích otázok s cieľom vytvoriť jasné pravidlá a postupy týkajúce sa počítačovej kriminality, ktorej súčasťou sú údaje uložené v cloude.

- V kontexte hodnotenia sa vyzdvihla aj účasť členských štátov na medzinárodných fórach (napríklad vo výbore Dohovoru o počítačovej kriminalite), na ktorých sa diskutuje o riešení týchto otázok.[6]

- Jeden členský štát predložil návrhy týkajúce sa prístupu k údajom uloženým v cloude, ako napríklad možnosť virtuálneho vyhľadávania v dátových centrách nachádzajúcich sa v iných krajinách bez toho, aby sa najprv muselo identifikovať fyzické umiestnenie serverov, a/alebo zavedenie povinnosti poskytovateľov dátových služieb poskytovať OPP heslá s cieľom umožniť im prístup k údajom.

[6] Výbor Dohovoru o počítačovej kriminalite prijal mandát na rokovania o dodatkovom protokole na riešenie týchto otázok.

ODPORÚČANIA

- ***Členské štáty by mali zvážiť možnosť uzavrieť osobitné dohody s najdôležitejšími poskytovateľmi cloudových služieb na skrátenie lehôt a získavanie údajov, ktoré sú prípustné na súde.***

- ***EÚ by mala naďalej riešiť výzvy, ktoré prináša cloud computing, s cieľom nájsť riešenia, ktorými by sa mohla zvýšiť kapacita na vyšetrovanie počítačovej kriminality, a to aj v kontexte prebiehajúceho expertného procesu o elektronických údajoch.***

XIV – UCHOVÁVANIE ÚDAJOV Z ELEKTRONICKÝCH KOMUNIKÁCIÍ

HLAVNÉ ZISTENIA A ZÁVERY

- Ukončením platnosti smernice 2006/24/ES rozsudkom Súdneho dvora z 8. apríla 2014 (spojené veci C-293/12 a C-594/12, "Digital Rights Ireland a Seitlinger a i.") vznikla právna neistota, najmä pokiaľ ide o právny štatút vnútroštátnych transpozičných predpisov. Členské štáty majú rozdielne prístupy k rozsudku, zachovaniu, zmene, náhrade alebo zrušeniu transpozičných právnych predpisov alebo k ukončeniu ich platnosti vnútroštátnymi súdmi.

- Viaceré členské štáty zdôraznili negatívne dôsledky uvedeného rozsudku na účinnosť vyšetrovania a stíhania trestných činov na vnútroštátnej úrovni, najmä pokiaľ ide o spoľahlivosť a prípustnosť dôkazov na súdoch na základe zhromažďovania údajov z elektronických komunikácií, ako aj na cezhraničnú justičnú spoluprácu medzi členskými štátmi a na medzinárodnej úrovni (obmedzené kapacity na poskytovanie a získavanie dôkazov). Neuchovávanie údajov alebo ich uchovávanie len na obmedzený čas sťažuje alebo dokonca znemožňuje zabezpečiť elektronické dôkazy v členských štátoch.

- Viaceré členské štáty zdôraznili, že spoločný prístup na úrovni EÚ by predstavoval pridanú hodnotu, a to vrátane možnosti nového legislatívneho rámca, ktorým by sa mohli harmonizovať podmienky a lehoty uchovávania údajov v členských štátoch.

- Medzitým Súdny dvor vo svojom rozsudku v spojených veciach C-203/15 a C-698/15 z 21. decembra 2016 („Tele 2 a Watson“) uviedol, že vnútroštátne právne predpisy, ktorými sa stanovuje všeobecné uchovávanie prevádzkových a lokalizačných údajov, ide nad rámec toho, čo je potrebné, a spresnil kritériá a podmienky, ktoré musia spĺňať vnútroštátne režimy uchovávania údajov v členských štátoch.

- V súčasnosti prebieha spoločný proces úvah, do ktorého sú zapojené inštitúcie EÚ a členské štáty, ktorým sa skúma problém uchovávania údajov s cieľom identifikovať právne a praktické riešenia súvisiacich výziev, ktoré vyplývajú z judikatúry Súdneho dvora.

ODPORÚČANIA

- ***Členské štáty a inštitúcie EÚ by mali viesť spoločný proces úvah s cieľom identifikovať právne a praktické riešenia problému uchovávania údajov z elektronických komunikácií na vnútroštátnej úrovni a na úrovni EÚ, berúc do úvahy zásady zakotvené v nedávnej judikatúre SD.***

XV – OPATRENIA PROTI DETSKEJ PORNOGRAFII A SEXUÁLNEMU ZNEUŽÍVANIU DETÍ ONLINE

HLAVNÉ ZISTENIA A ZÁVERY

- V čase hodnotenia väčšina členských štátov už transponovala smernicu Európskeho parlamentu a Rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii. Súčasný stav transpozície tejto smernice do vnútroštátnych opatrení možno nájsť na tejto adrese: http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32011L0093

- Vzhľadom na vývoj v spoločnosti a v technológiách, ktorým sa zvýšili možnosti komunikácie a šírenia informácií, ako aj možnosti páchania trestných činov online, sa v posledných rokoch výrazne zvýšilo sexuálne zneužívanie detí na internete (nadväzovanie stykov s nekalými úmyslami – „grooming“, posielanie nevyžiadaných správ so sexuálnym obsahom, počítačové šikanovanie atď.). V záujme účinného boja proti týmto formám trestnej činnosti sa v členských štátoch vykonáva široká škála preventívnych a donucovacích opatrení, ktoré zahŕňajú verejný aj súkromný sektor.

- V niektorých členských štátoch existuje vnútroštátna databáza zameraná na identifikáciu obetí na účely boja proti sexuálnemu zneužívaniu detí, alebo sa v čase hodnotenia práve vytvárala. Vo väčšine členských štátov však takáto vnútroštátna databáza neexistuje alebo v čase hodnotenia nebola dostatočne rozvinutá. V týchto prípadoch OPP využívajú len medzinárodné databázy a nástroje, najmä medzinárodnú databázu sexuálneho vykorisťovania detí Interpolu (ICSE-DB), ktorá je naozaj významným spravodajským a vyšetrovacím nástrojom na identifikáciu obetí a páchateľov, keďže umožňuje špecializovaným vyšetrovateľom výmenu údajov po celom svete.

- V jednom členskom štáte, ak polícia nemôže identifikovať obeť pomocou databázy, ale má dôvodné podozrenie o možnej totožnosti dieťaťa, pošle jednu alebo viac fotografií školám na identifikáciu, čo možno považovať za osvedčený postup.

- V členských štátoch existujú rozdielne prístupy k predchádzaniu opakovanej viktimizácii detí: okrem blokovania a/alebo odstraňovania detskej pornografie ide o tvorbu zoznamov nebezpečných médií, ktoré sa považujú za škodlivé pre maloletých, obmedzenie kontaktu s páchateľom, usmerňovanie a poradenstvo, ktoré obetiam poskytujú mimovládne organizácie, ako aj osobitné opatrenia na ochranu obetí a svedkov sexuálneho zneužívania detí pred negatívnymi následkami počas trestného konania.

- V niekoľkých členských štátoch neexistujú žiadne osobitné opatrenia zamerané na predchádzanie opakovanej viktimizácii detí, ale na tento účel sa spolupracuje s mimovládnymi organizáciami, špecializovanými nepolicajnými orgánmi a inštitúciami so zodpovednosťou v oblasti ochrany maloletých alebo s časťou platformy EMPACT zodpovednou za počítačovú kriminalitu, konkrétne prioritnú oblasť „online zneužívanie detí“.

- V členských štátoch sa zaviedli rôzne právne, technické, organizačné a informačné opatrenia s cieľom riešiť sexuálne vykorisťovanie/zneužívanie online, posielanie nevyžiadaných správ so sexuálnym obsahom, počítačové šikanovanie a sexuálnu turistiku zameranú na deti. Niekoľko členských štátov má špecializované jednotky alebo špecializovaných príslušníkov pracujúcich výlučne s materiálmi týkajúcimi sa sexuálneho zneužívania detí s cieľom identifikovať deti a páchateľov a viesť vyšetrovania. Osvedčeným postupom v jednom členskom štáte je posudzovanie pri nástupe do zamestnania a každoročné psychologické vyšetrenia špecializovaných príslušníkov polície pôsobiacich v tejto oblasti.

- Všetky členské štáty zaviedli v rôznom rozsahu preventívne opatrenia zamerané na podporu bezpečného používania internetu maloletými, často pod záštitou štátnych orgánov a v spolupráci so špecializovanými jednotkami a mimovládnymi organizáciami, ktoré pracujú s deťmi. Niektoré projekty v tejto oblasti spolufinancuje EÚ, ako je Európska sieť pre bezpečnejší internet (INSAFE) v rámci programu Európskej komisie Bezpečnejší internet.

- Preventívne opatrenia zahŕňajú napríklad projekty odbornej prípravy a informačné kampane zamerané na zvyšovanie povedomia a odbornú prípravu cieľových skupín (študenti, rodičia, vzdelávací pracovníci a iné skupiny) v oblasti hlavných potenciálnych rizík, ktorým maloleté osoby čelia pri používaní internetu, a rozvoja jeho zodpovedného využívania. Za osvedčený postup sa považujú moderné techniky, ktoré sa používajú v jednom členskom štáte a spočívajú v tom, že deti učia deti. V niektorých členských štátoch tieto činnosti organizuje aj polícia alebo sa na nich podieľa.

- Silným nástrojom na predchádzanie sexuálnemu zneužívaniu detí, najmä pre detí a mladistvých, je aj mediálne vzdelávanie a v niektorých členských štátoch sa informácie o bezpečnom správaní na internete určené deťom uverejňujú na špecializovaných webových stránkach. Ostatné členské štáty vypracovali brožúry alebo príručky alebo „školských sprievodcov“ o bezpečnom a efektívnom používaní internetu, počítačovom šikanovaní atď.

- Väčšina členských štátov má zavedenú službu horúcej linky, na ktorej sa môže anonymne oznamovať obsah zahŕňajúci sexuálne zneužívanie detí a ktorá často pôsobí aj ako linka pomoci pre deti, dospievajúcich a rodičov a poskytuje im anonymnú a bezplatnú pomoc cez telefón a online (webové stránky alebo platformy), a to napr. aj o tom, ako niečo nahlásiť polícii. Európska online platforma – www.reportchildsextourism.eu – obsahuje všetky vnútroštátne núdzové linky v Európe.

- Väčšina členských štátov má trestnoprávne úpravy, v ktorých sa stanovujú trestné činy a tresty pre páchateľov sexuálnej turistiky zameranej na deti, alebo uplatňujú iné opatrenia vrátane opatrení proti propagácii príležitostí na zneužívanie a sexuálnej turistiky zameranej na deti, ako je stanovené v článku 21 smernice 2011/93/EÚ. Opatrenia zamerané na zlepšenie odhaľovania tejto špecifickej formy trestnej činnosti zahŕňajú systémy monitorovania alebo oznamovania cestujúcich páchateľov sexuálnych trestných činov, opatrenia zahŕňajúce odvetvie cestovného ruchu a zahraničné služby, vysielanie styčných dôstojníkov do zahraničia, konfiškáciu cestovného pasu osoby odsúdenej za zneužívanie detí atď.

- Všeobecné opatrenia na včasné odhaľovanie sexuálneho zneužívania detí na internete zahŕňajú napríklad hliadkovanie na internete a vyšetrovania v utajení, ktoré sa ukazujú ako účinný nástroj v boji proti sexuálnemu vykorisťovaniu detí, ktoré sa odohráva v reálnom čase cez internet, ako aj softvérové filtre, ktoré sa však neuplatňujú vo všetkých členských štátoch, alebo často nie sú pre poskytovateľov internetových služieb povinné.

- Donucovacie opatrenia v prípadoch sexuálneho zneužívania detí na internete, ktoré zahŕňajú blokovanie prístupu, odstraňovanie obsahu alebo odstraňovanie webových stránok, sa vo všetkých členských štátoch neuplatňujú rovnako, a to aj pokiaľ ide o procesné podmienky týkajúce sa toho, či je pred takýmito opatreniami polície alebo na ich potvrdenie potrebný súdny príkaz.

- Vo väčšine členských štátov sa prijímajú právne a praktické opatrenia s cieľom natrvalo odstrániť z internetu online audiovizuálny materiál zobrazujúci sexuálne zneužívanie detí. Prístup spočívajúci vo vymazávaní možno považovať za opatrenie na riešenie tohto problému, ktorým však nemožno predchádzať tomu, aby neboli fotografie/videá maloletých dostupné na iných internetových stránkach. Iné členské štáty využívajú aj alebo len prístup spočívajúci v blokovaní prístupu, ktorý pozostáva z blokovania prístupu k webovým stránkam obsahujúcim detskú pornografiu, čím sa takýto materiál dočasne zneprístupní.

- Ak je materiál uložený na serveroch nachádzajúcich sa v zahraničí, zvyčajne sa použijú medzinárodné kanály, najmä Europol a jeho systém na zabezpečenú výmenu informácií SIENA alebo Interpol a jeho iniciatíva spočívajúca v blokovaní prístupu; horúce linky sa tiež môžu obrátiť na INHOPE (Medzinárodné združenie internetových horúcich liniek), ktoré zabezpečuje, aby sa detská pornografia určená jednému štátu, ale uložená v zahraničí, mohla odstrániť z internetu.

- V niekoľkých členských štátoch sa stránky s detským pornografickým obsahom blokujú a zneprístupňujú bez ohľadu na to, či sa nachádzajú na území EÚ alebo mimo neho, čo sa považuje za osvedčený postup.

- Na vykonávanie uvedených opatrení je dôležitá dobrá spolupráca medzi všetkými príslušnými zainteresovanými stranami, ako sú OPP, horúce linky, mimovládne organizácie a poskytovatelia služieb. V niektorých členských štátoch sú poskytovatelia služieb povinní prijať primerané kroky na znemožnenie používania takýchto materiálov, a to blokovaním prístupu na internetové stránky alebo odstraňovaním obsahu z nich, zatiaľ čo v iných členských štátoch sa takáto povinnosť vo vnútroštátnych právnych predpisoch neukladá, avšak uvedené opatrenia sa môžu prijímať v jednotlivých prípadoch na základe súdneho príkazu.

- Spolupráca v členských štátoch medzi OPP a domácimi poskytovateľmi služieb je vo všeobecnosti dobrá; poskytovatelia často odstraňujú detskú pornografiu okamžite a dobrovoľne, na základe oznámenia OPP, aj keď nie sú povinní tak urobiť. Ako príklad osvedčených postupov sa uvádza nástroj používaný v jednom členskom štáte, ktorého rozhranie obsahuje rovnakú ikonu pre všetkých poskytovateľov na oznamovanie webových stránok, na ktorých sa nachádza detská pornografia.

ODPORÚČANIA

- ***Členské štáty, ktoré tak zatiaľ neurobili, by mali vytvoriť národnú databázu na identifikáciu obetí v rámci boja proti sexuálnemu zneužívaniu detí alebo zabezpečiť prístup do databázy Interpolu. Členské štáty by tiež mali zvážiť vytvorenie vnútroštátnej siete na výmenu informácií o identifikácii obetí.***

- ***Členské štáty, ktoré tak zatiaľ neurobili, by mali zvážiť vypracovanie konkrétnych opatrení na predchádzanie opakovanej viktimizácii detí vrátane opatrení na ochranu obetí a svedkov sexuálneho zneužívania detí pred negatívnymi následkami počas trestného konania.***

- ***Členské štáty by mali zabezpečiť dobre fungujúcu spoluprácu medzi všetkými príslušnými zainteresovanými stranami s cieľom účinne bojovať proti trestným činom zameraným na deti na internete, a zvážiť zavedenie povinnosti pre poskytovateľov služieb, aby prijali vhodné opatrenia, ako je blokovanie prístupu, odstraňovanie obsahu alebo odstraňovanie webových stránok.***

XVI – MECHANIZMUS REAKCIE NA KYBERNETICKÉ ÚTOKY

HLAVNÉ ZISTENIA A ZÁVERY

- V čase hodnotenia už bola smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy transponovaná vo väčšine členských štátov. Súčasný stav transpozície tejto smernice do vnútroštátnych opatrení možno nájsť na tejto adrese: http://eur-lex.europa.eu/legal-content/SK/NIM/?uri=CELEX:32013L0040&qid=1506328148248

- Počítačové útoky sú meniaca sa hrozba; metódy a nástroje používané na vykonávanie takýchto útokov sú čoraz sofistikovanejšie a spektrum kybernetických útokov ohrozujúcich kybernetický priestor je veľmi široké. Hodnotením sa predovšetkým ukázalo, že došlo k významnému nárastu útokov využívajúcich ransomware – škodlivého softvéru, ktorý blokuje prístup k údajom, kým sa nezaplatí výkupné.

- Niektoré členské štáty sa v prípade kybernetických útokov spoliehajú na technickú pomoc zo strany súkromného sektora, keďže súkromné spoločnosti majú dobré odborné znalosti a pracujú s lepším vybavením a nižšími nákladmi. Okrem toho môžu pomáhať zhodnocovať dôsledky útokov na infraštruktúru a vypracúvať komplexné posúdenia situačného povedomia.

- V niektorých členských štátoch už existuje štruktúrovaný prístup angažovanosti viacerých agentúr, v niektorých prípadoch na základe verejno-súkromného partnerstva, zatiaľ čo v iných členských štátoch sa takýto prístup zatiaľ dostatočne nerozvinul alebo chýba, pričom mechanizmus koordinácie reakcie na kybernetické útoky funguje prevažne na základe neformálnej spolupráce.

- V čase hodnotenia už väčšina členských štátov zriadila svoju národnú jednotku CSIRT alebo boli v procese jej zriadenia, zatiaľ čo niekoľko členských štátov tak ešte neurobilo.

- Medzi hlavné úlohy jednotiek CSIRT patrí monitorovanie kybernetických incidentov a reakcia na ne, poskytovanie včasných varovaní, upozornení a analýz rizík a incidentov, ako aj nadväzovanie spolupráce so súkromným sektorom.

- V niektorých členských štátoch ide úloha vnútroštátnych jednotiek CSIRT ešte nad rámec týchto povinností, pretože spravujú databázy o hrozbách a incidentoch, podporujú výmenu informácií medzi rozličnými subjektmi, poskytujú poradenstvo a pomoc v oblasti ochrany počítačových systémov verejného a súkromného sektora, proaktívne vykonávajú činnosti na zníženie rizika incidentov v oblasti počítačovej bezpečnosti, venujú sa zvyšovaniu informovanosti a poskytujú odbornú prípravu, konajú ako sprostredkovateľ medzi súkromným sektorom, akademickou obcou a políciou a predstavujú vnútroštátne kontaktné miesta pre medzinárodnú spoluprácu.

- Vládne jednotky CSIRT majú na starosti najmä riadenie kríz a reakcie na kybernetické hrozby a incidenty týkajúce sa verejného sektora, ale v mnohých prípadoch aj kritickej infraštruktúry, a v obmedzených prípadoch aj súkromnej sféry, na ktoré sa však zvyčajne vzťahujú právomoci iných jednotiek CSIRT v súkromnom sektore.

- V niektorých členských štátoch vykonávajú vládne jednotky CSIRT koordinačné a dozorné funkcie pre iné príslušné zainteresované strany, čo sa javí v praxi ako užitočné, najmä v tých členských štátoch, v ktorých je mechanizmus reakcie na kybernetické útoky pomerne zložitý a/alebo v ktorých vo verejnom aj súkromnom sektore existuje súbežne značný počet rôznych jednotiek CSIRT.

- Jednotky CSIRT nemajú voči súkromným subjektom právomoci OPP, ale pokiaľ ide o útoky trestnej povahy (nie všetky kybernetické incidenty sú trestné činy), zohrávajú dôležitú úlohu pri podpore vyšetrovaní, pretože môžu pomôcť pri poskytovaní informácií a zabezpečovaní dôkazov. Preto je na tento účel veľmi dôležité, aby jednotky CSIRT dobre spolupracovali s OPP, pretože účinné získavanie informácií a dôkazov je nevyhnutné pre vyšetrovanie kybernetických útokov vzhľadom na to, že elektronické údaje sú veľmi dynamické a ľahko sa môžu stratiť. Ak je to potrebné, do vyšetrovania kybernetických incidentov sa môžu zapojiť spravodajské inštitúcie.

- Podľa smernice EÚ 2016/1148 (smernica NIS), ktorá sa má transponovať do vnútroštátnych právnych predpisov do 9. mája 2018, by členské štáty mali mať fungujúce jednotky CSIRT, ktoré spĺňajú určité požiadavky s cieľom zaručiť účinnú spôsobilosť na riešenie incidentov a rizík a zabezpečiť efektívnu spoluprácu na úrovni Únie.

- Digitálnu odolnosť nemôže dosiahnuť len vláda samotná; dôležitú úlohu zohráva aj súkromný sektor, najmä prevádzkovatelia základných služieb, informačných systémov a sietí, ktorí sú priamo zapojení do riadenia rizík a zaisťovania bezpečnosti svojich sietí a služieb.

- Podľa smernice NIS členské štáty zabezpečia, aby prevádzkovatelia základných služieb chránili bezpečnosť svojich sietí a informačných systémov a bezodkladne oznamovali príslušnému orgánu alebo jednotke CSIRT každý incident, ktorý má závažný vplyv na poskytovanie služby. Po tom, ako sa smernica o bezpečnosti sietí a informačných systémov v plnej miere vykoná, budú subjekty, ktoré spĺňajú kritériá vymedzenia pojmu „prevádzkovateľ základných služieb“, povinné oznamovať incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú.

- V čase hodnotenia už bol v niektorých členských štátoch súkromný sektor povinný oznamovať kybernetické incidenty OPP. V určitých prípadoch však bola táto povinnosť obmedzená na určité odvetvia súkromného sektora alebo na určité typy incidentov, pričom za nedodržiavanie oznamovacej povinnosti sa neukladali žiadne sankcie.

- V iných prípadoch sa zase oznamovanie incidentov uskutočňuje dobrovoľne, napriek tomu, že formálna povinnosť neexistuje; ako sa však zdôraznilo v niektorých správach, z dôvodu neochoty poskytovateľov služieb vystaviť sa škodám, ktoré môže utrpieť ich dobré meno, incidenty často neoznamujú. Podľa zistení vyplývajúcich z hodnotenia existuje reálne nebezpečenstvo, že bez povinnosti oznamovať incidenty ostane väčšina kybernetických incidentov zo strany orgánov nepovšimnutá. Ako sa zdôrazňuje v jednej individuálnej správe, OPP môžu poukázať na to, že vyšetrovanie môže byť tajné a dobré výsledky možno dosiahnuť aj bez poškodenia dobrého mena, a podnecovať tak k oznamovaniu incidentov.

- Systém povinného oznamovania, najmä v prípade závažných trestných činov, je dôležitý nielen na účely presadzovania práva, konkrétne s cieľom uľahčiť rýchle a úplné posúdenie situácie a rýchlejšie vykonávanie cielených protiopatrení, ale je tiež užitočný, pretože poskytuje orgánom lepší prehľad o hrozbách, umožňuje zostaviť komplexnú štatistiku o počte kybernetických bezpečnostných incidentov a prijímať vhodné preventívne opatrenia. Hodnotitelia preto považujú zavedenie riadneho právneho rámca, ktorým by sa ustanovila oznamovacia povinnosť, ako je to v niektorých členských štátoch, za osvedčený postup.

- Aby sa zabezpečila vysoká úroveň kybernetickej bezpečnosti a zodpovedné správanie lídrov, vývojárov a používateľov systémov, bezpečnostná situácia sa musí zlepšiť, a preto je dôležitým prvkom účinného prístupu ku kybernetickej bezpečnosti zvyšovanie informovanosti na všetkých úrovniach, ako sa deje v určitých členských štátoch.

- Keďže niekedy majú kybernetické hrozby a útoky cezhraničný rozmer, ako užitočná platforma na zlepšenie spolupráce medzi členskými štátmi, príslušnými inštitúciami a agentúrami a partnermi zo súkromného sektora na tvorbu a šírenie softvéru na boj proti škodlivému softvéru a obranu proti útokom na siete infraštruktúry sa javí platforma EMPACT.

- Za zmienku stojí úzka spolupráca medzi jednotkami CSIRT troch pobaltských štátov, ktoré v novembri 2015 podpísali memorandum o porozumení a zaviazali sa zintenzívniť spoluprácu v oblasti kybernetickej bezpečnosti a ochrany informačných systémov a sietí.

- Pri riešení kybernetických útokov mimo EÚ sa používajú formálne kanály vzájomnej právnej pomoci. Pretože však v prípade počítačovej kriminality zohráva dôležitú úlohu čas (z dôvodu nestálosti údajov), na účely rýchlejšej a efektívnejšej spolupráce sa využíva aj spolupráca a výmena informácií priamo medzi policajnými zbormi alebo cez Europol a Interpol. Niektoré členské štáty využívajú aj sieť kontaktných miest G7 – 24/7.

- Digitálna agenda pre Európu podnecuje členské štáty k tomu, aby do roku 2012 zriadili spoľahlivo fungujúcu sieť jednotiek CSIRT na vnútroštátnej úrovni, ktorá pokryje celú Európu. Európska komisia vyzvala členské štáty, aby posilnili spoluprácu medzi existujúcimi národnými jednotkami CSIRT a rozšírili existujúce mechanizmy spolupráce, ako je napríklad Európska skupina vládnych jednotiek CSIRT.

- Prostredníctvom celosvetových sietí jednotiek CSIRT, ako je IWWN, FIRST, Európska sieť vládnych jednotiek CSIRT a TF-CSIRT sa uskutočňuje komunikácia a spolupráca aj na medzinárodnej úrovni, a to s cieľom spolupracovať v oblasti kybernetických incidentov vrátane vzájomnej podpory pri riadení IT situácií a krízovom riadení v oblasti IT, keďže tieto siete vykonávajú pravidelné cvičenia. Siete jednotiek CSIRT môžu mať čiastočne podobné zameranie, napr. v prípade jednotiek CSIRT v rámci štátnej správy/orgánov, a čiastočne odlišné, napr. v prípade tímov z oblasti podnikania, vedy a orgánov.

ODPORÚČANIA

- ***S cieľom zaručiť primeranú úroveň ochrany a bezpečnosti národného kybernetického priestoru by členské štáty mali zabezpečiť účinný inštitucionálny rámec založený na prístupe zahŕňajúcom viacero agentúr, ktorého súčasťou bude aj dobre fungujúca spolupráca medzi všetkými zainteresovanými stranami zapojenými do kybernetickej bezpečnosti, v relevantných prípadoch aj vrátane súkromného sektora.***

- ***V súlade so smernicou NIS by členské štáty, ktoré tak ešte neurobili, mali zriadiť národné jednotky*** CSIRT. ***S cieľom zabezpečiť vysokú úroveň kybernetickej bezpečnosti by členské štáty mali zvážiť, či vládne jednotky*** CSIRT ***nepoveria funkciami, ktoré by im umožnili pôsobiť ako ústredné body koordinácie medzi ostatnými jednotkami*** CSIRT ***a zainteresovanými stranami podieľajúcimi sa na prevencii kybernetických hrozieb a reakcii na kybernetické incidenty.***

- ***Na tento účel by členské štáty mali zvážiť aj to, či vládne jednotky*** CSIRT ***nepoveria úlohami súvisiacimi so zhromažďovaním informácií o kybernetických incidentoch a ich analýzou, pričom by mali rozvíjať svoje schopnosti reagovať na hrozby a softvérové systémy včasného varovania a poskytovať cielenú odbornú prípravu v oblasti počítačovej kriminality a kybernetickej bezpečnosti.***

- ***V súlade so smernicou o bezpečnosti sietí a informačných systémov členské štáty zabezpečia, aby prevádzkovatelia základných služieb bez zbytočného odkladu oznamovali kybernetické incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú.***

- ***Členské štáty sa vyzývajú, aby sa zapojili do platformy EMPACT na boj proti kybernetickým útokom, ako aj do siete jednotiek*** CSIRT***, ako sa ustanovuje v smernici NIS, a v relevantných prípadoch aj do iných podobných sietí.***

XVII – SPOLUPRÁCA S AGENTÚRAMI EÚ

HLAVNÉ ZISTENIA A ZÁVERY

- Keďže počítačová kriminalita *stricto sensu* a trestné činy umožnené informačnými technológiami, ako aj ich vyšetrovanie často zahŕňajú viac členských štátov, prioritou je spolupráca a výmena informácií s agentúrami EÚ.

- Zásadnú úlohu tu zohráva Europol/Európske centrum boja proti počítačovej kriminalite (EC3), Eurojust, EJS a ENISA so širokým spektrom činností, ktoré zahŕňajú tvorbu analýz o trendoch počítačovej kriminality, koordináciu medzinárodných vyšetrovaní a stíhaní, vzájomnú výmenu informácií, analýzu kriminálnych spravodajských informácií, dôkazov a údajov a prispievanie k odbornej príprave na úrovni celej EÚ. Ich odborné znalosti a nástroje umožňujú vzájomnú spoluprácu medzi členskými štátmi a ich príslušnými OPP a prokuratúrami.

- Eurojust zohráva dôležitú úlohu pri koordinácii medzinárodných vyšetrovaní trestných činov a stíhaní ich páchateľov a pri poskytovaní právnej pomoci, pokiaľ ide o cezhraničnú spoluprácu a prenos dôkazov medzi členskými štátmi, čo sa ukazuje v prípade počítačovej kriminality ako obzvlášť užitočné. Takisto prispieva k zjednodušeniu a urýchľovaniu spolupráce s príslušnými orgánmi členských štátov a tretích krajín v oblasti počítačovej kriminality.

- Eurojust tiež zhromažďuje a šíri prípadové štúdie a osvedčené postupy, prispieva k odbornej príprave v oblasti počítačovej kriminality a podporuje výmenu skúseností medzi špecializovanými prokurátormi a sudcami v oblasti počítačovej kriminality, najmä podporou Európskej justičnej siete na boj proti počítačovej kriminalite.

- Europol uľahčuje spoluprácu a výmenu informácií medzi členskými štátmi, rozširuje operačné produkty a služby medzi vyšetrovacími službami, zabezpečuje forenznú a operačnú odbornú prípravu a informačné materiály. Cieľom Európskeho centra boja proti počítačovej kriminalite (EC3) je posilniť reakciu orgánov presadzovania práva na počítačovú kriminalitu v EÚ a pomáhať tak chrániť európskych občanov, podniky a vlády pred online trestnou činnosťou. EC3 poskytuje operačnú a vyšetrovaciu podporu vnútroštátnym útvarom vyšetrovania počítačovej kriminality v troch hlavných oblastiach: online podvody, online sexuálne vykorisťovanie detí a kybernetické útoky zasahujúce kritické infraštruktúry a informačné systémy v Európskej únii. Tieto činnosti podporuje jednotka kybernetického spravodajstva (CIT), ktorej analytici zhromažďujú a spracúvajú informácie z verejných, súkromných a otvorených zdrojov a identifikujú vznikajúce hrozby a opakujúce sa vzorce. S EC3 spolupracuje spoločná osobitná pracovná skupina pre počítačovú kriminalitu (J-CAT), ktorá pracuje na najdôležitejších medzinárodných prípadoch počítačovej kriminality, ktoré majú vplyv na členské štáty EÚ a ich občanov. Operačná skúsenosť ukazuje pridanú hodnotu včasného zapojenia špecializovaných styčných dôstojníkov – členov J-CAT do koordinácie veľkých operácií boja proti počítačovej kriminalite.

- Členské štáty vo všeobecnosti uznávajú podporu a koordináciu, ktorú im poskytujú Europol/EC3, Eurojust a EJS s pomocou svojich kontaktných miest, a považujú ich úlohu za veľmi dôležitú z hľadiska zvyšovania vzájomnej dôvery medzi vyšetrujúcimi orgánmi a prokurátormi a z hľadiska uľahčovania medzinárodnej spolupráce s tretími štátmi.

- Z hľadiska posilňovania technickej bezpečnosti informačných systémov je dôležitým príspevkom aj úloha agentúry ENISA pri zbere kybernetických varovaní a ich šírení pomocou automatizovaných systémov.

- Nie vždy sú však služby a produkty, ktoré môže poskytnúť Europol, Eurojust, EJS a agentúra ENISA v súvislosti s počítačovou kriminalitou, v plnej miere známe, a príslušní odborníci ich preto nevyužívajú naplno.

ODPORÚČANIA

- ***Členské štáty by mali čo najlepšie využívať služby a produkty, ktoré ponúka Eurojust, EJS a Europol v oblasti počítačovej kriminality, a zabezpečiť úzku spoluprácu medzi svojimi vnútroštátnymi jednotkami CSIRT a agentúrou ENISA.***

- ***Eurojust, Europol a ENISA by mali zvážiť zvyšovanie povedomia o svojich službách a existujúcich možnostiach spolupráce a o špecializovanej odbornej príprave, ktorú ponúkajú v oblasti počítačovej kriminality, ako aj aktívnu podporu podujatiam, ktoré posilnia medzinárodnú spoluprácu v oblasti boja proti počítačovej kriminalite.***

- ***Europol by mal tiež zúročiť využívanie systému SIENA vo vyšetrovacích službách, zvýšiť viditeľnosť projektov platformy EMPACT, skúmať najlepšie spôsoby využívania skupiny J-CAT a zvážiť, či by sa členským štátom nemal navrhnúť štandardný prístup k štrukturálnym prvkom pre databázy kriminálnych spravodajských služieb v oblasti počítačovej kriminality, a taktiež uľahčiť prijatie spoločnej taxonómie v oblasti počítačovej kriminality.***

- ***Agentúra ENISA by mala preskúmať, ako by bolo možné normalizovať koncepciu kybernetických varovaní, ktoré sa zbierajú a šíria prostredníctvom automatizovaných systémov, čo by umožnilo, aby bola štatistika o týchto upozorneniach porovnateľná a zosúladená vo všetkých členských štátoch.***

XVIII – SPOLOČNÉ VYŠETROVACIE TÍMY (JIT)

HLAVNÉ ZISTENIA A ZÁVERY

- Vzhľadom na častý cezhraničný rozmer počítačovej kriminality môže byť účasť v medzinárodne koordinovaných vyšetrovaniach prínosom pri účinnom stíhaní počítačovej kriminality.

- V rámci EÚ sú spoločné vyšetrovacie tímy (JIT) nástrojom medzinárodnej spolupráce v nadnárodných prípadoch trestnej činnosti na základe dohody medzi príslušnými orgánmi dvoch alebo viacerých členských štátov – justičných orgánov aj orgánov presadzovania práva –, ktorých cieľom je vykonávať spoločné vyšetrovania trestných činov.

- V čase hodnotenia sa niekoľko členských štátov – niektoré častejšie než iné – už podieľalo na spoločných vyšetrovacích tímoch v súvislosti s prípadmi počítačovej kriminality, zatiaľ čo iné členské štáty túto skúsenosť nemali.

- Zúčastnené členské štáty účasť v JIT vo všeobecnosti označujú za pozitívnu skúsenosť a považujú ich za účinný nástroj pri cezhraničných vyšetrovaniach, ktorý umožňuje priamu výmenu informácií medzi vyšetrovateľmi a včasné krížové zhromažďovanie dôkazov bez toho, aby sa museli predkladať samostatné formálne žiadosti o vzájomnú právnu pomoc.

- Vzhľadom na zdĺhavé postupy vzájomnej právnej pomoci prispieva využívanie spoločných vyšetrovacích tímov k skráteniu času vyšetrovania a k posilňovaniu dôvery medzi vnútroštátnymi orgánmi.

- Hoci účasť Eurojustu a Europolu pri vytváraní a činnosti spoločných vyšetrovacích tímov nie je povinná, ako to uvádzajú niektoré členské štáty, tieto dve agentúry môžu zohrávať pri zabezpečovaní efektívnosti a operačnej kapacity JIT dôležitú úlohu. Možnosť financovania spoločných vyšetrovacích tímov Europolom a Eurojustom považujú niektoré členské štáty za kľúčovú.

ODPORÚČANIA
• ***Členské štáty sa nabádajú, aby zvyšovali informovanosť odborníkov o možnostiach a výhodách spoločných vyšetrovacích tímov a ich využití v prípadoch počítačovej kriminality v záujme zefektívnenia vyšetrovaní.*** • ***Inštitúcie, agentúry a orgány EÚ, najmä Europol a Eurojust, by mali aj naďalej podporovať a uľahčovať vytváranie spoločných vyšetrovacích tímov a sprístupňovať adekvátne financovanie s cieľom pomôcť členským štátom, aby ich využívali častejšie.***

XIX – VZÁJOMNÁ PRÁVNA POMOC

HLAVNÉ ZISTENIA A ZÁVERY

- Účinný boj proti počítačovej kriminalite si vzhľadom na jej prevažne nadnárodný charakter často vyžaduje bezproblémovú a riadne fungujúcu medzinárodnú spoluprácu, ako aj využívanie vzájomnej právnej pomoci.

- Vnútroštátne právne úpravy členských štátov neobsahujú osobitné ustanovenia o žiadostiach o vzájomnú právnu pomoc v súvislosti s počítačovou kriminalitou, uplatňujú sa preto všeobecné postupy a podmienky týkajúce sa vzájomnej právnej pomoci.

- Väčšina členských štátov je zmluvnou stranou Dohovoru o vzájomnej pomoci v trestných veciach medzi členskými štátmi Európskej únie z 29. mája 2000 (dohovor o vzájomnej právnej pomoci), ktorý bol uzavretý v súlade s článkom 34 Zmluvy o Európskej únii, a jeho dodatkového protokolu z roku 2001. Zúčastňujú sa aj na schengenskom *acquis* a uplatňujú ho, z čoho vyplýva aj uplatniteľnosť ustanovení Schengenského dohovoru o justičnej spolupráci, čo je dôležité najmä pre členské štáty, ktoré nie sú zmluvnou stranou dohovoru o vzájomnej právnej pomoci. V prípade členských štátov, ktoré nie sú zmluvnými stranami uvedených mnohostranných dohovorov ani dvojstranných dohovorov, je vzájomná právna pomoc založená na zásade reciprocity.

- Žiadostiam justičných orgánov o vzájomnú právnu pomoc vo všeobecnosti predchádzajú žiadosti o urýchlené uchovanie elektronických dôkazov v podobe uložených počítačových údajov podľa článku 29 Budapeštianskeho dohovoru o počítačovej kriminalite z 22. novembra 2001.

- Lehota na odpoveď na žiadosť o vzájomnú právnu pomoc môže byť až niekoľko mesiacov, ale líši sa v závislosti od rozličných okolností, napr. toho, či sa vzájomná právna pomoc poskytuje na základe medzinárodnej dohody alebo reciprocity; v druhom prípade je lehota ešte dlhšia, pretože najprv je potrebné získať/poskytnúť ubezpečenie o reciprocite.

- V oblasti počítačovej kriminality, ktorá sa vyznačuje vysokou rýchlosťou, sú zdĺhavé postupy vzájomnej právnej pomoci dosť neefektívne s negatívnymi dôsledkami na vedenie a úspešnosť vyšetrovania, pretože elektronické dôkazy sú nestabilné a omeškania môžu viesť k strate údajov. Preto je vo všeobecnosti potrebné vybavovanie žiadostí o vzájomnú právnu pomoc v súvislosti s vyšetrovaniami počítačovej kriminality urýchliť. Zlepšenie kvality žiadostí o vzájomnú právnu pomoc by mohlo mať značný vplyv na urýchlenie ich vybavenia v iných krajinách.

- S cieľom dosiahnuť rýchlejšie reakcie využívajú niektoré členské štáty ako alternatívu k formálnym kanálom vzájomnej právnej pomoci kanály Europolu, Eurojustu a EJS, ako je J-CAT v rámci EC3, Interpol, sieť kontaktných miest G7, siete styčných dôstojníkov alebo bilaterálne kontakty; je však potrebné vziať do úvahy, že pri použití týchto menej formálnych kanálov je potrebné overovať, či sú tieto údaje prípustné ako dôkazy na súde.

- Za veľmi užitočnú sa pri uľahčovaní komunikácie a urýchľovaní vybavovania naliehavých žiadostí nielen medzi členskými štátmi, ale aj s tretími krajinami, považuje podpora zo stany Eurojustu, a to aj vzhľadom na fyzickú prítomnosť styčných prokurátorov z USA, Nórska a Švajčiarska v Eurojuste.

- Ako sa uvádza v mnohých jednotlivých správach, mnoho žiadostí o vzájomnú právnu pomoc v súvislosti s prípadmi počítačovej kriminality sa týka získania konkrétneho dôkazového materiálu, ktorý majú v držbe poskytovatelia služieb. Keďže na mnoho poskytovateľov služieb sa vzťahuje právomoc Spojených štátov amerických, pokiaľ ide o krajiny mimo EÚ, vzájomná právna pomoc v trestných veciach týkajúcich sa počítačovej kriminality sa žiada najmä od nich, preto má hladká spoluprácu s nimi kľúčový význam.

- Mnohé členské štáty však v tejto oblasti narážajú na prekážky, najmä v oblasti uchovávania údajov a zverejňovania IP adries majiteľov kont na Facebooku a iných sociálnych sieťach. Ako uviedli hodnotitelia v niektorých individuálnych správach, problémom, ktorý ovplyvňuje všetky členské štáty, je stále otázka prístupu do databáz sociálnych sietí s pôvodom v USA.

- Spojené štáty vo všeobecnosti podmieňujú takéto žiadosti prísnymi formálnymi a obsahovými požiadavkami, najmä pokiaľ ide o súvislosť medzi trestným činom a konkrétnym dôkazovým prvkom, ktorý je predmetom žiadosti o zaslanie.

- Podľa zistení vyplývajúcich z hodnotenia by bolo vhodné pracovať na hľadaní medzinárodných riešení na zlepšenie postupov vzájomnej právnej pomoci s tretími štátmi, ako napríklad s USA. Za osvedčený postup možno považovať používanie formulára žiadosti o vydanie príkazu na urýchlené predloženie, ktorú schvália vykonávajúce orgány daného štátu.

- V súlade s príslušnými právnymi predpismi USA o zisťovaní umiestnenia alebo získaní elektronickej pošty a akéhokoľvek obsahu komunikácie, ktorú uložil poskytovateľ služieb, je potrebný „príkaz na prehliadku“, ktorý musí spĺňať požiadavku na „dôvodné podozrenie“. Tento postup je časovo veľmi náročný a v mnohých prípadoch nevedie k vybaveniu žiadosti.

- Niektoré členské štáty potvrdzujú, že s cieľom zaistiť lepšie a rýchlejšie vybavovanie takýchto žiadostí sa ako užitočný ukázal rozvoj neformálnych a osobných kontaktov s príslušnými orgánmi tretích štátov pred zaslaním žiadosti o vzájomnú právnu pomoc.

- Za osvedčený postup teda možno považovať zriadenie systému registrácie žiadostí o vzájomnú právnu pomoc a systému ich správy, ktorý by umožňoval sledovať jednotlivé prípady od registrácie po zaslanie odpovede do žiadajúcej krajiny.

ODPORÚČANIA

- ***Členské štáty by mali preskúmať spôsoby, ako ešte viac zlepšiť kvalitu žiadostí o vzájomnú právnu pomoc, ktoré posielajú do iných krajín, najmä s cieľom zabezpečiť, aby boli riadne vyplnené, a ako urýchliť a zvýšiť kvalitu reakcií na žiadosti o vzájomnú právnu pomoc.***

- ***Členským štátom sa odporúča, aby zvýšili efektívnosť procesu komunikácie s inými členskými štátmi a tretími krajinami a zvážili zavedenie postupov, ktoré umožnia sledovať jednotlivé prípady od registrácie po zaslanie odpovede do žiadajúcej krajiny, ako je napr. systém registrácie žiadostí o vzájomnú právnu pomoc.***

- ***Členské štáty sa nabádajú, aby viac využívali nástroje Europolu, Eurojustu a EJS a aby rozvíjali neformálne kontakty s príslušnými zahraničnými orgánmi s cieľom získať rýchlejšie reakcie tretích krajín na žiadosti o vzájomnú právnu pomoc.***

- ***EÚ by mala naďalej pracovať na riešeniach s cieľom zlepšiť a urýchliť komunikáciu medzi členskými štátmi a tretími krajinami, najmä s USA, konkrétne pokiaľ ide o výmenu operatívnych informácií a vybavovanie žiadostí o vzájomnú právnu pomoc.***

- ***EÚ by mala zvážiť zriadenie rámca pre priamu spoluprácu s príslušnými poskytovateľmi služieb z krajín mimo EÚ.***

XX – ODBORNÁ PRÍPRAVA

HLAVNÉ ZISTENIA A ZÁVERY

- Vzhľadom na rýchly technický pokrok a meniacu sa povahu počítačovej kriminality a z toho vyplývajúcu potrebu prispôsobovať sa novým trendom a sofistikovanejším *modom operandi* má pravidelná a kontinuálna špecializovaná odborná príprava v oblasti počítačovej kriminality a kybernetickej bezpečnosti pre odborníkov z praxe na všetkých úrovniach, a to aj na začiatku kariéry, kľúčový význam pre úspešnosť vyšetrovania a stíhania počítačovej kriminality *stricto sensu* a trestných činov umožnených informačnými technológiami.

- Vo väčšine členských štátov sa do špecializovanej odbornej prípravy v oblasti počítačovej kriminality pre OPP investuje významné úsilie, prostriedky a ľudské zdroje, ale nie všetky členské štáty dosahujú rovnakú úroveň odbornej prípravy zameranej na justíciu a v niektorých členských štátoch nie je takáto odborná príprava, ak je vôbec k dispozícii, povinná.

- Vzhľadom na technické špecifiká počítačovej kriminality je však potrebná vysoká úroveň chápania problematiky zo strany OPP, ale aj sudcov, ktorí o prípadoch rozhodujú a pre OPP, prokurátorov a sudcov, ktorí sa zaoberajú počítačovou kriminalitou, má špecializovaná odborná príprava v oblasti zhromažďovania, analýzy a využívania elektronických dôkazov rovnako zásadný význam.

- Okrem odbornej prípravy, ktorú poskytujú verejné orgány (policajné alebo justičné akadémie alebo inštitúty odbornej prípravy atď.), poskytujú v niektorých členských štátoch odbornú prípravu v oblasti počítačovej kriminality aj externé subjekty, napr. univerzity a súkromné spoločnosti pôsobiace v tomto sektore, ktorých odborné znalosti sa ukazujú ako veľmi užitočné pre kvalitnú odbornú prípravu, alebo aj MVO. Niektoré členské štáty zriadili vysoko špecializované centrá excelentnosti, ktoré poskytujú odbornú prípravu v oblasti počítačovej kriminality.

- V niektorých členských štátoch sa odborná príprava poskytuje aj v rámci diaľkového vzdelávania, elektronického učenia sa (e-learning) alebo aj podcastmi (zvukovými záznamami), čo možno považovať za osvedčený postup a účinnú metódu odbornej prípravy.

- Okrem odbornej prípravy na vnútroštátnej úrovni poskytujú špecializovanú odbornú prípravu v oblasti počítačovej kriminality alebo sa na nej podieľajú aj príslušné orgány EÚ – EC3/Europol, ECTEG (Európska skupina pre vzdelávanie a odbornú prípravu v oblasti boja proti počítačovej kriminalite), Eurojust, OLAF, CEPOL a ENISA; členské štáty však vo všeobecnosti nevyužívajú plný potenciál týchto možností.

- Niektoré členské štáty majú na odbornú prípravu v oblasti počítačovej kriminality vyčlenený osobitný rozpočet. V niektorých členských štátoch treba vyvinúť väčšie úsilie o zlepšenie špecializovanej odbornej prípravy v oblasti počítačovej kriminality pre všetky kategórie úradníkov pracujúcich na prípadoch počítačovej kriminality.

- Podľa zistení vyplývajúcich z hodnotenia môže integrovaný prístup k spoločnej odbornej príprave sudcov, prokurátorov a OPP prispieť k zlepšovaniu znalostí o počítačovej kriminalite a fungovať ako platforma na výmenu skúseností a osvedčených postupov v oblasti počítačovej kriminality a na diskusiu o prekážkach týkajúcich sa prípustnosti dôkazov. Vzájomné hodnotenie však ukázalo, že tento typ spoločnej odbornej prípravy zatiaľ poskytuje len málo členských štátov.

ODPORÚČANIA

- ***Členské štáty by mali poskytovať komplexnú odbornú prípravu zahŕňajúcu celý životný cyklus prípadov počítačovej kriminality pre všetky zainteresované strany a odborníkov z praxe zapojených do boja proti počítačovej kriminalite, a najmä pravidelnejšie školenia pre zamestnancov justičných orgánov, a zvážiť vyčlenenie rozpočtových prostriedkov pre odbornú prípravu v oblasti počítačovej kriminality.***

- ***Členské štáty by mali zvážiť organizovanie spoločnej odbornej prípravy v oblasti počítačovej kriminality pre OPP, prokurátorov a sudcov, ako aj využívanie elektronického učenia sa.***

- ***Členské štáty by mali naplno využívať možnosti odbornej prípravy, ktoré poskytujú orgány EÚ, ako napr. EC3/Europol, ECTEG, Eurojust, OLAF, CEPOL a ENISA, a tie, ktoré ponúkajú akademické inštitúcie a súkromné spoločnosti, a zvážiť zriadenie centier excelentnosti s cieľom poskytovať špecializovanú odbornú prípravu v oblasti počítačovej kriminality.***

- ***Inštitúcie EÚ by mali zvýšiť finančné prostriedky EÚ na pomoc členským štátom, aby organizovali špecializovanejšie školenia pre vnútroštátnych odborníkov v oblasti počítačovej kriminality.***