II

(Nelegislatívne akty)

ODPORÚČANIA

ODPORÚČANIE KOMISIE (EÚ) 2021/1086

z 23. júna 2021

o zriadení spoločnej kybernetickej jednotky

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 292,

keďže:

(1) Kybernetická bezpečnosť je základným predpokladom úspechu digitálnej transformácie hospodárstva a spoločnosti. EÚ je odhodlaná zmobilizovať bezprecedentnú úroveň investícií s cieľom zaistiť, aby ľudia, podniky a subjekty verejného sektora dôverovali digitálnym nástrojom.

(2) Pandémia COVID-19 zvýšila význam prepojenosti a závislosť Európy od stabilných sietí a informačných systémov a poukázala na potrebu chrániť celý dodávateľský reťazec. Spoľahlivé a bezpečné sieťové a informačné systémy sú mimoriadne dôležité pre subjekty v prvej línii boja proti pandémii, ako sú nemocnice, zdravotnícke agentúry a výrobcovia vakcín. Koordinované úsilie EÚ s cieľom zabrániť najzávažnejším kybernetickým útokom proti takýmto subjektom, odhaľovať ich, odrádzať od nich, zmierňovať ich vplyvy a reagovať na ne by mohlo zabrániť stratám na životoch a pokusom o oslabenie schopnosti EÚ čo najrýchlejšie poraziť pandémiu. Posilnenie schopnosti EÚ účinne bojovať proti kybernetickým útokom navyše prispieva k rozvoju celosvetového, otvoreného, stabilného a bezpečného kybernetického priestoru.

(3) Príslušné inštitúcie a aktéri v oblasti kybernetickej bezpečnosti čelia cezhraničným kybernetickým hrozbám a čoraz častejším útokom, ktoré sú komplexnejšie, rozšírenejšie a cielenejšie ([1]), a preto by mali zlepšiť svoju schopnosť reagovať na takéto hrozby a útoky využívaním existujúcich zdrojov a lepšou koordináciou úsilia. Všetci príslušní aktéri v EÚ musia byť pripravení spoločne reagovať a vymieňať si informácie, a to na skôr základe „potreby zdieľať“ než na základe „potreby poznať“.

(4) Napriek značnému pokroku dosiahnutému vďaka spolupráci medzi členskými štátmi v oblasti kybernetickej bezpečnosti, najmä prostredníctvom skupiny pre spoluprácu (ďalej „skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti“) a siete jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT) zriadenej podľa smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 ([2]), stále neexistuje spoločná platforma EÚ na účinnú a bezpečnú výmenu informácií zhromaždených v rôznych kybernetickobezpečnostných komunitách, kde by príslušní aktéri mohli koordinovať a mobilizovať operatívne spôsobilosti. Vzniká tak riziko, že kybernetické hrozby a incidenty sa budú riešiť v dátových silách, a to s obmedzenou účinnosťou a vyššou zraniteľnosťou. Okrem toho chýba kanál technickej a operačnej spolupráce na úrovni EÚ so súkromným sektorom, pokiaľ ide o výmenu informácií a podporu reakcie na incidenty.

([1]) ENISA, 2020 *Threat Landscape* (Panoráma hrozieb); Europol, *Internet Organised Crime Threat Assessment* (IOCTA) 2020 (Posúdenie hrozieb vyplývajúcich z organizovaného zločinu páchaného prostredníctvom internetu).

([2]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

(5) Existujúce rámce, štruktúry, ako aj zdroje a odborné znalosti dostupné v členských štátoch a príslušných inštitúciách, orgánoch a agentúrach EÚ poskytujú pevný základ pre spoločnú reakciu na kybernetickobezpečnostné hrozby, incidenty a krízy ([3]). Z operačného hľadiska táto existujúca architektúra zahŕňa Koncepciu koordinovanej reakcie na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „koncepcia“) ([4]), sieť jednotiek CSIRT a Európsku sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe) ([5]), ako aj Európske centrum boja proti počítačovej kriminalite (EC3) a spoločnú pracovnú skupinu pre počítačovú kriminalitu (J-CAT) pri Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol) a protokol o reakcii na núdzové situácie v rámci presadzovania práva (EU LE ERP). Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, Spravodajské a situačné centrum EÚ (EU INTCEN), súbor nástrojov kybernetickej diplomacie ([6]) a projekty súvisiace s kybernetickou obranou realizované v rámci stálej štruktúrovanej spolupráce (PESCO) ([7]) takisto prispievajú k politickej a operačnej spolupráci v rôznych kybernetickobezpečnostných komunitách. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) má na základe svojho posilneného mandátu za úlohu podporovať operačnú spoluprácu ([8]), pokiaľ ide o kybernetickú bezpečnosť sietí a informačných systémov, používateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami a incidentmi. EÚ môže prostredníctvom integrovaných dojednaní o politickej reakcii na krízu (IPCR) koordinovať svoju politickú reakciu na závažné krízy, a to aj v prípade rozsiahlych kybernetických útokov.

(6) Stále však neexistuje mechanizmus na využívanie existujúcich zdrojov a poskytovanie vzájomnej pomoci medzi kybernetickými komunitami zodpovednými za bezpečnosť sietí a informačných systémov, boj proti počítačovej kriminalite, vykonávanie kybernetickej diplomacie, prípadne kybernetickej obrany v prípade krízy. Na úrovni EÚ nie je k dispozícii ani komplexný mechanizmus technickej a operačnej spolupráce medzi všetkými komunitami v oblasti situačnej informovanosti, pripravenosti a reakcie. Synergie s orgánmi presadzovania práva a spravodajskými komunitami by sa okrem toho mali dosiahnuť prostredníctvom Europolu a centra INTCEN.

(7) Komisia, vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku (vysoký predstaviteľ), členské štáty a príslušné inštitúcie, orgány a agentúry EÚ uznávajú význam analýzy silných a slabých stránok, nedostatkov a prekrývania v súčasnej architektúre kybernetickej bezpečnosti EÚ, ktorá vznikla v posledných rokoch. V nadväznosti na uvedenú analýzu Komisia po porade s členskými štátmi a so zapojením vysokého predstaviteľa vypracovala koncepciu spoločnej kybernetickej jednotky ako súčasť Stratégie EÚ pre bezpečnostnú úniu ([9]), digitálnej stratégie ([10]) a stratégie kybernetickej bezpečnosti ([11]).

([3]) Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe) bola zriadená členskými štátmi v reakcii na odporúčanie o koncepcii. Ide o sieť národných expertov na operačné a krízové riadenie, ktorú Komisia navrhla kodifikovať prostredníctvom smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148, COM(2020) 823 final, 2020/0359 (COD) navrhnutej v decembri 2020.

([4]) Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

([5]) V tomto odporúčaní sa zohľadňuje následná správa o cvičení podľa koncepcie na operačnej úrovni (Blue OLEx) z roku 2020, a najmä zhrnutie predsedníctva k strategickej politickej diskusii o spoločnej kybernetickej jednotke.

([6]) Závery Rady o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor nástrojov kybernetickej diplomacie“) z 19. júna 2017 (9916/17).

([7]) Ide najmä o projekty PESCO týkajúce sa „tímov rýchlej kybernetickej reakcie a vzájomnej pomoci v oblasti kybernetickej bezpečnosti“, ktoré koordinuje Litva, a „Koordinačného centra pre kybernetickú a informačnú oblasť“, ktoré koordinuje Nemecko.

([8]) V článku 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15) sa od agentúry vyžaduje, aby podporovala operačnú spoluprácu medzi členskými štátmi, inštitúciami, orgánmi, úradmi a agentúrami Únie a medzi zainteresovanými stranami. To zahŕňa podporu členských štátov, pokiaľ ide o operačnú spoluprácu v rámci siete jednotiek CSIRT, vypracovanie pravidelnej podrobnej technickej situačnej správy o kybernetickej bezpečnosti v EÚ týkajúcej sa incidentov a kybernetických hrozieb a pomoc pri rozvoji spoločnej reakcie na úrovni Únie a členských štátov na rozsiahle cezhraničné incidenty alebo krízy. Agentúra ENISA okrem toho v spolupráci s Európskou akadémiou bezpečnosti a obrany (EAB) prispieva k činnostiam odbornej prípravy.

([9]) Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov o stratégii EÚ pre bezpečnostnú úniu, COM(2020) 605 final.

([10]) Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Formovanie digitálnej budúcnosti Európy, COM(2020) 67 final.

([11]) Spoločné oznámenie Európskemu parlamentu a Rade: Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde, JOIN(2020) 18 final.

(8) Členské štáty by v čase krízy mali mať možnosť spoľahnúť sa na solidaritu EÚ vo forme koordinovanej pomoci, a to aj zo strany všetkých štyroch kybernetických komunít, t. j. civilnej oblasti, presadzovania práva ([12]), diplomacie a prípadne obrany. Rozsah zapojenia členov z jednej alebo viacerých komunít môže závisieť od povahy rozsiahleho incidentu alebo krízy a následne od typu protiopatrení, ktoré bude treba prijať v rámci reakcie. V prípade kybernetických hrozieb, incidentov a kríz sú dobre vyškolení experti a technické vybavenie základnými prostriedkami, ktoré môžu pomôcť predchádzať vážnym škodám a zaistiť skutočnú obnovu. Ústredným prvkom spoločnej kybernetickej jednotky preto budú jasne identifikované technické a operatívne spôsobilosti, najmä experti a vybavenie, ktoré budú v prípade potreby pripravené na nasadenie v členských štátoch. Platforma poskytne členom jedinečnú možnosť rozvíjať a koordinovať uvedené spôsobilosti prostredníctvom tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti, pričom sa zabezpečia primerané synergie s už existujúcimi projektmi v oblasti kybernetickej bezpečnosti realizovanými v rámci PESCO.

(9) Spoločná kybernetická jednotka predstavuje virtuálnu a fyzickú platformu a nevyžaduje vytvorenie dodatočného samostatného orgánu. Jej štruktúra by nemala ovplyvniť spôsobilosti a právomoci vnútroštátnych orgánov pre kybernetickú bezpečnosť a príslušných subjektov Únie. Spoločná kybernetická jednotka by mala byť zakotvená v memorandách o porozumení uzatvorených medzi jej členmi. Ako platforma pre bezpečnú a rýchlu operatívnu a technickú spoluprácu medzi subjektmi EÚ a orgánmi členských štátov by mala stavať na existujúcich štruktúrach, používať existujúce zdroje a spôsobilosti a zvyšovať ich hodnotu. Mala by takisto združovať všetky kybernetickobezpečnostné komunity, t. j. civilnú oblasť, presadzovanie práva, diplomaciu a obranu. Členovia platformy by mali plniť buď operatívnu alebo podpornú úlohu. Medzi operatívnych členov by mali patriť agentúra ENISA, Europol, tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU), Komisia, Európska služba pre vonkajšiu činnosť (vrátane centra INTCEN), sieť jednotiek CSIRT a EU-CyCLONe. Medzi podporných členov by mali patriť Európska obranná agentúra (EDA), skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, predseda horizontálnej pracovnej skupiny Rady pre kybernetické otázky a jeden zástupca príslušných projektov PESCO ([13]). Keďže členské štáty majú operatívne spôsobilosti a právomoci reagovať na rozsiahle kybernetické hrozby, incidenty a krízy, členovia platformy by sa pri dosahovaní svojich cieľov mali spoliehať, s pomocou príslušných subjektov Únie, predovšetkým na vlastné spôsobilosti.

(10) Spoločná kybernetická jednotka by mala byť novým impulzom pre proces, ktorý začal v roku 2017 v podobe koncepcie. Mala by prispieť k realizácii architektúry koncepcie a predstavovať rozhodujúci krok smerom k európskemu rámcu krízového riadenia kybernetickej bezpečnosti, v ktorom sa hrozby a riziká koordinovane a včas identifikujú, zmierňujú a riešia. V tomto duchu by spoločná kybernetická jednotka mala pomáhať EÚ pri reakcii na súčasné a blížiace sa hrozby.

(11) Operatívni a podporní členovia zapojení do spoločnej kybernetickej jednotky by mali mať možnosť spolupracovať v rámci reakcie EÚ na kybernetickobezpečnostné krízy so širšou škálou zainteresovaných strán. Pri vykonávaní funkcií v rámci svojich mandátov by členovia mali mať prospech zo zvýšenej pripravenosti a širšej situačnej informovanosti o všetkých aspektoch kybernetických hrozieb a incidentov a využívať ďalšie odborné znalosti o kybernetickej bezpečnosti. Mali by sa napríklad pravidelne zapájať do medzikomunitných cvičení, získať jasne vymedzenú úlohu v pláne reakcie EÚ na krízu, zviditeľňovať svoje činnosti prostredníctvom spoločnej komunikácie s verejnosťou a uzatvárať dohody o operačnej spolupráci so súkromným sektorom. Členovia prispievajúci do spoločnej kybernetickej jednotky by zároveň mali mať možnosť posilniť existujúce siete, ako napríklad sieť jednotiek CSIRT a EU-CyCLONe, a získať tak bezpečné nástroje na výmenu informácií a lepšie detekčné spôsobilosti (t. j. centrá bezpečnostných operácií, SOC), ako aj využívať dostupné operatívne spôsobilosti EÚ.

(12) Členovia spoločnej kybernetickej jednotky by sa mali zamerať na technickú a operačnú spoluprácu vrátane spoločných operácií. Členovia by mali prispievať k takejto spolupráci v rozsahu povolenom ich mandátmi. Spolupráca by mala vychádzať z prebiehajúceho úsilia a dopĺňať ho. V závislosti od druhu spolupráce sa môžu zapojiť ďalší členovia.

([12]) Relevantné aj pre justičnú spoluprácu.

([13]) Pozri poznámku pod čiarou č. 5. ESVČ a EDA v úlohe sekretariátu PESCO budú spolupracovať s koordinátormi príslušných projektov PESCO.

(13) Platforma by mala združovať technických a operatívnych expertov na krízové riadenie z členských štátov a subjektov EÚ s cieľom koordinovať reakcie na kybernetické hrozby, incidenty a krízy využitím existujúcich spôsobilostí a odborných znalostí. Experti zapojení do spoločnej kybernetickej jednotky budú môcť prostredníctvom fyzickej a virtuálnej platformy monitorovať a chrániť oveľa širšiu plochu útoku. Členovia by na tento účel pomocou platformy mali koordinovať úsilie v prípade cezhraničných incidentov a kríz, ako aj poskytovanie pomoci krajinám, v ktorých došlo k incidentom.

(14) Zriadenie spoločnej kybernetickej jednotky si vyžaduje postupný proces, pri ktorom sa využijú a zjednotia existujúce rámce a štruktúry uvedené v tomto odporúčaní vrátane mechanizmov spolupráce zriadených v rámci fór vedených členskými štátmi (napr. sieť jednotiek CSIRT, EU-CyCLONe, horizontálna pracovná skupina Rady pre kybernetické otázky, J-CAT a príslušné projekty PESCO) a zo strany inštitúcií, orgánov a agentúr EÚ, štruktúrovanú spoluprácu medzi agentúrou ENISA a tímom CERT-EU, ako aj v rámci medziinštitucionálnej skupiny pre výmenu informácií o kybernetickej bezpečnosti. Rámce pre hybridné hrozby, rámce civilnej ochrany ([14]) a odvetvové rámce ([15]) by sa mali primerane zapojiť. Podobne by sa malo vytvoriť štruktúrované prepojenie s IPCR ([16]). V prípade krízy to umožní rýchle a účinné zasielanie informácií subjektom s rozhodovacou právomocou na politickej úrovni zhromaždeným v Rade.

(15) Zriadenie spoločnej kybernetickej jednotky by preto malo prebiehať postupne a transparentne a malo by byť dokončené počas nasledujúcich dvoch rokov. Ciele stanovené v tomto odporúčaní by sa teda mali dosiahnuť v štyroch krokoch, ako sa uvádza v prílohe k tomuto odporúčaniu. Prípravný proces, ktorý bude organizovať a podporovať agentúra ENISA, so zapojením operatívnych a podporných členov na úrovni EÚ a členských štátov, by sa mal začať v prvých dvoch krokoch a prebiehať v rámci pracovnej skupiny vytvorenej Komisiou. Prípravné práce by sa mali riadiť zásadami vzájomnej angažovanosti, inkluzívnosti a dosahovania konsenzu. Malo by sa podporovať zapojenie všetkých členov, aby zazneli rôzne názory a stanoviská a dospelo sa k riešeniam, ktoré majú čo najširšiu podporu. Harmonogram jednotlivých krokov uvedených v tomto odporúčaní možno upraviť v závislosti od potrieb a na základe riadne odôvodnených podmienok.

(16) V rámci prvého kroku by sa prípravný proces mal začať identifikáciou príslušných dostupných operatívnych spôsobilostí EÚ a posúdením úloh a zodpovedností členov platformy. Počas druhého kroku by sa mal vypracovať plán reakcie EÚ na incidenty a krízy v súlade s koncepciou ([17]) a protokolom o reakcii na núdzové situácie v oblasti presadzovania práva, mali by sa začať činnosti súvisiace s pripravenosťou a situačnou informovanosťou, v súlade s aktom o kybernetickej bezpečnosti a nariadením o Europole ([18]) a malo by sa dokončiť posúdenie úloh a zodpovedností členov platformy. Pracovná skupina by mala predložiť výsledky tohto posúdenia Komisii a vysokému predstaviteľovi, ktorí sa o ne podelia s Radou. Komisia a vysoký predstaviteľ by mali v súlade so svojimi príslušnými právomocami na základe tohto posúdenia vypracovať spoločnú správu a vyzvať Radu, aby správu schválila prostredníctvom svojich záverov.

(17) Po tomto schválení sa sprevádzkuje spoločná kybernetická jednotka s cieľom dokončiť dva zostávajúce kroky procesu. V rámci tretieho kroku by členovia mali mať možnosť nasadiť v rámci spoločnej kybernetickej jednotky tímy rýchlej reakcie EÚ v súlade s postupmi vymedzenými v pláne reakcie EÚ na incidenty a krízy, využívať fyzickú aj virtuálnu platformu a prispievať k rôznym aspektom reakcie na incidenty (od komunikácie s verejnosťou až po následnú obnovu). V rámci posledného štvrtého kroku budú do platformy prizvané zainteresované strany zo súkromného sektora vrátane používateľov aj poskytovateľov kybernetickobezpečnostných riešení a služieb, čo členom umožní zlepšiť výmenu informácií a posilniť koordinovanú reakciu EÚ na kybernetické hrozby a incidenty.

([14]) Spoločná kybernetická jednotka by v tejto súvislosti mala vytvárať synergie s mechanizmom EÚ v oblasti civilnej ochrany (UCPM) s cieľom posilniť európsku pripravenosť a reakciu v prípade viacerých katastrof a núdzových situácií kybernetickej povahy.

([15]) Ako napríklad finančný sektor plánovaný podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2021/xx* [DORA].

([16]) Pozri odôvodnenie 5.

([17]) Pozri poznámku pod čiarou č. 3.

([18]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), ktorým sa nahrádzajú a zrušujú rozhodnutia Rady 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Ú. v. EÚ L 135, 24.5.2016, s. 53).

(18) Na konci tohto procesu pozostávajúceho zo štyroch krokov by členovia mali vypracovať správu o činnosti týkajúcu sa pokroku dosiahnutého pri vykonávaní štyroch krokov stanovených v odporúčaní, v ktorej opíšu úspechy a výzvy a ktorá by sa mala predložiť Komisii a vysokému predstaviteľovi. Komisia a vysoký predstaviteľ by mali na základe uvedenej správy vykonať posúdenie týchto výsledkov a vyvodiť závery pre budúcnosť spoločnej kybernetickej jednotky.

(19) Komisia, agentúra ENISA, Europol a tím CERT-EU by mali spoločnej kybernetickej jednotke poskytovať administratívnu, finančnú a technickú podporu v zmysle oddielu IV tohto odporúčania, v závislosti od dostupných rozpočtových prostriedkov a ľudských zdrojov. Kľúčom k zabezpečeniu účinnej prípravy a udržateľnosti spoločnej kybernetickej jednotky bude posilnenie operačných kyberneticko-bezpečnostných kapacít inštitúcií, orgánov a agentúr EÚ. Komisia má v úmysle zabezpečiť, aby pripravované nariadenie o spoločných záväzných pravidlách kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry EÚ (október 2021) poskytlo právny základ pre tento príspevok v prípade tímu CERT-EU.

(20) Agentúra ENISA má vzhľadom na svoj posilnený mandát podľa nariadenia (EÚ) 2019/881 („akt o kybernetickej bezpečnosti“) jedinečné postavenie na to, aby organizovala a podporovala spoločnú kybernetickú jednotku a prispievala k jej sprevádzkovaniu. Agentúra ENISA momentálne v súlade s ustanoveniami aktu o kybernetickej bezpečnosti zriaďuje bruselskú kanceláriu na podporu svojej štruktúrovanej spolupráce s tímom CERT-EU. Uvedená štruktúrovaná spolupráca vrátane priľahlých kancelárií poskytuje užitočný rámec na uľahčenie vytvorenia spoločnej kybernetickej jednotky, a to aj vrátane jej fyzického priestoru, ktorý by sa mal v prípade potreby sprístupniť členom, ako aj zamestnancom z iných príslušných inštitúcií, orgánov a agentúr EÚ. Fyzická platforma by sa mala využívať spolu s virtuálnou platformou, ktorá poskytuje nástroje na spoluprácu a bezpečnú výmenu informácií. Uvedené nástroje budú využívať množstvo informácií zhromaždených prostredníctvom európskeho kybernetického štítu ([19]) vrátane centier bezpečnostných operácií (ďalej len „SOC“) a stredísk pre výmenu a analýzu informácií (ďalej len „ISAC“).

(21) Protokol EÚ o reakcii na núdzové situácie v rámci presadzovania práva v prípade závažných cezhraničných kybernetických útokov, ktorý Rada prijala v roku 2018, pripisuje v rámci koncepcie ústrednú úlohu Európskemu centru boja proti počítačovej kriminalite (EC3) ([20]). Protokol umožňuje orgánom presadzovania práva EÚ nepretržite reagovať na rozsiahle cezhraničné útoky podozrivo škodlivej povahy prostredníctvom rýchlej reakcie a posúdenia, ako aj bezpečnej a včasnej výmeny kritických informácií v záujme účinnej koordinácie reakcií na cezhraničné incidenty. Okrem toho sa v ňom podrobnejšie rozpracúva spolupráca s ostatnými inštitúciami EÚ a celoeurópske krízové protokoly, ako aj krízová spolupráca so súkromným sektorom. Komunita presadzovania práva, podľa vhodnosti s podporou Europolu, by mala prispieť k spoločnej kybernetickej jednotke prijatím potrebných krokov v rámci celého vyšetrovacieho cyklu, a to v súlade s požiadavkami rámca trestného súdnictva a platnými postupmi zaobchádzania s elektronickými dôkazmi. Europol poskytuje operačnú podporu a uľahčuje operačnú spoluprácu v boji proti kybernetickým hrozbám od vzniku EC3 v roku 2013. Europol by mal podporovať platformu podľa svojho mandátu a prístupu policajnej práce založenej na spravodajstve, pričom by mal využívať všetky typy interných odborných znalostí, produktov, nástrojov a služieb relevantných pre reakciu na incidenty a krízy.

(22) V smernici 2013/40/EÚ o útokoch na informačné systémy sa od členských štátov vyžaduje zabezpečenie toho, aby mali k dispozícii funkčné vnútroštátne kontaktné miesto, ktoré je k dispozícii 24 hodín denne a sedem dní v týždni na účely výmeny informácií týkajúcich sa trestných činov uvedených v danej smernici. Sieť funkčných vnútroštátnych kontaktných miest by mala takisto prispievať k spoločnej kybernetickej jednotke tým, že v prípade potreby zabezpečí zapojenie orgánov presadzovania práva členských štátov.

(23) Komunita kybernetickej diplomacie v EÚ prispieva k podpore a ochrane globálneho, otvoreného, stabilného a bezpečného kybernetického priestoru, konkrétne k predchádzaniu škodlivým kybernetickým činnostiam, odrádzaniu od nich a reakciou na ne. EÚ v roku 2017 vytvorila rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti (súbor nástrojov kybernetickej diplomacie). Tento rámec je súčasťou širšej politiky EÚ v oblasti kybernetickej diplomacie. Prispieva k predchádzaniu konfliktom a k väčšej stabilite v medzinárodných vzťahoch. Umožňuje EÚ a členským štátom, prípadne v spolupráci s medzinárodnými partnermi, využívať všetky opatrenia spoločnej zahraničnej a bezpečnostnej politiky (ďalej len „SZBP“) v súlade s príslušnými postupmi na ich použitie s cieľom podporiť spoluprácu, zmierniť hrozby a ovplyvniť súčasné a možné budúce škodlivé správanie v kybernetickom priestore. Komunita kybernetickej diplomacie by mala v rámci spoločnej kybernetickej jednotky spolupracovať tak, že bude využívať celú škálu diplomatických opatrení a poskytovať podporu pri ich prijímaní, najmä pokiaľ ide o komunikáciu s verejnosťou, podporu spoločnej situačnej informovanosti a zapojenie tretích krajín v prípade krízy.

([19]) JOIN/2020/18 final, oddiel 1.2.
([20]) Zriadené nariadením (EÚ) 2016/794.

(24) Vysoký predstaviteľ by mal v súlade s rámcom koncepcie, ako aj prostredníctvom centra INTCEN prispievať k spoločnej kybernetickej jednotke budovaním nepretržitej spoločnej situačnej informovanosti založenej na vedomostiach o existujúcich a vznikajúcich hrozbách vrátane potrebnej strategickej situačnej informovanosti o každej udalosti.

(25) Cieľom EÚ a členských štátov v rámci komunity kybernetickej obrany je posilniť spôsobilosti kybernetickej obrany, ako aj synergie, koordináciu a spoluprácu medzi príslušnými inštitúciami, orgánmi a agentúrami EÚ, rovnako ako s členskými štátmi a medzi nimi, a to aj v súvislosti s misiami a operáciami spoločnej bezpečnostnej a obrannej politiky (ďalej len „SBOP“). Komunita funguje na základe medzivládnej správy na úrovni EÚ, vnútroštátnych štruktúr vojenského velenia a vojenských kapacít či kapacít a prostriedkov dvojakého využitia. Vzhľadom na odlišnú povahu spoločnej kybernetickej jednotky by sa mali vybudovať osobitné rozhrania, ktoré jej umožnia výmenu informácií s komunitou kybernetickej obrany ([21]).

(26) Stála štruktúrovaná spolupráca je právny rámec zavedený Lisabonskou zmluvou ([22]) a zriadený v roku 2017 v rámci Únie. Štruktúrovaná spolupráca viedla k vytvoreniu mnohých projektov PESCO v kybernetickej oblasti, čím prispela k splneniu záväzku 11 ([23]) „zabezpečiť väčšie úsilie pri spolupráci v oblasti kybernetickej obrany, ako sú výmena informácií, odborná príprava a operačná podpora“. ESVČ vrátane Vojenského štábu EÚ a EDA tvoria sekretariát PESCO, ktorý v rámci Únie slúži ako jednotné kontaktné miesto pre všetky záležitosti PESCO vrátane podporných a koordinačných funkcií súvisiacich s projektmi PESCO (napr. posúdenie návrhov nových projektov, vypracovanie správ o pokroku projektov atď.). Zástupcovia príslušných projektov PESCO by mali podporovať spoločnú kybernetickú jednotku, najmä pokiaľ ide o situačnú informovanosť a pripravenosť.

(27) Členovia by mali prostredníctvom spoločnej kybernetickej jednotky primerane zapojiť zainteresované strany zo súkromného sektora vrátane poskytovateľov a používateľov kybernetickobezpečnostných riešení a služieb s cieľom podporiť európsky rámec krízového riadenia kybernetickej bezpečnosti, a to pri riadnom zohľadnení právneho rámca pre výmenu údajov a bezpečnosť informácií. Poskytovatelia kybernetickej bezpečnosti by k tejto iniciatíve mali prispieť zdieľaním spravodajských informácií o hrozbách a poskytnutím špecialistov v oblasti reakcie na incidenty s cieľom rýchlo posilniť schopnosť jednotky reagovať na rozsiahle útoky a krízy. Používatelia kyberneticko-bezpečnostných tovarov a služieb, a to najmä tých, ktoré patria do rozsahu pôsobnosti smernice NIS, by mali mať možnosť vyhľadať pomoc a poradenstvo cez štruktúrované kanály prepojené so strediskami pre výmenu a analýzu informácií na úrovni EÚ (ISAC) ([24]), ktoré v súčasnosti chýbajú. Platforma by mohla prispieť aj k posilneniu spolupráce s medzinárodnými partnermi.

(28) Rozvoj a udržiavanie situačnej informovanosti si vyžaduje špičkové schopnosti odhaľovania narušení a ich prevencie. Spoločná kybernetická jednotka by sa mala opierať o najmodernejšiu sieť schopnú analyzovať škodlivé hrozby a incidenty, ktoré by mohli ovplyvniť komunikačné a informačné systémy v celej Únii. Spoločná kybernetická jednotka by preto okrem iných zdrojov mala využívať poznatky o hrozbách získané z komunikačných sietí monitorovaných vnútroštátnymi, odvetvovými a cezhraničnými SOC, aby jej členovia získali lepší prehľad o druhoch hrozieb v EÚ.

(29) Platforma by mala využívať vhodne zabezpečené komunikačné kanály s cieľom podporiť výmenu operatívnych informácií, prípadne aj vrátane dôverných materiálov. Takéto kanály by mohli vychádzať aj z existujúcej infraštruktúry, ako je sieťová aplikácia na zabezpečenú výmenu informácií (SIENA), ktorú používa Europol a komunita presadzovania práva. Ako sa uvádza v stratégii kybernetickej bezpečnosti, nástroje, ktoré používajú inštitúcie, orgány a agentúry EÚ, by mali dodržiavať pravidlá informačnej bezpečnosti, ktoré Komisia čoskoro navrhne.

([21]) Najmä prostredníctvom zastúpenia ESVČ s cieľom umožniť primerané zapojenie komunity kybernetickej obrany, ktorá je založená na dobrovoľných vnútroštátnych príspevkoch.

([22]) Články 42.6, 46 a protokol č. 10 ZEÚ.

([23]) Každý členský štát, ktorý sa zúčastňuje na PESCO, prijíma 20 individuálnych záväzkov rozdelených do piatich kľúčových oblastí stanovených v článku 2 protokolu č. 10 o PESCO, ktorý je pripojený k Zmluve o Európskej únii.

([24]) Medzi existujúce ISAC, ktoré by sa mohli zapojiť do takejto výmeny, patrí napríklad ISAC pre európsku energetiku (EE-ISAC) alebo ISAC pre európske finančné inštitúty (FI-ISAC).

(30) Komisia bude najmä prostredníctvom programu Digitálna Európa podporovať potrebné investície do zriadenia fyzickej a virtuálnej platformy, vytvorenia a udržiavania bezpečných komunikačných kanálov a spôsobilostí odbornej prípravy, ako aj do rozvoja a nasadenia detekčných spôsobilostí. Európsky obranný fond by navyše mohol pomôcť financovať kľúčové technológie a spôsobilosti v oblasti kybernetickej obrany, ktoré by posilnili pripravenosť jednotlivých štátov pri využívaní kybernetickej obrany,

PRIJALA TOTO ODPORÚČANIE:

I. ÚČEL TOHTO ODPORÚČANIA

1. Účelom tohto odporúčania je identifikovať činnosti potrebné na koordináciu úsilia EÚ zameraného na prevenciu, detekciu a zmierňovanie rozsiahlych kybernetických incidentov a kríz, odrádzanie od nich a reakciu na ne, a to prostredníctvom spoločnej kybernetickej jednotky. V tomto odporúčaní sa preto zároveň vymedzuje postup, čiastkové ciele a harmonogram, ktoré by členské štáty a príslušné inštitúcie, orgány a agentúry EÚ mali dodržiavať v súvislosti s vytvorením a rozvojom predmetnej platformy.

2. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by mali zabezpečiť, aby v prípade rozsiahlych kybernetickobezpečnostných incidentov a kríz koordinovali svoje úsilie prostredníctvom spoločnej kybernetickej jednotky, ktorá umožňuje vzájomnú pomoc ([25]) na základe odborných znalostí orgánov členských štátov a príslušných inštitúcií, orgánov a agentúr EÚ. Vďaka spoločnej kybernetickej jednotke by členovia takisto mali mať možnosť nadviazať spoluprácu so súkromným sektorom.

II. VYMEDZENIE POJMOV

3. Na účely tohto odporúčania:

a) „plán reakcie EÚ na kybernetickobezpečnostné incidenty a krízy“ je súbor úloh, spôsobov a postupov vedúcich k dokončeniu rámca EÚ pre reakciu na kybernetické krízy opísaného v bode 1 odporúčania Komisie z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „odporúčanie o koncepcii“);

b) „kybernetickobezpečnostné komunity“ sú skupiny založené na spolupráci pôsobiace v civilnej oblasti, oblasti presadzovania práva, diplomacie a obrany a zastupujúce členské štáty aj príslušné inštitúcie, orgány a agentúry EÚ, ktoré si vymieňajú informácie na účely dosiahnutia spoločných cieľov, záujmov a misií týkajúcich sa kybernetickej bezpečnosti;

c) „členovia zo súkromného sektora“ sú zástupcovia subjektov súkromného sektora, ktorí poskytujú alebo využívajú kybernetickobezpečnostné riešenia ([26]) a služby ([27]);

d) „rozsiahly incident“ je incident vymedzený v článku 4 ods. 7 smernice (EÚ) 2016/1148, ktorý má významný vplyv v najmenej dvoch členských štátoch;

e) „integrovaná situačná správa o kybernetickej bezpečnosti v EÚ“ je správa, v ktorej sa zhromažďujú vstupné informácie od členov spoločnej kybernetickej jednotky a ktorá vychádza z technickej situačnej správy o kybernetickej bezpečnosti v EÚ vymedzenej v článku 7 ods. 6 nariadenia (EÚ) 2019/881;

f) „tím rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti“ je tím zložený z uznávaných expertov na kybernetickú bezpečnosť pochádzajúcich najmä z jednotiek CSIRT členských štátov (s podporou agentúry ENISA, tímu CERT-EU a Europolu), ktorý je pripravený na diaľku pomáhať členom zasiahnutým rozsiahlymi incidentmi a krízami;

g) „memorandá o porozumení“ sú dohody medzi členmi, v ktorých sa stanovujú potrebné spôsoby spolupráce vrátane vymedzenia prostriedkov a postupov nevyhnutných na zriadenie a mobilizáciu tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti, ako aj na umožnenie vzájomnej pomoci.

([25]) V súlade s prístupom a so zásadami uvedenými v smernici (EÚ) 2016/1148 a článku 222 (ZFEÚ). Bez toho, aby bol dotknutý článok 42 ods. 7 Zmluvy o Európskej únii.
([26]) Vrátane predajcov softvéru.
([27]) Vrátane spravodajských informácií o hrozbách.

III. CIEĽ SPOLOČNEJ KYBERNETICKEJ JEDNOTKY

4. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by mali zabezpečiť **koordinovanú reakciu EÚ** na rozsiahle kybernetickobezpečnostné incidenty a krízy a následnú obnovu. Takáto reakcia by sa mala zabezpečiť predovšetkým medzi operatívnymi členmi, najmä agentúrou ENISA, Europolom, tímom CERT-EU, Komisiou, Európskou službou pre vonkajšiu činnosť (vrátane centra INTCEN), sieťou jednotiek CSIRT a sieťou EU-CyCLONe, a podpornými členmi, najmä predsedom skupiny pre spoluprácu v oblasti NIS, predsedom horizontálnej pracovnej skupiny Rady pre kybernetické otázky, Európskou obrannou agentúrou a jedným zástupcom príslušných projektov PESCO ([28]). Operatívni členovia by v rámci spoločnej kybernetickej jednotky mali byť schopní rýchlo a účinne zmobilizovať prevádzkové zdroje na vzájomnú pomoc. Na tento účel by sa v rámci spoločnej kybernetickej jednotky mali mechanizmy vzájomnej pomoci koordinovať na základe žiadosti jedného alebo viacerých členských štátov.

5. S cieľom zabezpečiť účinnú koordinovanú reakciu by operatívni a podporní členovia uvedení v bode 4 mali byť schopní vymieňať si najlepšie postupy, využívať nepretržitú **spoločnú situačnú informovanosť** a zabezpečiť potrebnú **pripravenosť** v rozsahu, ktorý im umožňujú ich mandáty. Títo členovia by mali zohľadňovať existujúce postupy a odborné znalosti rôznych kybernetickobezpečnostných komunít.

IV. VYMEDZENIE FUNGOVANIA SPOLOČNEJ KYBERNETICKEJ JEDNOTKY

6. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by na základe príspevku agentúry ENISA v súlade s článkom 7 ods. 7 nariadenia (EÚ) 2019/881 mali zabezpečiť **koordinovanú reakciu** na rozsiahle incidenty a krízy a následnú obnovu, a to prostredníctvom:

a) zriadenia, odbornej prípravy, testovania a koordinovaného nasadenia **tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti** na základe článku 7 ods. 4 nariadenia (EÚ) 2019/881 a článkov 3 a 4 nariadenia (EÚ) 2016/794;

b) koordinovaného zavedenia **virtuálnej a fyzickej platformy** založenej na štruktúrovanej spolupráci agentúry ENISA a tímu CERT-EU zakotvenej v článku 7 ods. 4 nariadenia 2019/881, ktorá by mala slúžiť ako podporná infraštruktúra pre technickú a operačnú spoluprácu medzi členmi a na získavanie príslušných zamestnancov a iných zdrojov od členov;

c) zostavenia a vedenia súpisu **operatívnych a technických spôsobilostí dostupných v EÚ** v rámci kybernetickobezpečnostných komunít ([29]) v Únii, ktoré sú pripravené na nasadenie v prípade rozsiahlych kybernetickobezpečnostných incidentov alebo kríz;

d) podávania správ Komisii a vysokému predstaviteľovi o skúsenostiach získaných pri **činnostiach operačnej spolupráce v oblasti kybernetickej bezpečnosti** v rámci kybernetickobezpečnostných komunít a medzi nimi.

7. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by mali zaistiť, aby spoločná kybernetická jednotka nepretržite zabezpečovala spoločnú **situačnú informovanosť** a **pripravenosť** na krízy umožnené kybernetickými technológiami medzi kybernetickobezpečnostnými komunitami, ako aj v rámci nich, pričom bude sledovať ciele stanovené v článku 7 nariadenia (EÚ) 2019/881 a článku 3 nariadenia (EÚ) 2016/794. Na tento účel by členské štáty a príslušné inštitúcie, orgány a agentúry EÚ mali v súlade s nariadením (EÚ) 2019/881 a nariadením (EÚ) 2016/794 umožniť vykonávanie týchto **podporných** operácií:

a) vypracovanie **integrovanej situačnej správy o kybernetickej bezpečnosti v EÚ** na základe zhromaždenia a analýzy všetkých relevantných informácií a spravodajských informácií o hrozbách;

b) používanie primeraných a bezpečných **nástrojov** v súlade s článkom 7 ods. 1 nariadenia (EÚ) 2019/881 na rýchlu výmenu informácií medzi členmi a s inými subjektmi;

c) **výmena informácií a odborných znalostí** potrebných na to, aby sa Únia mohla pripraviť na riadenie rozsiahlych incidentov a kríz umožnených kybernetickými technológiami, a to s podporou agentúry ENISA, ako sa stanovuje v článku 7 ods. 2 nariadenia (EÚ) 2019/881;

d) prijatie a testovanie národných **plánov reakcie na kybernetickobezpečnostné incidenty a krízy** ([30]) v súlade s článkom 7 ods. 2, 5 a 7 nariadenia (EÚ) 2019/881;

([28]) „Koordinačné centrum pre kybernetickú a informačnú oblasť“ (CIDCC) a „tímy rýchlej kybernetickej reakcie a vzájomná pomoc v oblasti kybernetickej bezpečnosti“ (CRRT).

([29]) V prípade potreby vrátane kybernetickoobrannej komunity.

([30]) Navrhnuté podľa článku 7 ods. 3 smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 [COM(2020) 823 final, 2020/0359 (COD)].

e) vypracovanie, riadenie a testovanie **plánu reakcie EÚ na kybernetickobezpečnostné incidenty a krízy**, a to aj prostredníctvom cvičení a odbornej prípravy medzi komunitami, v súlade s odporúčaním o koncepcii a na základe článku 7 ods. 3 návrhu Komisie na revidovanú smernicu (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii ([31]);

f) pomoc členom pri uzatváraní dohôd o výmene informácií, ako aj dohôd o operačnej spolupráci so **subjektmi súkromného sektora**, ktoré okrem iného poskytujú spravodajské informácie o hrozbách a služby reakcie na incidenty, a to s podporou agentúry ENISA, ako sa stanovuje v článku 7 ods. 1 nariadenia (EÚ) 2019/881;

g) vytvorenie štruktúrovaných synergií s **monitorovacími a detekčnými spôsobilosťami** na vnútroštátnej, odvetvovej a cezhraničnej úrovni, najmä s centrami bezpečnostných operácií;

h) pomoc členom pri **riadení** rozsiahlych incidentov a kríz v súlade s podpornou úlohou agentúry ENISA, ako sa stanovuje v článku 7 nariadenia (EÚ) 2019/881. To zahŕňa prispievanie k spoločnej situačnej informovanosti, podporu diplomatickej činnosti, pripisovanie politickej zodpovednosti, ako aj pripisovanie zodpovednosti v súvislosti s vyšetrovaním trestných činov, a to aj prostredníctvom Europolu ([32]), zosúladenie komunikácie s verejnosťou a uľahčenie obnovy po incidentoch.

8. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by v záujme vykonávania bodov 6 a 7 mali zabezpečiť:

a) vymedzenie organizačných aspektov spoločnej kybernetickej jednotky a **úloh a zodpovedností** operatívnych a podporných členov v rámci platformy, čo umožní účinné fungovanie platformy v súlade s aspektmi a so zásadami uvedenými v prílohe k tomuto odporúčaniu;

b) uzavretie **memoránd o porozumení**, v ktorých sa stanovujú potrebné spôsoby spolupráce medzi členmi uvedenými v bode 4.

9. V súlade s článkom 7 nariadenia (EÚ) 2019/881 by agentúra ENISA mala zabezpečiť koordináciu a podporu členských štátov a príslušných inštitúcií, agentúr a orgánov EÚ v rámci spoločnej kybernetickej jednotky, okrem iného aj tým, že bude fungovať ako sekretariát, organizovať zasadnutia a prispievať k vykonávaniu činností na úrovni členských štátov aj EÚ. Agentúra ENISA by mala zriadiť bezpečnú virtuálnu platformu aj fyzický priestor na usporadúvanie zasadnutí a uľahčovanie potrebných vykonávacích opatrení.

V. **ZRIADENIE SPOLOČNEJ KYBERNETICKEJ JEDNOTKY**

10. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by mali zabezpečiť, aby spoločná kybernetická jednotka vstúpila do prevádzkovej fázy **30. júna 2022**. Do tohto termínu by operatívni členovia mali sprístupniť operatívne spôsobilosti a expertov, ktorí môžu tvoriť základ tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti. Plány fyzickej a virtuálnej platformy by dovtedy mali byť riadne rozpracované.

11. Členské štáty a príslušné inštitúcie, orgány a agentúry EÚ by mali prispieť k fungovaniu spoločnej kybernetickej jednotky a zabezpečiť, aby bola úplne sprevádzkovaná do **30. júna 2023**. To by sa malo uskutočniť prostredníctvom štyroch po sebe nasledujúcich krokov, ktoré budú zamerané na dokončenie týchto činností:

a) krok 1 – posúdenie organizačných aspektov spoločnej kybernetickej jednotky a identifikácia operatívnych spôsobilostí dostupných v EÚ do **31. decembra 2021**;

b) krok 2 – príprava plánov reakcie na kybernetickobezpečnostné incidenty a krízy a vykonávanie činností v rámci spoločnej pripravenosti do **30. júna 2022**;

c) krok 3 – sprevádzkovanie spoločnej kybernetickej jednotky do **31. decembra 2022**;

d) krok 4 – rozšírenie spolupráce v rámci spoločnej kybernetickej jednotky o súkromné subjekty a podávanie správ o dosiahnutom pokroku do **30. júna 2023**.

Konkrétnejšie činnosti, ktoré sa majú vykonať v rámci štyroch po sebe nasledujúcich krokov, sú uvedené v prílohe k tomuto odporúčaniu.

([31]) COM(2020) 823 final.
([32]) V súlade s nariadením (EÚ) 2016/794.

12. V prvých dvoch krokoch by agentúra ENISA mala zorganizovať a podporiť prípravu spoločnej kybernetickej jednotky. Útvary Komisie by mali zvolať pracovnú skupinu zloženú z operatívnych a podporných členov s cieľom dokončiť túto prípravnú prácu. Útvary Komisie by mali vymenovať zástupcu za spolupredsedu pracovnej skupiny a do funkcie spolupredsedov by mali osloviť zástupcu vymenovaného vysokým predstaviteľom, pričom každý z nich prispieva do bodov programu v súlade so svojimi príslušnými právomocami, a zástupcu vybraného členskými štátmi.

13. Pred ukončením kroku 2 by sa pracovná skupina mala dohodnúť na záveroch svojho posúdenia organizačných aspektov spoločnej kybernetickej jednotky, ako aj na úlohách a zodpovednostiach operatívnych členov v rámci tejto platformy. Pracovná skupina by mala predložiť výsledky posúdenia Komisii a vysokému predstaviteľovi. Komisia a vysoký predstaviteľ by mali potom toto posúdenie poskytnúť Rade. Komisia a vysoký predstaviteľ by mali na základe tohto posúdenia vypracovať spoločnú správu a vyzvať Radu, aby uvedenú správu schválila prostredníctvom svojich záverov.

14. Spoločná kybernetická jednotka by mala byť sprevádzkovaná od kroku 3.

15. Agentúra ENISA a Komisia by mali zabezpečiť využívanie existujúcich zdrojov v rámci programov financovania EÚ, najmä programu Digitálna Európa, v súlade s platnými pravidlami vytvárania príslušných pracovných programov, aby boli členovia spoločnej kybernetickej jednotky vybavení dodatočnými spôsobilosťami odbornej prípravy, komunikačnými kapacitami a bezpečnou infraštruktúrou na výmenu informácií, čo umožní výmenu utajovaných skutočností, a to aj medzi komunitami.

VI. **PRESKÚMANIE**

16. Členské štáty by mali v súlade so svojimi príslušnými právomocami spolupracovať s Komisiou a vysokým predstaviteľom, aby do **30. júna 2025** posúdili účinnosť a efektívnosť spoločnej kybernetickej jednotky s cieľom vyvodiť závery pre jej budúcnosť. V predmetnom posúdení by sa malo zohľadniť vykonávanie uvedených štyroch krokov.

V Bruseli 23. júna 2021

Za Komisiu
Thierry BRETON
člen Komisie

PRÍLOHA

Postup zriadenia Spoločnej kybernetickej jednotky

V tejto prílohe sú podrobne opísané hlavné a podporné činnosti potrebné na zriadenie a sprevádzkovanie spoločnej kybernetickej jednotky.

1. *Krok 1 – Posúdenie organizačných aspektov spoločnej kybernetickej jednotky a identifikácia operatívnych spôsobilostí dostupných v EÚ*

HLAVNÉ ČINNOSTI

Operatívni členovia spoločnej kybernetickej jednotky, združení v pracovnej skupine zriadenej Komisiou a podporovanej agentúrou ENISA, by mali zhromažďovať informácie o existujúcich operatívnych spôsobilostiach vrátane zoznamu dostupných uznávaných expertov a ich príslušných odborných znalostí, dostupných nástrojov na riešenie incidentov, funkcií a aktív, dostupných portfólií odbornej prípravy a cvičení, ako aj existujúcich informácií a výsledkov analýzy spravodajských informácií. Na základe týchto informácií by operatívni členovia mali vypracovať **zoznam operatívnych spôsobilostí dostupných v EÚ**, ktoré bude možné použiť v prípade kybernetických incidentov alebo kríz, najmä zapojením tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti.

Pracovná skupina by mala začať s posudzovaním **organizačných aspektov** spoločnej kybernetickej jednotky, **ako aj úloh a zodpovedností operatívnych členov v rámci tejto platformy**.

S cieľom získať prehľad spôsobilostí a dohodnúť sa na postupoch by sa hlavné a pokiaľ možno aj podporné činnosti v rámci prvého kroku mali dokončiť do **31. decembra 2021 [6 mesiacov po prijatí]**.

2. *Krok 2 – Príprava plánov reakcie na kybernetickobezpečnostné incidenty a krízy a vykonávanie činností v rámci spoločnej pripravenosti*

HLAVNÉ ČINNOSTI

Operatívni členovia pracovnej skupiny by po konzultácii s podpornými členmi mali vypracovať **plán reakcie EÚ na kybernetickobezpečnostné incidenty a krízy**, ktorý by vychádzal z národných plánov reakcie na kybernetickobezpečnostné incidenty a krízy. Tento plán by mal obsahovať ciele pripravenosti EÚ, identifikované postupy a kanály na zabezpečenú výmenu informácií vrátane spôsobov zaobchádzania s informáciami, ako aj kritériá na aktiváciu mechanizmu vzájomnej pomoci na základe dohodnutej taxonómie klasifikácie incidentov a zoznamu spôsobilostí dostupných v EÚ.

Pred ukončením kroku dva by sa pracovná skupina mala dohodnúť na záveroch posúdenia organizačných aspektov spoločnej kybernetickej jednotky, ako aj na úlohách a zodpovednostiach operatívnych členov v rámci tejto platformy. Pracovná skupina by výsledky posúdenia mala predložiť Komisii a vysokému predstaviteľovi. Komisia a vysoký predstaviteľ by toto posúdenie mali oznámiť Rade. Komisia a vysoký predstaviteľ by mali v rozsahu svojich právomocí spolupracovať na príprave spoločnej správy z tohto posúdenia a vyzvať Radu, aby správu schválila vo svojich záveroch.

PODPORNÉ ČINNOSTI

Plán reakcie EÚ na kybernetickobezpečnostné incidenty a krízy by mal vychádzať z hlavných prvkov národných plánov reakcie na kybernetickobezpečnostné incidenty a krízy. V súlade s návrhom Komisie na prijatie smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 ([1]), by členské štáty mali prijať národné plány reakcie na kybernetickobezpečnostné incidenty a krízy. V národných plánoch, ktoré sa môžu stať predmetom partnerského preskúmania, by sa mali vymedziť ciele a spôsoby riadenia rozsiahlych kybernetickobezpečnostných incidentov a kríz. Národné plány by mali obsahovať najmä tieto prvky:

a) ciele vnútroštátnych opatrení a činností v oblasti pripravenosti;

b) úlohy a povinnosti príslušných orgánov na vnútroštátnej úrovni;

c) vnútroštátne postupy krízového riadenia a kanály na výmenu informácií;

d) identifikácia opatrení v oblasti pripravenosti vrátane cvičení a odbornej prípravy;

e) identifikácia príslušných verejných a súkromných zainteresovaných strán a potrebnej infraštruktúry;

f) vnútroštátne postupy a dohody medzi príslušnými vnútroštátnymi orgánmi a subjektmi vrátane tých, ktoré zodpovedajú za všetky kybernetické komunity, v snahe zabezpečiť efektívne zapojenie členských štátov do koordinovaného riadenia rozsiahlych kybernetickobezpečnostných incidentov a kríz na úrovni EÚ a jeho podpory.

Na základe informácií poskytnutých členskými štátmi a inštitúciami, orgánmi a agentúrami EÚ by mali operatívni členovia spoločnej kybernetickej jednotky vykonávať tieto podporné činnosti:

a) vypracovať prvú integrovanú situačnú správu EÚ vychádzajúcu z národných plánov reakcie na kybernetickobezpečnostné incidenty a krízy;

([1]) COM(2020) 823 final 2020/0359 (COD), Brusel, 16. 12. 2020.

b) vytvoriť komunikačné kapacity a nástroje na zabezpečenú výmenu informácií;

c) uľahčiť prijímanie protokolov pre vzájomnú pomoc medzi členmi;

d) organizovať cvičenia a odbornú prípravu medzi komunitami pre expertov zaradených do zoznamu operatívnych spôsobilostí dostupných v EÚ;

e) vypracovať viacročný plán koordinácie cvičení.

V prípade potreby by mali operatívni členovia konzultovať s podpornými členmi. Agentúra ENISA by s podporou Komisie, Europolu a tímu CERT-EU mala umožniť výmenu informácií vytvorením komunikačných kapacít a nástrojov na zabezpečenú výmenu informácií.

S cieľom zabezpečiť vypracovanie potrebných plánov a začať s vykonávaním spoločných činností by sa hlavné a pokiaľ možno aj podporné činnosti v rámci druhého kroku mali dokončiť do **30. júna 2022 [6 mesiacov po ukončení kroku 1]**.

3. *Krok 3 – Sprevádzkovanie spoločnej kybernetickej jednotky*

HLAVNÉ ČINNOSTI

Po tom, ako Rada v druhom kroku schváli závery Komisie k predmetnej správe, by operatívni členovia mali začať s koordináciou nasadzovania **tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti** v rámci spoločnej kybernetickej jednotky a zriadiť **fyzickú platformu**, ktorá by týmto tímom umožňovala výkon ich technických a operatívnych činností. Po skončení príprav v rámci druhého kroku by členovia mali dokončiť plán reakcie EÚ na kybernetickobezpečnostné incidenty a krízy. Operatívni členovia by mali zabezpečiť, aby experti a spôsobilosti zahrnuté do zoznamu operatívnych spôsobilostí dostupných v EÚ boli k dispozícii a pripravení podporiť činnosť tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti.

Na účely vykonávania plánu reakcie EÚ na kybernetickobezpečnostné incidenty a krízy by členovia mali stanoviť ročný pracovný program.

PODPORNÉ ČINNOSTI

Spoločnú kybernetickú jednotku môže využívať komunita kybernetickej diplomacie na zosúladenie komunikácie s verejnosťou. Cez platformu budú môcť členovia prispievať k pripisovaniu politickej zodpovednosti a zodpovednosti v zmysle trestného zákona, ktorým sa riadia policajné a justičné orgány. Okrem toho môže platforma pomôcť aj pri nápravných opatreniach a umožniť štruktúrované synergie s monitorovacími a detekčnými spôsobilosťami na vnútroštátnej a cezhraničnej úrovni.

V záujme sprevádzkovania spoločnej kybernetickej jednotky by sa hlavné a pokiaľ možno aj podporné činnosti v rámci tretieho kroku mali dokončiť do **31. decembra 2022 [6 mesiacov po ukončení kroku 2]**.

4. *Krok 4 – Rozšírenie spolupráce v rámci spoločnej kybernetickej jednotky o súkromné subjekty a podávanie správ o dosiahnutom pokroku*

HLAVNÉ ČINNOSTI

Členovia spoločnej kybernetickej jednotky by mali vypracovať **správu o pokroku dosiahnutom pri realizácii štyroch krokov stanovených v odporúčaní, v ktorej opíšu s ňou spojené výsledky a výzvy**. Správa by mala obsahovať štatistické informácie o činnostiach operačnej spolupráce vykonaných v uvedených štyroch krokoch. Mala by byť predložená Komisii a vysokému predstaviteľovi.

PODPORNÉ ČINNOSTI

V záujme rozširovania spôsobilostí a informácií dostupných tímom rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti by členovia mali zabezpečiť, aby spoločná kybernetická jednotka pomáhala pri uzatváraní **dohôd o výmene informácií a operačnej spolupráci medzi členmi a subjektmi súkromného sektora**, ktoré okrem iného poskytujú spravodajské informácie o hrozbách a služby reakcie na incidenty. Okrem iných činností by mali zaručovať aj to, aby spoločná kybernetická jednotka podporovala činnosti v rámci pravidelných dialógov a výmen informácií o hrozbách a zraniteľných miestach s používateľmi kybernetickobezpečnostných riešení, najmä tými, ktorí spadajú do rozsahu pôsobnosti smernice NIS, alebo sú združení v **strediskách pre výmenu a analýzu informácií na úrovni EÚ (ISAC)**.

Členské štáty by mali podporovať subjekty pôsobiace na ich území a zvlášť tie, ktoré spadajú do rozsahu pôsobnosti smernice NIS, tak, aby sa mohli aktívne zapájať do verejno-súkromných dialógov s ISAC na úrovni EÚ.

V snahe zaručiť riadne zapojenie súkromného sektora by sa hlavné a pokiaľ možno aj podporné činnosti v rámci štvrtého kroku mali dokončiť do **30. júna 2023 [6 mesiacov po ukončení kroku 3]**.

AKO RÝCHLO ZMOBILIZOVAŤ OPERATÍVNE SPÔSOBILOSTI V EÚ

KTO SPÔSOBILOSTI POSKYTUJE: operatívni členovia

KTO SPÔSOBILOSTI RIADI: členovia spoločnej kybernetickej jednotky v súlade s dohodnutými úlohami a zodpovednosťami

Krok	Cieľ	Úloha	Hlavná činnosť	Podporná činnosť
Krok 1 – Vymedzenie do **31. decembra 2021 [6 mesiacov po prijatí]**	PRIPRAVENOSŤ	**Identifikovať spôsobilosti**	**Operatívni členovia vypracujú zoznam operatívnych spôsobilostí dostupných v EÚ.**	
Krok 2 – Príprava do **30. júna 2022 [6 mesiacov do konca kroku 1]**	PRIPRAVENOSŤ	**Určiť príslušné postupy a opatrenia na aktiváciu spôsobilostí v prípade potreby**	**Operatívni členovia pripravia na úrovni EÚ plán reakcie na kybernetickobezpečnostné incidenty a krízy (rámec reakcie EÚ na kybernetickobezpečnostné krízy v rámci tejto koncepcie) na základe prijatých národných plánov.**	**Operatívni členovia vypracujú integrované situačné správy EÚ na základe technickej situačnej správy o kybernetickej bezpečnosti v EÚ.**
	PRIPRAVENOSŤ	**Výkon spôsobilostí**		**Členovia zorganizujú spoločné cvičenie a odbornú prípravu (medzi komunitami). Členovia vypracujú viacročný plán koordinácie cvičení.**
	SITUAČNÁ INFORMOVANOSŤ	**Zriadiť nástroje na výmenu informácií a žiadostí o podporu**		**Členovia zaistia bezpečnú a rýchlu výmenu informácií.**
FUNKČNÁ SPOLOČNÁ KYBERNETICKÁ JEDNOTKA Výsledok prípravných prác zrealizovaných členmi v rámci pracovnej skupiny, ktorú zriadi Komisia				
Krok 3 – Nasadenie do **31. decembra 2022 [6 mesiacov po dokončení kroku 2]**	PRIPRAVENOSŤ	**Prijať príslušné postupy, opatrenia a memorandá o porozumení na aktiváciu spôsobilostí v prípade potreby**	**Operatívni členovia dokončia plán reakcie na kybernetickobezpečnostné incidenty a krízy na úrovni EÚ a definujú jeho vykonávanie formou ročných pracovných programov.**	**Členovia podporia budovanie vnútroštátnych a cezhraničných spôsobilostí na monitorovanie a odhaľovanie vrátane centier bezpečnostných operácií.**
	KOORDINOVANÁ REAKCIA	**Nasadenie spôsobilostí v prípade potreby**	**Operatívni členovia koordinujú činnosť operačných tímov rýchlej reakcie EÚ v oblasti kybernetickej bezpečnosti cez virtuálnu a fyzickú platformu spoločnej kybernetickej jednotky v Bruseli.**	**Členovia koordinujú komunikáciu s verejnosťou a prispievajú k pripisovaniu politickej zodpovednosti a zodpovednosti v zmysle trestného zákona.**

Krok 4 – Rozšírenie a podávanie správ do **30. júna 2023 [6 mesiacov po dokončení kroku 3]**	SITUAČNÁ INFORMOVANOSŤ KOORDINOVANÁ REAKCIA	**Zabezpečiť možnosti rozširovania kapacít zapojením súkromného sektora s cieľom reagovať na vznikajúce potreby**	**Členovia predložia správu o dosiahnutom pokroku, v ktorej opíšu výsledky a výzvy s využitím štatistických informácií.**	**Členovia uzatvoria s poskytovateľmi kybernetickej bezpečnosti dohody o výmene informácií, ako aj dohody o operačnej spolupráci.** **Členovia uzatvoria dohody o výmene informácií s používateľmi kybernetickej bezpečnosti, zvlášť so subjektmi, na ktoré sa vzťahuje smernica NIS a sú združené v strediskách EU-ISAC**