ODPORÚČANIA

ODPORÚČANIE KOMISIE (EÚ) 2017/1584

z 13. septembra 2017

o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu

EURÓPSKA KOMISIA,

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

keďže:

(1) miera prepojenia a vzájomnej závislosti našich podnikov, ako aj občanov bez ohľadu na hranice a odvetvia hospodárstva je väčšia než kedykoľvek predtým, základom sa stalo používanie informačných a komunikačných technológií a spoliehanie sa na ne vo všetkých odvetviach hospodárskej činnosti. Členské štáty a inštitúcie EÚ musia byť dobre pripravené na kybernetické incidenty, ktoré môžu ovplyvniť organizácie viac než jedného členského štátu, alebo dokonca v celej Únii a ktoré môžu vážne narušiť vnútorný trh a všeobecnejšie aj siete a informačné systémy, od ktorých závisí hospodárstvo, demokracia a občianska spoločnosť v Únii.

(2) Kybernetické incidenty možno považovať za krízu na úrovni Únie, ak by narušenie spôsobené daným incidentom bolo príliš rozsiahle na to, aby ho zvládol sám dotknutý členský štát, alebo ak má vplyv na dva alebo viac členských štátov s takým ďalekosiahlym účinkom technického alebo politického významu, že si vyžaduje včasnú koordináciu a reakciu na politickej úrovni Únie.

(3) Kybernetické incidenty môžu vyvolať širšiu krízu a zasiahnuť odvetvia činnosti mimo hraníc sietí a informačných systémov a komunikačných sietí, preto ak má byť reakcia primeraná, musia sa použiť kybernetické aj nekybernetické zmierňujúce opatrenia.

(4) Kybernetické incidenty nemožno predvídať, často sa vyskytujú a vyvíjajú vo veľmi krátkom čase, preto musia dotknuté subjekty a subjekty zodpovedné za reakciu na incident a zmierňovanie jeho účinkov rýchlo koordinovať svoju reakciu. Okrem toho kybernetické incidenty často nie sú obmedzené na konkrétnu geografickú oblasť a môžu sa vyskytovať súčasne v mnohých krajinách alebo sa v nich ihneď rozšíriť.

(5) Účinná reakcia na kybernetické incidenty a krízy veľkého rozsahu na úrovni EÚ si vyžaduje rýchlu a účinnú spoluprácu všetkých relevantných zainteresovaných strán a závisí od pripravenosti a schopností jednotlivých členských štátov, ako aj koordinovaného spoločného opatrenia s podporou Únie. Včasná a účinná reakcia na incidenty je preto závislá od vopred stanovených a pokiaľ možno riadne odskúšaných postupov a mechanizmov spolupráce s jasne vymedzenými úlohami a povinnosťami hlavných aktérov na národnej aj únijnej úrovni.

(6) Vo svojich záveroch ([1]) o ochrane kritickej informačnej infraštruktúry z 27. mája 2011 Rada vyzvala členské štáty EÚ, aby „posilnili spoluprácu medzi členskými štátmi a na základe vnútroštátnych skúseností a výsledkov z oblasti krízového riadenia a v spolupráci s agentúrou ENISA prispeli k vývoju európskych mechanizmov spolupráce v prípade počítačových incidentov, ktoré sa majú otestovať v rámci ďalšieho počítačového cvičenia CyberEurope v roku 2012“.

(7) V oznámení z roku 2016 s názvom Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe ([2]) sa členské štáty vyzývajú, aby čo najviac využívali mechanizmy spolupráce stanovené v smernici o sieťovej a informačnej bezpečnosti ([3]) a aby zlepšovali

([1]) Závery Rady o ochrane kritických informačných infraštruktúr – Dosiahnuté ciele a ďalšie kroky na ceste ku globálnej kybernetickej bezpečnosti; dokument 10299/11, Brusel, 27. mája 2011.
([2]) COM(2016) 410 final z 5. júla 2016.
([3]) 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).

cezhraničnú spoluprácu v oblasti pripravenosti na kybernetické incidenty veľkého rozsahu. Ďalej sa v ňom uvádza, že koordinovaný prístup ku krízovej spolupráci medzi rôznymi prvkami kybernetického ekosystému, ktorý má byť stanovený v koncepcii, zvýši pripravenosť a že takouto koncepciou by sa mala zabezpečiť aj súčinnosť a súlad s existujúcimi mechanizmami krízového riadenia.

(8) V záveroch Rady ([1]) k uvedenému oznámeniu členské štáty vyzvali Komisiu, aby predložila takúto koncepciu orgánom a ďalším príslušným zainteresovaným stranám na posúdenie. V smernici NIS sa však nestanovuje rámec spolupráce Únie v prípade kybernetických incidentov a kríz veľkého rozsahu.

(9) Komisia uskutočnila konzultácie s členskými štátmi v rámci dvoch samostatných konzultačných seminárov, ktoré sa konali v Bruseli 5. apríla a 4. júla 2017 so zástupcami členských štátov z jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT), skupinou pre spoluprácu zriadenou v smernici NIS a horizontálnou pracovnou skupinou Rady pre kybernetické otázky, ako aj so zástupcami Európskej služby pre vonkajšiu činnosť (ESVČ), agentúry ENISA, Europolu/EC3 a Generálneho sekretariátu Rady (GSR).

(10) Táto koncepcia koordinovanej reakcie na kybernetické incidenty a krízy veľkého rozsahu na úrovni Únie, ktorá tvorí prílohu k tomuto odporúčaniu, je výsledkom uvedených konzultácií a dopĺňa oznámenie s názvom Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe.

(11) Opisujú a stanovujú sa v nej ciele a spôsoby spolupráce medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami EÚ (ďalej len „inštitúcie EÚ“) pri reagovaní na kybernetické incidenty a krízy veľkého rozsahu a to, ako možno pri existujúcich mechanizmoch krízového riadenia v plnej miere využívať existujúce subjekty kybernetickej bezpečnosti na úrovni EÚ.

(12) Pri reakcii na kybernetickú krízu v zmysle odôvodnenia 2 sa na koordináciu reakcie na politickej úrovni Únie v Rade budú využívať integrované dojednania EÚ o politickej reakcii na krízu (IPCR) ([2]) a Komisia bude uplatňovať ARGUS ([3]) – medziodvetvový krízový koordinačný proces na vysokej úrovni. Ak má kríza výrazný externý rozmer alebo sa týka spoločnej bezpečnostnej a obrannej politiky (SBOP), aktivuje sa krízový reakčný mechanizmus ([3]) Európskej služby pre vonkajšiu činnosť (ESVČ).

(13) Spoluprácu v prípade kybernetických incidentov alebo krízy zabezpečujú v určitých oblastiach odvetvové mechanizmy krízového riadenia na úrovni EÚ. Pokiaľ ide napríklad o európsky globálny navigačný satelitný systém (GNSS), v rozhodnutí Rady 2014/496/SZBP ([4]), sú už vymedzené príslušné úlohy Rady, vysokého predstaviteľa, Komisie, Agentúry pre európsky GNSS a členských štátov v rámci reťazca prevádzkových povinností zriadeného s cieľom reagovať na ohrozenie Únie, členských štátov alebo GNSS, a to aj v prípade kybernetických útokov. Toto odporúčanie by sa preto nemalo dotýkať takýchto mechanizmov.

(14) Členské štáty samotné nesú primárnu zodpovednosť za reakciu na kybernetické incidenty alebo krízy veľkého rozsahu, ktoré ich zasiahnu. Komisia, vysoký predstaviteľ a ďalšie inštitúcie alebo útvary EÚ však zohrávajú dôležitú úlohu, ktorá vychádza z práva Únie alebo z toho, že kybernetické incidenty a krízy môžu mať dosah na všetky odvetvia hospodárskej činnosti na jednotnom trhu, bezpečnosť a medzinárodné vzťahy Únie, ako aj na samotné inštitúcie.

(15) Ku kľúčovým aktérom zapojeným do reakcie na kybernetické krízy patria na úrovni Únie novozriadené štruktúry a mechanizmy podľa smernice NIS, konkrétne sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT), ako aj príslušné agentúry a orgány, najmä Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), Európske centrum boja proti počítačovej kriminalite v rámci Europolu (Europol/EC3), Centrum EÚ pre analýzu spravodajských informácií (INTCEN), Spravodajský útvar Vojenského štábu Európskej únie (EUMS INT) a situačné stredisko (SITROOM), ktoré spolupracujú ako SIAC (jednotná kapacita na analýzu spravodajských informácií EÚ), stredisko EÚ pre hybridné hrozby (v rámci INTCEN), tím reakcie na núdzové počítačové situácie v inštitúciách EÚ (CERT-EU) a Koordinačné centrum pre reakcie na núdzové situácie v Európskej komisii.

(16) Spoluprácu medzi členskými štátmi pri reagovaní na kybernetické incidenty na technickej úrovni zabezpečuje sieť jednotiek CSIRT zriadená v smernici NIS. Agentúra ENISA pre túto sieť zabezpečuje sekretariát a aktívne

([1]) Dokument 14540/16, 15. novembra 2016.
([2]) Ďalšie informácie možno nájsť v oddiele 3.1 Dodatku o krízovom riadení, mechanizmoch spolupráce a aktéroch na úrovni EÚ.
([3]) Tamtiež.
([4]) Rozhodnutie Rady 2014/496/SZBP z 22. júla 2014 o aspektoch rozmiestňovania, prevádzky a používania Európskeho globálneho navigačného satelitného systému, ktoré majú vplyv na bezpečnosť Európskej únie, a o zrušení jednotnej akcie 2004/552/SZBP (Ú. v. EÚ L 219, 25.7.2014, s. 53).

podporuje spoluprácu medzi jednotkami CSIRT. Jednotky CSIRT z jednotlivých štátov a CERT-EU spolupracujú a vymieňajú si informácie na dobrovoľnom základe a v prípade potreby aj v reakcii na kybernetické incidenty, ktoré majú vplyv na jeden alebo viac členských štátov. Na žiadosť zástupcu jednotky CSIRT ktoréhokoľvek členského štátu môžu prerokovať a pokiaľ možno určiť koordinovanú reakciu na incident, ktorý bol zistený v jurisdikcii daného členského štátu. Príslušné postupy sa stanovia v štandardných operačných postupoch (SOP) ([1]) siete jednotiek CSIRT.

(17) Sieť jednotiek CSIRT má takisto za úlohu prediskutovať, preskúmať a určiť ďalšie formy operačnej spolupráce, a to aj v súvislosti s kategóriami rizík a incidentov, včasnými varovaniami, so vzájomnou pomocou, zásadami a spôsobmi koordinácie, keď členské štáty reagujú na cezhraničné riziká a incidenty.

(18) Skupina pre spoluprácu zriadená článkom 11 smernice NIS má za úlohu poskytovať strategické usmernenia pre činnosti siete jednotiek CSIRT a diskutovať o spôsobilostiach a pripravenosti členských štátov a na dobrovoľnom základe hodnotiť národné stratégie v oblasti bezpečnosti sietí a informačných systémov a účinnosť jednotiek CSIRT, ako aj identifikovať najlepšie postupy.

(19) Osobitnou oblasťou činnosti v rámci skupiny pre spoluprácu je vypracovanie usmernení pre oznamovanie incidentov podľa článku 14 ods. 7 smernice NIS, a to pokiaľ ide o okolnosti, za ktorých sú prevádzkovatelia základných služieb povinní oznamovať incidenty podľa článku 14 ods. 3, a formát a postupy podávania takýchto oznámení ([2]).

(20) Uvedomenie si a pochopenie situácie v reálnom čase, stavu rizika a hrozieb získané prostredníctvom správ, hodnotení, výskumu, vyšetrovania, ako aj analýzy sú rozhodujúce na to, aby bolo možné prijímať informované rozhodnutia. Toto „situačné povedomie“ zo strany všetkých príslušných zainteresovaných strán je nevyhnutné na účinnú a koordinovanú reakciu. Situačné povedomie zahŕňa aspekty príčin, ale aj dosahu a pôvodu daného incidentu. Je zrejmé, že závisí od výmeny a spoločného používania informácií medzi príslušnými subjektmi vo vhodnom formáte a primerane bezpečným spôsobom pri uplatňovaní spoločnej taxonómie pri opise incidentu.

(21) Reakcia na kybernetické incidenty môže mať mnoho podôb od identifikácie technických opatrení, ktoré môžu zahŕňať dva alebo viacero subjektov spoločne vyšetrujúcich technické príčiny incidentu (napr. analýza škodlivého softvéru), cez určenie, ako môžu organizácie posúdiť, či sa ich incident dotkol (napr. ukazovatele narušenia) až po operačné rozhodnutia o uplatnení takýchto opatrení a na politickej úrovni rozhodnutia o použití iných nástrojov v závislosti od daného incidentu, ako napríklad rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti ([3]) alebo operačného protokolu EÚ na boj proti hybridným hrozbám ([4]).

(22) Pre prosperujúci digitálny jednotný trh v Európe je rozhodujúca dôvera občanov a podnikov v digitálne služby. Krízová komunikácia preto zohráva mimoriadne dôležitú úlohu pri zmierňovaní negatívnych následkov kybernetických incidentov a kríz. Možno ju použiť aj v súvislosti s rámcom pre spoločnú diplomatickú reakciu ako prostriedok na ovplyvnenie správania (potenciálnych) útočníkov zasahujúcich z územia tretích krajín. Aby bola politická reakcia účinná, je nevyhnutné zosúladiť verejnú komunikáciu na zmiernenie negatívneho vplyvu kybernetických incidentov a kríz s verejnou komunikáciou na ovplyvnenie útočníka.

(23) Poskytovanie informácií verejnosti o tom, ako možno zmierniť účinky incidentu na úrovni užívateľov a organizácií (napríklad inštalovaním záplaty alebo prijatím doplnkových opatrení na zabránenie ohrozeniu atď.), by mohlo byť účinným opatrením na zmiernenie kybernetických incidentov alebo kríz veľkého rozsahu.

(24) Prostredníctvom kybernetickej bezpečnosti infraštruktúr digitálnych služieb v rámci Nástroja na prepájanie Európy (NPE) Komisia vyvíja mechanizmus spolupráce vo forme platformy základných služieb (MeliCERTes) medzi jednotkami CSIRT zúčastnených členských štátov s cieľom zlepšiť ich úroveň pripravenosti, spoluprácu a reakciu na vznikajúce kybernetické hrozby a incidenty. Organizovaním súťažných výziev na predloženie návrhov na udelenie grantov v rámci NPE sa Komisia spolupodieľa na financovaní jednotiek CSIRT v členských štátoch s cieľom zlepšiť ich operačné kapacity na vnútroštátnej úrovni.

([1]) V procese prípravy, prijatie sa očakáva do konca roka 2017.
([2]) Tieto usmernenia majú byť dokončené do konca roka 2017.
([3]) Závery Rady o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“), dokument 9916/17.
([4]) Spoločný pracovný dokument útvarov Komisie Operačný protokol EÚ na boj proti hybridným hrozbám „operačný protokol EÚ“, SWD(2016) 227 final, 5. júla 2016.

(25) Cvičenia kybernetickej bezpečnosti na úrovni EÚ sú nevyhnutné na stimuláciu a zlepšenie spolupráce medzi členskými štátmi a súkromným sektorom. V tejto súvislosti agentúra ENISA od roku 2010 organizuje pravidelné celoeurópske cvičenia kybernetických incidentov („CyberEurope“).

(26) V záveroch Rady ([1]) o vykonávaní spoločného vyhlásenia predsedu Európskej rady, predsedu Európskej komisie a generálneho tajomníka Organizácie Severoatlantickej zmluvy sa vyzýva na posilnenie spolupráce v oblasti kybernetických cvičení prostredníctvom obojstrannej účasti personálu na príslušných cvičeniach, okrem iného v rámci programov Cyber Coalition a Cyber Europe.

(27) Neustále sa vyvíjajúca situácia v oblasti hrozieb a nedávne kybernetické incidenty naznačujú zvýšené riziko, ktorému Únia čelí, členské štáty by preto mali konať v súlade s týmto odporúčaním bez ďalšieho odkladu a v každom prípade najneskôr do konca roka 2018,

PRIJALA TOTO ODPORÚČANIE:

1. Členské štáty a inštitúcie EÚ by mali vytvoriť rámec EÚ pre reakciu na kybernetické krízy, zahŕňajúci ciele a spôsoby spolupráce podľa koncepcie v súlade s jej hlavnými zásadami.

2. Rámec EÚ pre reakciu na kybernetické krízy by mal predovšetkým identifikovať príslušných aktérov, inštitúcie EÚ a orgány členských štátov, a to na všetkých potrebných úrovniach (technickej, operačnej, strategickej/politickej), a ak je to nevyhnutné, vypracovať štandardné operačné postupy určujúce spôsob ich spolupráce v rámci mechanizmov krízového riadenia EÚ. Dôraz by sa mal klásť na umožnenie výmeny informácií bez zbytočného odkladu a koordináciu reakcií počas kybernetických incidentov a kríz veľkého rozsahu.

3. Na tento účel by mali príslušné orgány členských štátov spolupracovať na spresnení protokolov na výmenu informácií a spoluprácu. Skupina pre spoluprácu by si mala vymieňať skúsenosti o týchto otázkach s príslušnými inštitúciami EÚ.

4. Členské štáty by mali zabezpečiť, aby ich národné mechanizmy krízového riadenia dostatočne zohľadňovali reakciu na kybernetické incidenty, a mali by zabezpečiť nevyhnutné postupy pre spoluprácu na úrovni EÚ v kontexte rámca EÚ.

5. V súvislosti s existujúcimi mechanizmami EÚ v oblasti krízového riadenia a v súlade s koncepciou by členské štáty mali spolu s útvarmi Komisie a ESVČ vypracovať praktické vykonávacie usmernenia, pokiaľ ide o začlenenie svojich vnútroštátnych subjektov a postupov krízového riadenia a kybernetickej bezpečnosti do existujúcich mechanizmov krízového riadenia EÚ, ktorými sú najmä IPCR a krízový reakčný mechanizmus ESVČ. Členské štáty by mali predovšetkým zabezpečiť, aby boli zavedené vhodné štruktúry, ktoré umožnia efektívny tok informácií medzi vnútroštátnymi orgánmi krízového riadenia a ich zástupcami na úrovni EÚ v rámci krízových mechanizmov.

6. Členské štáty by mali v plnej miere využívať možnosti, ktoré ponúka program kybernetickej bezpečnosti infraštruktúr digitálnych služieb (DSI) v rámci Nástroja na prepájanie Európy (NPE), a mali by spolupracovať s Komisiou s cieľom zabezpečiť, aby mechanizmus spolupráce na platforme základných služieb, ktorý sa v súčasnosti buduje, poskytoval potrebné funkcie a spĺňal ich požiadavky na spoluprácu aj počas kybernetických kríz.

7. Členské štáty v spolupráci s agentúrou ENISA a vychádzajúc z predchádzajúcej práce v tejto oblasti by mali spolupracovať pri vývoji a prijímaní spoločnej taxonómie a vzorových situačných správ, ktoré slúžia na opis technických príčin a účinkov kybernetických incidentov, aby tak prispeli k ďalšiemu posilneniu svojej technickej a operačnej spolupráce počas kríz. V tejto súvislosti by členské štáty mali zohľadniť prebiehajúce činnosti v rámci skupiny pre spoluprácu, pokiaľ ide o usmernenia pre oznamovanie incidentov, a to najmä aspekty týkajúce sa formátu národných oznámení.

8. Postupy uvedené v rámci by sa mali testovať a v prípade potreby revidovať v nadväznosti na skúsenosti z účasti členských štátov na cvičeniach na vnútroštátnej, regionálnej a únijnej úrovni, ako aj na cvičeniach kybernetickej diplomacie a kybernetických cvičeniach NATO. Predovšetkým by mali byť testované v kontexte cvičení CyberEurope organizovaných agentúrou ENISA. Cvičenie CyberEurope v roku 2018 predstavuje prvú takúto možnosť.

([1]) Dokument ST 15283/16, 6. decembra 2016.

9. Členské štáty a inštitúcie EÚ by mali pravidelne trénovať svoje reakcie na kybernetické incidenty a krízy veľkého rozsahu na vnútroštátnej a európskej úrovni, v prípade potreby aj politické reakcie a ak je to vhodné, so zapojením subjektov súkromného sektora.

V Bruseli 13. septembra 2017

Za Komisiu
Mariya GABRIEL
členka Komisie

PRÍLOHA

Koncepcia koordinovanej reakcie na cezhraničné kybernetické incidenty a krízy veľkého rozsahu

ÚVOD

Táto koncepcia platí pre kybernetické incidenty, ktoré spôsobia príliš rozsiahle narušenie na to, aby ich dotknutý členský štát dokázal zvládnuť sám, alebo ktoré sa týkajú dvoch či viacerých členských štátov alebo inštitúcií EÚ s takým rôznorodým a výrazným dosahom technického alebo politického významu, že si vyžadujú promptnú koordináciu politiky a reakciu na politickej úrovni EÚ.

Takéto rozsiahle kybernetické incidenty sa považujú za kybernetickú „krízu".

V prípade celoúnijnej krízy zahŕňajúcej kybernetické aspekty koordinuje reakciu na politickej úrovni EÚ Rada pomocou integrovaných dojednaní EÚ o politickej reakcii na krízu (IPCR).

Koordinácia v rámci Komisie prebieha v súlade so systémom rýchleho varovania ARGUS.

Ak má kríza výrazný externý rozmer alebo sa týka spoločnej bezpečnostnej a obrannej politiky (SBOP), aktivuje sa krízový reakčný mechanizmus Európskej služby pre vonkajšiu činnosť (ESVČ).

Táto koncepcia opisuje, ako by mali tieto etablované mechanizmy krízového riadenia plne využiť existujúce subjekty kybernetickej bezpečnosti na úrovni EÚ, ako aj mechanizmy spolupráce medzi členskými štátmi.

Zohľadňuje pritom súbor riadiacich zásad (proporcionalita, subsidiarita, komplementárnosť a dôvernosť informácií), predstavuje hlavné ciele spolupráce (účinná reakcia, spoločné situačné povedomie, komunikácia s verejnosťou) na troch úrovniach (strategická/politická, operačná a technická), dotknuté mechanizmy a aktérov, ako aj činnosti potrebné na dosiahnutie uvedených hlavných cieľov.

Koncepcia nepokrýva celý cyklus krízového riadenia (prevencia/zmierňovanie, pripravenosť, reakcia, obnova); zameriava sa iba na reakciu. Zameriava sa však aj na určité ďalšie činnosti – najmä v spojení so spoločným situačným povedomím.

Zároveň treba poznamenať, že kybernetické incidenty môžu byť začiatkom alebo súčasťou širšej krízy, ktorá má vplyv aj na ďalšie odvetvia. Keďže sa predpokladá, že väčšina kybernetických kríz má dosah v reálnom svete, primeraná reakcia musí zahŕňať tak kybernetické, ako aj nekybernetické zmierňovacie činnosti. Činnosti v rámci reakcie na kybernetickú krízu treba koordinovať s ďalšími mechanizmami krízového riadenia na úrovni EÚ, členských štátov alebo odvetví.

Napokon treba poznamenať, že táto koncepcia nenahrádza ani ňou nie sú dotknuté existujúce mechanizmy, dojednania alebo nástroje špecifické pre určité odvetvia alebo politiky, ako napríklad pre európsky program Globálneho navigačného satelitného systému (GNSS) ([1]).

Riadiace zásady

Pri práci na dosahovaní cieľov, identifikácii potrebných činností a prideľovaní úloh a zodpovedností príslušným aktérom alebo mechanizmom sa uplatnili tieto riadiace zásady, ktoré treba rešpektovať aj pri príprave budúcich vykonávacích usmernení.

Proporcionalita: Veľká väčšina kybernetických incidentov zasahujúcich členské štáty ani zďaleka nedosahuje úroveň, ktorá by sa dala považovať za vnútroštátnu, a o to menej európsku „krízu". Základom spolupráce medzi členskými štátmi v reakcii na takéto incidenty je sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT) zriadená smernicou NIS ([2]). Vnútroštátne jednotky CSIRT dobrovoľne spolupracujú a vymieňajú si informácie na každodennom základe, podľa potreby aj v reakcii na kybernetické incidenty zasahujúce jeden alebo viacero členských štátov, v súlade so štandardnými operačnými postupmi (SOP) siete CSIRT. Koncepcia by preto mala tieto SOP v plnej miere využiť a mali by sa v nej premietnuť všetky prípadné ďalšie úlohy špecifické pre kybernetické krízy.

([1]) Rozhodnutie 2014/496/SZBP.
([2]) Smernica (EÚ) 2016/1148.

Subsidiarita: Zásada subsidiarity je kľúčová. Členské štáty samotné nesú primárnu zodpovednosť za reakciu na rozsiahle kybernetické incidenty alebo krízy, ktoré ich zasiahnu. Významnú rolu však zohráva aj Komisia, Európska služba pre vonkajšiu činnosť a ostatné inštitúcie, orgány, úrady a agentúry EÚ. Táto rola je jasne vymedzená v dojednaniach IPCR, no vyplýva aj z práva Únie či jednoducho zo skutočnosti, že kybernetické incidenty a krízy môžu mať dosah na všetky odvetvia hospodárskej činnosti na jednotnom trhu, bezpečnosť a medzinárodné vzťahy Únie, ako aj na samotné inštitúcie.

Komplementárnosť: Koncepcia plne zohľadňuje existujúce mechanizmy krízového riadenia na úrovni EÚ, konkrétne integrované dojednania EÚ o politickej reakcii na krízu (IPCR), ARGUS, krízový reakčný mechanizmus ESVČ, a začleňuje do nich nové štruktúry a mechanizmy podľa smernice NIS, a to sieť CSIRT, ako aj príslušné agentúry a orgány – konkrétne Agentúru Európskej únie pre sieťovú bezpečnosť a informačnú bezpečnosť (ENISA), Európske centrum boja proti počítačovej kriminalite (Europol/EC3), Centrum EÚ pre analýzu spravodajských informácií (INTCEN), Spravodajský útvar Vojenského štábu EÚ (EUMS INT) a situačné stredisko (SITROOM) v rámci centra INTCEN, ktoré spolupracujú v rámci jednotnej kapacity na analýzu spravodajských informácií; stredisko EÚ pre hybridné hrozby (zriadené v rámci centra INTCEN) a tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU). Koncepcia by pritom mala zároveň zabezpečiť, aby sa tieto subjekty vo vzájomnej interakcii a spolupráci v maximálnej možnej miere dopĺňali a aby sa ich činnosti čo najmenej prekrývali.

Dôvernosť informácií: Všetka výmena informácií v kontexte koncepcie musí rešpektovať platné pravidlá bezpečnosti ([1]), ochrany osobných údajov a semaforového protokolu ([2]). Pri výmene utajovaných skutočností bez ohľadu na použitý systém klasifikácie sa použijú dostupné akreditované nástroje ([3]). Pri spracovaní osobných údajov treba dodržiavať platné pravidlá EÚ, najmä všeobecné nariadenie o ochrane údajov ([4]), smernicu o súkromí a elektronických komunikáciách ([5]), ako aj nariadenie ([6])„o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami EÚ a o voľnom pohybe takýchto údajov“.

Hlavné ciele

Spolupráca podľa tejto koncepcie prebieha na troch už spomínaných úrovniach – politickej, operačnej a technickej. Na každej z nich môže spolupráca zahŕňať výmenu informácií, ako aj spoločné kroky, a má nasledujúce základné ciele.

— Umožniť účinnú reakciu: reakcia môže mať mnoho podôb od identifikácie technických opatrení, ktoré môžu zahŕňať dva alebo viacero subjektov spoločne vyšetrujúcich technické príčiny incidentu (napr. analýza škodlivého softvéru), cez určenie, ako môžu organizácie posúdiť, či sa ich incident dotkol (napr. ukazovatele narušenia) až po operačné rozhodnutia o uplatnení takýchto technických opatrení a na politickej úrovni rozhodnutia o aktivácii iných nástrojov v závislosti od daného incidentu, ako napríklad diplomatická reakcia EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“) alebo operačný protokol EÚ na boj proti hybridným hrozbám.

— Šíriť spoločné situačné povedomie: koordinovaná reakcia si vyžaduje, aby všetky relevantné subjekty na všetkých troch úrovniach (technickej, operačnej i politickej) dostatočne chápali udalosti, ktoré sa odohrávajú. Situačné povedomie môže zahŕňať technologické prvky príčin, ale aj dosahu a pôvodu daného incidentu. Keďže kybernetické incidenty môžu mať vplyv na mnoho rôznych odvetví (finančníctvo, energetika, doprava, zdravotníctvo atď.), je kľúčové, aby sa primerané informácie vo vhodnej forme dostali ku všetkým relevantným subjektom načas.

([1]) Rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii (Ú. v. EÚ L 72, 17.3.2015, s. 41) a rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53); rozhodnutie vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku z 19. apríla 2013 o bezpečnostných pravidlách Európskej služby pre vonkajšiu činnosť (Ú. v. EÚ C 190, 29.6.2013, s. 1); rozhodnutie Rady 2013/488/EÚ z 23. septembra 2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 274, 15.10.2013, s. 1).

([2]) https://www.first.org/tlp/.

([3]) V júni 2016 zahŕňali tieto prenosové kanály CIMS (systém správy utajovaných skutočností), ACID (šifrovací algoritmus), RUE (zabezpečený systém vytvárania, výmeny a ukladania dokumentov klasifikovaných ako RESTREINT UE/EU RESTRICTED) a sieť SOLAN. Medzi ďalšie prostriedky napr. na prenos utajovaných skutočností patrí PGP alebo S/MIME.

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

([5]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

([6]) Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1) – v procese preskúmania.

— Dohodnúť sa na kľúčových informáciách pre verejnosť ([1]): krízová komunikácia zohráva zásadnú rolu pri zmierňovaní škodlivých účinkov kybernetických incidentov a kríz, no dá sa použiť aj na ovplyvnenie správania (potenciálnych) útočníkov. Vhodné posolstvá môžu zároveň jasne poukázať na pravdepodobné dôsledky diplomatickej reakcie na ovplyvnenie správania útočníkov. Aby bola politická reakcia účinná, je nevyhnutné zosúladiť verejnú komunikáciu na zmiernenie negatívneho vplyvu kybernetických incidentov a kríz s verejnou komunikáciou na ovplyvnenie útočníka. Z hľadiska kybernetickej bezpečnosti je osobitne dôležité šírenie presných a užitočných informácií o tom, ako môže verejnosť zmierniť účinky incidentu (napríklad inštalácia tzv. záplat – patchov, doplnkové spôsoby, ako sa vyhnúť hrozbe, atď.).

SPOLUPRÁCA MEDZI ČLENSKÝMI ŠTÁTMI A MEDZI ČLENSKÝMI ŠTÁTMI A AKTÉRMI EÚ NA TECHNICKEJ, OPERAČNEJ A STRATEGICKEJ/POLITICKEJ ÚROVNI

Účinná reakcia na rozsiahle kybernetické incidenty alebo krízy na úrovni EÚ závisí od účinnej technickej, operačnej a strategickej/politickej spolupráce.

Na každej z týchto úrovní by mali zapojení aktéri vykonať konkrétne činnosti smerujúce k dosiahnutiu troch hlavných cieľov:

— koordinovanej reakcie,

— spoločného situačného povedomia,

— komunikácie s verejnosťou.

Počas trvania incidentu alebo krízy podradené úrovne spolupráce varujú, informujú a podporujú nadradené úrovne a tie zas podradeným úrovniam poskytujú usmernenia ([2]) a podľa potreby prijímajú rozhodnutia.

Spolupráca na technickej úrovni

Rozsah činností:

— Riešenie incidentov ([3]) počas kybernetickej krízy

— Monitorovanie incidentov a dohľad nad nimi vrátane nepretržitej analýzy hrozieb a rizík.

Potenciálni aktéri:

Na technickej úrovni je ústredným mechanizmom spolupráce podľa tejto koncepcie sieť jednotiek CSIRT, ktorej predsedá predsedníctvo a funkciu sekretariátu zabezpečuje agentúra ENISA.

— Členské štáty:

  — príslušné orgány a jednotné kontaktné miesta zriadené podľa smernice NIS

  — jednotky CSIRT

— Orgány/úrady/agentúry EÚ

  — ENISA

  — Europol/EC3

  — CERT-EU

([1]) Tu treba podotknúť, že verejná komunikácia môže znamenať tak poskytovanie informácií o incidente širokej verejnosti, ako aj technickejšie alebo operačnejšie informácie pre kľúčové odvetvia a/alebo zasiahnutých aktérov. To si môže vyžadovať použitie dôverných informačných kanálov a špecifických technických nástrojov či platforiem. V oboch prípadoch je komunikácia s individuálnymi subjektmi a širokou verejnosťou v ktoromkoľvek členskom štáte kompetenciou a zodpovednosťou daného členského štátu. Preto nesú v súlade so spomínanou zásadou subsidiarity členské štáty a národné jednotky CSIRT konečnú zodpovednosť za informácie, ktoré sa oznamujú na ich území, resp. ich občanom.

([2]) „Povolenie konať“ – pri kybernetickej kríze je rozhodujúci krátky reakčný čas na stanovenie primeraných zmierňujúcich opatrení. Aby sa tento krátky reakčný čas dosiahol, môže jeden členský štát druhému dobrovoľne udeliť „povolenie konať“, čím mu povolí okamžite prijať kroky bez potreby konzultácie s vyššími úrovňami alebo inštitúciami EÚ a bez absolvovania bežne vyžadovaného postupu úradnou cestou, ak sa to pri danom incidente nevyžaduje (napr. jednotka CSIRT by nemala byť povinná konzultovať s vyššími úrovňami postupovanie cenných informácií jednotke CSIRT v inom členskom štáte).

([3]) „Riešenie incidentov“ zahŕňa všetky postupy na podporu odhaľovania, analýzy a obmedzenia následkov incidentu a reakcie naň.

— Európska komisia

  — koordinačné centrum pre reakcie na núdzové situácie – ERCC (nepretržitá operačná služba v rámci GR ECHO) a určený vedúci útvar (ktorý sa zvolí spomedzi GR CNECT a GR HOME v závislosti od konkrétnej povahy incidentu), generálny sekretariát (sekretariát systému ARGUS), GR pre ľudské zdroje (riaditeľstvo pre bezpečnosť), GR DIGIT (riaditeľstvo pre informatickú bezpečnosť – operačný odbor)

  — pri ostatných agentúrach EÚ ([1]) príslušné gestorské GR Komisie alebo ESVČ (prvá kontaktná úroveň)

— ESVČ

  — SIAC (jednotná kapacita na analýzu spravodajských informácií: EU INTCEN a EUMS INT)

  — situačné stredisko EÚ a zvolený geografický alebo tematický útvar.

  — stredisko EÚ pre hybridné hrozby (v rámci EU INTCEN – kybernetická bezpečnosť v kontexte hybridných hrozieb)

Spoločné situačné povedomie:

— Vrámci bežnej technickej spolupráce na podporu situačného povedomia Únie by mala agentúra ENISA pravidelne pripravovať technickú situačnú správu EÚ v oblasti kybernetickej bezpečnosti, ktorá opisuje incidenty a hrozby a vychádza z verejne dostupných informácií, vlastných analýz a správ, ktoré jej (dobrovoľne) poskytli jednotky CSIRT členských štátov alebo jednotné kontaktné miesta podľa smernice NIS, Európske centrum boja proti počítačovej kriminalite (EC3) v rámci Europolu a CERT-EU a v náležitých prípadoch centrum EÚ pre spravodajské informácie (INTECEN) v rámci Európskej služby pre vonkajšiu činnosť (ESVČ). Táto správa by sa mala sprístupniť zodpovedným útvarom Rady, Komisie, VP/PK a sieti CSIRT.

— Pri závažných incidentoch predseda siete CSIRT vypracuje s pomocou agentúry ENISA situačnú správu EÚ o kybernetických incidentoch ([2]), ktorá sa predkladá predsedníctvu, Komisii a VP/PK prostredníctvom jednotky CSIRT rotujúceho predsedníctva.

— Všetky ostatné agentúry EÚ zodpovedajú svojmu príslušnému gestorskému GR, ktoré zas zodpovedá vedúcemu útvaru Komisie.

— CERT-EU poskytuje technické správy sieti CSIRT, inštitúciám a agentúram EÚ (podľa potreby) a systému ARGUS (ak sa aktivuje).

— Europol/EC3 a CERT-EU ([3]) zabezpečujú expertnú forenznú analýzu technických artefaktov a iných technických informácií pre sieť CSIRT.

— ESVČ SIAC: stredisko EÚ pre hybridné hrozby podáva v mene INTCEN správu príslušným odborom ESVČ.

Reakcia:

— Sieť jednotiek CSIRT si vymieňa technické podrobnosti a analýzy incidentu ako IP adresy, ukazovatele narušenia ([4]) atď. Tieto informácie by sa mali bez zbytočného odkladu, no najneskôr do 24 hodín od odhalenia incidentu poskytnúť agentúre ENISA.

— Členovia siete jednotiek CSIRT v súlade s jej štandardnými operačnými postupmi spolupracujú v snahe analyzovať dostupné technické artefakty a ďalšie technické informácie spojené s incidentom, aby identifikovali príčinu a možné zmierňujúce technické opatrenia.

— Agentúra ENISA v súlade so svojím mandátom ([5]) podporuje jednotky CSIRT v ich technických činnostiach, ktoré sa opierajú o jej odborné znalosti.

([1]) V závislosti od povahy a vplyvu incidentu na rôzne odvetvia činnosti (finančníctvo, doprava, energetika, zdravotníctvo atď.) sa zapoja relevantné agentúry alebo orgány EÚ.

([2]) Situačná správa EÚ o kybernetických incidentoch predstavuje súhrn vnútroštátnych správ, ktoré poskytli jednotky CSIRT jednotlivých členských štátov. Formát správy by mal byť opísaný v štandardných operačných postupoch siete jednotiek CSIRT.

([3]) V súlade s podmienkami a postupmi stanovenými v právnom rámci upravujúcom činnosť EC3.

([4]) Ukazovateľ narušenia (indicator of compromise – IOC) v rámci forenznej počítačovej analýzy znamená artefakt zistený v sieti alebo operačnom systéme, ktorý s vysokou mierou spoľahlivosti poukazuje na vniknutie do systému. Medzi bežné IOC patria tzv. podpisy vírusov, IP adresy, MD5 heše alebo škodlivé súbory či URL alebo doménové názvy botnetových C&C serverov.

([5]) Návrh nariadenia o Agentúre Európskej únie pre sieťová a informačnú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o kybernetickej bezpečnostnej certifikácii informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“), 13. september 2017.

— Jednotky CSIRT členských štátov koordinujú svoju technickú reakciu za pomoci agentúry ENISA a Komisie.

— ESVČ SIAC: stredisko EÚ pre hybridné hrozby aktivuje v mene INTCEN proces zberu počiatočných dôkazov.

Komunikácia s verejnosťou:

— Jednotky CSIRT vypracujú technické varovania ([1]) a upozornenia na zraniteľnosť ([2]), ktoré distribuujú v príslušných komunitách a na verejnosti podľa autorizačných postupov platných pre každý individuálny prípad.

— Agentúra ENISA pomáha pri vypracúvaní a šírení spoločných komunikačných materiálov siete jednotiek CSIRT.

— Agentúra ENISA koordinuje svoju verejnú komunikáciu so sieťou jednotiek CSIRT a útvarom hovorcu Komisie.

— Agentúra ENISA a EC3 koordinujú svoju verejnú komunikáciu na základe spoločného situačného povedomia, na ktorom sa zhodnú členské štáty. Oba subjekty koordinujú svoju verejnú komunikáciu s útvarom hovorcu Komisie.

— Ak sa kríza dotýka externej alebo spoločnej bezpečnostnej a obrannej politiky (SBOP), komunikácia s verejnosťou by sa mala koordinovať s ESVČ a útvarom hovorcu VP/PK.

Spolupráca na operačnej úrovni

Rozsah činností:

— príprava rozhodnutí na politickej úrovni

— koordinácia riadenia kybernetickej krízy (podľa potreby)

— vyhodnotenie dôsledkov a vplyvov na úrovni EÚ a návrh možných zmierňujúcich opatrení

Potenciálni aktéri:

— Členské štáty:

  — príslušné orgány a jednotné kontaktné miesta zriadené podľa smernice NIS

  — jednotky CSIRT, agentúry kybernetickej bezpečnosti

  — iné vnútroštátne rezortné orgány (v prípade incidentov alebo kríz zahŕňajúcich viacero odvetví)

— Orgány/úrady/agentúry EÚ

  — ENISA

  — Europol/EC3

  — CERT-EU

— Európska komisia

  — generálny tajomník (alebo jeho zástupca) SG (proces ARGUS)

  — GR CNECT/HOME

  — bezpečnostný orgán Komisie

  — iné GR (v prípade incidentov alebo kríz zahŕňajúcich viacero odvetví)

([1]) Odporúčania technickej povahy, ktoré zahŕňajú príčiny incidentu a možné zmierňujúce kroky.
([2]) Informácie o zraniteľných technických prvkoch, ktoré sa zneužívajú na poškodenie IT systémov.

— ESVČ

  — generálny tajomník zodpovedný za krízové riadenie (alebo jeho zástupca) a SIAC (EU INTCEN a EUMS INT)

  — stredisko EÚ pre hybridné hrozby

— Rada

  — predsedníctvo (predseda horizontálnej pracovnej skupiny pre kybernetické otázky alebo Coreper ([1])) s podporou Generálneho sekretariátu Rady alebo Politického a bezpečnostného výboru (PBV) ([2]) a v prípade aktivácie s podporou dojednaní IPCR

Situačné povedomie:

— podpora pri príprave politicko-strategických situačných správ (napr. správa o ISAA v prípade aktivácie IPCR)

— Horizontálna pracovná skupina Rady pre kybernetické otázky pripravuje stretnutia Coreperu, prípadne PBV

— v prípade aktivácie dojednaní IPCR

  — Predsedníctvo môže zvolať stretnutia za okrúhlym stolom na podporu prípravy na Coreper alebo PBV, pričom prizve relevantné zainteresované subjekty z členských štátov, inštitúcie, agentúry a tretie strany ako napr. tretie krajiny a medzinárodné organizácie. Ide o krízové stretnutia na identifikáciu problémov a prípravu návrhov činnosti v prierezových otázkach.

  — Vedúci útvar Komisie alebo ESVČ ako vedúci orgán procesu ISAA vypracuje správu o ISAA s príspevkami od agentúry ENISA, siete jednotiek CSIRT, Europolu/EC3, EUMS INT, INTCEN a všetkých ďalších relevantných aktérov. Správa o ISAA je celoúnijným hodnotením na základe posúdenia korelácie technických incidentov a kríz (analýza hrozieb, posúdenie rizika, netechnické dôsledky a vplyvy, nekybernetické aspekty daného incidentu alebo krízy atď.), ktorá zodpovedá potrebám operačnej a politickej úrovne.

— v prípade aktivácie systému ARGUS

  — CERT-EU a EC3 ([3]) priamo prispievajú k výmene informácií s Komisiou

— V prípade aktivácie krízového reakčného mechanizmu ESVČ:

  — SIAC zintenzívni zber informácií, zhrnie informácie zo všetkých zdrojov a vypracuje analýzu a posúdenie incidentu.

Reakcia (na žiadosť z politickej úrovne):

— cezhraničná spolupráca s jednotným kontaktným miestom a vnútroštátnymi príslušnými orgánmi (smernica NIS) na zmiernenie dôsledkov a vplyvov

— aktivácia všetkých technických zmierňujúcich opatrení a koordinácia technických kapacít potrebných na zastavenie alebo obmedzenie vplyvu útokov na napadnuté informačné systémy

— spolupráca, a ak sa tak rozhodne, koordinácia technických kapacít v záujme spoločnej alebo kolaboratívnej reakcie v súlade so ***štandardnými operačnými postupmi siete jednotiek CSIRT***

— vyhodnotenie potreby spolupráce s relevantnými tretími stranami

— (v prípade aktivácie) rozhodovanie v rámci procesu ARGUS

— (v prípade aktivácie) príprava rozhodnutí a koordinácia v rámci dojednaní IPCR

— (v prípade aktivácie) podpora rozhodovania ESVČ v rámci krízového reakčného mechanizmu ESVČ, a to aj z hľadiska kontaktu s tretími krajinami a medzinárodnými organizáciami, ako aj všetkých opatrení zameraných na ochranu misií a operácií SBOP a delegácií EÚ

([1]) Výbor stálych predstaviteľov známy aj ako Coreper (článok 240 Zmluvy o fungovaní Európskej únie – ZFEÚ) je zodpovedný za prípravu práce Rady Európskej únie.

([2]) Politický a bezpečnostný výbor je výbor Rady Európskej únie, ktorý sa zaoberá spoločnou zahraničnou a bezpečnostnou politikou (SZBP), ktorá sa spomína v článku 38 Zmluvy o Európskej únii.

([3]) V súlade s podmienkami a postupmi stanovenými v právnom rámci upravujúcom činnosť EC3.

Komunikácia s verejnosťou:

— dohoda na informáciách o incidente určených pre verejnosť

— ak sa kríza dotýka externej alebo spoločnej bezpečnostnej a obrannej politiky (SBOP), komunikácia s verejnosťou by sa mala koordinovať s ESVČ a útvarom hovorcu VP/PK.

Spolupráca strategickej/politickej úrovni

Potenciálni aktéri:

— za členské štáty ministerstvá zodpovedné za kybernetickú bezpečnosť

— za Európsku radu jej predseda

— za Radu rotujúce predsedníctvo

— pri opatreniach v rámci „súboru kybernetických nástrojov" PBV a Horizontálna pracovná skupina

— za Európsku komisiu predseda alebo určený podpredseda/komisár

— vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku/podpredseda Európskej komisie

Rozsah činností: strategické a politické riadenie kybernetických i nekybernetických aspektov krízy vrátane opatrení spadajúcich do rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti

Spoločné situačné povedomie:

— identifikácia vplyvov narušení spôsobených krízou na fungovanie Únie

Reakcia:

— aktivácia ďalších mechanizmov/nástrojov krízového riadenia v závislosti od povahy a dosahu incidentu – môže ísť napríklad o mechanizmus civilnej ochrany

— prijatie opatrení spadajúcich do rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti

— sprístupnenie núdzovej podpory zasiahnutým členským štátom, napríklad aktiváciou núdzového fondu kybernetickej bezpečnostnej reakcie ([1]) po jeho zriadení

— podľa potreby spolupráca a koordinácia s medzinárodnými organizáciami vrátane Organizácie Spojených národov (OSN), Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE), a najmä NATO

— vyhodnotenie dôsledkov pre vnútroštátnu bezpečnosť a obranu

Komunikácia s verejnosťou:

rozhodnutie o spoločnej stratégii komunikácie s verejnosťou.

KOORDINOVANÁ REAKCIA S ČLENSKÝMI ŠTÁTMI NA ÚROVNI EÚ V RÁMCI DOJEDNANÍ IPCR

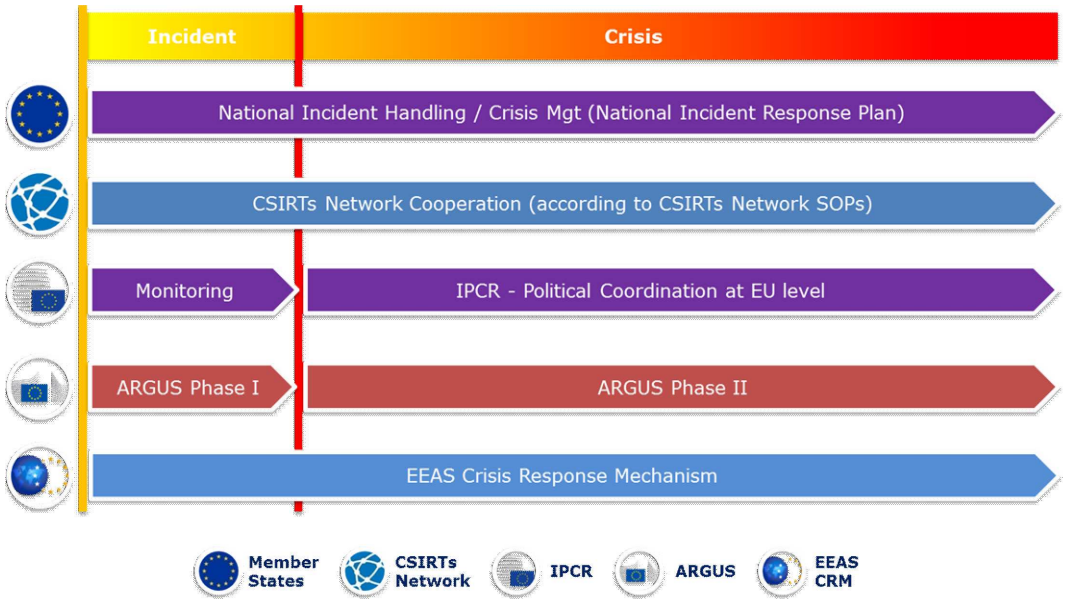
V súlade so zásadou komplementárnosti na úrovni EÚ tento oddiel predstavuje a zameriava sa najmä na hlavný cieľ a zodpovednosti a činnosti orgánov členských štátov, siete jednotiek CSIRT, agentúry ENISA, CERT-EU, Europolu/EC3, INTCENu, strediska EÚ pre hybridné hrozby a horizontálnej pracovnej skupiny Rady pre kybernetické otázky v procese IPCR. Predpokladá sa, že všetci aktéri budú konať v súlade so zavedenými postupmi na únijnej, resp. vnútroštátnej úrovni.

Treba poznamenať, že ako znázorňuje obrázok 1, bez ohľadu na aktiváciu mechanizmov krízového riadenia EÚ, pri všetkých incidentoch/krízach sa činnosti na vnútroštátnej úrovni i spolupráca v rámci siete jednotiek CSIRT (podľa potreby) riadia zásadami subsidiarity a proporcionality.

([1]) Núdzový fond kybernetickej bezpečnosti sa ako opatrenie navrhuje v spoločnom oznámení s názvom „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ", JOIN(2017) 450/1.

Obrázok 1

Reakcia na kybernetický incident/krízu na úrovni EÚ



Všetky ďalej uvedené činnosti sa musia vykonať v súlade so štandardnými operačnými postupmi/pravidlami uplatňovaných mechanizmov spolupráce a na základe stanovených mandátov a zodpovedností jednotlivých aktérov a inštitúcií. V záujme čo najlepšej spolupráce a účinnej reakcie na rozsiahle kybernetické incidenty a krízy môže byť potrebné tieto postupy/pravidlá doplniť alebo upraviť.

Pre každý individuálny incident platí, že nie všetci z uvedených aktérov musia nevyhnutne prijímať opatrenia. Koncepcia i príslušné štandardné operačné postupy mechanizmov spolupráce by však mali s ich potenciálnym zapojením počítať.

Vzhľadom na odlišné miery možného dosahu konkrétnych kybernetických incidentov a kríz na spoločnosť si vysoká flexibilita zapojenia odvetvových subjektov na všetkých úrovniach a primeraná reakcia vyžaduje tak kybernetické, ako aj nekybernetické zmierňovacie opatrenia.

Riadenie kybernetických kríz – integrácia kybernetickej bezpečnosti v procese IPCR

Dojednania IPCR opísané v štandardných operačných postupoch IPCR ([1]) sa riadia postupnosťou krokov, ktorá je opísaná nižšie (uplatnenie niektorých z nich bude závisieť od konkrétnej situácie).

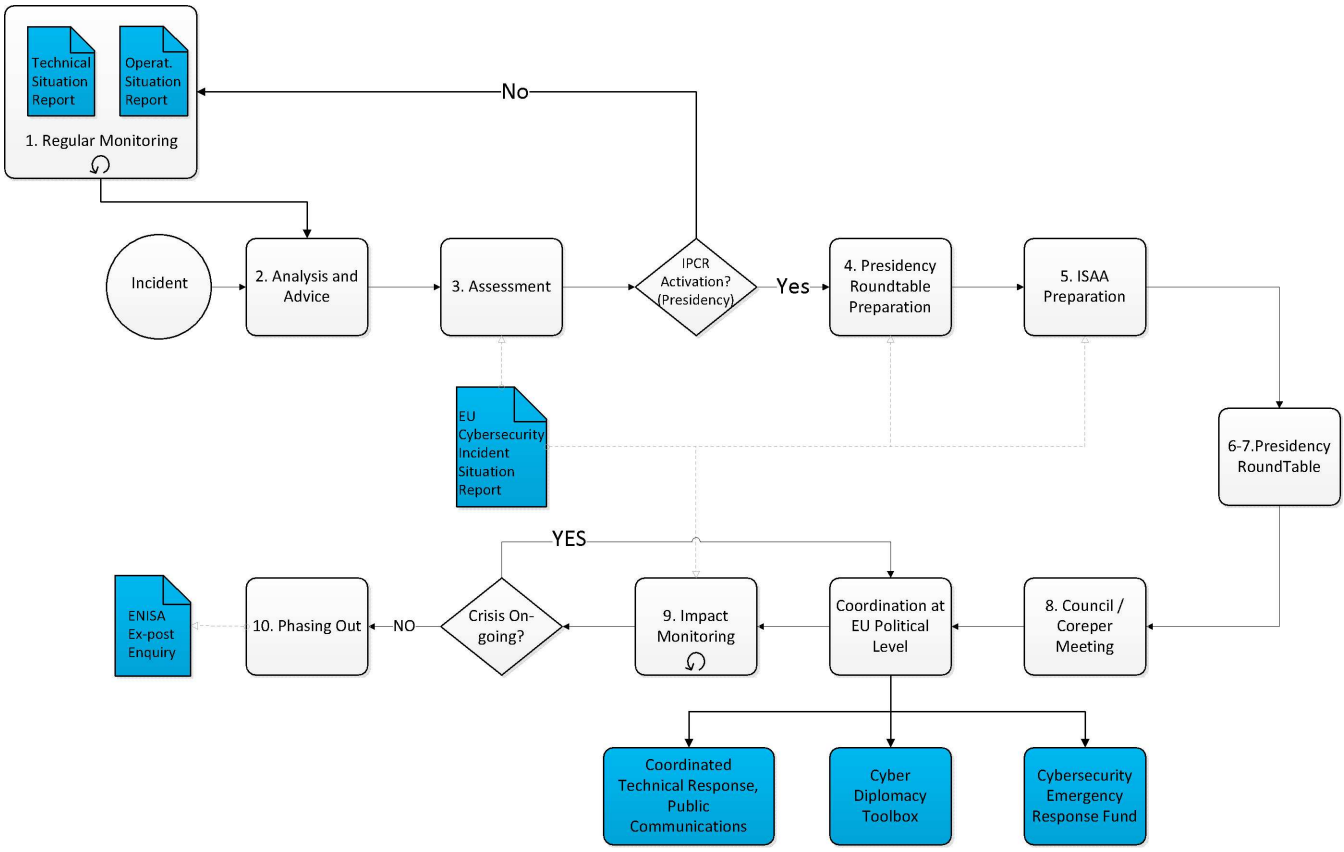
Pri každom kroku uvádzame činnosti spojené s kybernetickou bezpečnosťou i príslušných aktérov. V záujme lepšej čitateľnosti sa pri každom kroku uvádza text zo štandardných operačných postupov IPCR, za ktorým nasledujú činnosti podľa koncepcie. Tento postupný prístup zároveň umožňuje jasnú identifikáciu existujúcich **nedostatkov** v potrebných spôsobilostiach a postupoch, ktoré komplikujú účinnú reakciu na kybernetické krízy.

Na obrázku 2 nižšie ([2]) je graficky znázornený proces IPCR, pričom novozavedené prvky sú zvýraznené modrou.

([1]) Z dokumentu 12607/15 „Štandardné operačné postupy IPCR“, ktoré schválila skupina priateľov predsedníctva a ktoré vzal Coreper na vedomie v októbri 2015.
([2]) Zväčšenina obrázka je priložená v dodatku.

Obrázok 2

Prvky IPCR, ktoré sa týkajú kybernetickej bezpečnosti



Poznámka: Vzhľadom na povahu hybridných hrozieb v kybernetickej oblasti, ktoré sú koncipované tak, aby neprekročili prah rozpoznateľnej krízy, musí EÚ prijať opatrenia na prevenciu a zaistenie pripravenosti. Úlohou strediska EÚ pre hybridné hrozby je rýchlo analyzovať relevantné incidenty a informovať príslušné koordinačné štruktúry. Pravidelné správy strediska môžu prispieť k informovaniu tvorcov politiky v jednotlivých odvetviach a posilniť pripravenosť.

— **Krok 1 – Pravidelné odvetvové monitorovanie a varovanie**: existujúce pravidelné sektorové situačné správy a výstrahy upozorňujú predsedníctvo Rady na vznikajúcu krízu a jej možný vývoj;

— **Zistený nedostatok**: Momentálne na úrovni EÚ neexistujú žiadne pravidelné a koordinované situačné správy a varovania o kybernetických incidentoch (a hrozbách).

— **Koncepcia: Monitorovanie situácie a podávanie správ o kybernetickej bezpečnosti na úrovni EÚ**

— Agentúra ENISA bude **pravidelne pripravovať technickú situačnú správu EÚ v oblasti kybernetickej bezpečnosti** o kybernetických incidentoch a hrozbách, ktorá vychádza z verejne dostupných informácií, jej vlastných analýz a správ, ktoré jej (dobrovoľne) poskytli jednotky CSIRT členských štátov alebo jednotné kontaktné miesta podľa smernice NIS, Európske centrum boja proti počítačovej kriminalite (EC3) v rámci Europolu, CERT-EU a centrum EÚ pre spravodajské informácie (INTECEN) v rámci Európskej služby pre vonkajšiu činnosť (ESVČ). Táto správa by sa mala sprístupniť zodpovedným útvarom Rady, Komisie a sieti jednotiek CSIRT.

— V mene SIAC by malo stredisko EÚ pre hybridné hrozby pripravovať **operačnú situačnú správu EÚ v oblasti kybernetickej bezpečnosti**. Správa zároveň podporuje rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti.

— Obe správy sa poskytnú zainteresovaným stranám na úrovni EÚ i členských štátov s cieľom zvýšiť ich situačné povedomie, zabezpečiť informácie potrebné pre rozhodovanie a uľahčiť cezhraničnú regionálnu spoluprácu.

Po odhalení incidentu

— **Krok 2 – analýza a poradenstvo**: na základe dostupného monitorovania a varovania sa útvary Komisie, ESVČ a GSR navzájom informujú o možnom vývoji, aby boli pripravené poskytnúť predsedníctvu poradenstvo, pokiaľ ide o prípadnú aktiváciu (v celom rozsahu alebo v režime výmeny informácií) IPCR;

— **Koncepcia:**

— Za Komisiu GR CNECT, GR HOME, GR HR.DS a GR DIGIT s podporou agentúry ENISA, EC3 a CERT-EU.

— ESVČ. V nadväznosti na prácu SITROOM a spravodajské zdroje zabezpečuje stredisko EÚ pre hybridné hrozby situačné povedomie o skutočných a potenciálnych hybridných hrozbách ovplyvňujúcich EÚ a jej partnerov vrátane kybernetických hrozieb. Preto ak sa v analýze a posúdení vykonaných strediskom EÚ pre hybridné hrozby naznačí existencia možných hrozieb namierených proti členskému štátu, partnerskej krajine alebo organizácii, INTCEN bude podľa stanovených postupov (najprv) informovať na operačnej úrovni. Na operačnej úrovni sa potom pripravia odporúčania pre politicko-strategickú úroveň vrátane možnej aktivácie mechanizmov krízového riadenia v režime monitorovania (napr. krízový reakčný mechanizmus ESVČ alebo monitorovacia stránka IPCR).

— Predseda siete jednotiek CSIRT s pomocou agentúry ENISA vypracuje situačnú správu EÚ o kybernetických incidentoch ([1]), ktorú jednotka CSIRT rotujúceho predsedníctva predloží predsedníctvu, Komisii a VP/PK.

— **Krok 3 – Posúdenie/rozhodnutie o aktivácii IPCR**: predsedníctvo vyhodnotí potrebu politickej koordinácie, výmeny informácií alebo rozhodovania na úrovni EÚ. Na tento účel môže predsedníctvo zvolať neformálne stretnutie za okrúhlym stolom. Predsedníctvo vykoná počiatočnú identifikáciu oblastí, ktoré si vyžadujú zapojenie Coreperu alebo Rady. Táto identifikácia bude základom usmernenia na vypracovanie správ o integrovanom situačnom povedomí a analýze (ISAA). Podľa povahy krízy, jej možných dôsledkov a súvisiacich politických potrieb rozhodne predsedníctvo o vhodnosti zvolania stretnutí príslušných pracovných skupín Rady a/alebo Coreperu a/alebo PBV.

— **Koncepcia:**

— Účastníci okrúhleho stola:

— Útvary Komisie a ESVČ poskytnú predsedníctvu poradenstvo v oblastiach, v ktorých majú príslušné kompetencie.

— Zástupcovia členských štátov v horizontálnej pracovnej skupine pre kybernetické otázky s podporou expertov z hlavných zainteresovaných subjektov (jednotky CSIRT, príslušné orgány v oblasti kybernetickej bezpečnosti a ďalšie).

— Politické/strategické usmernenia pre správy o ISAA založené na najnovšej situačnej správe EÚ o kybernetických incidentoch a ďalších informáciách od účastníkov okrúhleho stola.

— Príslušné pracovné skupiny a výbory:

— horizontálna pracovná skupina pre kybernetické otázky.

Komisia, ESVČ a GSR po vzájomnej dohode a v spolupráci s predsedníctvom môžu rozhodnúť aj o aktivácii IPCR v režime výmeny informácií vytvorením krízovej stránky, aby sa pripravili podmienky pre prípadnú úplnú aktiváciu.

— **Krok 4 – Aktivácia IPCR/zhromažďovanie a výmena informácií**: po aktivácii (či už v režime výmeny informácií alebo úplnej aktivácii) sa na webovej platforme IPCR vytvorí krízová stránka, ktorá umožní špecifické výmeny informácií so zameraním na aspekty, ktoré prispejú k informovaniu na účely ISAA a príprave diskusie na politickej úrovni. Vedúci útvar ISAA (jeden z útvarov Komisie alebo ESVČ) bude určený v závislosti od okolností prípadu.

— **Krok 5 – vypracovanie správ o ISAA**: začne sa vypracovanie správ o ISAA. Komisia/ESVČ vydá správy o ISAA v súlade so štandardnými operačnými postupmi ISAA, a môže ďalej podporovať výmenu informácií na webovej

([1]) Situačná správa EÚ o kybernetických incidentoch predstavuje súhrn vnútroštátnych správ, ktoré poskytli jednotky CSIRT jednotlivých členských štátov. Formát správy by mal byť opísaný v štandardných operačných postupoch siete jednotiek CSIRT.

platforme IPCR alebo vydávať konkrétne žiadosti o informácie. Správy o ISAA budú prispôsobené potrebám danej politickej úrovne (t. j. Coreperu alebo Rade), ako to predsedníctvo vymedzilo a stanovilo vo svojich usmerneniach, čo umožní získať strategický prehľad o situácii a fundovanú diskusiu o bodoch programu, ktoré určilo predsedníctvo. V súlade so štandardnými operačnými postupmi na účely ISAA sa na základe povahy kybernetickej krízy rozhodne o tom, či správu o ISAA vypracuje jeden z útvarov Komisie (GR CNECT, GR HOME) alebo ESVČ.

Po aktivácii IPCR predsedníctvo navrhne v súvislosti s ISAA osobitné oblasti zamerania, s cieľom podporiť politickú koordináciu a/alebo rozhodovací proces v Rade. Predsedníctvo takisto po porade s útvarmi Komisie/ESVČ uvedie termín vydania správy;

— **Koncepcia:**

— Správa o ISAA obsahuje príspevky príslušných útvarov vrátane:

— siete jednotiek CSIRT, ktorá ich poskytla vo forme situačnej správy EÚ o kybernetických incidentoch;

— EC3, SITROOM-u, strediska EÚ pre hybridné hrozby, CERT-EU. Stredisko EÚ pre hybridné hrozby bude podľa potreby podporovať vedúci útvar ISAA a okrúhly stôl IPCR a poskytovať im informácie.

— Odvetvové agentúry a orgány EÚ závislé na dotknutých sektoroch

— orgány členských štátov (iné ako jednotky CSIRT).

— Zhromažďovanie vstupov týkajúcich sa ISAA ([1]):

— Komisia a agentúry EÚ: IT systém ARGUS zabezpečí pre ISAA vnútornú chrbticovú sieť. Agentúry EÚ budú zasielať svoje príspevky svojim príslušným zodpovedným generálnym riaditeľstvám, ktoré vložia príslušné informácie do systému ARGUS. Útvary Komisie a agentúry budú s členskými štátmi a medzinárodnými organizáciami zhromažďovať informácie z existujúcich odvetvových sietí a z iných relevantných zdrojov.

— Za ESVČ: situačné stredisko EÚ s podporou ďalších príslušných útvarov ESVČ zabezpečí pre ISAA vnútornú chrbticovú sieť a jednotné kontaktné miesto. ESVČ bude zhromažďovať informácie z tretích krajín a príslušných medzinárodných organizácií.

— **Krok 6 – Príprava neformálneho stretnutia za okrúhlym stolom organizovaného predsedníctvom**: predsedníctvo, ktorému pomáha Generálny sekretariát Rady, určí termín, program, účastníkov a očakávané výsledky (možné výstupy) tohto neformálneho stretnutia za okrúhlym stolom. GSR bude v mene predsedníctva dopĺňať relevantné informácie na webovú platformu IPCR a vydá najmä oznámenie o stretnutí;

— **Krok 7 – Stretnutie za okrúhlym stolom organizované predsedníctvom/prípravné opatrenia pre politickú koordináciu/rozhodovací proces EÚ**: predsedníctvo zvolá neformálne stretnutie za okrúhlym stolom s cieľom preskúmať situáciu a pripraviť a preskúmať body, ktorými sa má Coreper alebo Rada zaoberať. Neformálne stretnutie za okrúhlym stolom organizované predsedníctvom bude zároveň slúžiť aj ako fórum, kde sa budú vypracovávať, preskúmavať a prerokovávať všetky návrhy opatrení, ktoré sa majú predložiť Coreperu/Rade.

— **Koncepcia:**

— Horizontálna pracovná skupina Rady pre kybernetické otázky by mala pripraviť stretnutia PBV alebo Coreperu;

— **Krok 8 – Politická koordinácia a rozhodovanie na úrovni Coreperu/Rady**: Výsledky stretnutí Coreperu/Rady sa týkajú koordinácie činností v rámci reakcie na všetkých úrovniach, rozhodnutí o mimoriadnych opatreniach, politických vyhlásení atď. Tieto rozhodnutia predstavujú aj aktualizované politické/strategické usmernenie týkajúce sa ďalšieho vypracovávania správ o ISAA.

— **Koncepcia:**

— Politické rozhodnutia s cieľom koordinovať reakciu na kybernetickú krízu sa vykonávajú prostredníctvom činností (uskutočňovaných príslušnými aktérmi) opísaných v oddiele 1 „Spolupráca na strategickej/politickej, operačnej a technickej úrovni“, pokiaľ ide o **reakciu** a **verejnú komunikáciu**.

— Pri vypracovávaní správ o ISAA sa bude naďalej vychádzať zo spolupráce na technickej, operačnej a politickej/strategickej úrovni, pokiaľ ide o **situačné povedomie** opísané aj v oddiele 1.

([1]) štandardné operačné postupy ISAA.

— **Krok 9 – Monitorovanie vplyvu**: vedúci útvar ISAA bude s podporou prispievateľov k ISAA poskytovať informácie o vývoji krízy a vplyve prijatých politických rozhodnutí. Táto spätná väzba bude prispievať k vyvíjajúcemu sa procesu a podporí rozhodnutie predsedníctva pokračovať v účasti politickej úrovne EÚ alebo postupne obmedzovať IPCR;

— **Krok 10 – Postupná** deaktivácia: podľa toho istého postupu ako v prípade aktivácie môže predsedníctvo zvolať neformálne stretnutie za okrúhlym stolom s cieľom posúdiť, či udržiavať aktivitu IPCR alebo nie. Predsedníctvo môže rozhodnúť o deaktivácii alebo utlmení aktivácie.

— **Koncepcia:**

— Agentúra ENISA môžu byť vyzvaná, aby vykonala ex-post technické vyšetrovanie incidentu v súlade s ustanoveniami v jej mandáte, alebo k nemu prispela.

DODATOK

1. KRÍZOVÉ RIADENIE, MECHANIZMY SPOLUPRÁCE A AKTÉRI NA ÚROVNI EÚ

Mechanizmy krízového riadenia

Integrované dojednania o politickej reakcii na krízu (IPCR): integrované dojednania o politickej reakcii na krízu (IPCR), ktoré Rada schválila 25. júna 2013 ([1]), sú navrhnuté tak, aby v prípade veľkej krízy uľahčili včasnú koordináciu a reakciu na politickej úrovni EÚ. IPCR tiež podporujú koordináciu na politickej úrovni pri reakcii na využitie doložky o solidarite (článok 222 ZFEÚ) v zmysle rozhodnutia Rady 2014/415/EÚ o vykonávaní doložky o solidarite zo strany Únie prijatého 24. júna 2014. V štandardných operačných postupoch ([2]) sa stanovuje proces aktivácie a následné opatrenia, ktoré sa majú prijať.

ARGUS: Krízový koordinačný systém zriadený Európskou komisiou v roku 2005 s cieľom zabezpečiť osobitný koordinačný proces v prípade vážnej krízy zasahujúcej viacero odvetví. Opiera sa o rovnomenný spoločný systém rýchleho varovania (IT nástroj). ARGUS predpokladá dve fázy, pričom vo fáze II (v prípade veľkej krízy zasahujúcej viacero odvetví) sa zvolávajú stretnutia krízového koordinačného výboru (CCC) pod vedením predsedu Komisie alebo člena Komisie, ktorému bola pridelená zodpovednosť. CCC združuje zástupcov príslušných generálnych riaditeľstiev Komisie, kabinetov a ďalších útvarov EÚ s cieľom viesť a koordinovať reakciu Komisie na krízu. CCC, ktorému predsedá zástupca generálneho tajomníka, posudzuje situáciu, zvažuje možnosti a prijíma užitočné rozhodnutia, pokiaľ ide o nástroje a prostriedky EÚ patriace do zodpovednosti Komisie, a zabezpečuje vykonávanie týchto rozhodnutí ([3]) ([4]).

Krízový reakčný mechanizmus ESVČ: Krízový reakčný mechanizmus ESVČ je štruktúrovaný systém, ktorým ESVČ reaguje na krízu a núdzové situácie, ktoré majú vonkajšiu povahu alebo významný vonkajší rozmer (vrátane hybridných hrozieb) a ktoré môžu ovplyvňovať alebo skutočne ovplyvňujú záujmy EÚ alebo niektorého z členských štátov. Zabezpečením účasti príslušných úradníkov Komisie, ako aj úradníkov sekretariátu Rady na svojich stretnutiach uľahčuje krízový reakčný mechanizmus synergiu medzi diplomatickými, bezpečnostnými a obrannými zložkami s finančnými, obchodnými a kooperačnými nástrojmi riadenými Komisiou. Krízová jednotka môže byť aktivovaná na obdobie trvania krízy.

Mechanizmy spolupráce

Sieť jednotiek CSIRT: Sieť jednotiek pre riešenie počítačových bezpečnostných incidentov združuje všetky vnútroštátne a vládne jednotky CSIRT a CERT-EU. Cieľom siete je umožniť a zlepšiť výmenu informácií medzi jednotkami CSIRT o hrozbách a kybernetických incidentoch, ako aj spolupracovať pri reagovaní na kybernetické incidenty a krízy.

Horizontálna pracovná skupina Rady pre kybernetické otázky: táto pracovná skupina bola zriadená s cieľom zabezpečovať strategickú a horizontálnu koordináciu kybernetických politických otázok v Rade a možno ju zapojiť aj do legislatívnych či nelegislatívnych činností.

Aktéri

Agentúra ENISA: Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť bola zriadená v roku 2004. Agentúra úzko spolupracuje s členskými štátmi a súkromným sektorom na poskytovaní odporúčaní a riešení v oblastiach, ako sú napríklad celoeurópske cvičné simulácie v oblasti kybernetickej bezpečnosti, príprava národných stratégií kybernetickej bezpečnosti, spolupráca jednotiek CSIRT a budovanie kapacít. Agentúra ENISA spolupracuje priamo s jednotkami CSIRT v celej EÚ a pôsobí ako sekretariát siete jednotiek CSIRT.

ERCC: Koordinačné centrum pre reakcie na núdzové situácie v Komisii (v rámci generálneho riaditeľstva pre civilnú ochranu a operácie humanitárnej pomoci EÚ – GR ECHO) nepretržite podporuje a koordinuje celý rad činností v oblasti prevencie, pripravenosti a reakcie. Začalo svoju činnosť v roku 2013 a funguje ako centrála Komisie pre reakcie na krízu (spolupracuje s ostatnými krízovými štábmi EÚ), ako aj ústredné kontaktné miesto pre IPCR s nepretržitou prevádzkou.

([1]) 10708/13 – „Ukončenie procesu preskúmania dojednaní o núdzovej a krízovej koordinácii: dojednania o integrovanej politickej krízovej reakcii EÚ“, ktoré Rada schválila 24. júna 2013.
([2]) 12607/15 „Štandardné operačné postupy IPCR“, ktoré schválila skupina priateľov predsedníctva a ktoré vzal Coreper na vedomie v októbri 2015.
([3]) Ustanovenia Komisie o spoločnom systéme rýchleho varovania „ARGUS“, KOM(2005) 662 v konečnom znení, 23. decembra 2005.
([4]) Rozhodnutie Komisie 2006/25/ES, Euratom z 23. decembra 2005, ktorým sa mení a dopĺňa rokovací poriadok Komisie (Ú. v. EÚ L 19, 24.1.2006, s. 20), o vytvorení systému rýchleho varovania ARGUS.

Europol/EC3: Európske centrum boja proti počítačovej kriminalite (EC3), ktoré bolo zriadené v roku 2013 v rámci Europolu, podporuje reakciu orgánov presadzovania práva na počítačovú kriminalitu v EÚ. EC3 poskytuje operačnú a analytickú podporu pri vyšetrovacích činnostiach v členských štátoch a slúži ako ústredie pre kriminalistické a spravodajské informácie, pričom podporuje operácie a vyšetrovania v členských štátov poskytovaním operačnej analýzy, koordinácie a odborných znalostí, ako aj vysoko špecializovaných technických a digitálnych forenzných podporných kapacít.

CERT-EU: tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach má za úlohu zlepšiť ochranu inštitúcií, orgánov a agentúr EÚ pred kybernetickými hrozbami. Je členom siete jednotiek CSIRT. CERT-EU uzavrel technické dohody o zdieľaní informácií o kybernetických hrozbách s útvarom NATO pre počítačové incidenty (CIRC), niektorými tretími krajinami a hlavnými obchodnými aktérmi v oblasti kybernetickej bezpečnosti.

Spravodajská komunita EÚ pozostáva z Centra EÚ pre analýzu spravodajských informácií (INTCEN) a Spravodajského útvaru (EUMS INT) Vojenského štábu EÚ (**EUMS**) v rámci SIAC – **jednotnej kapacity na analýzu spravodajských informácií**. Poslaním SIAC je poskytovať spravodajské analýzy, včasné varovanie a informácie o situácii vysokému predstaviteľovi Európskej únie pre zahraničné veci a bezpečnostnú politiku a Európskej službe pre vonkajšiu činnosť (ESVČ). SIAC ponúka svoje služby v oblasti spoločnej zahraničnej a bezpečnostnej politiky (SZBP), spoločnej bezpečnostnej a obrannej politiky (SBOP) a boja proti terorizmu rôznym rozhodovacím orgánom EÚ, ako aj členským štátom. EU INTCEN a EUMS INT nie sú operačné agentúry a nie sú vybavené na zber informácií. Za operačnú úroveň spravodajských informácií sú zodpovedné členské štáty. SIAC sa zaoberá len strategickou analýzou.

Stredisko EÚ pre hybridné hrozby: V spoločnom oznámení o boji proti hybridným hrozbám z apríla 2016 sa za kontaktné miesto pre všetky zdrojové analýzy o hybridných hrozbách v EÚ určilo stredisko EÚ pre hybridné hrozby: jeho mandát bol v decembri 2016 schválený Komisiou prostredníctvom konzultácií medzi jednotlivými útvarmi. Stredisko EÚ pre hybridné hrozby má sídlo v INTCEN a je súčasťou SIAC, a teda spolupracuje s EUMS INT a má nastálo prideleného člena armády. Hybridné znamená cielené využívanie kombinácie viacerých skrytých/otvorených, vojenských a civilných nástrojov a stimulov, ako sú napríklad kybernetické útoky, dezinformačné kampane, špionáž, hospodársky tlak, využívanie spojeneckých síl alebo iných podvratných činností zo strany štátnych alebo neštátnych subjektov. Stredisko EÚ pre hybridné hrozby spolupracuje s rozsiahlou sieťou kontaktných miest v rámci Komisie, ako aj členských štátov, s cieľom poskytnúť integrovanú reakciu/celovládny prístup, ktoré sú v boji proti rôznym výzvam potrebné.

SITROOM EÚ: Situačné stredisko EÚ je súčasťou Centra EÚ pre analýzu spravodajských informácií (EU INTCEN) a poskytuje ESVČ operačné kapacity s cieľom zabezpečiť okamžitú a účinnú reakciu na krízy. Je stálym civilno-vojenským pohotovostným orgánom a zabezpečuje celosvetové monitorovanie a situačné povedomie v nepretržitej prevádzke.

Relevantné nástroje

Rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti: Rámec schválený v júni 2017 je súčasťou prístupu EÚ ku kybernetickej diplomacii, ktorá prispieva k predchádzaniu konfliktom, k zmierňovaniu hrozieb v oblasti kybernetickej bezpečnosti a väčšej stabilite v medzinárodných vzťahoch. Rámec v plnej miere využíva opatrenia v rámci spoločnej zahraničnej a bezpečnostnej politiky, v prípade potreby aj reštriktívne opatrenia. Využívanie opatrení v uvedenom rámci by malo podporovať spoluprácu, uľahčovať zmierňovanie okamžitých a dlhodobých hrozieb a ovplyvňovať správanie príslušných páchateľov a potenciálnych agresorov v dlhodobom horizonte.

2. KOORDINÁCIA V PRÍPADE KYBERNETICKEJ KRÍZY V RÁMCI DOJEDNANÍ IPCR – ÚROVEŇ HORIZONTÁLNEJ KOORDINÁCIE A POLITICKÁ ESKALÁCIA

Dojednania o IPCR sa môžu použiť (a boli použité) na riešenie technických a operačných otázok, ale vždy z politického alebo strategického hľadiska.

Pokiaľ ide o eskaláciu, IPCR sa môže použiť podľa úrovne krízy, a to prechodom z „režimu monitorovania“ do „režimu výmeny informácií“, ktorý predstavuje prvú úroveň aktivácie IPCR, či do „úplnej aktivácie IPCR“.

Úplná aktivácia je rozhodnutie, ktoré prináleží rotujúcemu predsedníctvu Rady EÚ. Komisia, ESVČ a GSR môžu aktivovať IPCR v režime výmeny informácií. Monitorovanie a výmena informácií aktivujú rôzne úrovne výmeny

informácií, pričom výmena informácií aktivuje dopyt po vypracovaní správ o ISAA. Pri úplnej aktivácii pribudnú k danému súboru nástrojov stretnutia IPCR pri okrúhlom stole, čím sa zabezpečí účasť predsedníctva pri okrúhlom stole (zvyčajne v osobe predsedu Coreperu II alebo odborníka z danej oblasti na úrovni radcu stáleho zastúpenia, ale vo výnimočných prípadoch sa stretnutia za okrúhlym stolom konali na ministerskej úrovni).

Aktéri

Vedúce postavenie má rotujúce predsedníctvo (obyčajne predseda Coreperu)

Európska rada je zastúpená kabinetom predsedu

Európska komisia je zastúpená na úrovni zástupcu generálneho tajomníka Rady alebo generálnych riaditeľstiev a/alebo odborníkov z danej oblasti,

ESVČ je zastúpená na úrovni zástupcu generálneho tajomníka Rady/výkonného riaditeľa a/alebo odborníkov z danej oblasti,

GSR je zastúpený kanceláriou generálneho tajomníka, tímom IPCR a zodpovednými GR

Rozsah činností: Vytvorenie spoločného integrovaného pohľadu na situáciu a zvyšovanie povedomia o problémoch alebo nedostatkoch na každej z troch úrovní s cieľom riešiť ich na politickej úrovni, prijímanie rozhodnutí v rámci stretnutí za okrúhlym stolom, pokiaľ spadajú do kompetencie účastníkov, alebo predkladanie návrhov opatrení, ktorými sa bude zaoberať Coreper II a Rada.

Spoločné situačné povedomie:

(neaktívne): Možno vytvoriť monitorovacie stránky IPCR s cieľom sledovať vývoj situácií, ktoré by mohli prerásť do krízy s dôsledkami pre EÚ

(výmena informácií IPCR): správy o ISAA vypracuje vedúci útvar ISAA na základe vstupov od útvarov Komisie, ESVČ a členských štátov (získaných prostredníctvom dotazníkov IPCR),

(úplná aktivácia IPCR): okrem správ o ISAA, neformálne stretnutia IPCR za okrúhlym stolom spájajú rôznych dotknutých aktérov v členských štátoch, Komisii, ESVČ, príslušných agentúrach atď., aby diskutovali o nedostatkoch a problémoch

Spolupráca a reakcia:

aktivácia/synchronizácia ďalších mechanizmov/nástrojov krízového riadenia v závislosti od povahy a dosahu incidentu. Môžu medzi ne patriť napríklad mechanizmus v oblasti civilnej ochrany, rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti alebo „spoločný rámec pre boj proti hybridným hrozbám".

Krízová komunikácia:

Sieť krízového komunikátora IPCR môže aktivovať predsedníctvo po porade s príslušnými útvarmi Komisie, GSR a ESVČ s cieľom podporiť vypracovávanie spoločných správ alebo rozvíjať najúčinnejšie komunikačné nástroje.

3. RIADENIE KYBERNETICKÝCH KRÍZ V SYSTÉME ARGUS – VÝMENA INFORMÁCIÍ V RÁMCI EURÓPSKEJ KOMISIE

Z dôvodu neočakávaných kríz, ako napr. teroristických útokov v Madride (marec 2004), cunami v juhovýchodnej Ázii (december 2004) či teroristických útokov v Londýne (júl 2005), ktoré si vyžadovali opatrenia na európskej úrovni, Komisia v roku 2005 vytvorila koordinačný systém ARGUS, podporovaný rovnomenným spoločným systémom rýchleho varovania ([1]) ([2]). Jeho cieľom je v prípade vážnej krízy zasahujúcej viacero odvetví poskytnúť špecifický **krízový koordinačný postup**, a tak umožniť výmenu informácií súvisiacich s krízou v reálnom čase a zabezpečiť rýchle prijímanie rozhodnutí.

ARGUS definuje dve fázy, a to v závislosti od závažnosti udalosti:

Fáza I: používa sa na „výmenu informácií" o kríze obmedzeného rozsahu.

([1]) Komisia Európskych spoločenstiev, 23. decembra 2005, Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Ustanovenia Komisie o spoločnom systéme rýchleho varovania „ARGUS", KOM(2005) 662 v konečnom znení.

([2]) Rozhodnutie 2006/25/ES, Euratom.

Medzi príklady nedávno nahlásených udalostí vo fáze I patria lesné požiare v Portugalsku a Izraeli, útok v Berlíne v roku 2016, záplavy v Albánsku, hurikán Matthew na Haiti a sucho v Bolívii. Každé GR môže otvoriť udalosť vo fáze I, keď usúdi, že situácia v jeho oblasti pôsobnosti je dostatočne závažná na to, že oprávňuje na výmenu informácií alebo z nej môže profitovať. Napríklad GR CNECT alebo GR HOME môže otvoriť udalosť vo fáze I, keď usúdia, že situácia z kybernetického hľadiska v ich príslušnej oblasti pôsobnosti je dostatočne závažná na to, že oprávňuje na výmenu informácií alebo z nej môže profitovať.

Fáza II: spúšťa sa v prípade závažnej krízy zasahujúcej viacero odvetví alebo predpokladanej alebo bezprostrednej hrozby pre Úniu.

Vo fáze II sa spustí osobitný koordinačný proces, ktorý Komisii umožní prijať rozhodnutia a riadiť rýchlu, koordinovanú a koherentnú reakciu na najvyššej úrovni v oblasti jej právomoci a v spolupráci s inými inštitúciami. Fáza II sa vzťahuje na vážnu krízu zasahujúcu viacero odvetví alebo predpokladanú či bezprostrednú hrozbu jej vzniku. Medzi príklady udalostí vo fáze II patrí migračná/utečenecká kríza (ktorá sa začala v roku 2015 a trvá dodnes), trojnásobná katastrofa vo Fukušime (2011) a výbuch sopky *Eyjafjallajökull* na Islande (2010).

Fázu II aktivuje predseda z vlastnej iniciatívy alebo na žiadosť člena Komisie. Predseda sa môže rozhodnúť, že politickú zodpovednosť za reakciu Komisie bude niesť komisár zodpovedný za útvar, ktorého sa daná kríza najviac dotýka, alebo on sám.

Počíta sa pri nej s mimoriadnymi zasadnutiami krízového koordinačného výboru (CCC), ktoré sa zvolávajú pod vedením predsedu alebo komisára, ktorému bola pridelená príslušná zodpovednosť, a zvoláva ich SG prostredníctvom IT nástroja ARGUS. Krízový koordinačný výbor je osobitný útvar operačného krízového riadenia, zriadený s cieľom viesť a koordinovať reakciu Komisie na krízu, ktorý združuje zástupcov príslušných generálnych riaditeľstiev Komisie, kabinetov a iných útvarov Komisie. **Tento výbor**, ktorému predsedá zástupca generálneho tajomníka, **posudzuje situáciu, zvažuje možnosti a prijíma rozhodnutia, ako aj zabezpečuje, aby sa rozhodnutia a opatrenia vykonávali**, a zároveň zabezpečuje, aby reakcia bola ucelená a konzistentná. Výboru poskytuje podporu SG.

4. KRÍZOVÝ REAKČNÝ MECHANIZMUS ESVČ

Krízový reakčný mechanizmus ESVČ sa aktivuje pri výskyte závažnej situácie alebo stavu núdze, ktorý sa týka alebo akokoľvek zahŕňa vonkajší rozmer EÚ. Krízový reakčný mechanizmus aktivuje zástupca generálneho tajomníka zodpovedný za krízové riadenie, a to po konzultácii s VP/PK alebo generálnym tajomníkom. Zástupcu generálneho tajomníka zodpovedného za krízové riadenie môže o spustenie krízového reakčného mechanizmu požiadať aj VP/PK, generálny tajomník alebo iný zástupca generálneho tajomníka či výkonný riaditeľ.

Tento krízový reakčný mechanizmus prispieva k súdržnej reakcii EÚ na krízu v rámci bezpečnostnej stratégie. Uľahčuje najmä súčinnosť medzi diplomatickými, bezpečnostnými a obrannými zložkami s finančnými, obchodnými a kooperačnými nástrojmi riadenými Komisiou.

Je prepojený so spoločným systémom rýchleho varovania (ARGUS) a integrovanými dojednaniami EÚ o politickej reakcii na krízu (IPCR) s cieľom využiť súčinnosť v prípade simultánnej aktivácie. Situačné stredisko v rámci ESVČ funguje ako komunikačný uzol medzi ESVČ a systémami reakcie na núdzové situácie v Rade a Komisii.

Zvyčajne je prvým krokom súvisiacim s implementáciou tohto mechanizmu zvolanie **krízového stretnutia** členov vyššieho manažmentu ESVČ, Komisie a Rady, ktorých sa daná kríza priamo dotýka. Na krízovom stretnutí sa posudzujú krátkodobé účinky krízy a môže sa dospieť k dohode o prijatí okamžitých opatrení alebo o aktivácii krízovej jednotky či zvolaní krízovej platformy. Tieto opatrenia možno realizovať v akomkoľvek časovom poradí.

Krízová jednotka je malá operačná jednotka, kde sa zástupcovia útvarov ESVČ, Komisie a Rady, ktoré sú zapojené do reakcie na danú krízu, stretávajú, aby priebežne monitorovali situáciu s cieľom poskytnúť subjektom s rozhodovacou právomocou na ústredí ESVČ podporu. V prípade aktivácie zabezpečuje krízová jednotka nepretržitú prevádzku.

Krízová platforma združuje príslušné útvary ESVČ, Komisie a Rady s cieľom poskytnúť posúdenie strednodobých a dlhodobých dôsledkov krízy a dohodnúť sa na opatreniach, ktoré sa majú prijať. Predsedá jej VP/PK alebo generálny tajomník či zástupca generálneho tajomníka zodpovedný za krízové riadenie. V rámci krízovej platformy sa hodnotí účinnosť opatrení EÚ v krajine alebo regióne zasiahnutom krízou, rozhoduje sa o zmenách dodatočných opatrení a diskutuje sa o návrhoch opatrení Rady. Krízová platforma zasadá ad hoc; preto sa neaktivuje natrvalo.

Pracovná skupina je zložená zo zástupcov útvarov zapojených do reakcie a môže byť aktivovaná s cieľom sledovať a uľahčiť vykonávanie reakcie EÚ. Hodnotí aj vplyv opatrení EÚ, pripravuje politické dokumenty a dokumenty s alternatívami, prispieva k príprave politického rámca pre krízový prístup, prispieva ku komunikačnej stratégii, a prijíma akékoľvek iné dojednania, ktoré môžu uľahčiť vykonávanie reakcie EÚ.

5. REFERENČNÉ DOKUMENTY

Nižšie je uvedený zoznam referenčných dokumentov, ktoré sa pri príprave tejto koncepcie zohľadnili:

— Európsky rámec spolupráce v prípade kybernetickej krízy, verzia 1, 17. októbra 2012

— Správa o spolupráci a riadení v prípade kybernetickej krízy, ENISA, 2014,

— Užitočné informácie pre reakciu na bezpečnostné incidenty, ENISA, 2014,

— Spoločné postupy krízového riadenia na úrovni EÚ a ich uplatniteľnosť na kybernetické krízy, ENISA 2015,

— Stratégie reakcie na incidenty a spolupráca v prípade kybernetickej krízy, ENISA, 2016,

— Štandardné operačné postupy EÚ v oblasti kybernetiky, ENISA, 2016,

— Príručka osvedčených postupov taxonómie v oblasti prevencie a odhaľovania incidentov, ENISA, 2017,

— Oznámenie o posilnení odolnosti kybernetického systému a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe, COM(2016) 410 final, 5. júla 2016,

— Závery Rady o posilnení európskeho systému kybernetickej odolnosti a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe – závery Rady z 15. novembra 2016, 14540/16,

— Rozhodnutie Rady 2014/415/EÚ z 24. júna 2014 o podrobnostiach vykonávania doložky o solidarite Úniou (Ú. v. EÚ L 192, 1.7.2014, s. 53),

— Ukončenie procesu preskúmania dojednaní o núdzovej a krízovej koordinácii: dojednania o integrovanej politickej reakcii na krízu EÚ, 10708/13, 7. júna 2013,

— Integrovaná situačná informovanosť a analýza – štandardné operačné postupy, DS 1570/15, 22. októbra 2015,

— Ustanovenia Komisie o spoločnom systéme rýchleho varovania „ARGUS“, KOM(2005) 662 v konečnom znení, 23. decembra 2005,

— Rozhodnutie Komisie 2006/25/ES z 23. decembra 2005, ktorým sa mení a dopĺňa rokovací poriadok Komisie (Ú. v. EÚ L 19, 24.1.2006, s. 20)

— Spôsob fungovania systému ARGUS, Európska komisia, 23. októbra 2013,

— Závery Rady o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“), dokument 9916/17,

— Operačný protokol EÚ na boj proti hybridným hrozbám „operačný protokol EÚ“, dokument SWD(2016) 227,

— Krízový reakčný mechanizmus ESVČ, 8. novembra 2016 [Ares(2017)880661] Spoločný pracovný dokument útvarov – Operačný protokol EÚ na boj proti hybridným hrozbám „operačný protokol EÚ“, SWD(2016) 227 final, 5. júla 2016.

— Spoločné oznámenie Európskemu parlamentu a Rade: Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie, JOIN (2016) 18 final, 6. apríla 2016,

— ESVČ(2016) 1674 – Pracovný dokument Európskej služby pre vonkajšiu činnosť – Stredisko EÚ pre hybridné hrozby – Mandát.

6. OSOBITNÉ PRVKY KYBERNETICKEJ BEZPEČNOSTI V PROCESE IPCR