EURÓPSKA
KOMISIA

V Bruseli 13. 9. 2017
C(2017) 6100 final

ODPORÚČANIE KOMISIE

z 13. 9. 2017

o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu

ODPORÚČANIE KOMISIE

z 13. 9. 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

[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.

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 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[4] 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)[5] a Komisia bude uplatňovať ARGUS[6] – 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[7] Európskej služby pre vonkajšiu činnosť (ESVČ).

---

2 COM(2016) 410 final z 5. júla 2016.

3 Smernica (EÚ) 2016/1148 o bezpečnosti sietí a informačných systémov („smernica NIS“) s cieľom dosiahnuť vysokú spoločnú úroveň bezpečnosti sietí a informačných systémov v Únii.

4 Dokument 14540/16, 15. november 2016.

5 Ďalšie informácie možno nájsť v oddiele 3.1 Dodatku o krízovom riadení, mechanizmoch spolupráce a aktéroch na úrovni EÚ.

6 Tamtiež.

7 Tamtiež.

(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 z 22. júla 2014 o aspektoch rozmiestňovania, prevádzky a používania Európskeho globálneho navigačného satelitného systému, ktoré majú vplyv na bezpečnosť Európskej únie, 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 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)[8] 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.

[8] V procese prípravy, prijatie sa očakáva do konca roka 2017.

(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[9].

(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[10] alebo operačného protokolu EÚ na boj proti hybridným hrozbám[11].

(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.

---

9 Tieto usmernenia majú byť dokončené do konca roka 2017.

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

11 Spoločný pracovný dokument útvarov Komisie Operačný protokol EÚ na boj proti hybridným hrozbám „operačný protokol EÚ“, SWD(2016) 227 final, 5.7.2016.

(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[12] 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

[12] Dokument ST 15283/16, 6. decembra 2016.

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.

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. 9. 2017

Za Komisiu
Mariya GABRIEL
členka Komisie

OVERENÁ KÓPIA ORIGINÁLU
Za generálneho tajomníka

Jordi AYET PUIGARNAU
Riaditeľ kancelárie
EURÓPSKA KOMISIA