# DOPORUČENÍ

## DOPORUČENÍ KOMISE (EU) 2017/1584

**ze dne 13. září 2017**

**o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize**

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 292 této smlouvy,

vzhledem k těmto důvodům:

(1) Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem ve všech odvětvích hospodářské činnosti, neboť naše společnosti a naši občané jsou vzájemně propojenější a závislejší než kdykoli předtím, a to napříč odvětvími i hranicemi. Kybernetický bezpečnostní incident, který zasáhne organizace ve více než jednom členském státě, nebo dokonce v celé Unii, s možnými vážnými narušeními vnitřního trhu a obecněji sítí a informačních systémů, na kterých stojí hospodářství, demokracie a společnost v Unii, je scénář, na nějž musí být členské státy a orgány EU dobře připraveny.

(2) Incident v oblasti kybernetické bezpečnosti lze považovat za krizi na úrovni Unie v případě, že je narušení způsobené daným incidentem příliš rozsáhlé na to, aby se s ním dotčený členský stát vypořádal sám, nebo pokud se dotýká dvou nebo více členských států a má tak rozsáhlý technicky nebo politicky významný dopad, že to vyžaduje rychlou koordinaci a reakci na politické úrovni EU.

(3) Kybernetické bezpečnostní incidenty mohou podnítit širší krize, které zasáhnou odvětví činnosti mimo rámec sítí a informačních systémů a komunikačních sítí; každá vhodná reakce musí být proto založena jak na kybernetických, tak na nekybernetických zmírňujících opatřeních.

(4) Kybernetické bezpečnostní incidenty jsou nepředvídatelné, vznikají a vyvíjejí se často ve velmi krátké době, a zasažené subjekty i osoby odpovědné za reakci na incidenty a zmírnění jejich účinků musí proto koordinovat svou reakci rychle. Kybernetické bezpečnostní incidenty navíc často nebývají omezeny jen na určitou zeměpisnou oblast a mohou se vyskytovat souběžně nebo se velmi rychle šířit do mnoha zemí.

(5) Účinná reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize na úrovni EU vyžaduje rychlou a účinnou spolupráci mezi všemi příslušnými zúčastněnými stranami a zakládá se na připravenosti a schopnosti jednotlivých členských států, jakož i na koordinovaném společném postupu podporovaném schopnostmi Unie. Včasná a účinná reakce na incidenty proto vychází z předem stanovených a co nejlépe nacvičených postupů a mechanismů spolupráce s jasně vymezenými úlohami a odpovědností hlavních aktérů na vnitrostátní úrovni i na úrovni Unie.

(6) Rada ve svých závěrech ([1]) o ochraně kritické informační infrastruktury ze dne 27. května 2011 vyzvala členské státy EU, aby „prohlubovaly spolupráci mezi členskými státy a na základě vnitrostátních zkušeností s řešením krizí a jejich výsledků a ve spolupráci s ENISA přispěly k vytvoření evropských mechanismů spolupráce při kybernetických incidentech, které budou vyzkoušeny v rámci příštího cvičení CyberEurope v roce 2012".

(7) Ve sdělení z roku 2016 „Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti" ([2]) byly členské státy vybídnuty, aby co nejvíce využívaly mechanismy spolupráce podle směrnice o bezpečnosti sítí a informací ([3]) a aby posílily přeshraniční spolupráci,

([1]) Závěry Rady o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti", dokument 10299/11, Brusel, 27. května 2011.
([2]) COM(2016) 410 final ze dne 5. července 2016.
([3]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

pokud jde o připravenost na rozsáhlý kybernetický bezpečnostní incident. Dále v něm bylo uvedeno, že koordinovaný přístup ke krizové spolupráci mezi jednotlivými prvky kybernetického ekosystému, který má být stanoven v plánu, by vedl ke zvýšení připravenosti a že takový plán by měl zároveň zajistit součinnost a soulad se stávajícími mechanismy řešení krizí.

(8) V závěrech Rady ([1]) ohledně výše uvedeného sdělení členské státy vyzvaly Komisi, aby předložila takový plán subjektům zřízeným podle směrnice o bezpečnosti sítí a informací a dalším příslušným zúčastněným stranám k projednání. Směrnice o bezpečnosti sítí a informací však nestanoví unijní rámec pro spolupráci v případě rozsáhlých kybernetických bezpečnostních incidentů a krizí.

(9) Komise konzultovala s členskými státy během dvou samostatných konzultačních seminářů, které se konaly dne 5. dubna a dne 4. července 2017 v Bruselu za účasti představitelů členských států z bezpečnostních týmů pro reakci na počítačové bezpečnostní incidenty (týmy typu CSIRT), skupiny pro spolupráci zřízené podle směrnice o bezpečnosti sítí a informací a Horizontální pracovní skupiny Rady pro otázky týkající se kybernetiky, jakož i zástupců Evropské služby pro vnější činnost (ESVČ), agentury ENISA, Europolu/EC3 a generálního sekretariátu Rady.

(10) Tento plán koordinované reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize na úrovni Unie, který je tvoří přílohu tohoto doporučení, je výsledkem výše uvedených konzultací a doplňuje sdělení „Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti“.

(11) Plán popisuje a stanoví cíle a způsoby spolupráce mezi členskými státy a orgány, institucemi, agenturami a jinými subjekty EU (dále jen „orgány EU“) v reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize a způsoby, jak mohou současné mechanismy řešení krizí v plné míře využít stávajících subjektů v oblasti kybernetické bezpečnosti na úrovni EU.

(12) V reakci na kybernetickou krizi ve smyslu 2. bodu odůvodnění bude Rada při koordinaci této reakce na politické úrovni Unie využívat integrovaná opatření pro politickou reakci na krize (IPCR) ([2]); Komise bude využívat proces meziodvětvové krizové koordinace na vysoké úrovni ARGUS ([3]). Pokud má krize významný externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), aktivuje se mechanismus Evropské služby pro vnější činnost (EVSČ) pro reakce na krize ([3]).

(13) V některých oblastech počítají odvětvové mechanismy řešení krizí na úrovni EU se spoluprací v případě kybernetických bezpečnostních incidentů nebo krizí. Například v rámci evropského globálního družicového navigačního systému (GNSS) již rozhodnutí Rady 2014/496/SZBP ([4]) vymezuje příslušné úlohy Rady, vysokého představitele, Komise, Agentury pro evropský GNSS a členských států v linii operačního vedení, která byla stanovena v reakci na hrozby pro Unii, členské státy nebo GNSS, včetně případů kybernetických útoků. Toto doporučení by se tudíž těchto mechanismů nemělo dotknout.

(14) V případě rozsáhlých kybernetických bezpečnostních incidentů nebo krizí majících dopad na členské státy jsou za reakci primárně odpovědné členské státy. Komise, vysoký představitel a další orgány a útvary EU však mohou hrát důležitou úlohu, jež pramení z práva Unie či ze skutečnosti, že kybernetické bezpečnostní incidenty a krize mohou mít dopad na všechny segmenty hospodářské činnosti na jednotném trhu, bezpečnostní a mezinárodní vztahy Unie i na orgány samotné.

(15) Na úrovni Unie patří mezi klíčové aktéry zapojené do reakce na kybernetické krize struktury a mechanismy nově zavedené směrnicí o bezpečnosti sítí a informací, a sice síť bezpečnostních týmů typu CSIRT, jakož i příslušné agentury a subjekty, zejména Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), Evropské centrum pro boj proti kyberkriminalitě při Europolu (Europol/EC3), Středisko EU pro analýzu zpravodajských informací (INTCEN), zpravodajské ředitelství Vojenského štábu EU (EUMS INT) a situační středisko (SITROOM), které spolupracují se SIAC (společnou zpravodajsko-analytickou složkou), střediskem EU pro hybridní hrozby (se sídlem v INTCEN), skupinou pro reakci na počítačové hrozby v evropských orgánech (CERT-EU) a střediskem pro koordinaci odezvy na mimořádné události v Evropské komisi.

(16) Spolupráci mezi členskými státy v reakci na kybernetické bezpečnostní incidenty na technické úrovni zajišťuje síť týmů typu CSIRT zřízená podle směrnice o bezpečnosti sítí a informací. Agentura ENISA zajišťuje sekretariát sítě

([1]) Dokument 14540/16, 15. listopadu 2016.
([2]) Další informace lze nalézt v oddíle 3.1 dodatku o řešení krizí, mechanismech spolupráce a aktérech na úrovni EU.
([3]) Tamtéž.
([4]) Rozhodnutí Rady 2014/496/SZBP ze dne 22. července 2014 o aspektech zavádění, provozu a využívání evropského globálního družicového navigačního systému majících dopad na bezpečnost Evropské unie a o zrušení společné akce 2004/552/SZBP (Úř. věst. L 219, 25.7.2014, s. 53).

a aktivně podporuje spolupráci mezi týmy typu CSIRT. Vnitrostátní týmy typu CSIRT a CERT-EU spolupracují a vyměňují si informace na dobrovolném základě, a pokud je to nezbytné, i v reakci na kybernetické bezpečnostní incidenty, které zasáhnou jeden nebo více členských států. Na žádost zástupce týmu typu CSIRT z některého členského státu mohou jednat o koordinované reakci na incident, který byl zjištěn v oblasti spadající do pravomoci tohoto členského státu, a pokud možno se na ní shodnout. Příslušné postupy budou stanoveny ve standardních operačních postupech sítě týmů typu CSIRT ([1]).

(17) Síť CSIRT má také za úkol projednávat, hledat a určovat další formy operativní spolupráce, a to i v souvislosti s kategoriemi rizik a incidentů, včasným varováním, vzájemnou pomocí a zásadami a způsoby spolupráce v případech, kdy členské státy reagují na přeshraniční rizika a incidenty.

(18) Skupina pro spolupráci zřízená podle článku 11 směrnice o bezpečnosti sítí a informací má za úkol poskytovat strategické vedení pro činnosti sítě týmů typu CSIRT a jednat o schopnostech a připravenosti členských států a na dobrovolném základě hodnotit národní strategie pro bezpečnost sítí a informačních systémů a účinnost týmů typu CSIRT a určovat osvědčené postupy.

(19) Zvláštní oblastí činnosti skupiny pro spolupráci je příprava pokynů pro hlášení incidentů podle čl. 14 odst. 7 směrnice o bezpečnosti sítí a informací, které se týkají okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty podle čl. 14 odst. 3, a formátu a postupů pro tato hlášení ([2]).

(20) Aby bylo možné přijímat informovaná rozhodnutí, je zcela zásadní využívat hlášení, hodnocení, výzkum, šetření a analýzy, tedy mít informace o aktuální situaci, akutních nebezpečích a hrozbách a rozumět jim. Tato „informovanost o situaci“ – u všech relevantních zúčastněných stran – je pro účinnou koordinovanou reakci nepostradatelná. Mezi informace o situaci patří i znalosti o příčinách, dopadu a původu incidentu. Má se za to, že to závisí na výměně a sdílení informací mezi příslušnými stranami ve vhodném formátu za použití společného názvosloví pro popis incidentu a s využitím náležitě zabezpečených způsobů.

(21) Reakce na kybernetický bezpečnostní incident může mít mnoho podob, od určení technických opatření, což může být to, že dva nebo více subjektů společně vyšetří technické příčiny incidentu (např. analýza malwaru), či určení způsobů, jak mohou organizace zjistit, zda byly zasaženy (např. indikátory narušení), až po operační rozhodnutí o použití těchto opatření a – na politické úrovni – rozhodnutí o využití dalších nástrojů v závislosti na typu incidentu, jako je rámec pro společnou reakci na nepřátelské činnosti v kyberprostoru ([3]) nebo operační protokol EU pro boj proti hybridním hrozbám ([4]).

(22) Důvěra evropských občanů a podniků v digitální služby má zásadní význam pro prosperující jednotný digitální trh. Proto krizová komunikace hraje zvláště významnou úlohu při zmírňování negativních dopadů kybernetických bezpečnostních incidentů a krizí. Komunikaci lze použít rovněž v kontextu rámce pro společnou diplomatickou reakci jako prostředek k ovlivnění chování (potenciálních) útočníků působících ze třetích zemí. Aby byla politická reakce účinná, je nutné, aby veřejná komunikace s cílem zmírnit negativní dopady kybernetických bezpečnostních incidentů a krizí byla sladěna s veřejnou komunikací s cílem ovlivnit útočníka.

(23) Účinným opatřením pro zmírnění dopadu rozsáhlého kybernetického bezpečnostního incidentu nebo krize by mohlo být informování občanů o tom, jak mohou na úrovni uživatelů a organizací omezit účinky incidentu (například instalací „záplaty“ nebo doplňujícími opatřeními na obranu proti hrozbě atd.).

(24) Komise prostřednictvím infrastruktury digitálních služeb v oblasti kybernetické bezpečnosti v rámci Nástroje pro propojení Evropy (CEF) vyvíjí mechanismus spolupráce platformy hlavních služeb, známý jako MeliCERTes, mezi zapojenými týmy typu CSIRT členských států, aby zvýšila úroveň jejich připravenosti, spolupráce a reakce na nové kybernetické hrozby či incidenty. Komise prostřednictvím konkurenčních výzev k předkládání návrhů pro udělování grantů v rámci Nástroje pro propojení Evropy spolufinancuje týmy typu CSIRT v členských státech za účelem zlepšení jejich provozní kapacity na vnitrostátní úrovni.

([1]) V přípravě; měly by být přijaty do konce roku 2017.
([2]) Pokyny mají být vypracovány do konce roku 2017.
([3]) Závěry Rady o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“), dokument 9916/17.
([4]) Společný pracovní dokument útvarů Komise „Operační protokol EU pro boj proti hybridním hrozbám (EU Playbook)“, SWD(2016) 227 final, 5. července 2016.

(25) Cvičení v oblasti kybernetické bezpečnosti na úrovni EU zásadním způsobem podněcují a zlepšují spolupráci mezi členskými státy a soukromým sektorem. Za tímto účelem agentura ENISA od roku 2010 organizuje pravidelná celoevropská cvičení zaměřená na kybernetické incidenty („Cyber Europe").

(26) Závěry Rady ([1]) o provádění společného prohlášení předsedy Evropské rady, předsedy Evropské komise a generálního tajemníka Severoatlantické aliance vyzývají k posílení spolupráce při kybernetických cvičeních prostřednictvím vzájemné účasti personálu na příslušných cvičeních, konkrétně i cvičení Cyber Coalition a Cyber Europe.

(27) Skutečnost, že oblast hrozeb se neustále vyvíjí, a nedávné kybernetické bezpečnostní incidenty jsou známkou rostoucího rizika, jemuž Unie čelí. Členské státy by měly jednat na základě tohoto doporučení bezodkladně a v každém případě do konce roku 2018,

PŘIJALA TOTO DOPORUČENÍ:

1) Členské státy a orgány EU by měly vytvořit rámec EU pro reakci na kybernetické bezpečnostní krize, který by zahrnoval cíle a způsoby spolupráce představené v plánu, jež se budou řídit hlavními zásadami, které jsou v plánu popsány.

2) Rámec EU pro reakci na kybernetické bezpečnostní krize by měl zejména určit zúčastněné subjekty, orgány EU a orgány členských států na všech potřebných úrovních – technické, provozní i strategické či politické – a v případě potřeby obsahovat standardní operační postupy, které vymezí způsob, jakým tyto zúčastněné subjekty spolupracují v rámci mechanismů EU pro řešení krizí. Důraz by měl být kladen na výměnu informací bez zbytečného odkladu a koordinování reakce během rozsáhlých kybernetických bezpečnostních incidentů a krizí.

3) Za tímto účelem by příslušné orgány členských států měly spolupracovat na dalším upřesnění protokolů pro sdílení informací a spolupráci. Skupina pro spolupráci by si měla vyměňovat zkušenosti v těchto otázkách s příslušnými orgány EU.

4) Členské státy by měly zajistit, aby jejich vnitrostátní mechanismy řešení krizí odpovídajícím způsobem řešily reakci na kybernetické bezpečnostní incidenty a zahrnovaly nezbytné postupy pro spolupráci na úrovni EU v souvislosti s rámcem EU.

5) Pokud jde o stávající mechanismy EU pro řešení krizí, v souladu s plánem by členské státy měly společně s útvary Komise a s ESVČ stanovit praktické prováděcí pokyny, pokud jde o integraci jejich vnitrostátních subjektů a postupů pro řešení krizí a kybernetické bezpečnosti do stávajících mechanismů EU pro řešení krizí, zejména opatření IPCR a mechanismu ESVČ pro reakce na krize. Zejména by členské státy měly zajistit zavedení vhodných struktur umožňujících efektivní tok informací mezi jejich vnitrostátními orgány pro řešení krizí a jejich zástupci na úrovni EU v souvislosti s mechanismy EU pro řešení krizí.

6) Členské státy by měly plně využívat příležitostí, které jim nabízí program pro infrastrukturu digitálních služeb v oblasti kybernetické bezpečnosti v rámci Nástroje pro propojení Evropy (CEF), a spolupracovat s Komisí s cílem zajistit, aby mechanismus spolupráce platformy hlavních služeb, který se v současné době vyvíjí, poskytoval nezbytné funkce a splňoval jejich požadavky na spolupráci i během kybernetických bezpečnostních krizí.

7) Členské státy by s pomocí agentury ENISA a v návaznosti na předchozí úsilí v této oblasti měly spolupracovat na vypracování a přijetí společného názvosloví a šablony pro situační zprávy, které popisují technické příčiny a dopady kybernetických bezpečnostních incidentů, s cílem dále zlepšit vzájemnou technickou a operativní spolupráci během krizí. V tomto ohledu by členské státy měly vzít v úvahu probíhající činnost skupiny pro spolupráci na vývoji pokynů pro hlášení incidentů, a zejména aspekty týkající se formátu národních hlášení.

8) Postupy stanovené v tomto rámci by měly být vyzkoušeny a v případě potřeby přezkoumány na základě poznatků získaných z účasti členského státu na cvičeních kybernetické bezpečnosti na vnitrostátní, regionální a unijní úrovni, jakož i na úrovni kybernetické diplomacie a NATO. Zejména by měly být vyzkoušeny v rámci cvičení CyberEurope organizovaných agenturou ENISA. Cvičení CyberEurope v roce 2018 je první takovou příležitostí.

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

9) Členské státy a orgány EU by měly pravidelně procvičovat svoji reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize na vnitrostátní a evropské úrovni, včetně svojí politické reakce, pokud bude potřeba, a s případným zapojením subjektů soukromého sektoru.

V Bruselu dne 13. září 2017.

*Za Komisi*
Mariya GABRIEL
*členka Komise*

*PŘÍLOHA*

**Plán koordinované reakce na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty a krize**

ÚVOD

Tento plán se týká kybernetických bezpečnostních incidentů, které způsobují narušení příliš rozsáhlé, aby je dotčený členský stát zvládnul sám, nebo které postihly více než jeden členský stát nebo orgán EU a jejichž dopad technického nebo politického významu je natolik rozsáhlý a významný, že vyžadují včasnou koordinaci politik a reakci na politické úrovni Unie.

Takové rozsáhlé kybernetické bezpečnostní incidenty se považují za kybernetickou bezpečnostní „krizi".

V případě krize s kybernetickými prvky napříč celou EU provádí koordinaci reakce na politické úrovni Unie Rada s využitím integrovaných opatření pro politickou reakci na krize (opatření IPCR).

V Komisi bude koordinace probíhat v souladu se systémem včasného varování ARGUS.

Pokud má krize významný externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), aktivuje se mechanismus ESVČ pro reakce na krize.

Tento plán popisuje, jak by tyto zavedené mechanismy řešení krizí měly naplno využívat stávajících subjektů v oblasti kybernetické bezpečnosti na úrovni EU i mechanismů spolupráce mezi členskými státy.

Plán přitom zohledňuje soubor hlavních zásad (proporcionalita, subsidiarita, komplementarita a důvěrnost informací) a představuje hlavní cíle spolupráce (účinná reakce, sdílení informací o situaci, komunikace s veřejností) na třech úrovních (strategická/politická, operační a technická), mechanismy a zapojené aktéry, jakož i kroky nutné ke splnění uvedených hlavních cílů.

Plán se nezaměřuje na celý životní cyklus řešení krize (prevence/zmírňování, připravenost, reakce, obnova), nýbrž jen na reakci. Některé činnosti, zvláště ty, které souvisí se sdílením informací o situaci, návrh nicméně řeší.

Důležité je zmínit i to, že kybernetické bezpečnostní incidenty mohou stát u zrodu nebo být součástí rozsáhlejší krize s dopadem na jiná odvětví. Vzhledem k tomu, že většina kybernetických bezpečnostních krizí má mít dopad na fyzický svět, musí se jakákoli vhodná reakce spoléhat jak na kybernetická, tak na nekybernetická zmírňující opatření. Činnosti v rámci reakce na kybernetické krize by měly být koordinovány s dalšími mechanismy řešení krizí na úrovni EU, vnitrostátní úrovni či sektorové úrovni.

A konečně je třeba uvést, že tento plán nenahrazuje a neměl by se dotýkat stávajících odvětvových nebo politických mechanismů, opatření nebo nástrojů, jako např. pro program globálního družicového navigačního systému ([1]).

**Hlavní zásady**

Při práci na dosažení cílů, určování nezbytných činností a přidělování rolí a odpovědností příslušným aktérům nebo mechanismům byly uplatněny následující hlavní zásady, které je také třeba dodržet při přípravě budoucích prováděcích pokynů.

*Proporcionalita*: Velká většina kybernetických bezpečnostních incidentů postihujících členské státy spadá výrazně pod úroveň toho, co lze považovat za vnitrostátní, natož evropskou „krizi". Základ pro spolupráci mezi členskými zeměmi při reakci na takové incidenty představuje síť bezpečnostních týmů pro reakci na počítačové bezpečnostní incidenty (tzv. týmy CSIRT) ustavená směrnicí o bezpečnosti sítí a informací ([2]). Národní týmy CSIRT spolupracují a dobrovolně si každý den vyměňují informace, mimo jiné, je-li to nutné, i v rámci reakce na kybernetické bezpečnostní incidenty, které postihly více než jeden členský stát, v souladu se standardními operačními postupy (SOP) sítě týmů CSIRT. Plán by měl proto tyto standardní operační postupy využít a měly by reflektovat jakékoli další konkrétní úkoly prováděné v souvislosti s kybernetickou bezpečnostní krizí.

([1]) Rozhodnutí 2014/496/SZBP.
([2]) Směrnice (EU) 2016/1148.

*Subsidiarita*: Zásada subsidiarity je klíčová. V případě rozsáhlých kybernetických bezpečnostních incidentů nebo krizí majících dopad na členské státy jsou za reakci primárně odpovědné členské státy. Důležitou úlohu však sehrávají také Komise, Evropská služba pro vnější činnost a další orgány, instituce a subjekty EU. Tato úloha je jasně stanovena v opatřeních IPCR, ale pramení rovněž z práva Unie či jen z toho, že kybernetické bezpečnostní incidenty a krize mohou mít dopad na všechny segmenty hospodářské činnosti na jednotném trhu, bezpečnostní a mezinárodní vztahy Unie i na orgány samotné.

*Komplementarita*: Plán plně zohledňuje stávající mechanismy řešení krizí na úrovni EU, a to integrovaná opatření EU pro politickou reakci na krize (IPCR EU), ARGUS a mechanismus ESVČ pro reakce na krize, začleňuje do nich nové struktury a mechanismy zřízené směrnicí o bezpečnosti sítí a informací, a to síť bezpečnostních týmů CSIRT, jakož i příslušné agentury a instituce, a to Evropskou agenturu pro bezpečnost sítí a informací (ENISA), Evropské centrum pro boj proti kyberkriminalitě při Europolu (Europol/EC3), Středisko EU pro analýzu zpravodajských informací (INTCEN), zpravodajské ředitelství Vojenského štábu EU (EUMS INT), situační středisko (SITROOM) při INTCEN, které pracují společně jako společná zpravodajsko-analytická složka (SIAC); a dále středisko EU pro hybridní hrozby (základnu má v INTCEN) a skupinu pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU). Tímto způsobem by měl plán rovněž maximalizovat komplementaritu a minimalizovat přesah jejich interakce a spolupráce.

*Důvěrnost informací*: Veškerá výměna informací v kontextu tohoto plánu se musí řídit příslušnými pravidly o bezpečnosti ([1]), o ochraně osobních údajů a tzv. „semaforovém protokolu" (Traffic Light Protocol, TLP) ([2]). Pro výměnu utajovaných informací musí být bez ohledu na klasifikační schéma použity dostupné akreditované nástroje ([3]). Při zpracování osobních údajů musí být dodrženy příslušné předpisy EU, a to zejména obecné nařízení o ochraně osobních údajů ([4]), směrnice o soukromí a elektronických komunikacích ([5]) a nařízení „o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Unie a o volném pohybu těchto údajů" ([6]).

**Hlavní cíle**

Spolupráce podle tohoto plánu sleduje výše uvedený tříúrovňový přístup – na rovině politické, operační a technické. Na každé z nich může spolupráce zahrnovat výměnu informací i společné kroky a jejím cílem je dosáhnout následujících hlavních cílů.

— Účinná reakce. Reakce může mít mnoho podob, od stanovení technických opatření, což může být to, že dva nebo více subjektů společně vyšetří technické příčiny incidentu (např. analýza malwaru), či určení způsobů, jak mohou organizace zjistit, zda byly zasaženy (např. indikátory narušení), až po operační rozhodnutí o použití těchto opatření a – na politické úrovni – rozhodnutí o spuštění dalších nástrojů v závislosti na typu incidentu, jako je diplomatická reakce EU na kybernetické činnosti se zlým úmyslem („soubor nástrojů pro kybernetickou diplomacii") nebo operační protokol EU pro boj proti hybridním hrozbám.

— Sdílení informací o situaci. Pro koordinovanou reakci je důležité, aby všichni zainteresovaní aktéři na všech třech úrovních (technické, operační a politické) dostatečně dobře rozuměli tomu, co se děje. K situačním informacím mohou patřit i technologické údaje o příčinách, dopadu a původu incidentu. Protože kybernetické bezpečnostní incidenty mohou mít dopad na mnoho odvětví (finančnictví, energetiku, dopravu, zdravotnictví atd.), je naprosto nezbytné, aby se příslušné informace ve vhodném formátu dostaly včas ke všem příslušným zainteresovaným stranám.

([1]) Rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi (Úř. věst. L 72, 17.3.2015, s. 41); rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 72, 17.3.2015, s. 53); rozhodnutí vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 19. dubna 2013 o bezpečnostních pravidlech pro Evropskou službu pro vnější činnost (Úř. věst. C 190, 29.6.2013, s. 1); rozhodnutí Rady 2013/488/EU ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 274, 15.10.2013, s. 1).

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

([3]) K červnu 2016 patřily k těmto přenosovým kanálům CIMS (Classified Information Management System), ACID (šifrovací algoritmus), RUE (zabezpečený systém pro vytváření, výměnu a ukládání dokumentů RESTREINT UE/EU RESTRICTED) a síť SOLAN. Mezi další způsoby např. přenášení utajovaných informací patří program PGP nebo standard S/MIME.

([4]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

([5]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

([6]) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1) – v současnosti předmětem přezkumu.

— Dohoda na hlavních sděleních v rámci komunikace s veřejností ([1]): Krizová komunikace hraje významnou úlohu při zmírňování negativních dopadů kybernetických bezpečnostních incidentů a krizí, lze ji však také využít k ovlivnění chování (případných) útočníků. Vhodné sdělení může tím, že podá jasný signál o pravděpodobných následcích diplomatické reakce, posloužit k ovlivnění chování agresorů. Aby politická reakce byla účinná, je nutné, aby veřejná komunikace s cílem zmírnit negativní dopady kybernetických bezpečnostních incidentů a krizí byla sladěná s veřejnou komunikací s cílem ovlivnit útočníka. Zvláště důležité pro kybernetickou bezpečnost je šíření přesných, vykonatelných informací o tom, jak může veřejnost zmírnit účinky incidentu (např. instalováním záplaty, provedením bezplatně nabídnutých úkonů pro obejití hrozby atd.)

SPOLUPRÁCE MEZI ČLENSKÝMI STÁTY A AKTÉRY ČLENSKÝCH STÁTŮ A EU NA TECHNICKÉ, OPERAČNÍ A STRATEGICKÉ/POLITICKÉ ÚROVNI

Účinná reakce na rozsáhlé kybernetické bezpečnostní incidenty nebo krize na úrovni EU závisí na účinné technické, operační a strategické/politické spolupráci.

Na každé z těchto úrovní by zúčastnění aktéři měli provádět konkrétní činnosti, pokud jde o dosažení tří hlavních cílů:

— koordinovaná reakce,

— sdílení informací o situaci,

— komunikace s veřejností.

V průběhu incidentu nebo krize nižší úrovně spolupráce varují, informují a podporují vyšší úrovně, které pak podle potřeby vydávají pokyny ([2]) a rozhodnutí nižším úrovním.

**Spolupráce na technické úrovni**

*Rozsah činností:*

— řešení incidentu ([3]) během kybernetické bezpečnostní krize

— monitoring a sledování incidentu včetně průběžné analýzy hrozeb a rizik

*Potenciální aktéři*

Na technické úrovni je ústředním mechanismem pro spolupráci podle tohoto plánu síť týmů CSIRT, které předsedá předsednictví a které sekretariát poskytuje agentura ENISA.

— Členské státy:

  — příslušné úřady a jednotná kontaktní místa zřízená podle směrnice o bezpečnosti sítí a informací

  — týmy CSIRT

— Orgány a instituce EU

  — ENISA

  — Europol/EC3

  — CERT-EU

([1]) Tady je třeba zmínit, že komunikace s veřejností může znamenat jak komunikování o incidentu s veřejností jako celkem, tak komunikaci více technických a operačních informací kritickým odvětvím a těm, kdo byli incidentem zasaženi. To může znamenat, že je nutné využít kanály pro šíření utajovaných informací a specifické technické nástroje/platformy. Komunikace s operátory/provozovateli a širší veřejností v rámci členského státu je však v obou případech výsadou a odpovědností každého členského státu. V souladu s výše uvedenou zásadou subsidiarity jsou to tedy členské státy a vnitrostátní týmy CSIRT, kdo má definitivní odpovědnost za informace šířené na jejich území a předávané jejich klientům.

([2]) „Povolení jednat“ – tváří v tvář kybernetické bezpečnostní krizi má zásadní důležitost krátká reakční doba nutná ke spuštění příslušných zmírňujících opatření. Aby mohla být reakční doba co nejkratší, může „povolení jednat“ vydávat jeden stát druhému a povolit mu jednat okamžitě, aniž by musel konzultovat s vyššími úrovněmi nebo orgány EU a použít za běžné situace povinné oficiální kanály, ledaže by to bylo v konkrétním případě vyžadováno (tj. např. tým CSIRT by nemusel konzultovat s vyššími úrovněmi, zda může týmu CSIRT v jiném členském státě poslat cenné informace).

([3]) „Řešením incidentu“ se rozumí veškeré postupy, které pomáhají incident odhalit, analyzovat, zamezit jeho šíření a reagovat na něj.

— Evropská komise

  — Středisko pro koordinaci odezvy na mimořádné události (ERCC) (služba s nepřetržitým provozem umístěná v GŘ ECHO) a jmenovaný vedoucí útvar (buď GŘ CNECT, nebo GŘ HOME podle konkrétní povahy incidentu), generální sekretariát (sekretariát ARGUS), GŘ HR (ředitelství pro bezpečnost), GŘ DIGIT (IT bezpečnostní operace)

  — U ostatních agentur EU ([1]) odpovídající mateřské generální ředitelství Komise, nebo ESVČ (první kontaktní místo)

— ESVČ

  — SIAC (společná zpravodajsko-analytická složka: EU INTCEN a EUMS INT)

  — Situační středisko EU a jmenovaná geografická nebo tematická služba

  — Středisko EU pro hybridní hrozby (součást EU INTCEN – kybernetická bezpečnost v hybridním kontextu)

*Sdílení informací o situaci:*

— Jako součást pravidelné spolupráce na technické úrovni na podporu informovanosti Unie o situaci by agentura ENISA měla pravidelně připravovat technickou zprávu EU o situaci v oblasti kybernetické bezpečnosti týkající se incidentů a hrozeb na základě veřejně dostupných informací, svých vlastních analýz a zpráv, které s ní (dobrovolně) sdílejí týmy CSIRT členských států nebo jednotná kontaktní místa podle směrnice o bezpečnosti sítí a informací, Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu, skupina CERT-EU a případně Evropské středisko pro analýzu zpravodajských informací (INTCEN) při Evropské službě pro vnější činnost (ESVČ). Zpráva by měla být k dispozici příslušným místům Rady, Komisi, vysoké představitelce/místopředsedkyni Komise a síti týmů CSIRT.

— V případě velkého incidentu připraví předseda sítě týmů CSIRT s pomocí agentury ENISA situační zprávu EU o kybernetickém bezpečnostním incidentu ([2]), jež se předloží předsednictví, Komisi a vysoké představitelce/místopředsedkyni Komise prostřednictvím týmu CSIRT rotujícího předsednictví.

— *Všechny ostatní agentury EU* podávají zprávy svému mateřskému generálnímu ředitelství, které dále podává zprávy vedoucímu útvaru Komise.

— *Skupina CERT-EU* podává technické zprávy síti týmů CSIRT, orgánům a agenturám EU (podle situace) a systému ARGUS (je-li aktivován).

— *Europol/EC3* ([3]) *a CERT-EU* poskytují odbornou forenzní analýzu technických artefaktů a další technické informace síti týmů CSIRT.

— SIAC ESVČ: Středisko EU pro hybridní hrozby jménem střediska INTCEN podává zprávy příslušným oddělením ESVČ.

*Reakce:*

— *Síť týmů CSIRT* si vyměňuje technické detaily a analýzu incidentu, např. IP adresy, indikátory narušení ([4]) atd. Tyto informace by měly být bez zbytečného prodlení, ale nejpozději do 24 hodin od detekování incidentu hlášeny agentuře ENISA.

— V souladu se standardními operačními postupy sítě týmů CSIRT spolupracují její členové na analýze existujících technických artefaktů a dalších technických informací týkajících se incidentu za účelem stanovení příčiny a možných technických zmírňujících opatření.

— Agentura ENISA pomáhá v souladu se svým mandátem ([5]) svými odbornými zkušenostmi týmům CSIRT v jejich technické činnosti.

---

([1]) Podle povahy a dopadu incidentu na různá odvětví činnosti (finančnictví, doprava, energetika, zdravotnictví atd.) budou zapojeny příslušné agentury nebo instituce EU.

([2]) Situační zpráva EU o kybernetickém bezpečnostním incidentu je souhrnem vnitrostátních zpráv poskytnutých vnitrostátními týmy CSIRT. Formát této zprávy by měl být popsán ve standardních operačních postupech sítě týmů CSIRT.

([3]) V souladu s podmínkami a postupy uvedenými v právním rámci centra EC3.

([4]) Indikátor narušení (indicator of compromise, IOC) – v počítačové forenzní analytice jde o artefakt na síti nebo v operačním systému, který s vysokou pravděpodobností ukazuje na narušení počítačového systému. K typickým IOC patří signatury a IP adresy virů, haše MD5 nebo malwarové soubory nebo internetové adresy nebo doménová jména řídících serverů botnetů.

([5]) Návrh nařízení o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost a o zrušení nařízení (EU) č. 526/2013 a o kybernetické bezpečnostní certifikaci informační a komunikační technologie (nařízení o kybernetické bezpečnosti), 13. září 2017.

— Týmy CSIRT členských států koordinují svoji činnost v oblasti technické reakce s pomocí agentury ENISA a Komise.

— SIAC ESVČ: Středisko EU pro hybridní hrozby jménem INTCEN spouští proces sběru prvotních důkazů.

*Komunikace s veřejností:*

— Týmy CSIRT v návaznosti na proces autorizace pro každý jednotlivý případ vypracovávají technická doporučení ([1]) a výstrahy o zranitelnostech ([2]) a šíří je mezi odbornou i laickou veřejností ve svých zemích.

— Agentura ENISA usnadňuje tvorbu a šíření společných komunikačních sdělení sítě týmů CSIRT.

— Agentura ENISA koordinuje svoji komunikaci s veřejností se sítí týmů CSIRT a útvarem mluvčího Komise.

— ENISA a EC3 koordinují svoji komunikaci s veřejností na základě sdílení informací o situaci dohodnutého mezi členskými státy. Oba subjekty koordinují svoji komunikaci s veřejností s útvarem mluvčího Komise.

— Pokud má krize externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), měla by být komunikace s veřejností koordinována s ESVČ a útvarem mluvčího vysoké představitelky/místopředsedkyně Komise.

**Spolupráce na operační úrovni**

*Rozsah činností:*

— Příprava rozhodování na politické úrovni

— Koordinace řízení kybernetické bezpečnostní krize (případně)

— Vyhodnocení následků a dopadu na úrovni EU a návrh možných zmírňujících opatření

*Potenciální aktéři*

— Členské státy:

  — příslušné úřady a jednotná kontaktní místa zřízená podle směrnice o bezpečnosti sítí a informací

  — týmy CSIRT, agentury pro kybernetickou bezpečnost

  — další vnitrostátní odvětvové orgány (v případě incidentu nebo krize zasahující více odvětví)

— Orgány a instituce EU

  — ENISA

  — Europol/EC3

  — CERT-EU

— Evropská komise

  — generální tajemník Generálního sekretariátu (příp. jeho zástupce) (proces ARGUS)

  — GŘ CNECT/HOME

  — bezpečnostní orgán Komise

  — další generální ředitelství (v případě incidentu nebo krize zasahující více odvětví)

([1]) Doporučení technické povahy o příčinách a možných zmírňujících krocích.
([2]) Informace o technické zranitelnosti, kterou někdo zneužívá, aby negativně ovlivnil systém IT.

— ESVČ

  — generální tajemník pro reakci na krizi (příp. jeho zástupce) a SIAC (EU INTCEN a EUMS INT)

  — středisko EU pro hybridní hrozby

— Rada

  — předsednictví (předseda Horizontální pracovní skupiny pro otázky týkající se kybernetiky nebo COREPER ([1])) s podporou Generálního sekretariátu Rady nebo Politického a bezpečnostního výboru (PSC) ([2]) a – jsou-li aktivována – s podporou opatření IPCR

*Informovanost o situaci:*

— Podpora přípravy politicko-strategických situačních zpráv (např. zprávy ISAA v případě aktivace opatření IPCR)

— *Horizontální pracovní skupina Rady pro otázky týkající se kybernetiky* připravuje zasedání COREPER nebo PSC

— V případě aktivace opatření IPCR:

  — Předsednictví může svolat schůze u kulatého stolu za účelem přípravy zasedání COREPER nebo PSC, na které pozve relevantní aktéry v členských státech, orgány, agentury a třetí strany jako země mimo EU a mezinárodní organizace. Jsou to krizové schůze, na kterých se identifikují slabá místa a vypracovávají návrhy pro průřezové otázky.

  — *Vedoucí útvar Komise nebo ESVČ* jako vedoucí ISAA připravuje zprávu ISAA, do které dále přispívají ENISA, síť týmů CSIRT, Europol/EC3, EUMS INT, INTCEN a všichni ostatní relevantní aktéři. Zpráva ISAA je celounijní posouzení založené na korelaci technického posouzení incidentů a krizí (analýza hrozeb, posouzení rizik, netechnické následky a účinky, nekybernetické aspekty incidentu nebo krize atd.), které je připraveno na míru potřebám operační a politické úrovně.

— V případě aktivace ARGUS:

  — CERT-EU a EC3 ([3]) přispívají přímo do výměny informací v rámci Komise.

— V případě aktivace mechanismu ESVČ pro reakce na krize:

  — SIAC zintenzivní sběr informací a sloučí informace ze všech zdrojů a připraví analýzu a posouzení incidentu.

*Reakce (na žádost politické úrovně):*

— Přeshraniční spolupráce s jednotným kontaktním místem a příslušnými vnitrostátními orgány (směrnice o bezpečnosti sítí a informací) na zmírňování následků a dopadů.

— Aktivace všech technických zmírňujících opatření a koordinace technických opatření nutných k zastavení nebo omezení dopadu útoků na zacílené informační systémy.

— Spolupráce a – pokud o tom bude rozhodnuto – koordinace technických kapacit za účelem společné nebo kolaborativní reakce v souladu se ***standardními operačními postupy sítě týmů CSIRT***.

— Vyhodnocení nutnosti spolupracovat s příslušnými třetími stranami.

— Rozhodování v rámci procesu ARGUS (bude-li aktivován).

— Příprava rozhodnutí a koordinace v rámci opatření IPCR (budou-li aktivována).

— Podpora rozhodování ESVČ prostřednictvím mechanismu ESVČ pro reakce na krize (bude-li aktivován), a to i pokud jde o kontakty se třetími zeměmi a mezinárodními organizacemi a veškerá opatření, jejichž cílem je ochrana misí a operací SBOP a delegací EU.

---

([1]) Výbor stálých zástupců neboli COREPER (článek 240 Smlouvy o fungování Evropské unie) zodpovídá za přípravu prací Rady Evropské unie.

([2]) Politický a bezpečnostní výbor (PSC) je výbor Rady Evropské unie zabývající se společnou zahraniční a bezpečnostní politikou (SZBP), jak je uvedeno v článku 38 Smlouvy o Evropské unii.

([3]) V souladu s podmínkami a postupy uvedenými v právním rámci centra EC3.

*Komunikace s veřejností:*

— Dohoda na sděleních pro veřejnost o incidentu.

— Pokud má krize externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), měla by být komunikace s veřejností koordinována s ESVČ a útvarem mluvčího vysoké představitelky/místopředsedkyně Komise.

**Spolupráce na strategické/politické úrovni**

*Potenciální aktéři*

— Pokud jde o členské státy, ministři příslušní pro kybernetickou bezpečnost.

— Pokud jde o Evropskou radu, předseda.

— Pokud jde o Radu, rotující předsednictví Rady.

— Při opatřeních v rámci „sady nástrojů kybernetické diplomacie", PSC a horizontální pracovní skupina.

— Pokud jde o Evropskou komisi, předseda nebo pověřený místopředseda/člen Komise.

— Vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku/místopředseda Komise.

*Rozsah činností*: strategické a politické řízení jak kybernetických, tak nekybernetických aspektů krize, včetně opatření na základě rámce pro společnou diplomatickou reakci EU na kybernetické činnosti se zlým úmyslem.

*Sdílená informovanost o situaci:*

— Určit dopady narušení způsobených krizí na fungování Unie.

*Reakce:*

— Aktivovat další mechanismy/nástroje řešení krizí v závislosti na povaze a dopadu incidentu. Ty mohou zahrnovat například mechanismus civilní ochrany.

— Přijmout opatření na základě rámce pro společnou diplomatickou reakci EU na kybernetické činnosti se zlým úmyslem.

— Zpřístupnit podporu při mimořádných událostech postiženým členským státům, například aktivací Fondu pro reakci při mimořádných událostech v oblasti kybernetické bezpečnosti ([1]), jakmile bude použitelný.

— Případná spolupráce a koordinace s mezinárodními organizacemi, jako jsou Organizace spojených národů (OSN), Organizace pro bezpečnost a spolupráci v Evropě (OBSE), a zejména NATO.

— Posoudit důsledky pro národní bezpečnost a obranu.

*Komunikace s veřejností:*

Rozhodnout o společné komunikační strategii vůči veřejnosti.

REAKCE KOORDINOVANÁ S ČLENSKÝMI STÁTY NA ÚROVNI EU V RÁMCI OPATŘENÍ IPCR

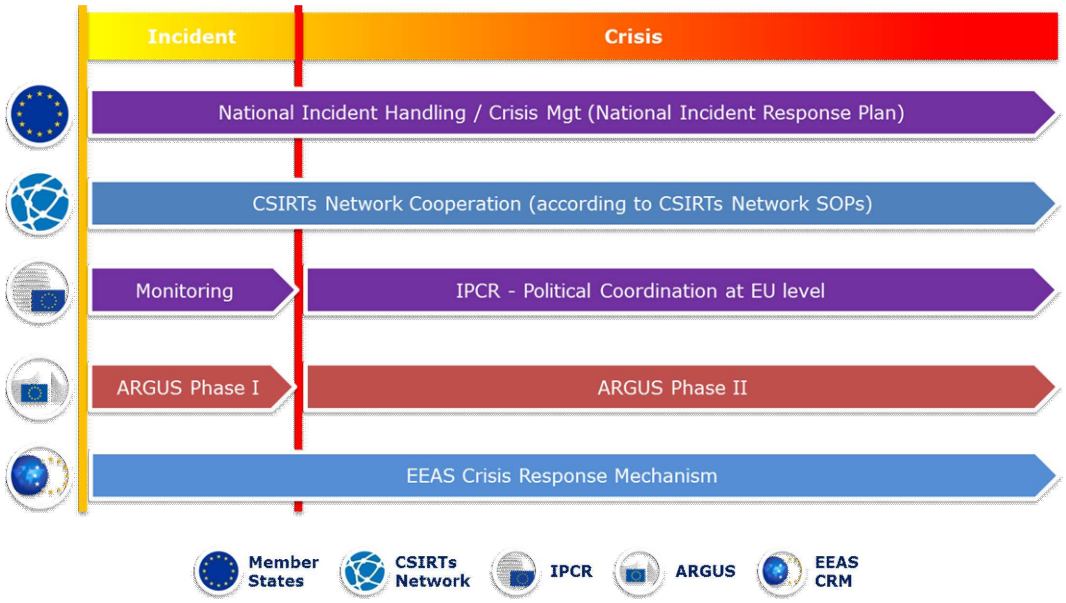
V souladu se zásadou komplementarity na úrovni EU vymezuje tento oddíl zejména hlavní cíle a povinnosti i činnosti orgánů členských států, sítě CSIRT, agentury ENISA, skupiny CERT-EU, Europolu/centra EC3, střediska INTCEN, střediska EU pro hybridní hrozby a Horizontální pracovní skupiny Rady pro otázky týkající se kybernetiky v rámci postupu IPCR a zaměřuje se na ně. Předpokládá se, že aktéři jednají v souladu se zavedenými postupy na úrovni EU nebo na vnitrostátní úrovni.

Je nezbytné upozornit, že, jak dokládá obrázek 1, bez ohledu na aktivaci mechanismů EU pro řešení krizí probíhají činnosti na vnitrostátní úrovni, jakož i spolupráce v rámci sítě týmů CSIRT (v případě potřeby) po dobu jakéhokoli incidentu/krize podle zásady subsidiarity a proporcionality.

([1]) Fond pro mimořádné události v oblasti kybernetické bezpečnosti je opatření navržené ve společném sdělení „Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450/1.

*Obrázek 1*

**Reakce na kybernetický bezpečnostní incident/krizi na úrovni EU**




Všechny činnosti popsané níže se mají provádět v souladu se standardními operačními postupy/pravidly zapojených mechanismů spolupráce a dále v souladu s ustavenými mandáty a pravomocemi jednotlivých aktérů a institucí. Je možné, že tyto postupy/pravidla bude nutné doplnit nebo upravit, aby bylo dosaženo co nejlepší spolupráce a co nejúčinnější reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize.

Je možné, že při některém konkrétním incidentu nebude od všech aktérů vyžadováno, aby přijali opatření. Nicméně plán a příslušné standardní operační postupy mechanismů spolupráce by měly předpokládat jejich možné zapojení.

Vzhledem k různé míře dopadu, jejž může mít kybernetický bezpečnostní incident na společnost, bude vysoký stupeň pružnosti, pokud jde o zapojení odvětvových aktérů na všech úrovních, a jakákoli náležitá reakce záviset jak na kybernetických, tak na nekybernetických zmírňujících opatřeních.

## Řešení kybernetických bezpečnostních krizí – začlenění kybernetické bezpečnosti do postupu IPCR

Opatření IPCR, popsaná ve standardních operačních postupech IPCR ([1]), se řídí posloupností podle kroků popsaných níže (uplatnění některých z těchto kroků bude záviset na situaci).

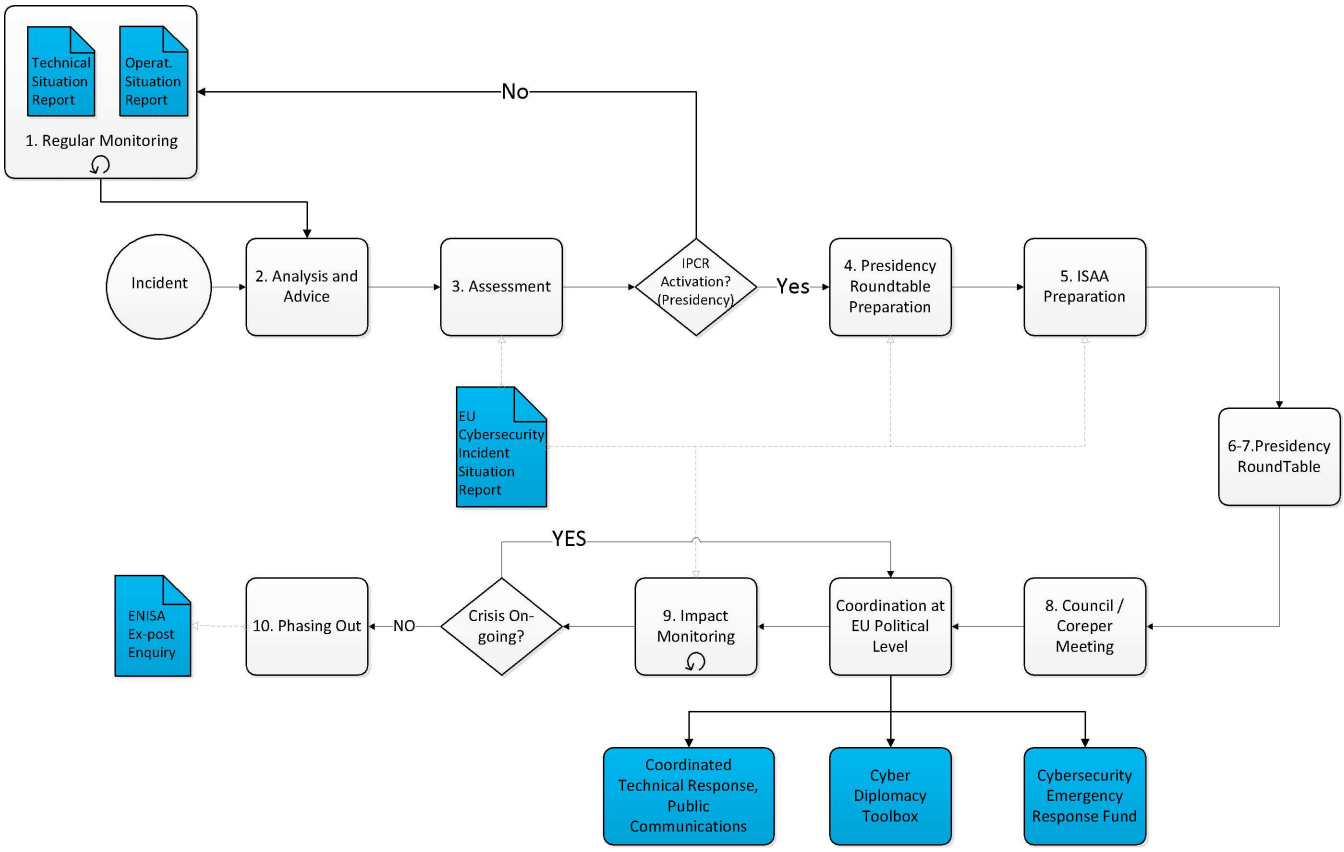
Při každém kroku uvádíme konkrétní činnosti a aktéry kybernetické bezpečnosti. Pro snazší orientaci je při každém kroku uveden text ze standardních operačních postupů IPCR a po něm následují konkrétní opatření plánu. Tento přístup založený na postupných krocích rovněž umožňuje jednoznačné určení stávajících **nedostatků** v nezbytných schopnostech a postupech, které brání účinné reakci na kybernetické bezpečnostní krize.

Obrázek 2 (níže ([2])) je grafické zobrazení postupu IPCR, v němž jsou nové prvky zvýrazněny modře.

([1]) Z dokumentu 12607/15 „Standardní operační postupy integrované politické reakce EU na krize“, který schválila Skupina přátel předsednictví a který vzal Výbor stálých zástupců na vědomí v říjnu 2015.
([2]) Větší verzi obrázku lze nalézt v dodatku.

*Obrázek 2*

**Konkrétní prvky kybernetické bezpečnosti v IPCR**




*Poznámka:* Vzhledem k povaze hybridních hrozeb v kybernetické oblasti, které jsou koncipovány tak, aby zůstaly pod prahem zřejmé krize, musí EU přijmout opatření v oblasti prevence a připravenosti. Středisko EU pro hybridní hrozby má za úkol rychle analyzovat relevantní incidenty a informovat příslušné koordinační struktury. Pravidelné podávání zpráv střediskem pro hybridní hrozby může přispět k utváření odvětvové politiky s cílem posílit připravenost.

— **Krok 1 – Pravidelné odvětvové monitorování a varování**: stávající pravidelné odvětvové situační zprávy a varování poskytují předsednictví Rady informace o rozvíjející se krizi a jejím možném vývoji.

— **Zjištěný nedostatek**: V současnosti neexistují pravidelné a koordinované zprávy o situaci v oblasti kybernetické bezpečnosti ani varování, pokud jde o kybernetické bezpečnostní incidenty (a hrozby) na úrovni EU.

— **Plán: monitorování situace v oblasti kybernetické bezpečnosti EU/podávání zpráv o této situaci**

— Agentura ENISA bude **pravidelně** připravovat **technickou zprávu EU o situaci v oblasti kybernetické bezpečnosti** týkající se kybernetických bezpečnostních incidentů a hrozeb na základě veřejně dostupných informací, svých vlastních analýz a zpráv, které s ní (dobrovolně) sdílejí týmy CSIRT členských států nebo jednotná kontaktní místa podle směrnice o bezpečnosti sítí a informací, Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu, skupina CERT-EU a Evropské středisko pro analýzu zpravodajských informací (INTCEN) při Evropské službě pro vnější činnost (ESVČ). Zpráva by měla být k dispozici příslušným útvarům Rady, Komise a síti týmů CSIRT.

— Středisko EU pro hybridní hrozby by jménem SIAC mělo vytvářet **operační zprávu EU o situaci v oblasti kybernetické bezpečnosti**. Tato zpráva rovněž představuje podporu pro rámec pro společnou diplomatickou reakci EU na kybernetické činnosti se zlým úmyslem.

— Obě zprávy jsou šířeny mezi zainteresovanými stranami na úrovni EU a členských států, aby přispívaly k jejich vlastní informovanosti o situaci, utvářely rozhodování a usnadňovaly přeshraniční regionální spolupráci.

Poté, co byl zjištěn incident

— **Krok 2 – Analýza a doporučení**: na základě dostupného monitorování a varování se útvary Komise, ESVČ a generální sekretariát Rady vzájemně informují o možném vývoji, aby byly připraveny poskytovat předsednictví doporučení pro případnou aktivaci (v plném rozsahu nebo v režimu sdílení informací) IPCR.

  — **Plán:**

    — Pokud jde o Komisi, GŘ CNECT, GŘ HOME, GŘ HR.DS a GŘ DIGIT, podporované agenturou ENISA, centrem EC3 a skupinou CERT-EU.

    — ESVČ. Středisko EU pro hybridní hrozby, které využívá práci situačního střediska EU (SITROOM) a zpravodajské zdroje, zajišťuje informovanost o situaci, pokud jde o skutečné a potenciální hybridní hrozby pro EU a její partnery, včetně kybernetických hrozeb. Proto v případě, že analýza a posouzení střediska EU pro hybridní hrozby naznačují existenci možných hrozeb namířených proti členskému státu, partnerské zemi nebo organizaci, INTCEN bude podle zavedených postupů informovat (v prvé řadě) na operační úrovni. Na operační úrovni se pak vypracují doporučení pro politicko-strategickou úroveň, včetně případné aktivace opatření pro řešení krizí v monitorovacím režimu (např. mechanismus ESVČ pro reakce na krize nebo monitorovací stránka IPCR).

    — Předseda sítě týmů CSIRT, jemuž je nápomocna agentura ENISA, připravuje situační zprávu EU o kybernetických bezpečnostních incidentech ([1]), jež se předkládá předsednictví, Komisi a vysokému představiteli/místopředsedovi Komise prostřednictvím týmu CSIRT rotujícího předsednictví.

— **Krok 3 – Posouzení/rozhodnutí o aktivaci opatření IPCR**: předsednictví posoudí, zda je zapotřebí politická koordinace, výměna informací či rozhodování na úrovni EU. Za tímto účelem může předsednictví svolat neformální zasedání u kulatého stolu. Předsednictví předběžně určí oblasti, které vyžadují zapojení výboru COREPER či Rady. To bude základem pokynů pro vypracování zpráv týkajících se integrované informovanosti o situaci a analýzy situace (ISAA). S přihlédnutím k povaze krize, jejím možným dopadům a souvisejícím politickým potřebám rozhodne předsednictví o tom, zda je vhodné svolat zasedání příslušných pracovních skupin Rady a/nebo výboru COREPER a/nebo Politického a bezpečnostního výboru.

  — **Plán:**

    — Účastníci zasedání u kulatého stolu:

      — Útvary Komise a ESVČ budou poskytovat předsednictví poradenství ve svých příslušných oblastech působnosti.

      — Zástupci členských států v Horizontální pracovní skupině pro otázky týkající se kybernetiky, podporovaní odborníky z hlavních měst (týmy CSIRT, orgány příslušné pro kybernetickou bezpečnost atd.).

      — Politické/strategické pokyny pro zprávy ISAA založené na nejnovější situační zprávě EU o kybernetických bezpečnostních incidentech a dalších informacích poskytnutých účastníky zasedání u kulatého stolu.

      — Příslušné pracovní skupiny a výbory:

        — Horizontální pracovní skupina pro otázky týkající se kybernetiky.

  Komise, ESVČ a generální sekretariát Rady, s plným souhlasem a zapojením předsednictví, mohou rovněž rozhodnout o aktivaci IPCR v režimu sdílení informací tím, že vytvoří stránku věnovanou krizi, aby připravily podmínky pro případnou úplnou aktivaci.

— **Krok 4 – Aktivace IPCR/shromažďování a výměna informací**: po aktivaci (ať už v režimu sdílení informací nebo v plném rozsahu) je na webové platformě IPCR vytvořena stránka věnovaná krizi, umožňující konkrétní výměnu informací se zaměřením na aspekty, které budou přispívat ke zprávám ISAA a připravovat diskusi na politické úrovni. To, který útvar bude vedoucím (některý z útvarů Komise nebo ESVČ), bude záviset na okolnostech případu.

— **Krok 5 – Vytváření ISAA**: bude iniciováno vypracování zpráv ISAA. Komise/ESVČ vydá zprávy ISAA, jak je uvedeno ve standardních operačních postupech ISAA, a může dále podporovat výměnu informací na webové

([1]) Situační zpráva EU o kybernetických bezpečnostních incidentech je souhrnem vnitrostátních zpráv poskytnutých vnitrostátními týmy CSIRT. Formát této zprávy by měl být popsán ve standardních operačních postupech sítě týmů CSIRT.

platformě IPCR nebo předkládat konkrétní žádosti o informace. Zprávy ISAA budou přizpůsobeny potřebám na politické úrovni (tj. výboru COREPER nebo Rady), jak je vymezí předsednictví a jak budou stanoveny v jeho pokynech, což umožní strategický přehled o situaci a kvalifikovanou rozpravu o bodech programu vymezených předsednictvím. O tom, zda zprávu ISAA vypracuje jeden z útvarů Komise (GŘ CNECT, GŘ HOME), nebo ESVČ, se rozhodne v souladu se standardními operačními postupy ISAA podle povahy kybernetické bezpečnostní krize.

V návaznosti na aktivaci IPCR nastíní předsednictví konkrétní oblasti, na které se ISAA soustředí, aby podporovala politickou koordinaci a/nebo rozhodovací proces v Radě. Předsednictví rovněž po konzultacích s útvary Komise/ESVČ určí načasování zprávy.

— **Plán:**

— Zpráva ISAA obsahuje příspěvky relevantních útvarů, včetně:

— sítě týmů CSIRT v podobě situační zprávy EU o kybernetických bezpečnostních incidentech,

— centra EC3, střediska SITROOM, střediska EU pro hybridní hrozby, skupiny CERT-EU; středisko EU pro hybridní hrozby bude případně podporovat vedoucí útvar ISAA a kulatý stůl IPCR a poskytovat jim příspěvky,

— odvětvových agentur a subjektů EU v závislosti na dotčených odvětvích,

— orgánů členských států (jiných než týmů CSIRT).

— Shromažďování vstupů ISAA ([1]):

— Komise a agentury EU: interní páteřní síť pro ISAA bude zajišťována informačním systémem ARGUS. Agentury EU musí své příspěvky zaslat svému příslušnému GŘ, které pak relevantní informace vloží do systému ARGUS. Útvary Komise a agentury shromáždí informace ze stávajících odvětvových sítí vytvořených spolu s členskými státy a mezinárodními organizacemi a z dalších relevantních zdrojů.

— Pokud jde o ESVČ: interní páteřní síť a jednotné kontaktní místo budou zajišťovány situačním střediskem EU za podpory dalších relevantních oddělení ESVČ. ESVČ bude shromažďovat informace z třetích zemí a z relevantních mezinárodních organizací.

— **Krok 6 – Příprava neformálního kulatého stolu předsednictví**: předsednictví, kterému je nápomocen generální sekretariát Rady, vymezí časový plán, program, účastníky a očekávané výsledky (možné výstupy) neformálního zasedání předsednictví u kulatého stolu. Generální sekretariát Rady bude jménem předsednictví předávat příslušné informace webové platformě IPCR, a zejména vydá oznámení o zasedání.

— **Krok 7 – Kulatý stůl předsednictví/přípravná opatření pro politickou koordinaci/rozhodování EU**: předsednictví uspořádá neformální kulatý stůl, aby vyhodnotilo situaci a připravilo a posoudilo body, na které má být upozorněn výbor COREPER nebo Rada. Neformální kulatý stůl předsednictví bude také fórem pro vypracování, posouzení a projednání veškerých návrhů opatření, které mají být předloženy výboru COREPER/Radě.

— **Plán:**

— Horizontální pracovní skupina Rady pro otázky týkající se kybernetiky by měla připravit zasedání Politického a bezpečnostního výboru nebo výboru COREPER.

— **Krok 8 – Politická koordinace a rozhodování ve výboru COREPER/v Radě**: výsledky zasedání výboru COREPER/Rady se týkají koordinace činností v oblasti reakce na všech úrovních, rozhodnutí o mimořádných opatřeních, politických prohlášeních atd. Tato rozhodnutí rovněž představují aktualizované politické/strategické pokyny pro další vytváření zpráv ISAA.

— **Plán:**

— Politické rozhodnutí o koordinaci reakce na kybernetickou bezpečnostní krizi se uskutečňuje prostřednictvím činností (prováděných příslušnými aktéry) popsaných výše v oddíle 1 „Spolupráce na strategické/politické, operační a technické úrovni“, pokud jde o **reakci** a **komunikaci s veřejností**.

— Vytváření ISAA pokračuje na technické, operační a politické/strategické úrovni, pokud jde o **informovanost o situaci**, popsanou rovněž výše v oddíle 1.

([1]) Standardní operační postupy ISAA.

— **Krok 9 – Monitorování dopadu**: vedoucí útvar ISAA s podporou přispěvatelů ISAA poskytne informace o vývoji krize a dopadu přijatých politických rozhodnutí. Tato zpětnovazební smyčka bude podporovat proces a rozhodnutí předsednictví při pokračujícím zapojení politické úrovně EU nebo při postupném omezování opatření IPCR.

— **Krok 10 – Postupné ukončování**: předsednictví může stejným postupem jako při aktivaci svolat neformální zasedání u kulatého stolu s cílem posoudit možnost, zda zachovat aktivní opatření IPCR, či nikoli. Předsednictví může rozhodnout o ukončení nebo omezení aktivace.

— **Plán:**

— Agentura ENISA může být vyzvána k tomu, aby přispěla k technickému šetření incidentu *ex post* nebo aby je provedla v souladu s ustanoveními svého mandátu.

*DODATEK*

1. MECHANISMY PRO ŘEŠENÍ KRIZÍ, MECHANISMY SPOLUPRÁCE A AKTÉŘI NA ÚROVNI EU

**Mechanismy pro řešení krizí**

*Integrovaná opatření EU pro politickou reakci na krize (IPCR)*: Integrovaná opatření EU pro politickou reakci na krize (dále jen „IPCR“), jež schválila Rada dne 25. června 2013 ([1]), mají usnadnit včasnou koordinaci a reakci na politické úrovni EU v případě závažné krize. IPCR rovněž na politické úrovni podporují koordinaci reakce na uplatnění doložky solidarity (článek 222 SFEU), jak je uvedeno v rozhodnutí Rady 2014/415/EU o provádění doložky solidarity Unií, přijatém dne 24. června 2014. Standardní operační postupy IPCR ([2]) stanoví aktivační postup a následné kroky.

*ARGUS*: Systém pro koordinaci v krizových situacích, který zřídila Evropská komise v roce 2005 s cílem stanovit zvláštní koordinační postup v případě závažných krizí zasahujících více odvětví. Opírá se o všeobecný systém rychlého varování (nástroj IT) se stejným názvem. Systém ARGUS má dvě fáze, přičemž v druhé fázi (v případě závažné více odvětvové krize) svolává z pověření předsedy Komise nebo člena Komise, kterému byla přidělena odpovědnost, zasedání krizového koordinačního výboru. V tomto výboru se setkávají zástupci příslušných generálních ředitelství Komise, kabinetů a jiných útvarů EU, aby mohli vést a koordinovat reakci Komise na danou krizi. Výbor, kterému předsedá zástupce generálního tajemníka, zhodnotí situaci, zváží možnosti řešení a přijme vykonavatelná rozhodnutí týkající se nástrojů a prostředků EU, za které má Komise odpovědnost, a zajistí realizaci přijatých rozhodnutí ([3]) ([4]).

*Mechanismus ESVČ pro reakce na krize*: Mechanismus ESVČ pro reakce na krize je strukturovaný systém, který ESVČ umožňuje reagovat na krize a mimořádné situace s externí povahou nebo významným vnějším rozměrem – včetně hybridních hrozeb –, které by mohly mít nebo reálně mají dopad na zájmy EU nebo kteréhokoli členského státu. Mechanismus zajišťuje účast příslušných úředníků Komise a generálního sekretariátu Rady na zasedáních v tomto rámci, čímž podporuje součinnost mezi úsilím v oblasti diplomacie, bezpečnosti a obrany s finančními a obchodními nástroji a nástroji spolupráce řízenými Komisí. Krizová jednotka může být aktivována po celou dobu trvání krize.

**Mechanismy spolupráce**

*Síť bezpečnostních týmů typu CSIRT*: Síť bezpečnostních týmů typu CSIRT (Computer Security Incident Response Team Network) sdružuje všechny vnitrostátní a vládní týmy typu CSIRT a CERT-EU. Účelem této sítě je umožnit a posílit sdílení informací mezi týmy typu CSIRT o kybernetických bezpečnostních hrozbách a incidentech a rovněž spolupracovat při reakci na incidenty a krize v této oblasti.

*Horizontální pracovní skupina Rady pro otázky týkající se kybernetiky*: Tato pracovní skupina, která byla zřízena s cílem zajistit v Radě strategickou a horizontální koordinaci politických záležitostí v oblasti kybernetiky, se může se zapojovat do legislativní i nelegislativní činnosti.

**Subjekty**

*ENISA*: Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) byla zřízena v roce 2004. Úzce spolupracuje s členskými státy a soukromým sektorem s cílem poskytovat poradenství a řešení pro záležitosti, jako jsou celoevropská cvičení v oblasti kybernetické bezpečnosti, vypracování národních strategií kybernetické bezpečnosti, spolupráce týmů typu CSIRT a budování jejich kapacit. ENISA spolupracuje přímo s týmy CSIRT v celé EU a zajišťuje sekretariát síti CSIRT.

*Středisko pro koordinaci odezvy na mimořádné události*: Středisko pro koordinaci odezvy na mimořádné události v rámci Komise (Generálního ředitelství pro evropskou civilní ochranu a operace humanitární pomoci (GŘ ECHO)) nepřetržitě (7 dní v týdnu, 24 hodin denně) podporuje a koordinuje řadu činností v oblasti prevence, připravenosti a reakce. Středisko, které zahájilo svou činnost v roce 2013, funguje jako centrála reakcí Komise na krize (ve spolupráci s dalšími krizovými středisky EU), mimo jiné jakožto ústřední kontaktní místo IPCR s nepřetržitým provozem.

([1]) Dokument 10708/13 „Dokončení přezkumného postupu opatření pro koordinaci při krizích: integrovaná opatření EU pro politickou reakci na krize“, schválený Radou dne 24. června 2013.
([2]) Dokument 12607/15 „Standardní operační postupy integrované politické reakce EU na krize“, který schválila Skupina přátel předsednictví a který vzal COREPER na vědomí v říjnu 2015.
([3]) Předpisy Komise o všeobecném systému rychlého varování „ARGUS“, KOM(2005) 662 v konečném znění, 23. prosince 2005.
([4]) Rozhodnutí Komise 2006/25/ES, Euratom ze dne 23. prosince 2005, kterým se mění jednací řád Komise (Úř. věst. L 19, 24.1.2006, s. 20), kterým se zřizuje obecný systém včasného varování „ARGUS“.

*Europol/EC3*: Evropské centrum pro boj proti kyberkriminalitě (EC3), zřízené v roce 2013 v rámci Europolu, podporuje reakci donucovacích orgánů na kyberkriminalitu v EU. EC3 poskytuje operační a analytickou podporu členským státům při vyšetřování a slouží jako ústřední bod pro výměnu informací a zpravodajství o trestné činnosti. Podporuje operace a vyšetřování vedené členskými státy poskytováním operační analýzy, koordinace a odborných znalostí, jakož i vysoce specializovaných technických dovedností a digitální forenzní podpory.

*CERT-EU*: Skupina pro reakci na počítačové hrozby v evropských orgánech, institucích a jiných subjektech je pověřena zlepšováním ochrany evropských institucí, orgánů a jiných subjektů před kybernetickými hrozbami. Je členem sítě týmů CSIRT. Skupina CERT-EU má technické dohody o sdílení informací o kybernetických hrozbách se složkou NATO pro schopnost reakce na počítačové incidenty (NCIRC), některými třetími zeměmi a hlavními komerčními subjekty v oblasti kybernetické bezpečnosti.

Zpravodajská síť EU zahrnuje Středisko EU pro analýzu zpravodajských informací (**EU INTCEN**) a zpravodajské ředitelství Vojenského štábu EU (EUMS INT) v rámci ujednání o **společné zpravodajsko-analytické složce** (SIAC). Posláním SIAC je poskytovat vysokému představiteli Evropské unie pro zahraniční věci a bezpečnostní politiku a Evropské službě pro vnější činnost (ESVČ) zpravodajské analýzy, včasná varování a informovanost o situaci. SIAC nabízí své služby různým orgánům EU v oblasti společné zahraniční a bezpečnostní politiky (SZBP), společné bezpečnostní a obranné politiky (SBOP) a boje proti terorismu, jež mají rozhodovací pravomoc, jakož i členským státům. EU INTCEN a EUMS INT nejsou operační agentury a nemohou shromažďovat údaje. Za operativní úroveň zpravodajství odpovídají členské státy, SIAC se zabývá pouze strategickou analýzou.

*Středisko EU pro hybridní hrozby*: Společné sdělení o boji proti hybridním hrozbám z dubna 2016 označuje středisko EU pro hybridní hrozby za ústřední bod pro všechny výchozí analýzy týkající se hybridních hrozeb v EU. Jeho mandát byl schválen v prosinci 2016 Komisí prostřednictvím konzultací mezi jednotlivými útvary. Středisko EU pro hybridní hrozby bylo zřízeno při EU INTCEN a je součástí SIAC, spolupracuje tedy s EUMS INT a je mu přidělen stálý vojenský zástupce. „Hybridní" označuje úmyslné použití kombinace různých skrytých či zjevných, vojenských či civilních nástrojů a mechanismů, jako jsou kybernetické útoky, dezinformační kampaně, špionáž, ekonomický tlak, využívání zástupných aktivit nebo jiná podvratná činnost, státním či nestátním subjektem. Středisko EU pro hybridní hrozby spolupracuje s rozsáhlou sítí kontaktních míst v rámci Komise i členských států s cílem zajistit integrovanou reakci/integrovaný přístup celé státní správy, jež jsou nezbytné při řešení různých výzev.

*Situační středisko EU*: Situační středisko EU je součástí Střediska EU pro analýzu zpravodajských informací (EU INTCEN) a poskytuje operační kapacitu ESVČ, aby bylo možné zajistit okamžitou a účinnou reakci na krizové situace. Je to stálý civilně-vojenský pohotovostní subjekt, který zajišťuje monitorování a informovanost o situaci v celosvětovém měřítku a je schopen fungovat nepřetržitě (7 dní v týdnu, 24 hodin denně).

**Relevantní nástroje**

*Rámec pro společnou diplomatickou reakci EU na kybernetické činnosti se zlým úmyslem*: Tento rámec, dohodnutý v červnu 2017, je součástí přístupu EU ke kybernetické diplomacii, jenž přispívá k předcházení konfliktům, zmírňování kybernetických bezpečnostních hrozeb a větší stabilitě v oblasti mezinárodních vztahů. Rámec plně využívá opatření v oblasti společné zahraniční a bezpečnostní politiky, včetně případných omezujících opatření. Používání opatření v tomto rámci by mělo podpořit spolupráci, usnadnit zmírňování okamžitých a dlouhodobých hrozeb a ovlivňovat chování příslušných pachatelů a potenciálních agresorů v dlouhodobém horizontu.

2. KRIZOVÁ KOORDINACE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI V OPATŘENÍCH IPCR – ROVINA HORIZONTÁLNÍ KOORDINACE A POLITICKÁ ESKALACE

Opatření IPCR mohou být používána (a jsou používána) k řešení technických a operačních otázek, ale vždy z politického či strategického hlediska.

V případě eskalace mohou být použita podle závažnosti krize tak, že se z „režimu monitorování" přejde na „režim sdílení informací", který je první úrovní aktivace IPCR, a poté na „plnou aktivaci IPCR".

O aktivaci plného režimu rozhoduje rotující předsednictví Rady EU. Komise, ESVČ a generální sekretariát Rady mohou aktivovat IPCR v režimu sdílení informací. V režimu monitorování a režimu sdílení informací se spustí různé úrovně výměny informací; v režimu sdílení informací se aktivuje žádost o vypracování zpráv ISAA. Při plné aktivaci se soubor

nástrojů doplní o zasedání IPCR u kulatého stolu, při nichž k jednacímu stolu zasedne předsednictví (obvykle předseda výboru COREPER II nebo odborník na danou oblast na úrovni poradců stálého zastoupení, ve výjimečných případech zasedání u kulatého stolu na ministerské úrovni).

*Aktéři*

Vedení: rotující předsednictví (zpravidla předseda výboru COREPER)

Za Evropskou radu – kabinet předsedy

Za Evropskou komisi – úroveň zástupce generálního tajemníka/GŘ a/nebo odborníků na danou oblast

Za ESVČ – úroveň zástupce generálního tajemníka/výkonného ředitele a/nebo odborníků na danou oblast

Za generální sekretariát Rady – kabinet generálního tajemníka, tým IPCR a příslušná GŘ

*Rozsah činností*: Vytvoření společného uceleného obrazu o situaci a zvyšování povědomí o nedostatcích či problémech na každé ze tří úrovní, aby je bylo možné řešit na politické úrovni; tvorba rozhodnutí u jednacího stolu, pokud spadají do kompetence účastníků, nebo návrhů opatření, které směřují do výboru COREPER II a poté do Rady.

*Sdílená informovanost o situaci:*

(IPCR neaktivní:) Mohou být vypracovávány monitorovací stránky IPCR s cílem sledovat vývoj situací, které by mohly eskalovat do podoby krize s důsledky pro EU.

(IPCR v režimu sdílení informací:) Vedoucí ISAA vypracuje na základě informací od útvarů Komise, ESVČ a členských států (prostřednictvím dotazníků IPCR) zprávy ISAA.

(IPCR v režimu plné aktivace:) Kromě zpráv ISAA probíhají neformální zasedání IPCR u kulatého stolu za účasti různých zúčastněných subjektů členských států, Komise, ESVČ, příslušných agentur atd. s cílem projednat nedostatky a problémy.

*Spolupráce a reakce:*

Podle povahy a dopadu daného incidentu se aktivují/synchronizují další mechanismy/nástroje pro řešení krizí. Mohou zahrnovat například mechanismus civilní ochrany, rámec pro společnou diplomatickou reakci EU na kybernetické činnosti se zlým úmyslem nebo Společný rámec pro boj proti hybridním hrozbám.

*Krizová komunikace:*

Předsednictví může po konzultaci s příslušnými útvary Komise, generálního sekretariátu Rady a ESVČ aktivovat síť krizových komunikátorů IPCR za účelem podpory vypracování společných sdělení nebo zjištění nejúčinnějších komunikačních nástrojů.

3. ŘEŠENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH KRIZÍ V SYSTÉMU ARGUS – SDÍLENÍ INFORMACÍ V RÁMCI EVROPSKÉ KOMISE

Komise v roce 2005 v reakci na neočekávané krize, které vyžadovaly kroky na evropské úrovni, tj. teroristické útoky v Madridu (březen 2004), tsunami v jihovýchodní Asii (prosinec 2004) a teroristické útoky v Londýně (červenec 2005), zřídila koordinační systém ARGUS podporovaný stejnojmenným všeobecným systémem rychlého varování ([1]) ([2]). Jeho cílem je stanovit **zvláštní koordinační postup** v případě závažných krizí zasahujících více odvětví, tak aby bylo možné v reálném čase sdílet informace související s danou krizí a zajistit rychlé rozhodování.

Podle závažnosti události má systém ARGUS dvě fáze:

*Fáze I* se používá pro „sdílení informací“ o krizi omezeného rozsahu.

([1]) Komise Evropských společenství, 23. prosince 2005, sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Předpisy Komise o všeobecném systému rychlého varování „ARGUS“, KOM(2005) 662 v konečném znění.

([2]) Rozhodnutí 2006/25/ES, Euratom.

Příklady nedávných událostí nahlášených v rámci fáze I zahrnují lesní požáry v Portugalsku a Izraeli, útok v Berlíně v roce 2016, záplavy v Albánii, hurikán Matthew na Haiti a sucho v Bolívii. Operaci fáze I může zahájit kterékoli generální ředitelství, usoudí-li, že je situace v jeho oblasti působnosti natolik vážná, že je sdílení informací opodstatněné nebo přínosné. Například GŘ CNECT nebo GŘ HOME mohou zahájit operaci fáze I, usoudí-li, že kybernetická situace v jejich příslušné oblasti působnosti je natolik vážná, že je sdílení informací opodstatněné nebo přínosné.

*Fáze II* se spustí v případě závažných krizí zasahujících více odvětví či v případě předpokládané nebo bezprostřední hrozby pro Unii.

Fáze II spustí zvláštní koordinační postup, který Komisi umožní v oblasti její působnosti a ve spolupráci s ostatními orgány přijímat rozhodnutí a řídit rychlou, koordinovanou a soudržnou reakci na nejvyšší úrovni. Fáze II je určena pro případy závažných krizí zasahujících více odvětví či případy předpokládané nebo bezprostřední hrozby takové krize. K příkladům reálných událostí, kdy byla spuštěna fáze II, patří migrační/uprchlická krize (od roku 2015 dosud), trojnásobná katastrofa ve Fukušimě (2011) a erupce sopky *Eyjafjallajökull* na Islandu (2010).

Fázi II aktivuje předseda z vlastního podnětu nebo na žádost některého člena Komise. Předseda může přidělit politickou odpovědnost za reakci Komise některému komisaři odpovědnému za útvar nejvíce dotčený danou krizí, nebo se může rozhodnout, že si odpovědnost ponechá.

Fáze II zahrnuje mimořádná zasedání krizového koordinačního výboru. Zasedání se svolávají z pověření předsedy Komise nebo člena Komise, kterému byla přidělena odpovědnost. Zasedání svolává generální sekretariát prostřednictvím nástroje IT systému ARGUS. Krizový koordinační výbor je zvláštní operační struktura řešení krizí zřízená za účelem vedení a koordinace reakce Komise na krizi. Sdružuje zástupce relevantních generálních ředitelství Komise, kabinetů a dalších útvarů EU. **Výbor**, kterému předsedá zástupce generálního tajemníka, **hodnotí situaci, zvažuje možnosti řešení a přijímá rozhodnutí a také zajišťuje, aby rozhodnutí a opatření byla provedena** a zároveň aby byla reakce jednotná a soudržná. Generální sekretariát poskytuje výboru podporu.

## 4. MECHANISMUS ESVČ PRO REAKCE NA KRIZE

Mechanismus ESVČ pro reakce na krize se aktivuje v okamžiku, kdy nastane vážná situace nebo mimořádná událost, která se jakýmkoli způsobem týká vnějšího rozměru EU. Mechanismus aktivuje náměstek generálního tajemníka Rady EU pro reakci na krize po konzultaci s vysokým představitelem nebo generálním tajemníkem. Náměstka generálního tajemníka pro reakci na krize může o aktivaci mechanismu pro reakce na krize požádat také vysoký představitel, generální tajemník nebo jiný zástupce generálního tajemníka či výkonný ředitel.

Mechanismus pro reakce na krize přispívá k soudržné reakci EU na krize v rámci bezpečnostní strategie. Zejména usnadňuje součinnost diplomatického, bezpečnostního a obranného úsilí s finančními a obchodními nástroji a nástroji spolupráce řízenými Komisí.

Mechanismus je propojen se všeobecným systémem reakce na mimořádné události Komise (ARGUS) a integrovanými opatřeními EU pro politickou reakci na krize (IPCR), aby bylo možné využít synergie v případě jejich paralelní aktivace. Situační středisko v rámci ESVČ funguje jako komunikační centrum mezi ESVČ a systémy reakce na mimořádné situace v Radě a Komisi.

Prvním opatřením souvisejícím s prováděním mechanismu pro reakce na krize je obvykle svolání **krizového zasedání** vysokých úředníků ESVČ, Komise a Rady, kterých se daná krize přímo týká. Krizové zasedání posoudí krátkodobé dopady krize a může rozhodnout o přijetí okamžitých opatření, o aktivaci krizové jednotky nebo o svolání krizové platformy. Tyto kroky mohou následovat v jakémkoli pořadí.

**Krizová jednotka** je menší operační místnost, kde se scházejí zástupci ESVČ a útvarů Komise a Rady zapojených do reakce na krizi, aby trvale monitorovali situaci s cílem poskytnout podporu osobám s rozhodovací pravomocí v ústředí ESVČ. Je-li krizová jednotka aktivována, funguje nepřetržitě (24 hodin denně, 7 dní v týdnu).

**Krizová platforma** sdružuje příslušné útvary ESVČ, Komise a Rady s cílem zhodnotit střednědobé a dlouhodobé následky krizí a dohodnout se na opatřeních, která mají být přijata. Předsedá jí vysoký představitel, generální tajemník nebo náměstek generálního tajemníka pro reakce na krize. Krizová platforma hodnotí účinnost opatření EU v zemi nebo regionu zasažených krizí, rozhoduje o změnách podoby dalších opatření a projednává návrhy opatření Rady. Krizová platforma se schází *ad hoc*, není proto trvale aktivována.

**Pracovní skupina** je složena ze zástupců útvarů zapojených do dané reakce na krizi. Může být aktivována, aby sledovala a usnadňovala provádění reakce EU. Hodnotí dopady opatření EU, připravuje politické dokumenty a návrhy možností, přispívá k přípravě politického rámce pro krizový přístup, přispívá ke komunikační strategii a přijímá jakákoli další opatření, která mohou usnadnit provádění reakce EU.

## 5. REFERENČNÍ DOKUMENTY

Níže je uveden seznam referenčních dokumentů, které byly zohledněny při přípravě tohoto plánu:

— The European Cyber Crises Cooperation Framework (Evropský rámec pro spolupráci v oblasti kybernetických krizí), verze 1, 17. října 2012

— Report on Cyber Crisis Cooperation and Management (Zpráva o spolupráci a řízení v případě kybernetické krize), ENISA, 2014

— Actionable Information for Security Incident Response (Informace využitelné pro reakci na bezpečnostní incidenty), ENISA, 2014

— Common practices of EU-level crisis management and applicability to cyber crises (Společné postupy řešení krizí na úrovni EU a jejich použitelnost na kybernetické krize), ENISA, 2015

— Strategies for Incident Response and Cyber Crisis Cooperation (Strategie reakce na incidenty a spolupráce v případě kybernetické krize), ENISA, 2016

— EU Cyber Standard Operating Procedures (Standardní operační postupy EU v oblasti kybernetiky), ENISA, 2016

— A good practice guide of using taxonomies in incident prevention and detection (Příručka osvědčených postupů pro používání taxonomie v prevenci a odhalování incidentů), ENISA, 2017

— Sdělení „Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti", COM(2016) 410 final, 5. července 2016

— Závěry Rady o posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti – závěry Rady (15. listopadu 2016), 14540/16

— Rozhodnutí Rady 2014/415/EU ze dne 24. června 2014 o způsobu provádění doložky solidarity Unií (Úř. věst. L 192, 1.7.2014, s. 53)

— Dokončení přezkumného postupu opatření pro koordinaci při krizích: integrovaná opatření pro politickou reakci EU na krize (opatření IPCR), 10708/13, 7. června 2013

— Integrated Situational Awareness and Analysis (ISAA) – Standard Operating Procedures (Integrovaná informovanost o situaci a analýza situace (ISAA) – Standardní operační postupy), DS 1570/15, 22. října 2015

— Předpisy Komise o všeobecném systému rychlého varování „ARGUS", KOM(2005) 662 v konečném znění, 23. prosince 2005

— Rozhodnutí Komise 2006/25/ES, Euratom ze dne 23. prosince 2005, kterým se mění jednací řád Komise (Úř. věst. L 19, 24.1.2006, s. 20)

— ARGUS Modus Operandi, Evropská komise, 23. října 2013

— Závěry Rady o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky"), 9916/17

— EU operational protocol for countering hybrid threats („EU Playbook") (Operační protokol EU pro boj proti hybridním hrozbám (EU Playbook)), SWD(2016) 227

— EEAS Crisis Response Mechanism (Mechanismus ESVČ pro reakce na krize), 8. listopadu 2016 (Ares(2017)880661). Společný pracovní dokument útvarů „Operační protokol EU pro boj proti hybridním hrozbám (EU Playbook)", SWD(2016) 227 final, 5. července 2016

— Společné sdělení Evropskému parlamentu a Radě: Společný rámec pro boj proti hybridním hrozbám – reakce Evropské unie, JOIN/2016/018 final, 6. dubna 2016

— Dokument ESVČ(2016) 1674 – pracovní dokument Evropské služby pro vnější činnost – středisko EU pro hybridní hrozby – působnost

6. KONKRÉTNÍ PRVKY KYBERNETICKÉ BEZPEČNOSTI V RÁMCI POSTUPU IPCR