Rada
Evropské unie

Brusel 6. prosince 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Příjemce:	Delegace
Předmět:	Závěry Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA)

Delegace naleznou v příloze závěry Rady o Agentuře Evropské unie pro kybernetickou bezpečnost ve znění schváleném Radou na jejím zasedání konaném dne 6. prosince 2024.

PŘÍLOHA

Návrh závěrů Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA)

RADA EVROPSKÉ UNIE

1. POUKAZUJE na to, že výzvy vyplývající z globálního kyberprostoru nebyly nikdy tak složité, rozmanité a závažné jako v současnosti, což je důsledkem propracovanosti nově vznikajících kybernetických hrozeb, neustále se měnícího bezpečnostního prostředí a současného geopolitického napětí. EU a její členské státy by proto měly nadále vyvíjet úsilí o zvýšení odolnosti s cílem účinně identifikovat a řešit stávající a nově vznikající hrozby a výzvy. ZDŮRAZŇUJE, že práce směřující ke zvýšení úrovně kybernetické odolnosti by měla pokračovat na základě celospolečenského přístupu. ZDŮRAZŇUJE, že v nadcházejících letech by se EU a její členské státy měly zaměřit na účinné provádění legislativních a nelegislativních iniciativ, jež podporují všechna opatření, která byla v tomto ohledu dosud přijata, a přispívají k nim.

2. PŘIPOMÍNAJÍC, že národní bezpečnost zůstává výhradní odpovědností každého členského státu, UZNÁVÁ, že EU a její členské státy v posledních letech intenzivně spolupracovaly na vytvoření nezbytného institucionálního uspořádání a forem spolupráce v kybernetické oblasti na vnitrostátní i unijní úrovni. VÍTÁ nejrůznější legislativní a nelegislativní iniciativy, jež EU a jejím členským státům poskytly silný a spolehlivý rámec v této oblasti, který zvyšuje celkovou kybernetickou odolnost Unie. Tento rámec se rozvinul tak, že nyní zahrnuje několik aspektů kybernetické oblasti: bezpečnost, diplomacii, prosazování práva a obranu. KONSTATUJE, že součástí ekosystému kybernetické bezpečnosti EU je velký počet aktérů, včetně orgánů členských států pro kybernetickou bezpečnost, skupiny pro spolupráci v oblasti bezpečnosti sítí a informací (NIS CG), sítě CSIRT, Evropské sítě styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), sítě národních koordinačních center (NCC), Evropské skupiny pro certifikaci kybernetické bezpečnosti (ECCG), Komise, Evropské služby pro vnější činnost (ESVČ), Agentury Evropské unie pro kybernetickou bezpečnost (ENISA), Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC), CERT-EU, Evropské obranné agentury (EDA) a Evropského centra Europolu pro boj proti kyberkriminalitě (EC3), přičemž každý z nich plní svou úlohu při provádění celounijního rámce kybernetické bezpečnosti.

3. UZNÁVÁ, že ENISA se v posledních dvou desetiletích osvědčila jako neocenitelný subjekt v evropském ekosystému kybernetické bezpečnosti a hraje klíčovou úlohu při aktivní podpoře členských států a orgánů, institucí a jiných subjektů EU při provádění a rozvoji politik v oblasti kybernetické bezpečnosti, při budování jejich kapacit a připravenosti, při jejich spolupráci a při podpoře informovanosti a certifikace v oblasti kybernetické bezpečnosti.

OBECNÁ POLITICKÁ DOPORUČENÍ

4. VYZÝVÁ Komisi, aby využila **hodnocení aktu o kybernetické bezpečnosti** jako příležitost k posouzení toho, jak může přispět ke zjednodušení složitého kybernetického ekosystému, a tím zvýšit účinnost a efektivní využívání zdrojů. VYZÝVÁ proto Komisi, aby zajistila, že mandát ENISA na podporu členských států a orgánů, institucí a jiných subjektů EU bude cílený a jasně vymezený a bude vedle přesnějšího rozdělení úkolů a pravomocí s ohledem na další aktéry zahrnovat také konkrétní strategické cíle a prioritní úkoly. V tomto ohledu VYZÝVÁ Komisi, aby přezkoumala a dále posílila úlohu ENISA při podpoře operativní spolupráce na úrovni EU a mezi členskými státy při zvyšování kybernetické odolnosti, a to s ohledem na pravomoci členských států v této oblasti. Dále Komisi VYZÝVÁ, aby posílila poradní úlohu ENISA při poskytování odborných a fakticky podložených pokynů a doporučení, pokud jde o provádění stávajících a budoucích legislativních a nelegislativních iniciativ EU, a zároveň zajistila soudržný rámec EU v oblasti kybernetické bezpečnosti.

5. Ve stejném duchu VYBÍZÍ Komisi, aby zvážila zefektivnění úlohy ENISA, pokud jde o úkoly, které nejsou podstatou jejího poslání. ZDŮRAZŇUJE, že **povinnosti** ENISA **byly výrazně rozšířeny** nedávnými legislativními iniciativami, mimo jiné včetně NIS 2, aktu o kybernetické odolnosti a aktu o kybernetické solidaritě. BERE NA VĚDOMÍ, že ENISA obdržela v důsledku některých těchto iniciativ dodatečné zdroje, zároveň však ZDŮRAZŇUJE, že rozšíření povinností agentury ENISA a rostoucí složitost kybernetických hrozeb a výzev vedly ke značnému nárůstu jejích úkolů, což by se mělo odrazit v **odpovídajících zdrojích** – lidských, finančních i technických –, aby agentura mohla v plném rozsahu plnit všechny úkoly spadající do její pravomoci, aniž by se předjímalo jednání o víceletém finančním rámci. Za tímto účelem VYZÝVÁ Komisi, aby při přípravě návrhu souhrnného rozpočtu Unie stanovila prioritu opatření a upřednostňovala úkoly související s podporou členských států při posilování jejich kybernetické odolnosti, operativní spolupráce a rozvoje a provádění práva Unie.

PODPORA ROZVOJE A PROVÁDĚNÍ POLITIK ZE STRANY AGENTURY ENISA

6. PŘIPOMÍNÁ, že podle stávajícího právního rámce v oblasti kybernetické bezpečnosti je agentuře ENISA svěřeno několik klíčových povinností v oblasti podpory a poradenství v celé EU. VÍTÁ v tomto ohledu úlohu ENISA při poskytování **pomoci členským státům** za účelem účinného provádění legislativních a nelegislativních iniciativ. VYZÝVÁ agenturu ENISA, aby v úzké spolupráci s NIS CG a Komisí i nadále poskytovala obecné poznatky a analýzu týkající se současného právního prostředí, pokud jde o kybernetickou bezpečnost. VYBÍZÍ agenturu ENISA, aby pravidelně a strukturovaným způsobem sdílela a aktivně prosazovala technické pokyny a osvědčené postupy, jež členským státům pomáhají při provádění politiky a právních předpisů v oblasti kybernetické bezpečnosti.

7. UZNÁVÁ zásadní úlohu agentury ENISA při rozvoji **evropských systémů certifikace kybernetické bezpečnosti**, které podporují důvěru v produkty, služby a procesy IKT a dále v řízené bezpečnostní služby s ohledem na připravovanou cílenou změnu aktu o kybernetické bezpečnosti. ZDŮRAZŇUJE, že členské státy a odvětví jsou znepokojeny zdlouhavým procesem výběru, vypracovávání a přijímání systémů certifikace kybernetické bezpečnosti; NALÉHAVĚ proto VYZÝVÁ Komisi, aby využila hodnocení aktu o kybernetické bezpečnosti jako příležitost k nalezení způsobů, jak dosáhnout jednoduššího, transparentnějšího a rychlejšího přístupu k rozvoji systémů certifikace kybernetické bezpečnosti v EU založeného na posouzení rizik, a zároveň ZDŮRAZŇUJE důležitou úlohu členských států v tomto procesu. Kromě toho ZDŮRAZŇUJE, že je důležité výslovně určit odpovědnost za údržbu každého systému certifikace. Dále PŘIPOMÍNÁ, že ENISA by při přípravě návrhů systémů měla prostřednictvím formálního, otevřeného, transparentního a inkluzivního procesu včas konzultovat všechny příslušné zúčastněné strany a že Komise by při posuzování účinnosti a využívání přijatých systémů měla otevřeným, transparentním a inkluzivním způsobem vést konzultace. VYBÍZÍ agenturu ENISA, aby dále posilovala spolupráci s komunitou zabývající se ochranou údajů, ve vhodných případech zejména s Evropským sborem pro ochranu osobních údajů, a s příslušnými vnitrostátními orgány, se zvláštním ohledem na podporu synergií v souvislosti s rozvojem budoucích evropských systémů certifikace kybernetické bezpečnosti.

8. S cílem zabránit zbytečné administrativní zátěži, která by mohla vzniknout v důsledku složitého rámce pro podávání zpráv, VYZÝVÁ agenturu ENISA, aby ve spolupráci s Komisí pokračovala ve výměně informací s členskými státy o praktických aspektech, zjednodušení a zefektivnění postupu podávání zpráv. Dále PŘIPOMÍNÁ svou výzvu Komisi, aby s podporou agentury ENISA a dalších příslušných subjektů EU připravila mapování relevantních oznamovacích povinností stanovených v příslušných legislativních aktech EU týkajících se kybernetických a digitálních otázek. PŘIPOMÍNÁ, že výměna informací mezi agenturou ENISA a členskými státy je založena na vztahu důvěry, v němž je zaručena bezpečnost a důvěrnost v souladu s aktem o kybernetické bezpečnosti a příslušnými pravidly a protokoly, a měla by být omezena na to, co je relevantní a přiměřené účelu výměny. ZDŮRAZŇUJE, že je třeba zacházet s údaji a informacemi s náležitou péčí.

9. ZDŮRAZŇUJE skutečnost, že ENISA je odpovědná za zřízení a udržování **jednotné platformy pro podávání zpráv podle aktu o kybernetické odolnosti**, která bude mít konkrétní operativní přidanou hodnotu, zejména pokud jde o aktivně zneužívané zranitelnosti a závažné incidenty ovlivňující bezpečnost produktů s digitálními prvky. Vzhledem k široké oblasti působnosti tohoto horizontálního právního předpisu by jednotná platforma pro podávání zpráv měla být účinným a bezpečným nástrojem pro usnadnění sdílení informací mezi vnitrostátními týmy CSIRT a agenturou ENISA. V důsledku toho NALÉHAVĚ VYZÝVÁ agenturu ENISA, aby vedle vyčlenění dostatečných lidských zdrojů jako klíčovou prioritu urychlila zřízení platformy, a zajistila tak její připravenost ve lhůtě stanovené v aktu o kybernetické odolnosti.

10. UZNÁVÁ úlohu agentury ENISA při vytváření **Evropské databáze zranitelností**, jejímž cílem je zajistit větší transparentnost v souvislosti s odhalováním zranitelností a zároveň zajistit vhodné zacházení s citlivými údaji. S ohledem na konec lhůty pro provedení směrnice NIS 2 ve vnitrostátním právu NALÉHAVĚ VYZÝVÁ agenturu ENISA, aby zintenzivnila veškerou činnost nezbytnou k zajištění hladkého fungování této databáze. Současně VYZÝVÁ skupinu NIS CG, aby s pomocí agentury ENISA dále zveřejňovala pokyny, politiky a postupy týkající se zveřejňování zranitelností.

11. UZNÁVÁ přínosy **akce** agentury ENISA na **podporu kybernetické bezpečnosti**, která funguje jako soubor služeb kybernetické bezpečnosti dostupných členským státům jako doplněk k jejich úsilí, jakož i zkušenosti agentury ENISA získané při jeho provádění. V tomto ohledu ZDŮRAZŇUJE, že by ENISA měla hrát ústřední úlohu při správě a provozu rezervy EU pro kybernetickou bezpečnost. VYZÝVÁ agenturu ENISA, aby okamžitě po vstupu aktu o kybernetické solidaritě v platnost zahájila mapování potřebných služeb a jejich dostupnosti s cílem zajistit, aby byla rezerva EU pro kybernetickou bezpečnost co nejužitečnější a přizpůsobená potřebám uživatelů ve všech členských státech. VYZÝVÁ agenturu ENISA, aby poté, co bude pověřena, zapojila členské státy, zejména shromažďováním informací o požadovaných kritériích a informováním o nadcházejících nabídkových řízeních, a to již v rané fázi procesu vytváření rezervy EU pro kybernetickou bezpečnost. VYZÝVÁ agenturu ENISA, aby poté, co bude pověřena, zajistila, že proces výběru důvěryhodných poskytovatelů řízených bezpečnostních služeb bude transparentní, otevřený a spravedlivý a umožní účast poskytovatelů ze všech členských států bez ohledu na jejich velikost. Dále PŘIPOMÍNÁ, že ENISA je povinna vydat bez zbytečného odkladu pokyny k interoperabilitě pro přeshraniční střediska pro kybernetickou bezpečnost.

12. ZDŮRAZŇUJE, že **sledování trendů týkajících se nově vznikajících technologií** v rychle se vyvíjející oblasti, jako je kybernetika, má klíčový význam pro zachování a další posílení naší kybernetické pozice. UZNÁVÁ činnost, kterou ENISA vyvíjí s cílem upozornit veřejnost na rizika a možnosti technologií, jako je umělá inteligence a kvantová výpočetní technika, a usnadnit tak lepší porozumění současným výzvám. VYBÍZÍ agenturu ENISA, aby k těmto úkolům dále přispívala, aktivně se zasazovala o provádění svých doporučení a aby poskytovala poradenství a v příslušných případech spolupracovala s ECCC.

PODPORA, KTEROU ENISA POSKYTUJE ČLENSKÝM STÁTŮM S CÍLEM POSÍLIT KYBERNETICKOU ODOLNOST A OPERATIVNÍ SPOLUPRÁCI

13. ZDŮRAZŇUJE, že ENISA plní důležitou úlohu coby **sekretariát dvou sítí na úrovni EU pro kybernetickou spolupráci vedenou členskými státy – sítě CSIRT a sítě EU-CyCLONe**. ZDŮRAZŇUJE cennou účast agentury ENISA v NIS CG, zejména prostřednictvím jejího aktivního zapojení a technických příspěvků v jednotlivých oblastech činnosti. VYBÍZÍ agenturu ENISA, aby v budoucnu nadále podporovala fungování a spolupráci těchto sítí, neboť představují základní kanály pro spolupráci členských států na různých úrovních.

14. ZNOVU OPAKUJE, že je třeba posílit **společné situační povědomí** na úrovni EU, které přispívá ke kybernetické pozici EU, v souvislosti s odhalováním kybernetických bezpečnostních incidentů, jejich prevencí a reakcí na ně. V tomto ohledu ZDŮRAZŇUJE význam prognostických činností, pravidelných zpráv a posuzování hrozeb agentury ENISA, které všechny přispívají ke zlepšení situačního povědomí. VYBÍZÍ agenturu ENISA, aby v úzké spolupráci s členskými státy přispívala k rozvoji situačního povědomí na úrovni EU. V této souvislosti UZNÁVÁ důležitou úlohu agentury ENISA spolu s CERT-EU a Europolem při podpoře Rady prostřednictvím situačních brífinků v rámci souboru nástrojů pro diplomacii v oblasti kybernetiky, které doplňují situační povědomí na základě informací poskytovaných společnou zpravodajsko-analytickou složkou (SIAC), a ZDŮRAZŇUJE, že je třeba vytvořit komplexní přehled hrozeb z různých zdrojů, včetně soukromého sektoru. VYBÍZÍ v tomto ohledu k dalšímu rozvoji spolupráce agentury ENISA s ESVČ, a zejména se Zpravodajským a informačním centrem (INTCEN), při plném respektování jejich příslušných mandátů.

15. ZDŮRAZŇUJE, že situační a analytické středisko pro kybernetické hrozby při Komisi plní interní funkci v rámci Komise a je podporováno svou spoluprací s agenturou ENISA a CERT-EU. Aby byl vytvořen maximální potenciál pro synergie a snížila se složitost v rámci kybernetického ekosystému EU, VYZÝVÁ Komisi, aby zohlednila výsledky hodnocení aktu o kybernetické bezpečnosti, jakož i diskuse o hodnocení kybernetického plánu s cílem zefektivnit úkoly situačního a analytického střediska pro kybernetické hrozby při Komisi a související úkoly agentury ENISA. VYBÍZÍ Komisi, aby zabránila zbytečnému zdvojování úkolů a zároveň zachovala ústřední úlohu agentury ENISA, která přispívá k rozvoji společného situačního povědomí na úrovni Unie na podporu členských států, s náležitým ohledem na jejich vnitrostátní pravomoci.

16. ZDŮRAZŇUJE, že rozvoj společného situačního povědomí je předpokladem pro včasné a účinné řešení krizí v Unii jako celku. VYZDVIHUJE skutečnost, že na úrovni EU je do **reakce na rozsáhlé kybernetické bezpečnostní incidenty** zapojena řada klíčových aktérů a že v případě takových incidentů se účinná spolupráce mezi členskými státy opírá především o síť CSIRT a EU-CyCLONe. ENISA hraje při řešení kybernetických krizí významnou úlohu jako sekretariát sítě CSIRT a EU-CyCLONe. VYZÝVÁ Komisi, aby využila hodnocení kybernetického plánu k řádnému zohlednění dodatečných úkolů a povinností, pokud jde o přispívání k rozvoji koordinované reakce na rozsáhlé přeshraniční kybernetické incidenty nebo krize, jakož i úlohy, která byla svěřena agentuře ENISA coby sekretariátu sítě CSIRT a EU-CyCLONe a nedávnými právními předpisy v oblasti kybernetické bezpečnosti.

17. ZDŮRAZŇUJE, že je důležité pořádat pravidelná **cvičení v oblasti kybernetické bezpečnosti**, která výrazně zvýší připravenost EU při reakci na incidenty a krize. UZNÁVÁ, že ENISA v této oblasti shromáždila cenné a rozsáhlé zkušenosti na podporu členských států. UZNÁVÁ důležitou úlohu agentury ENISA ve fázi plánování, přípravy, provádění a hodnocení cvičení v oblasti kybernetické bezpečnosti a ZDŮRAZŇUJE, že by měla i nadále zůstat jedním z ústředních aktérů na úrovni EU, přičemž je třeba mít na paměti, že tato cvičení by měla být prováděna na základě strukturovaných rámců a společné terminologie. VYZÝVÁ agenturu ENISA, síť CSIRT a EU-CyCLONe, aby co nejúčinněji využívaly stávající pravidelná cvičení k testování a zlepšení rámce EU pro reakci na krize a zajistily maximální využití získaných poznatků.

SPOLUPRÁCE AGENTURY ENISA S DALŠÍMI AKTÉRY V KYBERNETICKÉM EKOSYSTÉMU

18. ZNOVU OPAKUJE, že vzhledem k horizontální povaze kybernetické bezpečnosti má **spolupráce mezi všemi aktéry na úrovni členských států a Unie** zásadní význam, a proto ZDŮRAZŇUJE, že zvýšení celkové kybernetické odolnosti na evropské úrovni rovněž vyžaduje spolupráci mezi agenturou ENISA a dalšími příslušnými subjekty v kybernetické oblasti.

19. ZDŮRAZŇUJE, že schopnost orgánů, institucí a jiných subjektů EU zachovat kybernetickou bezpečnost je důležitá pro celkovou kybernetickou odolnost na úrovni EU, v níž hraje neocenitelnou úlohu CERT-EU. V tomto ohledu VÍTÁ zavedenou strukturovanou spolupráci mezi CERT-EU a agenturou ENISA a VYBÍZÍ je, aby v budoucnu pokračovaly v úzké spolupráci.

20. Díky dosažené finanční autonomii bude ECCC v souladu se svým mandátem významně přispívat k rozvoji silného evropského ekosystému pro výzkum, průmysl a technologie v oblasti kybernetické bezpečnosti, který bude zahrnovat dovednosti pro rozvoj pracovních sil. VYBÍZÍ agenturu ENISA a ECCC, aby pokračovaly v úzké spolupráci, zejména pokud jde o potřeby a priority v oblasti výzkumu a inovací, jakož i kybernetické dovednosti, s cílem zvýšit konkurenceschopnost odvětví kybernetické bezpečnosti Unie. VYZÝVÁ Komisi, aby prozkoumala, jak lze dále optimalizovat synergie v činnosti agentury ENISA a ECCC a jak lépe zefektivnit činnosti v souladu s jejich příslušnými mandáty.

21. ZDŮRAZŇUJE, že pravidelné poskytování aktuálních informací o prostředí hrozeb přispívá k lepšímu určení toho, která opatření a nástroje jsou pro účinný boj proti kyberkriminalitě zapotřebí. VYZDVIHUJE přidanou hodnotu zpráv o společném posouzení kybernetické bezpečnosti (J-CAR) na úrovni EU, které jsou výsledkem vzájemné spolupráce mezi agenturou ENISA, centra EC3 při Europolu a CERT-EU a které již poskytly cenné informace při řešení různých výzev, včetně boje proti kyberkriminalitě. VYZÝVÁ agenturu ENISA a Europol, aby v budoucnu pokračovaly ve strukturované spolupráci.

22. ZDŮRAZŇUJE, že kybernetická obrana představuje důležitou a neustále se rozvíjející část boje proti hrozbám plynoucím z kyberprostoru. POUKAZUJE na to, že je třeba, aby ENISA spolupracovala s ESVČ a Komisí v případech, kdy plní svou úlohu při podpoře provádění politiky EU v oblasti kybernetické obrany, a to v úzké spolupráci s EDA, ECCC a komunitou zabývající se kybernetickou obranou. ZDŮRAZŇUJE úlohu agentury ENISA jako civilní agentury. ZDŮRAZŇUJE, že je důležité v rámci EU prohloubit a zefektivnit civilně-vojenskou spolupráci v oblasti kybernetiky, včetně jasného rozdělení úloh a odpovědností mezi oběma komunitami a mezi EU a NATO při plném dodržování zásad inkluzivnosti, reciprocity, vzájemné otevřenosti a transparentnosti, jakož i rozhodovací samostatnosti obou organizací. VYBÍZÍ agenturu ENISA, aby pokračovala v pracovním ujednání s Komunikační a informační agenturou NATO.

23. VYBÍZÍ EU, aby nadále prosazovala naše společné hodnoty a společné úsilí v rámci globálních fór s cílem zajistit svobodný, globální, otevřený a bezpečný kyberprostor. ZDŮRAZŇUJE, že přeshraniční povaha kybernetických hrozeb a incidentů vyžaduje silnou a účinnou spolupráci nejen na úrovni EU, ale také s **mezinárodními organizacemi a partnery**. KONSTATUJE, že mezinárodní angažovanost agentury ENISA by se měla zaměřit na strategické partnery a kandidátské země EU v souladu se společnou zahraniční a bezpečnostní politikou EU. ZDŮRAZŇUJE, že v rámci své mezinárodní angažovanosti by měla ENISA jednat v souladu se svým mandátem a příslušnými ustanoveními aktu o kybernetické bezpečnosti. UZNÁVÁ, že je nezbytné v souladu s příslušnými postupy vyjasnit mezinárodní angažovanost agentury ENISA, a zejména zajistit, aby její správní rada byla řádně a včas informována o souvisejících činnostech. VYBÍZÍ agenturu ENISA, aby se zapojila do příslušných mezinárodních rámců pro spolupráci v oblasti kybernetické bezpečnosti, včetně organizací, jako jsou NATO a OBSE.

24. OPAKUJE, že EU a její členské státy často poukazovaly na nedostatky v **dovednostech v oblasti kybernetické bezpečnosti**. PŘIPOMÍNÁ, že Komise a ENISA zavedly široký zastřešující rámec pro poskytování pokynů všem zúčastněným stranám, jako je evropský rámec dovedností v oblasti kybernetické bezpečnosti, sdělení o Akademii dovedností v oblasti kybernetické bezpečnosti a každoročně organizovaná evropská konference o kybernetických dovednostech, a VYBÍZÍ Komisi a agenturu ENISA, aby na tyto iniciativy navázaly se zvláštním ohledem na probíhající diskusi o konsorciu evropské digitální infrastruktury (EDIC). Za tímto účelem VYZÝVÁ Komisi, aby spolupracovala s členskými státy, které mají zájem o zřízení tohoto konsorcia. UZNÁVÁ, že ENISA i ECCC jsou pověřeny podporou dovedností v celé Unii. VYZÝVÁ agenturu ENISA, aby se přednostně zaměřila na podporu úsilí členských států v oblasti dovedností a vzdělávání, posilování povědomí veřejnosti a ve vhodných případech na spolupráci s centrem ECCC.

25. OCEŇUJE, že ENISA v posledních letech navázala **spolupráci se soukromým sektorem**. PŘIPOMÍNÁ, že vzhledem k tomu, že soukromý sektor neustále monitoruje prostředí kybernetických hrozeb, mohly by informace shromážděné tímto odvětvím přispět ke zlepšení společného situačního povědomí. VYZÝVÁ proto agenturu ENISA, aby v úzké spolupráci s členskými státy a se všemi subjekty EU posílila spolupráci se soukromým sektorem.

26. VYZÝVÁ Komisi a agenturu ENISA, aby zvážily způsoby, jak posílit spolupráci mezi agenturou ENISA a evropskými **normalizačními** orgány. ZDŮRAZŇUJE, že by ENISA měla zvýšit své odborné znalosti týkající se evropské normalizace v oblasti kybernetické bezpečnosti mimo jiné tím, že bude sledovat normalizační činnost a podílet se na ní.

27. NALÉHAVĚ VYZÝVÁ Komisi a agenturu ENISA, aby prozkoumaly, jak dále optimalizovat fungování rámce EU pro kybernetickou bezpečnost, a zohlednily přitom doporučení a návrhy obsažené v těchto závěrech. Klíčovými prvky pro řešení současných i budoucích výzev budou trvalá spolupráce, stanovení priorit v rámci úkolů a zdrojů, jakož i zjednodušení složitého kybernetického prostředí.