POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY

PARLAMENTNÍ INSTITUT

DOKUMENTY EU

Kybernetická bezpečnost pro EU

Informační podklad ke společnému sdělení Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU a k návrhu nařízení o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií

Obsah:

Podklad k dokumentům Rady č. 12183/17 a 12211/17
leden 2018
zpracoval: Martin Kuta

AKTUÁLNÍ VYDÁNÍ:

Název: Kybernetická bezpečnost pro EU
Zpracoval: Kuta, M.
Číslo: Podklad k dokumentům č. 12183/17 a 12211/17
Datum: leden 2018

Klíčová slova:
Kybernetický; bezpečnost; obrana; SBOP; sdělení; certifikace; ENISA

ŘADA: DOKUMENTY EU

Typ řady: interní
První vydání řady: říjen 2004
Frekvence vydání řady: nepravidelná
Zaměření: Informační podklady k dokumentům EU projednávaným VEZ
Jazyk: CZ
Vydavatel: Kancelář Poslanecké sněmovny, Sněmovní 4, 118 26 Praha 1

PARLAMENTNÍ INSTITUT plní úkoly vědeckého, informačního a vzdělávacího střediska pro Poslaneckou sněmovnu, její orgány, poslance a Kancelář Poslanecké sněmovny, pro Senát, jeho orgány, senátory a Kancelář Senátu. Naše činnosti a produkty uvádíme níže.

Oddělení všeobecných studií	**STUDIE** Srovnávací studie Analytické studie	**ODPOVĚDI NA DOTAZ** Stručné odpovědi na dotazy členů Parlamentu	**VYBRANÁ TÉMATA** Studie zpracované k aktuálním problematikám	**MONITORING** Vybrané hospodářské měnové a sociální ukazatele	**MIGRACE** Přehled aktualit v oblasti migrace za vybrané období
	PŘEHLED SZBP Společná zahraniční a bezpečnostní politika EU	**EUROZÓNA+** Přehled ekonomických událostí v EU	**PODKLADY** pro zahraničně politická jednání	**PŘEDNÁŠKY** pro zahraniční delegace, PS, Senát	
Oddělení pro evropské záležitosti	**STANOVISKA** kompatibility nevládních návrhů zákonů s právem EU	**KONZULTACE** k předkládaným vládním návrhům zákonů	**DOKUMENTY EU** Výběr z aktů a dokumentů EU zaslaných PS	**ZPRÁVY** Aktuální agenda v Bruselu	**PODKLADY** pro jednání výboru na mezinárodní úrovni
Oddělení komunikace a vzdělávání	**INFORMAČNÍ STŘEDISKO** Informace o činnosti Poslanecké sněmovny a prohlídky budov	**ECPRD** Spolupráce s Evropským centrem pro parlamentní výzkum a dokumentaci	**PŘEDNÁŠKY** pro Poslaneckou sněmovnu, pro školy, veřejnost	**INFORMAČNÍ MATERIÁLY** o fungování Poslanecké sněmovny, o legislativním procesu	**ZÁPISY** ze schůzí, seminářů, přednášek, kulatých stolů

SPOLEČNÉ SDĚLENÍ

Společné sdělení Evropskému parlamentu a Radě - Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU
JOIN(2017) 450 v konečném znění, kód Rady 12211/17

NÁVRH NAŘÍZENÍ

Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)
KOM(2017) 477 v konečném znění, kód Rady 12183/17
Interinstitucionální spis 2017/0225/COD

- Právní základ:
  Článek 114 Smlouvy o fungování Evropské unie.

- Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:
  26. 9. 2017 (JOIN(2017) 450)
  11. 10. 2017 (KOM(2017) 477)

- Procedura:
  Řádný legislativní postup.

- Předběžné stanovisko vlády (dle § 109a odst. 1 jednacího řádu PS):
  Datované dnem 10. října 2017 (KOM(2017) 477) a 24. října 2017 (JOIN(2017) 450), doručené do výboru pro evropské záležitosti dne 16. ledna 2018 prostřednictvím systému ISAP.

- Hodnocení z hlediska principu subsidiarity:
  Návrh nařízení je v souladu s principem subsidiarity, neboť se rozšiřuje mandát Agentury ENISA, jejíž činnost má směřovat ke sdružování znalosti, technologické podpoře a asistenci orgánům, institucím a agenturám EU a odpovídajícím subjektům členských států.

- Odůvodnění a předmět:
  Společné sdělení Evropskému parlamentu a Radě - Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

  Společné sdělení JOIN(2017) 450 Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU vychází z předpokladu, že civilní infrastruktura a vojenské kapacity se v současnosti opírají o bezpečné digitální systémy. Na základě strategických dokumentů a závěrů institucí EU (závěry Evropské rady z června 2017 a Globální strategie EU pro společnou zahraniční a bezpečnostní politiku z června 2016)[1] sdělení předložila Evropská komise (EK) ve spolupráci s vysokou představitelkou Unie pro zahraniční věci a bezpečnostní politikou (potažmo Evropskou

[1] Viz Přehled SZBP EU 6/2017, s. 18–19. ISSN 2533-4263. Dostupné z: http://www.psp.cz/sqw/text/orig2.sqw?idd=117671.
K EUGS viz Přehled SZBP EU 6/2016, s. 11–12. ISSN 2533-4263. Dostupné z: http://www.psp.cz/sqw/text/orig2.sqw?idd=93678.

službou vnější činnosti, ESVČ). Dle studií roste počet kybernetických útoků a kybernetické trestné činnosti a jejich výskyt se má v budoucnu ještě zvýšit. Vedle zranitelnosti civilní infrastruktury jsou dalšími klíčovými motivy též proměna vedení války a užití kybernetických nástrojů k realizaci hybridních hrozeb (vedení informační války, ovlivňování veřejného mínění, atd.). Zvyšování kybernetické bezpečnosti EU souvisí rovněž s digitální ekonomikou a jednotným digitálním trhem.

Povaha hrozby (kybernetická ne-bezpečnost) i nadále spadá do plné působnosti členských států, které jsou zodpovědné za zajištění své národní bezpečnosti. EK a vysoká představitelka ale upozorňují na přeshraniční charakter hrozby, a proto navrhují vlastní soubor opatření, která členským státům poskytnou pobídky a podporu pro rozvoj a údržbu vnitrostátních schopností a kapacit, které povedou k vyšší odolnosti států i Unie jako celku, a také opatření posilující odolnost na úrovni agentur, institucí a orgánů EU.

Návrh tzv. aktu o kybernetické bezpečnosti

V roce 2013 představila EK strategii kybernetické bezpečnosti EU, na jejímž základě vznikla Agentura EU pro bezpečnost sítí a informací (ENISA) a směrnice o bezpečnosti sítí a informačních systémů.[2] Směrnice o bezpečnosti sítí a informací zavedla bezpečnostní požadavky formou právních povinností pro klíčové subjekty (ekonomické subjekty, provozovatelé služeb, dodavatelé služeb). Z důvodu zvyšování důvěry a bezpečnosti jednotného digitálního trhu se navrhuje také certifikace bezpečnosti produktů a služeb na jednotném digitálním trhu. Dále je rovněž nutné překonat rozdílnou certifikaci služeb a produktů napříč jednotlivými členskými státy.

Dřívější nařízení o agentuře ENISA stanovuje, že je zodpovědná za udržení vysoké odbornosti, poskytuje asistenci orgánům, institucím a subjektům Unie a členských států při zajišťování opatření v souvislosti s bezpečností sítí a informací. Nově se v souvislosti se záměrem zřízení evropského rámce certifikace produktů a služeb navrhuje, aby řízení a odborné poradenství nad ním převzala agentura ENISA. Kvůli prioritě kybernetické bezpečnosti v systému unijního ekosystému se rovněž navrhuje změna mandátu a organizační struktury agentury ENISA.

- Obsah a dopad:

Společné sdělení Evropskému parlamentu a Radě - Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

Sdělení se věnuje třem oblastem, které jsou dle navrhovatelů klíčové pro posílení kybernetické bezpečnosti a umožnění pokročení k digitální ekonomice.

První oblastí je budování odolnosti EU vůči kybernetickým útokům (kapitola 2 předloženého sdělení). Tato kapitola se věnuje opatřením, kterými by měla být posílena odolnost institucí členských států a členských států samotných, dále potom agentur, institucí a orgánů EU. Kybernetická bezpečnost by měla být pojata jako celospolečenská výzva, na kterou musejí reagovat vláda, ekonomika i společnost. EK a vysoká představitelka proto navrhují opatření, která se dotýkají vládních a unijních agentur (podpora agentur, standardů, reakce na kybernetické hrozby, zvyšování kapacit a dovedností), ekonomiky (jednotný trh kybernetické bezpečnosti) a společnosti (zvyšování povědomí a informovanosti o kybernetických hrozbách). V této souvislosti se EU zaměří také na budování společných webových portálů, které budou upozorňovat na škodlivý a nebezpečný software, dále potom na dezinformační kampaně a falešné zprávy. EU bude dále také klást důraz na výzkum a vzdělávání. V průběhu roku 2018 by mělo být vytvořeno

[2] Nařízení (EU) č. 526/2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004.
Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Evropské výzkumné a odborné středisko pro kybernetickou bezpečnost s cílem posílit rozvoj a zavádění technologií v oblasti kybernetické bezpečnosti pro agentury na unijní úrovni i úrovni jednotlivých členských států. Výzkumné středisko by se mělo zaměřit na šifrování v produktech a službách a využít přínosů dalších agentur s podobným zaměřením (například agentura ENISA). S výzkumem souvisí také fakt, že výzkum a vývoj kybernetických nástrojů posiluje celkovou obranyschopnost jednotlivých států a Unie jako celku, a proto výzkumné aktivity by mohly být financovány ze zdrojů Evropského obranného fondu.

Druhá oblast sdělení se věnuje **budování účinného kybernetického odrazování** ze strany agentur EU (kapitola 3). Prostřednictvím budování silné reakce a transparentního prostředí a zjednodušení dopadení případných pachatelů kybernetické bezpečnosti bude EU usilovat o odrazení případných útoků. Trestněprávní definice kybernetických útoků byla v minulosti stanovena směrnicí o útocích na informační systémy (směrnice EP a Rady 2013/40/40 ze dne 12. srpna 2013 o útocích na informační systémy[3]) s cílem zjednodušit přeshraniční spolupráci orgánů činných v trestním řízení při jejich vyšetřování. Klíčovými opatřeními v této kapitole jsou identifikace původců (pachatelů) kybernetické bezpečnosti, která si vyžádá deanonymizaci přístupu k internetu a síťovým službám (s tím související zavádění nového protokolu IPv6), dále posílení reakce donucovacích orgánů a jejich spolupráce napříč Unií (například přístup k elektronickým důkazům). Agentury Europol a Eurojust mají přispívat ke zlepšení a zintenzivnění spolupráce, koordinaci činnosti, chápání kybernetické hrozby a přístupu k ní napříč unií. EK rovněž navrhuje financování boje proti kyberkriminalitě ze zdrojů Fondu pro vnitřní bezpečnost. EU by měla rovněž vyvinout jasný politický tlak na vnější původce kybernetických útoků prostřednictvím již dříve přijatých nástrojů diplomatické reakce.[4] Kvůli zahrnující povaze kybernetické hrozby se navrhuje posílit spolupráci veřejného a soukromého sektoru.

EU rovněž bude usilovat o **posilování mezinárodní spolupráce v oblasti kybernetické bezpečnosti**. Součástí této snahy je spolupráce s partnerskými a třetími zeměmi. EU bude dále podporovat rozvoj dialogu o kybernetické bezpečnosti. V kyberprostoru dle EU platí mezinárodní právo (Charta OSN); EU podporuje normy, pravidla a zásady odpovědného chování států formulovaných OSN. I na globální úrovni EU podporuje budování kapacit v oblasti kybernetické bezpečnosti. Stěžejní zůstává spolupráce EU a NATO v oblasti kybernetické bezpečnosti včetně spolupráce ve výzkumu a inovacích, cvičení a posilování připravenosti a budování vnitřní kapacity čelit kybernetickým hrozbám.

Návrh tzv. aktu o kybernetické bezpečnosti

Je navrhována **změna mandátu Agentury ENISA**, která byla identifikována jako systémově logická instituce pro dosažení cílů v nařízení i ostatních strategických materiálech Unie. Agentura plní úkoly pro zajištění vysoké úrovně kybernetické bezpečnosti (odborné středisko pro kybernetickou bezpečnost, asistenční instituce jiným subjektům Unie a členských států, asistenční instituce při budování a připravenosti kapacit kybernetické bezpečnosti, jejich zvyšování, koordinátor spolupráce mezi unií a členskými státy, garant certifikace služeb a produktů jednotného digitálního trhu). Nově jsou stanoveny následující úkoly agentury ENISA:

- Tvorba a provádění politik a práva EU: poskytování poradenství při tvorbě politik a asistence při jejich provádění, provádění pravidelného přezkumu v dané oblasti politik EU v případě narušení bezpečnosti či ztrátě integrity subjektů, které splňovaly požadavky existujícího rámce;

[3] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32013L0040.

[4] K přijetí rámce nástrojů diplomatické reakce viz Přehled SZBP EU 6/2017, s. 17. ISSN 2533-4263. Dostupné z: http://www.psp.cz/sqw/text/orig2.sqw?idd=117671.

- Budování kapacit: asistence a podpora členským států a dalším subjektům EU při zdokonalování, prevenci, odhalování a analýze kyber-bezpečnostních problémů a incidentů (podpora skupinám pro prevenci a řešení kybernetických hrozeb – CERT), podpora při řešení kybernetických incidentů, podpora členským státům při budování národních strategií, zvyšování úrovně a školení;
- Operativní spolupráce na úrovni EU: asistence a podpora při operativní spolupráci mezi orgány a agenturami na úrovni EU i členských států (výměna zkušeností, poskytování vzájemného poradenství, konzultace při zavádění praktických opatření, pořádání cvičení), vypracování pravidelné technické zprávy o situaci v oblasti kybernetické bezpečnosti EU; agentura též bude fungovat jako sekretariát sítě CSIRT (národních skupin pro řešení kybernetických incidentů);
- Certifikace, normalizace služeb a produktů souvisejících s jednotným digitálním trhem EU: vypracování návrhů společné certifikace, zajištění funkčnosti evropské skupiny pro certifikaci, provádění dozoru nad certifikací, analytická činnost trendů na trhu kybernetické bezpečnosti;
- Znalosti, informace, zvyšování informovanosti: analytická činnost nových technologií, dlouhodobé analýzy kyber-bezpečnostních hrozeb, poradenství o pokynech a osvědčených postupech týkajících se bezpečnosti sítí a informačních systémů, bezpečnosti internetové infrastruktury, zajištění informovanosti o kybernetické bezpečnosti, analýza incidentů, pořádání informačních kampaní za zvýšení kybernetické bezpečnosti;
- Výzkum a vývoj: asistence při prioritizování výzkumných potřeb, asistence při inicializačních fázích výzkumných a vývojových programů;
- Mezinárodní spolupráce se třetími zeměmi (a odpovídajícími agenturami), pozorovatelský status při konání nadnárodních cvičení, výměna informací a osvědčených postupů se třetími stranami po souhlasu EK.

Nařízení dále upravuje strukturu agentury (správní rada, výkonná rada, výkonný ředitel, stálá skupina zúčastněných stran), úpravu činnosti dle jednotného programového dokumentu, jeho vypracování a projednání na úrovni orgánů agentury a orgánů EU a další principy práce agentury (důvěrnost, transparentnost, přístup k dokumentům). Na činnosti agentury se finančně podílejí EU (z rozpočtu EU) a členské státy a třetí strany formou příspěvků.

Nařízením se dále zavádí rámec pro certifikaci kybernetické bezpečnosti. Za vypracování a přijetí evropského systému certifikace kybernetické bezpečnosti je odpovědná agentura ENISA na základě žádosti EK. Certifikace produktů a služeb směřuje k ochraně údajů, předcházení nedovolenému nakládání s nimi, jejich zpracování a přístupu k nim, zajištění deanonymizace přístupu k údajům a nakládání s nimi, zajištění ochrany před jejich zničením, obnovení přístupu k nim po incidentech. Navrhují se tři úrovně záruky (základní, významná a vysoká) dle důvěry v deklarované či uváděné kybernetickobezpečnostní kvality produktu či služeb. Certifikace produktů a služeb probíhá na základě splnění požadavků. Certifikace je až na výjimky, které jsou stanoveny právem EU, dobrovolná.

Agentura ENISA vypracuje společný evropský certifikační rámec; certifikaci jednotlivých produktů a služeb provádějí na úrovni členských států subjekty posuzování shody, které jsou akreditovány vnitrostátními dozorovými orgány. Tyto dozorové vnitrostátní orgány jsou určeny členskými státy a o jejich pověření je informována EK. Pro tyto vnitrostátní orgány dozoru vznikají tímto nařízením nové oblasti činnosti (dohled a právní vymáhání plnění požadavků evropského certifikačního rámce, řešení stížností v souvislosti s certifikací, dohled nad subjekty posuzování shody, dozor nad certifikací podle evropského certifikačního rámce na vnitrostátní úrovni).

Členské státy nesmějí zavádět nové certifikace pro ty služby a produkty, které již byly certifikovány podle evropského certifikačního rámce.

Odpovídající vnitrostátní instituce se sdružují v nově zřízené Evropské skupině pro certifikaci kybernetické bezpečnosti; ta zajišťuje vyšší míru spolupráce a komunikace mezi vnitrostátními institucemi a institucemi na evropské úrovni (Evropskou komisí a agenturou ENISA).

Dopad na státní rozpočet a právní řád ČR:

Společné sdělení Evropskému parlamentu a Radě - Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

Jedná se o nelegislativní dokument bez přímého dopadu na právní řád a státní rozpočet ČR.

Návrh tzv. aktu o kybernetické bezpečnosti

Jedná se o nařízení s dopadem na zákon o kybernetické bezpečnosti v případě, že se Národní úřad pro kybernetickou a informační bezpečnost stane dozorovým orgánem dle části nařízení o certifikačním rámci.

Rovněž má nařízení dopad na rozpočet ČR; především plnění dozorového orgánu (instituce) vykonávajícího dohled, vymáhání a dozor nad certifikací a udělování certifikace podle evropského certifikačního rámce.

- Stanovisko vlády ČR:
  Společné sdělení Evropskému parlamentu a Radě - Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

  Rámcovou pozici pro Parlament České republiky k uvedenému sdělení vypracoval Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Vláda ČR předložený materiál vítá a oceňuje a považuje za důležitou problematiku. V obecné rovině se vláda ztotožňuje s předpokladem, že za bezpečnost odpovídají členské státy. Význam sdělení spočívá v případném uvedení zvažovaných opatření do praxe a následném posílení kybernetické bezpečnosti členských států i Unie jako celku. Vláda rovněž dále podporuje stanovisko předkladatelů sdělení o aplikaci mezinárodního práva v kyberprostoru. ČR dále podporuje iniciativu na nejvyšší nadnárodní úrovni na vytvoření platformy zahrnující světové hráče kybernetické bezpečnosti. EU a ČR by tím mohly získat navázání dialogu o kyberprostoru mezi Unií a třetími státy, jehož prostřednictvím by měly být zdůrazňovány zásady náležité péče a odpovědnosti států za dění v kybernetickém prostoru.

  Obecně vláda materiál oceňuje a zaujímá kladné stanovisko. Ke konkrétním bodům vláda zaujala dílčí, veskrze kladné postoje. Vláda upozorňuje na výklad některých pojmů, jimž by měla být v době zavádění konkrétních opatření věnována náležitá pozornost. V případě odhalování kybernetických útoků je vláda toho názoru, že by byla vhodnější podpora, asistence a koordinace ze strany unijních institucí (Europol, Eorujust) namísto normativního sjednocování postupů (v této otázce je ale třeba upozornit na předběžný charakter sdělení, nejedná se o návrh). Vláda ale obecně zastává názor, že jakákoli spolupráce musí mít povahu mezistátní, nikoli nadnárodní (přístup k datům), ačkoli s rozšířením cloudových služeb se dá očekávat nárůst nutnosti přeshraniční spolupráce odpovědných institucí.

  V souvislosti s vojenským rozměrem kybernetické bezpečnosti ČR podporuje činnost spadající do společné bezpečnostní a obranné politiky (SBOP), spolupráci mezi vojenským a civilním výzkumným odvětvím, spolupráci mezi EU a NATO (s tím souvisí harmonizace přístupu k utajovaným informacím).

Návrh tzv. aktu o kybernetické bezpečnosti

Vláda ČR vítá posílení mandátu agentury ENISA, ale odmítla spojení této problematiky s vytvořením certifikačního rámce; preferuje oddělení předpisů.

Vláda oceňuje změny mandátu agentury ENISA s důrazem na oblast vzdělávání a pro potřeby členských států (vláda odmítá činnost agentury na komerční bázi).

K tématu certifikace vláda uvádí, že se jedná o v českém prostředí novou činnost, která je v současnosti řešena standardizací. Certifikace není pojímána jako nežádoucí. Vláda ale upozorňuje, že certifikační rámec podléhá souhlasu EK, a je toho názoru, že by byla žádoucí větší míra zapojení členských států (schválení prostřednictvím Rady, případně COREPER). Certifikační rámec by měl být dále dopracován, aby byly odstraněny nedostatky související s neharmonizovaným způsobem akreditace subjektů posuzování shody.

Vláda je toho názoru, že členské státy by měly mít možnost vyjmout certifikaci služeb a produktů podle evropského rámce v případě zajišťování obrany a bezpečnosti států, zpracovávání utajovaných informací a národní bezpečnosti a veřejných zakázek s tím spojených.

Kvůli naznačeným problémům v rámcové pozici není část o certifikaci (a tedy celé nařízení) podporováno.

Oběma dokumenty se zabýval Senát Parlamentu ČR. Na schůzi dne 22. 11. 2017 výbor pro záležitosti EU doporučil plénu Senátu dokument projednat.[5] Plénum Senátu se dokumentem zabývalo na zasedání dne 6. 12. 2017 a přijalo usnesení dle návrhu výboru.[6]

- Předpokládaný harmonogram projednávání v orgánech EU:
  V Radě se návrhem nařízení zabývá Horizontální pracovní skupina pro kybernetické otázky (HWPCI), poslední jednání v jejím rámci proběhlo 9. ledna 2018.

  V Evropském parlamentu byl návrh nařízení přidělen výboru pro průmysl, výzkum a energetiku (ITRE), kde byla jako zpravodajka určena Angelika Niebler. Mezi stínovými zpravodaji figurují rovněž Evžen Tošenovský a Pavel Telička. O konzultaci byl požádán výbor pro zahraniční věci (AFET), výbor pro rozpočet (BUDG), výbor pro vnitřní trh a ochranu spotřebitelů (IMCO) a výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE). Hlasování o návrhu ve výboru je plánováno na 19. června 2018.

  Další harmonogram projednávání prozatím není znám.

- Projednávání ve výboru pro evropské záležitosti PS PČR:
  Výbor pro evropské záležitosti PS PČR projednal dokument dne 31. 1. 2018 a usnesením č. 22 přijal tyto závěry:

  Výbor pro evropské záležitosti

  1. **souhlasí** s navrženou strategií posilování kybernetické odolnosti, schopnosti odrazování a mezinárodní spolupráce v otázkách kybernetické bezpečnosti;

  2. **vítá** důraz na vzdělání a osvětu v oblasti kybernetické bezpečnosti;

[5] Usnesení 138 ze 16. schůze výboru pro záležitosti EU dne 22. 11. 2017. Dostupné z: http://www.senat.cz/xqw/xervlet/pssenat/htmlhled?action=doc&value=86109.
[6] Usnesení Senátu č. 311 z 11. schůze dne 6. 12. 2017. Dostupné z: http://www.senat.cz/xqw/xervlet/pssenat/original/86251/72321.

3. **podporuje** předloženou změnu fungování agentury ENISA a prodloužení jejího mandátu na dobu neurčitou;

4. **souhlasí** s vytvořením společného rámce pro certifikaci kybernetické bezpečnosti za předpokladu, že bude zajištěna flexibilita a adaptabilita certifikačních schémat s ohledem na vývoj nových technologií;

5. vzhledem ke skutečnosti, že kybernetickou obranu a bezpečnost nelze oddělit, **podporuje** myšlenku financování kybernetické obrany z Evropského obranného fondu a začlenění kybernetické obrany do rámce stálé strukturované spolupráce (PESCO).

6. **pověřuje** předsedu výboru pro evropské záležitosti, aby v rámci politického dialogu postoupil toto usnesení předsedovi Evropské komise.