Evropský parlament
2019-2024

Výbor pro ústavní záležitosti

2022/0085(COD)

31.1.2023

STANOVISKO

Výboru pro ústavní záležitosti

pro Výbor pro průmysl, výzkum a energetiku

k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Zpravodajka: Markéta Gregorová

PA_Legam

STRUČNÉ ODŮVODNĚNÍ

Orgány, instituce a jiné subjekty Evropské unie v posledních letech působí ve stále více digitalizovaném prostředí, pro které je charakteristický neustálý technologický vývoj a z něj vyplývající rostoucí míra ohrožení kybernetické bezpečnosti. Tato situace se ještě zhoršila po vypuknutí pandemie COVID-19 a s ní souvisejícím rozšíření práce na dálku, neboť během této doby rostl počet sofistikovaných útoků z celé řady zdrojů.

Prostředí kybernetické bezpečnosti, které zahrnuje správu, kybernetickou hygienu, celkovou schopnost a vyspělost, se v současné době v jednotlivých orgánech, institucích a jiných subjektech Unie značně liší, což vytváří další překážku otevřené, efektivní a nezávislé evropské správy.

Zpravodajka tudíž souhlasí s tím, že je nezbytný stejný základní přístup všech orgánů, institucí a jiných subjektů Unie k zavedení společných systémů a požadavků na kybernetickou bezpečnost a zajištění toho, aby se kybernetická bezpečnost vyvíjela stejným směrem, a tak přispěla k efektivitě a nezávislosti evropské správy.

Zpravodajka se dále domnívá, že pro ochranu všech zaměstnanců, dat, komunikačních sítí, informačních systémů a rozhodovacích procesů EU je zásadně důležitý robustní a jednotný bezpečnostní rámec, který také přispívá k demokratickému fungování Evropské unie. Posílená bezpečnostní kultura orgánů, institucí a jiných subjektů Unie by také připravila Evropu na digitální éru a vybudovala ekonomiku, která obstojí i v budoucnosti a slouží lidem.

POZMĚŇOVACÍ NÁVRHY

Výbor pro ústavní záležitosti vyzývá Výbor pro průmysl, výzkum a energetiku jako příslušný výbor, aby zohlednil tyto pozměňovací návrhy:

Pozměňovací návrh 1

Návrh nařízení
Bod odůvodnění 1

Znění navržené Komisí	*Pozměňovací návrh*
(1) V digitálním věku tvoří informační a komunikační technologie základ otevřené, efektivní a nezávislé unijní správy. Vyvíjející se technologie a větší složitost a vzájemná propojenost digitálních systémů zesilují kybernetická bezpečnostní rizika, což činí unijní správu zranitelnější vůči kybernetickým hrozbám a incidentům, které v konečném důsledku ohrožují kontinuitu činností správy a	(1) V digitálním věku tvoří informační a komunikační technologie základ otevřené, efektivní a nezávislé unijní správy. Vyvíjející se technologie a větší složitost a vzájemná propojenost digitálních systémů zesilují kybernetická bezpečnostní rizika, což činí unijní správu zranitelnější vůči kybernetickým hrozbám a incidentům, které v konečném důsledku ohrožují kontinuitu činností správy a

schopnost zabezpečovat její data. Širší využívání služeb cloudu, všudypřítomné používání informačních technologií, vysoká úroveň digitalizace, práce na dálku a vyvíjející se technologie a propojenost jsou nyní základními prvky všech činností správních subjektů v Unii, zatím však není dostatečně vybudována digitální odolnost.	schopnost zabezpečovat její data. Širší využívání služeb cloudu, všudypřítomné používání ***informačních a komunikačních technologií („IKT“),*** vysoká úroveň digitalizace, práce na dálku a vyvíjející se technologie a propojenost jsou nyní základními prvky všech činností správních subjektů v Unii, zatím však není dostatečně vybudována digitální odolnost.

Odůvodnění

V návrhu Komise se objevuje výraz „informační technologie“, který by však měl znít „informační a komunikační technologie“, což je standardní termín používaný ve směrnici NIS 2 a v aktu EU o kybernetické bezpečnosti.

Pozměňovací návrh 2

Návrh nařízení
Bod odůvodnění 2

Znění navržené Komisí	*Pozměňovací návrh*
(2) Prostředí kybernetických hrozeb, v němž působí orgány, instituce a jiné subjekty Unie, se neustále vyvíjí. Taktika, metody a postupy používané aktéry hrozeb se neustále vyvíjejí, avšak hlavní motivy takových útoků se nijak výrazně nemění, a to od krádeže cenných neveřejných informací přes získání finančních prostředků a manipulaci s veřejným míněním až po narušení digitální infrastruktury. Tempo, jímž provádějí své kybernetické útoky, se stále zvyšuje, přičemž jejich kampaně jsou stále sofistikovanější a automatizovanější, zaměřují se na exponované prostory k útoku, které se stále rozšiřují, a rychle využívají zranitelná místa.	(2) Prostředí kybernetických hrozeb, v němž působí orgány, instituce, úřady a jiné subjekty Unie, se neustále vyvíjí. Taktika, metody a postupy používané aktéry hrozeb se neustále vyvíjejí, avšak hlavní motivy takových útoků se nijak výrazně nemění, a to od krádeže cenných neveřejných informací přes získání finančních prostředků a manipulaci s veřejným míněním až po narušení digitální infrastruktury. Tempo, jímž provádějí své kybernetické útoky, se stále zvyšuje, přičemž jejich kampaně a metody jsou stále sofistikovanější a automatizovanější, zaměřují se na exponované prostory k útoku, které se stále rozšiřují, a rychle využívají zranitelná místa.

Pozměňovací návrh 3

Návrh nařízení
Bod odůvodnění 3

Znění navržené Komisí	*Pozměňovací návrh*
(3) V prostředí informačních technologií orgánů, institucí a jiných subjektů Unie existují vzájemné závislosti a integrované toky dat a jejich uživatelé spolu úzce spolupracují. Tato vzájemná propojenost znamená, že jakékoli narušení, a dokonce i takové narušení, které je původně omezeno na jeden orgán, instituci nebo jiný subjekt Unie, může mít širší dominové účinky, jež mohou potenciálně vést k dalekosáhlým negativním dopadům na ostatní. Prostředí informačních technologií některých orgánů, institucí nebo jiných subjektů je navíc propojeno s informačním prostředím členských států, z čehož vyplývá, že incident v rámci jednoho subjektu Unie představuje riziko pro kybernetickou bezpečnost prostředí informačních technologií členských států, a naopak.	(3) V prostředí informačních a komunikačních technologií orgánů, institucí, ***úřadů*** a jiných subjektů Unie existují vzájemné závislosti a integrované toky dat a jejich uživatelé spolu úzce spolupracují. Tato vzájemná propojenost znamená, že jakékoli narušení, a dokonce i takové narušení, které je původně omezeno na jeden orgán, instituci, ***úřad*** nebo jiný subjekt Unie, může mít širší dominové účinky, jež mohou potenciálně vést k dalekosáhlým negativním dopadům na ostatní. Prostředí informačních a komunikačních technologií některých orgánů, institucí, ***úřadů*** nebo jiných subjektů je navíc propojeno s informačním a komunikačním prostředím členských států, z čehož vyplývá, že incident v rámci jednoho subjektu Unie představuje riziko pro kybernetickou bezpečnost prostředí informačních a komunikačních technologií členských států, a naopak.

Pozměňovací návrh 4
Návrh nařízení
Bod odůvodnění 4

Znění navržené Komisí	*Pozměňovací návrh*
(4) Orgány, instituce a jiné subjekty Unie jsou atraktivní cíle, které musejí čelit vysoce kvalifikovaným a dobře finančně zajištěným aktérům hrozeb, jakož i jiným hrozbám. Přitom úroveň a vyspělost kybernetické odolnosti a schopnost odhalovat nepřátelské činnosti v kyberprostoru a reagovat na ně se u zmíněných subjektů značně liší. Pro fungování evropské správy je tak nezbytné, aby orgány, instituce a jiné subjekty Unie dosáhly vysoké společné úrovně kybernetické bezpečnosti prostřednictvím základní úrovně kybernetické bezpečnosti (soubor minimálních pravidel k zajištění kybernetické bezpečnosti, s nimiž musí být	(4) Orgány, instituce, ***úřady*** a jiné subjekty Unie jsou atraktivní cíle, které musejí čelit vysoce kvalifikovaným a dobře finančně zajištěným aktérům hrozeb, jakož i jiným hrozbám. Přitom úroveň a vyspělost kybernetické odolnosti a schopnost odhalovat nepřátelské činnosti v kyberprostoru a reagovat na ně se u zmíněných subjektů značně liší. Pro fungování evropské správy je tak nezbytné, aby orgány, instituce***, úřady*** a jiné subjekty Unie dosáhly vysoké společné úrovně kybernetické bezpečnosti prostřednictvím základní úrovně kybernetické bezpečnosti (soubor společných minimálních pravidel k zajištění kybernetické bezpečnosti,

sítě a informační systémy v souladu, aby se minimalizovala kybernetická bezpečnostní rizika), výměny informací a spolupráce.	s nimiž musí být sítě a informační systémy v souladu, aby se omezila kybernetická bezpečnostní rizika), p***ravidelné a efektivní*** výměny informací a spolupráce, ***a školení v oblasti kybernetické bezpečnosti***.

Pozměňovací návrh 5

Návrh nařízení
Bod odůvodnění 7

Znění navržené Komisí	*Pozměňovací návrh*
(7) Rozdíly mezi orgány, institucemi a jinými subjekty Unie vyžadují pružnost při provádění, protože univerzální řešení nebude vyhovovat všem. Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti by neměla obsahovat žádné povinnosti přímo zasahující do plnění úkolů orgánů, institucí nebo jiných subjektů Unie nebo narušující jejich institucionální autonomii. Tyto orgány, instituce a jiné subjekty by tak měly zavést své vlastní rámce pro řízení, správu a kontrolu kybernetických bezpečnostních rizik a přijmout své vlastní základní soubory opatření k zajištění kybernetické bezpečnosti a plány kybernetické bezpečnosti.	(7) Rozdíly mezi orgány, institucemi, ***úřady*** a jinými subjekty Unie vyžadují pružnost při provádění, protože univerzální řešení nebude vyhovovat všem. Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti by měla podporovat plnění úkolů orgánů, institucí, ***úřadů*** nebo jiných subjektů Unie a zohledňovat jejich institucionální autonomii. Tyto orgány, instituce, ***úřady*** a jiné subjekty by tak měly zavést své vlastní rámce pro řízení, správu a kontrolu kybernetických bezpečnostních rizik a přijmout své vlastní ***základní soubory opatření k zajištění kybernetické bezpečnosti a plány kybernetické bezpečnosti vycházející ze společného rámce stanoveného tímto nařízením.***

Pozměňovací návrh 6
Návrh nařízení
Bod odůvodnění 8

Znění navržené Komisí	*Pozměňovací návrh*
(8) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na orgány, instituce nebo jiné subjekty Unie nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových	(8) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na orgány, instituce***, úřady*** nebo jiné subjekty Unie nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových

opatření. Cílem každého orgánu, instituce a jiného subjektu Unie by mělo být, aby přiměřenou část svého rozpočtu na informační technologie vynaložily na zlepšení úrovně své kybernetické bezpečnosti; z dlouhodobého hlediska by měl být sledován cíl v řádu 10 %.	opatření. Cílem každého orgánu, instituce, ***úřadu*** a jiného subjektu Unie ***by mělo být,*** aby přiměřenou část svého rozpočtu ***ve střednědobém či dlouhodobém horizontu a více alespoň 10 %*** vynaložily na informační a komunikační technologie na zlepšení úrovně své kybernetické bezpečnosti;

Pozměňovací návrh 7

Návrh nařízení
Bod odůvodnění 9

Znění navržené Komisí	*Pozměňovací návrh*
(9) Vyšší společná úroveň kybernetické bezpečnosti vyžaduje, aby dohled nad kybernetickou bezpečností přešel na nejvyšší úroveň vedení každého orgánu, instituce nebo jiného subjektu Unie, které by mělo schválit základní soubor opatření k zajištění kybernetické bezpečnosti, který by měl řešit rizika zjištěná v rámci, jenž má být každým orgánem, institucí nebo jiným subjektem zaveden. Nedílnou součásti základního souboru opatření k zajištění kybernetické bezpečnosti ve všech orgánech, institucích a jiných subjektech Unie je řešení kultury kybernetické bezpečnosti, tedy každodenní praxe v oblasti kybernetické bezpečnosti.	(9) Vyšší společná úroveň kybernetické bezpečnosti vyžaduje, aby dohled nad kybernetickou bezpečností přešel na společný výbor EU s nejvyšší úrovní vedení každého orgánu, instituce, ***úřad*** nebo jiného subjektu Unie, které by mělo schválit základní soubor opatření k zajištění kybernetické bezpečnosti, který by měl řešit rizika zjištěná v rámci, jenž má být každým orgánem, institucí, ***úřadem*** nebo jiným subjektem zaveden. Nedílnou součásti základního souboru opatření k zajištění kybernetické bezpečnosti ve všech orgánech, institucích, ***úřadech*** a jiných subjektech Unie by se mělo stát řešení kultury kybernetické bezpečnosti, tedy každodenní praxe v oblasti kybernetické bezpečnosti.

Pozměňovací návrh 8

Návrh nařízení
Bod odůvodnění 10

Znění navržené Komisí	*Pozměňovací návrh*
(10) Orgány, instituce a jiné subjekty Unie by měly posuzovat rizika související se vztahy s dodavateli a poskytovateli služeb, včetně poskytovatelů služeb	(10) Orgány, instituce, ***úřady*** a jiné subjekty Unie by měly posuzovat rizika související se vztahy s dodavateli a poskytovateli služeb, včetně poskytovatelů

ukládání a zpracování dat nebo řízených bezpečnostních služeb, a přijímat vhodná opatření k řešení těchto rizik. Tato opatření by měla být součástí základního souboru opatření k zajištění kybernetické bezpečnosti a měla by být dále upřesněna v pokynech nebo doporučeních centra CERT-EU. Při stanovení opatření a pokynů by měly být náležitě zohledněny příslušné právní předpisy a politiky EU, včetně posouzení rizik a doporučení vydávaných skupinou pro spolupráci v oblasti bezpečnosti sítí a informací (skupinou NIS), jako je koordinované posouzení rizik v EU a souboru opatření EU pro kybernetickou bezpečnost sítí 5G. Mohla by být rovněž vyžadována certifikace příslušných produktů, služeb a procesů IKT, a to v rámci konkrétních evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881.

služeb ukládání a zpracování dat nebo řízených bezpečnostních služeb, a přijímat vhodná opatření k řešení těchto rizik. ***Tito dodavatelé a poskytovatelé služeb by měli být důkladně prověřeni s ohledem na celý rozsah dodavatelského řetězce a hospodářské a politické prostředí, v němž působí. Pokud vztahy s takovými dodavateli a poskytovateli služeb představují riziko pro integritu demokratických procesů v EU, měly by být bez zbytečného odkladu ukončeny.*** Tato opatření by měla být součástí základního souboru opatření k zajištění kybernetické bezpečnosti a měla by být dále upřesněna v pokynech nebo doporučeních centra CERT-EU. Při stanovení opatření a pokynů by měly být náležitě zohledněny příslušné právní předpisy a politiky EU, včetně posouzení rizik a doporučení vydávaných skupinou pro spolupráci v oblasti bezpečnosti sítí a informací (skupinou NIS), jako je koordinované posouzení rizik v EU a souboru opatření EU pro kybernetickou bezpečnost sítí 5G. Dále s ohledem na ***typy hrozeb a důležitost budování odolnosti*** by měla být rovněž vyžadována certifikace příslušných produktů, služeb a procesů IKT používaných v ***orgánech, institucích, úřadech a jiných subjektech Unie***, a to v rámci konkrétních evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881.

Pozměňovací návrh 9

Návrh nařízení
Bod odůvodnění 13

Znění navržené Komisí	*Pozměňovací návrh*
(13) Mnohé kybernetické útoky jsou součástí širších kampaní, které cílí na skupiny orgánů, institucí a jiných subjektů Unie nebo na zájmové komunity, jež	(13) Mnohé kybernetické útoky jsou součástí širších kampaní, které cílí na skupiny orgánů, institucí, ***úřadů*** a jiných subjektů Unie nebo na zájmové komunity,

orgány, instituce a jiné subjekty Unie zahrnují. S cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů by orgány, instituce a jiné subjekty Unie měly centru CERT-EU oznamovat významné kybernetické hrozby, významná zranitelná místa a významné incidenty a sdílet vhodné technické podrobnosti, jež umožňují odhalovat podobné kybernetické hrozby v rámci jiných orgánů, institucí a jiných subjektů Unie, zmírňovat dopady takových hrozeb a na tyto hrozby reagovat. Podle stejného přístupu, jaký se předpokládá ve směrnici [návrhu směrnice NIS 2], by subjekty, které se dozvědí o významném incidentu, měly mít povinnost předložit centru CERT-EU počáteční oznámení do 24 hodin. Taková výměna informací by měla centru CERT-EU umožnit šířit tyto informace do jiných orgánů, institucí nebo jiných subjektů Unie, jakož i vhodným protějškům, s cílem pomoci chránit prostředí informačních technologií Unie a prostředí informačních prostředí protějšků Unie před podobnými incidenty, hrozbami a zranitelnými místy.

jež orgány, instituce, ***úřady*** a jiné subjekty Unie zahrnují. S cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů by orgány, instituce, ***úřady*** a jiné subjekty Unie měly centru CERT-EU oznamovat významné kybernetické hrozby, významná zranitelná místa a významné incidenty a sdílet vhodné technické podrobnosti, jež umožňují odhalovat podobné kybernetické hrozby v rámci jiných orgánů, institucí, ***úřadů*** a jiných subjektů Unie, zmírňovat dopady takových hrozeb a na tyto hrozby reagovat. Podle stejného přístupu, jaký se předpokládá ve směrnici [návrhu směrnice NIS 2], by subjekty, které se dozvědí o významném incidentu, měly mít povinnost předložit centru CERT-EU ***bez zbytečného odkladu a v každém případě do 24 hodin včasné varování. Orgánům, institucím, úřadům a jiným subjektům Unie by měly být přiděleny dostatečné zdroje, aby mohly rychle a účinně plnit své oznamovací povinnosti s cílem zajistit správné fungování navrženého systému.*** Taková výměna informací by měla centru CERT-EU umožnit šířit tyto informace do jiných orgánů, institucí, ***úřadů*** nebo jiných subjektů Unie, jakož i vhodným protějškům, s cílem pomoci chránit prostředí informačních a komunikačních technologií Unie a prostředí informačních a komunikačních technologií protějšků Unie před podobnými incidenty, hrozbami a zranitelnými místy.

Pozměňovací návrh 10

Návrh nařízení
Bod odůvodnění 14

Znění navržené Komisí	*Pozměňovací návrh*
(14) Kromě uložení více úkolů centru CERT-EU a rozšíření jeho úlohy by měl být zřízen Interinstitucionální výbor pro kybernetickou bezpečnost (IICB), který by	(14) Kromě uložení více úkolů centru CERT-EU a rozšíření jeho úlohy by měl být zřízen Interinstitucionální výbor pro kybernetickou bezpečnost (IICB), který by

měl usnadňovat dosažení vysoké společné úrovně kybernetické bezpečnosti u orgánů, institucí a jiných subjektů Unie tak, že bude sledovat provádění tohoto nařízení ze strany orgánů, institucí a jiných subjektů Unie, dohlížet na plnění obecných priorit a cílů centrem CERT-EU a poskytovat centru CERT-EU strategické řízení. Výbor IICB by měl zajišťovat zastoupení orgánů a zahrnovat zástupce jiných subjektů a institucí prostřednictvím sítě agentur Unie.

měl usnadňovat dosažení vysoké společné úrovně kybernetické bezpečnosti u orgánů, institucí, ***úřadů*** a jiných subjektů Unie tak, že bude sledovat provádění tohoto nařízení ze strany orgánů, institucí, ***úřadů*** a jiných subjektů Unie, dohlížet na plnění obecných priorit a cílů centrem CERT-EU a poskytovat centru CERT-EU strategické řízení. Výbor IICB by měl zajišťovat ***rovné*** zastoupení orgánů a zahrnovat zástupce jiných subjektů, ***úřadů*** a institucí prostřednictvím sítě agentur Unie.

Pozměňovací návrh 11

Návrh nařízení
Bod odůvodnění 16

Znění navržené Komisí	*Pozměňovací návrh*
(16) Výbor IICB by měl sledovat dodržování tohoto nařízení, jakož i následná opatření přijímaná v návaznosti na pokyny a doporučení a na výzvy k přijetí opatření vydávané centrem CERT-EU. V technických záležitostech by měly výbor IICB podporovat technické poradní skupiny ve složení, jež výbor IICB považuje za vhodné, které by měly dle potřeby úzce spolupracovat s centrem CERT-EU, orgány, institucemi nebo jinými subjekty Unie a dalšími zúčastněnými stranami. V případě potřeby by měl výbor IICB vydávat nezávazná varování a doporučovat audity.	(16) Výbor IICB by měl sledovat dodržování tohoto nařízení, jakož i následná opatření přijímaná v návaznosti na pokyny a doporučení a na výzvy k přijetí opatření vydávané centrem CERT-EU. V technických záležitostech by měly výbor IICB podporovat technické poradní skupiny, které by měly případně úzce spolupracovat s centrem CERT-EU, orgány, institucemi, ***úřady*** nebo jinými subjekty Unie a dalšími zúčastněnými stranami. V případě potřeby by měl výbor IICB vydávat varování a ***doporučení*** pro audity.

Pozměňovací návrh 12

Návrh nařízení
Bod odůvodnění 17

Znění navržené Komisí	*Pozměňovací návrh*
(17) Úkolem centra CERT-EU by mělo být přispívat k bezpečnosti prostředí informačních technologií ve všech orgánech, institucích a jiných subjektech	(17) Úkolem centra CERT-EU by mělo být přispívat k bezpečnosti prostředí informačních a komunikačních technologií ve všech orgánech, institucích, ***úřadů*** a

Unie. Centrum CERT-EU by mělo jednat jako jakýsi specializovaný koordinátor orgánů, institucí a jiných subjektů Unie pro účely koordinovaného zpřístupňování informací o zranitelných místech v evropském registru zranitelných míst podle článku 6 směrnice [návrhu směrnice NIS 2].

jiných subjektech Unie. Centrum CERT-EU by mělo jednat jako jakýsi specializovaný koordinátor orgánů, institucí, ***úřadů*** a jiných subjektů Unie pro účely koordinovaného zpřístupňování informací o zranitelných místech v evropském registru zranitelných míst podle článku 6 směrnice [návrhu směrnice NIS 2].

Pozměňovací návrh 13

Návrh nařízení
Bod odůvodnění 18

Znění navržené Komisí	*Pozměňovací návrh*
(18) V roce 2020 řídící rada CERT-EU stanovila pro CERT-EU nový strategický cíl zajistit pro všechny orgány, instituce a jiné subjekty Unie komplexní úroveň kybernetické obrany s vhodnou šířkou a hloubkou a s neustálým přizpůsobováním se aktuálním nebo potenciálním hrozbám, včetně útoků zaměřených na mobilní zařízení, prostředí cloudu a zařízení internetu věcí. Tento strategický cíl zahrnuje také široké spektrum bezpečnostních operačních středisek, jež monitorují sítě, a nepřetržité monitorování vysoce rizikových hrozeb. U větších orgánů, institucí a jiných subjektů Unie by centrum CERT-EU mělo podporovat jejich týmy pro bezpečnost informačních technologií, včetně nepřetržitého monitorování v první linii. Menším a některým středně velkým orgánům, institucím a jiným subjektům by centrum CERT-EU mělo poskytovat veškeré služby.	(18) V roce 2020 řídící rada CERT-EU stanovila pro CERT-EU nový strategický cíl zajistit pro všechny orgány, instituce, ***úřady*** a jiné subjekty Unie komplexní úroveň kybernetické obrany s vhodnou šířkou a hloubkou a s neustálým přizpůsobováním se aktuálním nebo potenciálním hrozbám, včetně útoků zaměřených na mobilní zařízení, prostředí cloudu a zařízení internetu věcí. Tento strategický cíl zahrnuje také široké spektrum bezpečnostních operačních středisek, jež monitorují sítě, a nepřetržité monitorování vysoce rizikových hrozeb. U větších orgánů, institucí, ***úřadů*** a jiných subjektů Unie by centrum CERT-EU mělo podporovat jejich týmy pro bezpečnost informačních a komunikačních technologií, včetně nepřetržitého monitorování v první linii. Menším a některým středně velkým orgánům, institucím, ***úřadům*** a jiným subjektům by centrum CERT-EU mělo poskytovat veškeré služby.

Pozměňovací návrh 14

Návrh nařízení
Bod odůvodnění 19 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(19a) S cílem zajistit lepší provádění opatření a pokynů v oblasti kybernetické bezpečnosti pro orgány, instituce, úřady a jiné subjekty Unie a upevnit v nich kulturu kybernetické bezpečnosti by centrum CERT-EU mělo rovněž posílit spolupráci s evropskou sítí a centrem kompetencí pro kybernetickou bezpečnost.

Pozměňovací návrh 15

Návrh nařízení
Bod odůvodnění 20

Znění navržené Komisí	*Pozměňovací návrh*
(20) Při podpoře operační kybernetické bezpečnosti by centrum CERT-EU mělo využívat dostupné odborné znalosti Agentury Evropské unie pro kybernetickou bezpečnost, a to prostřednictvím strukturované spolupráce, jak stanoví nařízení Evropského parlamentu a Rady (EU) 2019/881[5]. V případě potřeby by měla být učiněna speciální ujednání mezi oběma subjekty o praktické podobě takové spolupráce a mělo by se zabránit zdvojování činností. Centrum CERT-EU by mělo spolupracovat s Agenturou Evropské unie pro kybernetickou bezpečnost při analýze hrozeb a pravidelně s touto agenturou sdílet svou zprávu o prostředí hrozeb.	(20) Při podpoře operační kybernetické bezpečnosti by centrum CERT-EU mělo využívat dostupné odborné znalosti Agentury Evropské unie pro kybernetickou bezpečnost, a to prostřednictvím strukturované spolupráce, jak stanoví nařízení Evropského parlamentu a Rady (EU) 2019/881. Měla by být učiněna speciální ujednání mezi oběma subjekty o praktické podobě takové spolupráce a mělo by se zabránit zdvojování činností. Centrum CERT-EU by mělo spolupracovat s Agenturou Evropské unie pro kybernetickou bezpečnost při analýze hrozeb a pravidelně s touto agenturou sdílet svou zprávu o prostředí hrozeb.
[5] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).	[5] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

Pozměňovací návrh 16
Návrh nařízení
Bod odůvodnění 24

Znění navržené Komisí	*Pozměňovací návrh*
(24) Jelikož služby a úkoly centra CERT-EU jsou v zájmu všech orgánů, institucí a jiných subjektů Unie, měl by každý orgán, instituce a jiný subjekt Unie s výdaji v oblasti informačních technologií přispívat na tyto služby a úkoly spravedlivým dílem. Těmito příspěvky není dotčena rozpočtová autonomie orgánů, institucí a jiných subjektů Unie.	(24) Jelikož služby a úkoly centra CERT-EU jsou v zájmu všech orgánů, institucí, ***úřadů*** a jiných subjektů Unie, měl by každý orgán, instituce, ***úřad*** a jiný subjekt Unie s výdaji v oblasti informačních a komunikačních technologií ***úměrně*** přispívat na tyto služby a úkoly. Těmito příspěvky není dotčena rozpočtová ***kapacita*** orgánů, institucí, ***úřadů*** a jiných subjektů Unie.

Pozměňovací návrh 17

Návrh nařízení
Bod odůvodnění 25

Znění navržené Komisí	*Pozměňovací návrh*
(25) IICB by za pomoci týmu CERT-EU měla přezkoumat a vyhodnotit provádění tohoto nařízení a měla by o svých zjištěních informovat Komisi. Na základě těchto informací by Komise měla podávat zprávy Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů,	(25) IICB by za pomoci týmu CERT-EU měla přezkoumat a vyhodnotit provádění tohoto nařízení a měla by o svých zjištěních informovat Komisi. Na základě těchto informací by Komise měla ***přinejmenším každé tři roky*** podávat zprávy Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů.

Pozměňovací návrh 18

Návrh nařízení
Čl. 1 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) orgánům, institucím a jiným subjektům Unie povinnosti s cílem zavést interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik;	a) orgánům, institucím, ***úřadům*** a jiným subjektům Unie povinnosti s cílem zavést interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik;

Pozměňovací návrh 19

Návrh nařízení
Čl. 1 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) pravidla týkající se organizace a provozu Centra pro kybernetickou bezpečnost orgánů, institucí a jiných subjektů Unie (CERT-EU) a organizace a provozu Interinstitucionálního výboru pro kybernetickou bezpečnost (IICB).	c) pravidla týkající se organizace a provozu Centra pro kybernetickou bezpečnost orgánů, institucí, ***úřadů*** a jiných subjektů Unie (CERT-EU) a ***fungování***, organizace a provozu Interinstitucionálního výboru pro kybernetickou bezpečnost (IICB).

Pozměňovací návrh 20

Návrh nařízení
Článek 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	Článek 2a
	Zpracování osobních údajů
	Zpracování osobních údajů podle tohoto nařízení centrem CERT-EU, IICB a všemi orgány, institucemi a jinými subjekty Unie se provádí v souladu s nařízením Evropského parlamentu a Rady (EU) 2018/1725.

Pozměňovací návrh 21

Návrh nařízení
Čl. 3 – odst. 1 – bod 2

Znění navržené Komisí	*Pozměňovací návrh*
2) „sítí a informačním systémem“ síť a informační systém ve smyslu čl. 4 odst. 1 směrnice [návrh směrnice NIS 2];	2) „sítí a informačním systémem“ síť a informační systém, jak jsou definovány ***v čl. 6 bodu 1*** směrnice [návrh směrnice NIS 2];

Pozměňovací návrh 22

Návrh nařízení
Čl. 3 – odst. 1 – bod 4

Znění navržené Komisí	*Pozměňovací návrh*
4) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 4 odst. 3 směrnice [návrh směrnice NIS 2];	4) ***„kybernetickou bezpečností“ kybernetická bezpečnost, jak je definována v čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) 2019/881[1a];***
	[1A] nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

Pozměňovací návrh 23

Návrh nařízení
Čl. 3 – odst. 1 – bod 5

Znění navržené Komisí	*Pozměňovací návrh*
5) „nejvyšší úrovní vedení“ vedoucí, vedení nebo koordinační orgán a orgán dohledu na nejvyšší správní úrovni, odpovídající za vysokou úroveň správních opatření v každém orgánu, instituci nebo jiném subjektu Unie;	5) „nejvyšší úrovní vedení“ vedoucí, vedení nebo koordinační orgán a orgán dohledu na nejvyšší správní úrovni ***s mandátem přijímat nebo schvalovat rozhodnut***í, odpovídající za vysokou úroveň správních opatření v každém orgánu, instituci, ***úřadu*** nebo jiném subjektu Unie;

Pozměňovací návrh 24

Návrh nařízení
Čl. 3 – odst. 1 – bod 7

Znění navržené Komisí	*Pozměňovací návrh*

7) „Významným incidentem“ se rozumí jakýkoli incident, pokud nemá ***omezený dopad a není pravděpodobné, že je již dobře znám z hlediska metody nebo technologie***.	7) „významnou událostí“ incident, který dotčenému subjektu Unie způsobil nebo může způsobit vážné provozní narušení fungování subjektu Unie nebo finanční ztrátu, nebo který ovlivnil nebo může ovlivnit jiné fyzické nebo právnické osoby tím, že způsobuje značnou hmotnou či nehmotnou újmu;

Pozměňovací návrh 25

Návrh nařízení
Čl. 3 – odst. 1 – bod 11

Znění navržené Komisí	*Pozměňovací návrh*
11) „významnou kybernetickou hrozbou“ kybernetická hrozba s úmyslem, příležitostí a schopností způsobit významný incident;	11) „významnou kybernetickou hrozbou“ ***kybernetická hrozba, jak je definována v čl. 6 bodě 11 směrnice [návrh směrnice NIS 2];***

Pozměňovací návrh 26

Návrh nařízení
Čl. 3 – odst. 1 – bod 14

Znění navržené Komisí	*Pozměňovací návrh*
14) „kybernetickým bezpečnostním rizikem“ jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů;	14) „rizikem“ jakékoli riziko, ***jak je definováno v čl. 6 odst. 9 směrnice [návrh směrnice NIS 2***];

Pozměňovací návrh 27

Návrh nařízení
Čl. 3 – odst. 1 – bod 14 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	14a) „informačním a komunikačním prostředím“ jakýkoli produkt, služba a proces IKT, na místě nebo virtuální, jak jsou definovány v článku 2, body 12, 13, 14 nařízení (EU) 2019/881, a veškeré sítě

	a informační systémy bez ohledu na to, zda jsou vlastněny a provozovány orgánem, institucí nebo jiným subjektem Unie nebo hostovány či provozovány třetí stranou, včetně mobilních zařízení, korporátních sítí a obchodních sítí, které nejsou připojeny k internetu, a jakýchkoli zařízení připojených k prostředí IKT;

Odůvodnění

Termín přesunut z čl. 4 odst. 2 tohoto návrhu do článku s definicemi vzhledem k tomu, že tento pojem je v celém textu jednotně používán. Navrhovaná definice tohoto pojmu vychází z definic jeho složek z článku 2 nařízení (EU) 2019/881 (aktu o kybernetické bezpečnosti).

Pozměňovací návrh 28

Návrh nařízení
Čl. 3 – odst. 1 – bod 15

Znění navržené Komisí	*Pozměňovací návrh*
15) „společnou kybernetickou jednotkou“ virtuální a fyzická platforma pro spolupráci různých komunit v oblasti kybernetické bezpečnosti v Unii, se zaměřením na operativní a technickou koordinaci v boji proti významným přeshraničním kybernetickým hrozbám a incidentům ve smyslu doporučení Komise ze dne 23. června 2021;	***vypouští se***

Pozměňovací návrh 29
Návrh nařízení
Čl. 4 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Každý orgán, instituce a jiný subjekt Unie zřídí svůj vlastní interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik (dále jen „rámec“) na podporu poslání subjektu a výkonu jeho institucionální autonomie. Na tuto práci dohlíží nejvyšší úroveň vedení subjektu, aby bylo zajištěno účinné a	1. ***Na základě celkových bezpečnostních auditů*** každý orgán, instituce a jiný subjekt Unie zřídí svůj vlastní interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik (dále jen „rámec“) na podporu poslání subjektu a výkonu jeho institucionální autonomie ***s přihlédnutím k soudržnosti a***

obezřetné řízení všech kybernetických bezpečnostních rizik. Rámec bude zaveden nejpozději do … [15 měsíců od vstupu tohoto nařízení v platnost].

interoperabilitě svého rámce s opatřeními ostatních příslušných orgánů, institucí a agentur. Na tuto práci dohlíží nejvyšší úroveň vedení subjektu, která je odpovědná za to, aby bylo zajištěno účinné a obezřetné řízení všech kybernetických bezpečnostních rizik. Rámec bude zaveden nejpozději do .... [15 měsíců od data vstupu tohoto nařízení v platnost].

Pozměňovací návrh 30

Návrh nařízení
Čl. 4 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Rámec zahrnuje celé prostředí informačních technologií dotčeného orgánu, instituce nebo jiného subjektu Unie, včetně jakéhokoli prostředí informačních technologií v jejich prostorách, externě zajišťovaných aktiv a služeb v prostředí cloud computingu nebo hostovaných třetími stranami, mobilních zařízení, podnikových sítí, obchodních sítí nepřipojených k internetu a jakýchkoli zařízení připojených k prostředí informačních technologií. Rámec zohledňuje řízení kontinuity činnosti v době krize a bere v úvahu bezpečnost dodavatelského řetězce, jakož i řízení lidských rizik, jež by mohla ovlivnit kybernetickou bezpečnost dotčeného orgánu, instituce nebo jiného subjektu Unie.	2. Rámec zahrnuje celé prostředí informačních a komunikačních technologií dotčeného orgánu, instituce, ***úřadu*** nebo jiného subjektu Unie, včetně jakéhokoli prostředí informačních a komunikačních technologií v jejich prostorách, externě zajišťovaných aktiv a služeb v prostředí cloud computingu nebo hostovaných třetími stranami, mobilních zařízení, podnikových sítí, obchodních sítí nepřipojených k internetu a jakýchkoli zařízení připojených k prostředí informačnícha komunikačních technologií. Rámec zohledňuje řízení kontinuity činnosti v době krize a bere v úvahu bezpečnost dodavatelského řetězce, jakož i řízení lidských rizik, jež by mohla ovlivnit kybernetickou bezpečnost dotčeného orgánu, instituce, ***úřadu*** nebo jiného subjektu Unie.

Pozměňovací návrh 31
Návrh nařízení
Čl. 4 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Každý orgán, instituce a jiný subjekt Unie má zaveden účinný mechanismus zajišťující, že přiměřená část	4. Každý orgán, instituce, ***úřad*** a jiný subjekt Unie má zaveden účinný mechanismus zajišťující, že ***alespoň 10 %***

rozpočtu na informační technologie bude vynaložena na kybernetickou bezpečnost.

celkového rozpočtu na informační a komunikační technologie bude vynaloženo na kybernetickou bezpečnost ***ve střednědobém horizontu***.

Pozměňovací návrh 32

Návrh nařízení
Čl. 4 – odst. 5 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	5a. Místní referent pro kybernetickou bezpečnost spolupracuje s pověřencem pro ochranu osobních údajů uvedeným v článku 43 nařízení (EU) 2018/1725 při řešení překrývajících se činností týkajících se záměrné a standardní ochrany osobních údajů u opatření v oblasti kybernetické bezpečnosti, při výběru opatření v oblasti kybernetické bezpečnosti, která zahrnují ochranu osobních údajů, integrované řízení rizik a integrované řešení bezpečnostních incidentů.

Pozměňovací návrh 33

Návrh nařízení
Čl. 5 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Nejvyšší úroveň vedení každého orgánu, instituce nebo jiného subjektu Unie schválí základní soubor opatření k zajištění vlastní kybernetické bezpečnosti subjektu pro řešení rizik zjištěných v rámci uvedeném v čl. 4 odst. 1. Činí tak na podporu svého poslání a výkonu své institucionální autonomie. Základní soubor opatření k zajištění kybernetické bezpečnosti musí být zaveden nejpozději do … [18 měsíců od vstupu tohoto nařízení v platnost] a řeší oblasti uvedené v příloze I a opatření uvedená v příloze II.	1. Nejvyšší úroveň vedení každého orgánu, instituce, ***úřadu*** nebo jiného subjektu Unie schválí základní soubor opatření k zajištění vlastní kybernetické bezpečnosti subjektu pro řešení rizik zjištěných v rámci uvedeném v čl. 4 odst. 1. Činí tak na podporu svého poslání a výkonu své institucionální autonomie ***v plném souladu s požadavky tohoto nařízení a s přihlédnutím k pokynům a doporučením přijatým IICB na návrh skupiny CERT-EU a příslušných unijních systémů certifikace kybernetické***

	bezpečnosti. Základní soubor opatření k zajištění kybernetické bezpečnosti bude zaveden nejpozději do … nejpozději do … [18 měsíců od data vstupu tohoto nařízení v platnost] a řeší oblasti uvedené v příloze I a opatření uvedená v příloze II.

Pozměňovací návrh 34

Návrh nařízení
Čl. 5 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Vrcholné vedení každého orgánu, instituce a jiného subjektu Unie pravidelně absolvuje zvláštní školení, aby získalo dostatečné znalosti a dovednosti umožňující posuzovat a vyhodnocovat kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz organizace.	2. Vrcholné vedení každého orgánu, instituce, ***úřadu*** a jiného subjektu Unie pravidelně absolvuje zvláštní školení, aby získalo dostatečné znalosti a dovednosti umožňující posuzovat a vyhodnocovat kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz organizace, ***s využitím odpovídajících zdrojů. Kromě těchto specifických školení a za účelem budování a konsolidace kultury kybernetické bezpečnosti se do plánu kybernetické bezpečnosti zahrne pravidelná odborná příprava pracovníků v oblasti kybernetické bezpečnosti, která bude alespoň jednou za dva roky aktualizována. Musí být zajištěny dostatečné zdroje pro zajištění kvalitní odborné přípravy.***

Pozměňovací návrh 35

Návrh nařízení
Čl. 6 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Každý orgán, instituce a jiný subjekt Unie provádí alespoň každé tři roky hodnocení vyspělosti kybernetické bezpečnosti, které zahrnuje všechny prvky jejich prostředí informačních technologií popsané v článku 4, přičemž zohlední příslušné pokyny a	Každý orgán, instituce, ***úřad*** nebo jiný subjekt Unie provede posouzení vyspělosti v oblasti kybernetické bezpečnosti do... ***[6 měsíců od vstupu nařízení v platnost]*** a poté alespoň každé dva roky hodnocení vyspělosti kybernetické bezpečnosti, které

doporučení přijaté v souladu s článkem 13.	zahrnuje všechny prvky jejich prostředí informačních technologií popsané v článku 4, přičemž zohlední příslušné pokyny a doporučení přijaté v souladu s článkem 13. ***Hodnocení vyspělosti musí být založeno na nezávislých auditech kybernetické bezpečnosti ověřených poskytovatelů.***

Pozměňovací návrh 36

Návrh nařízení
Čl. 7 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Na základě závěrů vyvozených z hodnocení vyspělosti a s ohledem na aktiva a rizika zjištěná podle článku 4 nejvyšší úroveň vedení každého orgánu, instituce nebo jiného subjektu EU po zavedení rámce pro řízení, správu a kontrolu rizik a základního souboru opatření k zajištění kybernetické bezpečnosti bez zbytečného prodlení schválí plán kybernetické bezpečnosti. Cílem plánu je zvýšit celkovou kybernetickou bezpečnost dotčeného subjektu, a tím přispět k dosažení nebo posílení vysoké společné úrovně kybernetické bezpečnosti ve všech orgánech, institucích a jiných subjektech Unie. Na podporu poslání subjektu na základě jeho institucionální autonomie zahrnuje plán přinejmenším oblasti uvedené v příloze I, opatření uvedená v příloze II, jakož i opatření týkající se připravenosti na incidenty, reakce na incidenty a zotavení z incidentů, jako je monitorování a vedení protokolů bezpečnosti. Plán se nejméně každé tři roky reviduje, a to na základě hodnocení vyspělosti provedených podle článku 6.	1. Na základě závěrů vyvozených z hodnocení vyspělosti a s ohledem na aktiva a rizika zjištěná podle článku 4 nejvyšší úroveň vedení každého orgánu, instituce, ***úřadu*** nebo jiného subjektu EU po zavedení rámce pro řízení, správu a kontrolu rizik a základního souboru opatření k zajištění kybernetické bezpečnosti bez zbytečného prodlení schválí plán kybernetické bezpečnosti. Cílem plánu je zvýšit celkovou kybernetickou bezpečnost dotčeného subjektu, a tím přispět k dosažení nebo posílení vysoké společné úrovně kybernetické bezpečnosti ve všech orgánech, institucích, ***úřadech*** a jiných subjektech Unie. Na podporu poslání subjektu na základě jeho institucionální autonomie zahrnuje plán přinejmenším oblasti uvedené v příloze I, opatření uvedená v příloze II, jakož i opatření týkající se připravenosti na incidenty, reakce na incidenty a zotavení z incidentů, jako je bezpečnostní p***osouzení dodavatelů a služeb***, monitorování a vedení protokolů bezpečnosti. Plán se nejméně každé ***dva*** roky reviduje, a to na základě hodnocení vyspělosti provedených podle článku 6.

Pozměňovací návrh 37

Návrh nařízení
Čl. 7 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Plán kybernetické bezpečnosti obsahuje úkoly zaměstnanců a odpovědnost za jeho provádění.	2. Plán kybernetické bezpečnosti obsahuje úkoly zaměstnanců, ***připravenost*** a odpovědnost za jeho provádění.

Pozměňovací návrh 38

Návrh nařízení
Čl. 7 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Plán kybernetické bezpečnosti zohledňuje příslušné pokyny a doporučení vydané centrem CERT-EU.	3. Plán kybernetické bezpečnosti ***zahrnuje navrhovaná opatření stanovená*** ve všech příslušných pokynech a doporučeních vydaných centrem CERT-EU.

Pozměňovací návrh 39

Návrh nařízení
Čl. 7 – odst. 3 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	3a. Orgány, instituce a jiné subjekty Unie předloží své plány kybernetické bezpečnosti Interinstitucionálnímu výboru pro kybernetickou bezpečnost (IICB). Tyto plány jsou sdíleny v co největší míře, aniž by hrozilo odhalení nebo zpřístupnění citlivých nebo důvěrných informací o konkrétních technických opatřeních a schopnostech subjektu Unie v oblasti kybernetické bezpečnosti neoprávněným třetím stranám.

Pozměňovací návrh 40

Návrh nařízení
Čl. 9 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) sledovat provádění tohoto nařízení orgány, institucemi a jinými subjekty Unie;	a) sledovat provádění tohoto nařízení orgány, institucemi, ***úřady*** a jinými subjekty Unie ***a poskytovat doporučení k dosažení vysoké společné úrovně kybernetické bezpečnosti***;

Pozměňovací návrh 41

Návrh nařízení
Čl. 9 – odst. 3 – pododstavec 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
Výbor IICB sestává ze tří zástupců nominovaných sítí agentur Unie (EUAN) na návrh jejího poradního výboru pro IKT, aby zastupovali zájmy orgánů a jiných subjektů, které provozují své vlastní prostředí informačních technologií, a po jednom zástupci vyslaném každým z těchto subjektů:	Výbor IICB sestává ze tří zástupců nominovaných sítí agentur Unie (EUAN) na návrh jejího poradního výboru pro IKT, aby zastupovali zájmy ***úřadů***, orgánů a jiných subjektů, které provozují své vlastní prostředí informačních a komunikačních technologií, a po jednom zástupci vyslaném každým z těchto subjektů:

Pozměňovací návrh 42

Návrh nařízení
Čl. 9 – odst. 3 – pododstavec 1 – písm. k a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ka) evropský inspektor ochrany údajů.

Pozměňovací návrh 43

Návrh nařízení
Čl. 10 – odst. 1 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) na základě návrhu vedoucího centra CERT-EU schvaluje doporučení k dosažení vysoké společné úrovně kybernetické bezpečnosti určená jednomu nebo všem orgánům, institucím a jiným

	subjektům Unie;

Pozměňovací návrh 44

Návrh nařízení
Čl. 11 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) vydat varování; je-li to nezbytné vzhledem k závažnému kybernetickému bezpečnostnímu riziku, okruh osob, jimž je varování určeno, se vhodně omezí;	a) vydat varování; je-li to nezbytné vzhledem k závažnému kybernetickému bezpečnostnímu riziku, okruh osob, jimž je varování určeno, se vhodně omezí, ***a to s pomocí společně dohodnuté metodiky***;

Pozměňovací návrh 45

Návrh nařízení
Čl. 11 – odst. 1 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) doporučit, aby příslušná auditorská služba provedla audit.	b) ***pověřit*** příslušnou auditorskou službu, aby provedla audit.

Pozměňovací návrh 46

Návrh nařízení
Čl. 12 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Posláním CERT-EU, autonomního interinstitucionálního centra kybernetické bezpečnosti pro všechny orgány, instituce a agentury Unie, je přispívat k bezpečnosti neutajovaného IT prostředí všech orgánů, institucí a jiných subjektů Unie, a to tak, že jim poskytuje poradenství v oblasti kybernetické bezpečnosti, pomáhá jim předcházet incidentům, odhalovat incidenty, zmírňovat incidenty a reagovat na incidenty a působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro koordinaci reakcí na	1. Posláním CERT-EU, autonomního interinstitucionálního centra kybernetické bezpečnosti pro všechny orgány, instituce, ***úřady*** a agentury Unie, je přispívat k bezpečnosti neutajovaného IKT prostředí všech orgánů, institucí, ***úřadů*** a jiných subjektů Unie, a to tak, že jim poskytuje poradenství v oblasti kybernetické bezpečnosti, pomáhá jim předcházet incidentům, odhalovat incidenty, zmírňovat incidenty a reagovat na incidenty a působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro

incidenty.	koordinaci reakcí na incidenty.

Pozměňovací návrh 47

Návrh nařízení
Čl. 12 – odst. 2 – písm. d

Znění navržené Komisí	*Pozměňovací návrh*
d) upozorňuje výbor IICB na jakýkoli problém týkající se provádění tohoto nařízení a provádění pokynů, doporučení a výzev k přijetí opatření;	d) upozorňuje výbor IICB na jakýkoli problém týkající se provádění tohoto nařízení a provádění pokynů, doporučení a výzev k přijetí opatření ***a předkládá návrhy pro nápravu;***

Pozměňovací návrh 48

Návrh nařízení
Čl. 12 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Centrum CERT-EU se zapojuje do strukturované spolupráce s Agenturou Evropské unie pro kybernetickou bezpečnost v oblasti budování kapacit, operativní spolupráce a dlouhodobých strategických analýz kybernetických hrozeb v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/881.	4. Centrum CERT-EU se zapojuje do strukturované spolupráce s Agenturou Evropské unie pro kybernetickou bezpečnost v oblasti budování kapacit, operativní spolupráce a dlouhodobých strategických analýz kybernetických hrozeb v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/881. ***Kromě toho může centrum CERT-EU spolupracovat a vyměňovat si informace s centrem Europolu pro boj proti kyberkriminalitě.***

Pozměňovací návrh 49

Návrh nařízení
Čl. 12 – odst. 5 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
5. Centrum CERT-EU může poskytovat tyto služby, které nejsou popsány v jeho katalogu služeb (dále jen	5. Centrum CERT-EU může ***orgánům, institucím, úřadům a jiným subjektům*** Unie poskytovat tyto služby,

„zpoplatněné služby“):

které nejsou popsány v jeho katalogu služeb (dále jen „zpoplatněné služby“):

Pozměňovací návrh 50

Návrh nařízení
Čl. 12 – odst. 5 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) služby, které podporují kybernetickou bezpečnost prostředí informačních technologií orgánů, institucí nebo jiných subjektů Unie, jiné než služby uvedené v odstavci 2, na základě dohod o úrovni služeb, a to s výhradou dostupných zdrojů;	a) služby, které podporují kybernetickou bezpečnost prostředí informačních a komunikačních technologií orgánů, institucí, ***úřadů*** nebo jiných subjektů Unie, jiné než služby uvedené v odstavci 2, na základě dohod o úrovni služeb, a to s výhradou dostupných zdrojů;

Pozměňovací návrh 51

Návrh nařízení
Čl. 12 – odst. 5 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) služby, které podporují operace nebo projekty orgánů, institucí a dalších subjektů Unie v oblasti kybernetické bezpečnosti, jiné než služby na ochranu jejich prostředí informačních technologií, na základě písemných dohod a po předchozím schválení výborem IICB;	b) služby, které podporují operace nebo projekty orgánů, institucí, ***úřadů*** a dalších subjektů Unie v oblasti kybernetické bezpečnosti, jiné než služby na ochranu jejich prostředí informačních a komunikačních technologií, na základě písemných dohod a po předchozím schválení výborem IICB;

Pozměňovací návrh 52
Návrh nařízení
Čl. 12 – odst. 5 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) služby, které podporují bezpečnost prostředí informačních technologií jiných	c) služby, které podporují bezpečnost prostředí informačních a komunikačních

organizací než orgánů, institucí a jiných subjektů Unie, které úzce spolupracují s orgány, institucemi nebo jinými subjekty Unie například tak, že jim byly uloženy úkoly nebo povinnosti podle práva Unie, a to na základě písemných dohod a po předchozím schválení výborem IICB.

technologií jiných organizací než orgánů, institucí, ***úřadů*** a jiných subjektů Unie, které úzce spolupracují s orgány, institucemi, ***úřady*** nebo jinými subjekty Unie například tak, že jim byly uloženy úkoly nebo povinnosti podle práva Unie, a to na základě písemných dohod a po předchozím schválení výborem IICB.

Pozměňovací návrh 53

Návrh nařízení
Čl. 12 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Centrum CERT-EU může v úzké spolupráci s Agenturou Evropské unie pro kybernetickou bezpečnost, je-li to použitelné, organizovat cvičení v oblasti kybernetické bezpečnosti za účelem testování úrovně kybernetické bezpečnosti orgánů, institucí a jiných subjektů Unie.	6. Centrum CERT-EU může v úzké spolupráci s Agenturou Evropské unie pro kybernetickou bezpečnost, je-li to použitelné, organizovat cvičení v oblasti kybernetické bezpečnosti za účelem pravidelného testování úrovně kybernetické bezpečnosti orgánů, institucí, ***úřadů*** a jiných subjektů Unie. ***Kromě toho může centrum CERT-EU prostřednictvím posílené spolupráce a společných programů s Evropskou sítí a centrem kompetencí pro kybernetickou bezpečnost podporovat výzkum a inovace a pomáhat při posilování kapacit orgánů, institucí a jiných subjektů Unie v oblasti kybernetické bezpečnosti.***

Pozměňovací návrh 54

Návrh nařízení
Čl. 12 – odst. 7

Znění navržené Komisí	*Pozměňovací návrh*
7. Centrum CERT-EU může poskytovat pomoc orgánům, institucím a jiným subjektům Unie v souvislosti s incidenty v utajovaných prostředích informačních technologií, pokud o to dotyčný zúčastněný subjekt výslovně	7. Centrum CERT-EU poskytuje pomoc orgánům, institucím, ***úřadům*** a jiným subjektům Unie v souvislosti s incidenty v utajovaných prostředích informačních technologií, ***a pokud má tým CERT -EU k tomu potřebné zdroje nebo***

požádá.	***od dotčeného subjektu tyto zdroje obdrží.***

Pozměňovací návrh 55

Návrh nařízení
Čl. 14 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Vedoucí centra CERT-EU předkládá výboru IICB a předsedovi výboru IICB pravidelné zprávy o výsledcích činnosti centra CERT-EU, finančním plánu, příjmech, plnění rozpočtu, uzavřených dohodách o úrovni služeb a písemných dohodách, spolupráci s protějšky a partnery a o misích podniknutých jeho zaměstnanci, včetně zpráv podle čl. 10 odst. 1.	Vedoucí centra CERT-EU předkládá výboru IICB a předsedovi výboru IICB ***nejméně jednou ročně*** zprávy o výsledcích činnosti centra CERT-EU, finančním plánu, příjmech, plnění rozpočtu, uzavřených dohodách o úrovni služeb a písemných dohodách, spolupráci s protějšky a partnery a o misích podniknutých jeho zaměstnanci, včetně zpráv podle čl. 10 odst. 1.

Pozměňovací návrh 56

Návrh nařízení
Čl. 16 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Centrum CERT-EU spolupracuje s vnitrostátními protějšky v členských státech, včetně týmů CERT, národních center pro kybernetickou bezpečnost, týmů CSIRT a jednotných kontaktních míst uvedených v článku 8 směrnice [návrh směrnice NIS 2] a vyměňuje si s nimi informace ohledně hrozeb, zranitelných míst a incidentů v oblasti kybernetické bezpečnosti, ohledně možných protiopatření a ohledně veškerých záležitostí, které mají význam pro zlepšení ochrany prostředí informačních technologií v orgánech, institucích nebo jiných subjektech Unie, a to i prostřednictvím sítě týmů CSIRT uvedené v článku 13 směrnice [návrhu směrnice NIS 2].	1. Centrum CERT-EU spolupracuje s vnitrostátními protějšky v členských státech, včetně týmů CERT, národních center pro kybernetickou bezpečnost, týmů CSIRT a jednotných kontaktních míst uvedených v článku 8 směrnice [návrh směrnice NIS 2] a vyměňuje si s nimi informace ohledně hrozeb, zranitelných míst a incidentů v oblasti kybernetické bezpečnosti, ohledně možných protiopatření a ohledně veškerých záležitostí, které mají význam pro zlepšení ochrany prostředí informačních technologií v orgánech, institucích, ***úřadech*** nebo jiných subjektech Unie, a to i prostřednictvím sítě týmů CSIRT uvedené v článku 13 směrnice [návrhu směrnice NIS 2].

Pozměňovací návrh 57

Návrh nařízení
Čl. 16 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Centrum CERT-EU si s vnitrostátními protějšky v členských státech může vyměňovat informace týkající se konkrétních incidentů za účelem usnadnění odhalování obdobných kybernetických hrozeb, a to bez souhlasu dotčeného zúčastněného subjektu. Informace týkající se konkrétních incidentů, které odhalují totožnost cíle kybernetického bezpečnostního incidentu, si může centrum CERT-EU vyměňovat pouze se souhlasem dotčeného zúčastněného subjektu.	2. Centrum CERT-EU si s vnitrostátními protějšky v členských státech může vyměňovat informace týkající se konkrétních incidentů za účelem usnadnění odhalování obdobných kybernetických hrozeb, ***a to bez souhlasu dotčených orgánů, institucí, úřadů či jiných subjektů Unie, pokud zpracování osobních údajů splňuje platná ustanovení nařízení (EU) 2018/1725.*** Informace týkající se konkrétních incidentů, které odhalují totožnost cíle kybernetického bezpečnostního incidentu, si může centrum CERT-EU vyměňovat pouze se souhlasem dotčených ***orgánů, institucí, úřadů či jiných subjektů Unie.***

Pozměňovací návrh 58

Návrh nařízení
Čl. 17 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Centrum CERT-EU může spolupracovat s protějšky v nečlenských státech, včetně protějšků zaměřených na konkrétní průmyslová odvětví, ohledně nástrojů a metod, jako například techniky, taktiky, postupů a osvědčených postupů, jakož i ohledně kybernetických hrozeb a zranitelných míst. Pro účely veškeré spolupráce s těmito protějšky, včetně spolupráce na základě rámců, v nichž protějšky ze zemí mimo EU spolupracují s vnitrostátními protějšky členských států, požádá centrum CERT-EU výbor IICB o předchozí souhlas.	1. Centrum CERT-EU může spolupracovat s protějšky v nečlenských státech, včetně protějšků zaměřených na konkrétní průmyslová odvětví, ohledně nástrojů a metod, jako například techniky, taktiky, postupů a osvědčených postupů, jakož i ohledně kybernetických hrozeb a zranitelných míst. Pro účely veškeré spolupráce s těmito protějšky, včetně spolupráce na základě rámců, v nichž protějšky ze zemí mimo EU spolupracují s vnitrostátními protějšky členských států, požádá centrum CERT-EU výbor IICB o předchozí souhlas. ***Každá taková spolupráce musí respektovat demokratickou integritu EU.***

Pozměňovací návrh 59

Návrh nařízení
Čl. 17 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Centrum CERT-EU může v zájmu shromažďování informací o obecných a konkrétních hrozbách, zranitelných místech a možných protiopatřeních spolupracovat s dalšími partnery, jako jsou komerční subjekty, mezinárodní organizace, vnitrostátní subjekty zemí mimo Evropskou unii nebo jednotliví odborníci. Pro účely širší spolupráce s těmito partnery požádá centrum CERT-EU výbor IICB o předchozí souhlas.	2. Centrum CERT-EU může v zájmu shromažďování informací o obecných a konkrétních hrozbách, zranitelných místech a možných protiopatřeních spolupracovat s dalšími partnery, jako jsou komerční subjekty, mezinárodní organizace, vnitrostátní subjekty zemí mimo Evropskou unii nebo jednotliví odborníci. Pro účely širší spolupráce s těmito partnery požádá centrum CERT-EU výbor IICB o předchozí souhlas. ***Každá taková spolupráce musí respektovat demokratickou integritu EU.***

Pozměňovací návrh 60

Návrh nařízení
Čl. 17 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Centrum CERT-EU může se souhlasem zúčastněného subjektu dotčeného incidentem poskytnout informace týkající se tohoto incidentu partnerům, kteří mohou přispět k jeho analýze.	3. Centrum CERT-EU může se souhlasem ***orgánů, institucí, úřadů či jiných subjektů Uni***e dotčených incidentem poskytnout informace týkající se tohoto incidentu partnerům, kteří mohou přispět k jeho analýze.

Pozměňovací návrh 61

Návrh nařízení
Čl. 19 – odst. -1 (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	-1. Orgány, instituce, úřady a agentury Unie poskytují centru CERT-EU informace o kybernetických hrozbách, incidentech, téměř nastalých incidentech a zranitelných místech, které se jich

dotýkají. Centrum CERT-EU zajistí, aby v zájmu usnadnění sdílení informací se zúčastněnými subjekty Unie byly k dispozici účinné komunikační prostředky. Centrum CERT-EU může dát přednost zpracování povinných oznámení před dobrovolnými oznámeními.

Pozměňovací návrh 62

Návrh nařízení
Čl. 19 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Aby se centru CERT-EU umožnilo koordinovat řízení zranitelnosti a reakce na incidenty, může požádat orgány, instituce a jiné subjekty Unie o poskytnutí informací ze soupisů jejich příslušných systémů informačních technologií, které mají význam pro podporu ze strany centra CERT-EU. Dožádaný orgán, instituce nebo jiný subjekt bez zbytečného odkladu předá požadované informace a všechny jejich následné aktualizace.	1. ***Aby mohlo centrum CERT-EU plnit své poslání a úkoly vymezené v článku 12, může požádat subjekty Unie*** o poskytnutí informací ze soupisů jejich příslušných systémů informačních technologií, ***včetně informací o kybernetických hrozbách, téměř nastalých incidentech, zranitelných místech, indikátorech narušení, varováních při ohrožení kybernetické bezpečnosti a doporučeních týkajících se konfigurace nástrojů kybernetické bezpečnosti určených k odhalování kybernetických incidentů.*** Dožádaný subjekt bez zbytečného odkladu předá požadované informace a všechny jejich následné aktualizace.

Pozměňovací návrh 63

Návrh nařízení
Čl. 19 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Orgány, instituce a jiné subjekty Unie na žádost centra CERT-EU a bez zbytečného odkladu digitální informace vytvořené použitím elektronických zařízení, která se podílela na jejich příslušných incidentech. Centrum CERT-EU může dále upřesnit, které typy těchto	2. Orgány, instituce, ***úřady*** a jiné subjekty Unie na žádost centra CERT-EU a bez zbytečného odkladu digitální informace vytvořené použitím elektronických zařízení, která se podílela na jejich příslušných incidentech. Centrum CERT-EU může dále upřesnit, které typy

digitálních informací požaduje pro situační přehled a reakci na incidenty.	těchto digitálních informací požaduje pro situační přehled a reakci na incidenty.

Pozměňovací návrh 64
Návrh nařízení
Čl. 20 – název

Znění navržené Komisí	*Pozměňovací návrh*
Oznamovací povinnosti	***Povinnost*** hlásit se

Pozměňovací návrh 65

Návrh nařízení
Čl. 20 – odst. 1 – pododstavec 1

Znění navržené Komisí	*Pozměňovací návrh*
Všechny orgány, instituce a jiné subjekty Unie předloží centru CERT-EU první oznámení o významných kybernetických hrozbách, významných zranitelných místech a významných incidentech, a to bez zbytečného odkladu, v každém případě do 24 hodin poté, co se o nich dozvěděly.	Všechny orgány, instituce, ***úřady*** a jiné subjekty Unie poskytnou centru CERT-EU ***včasné varován***í o významných kybernetických hrozbách, významných zranitelných místech a významných incidentech, a to bez zbytečného odkladu, v každém případě do 24 hodin poté, co se o nich dozvěděly. ***Toto včasné varování případně uvede, zda je významný incident pravděpodobně způsoben nezákonným nebo zlovolným jednáním a zda má nebo by mohl mít přeshraniční dopad.***

Pozměňovací návrh 66

Návrh nařízení
Čl. 20 – odst. 1 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
V řádně odůvodněných případech a po dohodě s centrem CERT-EU se dotčený orgán, instituce nebo jiný subjekt Unie může odchýlit od lhůty stanovené v předchozím odstavci.	V řádně odůvodněných případech a po dohodě s centrem CERT-EU se dotčená instituce, dotčený orgán, ***úřad*** nebo jiný subjekt Unie může odchýlit od této stanovené v odstavci lhůty.

Pozměňovací návrh 67

Návrh nařízení
Čl. 20 – odst. 2 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
2. Orgány, instituce a jiné subjekty Unie dále bez zbytečného prodlení oznámí orgánu CERT-EU vhodné technické podrobnosti o kybernetických hrozbách, zranitelných místech a incidentech, které umožňují odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů. Oznámení obsahují tyto prvky, jsou-li dostupné:	2. Orgány, instituce, úřady a jiné subjekty Unie dále ***bez zbytečného odkladu a v každém případě do 72 hodin poté, co se o incidentu dozvěděly, zašlou týmu CERT-EU oznámení, aktualizují včasné varování a poskytnou počáteční posouzení*** s náležitými technickými podrobnostmi o kybernetických hrozbách, zranitelných místech a incidentech, které umožňují odhalení, reakci na incident nebo opatření ke zmírnění jeho dopadu. Oznámení obsahují tyto prvky, jsou-li dostupné:

Pozměňovací návrh 68
Návrh nařízení
Čl. 20 – odst. 2 – pododstavec 1 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	V řádně odůvodněných případech a po dohodě s centrem CERT-EU se dotčená instituce, dotčený orgán, úřad nebo jiný subjekt Unie může odchýlit od této lhůty.

Pozměňovací návrh 69

Návrh nařízení
Čl. 20 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Nejpozději jeden měsíc po předložení oznámení o incidentu předloží orgány, instituce a jiné subjekty Unie centru CERT-EU závěrečnou zprávu obsahující alespoň:
	a) podrobný popis významného incidentu, jeho závažnost a dopad;

	b) druh hrozby nebo základní příčinu, která významný incident pravděpodobně spustila;
	c) učiněná a probíhající opatření ke zmírnění následků;
	d) případně přeshraniční dopad významného incidentu;
	v případě přetrvávajících významných incidentů v době předložení závěrečné zprávy uvedené v prvním podosdstavci zprávu o pokroku v daném okamžiku a závěrečnou zprávu do jednoho měsíce od vyřešení incidentu.

Pozměňovací návrh 70

Návrh nařízení
Čl. 20 – odst. 2 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2b. V řádně odůvodněných případech a po dohodě s centrem CERT-EU se dotčený orgán, instituce, úřad nebo jiný subjekt Unie může odchýlit od lhůty stanovené v odstavci 2a.

Pozměňovací návrh 71

Návrh nařízení
Čl. 20 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Orgán CERT-EU předkládá agentuře ENISA měsíční souhrnnou zprávu obsahující anonymizované a agregované údaje o významných kybernetických hrozbách, významných zranitelných místech a významných incidentech oznámených v souladu s odstavcem 1.	3. Orgán CERT-EU předkládá agentuře ENISA měsíční souhrnnou zprávu obsahující anonymizované a agregované údaje o významných kybernetických hrozbách, významných zranitelných místech a významných incidentech oznámených v souladu s odstavcem 1. ***Tato zpráva je podkladem pro dvouletou zprávu o stavu kybernetické bezpečnosti v Unii podle článku 18 směrnice [návrh směrnice NIS 2].***

Pozměňovací návrh 72

Návrh nařízení
Čl. 20 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Výbor IICB může vydávat pokyny nebo doporučení týkající se způsobů oznamování a obsahu oznámení. Centrum CERT-EU šíří vhodné technické podrobnosti s cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů ze strany orgánů, institucí nebo jiných subjektů Unie.	4. Výbor IICB vydává pokyny nebo doporučení týkající se způsobů oznamování a obsahu oznámení. Centrum CERT-EU šíří vhodné technické podrobnosti s cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů ze strany orgánů, institucí, ***úřadů*** nebo jiných subjektů Unie.

Pozměňovací návrh 73

Návrh nařízení
Čl. 20 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Oznamovací povinnosti se nevztahují na utajované informace EU a na informace, které orgán, instituce nebo jiný subjekt Unie obdržely od bezpečnostní a zpravodajské služby nebo donucovacího orgánu členského státu za výslovné podmínky, že nebudou sdíleny s orgánem CERT-EU.	***vypouští se***

Pozměňovací návrh 74

Návrh nařízení
Čl. 24 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Komise podá Evropskému parlamentu a Radě zprávu o provádění tohoto nařízení nejpozději 48 měsíců po vstupu tohoto nařízení v platnost a poté	2. Komise podá Evropskému parlamentu a Radě zprávu o provádění tohoto nařízení nejpozději ***36 měsíců*** po vstupu tohoto nařízení v platnost a poté

každé tři roky.	každé ***dva*** roky.

Pozměňovací návrh 75

Návrh nařízení
Čl. 24 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Komise vyhodnotí fungování tohoto nařízení a podá zprávu Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů nejdříve pět let ode dne jeho vstupu v platnost.	3. Komise vyhodnotí fungování tohoto nařízení a podá zprávu Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů nejdříve ***tři*** roky ode dne jeho vstupu v platnost, ***vzhledem k rychle se vyvíjejícímu prostředí kybernetických hrozeb.***

Pozměňovací návrh 76

Návrh nařízení
Příloha I – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
V základním souboru opatření k zajištění kybernetické bezpečnosti je třeba řešit následující oblasti:	V základním souboru opatření k zajištění kybernetické bezpečnosti je třeba řešit ***alespoň*** následující oblasti:

Pozměňovací návrh 77

Návrh nařízení
Příloha I – odst. 1 – bod 1 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	1a) pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 78

Návrh nařízení
Příloha I – odst. 1 – bod 3

Znění navržené Komisí	*Pozměňovací návrh*
3) správa aktiv, včetně seznamu aktiv v oblasti informačních technologií a zmapování sítí informačních technologií;	3) nabytí a správa aktiv, včetně seznamu aktiv v oblasti informačních technologií a zmapování sítí informačních technologií;

Pozměňovací návrh 79

Návrh nařízení
Příloha I – odst. 1 – bod 7

Znění navržené Komisí	*Pozměňovací návrh*
7) akvizice, vývoj a údržba systémů;	7) akvizice, vývoj a údržba systémů, ***včetně vývoje interního softwaru s otevřeným zdrojovým kódem;***

Pozměňovací návrh 80

Návrh nařízení
Příloha I – odst. 1 – bod 7 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	7a) audity kybernetické bezpečnosti;

Pozměňovací návrh 81

Návrh nařízení
Příloha I – odst. 1 – bod 9

Znění navržené Komisí	*Pozměňovací návrh*
9) řízení incidentů, včetně přístupů pro zlepšení připravenosti na incidenty, reakce na incidenty a zotavení z incidentů, a spolupráce s centrem CERT-EU, jako je zachování monitorování a vedení protokolů bezpečnosti;	9) řízení incidentů, včetně přístupů pro zlepšení připravenosti na incidenty, reakce na incidenty, dodržování a zkrácení lhůt pro oznamovací povinnosti a zotavení z incidentů, a spolupráce s centrem CERT-EU, jako je zachování monitorování a vedení protokolů bezpečnosti;

Pozměňovací návrh 82

Návrh nařízení
Příloha II – odst. 1 – bod 3 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	3a) pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 83

Návrh nařízení
Příloha II – odst. 1 – bod 4 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) odstranění smluvních překážek, které omezují sdílení informací ohledně incidentů, zranitelných míst a kybernetických hrozeb obdržených od poskytovatelů služeb informačních technologií s centrem CERT-EU,	a) odstranění smluvních překážek, které omezují sdílení informací ohledně incidentů, zranitelných míst a kybernetických hrozeb obdržených od poskytovatelů služeb informačních technologií s centrem CERT-EU,

POSTUP VE VÝBORU POŽÁDANÉM O STANOVISKO

Název	Stanovení opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie
Referenční údaje	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Příslušný výbor Datum oznámení na zasedání	ITRE 4.4.2022
Výbor, který vypracoval stanovisko Datum oznámení na zasedání	AFCO 4.4.2022
Zpravodaj(ka) Datum jmenování	Markéta Gregorová 20.6.2022
Projednání ve výboru	26.10.2022 1.12.2022
Datum přijetí	25.1.2023
Výsledek konečného hlasování	+: 24 –: 0 0: 0
Členové přítomní při konečném hlasování	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Náhradníci přítomní při konečném hlasování	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Náhradníci (čl. 209 odst. 7) přítomní při konečném hlasování	Leszek Miller

JMENOVITÉ KONEČNÉ HLASOVÁNÍ
VE VÝBORU POŽÁDANÉM O STANOVISKO

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se