POZMĚŇOVACÍ NÁVRHY 001-280
které předložil Výbor pro průmysl, výzkum a energetiku

Zpráva
Bart Groothuis **A9-0313/2021**
Vysoká společná úroveň kybernetické bezpečnosti

Návrh směrnice (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Pozměňovací návrh 1

Návrh směrnice
Název

Znění navržené Komisí	*Pozměňovací návrh*
Návrh	Návrh
SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY	SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY
o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148	o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii ***(směrnice NIS 2)*** a o zrušení směrnice (EU) 2016/1148

Pozměňovací návrh 2

Návrh směrnice
Bod odůvodnění 1

Znění navržené Komisí	*Pozměňovací návrh*
(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/1148[11] bylo budovat schopnosti v oblasti kybernetické bezpečnosti v Unii, zmírňovat hrozby pro	(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/1148[11]**,** ***běžně označované jako „směrnice NIS“*** bylo budovat schopnosti v oblasti

sítě a informační systémy užívané k poskytování základních služeb v klíčových odvětvích a zajišťovat kontinuitu takových služeb v případě kybernetických bezpečnostních incidentů, a přispívat tak k účinnému fungování hospodářství a společnosti v Unii.

kybernetické bezpečnosti v Unii, zmírňovat hrozby pro sítě a informační systémy užívané k poskytování základních služeb v klíčových odvětvích a zajišťovat kontinuitu takových služeb v případě kybernetických bezpečnostních incidentů, a přispívat tak k ***bezpečnosti a*** účinnému fungování hospodářství a společnosti v Unii.

---

[11] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194/1, 19.7.2016, s. 1).

[11] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194/1, 19.7.2016, s. 1).

Pozměňovací návrh 3

Návrh směrnice
Bod odůvodnění 3

Znění navržené Komisí	*Pozměňovací návrh*
(3) Sítě a informační systémy se rozvinuly v ústřední prvek každodenního života s rychlou digitální transformací a vzájemnou propojeností společnosti, včetně přeshraniční výměny. Tento vývoj vedl k prudkému rozšíření prostředí kybernetických bezpečnostních hrozeb a přináší nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost výskytu a dopad kybernetických bezpečnostních incidentů narůstají a představují značnou hrozbu pro fungování sítí a informačních systémů. V důsledku toho mohou kybernetické incidenty brzdit provádění hospodářských činností na vnitřním trhu, způsobovat finanční ztráty, narušovat důvěru uživatelů a způsobovat velké škody hospodářství a společnosti Unie. Připravenost a účinnost v oblasti kybernetické bezpečnosti jsou dnes proto	(3) Sítě a informační systémy se rozvinuly v ústřední prvek každodenního života s rychlou digitální transformací a vzájemnou propojeností společnosti, včetně přeshraniční výměny. Tento vývoj vedl k prudkému rozšíření prostředí kybernetických bezpečnostních hrozeb a přináší nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost výskytu a dopad kybernetických bezpečnostních incidentů narůstají a představují značnou hrozbu pro fungování sítí a informačních systémů. V důsledku toho mohou kybernetické incidenty brzdit provádění hospodářských činností na vnitřním trhu, způsobovat finanční ztráty, narušovat důvěru uživatelů a způsobovat velké škody hospodářství a společnosti Unie. Připravenost a účinnost v oblasti kybernetické bezpečnosti jsou dnes proto

pro řádné fungování vnitřního trhu důležitější než kdy předtím.	pro řádné fungování vnitřního trhu důležitější než kdy předtím. ***Kybernetická bezpečnost je navíc klíčovým faktorem, který mnoha kritickým odvětvím umožňuje zapojit se do digitální transformace a plně využívat hospodářských, sociálních a udržitelných přínosů digitalizace.***

Pozměňovací návrh 4

Návrh směrnice
Bod odůvodnění 3 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(3a) Rozsáhlé kybernetické bezpečnostní incidenty a krize na úrovni Unie vyžadují koordinovaná opatření k zajištění rychlé a účinné reakce z důvodu vysokého stupně vzájemné závislosti mezi jednotlivými odvětvími a zeměmi. Pro zajištění bezpečnosti Unie v rámci jejích hranic i mimo ně má zásadní význam dostupnost kyberneticky odolných sítí a informačních systémů a dostupnost, důvěrnost a integrita údajů, jelikož kybernetické hrozby mohou přicházet i ze zemí mimo Unii. Snaha EU získat významnější geopolitickou úlohu vyžaduje rovněž důvěryhodnou kybernetickou ochranu a odrazování, včetně schopnosti včas a účinně identifikovat zlovolná opatření a odpovídajícím způsobem na ně reagovat.

Pozměňovací návrh 5

Návrh směrnice
Bod odůvodnění 5

Znění navržené Komisí	*Pozměňovací návrh*
(5) Všechny tyto rozdíly vyvolávají roztříštěnost vnitřního trhu a mohou mít škodlivý účinek na jeho fungování s tím, že	(5) Všechny tyto rozdíly vyvolávají roztříštěnost vnitřního trhu a mohou mít škodlivý účinek na jeho fungování s tím, že

ovlivňují zejména přeshraniční poskytování služeb a úroveň odolnosti v oblasti kybernetické bezpečnosti v důsledku uplatňování odlišných norem. Cílem této směrnice je takové značné rozdíly mezi členskými státy odstranit, zejména stanovením minimálních pravidel upravujících fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce příslušných orgánů v každém členském státě, aktualizací seznamu odvětví a činností, na něž se vztahují povinnosti v oblasti kybernetické bezpečnosti, a zavedením účinných nápravných opatření a sankcí, jež napomáhají účinnému vymáhání těchto povinností. Směrnice (EU) 2016/1148 by proto měla být zrušena a nahrazena touto směrnicí.	ovlivňují zejména přeshraniční poskytování služeb a úroveň odolnosti v oblasti kybernetické bezpečnosti v důsledku uplatňování odlišných norem. ***Tyto rozdíly by v konečném důsledku mohly vést k větší zranitelnosti některých členských států vůči hrozbám v oblasti kybernetické bezpečnosti, což může mít dopady na celou Unii.*** Cílem této směrnice je takové značné rozdíly mezi členskými státy odstranit, zejména stanovením minimálních pravidel upravujících fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce příslušných orgánů v každém členském státě, aktualizací seznamu odvětví a činností, na něž se vztahují povinnosti v oblasti kybernetické bezpečnosti, a zavedením účinných nápravných opatření a sankcí, jež napomáhají účinnému vymáhání těchto povinností. Směrnice (EU) 2016/1148 by proto měla být zrušena a nahrazena touto směrnicí ***(směrnice NIS 2)***.

Pozměňovací návrh 6

Návrh směrnice
Bod odůvodnění 6

Znění navržené Komisí	*Pozměňovací návrh*
(6) Tato směrnice ponechává nedotčenou schopnost členských států přijímat nezbytná opatření, aby zajistily ochranu svých základních bezpečnostních zájmů, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. V souladu s článkem 346 SFEU není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho veřejné bezpečnosti. V tomto ohledu jsou relevantní pravidla členských států a Unie o ochraně utajovaných informací, dohody o	(6) Tato směrnice ponechává nedotčenou schopnost členských států přijímat nezbytná opatření, aby zajistily ochranu svých základních bezpečnostních zájmů, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily ***prevenci,*** vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. V souladu s článkem 346 SFEU není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho veřejné bezpečnosti. V tomto ohledu jsou relevantní pravidla členských států a Unie o ochraně utajovaných informací, dohody o

zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol)[14].

[14] Semaforový protokol je prostředek pro toho, kdo sdílí informace, aby informoval své publikum o jakýchkoli omezeních dalšího šíření těchto informací. Používá se téměř ve všech komunitách CSIRT a některých střediscích pro sdílení a analýzu informací (ISAC).

zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol)[14].

[14] Semaforový protokol je prostředek pro toho, kdo sdílí informace, aby informoval své publikum o jakýchkoli omezeních dalšího šíření těchto informací. Používá se téměř ve všech komunitách CSIRT a některých střediscích pro sdílení a analýzu informací (ISAC).

Pozměňovací návrh 7

Návrh směrnice
Bod odůvodnění 7

Znění navržené Komisí	*Pozměňovací návrh*
(7) Se zrušením směrnice (EU) 2016/1148 by vzhledem k aspektům uvedeným ve 4. až 6. bodě odůvodnění měla být oblast působnosti podle odvětví rozšířena na větší část ekonomiky. Odvětví pokrytá směrnicí (EU) 2016/1148 by proto měla být rozšířena tak, aby bylo zajištěno komplexní pokrytí odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu. ***Pravidla*** by se ***neměla*** lišit podle toho, zda jsou subjekty provozovateli základních služeb nebo poskytovateli digitálních služeb. Toto rozlišení se ukázalo jako zastaralé, neboť nezohledňuje skutečnou důležitost odvětví nebo služeb z hlediska společenských a hospodářských činností na vnitřním trhu.	(7) Se zrušením směrnice (EU) 2016/1148 by vzhledem k aspektům uvedeným ve 4. až 6. bodě odůvodnění měla být oblast působnosti podle odvětví rozšířena na větší část ekonomiky. Odvětví pokrytá směrnicí (EU) 2016/1148 by proto měla být rozšířena tak, aby bylo zajištěno komplexní pokrytí odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu. ***Požadavky na řízení rizik a oznamovací povinnosti*** by se ***neměly*** lišit podle toho, zda jsou subjekty provozovateli základních služeb nebo poskytovateli digitálních služeb. Toto rozlišení se ukázalo jako zastaralé, neboť nezohledňuje skutečnou důležitost odvětví nebo služeb z hlediska společenských a hospodářských činností na vnitřním trhu.

Pozměňovací návrh 8

Návrh směrnice
Bod odůvodnění 8

Znění navržené Komisí	*Pozměňovací návrh*
(8) V souladu se směrnicí (EU) 2016/1148 byly členské státy odpovědné za určení toho, které subjekty splňují kritéria pro zařazení mezi provozovatele základních služeb (dále jen „proces určování“). S cílem odstranit značné rozdíly mezi členskými státy v tomto ohledu a zajistit právní jistotu pro všechny příslušné subjekty, pokud jde o požadavky na řízení rizik a povinnosti hlášení, by mělo být stanoveno jednotné kritérium, které určí subjekty, jež spadají do oblasti působnosti této směrnice. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti působnosti této směrnice spadaly všechny střední a velké podniky ve smyslu doporučení Komise 2003/361/ES[15], které působí v odvětvích nebo poskytují druh služeb, na něž se vztahuje tato směrnice. ***Od členských států by nemělo být vyžadováno, aby stanovily seznam subjektů, které splňují toto obecně použitelné kritérium související s velikostí podniku.***	(8) V souladu se směrnicí (EU) 2016/1148 byly členské státy odpovědné za určení toho, které subjekty splňují kritéria pro zařazení mezi provozovatele základních služeb (dále jen „proces určování“). S cílem odstranit značné rozdíly mezi členskými státy v tomto ohledu a zajistit právní jistotu pro všechny příslušné subjekty, pokud jde o požadavky na řízení rizik a povinnosti hlášení, by mělo být stanoveno jednotné kritérium, které určí subjekty, jež spadají do oblasti působnosti této směrnice. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti působnosti této směrnice spadaly všechny střední a velké podniky ve smyslu doporučení Komise 2003/361/ES[15], které působí v odvětvích nebo poskytují druh služeb, na něž se vztahuje tato směrnice.
[15] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).	[15] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

Pozměňovací návrh 9

Návrh směrnice
Bod odůvodnění 9

Znění navržené Komisí	*Pozměňovací návrh*
(9) Tato směrnice by se však měla vztahovat i na malé subjekty nebo mikrosubjekty, které splňují určitá kritéria, jež naznačují klíčovou úlohu pro hospodářství nebo společnosti členských	(9) Tato směrnice by se však měla vztahovat i na malé subjekty nebo mikrosubjekty, které splňují určitá kritéria, jež naznačují klíčovou úlohu pro hospodářství nebo společnosti členských

států nebo pro konkrétní odvětví či konkrétní druhy služeb. ***Členské státy by měly být odpovědné za stanovení seznamu takových subjektů a předložit ho Komisi.***	států nebo pro konkrétní odvětví či konkrétní druhy služeb.

Pozměňovací návrh 10

Návrh směrnice
Bod odůvodnění 9 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(9a) Členské státy by měly sestavit seznam všech základních a důležitých subjektů. Tento seznam by měl zahrnovat subjekty, které splňují obecně platná kritéria týkající se velikosti, jakož i malé podniky a mikropodniky, které splňují určitá kritéria, jež ukazují na jejich klíčovou úlohu pro hospodářství nebo společností členských států. Aby týmy pro reakce na počítačové bezpečnostní incidenty (CSIRT) a příslušné orgány mohly těmto subjektům poskytovat pomoc a varovat je před kybernetickými incidenty, které by je mohly postihnout, je důležité, aby tyto orgány měly správné kontaktní údaje těchto subjektů. Základní a důležité subjekty by proto měly příslušným orgánům poskytovat alespoň tyto informace: název subjektu, adresu a aktuální kontaktní údaje, jako jsou e-mailové adresy, rozsah IP adres, telefonní čísla a příslušná odvětví a pododvětví uvedená v přílohách I a II. Subjekty by měly příslušným orgánům oznamovat veškeré změny těchto informací. Členské státy by měly bez zbytečného odkladu zajistit, aby tyto informace mohly být snadno poskytovány prostřednictvím jednotného kontaktního místa. Za tímto účelem by Agentura ENISA spolu se skupinou pro spolupráci měla bez zbytečného odkladu vydat pokyny a šablony pro oznamovací povinnosti. Členské státy by měly Komisi a skupině pro spolupráci oznámit počet základních a

důležitých subjektů. Členské státy by měly Komisi pro účely přezkumu uvedeného v této směrnici rovněž oznámit názvy malých podniků a mikropodniků, které byly určeny základní a důležité subjekty, aby Komise mohla posoudit soudržnost přístupů jednotlivých členských států. Tyto informace by měly být považovány za přísně důvěrné.

Pozměňovací návrh 11

Návrh směrnice
Bod odůvodnění 10

Znění navržené Komisí	*Pozměňovací návrh*
(10) Komise může ve spolupráci se skupinou pro spolupráci vydávat pokyny ohledně plnění kritérií platných pro mikropodniky a malé podniky.	(10) Komise by ve spolupráci se skupinou pro spolupráci ***a relevantními zúčastněnými stranami měla*** vydávat pokyny ohledně plnění kritérií platných pro mikropodniky a malé podniky. ***Komise by rovněž měla zajistit, že budou všem mikropodnikům a malým podnikům spadajícím do oblasti působnosti této směrnice poskytovány vhodné pokyny. V této souvislosti by Komise s podporou členských států měla mikropodnikům a malým podnikům poskytovat informace.***

Pozměňovací návrh 12

Návrh směrnice
Bod odůvodnění 10 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	***(10a) Komise by rovněž měla vydat pokyny s cílem pomoci členským státům správně provádět ustanovení týkající se oblasti působnosti této směrnice a vyhodnotit přiměřenost povinností stanovených touto směrnicí, zejména pokud jde o subjekty s komplexními obchodními modely nebo provozním prostředím, kdy určitý subjekt**

	může současně splňovat kritéria stanovená pro základní i důležité subjekty nebo současně vykonávat činnosti, z nichž některé spadají do oblasti působnosti této směrnice, a jiné nikoli.

Pozměňovací návrh 13

Návrh směrnice
Bod odůvodnění 12

Znění navržené Komisí	*Pozměňovací návrh*
(12) Právní předpisy a nástroje specifické pro jednotlivá odvětví mohou přispět k zajištění vysoké úrovně kybernetické bezpečnosti při současném plném zohlednění zvláštností a složitosti těchto odvětví. Pokud právní akt Unie specifický pro určité odvětví vyžaduje, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik***,*** nebo aby oznamovaly incidenty ***nebo závažné kybernetické hrozby s*** alespoň ***rovnocenným účinkem*** jako povinnosti stanovené v této směrnici, měla by platit tato ustanovení specifická pro dané odvětví, včetně ustanovení o dohledu a vymáhání. Komise ***může*** vydávat pokyny v souvislosti s prováděním lex specialis. Tato směrnice nebrání přijetí dalších aktů Unie specifických pro určitá odvětví a týkajících se opatření k řízení kybernetických bezpečnostních rizik a oznamování incidentů. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a energetiky.	(12) Právní předpisy a nástroje specifické pro jednotlivá odvětví mohou přispět k zajištění vysoké úrovně kybernetické bezpečnosti při současném plném zohlednění zvláštností a složitosti těchto odvětví. ***Akty Unie specifické pro určitá odvětví, které vyžadují, aby základní nebo důležité subjekty přijímaly opatření k řízení kybernetických bezpečnostních rizik nebo oznamovaly závažné incidenty, by pokud možno měly být v souladu s příslušnou terminologií a odkazovat na definice stanovené v této směrnici.*** Pokud právní akt Unie specifický pro určité odvětví vyžaduje, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik nebo aby oznamovaly incidenty***, a pokud tyto požadavky mají*** alespoň ***rovnocenný účinek*** jako povinnosti stanovené v této směrnici ***a pokud se vztahují na všechny bezpečnostní aspekty operací a služeb poskytovaných základními a důležitými subjekty,*** měla by platit tato ustanovení specifická pro dané odvětví, včetně ustanovení o dohledu a vymáhání. Komise ***by měla*** vydávat ***komplexní*** pokyny v souvislosti s prováděním lex specialis ***s přihlédnutím k příslušným stanoviskům, odborným znalostem a osvědčeným postupům agentury ENISA a skupiny pro spolupráci***. Tato směrnice nebrání přijetí dalších aktů Unie specifických pro určitá odvětví a týkajících se opatření k řízení

kybernetických bezpečnostních rizik a oznamování incidentů***, které řádně zohlední potřebu komplexního a soudržného rámce pro kybernetickou bezpečnost***. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a energetiky.

Pozměňovací návrh 14

Návrh směrnice
Bod odůvodnění 14

Znění navržené Komisí	*Pozměňovací návrh*
(14) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) XXX/XXX[17] a k této směrnici. Za tímto účelem by členské státy měly zajistit, aby klíčové subjekty a rovnocenné subjekty podle směrnice (EU) XXX/XXX byly považovány za základní subjekty podle této směrnice. Členské státy by také měly zajistit, aby jejich strategie kybernetické bezpečnosti stanovily rámec politik pro posílení koordinace mezi ***příslušným orgánem*** podle této směrnice a ***příslušným orgánem*** podle směrnice (EU) XXX/XXX v souvislosti se sdílením informací o incidentech a kybernetických hrozbách a plněním úkolů v oblasti dohledu. Orgány by podle obou směrnic měly spolupracovat a vyměňovat si informace, zejména informace týkající se určení klíčových subjektů, kybernetických hrozeb, kybernetických bezpečnostních rizik, incidentů dotýkajících se klíčových subjektů a opatření v oblasti kybernetické bezpečnosti přijatých klíčovými subjekty. Příslušným orgánům podle této směrnice by mělo být umožněno, aby na žádost příslušných orgánů podle směrnice (EU) XXX/XXX vykonávaly své dohledové a	(14) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) XXX/XXX[17] a k této směrnici. Za tímto účelem by členské státy měly zajistit, aby klíčové subjekty a rovnocenné subjekty podle směrnice (EU) XXX/XXX byly považovány za základní subjekty podle této směrnice. Členské státy by také měly zajistit, aby jejich strategie kybernetické bezpečnosti stanovily rámec politik pro posílení koordinace mezi ***příslušnými orgány v rámci jednotlivých členských států i mezi nimi*** podle této směrnice a podle směrnice (EU) XXX/XXX***,*** v souvislosti se sdílením informací o incidentech a kybernetických hrozbách a plněním úkolů v oblasti dohledu. Orgány by podle obou směrnic měly spolupracovat a vyměňovat si ***bez zbytečného odkladu*** informace, zejména informace týkající se určení klíčových subjektů, kybernetických hrozeb, kybernetických bezpečnostních rizik, incidentů dotýkajících se klíčových subjektů a opatření v oblasti kybernetické bezpečnosti přijatých klíčovými subjekty. Příslušným orgánům podle této směrnice by mělo být umožněno, aby na žádost příslušných orgánů podle směrnice (EU)

vymáhací pravomoci vůči subjektu, který byl označen jako klíčový. Oba orgány by za tímto účelem měly spolupracovat a vyměňovat si informace.	XXX/XXX vykonávaly své dohledové a vymáhací pravomoci vůči subjektu, který byl označen jako klíčový. Oba orgány by za tímto účelem měly spolupracovat a vyměňovat si informace***, pokud možno v reálném čase***.
[17] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]	[17] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

Pozměňovací návrh 15

Návrh směrnice
Bod odůvodnění 15

Znění navržené Komisí	*Pozměňovací návrh*
(15) Podpora a ochrana spolehlivého, odolného a bezpečného systému doménových jmen jsou klíčovým faktorem pro zachování integrity internetu a jsou nezbytné pro jeho nepřetržitý a stabilní provoz, na kterém závisí digitální ekonomika a společnost. Tato směrnice by se proto měla vztahovat na ***všechny poskytovatele služeb systému doménových jmen v celém řetězci řešení systému*** doménových jmen***, včetně operátorů kořenových jmenných serverů, serverů internetových domén nejvyšší úrovně, autoritativních jmenných serverů pro doménová jména a rekurzivních resolverů***.	(15) Podpora a ochrana spolehlivého, odolného a bezpečného systému doménových jmen jsou klíčovým faktorem pro zachování integrity internetu a jsou nezbytné pro jeho nepřetržitý a stabilní provoz, na kterém závisí digitální ekonomika a společnost. Tato směrnice by se proto měla vztahovat na ***servery internetových domén nejvyšší úrovně, veřejně dostupné rekurzivní služby pro překlad*** doménových jmen ***pro koncové uživatele internetu a autoritativní služby pro překlad doménových jmen. Tato směrnice se nevztahuje na kořenové jmenné servery***.

Pozměňovací návrh 16

Návrh směrnice
Bod odůvodnění 19

Znění navržené Komisí	*Pozměňovací návrh*
(19) Poskytovatelé poštovních služeb ve smyslu směrnice Evropského parlamentu a Rady 97/67/ES[18] a rovněž poskytovatelé expresních a kurýrních doručovacích služeb by měli této směrnici podléhat,	(19) Poskytovatelé poštovních služeb ve smyslu směrnice Evropského parlamentu a Rady 97/67/ES[18] a rovněž poskytovatelé expresních a kurýrních doručovacích služeb by měli této směrnici podléhat,

pokud poskytují alespoň jeden z kroků v poštovním řetězci, a zejména výběr, třídění nebo dodání, včetně služeb souvisejících s vyzvedáváním. Přepravní služby, které nejsou poskytovány ve spojení s některým z těchto kroků, by neměly spadat do oblasti působnosti poštovních služeb.	pokud poskytují alespoň jeden z kroků v poštovním řetězci, a zejména výběr, třídění nebo dodání, včetně služeb souvisejících s vyzvedáváním***, a současně by měla být zohledněna míra jejich závislosti na síťových a informačních systémech***. Přepravní služby, které nejsou poskytovány ve spojení s některým z těchto kroků, by neměly spadat do oblasti působnosti poštovních služeb.
[18] Směrnice Evropského parlamentu a Rady 97/67/ES ze dne 15. prosince 1997 o společných pravidlech pro rozvoj vnitřního trhu poštovních služeb Společenství a zvyšování kvality služby (Úř. věst. L 15, 21.1.1998, s. 14).	[18] Směrnice Evropského parlamentu a Rady 97/67/ES ze dne 15. prosince 1997 o společných pravidlech pro rozvoj vnitřního trhu poštovních služeb Společenství a zvyšování kvality služby (Úř. věst. L 15, 21.1.1998, s. 14).

Pozměňovací návrh 17

Návrh směrnice
Bod odůvodnění 20

Znění navržené Komisí	*Pozměňovací návrh*
(20) Tyto rostoucí vzájemné závislosti jsou výsledkem stále více přeshraniční a vzájemně propojené sítě poskytování služeb pomocí klíčových infrastruktur v celé Unii v odvětvích energetiky, dopravy, digitální infrastruktury, pitné a odpadní vody, zdravotnictví, některých prvků veřejné správy a rovněž vesmíru, pokud jde o poskytování určitých služeb závisejících na pozemních infrastrukturách, které vlastní, řídí a provozují buď členské státy, nebo soukromé subjekty, a proto nezahrnují infrastruktury vlastněné, řízené a provozované Unií nebo jménem Unie v rámci jejích vesmírných programů. Tyto vzájemné závislosti znamenají, že jakékoli narušení hospodářské soutěže, a dokonce i takové narušení, které je původně omezeno na jeden subjekt nebo jedno odvětví, může mít širší dominové účinky, jež mohou potenciálně mít dalekosáhlé negativní	(20) Tyto rostoucí vzájemné závislosti jsou výsledkem stále více přeshraniční a vzájemně propojené sítě poskytování služeb pomocí klíčových infrastruktur v celé Unii v odvětvích energetiky, dopravy, digitální infrastruktury, pitné a odpadní vody, zdravotnictví, některých prvků veřejné správy a rovněž vesmíru, pokud jde o poskytování určitých služeb závisejících na pozemních infrastrukturách, které vlastní, řídí a provozují buď členské státy, nebo soukromé subjekty, a proto nezahrnují infrastruktury vlastněné, řízené a provozované Unií nebo jménem Unie v rámci jejích vesmírných programů. Tyto vzájemné závislosti znamenají, že jakékoli narušení hospodářské soutěže, a dokonce i takové narušení, které je původně omezeno na jeden subjekt nebo jedno odvětví, může mít širší dominové účinky, jež mohou potenciálně mít dalekosáhlé negativní

dopady na poskytování služeb na celém vnitřním trhu. Pandemie COVID-19 ***prokázala*** zranitelnost našich stále více vzájemně závislých společností, jsou-li vystaveny málo pravděpodobným rizikům.	dopady na poskytování služeb na celém vnitřním trhu. ***Vystupňované útoky na síťové a informační systémy během*** pandemie COVID-19 ***poukázaly na*** zranitelnost našich stále více vzájemně závislých společností, jsou-li vystaveny málo pravděpodobným rizikům.

Pozměňovací návrh 18

Návrh směrnice
Bod odůvodnění 24

Znění navržené Komisí	*Pozměňovací návrh*
(24) Členské státy by měly být náležitě vybaveny jak po technické, tak po organizační stránce, aby mohly předcházet incidentům a rizikům spojeným se sítěmi a informačními systémy, odhalovat je, reagovat na ně a zmírňovat je. Členské státy by proto měly ***zajistit, aby dobře fungovaly jejich týmy CSIRT, rovněž označované jako týmy CERT (týmy pro reakci na počítačové hrozby)***, ***které budou splňovat*** základní požadavky***,*** tak aby byly zaručeny jejich efektivní a kompatibilní schopnosti řešit incidenty a rizika a aby byla zajištěna účinná spolupráce na úrovni Unie. V zájmu posílení důvěry mezi subjekty a týmy CSIRT v případech, kdy je tým CSIRT součástí příslušného orgánu, by členské státy měly zvážit funkční oddělení operativních úkolů plněných týmy CSIRT, zejména v souvislosti se sdílením informací a podporou poskytovanou subjektům, od činností příslušných orgánů v oblasti dohledu.	(24) Členské státy by měly být náležitě vybaveny jak po technické, tak po organizační stránce, aby mohly předcházet incidentům a rizikům spojeným se sítěmi a informačními systémy, odhalovat je, reagovat na ně a zmírňovat je. Členské státy by proto měly ***na základě této směrnice určit jeden nebo více týmů CSIRT a zajistit, aby dobře fungovaly***, ***splňovaly*** základní požadavky tak***,*** aby byly zaručeny jejich efektivní a kompatibilní schopnosti řešit incidenty a rizika a aby byla zajištěna účinná spolupráce na úrovni Unie***. Členské státy mohou jako týmy CSIRT určit stávající týmy pro reakci na počítačové hrozby (CERT).*** V zájmu posílení důvěry mezi subjekty a týmy CSIRT v případech, kdy je tým CSIRT součástí příslušného orgánu, by členské státy měly zvážit funkční oddělení operativních úkolů plněných týmy CSIRT, zejména v souvislosti se sdílením informací a podporou poskytovanou subjektům, od činností příslušných orgánů v oblasti dohledu.

Pozměňovací návrh 19

Návrh směrnice
Bod odůvodnění 25

Znění navržené Komisí	*Pozměňovací návrh*
(25) Pokud jde o osobní údaje, týmům CSIRT by mělo být umožněno, aby v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679[19] jménem a na žádost subjektu podle této směrnice aktivně prohledávaly sítě a informační systémy, které používá k poskytování svých služeb. Členské státy by se měly zaměřit na to, aby všem odvětvovým týmům CSIRT zajistily stejné technické podmínky. Při budování vnitrostátních týmů CSIRT mohou členské státy požádat o součinnost Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA).	(25) Pokud jde o osobní údaje, týmům CSIRT by mělo být umožněno, aby v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679[19] jménem a na žádost subjektu podle této směrnice***, nebo v případě vážného ohrožení národní bezpečnosti,*** aktivně prohledávaly sítě a informační systémy, které používá k poskytování svých služeb. Členské státy by se měly zaměřit na to, aby všem odvětvovým týmům CSIRT zajistily stejné technické podmínky. Při budování vnitrostátních týmů CSIRT mohou členské státy požádat o součinnost Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA).
[19] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).	[19] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

Pozměňovací návrh 20

Návrh směrnice
Bod odůvodnění 25 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(25a) Týmy CSIRT by měly být na žádost subjektu schopny průběžně vyhledávat, spravovat a sledovat veškerá aktiva orientovaná na internet, a to jak v provozovnách, tak mimo ně, aby pochopily, jaké celkové riziko pro daný podnik vyplývá z nově objeveného ohrožení dodavatelského řetězce nebo kritických zranitelných míst. Informace o tom, zda subjekt provozuje privilegované

	rozhraní pro správu, ovlivňuje rychlost přijímání zmírňujících opatření.

Pozměňovací návrh 21

Návrh směrnice
Bod odůvodnění 26

Znění navržené Komisí	*Pozměňovací návrh*
(26) S ohledem na význam mezinárodní spolupráce na poli kybernetické bezpečnosti by týmy CSIRT měly mít možnost účastnit se kromě sítě CSIRT zřízené touto směrnicí také dalších sítí pro mezinárodní spolupráci.	(26) S ohledem na význam mezinárodní spolupráce na poli kybernetické bezpečnosti by týmy CSIRT měly mít možnost účastnit se kromě sítě CSIRT zřízené touto směrnicí také dalších sítí pro mezinárodní spolupráci***, včetně týmů CSIRT ze třetích zemí, pokud by docházelo ke vzájemné spolupráci, která by měla přínos pro bezpečnost občanů a subjektů, s cílem přispět k rozvoji standardů Unie, které mohou formovat podmínky v oblasti kybernetické bezpečnosti na mezinárodní úrovni***. ***Členské státy by rovněž mohly prozkoumat možnost prohloubení spolupráce s podobně smýšlejícími partnerskými zeměmi a mezinárodními organizacemi s cílem zajistit mnohostranné dohody o kybernetických normách, odpovědném chování státu a nestátních subjektů v kyberprostoru a účinné globální digitální správě, jakož i vytvořit otevřený, svobodný, stabilní a bezpečný kyberprostor založený na mezinárodním právu.***

Pozměňovací návrh 22

Návrh směrnice
Bod odůvodnění 26 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(26a) Politiky v oblasti kybernetické hygieny poskytují základy pro ochranu infrastruktur sítí a informačních systémů,

	hardwaru, softwaru a bezpečnosti aplikací on-line a údajů o podnicích nebo o koncových uživatelích, na něž se subjekty spoléhají. Politiky v oblasti kybernetické hygieny zahrnující společný základní soubor postupů, mimo jiné aktualizace softwaru a hardwaru, změny hesel, řízení nových instalací, omezení přístupových účtů na úrovni administrátorů a zálohování údajů, umožňují proaktivní rámec připravenosti a celkové bezpečnosti a ochrany v případě incidentů nebo hrozeb. Agentura ENISA by měla sledovat a hodnotit politiky členských států v oblasti kybernetické hygieny a zkoumat režimy na úrovni EU, které by umožňovaly přeshraniční kontroly zajišťující rovnocennost nezávisle na požadavcích členských států.

Pozměňovací návrh 23

Návrh směrnice
Bod odůvodnění 26 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(26b) Využívání umělé inteligence (UI) v kybernetické bezpečnosti má potenciál zlepšit odhalování a zastavit útoky na sítě a informační systémy, a umožnit tak přesun zdrojů směrem k důmyslnějším útokům. Členské státy by proto měly ve svých vnitrostátních strategiích podporovat využívání (polo)automatizovaných nástrojů v oblasti kybernetické bezpečnosti a sdílení údajů potřebných pro odbornou přípravu a zlepšování automatizovaných nástrojů v oblasti kybernetické bezpečnosti. Za účelem zmírnění rizika nepřiměřeného zásahu do práv a svobod jednotlivců, které mohou systémy využívající umělou inteligenci představovat, se použijí požadavky na záměrnou a standardní ochranu údajů stanovené v článku 25 nařízení (EU) 2016/679. Tato rizika by

mohla dále být zmírněna začleněním vhodných záruk, jako je pseudonymizace, šifrování, přesnost údajů a minimalizace údajů.

Pozměňovací návrh 24

Návrh směrnice
Bod odůvodnění 26 c (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(26c) Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem přispívají k vyšší míře transparentnosti a mají pozitivní dopad na účinnost průmyslové inovace. Otevřené normy usnadňují interoperabilitu mezi bezpečnostními nástroji a přispívají k bezpečnosti odvětvových zúčastněných stran. Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou pomáhat širší komunitě vývojářů, a umožnit tak jednotlivým subjektům uplatňovat diverzifikaci prodejců a strategie otevřené bezpečnosti. Otevřená bezpečnost může vést k transparentnějšímu procesu ověřování nástrojů souvisejících s kybernetickou bezpečností a ke komunitnímu procesu zjišťování zranitelných míst. Členské státy by proto měly podporovat přijímání softwaru s otevřeným zdrojovým kódem a otevřených standardů tím, že budou provádět politiky spojené s využíváním otevřených dat a otevřených zdrojů v rámci koncepce „bezpečnost prostřednictvím transparentnosti“. Politiky, které podporují přijímání a udržitelné využívání nástrojů kybernetické bezpečnosti s otevřeným zdrojovým kódem, mají zvláštní význam pro malé a střední podniky, které se potýkají se značnými prováděcími náklady, jež by bylo možné minimalizovat tím, že bude zapotřebí méně specifických aplikací nebo nástrojů.

Pozměňovací návrh 25

Návrh směrnice
Bod odůvodnění 26 d (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(26d) Partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti mohou poskytnout vhodný rámec pro výměnu znalostí, sdílení osvědčených postupů a zavedení společné úrovně porozumění mezi všemi zúčastněnými stranami. Členské státy by měly v rámci svých národních strategií kybernetické bezpečnosti přijmout politiky na podporu vytváření partnerství veřejného a soukromého sektoru specificky zaměřených na kybernetickou bezpečnost. Tyto politiky by měly mimo jiné vyjasnit rozsah a zúčastněné strany, model řízení, dostupné možnosti financování a interakci mezi zúčastněnými stranami. Partnerství veřejného a soukromého sektoru mohou využít odborné znalosti subjektů ze soukromého sektoru na podporu příslušných orgánů členských států při vývoji špičkových služeb a procesů, mimo jiné včetně výměny informací, včasného varování, nácviků kybernetických hrozeb a incidentů, krizového řízení a plánování odolnosti.

Pozměňovací návrh 26

Návrh směrnice
Bod odůvodnění 27

Znění navržené Komisí	*Pozměňovací návrh*
(27) V souladu s přílohou doporučení Komise (EU) 2017/1548 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (dále jen „plán“)[20] by rozsáhlý incident měl	(27) V souladu s přílohou doporučení Komise (EU) 2017/1548 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (dále jen „plán“)20 by rozsáhlý incident měl

označovat incident s významným dopadem na nejméně dva členské státy nebo takový incident, při kterém narušení přesahuje schopnost členského státu na něj reagovat. V závislosti na jejich příčině a dopadu mohou rozsáhlé incidenty eskalovat a přejít ve skutečné krize, jež neumožní řádné fungování vnitřního trhu. Vzhledem k širokému dopadu a ve většině případů i přeshraniční povaze takových incidentů by členské státy a příslušné orgány, instituce a agentury Unie měly na technické, operativní a politické úrovni spolupracovat a odpovídajícím způsobem koordinovat reakci v celé Unii.	označovat incident s významným dopadem na nejméně dva členské státy nebo takový incident, při kterém narušení přesahuje schopnost členského státu na něj reagovat. V závislosti na jejich příčině a dopadu mohou rozsáhlé incidenty eskalovat a přejít ve skutečné krize, jež neumožní řádné fungování vnitřního trhu ***nebo představují vážná rizika pro veřejnou bezpečnost subjektů nebo občanů v několika členských státech nebo v Unii jako celku***. Vzhledem k širokému dopadu a ve většině případů i přeshraniční povaze takových incidentů by členské státy a příslušné orgány, instituce a agentury Unie měly na technické, operativní a politické úrovni spolupracovat a odpovídajícím způsobem koordinovat reakci v celé Unii.
[20] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).	[20] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

Pozměňovací návrh 27

Návrh směrnice
Bod odůvodnění 27 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(27a) Členské státy by se měly ve svých národních strategiích kybernetické bezpečnosti zabývat specifickými potřebami malých a středních podniků v oblasti kybernetické bezpečnosti. Malé a střední podniky představují v rámci Unie významný podíl průmyslového a obchodního trhu a často mají problém přizpůsobit se novým obchodním postupům v propojenějším světě, orientovat se v digitálním prostředí v situaci, kdy zaměstnanci pracují z domova a obchodní činnost stále častěji probíhá on-line. Některé malé a střední podniky

čelí specifickým problémům v oblasti kybernetické bezpečnosti, jako je nízké povědomí o kybernetickém prostoru, nedostatečná bezpečnost IT na dálku, vysoké náklady na řešení v oblasti kybernetické bezpečnosti a zvýšená míra ohrožení, například ransomware, v souvislosti s nimiž by se jim mělo dostat vedení a podpory. Členské státy by měly zavést jednotné kontaktní místo pro kybernetickou bezpečnost pro malé a střední podniky, které malým a středním podnikům buď poskytne vedení a podporu, nebo je nasměruje k příslušným subjektům pro vedení a podporu v otázkách týkajících se kybernetické bezpečnosti. Členské státy jsou vybízeny, aby malým podnikům a mikropodnikům, které nemají příslušné kapacity, nabízely také služby, jako je konfigurace internetových stránek a vedení protokolů.

Pozměňovací návrh 28

Návrh směrnice
Bod odůvodnění 27 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(27b) Členské státy by měly v rámci svých národních strategií kybernetické bezpečnosti přijmout politiky na podporu aktivní kybernetické obrany. Aktivní kybernetická obrana je proaktivní prevence, zjišťování, monitorování, analýza a zmírňování narušení bezpečnosti sítě v kombinaci s využitím schopností nasazených v síti, která je předmětem útoku, i mimo ni. Má-li být možné vyvíjet jednotné úsilí o úspěšné odhalování, prevenci a řešení útoků proti sítím a informačním systémům, je zásadně důležitá schopnost rychle a automaticky sdílet a chápat informace a analýzy týkající se hrozeb, varování v souvislosti s kybernetickými aktivitami a opatření reakce. Aktivní kybernetická obrana

spočívá na obranné strategii, která vylučuje útočná opatření proti kritické civilní infrastruktuře.

Pozměňovací návrh 29

Návrh směrnice
Bod odůvodnění 28

Znění navržené Komisí	*Pozměňovací návrh*
(28) Využití zranitelných míst v sítích a informačních systémech může způsobit vážná narušení a škody, a rychlé určení a náprava těchto zranitelností je proto důležitým faktorem při snižování kybernetických bezpečnostních rizik. Subjekty, které takové systémy vyvíjejí, by proto měly stanovit vhodné postupy k řešení zranitelných míst, jakmile jsou zjištěna. Jelikož zranitelná místa jsou často zjištěna a ohlášena (odhalena) třetími stranami (subjekty ohlašujícími incidenty), výrobce nebo poskytovatel produktů nebo služeb IKT by měl rovněž zavést nezbytné postupy pro získávání informací o zranitelných místech od třetích stran. Vodítko pro řešení zranitelností a odhalování zranitelností v této souvislosti poskytují mezinárodní normy ISO/IEC 30111 a ISO/IEC 29417. ***Pokud jde o*** odhalování ***zranitelných míst,*** je ***obzvláště důležitá*** koordinace mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT. Koordinované odhalování zranitelností specifikuje strukturovaný proces, jehož prostřednictvím jsou zranitelná místa hlášena organizacím takovým způsobem, který organizaci umožní diagnostikovat a odstranit zranitelnost dříve, než budou podrobné informace o ní sděleny třetím stranám nebo veřejnosti. Koordinované odhalování zranitelností by také mělo zahrnovat koordinaci mezi subjektem ohlašujícím incidenty a organizací, pokud jde	(28) Využití zranitelných míst v sítích a informačních systémech může způsobit vážná narušení a škody, a rychlé určení a náprava těchto zranitelností je proto důležitým faktorem při snižování kybernetických bezpečnostních rizik. Subjekty, které takové systémy vyvíjejí, by proto měly stanovit vhodné postupy k řešení zranitelných míst, jakmile jsou zjištěna. Jelikož zranitelná místa jsou často zjištěna a ohlášena (odhalena) třetími stranami (subjekty ohlašujícími incidenty), výrobce nebo poskytovatel produktů nebo služeb IKT by měl rovněž zavést nezbytné postupy pro získávání informací o zranitelných místech od třetích stran. Vodítko pro řešení zranitelností a odhalování zranitelností v této souvislosti poskytují mezinárodní normy ISO/IEC 30111 a ISO/IEC 29417. ***Pro usnadnění dobrovolného rámce pro*** odhalování ***zranitelností*** je ***zvláště důležité posílení*** koordinace mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT. Koordinované odhalování zranitelností specifikuje strukturovaný proces, jehož prostřednictvím jsou zranitelná místa hlášena organizacím takovým způsobem, který organizaci umožní diagnostikovat a odstranit zranitelnost dříve, než budou podrobné informace o ní sděleny třetím stranám nebo veřejnosti. Koordinované odhalování zranitelností by také mělo zahrnovat koordinaci mezi subjektem ohlašujícím incidenty a organizací, pokud

o načasování odstranění a zveřejnění zranitelných míst.	jde o načasování odstranění a zveřejnění zranitelných míst.

Pozměňovací návrh 30

Návrh směrnice
Bod odůvodnění 28 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(28a) Komise, agentura ENISA a členské státy by měly i nadále podporovat mezinárodní sbližování s normami a stávajícími odvětvovými osvědčenými postupy v oblasti řízení rizik, např. v oblastech posuzování bezpečnosti dodavatelského řetězce, sdílení informací a odhalování zranitelností.

Pozměňovací návrh 31

Návrh směrnice
Bod odůvodnění 29

Znění navržené Komisí	*Pozměňovací návrh*
(29) Členské státy by proto měly stanovit příslušnou vnitrostátní politiku a přijmout tak opatření k usnadnění koordinovaného odhalování zranitelností. V této ***souvislosti*** by členské státy měly ***určit tým CSIRT***, ***který převezme úlohu „koordinátora“ a v případě potřeby bude působit jako zprostředkovatel mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT***. ***Úkoly koordinátora týmů CSIRT by měly zahrnovat zejména určení*** a ***kontaktování dotčených subjektů***, ***podporu subjektů ohlašujících incidenty***, ***dojednávání harmonogramů odhalení a řízení zranitelností, které se dotýkají mnoha organizací (odhalování zranitelností ohrožujících více stran)***. ***Pokud se zranitelná místa dotýkají více výrobců***	(29) Členské státy by proto měly ***ve spolupráci s agenturou ENISA*** stanovit příslušnou vnitrostátní politiku a přijmout tak opatření k usnadnění koordinovaného odhalování zranitelností. V ***rámci*** této ***vnitrostátní politiky*** by členské státy měly ***řešit problémy***, s ***nimiž se potýkají výzkumní pracovníci zabývající se zranitelností***. ***Subjekty*** a ***fyzické osoby***, ***které zkoumají zranitelnosti***, ***mohou být v některých členských státech vystaveny trestní a občanskoprávní odpovědnosti***. ***Členské státy*** jsou ***proto vybízeny, aby vydaly pokyny týkající se nestíhání výzkumu v oblasti bezpečnosti informací a vynětí těchto činností z občanskoprávní odpovědnosti***.

nebo poskytovatelů produktů nebo služeb IKT, kteří jsou ***usazení ve více než jednom členském státě, určené týmy CSIRT z každého z dotčených členských států by měly spolupracovat v rámci sítě CSIRT***.

Pozměňovací návrh 32

Návrh směrnice
Bod odůvodnění 29 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(29a) Členské státy by měly určit tým CSIRT, který převezme úlohu „koordinátora“ a v případě potřeby bude působit jako zprostředkovatel mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů či služeb IKT, u nichž je pravděpodobné, že budou zranitelnostmi dotčeny. K úkolům koordinátora by mělo patřit zejména určení a kontaktování dotčených subjektů, podpora subjektů ohlašujících incidenty, dojednávání harmonogramů odhalení a řízení zranitelností, které se dotýkají více organizací (odhalování zranitelností ohrožujících více stran). Pokud se zranitelnosti dotýkají více výrobců nebo poskytovatelů produktů či služeb IKT, kteří jsou usazeni ve více než jednom členském státě, určené týmy CSIRT z každého z dotčených členských států by měly v rámci sítě CSIRT spolupracovat.

Pozměňovací návrh 33

Návrh směrnice
Bod odůvodnění 30

Znění navržené Komisí	*Pozměňovací návrh*
(30) Přístup ke správným a včasným informacím o zranitelnostech dotýkajících se produktů a služeb IKT přispívá	(30) Přístup ke správným a včasným informacím o zranitelnostech dotýkajících se produktů a služeb IKT přispívá

k zesílenému řízení kybernetických bezpečnostních rizik. V ***této souvislosti jsou*** zdroje veřejně přístupných informací o zranitelných místech důležitým nástrojem pro subjekty a jejich uživatele, ale i pro příslušné vnitrostátní orgány ***v Unii*** a týmy CSIRT. Z tohoto důvodu by agentura ENISA měla ***zavést registr*** zranitelností, kde základní a důležité subjekty a jejich dodavatelé, a stejně tak i subjekty, které nespadají do oblasti působnosti této směrnice, mohou na základě dobrovolnosti odhalovat zranitelná místa a poskytovat o nich informace, jež uživatelům umožní přijímat vhodná opatření ke zmírnění dopadů.	k zesílenému řízení kybernetických bezpečnostních rizik. Zdroje veřejně přístupných informací o zranitelných místech ***jsou*** důležitým nástrojem pro subjekty a jejich uživatele, ale i pro příslušné vnitrostátní orgány a týmy CSIRT. Z tohoto důvodu by agentura ENISA měla ***vytvořit databázi*** zranitelností, kde základní a důležité subjekty a jejich dodavatelé, a stejně tak i subjekty, které nespadají do oblasti působnosti této směrnice, mohou na základě dobrovolnosti odhalovat zranitelná místa a poskytovat o nich informace, jež uživatelům umožní přijímat vhodná opatření ke zmírnění dopadů. ***Tato databáze má za cíl zabývat se jedinečnými výzvami, které představují rizika v oblasti kybernetické bezpečnosti pro evropské subjekty. Agentura ENISA by nadto měla zavést odpovědný postup týkající se procesu zveřejňování, který poskytne subjektům čas k přijetí opatření zmírňujících jejich zranitelnosti, a uplatňovat nejmodernější opatření v oblasti kybernetické bezpečnosti a strojově čitelné datové soubory a odpovídající rozhraní (API). V zájmu podpory kultury odhalování zranitelností by odhalení nemělo způsobit újmu ohlašujícímu subjektu.***

Pozměňovací návrh 34

Návrh směrnice
Bod odůvodnění 31

Znění navržené Komisí	*Pozměňovací návrh*
(31) ***Ačkoli podobné registry nebo databáze zranitelností existují, jsou hostovány a spravovány subjekty, které nejsou usazeny v Unii. Evropský registr zranitelností spravovaný*** agenturou ENISA by ***poskytl lepší transparentnost procesu odhalování předtím***, ***než je zranitelné místo oficiálně zveřejněno, a odolnost***	(31) ***Evropská*** databáze zranitelností ***spravovaná*** agenturou ENISA by ***měla prostřednictvím svého rámce pro určování***, ***sledování a bodování zranitelností využívat společný registr zranitelností a expozic (CVE). V zájmu zabránění zdvojování činnosti a*** úsilí o ***doplňkovost*** by agentura ENISA měla

v případech narušení nebo přerušení poskytování podobných služeb. S cílem zabránit zdvojení úsilí ***a v co největší možné míře usilovat*** o ***komplementaritu,*** by agentura ENISA měla zkoumat možnost uzavření strukturovaných dohod o spolupráci s podobnými registry v jurisdikcích třetích zemí.	***dále*** zkoumat možnost uzavření strukturovaných dohod o spolupráci s ***dalšími*** podobnými registry ***nebo databázemi v*** jurisdikcích třetích zemí.

Pozměňovací návrh 35

Návrh směrnice
Bod odůvodnění 33

Znění navržené Komisí	*Pozměňovací návrh*
(33) Při vypracování pokynů by skupina pro spolupráci měla důsledně: mapovat vnitrostátní řešení a zkušenosti, posuzovat dopad výstupů skupiny pro spolupráci na přístupy členských států, diskutovat o problémech spojených s prováděním a formulovat konkrétní doporučení, která je třeba zohlednit prostřednictvím lepšího provádění stávajících pravidel.	(33) Při vypracování pokynů by skupina pro spolupráci měla důsledně: mapovat vnitrostátní řešení a zkušenosti, posuzovat dopad výstupů skupiny pro spolupráci na přístupy členských států, diskutovat o problémech spojených s prováděním a formulovat konkrétní doporučení **–** ***zejména pokud jde o usnadnění harmonizace při provádění této směrnice mezi členskými státy*** **–**, která je třeba zohlednit prostřednictvím lepšího provádění stávajících pravidel. V ***zájmu podpory kompatibility řešení v oblasti kybernetické bezpečnosti uplatňovaných v jednotlivých odvětvích v celé Unii by měla skupina pro spolupráci rovněž mapovat vnitrostátní řešení. To je obzvláště důležité pro odvětví, která jsou ze své povahy mezinárodní a přeshraniční.***

Pozměňovací návrh 36

Návrh směrnice
Bod odůvodnění 34

Znění navržené Komisí	*Pozměňovací návrh*
(34) Skupina pro spolupráci by i nadále	(34) Skupina pro spolupráci by i nadále

měla být flexibilním fórem a měla by být schopna reagovat na měnící se a nové priority a výzvy politik, a přitom brát v úvahu dostupnost zdrojů. Měla by organizovat pravidelná společná setkání s relevantními soukromými zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou a shromažďování vstupů týkajících se vznikajících politických výzev. S cílem posílit spolupráci na úrovni Unie by skupina měla zvážit pozvání k účasti na její činnosti pro instituce a agentury Unie zapojené do politiky v oblasti kybernetické bezpečnosti, jako je ***Evropské centrum pro boj proti kyberkriminalitě (EC3)***, Agentura Evropské unie pro bezpečnost letectví (EASA) a Agentura Evropské unie pro kosmický program (EUSPA).	měla být flexibilním fórem a měla by být schopna reagovat na měnící se a nové priority a výzvy politik, a přitom brát v úvahu dostupnost zdrojů. Měla by organizovat pravidelná společná setkání s relevantními soukromými zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou a shromažďování vstupů týkajících se vznikajících politických výzev. S cílem posílit spolupráci na úrovni Unie by skupina měla zvážit pozvání k účasti na její činnosti pro ***příslušné*** instituce a agentury Unie zapojené do politiky v oblasti kybernetické bezpečnosti, jako je ***Europol***, Agentura Evropské unie pro bezpečnost letectví (EASA) a Agentura Evropské unie pro kosmický program (EUSPA).

Pozměňovací návrh 37

Návrh směrnice
Bod odůvodnění 35

Znění navržené Komisí	*Pozměňovací návrh*
(35) ***Příslušné orgány*** a ***týmy CSIRT*** by měly být zmocněny ***se účastnit*** výměnných ***programů*** pro úředníky z jiných členských států ***za účelem zlepšení spolupráce***. Příslušné orgány by měly přijmout nezbytná opatření, jež umožní úředníkům z jiných členských států účinně se zapojit do činností hostitelského příslušného orgánu.	(35) ***Za účelem zlepšení spolupráce*** a ***posílení důvěry mezi členskými státy*** by měly být ***příslušné orgány a týmy CSIRT*** zmocněny k ***účasti na*** výměnných ***programech*** pro úředníky z jiných členských států***, a to v mezích strukturovaných pravidel a mechanismů, které zakládají oblast působnosti a případně požadovanou bezpečnostní prověrku úředníků účastnících se těchto výměnných programů***. Příslušné orgány by měly přijmout nezbytná opatření, jež umožní úředníkům z jiných členských států účinně se zapojit do činností hostitelského příslušného orgánu ***nebo týmu CSIRT***.

Pozměňovací návrh 38

Návrh směrnice
Bod odůvodnění 36

Znění navržené Komisí	*Pozměňovací návrh*
(36) Unie by ve vhodných případech měla v souladu s článkem 218 SFEU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a zorganizují jejich účast na některých činnostech skupiny pro spolupráci a sítě CSIRT. Takové dohody by měly zajistit odpovídající ochranu údajů.	(36) Unie by ve vhodných případech měla v souladu s článkem 218 SFEU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a zorganizují jejich účast na některých činnostech skupiny pro spolupráci a sítě CSIRT. Takové dohody by měly zajistit ***zájmy Unie a*** odpovídající ochranu údajů. ***Tím není dotčeno právo členských států spolupracovat s podobně smýšlejícími třetími zeměmi na řízení zranitelností a řízení rizik v oblasti kybernetické bezpečnosti, jež usnadní podávání zpráv a obecné sdílení informací v souladu s právem Unie.***

Pozměňovací návrh 39

Návrh směrnice
Bod odůvodnění 38

Znění navržené Komisí	*Pozměňovací návrh*
(38) Pro účely této směrnice by pojem „riziko“ měl poukazovat na možnost ztráty nebo narušení způsobených kybernetickým bezpečnostním incidentem a měl by být vyjádřen jako kombinace rozsahu takové ztráty nebo narušení a pravděpodobnosti vzniku uvedeného incidentu.	***vypouští se***

Pozměňovací návrh 40

Návrh směrnice
Bod odůvodnění 39

Znění navržené Komisí	*Pozměňovací návrh*
(39) Pro účely této směrnice by pojem	***vypouští se***

„případy, kdy téměř došlo k incidentu“ měl poukazovat na událost, která by mohla potenciálně způsobit škodu, ale jejímu plnému projevení bylo úspěšně zabráněno.

Pozměňovací návrh 41

Návrh směrnice
Bod odůvodnění 40

Znění navržené Komisí	*Pozměňovací návrh*
(40) Opatření pro řízení rizik by měla zahrnovat opatření pro určení veškerých rizik incidentů, předcházení incidentům, jejich odhalování ***a řešení*** a zmírňování jejich dopadu. Bezpečnost sítí a informačních systémů by měla zahrnovat bezpečnost uchovávaných, předávaných a zpracovávaných údajů.	(40) Opatření pro řízení rizik by měla zahrnovat opatření pro určení veškerých rizik incidentů, předcházení incidentům, jejich odhalování***, reakci na ně, zotavení se z nich*** a zmírňování jejich dopadu. Bezpečnost sítí a informačních systémů by měla zahrnovat bezpečnost uchovávaných, předávaných a zpracovávaných údajů. V ***zájmu získání úplného obrazu o bezpečnosti informačního systému by měly tyto systémy zajistit systémovou analýzu, rozčleněnou podle jednotlivých procesů a interakcí mezi subsystémy a zohledňující lidský faktor.***

Pozměňovací návrh 42

Návrh směrnice
Bod odůvodnění 41

Znění navržené Komisí	*Pozměňovací návrh*
(41) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na základní a důležité subjekty nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření.	(41) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na základní a důležité subjekty nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření ***a evropských nebo mezinárodních norem, jako jsou ISO31000 a ISA/IEC 27005***.

Pozměňovací návrh 43

Návrh směrnice
Bod odůvodnění 43

Znění navržené Komisí	*Pozměňovací návrh*
(43) Řešení kybernetických bezpečnostních rizik vyplývajících z dodavatelského řetězce subjektu nebo jeho vztahů s dodavateli je zvlášť důležité vzhledem k počtu incidentů, kdy se subjekty staly obětí ***kybernetických útoků*** a kdy nepřátelské subjekty byly schopny narušit bezpečnost sítí a informačních systémů daného subjektu tím, že využily zranitelných míst v produktech a službách třetí strany. Subjekty by proto měly posoudit a zohlednit celkovou kvalitu produktů a postupů kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů k zajištění bezpečného vývoje.	(43) Řešení kybernetických bezpečnostních rizik vyplývajících z dodavatelského řetězce subjektu nebo jeho vztahů s dodavateli***, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo řízených bezpečnostních služeb,*** je zvlášť důležité vzhledem k počtu incidentů, kdy se subjekty staly obětí ***útoků na sítě a informační systémy*** a kdy nepřátelské subjekty byly schopny narušit bezpečnost sítí a informačních systémů daného subjektu tím, že využily zranitelných míst v produktech a službách třetí strany. Subjekty by proto měly posoudit a zohlednit celkovou kvalitu a ***odolnost*** produktů a ***služeb, opatření v oblasti kybernetické bezpečnosti, která zahrnují, a*** postupů kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů k zajištění bezpečného vývoje. ***Subjekty by měly být zejména vybízeny, aby začlenily opatření v oblasti kybernetické bezpečnosti do smluvních ujednání se svými přímými dodavateli a poskytovateli služeb. Subjekty by mohly přihlížet k rizikům v oblasti kybernetické bezpečnosti, jež mají původ u dodavatelů a poskytovatelů služeb dalších úrovní.***

Pozměňovací návrh 44

Návrh směrnice
Bod odůvodnění 44

Znění navržené Komisí	*Pozměňovací návrh*
(44) Mezi poskytovateli služeb mají	(44) Mezi poskytovateli služeb mají

zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o odhalování a řešení incidentů poskytovatelé řízených bezpečnostních služeb v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Tito poskytovatelé řízených bezpečnostních služeb však jsou rovněž sami cíli kybernetických útoků a kvůli své úzké integraci do provozu operátorů představují zvlášť vysoké kybernetické bezpečnostní riziko. Subjekty by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat se zvýšenou pečlivostí.	zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o ***prevenci,*** odhalování a řešení incidentů ***a zotavení se z nich*** poskytovatelé řízených bezpečnostních služeb v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Tito poskytovatelé řízených bezpečnostních služeb však jsou rovněž sami cíli kybernetických útoků a kvůli své úzké integraci do provozu operátorů představují zvlášť vysoké kybernetické bezpečnostní riziko. Subjekty by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat se zvýšenou pečlivostí.

Pozměňovací návrh 45

Návrh směrnice
Bod odůvodnění 45

Znění navržené Komisí	*Pozměňovací návrh*
(45) Subjekty by rovněž měly řešit kybernetická bezpečnostní rizika vyplývající z jejich interakcí a vztahů s jinými zúčastněnými stranami v rámci širšího ekosystému. Subjekty by zejména měly přijetím vhodných opatření zajistit, že jejich spolupráce s akademickými a výzkumnými institucemi probíhá v souladu s jejich politikami kybernetické bezpečnosti a řídí se osvědčenými postupy, pokud jde o bezpečný přístup a šíření informací obecně a ochranu duševního vlastnictví zvláště. Podobně by subjekty, jsou-li závislé na službách transformace dat a analýzy dat poskytovaných třetími stranami, vzhledem k důležitosti a hodnotě dat pro jejich činnost měly přijmout veškerá vhodná opatření v oblasti kybernetické bezpečnosti.	(45) Subjekty by rovněž měly řešit kybernetická bezpečnostní rizika vyplývající z jejich interakcí a vztahů s jinými zúčastněnými stranami v rámci širšího ekosystému***, včetně boje proti průmyslové špionáži a ochrany obchodního tajemství***. Subjekty by zejména měly přijetím vhodných opatření zajistit, že jejich spolupráce s akademickými a výzkumnými institucemi probíhá v souladu s jejich politikami kybernetické bezpečnosti a řídí se osvědčenými postupy, pokud jde o bezpečný přístup a šíření informací obecně a ochranu duševního vlastnictví zvláště. Podobně by subjekty, jsou-li závislé na službách transformace dat a analýzy dat poskytovaných třetími stranami, vzhledem k důležitosti a hodnotě dat pro jejich činnost měly přijmout veškerá vhodná opatření v oblasti kybernetické bezpečnosti.

Pozměňovací návrh 46

Návrh směrnice
Bod odůvodnění 45 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(45a) Subjekty by měly přijmout širokou škálu základních postupů v oblasti kybernetické hygieny, k nimž patří architektura nulové důvěry, aktualizace softwaru, konfigurace zařízení, segmentace sítě, řízení identity a přístupu nebo povědomí uživatelů. Dále by měly pořádat školení pro své zaměstnance zaměřená na kybernetické hrozby spojené s podnikovým e-mailem, na phishing či na techniky sociálního inženýrství. Subjekty by dále měly hodnotit své vlastní schopnosti v oblasti kybernetické bezpečnosti a v zájmu automatizace svých schopností a ochrany síťové architektury případně usilovat o integraci technologií, které zvyšují kybernetickou bezpečnost a zakládají se na umělé inteligenci nebo systémech strojového učení.

Pozměňovací návrh 47

Návrh směrnice
Bod odůvodnění 46

Znění navržené Komisí	*Pozměňovací návrh*
(46) K dalšímu řešení klíčových rizik dodavatelského řetězce a na pomoc subjektům působícím v odvětvích, na něž se vztahuje tato směrnice, aby odpovídajícím způsobem řídily dodavatelský řetězec a kybernetická bezpečnostní rizika související s dodavateli, by skupina pro spolupráci, jež zahrnuje příslušné vnitrostátní orgány, ve spolupráci s Komisí a agenturou ENISA měla provést koordinovaná posouzení rizik	(46) K dalšímu řešení klíčových rizik dodavatelského řetězce a na pomoc subjektům působícím v odvětvích, na něž se vztahuje tato směrnice, aby odpovídajícím způsobem řídily dodavatelský řetězec a kybernetická bezpečnostní rizika související s dodavateli, by skupina pro spolupráci, jež zahrnuje příslušné vnitrostátní orgány, ve spolupráci s Komisí a agenturou ENISA měla provést koordinovaná posouzení rizik

dodavatelských řetězců ***v jednotlivých odvětvích***, jak bylo již provedeno pro sítě 5G v návaznosti na doporučení (EU) 2019/534 o kybernetické bezpečnosti sítí 5G[21], za účelem určení příslušných hrozeb a zranitelných míst v každém odvětví, v němž existují kritické služby ***IKT***, systémy nebo produkty IKT.	dodavatelských řetězců, jak bylo již provedeno pro sítě 5G v návaznosti na doporučení (EU) 2019/534 o kybernetické bezpečnosti sítí 5G[21], za účelem určení příslušných hrozeb a zranitelných míst v každém odvětví, v němž existují kritické služby, systémy nebo produkty IKT ***a IKS (informačních a komunikačních systémů)***. ***Uvedená posouzení rizik by měla určit opatření, plány zmírňování a osvědčené postupy ve vztahu ke kritickým závislostem, potenciálním jediným bodům selhání, hrozbám, zranitelnostem a dalším rizikům spojeným s dodavatelským řetězcem a měla by prozkoumat způsoby, jak subjekty dále podněcovat, aby je šířeji přijímaly. Potenciální netechnické rizikové faktory, jako je nepatřičný vliv třetí země na dodavatele a poskytovatele služeb, zejména v případě alternativních modelů správy, zahrnují skryté zranitelnosti nebo „zadní vrátka“ a možné systémové narušení dodávek, zejména v případě technologické závislosti nebo závislosti na poskytovateli.***
[21] Doporučení Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G (Úř. věst. L 88, 29.3.2019, s. 42).	[21] Doporučení Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G (Úř. věst. L 88, 29.3.2019, s. 42).

Pozměňovací návrh 48

Návrh směrnice
Bod odůvodnění 47

Znění navržené Komisí	*Pozměňovací návrh*
(47) Posouzení rizik dodavatelského řetězce by s ohledem na charakteristické rysy dotčeného odvětví měla zohlednit jak technické, tak případné netechnické faktory včetně faktorů vymezených v doporučení (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G	(47) Posouzení rizik dodavatelského řetězce by s ohledem na charakteristické rysy dotčeného odvětví měla zohlednit jak technické, tak případné netechnické faktory včetně faktorů vymezených v doporučení (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G

v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. K určení dodavatelských řetězců, které by měly podléhat koordinovanému posouzení rizik, by měla být vzata v úvahu tato kritéria: (i) rozsah, v jakém základní a důležité subjekty využívají konkrétní kritické služby, systémy a produkty IKT a jsou na nich závislé; (ii) relevantnost konkrétních služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; (iii) dostupnost alternativních služeb, systémů nebo produktů IKT; (iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT vůči narušení a v) u vznikajících služeb, systémů nebo produktů IKT jejich budoucí význam pro činnost subjektů.	v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. K určení dodavatelských řetězců, které by měly podléhat koordinovanému posouzení rizik, by měla být vzata v úvahu tato kritéria: (i) rozsah, v jakém základní a důležité subjekty využívají konkrétní kritické služby, systémy a produkty IKT a jsou na nich závislé; (ii) relevantnost konkrétních služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; (iii) dostupnost alternativních služeb, systémů nebo produktů IKT; (iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT ***během celého jejich životního cyklu*** vůči narušení a v) u vznikajících služeb, systémů nebo produktů IKT jejich budoucí význam pro činnost subjektů. ***Zvláštní důraz je třeba dále klást na služby, systémy nebo produkty IKT, které podléhají specifickým požadavkům pocházejícím z třetích zemí.***

Pozměňovací návrh 49

Návrh směrnice
Bod odůvodnění 47 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(47a) Skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti, zřízená podle článku 22 nařízení Evropského parlamentu a Rady (EU) 2019/881[1a], by měla vydat stanovisko k posouzení bezpečnostních rizik konkrétních kritických služeb, systémů nebo produktů IKT a IKS. Skupina pro spolupráci a agentura ENISA by měly k tomuto stanovisku přihlížet.
	[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 50

Návrh směrnice
Bod odůvodnění 50

Znění navržené Komisí	*Pozměňovací návrh*
(50) Vzhledem k rostoucímu významu interpersonálních komunikačních služeb nezávislých na číslech je nutné zajistit, aby i tyto služby podléhaly odpovídajícím bezpečnostním požadavkům v souladu s jejich zvláštní povahou a ekonomickým významem. Provozovatelé takových služeb by tedy měli rovněž zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Vzhledem k tomu, že poskytovatelé interpersonálních komunikačních služeb nezávislých na číslech obvykle nevykonávají skutečnou kontrolu nad přenosem signálů v sítích, lze míru rizika pro ***tyto služby*** v některých ohledech považovat za nižší než v případě tradičních služeb elektronických komunikací. Totéž platí o interpersonálních komunikačních službách, které využívají čísla a které nevykonávají skutečnou kontrolu nad přenosem signálů.	(50) Vzhledem k rostoucímu významu interpersonálních komunikačních služeb nezávislých na číslech je nutné zajistit, aby i tyto služby podléhaly odpovídajícím bezpečnostním požadavkům v souladu s jejich zvláštní povahou a ekonomickým významem. Provozovatelé takových služeb by tedy měli rovněž zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Vzhledem k tomu, že poskytovatelé interpersonálních komunikačních služeb nezávislých na číslech obvykle nevykonávají skutečnou kontrolu nad přenosem signálů v sítích, lze míru rizika pro ***bezpečnost sítí u těchto služeb*** v některých ohledech považovat za nižší než v případě tradičních služeb elektronických komunikací. Totéž platí o interpersonálních komunikačních službách, které využívají čísla a které nevykonávají skutečnou kontrolu nad přenosem signálů. ***Jelikož se však prostor k útoku stále rozšiřuje, stávají se oblíbenými vektory útoků interpersonální komunikační služby nezávislé na číslech, mj. služby sociálních médií pro zasílání zpráv. Aktéři s nekalými úmysly využívají platformy ke komunikaci, při níž se snaží nalákat oběti, aby otevřely napadené internetové stránky. Tím se zvyšuje pravděpodobnost incidentů spojených***

	s využíváním osobních údajů, což má pak důsledky pro bezpečnost informačních systémů.

Pozměňovací návrh 51

Návrh směrnice
Bod odůvodnění 51

Znění navržené Komisí	*Pozměňovací návrh*
(51) Vnitřní trh více než kdy předtím spoléhá na fungování internetu. Na službách poskytovaných po internetu jsou závislé služby prakticky všech základních a důležitých subjektů. S cílem zajistit bezproblémové poskytování služeb základních a důležitých subjektů je důležité, aby veřejné sítě elektronických komunikací, jako jsou například internetové páteřní sítě nebo podmořské komunikační kabely, měly zavedena odpovídající opatření v oblasti kybernetické bezpečnosti a hlásily incidenty, které se jich týkají.	(51) Vnitřní trh více než kdy předtím spoléhá na fungování internetu. Na službách poskytovaných po internetu jsou závislé služby prakticky všech základních a důležitých subjektů. S cílem zajistit bezproblémové poskytování služeb základních a důležitých subjektů je důležité, aby ***všechny*** veřejné sítě elektronických komunikací, jako jsou například internetové páteřní sítě nebo podmořské komunikační kabely, měly zavedena odpovídající opatření v oblasti kybernetické bezpečnosti a hlásily ***závažné*** incidenty, které se jich týkají. ***Členské státy by měly zajistit zachování integrity a dostupnosti těchto veřejných sítí elektronických komunikací a měly by zvážit jejich ochranu před sabotáží a špionáží zásadního bezpečnostního zájmu. Informace o incidentech, např. v souvislosti s podmořskými komunikačními kabely, by měly být aktivně sdíleny mezi členskými státy.***

Pozměňovací návrh 52

Návrh směrnice
Bod odůvodnění 52

Znění navržené Komisí	*Pozměňovací návrh*
(52) Ve vhodných případech by subjekty měly informovat příjemce svých služeb o konkrétních a závažných hrozbách a	(52) Ve vhodných případech by subjekty měly informovat příjemce svých služeb o konkrétních a závažných hrozbách a

o opatřeních, která mohou přijmout, aby snížili riziko, jež jim z těchto hrozeb vyplývá. ***Požadavek na informování příjemců o hrozbách*** by subjekty ***neměl*** zbavovat povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření s cílem zamezit jakýmkoli kybernetickým hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o bezpečnostních hrozbách by měly být příjemcům poskytovány zdarma.	o opatřeních, která mohou přijmout, aby snížili riziko, jež jim z těchto hrozeb vyplývá. ***To*** by subjekty ***nemělo*** zbavovat povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření s cílem zamezit jakýmkoli kybernetickým hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o bezpečnostních hrozbách by měly být příjemcům poskytovány zdarma ***a měly by být formulovány ve snadno srozumitelném jazyce***.

Pozměňovací návrh 53

Návrh směrnice
Bod odůvodnění 53

Znění navržené Komisí	*Pozměňovací návrh*
(53) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli příjemce služby zejména informovat o konkrétních a závažných kybernetických hrozbách a o opatřeních, která mohou přijmout, aby chránili bezpečnost své komunikace, například použitím specifických druhů softwaru nebo ***šifrovacích*** technologií.	(53) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli ***zavést záměrnou a standardní bezpečnost a*** příjemce služby ***by měli*** zejména informovat o konkrétních a závažných kybernetických hrozbách a o opatřeních, která mohou přijmout, aby chránili bezpečnost ***svého zařízení a*** své komunikace, například použitím specifických druhů ***šifrovacího*** softwaru nebo ***jiných bezpečnostních*** technologií ***zaměřených na data***.

Pozměňovací návrh 54

Návrh směrnice
Bod odůvodnění 54

Znění navržené Komisí	*Pozměňovací návrh*
(54) S cílem zajistit bezpečnost sítí a služeb elektronické komunikace by mělo být podporováno použití šifrování, a ***zejména šifrování mezi koncovými body***,	(54) S cílem zajistit bezpečnost sítí a služeb elektronické komunikace by mělo být podporováno použití šifrování ***a dalších bezpečnostních technologií***

a v případě nutnosti by pro poskytovatele těchto služeb a sítí v souladu se zásadami bezpečnosti a ***soukromí standardně*** a ***záměrně*** pro účely článku 18 mělo být povinné. Použití šifrování mezi koncovými body by mělo být v souladu s pravomocemi členských států zajistit ochranu podstatných zájmů své bezpečnosti a veřejné bezpečnosti a umožnit vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. ***Řešení k zajištění zákonného přístupu k informacím v rámci komunikace šifrované mezi koncovými body by měla zachovat účinnost*** šifrování ***při ochraně soukromí a bezpečnosti komunikací, a současně poskytnout*** účinnou ***reakci na trestnou činnost***.	***zaměřených na data***, k ***nimž patří tokenizace, segmentace, regulace přístupu, označování, silná identita, řízení přístupu a automatizovaná rozhodnutí o přístupu***, a v případě nutnosti by pro poskytovatele těchto služeb a sítí v souladu se zásadami ***standardní a záměrné*** bezpečnosti a ***standardního*** a ***záměrného soukromí*** pro účely článku 18 mělo být povinné. Použití šifrování mezi koncovými body by mělo být v souladu s pravomocemi členských států zajistit ochranu podstatných zájmů své bezpečnosti a veřejné bezpečnosti a umožnit vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. ***To by však nemělo vést ke snahám o oslabení*** šifrování ***mezi koncovými body, které je zásadní technologií pro*** účinnou ***ochranu údajů a soukromí***.

Pozměňovací návrh 55

Návrh směrnice
Bod odůvodnění 54 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(54a) V zájmu zajištění bezpečnosti a zabránění zneužívání a manipulaci se sítěmi a službami elektronických komunikací je třeba podporovat používání interoperabilních standardů bezpečného směrování, jež zajistí integritu a spolehlivost směrovacích funkcí v celém ekosystému provozovatelů internetu.

Pozměňovací návrh 56

Návrh směrnice
Bod odůvodnění 54 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(54b) V zájmu zajištění funkčnosti

	a integrity internetu a omezení bezpečnostních problémů souvisejících s DNS by měly být příslušné zúčastněné strany, včetně podniků, poskytovatelů internetových služeb a prodejců prohlížečů v Unii, podněcovány k tomu, aby přijaly strategii diverzifikace překladu jmen DNS. Členské státy by nadto měly podporovat rozvoj a používání veřejné a bezpečné evropské služby resolverů DNS.

Pozměňovací návrh 57

Návrh směrnice
Bod odůvodnění 55

Znění navržené Komisí	*Pozměňovací návrh*
(55) Tato směrnice stanoví dvoustupňový přístup k hlášení incidentů, tak aby bylo dosaženo správné rovnováhy mezi rychlým hlášením, které pomáhá snížit potenciální šíření incidentů a umožňuje subjektům žádat o podporu, na jedné straně a podrobným hlášením, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje odolnost jednotlivých společností a celých odvětví vůči kybernetickým hrozbám, na straně druhé. Jakmile se subjekty ***dozvědí o*** incidentu, měly by být povinny předložit počáteční oznámení ***do 24 hodin a*** poté ***závěrečnou*** zprávu nejpozději do jednoho měsíce***. Počáteční oznámení by mělo obsahovat pouze informace, které jsou zcela nezbytné, aby byl příslušný orgán zpraven o incidentu***, a ***které subjektu umožňují v případě potřeby*** požádat o ***pomoc. V tomto oznámení by v daném případě mělo být uvedeno, zda je incident pravděpodobně způsoben protiprávním či zlovolným jednáním. Členské státy by měly zajistit, aby požadavek na předložení tohoto počátečního oznámení neodváděl zdroje*** ohlašujícího subjektu ***od činností souvisejících s řešením incidentu, které by***	(55) Tato směrnice stanoví dvoustupňový přístup k hlášení incidentů, tak aby bylo dosaženo správné rovnováhy mezi rychlým hlášením, které pomáhá snížit potenciální šíření incidentů a umožňuje subjektům žádat o podporu, na jedné straně a podrobným hlášením, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje odolnost jednotlivých společností a celých odvětví vůči kybernetickým hrozbám, na straně druhé. Jakmile se subjekty o incidentu ***dozvědí***, měly by být povinny předložit počáteční oznámení a poté ***souhrnnou*** zprávu nejpozději do jednoho měsíce ***od předložení počátečního oznámení. Harmonogram původního oznámení incidentů by neměl subjektům bránit v tom, aby incidenty ohlašovaly dříve***, a ***proto by měly mít možnost*** požádat o ***podporu týmy CSIRT a rychle tak umožnit zmírnění a případně omezení šíření ohlášeného incidentu. Týmy CSIRT mohou požádat o průběžnou zprávu o podstatných změnách stavu a přihlížejí přitom k reakci*** ohlašujícího subjektu na incident a k ***jeho*** úsilí o ***nápravu***.

měly mít přednost. Aby se dále zabránilo tomu, že by povinnosti hlášení incidentu odváděly zdroje od řešení reakce na incident ***nebo jinak narušovaly*** úsilí ***subjektů v tomto ohledu, členské státy by měly rovněž stanovit, že v řádně odůvodněných případech a po dohodě s příslušnými orgány nebo s týmy CSIRT se dotyčný subjekt může odchýlit od lhůt 24 hodin pro počáteční oznámení a jeden měsíc pro konečnou zprávu***.

Pozměňovací návrh 58

Návrh směrnice
Bod odůvodnění 55 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(55a) Závažný incident může mít dopad důvěrnost, integritu nebo dostupnost služby. Základní a důležité subjekty by měly týmům CSIRT oznámit závažné incidenty, které mají dopad na dostupnost jejich služby, do 24 hodin po zjištění incidentu. O závažných incidentech, které naruší důvěrnost a integritu jejich služeb, by měly týmy CSIRT uvědomit do 72 hodin po zjištění incidentu. Mezi typy incidentů se nerozlišuje na základě závažnosti incidentu, ale podle toho, do jaké míry je pro ohlašující subjekt obtížné posoudit incident a jeho význam, a podle schopnosti subjektu hlásit informace, které mohou být pro CSIRT užitečné. Počáteční oznámení by mělo obsahovat informace, které jsou nezbytné k informování týmu CSIRT o incidentu a díky nimž může subjekt v případě potřeby požádat o pomoc. Členské státy by měly zajistit, aby požadavek na provedení tohoto počátečního oznámení neodváděl zdroje oznamujícího subjektu od činností souvisejících s řešením incidentu, které by měly mít přednost. S cílem předejít tomu, že by povinnosti hlášení incidentu odváděly zdroje od řešení reakce na

incident nebo jinak narušovaly úsilí subjektů v tomto ohledu, by členské státy měly rovněž stanovit, že v řádně odůvodněných případech a po dohodě s CSIRT se dotyčný subjekt může odchýlit od lhůt stanovených pro počáteční oznámení a pro předložení komplexní zprávy.

Pozměňovací návrh 59

Návrh směrnice
Bod odůvodnění 59

Znění navržené Komisí	*Pozměňovací návrh*
(59) Udržování přesných a úplných databází doménových jmen ***a*** registračních údajů (takzvaných „údajů WHOIS“) ***a poskytování zákonného přístupu k těmto údajům*** má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému doménových jmen (DNS), což na druhé straně přispívá k vyšší společné úrovni kybernetické bezpečnosti v Unii. Pokud zpracování údajů zahrnuje osobní údaje, musí takové zpracování být v souladu s právem Unie v oblasti ochrany údajů.	(59) Udržování přesných***, ověřených*** a úplných databází doménových jmen registračních údajů (takzvaných „údajů WHOIS“) má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému doménových jmen (DNS), což na druhé straně přispívá k vyšší společné úrovni kybernetické bezpečnosti v Unii ***a k potírání nezákonných činností. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace doménových jmen by proto měly shromažďovat údaje o registraci doménových jmen, které by měly zahrnovat přinejmenším jméno držitele registrace, jeho fyzickou a e-mailovou adresu a telefonní číslo. Shromážděné údaje nemusí být v praxi vždy zcela přesné, nicméně registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace doménových jmen by měly zavést a uplatňovat přiměřené postupy, kterými ověří, zda fyzické nebo právnické osoby, které žádají o doménové jméno nebo takové jméno vlastní, poskytly takové kontaktní údaje, jejichž pomocí je možné je zastihnout a očekávat od nich odpověď. V případě uplatnění zásady vynaložení nejvyššího úsilí by tyto ověřovací postupy měly být odrazem osvědčených postupů, které se v***

	daném odvětví nyní používají. V těchto osvědčených ověřovacích postupech by se měl projevit pokrok, jehož bylo dosaženo v rámci elektronické identifikace. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace doménových jmen by měly své postupy a procesy zveřejnit, aby zajistily integritu a dostupnost údajů o registraci doménových jmen. Pokud zpracování údajů zahrnuje osobní údaje, musí takové zpracování být v souladu s právem Unie v oblasti ochrany údajů.

Pozměňovací návrh 60

Návrh směrnice
Bod odůvodnění 60

Znění navržené Komisí	*Pozměňovací návrh*
(60) Dostupnost a včasný přístup k ***těmto*** údajům pro ***orgány veřejné správy***, včetně ***příslušných orgánů*** podle unijního nebo vnitrostátního práva za účelem prevence, vyšetřování či stíhání trestných činů***, pro*** týmy CERT ***(týmy*** CSIRT***)*** a***, pokud jde*** o ***údaje jejich zákazníků, pro poskytovatele elektronických komunikačních sítí*** a ***služeb*** a ***poskytovatele technologií*** a služeb ***v oblasti kybernetické bezpečnosti jednající jménem těchto zákazníků, má zásadní význam pro prevenci a boj proti zneužívání*** systému ***doménových jmen, a zejména pro prevenci a odhalování kybernetických bezpečnostních incidentů a reakci*** na ***tyto incidenty. Pokud se takový přístup týká osobních údajů, měl by být v souladu s právem Unie v oblasti ochrany údajů.***	(60) Dostupnost a včasný přístup k údajům ***o registraci doménových jmen má*** pro ***oprávněné uchazeče o přístup zásadní význam s ohledem na kybernetickou bezpečnost a potírání nezákonných činností v on-line ekosystému. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén by proto měly být povinny umožnit v souladu s právem Unie na ochranu osobních údajů oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci domén, včetně osobních údajů. Oprávnění žadatelé o přístup by měli předložit řádně odůvodněnou žádost o přístup k údajům o registraci doménových jmen na základě unijních nebo vnitrostátních právních předpisů a mezi ně mohou patřit i příslušné orgány*** podle unijního nebo vnitrostátního práva za účelem prevence, vyšetřování či stíhání trestných činů ***a vnitrostátní*** týmy CERT ***nebo*** CSIRT**.** ***Členské státy by měly zajistit, aby registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace***

	doménových jmen bez zbytečného odkladu a v každém případě do 72 hodin reagovaly na žádosti oprávněných žadatelů o zpřístupnění údajů o registraci domén. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén by měly stanovit postupy a procesy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Postup poskytování přístupu může také obsahovat užívání rozhraní, portálu nebo jiných technických nástrojů k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Za účelem podpory harmonizovaných postupů na vnitřním trhu může Komise přijmout pokyny k takovým postupům, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních údajů.

Pozměňovací návrh 61

Návrh směrnice
Bod odůvodnění 61

Znění navržené Komisí	*Pozměňovací návrh*
(61) S cílem zajistit dostupnost přesných a úplných údajů o registraci domén by registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně (takzvaní registrátoři) měly shromažďovat údaje o registraci domén a zaručovat integritu a dostupnost těchto údajů. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně by zejména měly stanovit politiky a postupy pro shromažďování a uchovávání přesných a úplných registračních údajů a rovněž zamezit uvádění nesprávných registračních údajů a opravovat je v souladu s pravidly Unie o ochraně osobních údajů.	***vypouští se***

Pozměňovací návrh 62

Návrh směrnice
Bod odůvodnění 62

Znění navržené Komisí	*Pozměňovací návrh*
(62) Registry internetových domén nejvyšší úrovně a subjekty poskytující ***jim*** služby registrace domén by měly veřejně zpřístupnit údaje o registraci domén, ***které nespadají do oblasti působnosti pravidel Unie na ochranu osobních údajů, například údajů, které*** se ***týkají právnických osob[25].*** Registry internetových domén nejvyšší úrovně a subjekty ***poskytující služby registrace domén nejvyšší úrovně by také měly v souladu s právem Unie na ochranu osobních údajů umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci domén týkajícím se fyzických osob***. ***Členské státy*** by měly ***zajistit, aby registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén bez zbytečného odkladu reagovaly na žádosti oprávněných žadatelů o přístup o zpřístupnění údajů o registraci domén. Registry*** internetových domén nejvyšší úrovně a ***subjekty poskytující jim*** služby registrace domén by měly ***stanovit politiky a postupy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Postup poskytování přístupu může také obsahovat užívání rozhraní, portálu nebo jiného technického nástroje k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Za účelem podpory harmonizovaných postupů na vnitřním trhu může Komise přijmout pokyny o takových postupech, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních údajů.***	(62) Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén by měly ***být povinny*** veřejně zpřístupnit údaje o registraci domén, ***jejichž součástí nejsou osobní údaje. Je třeba rozlišovat mezi fyzickými a právnickými osobami[25]. Jedná-li*** se ***o právnické osoby, měly by*** registry internetových domén nejvyšší úrovně a subjekty ***veřejně zpřístupnit alespoň jméno držitele registrace, jeho fyzickou a e-mailovou adresu a telefonní číslo***. ***Právnické osoby*** by měly ***být povinny poskytnout obecnou e-mailovou adresu, kterou lze veřejně zpřístupnit, nebo by měly souhlasit se zveřejněním osobní e-mailové adresy. Na žádost registrů*** internetových domén nejvyšší úrovně a ***subjektů poskytujících*** služby registrace domén by měly ***být právnické osoby schopny takový souhlas prokázat***.

[25] Viz 14. bod odůvodnění NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, kde se uvádí, že „toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby“.

[25] Viz 14. bod odůvodnění NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, kde se uvádí, že „toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby“.

Pozměňovací návrh 63

Návrh směrnice
Bod odůvodnění 63

Znění navržené Komisí	*Pozměňovací návrh*
(63) Všechny základní a důležité subjekty podle této směrnice by měly podléhat pravomoci členského státu, ve kterém poskytují své služby. Poskytuje-li subjekt služby ve více než jednom členském státě, měl by podléhat samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by měly spolupracovat, poskytovat si navzájem pomoc a v případě potřeby provádět společné akce v oblasti dohledu.	(63) Všechny základní a důležité subjekty podle této směrnice by měly podléhat pravomoci členského státu, ve kterém poskytují své služby ***nebo vykonávají svou činnost***. Poskytuje-li subjekt služby ve více než jednom členském státě, měl by podléhat samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by měly spolupracovat, poskytovat si navzájem pomoc a v případě potřeby provádět společné akce v oblasti dohledu.

Pozměňovací návrh 64

Návrh směrnice
Bod odůvodnění 64

Znění navržené Komisí	*Pozměňovací návrh*
(64) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb systému doménových jmen, registrů internetových domén nejvyšší úrovně, poskytovatelů sítí pro doručování obsahu, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a poskytovatelů digitálních služeb by	(64) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb systému doménových jmen, registrů internetových domén nejvyšší úrovně, poskytovatelů sítí pro doručování obsahu, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a poskytovatelů digitálních služeb by

pravomoc nad těmito subjekty měl mít pouze jeden členský stát. Pravomoc by měl mít ten členský stát, v němž má daný subjekt v rámci Unie hlavní místo obchodní činnosti. Kritérium místa obchodní činnosti pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavního místa obchodní činnosti, a tudíž ani nejsou rozhodujícími kritérii pro jeho určení. Hlavní místo obchodní činnosti by mělo být místo v Unii, kde jsou přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa společnosti v Unii. Pokud taková rozhodnutí nejsou v Unii přijímána, mělo by se mít za to, že hlavní místo obchodní činnosti je v členském státě, ve kterém má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, mělo by se za hlavní místo obchodní činnosti skupiny podniků považovat hlavní místo obchodní činnosti řídícího podniku.

pravomoc nad těmito subjekty měl mít pouze jeden členský stát. Pravomoc by měl mít ten členský stát, v němž má daný subjekt v rámci Unie hlavní místo obchodní činnosti. Kritérium místa obchodní činnosti pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavního místa obchodní činnosti, a tudíž ani nejsou rozhodujícími kritérii pro jeho určení. Hlavní místo obchodní činnosti by mělo být místo v Unii, kde jsou přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa společnosti v Unii. Pokud taková rozhodnutí nejsou v Unii přijímána, mělo by se mít za to, že hlavní místo obchodní činnosti je v členském státě, ve kterém má subjekt ***buď*** provozovnu s nejvyšším počtem zaměstnanců v Unii***, nebo provozovnu, v níž se operace v oblasti kybernetické bezpečnosti provádějí***. Pokud jsou služby prováděny skupinou podniků, mělo by se za hlavní místo obchodní činnosti skupiny podniků považovat hlavní místo obchodní činnosti řídícího podniku.

Pozměňovací návrh 65

Návrh směrnice
Bod odůvodnění 65 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(65a) Agentura ENISA by měla vytvořit a vést registr informací o základních a

	důležitých subjektech, mezi něž patří poskytovatelé služeb DNS, registry doménových jmen nejvyšší úrovně a poskytovatelé služeb cloud computingu, služeb datových center, sítí pro doručování obsahu, on-line tržišť, internetových vyhledávačů a platforem sociálních sítí. Tyto základní a důležité subjekty by měly agentuře ENISA předložit svá jména, adresy a aktuální kontaktní údaje. Měly by agenturu ENISA uvědomit o všech změnách údajů, a to neprodleně, nejpozději však do dvou týdnů od data, kdy změna začala platit. ENISA by měla tyto informace předat příslušnému jednotnému kontaktnímu místu. Základní a důležité subjekty, které předkládají své informace agentuře ENISA, proto nejsou povinny samostatně informovat příslušný orgán v daném členském státě. Agentura ENISA by měla vypracovat jednoduchý a veřejně dostupný program aplikací, který by tyto subjekty mohly používat k aktualizaci svých informací. Agentura ENISA by navíc měla zavést vhodné protokoly pro klasifikaci informací a řízení rizik s cílem zajistit bezpečnost a důvěrnost zpřístupněných informací a přístup k těmto informacím, jejich uchovávání a přenos by měla omezit na zamýšlené uživatele.

Pozměňovací návrh 66

Návrh směrnice
Bod odůvodnění 66

Znění navržené Komisí	*Pozměňovací návrh*
(66) Pokud jsou podle ustanovení této směrnice vyměňovány, hlášeny nebo jinak sdíleny informace, které jsou ***podle unijních*** nebo ***vnitrostátních předpisů*** považovány za utajované, měla by se použít odpovídající zvláštní pravidla o nakládání s utajovanými informacemi.	(66) Pokud jsou podle ustanovení této směrnice vyměňovány, hlášeny nebo jinak sdíleny informace, které jsou ***v souladu s unijními*** nebo ***vnitrostátními předpisy*** považovány za utajované, měla by se použít odpovídající zvláštní pravidla o nakládání s utajovanými informacemi.

	Kromě toho by agentura ENISA měla mít zavedenou infrastrukturu, postupy a pravidla pro nakládání s citlivými a utajovanými informacemi v souladu s platnými bezpečnostními pravidly na ochranu utajovaných informací EU.

Pozměňovací návrh 67

Návrh směrnice
Bod odůvodnění 68

Znění navržené Komisí	*Pozměňovací návrh*
(68) Subjekty by měly být motivovány k tomu, aby společně využívaly pákového efektu svých individuálních znalostí a praktických zkušeností na strategické, taktické a operativní úrovni a tím posílit své schopnosti odpovídajícím způsobem posuzovat a sledovat kybernetické hrozby, bránit se jim a reagovat na ně. Je proto nezbytné umožnit vznik mechanismů na úrovni Unie pro dobrovolná ujednání o sdílení informací. Členské státy by za tímto účelem měly aktivně podporovat a motivovat také relevantní subjekty, jež nespadají do oblasti působnosti této směrnice, aby se účastnily takovýchto mechanismů pro sdílení informací. Tyto mechanismy by měly fungovat v plném souladu s pravidly Unie v oblasti hospodářské soutěže a s právními předpisy Unie o ochraně údajů.	(68) Subjekty by měly být motivovány ***a podporovány členskými státy*** k tomu, aby společně využívaly pákového efektu svých individuálních znalostí a praktických zkušeností na strategické, taktické a operativní úrovni a tím posílit své schopnosti odpovídajícím způsobem posuzovat a sledovat kybernetické hrozby, bránit se jim a reagovat na ně. Je proto nezbytné umožnit vznik mechanismů na úrovni Unie pro dobrovolná ujednání o sdílení informací. Členské státy by za tímto účelem měly aktivně podporovat a motivovat také relevantní subjekty, jež nespadají do oblasti působnosti této směrnice***, jako jsou subjekty zaměřené na služby a výzkum v oblasti kybernetické bezpečnosti***, aby se účastnily takovýchto mechanismů pro sdílení informací. Tyto mechanismy by měly fungovat v plném souladu s pravidly Unie v oblasti hospodářské soutěže a s právními předpisy Unie o ochraně údajů.

Pozměňovací návrh 68

Návrh směrnice
Bod odůvodnění 69

Znění navržené Komisí	*Pozměňovací návrh*
(69) Zpracování osobních údajů v rozsahu nezbytně nutném a přiměřeném pro zajištění bezpečnosti sítí a informací ze strany subjektů, které provádějí ***orgány veřejné správy, týmy CERT,*** týmy CSIRT a poskytovatelé bezpečnostních technologií a služeb, ***by mělo představovat oprávněný zájem dotčeného správce údajů*** podle nařízení (EU) 2016/679. ***To by mělo zahrnovat*** opatření týkající se prevence, odhalování ***a*** analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměnu informací v rámci odstraňování a koordinovaného odhalování zranitelných míst, a také dobrovolnou výměnu informací o těchto incidentech, kybernetických hrozbách a zranitelných místech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích***. Taková opatření mohou vyžadovat*** zpracovávání ***těchto druhů*** osobních údajů***:*** IP adres, jednotných adres zdroje (URL), doménových jmen ***a*** e-mailových adres.	(69) Zpracování osobních údajů v rozsahu nezbytně nutném a přiměřeném pro zajištění bezpečnosti sítí a informací ze strany ***základních a důležitých*** subjektů, které provádějí týmy CSIRT a poskytovatelé bezpečnostních technologií a služeb ***je nezbytné pro splnění jejich právních povinností stanovených v této směrnici. Takové zpracování osobních údajů může být nezbytné i pro účely oprávněných zájmů základních a důležitých subjektů. Pokud tato směrnice vyžaduje zpracování osobních údajů pro účely kybernetické bezpečnosti a bezpečnosti sítě a informací v souladu s ustanoveními článků 18***, ***20 a 23 směrnice, považuje se toto zpracování za nezbytné pro splnění právní povinnosti*** podle ***čl. 6 odst. 1 písm. c)*** nařízení (EU) 2016/679. ***Pro účely článků 26 a 27 této směrnice se zpracování uvedené v čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 považuje za nezbytné pro účely oprávněných zájmů základních a důležitých subjektů.*** Opatření týkající se prevence, odhalování***, identifikace, zamezení šíření,*** analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměnu informací v rámci odstraňování a koordinovaného odhalování zranitelných míst, a také dobrovolnou výměnu informací o těchto incidentech, kybernetických hrozbách a zranitelných místech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích ***vyžadují*** zpracovávání ***určitých kategorií*** osobních údajů***, například*** IP adres, jednotných adres zdroje (URL), doménových jmen***,*** e-mailových adres***, časových razítek, informací o operačním systému nebo prohlížeči, souborů cookies nebo jiných informací označující modus operandi***.

Pozměňovací návrh 69

Návrh směrnice
Bod odůvodnění 71

Znění navržené Komisí	*Pozměňovací návrh*
(71) K zajištění účinného vymáhání by měl být stanoven minimální seznam správních sankcí za porušení povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení, jež stanoví tato směrnice, čímž se vytvoří jasný a jednotný rámec pro takové sankce v celé Unii. Náležitá pozornost by měla být věnována povaze, závažnosti a době trvání protiprávního jednání, ***skutečné*** způsobené škodě či ztrátám ***nebo potenciálním škodám či ztrátám, které mohly být vyvolány***, úmyslné nebo nedbalostní povaze protiprávního jednání, opatřením přijatým za účelem prevence nebo zmenšení způsobené škody nebo ztrát, míře odpovědnosti nebo jakémukoli relevantnímu protiprávnímu jednání v minulosti, míře spolupráce s příslušným orgánem a jakýmkoli jiným přitěžujícím nebo polehčujícím faktorům. ***Uložení sankcí*** včetně správních pokut by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a ***Listinou*** základních práv Evropské unie, včetně účinné právní ochrany ***a*** spravedlivého procesu.	(71) K zajištění účinného vymáhání by měl být stanoven minimální seznam správních sankcí za porušení povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení, jež stanoví tato směrnice, čímž se vytvoří jasný a jednotný rámec pro takové sankce v celé Unii. Náležitá pozornost by měla být věnována povaze, závažnosti a době trvání protiprávního jednání, způsobené škodě či ztrátám, úmyslné nebo nedbalostní povaze protiprávního jednání, opatřením přijatým za účelem prevence nebo zmenšení způsobené škody nebo ztrát, míře odpovědnosti nebo jakémukoli relevantnímu protiprávnímu jednání v minulosti, míře spolupráce s příslušným orgánem a jakýmkoli jiným přitěžujícím nebo polehčujícím faktorům. ***Sankce,*** včetně správních pokut***, by měly být přiměřené a jejich uložení*** by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a ***Listiny*** základních práv Evropské unie ***(dále jen „Listina“)***, včetně účinné právní ochrany***,*** spravedlivého procesu***, presumpce neviny a práv na obhajobu***.

Pozměňovací návrh 70

Návrh směrnice
Bod odůvodnění 72

Znění navržené Komisí	*Pozměňovací návrh*
(72) S cílem zajistit účinné vymáhání povinností stanovených v této směrnici by každý příslušný orgán měl mít pravomoc	(72) S cílem zajistit účinné vymáhání povinností stanovených v této směrnici by každý příslušný orgán měl mít pravomoc

ukládat správní pokuty nebo požadovat uložení správních pokut.	ukládat správní pokuty nebo požadovat uložení správních pokut***, pokud k porušení došlo úmyslně či z důvodu nedbalosti nebo pokud byl dotčený subjekt na porušení předpisů upozorněn***.

Pozměňovací návrh 71

Návrh směrnice
Bod odůvodnění 76

Znění navržené Komisí	*Pozměňovací návrh*
(76) Aby se dále posílila účinnost a odrazující účinek sankcí, jež mají být uloženy za porušení povinností stanovených podle této směrnice, měly by být příslušné orgány oprávněny ***uplatňovat sankce spočívající v pozastavení*** osvědčení nebo povolení ***týkajícího*** se části nebo všech služeb, jež poskytuje základní subjekt, a uložení dočasného zákazu výkonu řídící funkce fyzické osoby. Vzhledem k závažnosti a dopadu ***těchto sankcí*** na činnost subjektů a v konečném důsledku na jejich zákazníky, ***měly by*** být uplatňovány pouze úměrně závažnosti porušení a s ohledem na konkrétní okolnosti každého případu, včetně úmyslné nebo nedbalostní povahy porušení, opatřením přijatým k zamezení nebo zmírnění způsobené škody nebo ztrát. Tyto ***sankce*** by se měly používat jen jako krajní prostředek, což znamená pouze po vyčerpání ostatních relevantních donucovacích opatření, jež stanoví tato směrnice, a pouze po dobu, než subjekty, vůči kterým jsou uplatněny, přijmou nezbytná opatření k nápravě nedostatků nebo k dosažení souladu s požadavky příslušného orgánu, kvůli kterým ***byly*** tyto ***sankce*** uloženy. Uložení takových ***sankcí*** musí podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny ***základních práv Evropské unie***, včetně účinné právní ochrany, spravedlivého procesu,	(76) Aby se dále posílila účinnost a odrazující účinek sankcí, jež mají být uloženy za porušení povinností stanovených podle této směrnice, měly by být příslušné orgány oprávněny ***dočasně pozastavit*** osvědčení nebo povolení ***týkající*** se části nebo všech ***příslušných*** služeb, jež poskytuje základní subjekt, a ***požadovat*** uložení dočasného zákazu výkonu řídící funkce fyzické osoby ***na úrovni výkonného ředitele nebo zákonného zástupce. Pro dočasný zákaz výkonu řídících funkcí fyzické osoby na úrovni výkonného ředitele nebo zákonného zástupce v subjektech veřejné správy by měly členské státy vypracovat zvláštní postupy a pravidla. Při vypracovávání těchto postupů a pravidel by měly zohlednit specifika jednotlivých úrovní a svých systémů veřejné správy.*** Vzhledem k ***jejich*** závažnosti a dopadu na činnost subjektů a v konečném důsledku na jejich zákazníky, ***by tato dočasná pozastavení nebo tyto zákazy měly*** být uplatňovány pouze úměrně závažnosti porušení a s ohledem na konkrétní okolnosti každého případu, včetně úmyslné nebo nedbalostní povahy porušení, opatřením přijatým k zamezení nebo zmírnění způsobené škody nebo ztrát. ***Tato dočasná pozastavení nebo*** tyto ***dočasné zákazy*** by se měly používat jen jako krajní prostředek, což znamená pouze po vyčerpání ostatních relevantních

presumpce neviny a práva na obhajobu.	donucovacích opatření, jež stanoví tato směrnice, a pouze po dobu, než subjekty, vůči kterým jsou uplatněny, přijmou nezbytná opatření k nápravě nedostatků nebo k dosažení souladu s požadavky příslušného orgánu, kvůli kterým ***byla tato dočasná pozastavení nebo*** tyto ***dočasné zákazy*** uloženy. Uložení takových ***dočasných pozastavení nebo zákazů*** musí podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny, včetně účinné právní ochrany, spravedlivého procesu, presumpce neviny a práva na obhajobu.

Pozměňovací návrh 72

Návrh směrnice
Bod odůvodnění 79

Znění navržené Komisí	*Pozměňovací návrh*
(79) Měl by být zaveden mechanismus vzájemného hodnocení, který umožní, aby provádění politik kybernetické bezpečnosti, včetně úrovně schopností a dostupných zdrojů členských států, posuzovali odborníci určení členskými státy.	(79) Měl by být zaveden mechanismus vzájemného hodnocení, který umožní, aby provádění politik kybernetické bezpečnosti, včetně úrovně schopností a dostupných zdrojů členských států, posuzovali ***nezávislí*** odborníci určení členskými státy. ***Vzájemná hodnocení mohou poskytnout cenné poznatky a doporučení, jež posílí celkové schopnosti v oblasti kybernetické bezpečnosti. Mohou zejména přispět ke snazšímu předávání technologií, nástrojů, opatření a procesů mezi členskými státy zapojenými do vzájemného hodnocení, vytvořit funkční způsob, jak sdílet osvědčené postupy mezi členskými státy s různou úrovní vyspělosti v oblasti kybernetické bezpečnosti a umožnit zavedení vysoké společné úrovně kybernetické bezpečnosti v celé Unii. Před vzájemným hodnocením by měl členský stát, který je předmětem přezkumu, provést sebehodnocení kontrolovaných aspektů a všech další cílených otázek, které členskému státu, jenž je předmětem vzájemného hodnocení, sdělí určení***

	odborníci před zahájením procesu. S cílem zjednodušit celý proces a zabránit procedurálním nesrovnalostem a zpožděním by Komise měla ve spolupráci s agenturou ENISA a skupinou pro spolupráci vypracovat šablony pro sebehodnocení kontrolovaných aspektů, které členské státy, jež jsou předmětem přezkumu, vyplní a dodají určeným odborníkům před zahájením procesu vzájemného hodnocení.

Pozměňovací návrh 73

Návrh směrnice
Bod odůvodnění 80

Znění navržené Komisí	*Pozměňovací návrh*
(80) Za účelem zohlednění nových kybernetických hrozeb, technologického vývoje nebo odvětvových zvláštností by Komisi měla být svěřena pravomoc přijmout akty v souladu s článkem 290 SFEU, pokud jde o prvky související s opatřeními v oblasti ***řízení rizik***, jež vyžaduje tato směrnice. Komise by rovněž měla být zmocněna přijmout akty v přenesené pravomoci, jimiž stanoví, které kategorie základních subjektů budou povinny získat osvědčení a podle kterých konkrétních evropských systémů certifikace kybernetické bezpečnosti. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[26]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na zasedání skupin odborníků Komise, jež se	(80) Za účelem zohlednění nových kybernetických hrozeb, technologického vývoje nebo odvětvových zvláštností by Komisi měla být svěřena pravomoc přijmout akty v souladu s článkem 290 SFEU, pokud jde o prvky související s opatřeními ***řízení rizik*** v oblasti ***kybernetické bezpečnosti a s povinnostmi hlášení***, jež vyžaduje tato směrnice. Komise by rovněž měla být zmocněna přijmout akty v přenesené pravomoci, jimiž stanoví, které kategorie základních ***a důležitých*** subjektů budou povinny získat osvědčení a podle kterých konkrétních evropských systémů certifikace kybernetické bezpečnosti. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[26]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup

věnují přípravě aktů v přenesené pravomoci.	na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.
[26] Úř. věst. L 123, 12.5.2016, s. 1.	[26] Úř. věst. L 123, 12.5.2016, s. 1.

Pozměňovací návrh 74

Návrh směrnice
Bod odůvodnění 81

Znění navržené Komisí	*Pozměňovací návrh*
(81) Za účelem zajištění jednotných podmínek k provedení příslušných ustanovení této směrnice týkajících se procesních opatření nezbytných pro fungování skupiny pro spolupráci***, technických prvků opatření k řízení rizik nebo druhu informací, formátu*** a postupu oznamování incidentů by Komisi měly být svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011.[27]	(81) Za účelem zajištění jednotných podmínek k provedení příslušných ustanovení této směrnice týkajících se procesních opatření nezbytných pro fungování skupiny pro spolupráci a postupu oznamování incidentů by Komisi měly být svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011.[27]
[27] Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).	[27] Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

Pozměňovací návrh 75

Návrh směrnice
Bod odůvodnění 82

Znění navržené Komisí	*Pozměňovací návrh*
(82) Komise by měla provádět pravidelný přezkum této směrnice za konzultace se zainteresovanými stranami, zejména	(82) Komise by měla provádět pravidelný přezkum této směrnice za konzultace se zainteresovanými stranami, zejména

pokud jde o ***nutnost změn*** s ohledem na měnící se společenské, politické, technologické nebo tržní podmínky.	pokud jde o ***rozhodnutí, zda je vhodné navrhnout změny*** s ohledem na měnící se společenské, politické, technologické nebo tržní podmínky. ***V rámci přezkumů by Komise měla posoudit, jaký význam mají odvětví, pododvětví a druhy subjektů uvedené v přílohách pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Komise by měla mimo jiné posoudit, zda by poskytovatelé digitálních služeb, kteří jsou klasifikováni jako velmi velké on-line platformy ve smyslu článku 25 nařízení (EU) XXXX/XXXX [jednotný trh digitálních služeb (akt o digitálních službách)] nebo jako strážci služeb ve smyslu čl. 2 odst. 1 nařízení (EU) XXXX/XXXX [spravedlivé trhy otevřené hospodářské soutěži v digitálním odvětví (akt o digitálních trzích)], měli být podle této směrnice označeni za základní subjekty. Mimoto by Komise měla posoudit, zda je vhodné změnit přílohu I směrnice Evropského parlamentu a Rady 2020/1828[1a] doplněním odkazu na tuto směrnici.***
	[1a]Směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES (Úř. věst. L 409, 4.12.2020, s. 1).

Pozměňovací návrh 76

Návrh směrnice
Bod odůvodnění 82 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(82a) Tato směrnice stanoví požadavky v oblasti kybernetické bezpečnosti pro členské státy, jakož i pro základní a důležité subjekty usazené v Unii. Tyto požadavky na kybernetickou bezpečnost

	by měly rovněž uplatňovat orgány, instituce a jiné subjekty Unie na základě legislativního aktu Unie.

Pozměňovací návrh 77

Návrh směrnice
Bod odůvodnění 82 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(82b) Tato směrnice vytváří nové úkoly pro agenturu ENISA, čímž posiluje její úlohu. V důsledku této směrnice by rovněž mohl vzniknout požadavek, aby plnění úkolů agenturou ENISA, které jí nyní stanoví nařízení (EU) 2019/881, odpovídalo vyššímu standardu než dříve. S cílem zajistit, aby agentura ENISA měla potřebné finanční a lidské zdroje pro stávající a nové činnosti, jež má v rámci svých úkolů vykonávat, a aby splňovala veškeré vyšší standardy vyplývající z její posílené úlohy, měl by být odpovídajícím způsobem navýšen její rozpočet. V zájmu zajištění účinného využívání zdrojů by navíc měla být agentuře ENISA poskytnuta větší flexibilita, pokud jde o její možnosti interního přidělování zdrojů, aby tak mohla účinně vykonávat své úkoly a plnit očekávání.

Pozměňovací návrh 78

Návrh směrnice
Bod odůvodnění 84

Znění navržené Komisí	*Pozměňovací návrh*
(84) Tato směrnice dodržuje základní práva a ctí zásady uznané Listinou ***základních práv Evropské unie***, zejména právo na respektování soukromého života a komunikace, právo na ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní	(84) Tato směrnice dodržuje základní práva a ctí zásady uznané Listinou, zejména právo na respektování soukromého života a komunikace, právo na ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý

ochranu a spravedlivý proces. Tato směrnice by měla být prováděna v souladu s těmito právy a zásadami**,**	proces. ***Patří sem i právo příjemců služeb poskytovaných základními a důležitými subjekty na účinnou právní ochranu před soudem.*** Tato směrnice by měla být prováděna v souladu s těmito právy a zásadami**.**

Pozměňovací návrh 79

Návrh směrnice
Čl. 1 – odst. 2 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) stanoví povinnosti členských států v oblasti dohledu a vymáhání.

Pozměňovací návrh 80

Návrh směrnice
Čl. 2 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Tato směrnice se vztahuje na veřejné a soukromé subjekty druhu, který je v příloze I označován za základní a v příloze II za důležitý. Tato směrnice se nevztahuje na ***subjekty, které splňují definici mikropodniků a malých podniků ve smyslu*** doporučení Komise 2003/361/ES**.**[28]	1. Tato směrnice se vztahuje na veřejné a soukromé ***základní a důležité*** subjekty ***takového*** druhu, který je v příloze I označován za základní a v příloze II za důležitý***, jež poskytují své služby nebo vykonávají svou činnost v rámci Unie***. Tato směrnice se nevztahuje na ***malé podniky nebo mikropodniky ve smyslu čl. 2 odst. 2 a 3 přílohy*** doporučení Komise 2003/361/ES[28]***. Ustanovení čl. 3 odst. 4 přílohy tohoto doporučení se nepoužije.***
[28] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).	[28] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

Pozměňovací návrh 81

Návrh směrnice
Čl. 2 – odst. 2 – pododstavec 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
Tato směrnice se ***však*** vztahuje také na ***subjekty uvedené v přílohách I*** a ***II*** bez ohledu na jejich velikost, pokud:	Tato směrnice se vztahuje také na ***základní*** a ***důležité subjekty*** bez ohledu na jejich velikost, pokud:

Pozměňovací návrh 82

Návrh směrnice
Čl. 2 – odst. 2 – pododstavec 1 – písm. d

Znění navržené Komisí	*Pozměňovací návrh*
d) by ***možné*** narušení služby poskytované tímto subjektem mohlo mít vliv na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví;	d) by narušení služby poskytované tímto subjektem mohlo mít vliv na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví;

Pozměňovací návrh 83

Návrh směrnice
Čl. 2 – odst. 2 - subodst. 1 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) by ***možné*** narušení služby poskytované tímto subjektem mohlo vyvolat systémová rizika, zejména pro ta odvětví, kde by takové narušení mohlo mít přeshraniční dopad;	e) by narušení služby poskytované tímto subjektem mohlo vyvolat systémová rizika, zejména pro ta odvětví, kde by takové narušení mohlo mít přeshraniční dopad;

Pozměňovací návrh 84

Návrh směrnice
Čl. 2 – odst. 2 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
Členské státy stanoví seznam subjektů určených podle písmen b) až f) a předloží	***vypouští se***

jej je do [6 měsíců po uplynutí lhůty pro provedení] Komisi. Členské státy tento seznam pravidelně přezkoumávají, a to alespoň každé dva roky od předložení, a v případě potřeby jej aktualizují.

Pozměňovací návrh 85

Návrh směrnice
Čl. 2 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Do … [6 měsíců po uplynutí lhůty pro provedení ve vnitrostátním právu] členské státy sestaví seznam základních a důležitých subjektů, včetně subjektů uvedených v odstavci 1 a subjektů určených podle odst. 2 písm. b) až f) a čl. 24 odst. 1. Členské státy tento seznam pravidelně přezkoumávají, a to alespoň každé dva roky od předložení, a v případě potřeby jej aktualizují.

Pozměňovací návrh 86

Návrh směrnice
Čl. 2 – odst. 2 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2b. Členské státy zajistí, aby základní a důležité subjekty předkládaly příslušným orgánům alespoň tyto informace:
	a) název subjektu;
	b) adresu a aktuální kontaktní údaje, včetně e-mailových adres, rozsahu IP adres a telefonních čísel; a
	c) příslušná odvětví a pododvětví uvedená v přílohách I a II.
	Základní a důležité subjekty oznámí všechny změny údajů, které předložily v souladu s prvním pododstavcem, a to

	neprodleně, nejpozději však do dvou týdnů od data, kdy změna začala platit. Komise bez zbytečného odkladu vydá za tímto účelem za pomoci agentury ENISA pokyny a šablony týkající se povinností stanovených v tomto odstavci.

Pozměňovací návrh 87

Návrh směrnice
Čl. 2 – odst. 2 c (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2c. Do...[6 měsíců po uplynutí lhůty pro provedení ve vnitrostátním právu] a poté každé dva roky oznámí členské státy:
	a) Komisi a skupině pro spolupráci počet všech základních a důležitých subjektů určených pro každé odvětví a pododvětví uvedené v přílohách I a II;
	b) Komisi názvy subjektů určených podle odst. 2 písm. b) až f).

Pozměňovací návrh 88

Návrh směrnice
Čl. 2 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Touto směrnicí nejsou dotčeny směrnice Rady 2008/114/ES[30] a směrnice Evropského parlamentu a Rady 2011/93/EU[31] a 2013/40/EU[32].	4. Touto směrnicí nejsou dotčeny směrnice Rady 2008/114/ES[30] a směrnice Evropského parlamentu a Rady 2011/93/EU[31] a 2013/40/EU[32] ***a 2002/58/ES[32a]***.
[30] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.12.2008, s. 75).	[30] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.12.2008, s. 75).
[31] Směrnice Evropského parlamentu a Rady	[31] Směrnice Evropského parlamentu a Rady

2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV (Úř. věst. L 335, 17.12.2011, s. 1).

[32] 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 (Úř. věst. L 218, 14.8.2013, s. 8).

2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV (Úř. věst. L 335, 17.12.2011, s. 1).

[32] 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 (Úř. věst. L 218, 14.8.2013, s. 8).

[32a] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

Pozměňovací návrh 89

Návrh směrnice
Čl. 2 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Pokud ustanovení právních aktů Unie pro konkrétní odvětví vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení rizik v oblasti kybernetické bezpečnosti nebo aby oznamovaly incidenty ***či významné kybernetické hrozby***, a pokud je účinek těchto opatření alespoň rovnocenný účinku povinností stanovených v této směrnici, příslušná ustanovení této směrnice, včetně ustanovení o dohledu a vymáhání v kapitole VI, se neuplatní.	6. Pokud ustanovení právních aktů Unie pro konkrétní odvětví vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení rizik v oblasti kybernetické bezpečnosti nebo aby oznamovaly incidenty, a pokud je účinek těchto opatření alespoň rovnocenný účinku povinností stanovených v této směrnici, příslušná ustanovení této směrnice, včetně ustanovení o dohledu a vymáhání v kapitole VI, se neuplatní. ***Komise bez zbytečného odkladu vydá pokyny týkající se provádění odvětvových aktů práva Unie s cílem zajistit, aby tyto akty splňovaly požadavky na kybernetickou bezpečnost stanovené touto směrnicí a aby nedocházelo k překrývání v předpisech či právní nejistotě. Při přípravě těchto pokynů zohlední Komise osvědčené***

postupy a odborné znalosti agentury ENISA a skupiny pro spolupráci.

Pozměňovací návrh 90

Návrh směrnice
Čl. 2 – odst. 6 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	6a. Základní a důležité subjekty, týmy CSIRT a poskytovatelé bezpečnostních technologií a služeb zpracovávají osobní údaje v míře nezbytně nutné a přiměřené pro účely zajištění kybernetické bezpečnosti a bezpečnosti sítí a informací, aby splnily povinnosti stanovené v této směrnici. Toto zpracovávání osobních údajů pro účely této směrnice se provádí v souladu s nařízením (EU) 2016/679, zejména s jeho článkem 6.

Pozměňovací návrh 91

Návrh směrnice
Čl. 2 – odst. 6 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	6b. Zpracování osobních údajů podle této směrnice poskytovateli veřejných sítí elektronických komunikací nebo poskytovatelů veřejně dostupných služeb elektronických komunikací uvedenými v příloze I bodě 8 se provádí v souladu se směrnicí 2002/58/ES.

Pozměňovací návrh 92

Návrh směrnice
Čl. 4 – odst. 1 – bod 4 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	4a) „případem, kdy téměř došlo k incidentu“ událost, která mohla narušit dostupnost, autenticitu, integritu nebo důvěrnost údajů nebo která mohla způsobit škodu, ale jejímu negativnímu dopadu bylo úspěšně zabráněno;

Pozměňovací návrh 93

Návrh směrnice
Čl. 4 – odst. 1 – bod 6

Znění navržené Komisí	*Pozměňovací návrh*
6) „řešením incidentu“ veškeré akce a postupy, jejichž cílem je ***incident*** odhalit, analyzovat, zamezit jeho šíření a reagovat na něj;	6) „řešením incidentu“ veškeré akce a postupy, jejichž cílem je ***incidentu předejít,*** odhalit ***jej***, analyzovat, zamezit jeho šíření a reagovat na něj;

Pozměňovací návrh 94

Návrh směrnice
Čl. 4 – odst. 1 – bod 7a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	7a) „rizikem“ potenciální ztráta nebo narušení v důsledku incidentu, přičemž toto riziko je vyjádřeno jako kombinace rozsahu takové ztráty nebo takového narušení a pravděpodobnosti vzniku tohoto incidentu;

Pozměňovací návrh 95

Návrh směrnice
Čl. 4 – odst. 1 – bod 11

Znění navržené Komisí	*Pozměňovací návrh*
11) „technickou specifikací“ technická	11) „technickou specifikací“ technická

specifikace ***ve smyslu*** čl. 2 ***bodu 4*** nařízení (EU) č. ***1025***/***2012***;	specifikace ***podle definice v*** čl. 2 ***bodě 20*** nařízení (EU) č. ***2019***/***881***;

Pozměňovací návrh 96

Návrh směrnice
Čl. 4 – odst. 1 – bod 13

Znění navržené Komisí	*Pozměňovací návrh*
13) „systémem doménových jmen (DNS)“ hierarchický distribuovaný systém doménových jmen, který umožňuje ***koncovým uživatelům přístup ke službám*** a ***zdrojům na*** internetu;	13) „systémem doménových jmen (DNS)“ hierarchický distribuovaný systém doménových jmen, který umožňuje ***identifikaci internetových služeb a zdrojů*** a ***současně umožňuje, aby zařízení koncových uživatelů využívala služby směrování*** internetu ***a připojení za účelem přístupu k těmto službám a zdrojům***;

Pozměňovací návrh 97

Návrh směrnice
Čl. 4 – odst. 1 – bod 14

Znění navržené Komisí	*Pozměňovací návrh*
14) „poskytovatelem služeb systému doménových jmen (DNS)“ subjekt, který poskytuje ***rekurzívní nebo autoritativní služby pro překlad doménových jmen koncovým uživatelům internetu a dalším poskytovatelům služeb DNS;***	14) „poskytovatelem služeb systému doménových jmen (DNS)“ subjekt, který poskytuje***:***

Pozměňovací návrh 98

Návrh směrnice
Čl. 4 – odst. 1 – bod 14 – písm. a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	a) otevřené a veřejné rekurzívní služby pro překlad doménových jmen koncovým uživatelům internetu; nebo

Pozměňovací návrh 99

Návrh směrnice
Čl. 4 – odst. 1 – bod 14 – písm. b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	b) autoritativní služby pro překlad doménových jmen jako službu, kterou mohou zajistit subjekty třetích stran;

Pozměňovací návrh 100

Návrh směrnice
Čl. 4 – odst. 1 – bod 15

Znění navržené Komisí	*Pozměňovací návrh*
15) „registrem internetových domén nejvyšší úrovně“ subjekt, kterému byla delegována konkrétní TLD a je odpovědný za správu TLD, včetně registrace doménových jmen v rámci TLD a technického provozu TLD, včetně provozu jejích jmenných serverů, vedení jejích databází a distribuce souborů zón TLD mezi jmennými servery;	15) „registrem internetových domén nejvyšší úrovně“ subjekt, kterému byla delegována konkrétní TLD a je odpovědný za správu TLD, včetně registrace doménových jmen v rámci TLD a technického provozu TLD, včetně provozu jejích jmenných serverů, vedení jejích databází a distribuce souborů zón TLD mezi jmennými servery***, bez ohledu na to, zda kteroukoli z těchto operací provádí subjekt nebo je zajišťována externě***;

Pozměňovací návrh 101

Návrh směrnice
Čl. 4 – odst. 1 – bod 15 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	15a) „službami registrace doménových jmen“ služby poskytované registry a registrátory doménových jmen, poskytovateli služeb ochrany osobních údajů nebo registrace proxy serverů, makléři nebo prodejci domén a jakékoli další služby, které souvisí s registrací doménových jmen;

Pozměňovací návrh 102

Návrh směrnice
Čl. 4 – odst. 1 – bod 23 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	23a) „veřejnou sítí elektronických komunikací“ veřejná síť elektronických komunikací ve smyslu definice v čl. 2 bodu 8 směrnice (EU) 2018/1972;

Pozměňovací návrh 103

Návrh směrnice
Čl. 4 – odst. 1 – bod 23 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	23b) „službou elektronických komunikací“ služba elektronických komunikací ve smyslu definice v čl. 2 bodu 4 směrnice (EU) 2018/1972;

Pozměňovací návrh 104

Návrh směrnice
Čl. 5 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Každý členský stát přijme národní strategii kybernetické bezpečnosti, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji. Národní strategie kybernetické bezpečnosti zahrnuje zejména:	1. Každý členský stát přijme národní strategii kybernetické bezpečnosti, ve které vymezí strategické cíle***, technické, organizační a finanční zdroje potřebné k jejich dosažení*** a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji. Národní strategie kybernetické bezpečnosti zahrnuje zejména:

Pozměňovací návrh 105

Návrh směrnice
Čl. 5 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) definici cílů a priorit strategie kybernetické bezpečnosti ***členských států***;	a) definici cílů a priorit strategie kybernetické bezpečnosti ***členského státu***;

Pozměňovací návrh 106

Návrh směrnice
Čl. 5 – odst. 1 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) správní rámec pro naplnění těchto cílů a priorit, včetně politik uvedených v odstavci 2 ***a úloh a povinností veřejných orgánů a subjektů i dalších relevantních subjektů***;	b) správní rámec pro naplnění těchto cílů a priorit, včetně politik uvedených v odstavci 2;

Pozměňovací návrh 107

Návrh směrnice
Čl. 5 – odst. 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) rámec pro přiřazení úloh a povinností veřejných orgánů a subjektů i dalších relevantních aktérů na podporu spolupráce a koordinace na vnitrostátní úrovni mezi příslušnými orgány určenými podle čl. 7 odst. 1 a čl. 8 odst. 1, jednotným kontaktním místem určeným podle čl. 8 odst. 3 a týmy CSIRT určenými podle článku 9;

Pozměňovací návrh 108

Návrh směrnice
Čl. 5 – odst. 1 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) seznam různých orgánů a subjektů zapojených do provádění národní strategie kybernetické bezpečnosti;	e) seznam různých orgánů a subjektů zapojených do provádění národní strategie kybernetické bezpečnosti***, včetně kontaktního místa pro kybernetickou bezpečnost pro malé a střední podniky, které poskytuje podporu při provádění konkrétních opatření v oblasti kybernetické bezpečnosti***;

Pozměňovací návrh 109

Návrh směrnice
Čl. 5 – odst. 1 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) politický rámec pro lepší koordinaci mezi příslušnými orgány podle této směrnice a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX[38] [směrnice o odolnosti kritických subjektů] pro účely sdílení informací o incidentech a kybernetických hrozbách pro výkon úkolů v oblasti dohledu.	f) politický rámec pro lepší koordinaci mezi příslušnými orgány podle této směrnice a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX[38] [směrnice o odolnosti kritických subjektů]***, jak na vnitrostátní úrovni, tak i mezi členskými státy,*** pro účely sdílení informací o incidentech a kybernetických hrozbách pro výkon úkolů v oblasti dohledu.
[38] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]	[38] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

Pozměňovací návrh 110

Návrh směrnice
Čl. 5 – odst. 1 – písm. f a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	fa) posouzení obecné úrovně povědomí občanů o kybernetické bezpečnosti.

Pozměňovací návrh 111

Návrh směrnice
Čl. 5 – odst. 2 – point -a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	-a) politiku týkající se kybernetické bezpečnosti pro každé odvětví, na něž se vztahuje tato směrnice;

Pozměňovací návrh 112

Návrh směrnice
Čl. 5 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) pokyny týkající se zařazení a specifikace požadavků na kybernetickou bezpečnost produktů a služeb IKT při zadávání veřejných zakázek;	b) pokyny týkající se zařazení a specifikace požadavků na kybernetickou bezpečnost produktů a služeb IKT při zadávání veřejných zakázek***, a to i pokud jde o požadavky na šifrování a o využívání produktů kybernetické bezpečnosti s otevřeným zdrojovým kódem***;

Pozměňovací návrh 113

Návrh směrnice
Čl. 5 – odst. 2 – písm. d

Znění navržené Komisí	*Pozměňovací návrh*
d) politiku týkající se udržení celkové dostupnosti a integrity veřejného jádra otevřeného internetu;	d) politiku týkající se udržení celkové dostupnosti a integrity veřejného jádra otevřeného internetu***, včetně kybernetické bezpečnosti podmořských komunikačních kabelů***;

Pozměňovací návrh 114

Návrh směrnice
Čl. 5 – odst. 2 – písm. d a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	da) politiku na podporu rozvoje a integrace nových technologií, jako je umělá inteligence, v rámci nástrojů a aplikací zvyšujících kybernetickou bezpečnost;

Pozměňovací návrh 115

Návrh směrnice
Čl. 5 – odst. 2 – písm. d b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	db) politiku na podporu integrace nástrojů a aplikací s otevřeným zdrojovým kódem;

Pozměňovací návrh 116

Návrh směrnice
Čl. 5 – odst. 2 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) politiku za účelem podpory akademických a výzkumných institucí při vývoji nástrojů kybernetické bezpečnosti a zabezpečené síťové infrastruktury;	f) politiku za účelem podpory akademických a výzkumných institucí při vývoji***, zlepšování a zavádění*** nástrojů kybernetické bezpečnosti a zabezpečené síťové infrastruktury;

Pozměňovací návrh 117

Návrh směrnice
Čl. 5 – odst. 2 – písm. h

Znění navržené Komisí	*Pozměňovací návrh*
h) politiku ***řešící zvláštní potřeby***	h) politiku ***na podporu kybernetické***

malých a ***středních podniků***, ***zejména*** těch, které nespadají do oblasti působnosti této směrnice, ***v souvislosti s*** pokyny a ***podporou při zlepšování jejich odolnosti vůči kybernetickým hrozbám.***	***bezpečnosti malých*** a ***středních podniků***, ***včetně*** těch, které nespadají do oblasti působnosti této směrnice, ***která řeší jejich specifické potřeby a poskytuje snadno dostupné*** pokyny a ***podporu, mimo jiné pokyny k řešení výzev v rámci dodavatelského řetězce;***

Pozměňovací návrh 118

Návrh směrnice
Čl. 5 – odst. 2 – písm. h a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ha) politiku na podporu kybernetické hygieny zahrnující základní soubor postupů a kontrol a zvyšování obecného povědomí občanů o kybernetických bezpečnostních hrozbách a osvědčených postupech;

Pozměňovací návrh 119

Návrh směrnice
Čl. 5 – odst. 2 – písm. h b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	hb) politiku na podporu aktivní kybernetické obrany.

Pozměňovací návrh 120

Návrh směrnice
Čl. 5 – odst. 2 – písm. h c (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	hc) politiku, která orgánům pomůže rozvíjet kompetence a porozumění v oblasti bezpečnostních záležitostí pro účely navrhování, výstavby a řízení propojených míst;

Pozměňovací návrh 121

Návrh směrnice
Čl. 5 – odst. 2 – písm. h d (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	hd) politiku zaměřenou konkrétně na hrozbu útoků prostřednictvím vyděračského softwaru (ransomware) a narušování obchodního modelu těchto útoků;

Pozměňovací návrh 122

Návrh směrnice
Čl. 5 – odst. 2 – písm. h e (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	he) politiku, včetně příslušných postupů a správních rámců, na podporu a prosazování vytváření partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 123

Návrh směrnice
Čl. 5 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Členské státy oznámí své národní strategie kybernetické bezpečnosti Komisi do tří měsíců od jejich přijetí. Členské státy mohou z oznámení vyloučit konkrétní informace, pokud je to ***naprosto*** nezbytné pro zachování národní bezpečnosti.	3. Členské státy oznámí své národní strategie kybernetické bezpečnosti Komisi do tří měsíců od jejich přijetí. Členské státy mohou z oznámení vyloučit konkrétní informace, pokud je to nezbytné pro zachování národní bezpečnosti.

Pozměňovací návrh 124

Návrh směrnice
Čl. 5 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Členské státy posuzují své národní strategie kybernetické bezpečnosti alespoň každé čtyři roky podle klíčových ukazatelů výkonnosti a v případě potřeby je změní. Při zpracování národní strategie a klíčových ukazatelů výkonnosti pro posouzení strategie poskytuje členským státům na jejich žádost součinnost Evropská agentura pro bezpečnost sítí a informací (ENISA).	4. Členské státy posuzují své národní strategie kybernetické bezpečnosti alespoň každé čtyři roky podle klíčových ukazatelů výkonnosti a v případě potřeby je změní. Při zpracování národní strategie a klíčových ukazatelů výkonnosti pro posouzení strategie poskytuje členským státům na jejich žádost součinnost Evropská agentura pro bezpečnost sítí a informací (ENISA). ***Agentura ENISA poskytne členským státům pokyny s cílem uvést své již formulované vnitrostátní strategie kybernetické bezpečnosti do souladu s požadavky a povinnostmi stanovenými v této směrnici.***

Pozměňovací návrh 125

Návrh směrnice
Čl. 6 – název

Znění navržené Komisí	*Pozměňovací návrh*
Koordinované ***zveřejňování informací o zranitelnostech*** a ***Evropský registr*** zranitelností	Koordinované ***odhalování zranitelností*** a ***Evropská databáze*** zranitelností

Pozměňovací návrh 126

Návrh směrnice
Čl. 6 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Každý členský stát určí jeden ze svých týmů CSIRT podle článku 9 jako koordinátora za účelem koordinovaného ***zveřejňování informací o zranitelnostech***. Tento určený tým CSIRT vystupuje jako	1. Každý členský stát určí jeden ze svých týmů CSIRT podle článku 9 jako koordinátora za účelem koordinovaného ***odhalování zranitelností***. Tento určený tým CSIRT vystupuje jako důvěryhodný

důvěryhodný zprostředkovatel, který ***v případě potřeby*** usnadňuje interakci mezi oznamujícím subjektem a výrobcem nebo poskytovatelem produktů nebo služeb IKT. Pokud se hlášená zranitelnost týká více výrobců nebo poskytovatelů produktů nebo služeb IKT v celé Unii, spolupracuje určený tým CSIRT z každého členského státu v rámci sítě CSIRT.	zprostředkovatel, který ***na žádost oznamujícího subjektu*** usnadňuje interakci mezi oznamujícím subjektem a výrobcem nebo poskytovatelem produktů nebo služeb IKT. Pokud se hlášená zranitelnost týká více výrobců nebo poskytovatelů produktů nebo služeb IKT v celé Unii, spolupracuje určený tým CSIRT z každého členského státu v rámci sítě CSIRT.

Pozměňovací návrh 127

Návrh směrnice
Čl. 6 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Agentura ENISA vytvoří a spravuje ***Evropský registr*** zranitelností. Za tímto účelem ENISA zřídí a spravuje informační systémy, politiky a postupy s cílem zejména umožnit důležitým a základním subjektům a jejich dodavatelům sítí a informačních systémů odhalovat a registrovat zranitelná místa v produktech nebo službách IKT ***a poskytovat*** přístup k informacím o ***těchto zranitelnostech*** uvedeným v ***registru všem zúčastněným stranám***. V ***registru*** jsou zejména uvedeny informace popisující ***slabé*** místo, dotčený produkt IKT nebo služby IKT ***a*** závažnost této zranitelnosti z hlediska okolností, za nichž může být využita, dostupnost příslušných oprav***, a*** pokud opravy nejsou dostupné, pokyny pro uživatele zranitelných produktů a služeb, jak ***mohou být*** rizika vyplývající z odhalených ***slabých*** míst ***zmírněna***.	2. Agentura ENISA vytvoří a spravuje ***Evropskou databázi zranitelností s využitím globálního registru společných*** zranitelností ***a expozic (CVE)***. Za tímto účelem ENISA zřídí a spravuje informační systémy, politiky a postupy ***a přijme technická a organizační opatření nezbytná k zajištění bezpečnosti a integrity databáze*** s cílem zejména umožnit důležitým a základním subjektům a jejich dodavatelům sítí a informačních systémů***, jakož i subjektům, které nespadají do působnosti této směrnice, a jejich dodavatelům,*** odhalovat a registrovat zranitelná místa v produktech nebo službách IKT***. Všem zúčastněným stranám je poskytnut*** přístup k informacím o ***zranitelných místech*** uvedeným v ***databázi, u nichž je možnost oprav nebo zmírňujících opatření***. V ***databázi*** jsou zejména uvedeny informace popisující ***zranitelné*** místo, dotčený produkt IKT nebo služby IKT***,*** závažnost této zranitelnosti z hlediska okolností, za nichž může být využita, ***a*** dostupnost příslušných oprav***.*** Pokud opravy nejsou dostupné, ***jsou součástí databáze i*** pokyny pro uživatele zranitelných produktů a služeb ***IKT ohledně toho***, jak ***lze*** rizika vyplývající z odhalených ***zranitelných*** míst ***zmírnit***.

Pozměňovací návrh 128

Návrh směrnice
Čl. 7 – odst. 1 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	1a. Pokud členský stát určí více než jeden příslušný orgán uvedený v odstavci 1, jasně uvede, který z těchto příslušných orgánů bude působit jako koordinátor pro řešení rozsáhlých incidentů a krizí.

Pozměňovací návrh 129

Návrh směrnice
Čl. 7 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Každý členský stát určí kapacity, prostředky a postupy, které mohou být nasazeny v případě krize pro účely této směrnice.	*(Netýká se českého znění.)*

Pozměňovací návrh 130

Návrh směrnice
Čl. 7 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Členské státy oznámí Komisi své určené příslušné orgány podle odstavce 1 a předloží své národní plány reakce na kybernetické bezpečnostní incidenty a krize podle odstavce 3 do tří měsíců od tohoto určení a přijetí těchto plánů. Členské státy mohou z plánu vyloučit konkrétní informace, pokud je to naprosto nezbytné pro jejich národní bezpečnost.	4. Členské státy oznámí Komisi své určené příslušné orgány podle odstavce 1 a předloží ***síti EU-CyCLONe*** své národní plány reakce na kybernetické bezpečnostní incidenty a krize podle odstavce 3 do tří měsíců od tohoto určení a přijetí těchto plánů. Členské státy mohou z plánu vyloučit konkrétní informace, pokud je to naprosto nezbytné pro jejich národní bezpečnost.

Pozměňovací návrh 131

Návrh směrnice
Čl. 8 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Každý členský stát určí ***jedno*** vnitrostátní jednotné kontaktní místo pro kybernetickou bezpečnost („jednotné kontaktní místo“). Určí-li členský stát pouze jeden příslušný orgán, je tento orgán rovněž jednotným kontaktním místem pro tento členský stát.	3. Každý členský stát určí ***jeden z příslušných orgánů uvedených v odstavci 1 jako*** vnitrostátní jednotné kontaktní místo pro kybernetickou bezpečnost (***dále jen*** „jednotné kontaktní místo“). Určí-li členský stát pouze jeden příslušný orgán, je tento orgán rovněž jednotným kontaktním místem pro tento členský stát.

Pozměňovací návrh 132

Návrh směrnice
Čl. 8 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Každé jednotné kontaktní místo plní styčnou funkci pro účely přeshraniční spolupráce orgánů svého členského státu s příslušnými orgány v jiných členských státech a také meziodvětvové spolupráce s jinými příslušnými vnitrostátními orgány ve svém členském státě.	4. Každé jednotné kontaktní místo plní styčnou funkci pro účely přeshraniční spolupráce orgánů svého členského státu s příslušnými orgány v jiných členských státech***, s Komisí a s agenturou ENISA*** a také ***pro účely*** meziodvětvové spolupráce s jinými příslušnými vnitrostátními orgány ve svém členském státě.

Pozměňovací návrh 133

Návrh směrnice
Čl. 9 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 10 odst. 2.	2. Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje ***a disponoval technickými dovednostmi*** pro účinné plnění svých úkolů podle čl. 10

odst. 2.

Pozměňovací návrh 134

Návrh směrnice
Čl. 9 – odst. 6 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	6a. Členské státy zajistí možnost účinné, účelné a bezpečné výměny informací na všech stupních utajení mezi svými vlastními týmy CSIRT a týmy CSIRT ze třetích zemí na stejném stupni utajení.

Pozměňovací návrh 135

Návrh směrnice
Čl. 9 – odst. 6 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	6b. Aniž by byly dotčeny právní předpisy Unie, zejména nařízení (EU) 2016/679, týmy CSIRT spolupracují s týmy CSIRT nebo rovnocennými orgány z kandidátských zemí Unie a jiných třetích zemí na západním Balkáně a ve Východním partnerství, a je-li to možné, poskytují jim podporu v oblasti kybernetické bezpečnosti.

Pozměňovací návrh 136

Návrh směrnice
Čl. 9 – odst. 7

Znění navržené Komisí	*Pozměňovací návrh*
7. Členské státy bez zbytečného odkladu oznámí Komisi týmy CSIRT určené podle odstavce 1**,** koordinátora CSIRT určeného podle čl. 6 odst. 1 ***a*** jejich	7. Členské státy bez zbytečného odkladu oznámí Komisi týmy CSIRT určené podle odstavce 1 ***a*** koordinátora CSIRT určeného podle čl. 6 odst. 1***, včetně***

úkoly stanovené v souvislosti se subjekty uvedenými v přílohách I a ***II***.	jejich ***úkolů stanovených ve vztahu k základním*** a ***důležitým subjektům***.

Pozměňovací návrh 137

Návrh směrnice
Čl. 10 – název

Znění navržené Komisí	*Pozměňovací návrh*
Požadavky na týmy CSIRT a jejich úkoly	Požadavky na týmy CSIRT a jejich ***technické dovednosti a*** úkoly

Pozměňovací návrh 138

Návrh směrnice
Čl. 10 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) týmy CSIRT jsou vybaveny vhodným systémem ***řízení*** a ***směrování*** požadavků, zejména pro usnadnění účelného a efektivního předávání;	c) týmy CSIRT jsou vybaveny vhodným systémem ***pro klasifikaci, směrování*** a ***sledování*** požadavků, zejména pro usnadnění účelného a efektivního předávání;

Pozměňovací návrh 139

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

Znění navržené Komisí	*Pozměňovací návrh*
	ca) týmy CSIRT musí mít zavedeny vhodné kodexy chování, aby byla zajištěna důvěrnost a důvěryhodnost jejich fungování;

Pozměňovací návrh 140

Návrh směrnice
Čl. 10 – odst. 1 – písm. d

Znění navržené Komisí	*Pozměňovací návrh*
d) týmy CSIRT jsou náležitě personálně obsazeny tak, aby byly kdykoli k dispozici;	d) týmy CSIRT jsou náležitě personálně obsazeny tak, aby byly kdykoli k dispozici ***a zajistily vhodné rámce odborné přípravy svých zaměstnanců***;

Pozměňovací návrh 141

Návrh směrnice
Čl. 10 – odst. 1 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) týmy CSIRT jsou vybaveny redundantními systémy a záložním pracovním prostorem pro zajištění kontinuity jejich služeb;	e) týmy CSIRT jsou vybaveny redundantními systémy a záložním pracovním prostorem pro zajištění kontinuity jejich služeb***, včetně široké konektivity napříč sítěmi, informačních systémů, služeb a zařízení***;

Pozměňovací návrh 142

Návrh směrnice
Čl. 10 – odst. 1 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	1a. Týmy CSIRT si osvojí alespoň tyto technické dovednosti:
	a) schopnost provádět monitorování sítí a informačních systémů v reálném čase nebo téměř v reálném čase a odhalovat anomálie;
	b) schopnost podporovat prevenci a odhalování průniku;
	c) schopnost shromažďovat údaje a provádět komplexní forenzní analýzu údajů a reverzní inženýrství kybernetických hrozeb;

	d) schopnost filtrovat škodlivý provoz na internetu;
	e) schopnost prosazovat přísné ověřování, přístupová práva a kontroly vstupu; a
	f) schopnost analyzovat kybernetické hrozby.

Pozměňovací návrh 143

Návrh směrnice
Čl. 10 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) monitorování kybernetických hrozeb, zranitelností a incidentů na vnitrostátní úrovni;	a) monitorování kybernetických hrozeb, zranitelností a incidentů na vnitrostátní úrovni ***a získávání zpravodajských informací o hrozbách v reálném čase***;

Pozměňovací návrh 144

Návrh směrnice
Čl. 10 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) vydávání včasných varování a upozornění, oznamování a šíření informací o kybernetických hrozbách, zranitelnostech a incidentech základním a důležitým subjektům a dalším příslušným zúčastněným stranám;	b) vydávání včasných varování a upozornění, oznamování a šíření informací o kybernetických hrozbách, zranitelnostech a incidentech základním a důležitým subjektům a dalším příslušným zúčastněným stranám***, pokud možno v téměř reálném čase***;

Pozměňovací návrh 145

Návrh směrnice
Čl. 10 – odst. 2 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) reakce na incidenty;	c) reakce na incidenty ***a poskytování***

pomoci zúčastněným subjektům;

Pozměňovací návrh 146

Návrh směrnice
Čl. 10 – odst. 2 – písm. e

Znění navržené Komisí	*Pozměňovací návrh*
e) provádění aktivního skenování sítě a informačních systémů používaných k poskytování služeb subjektu***, který o to požádal***;	e) provádění aktivního skenování sítě a informačních systémů používaných k poskytování služeb subjektu ***na základě jeho žádosti nebo v případě závažného ohrožení národní bezpečnosti***;

Pozměňovací návrh 147

Návrh směrnice
Čl. 10 – odst. 2 – písm. f a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	fa) na žádost subjektu umožnění a konfigurace protokolování sítě za účelem ochrany údajů, včetně osobních údajů, před jejich neoprávněnou exfiltrací;

Pozměňovací návrh 148

Návrh směrnice
Čl. 10 – odst. 2 – písm. f b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	fb) podpora zavádění bezpečných nástrojů pro sdílení informací podle čl. 9 odst. 3.

Pozměňovací návrh 149

Návrh směrnice
Čl. 10 – odst. 4 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
4. V zájmu usnadnění spolupráce prosazují týmy CSIRT přijetí a používání společných či standardních postupů, klasifikace a taxonomie v oblasti:	4. V zájmu usnadnění spolupráce prosazují týmy CSIRT ***automatizaci výměny informací,*** přijetí a používání společných či standardních postupů, klasifikace a taxonomie v oblasti:

Pozměňovací návrh 150

Návrh směrnice
Čl. 11 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby ***buď*** jejich ***příslušné orgány, nebo*** týmy CSIRT obdržely hlášení o incidentech a ***významných*** kybernetických hrozbách a ***o*** případech, kdy téměř došlo k incidentu, ***podaná*** podle ***této směrnice. Pokud členský stát rozhodne, že jeho týmy CSIRT nemají tato hlášení přijímat, bude týmům CSIRT*** v ***rozsahu nezbytném pro plnění jejich úkolů povolen přístup k údajům o incidentech hlášených základními nebo důležitými subjekty podle článku 20.***	2. Členské státy zajistí, aby jejich týmy CSIRT obdržely hlášení o ***významných*** incidentech ***podle článku 20*** a ***o*** kybernetických hrozbách a případech, kdy téměř došlo k incidentu, podle ***článku 27 prostřednictvím jednotného kontaktního místa uvedeného*** v ***čl. 20 odst. 4a.***

Pozměňovací návrh 151

Návrh směrnice
Čl. 11 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. V rozsahu nezbytném pro účelné plnění úkolů a povinností stanovených touto směrnicí zajistí členské státy vhodnou spolupráci mezi příslušnými orgány ***a*** jednotnými kontaktními místy ***a*** donucovacími orgány, úřady pro ochranu	4. V rozsahu nezbytném pro účelné plnění úkolů a povinností stanovených touto směrnicí zajistí členské státy vhodnou spolupráci mezi příslušnými orgány***,*** jednotnými kontaktními místy***,*** ***týmy CSIRT,*** donucovacími orgány***,***

osobních údajů a orgány odpovědnými za kritickou infrastrukturu podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] a vnitrostátními finančními orgány určenými v souladu s nařízením Evropského parlamentu a Rady (EU) XXXX/XXXX[39] [nařízení DORA] v daném členském státě.	***vnitrostátními regulačními orgány nebo jinými příslušnými orgány odpovědnými za veřejné sítě elektronické komunikace nebo veřejně dostupné služby elektronických komunikací ve smyslu směrnice (EU) 2018/1972***, úřady pro ochranu osobních údajů a orgány odpovědnými za kritickou infrastrukturu podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] a vnitrostátními finančními orgány určenými v souladu s nařízením Evropského parlamentu a Rady (EU) XXXX/XXXX39 [nařízení DORA] v daném členském státě***, a to v souladu s jejich příslušnými kompetencemi***.
[39] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]	[39] [vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]

Pozměňovací návrh 152

Návrh směrnice
Čl. 11 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Členské státy zajistí, aby jejich příslušné orgány pravidelně poskytovaly informace příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] o kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech postihujících základní subjekty určené jako kritické nebo jako subjekty rovnocenné kritickým subjektům podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů], jakož i o opatřeních, jež příslušné orgány přijaly v reakci na tato rizika a incidenty.	5. Členské státy zajistí, aby jejich příslušné orgány pravidelně ***a včas*** poskytovaly informace příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] o kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech postihujících základní subjekty určené jako kritické nebo jako subjekty rovnocenné kritickým subjektům podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů], jakož i o opatřeních, jež příslušné orgány přijaly v reakci na tato rizika a incidenty.

Pozměňovací návrh 153

Návrh směrnice
Čl. 12 – odst. 3 – pododstavec 1

Znění navržené Komisí	*Pozměňovací návrh*
Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Činností skupiny pro spolupráci se jako ***pozorovatel*** účastní Evropská služba pro vnější činnost. Činností skupiny pro spolupráci se mohou účastnit evropské orgány dohledu v souladu s čl. 17 odst. 5 písm. c) nařízení (EU) XXXX/XXXX [nařízení DORA].	Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Činností skupiny pro spolupráci se jako ***pozorovatelé*** účastní ***Evropský parlament a*** Evropská služba pro vnější činnost. Činností skupiny pro spolupráci se mohou účastnit evropské orgány dohledu v souladu s čl. 17 odst. 5 písm. c) nařízení (EU) XXXX/XXXX [nařízení DORA].

Pozměňovací návrh 154

Návrh směrnice
Čl. 12 – odst. 3 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
Tam, kde je to vhodné, může skupina pro spolupráci přizvat ke spolupráci zástupce příslušných zúčastněných stran.	Tam, kde je to vhodné, může skupina pro spolupráci přizvat ke spolupráci zástupce příslušných zúčastněných stran***, například Evropský sbor pro ochranu osobních údajů a zástupce odvětví***.

Pozměňovací návrh 155

Návrh směrnice
Čl. 12 – odst. 4 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) vyměňovat si osvědčené postupy a informace související s uplatňováním této směrnice, včetně informací souvisejících s kybernetickými hrozbami, incidenty, zranitelnostmi, případy, kdy téměř došlo k incidentu, iniciativami zaměřenými na zvyšování informovanosti, školením, cvičením a dovednostmi, budováním kapacit, jakož i ***normami*** a ***technickými***	b) vyměňovat si osvědčené postupy a informace související s uplatňováním této směrnice, včetně informací souvisejících s kybernetickými hrozbami, incidenty, zranitelnostmi, případy, kdy téměř došlo k incidentu, iniciativami zaměřenými na zvyšování informovanosti, školením, cvičením a dovednostmi, budováním kapacit, ***normami a technickými***

specifikacemi;	***specifikacemi,*** jakož i ***určováním základních*** a ***důležitých subjektů***;

Pozměňovací návrh 156

Návrh směrnice
Čl. 12 – odst. 4 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) mapovat vnitrostátní řešení s cílem podporovat kompatibilitu řešení v oblasti kybernetické bezpečnosti uplatňovaných v každém konkrétním odvětví v celé Unii;

Pozměňovací návrh 157

Návrh směrnice
Čl. 12 – odst. 4 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) vyměňovat si doporučení a spolupracovat s Komisí na nových politických iniciativách v oblasti kybernetické bezpečnosti;	c) vyměňovat si doporučení a spolupracovat s Komisí na nových politických iniciativách v oblasti kybernetické bezpečnosti ***a na celkové soudržnosti odvětvových požadavků na kybernetickou bezpečnost***;

Pozměňovací návrh 158

Návrh směrnice
Čl. 12 – odst. 4 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) projednávat zprávy o vzájemném hodnocení podle čl. 16 odst. 7;	f) projednávat zprávy o vzájemném hodnocení podle čl. 16 odst. 7 ***a vypracovávat závěry a doporučení***;

Pozměňovací návrh 159

Návrh směrnice
Čl. 12 – odst. 4 – písm. f a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	fa) provádět koordinovaná posouzení bezpečnostních rizik, která mohou být zahájena podle čl. 19 odst. 1 ve spolupráci s Komisí a agenturou ENISA;

Pozměňovací návrh 160

Návrh směrnice
Čl. 12 – odst. 4 – písm. k a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ka) předkládat Komisi zprávy o zkušenostech získaných na strategické a operativní úrovni pro účely přezkumu uvedeného v článku 35;

Pozměňovací návrh 161

Návrh směrnice
Čl. 12 – odst. 4 – písm. k b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	kb) provádět každoročně ve spolupráci s agenturou ENISA, Europolem a vnitrostátními donucovacími orgány hodnocení toho, které státy poskytují útočiště pachatelům trestných činů využívajících vyděračský software (ransomware).

Pozměňovací návrh 162

Návrh směrnice
Čl. 12 – odst. 8

Znění navržené Komisí	*Pozměňovací návrh*
8. Skupina pro spolupráci se schází pravidelně, alespoň ***jednou*** ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za účelem ***podpory*** strategické spolupráce a výměny informací.	8. Skupina pro spolupráci se schází pravidelně, alespoň ***dvakrát*** ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za účelem ***usnadnění*** strategické spolupráce a výměny informací.

Pozměňovací návrh 163

Návrh směrnice
Čl. 13 – odst. 3 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) usnadňuje sdílení a přenos technologií a příslušných opatření, politik, osvědčených postupů a rámců mezi týmy CSIRT;

Pozměňovací návrh 164

Návrh směrnice
Čl. 13 – odst. 3 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) zajišťuje interoperabilitu, pokud jde o normy pro sdílení informací;

Pozměňovací návrh 165

Návrh směrnice
Čl. 14 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na	1. Za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na

operační úrovni a pro zajištění pravidelné výměny informací mezi členskými státy a institucemi, orgány a agenturami Unie se tímto zřizuje Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe).

operační úrovni a pro zajištění pravidelné výměny ***relevantních*** informací mezi členskými státy a institucemi, orgány a agenturami Unie se tímto zřizuje Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe).

Pozměňovací návrh 166

Návrh směrnice
Čl. 14 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Síť EU-CyCLONe je tvořena zástupci orgánů krizového řízení členských států určených podle článku 7, Komise a agentury ENISA. Agentura ENISA zajišťuje služby sekretariátu a podporuje bezpečnou výměnu informací.	2. Síť EU-CyCLONe je tvořena zástupci orgánů krizového řízení členských států určených podle článku 7, Komise a agentury ENISA. Agentura ENISA zajišťuje služby sekretariátu ***sítě EU-CyCLONe*** a podporuje bezpečnou výměnu informací.

Pozměňovací návrh 167

Návrh směrnice
Čl. 14 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Síť EU-CyCLONe pravidelně podává skupině pro spolupráci zprávy o ***kybernetických hrozbách,*** incidentech ***a*** trendech***,*** se zvláštním zaměřením na jejich dopad na základní a důležité subjekty.	5. Síť EU-CyCLONe pravidelně podává skupině pro spolupráci zprávy o ***rozsáhlých*** incidentech ***a krizích i o*** trendech se zvláštním zaměřením na jejich dopad na základní a důležité subjekty.

Pozměňovací návrh 168

Návrh směrnice
Čl. 15 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Agentura ENISA ve spolupráci s	1. Agentura ENISA ve spolupráci s

Komisí vydává jednou za dva roky zprávu o stavu kybernetické bezpečnosti v Unii. Ve ***zprávě*** uvede zejména posouzení:	Komisí vydává jednou za dva roky zprávu o stavu kybernetické bezpečnosti v Unii ***a tuto zprávu předkládá a prezentuje Evropskému parlamentu***. ***Zprávu dodá*** ve ***strojově čitelném formátu a*** uvede ***v ní*** zejména posouzení:

Pozměňovací návrh 169

Návrh směrnice
Čl. 15 – odst. 1 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) obecné úrovně informovanosti a hygieny v oblasti kybernetické bezpečnosti mezi občany a subjekty, včetně malých a středních podniků, jakož i obecné úrovně bezpečnosti připojených zařízení;

Pozměňovací návrh 170

Návrh směrnice
Čl. 15 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) indexu kybernetické bezpečnosti umožňující agregované posouzení úrovně vyspělosti kapacit v oblasti kybernetické bezpečnosti.	c) indexu kybernetické bezpečnosti umožňující agregované posouzení úrovně vyspělosti kapacit v oblasti kybernetické bezpečnosti ***v celé Unii, včetně sladění národních strategií kybernetické bezpečnosti členských států***.

Pozměňovací návrh 171

Návrh směrnice
Čl. 15 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Ve zprávě uvede konkrétní doporučení k této oblasti politiky zaměřená	2. Ve zprávě uvede konkrétní ***překážky a*** doporučení k této oblasti politiky

na zvýšení úrovně kybernetické bezpečnosti v celé Unii a shrne zjištění za dané období z technických situačních zpráv EU v oblasti kybernetické bezpečnosti vydaných agenturou ENISA podle čl. 7 odst. 6 nařízení (EU) 2019/881.	zaměřená na zvýšení úrovně kybernetické bezpečnosti v celé Unii a shrne zjištění za dané období z technických situačních zpráv EU v oblasti kybernetické bezpečnosti vydaných agenturou ENISA podle čl. 7 odst. 6 nařízení (EU) 2019/881.

Pozměňovací návrh 172

Návrh směrnice
Čl. 15 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Agentura ENISA ve spolupráci s Komisí a podle pokynů od skupiny pro spolupráci a sítě CSIRT vypracuje metodiku, včetně příslušných proměnných indexu kybernetické bezpečnosti uvedeného v odst. 1 písm. e).

Pozměňovací návrh 173

Návrh směrnice
Čl. 16 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA stanoví nejpozději do 18 měsíců po vstupu této směrnice v platnost metodiku a obsah vzájemných hodnocení pro posuzování účelnosti politik členských států v oblasti kybernetické bezpečnosti. Hodnocení provádějí techničtí odborníci na kybernetickou bezpečnost z členských států ***jiných, než je posuzovaný členský stát***, přičemž hodnocení zahrnují alespoň:	1. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA stanoví nejpozději do 18 měsíců po vstupu této směrnice v platnost metodiku a obsah vzájemných hodnocení pro posuzování účelnosti politik členských států v oblasti kybernetické bezpečnosti. ***Vzájemná*** hodnocení provádějí ***při konzultacích s agenturou ENISA*** techničtí odborníci na kybernetickou bezpečnost z ***alespoň dvou*** členských států ***odlišných od posuzovaného členského státu***, přičemž hodnocení zahrnují alespoň:

Pozměňovací návrh 174

Návrh směrnice
Čl. 16 – odst. 1 – písm. iii

Znění navržené Komisí	*Pozměňovací návrh*
iii) provozní kapacity a účelnost týmů CSIRT;	iii) provozní kapacity a účelnost týmů CSIRT ***při vykonávání jejich úkolů***;

Pozměňovací návrh 175

Návrh směrnice
Čl. 16 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. O organizačních aspektech vzájemných hodnocení rozhoduje Komise za podpory agentury ENISA a po konzultaci se skupinou pro spolupráci je stanoví podle kritérií definovaných v metodice uvedené v odstavci 1. Při vzájemných hodnoceních se posuzují aspekty uvedené v odstavci 1 u všech členských států a odvětví, včetně cílené problematiky, která je specifická pro jeden nebo několik členských států nebo pro jedno nebo několik odvětví.	3. O organizačních aspektech vzájemných hodnocení rozhoduje Komise za podpory agentury ENISA a po konzultaci se skupinou pro spolupráci je stanoví podle kritérií definovaných v metodice uvedené v odstavci 1. Při vzájemných hodnoceních se posuzují aspekty uvedené v odstavci 1 u všech členských států a odvětví, včetně cílené problematiky, která je specifická pro jeden nebo několik členských států nebo pro jedno nebo několik odvětví. ***Určení odborníci provádějící hodnocení sdělí před jeho zahájením tuto cílenou problematiku členskému státu, na který se vzájemné hodnocení vztahuje.***

Pozměňovací návrh 176

Návrh směrnice
Čl. 16 – odst. 3 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	3a. Před zahájením procesu vzájemného hodnocení provede členský stát, na který se toto hodnocení vztahuje, sebehodnocení u posuzovaných aspektů a poskytne toto sebehodnocení určeným odborníkům.

Pozměňovací návrh 177

Návrh směrnice
Čl. 16 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Vzájemná hodnocení zahrnují skutečné nebo virtuální návštěvy na místě i externí výměny. S ohledem na zásadu dobré spolupráce poskytnou posuzované členské státy určeným odborníkům požadované informace potřebné k posouzení kontrolovaných aspektů. Veškeré informace získané v rámci procesu vzájemného hodnocení lze použít pouze pro tento účel. Odborníci účastnící se vzájemného hodnocení nesmí sdělit žádné citlivé nebo důvěrné informace získané v průběhu tohoto hodnocení žádným třetím stranám.	4. Vzájemná hodnocení zahrnují skutečné nebo virtuální návštěvy na místě i externí výměny. S ohledem na zásadu dobré spolupráce poskytnou posuzované členské státy určeným odborníkům požadované informace potřebné k posouzení kontrolovaných aspektů. ***Komise ve spolupráci s agenturou ENISA vypracuje vhodné kodexy chování, které budou tvořit základ pracovních metod určených odborníků.*** Veškeré informace získané v rámci procesu vzájemného hodnocení lze použít pouze pro tento účel. Odborníci účastnící se vzájemného hodnocení nesmí sdělit žádné citlivé nebo důvěrné informace získané v průběhu tohoto hodnocení žádným třetím stranám.

Pozměňovací návrh 178

Návrh směrnice
Čl. 16 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Členský stát zajistí, aby byly ostatní členské státy, Komise a agentura ENISA bez zbytečného odkladu informovány o případném riziku střetu zájmů týkajícím se určených odborníků.	6. Členský stát zajistí, aby byly ostatní členské státy, Komise a agentura ENISA ***před zahájením procesu vzájemného hodnocení*** bez zbytečného odkladu informovány o případném riziku střetu zájmů týkajícím se určených odborníků.

Pozměňovací návrh 179

Návrh směrnice
Čl. 16 – odst. 7

Znění navržené Komisí	*Pozměňovací návrh*
7. Odborníci účastnící se vzájemných hodnocení vypracují návrhy zpráv o zjištěních a závěrech hodnocení. Zprávy předloží Komisi, skupině pro spolupráci, síti CSIRT a agentuře ENISA. Zprávy se projednají ve skupině pro spolupráci a v síti CSIRT. Zprávy mohou být zveřejněny na vyhrazených internetových stránkách skupiny pro spolupráci.	7. Odborníci účastnící se vzájemných hodnocení vypracují návrhy zpráv o zjištěních a závěrech hodnocení. ***Zprávy obsahují doporučení s cílem dosáhnout zlepšení v aspektech, jichž se týká proces vzájemného hodnocení. Zprávy*** předloží Komisi, skupině pro spolupráci, síti CSIRT a agentuře ENISA. Zprávy se projednají ve skupině pro spolupráci a v síti CSIRT. Zprávy mohou být zveřejněny na vyhrazených internetových stránkách skupiny pro spolupráci ***s vyloučením citlivých a důvěrných informací***.

Pozměňovací návrh 180

Návrh směrnice
Čl. 17 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby členové vedoucího orgánu pravidelně absolvovali zvláštní školení, a ***získali tak dostatečné znalosti a dovednosti***, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na ***provoz subjektu***.	2. Členské státy zajistí, aby členové vedoucího orgánu ***základních a důležitých subjektů*** pravidelně absolvovali zvláštní školení, a ***vybízejí základní a důležité subjekty, aby nabízely podobné školení všem zaměstnancům***, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na ***služby poskytované subjektem***.

Pozměňovací návrh 181

Návrh směrnice
Čl. 18 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická ***a*** organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě	1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická***, provozní a*** organizační opatření k řízení

a informační systémy, jež tyto subjekty používají pro poskytování svých služeb. S ohledem na nejnovější technický vývoj musí tato opatření zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika.	bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro ***svůj provoz nebo*** poskytování svých služeb***, a k předcházení incidentům nebo minimalizaci jejich dopadů na příjemce jejich služeb a na další služby***. S ohledem na nejnovější technický vývoj ***a na evropské nebo mezinárodní normy*** musí tato opatření zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika.

Pozměňovací návrh 182

Návrh směrnice
Čl. 18 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) řešení incidentů ***(prevence a odhalování incidentů a reakce na ně)***;	b) řešení incidentů;

Pozměňovací návrh 183

Návrh směrnice
Čl. 18 – odst. 2 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) řízení kontinuity provozu a krizové řízení;	c) řízení kontinuity provozu***, jako např. správa zálohování*** a ***obnova provozu po havárii a*** krizové řízení;

Pozměňovací návrh 184

Návrh směrnice
Čl. 18 – odst. 2 – písm. d

Znění navržené Komisí	*Pozměňovací návrh*
d) zabezpečení dodavatelského řetězce včetně bezpečnostních aspektů týkajících	d) zabezpečení dodavatelského řetězce včetně bezpečnostních aspektů týkajících

se vztahů mezi každým subjektem a jeho dodavateli nebo poskytovateli ***služeb, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo řízených bezpečnostních*** služeb;	se vztahů mezi každým subjektem a jeho dodavateli nebo poskytovateli služeb;

Pozměňovací návrh 185

Návrh směrnice
Čl. 18 – odst. 2 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) politiky a postupy (testování a audit) za účelem posouzení účelnosti opatření k řízení rizik v oblasti kybernetické bezpečnosti;	f) politiky a postupy (***školení,*** testování a audit) za účelem posouzení účelnosti opatření k řízení rizik v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 186

Návrh směrnice
Čl. 18 – odst. 2 – písm. f a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	fa) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 187

Návrh směrnice
Čl. 18 – odst. 2 – písm. g

Znění navržené Komisí	*Pozměňovací návrh*
g) používání kryptografie ***a šifrování.***	g) používání kryptografie***, např. šifrování tam, kde je to vhodné;***

Pozměňovací návrh 188

Návrh směrnice
Čl. 18 – odst. 2 – písm. g a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ga) používání vícefaktorových autentizační řešení nebo trvalých autentizačních řešení, zabezpečené hlasové, obrazové a textové komunikace, a případně zabezpečených systémů tísňové komunikace v rámci subjektu.

Pozměňovací návrh 189

Návrh směrnice
Čl. 18 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Členské státy zajistí, aby v případě, že subjekt zjistí, že jeho služby nebo úkoly neodpovídají požadavkům stanoveným v odstavci 2, neprodleně přijal všechna nezbytná nápravná opatření, aby dotčená služba požadavky splňovala.	4. Členské státy zajistí, aby v případě, že subjekt zjistí, že jeho služby nebo úkoly neodpovídají požadavkům stanoveným v odstavci 2, neprodleně přijal všechna nezbytná***, vhodná a přiměřená*** nápravná opatření, aby dotčená služba požadavky splňovala.

Pozměňovací návrh 190

Návrh směrnice
Čl. 18 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Komise může přijmout prováděcí akty, aby stanovila technické a metodické specifikace prvků uvedených v odstavci 2. Při přípravě těchto aktů postupuje Komise v souladu s přezkumným postupem uvedeným v čl. 37 odst. 2 a v maximální možné míře dodržuje mezinárodní a evropské normy, jakož i příslušné technické specifikace.	***vypouští se***

Pozměňovací návrh 191

Návrh směrnice
Čl. 18 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Komisi je svěřena pravomoc přijmout v souladu s článkem 36 akty v přenesené pravomoci, kterými doplní prvky stanovené v odstavci 2, aby zohledňovaly nové kybernetické hrozby, technologický vývoj nebo specifičnosti daného odvětví.	6. Komisi je svěřena pravomoc přijmout v souladu s článkem 36 akty v přenesené pravomoci, kterými doplní prvky stanovené v odstavci 2 ***tohoto článku***, aby zohledňovaly nové kybernetické hrozby, technologický vývoj nebo specifičnosti daného odvětví***, a rovněž doplní tuto směrnici stanovením technických a metodických specifikací opatření uvedených v odstavci 2 tohoto článku***.

Pozměňovací návrh 192

Návrh směrnice
Čl. 19 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Skupina pro spolupráci může v součinnosti s Komisí a agenturou ENISA provést koordinované posouzení rizik dodavatelských řetězců u specifických kritických služeb, systémů nebo produktů IKT, přičemž zohlední technické, případně netechnické rizikové faktory.	1. Skupina pro spolupráci může v součinnosti s Komisí a agenturou ENISA provést koordinované posouzení rizik dodavatelských řetězců u specifických kritických služeb, systémů nebo produktů IKT ***a informačního a komunikačního systému (IKS)***, přičemž zohlední technické, případně netechnické rizikové faktory.

Pozměňovací návrh 193

Návrh směrnice
Čl. 19 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA určí specifické kritické služby, systémy nebo produkty IKT, jež mohou být předmětem koordinovaného posouzení rizik uvedeného v odstavci 1.	2. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA, ***a případně s příslušnými odpovědnými stranami,*** určí specifické kritické služby, systémy nebo produkty IKT ***a IKS***, jež mohou být předmětem koordinovaného posouzení rizik uvedeného v odstavci 1.

Pozměňovací návrh 194

Návrh směrnice
Čl. 20 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Členské státy zajistí, aby základní a důležité subjekty neprodleně oznamovaly ***příslušným orgánům nebo*** týmu CSIRT v souladu s odstavci 3 a 4 každý ***incident, který má*** závažný ***dopad na poskytování jejich služeb. Ve vhodných případech tyto subjekty neprodleně informují příjemce svých služeb o incidentech, které by mohly negativně ovlivnit poskytování dané služby***. Členské státy zajistí, aby tyto subjekty oznamovaly mimo jiné všechny informace, které ***příslušným orgánům nebo*** týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu.	1. Členské státy zajistí, aby základní a důležité subjekty neprodleně oznamovaly týmu CSIRT v souladu s odstavci 3 a 4 každý závažný ***incident***. Členské státy zajistí, aby tyto subjekty oznamovaly mimo jiné všechny informace, které týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu.

Pozměňovací návrh 195

Návrh směrnice
Čl. 20 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby základní a důležité subjekty neprodleně oznamovaly příslušným orgánům nebo týmu CSIRT každou významnou kybernetickou hrozbu,	

kterou tyto subjekty zjistí a která by mohla mít za následek významný incident.	
Ve vhodných případech ***tyto*** subjekty ***neprodleně informují*** příjemce svých služeb***, které mohou být ovlivněny významnou kybernetickou hrozbou, o všech*** krocích nebo nápravných opatřeních***,*** jež ***uvedení*** příjemci ***mohou učinit v reakci na danou hrozbu.*** Ve vhodných případech subjekty ***tyto*** příjemce ***uvědomí také o hrozbě*** samotné***. Ohlášení nezakládá*** u oznamujícího subjektu ***vyšší míru*** právní odpovědnosti.	2. Ve vhodných případech ***členské státy zajistí, aby základní a důležité*** subjekty ***informovaly neprodleně*** příjemce svých služeb ***o ochranných*** nebo nápravných opatřeních ***v souvislosti s konkrétními incidenty a známými riziky***, jež ***mohou*** příjemci ***učinit***. Ve vhodných případech subjekty příjemce ***svých služeb informují*** o samotném ***incidentu nebo známém riziku***. ***Informování příjemců probíhá v souladu se zásadou vynaložení nejvyššího úsilí a nezakládá*** u oznamujícího subjektu ***vyšší míru*** právní odpovědnosti.

Pozměňovací návrh 196

Návrh směrnice
Čl. 20 – odst. 3 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
3. ***Incident se považuje za významný***, ***jestliže***:	3. ***Při posuzování závažnosti incidentu jsou vzaty v úvahu zejména tyto parametry***, ***jsou-li k dispozici***:

Pozměňovací návrh 197

Návrh směrnice
Čl. 20 – odst. 3 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) ***incident dotčenému subjektu způsobil nebo může způsobit podstatné provozní narušení nebo finanční ztráty***;	a) ***počet příjemců služeb dotčených incidentem***;

Pozměňovací návrh 198

Návrh směrnice
Čl. 20 – odst. 3 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) ***incident způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značné hmotné nebo nehmotné ztráty.***	b) ***délka trvání incidentu;***

Pozměňovací návrh 199

Návrh směrnice
Čl. 20 – odst. 3 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) zeměpisný rozsah oblasti dotčené incidentem;

Pozměňovací návrh 200

Návrh směrnice
Čl. 20 – odst. 3 – písm. b b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	bb) rozsah, v jakém je incidentem ovlivněno fungování a kontinuita služby;

Pozměňovací návrh 201

Návrh směrnice
Čl. 20 – odst. 3 – písm. b c (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	bc) rozsah dopadu incidentu na společenské a ekonomické činnosti.

Pozměňovací návrh 202

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
Členské státy zajistí, aby za účelem oznámení podle odstavce 1 dotčené subjekty předložily ***příslušným orgánům nebo*** týmu CSIRT:	Členské státy zajistí, aby za účelem oznámení podle odstavce 1 dotčené subjekty předložily týmu CSIRT:

Pozměňovací návrh 203

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) ***neprodleně, nejpozději však do 24 hodin po zjištění*** incidentu, ***první oznámení, v němž případně uvedou***, ***zda byl incident pravděpodobně způsoben neoprávněným nebo svévolným zásahem;***	a) ***první oznámení závažného*** incidentu, ***které obsahuje tyto informace***, ***jež oznamující subjekt získal na základě zásady vynaložení nejvyššího úsilí:***

Pozměňovací návrh 204

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. a – písm. i (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	i) pokud jde o incidenty, které významně narušily dostupnost služeb poskytovaných subjektem, tým CSIRT je informován neprodleně, nejpozději však do 24 hodin po zjištění incidentu;

Pozměňovací návrh 205

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. a – písm. ii (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ii) pokud jde o incidenty, které mají významný dopad na subjekt s výjimkou dostupnosti služeb poskytovaných subjektem, tým CSIRT je informován neprodleně, nejpozději však do 72 hodin po zjištění incidentu;

Pozměňovací návrh 206

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. a – písm. iii (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	iii) pokud jde o incidenty, které mají významný dopad na služby poskytovatele služeb vytvářejících důvěru ve smyslu čl. 13 bodu 19 nařízení (EU) č. 910/2014 nebo na osobní údaje spravované poskytovatelem služeb vytvářejících důvěru, tým CSIRT je informován neprodleně, nejpozději však do 24 hodin po zjištění incidentu;

Pozměňovací návrh 207

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) ***na žádost příslušného orgánu nebo týmu CSIRT průběžnou*** zprávu o podstatných změnách stavu;	b) ***průběžnou*** zprávu o podstatných změnách stavu ***na žádost týmu CSIRT***;

Pozměňovací návrh 208

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. c – návětí

Znění navržené Komisí	*Pozměňovací návrh*
c) nejpozději do jednoho měsíce od předložení ***oznámení podle písmene a) závěrečnou*** zprávu zahrnující alespoň:	c) nejpozději do jednoho měsíce od předložení ***prvního oznámení souhrnnou*** zprávu zahrnující alespoň:

Pozměňovací návrh 209

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 1 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) v případě, že v době předložení souhrnné zprávy podle písmene c) incident probíhá, předloží se závěrečná zpráva jeden měsíc po vyřešení incidentu;

Pozměňovací návrh 210

Návrh směrnice
Čl. 20 – odst. 4 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
Členské státy zajistí, aby se dotčený subjekt mohl v odůvodněných případech a po dohodě s příslušnými orgány nebo týmem CSIRT odchýlit od lhůt stanovených v písmeni a) a c).	Členské státy zajistí, aby se dotčený subjekt mohl v odůvodněných případech a po dohodě s týmem CSIRT odchýlit od lhůt stanovených v písm. a) bodě i) a ii) a písmeni c). ***Členské státy zajistí důvěrnost a odpovídající ochranu citlivých informací o incidentech sdílených s týmy CSIRT a přijmou opatření a postupy pro sdílení a opětovné využívání informací o incidentech.***

Pozměňovací návrh 211

Návrh směrnice
Čl. 20 – odst. 4 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	4a. Členské státy zřídí jednotné kontaktní místo pro všechna oznámení požadovaná podle této směrnice a dalších příslušných právních předpisů Unie. Agentura ENISA ve spolupráci se skupinou pro spolupráci vypracuje a neustále zdokonaluje společné šablony hlášení prostřednictvím pokynů, které zjednoduší a zefektivní informace uvedené v hlášeních, jež vyžadují právní předpisy Unie, a sníží zátěž pro subjekty ohlašující incidenty.

Pozměňovací návrh 212

Návrh směrnice
Čl. 20 – odst. 4 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	4b. Základní a důležité subjekty uvedené v čl. 24 odst. 1 mohou splnit požadavky stanovené v odstavci 1 tohoto článku informováním týmu CSIRT členského státu, ve kterém mají tyto subjekty hlavní provozovnu v Unii, a informováním základních a důležitých subjektů, kterým poskytují služby, o každém závažném incidentu, o němž je známo, že bude mít dopad na příjemce služeb.

Pozměňovací návrh 213

Návrh směrnice
Čl. 20 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. ***Příslušné vnitrostátní orgány nebo tým*** CSIRT ***poskytnou*** do 24 hodin po obdržení prvního oznámení podle odst. 4	5. ***Tým*** CSIRT ***poskytne*** do 24 hodin po obdržení prvního oznámení podle odst. 4 písm. a) oznamujícímu subjektu své

písm. a) oznamujícímu subjektu své vyjádření, včetně prvních připomínek k incidentu, a na žádost subjektu doporučí možná zmírňující opatření***. Pokud tým CSIRT neobdržel oznámení podle odstavce 1, doporučení vydá příslušný orgán ve spolupráci s týmem CSIRT.*** Pokud o to dotčený subjekt požádá, poskytne mu tým CSIRT další technickou podporu. Jestliže existuje podezření, že má incident povahu trestného činu, doporučí ***příslušné vnitrostátní orgány nebo*** tým CSIRT také ohlášení tohoto incidentu orgánům činným v trestním řízení.

vyjádření, včetně prvních připomínek k incidentu, a na žádost subjektu doporučí možná zmírňující opatření ***a poskytne včasné poradenství***. Pokud o to dotčený subjekt požádá, poskytne mu tým CSIRT další technickou podporu. Jestliže existuje podezření, že má incident povahu trestného činu, doporučí tým CSIRT také ohlášení tohoto incidentu orgánům činným v trestním řízení. ***Tým CSIRT může sdílet informace o incidentu s dalšími základními a důležitými subjekty, přičemž zajistí důvěrnost informací poskytnutých subjektem ohlašujícím incidenty.***

Pozměňovací návrh 214

Návrh směrnice
Čl. 20 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 1 týká dvou nebo více členských států, informuje ***příslušný orgán nebo*** tým CSIRT, ***jimž*** byl incident ohlášen, ostatní dotčené členské státy a agenturu ENISA***.*** Příslušné ***orgány,*** týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.	6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 1 týká dvou nebo více členských států, informuje tým CSIRT, ***jemuž*** byl incident ohlášen, ostatní dotčené členské státy a agenturu ENISA ***a poskytne*** příslušné ***informace.*** Týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.

Pozměňovací návrh 215

Návrh směrnice
Čl. 20 – odst. 7

Znění navržené Komisí	*Pozměňovací návrh*
7. Pokud je nezbytné informovat veřejnost, aby se incidentu zabránilo nebo aby se probíhající incident vyřešil, nebo	7. Pokud je nezbytné informovat veřejnost, aby se incidentu zabránilo nebo aby se probíhající incident vyřešil, nebo

pokud je zveřejnění incidentu jinak ve veřejném zájmu, může ***příslušný orgán nebo*** tým CSIRT, případně ***orgány nebo*** týmy CSIRT jiných dotčených členských států po konzultaci s dotčeným subjektem informovat veřejnost o incidentu nebo požadovat, aby tak učinil daný subjekt.	pokud je zveřejnění incidentu jinak ve veřejném zájmu, může tým CSIRT, případně týmy CSIRT jiných dotčených členských států po konzultaci s dotčeným subjektem informovat veřejnost o incidentu nebo požadovat, aby tak učinil daný subjekt.

Pozměňovací návrh 216

Návrh směrnice
Čl. 20 – odst. 7 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	7a. Týmy CSIRT poskytnou neprodleně jednotným kontaktním místům, a případně příslušným orgánům, informace o závažných incidentech oznámených v souladu s odstavcem 1.

Pozměňovací návrh 217

Návrh směrnice
Čl. 20 – odst. 8

Znění navržené Komisí	*Pozměňovací návrh*
8. Na žádost ***příslušného orgánu nebo*** tým CSIRT postoupí jednotné kontaktní místo hlášení obdržená podle odstavce 1 ***a 2*** jednotným kontaktním místům dalších dotčených členských států.	8. Na žádost týmu CSIRT postoupí jednotné kontaktní místo hlášení obdržená podle odstavce 1 jednotným kontaktním místům dalších dotčených členských států***, přičemž zajistí důvěrnost a odpovídající ochranu informací poskytnutých subjektem ohlašujícím incidenty***.

Pozměňovací návrh 218

Návrh směrnice
Čl. 20 – odst. 9

Znění navržené Komisí	*Pozměňovací návrh*
9. Jednotné kontaktní místo předkládá každý měsíc agentuře ENISA souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o incidentech, závažných kybernetických hrozbách a případech, kdy téměř došlo k incidentu, oznámených podle odstavce 1 ***a 2*** a ***podle*** článku 27. V zájmu větší srovnatelnosti poskytovaných informací může agentura ENISA vydat technické pokyny k parametrům informací, jež mají být v souhrnné zprávě uvedeny.	9. Jednotné kontaktní místo předkládá každý měsíc agentuře ENISA souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o incidentech, závažných kybernetických hrozbách a případech, kdy téměř došlo k incidentu, oznámených podle odstavce 1 ***tohoto článku*** a článku 27. V zájmu větší srovnatelnosti poskytovaných informací může agentura ENISA vydat technické pokyny k parametrům informací, jež mají být v souhrnné zprávě uvedeny.

Pozměňovací návrh 219

Návrh směrnice
Čl. 20 – odst. 10

Znění navržené Komisí	*Pozměňovací návrh*
10. Příslušné orgány poskytnou příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] informace o incidentech a kybernetických hrozbách oznámených podle ***odstavců*** 1 a ***2*** základními subjekty určenými jako kritické subjekty nebo subjekty, které jsou rovnocenné kritickým subjektům, podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů].	10. Příslušné orgány poskytnou příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] informace o incidentech a kybernetických hrozbách oznámených podle ***odstavce*** 1 ***tohoto článku*** a ***článku 27*** základními subjekty určenými jako kritické subjekty nebo subjekty, které jsou rovnocenné kritickým subjektům, podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů].

Pozměňovací návrh 220

Návrh směrnice
Čl. 20 – odst. 11

Znění navržené Komisí	*Pozměňovací návrh*
11. Komise může přijmout prováděcí akty dále upřesňující ***druh informací, formát a*** postup oznámení předkládaných	11. Komise může přijmout prováděcí akty dále upřesňující postup oznámení předkládaných podle odstavce 1 ***tohoto***

podle odstavce 1 ***a 2. Komise může rovněž přijmout prováděcí akty dále upřesňující případy, kdy se incident považuje za významný, jak je uvedeno v odstavci 3***. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2.	***článku a článku 27***. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2.

Pozměňovací návrh 221

Návrh směrnice
Čl. 20 – odst. 11 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	11a. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 36 za účelem doplnění této směrnice stanovením typu informací předkládaných podle odstavce 1 tohoto článku a dalším upřesněním parametrů, které je třeba zohlednit při posuzování závažnosti incidentu, jak je uvedeno v odstavci 3 tohoto článku.

Pozměňovací návrh 222

Návrh směrnice
Čl. 21 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. ***K prokázání splnění některých požadavků článku 18 mohou členské státy požadovat***, aby základní a důležité subjekty certifikovaly některé produkty ***IKT***, služby ***IKT*** a procesy IKT ***podle zvláštních*** evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881. ***Produkty, služby a procesy podléhající certifikaci mohou být vyvinuty základním nebo důležitým subjektem nebo pořízeny od třetích stran***.	1. ***Členské státy v návaznosti na pokyny agentury ENISA, Komise a poradní skupiny podporují***, aby základní a důležité subjekty certifikovaly některé produkty, služby a procesy IKT ***– buď vyvinuté základním nebo důležitým subjektem nebo pořízené od třetích stran – , podle*** evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881 ***nebo – pokud tyto systémy ještě nejsou k dispozici – v rámci podobných mezinárodně uznávaných systémů certifikace***. ***Členské státy kromě toho podporují základní***

	a důležité subjekty, aby využívaly kvalifikované služby vytvářející důvěru podle nařízení (EU) č. 910/2014.

Pozměňovací návrh 223

Návrh směrnice
Čl. 21 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci ***upřesňující***, které kategorie základních subjektů ***budou*** povinny obstarat si certifikát ***a*** podle ***kterých*** konkrétních evropských systémů certifikace kybernetické bezpečnosti podle ***odstavce 1***. Akty v přenesené pravomoci se ***přijímají v souladu s článkem 36***.	2. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci ***v souladu s článkem 36 za účelem doplnění této směrnice upřesněním***, které kategorie základních ***a důležitých*** subjektů ***jsou*** povinny obstarat si certifikát podle konkrétních evropských systémů certifikace kybernetické bezpečnosti podle ***článku 49 nařízení (EU) 2019/881***. ***Tyto*** akty v přenesené pravomoci se ***zohlední, pokud se zjistí nedostatečná úroveň kybernetické bezpečnosti. Tomuto zohlednění předchází posouzení dopadu a v aktech je stanoveno prováděcí období***.

Pozměňovací návrh 224

Návrh směrnice
Čl. 21 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Komise může požádat agenturu ENISA, aby v případech, kdy není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2, připravila návrh systému podle čl. 48 odst. 2 nařízení (EU) 2019/881.	3. Komise může ***po konzultaci s poradní skupinou a Evropskou skupinou pro certifikaci kybernetické bezpečnosti*** požádat agenturu ENISA, aby v případech, kdy není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2, připravila návrh systému podle čl. 48 odst. 2 nařízení (EU) 2019/881.

Pozměňovací návrh 225

Návrh směrnice
Čl. 22 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Agentura ENISA ve spolupráci se členskými státy vydá doporučení a pokyny týkající se technických oblastí, které by měly být zohledněny ve vztahu k odstavci 1, jakož i s ohledem na již existující normy, včetně vnitrostátních norem členských států, které by umožnily tyto oblasti pokrýt.	2. Agentura ENISA ve spolupráci se členskými státy***, a případně po konzultaci s příslušnými zúčastněnými stranami,*** vydá doporučení a pokyny týkající se technických oblastí, které by měly být zohledněny ve vztahu k odstavci 1, jakož i s ohledem na již existující normy, včetně vnitrostátních norem členských států, které by umožnily tyto oblasti pokrýt.

Pozměňovací návrh 226

Návrh směrnice
Čl. 22 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Komise ve spolupráci s agenturou ENISA podporuje a prosazuje rozvoj a provádění norem pro harmonizované provádění čl. 18 odst. 1 a 2 stanovených příslušnými orgány Unie a mezinárodními normalizačními organizacemi. Komise podporuje aktualizaci těchto norem s ohledem na technologický vývoj.

Pozměňovací návrh 227

Návrh směrnice
Čl. 23 – název

Znění navržené Komisí	*Pozměňovací návrh*
Databáze doménových jmen a registračních údajů	***Struktura*** databáze doménových jmen a registračních údajů

Pozměňovací návrh 228

Návrh směrnice
Čl. 23 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Aby členské státy přispěly k bezpečnosti, stabilitě a odolnosti DNS, ***zajistí***, aby registry TLD a subjekty poskytující služby registrace doménových jmen ***pro TLD*** shromažďovaly a uchovávaly přesné a úplné údaje o registraci doménových jmen ve ***vyhrazeném databázovém zařízení, a to s náležitou péčí podle právních předpisů Unie o ochraně osobních údajů, pokud jde o data, jež jsou osobními údaji.***	1. Aby členské státy přispěly k bezpečnosti, stabilitě a odolnosti DNS, ***požadují***, aby registry TLD a subjekty poskytující služby registrace doménových jmen shromažďovaly a uchovávaly přesné***,*** ***ověřené*** a úplné údaje o registraci doménových jmen ve ***struktuře databáze provozované za tímto účelem.***

Pozměňovací návrh 229

Návrh směrnice
Čl. 23 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy zajistí, aby databáze údajů o registraci doménových jmen ***uvedené*** v odstavci 1 ***obsahovaly*** podstatné informace umožňující identifikaci a kontaktování držitelů doménových jmen a kontaktní místa spravující doménová jména v registrech TLD.	2. Členské státy zajistí, aby ***struktura*** databáze údajů o registraci doménových jmen ***uvedená*** v odstavci 1 ***obsahovala*** podstatné informace ***zahrnující alespoň jména držitelů registrace, jejich fyzickou a e-mailovou adresu a také jejich telefonní číslo*** umožňující identifikaci a kontaktování držitelů doménových jmen a kontaktní místa spravující doménová jména v registrech TLD.

Pozměňovací návrh 230

Návrh směrnice
Čl. 23 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Členské státy zajistí, aby registry	3. Členské státy zajistí, aby registry

TLD a subjekty poskytující služby registrace doménových jmen ***pro TLD*** měly zavedeny zásady a postupy zajišťující, aby ***databáze zahrnovaly*** přesné a úplné informace. Členské státy zajistí, aby byly tyto zásady a postupy veřejně dostupné.	TLD a subjekty poskytující služby registrace doménových jmen měly zavedeny zásady a postupy zajišťující, aby ***databázová struktura zahrnovala*** přesné***, ověřené*** a úplné informace. Členské státy zajistí, aby byly tyto zásady a postupy veřejně dostupné.

Pozměňovací návrh 231

Návrh směrnice
Čl. 23 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen ***pro TLD zveřejnily*** neprodleně po registraci doménového jména údaje o registraci domény, které nejsou osobními údaji.	4. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen ***zveřejňovaly*** neprodleně po registraci doménového jména údaje o registraci domény, které nejsou osobními údaji. ***Jedná-li se o držitele registrace – právnické osoby, měly by veřejně přístupné údaje o registraci domény zahrnovat alespoň název držitele registrace, jeho fyzickou a e-mailovou adresu a telefonní číslo.***

Pozměňovací návrh 232

Návrh směrnice
Čl. 23 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
5. Členské státy ***zajistí***, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD poskytovaly přístup ke konkrétním údajům o registraci doménových jmen na oprávněnou a řádně odůvodněnou žádost oprávněných žadatelů o přístup, a to v souladu s právními předpisy Unie o ochraně osobních údajů. Členské státy ***zajistí***, aby registry TLD a subjekty poskytující služby registrace doménových	5. Členské státy ***vyžadují***, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD poskytovaly přístup ke konkrétním údajům o registraci doménových jmen***, včetně osobních údajů,*** na oprávněnou a řádně odůvodněnou žádost oprávněných žadatelů o přístup, a to v souladu s právními předpisy Unie o ochraně osobních údajů. Členské státy ***vyžadují***, aby registry TLD a subjekty poskytující služby registrace

jmen ***pro TLD neprodleně reagovaly na všechny*** žádosti o přístup. Členské státy zajistí, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.	doménových jmen ***reagovaly neprodleně, a v každém případě do 72 hodin od obdržení*** žádosti o přístup. Členské státy zajistí, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.

Pozměňovací návrh 233

Návrh směrnice
Čl. 24 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Pro účely této směrnice se má za to, že hlavním místem obchodní činnosti subjektů uvedených v odstavci 1 v Unii je členský stát, v němž přijímají rozhodnutí týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti. Jestliže tato rozhodnutí nejsou přijímána v žádné provozovně v Unii, má se za to, že hlavní místo obchodní činnosti je v členském státě, kde mají subjekty provozovnu s nejvyšším počtem zaměstnanců v ***Unii***.	2. Pro účely této směrnice se má za to, že hlavním místem obchodní činnosti subjektů uvedených v odstavci 1 v Unii je členský stát, v němž přijímají rozhodnutí týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti. Jestliže tato rozhodnutí nejsou přijímána v žádné provozovně v Unii, má se za to, že hlavní místo obchodní činnosti je v členském státě, kde mají subjekty ***buď*** provozovnu s nejvyšším počtem zaměstnanců v ***Unii, nebo provozovnu, v níž se provádějí operace v oblasti kybernetické bezpečnosti***.

Pozměňovací návrh 234

Návrh směrnice
Čl. 25 – název

Znění navržené Komisí	*Pozměňovací návrh*
Registr ***základních a důležitých subjektů***	Registr ***agentury ENISA***

Pozměňovací návrh 235

Návrh směrnice
Čl. 25 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. Agentura ENISA vytvoří a vede registr základních a důležitých subjektů uvedených v čl. 24 odst. 1***. Subjekty předloží [nejpozději do 12 měsíců od vstupu této směrnice v platnost] agentuře ENISA*** tyto informace:	1. Agentura ENISA vytvoří a vede ***zabezpečený*** registr základních a důležitých subjektů uvedených v čl. 24 odst. 1***, jenž zahrnuje*** tyto informace:

Pozměňovací návrh 236

Návrh směrnice
Čl. 25 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) aktuální kontaktní údaje, ***včetně e-mailových*** adres a ***telefonních čísel subjektů***.	c) aktuální kontaktní údaje, ***jako jsou e-mailové adresy, rozsah IP*** adres***, telefonní čísla*** a ***příslušná odvětví a pododvětví uvedená v přílohách I a II***.

Pozměňovací návrh 237

Návrh směrnice
Čl. 25 – odst. 1 – pododstavec 1 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	Do … [12 měsíců ode dne vstupu této směrnice v platnost] předloží základní a důležité subjekty informace uvedené v prvním pododstavci agentuře ENISA.

Pozměňovací návrh 238

Návrh směrnice
Čl. 26 – odst. 1 – návětí

Znění navržené Komisí	*Pozměňovací návrh*
1. ***Aniž je dotčeno nařízení (EU) 2016/679 členské*** státy zajistí, aby základní	1. ***Členské*** státy zajistí, aby základní a ***důležité subjekty a jiné příslušné***

a ***důležité*** subjekty mohly mezi sebou sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, zranitelností, indikátorů narušení, taktiky, ***technik a postupů***, varování při ohrožení kybernetické bezpečnosti a ***konfiguračních*** nástrojů, pokud toto sdílení informací:	subjekty ***nespadající do oblasti působnosti této směrnice*** mohly mezi sebou sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, ***případů, kdy téměř došlo k incidentu,*** zranitelností, ***technik a postupů, metadat a dat obsahu,*** indikátorů narušení, ***nepřátelské*** taktiky, ***modu operandi, informací specifických pro daný subjekt***, varování při ohrožení kybernetické bezpečnosti***, taktiky průmyslové špionáže*** a ***doporučené konfigurace bezpečnostních*** nástrojů, pokud toto sdílení informací:

Pozměňovací návrh 239

Návrh směrnice
Čl. 26 – odst. 1 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) zvyšuje úroveň kybernetické bezpečnosti, zejména zvyšováním informovanosti o kybernetických hrozbách, omezováním nebo bráněním schopnosti těchto hrozeb šířit se, podporou obranných kapacit, zveřejňováním informací o zranitelnostech a jejich nápravou, prostřednictvím metod zjišťování hrozeb, strategií zmírňování nebo fází reakce a obnovy.	b) zvyšuje úroveň kybernetické bezpečnosti, zejména zvyšováním informovanosti o kybernetických hrozbách, omezováním nebo bráněním schopnosti těchto hrozeb šířit se, podporou obranných kapacit, zveřejňováním informací o zranitelnostech a jejich nápravou, prostřednictvím metod zjišťování***, omezování a prevence*** hrozeb, strategií zmírňování nebo fází reakce a obnovy ***nebo podporou společného výzkumu kybernetických hrozeb ze strany subjektů veřejného a soukromého sektoru***.

Pozměňovací návrh 240

Návrh směrnice
Čl. 26 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Členské státy ***zajistí, aby k výměně informací docházelo v*** důvěryhodných ***komunitách*** základních a důležitých	2. Členské státy ***usnadní výměnu informací tím, že umožní vytvoření*** důvěryhodných ***komunit*** základních

subjektů. Tato výměna bude probíhat prostřednictvím ujednání o sdílení informací s ohledem na potenciálně citlivou povahu sdílených informací ***v souladu s pravidly práva Unie uvedenými v odstavci 1***.

a důležitých subjektů ***a jejich poskytovatelů služeb nebo případně dalších dodavatelů***. Tato výměna bude probíhat prostřednictvím ujednání o sdílení informací s ohledem na potenciálně citlivou povahu sdílených informací.

Pozměňovací návrh 241

Návrh směrnice
Čl. 26 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Členské státy ***stanoví pravidla upřesňující postup***, provozní prvky (včetně použití vyhrazených platforem IKT***), obsah*** a ***podmínky ujednání o sdílení informací podle odstavce 2***. ***Tato pravidla rovněž*** podrobně ***upravují*** zapojení veřejných orgánů do těchto ujednání***, jakož i provozní prvky, včetně využití vyhrazených platforem IT***. Členské státy nabídnou podporu při uplatňování těchto ujednání v souladu se svými politikami uvedenými v čl. 5 odst. 2 písm. g).	3. Členské státy ***usnadní vznik ujednání o sdílení informací o kybernetické bezpečnosti uvedených v odstavci 2 tím***, ***že zpřístupní*** provozní prvky (včetně použití vyhrazených platforem IKT a ***nástrojů pro automatizaci) a obsah***. ***Členské státy*** podrobně ***upraví*** zapojení veřejných orgánů do těchto ujednání ***a mohou stanovit určité podmínky pro informace zpřístupněné příslušnými orgány nebo týmy CSIRT***. Členské státy nabídnou podporu při uplatňování těchto ujednání v souladu se svými politikami uvedenými v čl. 5 odst. 2 písm. g).

Pozměňovací návrh 242

Návrh směrnice
Čl. 27 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Členské státy zajistí, ***aniž je dotčen článek 3,*** aby ***subjekty, které nespadají do oblasti působnosti této směrnice,*** mohly ***dobrovolně oznamovat významné incidenty, kybernetické hrozby nebo případy, kdy téměř došlo k incidentu. Při zpracování oznámení postupují členské státy postupem uvedeným v článku 20.***	Členské státy zajistí, aby mohly ***týmům CSIRT dobrovolně podávat*** oznámení***:***

Členské státy mohou dát přednost zpracování povinných oznámení před dobrovolnými oznámeními. Na základě dobrovolného oznámení nesmí být oznamujícímu subjektu uloženy žádné další povinnosti, které by mu nebyly uloženy, kdyby toto oznámení neučinil.

Pozměňovací návrh 243

Návrh směrnice
Čl. 27 – odst. 1 – písm. a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	a) základní a důležité subjekty, pokud jde o kybernetické hrozby a případy, kdy téměř došlo k incidentu;

Pozměňovací návrh 244

Návrh směrnice
Čl. 27 – odst. 1 – písm. b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	b) subjekty, které nespadají do oblasti působnosti této směrnice, pokud jde o závažné incidenty, kybernetické hrozby nebo případy, kdy téměř došlo k incidentu.

Pozměňovací návrh 245

Návrh směrnice
Čl. 27 – odst. 1 – pododstavec 1 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	Při zpracování těchto oznámení postupují členské státy postupem uvedeným v článku 20. Členské státy mohou dát přednost zpracování povinných oznámení před dobrovolnými oznámeními. V

	případě potřeby poskytnou týmy CSIRT jednotnému kontaktnímu místu a případně příslušným orgánům informace o oznámeních obdržených podle tohoto článku, přičemž zajistí důvěrnost a náležitou ochranu informací, jež poskytl oznamující subjekt. Na základě dobrovolného oznámení nesmí být oznamujícímu subjektu uloženy žádné další povinnosti, které by mu nebyly uloženy, kdyby toto oznámení neučinil.

Pozměňovací návrh 246

Návrh směrnice
Čl. 28 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Při řešení incidentů, v jejichž důsledku došlo k porušení ochrany osobních údajů, příslušné orgány úzce spolupracují s orgány pro ochranu osobních údajů.	2. Při řešení incidentů, v jejichž důsledku došlo k porušení ochrany osobních údajů, příslušné orgány úzce spolupracují s orgány pro ochranu osobních údajů. ***Činí tak v souladu se svými pravomocemi a úkoly podle nařízení (EU) 2016/679.***

Pozměňovací návrh 247

Návrh směrnice
Čl. 29 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) kontrolám na místě i externímu dohledu, včetně namátkových kontrol;	a) kontrolám na místě i externímu dohledu včetně namátkových kontrol ***prováděným školenými odborníky***;

Pozměňovací návrh 248

Návrh směrnice
Čl. 29 – odst. 2 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) šetřením případů nedodržování povinností a jeho dopadům na bezpečnost služeb;

Pozměňovací návrh 249

Návrh směrnice
Čl. 29 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) ***pravidelným*** auditům;	b) ***ročním a cíleným bezpečnostním*** auditům***, které provádí kvalifikované nezávislé subjekty nebo příslušné orgány***;

Pozměňovací návrh 250

Návrh směrnice
Čl. 29 – odst. 2 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) ***cíleným bezpečnostním*** auditům na ***základě posouzení rizik*** nebo ***dostupných informací týkajících se rizik***;	c) auditům ***ad hoc v případech odůvodněných*** na ***místě závažným mimořádným incidentem*** nebo ***nedodržením povinností ze strany základního subjektu***;

Pozměňovací návrh 251

Návrh směrnice
Čl. 29 – odst. 2 – pododstavce 1a a 1b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	Cílené bezpečnostní audity uvedené v prvním pododstavci písmene b) jsou založeny na posouzení rizik, jež provede příslušný orgán nebo auditovaný subjekt, nebo na jiných dostupných informacích

týkajících se rizik.

Výsledky cíleného bezpečnostního auditu se zpřístupní příslušnému orgánu. Náklady na takový cílený bezpečnostní audit provedený kvalifikovaným nezávislým subjektem hradí dotčený subjekt.

Pozměňovací návrh 252

Návrh směrnice
Čl. 29 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Při výkonu své pravomoci podle odst. 2 písm. a) až d) příslušné orgány minimalizují dopady na obchodní procesy daného subjektu.

Pozměňovací návrh 253

Návrh směrnice
Čl. 29 – odst. 4 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) vydat závazné pokyny nebo příkaz požadující, aby tyto subjekty napravily zjištěné nedostatky nebo porušení povinností stanovených v této směrnici;	b) vydat závazné pokyny***, včetně pokynů týkajících se opatření nezbytných k zabránění incidentu nebo jeho nápravě, lhůt pro provedení těchto opatření a podávání zpráv o jejich provedení,*** nebo příkaz požadující, aby tyto subjekty napravily zjištěné nedostatky nebo porušení povinností stanovených v této směrnici;

Pozměňovací návrh 254

Návrh směrnice
Čl. 29 – odst. 4 – písm. i

Znění navržené Komisí	*Pozměňovací návrh*
i) učinit veřejné prohlášení, které identifikuje právnické a fyzické osoby odpovědné za porušení povinnosti stanovené v této směrnici a povahu tohoto porušení;	***vypouští se***

Pozměňovací návrh 255

Návrh směrnice
Čl. 29 – odst. 4 – písm. j

Znění navržené Komisí	*Pozměňovací návrh*
j) uložit nebo požádat o uložení správní pokuty podle ***vnitrostátních právních*** předpisů příslušnými orgány nebo soudy podle článku 31 vedle opatření uvedených v písmenech a) až i) tohoto odstavce ***nebo namísto těchto opatření***, a to v závislosti na okolnostech každého jednotlivého případu.	j) uložit nebo požádat o uložení správní pokuty podle ***vnitrostátního práva*** předpisů příslušnými orgány nebo soudy podle článku 31 vedle opatření uvedených v písmenech a) až i) tohoto odstavce, a to v závislosti na okolnostech každého jednotlivého případu.

Pozměňovací návrh 256

Návrh směrnice
Čl. 29 – odst. 5 – pododstavec 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) ***pozastavit*** nebo požádat certifikační nebo schvalovací orgán o pozastavení certifikace nebo schválení týkající se všech nebo některých služeb nebo činností poskytovaných základním subjektem;	a) ***dočasně pozastavit*** nebo požádat certifikační nebo schvalovací orgán o ***dočasné*** pozastavení certifikace nebo schválení týkající se všech nebo některých ***příslušných*** služeb nebo činností poskytovaných základním subjektem;

Pozměňovací návrh 257

Návrh směrnice
Čl. 29 – odst. 5 – pododstavec 1 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) uložit nebo požadovat, aby příslušné orgány nebo soudy v souladu s ***vnitrostátními právními předpisy*** uložily dočasný zákaz výkonu manažerských funkcí v tomto subjektu jakékoli osobě, která má manažerskou odpovědnost na úrovni výkonného ředitele nebo zákonného zástupce v tomto základním subjektu***, i jakékoli jiné fyzické osobě odpovědné za porušení***.	b) ***jako krajní prostředek*** uložit nebo požadovat, aby příslušné orgány nebo soudy v souladu s ***vnitrostátním právem*** uložily dočasný zákaz výkonu manažerských funkcí v tomto subjektu jakékoli osobě, která má manažerskou odpovědnost na úrovni výkonného ředitele nebo zákonného zástupce v tomto základním subjektu.

Pozměňovací návrh 258

Návrh směrnice
Čl. 29 – odst. 5 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
Tato omezující opatření se použijí pouze do doby, než subjekt přijme opatření nezbytná k odstranění nedostatků nebo splnění požadavků příslušného orgánu, kvůli nimž byla tato omezující opatření uplatněna.	***Dočasná pozastavení nebo zákazy podle tohoto odstavce*** se použijí pouze do doby, než subjekt přijme opatření nezbytná k odstranění nedostatků nebo splnění požadavků příslušného orgánu, kvůli nimž byla tato omezující opatření uplatněna. ***Uložení takových dočasných pozastavení nebo zákazů musí podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny, včetně účinné právní ochrany, spravedlivého procesu, presumpce neviny a práva na obhajobu.***

Pozměňovací návrh 259

Návrh směrnice
Čl. 29 – odst. 7 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) ***skutečně*** způsobené škody nebo vzniklé ztráty, ***případně potenciální škody nebo ztráty, které mohly být způsobeny,***	c) způsobené škody nebo vzniklé ztráty, ***včetně finančních*** nebo ***ekonomických ztrát***, ***účinků*** na jiné služby ***a počtu***

pokud je lze určit. Při hodnocení tohoto aspektu je třeba zohlednit mimo jiné skutečné nebo ***potenciální finanční nebo ekonomické ztráty***, ***účinky*** na jiné služby***, počet postižených nebo potenciálně*** postižených uživatelů;	postižených uživatelů;

Pozměňovací návrh 260

Návrh směrnice
Čl. 29 – odst. 7 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) veškerá relevantní porušení, kterých se dotyčný subjekt dopustil v minulosti;

Pozměňovací návrh 261

Návrh směrnice
Čl. 29 – odst. 9

Znění navržené Komisí	*Pozměňovací návrh*
9. Členské státy zajistí, aby jejich příslušné orgány při výkonu svých pravomocí v oblasti dohledu a vymáhání zaměřených na zajištění dodržování povinností podle této směrnice ze strany základního subjektu určeného podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za kritický subjekt nebo subjekt, který je rovnocenný kritickému subjektu, informovaly příslušné orgány ***daného členského státu*** určené podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]. Na žádost příslušných orgánů podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] mohou příslušné orgány vykonávat své dohledové a donucovací pravomoci u základního subjektu označeného jako kritický nebo rovnocenný kritickému subjektu.	9. Členské státy zajistí, aby jejich příslušné orgány při výkonu svých pravomocí v oblasti dohledu a vymáhání zaměřených na zajištění dodržování povinností podle této směrnice ze strany základního subjektu určeného podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za kritický subjekt nebo subjekt, který je rovnocenný kritickému subjektu, informovaly příslušné orgány ***všech příslušných členských států*** určené podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]. Na žádost příslušných orgánů podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] mohou příslušné orgány vykonávat své dohledové a donucovací pravomoci u základního subjektu označeného jako kritický nebo rovnocenný kritickému subjektu.

Pozměňovací návrh 262

Návrh směrnice
Čl. 29 – odst. 9 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	9a. Členské státy zajistí, aby jejich příslušné orgány spolupracovaly s relevantními příslušnými orgány dotčeného členského státu určenými podle nařízení (EU) XXXX/XXXX [DORA].

Pozměňovací návrh 263

Návrh směrnice
Čl. 30 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Při předložení důkazů nebo informací naznačujících, že důležitý subjekt neplní povinnosti stanovené v této směrnici, zejména v článcích 18 a 20, členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření prostřednictvím dohledových opatření ex post.	1. Při předložení důkazů nebo informací naznačujících, že důležitý subjekt neplní povinnosti stanovené v této směrnici, zejména v článcích 18 a 20, členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření prostřednictvím dohledových opatření ex post. ***Členské státy zajistí, aby tato opatření byla účinná, přiměřená a odrazujícím a to s přihlédnutím k okolnostem každého jednotlivého případu.***

Pozměňovací návrh 264

Návrh směrnice
Čl. 30 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) kontrolám na místě i externímu dohledu ex post;	a) kontrolám na místě i externímu dohledu ex post***, jež provádějí vyškolení odborníci***;

Pozměňovací návrh 265

Návrh směrnice
Čl. 30 – odst. 2 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) šetření případů nedodržování předpisů a jejich dopadům na bezpečnost služeb;

Pozměňovací návrh 266

Návrh směrnice
Čl. 30 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) cíleným bezpečnostním auditům ***na základě posouzení rizik*** nebo ***dostupných informací týkajících se rizik***;	b) cíleným bezpečnostním auditům***,*** ***které provádí kvalifikované nezávislé subjekty*** nebo ***příslušné orgány***;

Pozměňovací návrh 267

Návrh směrnice
Čl. 30 – odst. 2 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) bezpečnostním prověrkám na základě objektivních, korektních a transparentních kritérií posouzení rizik;	c) bezpečnostním prověrkám na základě objektivních, ***nediskriminačních,*** korektních a transparentních kritérií posouzení rizik;

Pozměňovací návrh 268

Návrh směrnice
Čl. 30 – odst. 2 – pododstavce 1a a 1 b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	Cílené bezpečnostní audity uvedené v prvním pododstavci písmena b) jsou založeny na posouzení rizik, jež provede příslušný orgán nebo auditovaný subjekt, nebo na jiných dostupných informacích týkajících se rizik.
	Výsledky cíleného bezpečnostního auditu se zpřístupní příslušnému orgánu. Náklady na takový cílený bezpečnostní audit, který provede kvalifikovaný nezávislý subjekt, hradí dotčený subjekt.

Pozměňovací návrh 269

Návrh směrnice
Čl. 30 – odst. 4 – písm. h

Znění navržené Komisí	*Pozměňovací návrh*
h) učinit veřejné prohlášení, které identifikuje právnické a fyzické osoby odpovědné za porušení povinnosti stanovené v této směrnici a povahu tohoto porušení;	***vypouští se***

Pozměňovací návrh 270

Návrh směrnice
Čl. 30 – odst. 4 – písm. i

Znění navržené Komisí	*Pozměňovací návrh*
i) uložit nebo požádat o uložení správní pokuty podle ***vnitrostátních právních předpisů*** příslušnými orgány nebo soudy podle článku 31 vedle opatření uvedených v písmenech a) až h) tohoto odstavce ***nebo namísto těchto opatření***, a to v závislosti na okolnostech každého jednotlivého případu.	i) uložit nebo požádat o uložení správní pokuty podle ***vnitrostátního práva*** příslušnými orgány nebo soudy podle článku 31 vedle opatření uvedených v písmenech a) až h) tohoto odstavce, a to v závislosti na okolnostech každého jednotlivého případu.

Pozměňovací návrh 271

Návrh směrnice
Čl. 31 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě opatření uvedených v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a čl. 30 odst. 4 písm. a) až h) ***či místo nich***.	2. Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě opatření uvedených v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a čl. 30 odst. 4 písm. a) až h).

Pozměňovací návrh 272

Návrh směrnice
Čl. 32 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
1. Pokud mají příslušné orgány informace naznačující, že porušení povinností stanovených v článcích 18 a 20 základním nebo důležitým subjektem má za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 ***odst.*** 12 nařízení (EU) 2016/679, které musí být oznámeno podle článku 33 uvedeného nařízení, uvědomí v ***přiměřené lhůtě*** orgány dohledu příslušné podle článků 55 a 56 uvedeného nařízení.	1. Pokud mají příslušné orgány informace naznačující, že porušení povinností stanovených v článcích 18 a 20 základním nebo důležitým subjektem má za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 ***bodu*** 12 nařízení (EU) 2016/679, které musí být oznámeno podle článku 33 uvedeného nařízení, uvědomí ***o tom bez zbytečného prodlení a*** v ***každém případě do 72 hodin od okamžiku, kdy se o porušení zabezpečení údajů dozvěděly,*** orgány dohledu příslušné podle článků 55 a 56 uvedeného nařízení.

Pozměňovací návrh 273

Návrh směrnice
Čl. 32 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Pokud má dozorový úřad příslušný podle nařízení (EU) 2016/679 sídlo v jiném členském státě než příslušný orgán, ***může*** příslušný orgán ***informovat*** dozorový úřad se sídlem ve stejném členském státě.	3. Pokud má dozorový úřad příslušný podle nařízení (EU) 2016/679 sídlo v jiném členském státě než příslušný orgán, ***informuje*** příslušný orgán dozorový úřad se sídlem ve stejném členském státě.

Pozměňovací návrh 274

Návrh směrnice
Čl. 35 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Komise pravidelně přezkoumává fungování této směrnice a podává zprávu Evropskému parlamentu a Radě. Ve zprávě se zejména posoudí význam odvětví, pododvětví, velikosti a druhu subjektů uvedených v přílohách I a II pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT z hlediska zkušeností získaných na strategické a operativní úrovni. ***První zprávu předloží do ... [54 měsíců od data vstupu této směrnice v platnost].***	***Do ... [42 měsíců po datu vstupu této směrnice v platnost] a poté každých 36 měsíců přezkoumá*** Komise fungování této směrnice a ***podá*** zprávu Evropskému parlamentu a Radě. Ve zprávě se zejména posoudí význam odvětví, pododvětví, velikosti a druhu subjektů uvedených v přílohách I a II pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT z hlediska zkušeností získaných na strategické a operativní úrovni. ***V případě potřeby se ke zprávě přiloží legislativní návrh.***

Pozměňovací návrh 275

Návrh směrnice
Čl. 36 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 18 odst. 6 a v čl. 21 odst. 2 je svěřena Komisi na dobu pěti let ode dne […]	2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 18 odst. 6***, v čl. 20 odst. 11a*** a v čl. 21 odst. 2 je svěřena Komisi na dobu pěti let ode dne […]

Pozměňovací návrh 276

Návrh směrnice
Čl. 36 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 18 odst. 6 a v čl. 21 odst. 2 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.	3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 18 odst. 6***, v čl. 20 odst. 11a*** a v čl. 21 odst. 2 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

Pozměňovací návrh 277

Návrh směrnice
Čl. 36 – odst. 6

Znění navržené Komisí	*Pozměňovací návrh*
6. Akt v přenesené pravomoci přijatý podle čl. 18 odst. 6 a čl. 21 odst. 2 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.	6. Akt v přenesené pravomoci přijatý podle čl. 18 odst. 6***, čl. 20 odst. 11a*** a čl. 21 odst. 2 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Pozměňovací návrh 278

Návrh směrnice
Čl. 42 – odst. 1a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	Články 39 a 40 se však použijí ode dne... [18 měsíců po datu vstupu této směrnice v platnost].

Pozměňovací návrh 279

Návrh směrnice
Příloha I – bod 2 – písm. d – odrážka 2 (nová)

Znění navržené Komisí

Pozměňovací návrh

2. Doprava	d) silniční	**— *provozovatelé služeb inteligentního dobíjení pro elektrická vozidla***

Pozměňovací návrh 280

Návrh směrnice
Příloha II – tabulka – řádek 6 a (nový)

Znění navržené Komisí

Pozměňovací návrh

6a. Vzdělání a výzkum		**— *vysokoškolské a výzkumné instituce***