EUROPEAN UNION AGENCY
FOR CYBERSECURITY

VNITROSTÁTNÍ RÁMEC PRO POSOUZENÍ SCHOPNOSTÍ

PROSINEC 2020

O AGENTUŘE ENISA

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) je agenturou Unie, která usiluje o dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Evropě. Agentura Evropské unie pro kybernetickou bezpečnost, která byla zřízena v roce 2004 a následně posílena aktem EU o kybernetické bezpečnosti, se podílí na kybernetické politice EU, prostřednictvím systémů certifikace kybernetické bezpečnosti zvyšuje důvěryhodnost produktů, služeb a procesů IKT, spolupracuje s členskými státy a subjekty EU a pomáhá Evropě připravit se na budoucí kybernetické výzvy. Sdílením znalostí, budováním schopností a zvyšováním povědomí usiluje agentura společně s hlavními zúčastněnými stranami o posílení důvěry v propojenou ekonomiku, o podporu odolnosti infrastruktury Unie, a především o zajištění digitální bezpečnosti evropské společnosti a občanů. Více informací viz www.enisa.europa.eu.

KONTAKT

Autory kontaktujte na team@enisa.europa.eu.
Sdělovací prostředky se s dotazy ohledně tohoto dokumentu mohou obrátit na press@enisa.europa.eu.

AUTOŘI

Anna Sarri, Pinelopi Kyranoudi – Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

PODĚKOVÁNÍ

Agentura ENISA by chtěla poděkovat a vyjádřit uznání všem odborníkům, kteří se zúčastnili a významně přispěli k této zprávě, zejména následujícím, uvedeným v abecedním pořadí:

Centrum pro kybernetickou bezpečnost (Belgie)

CFCS – Center for Cybersikkerhed (Dánsko), Thomas Wulff

Evropské centrum pro boj proti kyberkriminalitě – EC3, Adrian-Ionut Bobeica

Evropské centrum pro boj proti kyberkriminalitě – EC3, Alzofra Martinez Alvaro

Maltská agentura pro informační technologie (Malta), Katia Bonello a Martin Camilleri

Ministerstvo digitální politiky (Řecko), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali a Sotiris Vasilos

Ministerstvo hospodářství a spojů (Estonsko), Anna-Liisa Pärnalaas

Ministerstvo národní bezpečnosti (Španělsko), Maria Mar Lopez Gil

Ministerstvo spravedlnosti a veřejné bezpečnosti (Norsko), Robin Bakke

Národní bezpečnostní úřad (Slovensko)

Národní úřad pro kybernetickou a informační bezpečnost (Česká republika), Veronika Netolická

NCTV, Ministerstvo spravedlnosti a bezpečnosti (Nizozemsko)

Odbor politiky kybernetické bezpečnosti, Ministerstvo životního prostředí, klimatu a spojů (Irsko), James Caffrey

Oxfordská univerzita – Centrum pro globální schopnosti kybernetické bezpečnosti, Carolin Weisser Harris

Portugalské centrum pro národní kybernetickou bezpečnost (Portugalsko), Alexandre Leite a Pedro Matos

Spolkové ministerstvo vnitra (Německo), Sascha-Alexander Lettgen

Úřad pro informační bezpečnost (Slovinská republika), Marjan Kavčič
Ústřední státní úřad pro rozvoj digitální společnosti (Chorvatsko), Marin Ante Pivčević
Vláda Italské republiky (Itálie)

Agentura ENISA by rovněž za cenný příspěvek k této studii ráda poděkovala všem odborníkům, kteří se na ní podíleli, ovšem přáli si zůstat v anonymitě.

PRÁVNÍ UPOZORNĚNÍ

OZNÁMENÍ TÝKAJÍCÍ SE AUTORSKÝCH PRÁV

ISBN: 978-92-9204-473-2

DOI: 10.2824/200111

KATALOG: TP-02-21-253-CS-N

1. OBSAH

REJSTŘÍK POJMŮ

ZKRATKA	DEFINICE
C2M2	model vyspělosti schopností v oblasti kybernetické bezpečnosti
CCRA	dohoda o uznávání společných kritérií
CCSMM	komunitní model vyspělosti schopností v oblasti kybernetické bezpečnosti
CMM	model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy
CMMC	certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti
CPI	index kybernetických schopností
CSIRT	bezpečnostní týmy typu CSIRT
CVD	koordinované zveřejňování zranitelností
DPA	zákon o ochraně údajů
DSM	jednotný digitální trh
ECCG	Evropská skupina pro certifikaci kybernetické bezpečnosti
ECSM	Evropský měsíc kybernetické bezpečnosti
ECSO	Evropská organizace pro kybernetickou bezpečnost
EQF	evropský rámec kvalifikací
ESVO	Evropské sdružení volného obchodu.
EU	Evropská unie
GCI	globální index kybernetické bezpečnosti
GDPR	obecné nařízení o ochraně osobních údajů
GDS	Státní digitální služba
IA-CM	model útvaru interního auditu pro veřejný sektor
IKT	informační a komunikační technologie
ISMM	model vyspělosti bezpečnosti informací pro rámec kybernetické bezpečnosti NIST
ITU	Mezinárodní telekomunikační unie
KII	kritická informační infrastruktura
LEA	donucovací orgán
MS	členský stát

MSP	malé a střední podniky
NCSS	národní strategie kybernetické bezpečnosti
NIS	bezpečnost sítí a informací
NIST	Národní ústav pro normalizaci a technologie (National Institute of Standards and Technology)
NLO	národní styční úředníci
OES	provozovatelé základních služeb
OT	provozní technologie
PET	technologie zvyšující ochranu soukromí
PIMS	systém správy osobních údajů
PPP	partnerství veřejného a soukromého sektoru
Q-C2M2	katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti
SOG-IS MRA	skupina vedoucích pracovníků pro bezpečnost informačních systémů, dohoda o vzájemném uznávání
UI	umělá inteligence
VaV	výzkum a vývoj

SHRNUTÍ

Protože se současné kybernetické hrozby neustále rozšiřují a kybernetické útoky nabírají na síle a zvyšuje se jejich počet, musí členské státy EU účinně reagovat dalším rozvojem a přizpůsobováním svých národních strategií kybernetické bezpečnosti (NCSS). Od zveřejnění prvních studií agentury ENISA týkajících se NCSS v roce 2012 učinily členské státy EU a země ESVO velký pokrok při vypracování a provádění svých strategií.

Tato zpráva představuje příspěvek agentury ENISA k vybudování vnitrostátního rámce pro posouzení schopností.

Cílem tohoto rámce je poskytnout členským státům prostředek pro vlastní posouzení jejich úrovně vyspělosti prostřednictvím posouzení jejich cílů v oblasti NCSS, který jim pomůže zlepšit a vybudovat schopnosti týkajících se kybernetické bezpečnosti na strategické i provozní úrovni.

Nastiňuje jednoduchý reprezentativní náhled na úroveň vyspělosti kybernetické bezpečnosti členského státu. Vnitrostátní rámec pro posouzení schopností je nástroj, který členským státům pomůže:

- poskytovat užitečné informace pro vypracování dlouhodobé strategie (např. osvědčené postupy, pokyny),
- zjistit chybějící prvky v rámci NCSS,
- dále rozvíjet schopnosti v oblasti kybernetické bezpečnosti,
- podporovat odpovědnost politických opatření,
- zajišťovat důvěryhodnost ze strany široké veřejnosti a mezinárodních partnerů,
- podporovat dosah a zlepšovat vnímání veřejnosti jakožto transparentní organizace,
- předjímat budoucí problémy,
- určovat poučení a osvědčené postupy,
- poskytovat základ pro schopnosti v oblasti kybernetické bezpečnosti v celé EU, aby se usnadnily diskuse, a
- vyhodnocovat vnitrostátní schopnosti týkající se kybernetické bezpečnosti.

Tento rámec byl navržen s pomocí odborníků agentury ENISA a zástupců devatenácti členských států a zemí ESVO[1]. Cílovou skupinou této zprávy jsou politici, odborníci a státní úředníci odpovídající za nebo podílející se na navrhování, provádění a vyhodnocování NCSS a obecněji schopností v oblasti kybernetické bezpečnosti.

[1]Byly vedeny rozhovory se zástupci těchto členských států a zemí ESVO: Belgie, Česká republika, Dánsko, Estonsko, Chorvatsko, Irsko, Itálie, Lichtenštejnsko, Maďarsko, Malta, Německo, Nizozemsko, Norsko, Portugalsko, Řecko, Slovensko, Slovinsko, Španělsko, Švédsko.

Vnitrostátní rámec pro posouzení schopností zahrnuje sedmnáct strategických cílů a je rozdělen do čtyř hlavních klastrů.

- Klastr č. 1: Řízení a normy kybernetické bezpečnosti
    1. Vypracovat vnitrostátní pohotovostní plán kybernetické bezpečnosti
    2. Vytvořit základní bezpečnostní opatření
    3. Zabezpečit digitální identitu a budovat důvěru v digitální veřejné služby

- Klastr č. 2: Budování schopností a zvyšování povědomí
    4. Pořádat cvičení v oblasti kybernetické bezpečnosti
    5. Vytvořit schopnost reakce na incident
    6. Zvyšovat povědomí uživatelů
    7. Zlepšit programy odborné přípravy a vzdělávání
    8. Podporovat VaV
    9. Poskytovat pobídky soukromému sektoru k investování do bezpečnostních opatření
    10. Zlepšit kybernetickou bezpečnost dodavatelského řetězce

- Klastr č. 3: Právní a regulační povinnosti
    11. Chránit kritickou informační infrastrukturu, OES a DSP
    12. Bojovat proti kyberkriminalitě
    13. Vytvořit mechanismy hlášení incidentu
    14. Zesílit informační soukromí a ochranu údajů

- Klastr č. 4: Spolupráce
    15. Vytvořit partnerství veřejného a soukromého sektoru
    16. Institucionalizovat spolupráci mezi veřejnými agenturami
    17. Zapojit se do mezinárodní spolupráce

1. ÚVOD

Směrnice o bezpečnosti sítí a informací (NIS) z července 2016 požaduje, aby členské státy EU přijaly národní strategie pro bezpečnost sítí a informačních systémů, nazývanou rovněž NCSS (národní strategie kybernetické bezpečnosti), jak stanoví její články 1 a 7. S ohledem na to je NCSS definována jako rámec, který stanovuje strategické zásady, pokyny, strategické cíle, priority, vhodné politiky a regulační opatření. Předpokládaným cílem NCSS je dosažení a zachování vysoké úrovně zabezpečení sítí a systémů, což umožní členským státům zmírnit potenciální hrozby. Dále se může NCSS rovněž stát katalyzátorem průmyslového rozvoje a hospodářského a sociálního pokroku.

Akt EU o kybernetické bezpečnosti stanoví, že ENISA bude podporovat šíření osvědčených postupů týkajících se určení a provádění NCSS prostřednictvím podpory členských států při přijetí směrnice NIS a shromažďováním cenných názorů s jejich zkušenostmi. Agentura ENISA proto vypracovala několik nástrojů, které členským státům pomohou s přípravou, prováděním a posouzením jejich národních strategií kybernetické bezpečnosti (NCSS).

Agentura ENISA se v rámci tohoto mandátu zaměřuje na vypracování vnitrostátního rámce pro vlastní posouzení schopností, který bude měřit úroveň vyspělosti různých NCSS. Cílem této zprávy je představit studii týkající se definování rámce pro vlastní posouzení.

1.1 OBLAST PŮSOBNOSTI A CÍLE STUDIE

Hlavním cílem této studie je vytvořit vnitrostátní rámec pro vlastní posouzení schopností, dále nazývaný vnitrostátní rámec pro posouzení schopností, který bude měřit úroveň vyspělosti schopností členských států v oblasti kybernetické bezpečnosti. Konkrétněji by měl tento rámec zmocnit členské státy k:

- posouzení jejich vnitrostátních schopností v oblasti kybernetické bezpečnosti,
- zvyšování povědomí o úrovni vyspělosti země,
- zjištění oblastí pro zlepšení a
- budování schopností kybernetické bezpečnosti.

Tento rámec by měl pomoci členským státům a konkrétně vnitrostátním politikům při provádění vlastního posouzení s cílem zlepšit vnitrostátní schopnosti v oblasti kybernetické bezpečnosti.

1.2 METODICKÝ PŘÍSTUP

Metodický přístup používaný k vypracování vnitrostátního rámce pro vlastní posouzení schopností vychází ze čtyř hlavních kroků:

1. **Analýza podkladů:** první krok zahrnoval rozsáhlý přezkum literatury, aby byly shromážděny osvědčené postupy týkající se vypracování rámce pro posouzení vyspělosti pro národní strategie kybernetické bezpečnosti. Analýza podkladů se zaměřuje na systematickou analýzu příslušných dokumentů o budování schopností a stanovení strategie v oblasti kybernetické bezpečnosti, stávající NCSS členských států a porovnání stávajících modelů vyspělosti kybernetické bezpečnosti. Porovnání stávajících modelů vyspělosti bylo provedeno přijetím rámce analýzy vypracovaného

pro účely této studie. Tento rámec analýzy vychází z Beckerovy[2] metodologie pro vypracování modelů vyspělosti, která stanoví obecný a konsolidovaný model postupů pro navrhování modelů vyspělosti a uvádí jasné požadavky na vypracování modelů vyspělosti. Tento rámec analýzy byl dále přizpůsoben tak, aby vyhovoval potřebám této studie.

2. **Shromáždění názorů odborníků a zúčastněných stran:** na základě dat získaných analýzou podkladů a souvisejícími předběžnými zjištěními v analýze tato fáze zahrnovala určení vytipovaných odborníků, kteří mají zkušenost s vypracováním a provedením NCSS nebo s modely vyspělosti, a jejich pozvání k rozhovoru. Agentura ENISA se obrátila na svou odbornou skupinu pro národní strategie kybernetické bezpečnosti a národních styčných úředníků (NLO), aby v jednotlivých členských státech našla příslušné odborníky. Dále rozhovory poskytli někteří odborníci podílející se na vypracování modelů vyspělosti. Celkem bylo provedeno 22 rozhovorů, z nichž devatenáct poskytli zástupci agentur pro kybernetickou bezpečnost různých členských států (a zemí ESVO).
3. **Analýza inventarizační části:** data získaná analýzou podkladů a z rozhovorů byla následně analyzována, aby byly stanoveny osvědčené postupy při navrhování rámců pro vlastní posouzení k měření vyspělosti NCSS, aby se porozumělo požadavkům členských států a aby se určilo, která data lze reálně získávat v různých evropských zemích[3]. Tato analýza umožnila doladění předběžného modelu vypracovaného v předchozích krocích a úpravy souborů ukazatelů zahrnutých do modelu, úrovně vyspělosti a jejího rozsahu.
4. **Dokončení modelu:** dále odborníci agentury ENISA na danou oblast přezkoumali aktualizovanou verzi vnitrostátních rámců pro vlastní posouzení schopností, což následně ověřili odborníci na pracovním setkání, které se konalo v říjnu 2020, tedy před vydáním této publikace.

1.3 CÍLOVÁ SKUPINA

Cílovou skupinou této zprávy jsou politici, odborníci a státní úředníci odpovídající za nebo podílející se na navrhování, provádění a vyhodnocování NCSS a obecněji schopnostmi v oblasti kybernetické bezpečnosti. Dále by bylo přínosné, kdyby zjištění formalizovaná v tomto dokumentu posoudili odborníci na politiky kybernetické bezpečnosti a výzkumní pracovníci na vnitrostátní i evropské úrovni.

[2] J. Becker, R. Knackstedt a J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application“, Business & Information Systems Engineering, sv. 1, č. 3, s. 213–222, červen 2009.
[3] Pro účely tohoto výzkumu se evropskými zeměmi uvedenými v této zprávě rozumí 27 členských států EU.

2. SOUVISLOSTI

2.1 PŘEDCHOZÍ PRÁCE TÝKAJÍCÍ SE ŽIVOTNÍHO CYKLU NCSS

Jak je uvedeno v aktu EU o kybernetické bezpečnosti, jedním z hlavních cílů agentury ENISA je podpora členských států při vypracování národních strategií pro bezpečnost sítí a informačních systémů, podpora šíření těchto strategií a sledování jejich provádění. Agentura ENISA v rámci svého mandátu vypracovala ohledně tohoto tématu několik dokumentů, aby podpořila sdílení osvědčených postupů a provádění NCSS v EU:

- „Praktický průvodce fází přípravy a realizace NCSS“[4] vydaný roku 2012
- „Stanovení kurzu pro vnitrostátní snahy o zvýšení bezpečnosti v kyberprostoru“[5] z roku 2012
- První rámec agentury ENISA pro hodnocení NCSS členského státu, vydaný[6] v roce 2014
- „On-line interaktivní mapa NCSS“[7], vydaná v roce 2014.
- „Průvodce osvědčenými postupy pro NCSS“[8] vydaný v roce 2016
- „Nástroj pro hodnocení národních strategií kybernetické bezpečnosti“[9], vydaný v roce 2018.
- „Osvědčené postupy pro inovaci kybernetické bezpečnosti v rámci NCSS“[10], vydané v roce 2019

PŘÍLOHA A uvádí stručné shrnutí hlavních publikací agentury ENISA k tomuto tématu.

Výše uvedené průvodce a dokumenty byly prostudovány v rámci analýzy podkladů. Základním prvkem vnitrostátního rámce pro posouzení schopností je zejména „Nástroj pro hodnocení národních strategií kybernetické bezpečnosti“[11]. Vnitrostátní rámec pro posouzení schopností vychází z cílů uvedených v on-line nástroji pro hodnocení NCSS.

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.
[6] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.
[7] National Cybersecurity Strategies – Interactive Map (ENISA, 2014, aktualizováno v roce 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[8] Tento dokument aktualizuje průvodce z roku 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.
[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 SPOLEČNÉ CÍLE URČENÉ V RÁMCI EVROPSKÉ NCSS

Nerovnost mezi různými členskými státy ztěžuje stanovení společných činností nebo akčních plánů v různých vnitrostátních souvislostech, právních rámcích a politických agendách. NCSS členských států mají ovšem často různé strategické cíle týkající se stejných témat. Na základě předchozí práce agentury ENISA a analýzy NCSS členských států bylo stanoveno 22 strategických cílů. Patnáct z těchto strategických cílů již bylo určeno během předchozí práce agentury ENISA, dva byly nově doplněny touto studií a pět cílů bylo stanoveno pro budoucí úvahy.

2.2.1 Společné strategické cíle členských států

Následující tabulka ukazuje na základě předchozí práce agentury ENISA, konkrétně na základě Nástroje pro posuzování národních strategií kybernetické bezpečnosti[12], výše uvedený soubor patnácti strategických cílů, jež jsou obecně zahrnuty do NCSS členských států. Tyto cíle načrtnou základ celkové „národní filozofie“ tématu. Další informace o níže uvedených cílech najdete ve zprávě agentury ENISA „NCSS Good Practice Guide“[13].

Tabulka 1: Společné strategické cíle zahrnuté do NCSS členských států

ID	Strategické cíle NCSS	Cíle
1	Vypracovat vnitrostátní pohotovostní plány kybernetické bezpečnosti	▶ Představit a vysvětlit kritéria, jež se mají používat k označení situace za krizovou ▶ Stanovit klíčové postupy a činnosti pro zvládnutí krize ▶ Jasně definovat úlohy a odpovědnosti různých zúčastněných stran během kybernetické krize ▶ Představit a vysvětlit kritéria pro ukončení krize a/nebo kdo bude oprávněn ukončení krize vyhlásit
2	Vytvořit základní bezpečnostní opatření	▶ Harmonizovat různé postupy organizace ve veřejném i soukromém sektoru ▶ Nalézt společnou řeč mezi příslušnými veřejnými orgány a organizacemi a otevřít bezpečné komunikační kanály ▶ Umožnit různým zúčastněným stranám, aby kontrolovaly a posuzovaly své schopnosti v oblasti kybernetické bezpečnosti ▶ Sdílet informace o osvědčených postupech v oblasti kybernetické bezpečnosti ve všech průmyslových odvětvích ▶ Pomoci zúčastněným stranám upřednostňovat jejich investice do bezpečnosti
3	Pořádat cvičení v oblasti kybernetické bezpečnosti	▶ Stanovit, co se musí testovat (plány a postupy, lidi, infrastrukturu, schopnosti reakce, schopnosti spolupráce, komunikace atd.) ▶ Vytvořit vnitrostátní plánovací tým pro kybernetickou bezpečnost, který bude mít jasný mandát ▶ Integrovat kybernetickou bezpečnost v rámci životního cyklu národní strategie kybernetické bezpečnosti nebo vnitrostátního pohotovostního plánu kybernetické bezpečnosti
4	Vytvořit schopnost reakce na incident	▶ Mandát – týká se pravomocí, úloh a odpovědností, jež musí týmu přidělit příslušná vláda ▶ Portfolio služeb – zahrnuje služby, které tým poskytuje svému zřizovateli nebo je využívá pro své interní fungování ▶ Provozní schopnosti – týkají se technických a provozních požadavků, které musí tým splnit

[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.
[13] Tento dokument aktualizuje průvodce z roku 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

ID	Strategické cíle NCSS	Cíle
		▶ Schopnosti spolupráce – zahrnují požadavky týkající se sdílení informací s dalšími týmy, které nepatří do předchozích tří kategorií, např. s politiky, armádou, regulátory, provozovateli (kritické informační infrastruktury), donucovacími orgány
5	Zvyšovat povědomí uživatelů	▶ Identifikovat nedostatky ve znalostech týkajících se problematiky kybernetické a informační bezpečnosti ▶ Odstranit tyto nedostatky zvýšením povědomí nebo rozvojem/zlepšením znalostních základů
6	Zlepšit programy odborné přípravy a vzdělávání	▶ Zlepšit provozní schopnosti stávajících pracovníků informační bezpečnosti ▶ Vybízet studenty, aby se přidali, a pak je připravit na vstup do odvětví kybernetické bezpečnosti ▶ Podporovat a podněcovat vztahy mezi akademickým prostředím zabývajícím se kybernetickou bezpečností a odvětvím bezpečnosti informací ▶ Sladit odbornou přípravu v oblasti kybernetické bezpečnosti s potřebami podniků
7	Podporovat VaV	▶ Určit skutečné příčiny zranitelná místa namísto náprav jejich dopadů ▶ Spojit vědce z různých oborů, aby předložili řešení víceoborových a složitých problémů, jako jsou fyzické kybernetické hrozby ▶ Shromáždit požadavky odvětví a zjištění výzkumu, což usnadní přechod z teorie do praxe ▶ Nalézt cesty nejen k zachování, ale rovněž ke zvýšení úrovně kybernetické bezpečnosti výrobků a služeb a současně podporovat stávající kybernetické infrastruktury
8	Poskytovat pobídky soukromému sektoru k investování do bezpečnostních opatření	▶ Identifikovat možné pobídky pro soukromé společnosti, aby investovaly do bezpečnostních opatření ▶ Poskytovat pobídky společnostem, aby podporovaly investice do bezpečnosti
9	Ochránit kritické informační infrastruktury, OES a DSP (KII)	▶ Určit kritickou informační infrastrukturu ▶ Určit a zmírnit příslušná rizika pro KII
10	Bojovat proti kyberkriminalitě	▶ Přijmout zákony v oblasti kybernetické kriminality ▶ Zvýšit účinnost donucovacích orgánů
11	Vytvořit mechanismy hlášení incidentu	▶ Získat znalosti o celkovém prostředí hrozeb ▶ Posoudit dopady incidentu (např. narušení bezpečnosti, poruchy sítě, přerušení služeb) ▶ Získat znalosti o stávajících a nových zranitelných místech a druzích útoků ▶ Aktualizovat bezpečnostní opatření na základě výše uvedeného ▶ Provádět ustanovení směrnice NIS o hlášení incidentu
12	Zesílit informační soukromí a ochranu údajů	▶ Přispět k posílení základních práv v oblasti ochrany soukromí a ochrany údajů
13	Vytvořit partnerství veřejného a soukromého sektoru (PPP)	▶ Odstrašení (odstrašit útočníky) ▶ Ochrana (využívá výzkum nových bezpečnostních hrozeb) ▶ Detekce (využívá sdílení informací při řešení nových hrozeb) ▶ Reakce (zajistit schopnosti zvládnutí počátečního dopadu incidentu) ▶ Zotavení (zajistit schopnosti nápravy konečného dopadu incidentu)
14	Institucionalizovat spolupráci mezi veřejnými agenturami	▶ Zlepšit spolupráci mezi veřejnými agenturami s odpovědnostmi a kompetencemi týkajícími se kybernetické bezpečnosti ▶ Zabránit překrývání kompetencí a prostředků veřejných agentur ▶ Zlepšit a institucionalizovat spolupráci mezi veřejnými agenturami v různých oblastech kybernetické bezpečnosti
15	Zapojit se do mezinárodní spolupráce (nejen v MS EU)	▶ Výhoda vytvoření společného znalostního základu více členských států EU

ID	Strategické cíle NCSS	Cíle
		▶ Vznik synergických účinků mezi vnitrostátními orgány kybernetické bezpečnosti ▶ Umožnit a zintenzivnit boj proti mezinárodnímu zločinu

2.2.2 Další strategické cíle

Na základě provedené analýzy podkladů a rozhovorů vedených agenturou ENISA byly stanoveny další strategické cíle. Členské státy se těmito tématy stále více zabývají ve svých NCSS nebo pro ně definují akční plány. Jsou uvedeny rovněž příklady činností členských států. Pochází-li příklad z veřejně dostupného zdroje, je uveden odkaz. Pokud příklady vychází z důvěrných rozhovorů s úředníky členských států EU, není odkaz uveden.

Byly určeny tyto další strategické cíle:

- zlepšit kybernetickou bezpečnost dodavatelského řetězce a
- zabezpečit digitální identitu a budovat důvěry v digitální veřejné služby.

Zlepšit kybernetickou bezpečnost dodavatelského řetězce

Malé a střední podniky (MSP) jsou páteří evropského hospodářství. Představují 99 % všech podniků v EU[14] a v roce 2015 bylo odhadováno, že MSP vytváří kolem 85 % nových pracovních míst a zaměstnávají dvě třetiny pracovníků z celého soukromého sektoru EU. Protože MSP dále poskytují služby velkým společnostem a stále častěji spolupracují s veřejnou správou[15], je nutné poznamenat, že v dnešním propojeném světě tvoří slabý článek, na který se zaměřují kybernetické útoky. Ve skutečnosti jsou MSP nejvíce vystaveny kybernetickým útokům, ovšem často si nemohou dovolit investovat adekvátní prostředky do kybernetické bezpečnosti[16]. Kybernetickou bezpečnost dodavatelského řetězce je tedy třeba zlepšovat se zaměřením na MSP.

Kromě tohoto systematického přístupu mohou členské státy rovněž zdůrazňovat úsilí konkrétních služeb a produktů IKT v oblasti kybernetické bezpečnosti, jež jsou považovány za zásadní: technologie IKT používané v kritické informační infrastruktuře, bezpečnostní mechanismy prosazované v odvětví telekomunikací (kontrolní prostředky na úrovni ISP...), důvěryhodné služby, jak jsou definovány v nařízení eIDAS, a poskytovatelé cloudových služeb. Například Polsko se ve své národní strategii kybernetické bezpečnosti pro období 2019–2024[17] zavázalo vypracovat systém národního posouzení a certifikace, který se stane mechanismem zajištění kvality dodavatelského řetězce. Tento systém certifikace bude sladěn s rámcem certifikace EU pro digitální produkty, služby a postupy IKT podle aktu EU o kybernetické bezpečnosti (2019/881).

Zlepšení kybernetické bezpečnosti dodavatelského řetězce má tedy nejvyšší důležitost. Toho lze dosáhnout mimo jiné stanovením silných strategií podporujících MSP, vydáním pokynů pro požadavky v oblasti kybernetické bezpečnosti ve správě zadávání veřejných zakázek, podporou spolupráce v rámci soukromého sektoru, vytvářením PPP, podporou mechanismů

[14] https://ec.europa.eu/growth/smes/.
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm.
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study.
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

koordinovaného zveřejňování zranitelností (CVD)[18], vytvořením režimu certifikace produktů, včetně prvků kybernetické bezpečnosti v digitálních iniciativách pro MSP, a financování rozvoje dovedností.

Zabezpečit digitální identitu a budovat důvěru v digitální veřejné služby

Komise v únoru 2020 představila svou vizi digitální transformace EU ve sdělení „Formování digitální budoucnosti Evropy“[19] s cílem poskytnout inkluzivní technologie, které budou sloužit lidem a respektovat základní hodnoty EU. Sdělení zejména uvádí, že podpora digitální transformace veřejné správy v celé Evropě je zásadní. V tomto ohledu má nejvyšší význam budování důvěry ve státní správu související s digitální identitou a důvěry ve veřejné služby. To je ještě zásadnější, přihlédneme-li ke skutečnosti, že jsou transakce ve veřejném sektoru a výměna údajů často citlivé povahy.

Mnoho zemí vyjádřilo svůj záměr k řešení tohoto tématu ve svých NCSS, například: Dánsko, Estonsko, Francie, Lucembursko, Malta, Nizozemsko, Spojené království a Španělsko. Některé z těchto zemí rovněž uvedly, že je možné tento strategický cíl vyřešit v rámci širšího plánu:

- Estonsko spojilo svůj související akční plán „Bezpečnost elektronické identity a možnosti elektronického ověřování“ se širší Digitální agendou 2020 pro Estonsko.
- Francouzská NCSS uvádí, že ministr odpovědný za digitální technologie dohlédne na vytvoření plánu „na ochranu digitálních životů, soukromí a osobních údajů Francouzů“.
- Nizozemská NCSS stanoví, že jsou kybernetická bezpečnost ve veřejné správě a rovněž veřejné služby poskytované občanům a podnikům, podrobněji projednány v Širší agendě pro digitální státní správu.
- Protože vláda Spojeného království dále přesouvá své služby do on-line prostoru, vytvořila Státní digitální službu (GDS), která zajistí, že všechny nové digitální služby vytvářené nebo zadávané vládou budou s podporou britského národního centra pro kybernetickou bezpečnost (NCSC) „ze své podstaty bezpečné“.

2.2.3 Další projednávané strategické cíle

Během fáze analýzy podkladů a rozhovorů vedených agenturou ENISA byly prostudovány další strategické cíle. Bylo ovšem rozhodnuto, že by tyto cíle neměly tvořit součást rámce pro vlastní posouzení. PŘÍLOHA C – Další studované cíle

Stanoví definice pro tyto jednotlivé cíle, což bude dále možné použít jako základ pro diskuse o možných zlepšeních NCSS.

Tyto strategické cíle byly prostudovány s ohledem na budoucnost:

- připravit odvětvové strategie kybernetické bezpečnosti,
- boj proti dezinformačním kampaním,
- zajistit nejmodernější technologie (5G, UI, kvantová výpočetní technika…),
- zajistit svrchovanost v oblasti údajů a
- poskytnout pobídky pro rozvoj odvětví kybernetického pojištění.

[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.
[19] Formování digitální budoucnosti Evropy, COM(2020) 67 final: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM%3A2020%3A67%3AFIN.

2.3 HLAVNÍ POZNATKY Z POROVNÁNÍ

Analýza podkladů stávajících modelů vyspělosti v oblasti kybernetické bezpečnosti byla provedena s cílem shromáždit informace a podklady na podporu návrhu vnitrostátního rámce pro vlastní posouzení schopností v oblasti NCSS. Proto byl proveden rozsáhlý přezkum literatury týkající se stávajících modelů, který doplnil zjištění počátečního výzkumu působnosti modelů vyspělosti kybernetické bezpečnosti a stávajících NCSS a který je uveden v částech 2.1 a 2.2. Tento systematický přezkum podporuje výběr a odůvodnění úrovní vyspělosti rámce posuzování a definování různých oblastí a ukazatelů.

V rámci systematického přezkumu modelů vyspělosti bylo podle svých klíčových vlastností vyhodnocováno a analyzováno deset modelů. Celkový přehled hlavních vlastností jednotlivých modelů přezkoumávaných v rámci této studie přináší Tabulka 2: Přehled analyzovaných modelů vyspělosti a podrobnější analýzu přináší PŘÍLOHA A.

Tabulka 2: Přehled analyzovaných modelů vyspělosti

Název modelu	Č. úrovně vyspělosti	Počet atributů	Metoda posouzení	Představení výsledků
Model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy (CMM)	5	5 hlavních dimenzí	Spolupráce s místní organizací pro doladění modelu před jeho použitím ve vnitrostátním kontextu	Radar s 5 částmi
Model vyspělosti schopností v oblasti kybernetické bezpečnosti (C2M2)	4	10 hlavních oblastí	Metodologie a nástroje sebehodnocení	Hodnoticí tabulka s koláčovými grafy
Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury	Není k dispozici (4 úrovně)	5 hlavních funkcí	Vlastní posouzení	Není k dispozici
Katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti (Q-C2M2)	5	5 hlavních oblastí	Není k dispozici	Není k dispozici
Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC)	5	17 hlavních oblastí	Posouzení externími auditory	Není k dispozici
Komunitní model vyspělosti schopností v oblasti kybernetické bezpečnosti (CCSMM)	5	6 hlavních oblastí	Posouzení s komunitami za přispění státu a federálních donucovacích orgánů	Není k dispozici
Model vyspělosti bezpečnosti informací pro rámec kybernetické bezpečnosti NIST (ISMM)	5	23 posuzovaných oblastí	Není k dispozici	Není k dispozici
Model útvaru interního auditu pro veřejný sektor (JA-CM)	5	6 prvků	Vlastní posouzení	Není k dispozici
Globální index kybernetické bezpečnosti (GCI)	Není k dispozici	5 pilířů	Vlastní posouzení	Hodnoticí tabulka
Index kybernetických schopností (CPI)	Není k dispozici	4 kategorie	Hodnocení provedené Economist Intelligence Unit	Hodnoticí tabulka

Tento systematický přezkum umožnil učinit závěry ohledně osvědčených postupů přijatých v rámci stávajících modelů, aby se podpořila příprava konceptuálního modelu pro současný

model vyspělosti. Porovnání podpořilo zejména definování úrovní vyspělosti, vytvoření klastrů oblastí a výběr ukazatelů, stejně jako vhodnou metodologii vizualizace pro výsledky modelu. Nejdůležitější zjištění těchto jednotlivých prvků podrobně uvádí Tabulka 3.

Tabulka 3: Hlavní poznatky z porovnání

Vlastnost	Hlavní poznatek
Úrovně vyspělosti	▶ Pětiúrovňová stupnice úrovně vyspělosti pro rámce pro posouzení schopností v oblasti kybernetické bezpečnosti je obecně přijímána a umožňuje strukturované výsledky posouzení (vyčerpávající přehled definic úrovní vyspělosti jednotlivých modelů přináší Tabulka 6 Srovnání úrovní vyspělosti) ▶ Všechny modely poskytují podrobné definice jednotlivých úrovní vyspělosti, které jsou následně přizpůsobeny různým oblastem či jejich klastrem ▶ Při měření vyspělosti schopností v oblasti kybernetické bezpečnosti se typicky posuzují dva hlavní aspekty: vyspělost strategií a vyspělost postupů pro strategie provedení
Atributy	▶ Srovnávací analýza atributů stávajících modelů vyspělosti ukazuje různorodé výsledky s průměrně čtyřmi až pěti atributy na model ▶ Model vycházející ze zhruba čtyř nebo pěti atributů poskytuje zemím správnou granularitu dat, protože jsou seskupeny příslušné oblasti a je zajištěna srozumitelnost výsledků (popis atributů jednotlivých modelů přináší Tabulka 7: Srovnání atributů/dimenzí) ▶ Hlavní zásady uplatňované ve všech modelech při definování klastrů jsou založeny na soudržnosti prvků v jednotlivém klastru
Metoda posouzení	▶ Metody posouzení používané v různých analyzovaných modelech se od sebe liší ▶ Nejběžnější metoda posouzení je založena na vlastním posouzení
Představení výsledků	▶ Je důležité, aby výsledky byly představeny s různým členěním ▶ Metodologie vizualizace by měla být samozřejmá a snadno srozumitelná

Konceptuální model byl vypracován podle porovnání různých modelů vyspělosti a rovněž předchozích prací agentury ENISA. Pro vypracování ukazatelů používaných pro jednotlivé atributy bylo rovněž rozhodnuto vycházet z *on-line interaktivního nástroje agentury ENISA*.

2.4 PROBLÉMY PŘI POSUZOVÁNÍ NCSS

Členské státy čelí při budování schopností v oblasti kybernetické bezpečnosti mnoha výzvám, a ještě konkrétněji při zajištění, aby jejich schopnosti držely krok s nejnovějším vývojem. Níže je uveden přehled problémů zjištěných a projednávaných v rámci této studie se členskými státy.

- **Potíže v oblastech koordinace a spolupráce:** Koordinace činností v oblasti kybernetické bezpečnosti na vnitrostátní úrovni kvůli vytvoření účinné reakce na problémy kybernetické bezpečnosti se ukázala jako obtížná kvůli vysokému počtu zúčastněných stran.
- **Nedostatečné zdroje na provádění posouzení:** Podle místních podmínek a vnitrostátní struktury řízení kybernetické bezpečnosti může posuzování NCSS a jejích cílů trvat i déle než patnáct dnů.
- **Nedostatečná podpora rozvoje schopností v oblasti kybernetické bezpečnosti:** Některé členské státy uvedly, že v zájmu ochrany rozpočtu a získání podpory na rozvoj schopností v oblasti kybernetické bezpečnosti musí nejprve provést fázi hodnocení a určit nedostatky a omezení.
- **Potíže při připisování úspěchů a změnách strategie:** Protože se hrozby neustále vyvíjejí a technologie zlepšuje, je nutné podle toho neustále upravovat akční plány.

Ovšem hodnocení NCSS a připisování změn vlastní strategii zůstává náročným úkolem. To naopak ztěžuje určování omezení a nedostatků NCSS.

- **Obtíže s měřením účinnosti NCSS:** Lze shromažďovat údaje pro měření různých oblastí, například pokroku, provádění, vyspělosti a účinnosti. Zatímco měření pokroku a provádění je relativně snadné porovnat s měřením účinnosti, ta se lépe uplatní při hodnocení výsledků a dopadů NCSS. V rozhovorech vedených agenturou ENISA velký počet členských států uvedl, že kvantitativní měření účinnosti NCSS je důležité, ovšem představuje rovněž velice obtížný úkol, který je v některých případech téměř nemožný.
- **Potíže s přijetím společného rámce:** Členské státy EU fungují v různých podmínkách, pokud jde o politiku, organizace, kulturu, společenskou strukturu a vyspělost NCSS. Některé členské státy dotazované v rámci této studie uvedly, že by mohlo být obtížné obhajovat a používat „jediný rámec pro vlastní posouzení vhodný pro všechny“.

2.5 VÝHODY VNITROSTÁTNÍHO POSOUZENÍ SCHOPNOSTÍ

Všechny členské státy EU disponují od roku 2017 NCSS[20]. Kromě pozitivního vývoje je rovněž důležité, že členské státy mohou tyto NCSS správně posoudit, a tím do svého plánování a provádění svých strategií vnést přidanou hodnotu.

Jedním z cílů vnitrostátního rámce pro posouzení schopností je hodnotit schopnosti v oblasti kybernetické bezpečnosti podle priorit stanovených v různých NCSS. Rámec v zásadě posuzuje úroveň vyspělosti schopností v oblasti kybernetické bezpečnosti členských států v oblastech definovaných cíli NCSS. Výsledky rámce tedy podpoří tvůrce politik členských států při definování národní strategie kybernetické bezpečnosti, protože jim poskytnou informace o podmínkách v zemi[21]. Vnitrostátní rámec pro posouzení schopností má pomáhat členským státům s určováním oblastí zlepšení a budováním schopností.

Cílem tohoto rámce je poskytnout členským státům prostředek pro vlastní posouzení jejich úrovně vyspělosti prostřednictvím posouzení jejich cílů v oblasti NCSS, jež jim pomůže vylepšit a vybudovat schopnosti týkající se kybernetické bezpečnosti na strategické i provozní úrovni.

Z praktičtějšího hlediska byly na základě rozhovorů vedených agenturou ENISA s několika agenturami odpovědnými v různých členských státech za oblast kybernetické bezpečnosti zjištěny a zdůrazněny následující přednosti vnitrostátního rámce pro posouzení schopností:

- poskytovat užitečné informace pro vypracování dlouhodobé strategie (např. osvědčené postupy, pokyny),
- zjistit chybějící prvky v rámci NCSS,
- dále rozvíjet schopnosti v oblasti kybernetické bezpečnosti,
- podporovat odpovědnost politických opatření,
- zajišťovat důvěryhodnost ze strany široké veřejnosti a mezinárodních partnerů,
- podporovat dosah a zlepšovat vnímání veřejnosti jakožto transparentní organizace,
- předjímat budoucí problémy,
- určovat poučení a osvědčené postupy,
- poskytovat základ pro schopnosti v oblasti kybernetické bezpečnosti v celé EU, aby se usnadnily diskuse, a
- vyhodnocovat vnitrostátní schopnosti týkající se kybernetické bezpečnosti.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), s. 468–486.

3. METODOLOGIE VNITROSTÁTNÍHO RÁMCE PRO POSOUZENÍ SCHOPNOSTÍ

3.1 HLAVNÍ CÍL

Hlavním cílem vnitrostátního rámce pro posouzení schopností je stanovení úrovně schopností **členských států** v oblasti kybernetické bezpečnosti, aby se podpořilo jejich hodnocení vnitrostátní schopnosti v oblasti kybernetické bezpečnosti, zvyšování povědomí o úrovni vyspělosti země, určení oblastí ke zlepšení a budování schopností v oblasti kybernetické bezpečnosti.

3.2 ÚROVNĚ VYSPĚLOSTI

Rámec je založen na **pěti úrovních vyspělosti** definujících fáze, jimiž členské státy prochází při budování schopností v oblasti kybernetické bezpečnosti v oblastech jednotlivých cílů NCSS. Tyto úrovně představují zvyšující se úrovně vyspělosti, počínaje první **úrovní 1**, kdy členské státy nemají jasně stanovený přístup pro zlepšování schopností v oblasti kybernetické bezpečnosti v oblastech cílů NCSS, a konče **úrovní 5**, kdy je strategie budování schopností v oblasti kybernetické bezpečnosti dynamická a přizpůsobuje se vývoji okolního prostředí. Tabulka 4 ukazuje stupnici úrovní vyspělosti s popisem každé této úrovně.

Tabulka 4: Pětiúrovňová stupnice vyspělosti agentury ENISA pro vnitrostátní rámec pro posouzení schopností

ÚROVEŇ 1 – POČÁTEČNÍ / AD HOC	ÚROVEŇ 2 – RANÁ DEFINICE	ÚROVEŇ 3 – VYTVOŘENÍ	ÚROVEŇ 4 – OPTIMALIZACE	ÚROVEŇ 5 – ADAPTABILITA
Členský stát nemá jasně definovaný přístup pro budování schopností v oblasti kybernetické bezpečnosti a tématech uvedených v cílech NCSS. Země nicméně může disponovat některými obecnými cíli a provádět určité studie (technické, politické, strategické), aby se její schopnosti zlepšily.	Je definován vnitrostátní přístup k budování schopností v oblastech uvedených v cílech NCSS. Existují akční plány nebo činnosti k dosažení výsledků, byť v rané fázi. Dále mohou být určeny a/nebo zapojeny aktivní zúčastněné strany.	Je jasně určen akční plán pro budování schopností v oblasti upravené cíli NCSS a podporují jej příslušné zúčastněné subjekty. Postupy a činnosti jsou na vnitrostátní úrovni prosazovány a prováděny jednotně. Činnosti jsou definovány a zdokumentovány s jasným rozdělením prostředků, řízením a souborem lhůt.	Akční plán je pravidelně posuzován: má přednost, je optimalizovaný a udržitelný. Výsledky činností při budování schopností v oblasti kybernetické bezpečnosti jsou pravidelně hodnoceny. Při provádění těchto činností jsou určeny faktory úspěchu, problémy a nedostatky.	Strategie budování schopností v oblasti kybernetické bezpečnosti je dynamická a adaptivní. Nepřetržitá pozornost věnovaná vývoji prostředí (technologický pokrok, globální konflikty, nové hrozby...) podporuje schopnost rychlého rozhodování a schopnost rychle prosazovat zlepšení.

3.3 KLASTRY A ZASTŘEŠUJÍCÍ STRUKTURA RÁMCE PRO VLASTNÍ POSOUZENÍ

Rámec pro vlastní posouzení charakterizují **čtyři klastry**: I) Řízení a normy kybernetické bezpečnosti; II) Budování schopností a zvyšování povědomí; III) Právní a regulační povinnosti a IV) Spolupráce. Každý klastr zahrnuje hlavní tematickou oblast budování schopností v oblasti kybernetické bezpečnosti v zemi a obsahuje soubor různých cílů, jež mohou členské státy zahrnout do svých NCSS. Konkrétně:

- **I) Řízení a normy kybernetické bezpečnosti**: tento klastr měří schopnosti členského státu pro vytvoření správného řízení, norem a osvědčených postupů v oblasti kybernetické bezpečnosti. Tato oblast se zabývá různými aspekty kybernetické obrany a odolnosti a současnou podporou rozvoje vnitrostátního odvětví kybernetické bezpečnosti a budování důvěry ve státní správu.
- **II) Budování schopností a zvyšování povědomí:** tento klastr se týká schopnosti členských států zvyšovat povědomí o rizicích a hrozbách kybernetické bezpečnosti a jejich odstraňování. Dále tato oblast hodnotí schopnost země nepřetržitě budovat schopnosti v oblasti kybernetické bezpečnosti a zvyšovat celkovou úroveň znalostí a dovedností v této oblasti. Zabývá se rozvojem trhu s kybernetickou bezpečností a pokroku ve VaV kybernetické bezpečnosti. Tento klastr reorganizuje všechny cíle, aby vznikl základ podporující budování schopností.
- **III) Právní a regulační povinnosti:** tento klastr hodnotí schopnost členských států zavádět nezbytné právní a regulační nástroje k řešení a boji proti vzestupu kybernetické kriminality a souvisejících kybernetických incidentů a k ochraně kritické informační infrastruktury. Dále tato oblast posuzuje schopnost členských států vytvořit právní rámec za účelem chránit občany a podniky například v případě vyváženosti bezpečnosti a soukromí.
- **IV) Spolupráce:** tento klastr hodnotí spolupráci a sdílení informací mezi různými skupinami zúčastněných stran na vnitrostátní i mezinárodní úrovni jakožto důležitý nástroj pro lepší pochopení a reakci na neustále se měnící prostředí hrozeb.

Cíle, které byly zahrnuty do modelu, jsou cíle obecně přijímané členskými státy a byly vybrány mezi cíli uvedenými v části 2.2. Model zejména posuzuje tyto cíle:

- 1. Vypracovat vnitrostátní pohotovostní plány kybernetické bezpečnosti (I)
- 2. Vytvořit základní bezpečnostní opatření (I)
- 3. Zabezpečit digitální identitu a budovat důvěru v digitální veřejné služby (II)
- 4. Vytvořit schopnost reakce na incident (II)
- 5. Zvyšovat povědomí uživatelů (II)
- 6. Pořádat cvičení v oblasti kybernetické bezpečnosti (II)
- 7. Zlepšit programy odborné přípravy a vzdělávání (II)
- 8. Podporovat VaV (II)
- 9. Poskytovat pobídky soukromému sektoru k investování do bezpečnostních opatření (II)
- 10. Zlepšit kybernetické bezpečnosti dodavatelského řetězce (II)
- 11. Ochránit kritické informační infrastruktury, OES a DSP (III)
- 12. Bojovat proti kybernetické kriminalitě (III)
- 13. Vytvořit mechanismy hlášení incidentů (III)
- 14. Zesílit informační soukromí a ochranu údajů (III)
- 15. Institucionalizovat spolupráci mezi veřejnými agenturami (IV)
- 16. Zapojit se do mezinárodní spolupráce (IV)
- 17. Vytvářet partnerství veřejného a soukromého sektoru (IV)

Tyto čtyři klastry a výchozí cíle jsou spojeny do modelu, aby vznikl holistický náhled na vyspělost schopností členských států v oblasti kybernetické bezpečnosti. Obrázek 1 představuje zastřešující strukturu rámce pro vlastní posouzení a ukazuje, jak jsou tyto prvky, konkrétně cíle, klastry a rámec pro vlastní posouzení, spojeny s hodnocením výsledků země.

Obrázek 1: Struktura rámce pro vlastní posouzení

U jednotlivých cílů obsažených v rámci pro vlastní posouzení existuje řada ukazatelů rozdělených do pěti úrovní vyspělosti. Každý ukazatel je založen na uzavřených otázkách (ano/ne). Ukazatel může být povinný nebo nepovinný.

3.4 MECHANISMUS HODNOCENÍ

Mechanismus hodnocení rámce pro vlastní posouzení zohledňuje výše uvedené prvky a zásady uvedené v části 3.5. Tento model ve skutečnosti stanoví skóre podle hodnoty dvou

parametrů – **úroveň vyspělosti** a **míru splnění**. Každý z těchto parametrů lez vypočítat na různých úrovních: i) podle jednotlivých cílů; ii) podle klastrů cílů nebo iii) celkově.

Skóre na úrovni cíle

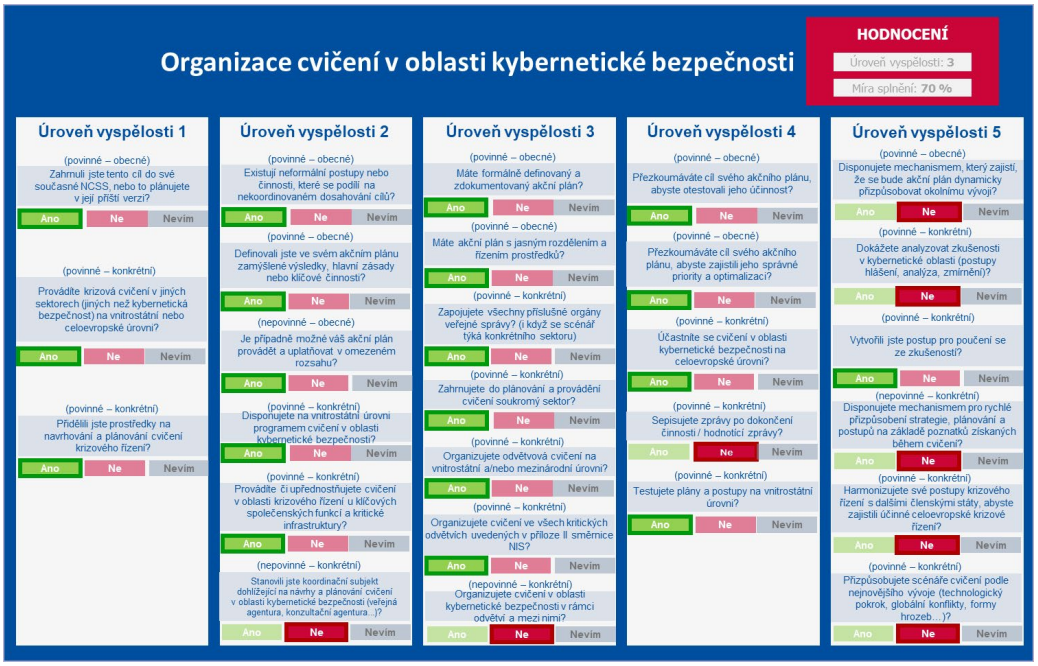
Skóre úrovně vyspělosti nabízí přehled úrovně vyspělosti tím, že ukazuje, jaké existují schopnosti a postupy. Skóre úrovně vyspělosti se vypočítá jako nejvyšší úroveň, kdy respondent vyhoví všem povinným položkám (tj. odpověď ANO na všechny povinné otázky), a navíc jsou splněny všechny povinné položky předcházejících úrovní vyspělosti.

Míra splnění ukazuje rozsah splnění všech ukazatelů s kladnou odpovědí, a to bez ohledu na jejich úroveň. Jedná se o doplňkovou hodnotu, jež zohledňuje všechny ukazatele pro hodnocení cíle. Míra splnění se vypočítá jako poměr mezi celkovým počtem otázek v rámci cíle a počtem otázek s kladnou odpovědí.

Je důležité vyjasnit, že ve zbývajícím dokumentu se slovo ***skóre*** používá jak pro hodnoty úrovně vyspělosti, tak pro míru splnění.

Obrázek 2 – Mechanismus hodnocení podle jednotlivých cílů nabízí vizualizaci mechanismu hodnocení popsaného v části 3.1, o němž bude podrobněji pojednáno níže.

Obrázek 2: Mechanismus hodnocení podle jednotlivých cílů



Obrázek 2 ukazuje příklad, jak se vypočítá úroveň vyspělosti podle cíle. Je třeba poznamenat, že respondent splnil všechny povinné položky prvních tří úrovní vyspělosti a jen některé položky úrovně 4. Skóre tedy ukazuje, že ***úroveň vyspělosti respondenta se nachází na úrovni 3 pro cíl „Organizace cvičení v oblasti kybernetické bezpečnosti“****.*

Nicméně v příkladu, který znázorňuje Obrázek 2, nedokáže úroveň vyspělosti cíle zachytit informaci poskytnutou ukazateli s kladným skóre a nad úrovní vyspělosti 3. V tomto případě může míra splnění poskytnout přehled všech prvků, které respondent provádí pro splnění dotčeného cíle i přes skutečnou úroveň vyspělosti. V tomto případě se poměr mezi celkovým počtem otázek v rámci cíle a počtem otázek s kladnou odpovědí rovná 19/27, tj. ***míra splnění činí 70 %****.*

Aby se skóre dále přizpůsobilo konkrétním podmínkám členských států a rovněž bylo možné zajistit soudržný přehled, vypočítá se ze dvou různých vzorků na úrovni klastru a na celkové úrovni.

- **Obecná skóre:** jeden kompletní vzorek pokrývající všechny cíle v klastru nebo v celkovém rámci (od 1 do 17).
- **Konkrétní skóre:** jeden specifický vzorek zahrnující pouze cíle vybrané členským státem (obvykle odpovídají cílům uvedeným v NCSS konkrétní země) z klastru nebo z celkového rámce.

Skóre na úrovni klastru

Obecná úroveň vyspělosti jednotlivých klastrů se vypočítá jako aritmetický průměr úrovně vyspělosti všech cílů v dotčeném klastru.

Konkrétní úroveň vyspělosti jednotlivých klastrů se vypočítá jako aritmetický průměr úrovně vyspělosti cílů v dotčeném klastru, které si členský stát vybral k posouzení (obvykle odpovídají cílům uvedeným v NCSS konkrétní země).

Například Obrázek 1 ukazuje, že se klastr (I) Řízení a normy kybernetické bezpečnosti skládá ze tří cílů. Za předpokladu, že si respondent zvolí posouzení pouze prvních dvou cílů, ale nikoli třetího, a za předpokladu, že první dva cíle vyspělosti představují úrovně vyspělosti 2 a 4, pak se klastr zahrnující všechny cíle nachází na úrovni 2 (klastr (I) obecná úroveň vyspělosti = (2 + 4) / 3), zatímco úroveň klastru zahrnujícího pouze konkrétní hodnotitelem vybrané cíle je 3 (klastr (I) konkrétní úroveň vyspělosti = (2 + 4) / 2).

Obecná míra splnění u jednotlivých klastrů se vypočítá jako poměr mezi celkovým počtem otázek v rámci dotčeného klastru a počtem otázek s kladnou odpovědí.

Konkrétní míra splnění u jednotlivých klastrů se vypočítá jako poměr mezi celkovým počtem otázek v rámci dotřeného klastru týkajících se cílů, jež si členský stát vybral k posouzení (obvykle odpovídají cílům uvedeným v NCSS konkrétní země), a počtem otázek s kladnou odpovědí.

Skóre na celkové úrovni

Celková obecná úroveň vyspělosti země se vypočítá jako aritmetický průměr úrovně vyspělosti všech cílů v dotčeném rámci – od 1 do 17.

Celková konkrétní úroveň vyspělosti země se vypočítá jako aritmetický průměr úrovně vyspělosti cílů v dotčeném rámci, které si členský stát vybral k posouzení (obvykle odpovídají cílům uvedeným v NCSS konkrétní země).

Celková obecná míra splnění u země se vypočítá jako poměr mezi celkovým počtem otázek v dotčeném rámci (od 1 do 17) a počtem otázek s kladnou odpovědí.

Konkrétní míra splnění u země se vypočítá jako poměr mezi celkovým počtem otázek v cílech dotčeného rámce, jež si členský stát vybral k posouzení (obvykle odpovídají cílům uvedeným v NCSS konkrétní země), a počtem otázek s kladnou odpovědí.

Respondenti mohou u jednotlivých ukazatelů zvolit jako odpověď třetí možnost „nevím / není k dispozici“. V tomto případě bude tento ukazatel vyloučen z celkového výpočtu výsledků.

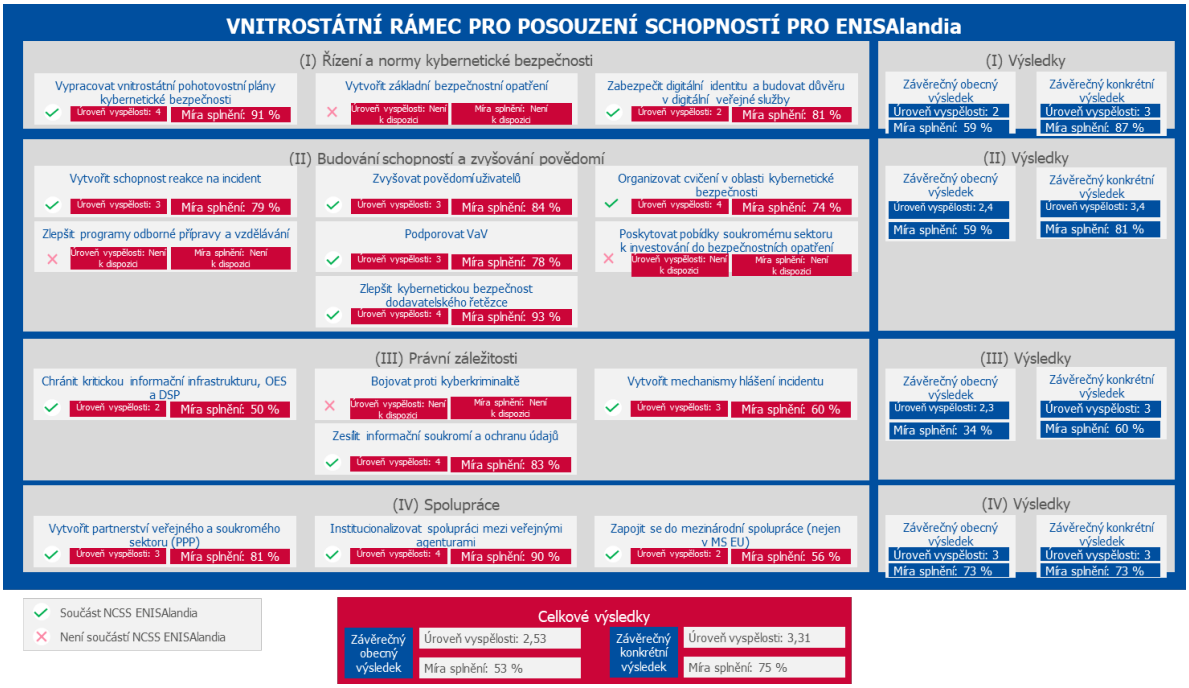
Úrovně vyspělosti na úrovni klastru a celkové úrovni se vypočítají pomocí aritmetického průměru, aby byl patrný pokrok mezi dvěma posouzeními. Alternativa skládající se z výpočtu úrovní vyspělosti klastru a celkové úrovně vyspělosti jako úrovně vyspělosti alespoň jednoho

cíle vyspělosti – i když z hlediska vyspělosti důležitého – nemůže zachytit pokrok učiněný v oblastech náležejících do jiných cílů.

Protože jsou úroveň klastru a celková úroveň kvůli podávání zpráv konsolidovány, byl zvolen aritmetický průměr. Pro větší přesnost použijte při podávání zpráv skóre na úrovni cíle.

Obrázek 3 níže shrnuje mechanismy hodnocení na různých úrovních modelu (cíl, klastr, celkem).

Obrázek 3: Mechanismus celkového hodnocení



3.5 POŽADAVKY NA RÁMEC PRO VLASTNÍ POSOUZENÍ

Vnitrostátní rámec pro posouzení schopností představený v této části vychází z potřeb zdůrazněných členskými státy a ze souboru níže uvedených požadavků:

- Členské státy uplatňují vnitrostátní rámec pro vlastní posouzení schopností jako rámec pro vlastní posouzení dobrovolně.
- Vnitrostátní rámec pro posouzení schopností se zaměřuje na hodnocení schopností členských států v oblasti kybernetické bezpečnosti s ohledem na sedmnáct cílů. Členský stát si nicméně může zvolit cíle, které chce posuzovat, a posoudit pouze dílčí výběr z těchto sedmnácti cílů.
- Rámec pro vlastní posouzení se zaměřuje na hodnocení úrovně vyspělosti schopností členských států v oblasti kybernetické bezpečnosti.
- Výsledky posouzení nebudou zveřejněny, dokud o tom nerozhodne sám členský stát z vlastní iniciativy.
- Členský stát může zveřejnit výsledky posouzení uvedením úrovně vyspělosti schopností země v oblasti kybernetické bezpečnosti, klastru cílů nebo i jediného cíle.
- Všechny posuzované cíle jsou v rámci posouzení stejně důležité, mají tedy stejný význam. To platí i pro použité ukazatele zavedené v jeho rámci.
- Členský stát bude moci sledovat svůj pokrok v čase.

Rámec pro vlastní posouzení se zaměřuje na podporu členských států při budování schopností v oblasti kybernetické bezpečnosti. Proto zahrnuje rovněž soubor doporučení a pokynů, které evropské země využijí při zvyšování své úrovně vyspělosti.

Poznámka: tato doporučení nebo pokyny jsou obecné a jsou založeny na publikacích agentury ENISA a zkušenostech z jiných zemí a budou vycházet z výsledků vlastních posouzení.

4. UKAZATELE VNITROSTÁTNÍHO RÁMCE PRO POSOUZENÍ SCHOPNOSTÍ

4.1 RÁMCOVÉ UKAZATELE

Tato část pojednává o vnitrostátním rámci pro posouzení schopností agentury ENISA. Následující části jsou uspořádány do klastrů.

U každého klastru je uveden komplexní soubor ukazatelů, který má podobu otázek odpovídajících dotčené úrovni vyspělosti. Tento dotazník je hlavním nástrojem vlastního posouzení. U jednotlivých cílů upozorňujeme na dva soubory ukazatelů:

- soubor obecných otázek ke strategické vyspělosti (devět obecných otázek) označených pro jednotlivé úrovně vyspělosti jako a) až c), které se opakují u každého cíle, a
- soubor otázek týkajících se schopností v oblasti kybernetické bezpečnosti (319 otázek týkajících se schopností v oblasti kybernetické bezpečnosti) očíslovaných u jednotlivých úrovní vyspělosti 1 až 10, jež jsou konkrétní pro oblast, která se vztahuje na daný cíl.

Každá otázka je uvedena s označením (0–1) informujícím, zda je otázka pro dotčenou úroveň vyspělosti povinným (1), nebo nepovinným (0) ukazatelem.

Každou otázku lze určit pomocí identifikačního čísla, které se skládá z:

- čísla cíle,
- úrovně vyspělosti a
- čísla otázky.

Například otázka s ID 1.2.4 je čtvrtou otázkou úrovně vyspělosti 2 strategického cíle (I) „Vypracovat vnitrostátní pohotovostní plány kybernetické bezpečnosti“.

Je třeba poznamenat, že nebude-li uvedeno jinak, týkají se otázky v celém tomto dotazníku otázky vnitrostátní úrovně. Ve všech otázkách se oslovení „vy“ týká obecně členského státu a nevztahuje se na jednotlivce či správní orgán provádějící posouzení.

Definice jednotlivých cílů najdete v kapitolách 2.2–Společné cíle určené v rámci evropské NCSS.

4.1.1 Klastr č. 1: Řízení a normy kybernetické bezpečnosti

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
1 – Vypracovat vnitrostátní pohotovostní plány kybernetické bezpečnosti	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Začali jste pracovat na přípravě vnitrostátních pohotovostních plánů kybernetické bezpečnosti? *Např.* stanovením hlavních cílů, oblasti působnosti a/nebo zásad pohotovostních plánů…	1	Disponujete doktrínou / národní strategií, jež uvádí kybernetickou bezpečnost jako krizový faktor (tj. vzorový plán, strategii atd.)?	1	Máte vnitrostátní plán krizového řízení v oblasti kybernetické bezpečnosti?	1	Jste spokojeni s počtem nebo procentním podílem kritických odvětví zahrnutých do vnitrostátního pohotovostního plánu kybernetické bezpečnosti?	1	Využíváte po kybernetických cvičeních nebo skutečných krizích na vnitrostátní úrovni postup poučení se ze zkušeností?	1
	2	Panuje obecná shoda, že kybernetické incidenty představují krizový faktor, který by mohl ohrozit národní bezpečnost?	0	Disponujete centrem pro shromažďování informací a jejich předávání rozhodujícím činitelům? *Tj.* jakékoliv postupy, platformy nebo místa zajišťující, že budou mít všechny subjekty reagující na krizi přístup ke stejným informacím v reálném čase o kybernetické krizi.	1	Máte konkrétní postupy krizového řízení v oblasti kybernetické bezpečnosti na vnitrostátní úrovni?	1	Organizujete dostatečně často činnosti (tj. cvičení) související s vnitrostátními pohotovostními plány kybernetické bezpečnosti?	1	Testujete národní plán pravidelně?	1
	3	Provedli jste studie (technické, operační, politické) v oblasti vnitrostátních pohotovostních plánů kybernetické bezpečnosti?	0	Jsou využity vhodné prostředky pro dohled nad přípravou a prováděním vnitrostátních pohotovostních plánů kybernetické bezpečnosti?	1	Disponujete komunikačními týmy speciálně proškolenými pro reakci na kybernetické krize a informování veřejnosti?	1	Máte dostatek lidí pro krizové plánování, přezkum zkušeností a provádění změn?	1	Máte vhodné nástroje a platformy k budování povědomí o situaci?	1
	4	-		Disponujete metodologií pro posouzení kybernetických hrozeb na vnitrostátní úrovni, která zahrnuje postupy posouzení dopadů?	0	Zapojili jste všechny příslušné vnitrostátní zúčastněné strany (národní bezpečnost, obranu, civilní obranu, donucovací orgány, ministerstva, úřady atd.?)	1	Máte na vnitrostátní úrovni dostatek lidí proškolených pro reakci na kybernetické krize?	1	Postupujete při sledování a zlepšování pohotovostního plánu kybernetické bezpečnosti podle konkrétního modelu vyspělosti?	0
	5	-		-		Disponujete vhodnými zařízeními a situačními středisky pro krizové řízení?	1	-		Máte prostředky buď specializované na předjímání hrozeb, nebo práci na budoucí kybernetické bezpečnosti pro řešení budoucích krizí či problémů?	0
	6	-		-		Zapojujete v případě potřeby zahraniční zúčastněné strany z EU?	0	-		-	

	7	-		-		Zapojujete v případě potřeby zahraniční zúčastněné strany ze zemí mimo EU?	0	-		-	
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
2 – Vytvořit základní bezpečnostní opatření	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Vypracovali jste studii zjišťující požadavky a nedostatky **veřejných** organizací podle mezinárodně uznávaných norem? *Např.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Jsou navržena bezpečnostní opatření odpovídající mezinárodním/vnitrostátním normám?	1	Jsou základní bezpečnostní opatření povinná?	1	Existuje postup časté aktualizace základních bezpečnostních opatření?	1	Disponujete postupem zesílení odolnosti IKT, jestliže tato opatření incident nevyřeší?	1
	2	Vypracovali jste studii zjišťující požadavky a nedostatky **soukromých** organizací podle mezinárodně uznávaných norem? Např. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Je při definování základních bezpečnostních opatření konzultován soukromý sektor a další zúčastněné strany?	1	Provádíte v kritických sektorech horizontální bezpečnostní opatření?	1	Existuje mechanismus sledování pro přezkum uplatňování základních bezpečnostních opatření?	1	Posuzujete příslušnost nových norem vypracovaných jako reakce na nejnovější vývoj, pokud jde o formy hrozeb?	1
	3	-		-		Provádíte v kritických sektorech konkrétní bezpečnostní opatření?	1	Existuje vnitrostátní orgán kontrolující prosazování či neprosazování základních bezpečnostních opatření?	1	Máte nebo propagujete vnitrostátní postup koordinovaného zveřejňování zranitelností (CVD)?	1
	4	-				Odpovídají základní bezpečnostní opatření příslušným certifikačním režimům?	1	Disponujete postupem identifikace organizací, které ve stanoveném čase neplní pokyny?	1	-	
	5	-		-		Existuje proces vlastního posouzení rizik zaměřený na základní bezpečnostní opatření?	1	Existuje kontrolní proces zajišťující správné uplatňování bezpečnostních opatření?	1	-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
2 – Vytvořit základní bezpečnostní opatření	6	-		-		Přezkoumáváte v procesu zadávání veřejných zakázek správních orgánů povinná bezpečnostní opatření?	0	Definujete nebo aktivně podporujete přijímání bezpečnostních norem pro vývoj kritických IT/OT produktů (zdravotnická zařízení, síťová a autonomní vozidla, profesionální vysílací vybavení, vybavení těžkého průmyslu…)?	0	-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
3 – Zabezpečit digitální identitu a budovat důvěru v digitální veřejné služby	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Vypracovali jste studie nebo analýzy nedostatků identifikující potřebu zabezpečit digitální veřejné služby pro občany či podniky?	1	Analyzujete rizika, abyste stanovili profil rizika věcí či služeb, než je přesunete do cloudu, nebo využití jakéhokoli projektu digitální transformace?	1	Podporujete metodologie „soukromí již od návrhu“ ve všech projektech elektronické veřejné správy?	1	Shromažďujete ukazatele o incidentech kybernetické bezpečnosti, kdy došlo k narušení digitálních veřejných služeb?	1	Účastníte se evropských pracovních skupin pro zachování norem a/nebo formulování nových požadavků na důvěryhodné elektronické služby (elektronické podpisy, elektronické pečetě, služby elektronického doporučeného doručování, časová razítka, autentizace internetových stránek)? Např. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU...	1
	2	-		Máte strategii budování nebo propagace vnitrostátních systémů elektronické identifikace pro občany a podniky?	1	Spolupracujete na navrhování a realizaci bezpečných digitálních veřejných služeb se soukromými zúčastněnými stranami?	1	Provedli jste vzájemné uznávání prostředků elektronické identifikace s jinými členskými státy?	1	Účastníte se aktivně vzájemných přezkumů v rámci režimů oznamování elektronické identifikace Evropské komisi?	1

	3	-		Disponujete strategií budování nebo podpory bezpečných vnitrostátních důvěryhodných elektronických služeb (elektronické podpisy, elektronické pečetě, služby elektronického doporučeného doručování, časová razítka, autentizace internetových stránek) pro občany a podniky?	1	Provádíte pro všechny digitální veřejné služby minimální bezpečnostní základ?	1	-		-	
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
3 – Zabezpečit digitální identitu a budovat důvěru v digitální veřejné služby	4	-		Máte strategii pro cloud státní správy (cloudová výpočetní strategie zaměřená na státní správu a veřejné orgány, jako jsou ministerstva, vládní agentury a veřejná správa…), která zohledňuje aspekty bezpečnosti?	0	Jsou občanům a podnikům k dispozici jakékoliv systémy elektronické identifikace s podstatnou či vysokou úrovní zabezpečení podle přílohy nařízení eIDAS (EU) č. 910/2014?	1	-		-	
	5	-		-		Využíváte digitální veřejné služby vyžadující systémy elektronické identifikace s podstatnou či vysokou úrovní zabezpečení podle přílohy nařízení eIDAS (EU) č. 910/2014?	1	-		-	
	6	-		-		Jsou u vás důvěryhodní poskytovatelé služeb pro občany a podniky (elektronické podpisy, elektronické pečetě, služby elektronického doporučeného doručování, časová razítka, autentizace internetových stránek)?	1	-		-	
	7	-		-		Podporujete přijímání základních bezpečnostních opatření pro všechny modely využití cloudů (např. soukromé, veřejné, hybridní. IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Klastr č. 2: Budování schopností a zvyšování povědomí

Cíl NCSS	Č.	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
4 – Vytvořit schopnost reakce na incident	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Disponujete schopnostmi pro neformální reakce na incidenty řízené v rámci veřejného a soukromého sektoru nebo mezi nimi?	1	Máte alespoň jeden oficiální vnitrostátní tým CSIRT?	1	Disponujete schopnostmi pro reakci na incidenty u sektorů uvedených v příloze II směrnice NIS?	1	Definovali jste a propagujete standardizované postupy reakce na incident a režimy klasifikace incidentů?	1	Máte jakékoli mechanismy včasného odhalení, určování, prevence, reakce a zmírňování zranitelností nultého dne?	1
	2	-		Mají vaše vnitrostátní týmy CSIRT jasně stanovený rozsah intervence? Např. podle cíleného sektoru, druhů incidentů, dopadů.	1	Existuje ve vaší zemi mechanismus spolupráce týmů CSIRT při reakci na incidenty?	1	Vyhodnocujete svou schopnost reakce na incidenty, abyste zajistili, že budete mít dostatečné prostředky a dovednosti k provádění úkolů stanovených v bodu (2) přílohy I směrnice NIS?	1	-	
	3	-		Mají vaše vnitrostátní týmy CSIRT definovány vztahy s ostatními vnitrostátními zúčastněnými stranami týkající se národní kybernetické bezpečnosti a postupů reakce na incidenty (např. LEA, armáda, ISP, NCSC)?	0	Mají vaše vnitrostátní týmy CSIRT schopnost reakce na incidenty podle přílohy I směrnice NIS? Tj. musí u nich být zajištěna dostupnost, fyzické zabezpečení, kontinuita činnosti, mezinárodní spolupráce, sledování incidentů, schopnosti včasného varování a výstrah, reakce na incidenty, analýzy rizik a povědomí o situaci, spolupráce se soukromým sektorem, standardní postupy...	1	-		-	
	4	-				Existuje mechanismus spolupráce s dalšími sousedními zeměmi zaměřený na incidenty?	1	-		-	
	5	-		-		Stanovili jste formálně jasné strategie a postupy pro řešení incidentů?	1	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
4 – Vytvořit schopnost reakce na incident	6	-		-		Účastní se vaše vnitrostátní týmy CSIRT cvičení kybernetické bezpečnosti na vnitrostátní i mezinárodní úrovni?	1	-		-	
	7	-		-		Zapojují se vaše vnitrostátní týmy CSIRT do FIRST (fóra týmů pro reakci na bezpečnostní incidenty počítačů)?	0	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
5 – Zvyšovat povědomí uživatelů	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Uznávají státní správa, soukromý sektor nebo běžní uživatelé alespoň minimálně, že je nutné zvyšovat povědomí o záležitostech kybernetické bezpečnosti a soukromí?	1	Identifikovali jste specifickou cílovou skupinu pro zvyšování povědomí uživatelů? *Např.* běžní uživatelé, mladí lidé, komerční uživatelé (které lze dále shrnout jako: MSP, OES, DSP atd.).	1	Vypracovali jste komunikační plány / strategie kampaní?	1	Navrhli jste metriku pro hodnocení vašich kampaní ve fázi plánování?	1	Disponujete mechanismy zajišťujícími, že budou kampaně na zvýšení povědomí neustále relevantní pro technologický pokrok, změny forem hrozeb a vnitrostátní bezpečnostní směrnice?	1
	2	Provádí veřejné agentury v rámci svých organizací *ad hoc* kampaně na zvyšování povědomí o kybernetické bezpečnosti? Např. v důsledku incidentu kybernetické bezpečnosti.	0	Navrhli jste projektový plán na zvyšování povědomí o problémech informační bezpečnosti a soukromí?	1	Disponujete postupem pro vytváření obsahu na úrovni státní správy?	1	Vyhodnocujete své kampaně po realizaci?	1	Provádíte pravidelná hodnocení nebo studie pro stanovení posunu opatření nebo změn chování týkajících se záležitostí kybernetické bezpečnosti v soukromém a veřejném sektoru?	1

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
5 – Zvyšovat povědomí uživatelů	3	Provádí veřejné agentury v rámci svých organizací *ad hoc* kampaně na zvyšování povědomí o kybernetické bezpečnosti zaměřené na obecnou veřejnost? Např. v důsledku incidentu kybernetické bezpečnosti.	0	Máte k dispozici snadno identifikovatelné prostředky (např. jednotný on-line portál, sady pro zvyšování povědomí) pro všechny uživatele, kteří se chtějí vzdělávat v otázkách kybernetické bezpečnosti a soukromí?	1	Máte nějaké mechanismy k určení cílových oblastí pro zvyšování povědomí (tj. forem hrozeb ENISA, vnitrostátní oblasti, zahraniční oblasti, zpětná vazba od vnitrostátních center pro kybernetickou kriminalitu atd.)?	1	Existují u vás jakékoli mechanismy pro určení nejdůležitějších mediálních nebo komunikačních kanálů podle cílových skupin, aby se maximalizoval dosah a zapojení? Např. různé druhy digitálních médií, brožury, elektronická pošta, výukový materiál, plakáty v rušných oblastech, televize, rozhlas…	1	Konzultujete behaviorální odborníky, abyste své kampaně přizpůsobovali pro cílovou skupinu?	1
	4	-		-		Podílí se u vás na vytváření obsahu společně zúčastněné strany s odborníky a komunikačními týmy?	1			-	
	5	-		-		Zapojujete do svých činností na zvyšování povědomí soukromý sektor, abyste podporovali a šířili zprávy pro širší publikum?	1	-		-	
	6	-		-		Připravujete konkrétní iniciativy pro zvyšování povědomí pro vedoucí pracovníky veřejného, soukromého a akademického sektoru nebo občanské společnosti?	1	-		-	
	7	-		-		Účastníte se kampaní agentury ENISA Evropský měsíc kybernetické bezpečnosti (ECSM)?	0	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
6 – Organizovat cvičení v oblasti kybernetické bezpečnosti	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						

6 – Organizovat cvičení v oblasti kybernetické bezpečnosti	1	Provádíte krizová cvičení v jiných sektorech (jiných než kybernetická bezpečnost) na vnitrostátní nebo celoevropské úrovni?	1	Disponujete na vnitrostátní úrovni programem cvičení v oblasti kybernetické bezpečnosti?	1	Zapojujete všechny příslušné orgány veřejné správy? (i když se scénář týká konkrétního sektoru)	1	Sepisujete zprávy po dokončení činnosti / hodnotící zprávy?	1	Dokážete analyzovat zkušenosti v kybernetické oblasti (postupy hlášení, analýza, zmírnění)?	1
	2	Přidělili jste prostředky na navrhování a plánování cvičení krizového řízení?	1	Provádíte či upřednostňujete cvičení v oblasti krizového řízení u klíčových společenských funkcí a kritické infrastruktury?	1	Zahrnujete do plánování a provádění cvičení soukromý sektor?	1	Testujete plány a postupy na vnitrostátní úrovni?	1	Vytvořili jste postup pro poučení se ze zkušeností?	1
	3	-		Stanovili jste koordinační subjekt dohlížející na návrhy a plánování cvičení v oblasti kybernetické bezpečnosti (veřejná agentura, konzultační agentura...)?	0	Organizujete odvětvová cvičení na vnitrostátní a/nebo mezinárodní úrovni?	1	Účastníte se cvičení v oblasti kybernetické bezpečnosti na celoevropské úrovni?	1	Přizpůsobujete scénáře cvičení podle nejnovějšího vývoje (technologický pokrok, globální konflikty, formy hrozeb…)?	1
	4	-		-		Organizujete cvičení ve všech kritických odvětvích uvedených v příloze II směrnice NIS?	1	-		Harmonizujete své postupy krizového řízení s dalšími členskými státy, abyste zajistili účinné celoevropské krizové řízení?	1
	5	-		-		Organizujete cvičení v oblasti kybernetické bezpečnosti v rámci odvětví a mezi nimi?	1	-		Disponujete mechanismem pro rychlé přizpůsobení strategie, plánování a postupů na základě poznatků získaných během cvičení?	0
	6	-		-		Organizujete cvičení v oblasti kybernetické bezpečnosti podle různých úrovní? (Technická a provozní úroveň, úroveň postupů, úroveň rozhodování, politická úroveň…)	0	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
7 – Zlepšit programy odborné přípravy a vzdělávání	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Zvažujete vypracování programů školení a vzdělávání v oblasti kybernetické bezpečnosti?	1	Organizujete kurzy týkající se kybernetické bezpečnosti?	1	Zabývá se vaše země kulturou kybernetické bezpečnosti v rané fázi vzdělávání studentů? Zabýváte se kybernetickou bezpečností například na středních a vysokých školách?	1	Požadujete akreditace a certifikace pracovníků soukromého a veřejného sektoru?	1	Disponujete mechanismy zajišťujícími, že budou programy školení a vzdělávání neustále relevantní pro nové technologické poznatky, změny forem hrozeb, právní předpisy a vnitrostátní bezpečnostní směrnice?	1
	2	-		Nabízí vysoké školy ve vaší zemi doktoráty (titul Ph.D.) v oblasti kybernetické bezpečnosti jako samostatného oboru, nikoli jako předmětu výuky počítačové vědy?	1	Disponujete národními výzkumnými laboratořemi a vzdělávacími institucemi specializujícími se na kybernetickou bezpečnost?	1	Vypracovala vaše země programy školení či mentorování v oblasti kybernetické bezpečnosti, které podpoří vnitrostátní startupy a MSP?	1	Vytváříte akademická střediska excelence v oblasti kybernetické bezpečnosti, která fungují jako centra výzkumu a vzdělávání?	1
	3	-		Plánujete školení pedagogických pracovníků, bez ohledu na jejich odbornost, v oblasti informační bezpečnosti a problematice soukromí? Např. on-line bezpečnost, ochrana osobních údajů, kyberšikana.	1	Podporujete/financujete kurzy a školicí plány v oblasti kybernetické bezpečnosti pro zaměstnance agentur zaměstnanosti členského státu?	1	Aktivně podporujete zařazení kurzů informační bezpečnosti do vyššího vzdělávání nejen u studentů počítačových věd, ale rovněž všech dalších profesních odborností? Např. kurzy organizované podle potřeb konkrétních profesí.	1	Účastní se akademické instituce hlavních mezinárodních diskusí v oblasti vzdělávání a výzkumu týkajících se kybernetické bezpečnosti?	0
	4	-		-		Disponujete kurzy kybernetické bezpečnosti a/nebo specializovanými osnovami pro úrovně 5 až 8 EQF (evropského rámce kvalifikací)?	1	Posuzujete pravidelně nedostatky v dovednostech (nedostatek pracovníků kybernetické bezpečnosti) v oblasti kybernetické bezpečnosti?	1	-	
	5	-		-		Podporujete a/nebo propagujete iniciativy na zahrnutí kurzů internetové bezpečnosti do primárního a sekundárního vzdělávání?	1	Podporujete vytváření sítí a sdílení informací mezi akademickými institucemi na vnitrostátní i mezinárodní úrovni?	1		

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
7 - Zlepšit programy odborné přípravy a vzdělávání	6	-		-		Financujete nebo nabízíte bezplatně základní školení kybernetické bezpečnosti určená občanům?	0	Zapojujete v jakékoli podobě do vzdělávacích iniciativ v oblasti kybernetické bezpečnosti soukromý sektor? Např. navrhování a poskytování kurzů, stáže, pracovní umístění…	1	-	
	7	-		-		Pořádáte každoroční akce s tematikou informační bezpečnosti (např. soutěže v hackování nebo hackathony)?	0	Provádíte mechanismy financování, abyste podpořili udělování titulů v oblasti kybernetické bezpečnosti? Např. stipendia, garantované stáže, garantovaná pracovní místa v konkrétních odvětvích nebo funkcích ve veřejném sektoru	0	-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
8 – Podporovat VaV	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Vypracovali jste studie nebo analýzy ke stanovení priorit VaV v oblasti kybernetické bezpečnosti?	1	Máte postup stanovení priorit VaV (např. vznikající témata pro zastrašování, ochranu, odhalování a přizpůsobování se novým druhům kybernetických útoků)?	1	Existuje plán na propojení iniciativ VaV s reálnou ekonomikou?	1	Jsou iniciativy VaV v oblasti kybernetické bezpečnosti v souladu s příslušnými strategickými cíli, např. DSM, H2020, Digitální Evropa, strategie kybernetické bezpečnosti Evropské unie?	1	Spolupracujete na vnitrostátní úrovni s nějakými mezinárodními iniciativami VaV spojenými s kybernetickou bezpečností?	1
	2	-		Je do stanovení priorit VaV zapojen soukromý sektor?	1	Existují nějaké vnitrostátní projekty související s kybernetickou bezpečností?	1	Existuje režim hodnocení iniciativ VaV?	1	Jsou priority VaV sladěny se současnými nebo budoucími předpisy (vnitrostátní úroveň)?	1

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
8 – Podporovat VaV	3	-		Je do stanovení priorit VaV zapojena akademická obec?	1	Disponujete místními/regionálními ekosystémy startupů a dalšími kanály pro vytváření sítí (např. technologické parky, inovační klastry, akcemi/platformami pro vytváření sítí) podporujícími inovaci (včetně startupů zabývajících se kybernetickou bezpečností)?	1	Jsou uzavřeny nějaké dohody o spolupráci s vysokými školami a dalšími výzkumnými zařízeními?	1	Účastníte se hlavních diskusí o jednom či více klíčových tématech VaV na mezinárodní úrovni?	0
	4	-		Existují nějaké vnitrostátní iniciativy VaV související s kybernetickou bezpečností?	0	Investuje se do programů VaV kybernetické bezpečnosti v rámci akademické obce a soukromého sektoru?	1	Existuje uznávaný institucionální orgán dohlížející na činnosti VaV v oblasti kybernetické bezpečnosti?	0	-	
	5	-		-		Máte funkce v odvětví průmyslového výzkumu na vysokých školách, aby došlo ke spojování předmětů výzkumu a poptávky na trhu?	1	-		-	
	6	-		-		Máte specializované programy financování VaV pro kybernetickou bezpečnost?	0	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
9– Poskytovat pobídky soukromému sektoru k investování do bezpečnostních opatření	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						

	1	Existuje průmyslová strategie nebo politická vůle k podpoře rozvoje odvětví kybernetické bezpečnosti?	1	Je do stanovení pobídek zapojen soukromý sektor?	1	Existují ekonomické/regulační či jiné pobídky k podpoře investic do kybernetické bezpečnosti?	1	Existují nějací soukromí aktéři reagující na pobídky investováním do bezpečnostních opatření? Např. investoři specializující se na kybernetickou bezpečnost a nespecializovaní investoři.	1	Zaměřujete pobídky na témata kybernetické bezpečnosti podle nejnovějšího vývoje hrozeb?	1
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
9– Poskytovat pobídky soukromému sektoru k investování do bezpečnostních opatření	2	–		Identifikovali jste konkrétní témata v oblasti kybernetické bezpečnosti, která se budou rozvíjet? Např. kryptografie, soukromí, nové formy ověřování, UI pro kybernetickou bezpečnost…	0	Podporujete (např. daňovými pobídkami) startupy a MSP zabývající se kybernetickou bezpečností?	1	Poskytujete pobídky soukromému sektoru, aby se zaměřoval na zabezpečení nejmodernějších technologií? Např. 5G, umělá inteligence, internet věcí, kvantová výpočetní technika…	1	–	
	3	–		–		Poskytujete daňové pobídky nebo jinou finanční motivaci investorům ze soukromého sektoru ve startupech zabývajících se kybernetickou bezpečností?	1	–		–	
	4	–		–		Usnadňujete přístup startupů a MSP v oblasti kybernetické bezpečnosti do procesu zadávání veřejných zakázek?	0	–		–	
	5	–		–		Jsou k dispozici finanční prostředky na pobídky soukromému sektoru?	0	–		–	

Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
10 – Zlepšit kybernetickou bezpečnost dodavatelského řetězce	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						

	1	Vypracovali jste studii o bezpečných osvědčených postupech pro správu dodavatelského řetězce používaných při zadávání veřejných zakázek v různých odvětvových segmentech a/nebo veřejném sektoru?	1	Provádíte posuzování kybernetické bezpečnosti v celém dodavatelském řetězci služeb a produktů IKT v kritických odvětvích (podle přílohy II směrnice NIS (2016/1148))?	1	Používáte režim bezpečnostní certifikace pro IKT produkty a služby? Např. SOG-IS MRA v Evropě (skupina vedoucích pracovníků pro bezpečnost informačních systémů, dohoda o vzájemné uznávání), dohoda o společném uznávání kritérií (CCRA), vnitrostátní a odvětvové iniciativy…	1	Máte k dispozici postup aktualizace posuzování kybernetické bezpečnosti dodavatelského řetězce služeb a produktů IKT v kritických odvětvích (podle přílohy II směrnice NIS (2016/1148))?	1	Sondujete klíčové prvky dodavatelského řetězce, abyste detekovali rané známky narušení? Např. bezpečnostní kontrolní prostředky na úrovni ISP, bezpečnostní sondy v hlavních částech infrastruktury…-	1

Cíl NCSS	Č.	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
10 – Zlepšit kybernetickou bezpečnost dodavatelského řetězce	2	-		Uplatňujete ve strategiích řízení veřejných zakázek normy zajišťující, že budou poskytovatelé produktů nebo služeb IKT splňovat základní požadavky na bezpečnost informací? Např. ISO/IEC 27001 a 27002, ISO/IEC 27036…	1	Aktivně podporujete bezpečnost a ochranu soukromí od začátku pomocí osvědčených postupů pro návrhy při vývoji IKT produktů a služeb? Např. bezpečný životní cyklus vývoje softwaru, životní cyklus internetu věcí	1	Máte k dispozici postup identifikace slabých míst v kybernetické bezpečnosti dodavatelského řetězce v kritických odvětvích (podle přílohy II směrnice NIS (2016/1148))?	1	-	
	3	-		-		Vypracováváte a poskytujete centrální katalogy s rozšířenými informacemi o stávajících normách informační bezpečnosti a ochraně soukromí, jež lze upravovat a používat v MSP?	1	Disponujete mechanismy zajišťujícími, že budou produkty a služby IKT důležité pro OES odolné z kybernetického hlediska (tj. schopnost zachování dostupnosti a zabezpečení proti kybernetickému incidentu)? Např. testováním, pravidelnými posouzeními, odhalováním narušených prvků…	1	-	
	4	-				Podílíte se aktivně na tvorbě certifikačního rámce EU pro digitální produkty, služby a procesy IKT, jak je stanoveno v aktu EU o kybernetické bezpečnosti (nařízení (EU) 2019/881)? Např. účast v Evropské skupině pro certifikaci kybernetické bezpečnosti (ECCG), podpora technických norem a postupů pro bezpečnost IKT produktů a služeb.	0	Podporujete rozvoj certifikačních režimů zaměřených na MSP, abyste zvýšili bezpečnost informací a přijímání norem v oblasti ochrany soukromí?	0	-	
	5	-		-		Poskytujete MSP nějaké pobídky pro přijímání norem v oblasti bezpečnosti a ochrany soukromí?	0	Uplatňujete nějaká ustanovení pobízející velké společnosti, aby zvyšovaly kybernetickou bezpečnost MSP ve svých dodavatelských řetězcích? Např. centra kybernetické bezpečnosti, školicí kampaně a kampaně na zvyšování povědomí…	0	-	
	6	-		-		Pobízíte dodavatele softwaru, aby podporovali MSP zajištěním bezpečných výchozích konfigurací produktů určených malým organizacím?	0	-		-	

4.1.3 Klastr č. 3: Právní a regulační povinnosti

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
11 – Chránit kritickou informační infrastrukturu, OES a DSP	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Panuje obecné přesvědčení, že provozovatelé KII přispívají k národní bezpečnosti?	1	Disponujete metodologií k určení zásadních služeb?	1	Uplatňujete směrnici NIS (2016/1148)?	1	Máte postup pro aktualizaci registru rizik?	1	Vytváříte a aktualizujete zprávy o typech hrozeb?	1
	2	-		Máte metodologii pro určování KII?	1	Uplatňujete směrnici (2008/114) o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu?	1	Disponujete dalšími mechanismy k hodnocení, zda jsou technická a organizační opatření, jež provádí OES, vhodná k řízení rizik pro bezpečnost sítí a informačních systémů? Např. pravidelné audity kybernetické bezpečnosti, vnitrostátní rámec pro provádění bezpečnostních opatření, technické nástroje poskytnuté vládou, jakými jsou detekční sondy nebo přezkumy konfigurací konkrétních systémů...	1	Dokážete na základě nejnovějšího vývoje, pokud jde o formy hrozeb, zahrnout do svého akčního plánu pro KII nové odvětví?	1
	3	-		Disponujete metodologií k určování OES?	1	Máte národní registr identifikovaných OES v jednotlivých kritických odvětvích?	1	Přezkoumáváte a následně aktualizujete seznam identifikovaných OES alespoň každé dva roky?	1	Dokážete na základě nejnovějšího vývoje, pokud jde o formy hrozeb, přizpůsobit nové požadavky ve svém akčním plánu pro KII?	1

Cíl NCSS	#										
11 – Chránit kritickou informační infrastrukturu, OES a DSP	4	-		Disponujete metodologií k určování poskytovatelů digitálních služeb?	1	Máte národní registr identifikovaných poskytovatelů digitálních služeb?	1	Disponujete dalšími mechanismy k hodnocení, zda jsou technická a organizační opatření, jež provádí poskytovatelé digitálních služeb, vhodná k řízení rizik pro bezpečnost sítí a informačních systémů? Např. pravidelné audity kybernetické bezpečnosti, vnitrostátní rámec pro provádění bezpečnostních opatření, technické nástroje poskytnuté vládou, jakými jsou detekční sondy nebo přezkumy konfigurací konkrétních systémů...	1	-	
	5	-		Máte jeden či více vnitrostátních orgánů dohlížejících na ochranu kritické informační infrastruktury a bezpečnost sítí a informačních systémů? Např. podle požadavků směrnice NIS (2016/1148).	1	Máte národní registr identifikovaných nebo známých rizik?	1	Přezkoumáváte a následně aktualizujete seznam identifikovaných poskytovatelů digitálních služeb alespoň každé dva roky?	1	-	
	6	-		Vypracováváte plány ochrany konkrétních odvětví? Např. zahrnutím základních opatření v oblasti kybernetické bezpečnosti (povinné nebo směrnice).	0	Disponujete metodologií ke zjištění závislostí KII?	1	Používáte režim certifikace bezpečnosti (vnitrostátní či mezinárodní), který pomáhá OES a poskytovatelům digitálních služeb s určováním bezpečných produktů IKT? Např. SOG-IS MRA v Evropě, vnitrostátní iniciativy...	1	-	
	7	-		-		Využíváte k určování, kvantifikaci a řízení rizik souvisejících s KII na vnitrostátní úrovni postupy řízení rizik?	1	Používáte k posouzení poskytovatelů služby spolupracujících s OES režim certifikace bezpečnosti nebo kvalifikační postup? Např. poskytovatelé služeb v oblasti odhalování incidentů, reakce na ně, auditů kybernetické bezpečnosti, cloudových služeb, chytrých karet...	1	-	
	8	-		-		Zapojujete se do procesu konzultací pro určování přeshraničních závislostí?	1	Disponujete mechanismy k měření úrovně dodržování základních opatření kybernetické bezpečnosti u OES a poskytovatelů digitálních služeb?	0	-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
11 – Chránit kritickou informační infrastrukturu, OES a DSP	9					Máte jednotné kontaktní místo odpovědné za koordinaci záležitostí týkajících se bezpečnosti sítí a informačních systémů na vnitrostátní úrovni a v rámci přeshraniční spolupráce na úrovni Unie?	1	Disponujete prostředky pro zajištění kontinuity služeb poskytovaných kritickými informačními infrastrukturami? Např. předjímání krizí, postupy obnovy kritických informačních systémů, obchodní kontinuitou bez IT, postupy zálohování odděleně od sítí…	0		
	10					Definujete základní bezpečnostní opatření (povinná nebo směrnice) pro poskytovatele digitálních služeb a všechna odvětví uvedená v příloze II směrnice NIS (2016/1148)?	1				
	11	-		-		Poskytujete nástroje nebo metodologie pro odhalování kybernetických incidentů?	1	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
12 – Bojovat proti kyberkriminalitě	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Vypracovali jste studii pro určování požadavků v oblasti prosazování práva (právní základ, prostředky, dovednosti…) pro účinný boj proti kybernetické kriminalitě?	1	Odpovídá váš vnitrostátní právní rámec beze zbytku příslušnému právnímu rámci EU, včetně směrnice 2013/40/EU o útocích na informační systémy? Např. neoprávněný přístup k informačním systémům, neoprávněné zasahování do informačních systémů, neoprávněné zasahování do údajů, neoprávněné sledování, nástroje použité k páchání trestných činů...	1	Existují v rámci vašich státních zastupitelství jednotky specializující se na kybernetickou kriminalitu?	1	Shromažďujete statistiky podle ustanovení čl. 14 odst. 1 směrnice 2013/40/EU (směrnice o útocích na informační systémy)?	1	Disponujete na vnitrostátní a/nebo vícestranné úrovni interinstitucionálními školeními nebo školicími semináři pro LEA, soudce, státní zástupce a vnitrostátní/vládní týmy CSIRT?	1
	2	Vypracovali jste studii pro určení požadavků státních zástupců a soudců (právní základ, prostředky, dovednosti…) pro účinný boj proti kybernetické kriminalitě?	1	Máte nějaké právní předpisy zabývající se krádežemi on-line totožnosti a osobních údajů?	1	Mají jednotky bojující proti kybernetické kriminalitě vlastní rozpočtové prostředky?	1	Shromažďujete samostatné statistiky kybernetické kriminality? Např. operační statistiky, statistiky trendů kybernetické kriminality, statistiky spáchaných kybernetických zločinů a vzniklých škod…	1	Účastníte se koordinovaných mezinárodních akcí zaměřených na narušení kriminálních činností? Např. infiltrace kriminálních hackerských fór, organizovaných skupin zabývajících se kybernetickou kriminalitou, uzavírání tržišť na darknetu botnetů…	1
	3	Podepsala vaše země budapešťskou Úmluvu Rady Evropy o počítačové kriminalitě?	1	Máte nějaké právní předpisy zabývající se porušováním práv duševního vlastnictví a autorského práva on-line?	1	Vytvořili jste centrální orgán/subjekt na koordinaci činnosti v oblasti boje proti kybernetické kriminalitě?	1	Vyhodnocujete vhodnost školení poskytovaných personálu LEA, soudnictví a vnitrostátních týmů CSIRT pro boj proti kybernetické kriminalitě?	1	Existuje jasné oddělení povinností mezi týmy CSIRT, LEA a soudnictví (státní zástupce a soudce), když spolupracují na boji proti kybernetické kriminalitě?	1

	4			Máte nějaké právní předpisy zabývající se obtěžováním on-line nebo kyberšikanou?	1	Vytvořili jste mechanismy spolupráce mezi příslušnými vnitrostátními institucemi zapojenými do boje proti kybernetické kriminalitě, včetně vnitrostátních týmů CSIRT pro prosazování práva?	1	Provádíte pravidelná hodnocení, abyste si zajistili dostatečné zdroje (lidské, rozpočtové a nástroje) pro jednotky bojující proti kybernetické kriminalitě v rámci LEA?	1	Usnadňuje váš rámec právních předpisů spolupráci mezi týmy CSIRT/LE a soudnictvím (státními zástupci a soudy)?	1
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
12 – Bojovat proti kybernetické kriminalitě	5			Disponujete nějakými právními předpisy pro řešení počítačových podvodů? Např. shoda s ustanoveními budapešťské Úmluvy Rady Evropy o počítačové kriminalitě.	1	Spolupracujete a sdílíte informace s dalšími členskými státy, které se týkají boje proti kybernetické kriminalitě?	1	Provádíte pravidelná hodnocení, abyste si zajistili dostatečné zdroje (lidské, rozpočtové a nástroje) pro jednotky bojující proti kybernetické kriminalitě v rámci orgánů pověřených stíháním?	1	Podílíte se na budování a udržování standardizovaných nástrojů a metodologií, forem a postupů, jež mají být sdíleny mezi zúčastněnými stranami v EU (LEA, týmy CSIRT, ENISA, EC3 Europolu…)?	1
	6	-		Disponujete nějakými právními předpisy pro ochranu dětí on-line? Např. shoda s ustanoveními směrnice 2011/93/EU a budapešťské Úmluvy Rady Evropy o počítačové kriminalitě...	1	Spolupracujete a sdílíte informace s agenturami EU (např. EC3 Europolu, Eurojust, agentura ENISA), které se týkají boje proti kybernetické kriminalitě?	1	Máte specializované soudy nebo soudce zabývající se případy kybernetické kriminality?	1	Disponujete pokročilými mechanismy pro zastrašování osob před atraktivitou kybernetické kriminality nebo účastí na ní?	0
	7	-		Určili jste operační vnitrostátní kontaktní místa pro výměnu informací a odpovídání na naléhavé žádosti o informace z členských států týkající se trestných činů uvedených ve směrnici 2013/40/EU (směrnice o útocích na informační systémy)?	1	Disponujete vhodnými nástroji pro boj proti kybernetické kriminalitě? Např. taxonomií a klasifikací kybernetické kriminality, nástroji pro shromažďování elektronických důkazů, forenzními počítačovými nástroji, důvěryhodnými platformami pro sdílení...	1	Máte prostředky pro poskytování podpory a pomoci obětem kybernetické kriminality (běžní uživatelé, MSP, velké společnosti)?	1	Používá vaše země pro efektivní reakci na velké kybernetické incidenty vzorový plán EU a/nebo protokol pro koordinovanou reakci při prosazování práva na naléhavé události (EU LE ERP)?	0
	8			Je součástí vaší agentury prosazování práva jednotka specializovaná na kybernetickou kriminalitu?	1	Disponujete standardními operačními postupy pro využívání elektronických důkazů?	1	Vytvořili jste institucionální rámec a mechanismy spolupráce mezi všemi relevantními zúčastněnými subjekty (např. LEA, vnitrostátní týmy CSIRT, soudní komunity) zahrnující soukromý sektor (např. provozovatele zásadních služeb, provozovatele služeb) tam, kde je to vhodné pro reakci na kybernetické útoky?	1	-	
	9			Vytvořili jste v souladu s článkem 35 Budapešťské úmluvy kontaktní místo s nepřetržitým provozem?	1	Podílí se vaše země na školicích příležitostech nabízených a/nebo podporovaných agenturami EU (např. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Usnadňuje váš rámec právních předpisů spolupráci mezi týmy CSIRT a LE?	1	-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
12 – Bojovat proti kyberkriminalitě	10	-		Vytvořili jste vnitrostátní kontaktní místo s nepřetržitým provozem pro protokol pro koordinovanou reakci při prosazování práva (EU LE ERP) zaměřené na reakce na velké kybernetické útoky?	1	Zvažuje vaše země přijetí druhého dodatkového protokolu budapešťské Úmluvy Rady Evropy o počítačové kriminalitě?	0	Máte mechanismy (např. nástroje, postupy) usnadňující výměnu informací a spolupráci mezi týmy CSIRT/LE a případně soudnictvím (státními zástupci a soudci) v oblasti boje proti kybernetické kriminalitě?	1	-	
	11			Poskytujete pravidelná specializovaná školení zúčastněným stranám podílejícím se na boji proti kybernetické kriminalitě (LEA, soudnictví, týmy CSIRT)? Např. školení o zaznamenávání/stíhání kybernetické kriminality, školení o shromažďování elektronických důkazů a zajišťování integrity mimo jiné v celém digitálním řetězci dohledu a počítačové forenzní vědy.	1						
	12			Ratifikovala vaše země budapešťskou Úmluvu Rady Evropy o počítačové kriminalitě nebo k ní přistoupila?	1			-	-	-	
	13	-		Podepsala a ratifikovala vaše země dodatkový protokol (kriminalizace činů rasistické a xenofobní povahy spáchané prostřednictvím počítačových systémů) budapešťské Úmluvy Rady Evropy o počítačové kriminalitě?	0	-	-	-		-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
13 – Vytvořit mechanismy hlášení incidentu	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Disponujete neformálními mechanismy sdílení informací o incidentech kybernetické bezpečnosti mezi soukromými organizacemi a vnitrostátními orgány?	1	Disponujete režimy hlášení pro všechny sektory uvedené v příloze II směrnice NIS?	1	Máte režim povinného hlášení incidentů, který funguje v praxi?	1	Využíváte harmonizovaný postup pro režimy hlášení incidentů v jednotlivých odvětvích?	1	Vypracováváte roční zprávy o incidentech?	1
	2	-		Provedli jste požadavky na oznamování pro poskytovatele telekomunikačních služeb v souladu s článkem 40 směrnice (EU 2018/1972)? Tato směrnice stanoví, že členské státy zajistí, aby poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací bez zbytečného prodlení oznamovali příslušnému orgánu bezpečnostní incidenty s významným dopadem na provoz sítí či služeb.	1	Existuje mechanismus koordinace/spolupráce pro povinné hlášení incidentů podle GDPR, směrnice NIS, článku 40 (bývalého článku 13a) a nařízení eIDAS?	1	Disponujete režimy hlášení pro jiné sektory než uvedené ve směrnici NIS?	1	Máte nějaké zprávy o oblasti kybernetické bezpečnosti nebo jiné druhy analýzy vypracované subjektem, který dostává hlášení o incidentech?	1

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
13 – Vytvořit mechanismy hlášení incidentu	3	-		Provedli jste požadavky na oznamování pro poskytovatele důvěryhodných služeb v souladu s článkem 19 nařízení eIDAS (nařízení (EU) č. 910/2014)? Článek 19 mimo jiné stanoví, že poskytovatelé důvěryhodných služeb oznamují orgánu dohledu významné bezpečnostní incidenty/narušení.	1	Disponujete vhodnými nástroji pro zajištění důvěrnosti a integrity informací sdílených různými kanály hlášení?	1	Hodnotíte účinnost postupů hlášení incidentů? Např. ukazatele pro incidenty, které byly nahlášeny příslušnými kanály, čas nahlášení incidentu...	1	-	
	4	-		Provedli jste požadavky na oznamování pro poskytovatele digitálních služeb v souladu s článkem 16 směrnice NIS? Článek 16 stanoví, že poskytovatelé digitálních služeb bez zbytečného prodlení hlásí příslušnému orgánu nebo vnitrostátnímu týmu CSIRT incidenty, které mají významný dopad na poskytování služby uvedené v příloze III, kterou nabízejí v rámci Unie.	1	Disponujete platformou/nástrojem usnadňujícími postup hlášení?	0	Máte společnou vnitrostátní taxonomii týkající se klasifikace incidentů a kategorií prvotních příčin?	0	-	

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
14 – Zesílit informační soukromí a ochranu údajů	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Vypracovali jste studie či analýzy určující oblasti zlepšení pro lepší ochranu práv občanů na soukromí?	1	Je vnitrostátní úřad pro ochranu osobních údajů zapojen do problematiky kybernetické bezpečnosti (např. návrhy nových zákonů a předpisů o kybernetické bezpečnosti, definovaná minimální bezpečnostní opatření)?	1	Podporujete osvědčené postupy pro bezpečnostní opatření a ochranu dat od počátku ve veřejném a/nebo soukromém sektoru?	1	Provádíte pravidelná hodnocení, abyste si zajistili dostatečné zdroje (lidské, rozpočtové a nástroje) pro úřad ochrany osobních údajů?	1	Disponujete mechanismy pro sledování nejnovějšího technologického vývoje, abyste mu přizpůsobili příslušné směrnice a ustanovení/povinnosti právních předpisů?	1
	2	Vypracovali jste právní základ na vnitrostátní úrovni pro prosazování obecného nařízení o ochraně osobních údajů (nařízení EU 2016/679)? Např. zachování či zavedení konkrétnějších ustanovení nebo omezení pro pravidla nařízení.	0	-		Spouštíte programy na zvyšování povědomí a školicí programy týkající se tohoto tématu?	1	Vybízíte organizace a podniky, aby se nechaly certifikovat podle ISO/IEC 27701:2019 o systémech správy osobních údajů (PIMS)?	1	Aktivně se podílíte na iniciativách VaV týkajících se technologií zlepšujících ochranu soukromí (PET) a podporujete je?	0
	3	-		-		Koordinujete postupy podávání zpráv v rámci DPA?	1	-		-	
	4	-		-		Propagujete nebo podporujete vypracování technických norem pro informační bezpečnost a ochranu soukromí? Jsou některé z nich navrženy přímo pro malé a střední podniky (MSP)?	0	-		-	
	5	-		-		Poskytujete praktické a upravitelné pokyny na podporu různých druhů správců údajů při plnění požadavků a povinností v oblasti ochrany soukromí a osobních údajů?	0	-		-	

4.1.4 Klastr č. 4: Spolupráce

Cíl NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
15 – Vytvořit partnerství veřejného a soukromého sektoru (PPP)	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Panuje obecná shoda, že PPP přispívají různými prostředky ke zvýšení úrovně kybernetické bezpečnosti v zemi? Např. společným zájmem na zlepšování kybernetické bezpečnosti v průmyslu, spoluprací při budování příslušného regulačního rámce kybernetické bezpečnosti, podporou VaV...	1	Máte vnitrostátní akční plán pro vytváření PPP?	1	Vytváříte partnerství veřejného a soukromého sektoru?	1	Vytváříte PPP mezi odvětvími?	1	Jste na základě nejnovějšího technologického vývoje a vývoje norem schopni přizpůsobovat nebo vytvářet PPP?	1
	2	-		Stanovíte právní nebo smluvní základ (konkrétní zákony, NDA, duševní vlastnictví) pro oblast působnosti PPP?	1	Vytváříte specifická odvětvová PPP?	1	Zaměřujete se ve vytvořených PPP rovněž na spolupráci veřejných subjektů s veřejnými subjekty a soukromých se soukromými?	1		
	3	-		–		Poskytujete finanční prostředky pro vytváření PPP?	1	Podporujete PPP mezi malými a středními podniky (MSP)?	1	-	
	4	-		–		Řídí veřejné instituce PPP celkově? Tj. jednotné kontaktní místo veřejného sektoru řídící a koordinující PPP, veřejné orgány předem souhlasí s tím, čeho chtějí dosáhnout, jasné pokyny ze strany veřejné správy týkající se jejich potřeb a omezení soukromého sektoru…	1	Hodnotíte výsledky PPP?	1	-	

	5	-		–		Jste členem smluvního partnerství veřejného a soukromého sektoru (cPPP) Evropské organizace pro kybernetickou bezpečnost (ECSO)?	0	-		-	
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
15 – Vytvořit partnerství veřejného a soukromého sektoru (PPP)	6	-		-		Podílí se u vás jedno či více PPP na činnostech týmu CSIRT?	0	-		-	
	7					Podílí se u vás jedno či více PPP na ochraně kritické informační infrastruktury?	0				
	8	-		-		Podílí se u vás jedno či více PPP na zvyšování povědomí o kybernetické bezpečnosti a rozvoji dovedností?	0	-		-	

Cíl NCSS	**Č.**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
16 – Institucionalizovat spolupráci mezi veřejnými agenturami	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		
	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						

	1	Existují u vás neformální komunikační kanály mezi veřejnými agenturami?	1	Disponujete vnitrostátním režimem spolupráce zaměřeným na kybernetickou bezpečnost? Např. poradní orgány, řídicí skupiny, fóra, rady, kybernetická centra nebo odborné skupiny.	1	Účastní se tohoto režimu spolupráce veřejné orgány?	1	Zajišťujete, že existují kanály spolupráce v oblasti kybernetické bezpečnosti alespoň mezi těmito veřejnými orgány: zpravodajské služby, tuzemské donucovací orgány, orgány pověřené stíháním, státní aktéři, vnitrostátní týmy CSIRT a armáda?	1	Dostávají veřejné agentury jednotné minimální informace o nejnovějším vývoji, pokud jde o formy hrozeb, a povědomí o situaci v oblasti kybernetické bezpečnosti?	1
	2	-		-		Vytváříte platformy spolupráce zaměřené na výměnu informací?	1	Hodnotíte úspěchy a limity různých režimů spolupráce při podpoře účinné spolupráce?	1	-	
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
16 – Institucionalizovat spolupráci mezi veřejnými agenturami	3	-		-		Stanovili jste oblast působnosti platforem spolupráce (např. úkoly a odpovědnosti, počet tematických oblastí)?	1	-		-	
	4	-		-		Pořádáte každoroční setkání?	1	-		-	
	5	-		-		Disponujete mechanismy spolupráce mezi příslušnými orgány napříč geografickými regiony? Např. sítěmi bezpečnostních korespondentů v jednotlivých regionech, úředník pro kybernetickou bezpečnost v regionálních hospodářských komorách…	1	-		-	

Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
17 – Zapojit se do mezinárodní spolupráce (nejen s členskými státy EU)	a)	Zahrnuli jste tento cíl do své současné NCSS, nebo to plánujete v její příští verzi?	1	Existují neformální postupy nebo činnosti, které se podílí na nekoordinovaném dosahování cílů?	1	Máte formálně definovaný a zdokumentovaný akční plán?	1	Přezkoumáváte cíl svého akčního plánu, abyste otestovali jeho účinnost?	1	Disponujete mechanismem, který zajistí, že se bude akční plán dynamicky přizpůsobovat okolnímu vývoji?	1
	b)			Definovali jste ve svém akčním plánu zamýšlené výsledky, hlavní zásady nebo klíčové činnosti?	1	Máte akční plán s jasným rozdělením a řízením prostředků?	1	Přezkoumáváte cíl svého akčního plánu, abyste zajistili jeho správné priority a optimalizaci?	1		

	c)			Je případně možné váš akční plán provádět a uplatňovat v omezeném rozsahu?	0						
	1	Máte strategii pro mezinárodní spolupráci?	1	Uzavřeli jste smlouvy o spolupráci s jinými zeměmi (dvoustranné, vícestranné) nebo s partnery u jiných zemí? Např. sdílení informací, budování schopností, pomoc…	1	Vyměňujete si strategické informace? Např. politika na vysoké úrovni, vnímání rizik...	1	Zapojují se vnitrostátní agentury pro kybernetickou bezpečnost ve vaší zemi do mezinárodních režimů spolupráce?	1	Vedete diskuse o jednom či více tématech vícestranných dohod?	1
	2	Existují u vás neformální kanály pro spolupráci s jinými zeměmi?	1	Máte jednotné kontaktní místo, které dokáže být prostředníkem pro zajištění přeshraniční spolupráce s orgány členského státu (skupina pro spolupráci, síť CSIRT…)?	1	Vyměňujete si taktické informace? Např. věstník o původcích hrozeb, ISAC, TTP…	1	Posuzujete pravidelně výsledky iniciativ v oblasti mezinárodní spolupráce?	1	Vedete diskuse o jednom či více tématech mezinárodních smluv či úmluv?	1
Cíl NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
17 – Zapojit se do mezinárodní spolupráce (nejen s členskými státy EU)	3	Vyjádřilo veřejné vedení svůj záměr zapojit se do mezinárodní spolupráce v oblasti kybernetické bezpečnosti?	1	Zapojují se vaši odborníci do mezinárodní spolupráce?	1	Vyměňujete si informace na operační úrovni? Např. informace o koordinaci operací, pokračující incidenty, IOC…	1	-		Diskutujete nebo jednáte o jednom či více tématech v rámci mezinárodních expertních skupin? Např. Globální komise pro stabilitu v kyberprostoru, skupina pro spolupráci ENISA NIS, skupina vládních expertů OSN pro bezpečnost informací...	1
	4	-		-		Zapojujete se do mezinárodních cvičení kybernetické bezpečnosti?	1	-		-	
	5	-		-		Zapojujete se do mezinárodních iniciativ na budování schopností? Např. školení, rozvoj dovedností, postupy navrhování norem…	0	-		-	
	6	-		-		Uzavřeli jste smlouvy o vzájemné pomoci s jinými zeměmi? Např. činnosti LEA, soudní řízení, schopnosti vzájemné reakce na incidenty, sdílení prostředků v oblasti kybernetické bezpečnosti…	0	-		-	

	7	-		-		Podepsali jste nebo ratifikovali mezinárodní smlouvy či úmluvy v oblasti kybernetické bezpečnosti? Např. Mezinárodní kodex chování v oblasti kybernetické bezpečnosti, Úmluvu o počítačové kriminalitě.	0	-		-	

4.2 POKYNY K POUŽITÍ RÁMCE

Tato část se zaměřuje na poskytnutí některých pokynů a doporučení členským státům týkajících se zavedení rámce a vyplnění dotazníku. Níže uvedená doporučení vychází zejména ze zpětné vazby shromážděné při rozhovorech se zástupci členských států:

- **Předjímat koordinační činnosti pro shromažďování a konsolidaci dat.** Většina členských států uznává, že provádění vlastních posouzení by mělo zabrat přibližně patnáct člověkodnů. Pro provedení vlastního posouzení musel být vyžádán velký počet zúčastněných stran. Proto bylo doporučeno vyhradit čas na přípravnou fázi, aby se určili všichni účastníci ze správních orgánů, veřejných agentur a soukromého sektoru.
- **Určit centrální orgán odpovědný za provedení vlastního posouzení na vnitrostátní úrovni.** Protože může být ke shromáždění materiálu pro všechny ukazatele vnitrostátního rámce pro posouzení schopností nutné oslovit mnoho zúčastněných stran, doporučuje se určit centrální orgán nebo agenturu pověřené provedením vlastního posouzení, které bude kontaktovat a koordinovat všechny příslušné zúčastněné strany.
- **Využít provedení posouzení ke sdílení a sdělování témat v oblasti kybernetické bezpečnosti.** Poučení sdílená členskými státy ukázala, že diskuse (buď jako individuální rozhovory, nebo jako společná pracovní setkání) představují dobrou příležitost pro podporu dialogu o tématech kybernetické bezpečnosti a sdílení společných stanovisek a oblastí zlepšení. Kromě objasnění hlavních úspěchů může k podpoře témat kybernetické bezpečnosti přispět i sdílení výsledků.
- **Využít NCSS jako rámce pro výběr cílů posouzení.** Sedmnáct cílů, které tvoří vnitrostátní rámec pro posouzení schopností, bylo stanoveno na základě cílů, jež jsou běžně zahrnuty v NCSS členských států. Tyto cíle zahrnuté do NCSS by měly být použity pro stanovení oblasti působnosti posouzení. Nicméně NCSS by neměly posouzení omezovat. Protože se NCSS přirozeně zaměřují na priority, jsou v nich některé oblasti účelově opominuty. To ovšem neznamená, že dotčená schopnost neexistuje. Bude-li například v NCSS opominut konkrétní cíl, ovšem země v souvislosti s ním disponuje schopnostmi v oblasti kybernetické bezpečnosti, může být tento cíl posouzen.
- **Když se rozsah NCSS bude vyvíjet, zajistěte, že výklad výsledků bude soudržný s vývojem NCSS.** Životní cyklus NCSS je záležitost několika let. Některé NCSS členských států jsou obvykle prosazovány pomocí tří- až pětiletého plánu se změnami oblasti působnosti mezi dvěma po sobě následujícími verzemi NCSS. Proto musí být zvláštní pozornost věnována prezentaci výsledků vlastního posouzení u dvou verzí NCSS: změny oblasti působnosti mohou ovlivnit závěrečné skóre vyspělosti. Doporučujeme porovnat výsledky úplné oblasti působnosti u strategických cílů mezi jednotlivými roky (tj. celkové obecné skóre).

Připomínka k mechanismu hodnocení – příklad na míře splnění

Mechanismus hodnocení se skládá ze dvou úrovní skóre:
i) **celková obecná míra splnění** na základě úplného seznamu strategických cílů uvedených v rámci pro vlastní posouzení a
ii) **celková konkrétní míra splnění** vycházející ze strategických cílů vybraných členským státem (obvykle odpovídá cílům uvedeným v NCSS konkrétní země).

Podle svého návrhu (viz část 3.1 o mechanismu hodnocení) se celková konkrétní míra splnění rovná celkové obecné míře splnění nebo je vyšší, protože ta může obsahovat cíle nezahrnuté členským státem, což celkovou obecnou míru splnění snižuje. Když členský stát přidá nový cíl, celková míra splnění se zvýší (tj. je pokryto více ukazatelů vyspělosti), naopak se může snížit celková konkrétní vyspělost (bude-li se nově přidaný cíl nacházet v počáteční fázi, takže bude mít nízkou úroveň vyspělosti).

- **Při vyplňování dotazníku vlastního posouzení nezapomínejte na to, že primárním cílem je pomoci členskému státu s budování schopností v oblasti kybernetické bezpečnosti.** Proto doporučujeme, abyste při vyplňování dotazníku, i když může být někdy obtížné jasně odpovědět na některé otázky, vybírali odpovědi, které jsou nejvíce obecně akceptované. Bude-li například odpověď na otázku znít pro určitou oblast působnosti ANO a pro jinou NE, měl by členský stát myslet na to, že odpověď NE vyžaduje akci: buď plán nápravy, nebo plán práce na zlepšení, jež musí být zohledněny pro budoucí vývoj.

5. DALŠÍ KROKY

5.1 BUDOUCÍ ZLEPŠENÍ

Při rozhovorech se zástupci členských států a během fáze analýzy podkladů byla jako potenciální budoucí vývoj stanovena následující doporučení pro zlepšení vnitrostátního rámce pro posouzení schopností:

- **Vypracovat systém hodnocení, který umožní vyšší přesnost.** Například je možné namísto binární odpovědi ANO/NE zavést procento splnění, které bude lépe odrážet složitost konsolidování schopností na vnitrostátní úrovni. Jako první krok byl zvolen jednoduchý přístup s odpověďmi ANO/NE.
- **Zavést kvantitativní metriku pro měření účinnosti NCSS členských států.** Vnitrostátní rámec pro posouzení schopností se zaměřuje na hodnocení úrovně vyspělosti schopností členských států v oblasti kybernetické bezpečnosti. To by mohla doplňovat metrika pro měření účinnosti činností a akčních plánů provedených členskými státy pro budování těchto schopností. Zavedení této metriky v současné fázi se nejeví jako realistické, protože: neexistuje dostatečná zpětná vazba z praxe, je obtížné nalézt smysluplné ukazatele spojující výsledek s prováděním NCSS a stanovit realistické ukazatele, které lze následně shromažďovat. To ovšem zůstává předmětem budoucí práce.
- **Posun od provádění vlastního posouzení k přístupu posouzení.** Potenciálním budoucím vývojem tohoto rámce může být posun k přístupu posouzení, který posoudí vyspělost schopností členských států v oblasti kybernetické bezpečnosti soudržněji. Bude-li posouzení provádět třetí strana, může to skutečně umožnit minimalizovat možné vychýlení.

PŘÍLOHA A – PŘEHLED VÝSLEDKŮ ANALÝZY PODKLADŮ

Příloha A uvádí přehled předchozí práce agentury ENISA ohledně NCSS a přezkum příslušných veřejně dostupných modelů vyspělosti schopností v oblasti kybernetické bezpečnosti. Při výběru a přezkumu modelů jsou zohledňovány následující předpoklady:

- Ne všechny modely vychází z přísné výzkumné metodiky.
- Struktura a výsledky modelů nejsou vždy vysvětleny důkladně a s jasnými vazbami mezi jednotlivými prvky charakterizujícími modely.
- Některé modely neuvádí podrobnosti o vývoji, struktuře a metodologii posuzování.
- Další modely a nástroje, které jsme našli, nenabízí žádné podrobnosti o struktuře a obsahu, a proto nejsou uvedeny.
- Výběr přezkoumávaných modelů je založen na zeměpisném pokrytí. Zaměřovali jsme se především na modely vyspělosti schopností v oblasti kybernetické bezpečnosti s cílem posoudit výsledky evropských zemí. Je ovšem důležité rozšířit zeměpisné pokrytí na analyzování osvědčených postupů při budování modelů vyspělosti po celém světě.

Tento systematický přezkum příslušných veřejně dostupných modelů vyspělosti schopností v oblasti kybernetické bezpečnosti byl proveden s využitím přizpůsobeného analytického rámce založeného na metodice stanovené Beckerem pro vývoj modelů vyspělosti[22]. U každého ze stávajících modelů vyspělosti byly analyzovány tyto prvky:

- **Název modelu vyspělosti:** název modelu vyspělosti a hlavní odkazy.
- **Zdrojová instituce:** veřejná nebo soukromá instituce odpovídající za navržení modelu.
- **Obecný účel a cíl:** celková oblast působnosti modelu a zamýšlených cílů.
- **Počet a definice úrovní:** počet úrovní vyspělosti modelu, jakož i jejich obecný popis.
- **Počet a názvy atributů:** počet a názvy atributů využívaných modelem vyspělosti. Analýza atributů má trojí cíl:
  - Shrnutí modelu vyspělosti do snadno pochopitelných částí.
  - Klastr několika atributů do celků plnících stejný cíl.
  - Nabídnout různá stanoviska k předmětu úrovně vyspělosti.
- **Metoda posouzení:** metoda posouzení modelu vyspělosti.
- **Představení výsledků:** stanovení metody vizualizace výsledků modelu vyspělosti. Principem tohoto kroku je, že modely vyspělosti selhávají, jsou-li příliš složité, a proto musí způsob představení odpovídat praktickým potřebám.

[22] J. Becker, R. Knackstedt a J. Pöppelbuß, „Developing Maturity Models for IT Management: A Procedure Model and its Application“, Business & Information Systems Engineering, sv. 1, č. 3, s. 213–222, červen 2009.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Předchozí práce týkající se NCSS

Agentura ENISA v rámci této rané práce zveřejnila v roce 2012 dva dokumenty týkající se tohoto tématu. Za prvé průvodce „Practical guide on the development and execution phase of NCSS“[23] navrhoval soubor konkrétních opatření pro účinné provedení NCSS a představil životní cyklus NCSS ve čtyřech fázích: příprava strategie, realizace strategie, hodnocení strategie a udržení strategie. Za druhé dokument s názvem „Setting the course for national efforts to strengthen security in cyberspace“[24] načrtl stav strategií kybernetické bezpečnosti v EU a po roce 2012 a navrhl, aby členské státy určily společná témata a rozdíly svých NCSS.

V roce 2014 byl zveřejněn první rámec agentury ENISA pro posouzení NCSS[25]. Tento rámec obsahuje doporučení a osvědčené postupy, jakož i soubor nástrojů pro budování schopností při hodnocení NCSS (např. určené cíle, vstupy, výstupy, klíčové ukazatele výkonnosti…). Tyto nástroje jsou přizpůsobeny měnícím se potřebám zemí s různými úrovněmi vyspělosti svého strategického plánování. Ve stejném roce agentura ENISA zveřejnila interaktivní mapu „Online NCSS Interactive Map“[26], která uživatelům umožňuje rychlý náhled NCSS všech členských států a zemí ESVO, včetně jejich strategických cílů a osvědčených příkladů provádění. Původně byla vyhotovena jako soupis NCSS (2014), pak byla v roce 2018 rozšířena o příklady uplatňování a od roku 2019 nyní mapa slouží jako *informační centrum* pro centralizaci údajů poskytovaných členskými státy o jejich úsilí o zvýšení národní kybernetické bezpečnosti.

Průvodce „NCSS Good Practice Guide“ z roku 2016[27] určuje patnáct strategických cílů. Tento průvodce rovněž analyzuje stav provádění NCSS jednotlivých členských států a určuje různé nedostatky a problémy s tímto prováděním.

Agentura ENISA následně v roce 2018 vydala „National Cybersecurity Strategies Evaluation Tool“[28]: interaktivní nástroj pro vlastní posouzení, jenž členským státům pomáhá vyhodnotit jejich vlastní strategické priority a cíle související s jejich NCSS. Tento nástroj pomocí souboru jednoduchých otázek poskytuje členským státům konkrétní doporučení pro zlepšení provádění jednotlivých cílů. A nakonec, dokument „Good practices in innovation on Cybersecurity under the NCSS“[29], vydaný roku 2019, představuje téma inovace kybernetické bezpečnosti v rámci NCSS. Tento dokument podle názorů odborníků na toto téma stanoví problémy a osvědčené postupy v různých dimenzích inovace, aby se usnadnilo navrhování budoucích inovativních strategických cílů.

A.1 Model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy (CMM)

Model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy (CMM) vypracovalo Centrum pro globální schopnosti v oblasti kybernetické bezpečnosti (dále jen „Centrum pro schopnosti“), součást školy Oxford Martin School na Oxfordské univerzitě. Cílem Centra pro schopnosti je budování schopností v oblasti kybernetické bezpečnosti ve Spojeném království i v zahraničí prostřednictvím uplatňování modelu vyspělosti schopností v oblasti kybernetické

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012) https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012) https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.
[25] An evaluation framework for NCSS (ENISA, 2014) https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.
[26] National Cybersecurity Strategies – Interactive Map (ENISA, 2014, aktualizováno v roce 2019) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[27] Tento dokument aktualizuje průvodce z roku 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[28] National Cybersecurity Strategies Evaluation Tool (2018) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

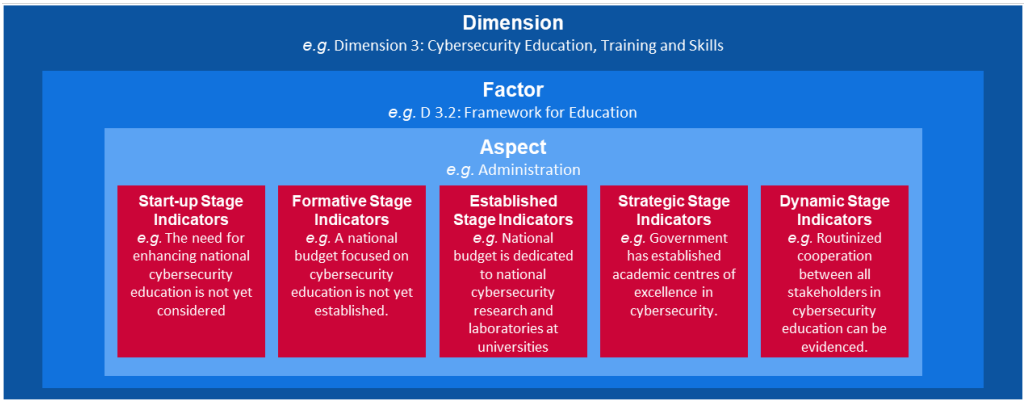
bezpečnosti (CMM). CMM se přímo zaměřuje na země, které si přejí zlepšit své schopnosti v oblasti kybernetické bezpečnosti. CMM byl poprvé použit v roce 2014 a následně v roce 2016 na základě svého použití přezkoumána jedenácti národními experty na kybernetickou bezpečnost.

Atributy/dimenze

CMM dělí schopnost v oblasti kybernetické bezpečnosti do **pěti dimenzí** představujících klastry schopností v oblasti kybernetické bezpečnosti. Každý klastr představuje různou výzkumnou „optiku“, jejímž prostřednictvím lze studovat a pochopit schopnosti v oblasti kybernetické bezpečnosti. V rámci těchto pěti dimenzí pak **faktory** popisují podrobnosti disponování schopnostmi v oblasti kybernetické bezpečnosti. Tyto podrobnosti jsou prvky, jež přispívají ke zlepšení vyspělosti schopností v oblasti kybernetické bezpečnosti v jednotlivých dimenzích. U jednotlivých faktorů představuje několik **aspektů** jeho různé prvky. Aspekty představují organizační metody dělení ukazatelů na menší, snadněji pochopitelnější klastry. Každý aspekt je pak hodnocen pomocí **ukazatelů** popisujících kroky, opatření nebo stavební bloky, které jsou v jednotlivých fázích vyspělosti indikativní (definici najdete v následující části) v rámci odlišných aspektů, faktorů a dimenzí.

Výše uvedené pojmy lze uspořádat jako na obrázku níže.

Obrázek 4: Příklad ukazatelů CMM



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimenze např. dimenze 3: Vzdělávání, školení a dovednosti v oblasti kybernetické bezpečnosti
Factor e.g. D 3.2: Framework for Education	Faktor např. D 3.2: Rámec pro vzdělávání
Aspect e.g. Administration	Aspekt např. správa
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Ukazatele počáteční fáze např. není dosud přihlédnuto ke zlepšenému vnitrostátnímu vzdělávání v oblasti kybernetické bezpečnosti
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Ukazatele fáze utváření např. dosud nebyl stanoven vnitrostátní rozpočet zaměřený na vzdělávání v oblasti kybernetické bezpečnosti
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Ukazatele fáze vytvořeno např. je vytvořen vnitrostátní rozpočet na univerzitní výzkum a laboratoře zabývající se kybernetickou bezpečností
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Ukazatele strategické fáze např. lze doložit, že vláda vytvořila akademické středisko excelence v oblasti kybernetické bezpečnosti.

Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Ukazatele dynamické fáze např. rutinní spolupráce mezi všemi zúčastněnými stranami.

O pěti dimenzích je podrobně pojednáno níže:

i vypracování politiky a strategie v oblasti kybernetické bezpečnosti (šest faktorů);
ii podpora odpovědné kultury v oblasti kybernetické bezpečnosti ve společnosti (pět faktorů);
iii rozvoj znalostí v oblasti kybernetické bezpečnosti (tři faktory);
iv vytvoření účinného právního a regulačního rámce (tři faktory) a
v řízení rizik pomocí norem, organizací a technologií (sedm faktorů).

Úrovně vyspělosti

CMM využívá pro stanovení, do jaké míry země pokročila ohledně určitých faktorů/aspektů schopností v oblasti kybernetické bezpečnosti, **pět úrovní vyspělosti**. Tyto úrovně slouží jako rychlý přehled stávajících schopností v oblasti kybernetické bezpečnosti:

- **Začátek:** v této fázi vyspělost v oblasti kybernetické bezpečnosti neexistuje nebo je velmi omezená. Mohou být vedeny první diskuse o budování schopností v oblasti kybernetické bezpečnosti, ale dosud nejsou přijata žádná konkrétní opatření. V této fázi chybí pozorovatelný důkaz.
- **Utváření:** některé charakteristiky aspektů se začínají vyvíjet a jsou formulovány, ovšem mohou být jednorázové, neorganizované, špatně definované – nebo jednoduše „nové“. Ovšem je možné jasně doložit důkazy této činnosti.
- **Vytvořeno:** prvky tohoto aspektu existují a fungují. Nevěnuje se však dostatečná pozornost relativnímu přidělování prostředků. Při rozhodování se nečiní příliš kompromisů ohledně „souvisejících“ investic do různých prvků aspektu. Tento aspekt je ale funkční a definovaný.
- **Strategická:** vybírá se, které části aspektů jsou důležité a které méně důležité pro konkrétní organizaci či stát. Strategická fáze odráží skutečnost, že jsou tato rozhodnutí prováděna podle konkrétní situace jednotlivých států či organizací.
- **Dynamická:** v této fázi jsou k dispozici jasné mechanismy změny strategie podle aktuálních okolností, jakými jsou technologie v oblasti hrozeb, globální konflikt nebo zásadní změna v jedné z dotčených oblastí (např. kyberkriminalita nebo soukromí). Dynamické organizace vyvíjí metody změny strategie za pochodu. Tato fáze je charakterizována rychlým rozhodováním, přerozdělováním prostředků a neustálou pozorností věnovanou měnícímu se prostředí.

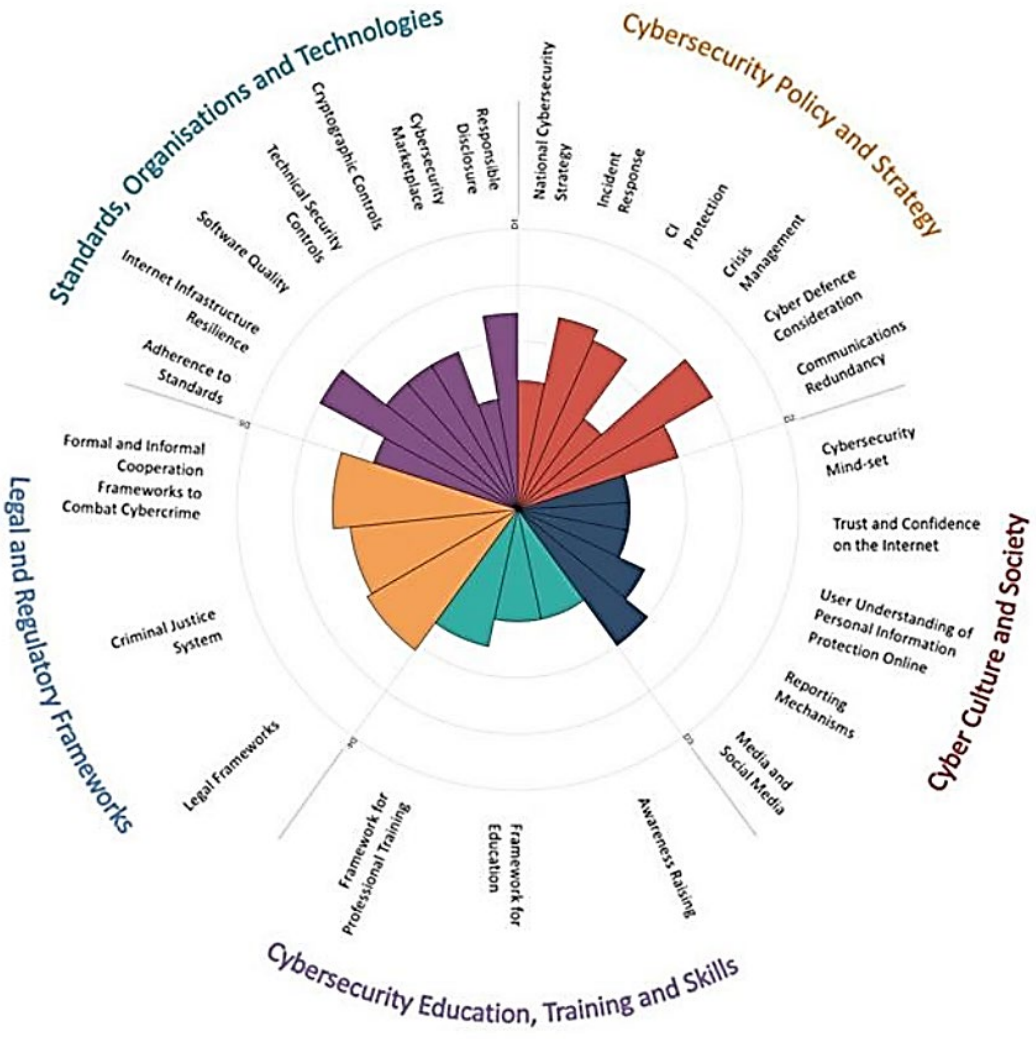
Metoda posouzení

Protože Centrum pro schopnosti dostatečně důkladně a podrobně nechápe jednotlivé tuzemské kontexty, v nichž se model používá, zajišťuje přezkum vyspělosti schopností v oblasti kybernetické bezpečnosti společně s mezinárodními organizacemi, hostitelskými ministerstvy nebo organizacemi dotčených zemí. Aby mohly Centrum pro schopnosti a hostitelská organizace posoudit úroveň vyspělosti pěti dimenzí CMM, musí se v průběhu dvou až tří dnů sejít s příslušnými zúčastněnými stranami veřejného a soukromého sektoru a zaměřit se na tyto dimenze CMM v rámci odborných skupin. Různé skupiny zúčastněných stran projednají každou dimenzi alespoň dvakrát. Tím se získá předběžný soubor dat pro následné posouzení.

Režim nebo představení výsledků

CCM poskytne prostřednictvím radaru skládajícího se z pěti částí, každé pro jednu dimenzi, přehled o úrovni vyspělosti jednotlivých zemí. Každá dimenze bude představovat jednu pětinu grafu s pěti fázemi vyspělosti pro jednotlivé faktory vycházejícími ze středu grafu; jak vidíte níže, „začátek“ se nachází nejblíže středu grafu a „dynamická fáze“ na kraji.

Obrázek 5 CMM: Přehled výsledků



Standards, Organisations and Technologies	Normy, organizace a technologie
Legal Regulatory Frameworks	Právní regulační rámce
Cybersecurity Education, Training and Skills	Vzdělávání, školení a dovednosti v oblasti kybernetické bezpečnosti
Cybersecurity Policy and Strategy	Politika a strategie v oblasti kybernetické bezpečnosti
Cyber Culture and Society	Kybernetická kultura a společnost
Responsible Disclosure	Odpovědné zveřejňování
Cybersecurity market place	Trh s kybernetickou bezpečností
Cryptographic Controls	Kryptografické kontrolní prostředky
Technical Security Controls	Technické bezpečnostní kontroly
Software Quality	Kvalita softwaru
Internet Infrastructure Resilience	Odolnost internetové infrastruktury
Adherence to Standards	Dodržování norem
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Rámce formální a neformální spolupráce boje proti kybernetické kriminalitě
Criminal Justice System	Systém trestního soudnictví
Legal Frameworks	Právní rámce
Framework for Professional Training	Rámec pro odbornou přípravu
Framework for Education	Rámec pro vzdělávání

Awareness Raising	Zvyšování povědomí
Media and Social Medai	Média a sociální sítě
Reporting Mechanisms	Mechanismy podávání zpráv
User Understanding of Personal Information Protection Online	Chápání on-line ochrany osobních údajů uživatelem
Trust and Confidence on the Internet	Důvěra v internet a jeho důvěryhodnost
Cybersecurity Mind-set	Přístup v oblasti kybernetické bezpečnosti
Communications Redundancy	Nadbytečnost komunikace
Cyber Defence Consideration	Zohlednění kybernetické ochrany
Crisis Management	Řešení krizí
CI Protection	Ochrana KI
Incident Response	Reakce na incidenty
National Cybersecurity Strategy	Národní strategie kybernetické bezpečnosti

Centrum pro globální schopnosti v oblasti kybernetické bezpečnosti , Oxford Martin School, Oxfordská univerzita, 2017.

A.2 Model vyspělosti schopností v oblasti kybernetické bezpečnosti (C2M2)

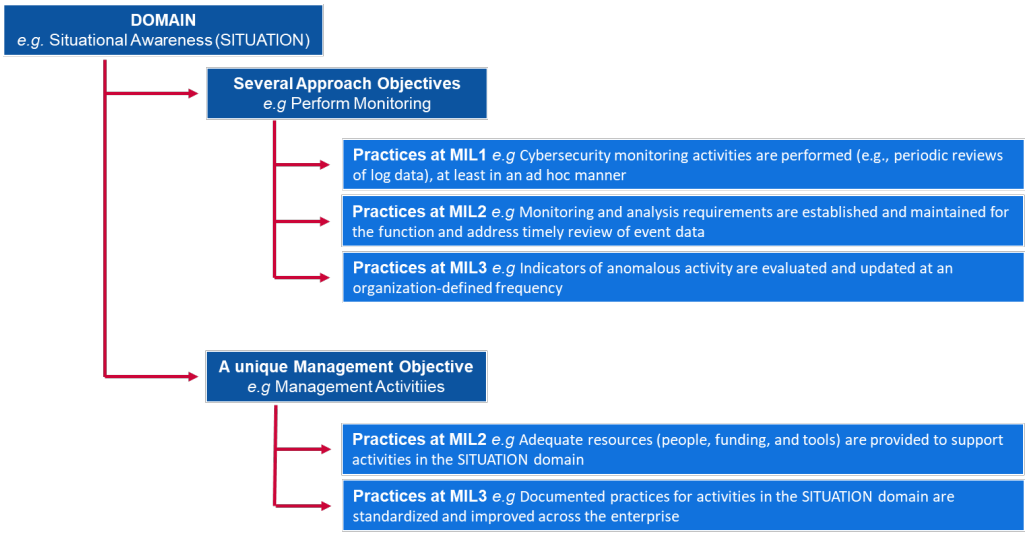
Model vyspělosti schopností v oblasti kybernetické bezpečnosti (C2M2) vypracovalo Ministerstvo energetiky USA ve spolupráci s odborníky ze soukromého i veřejného sektoru. Cílem Centra pro schopnosti je pomáhat organizacím ze všech odvětví, všech druhů a velikostí při hodnocení a zlepšování jejich programů kybernetické bezpečnosti a posilovat jejich provozní odolnost. C2M2 se zaměřuje na provádění a řízení kybernetických bezpečnostních postupů spojených s informacemi, informačními technologiemi (IT) a provozními technologiemi (OT) a prostředím, kde jsou využívány. C2M2 definuje modely vyspělosti jako: „soubor vlastností, atributů, ukazatelů nebo vzorců představujících schopnosti a pokrok v konkrétním oboru“. C2M2 byl poprvé použit v roce 2014, revidován pak v roce 2019.

Atributy/dimenze

C2M2 se zabývá **deseti oblastmi** představujícími logické seskupení postupů v oblasti kybernetické bezpečnosti. Každý soubor postupů představuje činnosti, které může organizace provádět za účelem vytvoření a vyspělosti schopností v dotčené oblasti. Každá oblast je následně spojena s **jedinečným cílem řízení** a **několika cíli přístupů**. V rámci cílů přístupu i řízení je podrobně definováno **několik postupů** popisujících institucionalizované činnosti.

Vztah mezi těmito pojmy je shrnut níže:

Obrázek 6: Příklad ukazatele C2M2



Domain eg Situational Awareness (SITUATION)	**Oblast** např. povědomí o situaci (SITUACE)
Several Approaches Objectives e.g. Perform Monitoring	**Několik cílů přístupu** např. provádění sledování
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Postupy MIL1** např. provádí se sledování kybernetických bezpečnostních činností (např. periodické přezkumy zaznamenaných dat), alespoň jednorázově
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Postupy MIL2** např. jsou vytvořeny a řízeny požadavky na sledování a analýzu funkčnosti a včasný přezkum dat o události
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Postupy MIL3** např. jsou s četností definovanou organizací vyhodnocovány a aktualizovány ukazatele anomální aktivity
A unique Management Objectve e.g. Management Activities	Jedinečný cíl řízení např. řídicí činnosti
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Postupy MIL2** např. jsou poskytnuty vhodné zdroje (lidé, finance a nástroje) na podporu činností v oblasti SITUACE
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Postupy MIL3** např. v podniku jsou standardizovány a vylepšovány zdokumentované postupy pro oblast SITUACE

O deseti oblastech je podrobně pojednáno níže:

i řízení rizik (RIZIKO);
ii řízení aktiv, změn a konfigurace (AKTIVA);
iii správa identit a přístupu (PŘÍSTUP)
iv řízení hrozeb a zranitelnosti (HROZBA);
v povědomí o situaci (SITUACE);
vi reakce na události a incidenty (REAKCE);
vii řízení dodavatelského řetězce a vnějších závislostí (ZÁVISLOSTI);
viii řízení pracovníků (PRACOVNÍCI);
ix architektura kybernetické bezpečnosti (ARCHITEKTURA) a
x řízení programu kybernetické bezpečnosti (PROGRAM).

Úrovně vyspělosti

C2M2 používá **čtyři** úrovně vyspělosti (pojmenované Úrovně ukazatelů vyspělosti – MIL) ke stanovení dvojího vývoje vyspělosti: pokrok v oblasti přístupu a pokrok v oblasti řízení. MIL mají rozsah od MIL0 do MIL3 a u každé oblasti se používají samostatně.

- **MIL0:** postupy se neprovádí.
- **MIL1:** provádí se počáteční postupy, ovšem mohou se provádět jen jednorázově.
- **MIL2:** charakteristiky řízení:
  - Postupy jsou dokumentovány.
  - Na podporu procesů jsou přiděleny vhodné zdroje.
  - Pracovníci provádějící postupy disponují vhodnými dovednostmi a znalostmi.
  - Jsou rozděleny odpovědnost a pravomoci k provádění postupů.

  Charakteristika přístupu:
  - Postupy jsou úplnější a pokročilejší než u MIL1.
- **MIL3:** charakteristiky řízení:

- Činnosti jsou řízeny politikami (nebo jinými organizačními směrnicemi).
- Výsledkové cíle pro činnosti oblasti se stanoví a jsou sledovány, aby byly zjevné výsledky.
- Zdokumentované postupy činností oblastí jsou v celém podniku standardizovány a zlepšovány.

Charakteristika přístupu:

- Postupy jsou úplnější a pokročilejší než u MIL2.

Metoda posouzení

C2M2 je určen k použití s **metodikou vlastního posouzení** a sadou nástrojů (dostupnou na požádání), jejichž pomocí organizace hodnotí a zlepšuje svůj program kybernetické bezpečnosti. Vlastní posouzení pomocí této sady nástrojů je možné dokončit za den, ovšem sadu nástrojů lze přizpůsobit i pro přísnější posouzení. Dále může být C2M2 použit jako průvodce vypracováním nového programu kybernetické bezpečnosti.

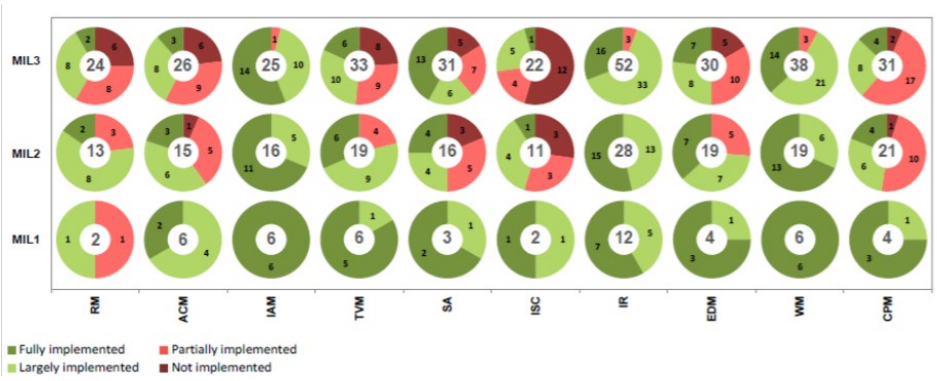
Obsah tohoto modelu může být prezentován s vysokou mírou abstrakce, takže jej mohou vykládat organizace různých druhů, s různou strukturou, velikostí a z různých odvětví. Široké použití tohoto modelu v odvětví může podpořit hodnocení schopností dotčeného odvětví v oblasti kybernetické bezpečnosti.

Režim nebo představení výsledků

C2M2 poskytuje hodnoticí zprávu vycházející z výsledků průzkumu. Tato zpráva uvádí výsledky ve dvou zobrazeních: jako zobrazení cílů, které ukazuje praktické odpovědi na otázky podle jednotlivých oblastí a jejich cílů, a zobrazení oblastí, jež uvádí odpovědi podle všech oblastí a MIL. Obě znázornění jsou založena na zástupném systému charakterizovaném koláčovými grafy, vždy po jednom na odpověď, a hodnoticím semaforem. Jak ukazuje Obrázek 7, červené oblasti koláčového grafu ukazují podíl otázek, na něž respondenti v průzkumu odpověděli „Neprovádí se“ (tmavě červená) nebo „Provádí se částečně“ (světle červená). Zelené oblasti ukazují počet otázek s odpověďmi „Provádí se ve velké míře“ (světle zelená) nebo „Provádí se zcela“ (tmavě zelená).

Obrázek 7 níže uvádí příklad výsledkové listiny na konci hodnocení vyspělosti. Na ose X se nachází deset oblastí C2M2 a na ose Y úrovně vyspělosti (MIL). Při pohledu na graf a oblasti Řízení rizik vidíte tři koláčové grafy, každý odpovídá jedné úrovni vyspělosti MIL1, ML2 a ML3. U oblasti RM graf ukazuje, že budou pro dosažení první úrovně vyspělosti, MIL1, hodnoceny dvě položky. V tomto případě jeden výsledek „Provádí se ve velké míře“ a jeden výsledek „Provádí se částečně“. Pro druhou úroveň vyspělosti, MIL2, model předpokládá posouzení třinácti položek. Dvě z těchto třinácti položek náleží první úrovni (MIL1) a jedenáct druhé úrovni (MIL2). To samé platí i pro třetí úroveň (MIL3).

Obrázek 7: C2M2 – Příklad znázornění oblastí



Fully implemented	Provádí se zcela
Largely implemented	Provádí se ve velké míře
Partially implemented	Provádí se částečně
Not implemented	Neprovádí se
MIL1	MIL1
MIL2	MIL2

MIL3	MIL3
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Zdroj: Ministerstvo energetiky USA, Odbor dodávek elektřiny a energetické spolehlivosti, 2015.

A.3 Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury

Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury vypracoval Národní ústav pro standardizaci a technologie (NIST). Zaměřuje se na vedení činností v oblasti kybernetické bezpečnosti a řízení rizik v rámci organizace. Uplatňuje se u všech typů organizací bez ohledu na velikost, stupeň kybernetického rizika nebo úrovně sofistikovanosti kybernetické bezpečnosti. Protože se jedná o rámec, a nikoli model, liší se jeho struktura od výše analyzovaných modelů.

Rámec se skládá ze tří částí: jádra rámce, úrovní provádějí a rámcových profilů:

- **Jádro rámce** tvoří soubor činností v oblasti kybernetické bezpečnosti, požadovaných výsledků a příslušných odkazů, jež jsou společné odvětvím kritické infrastruktury. Podobají se atributům nebo dimenzím u modelů vyspělosti schopností v oblasti kybernetické bezpečnosti.
- **Úrovně provádění rámce** (dále jen „úrovně“) poskytují kontext toho, jak organizace vnímá kybernetická bezpečnostní rizika, a jejích postupů pro řízení těchto rizik . Úrovně sahající od částečné (úroveň 1) po adaptivní (úroveň 4) popisují zvyšující se míru přísnosti a sofistikovanosti postupů řízení kybernetických bezpečnostních rizik. Úrovně nepředstavují úrovně vyspělosti, spíše mají podporovat rozhodování organizace ohledně způsobů řízení kybernetických bezpečnostních rizik a stanovení, které její dimenze mají vyšší prioritu a mohly by získat další zdroje.
- **Rámcový profil** (dále jen „profil“) představuje výsledky vycházející z potřeb podniků, jež organizace vybrala z rámcových kategorií a podkategorií. Profil lze charakterizovat s ohledem na sladění norem, pokynů a postupů podle jádra rámce v konkrétním scénáři provádění. Profily je možné používat k určování příležitostí ke zlepšení situace kybernetické bezpečnosti srovnáním „současného“ profilu („současného“ stavu) a „cílového“ profilu („budoucího“ stavu).

Jádro rámce

Jádro rámce tvoří pět **funkcí**. Jestliže se těmito funkcemi budeme zabývat najednou, poskytnou podrobný strategický náhled na životní cyklus řízení rizik v oblasti kybernetické bezpečnosti u organizace. Jádro rámce pak určuje základní hlavní **kategorie** a **podkategorie** jednotlivých funkcí a porovná je s příklady informativních odkazů, například stávajících norem, pokynů a postupů, u jednotlivých podkategorií.

Funkce a kategorie jsou podrobněji popsány níže:

i **Identifikovat:** organizace pochopí, jak řídit kybernetická bezpečnostní rizika u systémů, lidí, aktiv, dat a schopností.
   - Podkategorie: správa aktiv; obchodní prostředí; řízení; posouzení rizik a strategie řízení rizik

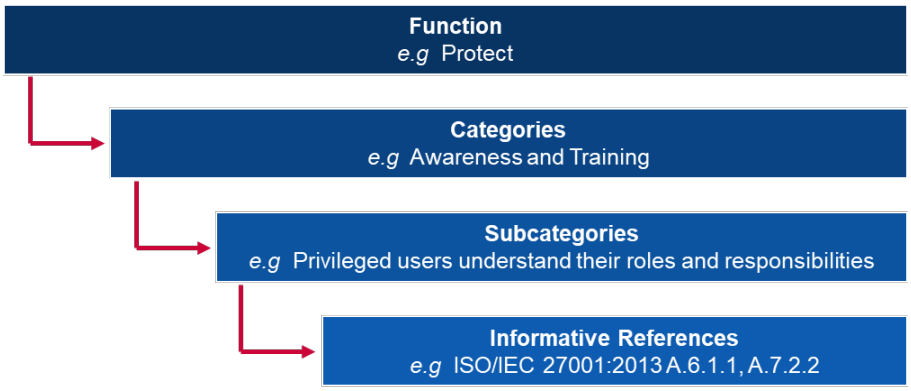
ii **Chránit:** vypracovat a provádět vhodné záruky k zajištění poskytování kritických služeb.
   - Podkategorie: správa identit a řízení přístupu; povědomí a školení; bezpečnost dat; procesy a postupy ochrany informací; údržba a ochranná technologie

iii **Odhalit:** vypracovat a provádět vhodné činnosti pro určování výskytu kybernetické bezpečnostní události.
- Podkategorie: anomálie a události; nepřetržité sledování bezpečnosti a procesy odhalování

iv **Reagovat:** vypracovat a provádět vhodné činnosti pro realizaci opatření u odhaleného kybernetického bezpečnostního incidentu.
- Podkategorie: plánování reakce; komunikace; analýza; zmírnění a zlepšení

v **Obnovit:** Vypracovat a provádět vhodné činnosti pro správu plánů na odolnost a obnovu všech schopností nebo služeb narušených kybernetickým bezpečnostním incidentem.
- Podkategorie: plánování obnovy; zlepšení a komunikace

Obrázek 8: Příklad rámce pro zlepšení kybernetické bezpečnosti kritické infrastruktury



Function e.g Project	**Funkce** např. projekt
Categories e.g Awarness and Training	**Kategorie** např. povědomí a školení
Subcategories e.g Privileged useres understand their roles and responsibilities	**Podkategorie** např. privilegovaní uživatelé chápou své úlohy a odpovědnosti
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informativní odkazy** např. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Úrovně

Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury je založen na **čtyřech úrovních**, z nichž každá je definována podle tří os: posuzování rizika, programu integrovaného řízení rizik a externí účasti. Tyto úrovně se nepovažují za úrovně vyspělosti, nýbrž za rámec poskytující organizaci kontext pro její vnímání kybernetických bezpečnostních rizik a procesů řízení těchto rizik.

- **Úroveň 1: Částečně**
  - **Posuzování rizika:** postupy řízení kybernetických rizik v organizaci nejsou formalizovány a rizika jsou řízena jednorázově a někdy reaktivně.
  - **Program integrovaného řízení rizik:** na úrovni organizace existuje omezené povědomí o kybernetických bezpečnostních rizicích. Organizace uplatňuje řízení kybernetických bezpečnostních rizik nepravidelně, případ od případu a nemusí disponovat postupy umožňujícími sdílení kybernetických bezpečnostních informací v rámci organizace.
  - **Externí účast:** organizace nechápe svou úlohu v širším ekosystému, pokud jde o její závislosti nebo závislé subjekty. Organizace si obecně není vědoma kybernetických rizik v dodavatelském řetězci produktů a služeb, jež poskytuje a využívá.
- **Úroveň 2: Informovanost o rizicích**
  - **Posuzování rizika:** postupy řízení rizik jsou schváleny vedením, ale nemusí být zakotveny jako zásady celé organizace.
  - **Program integrovaného řízení rizik:** na úrovni organizace existuje povědomí o kybernetických bezpečnostních rizicích, ovšem není vytvořen přístup k řízení

kybernetických bezpečnostních rizik v celé organizaci. Provádí se posuzování kybernetických rizik u organizačních i externích aktiv, ale typicky nejsou opakovatelná a neopakují se.
  - **Externí účast:** organizace obecně chápe svou úlohu v širším ekosystému, pokud jde buď o její závislosti, nebo o závislé subjekty, ovšem nikoli v obou případech. Dále si organizace uvědomuje kybernetická rizika v dodavatelském řetězci produktů a služeb, jež poskytuje a využívá, avšak tato rizika neřeší soudržně nebo formálně.

- **Úroveň 3: Opakovatelnost**
  - **Posuzování rizika:** postupy řízení rizik organizace jsou formálně schválené a vyjádřené jako zásady. Kybernetické bezpečnostní postupy organizace jsou pravidelně aktualizovány podle použitého posouzení rizika v případě změn obchodních/cílových požadavků a v případě změny, pokud jde o formy hrozeb a technologií.
  - **Program integrovaného řízení rizik:** existuje přístup k řízení kybernetických bezpečnostních rizik uplatňovaný v celé organizaci. Informované zásady, procesy a postupy pro rizika jsou definovány, uplatňovány v souladu s určením a přezkoumávány. Vyšší řídicí pracovníci zajišťují zohlednění kybernetické bezpečnosti na všech úrovních provozu organizace.
  - **Externí účast:** organizace chápe svou roli, závislosti a závislé subjekty v rámci širšího ekosystému a může přispívat k širšímu pochopení rizik v komunitě. Organizace si je vědoma kybernetických rizik souvisejících s dodavatelským řetězcem produktů a služeb, jež poskytuje a využívá.

- **Úroveň 4: Adaptivní**
  - **Posuzování rizika:** organizace přizpůsobuje své kybernetické bezpečnostní postupy podle předchozích a současných činností v této oblasti, a to včetně poučení a prediktivních ukazatelů.
  - **Program integrovaného řízení rizik:** existuje přístup k řízení kybernetických bezpečnostních rizik uplatňovaný v celé organizaci, který při řešení potenciálních kybernetických bezpečnostních událostí využívá informované zásady, procesů a postupů v oblasti rizik.
  - **Externí účast:** organizace chápe svou roli, závislosti a závislé subjekty v rámci širšího ekosystému a přispívá k širšímu pochopení rizik v komunitě.

Metoda posouzení

Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury je určen organizacím pro jejich vlastní posuzování rizik, aby racionalizovaly, zefektivnily a zkvalitnily svůj přístup a investice do kybernetické bezpečnosti. Aby mohla organizace posoudit účinnost investic, musí nejprve jasně pochopit své cíle a vztah mezi těmito cíli a podpůrnými kybernetickými bezpečnostními výsledky. Kybernetické bezpečnostní výsledky jádra rámce pomáhají při vlastním posouzení účinnosti investic a činností v oblasti kybernetické bezpečnosti.

A.4 Katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti (Q-C2M2)

Katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti (Q-C2M2) vypracovala v roce 2018 Právnická fakulta Katarské univerzity. Q-C2M2 vychází z několika stávajících modelů a vytváří komplexní metodologii posuzování pro zlepšení katarského rámce kybernetické bezpečnosti.

Atributy/dimenze

Q-C2M2 přejímá přístup Národního ústavu pro standardizaci a technologie (NIST) a jako hlavních oblastí modelu využívá pěti základních funkcí. Těchto pět základních funkcí se uplatňuje v katarském kontextu, protože jsou běžné v odvětvích kritické infrastruktury, důležitém prvku katarského rámce kybernetické bezpečnosti. Q-C2M2 je založen na **pěti oblastech**, každé z těchto oblastí se následně dělí do několika **podoblastí** pokrývajících celou škálu vyspělosti schopností v oblasti kybernetické bezpečnosti.

O těchto pěti oblastech je podrobně pojednáno níže:

i **Oblast pochopení** zahrnuje čtyři podoblasti: kybernetická správa, aktiva, rizika a školení.
ii Podoblastmi **oblasti bezpečnost** jsou bezpečnost dat, bezpečnost technologií, bezpečnost kontroly přístupu, bezpečnost komunikací a personální bezpečnost.
iii **Oblast expozice** zahrnuje podoblasti sledování, řízení incidentů, odhalování, analýza a expozice.
iv **Oblast reakce** zahrnuje plánování reakce, zmírnění a komunikaci při reakci.
v **Oblast udržitelnost** sestává z plánování obnovy, řízení kontinuity, zlepšení a externích závislostí.

Úrovně vyspělosti

Q-C2M2 používá **pět úrovní vyspělosti** hodnotících vyspělost schopností státního subjektu nebo nestátní organizace na hlavní funkční úrovni. Tyto úrovně se zaměřují na posuzování vyspělosti v pěti oblastech uvedených v předchozí části.

- **Počáteční:** využívá jednorázové postupy a procesy některých oblastí.
- **Provádějící:** jsou přijaty politiky pro provádění všech činností kybernetické bezpečnosti v dotčených oblastech s cílem dokončit provádění v určitém čase.
- **Rozvíjející:** provedené zásady a postupy pro rozvoj a zlepšení činností kybernetické bezpečnosti v dotčených oblastech s cílem navržení nových činností, které budou prováděny.
- **Adaptivní:** znovu se zabývá a přezkoumává činnosti kybernetické bezpečnosti a přijímá postupy založené na prediktivních ukazatelích odvozených z předchozích zkušeností a opatření.
- **Agilní:** pokračuje v uplatňování adaptivní fáze s přidaným důrazem na agilitu a rychlost při provádění činností v dotčených oblastech.

Metoda posouzení

Q-C2M2 se nachází v rané fázi výzkumu a není dosud dopracován tak, aby jej bylo možné používat. Jedná se o rámec, který by mohly v budoucnosti využívat katarské organizace při uplatňování podrobného modelu posuzování.

A.5 Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC)

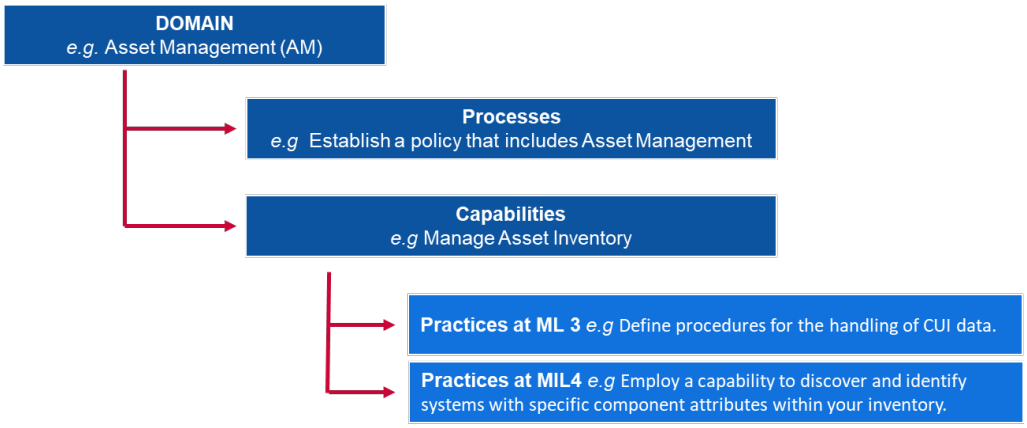
Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC) vypracovalo Ministerstvo obrany USA ve spolupráci s Carnegie Mellon University a Laboratoří aplikované fyziky Johns Hopkins University. Hlavním cílem ministerstva při přípravě tohoto modelu byla ochrana informací ze sektoru obranné průmyslové základny. Informace, kterými se CMMC zabývá, jsou utajeny buď jako „federální smluvní informace“, tedy informace poskytované vládou nebo vytvářené pro ni podle smlouvy neurčené ke zveřejnění, nebo jako „řízené neutajované informace“, což jsou informace, které vyžadují ochranu nebo kontrolu zveřejňování podle zákonů, právních předpisů a zásad platných pro celou státní správu. CMMC hodnotí vyspělost kybernetické bezpečnosti a uvádí osvědčené postupy, které doplňuje certifikační prvek pro zajištění provádění postupů souvisejících s jednotlivými úrovněmi vyspělosti. Nejnovější verze CMMC byla vydána v roce 2020.

Atributy/dimenze

CMMC se zabývá **sedmnácti oblastmi** představujícími klastry kybernetické bezpečnosti, procesů a schopností. Každá oblast se pak dělí na několik **procesů**, které se v těchto oblastech podobají; a jedna na mnoho **schopností** zasahujících do pěti úrovní vyspělosti. Tyto schopnosti (nebo schopnost) jsou dále podrobně rozděleny do **postupů** jednotlivých příslušných úrovní vyspělosti.

Vztah mezi těmito pojmy je uveden níže:

Obrázek 9: Příklad ukazatelů CMMC



DOMAIN e.g. Asset Management (AM)	**OBLAST** např. správa aktiv (AM)
Processes e.g Establish a policy that includes Asset Management	**Procesy** např. vytvořit politiku zahrnující správu aktiv
Capabilities e.g Manage Asset Inventory	**Schopnosti** např. správa inventáře aktiv
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Postupy MIL 3** např. definovat postupy pro nakládání s daty CUI
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Postupy MIL4** např. využít schopnost objevit a určit v inventáři systémy s konkrétními atributy komponentů

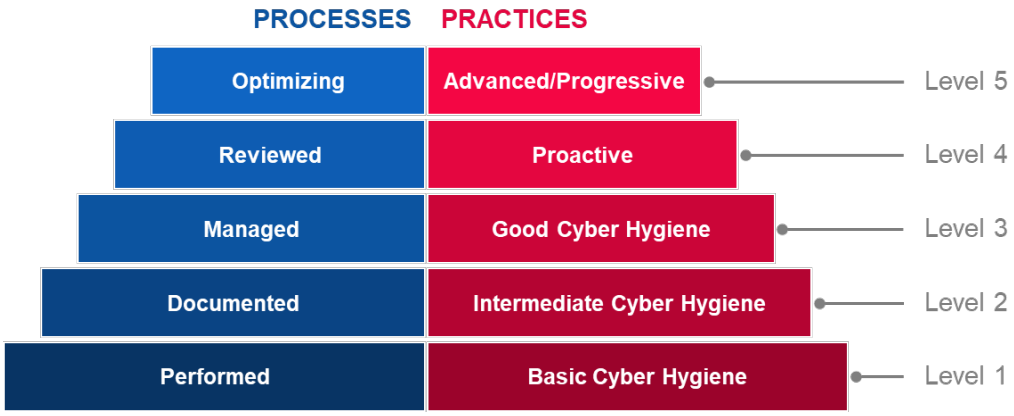
Sedmnáct oblastí je podrobně pojednáno níže:

i kontrola přístupu (AC);
ii správa aktiv (AM);
iii audit a odpovědnost (AU);
iv informovanost a školení (AT);
v řízení konfigurace (CM);
vi určování a ověření (IA);
vii reakce na incidenty (IR);
viii údržba (MA);
ix ochrana médií (MP);
x personální bezpečnost (PS);
xi fyzická ochrana (PE);
xii obnova (RE);
xiii řízení rizik (RM);
xiv posouzení bezpečnosti (CA);
xv povědomí o situaci (SA);
xvi ochrana systémů a komunikací (SC) a
xvii integrita systémů a informací (SI).

Úrovně vyspělosti

CMMC používá **pět úrovní vyspělosti** definovaných na základě procesů a postupů. Aby bylo možné dosáhnout určité úrovně vyspělosti podle CMMC, musí sama organizace splnit podmínky procesů a postupů pro dotčenou úroveň. To rovněž znamená splnění podmínek ze všech úrovní nižších než dotčená úroveň.

Obrázek 10: Úrovně vyspělosti CMMC



PROCESSES	PROCESY
Optimizing	Optimalizační
Reviewed	Přezkoumaný
Managed	Řízený
Documented	Zdokumentovaný
Performed	Provedené
PRACTICES	POSTUPY
Advanced/Progressive	Pokročilý/pokrokový
Proactive	Aktivní
Good Cyber Hygiene	Správná kybernetická hygiena
Intermediate Cyber Hygiene	Pokročilá kybernetická hygiena
Basic Cyber Hygiene	Základní kybernetická hygiena
Level 5	Úroveň 5
Level 4	Úroveň 4
Level 3	Úroveň 3
Level 2	Úroveň 2
Level 1	Úroveň 1

- **Úroveň 1**
  - **Procesy – provedené:** protože organizace může být schopna provádět tyto postupy pouze jednorázově a nemusí spoléhat na dokumentaci. Vyspělost procesu není pro úroveň 1 posouzena.
  - **Postupy – základní kybernetická hygiena:** úroveň 1 se zaměřuje na ochranu FCI (federálních smluvních informací) a skládá se pouze z postupů odpovídajících základním bezpečnostním zárukám.
- **Úroveň 2**
  - **Procesy – zdokumentované:** úroveň 2 vyžaduje, aby organizace vytvořila a zdokumentovala postupy a politiky, jimiž se budou řídit provádění týkající se CMMC. Dokumentace postupů umožňuje, aby je jednotlivci prováděli opakovatelně. Organizace rozvíjí schopnosti vyspělosti zdokumentováním svých procesů a jejich následným uplatňováním jako zdokumentovaných.
  - **Postupy – pokročilá kybernetická hygiena:** úroveň 2 slouží jako mezistupeň mezi úrovněmi 1 a 3 a skládá se z dílčího souboru bezpečnostních požadavků uvedených v NIST SP 800-171, jakož i v postupech uvedených v jiných normách a dokumentech.

- **Úroveň 3**
  - **Procesy – řízené:** úroveň 3 vyžaduje, aby organizace pro praktické provádění vypracovala, spravovala a zajistila prostředky pro plán demonstrující řízení činností pro praktické provedení. Tento plán může obsahovat informace o úkolech, cílech, projektových plánech, zajištění prostředků, požadovaném školení a účasti příslušných zúčastněných stran.
  - **Postupy – správná kybernetická hygiena:** úroveň 3 se zaměřuje na ochranu CUI a zahrnuje všechny bezpečnostní požadavky uvedené v NIST SP 800-171, jakož i postupy z jiných norem a dokumentů týkajících se zmírňování hrozeb.
- **Úroveň 4**
  - **Procesy – přezkoumané:** úroveň 4 vyžaduje, aby organizace přezkoumávala a hodnotila účinnost postupů. Kromě postupů hodnocení účinnosti musí být organizace na této úrovni schopny přijímat v případě nutnosti nápravná opatření a opakovaně informovat vyšší vedení o stavu problému.
  - **Postupy – aktivní:** úroveň 4 se zaměřuje na ochranu CUI (řízených neutajovaných informací) a zahrnuje dílčí soubor pokročilých bezpečnostních požadavků. Tyto postupy zlepšují schopnosti odhalování a reakce organizací při řešení a přizpůsobování se měnícím se taktikám, technikám a postupům.
- **Úroveň 5**
  - **Procesy – optimalizační:** úroveň 5 vyžaduje, aby organizace standardizovala a optimalizovala provádění procesů v rámci celé organizace.
  - **Postupy – pokročilé/aktivní:** úroveň 5 se zaměřuje na ochranu CUI. Tyto doplňující postupy zlepšují hloubku a sofistikovanost schopností v oblasti kybernetické bezpečnosti.

Metoda posouzení

CMMC je relativně nový model dokončený v prvním čtvrtletí 2020. Dosud jej proto nepoužila žádná organizace. Nicméně dodavatelé Ministerstva obrany USA předpokládají, že se při provádění auditů obrátí na certifikované auditory třetích subjektů. Ministerstvo obrany USA předpokládá, že budou jeho dodavatelé provádět osvědčené postupy, aby zvýšili kybernetickou bezpečnost a ochranu citlivých informací.

A.6 Komunitní model vyspělosti schopností v oblasti kybernetické bezpečnosti (CCSMM)

Komunitní model vyspělosti schopností v oblasti kybernetické bezpečnosti (CCSMM) vypracovalo Centrum pro zajištění a zabezpečení infrastruktury na Texaské univerzitě. Cílem CCSMM je lepší definování metod ke stanovení aktuálního stavu komunity, pokud jde o její kybernetickou připravenost, a vypracování plánu pro komunity, podle něhož budou postupovat při svých přípravách. Komunitami, na něž se zaměřuje CCSMM, jsou zejména místní nebo státní vlády. CCSMM byl navržen v roce 2007.

Atributy/dimenze

Úrovně vyspělosti jsou definovány těmito **šesti hlavními oblastmi**, jež pokrývají různé aspekty kybernetické bezpečnosti komunit a organizací. Tyto dimenze jsou jasně definovány pro všechny úrovně vyspělosti (podrobnosti přináší Obrázek 11: Přehled dimenzí CCSMM) Těmito šesti oblastmi jsou:

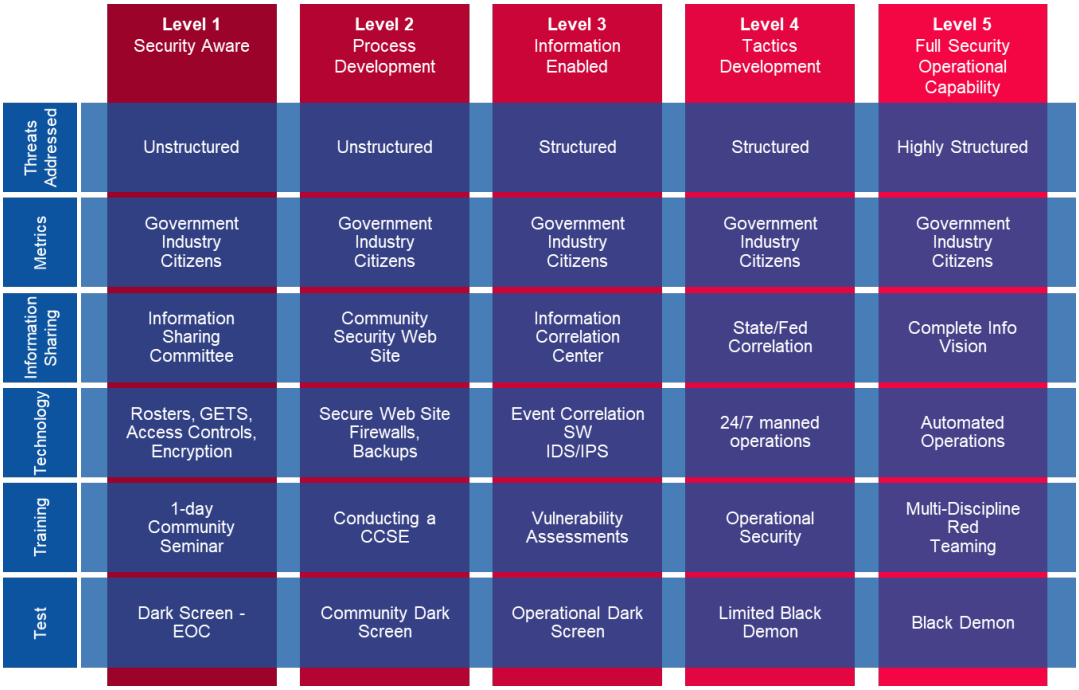
i řešené hrozby;
ii metrika;
iii sdílení informací;
iv technologie;
v školení a
vi testování.

Úrovně vyspělosti

CCSMM vychází z **pěti úrovní vyspělosti** založených na hlavních druzích hrozeb a činností řešených na dotčené úrovni:

- **Úroveň 1: bezpečnostní povědomí**
  Hlavním tématem činností na této úrovni je informování jednotlivců a organizací o hrozbách, problémech a záležitostech souvisejících s kybernetickou bezpečností.
- **Úroveň 2: příprava postupů**
  Úroveň, jejímž cílem je pomáhat komunitám ve vytváření a zlepšování bezpečnostních postupů nutných k účinnému řešení problémů v oblasti kybernetické bezpečnosti.
- **Úroveň 3: možnosti informovanosti**
  Navržena pro zlepšení mechanismů sdílení informací v rámci komunity, aby mohla komunita účinně porovnávat zdánlivě nesouvisející části informací.
- **Úroveň 4: vývoj taktiky**
  Tyto úrovňové prvky jsou navrženy pro lepší a aktivnější metody pro odhalování úroků a reakcí na ně. Na této úrovni by se měla uplatňovat většina preventivních metod.
- **Úroveň 5: úplná schopnost operační bezpečnosti**
  Tato úroveň představuje prvky, kterými by měla disponovat každá organizace, aby ji bylo možné považovat za operačně připravenou k řešení jakékoli kybernetické hrozby.

Obrázek 11: Přehled dimenzí CCSMM podle úrovní



Level 1 Security Aware	Úroveň 1 Bezpečnostní povědomí
Level 2 Process Development	Úroveň 2 Příprava postupů
Level 3 Information Enabled	Úroveň 3 Možnosti informovanosti
Level 4 Tactics Development	Úroveň 4 Vývoj taktiky
Level 5 Full Security Operational Capability	Úroveň 5 Úplná schopnost operační bezpečnosti
Threats Addressed	Řešené hrozby
Metrics	Metrika

Information sharing	Sdílení informací
Technology	Technologie
Training	Školení
Test	Testování
Unstructured	Nestrukturované
Governement Industry Citizens	Státní správa Průmysl Občané
Information Sharing Committee	Výbor pro sdílení informací
Rosters, GETS, Assess Controls, Encryption	Seznamy, GETS, kontroly přístupu, šifrování
1-dat Community Seminar	Jednodenní komunitní seminář
Dark Screen – EOC	Cvičení Dark Screen – EOC
Unstructured	Nestrukturované
Governement Industry Citizens	Státní správa Průmysl Občané
Community Security Web site	Internetová stránka o komunitní bezpečnosti
Secure Web Site Firewalls, Backups	Firewally, zálohy bezpečné internetové stránky
Conudcting a CCSE	Provedení CCSE
Community Dark Screen	Komunita Dark Screen
Structured	Strukturované
Governement Industry Citizens	Státní správa Průmysl Občané
Information Correlation Center	Centrum pro srovnávání informací
Event Correlation SW IDS/IPS	Srovnání událostí SW IDS/IPS
Vulnerability Assessment	Posouzení zranitelnosti
Operational Dark Screen	Operační cvičení Dark Screen
Structured	Strukturované
Governement Industry Citizens	Státní správa Průmysl Občané
State/Fed Correlation	Srovnání stát/federace
24/7 manned operations	Operace s nepřetržitou obsluhou
Operational Security	Operační bezpečnost
Limited Black Demon	Cvičení Limited Black Demon
Highly Structured	Vysoce strukturované
Governement Industry Citizens	Státní správa Průmysl Občané
Complete Info Vision	 Komplexní pojetí informací
Automated Operations	 Automatizované operace
Multi-Discipline Red Teaming	 Multidisciplinární Red Teaming
Black Demon	Cvičení Black Demon

Metoda posouzení

CCSMM je jako metoda posouzení určena k použití komunitami s účastí státních nebo federálních donucovacích orgánů. Zaměřuje se na pomoc komunitám při stanovení, co je nejdůležitější. Jaké jsou nejpravděpodobnější cíle a co je třeba chránit (a v jakém rozsahu). Při zohlednění těchto cílů lze vypracovat plány, aby všechny aspekty komunit dosáhly požadované úrovně vyspělosti v oblasti kybernetické bezpečnosti. Konkrétní poznatky vytvářené pomocí CCSMM pomáhají stanovit cíle různých testů a cvičení, které lze používat k měření účinnosti vytvořených programů.

A.7 Model vyspělosti bezpečnosti informací pro rámec kybernetické bezpečnosti NIST (ISMM)

Model vyspělosti bezpečnosti informací (ISMM) vypracovala Fakulta počítačových věd a techniky Univerzity ropy a nerostů krále Fahda v Saúdské Arábii. Předkládá nový model vyspělosti schopností hodnocení provádění opatření v oblasti kybernetické bezpečnosti. Cílem ISMM je, aby mohly organizace pravidelně a pomocí stejných nástrojů hodnotit svůj postupný pokrok provádění, aby se zajistilo zachování požadovaného stavu zabezpečení. ISMM byl vypracován v roce 2017.

Atributy/dimenze

ISMM vychází ze stávajících posuzovaných oblastí rámce NIST a doplňuje dimenzi posuzování shody. Tím vznikl model se **23 posuzovanými oblastmi** pro stav zabezpečení organizace. Těmito 23 posuzovanými oblastmi jsou:

i správa aktiv;
ii obchodní prostředí;
iii správa a řízení;
iv posouzení rizik;
v strategie řízení rizik;
vi posuzování shody;
vii kontrola přístupu;
viii informovanost a školení;
ix bezpečnost dat;
x procesy a postupy ochrany informací;
xi údržba;
xii ochranná technologie;
xiii anomálie a události;
xiv nepřetržité sledování bezpečnosti;
xv procesy odhalování;
xvi plánování reakce;
xvii komunikace při reakci;
xviii analýza reakce;
xix zmírnění reakce;
xx zlepšení reakce;
xxi plánování obnovy;
xxii zlepšení obnovy a
xxiii komunikace při obnově.

Úrovně vyspělosti

ISMM využívá **pět úrovní vyspělosti**, které nejsou naneštěstí v dostupné dokumentaci uvedeny podrobně.

- **Úroveň 1:** prováděný proces
- **Úroveň 2:** řízený proces
- **Úroveň 3:** zavedený proces
- **Úroveň 4:** předvídatelný proces
- **Úroveň 5:** optimalizační proces

Metoda posouzení

ISMM nenavrhuje organizacím pro provádění posouzení žádnou specifickou metodologii.

A.8 Model útvaru interního auditu pro veřejný sektor (JA-CM)

Model útvaru interního auditu pro veřejný sektor (IA-CM) připravila Výzkumná nadace Útvaru interního auditu s cílem zlepšovat schopnosti a advokační aktivity ve veřejném sektoru prostřednictvím vlastního posouzení. IA-CM se zaměřuje na profesionální auditory a kromě přehledu samotného modelu nabízí praktického průvodce pro použití modelu jako nástroje vlastního posouzení.

Přestože se IA-CM zaměřuje na schopnosti interních auditů spíše než na budování schopností v oblasti kybernetické bezpečnosti, je tento model nástrojem pro vlastní posouzení vyspělosti veřejných subjektů, který lze globálně použít na zlepšování postupů a účinnosti. Protože se nezaměřuje na kybernetickou bezpečnost, nebudou analyzovány jeho atributy. IA-CM vznikl v roce 2009.

Úrovně vyspělosti

Model útvaru interního auditu pro veřejný sektor (IA-CM) zahrnuje **pět úrovní vyspělosti**, z nichž každá popisuje vlastnosti a schopnosti aktivity interního auditu na dotčené úrovni. Úrovně schopností v modelu poskytují plán pro trvalé zlepšování.

- **Úroveň 1: počáteční**
  Žádné udržitelné, opakovatelné schopnosti – závislost na individuální práci
  - Jednorázová nebo nestrukturovaná.
  - Izolované samostatné audity nebo přezkumy přesnosti a shody u dokumentů a transakcí.
  - Výsledky závisí na dovednostech konkrétních osob ve funkci.
  - Nejsou zavedeny žádné odborné postupy kromě těch, jež vypracovaly profesní organizace.
  - Schvalování finančních prostředků vedením, podle potřeby.
  - Neexistující infrastruktura.
  - Auditoři jsou pravděpodobně součástí větší organizační jednotky.
  - Institucionální schopnosti nejsou rozvinuty.
- **Úroveň 2: infrastruktura**
  Udržitelné a opakovatelné postupy a procesy
  - Hlavní otázkou či problémem úrovně 2 je způsob, jak zavést a udržet opakovatelnost postupů, tedy schopnosti opakovatelnosti.
  - Vytváří se vztahy podávání zpráv při interních auditech, řídicí a administrativní infrastruktury a odborné postupy a procesy (pokyny, procesy a postupy pro interní audit).
  - Plánování auditů založeno v zásadě na prioritách vedení.
  - Pokračující spoléhání v zásadě na dovednosti a kompetence konkrétních osob.
  - Částečné dodržování norem.
- **Úroveň 3: integrovaná**
  Jednotné uplatňování řídicích a odborných postupů
  - Politiky, procesy a postupy interních auditů jsou definovány, zdokumentovány a začleněny do sebe navzájem i do infrastruktury organizace.
  - Řízení interních auditů a odborné postupy jsou dobře zavedené a jednotně používané na všechny činnosti interního auditu.
  - Interní audit začíná sladěním s činností organizace a riziky, jimž čelí.
  - Interní audit se vyvíjí od tradičního pouhého interního auditu k tomu, že se stává členem týmu a poskytuje poradenství o výsledcích a řízení rizik.
  - Zaměření na budování týmu a schopnosti činnosti interního auditu a jeho nezávislost a objektivitu.
  - Obecně odpovídá normám.
- **Úroveň 4: řízená**
  Integruje informace z celé organizace, aby se zlepšilo její vedení a řízení rizik
  - Interní audit a očekávání zúčastněných stran jsou shodná.
  - Provádí se metrika, aby byly vyhodnoceny a sledovány postupy a výsledky interního auditu.
  - Interní audit je považován za proces s významným příspěvkem pro organizaci.
  - Interní audit funguje jako nedílná součást řízení organizace a rizik.
  - Interní audit je správně řízenou obchodní jednotkou.

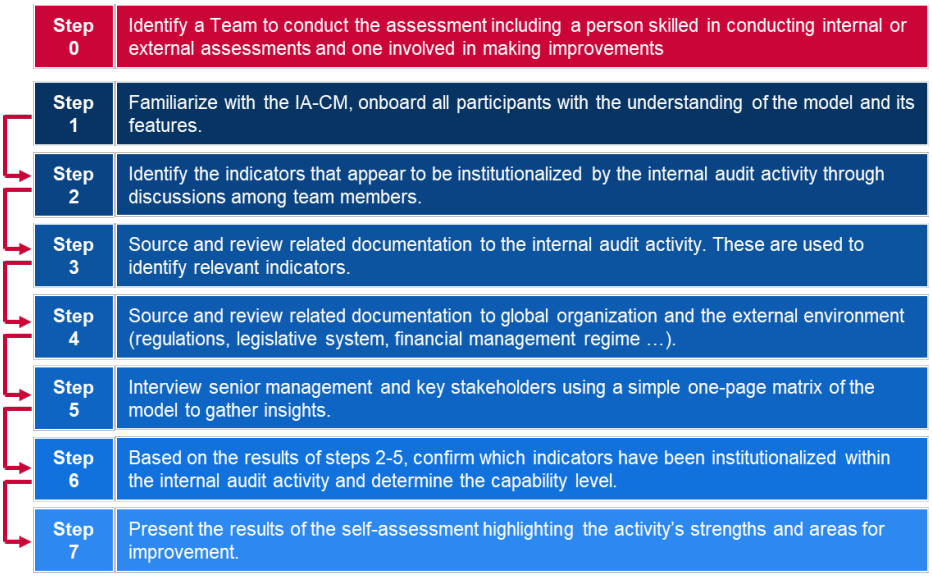
- Rizika jsou vyhodnocována a řízena kvantitativně.
- Existují požadované dovednosti a kompetence společně se schopnostmi pro obnovu a sdílení znalostí (v rámci interního auditu a napříč organizací).

- **Úroveň 5: optimalizační**
  Poučení z vnitřku i vnějšku organizace pro nepřetržité zlepšování
  - Interní audit představuje vzdělávací organizaci s nepřetržitým zlepšováním a inovací procesů.
  - Interní audit využívá informace uvnitř organizace i mimo ni a přispívá k plnění strategických cílů.
  - Špičkové/doporučované výsledky na úrovni osvědčených postupů.
  - Interní audit funguje jako kritická součást řízení a struktury organizace.
  - Špičkové odborné a specializované dovednosti.
  - Výsledky jednotlivců, jednotky a organizace jsou plně začleněny do
  - hlavních zlepšení výsledků.

Metoda posouzení

Model útvaru interního auditu pro veřejný sektor je zcela jasně určen pro vlastní posuzování. Poskytuje podrobné kroky použití IA-CM a vzorové prezentace, které lze přizpůsobit. Před začátkem vlastního posouzení je nutné určit konkrétní tým s minimálně jednou osobou se zkušenostmi s prováděním interních či externích hodnocení v rámci interních auditů a jednou osobou podílející se na zlepšení v této oblasti.

Obrázek 12: Kroky vlastního posouzení podle IC-AM



Step 0	Krok 0
Step 1	Krok 1
Step 2	Krok 2
Step 3	Krok 3
Step 4	Krok 4
Step 5	Krok 5
Step 6	Krok 6
Step 7	Krok 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Určení týmu provádějícího posouzení, včetně osoby se zkušenostmi s prováděním interních nebo externích posouzení a osoby podílející se na zlepšeních.

Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Seznámení se s IA-CM, se všemi účastníky a pochopením modelu a jeho funkcí.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Určení ukazatelů, které mají být činností auditu a v rámci diskusí mezi členy týmu institucionalizovány.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Získání a přezkum související s dokumentací pro provádění interního auditu. Použijí se k určení příslušných ukazatelů.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Získání a přezkum související dokumentace pro globální organizaci a vnější prostředí (předpisy, legislativní systém, režim finančního řízení…).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Rozhovory s vyšším vedením a hlavními zúčastněnými stranami pomocí jednoduchého jednostránkového vzoru kvůli získání náhledu dovnitř organizace.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Podle výsledků kroků 2–5 potvrdit, které ukazatele jsou institucionalizovány v rámci činnosti interního auditu, a stanovit úroveň schopností.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Prezentace výsledků vlastního posouzení se zvýrazněním silných stránek činnosti a oblastí pro zlepšení.

A.9 Globální index kybernetické bezpečnosti (GCI)

Globální index kybernetické bezpečnosti (GCI) je iniciativa Mezinárodní telekomunikační unie (ITU) zaměřená na přezkum závazku kybernetické bezpečnosti a situace ve všech oblastech ITU: Afrika, Severní a Jižní Amerika, arabské státy, Asie-Tichomoří, SNS a Evropa, se zaměřením zejména na země s vysokou úrovní závazků a postupy, které je možné doporučit. Cílem GCI je pomáhat zemím s určením oblastí zlepšení kybernetické bezpečnosti, jakož i jejich motivování k provádění činností s cílem zlepšení jejich hodnocení, tedy pomáhat se zvýšením celkové úrovně kybernetické bezpečnosti ve světě.

Protože se v případě GCI jedná o index, nikoli model vyspělosti, nepoužívá pro hodnocení a srovnání globálních závazků států a regionů úrovně vyspělosti, ale skóre.

Atributy/dimenze

Globální index kybernetické bezpečnosti (GCI) stojí na pěti pilířích globální agendy kybernetické bezpečnosti. Tyto pilíře tvoří pět dílčích indexů GCI a zahrnují soubor ukazatelů. Těmito pěti pilíři a ukazateli jsou:

i **Právní:** opatření založená na existenci právních institucí a rámců kybernetické bezpečnosti a boje proti kybernetické kriminalitě.
- Právní předpisy pro boj proti kybernetické kriminalitě.
- Předpisy v oblasti kybernetické bezpečnosti.
- Právní předpisy pro zadržování/omezování spamu.

ii **Technické:** opatření založená na existenci technických institucí a rámců kybernetické bezpečnosti.
- CERT/CIRT/CSRIT.
- Rámec uplatňování norem.
- Standardizační orgán.
- Technické mechanismy a schopnosti použité pro boj proti spamu.
- Využívání cloudů pro účely kybernetické bezpečnosti.

- Mechanismy on-line ochrany dětí.

iii **Organizační:** opatření založená na existenci institucí koordinujících politiky a strategie pro rozvoj kybernetické bezpečnosti na vnitrostátní úrovni.
- Národní strategie kybernetické bezpečnosti.
- Odpovědná agentura.
- Kybernetická bezpečnost.

iv **Budování schopností:** opatření založená na existenci programů výzkumu a vývoje, vzdělávání a školení, certifikovaných profesionálů a veřejných agentur podporujících budování schopností.
- Kampaně na zvyšování veřejného povědomí.
- Rámec pro certifikaci a akreditaci odborníků na kybernetickou bezpečnost.
- Odborné školicí kurzy v oblasti kybernetické bezpečnosti.
- Vzdělávací programy nebo akademické osnovy týkající se kybernetické bezpečnosti.
- Programy VaV kybernetické bezpečnosti.
- Pobídkové mechanismy.

v **Spolupráce:** opatření založená na existenci partnerství, rámců spolupráce a sítí pro sdílení informací.
- Bilaterální dohody.
- Multilaterální dohody.
- Účast na mezinárodních fórech/sdruženích.
- Partnerství veřejného a soukromého sektoru.
- Partnerství mezi agenturami a v rámci agentur.
- Osvědčené postupy.

Metoda posouzení

GCI je nástrojem vlastního posouzení na základě dotazníku[30] s binárními, předem zadanými odpověďmi a otevřenými otázkami. Použití binárních odpovědí eliminuje možnost hodnocení na základě stanoviska a všech možných výchylek k určitým druhům odpovědí. Předem zadané odpovědi šetří čas a umožňují přesnou analýzu dat. Kromě toho umožňuje jednoduchá dichotomická stupnice rychlejší a složitější vyhodnocení a nepotřebuje dlouhé odpovědi, což zrychluje a harmonizuje postup poskytování odpovědí a dalšího hodnocení. Respondent by měl pouze potvrdit přítomnost či absenci určitých, předem zadaných řešení v oblasti kybernetické bezpečnosti. Mechanismus on-line dotazníku, který se používá pro sběr odpovědí a nahrávání příslušného materiálu, umožňuje extrakci osvědčených postupů a provedení souboru tematických kvalitativních hodnocení skupinou odborníků.

Celkový proces CGI se provádí takto:

- Všem účastníkům je zaslána pozvánka, která je informuje o iniciativě a je v ní uvedena žádost o kontaktní místo odpovědné za sběr všech příslušných dat za vyplnění on-line dotazníku CGI. Během on-line průzkumu bude schválené kontaktní místo oficiálně ze strany ITU vyzváno k vyplnění dotazníku.
- Sběr primárních dat (u zemí, které neodpoví na dotazník):
  - ITU vypracuje počáteční návrh odpovědi na dotazník pomocí veřejně dostupných dat a on-line výzkumu.
  - Návrh dotazníku se zašle kontaktním místům k přezkumu.
  - Kontaktní místa odpovědi zpřesní a návrh dotazníku zašlou zpět.
  - Opravený návrh dotazníku se zašle kontaktnímu místu ke konečnému schválení.
  - Potvrzený dotazník se použije k analýze, stanovení skóre a hodnocení.
- Sběr sekundárních dat (u zemí, které odpoví na dotazník):
  - ITU zjistí chybějící odpovědi, podpůrné dokumenty, odkazy apod.
  - Kontaktní místo podle potřeby zpřesní odpovědi.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf.

- Opravený návrh dotazníku se zašle kontaktnímu místu ke konečnému schválení.
- Potvrzený dotazník se použije k analýze, stanovení skóre a hodnocení.

A.10 Index kybernetických schopností (CPI)

Index kybernetických schopností (CPI) vytvořil v roce 2011 výzkumný program Economist Intelligence Unit sponzorovaný Boozem Allenem Hamiltonem. CPI je „dynamický kvantitativní a kvalitativní model, […] který hodnotí konkrétní atributy kybernetického prostředí v rámci čtyř hnacích sil kybernetických schopností: právního a regulačního rámce; hospodářského a sociálního kontextu; technologické infrastruktury a použití v průmyslu, kdy jsou zkoumány digitální postupy v klíčových odvětvích“[31]. Cílem Indexu kybernetických schopností je hodnocení schopností zemí G20 odolat kybernetickým útokům a využívat požadovanou digitální infrastrukturu pro prosperující a bezpečnou ekonomiku. Hodnocení podle CPI se zaměřuje na devatenáct zemí G20 (kromě EU). Index pak poskytuje hodnocení zemí pro jednotlivé ukazatele.

Atributy/dimenze

Ukazatel kybernetických schopností (CPI) je založen na čtyřech hnacích silách těchto schopností. Konkrétní skóre zemí v jednotlivých kategoriích se pak měří pomocí několika ukazatelů. Kategoriemi a pilíři jsou:

i **Právní a regulační rámec**
- Státní závazek k rozvoji kybernetiky
- Politiky kybernetické ochrany
- Kybernetické cenzura (nebo její absence)
- Účinnost politik
- Ochrana práv duševního vlastnictví

ii **Hospodářský a sociální kontext**
- Úrovně vzdělání
- Technické dovednosti
- Otevřenost obchodování
- Míra inovace v obchodním prostředí

iii **Technologická infrastruktura**
- Přístup k informační a komunikační technologii
- Kvalita informační a komunikační technologie
- Dostupnost informační a komunikační technologie
- Investice do informační technologie
- Počet zabezpečených serverů

iv **Použití v průmyslu**
- Chytré sítě
- Elektronické zdravotnictví
- Elektronický obchod
- Inteligentní doprava
- Elektronická veřejná správa

Metoda posouzení

CPI je kvalitativní a kvantitativní hodnoticí model. Posouzení bylo provedeno The Economist Intelligence Unit pomocí kvantitativních ukazatelů z dostupných statistických údajů a pomocí odhadů v případech, kdy data chyběla. Hlavními použitými zdroji jsou Economist Intelligence Unit; Organizace OSN pro výchovu, vědu a kulturu (UNESCO); Mezinárodní telekomunikační unie (ITU) a Světová banka.

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf.

A.11 Index kybernetických schopností (CPI)

Tato část uvádí přehled hlavních zjištění analýz stávajících modelů vyspělosti. Tabulka 5: Přehled analyzovaných modelů vyspělosti poskytuje přehled o hlavních charakteristikách jednotlivých modelů podle upraveného Beckerova modelu. Tabulka 6 Srovnání úrovní vyspělosti přináší podrobné definice úrovní vyspělosti analyzovaných modelů. Tabulka 7 přináší přehled dimenzí nebo atributů použitých v jednotlivých modelech.

Tabulka 5: Přehled analyzovaných modelů vyspělosti

Název modelu	Zdrojová instituce	Účel	Cíl	Počet úrovní	Počet atributů	Metoda posouzení	Představení výsledků
Model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy (CMM)	Centrum pro globální schopnosti v oblasti kybernetické bezpečnosti Oxfordská univerzita	Zvýšení rozsahu a účinnosti mezinárodního budování schopností v oblasti kybernetické bezpečnosti	Země	5	5 hlavních dimenzí	Spolupráce s místní organizací na doladění modelu před jeho použitím ve vnitrostátním kontextu	Radar s 5 částmi
Model vyspělosti schopností v oblasti kybernetické bezpečnosti (C2M2)	Ministerstvo energetiky USA	Pomoc organizacím s hodnocením a zlepšeními jejich programů kybernetické bezpečnosti a posílení provozní odolnosti	Organizace všech odvětví, druhů a velikostí	4	10 hlavních oblastí	Metodologie a nástroje sebehodnocení	Hodnoticí tabulka s koláčovými grafy
Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury	Národní ústav pro standardizaci a technologie (NIST)	Rámec zaměřený na vedení činností v oblasti kybernetické bezpečnosti a řízení rizik v organizaci	Organizace	Není k dispozici (4 úrovně)	5 hlavních funkcí	Vlastní posouzení	-
Katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti (Q-C2M2)	Právnická fakulta Katarské univerzity	Vytvoření funkčního modelu, který bude možné použít pro hodnocení, měření a rozvoj katarského rámce kybernetické bezpečnosti	Katarské organizace	5	5 hlavních oblastí	–	-
Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC)	Ministerstvo obrany USA	Podpora postupů v oblasti kybernetické bezpečnosti pro zabezpečení informací	Organizace sektoru obranné průmyslové základny	5	17 hlavních oblastí	Posouzení externími auditory	-
Komunitní model vyspělosti schopností v oblasti kybernetické bezpečnosti (CCSMM)	Centrum pro zajištění a bezpečnost infrastruktury Texaské univerzity	Stanovení aktuálního stavu komunity, pokud jde o její kybernetickou připravenost, a vypracování plánu pro komunity, podle něhož budou postupovat při svých přípravách	Komunity (místní nebo státní vlády)	5	6 hlavních oblastí	Posouzení s komunitami za přispění státu a federálních donucovacích orgánů	-
Model vyspělosti bezpečnosti informací pro rámec kybernetické bezpečnosti NIST (ISMM)	Fakulta počítačových věd a techniky Univerzita ropy a nerostů krále Fahda, Saúdská Arábie.	Umožnit organizacím hodnotit postupný pokrok, aby zajistily zachování požadovaného stavu zabezpečení	Organizace	5	23 posuzovaných oblastí	–	-
Model útvaru interního auditu pro veřejný sektor (JA-CM)	Výzkumná nadace Institutu interních auditorů	Rozvoj schopností interního auditu a advokačních činností prostřednictvím vlastního posouzení ve veřejném sektoru	Organizace veřejného sektoru	5	6 prvků	Vlastní posouzení	-
Globální index kybernetické bezpečnosti (GCI)	Mezinárodní telekomunikační unie (ITU)	Přezkum závazků a situace v oblasti kybernetické bezpečnosti a pomoc zemím s určováním oblastí zlepšení, pokud jde o kybernetickou bezpečnost	Země	Není k dispozici	5 pilířů	Vlastní posouzení	Hodnoticí tabulka

Index kybernetických schopností (CPI)	The Economist Intelligence Unit a Booz Allen Hamilton	Hodnocení schopností zemí G20 odolat kybernetickým útokům a využívat požadovanou digitální infrastrukturu pro prosperující a bezpečnou ekonomiku.	Země G20	Není k dispozici	4 kategorie	Hodnocení provedené Economist Intelligence Unit	Hodnoticí tabulka

Tabulka 6 Srovnání úrovní vyspělosti

Model	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4	Úroveň 5
Model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy (CMM)	**Začátek** Vyspělost v oblasti kybernetické bezpečnosti neexistuje nebo je velmi omezená. Mohou být vedeny první diskuse o budování schopností v oblasti kybernetické bezpečnosti, ale dosud nejsou přijata žádná konkrétní opatření. V této fázi chybí pozorovatelný důkaz.	**Utváření** Některé charakteristiky aspektů se začínají vyvíjet a jsou formulovány, ovšem mohou být jednorázové, neorganizované, špatně definované – nebo jednoduše „nové“. Ovšem je možné jasně doložit důkazy této činnosti.	**Zřízena** Prvky tohoto aspektu existují a fungují. Nevěnuje se však dostatečná pozornost relativnímu přidělování prostředků. Při rozhodování se nečiní příliš kompromisů ohledně „souvisejících“ investic do různých prvků aspektu. Tento aspekt je ale funkční a definovaný.	**Strategická** Vybírá se, které části aspektů jsou důležité a které méně důležité pro konkrétní organizaci či stát. Strategická fáze odráží skutečnost, že jsou tato rozhodnutí prováděna podle situace jednotlivých států či organizací.	**Dynamická** Jsou k dispozici jasné mechanismy změny strategie podle aktuálních okolností, jakými jsou technologie v oblasti hrozeb, globální konflikt nebo zásadní změna v jedné z dotčených oblastí (např. kyberkriminalita nebo soukromí). Dynamické organizace vyvíjí metody změny strategie za pochodu. Tato fáze je charakterizována rychlým rozhodováním, přerozdělováním prostředků a neustálou pozorností věnovanou měnícímu se prostředí.
Model vyspělosti schopností v oblasti kybernetické bezpečnosti (C2M2)	**MIL0** Postupy se neprovádí.	**MIL1** Provádí se počáteční postupy, ovšem mohou se provádět jen jednorázově.	**MIL2** Charakteristiky řízení: Postupy jsou dokumentovány. Na podporu procesů jsou přiděleny vhodné zdroje. Pracovníci provádějící postupy disponují vhodnými dovednostmi a znalostmi. Jsou rozděleny odpovědnost a pravomoci k provádění postupů. Charakteristika přístupu: Postupy jsou úplnější a pokročilejší než u MIL1.	**MIL3** Charakteristiky řízení: Činnosti jsou řízeny politikami (nebo jinými organizačními směrnicemi). Výsledkové cíle pro činnosti oblasti se stanoví a jsou sledovány, aby byly zjevné výsledky. Zdokumentované postupy činností oblastí jsou v celém podniku standardizovány a zlepšovány. Charakteristika přístupu: Postupy jsou úplnější a pokročilejší než u MIL2.	–
Model vyspělosti bezpečnosti informací pro rámec kybernetické bezpečnosti NIST (ISMM)	**Prováděný proces**	**Řízený proces**	**Zavedený proces**	**Předvídatelný proces**	**Optimalizační proces**

Katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti (Q-C2M2)	**Počáteční** Využívá jednorázové postupy a procesy některých oblastí.	**Rozvíjející** Provedené zásady a postupy pro rozvoj a zlepšení činností kybernetické bezpečnosti v dotčených oblastech s cílem navržení nových činností, které budou prováděny.	**Provádějící** Jsou přijaty politiky pro provádění všech činností kybernetické bezpečnosti v dotčených oblastech s cílem dokončit provádění v určitém čase.	**Adaptivní** Znovu se zabývá a přezkoumává činnosti kybernetické bezpečnosti a přijímá postupy založené na prediktivních ukazatelích odvozených z předchozích zkušeností a opatření.	**Agilní** Pokračuje v uplatňování adaptivní fáze s přidaným důrazem na agilitu a rychlost při provádění činností v dotčených oblastech.
Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC)	**Procesy: Provedený** Protože organizace může být schopna provádět tyto postupy pouze jednorázově a nemusí spoléhat na dokumentaci, není vyspělost pro úroveň 1 posouzena. **Postupy: Základní kybernetická hygiena** Úroveň 1 se zaměřuje na ochranu FCI (federálních smluvních informací) a skládá se pouze z postupů odpovídajících základním bezpečnostním požadavkům.	**Procesy: Zdokumentovaný** Úroveň 2 vyžaduje, aby organizace vytvořila a zdokumentovala postupy a politiky, jimiž se budou řídit její činnosti týkající se CMMC. Dokumentace postupů umožňuje, aby je jednotlivci prováděli opakovatelně. Organizace rozvíjí schopnosti vyspělosti zdokumentováním svých procesů a jejich následným uplatňováním jako zdokumentovaných. **Postupy: Pokročilá kybernetická hygiena** Úroveň 2 slouží jako mezistupeň mezi úrovněmi 1 a 3 a skládá se z dílčího souboru bezpečnostních požadavků uvedených v NIST SP 800-171 a postupů uvedených v jiných normách a dokumentech.	**Procesy: Řízený** Úroveň 3 vyžaduje, aby organizace pro praktické provádění vypracovala, spravovala a zajistila prostředky pro plán demonstrující řízení činností. Tento plán může obsahovat informace o úkolech, cílech, projektových plánech, zajištění prostředků, požadovaném školení a účasti příslušných zúčastněných stran. **Postupy: Správná kybernetická hygiena**. Úroveň 3 se zaměřuje na ochranu CUI (řízené neutajované informace) a zahrnuje všechny bezpečnostní požadavky uvedené v NIST SP 800-171, jakož i další postupy z jiných norem a dokumentů týkajících se zmírňování hrozeb.	**Procesy: Přezkoumaný.** Úroveň 4 vyžaduje, aby organizace postupy přezkoumávala a hodnotila z hlediska účinnosti. Kromě postupů hodnocení účinnosti musí být organizace na této úrovni schopny přijímat v případě nutnosti nápravná opatření a opakovaně informovat vyšší vedení o stavu problému. **Postupy: Aktivní** Úroveň 4 se zaměřuje na ochranu CUI (řízených neutajovaných informací) a zahrnuje dílčí soubor pokročilých bezpečnostních požadavků. Tyto postupy zlepšují schopnosti odhalování a reakce organizací při řešení a přizpůsobování se měnícím se taktikám, technikám a postupům.	**Procesy: Optimalizační** Úroveň 5 vyžaduje, aby organizace standardizovala a optimalizovala provádění procesů v rámci celé organizace. **Postupy: Pokročilý/aktivní** Úroveň 5 se zaměřuje na ochranu CUI (řízených neutajovaných informací). Tyto doplňující postupy zlepšují hloubku a sofistikovanost schopností v oblasti kybernetické bezpečnosti.
Komunitní model vyspělosti schopností v oblasti kybernetické bezpečnosti (CCSMM)	**Bezpečnostní povědomí** Hlavním tématem činností na této úrovni je informování jednotlivců a organizací o hrozbách, problémech a záležitostech souvisejících s kybernetickou bezpečností.	**Příprava procesů** Úroveň, jejímž cílem je pomáhat komunitám ve vytváření a zlepšování bezpečnostních procesů nutných k účinnému řešení problémů v oblasti kybernetické bezpečnosti.	**Možnosti informovanosti** Navržena pro zlepšení mechanismů sdílení informací v rámci komunity, aby mohla komunita účinně porovnávat zdánlivě nesouvisející části informací.	**Vývoj taktiky** Tyto úrovňové prvky jsou navrženy pro lepší a aktivnější metody pro odhalování úroků a reakcí na ně. Na této úrovni by se měla uplatňovat většina preventivních metod.	**Úplná schopnost operační bezpečnosti** Tato úroveň představuje prvky, kterými by měla disponovat každá organizace, aby ji bylo možné považovat za operačně připravenou k řešení jakékoli kybernetické hrozby.
Model útvaru interního auditu pro veřejný sektor (JA-CM)	**Počáteční** Žádné udržitelné, opakovatelné schopnosti – závislost na individuální práci	**Infrastruktura** Udržitelné a opakovatelné postupy a procesy	**Integrovaná** Jednotné uplatňování řídicích a odborných postupů	**Řízená** Integruje informace z celé organizace, aby se zlepšilo její vedení a řízení rizik	**Optimalizační** Poučení z vnitřku i vnějšku organizace pro nepřetržité zlepšování

Tabulka 7: Srovnání atributů/dimenzí

	Model vyspělosti schopností v oblasti kybernetické bezpečnosti pro státy (CMM)	Model vyspělosti schopností v oblasti kybernetické bezpečnosti (C2M2)	Katarský model vyspělosti schopností v oblasti kybernetické bezpečnosti (Q-C2M2)	Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC)	Certifikace modelu vyspělosti schopností v oblasti kybernetické bezpečnosti (CMMC)	Model vyspělosti bezpečnosti informací pro rámec kybernetické bezpečnosti NIST (ISMM)	Rámec pro zlepšení kybernetické bezpečnosti kritické infrastruktury	Globální index kybernetické bezpečnosti (GCI)	Index kybernetických schopností (CPI)
Úrovně	Pět dimenzí rozdělených do několika faktorů obsahujících různé aspekty a ukazatele (Obrázek 4)	Deset oblastí, včetně jedinečného řízení cílů a několika cílů přístupu (Obrázek 6)	Pět oblastí rozdělených na dílčí podoblasti	Sedmnáct oblastí podrobně rozdělených do procesů a jedna do mnoha schopností , které se následně detailně dělí na postupy (Obrázek 9).	Šest hlavních oblastí	Dvacet tři posuzovaných oblastí	Pět funkcí se základními hlavními kategoriemi a podkategoriemi (Obrázek 8).	Pět pilířů, včetně několika ukazatelů	Čtyři kategorie s několika ukazateli
Atributy/dimenze	i Vypracování politiky a strategie v oblasti kybernetické bezpečnosti ii Podpora odpovědné kultury v oblasti kybernetické bezpečnosti ve společnosti iii Rozvoj znalostí v oblasti kybernetické bezpečnosti iv Vytvoření účinného právního a regulačního rámce v Řízení rizik pomocí norem, organizací a technologií	i Řízení rizik ii Řízení aktiv, změn a konfigurace iii Správa identit a přístupu iv Řízení hrozeb a zranitelnosti v Povědomí o situaci vi Reakce na události a incidenty vii Řízení dodavatelského řetězce a vnějších závislostí viii Řízení pracovníků ix Architektura kybernetické bezpečnosti x Řízení programu kybernetické bezpečnosti	i Pochopení (kybernetická správa, aktiva, rizika a školení) ii Bezpečnost (bezpečnost dat, bezpečnost technologií, bezpečnost kontroly přístupu, bezpečnost komunikací a personální bezpečnost) iii Expozice (sledování, řízení incidentů, odhalování, analýza a expozice) iv Reakce (plánování reakce, zmírnění a komunikace při reakci) v Udržitelnost (plánování obnovy, řízení kontinuity, zlepšení a externí závislosti)	i Kontrola přístupu ii Správa aktiv iii Audit a odpovědnost iv Informovanost a školení v Řízení konfigurace vi Určování a ověřování vii Reakce na incidenty viii Údržba ix Ochrana médií x Personální bezpečnost xi Fyzická ochrana xii Obnova xiii Řízení rizik xiv Hodnocení bezpečnosti xv Povědomí o situaci xvi Ochrana systémů a komunikací xvii Integrita systémů a informací	i Řešené hrozby ii Metrika iii Sdílení informací iv Technologie v Školení vi Testování	i Správa aktiv ii Obchodní prostředí iii Správa a řízení iv Posouzení rizik v Strategie řízení rizik vi Posuzování shody vii Kontrola přístupu viii Informovanost a školení ix Bezpečnost dat x Procesy a postupy ochrany informací xi Údržba xii Ochranná technologie xiii Anomálie a události xiv Nepřetržité sledování bezpečnosti xv Procesy odhalování xvi Plánování reakce xvii Komunikace při reakci xviii Analýza reakce xix Zmírnění reakce xx Zlepšení reakce xxi Plánování obnovy xxii Zlepšení obnovy xxiii Komunikace při obnově	i Určovat ii Chránit iii Odhalit iv Odpovědět v Obnovit	i Právní ii Technická iii Organizační iv Budování schopností v Spolupráce	i Právní a regulační rámec ii Hospodářský a sociální kontext iii Technologická infrastruktura iv Použití v průmyslu

PŘÍLOHA B – LITERATURA PRO ANALÝZU PODKLADŮ

Agentura Evropské unie pro bezpečnost sítí a informací (2012) NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

Agentura Evropské unie pro bezpečnost sítí a informací (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

Agentura Evropské unie pro bezpečnost sítí a informací (2016) Guidelines for SMEs on the security of personal data processing.

Agentura Evropské unie pro bezpečnost sítí a informací (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

Almuhammadi, S. a Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework“, in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. a Alsaleh, M. (2017) „Information Security Maturity Model for Nist Cyber Security Framework“, in Computer Science & Information Technology (CS & IT). K dispozici na adrese: https://airccj.org/CSCP/vol7/csit76505.pdf.

Anna, S. a kol. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML.

Becker, J., Knackstedt, R. a kol. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. K dispozici na adrese: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Bellasio, J. a kol. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. K dispozici na adrese: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf.

Bílý dům (2018) National Cyber Strategy of the United States of America. K dispozici na adrese: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Bourgue, R. (2012) „Introduction to Return on Security Investment“.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) Cybersecurity Capability Maturity Model (C2M2) Version 2.0. K dispozici na adrese https://apps.dtic.mil/sti/pdfs/AD1078768.pdf.

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. K dispozici na adrese: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf.

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity – Self-assessment Tool (bez data). K dispozici na adrese: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011) Specialised cybercrime units – Good practice study. K dispozici na adrese: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33.

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (bez data). K dispozici na adrese: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool.

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (bez data) „Welcome to the NCSS Training Tool".

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. K dispozici na adrese: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf.

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. K dispozici na adrese: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

Dekker, M. A. C. (2015) Guideline on Threats and Assets. K dispozici na adrese: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf.

Digital Slovenia (2016) Cybersecurity Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia.

Domingo-Ferrer, J. *a kol.* (2014) *Privacy and data protection by design - from policy to engineering.* K dispozici na této adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML.

Evropská komise (2012) Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. K dispozici na adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52012PC0238&qid=1612530221741&from=EN.

Evropská unie a Agentura Evropské unie pro bezpečnost sítí a informací (2017) Handbook on security of personal data processing. K dispozici na adrese: http://dx.publications.europa.eu/10.2824/569768.

Evropská unie a Agentura Evropské unie pro bezpečnost sítí a informací (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. K dispozici na této adrese: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe.

Federální rada (2018) National strategy for the protection of Switzerland against cyber risks.

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML.

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML.

Galan Manso, C. a kol. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small

and medium enterprises. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML.

Innsbrucká univerzita a kol. (2009) Understanding Maturity Models.

Institut interních auditorů (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

J.D., R. D. B. (2019) „Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework“, International Review of Law.

Kancelář francouzského premiéra (2014) French National Digital Security Strategy. K dispozici na adrese: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

Kancelář prezidenta USA (2015) Memorandum for Heads of Executive Departments and Agencies. K dispozici na adrese: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf.

Liveri, D. a kol. (2014) An evaluation framework for national cyber security strategies. Heraklion: ENISA. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *a kol.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML.

Mezinárodní telekomunikační unie (ITU) (2018) Guide to developing a national cybersecurity strategy. K dispozici na adrese: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

Mezinárodní telekomunikační unie (ITU) (2018) The Global Cybersecurity Index. K dispozici na adrese: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Ministerstvo hospodářství a spojů (2019) Cybersecurity Strategy – Republic of Estonia. K dispozici na adrese: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

Ministerstvo národní obrany Litevské republiky (2018) National Cyber Security Strategy

Ministerstvo pro hospodářskou soutěž a digitální, námořní a na služby zaměřenou ekonomiku (2016) Malta Cyber Security Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta.

Národní centrum kybernetické bezpečnosti (2015) Národní strategie kybernetické bezpečnosti České republiky. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf.

Národní ústav pro standardizaci a technologie (2018) Framework for Improving Critical Infrastructure Cybersecurity, verze 1.1. Gaithersburg, MD: Národní ústav pro standardizaci a technologie. K dispozici na adrese: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

National Cyber Security Strategies - Interactive Map (bez data). K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool (2018). K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Object Management Group (2008) Business Process Maturity Model. K dispozici na adrese: https://www.omg.org/spec/BPMM/1.0/PDF.

OECD, Evropská unie a Společné výzkumné středisko– – Evropská komise (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. K dispozici na adrese: https://www.oecd.org/sdd/42495745.pdf.

Organizace pro hospodářskou spolupráci a rozvoj (OECD) (2012) Cybersecurity policy making at a turning point. K dispozici na adrese: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

Ouzounis, E. (2012) „National Cyber Security Strategies – Practical Guide on Development and Execution".

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Předsednictvo Rady ministrů (2017) The Italian Cybersecurity Action Plan. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security.

Rada ministrů (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. K dispozici na adrese: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf.

Rada ministrů (2019) Portuguese Official Journal, sv. 1 — No. 108 – Usnesení Rady ministrů č. 92/2019. K dispozici na adrese: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf.

Rada vlády Lucemburského velkovévodství (2018) National Cybersecurity Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en.

Sarri, A., Kyranoudi, P. a Agentura Evropské unie pro kybernetickou bezpečnost (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. K dispozici na adrese: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Sekretariát Bezpečnostního výboru (2019) Finland's Cyber Security Strategy 2019. K dispozici na adrese: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.

Smith, R. (2015) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016

Smith, R. (2016) „Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016", in Smith, R., Core EU Legislation. London: Macmillan Education. K dispozici na adrese: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Spolkové kancléřství Rakouské republiky (2013) Austrian Cyber Security Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en.

Spolkové ministerstvo vnitra (2011) Cyber Security Strategy for Germany. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en.

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Strategie belgické vlády (2012) Cyber Security Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en.

Swedish Government (2017) Nationell strategi för samhällets informations – och cybersäkerhet. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view.

Trimintzios, P. a kol. (2011) Cyber Europe Report. K dispozici na adrese: https://www.enisa.europa.eu/publications/ce2010report.

Trimintzios, P., Gavrila, R. a Agentura Evropské unie pro bezpečnost sítí a informací (2013) *National-level risk assessments: an analysis report.* K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML.

Trimintzios, P., Gavrila, R. a kol. (2015) Report on cyber-crisis cooperation and management. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML.

Trimintzios, P., Ogee, A. a kol. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. K dispozici na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML.

UK National Cyber Security Strategy 2016-2021 (2016). K dispozici na adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Univerzita v Ghentu a kol. (2017) „Evaluating Business Process Maturity Models“, Journal of the Association for Information Systems. K dispozici na adrese: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais.

Úřad komisaře pro regulaci elektronických komunikací a pošt (2012) Cybersecurity Strategy of the Republic of Cyprus.

Úřední věstník Evropské unie (2008) SMĚRNICE RADY 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. K dispozici na adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32008L0114&qid=1612530775722&from=EN.

Vláda Dánského království – ministerstvo financí (2018) Danish Cyber and Information Security Strategy. K dispozici na adrese: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf.

Vláda Chorvatské republiky (2015) The National Cyber Security Strategy of The Republic of Croatia. K dispozici na adrese: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.

Vláda Irské republiky (2019) National Cyber Security Strategy. K dispozici na adrese: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.

Vláda Lotyšské republiky (2014) Cyber Security Strategy of Latvia. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

Vláda Maďarské republiky (2018) Strategy for the Security of Network and Information Systems. K dispozici na adrese: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse.

Vláda Nizozemského království (2018) National Cyber Security Agenda. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en.

Vláda Republiky Bulharsko (2015) National Cyber Security Strategy – Cyber-resistant Bulgaria 2020.

Vláda Rumunské republiky (2013) Cyber security strategy of Romania. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania.

Vláda Řecké republiky (2017) National Cyber Security Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view.

Vláda Slovenské republiky (2015) Cyber Security Concept of the Slovak Republic. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic.

Vláda Španělského království (2019) National Cyber Security Strategy. K dispozici na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en.

Wamala, D. F. (2011) „ITU National Cybersecurity Strategy Guide“. K dispozici na adrese: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

White, G. (2007) „The Community Cyber Security Maturity Model“, in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)

PŘÍLOHA C – DALŠÍ STUDOVANÉ CÍLE

Cíle podrobně uvedené níže byly prostudovány v rámci fáze analýzy podkladů a rozhovorů vedených agenturou ENISA. Následující cíle nejsou součástí vnitrostátního rámce pro posouzení schopností, nicméně objasňují témata, o nichž je přínosné diskutovat. V každé z následujících kapitol najdete vysvětlení pro vyřazení konkrétního cíle.

- Připravit odvětvové strategie kybernetické bezpečnosti
- Boj proti dezinformačním kampaním
- zajistit nejmodernější technologie (5G, UI, kvantová výpočetní technika…),
- zajistit svrchovanost v oblasti údajů a
- poskytnout pobídky pro rozvoj odvětví kybernetického pojištění.

Připravit odvětvové strategie kybernetické bezpečnosti

Přijetí konkrétních odvětvových strategií zaměřených na intervence a pobídky v cílovém odvětví bude jistě příčinou silnější decentralizované schopnosti. To platí zejména pro členské státy, jejichž OES se musí potýkat s různými rámci a nařízeními a kde vzhledem k transverzální povaze kybernetické bezpečnosti existuje mnoho závislostí. V některý členských státech běžně napočítáme desítky vnitrostátních úřadů a regulačních orgánů se znalostí specifik jednotlivých odvětví, které mají mandát prosazovat v těchto jednotlivých odvětvích konkrétní předpisy.

Například Dánsko spustilo šest cílených strategií zabývajících se činnostmi odvětví nejkritičtějších pro kybernetickou a informační bezpečnost, aby v oblasti kybernetické a informační bezpečnosti vznikla silnější decentralizovaná schopnost. Každá „odvětvová jednotka“ se bude podílet mimo jiné na posuzování hrozeb na odvětvové úrovni, sledování, prováděni připravenosti, tvorbě bezpečnostních systémů, sdílení znalostí a pokynech. Tyto konkrétní odvětvové strategie se týkají následujících odvětví:

- energetika,
- zdravotní péče,
- doprava,
- telekomunikace,
- finance a
- námořní odvětví.

Další členské státy vyjádřily zájem o zvážení konkrétních odvětvových strategií v oblasti kybernetické bezpečnosti, aby byly zohledněny všechny požadavky právních předpisů. Nicméně je třeba poznamenat, že tento cíl nemusí být vhodný pro všechny členské státy vzhledem k jejich velikosti, vnitrostátním politikám a vyspělosti. Velké potíže se zajištěním, aby tento rámec zahrnoval všechna specifika, způsobily, že agentura ENISA tento cíl do rámce nezahrnula.

Boj proti dezinformačním kampaním

Členské státy zahrnují do svých národních strategií kybernetické bezpečnosti základní principy, jakými jsou lidská práva, transparentnost a důvěra veřejnosti. To je velmi důležité zejména s ohledem na dezinformace, jež jsou šířeny prostřednictvím tradičních zpravodajských médií i sociálních sítí. Kromě toho je kybernetická bezpečnost v současnosti jednou z nejvýznamnější

volebních výzev. Činnosti jako šíření nepravdivých informací nebo negativní propaganda jsou před důležitými volbami pozorovány v mnoha zemích. Tato hrozba disponuje potenciálem k narušení demokratického procesu v EU. Komise navrhla na evropské úrovni akční plán[32] pro zesílení boje proti dezinformacím v Evropě: tento plán se zaměřuje na čtyři klíčové oblasti (odhalování, spolupráce, spolupráce s on-line platformami a povědomí) a slouží jako základ pro rozvoj schopností EU a spolupráce mezi členskými státy.

Čtyři z devatenácti zemí při rozhovorech vyjádřily svůj úmysl zabývat se otázkou boje proti dezinformacím a propagandě ve svých NCSS.

Například francouzská NCSS[33] uvádí, že: „je úkolem státu informovat občany o rizicích manipulace a technik propagandy používaných zločinnými subjekty na internetu. Například po teroristických útocích ve Francii v lednu 2015 vytvořila vláda informační platformu o rizicích spojených s islámskou radikalizací prostřednictvím elektronických komunikačních sítí: « Stop-djihadisme.gouv.fr ».“ Tento přístup by mohl být rozšířen, aby reagoval i na další projevy propagandy a destabilizace.

V dalším příkladu polská NCSS pro období 2019–2024 NCSS[34] uvádí, že: „jsou proti manipulativním aktivitám, například dezinformačním kampaním, nutná systémová opatření, aby se zvyšovalo povědomí občanů v kontextu ověřování autenticity informací a reakce na pokusy o jejich zkreslování.“

Ovšem během rozhovorů s agenturou ENISA několik členských států uvedlo, že tuto problematiku neřeší v rámci svých NCSS jako hrozbu kybernetické bezpečnosti, ale zabývají se jí spíš na širší společenské úrovni, například prostřednictvím politických iniciativ.

Zajistit nejmodernější technologie (5G, UI, kvantová výpočetní technika…)

Protože se formy současných kybernetických hrozeb nadále rozšiřují, způsobí rozvoj nových technologií pravděpodobně nárůst intenzity a počtu kybernetických útoků a rozmanitosti metod, prostředků a cílů jejich aktérů. Současně mají tato nová technologická řešení v podobě nejmodernějších technologií potenciál stát se stavebními bloky evropského digitálního trhu. Aby byla zaručena nadále se zvyšující digitální závislost členských států a vznik nových technologií, je třeba vytvořit pobídky a komplexní politiky podporující bezpečný a důvěryhodný rozvoj a využívání těchto technologií v EU.

Během fáze analýzy podkladů týkající se NCSS členských států se jako zajímavé pro členské státy ukázaly následující nejmodernější technologie: 5G, UI, kvantová výpočetní technika, kryptografie, zpracování dat na vstupním zařízení, vozidla připojená k internetu a autonomní vozidla, data velkého objemu a inteligentní data, blockchain, robotika a internet věcí.

Konkrétněji na začátku roku 2020 Evropská komise zveřejnila sdělení vzývající členské státy, aby podnikly kroky k provedení souboru opatření doporučených v závěrech souboru nástrojů 5G[35]. Tento soubor nástrojů 5G přichází v návaznosti na doporučení (EU) 2019/534 o kybernetické bezpečnosti sítí 5G, přijatého Komisí v roce 2019, které požaduje jednotný evropský přístup k zabezpečení sítí 5G[36].

Během rozhovorů vedených agenturou ENISA bylo zdůrazněno, že je toto téma spíše transverzálním tématem řešeným v NCSS než samostatným konkrétním cílem.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation.
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf.
[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission.
[36] https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32019H0534&from=EN.

Zajistit svrchovanost v oblasti údajů

Kyberprostor je možné vnímat na jedné straně jako obrovský společný prostor, který je snadno přístupný a poskytuje vysokou míru konektivity a možnost využívání skvělých příležitostí k sociálnímu a hospodářskému růstu. Na druhé straně je kyberprostor charakterizován slabou jurisdikcí, obtížným přiřazováním akcí, absencí hranic a propojenými systémy, které mohou být propustné a jejichž data mohou být odcizena, nebo k nim dokonce mohou mít přístup cizí vlády. Kromě těchto dvou hledisek se digitální ekosystém vyznačuje koncentrací platforem a infrastruktury on-line služeb do rukou jen několika málo zúčastněných stran. Všechny výše uvedené aspekty vedou členské státy k podpoře digitální suverenity. Dosažení digitální suverenity znamená, že budou občané i podniky moci bez omezení prosperovat s pomocí využívání digitálních služeb a produktů IKT, jež budou důvěryhodné a nikdo se nebude muset obávat o své osobní údaje, digitální majetek, ekonomickou nezávislost nebo politický vliv.

Svrchovanost v oblasti údajů nebo digitální suverenitu hájí členské státy na vnitrostátní i evropské úrovni. Přestože se nezdá, že by členské státy tuto problematiku zahrnuly do svých NCSS jako konkrétní cíl, zabývají se jí buď jako transverzálním principem, nebo vyhlašují svůj záměr zajistit digitální suverenitu na vnitrostátní úrovni v jednorázových publikacích a se zaměřením na klíčové technologie. Například v roce 2018 bylo ve francouzském strategickém přezkumu kybernetické obrany uvedeno, že „pro zajištění digitální suverenity má klíčový význam kontrola těchto technologií: šifrování komunikace, odhalování kybernetických útoků, profesionální mobilní vysílání, cloudová výpočetní technika a umělá inteligence“[37].

Na evropské úrovni se členské státy aktivně podílejí na definování evropské strategie pro data (COM/2020/66 final) a přípravě evropského rámce certifikace pro IKT, digitální produkty, služby a procesy stanoveného aktem EU o kybernetické bezpečnosti (2019/881), který má zajistit strategickou digitální autonomii na evropské úrovni.

Fáze rozhovorů s členskými státy ukázala, že je téma digitální suverenity často považováno za otázku, která je širší, než aby se omezovala pouze na kybernetickou bezpečnost. Členské státy proto nezahrnují toto téma do svých NCSS a těch několik málo, které tak učinily, je nepovažují za samostatný konkrétní cíl.

Poskytovat pobídky pro rozvoj odvětví kybernetického pojištění

Aktuální stav v odvětví kybernetického pojištění ukazuje, že globální trh nezpochybnitelně roste. Stále se však nachází pouze na začátku, protože musí být shromážděny údaje a musí být stanoveno ještě mnoho precedentů (např. tiché krytí, systémová kybernetická rizika...). Kromě toho jsou odhadované ztráty agregované na základě celosvětových kybernetických útoků o několik řádů vyšší než aktuální schopnost krytí tohoto odvětví (pracovní dokument Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). Rozvoj kybernetického pojištění nicméně může jistě přinést výhody a položit základy silných mechanismů. Mechanismy kybernetického pojištění mohou pomáhat při:

- zvyšování povědomí o kybernetických bezpečnostních rizicích ve společnostech,
- kvantitativním hodnocení vystavení kybernetickým rizikům,
- zlepšování řízení kybernetických bezpečnostních rizik,
- poskytování podpory organizacím, jež se stanou oběťmi kybernetických útoků, a
- nahrazování škod (hmotných či jiných) způsobených kybernetickými útoky.

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf.

Některé členské státy se již začaly tomuto tématu věnovat. Například:

- Estonsko přijalo ve své NCSS přístup „počkat a vidět“: „Kvůli obecnému zmírnění kybernetických rizik v soukromém sektoru bude v Estonsku na tomto základě analyzována poptávka a nabídka služeb kybernetického pojištění, budou sjednány zásady spolupráce dotčených subjektů, včetně sdílení informací, přípravy posouzení rizik atd. Dnes na estonském trhu působí jen několik málo poskytovatelů služeb kybernetického pojištění a prvním úkolem je zjistit, kdo a co nabízí. Za překážku rozvoje trhu s kybernetickým pojištěním je často považována složitost pojišťovací ochrany.“
- Rozvoj kybernetického pojištění ve své NCSS konkrétně podporuje Lucembursko: „Cíl 1: Vytváření nových produktů a služeb. Kvůli rozložení rizik a vybízení obětí digitálních kybernetických incidentů, aby při řešení incidentu a obnově systému postiženého zločinným jednáním hledaly odbornou pomoc, budou pojišťovací společnosti nabádány, aby vytvářely konkrétní produkty v oblasti kybernetického pojištění.“

Zpětná vazba respondentů byla ohledně tohoto tématu velmi rozmanitá: některé členské státy uvedly, že se kybernetické pojištění nedávno stalo předmětem diskuse, přičemž jiné konstatovaly, že i když je toto téma slibné, odvětví není dosud dostatečně vyzrálé. Velký počet respondentů však uvedl, že se tímto tématem nezabývají jejich NCSS, a to buď proto, že je považováno za příliš specifické, nebo nenáleží do rámce NCSS.

TP-02-21-253-CS-N

O agentuře ENISA – Agentuře Evropské unie pro kybernetickou bezpečnost

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) je agenturou Unie, která usiluje o dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Evropě. Agentura Evropské unie pro kybernetickou bezpečnost, která byla zřízena v roce 2004 a následně posílena aktem EU o kybernetické bezpečnosti, se podílí na kybernetické politice EU, prostřednictvím systémů certifikace kybernetické bezpečnosti zvyšuje důvěryhodnost produktů, služeb a procesů IKT, spolupracuje s členskými státy a subjekty EU a pomáhá Evropě připravit se na budoucí kybernetické výzvy. Sdílením znalostí, budováním schopností a zvyšováním povědomí usiluje agentura společně s hlavními zúčastněnými stranami o posílení důvěry v propojenou ekonomiku, o podporu odolnosti infrastruktury Unie, a především o zajištění digitální bezpečnosti evropské společnosti a občanů. Více informací viz www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-473-2
DOI: 10.2824/200111