EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NÁRODNÝ HODNOTIACI RÁMEC SPÔSOBILOSTÍ

DECEMBER 2020

O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúra Únie, ktorej úlohou je zabezpečovať vysokú spoločnú úroveň kybernetickej bezpečnosti v Európe. Agentúra EÚ, ktorá bola zriadená v roku 2004 a ktorej postavenie posilnil akt EÚ o kybernetickej bezpečnosti, prispieva k vytváraniu kybernetickej politiky EÚ a pomocou systémov certifikácie kybernetickej bezpečnosti zvyšuje dôveryhodnosť produktov, služieb a procesov IKT, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy v budúcnosti. Agentúra prostredníctvom spoločného využívania vedomostí, budovania kapacít a zvyšovania informovanosti spolupracuje s kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v rámci prepojenej ekonomiky, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zachovať digitálnu bezpečnosť európskej spoločnosti a občanov Európy. Viac informácií nájdete na stránke www.enisa.europa.eu.

KONTAKT

Na kontaktovanie autorov použite adresu team@enisa.europa.eu.
Pre otázky médií týkajúcich sa tohto dokumentu použite adresu press@enisa.europa.eu.

AUTORI

Anna Sarri, Pinelopi Kyranoudi – Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

POĎAKOVANIE

Agentúra ENISA by rada poďakovala a vyjadrila uznanie všetkým odborníkov, ktorí sa podieľali na tejto správe a poskytli hodnotné informácie, a to najmä týmto subjektom uvedenom v abecednom poradí:

Centrálny štátny úrad pre rozvoj digitálnej spoločnosti (Maďarsko), Marin Ante Pivcevic

Centrum pre kybernetickú bezpečnosť (Belgicko)

CFCS – Center for Cybersikkerhed (Denmark), Thomas Wulff

Divízia pre zásady kybernetickej bezpečnosti, Oddelenie životného prostredia, klímy a komunikácie (Írsko), James Caffrey

Európske centrum boja proti počítačovej kriminalite – EC3, Adrian-Ionut Bobeica

Európske centrum boja proti počítačovej kriminalite – EC3, Alzofra Martinez Alvaro

Maltská agentúra pre informačné technológie (Malta), Katia Bonello a Martin Camilleri

Ministerstvo digitálnej politiky (Grécko), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali a Sotiris Vasilos

Ministerstvo ekonomických záležitostí a komunikácie (Estónsko), Anna-Liisa Pärnalaas

Ministerstvo spravodlivosti a verejnej bezpečnosti (Nórsko), Robin Bakke

Národné bezpečnostné oddelenie (Španielsko), Maria Mar Lopez Gil

Národný bezpečnostný úrad (Slovensko)

Národný úrad pre kybernetickú a informačnú bezpečnosť (Česká republika), Veronika Netolická

NCTV, Ministerstvo spravodlivosti a bezpečnosti (Holandsko)

Portugalské národné centrum kybernetickej bezpečnosti (Portugalsko), Alexandre Leite a Pedro Matos

Spolkové ministerstvo vnútra (Nemecko), Sascha-Alexander Lettgen

Správa bezpečnosti informácií (Slovinská republika), Marjan Kavčič

Talianska vláda (Taliansko)

Univerzita v Oxforde – Centrum pre globálnu kybernetickú bezpečnosť Carolin Weisser Harris

Agentúra ENISA by takisto rada poďakovala všetkým odborníkom, ktorí poskytli údaje, ale uprednostnili anonymitu, za ich neoceniteľný príspevok do tejto štúdie.

PRÁVNE OZNÁMENIA

Je potrebné oznámiť, že toto vydanie predstavuje názory a interpretácie agentúry ENISA, pokiaľ nie je uvedené inak. Tento dokument by sa nemal považovať za právny krok agentúry ENISA alebo jej orgánov, pokiaľ nie je prijatý v súlade s nariadením (EÚ) č. 2019/881.
Tento dokument nevyhnutne nepredstavuje súčasný stav vývoja a agentúra ENISA ho môže z času na čas aktualizovať.

Zdroje tretích strán sú príslušným spôsobom uvedené. Agentúra ENISA nie je zodpovedná za obsah externých zdrojov, vrátane externých webových stránok, na ktoré tento dokument odkazuje.

Tento dokument je určený len na informačné účely. Musí byť dostupný zadarmo. Agentúra ENISA ani iná osoba, ktorá koná v jej mene, nenesú zodpovednosť za využitie informácií uvedených v tomto dokumente.

OZNÁMENIE TÝKAJÚCE SA AUTORSKÉHO PRÁVA

ISBN: 978-92-9204-486-2

DOI: 10.2824/978297

KATALÓG: TP-02-21-253-SK-N

1. OBSAH

GLOSÁR S POJMAMI

AKRONYM	VYMEDZENIE
AI	Umelá inteligencia
C2M2	Cybersecurity Capability Maturity Model (model zrelosti spôsobilosti kybernetickej bezpečnosti)
CCRA	Common Criteria Recognition Arrangement (Spoločná dohoda o uznávaní kritérií)
CCSMM	The Community Cybersecurity Maturity Model (model zrelosti kybernetickej bezpečnosti spoločenstva)
CII	Critical Information Infrastructure (kritická informačná infraštruktúra)
CMM	Cybersecurity Capacity Maturity Model for Nations (model zrelosti schopnosti kybernetickej bezpečnosti pre národy)
CMMC	Cybersecurity Maturity Model Certification (certifikácia modelu zrelosti kybernetickej bezpečnosti)
CPI	Cyber Power Index (index kybernetickej moci)
CSIRT	Computer Security Incident Response Teams (jednotky pre riešenie počítačových bezpečnostných incidentov)
CVD	Coordinated Vulnerability Disclosure (koordinované zverejňovanie informácií o zraniteľnosti)
DPA	Data Protection Act (zákon o ochrane osobných údajov)
DSM	Digital Single Market (jednotný digitálny trh)
ECCG	European Cybersecurity Certification Group (Európska skupina pre certifikáciu kybernetickej bezpečnosti)
ECSM	European Cybersecurity Month (európsky mesiac kybernetickej bezpečnosti)
ECSO	European Cyber Security Organisation (Európska organizácia kybernetickej bezpečnosti)
EKR	Európsky kvalifikačný rámec
EÚ	Európska únia
EZVO	Európske združenie voľného obchodu
GCI	Global Cybersecurity Index (globálny index kybernetickej bezpečnosti)
GDPR	Všeobecné nariadenie o ochrane údajov
GDS	Government Digital Service (vládna digitálna služba)
IA-CM	Internal Audit Capability Model for the Public Sector (model spôsobilosti vnútorného auditu pre verejný sektor)
IKT	Informačné a komunikačné technológie

ISMM	Information Security Maturity Model for NIST Cybersecurity Framework (model zrelosti bezpečnosti informácií pre rámec kybernetickej bezpečnosti NIST)
ITU	International Telecommunication Union (Medzinárodná telekomunikačná únia)
LEA	Law Enforcement Agency (orgán presadzovania práva)
MS	Member State (členský štát)
MSP	Malé a stredné podniky
NCSS	National Cybersecurity Strategies (národné stratégie kybernetickej bezpečnosti)
NIS	Network and Information Security (bezpečnosť sietí a informačných systémov)
NIST	National Institute of Standards and Technology (Národný inštitút pre normy a technológie)
NLO	National Liaison Officers (národní styční úradníci)
OES	Operators of Essential Services (prevádzkovatelia základných služieb)
OT	Operations Technology (prevádzková technológia)
PET	Privacy Enhancing Technologies (technológie na zvyšovanie súkromia)
PIMS	Privacy Information Management System (systém riadenia informácií o súkromí)
PPP	Public-private partnerships (verejno-súkromné partnerstvá)
Q-C2M2	Qatar Cybersecurity Capability Maturity Model (katarský model zrelosti spôsobilosti kybernetickej bezpečnosti)
R&D	Research & Development (výskum a vývoj)
SOG-IS MRA	Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement (skupina vedúcich pracovníkov pre bezpečnosť informačných systémov, dohoda o vzájomnom uznávaní)

ZHRNUTIE

Keďže momentálne podmienky kybernetických hrozieb stále silnejú a intenzita a počet kybernetických útokov sa stále zvyšuje, musia členské štáty EÚ efektívne reagovať ďalším vývojom a prispôsobovaním svojich národných stratégií kybernetickej bezpečnosti (NCSS). Od zverejnenia svojich prvých štúdií týkajúcich sa NCSS agentúrou ENISA v roku 2012, urobili členské štáty EÚ a krajiny EZVO obrovský pokrok vo vývoji a implementovaní svojich stratégií.

Táto správa predstavuje činnosti realizované agentúrou ENISA na vytvorenie národného hodnotiaceho rámca spôsobilostí (NCAF).

Cieľom rámca je poskytnúť členským štátom sebahodnotenie svojej úrovne zrelosti pomocou zhodnotenia ich cieľov NCSS, ktoré im pomôžu zlepšiť a vybudovať spôsobilosti kybernetickej bezpečnosti na strategickej aj prevádzkovej úrovni.

Opisuje jednoduchý reprezentatívny prehľad úrovne zrelosti kybernetickej bezpečnosti členských štátov. NCAF je nástrojom, ktorý pomôže členským štátom:

- Poskytnúť užitočné informácie pre rozvoj dlhodobej stratégie (napr. osvedčené postupy, usmernenia);
- Identifikovať chýbajúce prvky v rámci NCSS;
- Ďalej budovať spôsobilosti kybernetickej bezpečnosti;
- Prebrať zodpovednosť za politické kroky;
- Vniesť dôveryhodnosť smerom k širokej verejnosti a medzinárodným partnerom;
- Presiahnuť a vylepšiť verejný obraz ako transparentnej organizácie;
- Pripraviť sa na očakávané problémy;
- Identifikovať naučené lekcie a osvedčené posty;
- Vytvoriť východiskový bod pre postavenie kybernetickej bezpečnosti v rámci EÚ na uľahčenie diskusie a
- Vyhodnotiť národné spôsobilosti týkajúce sa kybernetickej bezpečnosti.

Tento rámec bol navrhnutý s podporou odborníkov na túto tému z agentúry ENISA a zástupcov z 19 členských štátov a krajín EZVO[1]. Cieľovou skupinou tejto správy sú politickí činitelia, odborníci a vládni úradníci zodpovední za alebo zapojení do navrhovania, implementovania a hodnotenia NCSS a, v širšej rovine, spôsobilostí kybernetickej bezpečnosti.

[1] Na rozhovoroch sa zúčastnili zástupcovia z týchto členských štátov a krajín EZVO: Belgicko, Chorvátsko, Česká republika, Dánsko, Estónsko, Nemecko, Grécko, Maďarsko, Írsko, Taliansko, Lichtenštajnsko, Malta, Holandsko, Nórsko, Portugalsko, Slovensko, Slovinsko, Španielsko, Švédsko.

Národný hodnotiaci rámec spôsobilostí zahŕňa 17 strategických cieľov a je štruktúrovaný do štyroch hlavných klastrov:

- Klaster č. 1: Riadenie a normy kybernetickej bezpečnosti
    1. Rozvoj národného kybernetického pohotovostného plánu
    2. Vytvorenie východiskových bezpečnostných opatrení
    3. Zaistenie digitálnej identity a vybudovanie dôvery vo verejné digitálne služby

- Klaster č. 2: Budovanie kapacít a povedomie
    4. Organizovanie cvičení v oblasti kybernetickej bezpečnosti
    5. Stanovenie spôsobilosti na reakciu na incidenty
    6. Zvýšenie informovanosti používateľov
    7. Posilnenie školiacich a vzdelávacích programov
    8. Podpora výskumu a vývoja
    9. Poskytnutie stimulov pre investície súkromného sektora do bezpečnostných opatrení
    10. Zlepšenie kybernetickej bezpečnosti dodávateľskej siete

- Klaster č. 3: Právne a zmluvné záležitosti
    11. Ochrana kritickej informačnej infraštruktúry, prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb
    12. Riešenie kybernetickej kriminality
    13. Vytvorenie mechanizmov nahlasovania incidentov
    14. Posilnenie ochrany súkromia a osobných údajov

- Klaster č. 4: Spolupráca
    15. Vytvorenie verejno-súkromného partnerstva
    16. Inštitucionalizovanie spolupráce medzi štátnymi orgánmi
    17. Zapojenie sa do medzinárodnej spolupráce

1. ÚVOD

V smernici o bezpečnosti sietí a informačných systémov (NIS), zverejnená v júli 2016, sa vyžaduje, aby členské štáty EÚ prijali národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov, ktorá sa tiež nazýva NCSS (Národná stratégia kybernetickej bezpečnosti) tak, ako sa stanovuje v článkoch 1 a 7. V tomto kontexte je NCSS definovaná ako rámec, ktorý určuje strategické princípy, usmernenia, strategické ciele, priority, vhodné postupy a regulačné opatrenia. Predvídaným cieľom NCSS je dosiahnuť a zachovať vysokú úroveň bezpečnosti sietí a systémov, a tým umožniť členským štátom zmierniť riziko potenciálnych hrozieb. NCSS okrem toho môže byť aj katalyzátorom priemyselného rozvoja a ekonomického a sociálneho pokroku.

Akt o kybernetickej bezpečnosti EÚ hovorí, že agentúra ENISA bude propagovať rozširovanie osvedčených postupov pri definovaní a implementovaní NCSS vo forme podpory členských štátov pri schvaľovaní smernice a zhromažďovaní hodnotnej spätnej väzby o svojich skúsenostiach. Na tento účel vyvinula agentúra ENISA niekoľko nástrojov, ktoré pomôžu členským štátom pri vývoji, implementovaní a hodnotení národných stratégií kybernetickej bezpečnosti (NCSS).

Ako súčasť svojho mandátu sa agentúra ENISA zameriava na národný rámec sebahodnotenia spôsobilostí, aby zhodnotila úroveň zrelosti rôznych NCSS. Cieľom tejto správy je predstaviť štúdiu realizovanú pri definovaní rámca sebahodnotenia.

1.1 ROZSAH PÔSOBNOSTI ŠTÚDIE

Hlavným cieľom tejto štúdie je vytvoriť národný rámec sebahodnotenia spôsobilostí, ďalej v texte len ako NCAF, na zmeranie úrovne zrelosti spôsobilostí kybernetickej bezpečnosti členských štátov. Konkrétnejšie by tento rámec mal umožniť členským štátom:

- vykonávať hodnotenie svojich národných spôsobilostí kybernetickej bezpečnosti;
- zvýšiť informovanosť o úrovni zrelosti krajiny;
- identifikovať oblasti na zlepšenie; a
- vytvoriť spôsobilosti kybernetickej bezpečnosti.

Tento rámec by mal pomôcť členským štátom a najmä národným politickým činiteľom pri realizácii sebahodnotenia s cieľom zlepšiť spôsobilosti v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni.

1.2 METODOLOGICKÝ PRÍSTUP

Metodologický prístup použitý pri budovaní rámca sebahodnotenia národných spôsobilostí je založený na štyroch hlavných krokoch:

1. **Teoretický prieskum**: Prvý krok zahŕňal rozsiahly prehľad literatúry v rámci zhromažďovania osvedčených postupov týkajúcich sa tvorby hodnotiaceho rámca zrelosti pre národné stratégie kybernetickej bezpečnosti. Sekundárny prieskum sa zameriava na systematickú analýzu relevantných dokumentov o budovaní kapacít kybernetickej bezpečnosti a definovaní stratégie, na existujúce NCSS v členských štátoch a na porovnanie existujúcich modelov zrelosti kybernetickej bezpečnosti. Vykonávanie cvičenia referenčného porovnávania existujúcich modelov zrelosti sa realizovalo prijatím rámca analýzy, ktorá vznikla na účely tejto štúdie. Rámec analýzy

je založený na Beckerovej[2] metodológii pre tvorbu modelov zrelosti, ktorá určuje všeobecný a konsolidovaný model postupov pre navrhovanie modelov zrelosti a stanovuje jasné požiadavky na tvorbu modelov zrelosti. Rámec analýzy sa ďalej prispôsobil tak, aby spĺňal potreby tejto štúdie.

2. **Zber názorov odborníkov a zainteresovaných strán**: Na základe údajov získaných zo sekundárneho prieskumu a súvisiacich predbežných zistení analýzy zahŕňala táto fáza identifikovanie odborníkov, ktorí majú skúsenosti pri tvorbe a implementácii NCSS alebo modelov zrelosti, a ich pozvanie na pohovor. Agentúra ENISA kontaktovala expertnú skupinu pre národné stratégie kybernetickej bezpečnosti a národných styčných úradníkov (NLO), aby našla v každom členskom štáte relevantných odborníkov. Okrem toho prebehli rozhovory s niektorými odborníkmi zapojenými do tvorby modelov zrelosti. Celkovo sa uskutočnilo 22 pohovorov, z ktorých 19 sa realizovalo so zástupcami agentúr pre kybernetickú bezpečnosť v rôznych členských štátoch (a krajinách EZVO).
3. **Analýza údajov o zhodnotení aktuálnej situácie:** Údaje zozbierané pomocou sekundárneho prieskumu a rozhovorov sa následne analyzovali, aby sa určili osvedčené postupy pri navrhovaní rámca sebahodnotenia na zmeranie zrelosti NCSS, na pochopenie potrieb členských štátov a na určenie toho, ktoré údaje je možné zbierať v rôznych európskych krajinách[3]. Táto analýza umožnila doladenie predbežného modelu vytvoreného v predchádzajúcich krokoch a vycibrenie súboru indikátorov, ktoré sú súčasťou modelu, úrovní zrelosti a ich rozmerov.
4. **Ukončenie modelu:** Potom odborníci na danú problematiku agentúry ENISA posúdili aktualizovanú verziu národného rámca sebahodnotenia spôsobilostí, ktorej platnosť následne potvrdili odborníci na seminári, ktorý sa uskutočnil v októbri 2020 pred jej zverejnením.

1.3 CIEĽOVÁ SKUPINA

Cieľovou skupinou tejto správy sú politickí činitelia, odborníci a vládni úradníci zodpovední za alebo zapojení do navrhovania, implementovania a hodnotenia NCSS a, v širšej rovine, spôsobilostí kybernetickej bezpečnosti. Okrem toho môžu byť zistenia formálne schválené v tomto dokumente hodnotné pre výskumníkov a odborníkov na stratégiu kybernetickej bezpečnosti na národnej alebo európskej úrovni.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213 – 222, Jun. 2009.
[3] Na účely tohto prieskumu zahŕňajú „európske krajiny, na ktoré sa v tejto správe odkazuje, 27 členských štátov EÚ.

2. ZÁKLADNÉ INFORMÁCIE

2.1 PREDCHÁDZAJÚCA PRÁCA NA ŽIVOTNOM CYKLE NCSS

Ako je uvedené v akte o kybernetickej bezpečnosti EÚ, jedným z hlavných cieľov agentúry ENISA je podpora členských štátov pri vytváraní národných stratégií v oblasti bezpečnosti sietí s informačných systémov, podpora rozširovania týchto stratégií a monitorovanie ich implementovania. Ako súčasť svojho mandátu zostavila agentúra ENISA niekoľko dokumentov týkajúcich sa tejto problematiky, aby podporila implementáciu NCSS v rámci celej EÚ:

- „Praktická príručka k fáze tvorby a realizácii NCSS“[4] zverejnená v roku 2012
- Dokument „Stanovenie kurzu pre národné snahy o posilnenie bezpečnosti v kybernetickom priestore“[5] zverejnený v roku 2012
- Prvý rámec agentúry ENISA pre hodnotenie NCSS členského štátu zverejnený[6] v roku 2014.
- „Online interaktívna mapa NCSS“[7] zverejnená v roku 2014.
- „Príručka osvedčených postupov NCSS“[8] zverejnená v roku 2016.
- „Hodnotiaci nástroj národných stratégií kybernetickej bezpečnosti“[9] zverejnený v roku 2018.
- „Osvedčené postupy pri inovovaní kybernetickej bezpečnosti podľa NCSS“[10] zverejnené v roku 2019.

PRÍLOHA A obsahuje krátky súhrn najdôležitejších publikácií agentúry ENISA k tejto téme.

Vyššie spomenuté príručky a dokumenty sa preštudovali ako súčasť teoretického prieskumu. Hlavným prvkom NCAF je najmä dokument „Hodnotiaci nástroj stratégií kybernetickej bezpečnosti“[11]. NCAF je založený na cieľoch, ktoré sú zahrnuté v online hodnotiacom nástroji NCSS.

[4] NCSS: Praktická príručka k tvorbe a realizácii (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Stanovenie kurzu pre národné snahy o posilnenie bezpečnosti v kybernetickom priestore (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] Hodnotiaci rámec pre NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] Národné stratégie kybernetickej bezpečnosti – interaktívna mapa (ENISA, 2014, aktualizované v roku 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Tento dokument je aktualizáciou príručky z roku 2012: Príručka osvedčených postupov NCSS: Navrhovanie a implementovanie národných stratégií kybernetickej bezpečnosti (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] Hodnotiaci nástroj národných stratégií kybernetickej bezpečnosti (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] Hodnotiaci nástroj národných stratégií kybernetickej bezpečnosti (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 SPOLOČNÉ CIELE IDENTIFIKOVANÉ V RÁMCI EURÓPSKEJ NCSS

Rozdiely medzi členskými štátmi komplikujú identifikovanie spoločných aktivít alebo akčných plánov v rámci rôznych národných kontextov, právnych rámcov a politických agend. NCSS členských štátov ale majú často strategické ciele, ktoré sú spojené s rovnakými témami. Na základe predchádzajúcej práce agentúry ENISA a analýzy NCSS členských štátov sa preto identifikovalo 22 strategických cieľov. 15 z týchto cieľov už bolo identifikovaných v predchádzajúcej práci agentúry ENISA, 2 ciele sa do tejto štúdie pridali ako nové a 5 cieľov sa určilo na zváženie v budúcnosti.

2.2.1 Spoločné strategické ciele členských štátov

Na základe predchádzajúcej práce agentúry ENISA, najmä dokumentu Hodnotiaci nástroj stratégií národnej kybernetickej bezpečnosti[12] je v tejto tabuľke uvedený vyššie spomenutý súbor 15 strategických cieľov, ktoré sú spoločné pre NCSS členských štátov. Ciele popisujú jadro celkovej „národnej filozofie“ k tejto téme. Ďalšie informácie o cieľoch uvedených nižšie nájdete v správe „Príručka osvedčených postupov NCSS“ agentúry ENISA[13].

Tabuľka 1: Spoločné strategické ciele členských štátov v ich NCSS

ID	Strategické ciele NCSS	Ciele
1	**Rozvoj národných kybernetických pohotovostných plánov**	▶ prezentovanie a vysvetlenie kritérií, ktoré by sa mali použiť pri definované situácie ako krízy; ▶ definovanie kľúčových procesov a krokov pri riešení krízy; a ▶ jasné definovanie úloh a povinností rôznych zainteresovaných strán počas kybernetickej krízy; ▶ prezentovanie a vysvetlenie kritérií ukončenia krízy a/alebo subjektu, ktorý má právomoc ju vyhlásiť.
2	**Vytvorenie východiskových bezpečnostných opatrení**	▶ harmonizovanie rôznych postupov, ktoré organizácie musia dodržať, vo verejnom aj súkromnom sektore; ▶ vytvorenie spoločného jazyka medzi kompetentnými verejnými orgánmi a organizáciami a otvorených zabezpečených komunikačných kanálov; ▶ možnosť pre rôzne zainteresované osoby kontrolovať a porovnávať svoje spôsobilosti kybernetickej bezpečnosti; ▶ poskytovanie informácií o osvedčených postupov kybernetickej bezpečnosti v každom priemyselnom sektore; a ▶ pomoc zainteresovaným osobám pri určovaní priorít ich investícií do bezpečnosti.
3	**Organizovanie cvičení v oblasti kybernetickej bezpečnosti**	▶ identifikovanie potrieb, ktoré je potrebné otestovať (plány a procesy, ľudia, infraštruktúra, schopnosti reakcie, schopnosti spolupráce, komunikácia atď.); ▶ stanovenie tímu plánovania cvičení v oblasti kybernetickej bezpečnosti s jasným mandátom; a ▶ integrovanie kybernetických cvičení do životného cyklu národnej stratégie kybernetickej bezpečnosti alebo národného kybernetického pohotovostného plánu.
4	**Stanovenie spôsobilosti na reakciu na incidenty**	▶ mandát – toto sa týka právomocí, úloh a povinností, ktoré musí príslušná vláda tímu udeliť; ▶ portfólio služieb – zahŕňa služby, ktoré tím poskytuje vo svojej oblasti pôsobenia alebo používa na svoje vlastné interné fungovanie; ▶ prevádzkové spôsobilosti – toto sa týka technických a prevádzkových požiadaviek, ktoré musí tím splniť; a

[12] Hodnotiaci nástroj národných stratégií kybernetickej bezpečnosti (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 je aktualizáciou príručky z roku 2012: Príručka osvedčených postupov NCSS: Navrhovanie a implementovanie národných stratégií kybernetickej bezpečnosti (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Strategické ciele NCSS	Ciele
		▶ spôsobilosti v rámci spolupráce – tie zahŕňajú požiadavky týkajúce sa poskytovania informácií iným tímom, ktoré nepatria do prvých troch kategórií, napr. politickí činitelia, armáda, regulačné orgány, prevádzkovatelia (kritickej informačnej infraštruktúry), orgány presadzovania práva.
5	Zvýšenie informovanosti používateľov	▶ identifikovanie medzier týkajúcich sa problémov kybernetickej bezpečnosti a bezpečnosti informácií; a ▶ vyplnenie týchto medzier prostredníctvom zvýšenia povedomia alebo rozvoja/posilnenia vedomostných základov.
6	Posilnenie školiacich a vzdelávacích programov	▶ zlepšenie prevádzkových spôsobilostí existujúcich zamestnancov bezpečnosti informácií; ▶ povzbudenie študentov k tomu, aby sa pridali a ich následná príprava na vstup do oblasti kybernetickej bezpečnosti; ▶ podpora a stimulovanie vzťahov medzi akademickými prostrediami kybernetickej bezpečnosti a odvetvím bezpečnosti informácií; a ▶ zladenie školenia o kybernetickej bezpečnosti s obchodnými potrebami.
7	Podpora výskumu a vývoja	▶ identifikovanie skutočných príčin zraniteľných miest namiesto nápravy ich vplyvu; ▶ spojenie vedcov z rôznych disciplín, ktorí poskytnú riešenia na viacdimenzionálne a komplexné problémy, ako napríklad fyzicko-kybernetické hrozby; ▶ spojenie potrieb odvetvia a zistení výskumu, a tým uľahčenie premeny z teórie na prax; a ▶ nájdete spôsobov, ktoré umožnia nie len udržiavať, ale aj zvyšovať úroveň kybernetickej bezpečnosti výrobkov a služieb, ktoré podporujú existujúcu kybernetickú infraštruktúru.
8	Poskytnutie stimulov pre investície súkromného sektora do bezpečnostných opatrení	▶ identifikovanie možných stimulov pre súkromné spoločnosti pre investovanie do bezpečnostných opatrení; a ▶ poskytnutie stimulov spoločnostiam v rámci podpory ich investovania do bezpečnosti.
9	Ochrana kritickej informačnej infraštruktúry, prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb (CII)	▶ identifikovanie kritickej informačnej infraštruktúry a ▶ identifikovanie a zníženie relevantných rizík na CII.
10	Riešenie kybernetickej kriminality	▶ vytvorenie zákonov v oblasti počítačovej kriminality a ▶ zvýšenie efektívnosti orgánov na presadzovanie práva.
11	Vytvorenie mechanizmov nahlasovania incidentov	▶ získanie vedomostí o celkovom prostredí hrozieb; ▶ zhodnotenie vplyvu incidentov (napr. narušenia bezpečnosti, zlyhania siete, prerušenia služieb); ▶ získanie vedomostí o existujúcich a nových zraniteľných miestach a typoch útokov; ▶ príslušná aktualizácia bezpečnostných opatrení; a ▶ implementovanie ustanovení smernice NIS o nahlasovaní incidentov.
12	Posilnenie ochrany súkromia a osobných údajov	▶ prispenie k posilneniu základných práv o ochrane súkromia a osobných údajov.
13	Vytvorenie verejno-súkromného partnerstva (PPP)	▶ odstrašenie (na odstrašenie útočníkov); ▶ ochrana (používa výskum nových informačných hrozieb); ▶ zisťovanie (používa zdieľanie informácií v rámci riešenia nových hrozieb); ▶ reakcia (poskytnutie spôsobilosti na riešenie prvotného dopadu incidentu); a ▶ zotavenie (poskytnutie spôsobilosti na riešenie konečného vplyvu incidentu).
14	Inštitucionalizovanie spolupráce medzi štátnymi orgánmi	▶ zlepšenie spolupráce medzi orgánmi s povinnosťami a kompetenciami súvisiacimi s kybernetickou bezpečnosťou; ▶ vyhýbanie sa prekrývaniu a kompetencií a zdrojov medzi verejnými orgánmi; a

ID	Strategické ciele NCSS	Ciele
		▶ zlepšenie a inštitucionalizovanie spolupráce medzi štátnymi orgánmi v rôznych oblastiach kybernetickej bezpečnosti.
15	Zapojenie sa do medzinárodnej spolupráce (nielen s členskými štátmi EÚ)	▶ získanie výhod z vytvorenia spoločnej vedomostnej základne medzi členskými štátmi EÚ; ▶ vytvorenie synergických efektov medzi národnými orgánmi kybernetickej bezpečnosti a ▶ umožnenie a zintenzívnenie boja proti nadnárodnému zločinu.

2.2.2 Ďalšie strategické ciele

Na základe uskutočneného sekundárneho prieskumu a rozhovorov, ktoré zorganizovala agentúra ENISA, boli identifikované ďalšie strategické ciele. Členské štáty sa vo svojich NCSS čoraz viac venujú týmto témam alebo definujú akčné plány k tej istej problematike. Takisto sú k dispozícii príklady aktivít implementovaných členskými štátmi. Ak pochádza príklad z verejne dostupného zdroja, je k dispozícii referencia. V prípadoch, v ktorých sú príklady založené na dôverných rozhovoroch úradníkmi členských štátov EÚ, nie je referencia k dispozícii.

Boli identifikované tieto ďalšie strategické ciele:

- zlepšenie kybernetickej bezpečnosti dodávateľskej siete a
- zaistenie digitálnej identity a vybudovanie dôvery vo verejné digitálne služby.

Zlepšenie kybernetickej bezpečnosti dodávateľskej siete

Malé a stredné podniky (MSP) sú oporou európskej ekonomiky. Prestavujú 99 % všetkých podnikov v EÚ[14] a v roku 2015 vznikol odhad, že malé a stredné podniky vytvorili približne 85 % nových pracovných pozícií a dve tretiny celkovej miery zamestnanosti v súkromnom sektore v EÚ. Keďže malé a stredné podniky poskytujú služby veľkým spoločnostiam a stále vo väčšej miere pracujú s verejnými správami[15], je potrebné mať na pamäti, že v dnešnom prepojenom kontexte sú malé a stredné podniky slabým článkom pre kybernetické útoky. Malé a stredné podniky sú skutočne najviac vystavené kybernetickým útokom, napriek tomu si nemôžu dovoliť adekvátne investovať do kybernetickej bezpečnosti[16]. Zvýšenie kybernetickej bezpečnosti dodávateľskej siete by sa preto malo uskutočňovať so zameraním sa na malé a stredné podniky.

Okrem tohto systematického prístupu môžu členské štáty svoje snahy zamerať na kybernetickú bezpečnosť konkrétnych IKT služieb a produktov, ktoré sa považujú za nevyhnutné: IKT technológie používané v kritickej informačnej infraštruktúre, bezpečnostné mechanizmy vynútené v telekomunikačnom sektore (kontroly na úrovni ISP…), dôveryhodné služby podľa definície nariadenia eIDAS a poskytovatelia cloudových služieb. Napríklad Poľsko sa vo svojej národnej kybernetickej stratégii na roky 2019 – 2024[17] zaviazalo vytvoriť hodnotiaci a certifikačný systém národnej kybernetickej bezpečnosti, ktorý bude slúžiť ako mechanizmus na zabezpečovanie kvality v dodávateľskej sieti. Tento certifikačný systém bude v súlade

[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

s certifikačným rámcom EÚ pre digitálne IKT produkty, služby a procesy ustanovené v akte o kybernetickej bezpečnosti EÚ (2019/881).

Zlepšenie kybernetickej bezpečnosti dodávateľskej siete je preto zásadne dôležité. Toto je okrem iného možné dosiahnuť stanovením silných stratégií na podporu malých a stredných podnikov, poskytnutím usmernení pre požiadavky kybernetickej bezpečnosti v procesoch obstarávania vo verejnej správe, podporou spolupráce v rámci súkromného sektora, tvorbou PPP vzťahov, podporou koordinovaných mechanizmov zverejňovania informácií o zraniteľnosti (CVD)[18], vytvorením certifikačnej schémy produktov, vrátane komponentov kybernetickej bezpečnosti v digitálnych iniciatívach pre malé a stredné podniky a financovaním rozvoja zručností.

Zaistenie digitálnej identity a vybudovanie dôvery vo verejné digitálne služby

Vo februári 2020 predstavila Komisia v správe „Formovanie digitálnej budúcnosti Európy“ svoju víziu pre digitálnu transformáciu EÚ[19] s cieľom poskytnutia inkluzívnych technológií, ktoré pracujú pre ľudí a dodržiavajú základné hodnoty EÚ. Správa hovorí najmä o tom, že podpora digitálnej transformácie verejných správ v Európe je zásadná. V tomto zmysle je najdôležitejšie budovanie dôvery vo vládu vzhľadom na digitálnu identitu a dôveru vo verejné služby. Toto je dokonca dôležitejšia pri zohľadnení skutočnosti, že výmeny údajov a transakcie verejného sektora sú často citlivej povahy.

Svoje zámer venovať sa tejto téme vo svojich NCSS vyjadrili mnohé krajiny, medzi nimi napríklad: Dánsko, Estónsko, Francúzsko, Luxembursko, Malta, Španielsko, Holandsko a Spojené kráľovstvo. Niektoré z týchto krajín sa tiež vyjadrili, že tento strategický cieľ môže byť pomenovaný ako súčasť širšieho plánu:

- Estónsko spáva svoj súvisiaci akčný plán k „bezpečnosti elektronickej identity a spôsobilosti elektronického overovania totožnosti“ so širšou digitálnou agendou Estónska na rok 2020.
- Francúzska NCSS naznačuje, že štátny tajomník zodpovedný za digitálnu technológiu dozerá na vytvorenie podrobného plánu „na ochranu digitálnych životov, súkromia a osobných údajov francúzskeho ľudu“.
- Holandsko NCSS uvádza, že kybernetická bezpečnosť vo verejnej správe, ako aj verejných službách poskytovaných občanom a podnikom, je podrobnejšie rozobratá vo všeobecnej agende pre digitálnu správu.
- Keďže vláda v Spojenom kráľovstve pokračuje v presúvaní stále väčšieho počtu služieb online, vytvorila vládnu digitálnu službu (GDS), aby zabezpečila, že všetky nové digitálne služby vybudované alebo zaobstarané vládou sú takisto zabezpečené ako štandard s podporou Britského národného centra kybernetickej bezpečnosti (NCSC).

2.2.3 Ostatné zvážené strategické ciele

Ostatné strategické ciele boli identifikované počas fázy sekundárneho prieskumu a ako súčasť rozhovorov, ktoré zorganizovala agentúra ENISA. Rozhodlo sa ale, že tieto ciele nebudú tvoriť časť rámca sebahodnotenia. PRÍLOHA C – Ostatné skúmané ciele obsahuje definície pre každý z týchto cieľov, ktoré sa môžu použiť na podporu budúcich rozhodnutí o možných zlepšeniach NCSS.

[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Formovanie digitálnej budúcnosti Európy, COM(2020) 67 konečná verzia: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

Na zváženie v budúcnosti boli preskúmané tieto strategické ciele:

- vývoj stratégií kybernetickej bezpečnosti špecifických pre konkrétny sektor;
- boj proti dezinformačným kampaniam;
- zaistenie pokročilej technológia (5G, AI, kvantová výpočtová technika…);
- zabezpečenie dátovej suverenity a
- poskytnutie stimulov na rozvoj odvetvia poistenia kybernetických rizík.

2.3 KĽÚČOVÉ PONAUČENIA Z CVIČENIA REFERENČNÉHO POROVNANIA

Sekundárny prieskum existujúcich modelov zrelosti týkajúci sa kybernetickej bezpečnosti sa uskutočnil s cieľom zhromaždiť informácie a dôkazy, ktoré pomôžu pri navrhovaní rámca sebahodnotenia národných spôsobilostí v oblasti NCSS. V tomto kontexte sa vykonal rozsiahly prehľad literatúry týkajúcej sa existujúcich modelov, ktorý doplnil zistenia z prvotného predbežného prieskumu modelov zrelosti kybernetickej bezpečnosti a existujúcich NCSS, ktoré sú spracované v oddieloch 2.1 a 2.2. Toto systematické posúdenie pomáha pri výbere a odôvodnení úrovní zrelosti hodnotiaceho rámca a definovaní rôznych rozmerov a indikátorov.

V rámci systematického posúdenia modelov zrelosti sa na základe ich kľúčových znakov posúdilo a analyzovalo 10 modelov. Súhrnný prehľad týchto kľúčových znakov každého posúdeného modelu v rámci tejto štúdie je dostupný v tabuľke 2: Prehľad analyzovaných modelov zrelosti a podrobnejšiu analýzu môžete nájsť v PRÍLOHE A.

Tabuľka 2: Prehľad analyzovaných modelov zrelosti

Názov modelu	Počet úrovní zrelosti	Počet atribútov	Metóda posudzovania	Predstavenie výsledkov
Model zrelosti kapacít kybernetickej bezpečnosti pre národy (CMM)	5	5 hlavných rozmerov	Spolupráca s miestnou organizáciou na doladení modelu pred jeho použitím v národnom kontexte	5-dielny radar
Model zrelosti spôsobilosti kybernetickej bezpečnosti (C2M2)	4	10 hlavných aspektov	Metodika sebahodnotenia a súbor nástrojov	Správa o stave s kruhovými grafmi
Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry	neuvedené (4 stupne)	5 hlavných funkcií	Sebahodnotenie	neuvedené
Katarský model zrelosti spôsobilosti kybernetickej bezpečnosti (Q-C2M2)	5	5 hlavných aspektov	neuvedené	neuvedené
Certifikácia modelu zrelosti kybernetickej bezpečnosti (CMMC)	5	17 hlavných aspektov	Hodnotenie audítormi tretej strany	neuvedené
Model zrelosti kybernetickej bezpečnosti spoločenstva (CCSMM)	5	6 hlavných rozmerov	Hodnotenie v rámci komunít so vstupnými informácií od štátu a federálnych orgánov presadzovania práva	neuvedené
Model zrelosti bezpečnosti informácií pre rámec kybernetickej bezpečnosti NIST (ISMM)	5	23 hodnotený ch oblastí	neuvedené	neuvedené
Model spôsobilosti vnútorného auditu (IA-CM) pre verejný sektor	5	6 prvkov	Sebahodnotenie	neuvedené

Globálny index kybernetickej bezpečnosti (GCI)	neuvedené	5 pilierov	Sebahodnotenie	Tabuľka s hodnotením
Index kybernetickej moci (CPI)	neuvedené	4 kategórie	Referenčné porovnávanie agentúrou Economist Intelligence Unit	Tabuľka s hodnotením

Tento systematický prehľad umožňuje robiť závery osvedčených postupoch prijatých v existujúcich modeloch s cieľom podpory rozvoja koncepčného modelu pre aktuálny model zrelosti. Cvičenie referenčného porovnávania pomohlo najmä pri definovaní úrovní zrelosti, vytvorenie klastrov rozmerov a výber indikátorov, ako aj vhodnú metodiku vizualizácie výsledkov modelu. Najrelevantnejšie zistenia pre každý z týchto prvkov sú detailne popísané v tabuľke 3.

Tabuľka 3: Kľúčové ponaučenia z cvičenia referenčného porovnania

Znak	Kľúčové ponaučenie
Úrovne zrelosti	▶ päťúrovňová stupnica zrelosti pre hodnotiaci rámec spôsobilosti kybernetickej bezpečnosti je všeobecne akceptovaná a dokáže poskytnúť hrubé výsledky hodnotenia (pozri tabuľku 6 Porovnanie úrovní zrelosti v rámci podrobného prehľadu definície úrovní zrelosti pre každý model); ▶ všetky modely poskytujú dôležitú definíciu každej úrovne zrelosti, ktorá sa potom prijme do rôznych rozmerov alebo klastrov aspektov; ▶ zvyčajne sa pri meraní zrelosti spôsobilostí v oblasti kybernetickej bezpečnosti hodnotia dva hlavné aspekty: zrelosť stratégií a zrelosť procesov používaných na implementovanie stratégií.
Atribúty	▶ komparatívna analýza atribútov existujúcich modelov zrelosti ukazuje homogénne výsledky s priemerným počtom atribútov na model medzi štyri a päť; ▶ možnosť spoľahnúť sa na štyri alebo päť atribútov poskytuje krajinám správnu úroveň podrobnosti údajov prostredníctvom zoskupenia relevantných rozmerov dokopy a zaistenia čitateľnosti výsledkov (pozri tabuľku 7: Porovnanie atribútov/rozmerov s popisom atribútov pre každý model); ▶ kľúčový princíp prijatý všetkými modelmi pri definovaní klastrov je založený na konzistentnosti prvku, ktorý je zoskupený v každom klastri.
Metóda posudzovania	▶ metóda posudzovania použité v rôznych analyzovaných modeloch sa od seba líšia; ▶ najbežnejšia metóda posudzovania je založená na sebahodnotení.
Predstavenie výsledkov	▶ je dôležité predstaviť výsledky na rôznej úrovni podrobnosti; ▶ metodika vizualizácie by mala byť celkom jasná a jednoducho čitateľná.

Koncepčný model bol vytvorený na základe cvičenia referenčného porovnávania rôznych modelov zrelosti, ako aj na predchádzajúcej práci agentúry ENISA. Takisto sa prijalo rozhodnutie využiť na tvorbu indikátorov zrelosti použitých pre každý atribút *interaktívny online nástroj agentúry ENISA*.

2.4 VÝZVY HODNOTENIA NCSS

Členské štáty čelia pri tvorbe spôsobilostí v oblasti kybernetickej bezpečnosti mnohým výzvam, predovšetkým pri zabezpečovaní toho, aby boli tieto spôsobilosti aktuálne a v súlade s najnovším vývojom. V ďalšej časti uvádzame súhrn identifikovaných výziev, o ktorých členské štáty v rámci tejto štúdie diskutovali:

- **Problémy v oblasti koordinácie a spolupráce:** Koordinovanie úsilia v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni s cieľom dosiahnuť efektívnu reakciu na problémy kybernetickej bezpečnosti sa môžu ukázať ako problém, a to vzhľadom na vysoký počet zainteresovaných strán.
- **Nedostatočné zdroje na vykonanie posúdenia:** V závislosti od miestnych podmienok a vnútroštátnej štruktúry riadenia kybernetickej bezpečnosti môže vyhodnotenie NCSS a jej cieľov trvať viac ako 15 osobodní.
- **Nedostatok podpory na rozvoj spôsobilostí v oblasti kybernetickej bezpečnosti:** Niektoré členské štáty vyhlásili, že v záujme ochrany rozpočtu a získania podpory na rozvoj spôsobilostí v oblasti kybernetickej bezpečnosti musia najprv uskutočniť hodnotiacu fázu a identifikovať nedostatky a obmedzenia.
- **Problémy pri prisudzovaní úspechov alebo zmien stratégii:** V reakcii na neustále sa vyvíjajúce hrozby a zlepšujúce sa technológie je nevyhnutné, aby sa akčné plány neustále prispôsobovali. Hodnotenie NCSS a pripisovanie zmien stratégii samotnej však aj naďalej zostáva náročnou úlohou. Tým sa následne sťažuje identifikácia obmedzení a nedostatkov NCSS.
- **Problémy s meraním efektívnosti NCSS:** Na zmeranie rôznych oblastí sa môžu zozbierať rôzne údaje, ako napríklad pokrok, implementácia, zrelosť a efektívnosť. Hoci meranie pokroku a implementácie je v porovnaní s meraním efektívnosti relatívne jednoduché, toto meranie je pre hodnotenie výsledkov a vplyvov NCSS stále zmysluplnejšie. Na základe rozhovorov, ktoré uskutočnila agentúra ENISA, množstvo členských štátov uviedlo, že kvantitatívne meranie efektívnosti NCSS je dôležité, ale predstavuje tiež veľmi náročnú úlohu, ktorá je v niektorých prípadoch až nemožná.
- **Problém s prijímaním spoločného rámca:** Členské štáty EÚ pôsobia v rôznych podmienkach z hľadiska politiky, organizácie, kultúry, štruktúry spoločnosti a zrelosti NCSS. Niektoré členské štáty, s ktorými prebehol rozhovor v rámci tejto štúdie, vyjadrili názor, že môže byť náročné obhájiť a používať „univerzálny“ rámec sebahodnotenia.

2.5 VÝHODY NÁRODNÉHO HODNOTENIA SPÔSOBILOSTÍ

Od roku 2017 majú všetky členské štáty EÚ NCSS[20]. Pri pozitívnom vývoji je tiež dôležité, aby boli členské štáty schopné správne vyhodnotiť svoje NCSS, čím vnesú pridanú hodnotu do svojho strategického plánovania a implementácie.

Jedným z cieľov národného hodnotiaceho rámca spôsobilostí je na základe priorít stanovených v rôznych NCSS vyhodnotiť spôsobilosti v oblasti kybernetickej bezpečnosti. V zásade hodnotí tento rámec úroveň zrelosti spôsobilostí v oblasti kybernetickej bezpečnosti členských štátov v oblastiach definovaných cieľmi NCSS. Výsledky rámca tak pomáhajú politickým činiteľom v členských štátoch pri definovaní národnej stratégie kybernetickej bezpečnosti tak, že im poskytujú tajné správy o aktuálnom stave v krajine[21]. NCAF je v podstate určený na pomoc členským štátom pri identifikovaní oblastí zlepšenia a budovaní spôsobilostí.

Cieľom rámca je poskytnúť členským štátom sebahodnotenie svojej úrovne zrelosti na základe posúdenia ich cieľov NCSS, ktoré im pomôžu zlepšiť a vybudovať spôsobilosti v oblasti kybernetickej bezpečnosti na strategickej aj prevádzkovej úrovni.

Na základe praktickejšieho prístupu založeného na rozhovoroch, ktoré uskutočnila agentúra ENISA s niekoľkými orgánmi zodpovednými za oblasť kybernetickej bezpečnosti v rôznych

[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), 468 – 486.

členských štátoch, boli identifikované a zdôraznené tieto výhody národného hodnotiaceho rámca spôsobilostí v oblasti kybernetickej bezpečnosti:

- Poskytnúť užitočné informácie pre rozvoj dlhodobej stratégie (napr. osvedčené postupy, usmernenia);
- Identifikovať chýbajúce prvky v rámci NCSS;
- Ďalej budovať spôsobilosti kybernetickej bezpečnosti;
- Prebrať zodpovednosť za politické kroky;
- Vniesť dôveryhodnosť smerom k širokej verejnosti a medzinárodným partnerom;
- Presiahnuť a vylepšiť verejný obraz ako transparentnej organizácie;
- Pripraviť sa na očakávané problémy;
- Identifikovať naučené lekcie a osvedčené posty;
- Vytvoriť východiskový bod pre postavenie kybernetickej bezpečnosti v rámci EÚ na uľahčenie diskusie a
- Vyhodnotiť národné spôsobilosti týkajúce sa kybernetickej bezpečnosti.

3. METODIKA NÁRODNÉHO HODNOTIACEHO RÁMCA SPÔSOBILOSTÍ V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

3.1 VŠEOBECNÝ ZÁMER

Hlavným cieľom NCAF je zmerať úroveň zrelosti spôsobilostí v oblasti kybernetickej bezpečnosti **členských štátov** a pomôcť im pri vykonávaní hodnotenia svojej národnej spôsobilosti v oblasti kybernetickej bezpečnosti, zvýšení informovanosti o úrovni zrelosti krajiny, identifikovaní oblastí na zlepšenie a tvorbu spôsobilostí v oblasti kybernetickej bezpečnosti.

3.2 ÚROVNE ZRELOSTI

Základom tohto rámca je **päť úrovní zrelosti**, ktoré definujú fázy, ktorými členské štáty prechádzajú pri budovaní spôsobilostí v oblasti kybernetickej bezpečnosti v oblasti, ktorá je obsiahnutá v každom cieli NCSS. Tieto úrovne predstavujú zvyšujúce sa úrovne zrelosti, začínajú od začiatočnej **úrovne 1**, v ktorej členské štáty jasne nedefinovali postup pri budovaní kapacít v oblasti kybernetickej bezpečnosti v oblastiach patriacich do cieľov NCSS, a končia **úrovňou 5**, v ktorej je stratégia budovania kapacít v oblasti kybernetickej bezpečnosti dynamická a prispôsobuje sa vývoju prostredia. Tabuľka 4 obsahuje stupnicu úrovne zrelosti s popisom každej úrovne zrelosti.

Tabuľka 4: Päťúrovňová stupnica zrelosti národného hodnotiaceho rámca spôsobilostí agentúry ENISA

ÚROVEŇ 1 – PRVOTNÁ/AD HOC	ÚROVEŇ 2 – PRVÁ DEFINÍCIA	ÚROVEŇ 3 – USTANOVENIE	ÚROVEŇ 4 – OPTIMALIZÁCIA	ÚROVEŇ 5 – PRISPÔSOBIVOSŤ
Členské štáty jasne nedefinovali postup pri tvorbe kapacít v oblasti kybernetickej bezpečnosti v oblastiach patriacich do cieľov NCSS. Napriek tomu môže krajina mať všeobecné ciele a uskutočniť niektoré štúdie (technické, politické, strategické) na zlepšenie národných spôsobilostí.	Bol definovaný národný prístup k tvorbe kapacít v oblasti patriacej do cieľov NCSS. Akčné plány alebo činnosti na dosiahnutie výsledkov sa uplatňujú, ale v prvotnej fáze. Okrem toho môžu byť identifikované a/alebo zapojené aktívne zainteresované strany.	Akčný plán pre budovanie kapacít v oblasti patriacej do cieľov NCSS je jasne definovaný a podporujú ho súvisiace zainteresované strany. Postupy a činnosti sa uplatňujú a implementujú jednotne na národnej úrovni. Činnosti sú definované a zdokumentované s jasným pridelením zdrojov a riadením a súborom konečných termínov.	Akčný plán sa pravidelne vyhodnocuje: prioritizuje sa, optimalizuje a je udržateľný. Efektívnosť činností budovania kapacít v oblasti kybernetickej bezpečnosti sa pravidelne meria. Identifikujú sa faktory úspechu, výzvy a nedostatky v implementácii činností.	Stratégia budovania kapacít v oblasti kybernetickej bezpečnosti je dynamická a prispôsobivá. Neustále pozornosť venovaná vývoju v oblasti životného prostredia (technologický pokrok, globálny konflikt, nové hrozby…) pomáha pri rýchlom rozhodovaní a schopnosti konať v rámci zlepšovania rýchlo.

3.3 ŠTRUKTÚRA KLASTROV A PREMOSTENIA RÁMCA SEBAHODNOTENIA

Rámec sebahodnotenia charakterizujú **štyri klastre**: (I) Riadenia a normy kybernetickej bezpečnosti, (II) Budovanie kapacít a informovanosť, (III) Právne a zmluvné záležitosti a (IV) Spolupráca. Každý z týchto klastrov zhŕňa kľúčovú tematickú oblasť pre budovanie kapacít v oblasti kybernetickej bezpečnosti v krajine a obsahuje skupinu rôznych cieľov, ktoré môžu členské štáty zahrnúť do svojich NCSS zahrnúť. Predovšetkým:

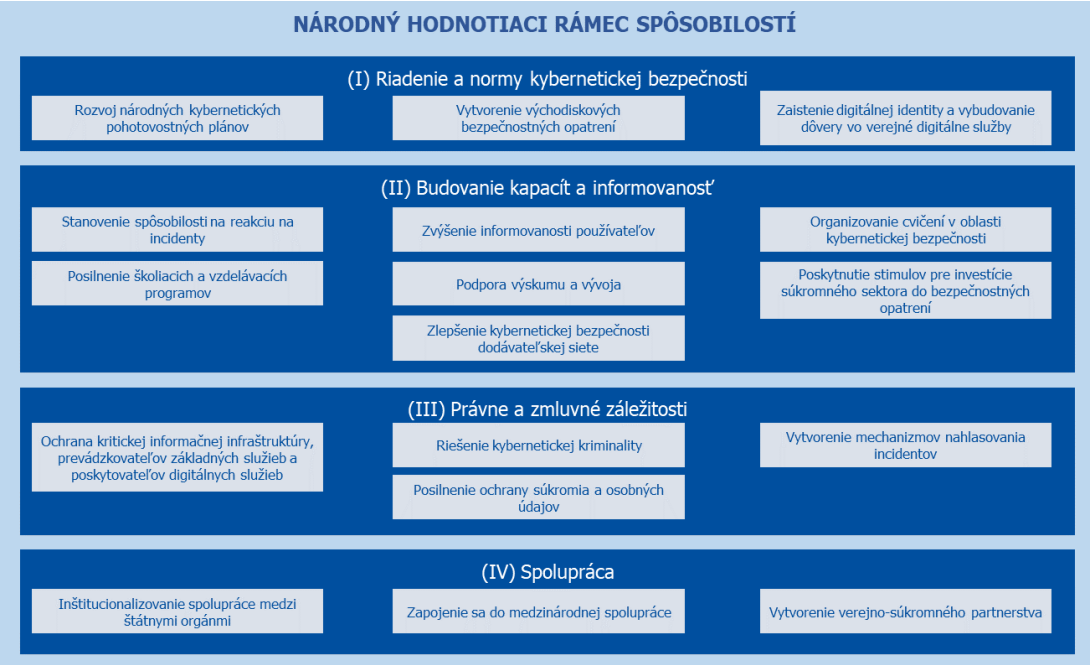
- **(I) Riadenie a normy kybernetickej bezpečnosti**: tento klaster meria schopnosť členských štátov zriadiť riadne riadenie, normy a osvedčené postupy v oblasti kybernetickej bezpečnosti. Tento rozmer berie do úvahy rôzne stránky kybernetickej obrany a odolnosti a zároveň podporuje rozvoj národného odvetvia kybernetickej bezpečnosti a buduje dôveru vo vlády;
- **(II) Budovanie kapacít a informovanosť**: tento klaster vyhodnocuje schopnosť členských štátov zvyšovať informovanosť o kybernetických rizikách a hrozbách a o tom, ako ich riešiť. Tento rozmer okrem toho meria schopnosť krajiny kontinuálne budovať spôsobilosti v oblasti kybernetickej bezpečnosti a zvyšovať celkovú úroveň znalostí a zručností v tejto oblasti. Zaoberá sa vývojom trhu kybernetickej bezpečnosti a pokrokom vo výskume a vývoji v oblasti kybernetickej bezpečnosti. Tento klaster preskupuje všetky ciele, čím vytvára základ pre podporu budovania kapacít;
- **(III) Právne a zmluvné záležitosti**: tento klaster meria schopnosť členských štátov zaviesť do praxe právne a regulačné nástroje na riešenie počítačovej kriminality a súvisiacich kybernetických incidentov a na boj proti nim, ako aj schopnosť chrániť kritickú informačnú infraštruktúru. Tento rozmer okrem toho hodnotí aj schopnosť členských štátov vytvárať právny rámec na ochranu občanov a podnikov, ako napríklad v prípade vyvažovania bezpečnosti a súkromia; a
- **(IV) Spolupráca:** tento klaster hodnotí spoluprácu a poskytovanie informácií medzi rôznymi skupinami zainteresovaných strán na národnej a medzinárodnej úrovni ako dôležitý nástroj pre lepšie pochopenie a reakciu na neustále sa meniace prostredie hrozieb.

Ciele, ktoré boli do modelu zahrnuté sú tie, ktoré členské štáty bežne prijímajú, a ktoré boli vybrané z cieľov uvedených v časti 2.2. Model hodnotí najmä tieto ciele:

- 1. Rozvoj národných kybernetických pohotovostných plánov (I)
- 2. Vytvorenie východiskových bezpečnostných opatrení (I)
- 3. Zaistenie digitálnej identity a vybudovanie dôvery vo verejné digitálne služby (I)
- 4. Stanovenie spôsobilosti na reakciu na incidenty (II)
- 5. Zvýšenie informovanosti používateľov (II)
- 6. Organizovanie cvičení v oblasti kybernetickej bezpečnosti (II)
- 7. Posilnenie školiacich a vzdelávacích programov (II)
- 8. Podpora výskumu a vývoja (II)
- 9. Poskytnutie stimulov pre investície súkromného sektora do bezpečnostných opatrení (II)
- 10. Zlepšenie kybernetickej bezpečnosti dodávateľskej siete (II)
- 11. Ochrana kritickej informačnej infraštruktúry, prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb (III)
- 12. Riešenie kybernetickej kriminality (III)
- 13. Vytvorenie mechanizmov nahlasovania incidentov (III)
- 14. Posilnenie ochrany súkromia a osobných údajov (III)
- 15. Inštitucionalizovanie spolupráce medzi štátnymi orgánmi (IV)
- 16. Zapojenie sa do medzinárodnej spolupráce (IV)
- 17. Vytvorenie verejno-súkromného partnerstva (IV)

Tieto štyri klastre a základné ciele sa skombinujú do modelu, ktorý poskytuje holistický pohľad na zrelosť spôsobilostí v oblasti kybernetickej bezpečnosti členských štátov. Obrázok 1 predstavuje ústrednú štruktúru rámca sebahodnotenia a ukazuje, ako sú tieto prvky, najmä ciele, klastre a rámce sebahodnotenia, prepojené na hodnotenie výkonnosti krajiny.

Obrázok 1: Štruktúra rámca sebahodnotenia



Pre každý cieľ zahrnutý do rámca sebahodnotenia existuje rad indikátorov, ktoré sú rozdelené v piatich úrovniach zrelosti. Každý indikátor je založený na zisťovacej (áno/nie) otázke. Indikátor môže byť povinný alebo nepovinný.

3.4 BODOVACÍ MECHANIZMUS

Bodovací mechanizmus rámca sebahodnotenia berie do úvahy prvky a princípy uvedené v časti 3.5. Model vlastne poskytuje skóre na základe hodnoty dvoch parametrov, a to **úrovne zrelosti** a **ukazovateľa krytia**. Každý z týchto parametrov je možné vypočítať na rôznych úrovniach: (i) podľa cieľa, (ii) podľa klastra cieľov alebo (iii) celkovo.

Skóre na úrovni cieľa

Skóre úrovne zrelosti poskytuje prehľad úrovne zrelosti tak, že udáva, ktoré spôsobilosti a postupy sa zaviedli do praxe. Skóre úrovne zrelosti sa vypočíta ako najvyššia úroveň, pre ktorú respondent splnil všetky predpoklady (*napr.* odpoveď ÁNO na všetky povinné otázky) okrem splnenia predpokladov predchádzajúcich úrovní zrelosti.

Ukazovateľ krytia udáva rozsah krytia všetkých indikátorov s kladnou odpoveďou bez ohľadu na ich úroveň. Je to doplnková hodnota, ktorá zohľadňuje všetky indikátory, ktorými sa cieľ meria. Ukazovateľ krytia sa vypočíta ako pomer celkového počtu otázok v rámci cieľa a počtu otázok s kladnou odpoveďou.

Je dôležité vysvetliť, že vo zvyšku dokumentu sa slovo ***skóre*** používa pre hodnoty úrovne zrelosti aj ukazovateľ krytia.

Obrázok 2 – Bodovací mechanizmus podľa cieľa poskytuje vizualizáciu hodnotiaceho mechanizmu uvedeného v časti 3.1, ktorý bude ďalej vysvetlený nižšie.

Obrázok 2: Bodovací mechanizmus podľa cieľa

Obrázok 2 udáva príklad toho, ako sa úroveň zrelosti vypočíta podľa cieľa. Treba poznamenať, že respondent splnil všetky predpoklady prvých troch úrovní zrelosti a len čiastočne splnil predpoklady úrovne 4. Skóre preto udáva, že ***úroveň zrelosti respondenta je úroveň 3 pre cieľ „Organizovanie cvičenia v oblasti kybernetickej bezpečnosti“****.*

V príklade uvedenom na obrázku 2 nie je však úroveň zrelosti cieľa schopná zachytiť informácie, ktoré poskytujú indikátory, ktoré majú pozitívne skóre a ktoré sú vyššie ako úroveň zrelosti 3. V takom prípade poskytuje ukazovateľ krytia prehľad o všetkých prvkoch, ktoré

respondent implementoval na to, aby dosiahol tento cieľ napriek jeho skutočnej úrovni zrelosti. V tomto prípade je pomer medzi celkovým počtom otázok v rámci cieľa a počtom otázok s kladnou odpoveďou rovný 19/27, t. j. ***hodnota ukazovateľa krytia je 70 %.***

Na prispôsobenie sa špecifikám členských štátov a súčasne umožniť konzistentný prehľad sa skóre okrem toho vypočíta z dvoch rôznych vzoriek na úrovni klastra a celkovej úrovni:

- **Všeobecné skóre:** jedna úplná vzorka zahŕňajúca všetky ciele obsiahnuté v klastri alebo v rámci celkového rámca (od jedna po 17);
- **špecifické skóre:** jedna špecifická vzorky zahŕňajúca len ciele vybrané členským štátom (zvyčajne zodpovedajú cieľom uvedeným v NCSS konkrétnej krajiny) v rámci klastra alebo v rámci celkového rámca.

Skóre na úrovni klastra

Všeobecná úroveň zrelosti pre každý klaster sa vypočíta ako aritmetický priemer úrovne zrelosti všetkých cieľov v rámci tohto klastra.

Špecifická úroveň zrelosti každého klastra sa vypočíta ako aritmetický priemer úrovne zrelosti cieľov v rámci tohto klastra, ktoré si členský štát zvolí na hodnotenie (zvyčajne zodpovedajú cieľom uvedeným v NCSS konkrétnej krajiny).

Napríklad obrázok 1 udáva, že klaster (I) Riadenie a normy kybernetickej bezpečnosti sa skladá z troch cieľov. Za predpokladu, že sa respondent rozhodne vyhodnotiť len prvé dva ciele, ale nie tretí cieľ, a za predpokladu, že prvé dva ciele predstavujú úroveň zrelosti 2 a 4 v tomto poradí, potom je úroveň zrelosti klastra pri zohľadnení všetkých cieľov úroveň 2 (klaster (I) všeobecná úroveň zrelosti = (2 + 4) / 3), zatiaľ čo úroveň zrelosti klastra pri zohľadnení len špecifických cieľov zvolených hodnotiteľom je úroveň 3 (klaster (I) špecifická úroveň zrelosti = (2 + 4) / 2).

Všeobecný ukazovateľ krytia každého klastra sa vypočíta ako pomer celkového počtu otázok v rámci klastra a počtu otázok s kladnou odpoveďou.

Špecifický ukazovateľ krytia každého klastra sa vypočíta ako pomer medzi celkovým počtom otázok v rámci klastra, ktoré sa týkajú cieľov, ktoré si členský štát vybral na hodnotenie (zvyčajne zodpovedajú cieľom uvedeným v NCSS konkrétnej krajiny), a počtu otázok s kladnou odpoveďou.

Skóre na celkovej úrovni

Celková všeobecná úroveň zrelosti krajiny sa vypočíta ako aritmetický priemer úrovne zrelosti všetkých cieľov v danom rámci, od jedna po 17.

Celková špecifická úroveň zrelosti krajiny sa vypočíta ako aritmetický priemer úrovne zrelosti cieľov v danom rámci, ktoré si členský štát zvolí na hodnotenie (zvyčajne zodpovedajú cieľom uvedeným v NCSS konkrétnej krajiny).

Celkový všeobecný ukazovateľ krytia krajiny sa vypočíta ako pomer celkového počtu otázok v rámci všetkých cieľov zahrnutých do rámca (od jedna po 17) a počtu otázok s kladnou odpoveďou.

Celkový špecifický ukazovateľ krytia krajiny sa vypočíta ako pomer medzi celkovým počtom otázok v rámci cieľov rámca, ktoré si členský štát vybral na hodnotenie (zvyčajne zodpovedajú cieľom uvedeným v NCSS konkrétnej krajiny), a počtu otázok s kladnou odpoveďou.

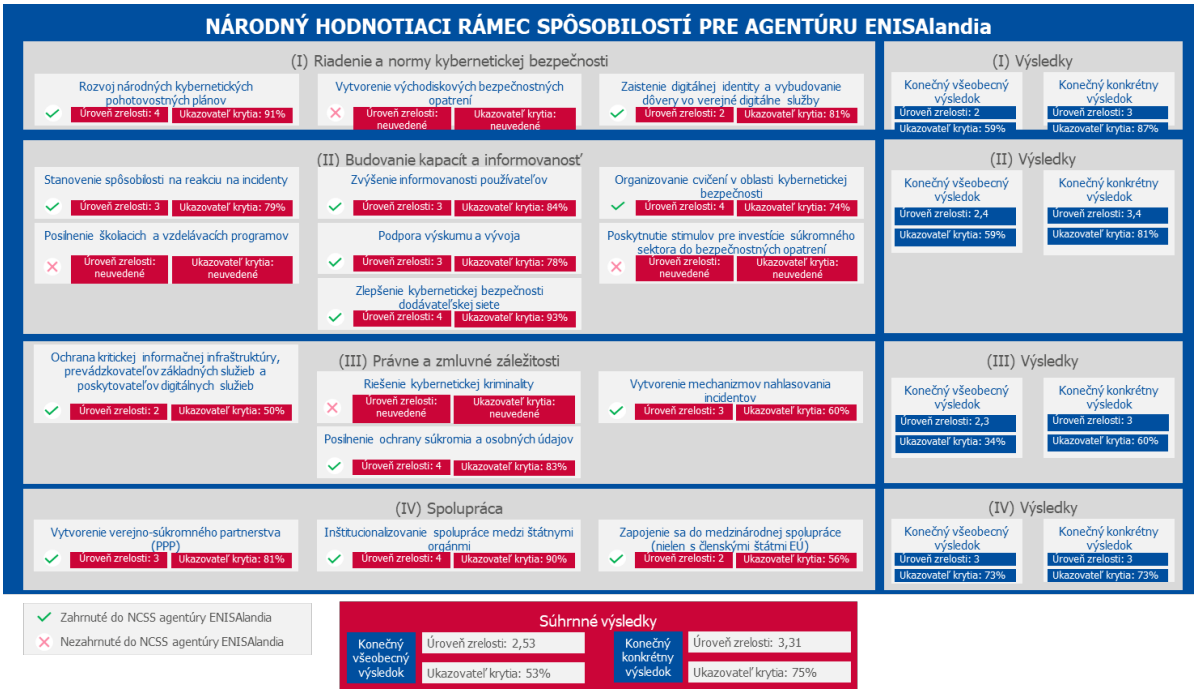
Pri každom ukazovateli si môžu respondenti vybrať ako svoju odpoveď tretiu možnosť „neviem/nevzťahuje sa“. V tomto prípade je ukazovateľ vylúčený z celkového výpočtu výsledkov.

Úrovne zrelosti na úrovni klastra a celkovej úrovni sa vypočítajú pomocou aritmetického priemeru, aby bolo možné ukázať progres medzi týmito dvomi hodnoteniami. Alternatíva pozostávajúca z výpočtu úrovní zrelosti klastra a celkovej úrovne zrelosti ako úrovne zrelosti najmenej zrelého cieľa, aj keď je táto možnosť relevantná z hľadiska zrelosti, nemôže v skutočnosti vysvetľovať progres dosiahnutý v oblastiach obsiahnutých v ostatných cieľoch.

Keďže úroveň klastra a celková úroveň sa na účely správy konsolidujú, padol výber na aritmetický priemer. Na účely podávania správ použite skóre na úrovni cieľa, ktoré sú presnejšie.

Na obrázku 3 nižšie je zobrazený súhrn bodovacích mechanizmov na rôznych úrovniach modelu (cieľ, klaster, celkovo).

Obrázok 3: Celkový bodovací mechanizmus



3.5 POŽIADAVKY NA RÁMEC SEBAHODNOTENIA

Národný hodnotiaci rámec spôsobilostí popísaný v tejto časti je založený na potrebách zdôraznených členskými štátmi a je vytvorený na základe súboru požiadaviek uvedených ďalej:

- Členské štáty uvádzajú NCAF do praxe na dobrovoľnej báze ako rámec sebahodnotenia;
- Cieľom NCAF je zmeranie spôsobilostí v oblasti kybernetickej bezpečnosti členských štátov pri zohľadnení 17 cieľov. Členský štát si ale môže vybrať ciele, ktoré chce hodnotiť, a vyhodnotiť len podskupinu zo 17 cieľov;
- Rámec sebahodnotenia je zameraný na meranie úrovne zrelosti spôsobilostí v oblasti kybernetickej bezpečnosti členského štátu;

- Výsledky hodnotenia sa nezverejnia, pokiaľ sa tak členský štát zo svojej vlastnej iniciatívy nerozhodne urobiť;
- Členský štát môže ukázať výsledky hodnotenia poskytnutím úrovne zrelosti spôsobilostí kybernetickej bezpečnosti krajiny, klastra cieľov alebo dokonca jedného cieľa;
- Všetky hodnotené ciele sú v rámci sebahodnotenia rovnako relevantné, a preto sú rovnako dôležité. To isté platí pre ukazovatele použité v ňom; a
- Členský štát môže sledovať svoje progres v čase.

Cieľom rámca sebahodnotenia je pomôcť členským štátom pri budovaní spôsobilostí v oblasti kybernetickej bezpečnosti, a preto obsahuje aj súbor odporúčaní alebo usmernení, ktoré majú pomôcť európskym krajinám pri zvyšovaní ich úrovne zrelosti.

Poznámka: tieto odporúčania alebo usmernenia sú všeobecné a vychádzajú z publikácií agentúry ENISA a zo skúseností iných krajín a budú založené na výsledku sebahodnotenia.

4. UKAZOVATELE NCAF

4.1 UKAZOVATELE RÁMCA

Táto časť opisuje indikátory národného rámca spôsobilostí ENISA. Tieto časti sú organizované podľa klastra.

Pre každý klaster zobrazuje tabuľka komplexný súbor ukazovateľov vo forme otázok typických pre danú úroveň zrelosti. Hlavným nástrojom sebahodnotenia je dotazník. Pre každý cieľ existujú dva súbory ukazovateľov, ktoré je potrebné si všímať:

- Súbor všeobecných otázok o zrelosti stratégie (9 všeobecných otázok), ktoré sú označené od „a“ po „c“ pre každú úroveň zrelosti a opakujú sa pri každom cieli; a
- Súbor otázok o kapacite kybernetickej bezpečnosti (319 otázok o kapacite kybernetickej bezpečnosti), ktoré sú očíslované od 1 po 10 pre každú úroveň zrelosti a sú špecifické pre oblasť, ktorej sa cieľ týka.

Každá otázka sa označí značkou (0 – 1), ktorá udáva, či je otázka povinným ukazovateľom (1) alebo nepovinným ukazovateľom (0) pre úroveň zrelosti.

Každú otázku je možné identifikovať podľa identifikačného čísla, ktoré obsahuje:

- číslo cieľa,
- úroveň zrelosti a
- číslo otázky.

Napríklad ID otázky 1.2.4 znamená, že otázka je štvrtá v úrovni zrelosti 2 strategického cieľa (I) „Rozvoj národných kybernetických pohotovostných plánov“.

Treba zdôrazniť, že pokiaľ sa neuvádza inak, je rozsah otázok v dotazníku na národnej úrovni. Vo všetkých otázkach odkazuje zámeno „vy“ všeobecne na členský štát a neodkazuje na jednotlivca alebo vládny orgán, ktorý hodnotenie vykonáva.

Definícia každého cieľa je uvedená v kapitole 2.2 – Spoločné ciele identifikované v rámci európskej NCSS.

4.1.1 Klaster č. 1: Riadenie a normy kybernetickej bezpečnosti

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
1 – Rozvoj národných kybernetických pohotovostných plánov	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Začali ste pracovať na budovaní národných a pohotovostných plánoch? *Napr.* príprava všeobecných cieľov, rozsahu a/alebo princípov pohotovostných plánov…	1	Máte princíp/národnú stratégiu, ktorá zahŕňa kybernetickú bezpečnosť ako krízový prvok (napr. detailný plán, stratégia atď.)?	1	Máte plán riadenia kybernetickej krízy na národnej úrovni?	1	Ste spokojní s počtom alebo percentuálnou hodnotou kritických sektorov zahrnutých do národného kybernetického pohotovostného plánu?	1	Máte v praxi zavedený proces získavania vedomostí po cvičeniach v oblasti kybernetickej bezpečnosti alebo skutočných krízach na národnej úrovni?	1
	2	Je všeobecne známe, že kybernetické incidenty predstavujú krízový prvok, ktorý by mohol ohroziť národnú bezpečnosť?	0	Máte centrálu, ktorá získava informácie a informuje riadiace subjekty? *Napr.* akékoľvek metódy, platformy alebo miesta, ktoré zaistia prístup k rovnakým informáciám v reálnom čase týkajúcim sa kybernetickej krízy pre všetkých aktívnych účastníkov reagujúcich na krízu.	1	Máte konkrétne postupy špecifické pre kybernetickú krízu na národnej úrovni?	1	Organizujete činnosti (napr. cvičenia) týkajúce sa národného kybernetického pohotovostného plánovania dostatočne často?	1	Máte proces, ktorým sa pravidelne testuje národný plán?	1
	3	Uskutočnili sa v oblasti kybernetického pohotovostného plánovania nejaké štúdie (technické, prevádzkové, politické)?	0	Sú do dohľadu nad vývojom a vykonávaním národných kybernetických pohotovostných plánov zapojené relevantné zdroje?	1	Máte komunikačný tím špeciálne vyškolený na reakcie na kybernetické krízy a informovanie verejnosti?	1	Máte dostatok ľudí, ktorí sa venujú plánovaniu krízy, vzdelávajú sa a vykonávajú zmeny?	1	Máte adekvátne nástroje a platformy na vytvorenie situačného povedomia?	1
	4	-		Máte metodika na vyhodnotenie kybernetickej hrozby na národnej úrovni, ktorá zahŕňa postupy na posúdenie vplyvu?	0	Zapájate všetky relevantné zainteresované strany (národná bezpečnosť, obrana, civilná ochrana, polícia, ministri, orgány atď.)?	1	Máte dostatok školených ľudí, ktorí dokážu reagovať na kybernetickú krízu na národnej úrovni?	1	Dodržiavate konkrétny model zrelosti na monitorovanie a zlepšenie kybernetického pohotovostného plánu?	0
	5	-		-		Máte adekvátne zariadenia krízového riadenia a situačné strediská?	1	-		Máte zdroje, ktoré sú buď špecializované v oblasti predvídania hrozieb alebo pracujú na potenciálnej kybernetickej bezpečnosti s cieľom pomenovať budúci krízu alebo výzvy zajtrajška?	0

	6	-		-	Spolupracujete v prípade potreby s medzinárodnými zainteresovanými stranami v EÚ?	0	-		-		
	7	-		-	Spolupracujete v prípade potreby s medzinárodnými zainteresovanými stranami mimo EÚ?	0	-		-		
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
2 – Vytvorenie východiskových bezpečnostných opatrení	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Uskutočnili ste štúdiu na identifikovanie požiadaviek a nedostatkov pre **verejné** organizácie na základe medzinárodne uznaných noriem? *napr.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Sú bezpečnostné opatrenia navrhnuté v súlade s medzinárodnými/národnými normami?	1	Sú východiskové bezpečnostné opatrenia povinné?	1	Existuje proces na časté aktualizovanie východiskových bezpečnostných opatrení?	1	Máte proces na posilnenie IKT, ak pri riešení incidentov zlyhajú opatrenia?	1
	2	Uskutočnili ste štúdiu na identifikovanie požiadaviek a nedostatkov pre **súkromné** organizácie na základe medzinárodne uznaných noriem? napr. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Diskutujete pri definovaní východiskových bezpečnostných opatrení so súkromným sektorom a inými zainteresovanými stranami?	1	Uplatňujete horizontálne bezpečnostné opatrenia v kritických sektoroch?	1	Je v praxi zavedený mechanizmus monitorovania, pomocou ktorého sa preskúmajú východiskové bezpečnostné opatrenia?	1	Posudzujete relevantnosť nových noriem, ktoré vzniknú ako reakcia na posledný vývoj v oblasti hrozieb?	1
	3	-		-		Uplatňujete bezpečnostné opatrenia špecifické pre konkrétne sektory v kritických sektoroch?	1	Existuje vnútroštátny orgán na kontrolu presadzovania východiskových bezpečnostných opatrení?	1	Máte alebo podporujete národný koordinovaný proces zverejňovania informácií o zraniteľnosti (CVD)?	1

	4	-				Sú východiskové bezpečnostné opatrenia v súlade s relevantnými certifikačnými schémami?	1	Máte v praxi zavedený proces na identifikovanie organizácií, ktoré v rámci určitého obdobia nedodržiavajú pravidlá?	1	-	
	5	-		-		Existuje proces sebahodnotenia pre východiskové bezpečnostné opatrenia?	1	Existuje proces auditu na zabezpečenie riadneho uplatňovania bezpečnostných opatrení?	1	-	
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
2 – Vytvorenie východiskových bezpečnostných opatrení	6	-		-		Preskúmavate počas procesu obstarávania vládnymi orgánmi povinné východiskové bezpečnostné opatrenie?	0	Definujete alebo aktívne podporujete prijímanie bezpečnostných noriem pre vývoj kritických produktov z oblasti IT/OT (zdravotnícke vybavenie, pripojené a autonómne vozidlá, profesionálna stanica, zariadenia ťažkého priemyslu...)?	0	-	

Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
3 – Zaistenie digitálnej identity a vybudovanie dôvery vo verejné digitálne služby	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Uskutočnili ste štúdie alebo analýzy nedostatkov s cieľom identifikovať potreby na zabezpečenie verejných digitálnych služieb pre obyvateľov a podniky?	1	Vykonávate analýzy rizík na určenie profilu rizík majetku alebo služieb pred ich presunutím do cloudu alebo na zapojenie projektov digitálnej transformácie?	1	Podporujete metodiky ochrany súkromia už v štádiu návrhu vo všetkých projektoch e-Government?	1	Zhromažďujete ukazovatele kybernetických incidentov zahŕňajúce porušenie verejných digitálnych služieb?	1	Ste súčasťou európskych pracovných skupín na udržiavanie štandardov a/alebo návrhu nových požiadaviek pre dôveryhodné elektronické služby (elektronický podpis, elektronické pečate, elektronické doručovacie služby pre registrované zásielky, časová pečiatka, autentifikácia webového sídla)? *Napr.* ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU...	1

	2	-		Máte stratégiu na vytvorenie alebo podporu bezpečných schém elektronickej identifikácie (eID) pre občanov a podniky?	1	Zahrnuli ste súkromné zainteresované strany do navrhovania a poskytovania zabezpečených verejných digitálnych služieb?	1	Implementovali ste s ostatnými členskými štátmi vzájomné uznávanie prostriedkov elektronickej identifikácie?	1	Zúčastňujete sa aktívne na recenzných hodnoteniach ako súčasť oznámenia schém elektronického ID Európskej komisii?	1
	3	-		Máte stratégiu na tvorbu alebo podporu zabezpečených národných dôveryhodných elektronických služieb (elektronické podpisy, elektronické pečate, elektronické doručovacie služby pre registrované zásielky, autentifikácia webového sídla) pre občanov a podniky?	1	Uplatňujete minimálne bezpečnostné východisko pre všetky verejné digitálne služby?	1	-		-	
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
3 – Zaistenie digitálnej identity a vybudovanie dôvery vo verejné digitálne služby	4	-		Máte stratégiu na vládnom cloude (počítačová stratégia cloudu zameraná na vládne a verejné orgány, ako napríklad ministerstvá, vládne orgány a verejné správy…), ktorá berie do úvahy dôsledky pre bezpečnosť?	0	Sú pre občanov a podniky dostupné nejaké schémy elektronickej identifikácie so značnou alebo vysokou úrovňou zabezpečenia podľa definície v prílohe k nariadeniu eIDAS (EÚ) č. 910/2014?	1	-		-	
	5	-		-		Máte verejné digitálne služby vyžadujúce schémy elektronickej identifikácie so značnou alebo vysokou úrovňou zabezpečenia podľa definície v prílohe k nariadeniu eIDAS (EÚ) č. 910/2014?	1	-		-	
	6	-		-		Máte poskytovateľov dôveryhodných služieb pre občanov a podniky (elektronické podpisy, elektronické doručovacie služby pre registrované zásielky, časová pečiatka, autentifikácia webového sídla)?	1	-		-	
	7	-		-		Podporujete prijatie východiskových bezpečnostných opatrení pre všetky modely zavádzania cloudov (napr. súkromné, verejné, hybridné, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Klaster č. 2: Budovanie kapacít a povedomie

Cieľ NCSS	Č.	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
4 – Stanovenie spôsobilosti na reakciu na incidenty	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Máte neoficiálne spôsobilosti na reakciu na incidenty, ktoré sa riadia v rámci alebo medzi súkromnými a verejnými sektormi?	1	Máte minimálne jednu oficiálnu národnú jednotku pre riešenie počítačových bezpečnostných incidentov?	1	Máte spôsobilosti na reakciu na incidenty pre sektory uvedené v prílohe II k smernici NIS?	1	Definovali ste a podporujete štandardizované postupy pre procesy reakcie na incidenty a schémy klasifikácie incidentov?	1	Máte mechanizmy na skoré zistenie, identifikovanie, prevenciu, reakcie a zmenšenie zraniteľností nultého dňa?	1
	2	-		Má vaša národná jednotka pre riešenie počítačových bezpečnostných incidentov jasne definovaný rozsah intervencie? *Napr.* v závislosti o cieľového sektora, typov incidentov, dopadov	1	Existuje vo vašej krajine mechanizmus spolupráce jednotky pre riešenie počítačových bezpečnostných incidentov, ktorý umožňuje reakciu na incidenty?	1	Hodnotíte svoju spôsobilosť reakcie na incidenty, aby ste zaistili, že máte adekvátne zdroje a zručnosti na uskutočňovanie úloh stanovených v bode (2) prílohy I k smernici NIS?	1	-	
	3	-		Má vaša národná jednotka pre riešenie počítačových bezpečnostných incidentov jasne definované vzťahy s ostatnými národnými zainteresovanými stranami, pokiaľ ide o národnú oblasť kybernetickej bezpečnosti a postup reakcie na incidenty (napr. LEA, military, ISPs, NCSC)?	0	Disponuje vaša národná jednotka pre riešenie počítačových bezpečnostných incidentov spôsobilosťou na rekciu na incidenty v súlade s prílohou I k smernici NIS? *Napr.* dostupnosť, fyzická bezpečnosť, kontinuita činností, medzinárodná spolupráca, monitorovanie incidentov, schopnosť včasného varovania a upozornení, reakcia na incidenty, analýza rizika a situačná informovanosť, spolupráca so súkromným sektorom, štandardné postupy...	1	-		-	
	4	-				Existuje mechanizmus spolupráce s ostatnými susednými krajinami týkajúci sa incidentov?	1	-		-	

	5	-		-		Definovali ste formálne jasné zásady a postupy riešenia incidentov?	1	-		-	
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
4 – Stanovenie spôsobilosti na reakciu na incidenty	6	-		-		Je vaša národná jednotka pre riešenie počítačových bezpečnostných incidentov súčasťou cvičení kybernetickej bezpečnosti na národnej a medzinárodnej úrovni?	1	-		-	
	7	-		-		Je vaša národná jednotka pre riešenie počítačových bezpečnostných incidentov členom FIRST (Fórum tímov pre riešenie počítačových incidentov)?	0	-		-	

Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
5 – Zvýšenie informovanosti používateľov	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Uznáva aspoň minimálne vláda, súkromný sektor a bežní používatelia, že existuje potreba zvyšovať informovanosť o kybernetickej bezpečnosti a problémoch ochrany súkromia?	1	Identifikovali ste konkrétnu cieľovú skupinu pre zvýšenie informovanosti používateľov? *Napr.* bežní používatelia, mladí ľudia, podnikoví používatelia (ktorí sa dajú ďalej rozdeliť na: SME, OES, DSP atď.)	1	Vytvorili ste komunikačné plány/stratégiu pre kampane?	1	Vypracujete merania na posudzovanie svojej kampane počas fázy plánovania?	1	Máte v praxi zavedené mechanizmy na zaistenie konštantnej relevantnosti kampaní na zvýšenie informovanosti o technologickom pokroku, zmenách v oblasti hrozieb, právnych nariadeniach a národných bezpečnostných smerniciach?	1

	2	Uskutočňujú verejné orgány kampane na zvýšenie informovanosti o kybernetickej bezpečnosti v rámci svojich organizácií na ad hoc báze? Napr. v dôsledku kybernetického incidentu.	0	Pripravujete plán projektu na zvýšenie informovanosti o bezpečnosti informácií a problémoch ochrany súkromia?	1	Máte proces na vytváranie obsahu na vládnej úrovni?	1	Posudzujete svoje kampane po ich realizácii?	1	Vykonávate pravidelné posudzovanie alebo preskúmanie s cieľom zmerať posun postoja alebo zmien správania týkajúcich sa kybernetickej bezpečnosti a otázok súkromia v súkromných a verejných sektoroch?	1
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
5 – Zvýšenie informovanosti používateľov	3	Vykonávajú verejné orgány kampane na ad hoc báze na zvýšenie informovanosti o kybernetickej bezpečnosti pre širokú verejnosť? *Napr.* v dôsledku kybernetického incidentu.	0	Máte k dispozícii zdroje jednoducho identifikovateľné (*napr.* jeden online portál, súbory nástrojov na zvyšovanie informovanosti) pre všetkých používateľov, ktorí sa snažia získavať informácie o kybernetickej bezpečnosti a problémoch ochrany súkromia?	1	Máte mechanizmy na identifikovanie cieľových oblastí na zvyšovanie informovanosti (napr. oblasť hrozieb agentúry ENISA, národné podmienky, medzinárodné podmienky, spätná väzba od národných centier pre počítačovú kriminalitu atď.)?	1	Máte zavedené nejaké mechanizmy na identifikovanie najrelevantnejších médií alebo komunikačného kanála v závislosti od cieľovej skupiny, aby ste maximalizovali dosah a zapojenie? *Napr.* rôzne druhy digitálnych médií, brožúry, e-maily, učebný materiál, plagáty v zaľudnených oblastiach, televízia, rádio…	1	Radíte sa s odborníkmi na správanie, aby vaše kampane prispôsobili cieľovej skupine?	1
	4	-		-		Spájate pri tvorbe obsahu zainteresované strany s odborníkmi a komunikačnými tímami?	1			-	
	5	-		-		Zapájate a angažujete súkromný sektor do svojej snahy o zvýšenie informovanosti, aby ste podporili a rozširovali odkazy širšiemu publiku?	1	-		-	
	6	-		-		Pripravujete konkrétne iniciatívy na zvýšenie informovanosti pre výkonných pracovníkov vo verejnom, súkromnom akademickom sektore alebo sektore občianskej spoločnosti?	1	-		-	
	7	-		-		Zúčastňujete sa na kampaniach európskeho mesiaca kybernetickej bezpečnosti (ECSM) agentúry ENISA?	0	-		-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
6 – Organizovanie cvičení v oblasti kybernetickej bezpečnosti	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
6 – Organizovanie cvičení v oblasti kybernetickej bezpečnosti	1	Uskutočňujete krízové cvičenia v ostatných sektoroch (iných ako je kybernetická bezpečnosť) na národnej alebo paneurópskej úrovni?	1	Máte program cvičení v oblasti kybernetickej bezpečnosti na národnej úrovni?	1	Zapájate všetky súvisiace orgány verejnej správy? (dokonca aj keď je scenár špecifický pre konkrétny sektor)	1	Zostavujete výročné správy o činnosti/hodnotiace správy?	1	Máte schopnosť vytvoriť analýzu ponaučenia zo skúseností pre kybernetickú bezpečnosť (procesy nahlasovania, analýza, zmiernenie)?	1
	2	Máte zdroje pridelené pre navrhovanie a plánovanie cvičení krízového riadenia?	1	Uskutočňujete alebo stanovujete priority pre cvičenia krízového riadenia pre nevyhnutné spoločenské funkcie a kritickú infraštruktúru?	1	Zapájate súkromný sektor do plánovania a realizácie týchto cvičení?	1	Testujete plány a postupy na národnej úrovni?	1	Zriadili ste proces ponaučenia zo skúseností?	1
	3	-		Identifikovali ste koordinačný orgán, ktorý bude dohliadať nad navrhovaním a plánovaním cvičení kybernetickej bezpečnosti (štátny orgán, poradenská firma...)?	0	Organizujete cvičenia špecifické pre konkrétny sektor na národnej a/alebo medzinárodnej úrovni?	1	Zúčastňujete sa na cvičeniach v oblasti kybernetickej bezpečnosti na paneurópskej úrovni?	1	Prispôsobujete scenáre cvičení v závislosti od najnovšieho vývoja (technologické pokroky, globálne konflikty, oblasť hrozieb...)?	1
	4	-		-		Organizujete cvičenia v rámci všetkých dôležitých sektorov uvedených v prílohe II smernice NIS?	1	-		Koordinujete svoje postupy krízového riadenia s ostatnými členskými štátmi, aby ste zaistili efektívne paneurópske krízové riadenie?	1
	5	-		-		Organizujete vnútrosektorové a/alebo medzisektorové cvičenia v oblasti kybernetickej bezpečnosti?	1	-		Máte v praxi zavedené mechanizmy na rýchle prispôsobenie stratégie, plánov a postupov zo získaných skúseností počas týchto cvičení?	0
	6	-		-		Organizujete cvičenia v oblasti kybernetickej bezpečnosti špecifické pre rôzne úrovne? (technická a prevádzková úroveň, úroveň postupov, úroveň rozhodovania, politická úroveň...)	0	-		-	

Cieľ NCSS	#	Level 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
7 – Posilnenie školiacich a vzdelávacích programov	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Zvažujete vytvorenie školenia v oblasti kybernetickej bezpečnosti a vzdelávacích programov?	1	Organizujete kurzy venované kybernetickej bezpečnosti?	1	Existuje vo vašej krajine kultúra kybernetickej bezpečnosti v skorej fáze vzdelávania študentov? Uprednostňujete napríklad vzdelávanie o kybernetickej bezpečnosti na druhom stupni základnej školy a na strednej škole?	1	Nabádate zamestnancov v súkromnom a verejnom sektore, aby získali akreditáciu alebo certifikáciu?	1	Máte v praxi zavedené mechanizmy na zaistenie konštantnej relevantnosti školení a vzdelávacích programov týkajúcich sa aktuálnych a vznikajúcich technologických pokrokov, zmien v oblasti hrozieb, právnych nariadení a národných bezpečnostných smerníc?	1
	2	-		Ponúkajú univerzity vo vašej krajiny doktorandské štúdium kybernetickej bezpečnosti ako samostatný odbor a nie ako predmet počítačovej vedy?	1	Máte národné výskumné laboratóriá a vzdelávacie inštitúcie, ktoré sa špecializujú na kybernetickú bezpečnosť?	1	Vytvorila vaša krajina školenia o kybernetickej bezpečnosti alebo mentorské programy na podporu začínajúcich podnikov a SME v členských štátoch?	1	Vytvárate akademické centrá excelentnosti v oblasti kybernetickej bezpečnosti, ktoré majú fungovať ako centrá výskumu a vzdelávania?	1
	3	-		Plánujete školiť pedagógov v oblasti kybernetickej bezpečnosti a problémov ochrany súkromia bez ohľadu na ich odbor? *Napr.* online bezpečnosť, ochrana osobných údajov, kybernetické šikanovanie.	1	Podporujete/financujete špecializované kurzy kybernetickej bezpečnosti a plány školení pre zamestnancov agentúr zamestnania v členských štátoch?	1	Podporujete aktívne zaradenie kurzov bezpečnosti informácií do vysokoškolského vzdelávania nielen pre študentov informatiky, ale aj pre všetky ostatné profesné špecializácie? *Napr.* kurzy prispôsobené potrebám konkrétnej profesie.	1	Zúčastňujú sa akademické inštitúcie na hlavných diskusiách v oblasti vzdelávania o kybernetickej bezpečnosti a výskume na medzinárodnej úrovni?	0
	4	-		-		Máte kurzy kybernetickej bezpečnosti a/alebo špecializovaný učebný plán pre úroveň EKR (európsky kvalifikačný rámec) 5 až 8?	1	Posudzujete pravidelne nedostatky v zručnostiach (nedostatok pracovníkov v oblasti kybernetickej bezpečnosti) v oblasti informačnej bezpečnosti?	1	-	

	5	-		-		Povzbudzujete a/alebo podporujete iniciatívy na zahrnutie kurzov bezpečnosti na internete do základného a stredoškolského vzdelávania?	1	Podporujete vytváranie sietí a spoločné využívanie informácií medzi akademickými inštitúciami na národnej aj medzinárodnej úrovni?	1		
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
7 - Posilnenie školiacich a vzdelávacích programov	6	-		-		Financujete alebo ponúkate občanom bezplatné základné školenia o kybernetickej bezpečnosti?	0	Zapájate súkromný sektor do každej formy iniciatív vzdelávania v oblasti kybernetickej bezpečnosti? *Napr.* navrhovanie a poskytovanie kurzov, stáže, odborné stáže…	1	-	
	7	-		-		Organizujete každoročné podujatia k informačnej bezpečnosti (napr. súťaže pre hackerov alebo programovacie maratóny)?	0	Implementujete finančné mechanizmy na vyzdvihnutie titulov v oblasti kybernetickej bezpečnosti? *Napr.* štipendiá, garantovaná prax/stáže, garantované pracovné miesta v konkrétnom odvetví alebo úlohy vo verejnom sektore	0	-	

Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
8 – Podpora výskumu a vývoja	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Uskutočnili ste štúdie alebo analýzy na identifikovanie priorít výskumu a vývoja v oblasti kybernetickej bezpečnosti?	1	Zaviedli ste procesy na stanovenie priorít výskumu a vývoja (napr. objavujúce sa témy o zabránení, ochrane, zistení a prijatí nových druhov kybernetických útokov)?	1	Existuje plán na prepojenie iniciatív výskumu a vývoja so skutočnou ekonomikou?	1	Sú iniciatívy výskumu a vývoja v oblasti kybernetickej bezpečnosti v súlade s relevantnými cieľmi stratégie, napr. DSM, H2020, Digitálne Európa, stratégia kybernetickej bezpečnosti Európskej únie?	1	Spolupracujete na národnej úrovni s medzinárodnými iniciatívami v oblasti výskumu a vývoja týkajúcimi sa kybernetickej bezpečnosti?	1

	2	-		Je súkromný sektor zapojený do stanovovania priorít výskumu a vývoja?	1	Zaviedli ste nejaké národné projekty súvisiace s kybernetickou bezpečnosťou?	1	Existuje hodnotiaci systém pre iniciatívy v oblasti výskumu a vývoja?	1	Sú priority výskumu a vývoja v súlade s aktuálnym alebo nadchádzajúcim nariadením (na národnej úrovni)?	1
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
8 – Podpora výskumu a vývoja	3	-		Je akademická oblasť zapojená do stanovovania priorít výskumu a vývoja?	1	Máte ekosystémy pre miestne/regionálne začínajúce podniky a ostatné kanály vytvárania sietí (napr. technologické parky, inovačné zoskupenia, podujatia/platformy na vytváranie sietí) na podporu inovácií (vrátane začínajúcich podnikov v oblasti kybernetickej bezpečnosti)?	1	Existujú nejaké dohody o spolupráci s univerzitami a inými výskumnými zariadeniami?	1	Zúčastňujete sa na hlavných diskusiách v jednej z mnohých moderných tém v rámci výskumu a vývoja na medzinárodnej úrovni?	0
	4	-		Existujú nejaké iniciatívy oblasti výskumu a vývoja týkajúce sa kybernetickej bezpečnosti?	0	Prebiehajú investície do programov výskumu a vývoja v oblasti kybernetickej bezpečnosti v akademickom prostredí a v súkromnom sektore?	1	Existuje uznávaný inštitucionálny orgán, ktorý dohliada na činnosti výskumu a vývoja?	0	-	
	5	-		-		Máte predsednícke funkcie pre priemyselný výskum na univerzitách, ktoré prepoja predmety výskumu s potrebami trhu?	1	-		-	
	6	-		-		Máte špecializované programy výskumu a vývoja v oblasti kybernetickej bezpečnosti?	0	-		-	

Cieľ NCSS	**#**	**Level 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
9 – Poskytnutie stimulov pre investície súkromného sektora v oblasti bezpečnostných opatrení	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						

	1	Existujú priemyselná stratégia alebo politická vôľa na podporu rozvoja odvetvia kybernetickej bezpečnosti?	1	Je súkromný sektor zapojený do navrhovania stimulov?	1	Existujú ekonomické/regulačné alebo iné druhy stimulov na podporu investícií do kybernetickej bezpečnosti?	1	Existujú nejakí súkromní činitelia, ktorí reagujú na stimuly investíciami do bezpečnostných opatrení? *Napr.* investori špecializujúci sa v kybernetickej bezpečnosti a nešpecializovaní investori	1	Zameriavate stimuly na témy kybernetickej bezpečnosti v závislosti od najnovšieho vývoja hrozieb?	1
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
9 – Poskytnutie stimulov pre investície súkromného sektora v oblasti bezpečnostných opatrení	2	-		Identifikovali ste konkrétne témy kybernetickej bezpečnosti, ktoré sa musia rozvíjať? *Napr.* kryptografia, súkromie, nová formy autentifikácie, AI pre kybernetickú bezpečnosť…	0	Poskytujete pomoc (napr. daňové stimuly) pre začínajúce podniky a malé a stredné podniky v oblasti kybernetickej bezpečnosti?	1	Poskytujete stimuly pre súkromný sektor na to, aby sa zameral na bezpečnosť pokročilých technológií? *Napr.* 5G, umelá inteligencia, IoT, kvantová výpočtová technika…	1	-	
	3	-		-		Poskytujete daňové stimuly alebo inú finančnú motiváciu pre investorov zo súkromného sektora pre začínajúce podniky v oblasti kybernetickej bezpečnosti?	1	-		-	
	4	-		-		Uľahčujete začínajúcim podnikom z oblasti kybernetickej bezpečnosti a malým a stredným podnikom prístup v procese verejného obstarávania?	0	-		-	
	5	-		-		Existuje rozpočet, ktorý sa používa na poskytovanie stimulov pre súkromný sektor?	0	-		-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
10 – Zlepšenie kybernetickej bezpečnosti dodávateľskej siete	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						

	1	Uskutočnili ste štúdiu o osvedčených bezpečnostných postupoch pre riadenie dodávateľskej siete, ktoré sa používa pri obstarávaní v rôznych segmentoch odvetvia a/alebo vo verejnom sektore?	1	Posudzujete kybernetickú bezpečnosť v celej dodávateľskej sieti služieb a produktov IKT v kritických sektoroch (ako je uvedené v prílohe II k smernici NIS (2016/1148))?	1	Používate systém certifikácie bezpečnosti pre produkty a služby na základe IKT? *napr.* SOG-IS MRA v Európe (skupina vedúcich pracovníkov pre bezpečnosť informačných systémov, dohoda o vzájomnom uznávaní), dohoda o vzájomnom uznávaní kritérií (CCRA), národné iniciatívy, iniciatívy v rámci sektorov…	1	Máte v praxi zavedený proces na aktualizovanie hodnotení kybernetickej bezpečnosti dodávateľskej siete služieb a produktov IKT v kritických sektoroch (ako je uvedené v prílohe II smernice NIS (2016/1148))?	1	Máte detekčné zariadenia v kľúčových prvkoch v dodávateľskej sieti na zistenie skorých znakov ohrozenia? *Napr.* bezpečnostné kontroly na úrovni ISP, bezpečnostné snímače v hlavných komponentoch infraštruktúry…	1

Cieľ NCSS	Č.	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
10 – Zlepšenie kybernetickej bezpečnosti dodávateľskej siete	2	-		Uplatňujete v rámci stratégií obstarávania verejnej správy normy na zabezpečenie toho, aby poskytovatelia produktov alebo služieb IKT spĺňajú základné požiadavky na informačnú bezpečnosť? *Napr.* ISO/IEC 27001 a 27002, ISO/IEC 27036…	1	Podporujete aktívne bezpečnosť a ochranu súkromia prostredníctvom navrhovania osvedčených postupov vo vývoji produktov a služieb IKT? *Napr.* životný cyklus vývoja bezpečnostných systémov, životný cyklus IoT	1	Máte v praxi zavedený proces na identifikovanie slabých miest dodávateľskej siete služieb kritických sektorov (ako je uvedené v prílohe II k smernici NIS (2016/1148))?	1	-	
	3	-		-		Vytvárate a poskytujete centralizované katalógy s podrobnejšími informáciami o existujúcej informačnej bezpečnosti a normách ochrany súkromia, ktoré môžu malé a stredné podniky rozšíriť a aplikovať?	1	Máte v praxi zavedený mechanizmus na zaistenie odolnosti produktov a služieb IKT, ktoré sú dôležité pre prevádzkovateľov základných služieb, proti kybernetickým útokom? (*Napr.* schopnosť zachovávať dostupnosť a bezpečnosť proti kybernetickému incidentu)? *Napr.* dôkladné testovanie, pravidelné hodnotenie, detekcia ohrozených prvkov…	1	-	
	4	-				Zúčastňujete sa aktívne na navrhovaní certifikačného rámca EÚ pre digitálne produkty, služby a procesy IKT podľa aktu o kybernetickej bezpečnosti prijatého v EÚ (nariadenie (EÚ) 2019/881)? *Napr.* účasť v skupine pre certifikáciu kybernetickej bezpečnosti (ECCG), podpora technických noriem a postupov pre bezpečnosť produktov/služieb IKT	0	Podporujete rozvoj systémov certifikácie zameraných na malé a stredné podniky s cieľom zlepšiť informačnú bezpečnosť a prijatie štandardu na ochranu súkromia?	0	-	
	5	-		-		Poskytujete malým a stredným podnikom nejaké druhy stimulov, aby prijali bezpečnostné normy a normy v oblasti ochrany súkromia?	0	Máte v praxi zavedené nejaké ustanovenia na povzbudenie veľkých spoločností pri zvyšovaní kybernetickej bezpečnosti malých podnikov v ich dodávateľských sieťach? *Napr.* centrum kybernetickej bezpečnosti, školiace kampane a kampane na zvyšovanie informovanosti…	0	-	

	6	-		-		Podporujete dodávateľov softvéru v tom, aby pomohli malým a stredným podnikom a zaistili bezpečné štandardné konfigurácie produktov určených pre malé organizácie?	0	-		-	

4.1.3 Klaster č. 3: Právne a zmluvné záležitosti

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
11 – Ochrana kritickej informačnej infraštruktúry, prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Existuje všeobecné porozumenie, že prevádzkovatelia CII prispievajú k národnej bezpečnosti?	1	Máte metodiku na identifikovanie nevyhnutných služieb?	1	Prijali ste smernicu NIS (2016/1148)?	1	Máte postup na aktualizovanie registra rizík?	1	Vytvárate a aktualizujete správy z oblasti hrozieb?	1

	2	-		Máte metodiku na identifikovanie CII?	1	Implementovali ste smernicu NIS (2008/114) o identifikácii a označení európskych kritických infraštruktúr a posúdení potreby zlepšiť ich ochranu?	1	Máte v praxi zavedené aj iné mechanizmy na zmeranie, či sú technické a organizačné opatrenia implementované prevádzkovateľom základných služieb vhodné na riadenie rizík pre bezpečnosť sietí a informačných systémov? Napr. pravidelné audity kybernetickej bezpečnosti, národný rámec pre implementovanie štandardných opatrení, technické nástroje poskytnuté vládou, ako napríklad detekčné zariadenia alebo prehľad konfigurácií špecifických pre konkrétny systém...	1	Ste v závislosti od posledného vývoja v oblasti hrozieb schopní zapojiť do svojho akčného plánu CII nový sektor?	1
	3	-		Máte metodiku na identifikovanie prevádzkovateľa základných služieb?	1	Máte národný register pre identifikovaných prevádzkovateľov základných služieb podľa kritického sektora?	1	Preskúmavate a následne aktualizujete zoznam identifikovaných prevádzkovateľov základných služieb aspoň každé dva roky?	1	Ste v závislosti od posledného vývoja v oblasti hrozieb schopní prijať do svojho akčného plánu CII nové požiadavky?	1

Cieľ NCSS	#										
11 – Ochrana kritickej informačnej infraštruktúry, prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb	4	-		Máte metodiku na identifikovanie poskytovateľov digitálnych služieb?	1	Máte národný register pre identifikovaných poskytovateľov digitálnych služieb?	1	Máte v praxi zavedené aj iné mechanizmy na zmeranie, či sú technické a organizačné opatrenia implementované poskytovateľom digitálnych služieb vhodné na riadenie rizík pre bezpečnosť sietí a informačných systémov? Napr. pravidelné audity kybernetickej bezpečnosti, národný rámec pre implementovanie štandardných opatrení, technické nástroje poskytnuté vládou, ako napríklad detekčné zariadenia alebo prehľad konfigurácií špecifických pre konkrétny systém...	1	-	
	5	-		Máte jeden alebo viac vnútroštátnych orgánov, ktoré poskytujú dohľad nad ochranou kritickej informačnej infraštruktúry a bezpečnosťou sietí a informačných systémov? Napr. podľa požiadavky smernice NIS (2016/1148)	1	Máte národný register rizík pre identifikované alebo známe riziká?	1	Preskúmavate a následne aktualizujete zoznam identifikovaných poskytovateľov digitálnych služieb aspoň každé dva roky?	1	-	
	6	-		Vytvárate plány ochrany špecifické pre konkrétne sektory? Napr. vrátane východiskových opatrení kybernetickej bezpečnosti (povinné alebo usmernenia)	0	Máte metodiku na mapovanie závislostí CII?	1	Používate systém certifikácie bezpečnosti (národný alebo medzinárodný) na pomoc prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb pri identifikovaní bezpečných produktov IKT? Napr. SOG-IS MRA v Európe, národné iniciatívy…	1	-	
	7	-		-		Zavádzate postupy riadenia rizík na identifikovanie, kvantifikovanie a riadenie rizík týkajúcich sa CII na národnej úrovni?	1	Používate systém certifikácie bezpečnosti alebo kvalifikačný postup na posúdenie poskytovateľov služby pracujúcich s prevádzkovateľom základných služieb? Napr. poskytovatelia služieb v oblasti detekcie incidentov, reakcie na incident, auditu kybernetickej bezpečnosti, cloudových služieb, čipových kariet…	1	-	

	8	-		-		Zapájate sa do konzultačného procesu na identifikovanie cezhraničných závislostí?	1	Máte v praxi zavedený mechanizmus na zmeranie úrovne dodržiavania východiskových opatrení kybernetickej bezpečnosti zo strany prevádzkovateľa základných služieb a poskytovateľov digitálnych služieb?	0	-	
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
11 – Ochrana kritickej informačnej infraštruktúry, prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb	9					Máte kontaktné miesto zodpovedné za koordinovanie záležitostí týkajúcich sa bezpečnosti sietí a informačných systémov na národnej úrovni a cezhraničnej spolupráce na úrovni Únie?	1	Uplatňujete nejaké právne úkony na zaistenie kontinuity poskytovaných služieb kritickou informačnou infraštruktúrou? Napr. očakávanie krízy, postupy na obnovu kritických informačných systémov, kontinuita činností bez IT, záložné postupy vzduchovej medzery…	0		
	10					Definujete východiskové opatrenia kybernetickej bezpečnosti (povinné alebo usmernenia) pre poskytovateľov digitálnych služieb a všetky sektory uvedené v prílohe II k smernici NIS (2016/1148)?	1				
	11	-		-		Poskytujete nástroje alebo metodiky na zistenie kybernetických incidentov?	1	-		-	

Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
12 – Riešenie počítačovej kriminality	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						

1	Uskutočnili ste štúdiu na identifikovanie požiadaviek presadzovania práva (právny základ, zdroje, zručnosti…) na efektívne riešenie počítačovej kriminality?	1	Je váš národný právny rámec úplne v súlade s relevantným právnym rámcom EÚ, vrátane smernice 2013/40/EÚ o útokoch na informačné systémy? Napr. protiprávny prístup do informačných systémov, protiprávny zásah do systému, protiprávny zásah do údajov, protiprávne odpočúvanie, nástroje použité na páchanie trestných činov...	1	Máte jednotky vyčlenené na riešenie počítačovej kriminality na prokuratúrach?	1	Zhromažďujete štatistické údaje podľa ustanovení článku 14 ods. 1 smernice 2013/40/EÚ (smernica o útokoch na informačné systémy)?	1	Máte medziinštitucionálne školenia alebo školiace pracovné semináre pre LEA, sudcov, prokurátorov a národné/vládne jednotky pre riešenie počítačových bezpečnostných incidentov na národnej úrovni a/alebo multilaterálnej úrovni?	1
2	Uskutočnili ste štúdiu na identifikovanie požiadaviek prokurátorov a sudcov (právny základ, zdroje, zručnosti…) na efektívne riešenie počítačovej kriminality?	1	Máte nejaké právne ustanovenie, ktoré sa zaoberá odcudzením identity na internete a krádeží osobných údajov?	1	Máte špecializovaný rozpočet pridelený jednotkám pre počítačovú kriminalitu?	1	Zhromažďujete samostatné štatistiky o počítačovej kriminalite? Napr. prevádzkové štatistiky, štatistiky o trendoch počítačovej kriminality, štatistiky o trestných stíhaniach pri počítačovej kriminalite a spôsobenej škode…	1	Zúčastňujete sa na koordinovaných akciách na medzinárodnej úrovni na rozbíjaní aktivít počítačovej kriminality? Napr. infiltrácia do zločineckých fór hackerov, organizované skupiny počítačovej kriminality, trhy na temných weboch a rozloženie botnetov…	1
3	Podpísala vaša krajina Dohovor o počítačovej kriminalite Rady Európskej únie z Budapešti?	1	Máte nejaké právne ustanovenie, ktoré sa zaoberá online duševným vlastníctvom a porušovaním autorských práv?	1	Zriadili ste centrálny orgán/subjekt na koordinovanie činností v oblasti boja proti počítačovej kriminalite?	1	Posudzujete adekvátnosť školení poskytovaných pre LEA, súdny personál a personál národnej jednotky pre riešenie počítačových bezpečnostných incidentov na riedenie počítačovej kriminality?	1	Existuje jasné oddelenie povinností v rámci jednotiek pre riešenie počítačových bezpečnostných incidentov, orgánov presadzovania práva a zamestnancov súdnej moci (prokurátori a sudcovia) pri ich spolupráci na riešenie počítačovej kriminality?	1
4			Máte nejaké právne ustanovenie, ktoré sa zaoberá obťažovaním na internete alebo kybernetickou šikanou?	1	Vytvorili ste mechanizmy spolupráce medzi relevantnými národnými inštitúciami zapojenými do boja proti počítačovej kriminalite, vrátane národných jednotiek pre riešenie počítačových bezpečnostných incidentov na presadzovanie práva?	1	Vykonávate pravidelné hodnotenia, aby ste zaistili dostatok zdrojov (ľudia, rozpočet a nástroje) vyčlenených pre jednotky bojujúce proti počítačovej kriminalite v rámci orgánov presadzovania práva?	1	Uľahčuje váš regulačný rámec spoluprácu medzi jednotkami pre riešenie počítačových bezpečnostných incidentov/LE a zamestnancami súdnej moci (prokurátori a sudcovia)?	1

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
12 – Riešenie počítačovej kriminality	5			Máte právne ustanovenie, ktoré sa zaoberá podvodmi súvisiacimi s počítačmi? Napr. dodržiavanie ustanovení Dohovoru o počítačovej kriminalite Rady Európskej únie z Budapešti	1	Spolupracujete a delíte sa o informácie s ostatnými členskými štátmi v oblasti boja proti počítačovej kriminalite?	1	Vykonávate pravidelné hodnotenia, aby ste zaistili dostatok zdrojov (ľudia, rozpočet a nástroje) vyčlenených pre jednotky bojujúce proti počítačovej kriminalite v rámci orgánov zodpovedných za stíhanie?	1	Zúčastňujete sa na budovaní a zachovávaní štandardizovaných nástrojov a metodík, foriem a postupov, ktoré sa majú spoločné používať so zainteresovanými stranami EÚ (LEA, jednotky pre riešenie počítačových bezpečnostných incidentov, ENISA, Europol, EC3…)?	1
	6	-		Máte právne ustanovenie, ktoré sa zaoberá ochranou detí na internete? Napr. dodržiavanie smernice 2011/93/EÚ a Dohovoru o počítačovej kriminalite Rady Európskej únie z Budapešti...	1	Spolupracujete a delíte sa o informácie s ostatnými agentúrami EÚ (napr. EC3 Europolu, Eurojust, ENISA) v oblasti boja proti počítačovej kriminalite?	1	Máte jednotky, osobitné súdy alebo špecializovaných sudcov, ktorí riešia prípady počítačovej kriminality?	1	Máte v praxi zavedené nejaké pokročilé mechanizmy na odradenie jednotlivcov od zapletenia sa alebo zapojenia sa do počítačovej kriminality?	0
	7	-		Identifikovali ste národné operačné kontaktné miesto na výmenu výmeny informácií a reagovanie na urgentné žiadosti o informácie z ostatných členských štátov v súvislosti s trestnými činmi definovanými v smernici 2013/40/EÚ (smernica o útokoch na informačné systémy)?	1	Máte adekvátne nástroje na riešenie počítačovej kriminality? Napr. taxonómia a klasifikácia počítačovej kriminality, nástroje na zber elektronických dôkazov, nástroje počítačovej forenznej analýzy, dôveryhodné platformy na výmenu informácií...	1	Máte zdroje vyhradené na poskytovanie podpory a pomoci obetiam počítačovej kriminality (bežní používatelia, malé a stredné podniky, veľké spoločnosti)?	1	Používa vaša krajina detailný plán EÚ a/alebo protokol reakcie na núdzové situácie v oblasti presadzovania práva (EÚ LE ERP) na efektívne zasiahnutie na rozsiahle kybernetické incidenty?	0
	8			Je súčasťou vášho orgánu na presadzovanie práva jednotka špecializovaná na počítačovú kriminalitu?	1	Máte štandardné operačné postupy na manipuláciu s elektronickými dôkazmi?	1	Zriadili ste medziinštitucionálny rámec a mechanizmy spolupráce medzi všetkými relevantnými zainteresovanými stranami (napr. LEA, národná jednotka pre riešenie počítačových bezpečnostných incidentov, súdne spoločenstvá), vrátane privátneho sektora (napr. prevádzkovatelia základných služieb, poskytovatelia služieb) tam, kde to bolo potrebné, na reakciu na kybernetické útoky?	1	-	
	9			Vytvorili ste kontaktné miesto s nepretržitou prevádzkou podľa čl. 35. Budapeštianskeho dohovoru?	1	Využíva vaša krajina príležitosti školení, ktoré ponúkajú a/alebo podporujú agentúry EÚ (napr. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Uľahčuje váš regulačný rámec spoluprácu medzi jednotkami pre riešenie počítačových bezpečnostných incidentov a LE?	1	-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
12 – Riešenie počítačovej kriminality	10	-		Vytvorili ste operačné kontaktné miesto s nepretržitou prevádzkou pre protokol reakcie na núdzové situácie v oblasti presadzovania práva EÚ (EÚ LE ERP) s cieľom reagovať na hlavné kybernetické útoky?	1	Zvažuje vaša krajina prijatie 2. dodatkového protokolu k Dohovoru o počítačovej kriminalite Rady Európskej únie z Budapešti?	0	Máte v praxi zavedené mechanizmy (napr. nástroje, postupy) na zjednodušenie výmeny informácií a spolupráce medzi jednotkou pre riešenie počítačových bezpečnostných incidentov/LE a prípadným súdnictvom (prokurátori, sudcovia) v oblasti boja proti počítačovej kriminalite?	1	-	
	11			Poskytujete pravidelné špecializované školenie pre zainteresované strany zapojené do riešenia počítačovej kriminality (LEA, súdnictvo, jednotky pre riešenie počítačových bezpečnostných incidentov)? Medziiným napr. školiace zasadania o plnení/súdnom stíhaní zločinov možných vďaka kybernetickému priestoru, školenia o zhromažďovaní elektronických dôkazov a zaistení integrity v rámci digitálneho reťazca väzby a počítačovej forenznej analýzy	1						
	12			Ratifikovala vaša krajina Dohovor o počítačovej kriminalite Rady Európskej únie z Budapešti alebo k nemu pristúpila?	1			-	-	-	
	13	-		Podpísala vaša krajina a ratifikovala dodatkový protokol (kriminalizácia skutkov rasizmu a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov) k Dohovoru o počítačovej kriminalite Rady Európskej únie z Budapešti?	0	-	-	-		-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
13 – Vytvorenie mechanizmov nahlasovania incidentov	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Máte neoficiálne mechanizmy poskytovania informácií o incidentoch v oblasti kybernetickej bezpečnosti medzi súkromnými organizáciami a vnútroštátnymi orgánmi?	1	Máte schému nahlasovania incidentov pre všetky sektory podľa prílohy II k smernici NIS?	1	Máte povinnú schému nahlasovania incidentov, ktorá v praxi funguje?	1	Máte harmonizovaný postup pre sektorové schémy nahlasovania incidentov?	1	Vytvárate každoročnú správu o incidentoch?	1
	2	-		Implementovali ste požiadavky oznámenia pre poskytovateľov telekomunikačných služieb v súlade s článkom 40 smernice (EÚ 2018/1972)? Podľa tejto smernice sa vyžaduje, aby členské štáty zabezpečili, že poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb oznámia bez zbytočného odkladu kompetentnému orgánu bezpečnostný incident, ktorý má významný vplyv na prevádzku sietí alebo služieb.	1	Existuje mechanizmus koordinácie/spolupráce pre povinnosti nahlasovania incidentov v súvislosti so všeobecným nariadením o ochrane údajov, smernicou o kybernetickej bezpečnosti (NIS), článkom 40 (ex-art13a) a nariadením eIDAS?	1	Máte schému nahlasovania incidentov pre iné sektory ako tie spadajúce pod smernicu NIS?	1	Sú v praxi zavedené nejaké správy o oblasti kybernetickej bezpečnosti alebo iné druhy analýzy, ktorú pripraví subjekt, ktorý správy o incidentoch dostáva?	1

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
13 – Vytvorenie mechanizmov nahlasovania incidentov	3	-		Implementovali ste požiadavky oznámenia pre poskytovateľov dôveryhodných služieb v súlade s článkom 19 nariadenia eIDAS (nariadene (EÚ) 910/2014)? Podľa článku 19 sa okrem iných požiadaviek vyžaduje, aby poskytovatelia dôveryhodných služieb oznámili dozornému orgánu významné incidenty/narušenia bezpečnosti.	1	Máte adekvátne nástroje na zaistenie dôvernosti a integrity informácií poskytnutých cez rôzne kanály nahlasovania?	1	Meriate efektívnosť postupov nahlasovania incidentov? *Napr.* ukazovatele incidentov, ktoré boli nahlásené prostredníctvom príslušných kanálov, načasovanie správy o incidente…	1	-	
	4	-		Implementovali ste požiadavky oznámenia pre poskytovateľov digitálnych služieb v súlade s článkom 16 smernice NIS? Podľa článku 16 sa vyžaduje, aby poskytovatelia digitálnych služieb bez zbytočného odkladu oznámili kompetentnému orgánu alebo národnej jednotke pre riešenie počítačových bezpečnostných incidentov každý incident, ktorý má významný vplyv na poskytovanie služieb tak, ako je uvedené v prílohe III, ktoré títo poskytovatelia ponúkajú v Únii.	1	Máte platformu/nástroj na zjednodušenie procesu nahlasovania?	0	Máte spoločnú taxonómiu na národnej úrovni na klasifikovanie incidentov a kategórie hlavných príčin?	0	-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
14 – Posilnenie ochrany súkromia a osobných údajov	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Uskutočnili ste štúdie alebo analýzy na identifikovanie oblastí zlepšenia ochrany práv na súkromie občanov?	1	Je národný orgán pre ochranu osobných údajov zapojený do záležitostí týkajúcich sa kybernetickej bezpečnosti (napr. navrhovanie nových zákonov a nariadení o kybernetickej bezpečnosti, definované minimálne bezpečnostné opatrenie)?	1	Podporujete osvedčené postupy v oblasti bezpečnostných opatrení a špecificky navrhnutú ochranu údajov pre verejný a/alebo súkromný sektor?	1	Vykonávate pravidelné hodnotenia, aby ste zabezpečili dostatok zdrojov (ľudia, rozpočet a nástroje) pre orgán pre ochranu osobných údajov?	1	Máte v praxi zavedené mechanizmy na monitorovanie najnovšieho vývoja v oblasti technológií, aby ste sa vedeli prispôsobiť príslušným usmerneniam a právnym ustanoveniami/povinnostiam?	1
	2	Vytvorili ste na národnej úrovni právny základ na presadzovanie všeobecného nariadenia o ochrane údajov (nariadenie EÚ č. 2016/679)? Napr. udržiavanie alebo zavedenie konkrétnejších ustanovení alebo obmedzení pravidiel nariadenia	0	-		Spustíte programy zvyšovania informovanosti a školiace programy k tejto téme?	1	Podporujete organizácie a podniky v získavaní certifikátov normy ISO/IEC 27701:2019 o systéme riadenia informácií o súkromí (PIMS)?	1	Aktívne sa zúčastňujete na iniciatívach v rámci výskumu a vývoja týkajúcich sa technológií na zvyšovanie súkromia (PET) a podporujete ich?	0
	3	-		-		Koordinujete postupy nahlasovania incidentov s orgánom pre ochranu osobných údajov?	1	-		-	
	4	-		-		Propagujete a podporujete vývoj technických noriem k informačnej bezpečnosti a súkromiu? Sú tieto normy konkrétne prispôsobené malým a stredným podnikom (MSP)?	0	-		-	

	5	-		-		Poskytujete praktické a rozšíriteľné usmernenia na podporu rôznych typov prevádzkovateľov pri plnení právnych požiadaviek a povinností týkajúcich sa ochrany súkromia a údajov?	0	-		-	

4.1.4 Klaster č. 4: Spolupráca

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
15 – Vytvorenie verejno-súkromného partnerstva (PPP)	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Existuje všeobecné uznanie, že verejno-súkromné partnerstvá rôznym spôsobom prispievajú k zvyšovaniu úrovne kybernetickej bezpečnosti v krajine? *Napr.* podelenie sa o záujmy o rast odvetvia kybernetickej bezpečnosti, spolupráca pri budovaní relevantné regulačného rámca kybernetickej bezpečnosti, podpora výskumu a vývoja...	1	Máte národný akčný plán na vytvorenie verejno-súkromných partnerstiev?	1	Vytvorili ste národné verejno-súkromné partnerstvá?	1	Vytvorili ste medzisektorové verejno-súkromné partnerstvá?	1	Dokážete v závislosti od najnovších technologických a regulačných pokrokov prijať alebo vytvoriť verejno-súkromné partnerstvá?	1
	2	-		Zabezpečujete právny alebo zmluvný rámec (konkrétne zákony, NDA, duševné vlastníctvo) na zahrnutie verejno-súkromných partnerstiev?	1	Vytvorili ste verejno-súkromné partnerstvá pre konkrétne sektory?	1	Zameriavate sa na spoluprácu medzi verejnými subjektmi a spoluprácu medzi súkromnými subjektmi vo vybudovaných verejno-súkromných partnerstvách?	1		
	3	-		-		Poskytujete financovanie na vytvorenie verejno-súkromných partnerstiev?	1	Podporujete verejno-súkromné partnerstvá medzi malými a strednými podnikmi (MSP)?	1	-	

	4	-		-		Sú verejné inštitúcie všeobecne na čele verejno-súkromných partnerstiev? *T. j.* jedno jednotné miesto kontaktu verejného sektora, ktoré spravuje a koordinuje PPP, verejné orgány sa vopred dohodnú na tom, čo chcú dosiahnuť, jasné usmernenia od verejnej správy k svojim potrebám a obmedzeniam pre súkromný sektor…	1	Meriate výsledky verejno-súkromných partnerstiev?	1	-	
	5	-		-		Ste členom zmluvného verejno-súkromného partnerstva (cPPP) Európskej organizácie kybernetickej bezpečnosti (ECSO)?	0	-		-	
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
15 – Vytvorenie verejno-súkromného partnerstva (PPP)	6	-		-		Existuje jeden alebo niekoľko PPP, ktoré pracujú na aktivitách národnej jednotky pre riešenie počítačových bezpečnostných incidentov?	0	-		-	
	7					Existuje jeden alebo niekoľko PPP, ktoré pracujú na záležitostiach ochrany kritickej informačnej infraštruktúry?	0				
	8	-		-		Existuje jeden alebo niekoľko PPP, ktoré pracujú na zvyšovaní povedomia o kybernetických otázkach a rozvoji zručností?	0	-		-	

Cieľ NCSS	**Č.**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
16 – Inštitucionalizovanie spolupráce medzi štátnymi orgánmi	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1
	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		

	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Máte neoficiálne kanály spolupráce medzi verejnými orgánmi?	1	Máte národnú schému spolupráce zameranú na kybernetickú bezpečnosť? *Napr.* dozorné rady, riadiace skupiny, fóra, rady, kybernetické centrá alebo skupiny na stretávanie odborníkov	1	Zúčastňujú sa štátne orgány na schéme spolupráce?	1	Zaisťujete, aby medzi týmito štátnymi orgánmi existovali kanály spolupráce venované kybernetickej bezpečnosti: spravodajské služby, domáce presadzovanie práva, orgány trestného stíhania, vládni činitelia, národná jednotka pre riešenie počítačových bezpečnostných incidentov a armáda?	1	Dostávajú štátny orgány jednotné minimálne informácie o najnovšom vývoji v oblasti hrozieb a situačné informácie o kybernetickej bezpečnosti?	1
	2	-		-		Vytvorili ste kooperačné platformy na výmenu informácií?	1	Meriate pri podpore efektívnej spolupráce úspech a obmedzenia rôznych schém spolupráce?	1	-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
16 – Inštitucionalizovanie spolupráce medzi štátnymi orgánmi	3	-		-		Definovali ste rozsah kooperačných platforiem (napr. úlohy a povinnosti, počet oblastí problémov)?	1	-		-	
	4	-		-		Organizujete každoročné zasadnutia?	1	-		-	
	5	-		-		Máte mechanizmy spolupráce medzi príslušnými orgánmi v rámci geografických regiónov? *Napr.* sieť bezpečnostných spravodajcov na každý región, referent pre kybernetickú bezpečnosť v regionálnych ekonomických komorách…	1	-		-	

Cieľ NCSS	#	Úroveň 1	R	Úroveň 2	R	Úroveň 3	R	Úroveň 4	R	Úroveň 5	R
17 – Zapojenie sa do medzinárodnej spolupráce (nielen s členskými štátmi EÚ)	a	Zahrniete tento cieľ do svojej aktuálnej NCSS alebo ho plánujete zahrnúť do jej ďalšej verzie?	1	Existujú neformálne postupy alebo aktivity, ktoré sa nekoordinovaným spôsobom podieľajú na dosahovaní cieľa?	1	Máte akčný plán, ktorý je oficiálne definovaný a zdokumentovaný?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste otestovali jeho funkčnosť?	1	Máte v praxi zavedené mechanizmy, ktoré zaistia, že akčný plán sa dynamicky zavedenie do environmentálneho vývoja?	1

	b			Definovali ste plánované výsledky, hlavné princípy alebo kľúčové aktivity svojho akčného plánu?	1	Máte akčný plán s jasným pridelením zdrojov a riadením?	1	Posudzujete svoj akčný plán s ohľadom na cieľ, aby ste zaistili, že sú v ňom správne stanovené priority a že je optimalizovaný?	1		
	c			Ak je to relevantné, je váš akčný plán implementovaný a už účinný v obmedzenom rozsahu?	0						
	1	Máte stratégiu medzinárodného zapojenia?	1	Máte dohody o spolupráci s ostatnými krajinami (bilaterálne, multilaterálne) alebo partnermi v iných krajinách? *Napr.* spoločné využívanie informácií, budovanie kapacít, pomoc…	1	Vymieňate si informácie na strategickej úrovni? *Napr.* stratégia na vysokej úrovni, vnímanie rizika...	1	Sú národné štátne orgány pre kybernetickú bezpečnosť vo vašej krajine zapojené do schém medzinárodnej spolupráce?	1	Vediete diskusie o jednej alebo viacerých témach v rámci multilaterálnych dohôd?	1
	2	Máte neoficiálne kanály spolupráce s ostatnými krajinami?	1	Máte jednotné kontaktné miesto, ktoré dokáže plniť styčnú úlohu s cieľom zabezpečiť cezhraničnú spoluprácu s orgánmi členských štátov (skupina pre spoluprácu, sieť jednotiek pre riešenie počítačových bezpečnostných incidentov…)?	1	Vymieňate si informácie na taktickej úrovni? *Napr.* bulletin aktérov hrozieb, ISAC, TTP…	1	Pravidelne vyhodnocujete výsledky iniciatív medzinárodnej spolupráce?	1	Vediete diskusie o jednej alebo viacerých témach v rámci medzinárodných dohôd alebo dohovorov?	1
Cieľ NCSS	**#**	**Úroveň 1**	**R**	**Úroveň 2**	**R**	**Úroveň 3**	**R**	**Úroveň 4**	**R**	**Úroveň 5**	**R**
17 – Zapojenie sa do medzinárodnej spolupráce (nielen s členskými štátmi EÚ)	3	Vyjadrili verejní vedúci predstavitelia zámer zapojiť sa do medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti?	1	Máte vyčlenených ľudí, ktorí sa zapájajú do medzinárodnej spolupráce?	1	Vymieňate si informácie na prevádzkovej úrovni? *Napr.* informácie o prevádzkovej koordinácii, prebiehajúce incidenty, IOC…	1	-		Vediete diskusie alebo rokovania na jednu alebo viaceré témy v rámci medzinárodných skupín expertov? *Napr.* celosvetová komisia pre stabilitu kybernetického priestoru (GCSC), ENISA, skupina pre spoluprácu NIS, Skupina OSN vládnych expertov pre bezpečnosť informácií (GGE)...	1
	4	-		-		Zapájate sa do medzinárodných cvičení v oblasti kybernetickej bezpečnosti?	1	-		-	
	5	-		-		Zapájate sa do medzinárodných iniciatív budovania kapacít? *Napr.* školenia, rozvoj zručností, navrhovanie štandardných postupov…	0	-		-	

	6	-		-		Uzavreli ste vzájomné dohody o pomoci s ostatnými krajinami? *Napr.* aktivity LEA, súdne konania, vytvorenie vzájomného vzťahu spôsobilostí na reakciu na incidenty, poskytnutie aktív pre kybernetickú bezpečnosť…	0	-		-
	7	-		-		Podpísali alebo ratifikovali ste medzinárodné dohody alebo dohovory v oblasti kybernetickej bezpečnosti? *Napr.* Medzinárodný kódex správania pre bezpečnosť informácií, Dohovor o počítačovej kriminalite	0	-		-

4.2 USMERNENIA PRE POUŽÍVANIE RÁMCA

Táto časť sa zameriava na poskytnutie niektorých usmernení a odporúčaní pre členské štáty k predstaveniu rámca a vyplneniu dotazníka. Nižšie uvedené odporúčania sú odvodené najmä zo spätnej väzby zozbieranej počas rozhovorov s predstaviteľmi členských štátov:

- **Predvídanie koordinovaných aktivít na zber údajov a ich konsolidovanie.** Väčšina členských štátov uznáva, že vykonanie takéhoto postupu sebahodnotenia by malo trvať približne 15 osobodní. Vykonanie sebahodnotenia si bude vyžadovať veľké množstvo rôznych zainteresovaných strán. Preto sa odporúča vyhradiť si čas na prípravnú fázu, aby bolo možné identifikovať všetky relevantné zainteresované strany v rámci vládnych orgánov, štátnych orgánov a súkromného sektora.
- **Identifikovanie centrálneho orgánu, ktorý je zodpovedný za dokončenie sebahodnotenia na národnej úrovni.** Keďže zber materiálu pre všetky ukazovatele NCAF môže zahŕňať množstvo zainteresovaných strán, odporúča sa mať k dispozícii centrálny orgán alebo úrad poverený dokončením sebahodnotenia prostredníctvom úzkej spolupráce a koordinácie so všetkými zainteresovanými stranami.
- **Použitie postupu hodnotenia ako spôsobu podelenia sa a komunikácie o témach kybernetickej bezpečnosti.** Zo skúseností členských štátov vyplýva, že diskusie (či už vo formáte individuálnych rozhovorov alebo kolektívnych seminárov) sú dobrou príležitosťou na podporu dialógu o témach kybernetickej bezpečnosti a na výmenu spoločných názorov a oblastí zlepšenia. Okrem objasnenia kľúčových úspechov môže šírenie výsledkov takisto pomôcť pri propagácii tém kybernetickej bezpečnosti.
- **Použitie NCSS ako rámca na výber cieľov podrobených vyhodnoteniu.** Na základe spoločných cieľov členských štátov v ich NCSS sa vytvorilo 17 cieľov, ktoré tvoria NCAF. Ciele, ktoré sú súčasťou NCSS, by sa mali použiť ako prostriedok na vytvorenie rámca hodnotenia. NCSS by ale nemala hodnotenie obmedzovať. Keďže sa NCSS prirodzene zameriava na priority, určité oblasti sú z nej zámerne vynechané. To ale neznamená, že daná spôsobilosť neexistuje. Napríklad v prípade, kedy sa z NCSS vynechá konkrétny cieľ, ale krajina má spôsobilosti v oblasti kybernetickej bezpečnosti týkajúce sa tohto cieľa, môže sa uskutočniť hodnotenie tohto cieľa.
- **Pri rozvoji NCSS zabezpečte, aby výklad skóre zostal v súlade s vývojom NCSS.** Životný cyklus NCSS je viacročný proces. NCSS niektorých členských štátov sa zvyčajne presadia s 3 až 5-ročným plánom so zmenami v rozsahu medzi dvomi za sebou idúcimi verziami NCSS. Preto je potrebné, aby sa mimoriadna pozornosť venovala prezentovaniu výsledkov sebahodnotenia medzi dvomi verziami NCSS: zmeny rozsahu môžu skutočne ovplyvniť konečné skóre zrelosti. Odporúča sa porovnať skóre celého rozsahu strategických cieľov z jedného roka s iným rokom (*t. j.* celkové všeobecné skóre).

Pripomienka k bodovaciemu mechanizmu – príklad ukazovateľa krytia
Bodovací mechanizmus zahŕňa dve úrovne skóre:
(i) **celkový všeobecný ukazovateľ krytia** na základe celého zoznamu strategických cieľov uvedených v rámci sebahodnotenia; a
(ii) **celkový špecifický ukazovateľ krytia** na základe strategických cieľov vybraných členskými štátmi (zvyčajne zodpovedajú cieľom uvedeným v NCSS konkrétnej krajiny).

Ako taký (pozri oddiel 3.1 o bodovacom mechanizme) bude celkový špecifický ukazovateľ krytia rovnaký alebo vyšší ako celkový všeobecný ukazovateľ krytia, pretože druhý z tejto dvojice môže zahŕňať ciele, ktoré nie sú súčasťou stratégie členských štátov, čím sa zníži celkový všeobecný ukazovateľ krytia. Ak členský štát pridá nový cieľ, celkový všeobecný ukazovateľ krytia sa zvýši (t. j. viac zahrnutých ukazovateľov zrelosti), naproti tomu celkové špecifická zrelosť sa môže znížiť (v prípade ak je novo pridaný cieľ v začiatočnej fáze a má preto nižšiu úroveň zrelosti).

- **Pri vypĺňaní dotazníka k sebahodnoteniu majte na pamäti, že primárnym cieľom je podpora členských štátov v budovaní kapacít v oblasti kybernetickej bezpečnosti.** Aj keď v niektorých prípadoch môže byť náročné odpovedať na otázku jednoznačným spôsobom, odporúča sa pri vypĺňaní sebahodnotenia vybrať odpoveď, ktorá je najbežnejšie akceptovaná. Ak je napríklad odpoveď na otázku ÁNO v určitom rozsahu, ale v inom rozsahu je to NIE, nemali by členské štáty zabúdať na to, že odpoveď NIE vyžaduje nejaké opatrenie: buď plán nápravy alebo plán pôsobenia na oblasť zlepšenia, na ktorý sa musí v budúcom rozvoji prihliadať.

5. ĎALŠIE KROKY

5.1 BUDÚCE ZLEPŠENIA

Počas rozhovorov so zástupcami členských štátov a počas fázy sekundárneho prieskumu boli ako potenciálny budúci vývoj identifikované tieto odporúčania na zlepšenie aktuálneho národného hodnotiaceho rámca spôsobilostí:

- **Vývoj bodovacieho systému, ktorý umožní vyššiu presnosť.** Namiesto binárnej odpovede ÁNO/NIE by sa napríklad mohla zaviesť percentuálna hodnota pokrytia, aby bolo možné lepšie objasniť komplexnosť konsolidácie spôsobilostí na národnej úrovni. Prvým krokom je jednoduchý postup s vybranou odpoveďou ÁNO/NIE.
- **Zavedenie kvantitatívnej metriky na zmeranie efektívnosti NCSS členských štátov.** Národný hodnotiaci rámec spôsobilostí sa skutočne zameriava na hodnotenie úrovne zrelosti spôsobilostí v oblasti kybernetickej bezpečnosti členských štátov. Je možné ho doplniť o metriku na zmeranie efektívnosti činností a akčných plánov implementovaných členskými štátmi na vybudovanie týchto spôsobilostí. V aktuálnej fáze sa nezdalo byť realistické vybudovať takúto metriku efektívnosti, pokiaľ uvážime, že: neexistuje dostatočná spätná väzba z tejto oblasti, je náročné nájsť zmysluplné ukazovatele, ktoré spoja výstup s implementáciou NCSS a je náročné vytvoriť realistické ukazovatele, ktoré je možné následne zhromaždiť. To ale zostáva témou do budúcnosti.
- **Posun z postupu sebahodnotenia na prístup hodnotenia.** Potenciálny budúci vývoj rámca môže predstavovať posun smerom k prístupu hodnotenia s cieľom posúdiť zrelosť spôsobilostí členských štátov v oblasti kybernetickej bezpečnosti, a to jednotnejším spôsobom. Minimalizovať potenciálnu odchýlku je skutočne možné vtedy, ak hodnotenie vykoná tretia strana.

PRÍLOHA A – PREHĽAD VÝSLEDKOV SEKUNDÁRNEHO PRIESKUMU

Príloha A obsahuje súhrn predchádzajúcej práce agentúry ENISA v oblasti NCSS a prehľad relevantných verejne dostupných modelov zrelosti kapacity v oblasti kybernetickej bezpečnosti. Pri výbere a preskúmaní modelov sa berú do úvahy tieto predpoklady:

- Nie všetky modely sú založené na prísnej metodike prieskumu;
- Štruktúra a výsledky modelov nie sú vždy podrobne vysvetlené s jasnými prepojeniami medzi rôznymi prvkami, ktoré každý model charakterizujú;
- Niektoré modely neponúkajú podrobnosti o procese vývoja, štruktúre a metodike hodnotenia;
- Ostatné modely a nástroje, ktoré sme našli, neponúkajú žiadne podrobnosti týkajúce sa štruktúry a obsahu, preto ich neuvádzame; a
- Výber modelov, ktoré sa majú posúdiť, je založený na geografickom pokrytí. Primárne sa zameriame na modely zrelosti kapacity v oblasti kybernetickej bezpečnosti, ktoré sú vytvorené na hodnotenie výkonu európskych krajín. Je ale dôležité rozšíriť geografické pokrytie a pri tvorbe modelov zrelosti na celom svete analyzovať osvedčené postupy.

Tento systematický prehľad relevantných verejne dostupných modelov zrelosti kapacity v oblasti kybernetickej bezpečnosti sa realizoval pomocou prispôsobeného rámca analýzy na základe metodiky definovanej Beckerom pre vyvíjanie modelov zrelosti[22]. Pre každý existujúci model zrelosti sa analyzovali tieto prvky:

- **Názov modelu zrelosti:** Názov modelu zrelosti a hlavné referencie;
- **Zdrojová inštitúcia:** Inštitúcia, verejná alebo súkromná, zodpovedná za navrhovanie modelu;
- **Všeobecný zámer a cieľ:** Celkový rozsah modelu a nezávislý cieľ/ciele;
- **Počet a definícia úrovní:** Počet úrovní zrelosti modelu, ako aj ich všeobecný popis;
- **Počet a názov atribútov:** Počet a názov atribútov, ktoré model zrelosti používa. Analýza atribútov má trojnásobný cieľ:
  - Rozbor modelu zrelosti na jednoducho zrozumiteľné časti;
  - Spojenie niekoľkých atribútov do klastrov atribútov s tým istým cieľom; a
  - Poskytnutie rozličných uhlov pohľadu na predmet úrovne zrelosti.
- **Metóda posudzovania:** Metóda posudzovania modelu zrelosti;

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213 – 222, Jun. 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

- **Prezentácia výsledkov**: Definovanie metódy vizualizácie výsledkov modelu zrelosti. Logika tohto kroku je, že modely zrelosti zvyknú zlyhať, ak sú príliš komplexné, a preto musí spôsob prezentácie spĺňať praktické potreby.

Predchádzajúca práca na NCSS

Agentúra ENISA zverejnila dva dokumenty na tému NCSS v roku 2012 ako súčasť svojich počiatočných snáh. Najprv navrhla v dokumente „Praktická príručka pre fázu vývoja a realizácie NCSS“[23] súbor konkrétnych krokov pre efektívnu implementáciu NCSS a predstavuje životný cyklus NCSS v štyroch fázach: vývoj stratégie, realizácia stratégie, hodnotenie stratégie a udržiavanie stratégie. Po druhé popísala v dokumente „Stanovenie kurzu pre národné snahy o posilnenie bezpečnosti v kybernetickom priestore“[24] stav stratégií kybernetickej bezpečnosti v rámci EÚ a mimo nej v roku 2012 a navrhla v ňom, že členské štáty by mali určiť spoločné predmety a rozdiely medzi ich NCSS.

V roku 2014 bol zverejnený prvý rámec agentúry ENISA pre hodnotenie NCSS členského štátu[25]. Tento rámec obsahuje odporúčania a osvedčené postupy, ako aj súbor nástrojov na budovanie kapacít na posúdenie NCSS (*napr.* identifikované ciele, vstupy, výstupy, kľúčové ukazovatele výkonu…). Tieto nástroje sú prispôsobené meniacim sa potrebám na rôznych úrovniach zrelosti v ich strategickom plánovaní. V tom istom roku zverejnila agentúra ENISA dokument „Online interaktívna mapa NCSS“[26], ktorý umožňuje používateľom rýchlo si prečítať NCSS všetkých členských štátov a krajín EZVO vrátane ich strategických cieľov a pozitívnych príkladov implementácie. Tento dokument bol najprv vytvorený ako archív NCSS (2014) a potom bol v roku 2018 doplnený o príklady implementácie a od roku 2019 funguje mapa ako *informačné centrum* na centralizovanie údajov poskytnutých členskými štátmi o svojich snahách pri zlepšovaní národnej kybernetickej bezpečnosti.

V roku 2016 bol zverejnený dokument „Príručka osvedčených postupov NCSS“[27], v ktorom je stanovených pätnásť strategických cieľov. Táto príručka tiež analyzuje stav implementácie NCSS v každom členskom štáte a identifikuje rôzne nedostatky a výzvy týkajúce sa tejto implementácie.

Následne v roku 2018 zverejnila agentúra ENISA dokument „Hodnotiaci nástroj stratégií kybernetickej bezpečnosti“[28]: interaktívny nástroj na sebahodnotenie, ktorý pomôže členským štátom posúdiť strategické priority a ciele týkajúce sa NCSS. Prostredníctvom súboru jednoduchých otázok poskytuje tento nástroj členským štátom konkrétne odporúčania na implementáciu každého cieľa. Nakoniec bol v roku 2019 zverejnený dokument „Osvedčené postupy pri inovovaní kybernetickej bezpečnosti podľa NCSS“[29], ktorý predstavuje tému inovácií v oblasti kybernetickej bezpečnosti podľa NCSS. Tento dokument vysvetľuje výzvy a osvedčené

[23] NCSS: Praktická príručka k tvorbe a realizácii (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Stanovenie kurzu pre národné snahy o posilnenie bezpečnosti v kybernetickom priestore (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] Hodnotiaci rámec pre NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] Národné stratégie kybernetickej bezpečnosti – interaktívna mapa (ENISA, 2014, aktualizované v roku 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Tento dokument je aktualizáciou príručky z roku 2012: Príručka osvedčených postupov NCSS: Navrhovanie a implementovanie národných stratégií kybernetickej bezpečnosti (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] Hodnotiaci nástroj národných stratégií kybernetickej bezpečnosti (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

postupy v rôznych rozmeroch inovácií tak, ako sú vnímané odborníkmi na túto tému s cieľom pomôcť navrhnúť budúce inovatívne strategické ciele.

A.1 Model zrelosti kapacít v oblasti kybernetickej bezpečnosti pre národy (CMM)

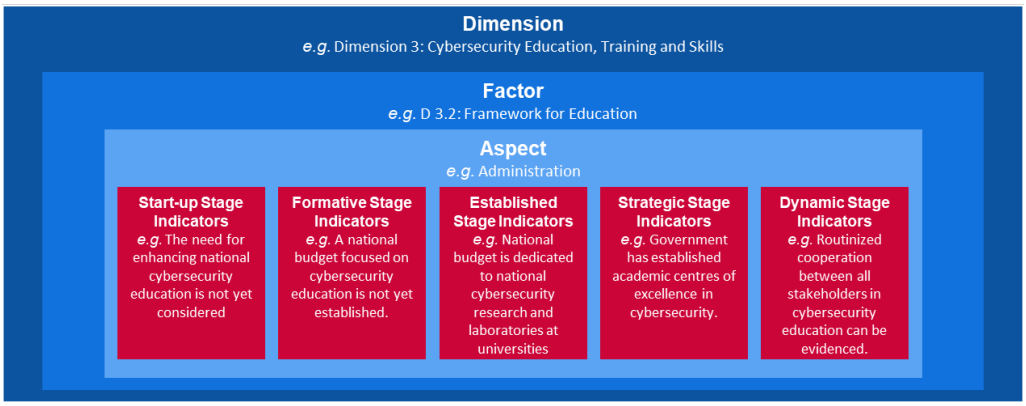
Model zrelosti kapacít v oblasti kybernetickej bezpečnosti pre národy (CMM) vyvinulo Globálne centrum kapacít v oblasti kybernetickej bezpečnosti (Centrum kapacít), ktoré je súčasťou Oxford Martin School v rámci Univerzity v Oxforde. Cieľom Centra kapacít je zvýšiť rozsah a efektívnosť budovania kapacít v oblasti kybernetickej bezpečnosti, v rámci Spojeného kráľovstva a na medzinárodnej úrovni, zavedením modelu zrelosti kapacít v oblasti kybernetickej bezpečnosti (CMM). CMM je priamo určený pre krajiny, ktoré chcú zvýšiť svoju národnú kapacitu v oblasti kybernetickej bezpečnosti. Pôvodne bol CMM zavedený v roku 2014, následne bol po používaní v roku 2016 prepracovaný počas posudzovanie 11 národných kapacít v oblasti kybernetickej bezpečnosti.

Atribúty/rozmery

Podľa CMM sa kapacita v oblasti kybernetickej bezpečnosti skladá z **piatich rozmerov**, ktoré predstavujú klastre kapacity v oblasti kybernetickej bezpečnosti. Každý klaster predstavuje rôzne „objektívy" prieskumu, cez ktoré je možné kapacitu v oblasti kybernetickej bezpečnosti študovať a pochopiť. V rámci týchto piatich aspektov popisujú **faktory** podrobnosti o vlastnení kapacity v oblasti kybernetickej bezpečnosti. Tieto podrobnosti sú prvkami, ktoré prispievajú k zlepšovaniu zrelosti kapacity v oblasti kybernetickej bezpečnosti v každom rozmere. Pre každý faktor predstavujú **aspekty** rôzne komponenty faktora. Aspekty predstavujú organizačnú metódu rozdelenie ukazovateľov na menšie klastre, ktoré sa jednoduchšie chápu. Každý aspekt sa potom posúdi pomocou **ukazovateľov** a popíšu sa kroky, akcie alebo stavebné bloky, ktoré poukazujú na konkrétnu fázu zrelosti (definovanú v ďalšej časti) v rámci jasného aspektu, faktora alebo rozmeru.

Uvedené výrazy je možné usporiadať podľa obrázku nižšie.

Obrázok 4: Príklad ukazovateľov CMM



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Rozmer napr. rozmer 3: Vzdelávanie, odborná príprava a zručnosti v oblasti kybernetickej bezpečnosti
Factor e.g. D 3.2: Framework for Education	Faktor napr. D 3.2: Rámec pre vzdelávanie
Aspect e.g. Administration	Aspekt napr.: správa
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Ukazovatele počiatočnej fázy napr. Ešte sa neuvažuje nad zlepšením vnútroštátneho vzdelávania v oblasti kybernetickej bezpečnosti

Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Ukazovatele formatívnej fázy napr. Národný rozpočet zameraný na vzdelávanie v oblasti kybernetickej bezpečnosti ešte nie zriadený
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Ukazovatele etablovanej fázy napr. Národný rozpočet je určený na národný výskum kybernetickej bezpečnosti a laboratóriá na univerzitách
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Ukazovatele strategickej fázy napr. Je možné dokázať, že vláda zriadila akademické centrum excelentnosti na vzdelávanie v oblasti kybernetickej bezpečnosti.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Ukazovatele dynamickej fázy napr. Rutinná spolupráca medzi všetkými zainteresovanými stranami

Päť rozmerov je detailne popísaných nižšie:

i Navrhnutie zásad a stratégie v oblasti kybernetickej bezpečnosti (6 faktorov);
ii Podpora zodpovednej kultúry v oblasti kybernetickej bezpečnosti v spoločnosti (5 faktorov);
iii Rozvoj vedomostí o kybernetickej bezpečnosti (3 faktory);
iv Vytvorenie efektívnych právnych a regulačných rámcov (3 faktory); a
v Riadenie rizík pomocou noriem, organizácií a technológií (7 faktorov).

Úrovne zrelosti

CMM používa **5 úrovní zrelosti** na určenie, do akej miery sa krajina posunula vzhľadom na určitý faktor/aspekt kapacity v oblasti kybernetickej bezpečnosti. Tieto úrovne slúžia ako zbežný prehľad existujúcej kapacity v oblasti kybernetickej bezpečnosti:

- **Počiatočná fáza**: V tejto fáze neexistuje buď žiadna zrelosť kybernetickej bezpečnosti, alebo je vo svojej počiatočnej podobe. Môžu existovať prvotné diskusie o budovaní kapacít v oblasti kybernetickej bezpečnosti, ale nepodnikli sa žiadne konkrétne kroky. V tejto fáze chýbajú pozorovateľné dôkazy;
- **Formatívna fáza**: Niektoré funkcie aspektov začali rásť a nadobúdať formu, ale môžu existovať len pre konkrétny prípad, môžu byť chaotické, nedostatočne definované alebo jednoducho „nové“. Dôkazy o tejto aktivite je však možné jasne preukázať;
- **Etablovaná fáza**: Prvky aspektu sú zavedené v praxi a fungujú. Zohľadnenie relatívneho pridelenia zdrojov však nebolo dobre premyslené. V súvislosti s „relatívnou“ investíciou do rôznych prvkov aspektu došlo k malým obchodným rozhodnutiam. Aspekt je ale funkčný a definovaný;
- **Strategická fáza**: Pre konkrétnu organizáciu alebo krajinu sa vybrali časti, ktoré sú dôležité a ktoré sú menej dôležité. Strategická fáza reflektuje skutočnosť, že tento výber sa uskutočnil v závislosti od národa alebo konkrétnych okolností organizácie a
- **Dynamická fáza**: V tejto fáze existujú jasné mechanizmy na zmenu stratégie v závislosti od prevažujúcich okolností, ako napríklad technológia prostredia hrozieb, globálny konflikt alebo významná zmena v oblasti záujmu (*napr.* počítačová kriminalita alebo súkromie). Dynamické organizácie vyvinuli metódy na jednoduchú zmenu stratégií. Charakteristikami tejto fázy je rýchle rozhodovanie, prerozdelenie zdrojov a neustála pozornosť venovaná meniacemu sa prostrediu.

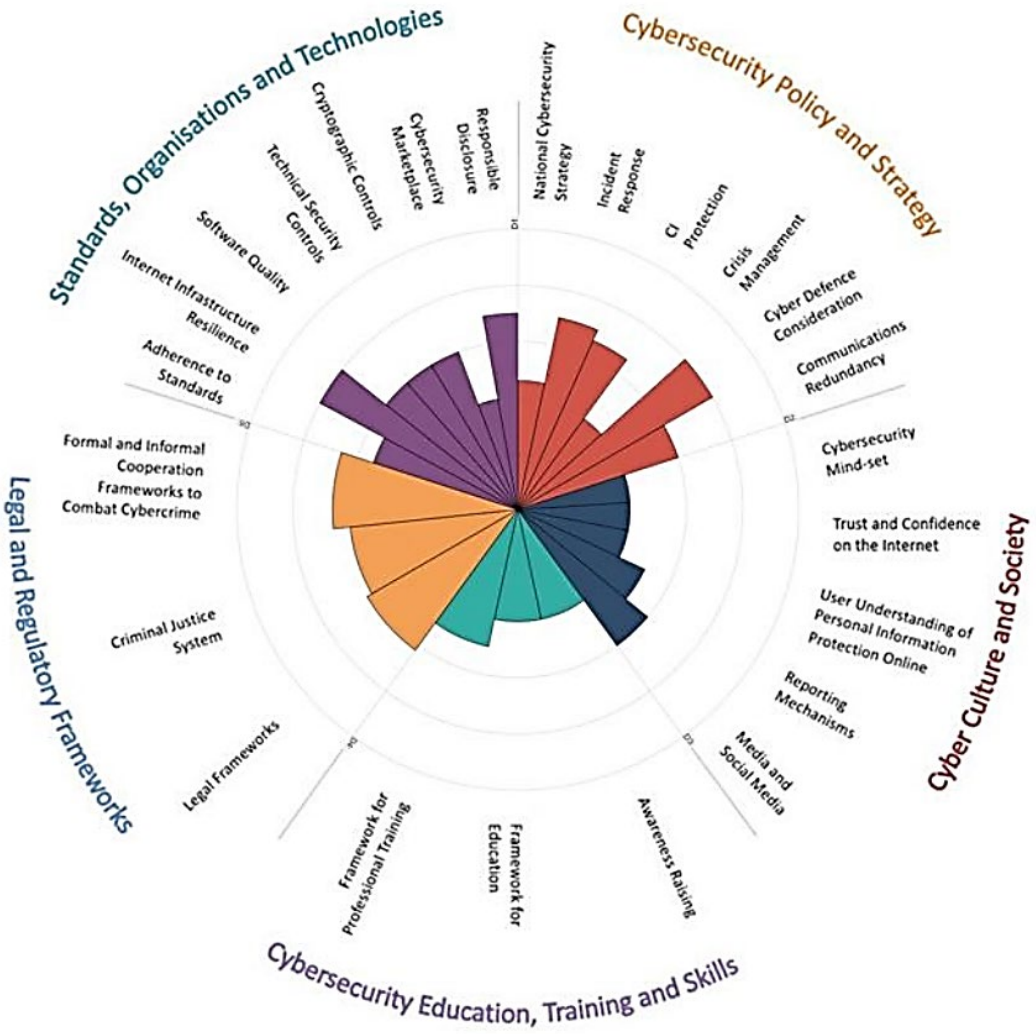
Metóda posudzovania

Keďže Centrum kapacít nemá dôkladné a podrobné informácie o kontexte v každej krajine, v ktorej sa model použije, pracuje spolu s medzinárodnými organizáciami, hostiteľskými ministrami alebo organizáciami v príslušnej krajine na posúdení zrelosti kapacít v oblasti kybernetickej bezpečnosti. Na posúdenie úrovne zrelosti piatich rozmerov zahrnutých v CMM sa Centrum kapacít a hostiteľské organizácie stretáva s príslušnými národnými zainteresovanými stranami z verejného a súkromného sektora počas 2 alebo 3 dní, kedy vytvoria skupinu respondentov pre rozmery v CMM. Každý rozmer prediskutujú rôzne klastre zainteresovaných strán minimálne dvakrát. Takto sa vytvorí predbežný súbor údajov pre následné posúdenie.

Spôsob alebo zobrazenie výsledkov

CMM poskytne prehľad úrovne zrelosti každej krajiny prostredníctvom radaru, ktorý sa bude skladať z piatich častí, jedna časť pre každý rozmer. Každý rozmer predstavuje jednu pätinu grafu s piatimi fázami zrelosti pre každý faktor, ktoré sa rozpínajú smerom von od stredu grafu, ako je zobrazené nižšie, „počiatočná fáza" je najbližšie k stredu grafu a „dynamická fáza" je na okraji.

Obrázok 5 CMM: Prehľad výsledkov



Standards, Organisations and Technologies	Normy, organizácie a technológie
Legal Regulatory Frameworks	Právne regulačné rámce
Cybersecurity Education, Training and Skills	Vzdelávanie, odborná príprava a zručnosti v oblasti kybernetickej bezpečnosti
Cybersecurity Policy and Strategy	Zásady a stratégie kybernetickej bezpečnosti
Cyber Culture and Society	Kybernetická kultúra a spoločnosť
Responsible Disclosure	Zodpovedná zverejňovanie údajov
Cybersecurity market place	Trhovisko kybernetickej bezpečnosti
Cryptographic Controls	Kryptografické riadiace prvky
Technical Security Controls	Technické bezpečnostné kontroly
Software Quality	Kvalita softvéru
Internet Infrastructure Resilience	Odolnosť internetovej infraštruktúry
Adherence to Standards	Dodržiavanie noriem

Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formálne a neformálne kooperačné rámce na boj s počítačovou kriminalitou
Criminal Justice System	Systém trestnej spravodlivosti
Legal Frameworks	Právne rámce
Framework for Professional Training	Rámec pre profesionálne školenie
Framework for Education	Rámec pre vzdelávanie
Awareness Raising	Zvyšovanie informovanosti
Media and Social Medai	Médiá a sociálne médiá
Reporting Mechanisms	Mechanizmy nahlasovania
User Understanding of Personal Information Protection Online	Pochopenie online ochrany osobných údajov používateľom
Trust and Confidence on the Internet	Dôvera a istota na internete
Cybersecurity Mind-set	Prístup ku kybernetickej bezpečnosti
Communications Redundancy	Nadbytočnosť komunikácia
Cyber Defence Consideration	Zváženie kybernetickej obrany
Crisis Management	Krízové riadenie
CI Protection	Ochrana CI
Incident Response	Reakcia na incidenty
National Cybersecurity Strategy	Národná stratégia kybernetickej bezpečnosti

Globálne centrum kapacít kybernetickej bezpečnosti Oxford Martin School, Univerzita v Oxforde, 2017.

A.2 Model zrelosti spôsobilosti kybernetickej bezpečnosti (C2M2)

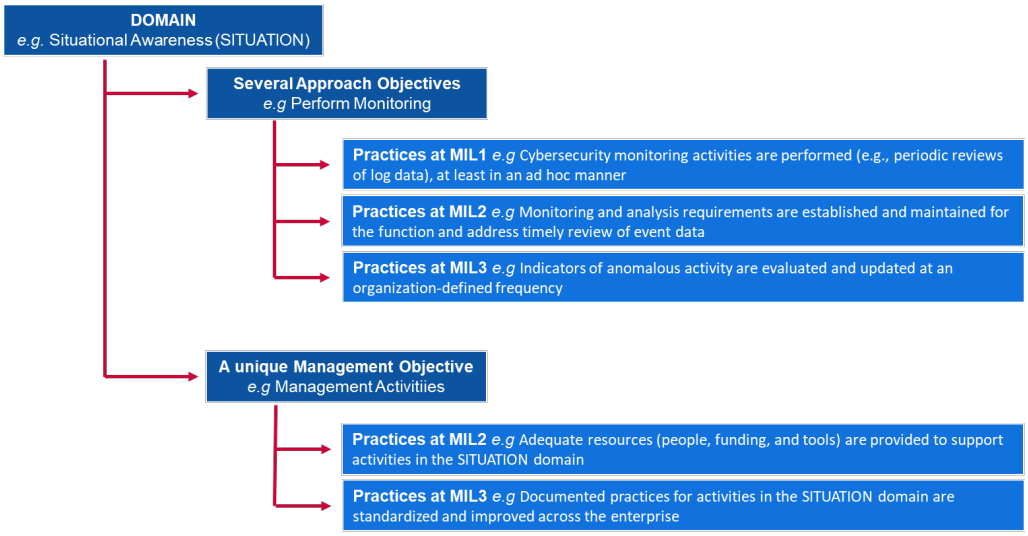
Model zrelosti kapacít v oblasti kybernetickej bezpečnosti (C2M2) vyvinulo americké Ministerstvo energetiky v spolupráci s expertmi zo súkromného a verejného sektora. Cieľom Centra kapacít je pomôcť organizáciám zo všetkých sektorov, typov a veľkostí posúdiť a zlepšiť ich programy kybernetickej bezpečnosti a posilniť prevádzkovú odolnosť. Model C2M2 sa zameriava na implementovanie a riadenie postupov kybernetickej bezpečnosti súvisiacich s aktívami spojenými s informáciami, informačnou technológiou (IT) a prevádzkovou technológiou (OT) a prostredím, v ktorom sa uplatňujú. Model C2M2 definuje modely zrelosti ako: „súbor charakteristík, atribútov, ukazovateľov alebo vzorov, ktoré predstavujú spôsobilosť a pokrok v konkrétnom odbore“. Model C2M2 bol pôvodne vytvorený v roku 2014 a v roku 2019 bol prepracovaný.

Atribúty/rozmery

Model C2M2 berie do úvahy **desať oblastí**, ktoré predstavujú logické zoskupenie postupov kybernetickej bezpečnosti. Každý súbor postupov predstavuje činnosti, ktoré dokáže organizácia vykonať na vytvorenie a rozvinutie spôsobilosti v tejto oblasti. Každá oblasť je spojená s **jedinečným cieľom riadenia** a **niekoľkými cieľmi prístupu**. V rámci cieľov riadenia aj prístupu je detailne uvedených **niekoľko postupov**, ktoré popisujú inštitucionalizované aktivity.

Vzťah medzi týmito pohľadmi je zhrnutý nižšie:

Obrázok 6: Príklad ukazovateľa C2M2



Domain eg Situational Awareness (SITUATION)	**Oblasť** napr. situačná informovanosť (SITUÁCIA)
Several Approaches Objectives e.g. Perform Monitoring	**Niekoľko cieľov prístupu** napr. vykonanie monitorovania
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 na MIL1** napr. vykonávajú činnosti monitorovania kybernetickej bezpečnosti (napr. pravidelné preskúmania údajov protokolov) minimálne ad hoc spôsobom
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Postupy na MIL2** napr. určenie a udržiavanie požiadavky na monitorovania a analýzu pre funkciu a riešenie včasného preskúmania údajov o udalosti
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Postupy na MIL3** napr. ukazovatele nezvyčajnej aktivity sa posúdia a aktualizujú v intervale definovanom organizáciou
A unique Management Objectve e.g. Management Activities	Jedinečný cieľ riadenia napr. riadiace činnosti
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Postupy na MIL2** napr. adekvátne zdroje (ľudia, finančné krytie a nástroje) sú k dispozícii na podporu činností v oblasti SITUÁCIE
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Postupy na MIL3** napr. zdokumentované postupy činností v oblasti SITUÁCIE sa v rámci podniku štandardizujú a zlepšia

Desať oblastí je detailne popísaných nižšie:

i Riadenie rizík (RIZIKO);
ii Riadenie aktív, zmien a konfigurácie (AKTÍVUM);
iii Riadenia prístupu a zisťovania identity (PRÍSTUP);
iv Riadenie hrozieb a zraniteľnosti (HROZBA);
v Situačná informovanosť (SITUÁCIA);
vi Reakcie na udalosti a incidenty (REAKCIA);
vii Riadenie dodávateľského reťazca a externých závislostí (ZÁVISLOSTI);
viii Riadenie pracovnej sily (PRACOVNÁ SILA);
ix Architektúra kybernetickej bezpečnosti (ARCHITEKTÚRA) a
x Riadenie programu kybernetickej bezpečnosti (PROGRAM).

Úrovne zrelosti

Model C2M2 používa **4 úrovne zrelosti** (pomenované ako úrovne ukazovateľov zrelosti – MIL (Maturity Indicator Level)) na určenie dvojitého pokroku zrelosti: pokrok prístupu a pokrok riadenia. Úrovne MIL existujú od MIL0 po MIL3 a sú určené na použitie nezávisle od každej oblasti.

- **MIL0**: Postupy sa nevykonajú.
- **MIL1**: Prvotné postupy sa vykonajú, ale môžu byť určené pre konkrétny prípad.
- **MIL2**: Charakteristiky riadenia:
  - Postupy sa zdokumentujú;
  - Sú k dispozícii adekvátne zdroje na podporu procesu;
  - Personál vykonávajúci tieto postupy má adekvátne zručnosti a vedomosti; a
  - Je pridelená zodpovednosť a oprávnenie na vykonávanie postupov.

  Charakteristika prístupu:
  - Postupy sú kompletnejšie alebo pokročilejšie ako v MIL1.

- **MIL3**: Charakteristiky riadenia:
  - Aktivity sa riadenia zásadami (alebo inými organizačnými smernicami);
  - Sú zriadenie a monitorujú sa ciele výkonu pre činnosti oblasti sa, aby bolo možné sledovať výsledok; a
  - Zdokumentované postupy činností oblasti sa štandardizujú a zlepšia v rámci celého podniku.

  Charakteristika prístupu:
  - Postupy sú kompletnejšie alebo pokročilejšie ako v MIL2.

Metóda posudzovania

Model C2M2 je určený na použitie s **metodikou sebahodnotenia** a súborom nástrojov (dostupným na požiadanie) pre organizáciu na zmeranie a zlepšenie programu kybernetickej bezpečnosti. Sebahodnotenie pomocou súboru nástrojov je možné dokončiť za jeden deň, ale súbor nástrojov by sa mohol prispôsobiť prísnejšiemu hodnoteniu. Model C2M2 je možné navyše použiť na navigovanie vývoja nového programu kybernetickej bezpečnosti.

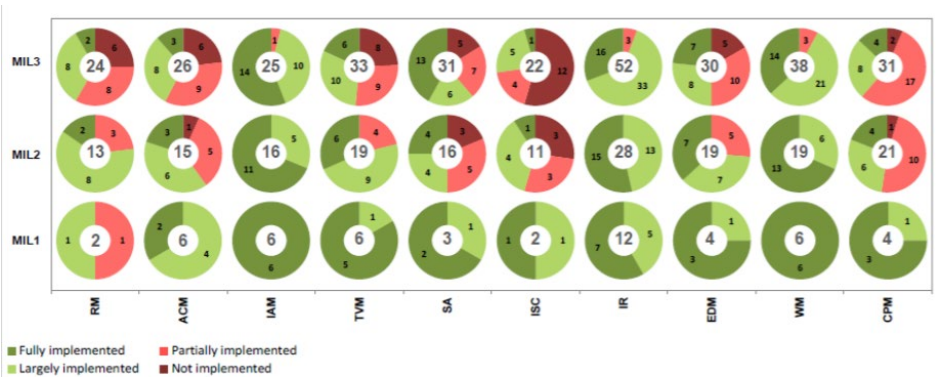
Obsah modelu je uvedený s vysokou úrovňou abstrakcie, takže ho môžu interpretovať organizácie rôznych druhov, štruktúr, veľkostí a z rôznych odvetví. Široké použitie modelu podľa sektora môže pomôcť pri referenčnom porovnávaní spôsobilostí v oblasti kybernetickej bezpečnosti tohto sektora.

Spôsob alebo zobrazenie výsledkov

Model C2M2 poskytuje bodovaciu správu hodnotenia, ktorá sa vygeneruje z výsledkov prieskumu. Táto správa predstavuje výsledky v dvoch pohľadoch: z pohľadu cieľa, ktorý ukazuje odpovede na praktické otázky podľa každej oblasti a jej cieľov a z pohľadu oblasti, ktorý ukazuje odpovede podľa všetkých oblastí a úrovní MIL. Obidva pohľady sú založené na systéme tvrdení, ktorý charakterizujú kruhové grafy (alebo „koláče“), jeden pre každú odpoveď, a bodovací mechanizmus semaforového systému. Ako je zobrazené na obrázku 7, červené sektory v koláčovom grafe udávajú počet otázok, na ktoré respondenti počas prieskumu uviedli odpoveď „neimplementované“ (tmavočervená) alebo „čiastočne implementované“ (svetločervená). Zelené sektory udávajú počet otázok, na ktoré respondenti uviedli odpoveď „zväčša implementované“ (svetlozelená) alebo „úplne implementované“ (tmavozelená).

Obrázok 7 nižšie je príkladom bodovacej karty na konci hodnotenia zrelosti. Na osi X je 10 oblastí modelu C2M2 a na osi Y sú úrovne zrelosti (MIL). Pri pohľade na graf a zohľadnení oblasti Riadenie rizík (RM), je možné si všimnúť tri kruhové grafy, jeden zodpovedá každej úrovni zrelosti ML1, ML2 a ML3. Pre oblasť RM zdôrazňuje tento graf, že na dosiahnutie prvej úrovne zrelosti, čiže ML1, existujú dve položky na hodnotenie. V tomto prípade má jedna bodovanie „zväčša implementované“ a jedna „čiastočne implementované“. Pre druhú úroveň zrelosti, čiže ML2, predpovedá model 13 položiek na hodnotenie. Dve z týchto 13 položiek patria do prevej úrovne ML1 a 11 do druhej úrovne ML2. To isté platí pre tretiu úroveň ML3.

Obrázok 7: C2M2 – Príklad prehľadu oblastí



Fully implemented	Úplne implementované
Largely implemented	Zväčša implementované

Partially implemented	Čiastočne implementované
Not implemented	Neimplementované
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: Americké Ministerstvo energetiky, úrad pre dodávku elektriny a energetickú spoľahlivosť, 2015.

A.3 Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry

Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry vyvinul Národný inštitút pre normy a technológie (NIST). Zameriava sa na riadenie aktivít v oblasti kybernetickej bezpečnosti a riadenie rizík v organizácii. Je určený pre všetky typy organizácií bez ohľadu na veľkosť, stupeň kybernetického rizika alebo sofistikovanosť kybernetickej bezpečnosti. Keďže tento rámce nie je modelom, je vytvorený inak ako predtým analyzované modely.

Rámec sa skladá z troch častí: jadro rámca, stupne implementácie a profily rámca:

- **Jadro rámca** je súbor aktivít kybernetickej bezpečnosti, želaných výsledkov a aplikovateľných referencií, ktoré sú spoločné v rámci sektorov kritickej infraštruktúry. Tie sa podobajú na atribúty alebo rozmery nachádzajúce sa v modeloch zrelosti kapacít kybernetickej bezpečnosti.
- **Stupne implementácie rámca** („stupne“) poskytujú kontext o tom, ako organizácia vníma kybernetické riziko a procesy používané na riadenie tohto rizika. Stupne, ktoré môžu byť čiastočné (stupeň 1) po adaptívne (stupeň 4), popisujú zvýšenie miery dôkladnosti a sofistikovanosti postupov riadenia kybernetického rizika. Stupne nepredstavujú úrovne zrelosti, skôr sú mienené ako pomoc pri organizačnom rozhodovaní o tom, ako riadiť kybernetické riziko, ako aj pri rozhodovaní, ktoré rozmery organizácie majú väčšiu prioritu a mohli by získať dodatočné zdroje.
- **Profil rámca** („profil“) predstavuje výsledky na základe obchodných potrieb, ktoré organizácia vybrala z kategórií a podkategórií rámca. Profil je možné charakterizovať s ohľadom na súlad s normami, usmerneniami a postupmi s jadrom rámca v konkrétnom scenári implementácie. Profily sa môžu použiť na identifikovanie príležitostí na zlepšenie stavu kybernetickej bezpečnosti pomocou porovnania „aktuálneho“ profilu (stav „tak ako je“) s „cieľovým“ profilom (stav, „ktorý má byť“).

Jadro rámca

Jadro rámca pozostáva z piatich **funkcií**. Keď sa tieto funkcie zoberú do úvahy spoločne, poskytujú vysokú úroveň strategického prehľadu o životnom cykle riadenia kybernetického rizika organizáciou. Jadro rámca potom identifikuje základné kľúčové **kategórie** a **podkategórie** pre každú funkciu a spojí ich s príkladom informatívnych referencií, ako napríklad existujúce normy, usmernenia a postupy pre každú podkategóriu.

Funkcie a kategórie sú detailne popísané nižšie:

i **Identifikovanie**: Rozvoj organizačného chápania spôsobu riadenia kybernetických rizík pre systémy, ľudí, majetok, údaje a spôsobilosti.
   - Podkategórie: správa majetku; obchodné prostredie; vláda; posúdenie rizík; a stratégia riadenia rizík

ii **Ochrana**: Rozvoj a implementácia vhodných záruk na zaistenie dodávania kritických služieb.

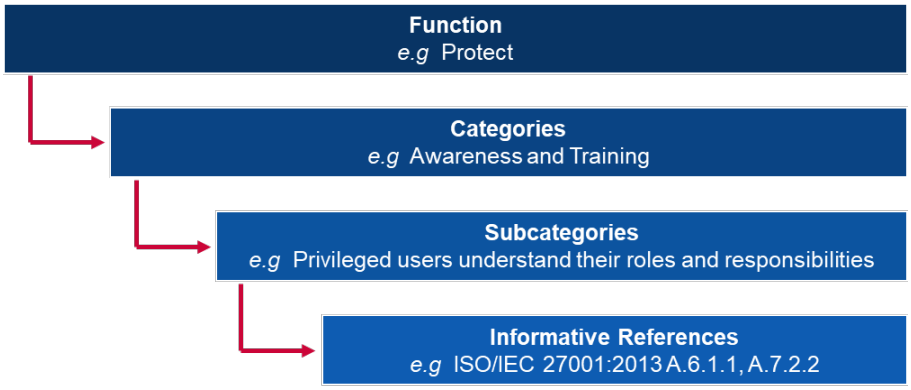
- Podkategórie: riadenie prístupu a zisťovania identity; informovanosť a odborná príprava; bezpečnosť údajov; procesy a postupy ochrany informácií; údržba; technológia ochrany

iii **Odhalenie**: Rozvoj a implementovanie vhodných činností na identifikovanie výskytu kybernetickej udalosti.
- Podkategórie: anomálie a udalosti; nepretržité monitorovanie bezpečnosti; proces detekcie.

iv **Reagovanie**: Rozvoj a implementovanie vhodných činností na podniknutie krokov s ohľadom na zistený kybernetický incident.
- Podkategórie: plánovanie reakcie; komunikácia; analýza; zmierňovanie a zlepšenia.

v **Obnovenie**: Rozvoj a implementovanie vhodných činností na udržiavanie plánov odolnosti a na obnovenie všetkých spôsobilostí alebo služieb, ktoré boli poškodené kybernetickým incidentom.
- Podkategórie: plánovanie obnovy; zlepšenia a komunikácia.

Obrázok 8: Príklad rámca pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry



Function e.g Project	**Funkcia** napr. projekt
Categories e.g Awarness and Training	**Kategórie** napr. povedomie a školenie
Subcategories e.g Privileged useres understand their roles and responsibilities	**Podkategórie** napr. privilegovaní používatelia chápu svoje úlohy a povinnosti
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informačné referencie** napr. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Stupne

Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry spočíva na **4 stupňoch**, z ktorých každý je definovaný na troch osiach: proces riadenia rizík, integrovaný program riadenia rizík a externá účasť. Tieto stupne sa nemajú považovať za úrovne zrelosti, ale ako rámec poskytujú organizáciám kontext pre svoje pohľady na kybernetické riziko a procesy používané na riadenie tohto rizika.

- **Stupeň 1: čiastočný**
  - **Proces riadenia rizík**: organizačné postupy riadenia kybernetických rizík nemajú formálnu podobu a riziko sa riadi ad hoc a niekedy reaktívnym spôsobom;
  - **Integrovaný program riadenia rizík**: na organizačnej úrovni existuje obmedzené povedomie o kybernetickom riziku. Organizácia implementuje riadenia kybernetických rizík na nepravidelnej báze od prípadu k prípadu a nemusí mať procesy, ktoré umožňujú poskytovanie informácií o kybernetickej bezpečnosti v rámci organizácie;
  - **Externá účasť**: organizácia nerozumie svojej úlohe vo väčšom ekosystéme buď s ohľadom na svoje závislosti alebo závislé subjekty. Organizácia si vo všeobecnosti nie je vedomá kybernetických rizík pre dodávateľský reťazec produktov a služieb, ktoré poskytuje a ktoré používa;

- **Stupeň 2: informovaný o riziku**
  - **Proces riadenia rizík**: postupy riadenia rizík schváli vedenie, ale nemusia byť určené ako stratégia v rámci organizácie;
  - **Integrovaný program riadenia rizík**: na organizačnej úrovni existuje povedomie o kybernetickom riziku, ale postup pre riadenie kybernetického rizika v celej organizácii neexistuje. Hodnotenie kybernetického rizika organizačných a externých aktív existuje, ale nie je zvyčajne opakovateľný ani sa nevyskytuje znova;
  - **Externá účasť**: organizácia vo všeobecnosti rozumie svojej úlohe vo väčšom ekosystéme buď s ohľadom na svoje vlastné závislosti alebo závislé subjekty, ale nie obidve tieto skupiny. Organizácia si je okrem toho vedomá kybernetických rizík pre dodávateľský reťazec, ktoré sú spojené s produktmi a službami, ktoré poskytuje a používa, ale s ohľadom na tieto riziká nekoná konzistentne alebo formálne;
- **Stupeň 3: opakovateľný**
  - **Proces riadenia rizík**: postupy riadenia rizík organizácie sú formálne schválené a vyjadrené vo forme stratégie. Organizačné postupy kybernetickej bezpečnosti sa pravidelne aktualizujú na základe aplikovania procesov riadenia rizík s ohľadom na zmeny v požiadavkách podniku/misie a meniacej sa oblasti hrozieb a technológií;
  - **Integrovaný program riadenia rizík**: existuje postup na riadenie kybernetického rizika v rámci celej organizácie. Stratégie využívajúce informácie o rizikách, proces a postupy sú definované, implementované podľa zámeru a preskúmané. Hlavní výkonní pracovníci zaistia zohľadnenie kybernetickej bezpečnosti vo všetkých líniách prevádzky v organizácii;
  - **Externá účasť**: organizácia rozumiem svojej úlohe, závislostiam a závislým subjektom vo väčšom ekosystéme a môže prispieť k širšiemu pochopeniu rizík v rámci spoločnosti. Organizácia si je vedomá kybernetických rizík pre dodávateľský reťazec, ktoré súvisia s produktmi a službami, ktoré poskytuje a ktoré používa;
- **Stupeň 4: adaptívny**
  - **Proces riadenia rizík**: organizácia prispôsobí svoje postupy kybernetickej bezpečnosti podľa predchádzajúcich a súčasných činností kybernetickej bezpečnosti, vrátane ponaučení zo skúseností a prediktívnych ukazovateľov;
  - **Integrovaný program riadenia rizík**: existuje postup na riadenie kybernetického rizika v rámci celej organizácie, ktorý uplatňuje stratégie využívajúce informácie o rizikách, procesy a postupy na pomenovanie potenciálnych kybernetických udalostí; a
  - **Externá účasť**: organizácia rozumie svojej úlohe, závislostiam a závislým subjektom vo väčšom ekosystéme a prispieva k širšiemu pochopeniu rizík v rámci spoločnosti.

Metóda posudzovania

Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry je určený pre organizácie na sebahodnotenie svojho rizika s cieľom zracionalizovať, zefektívniť a vytvoriť hodnotnejší prístup a investície do kybernetickej bezpečnosti. Na preskúmanie efektívnosti investícií musí organizácia najprv jasne rozumieť svojim organizačným cieľom, vzťahom medzi cieľmi a opornými výsledkami kybernetickej bezpečnosti. Výsledky kybernetickej bezpečnosti jadra rámca podporujú sebahodnotenie efektívnosti investovania a činností v oblasti kybernetickej bezpečnosti.

A.4 Katarský model zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti (Q-C2M2)

Katarský model zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti (Q-C2M2) vyvinula právnická fakulta Katarskej univerzity v roku 2018. Model Q-C2M2 je založený na rôznych existujúcich modeloch a tvorí komplexnú metodiku hodnotenia s cieľom zlepšiť katarský rámec kybernetickej bezpečnosti.

Atribúty/rozmery

Model Q-C2M2 preberá prístup rámca Národného inštitútu pre normy a technológie (NIST) pomocou piatich základných funkcií, ktoré sú hlavnými oblasťami modelu. Týchto päť základných funkcií sa používa v katarskom kontexte, pretože sú bežné v sektoroch kritickej infraštruktúry, čo je dôležitý prvok v katarskom rámci kybernetickej bezpečnosti. Model Q-C2M2 je založený na **piatich oblastiach**, z ktorých každá je rozdelená do niekoľkých **podoblastí**, ktoré pokrývajú celý rad zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti.

Päť oblastí je detailne popísaných nižšie:

i **Oblasť pochopenia** zahŕňa tieto podoblasti: výbor pre správu kybernetických záležitostí, riziká a školenie;
ii Podoblasti v **oblasti bezpečnosti** zahŕňajú bezpečnosť údajov, bezpečnosť technológie, bezpečnosť kontroly prístupu, bezpečnosť komunikácie a bezpečnosť personálu;
iii **Oblasť expozície** zahŕňa podoblasti monitoring, riadenie incidentov, detekcia, analýza a expozícia;
iv **Oblasť reakcie** zahŕňa plánovanie reakcií, zmierňovanie a komunikáciu o reakciách; a
v **Oblasť udržateľnosti** zahŕňa plánovanie obnovenia, riadenia kontinuity, zlepšovanie a externé závislosti.

Úrovne zrelosti

Model Q-C2M2 používa **5 úrovní zrelosti**, ktoré merajú zrelosť spôsobilosti štátneho subjektu alebo neštátnej organizácie na úrovni základnej funkcie. Tieto úrovne sú zamerané na hodnotenie zrelosti v piatich oblastiach, ktoré sú detailne popísané v predchádzajúcej časti.

- **Iniciovanie**: Používa v niektorých oblastiach ad hoc postupy a procesy kybernetickej bezpečnosti;
- **Implementovanie**: Prijaté stratégie na implementovanie všetkých aktivít kybernetickej bezpečnosti v oblastiach s cieľom dokončiť implementovanie v určitom čase;
- **Vývoj**: Implementované stratégie a postupy na vývoj a zlepšenie aktivít kybernetickej bezpečnosti v oblastiach s cieľom navrhnúť nové aktivity na zlepšenie;
- **Prispôsobenie**: Opätovné navštívenie a preskúmanie aktivít v oblasti kybernetickej bezpečnosti a prijatie postupov na základe prediktívnych ukazovateľov odvodených z predchádzajúcich skúseností a opatrení; a
- **Agilnosť**: Pokračovanie v uplatňovaní adaptívnej fázy so zvýšeným dôrazom na agilnosť a rýchlosť pri implementovaní aktivít v oblastiach.

Metóda posudzovania

Model Q-C2M2 je v začiatočnej fáze výskumu a ešte nie je pripravený na implementáciu. Je to rámec, ktorý by sa mohol v budúcnosti použiť na zavedenie detailného hodnotiaceho modelu pre katarské organizácie.

A.5 Certifikácia modelu zrelosti kybernetickej bezpečnosti (CMMC)

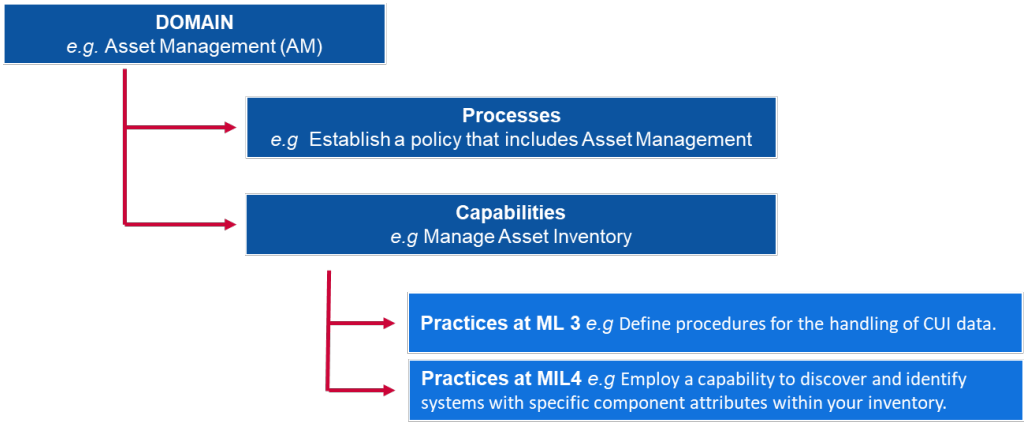
Certifikáciu modelu zrelosti kybernetickej bezpečnosti (CMMC) vyvinulo americké Ministerstvo obrany (DoD) v spolupráci s univerzitou Carnegie Mellon University a laboratóriom aplikovanej fyziky univerzity Johns Hopkins University. Hlavným cieľom DoD pri navrhovaní tohto modelu je ochrana informácií v sektore priemyselnej základne obrany (DIB). Informácie, na ktoré je CMMC zameraná, sa klasifikujú buď ako „federálne zmluvné informácie“, informácie poskytnuté alebo vygenerované vládou podľa zmluvy, ktoré nie sú určené na zverejnenie, alebo „regulované neutajené informácie“, čo sú informácie, ktoré vyžadujú ochranu alebo regulovanie rozširovania podľa zákonov, nariadení a stratégií celej vlády a v súlade s nimi. CMMC meria zrelosť kybernetickej bezpečnosti a poskytuje osvedčené postupy spolu s certifikačným prvkom, aby sa zaistila implementácia postupov súvisiacich s každou úrovňou zrelosti. Najnovšia verzia CMMC vyšla v roku 2020.

Atribúty/rozmery

CMMC zohľadňuje **sedemnásť oblastí**, ktoré predstavujú klastre procesov a spôsobilostí v oblasti kybernetickej bezpečnosti. Každá oblasť sa potom rozdelí na niekoľko **procesov**, ktoré sú v rámci oblastí podobné, a na jednu k mnohým **spôsobilostí**, ktoré pokrývajú päť úrovní zrelosti. Spôsobilosti (alebo spôsobilosť) sa potom podrobne rozdelia na **postupy** pre každú relevantnú úroveň zrelosti.

Vzťah medzi týmito pohľadmi je zobrazený nižšie:

Obrázok 9: Príklad ukazovateľov CMMC



DOMAIN e.g. Asset Management (AM)	**OBLASŤ** napr. správa majetku (AM)
Processes e.g Establish a policy that includes Asset Management	**Procesy** napr. vytvorenie stratégie, ktorá zahŕňa riadenie aktív
Capabilities e.g Manage Asset Inventory	**Spôsobilosti** napr. riadenie inventára aktív
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Postupy na ML 3** napr. definovane postupov pre zaobchádzanie s údajmi CUI
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Postupy na MIL4** napr. použitie spôsobilosti objaviť a identifikovať systémy s konkrétnymi atribútmi komponentu v rámci inventára

Sedemnásť oblastí je detailne popísaných nižšie:

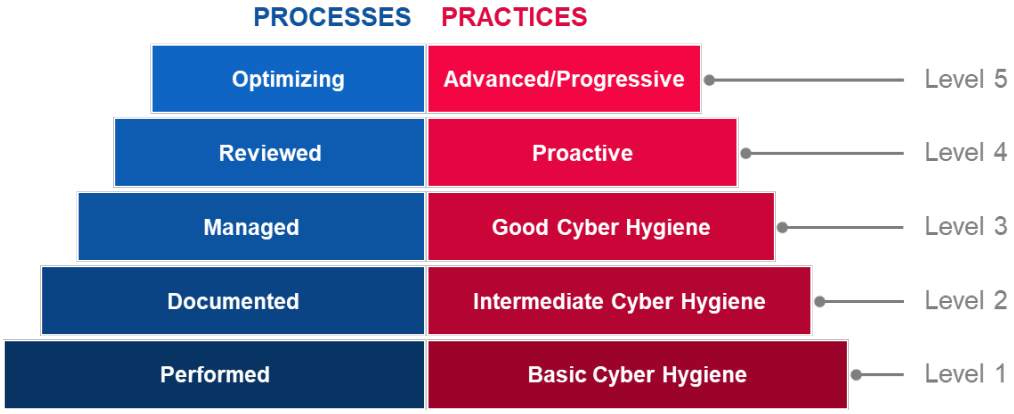
i Kontrola prístupu (AC);
ii Správa majetku (AM);
iii Audit a zodpovednosť (AU);
iv Informovanosť a odborná príprava (AT);
v Správa konfigurácie (CM);
vi Identifikácia a autentifikácia (IA);
vii Reakcia na incidenty (IR);
viii Údržba (MA);
ix Ochrana médií (MP);
x Bezpečnosť personálu (PS);
xi Fyzická ochrana (PE);
xii Obnova (RE);
xiii Riadenie rizík (RM);
xiv Analýza bezpečnosti (CA);
xv Situačná informovanosť (SA);
xvi Ochrana systémov a komunikácie (SC) a

xvii Integrita systémov a informácií (SI).

Úrovne zrelosti

CMMC používa **5 úrovní zrelosti**, ktoré sú definované na základe procesov a postupov. Na dosiahnutie určitej úrovne zrelosti v CMMC musí organizácia splniť predpoklady pre procesy a postupy určené pre túto úroveň. To tiež znamená splnenie predpokladov všetkých úrovní pod touto úrovňou.

Obrázok 10: Úrovne zrelosti CMMC



PROCESSES	PROCESY
Optimizing	Optimalizačné
Reviewed	Preskúmané
Managed	Riadené
Documented	Zdokumentované
Performed	Uskutočnené
PRACTICES	POSTUPY
Advanced/Progressive	Pokročilé/progresívne
Proactive	Proaktívne
Good Cyber Hygiene	Dobrá kybernetická hygiena
Intermediate Cyber Hygiene	Stredná kybernetická hygiena
Basic Cyber Hygiene	Základná 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 – uskutočnené**: keďže organizácia môže byť schopná uskutočniť ad hoc spôsobom len tieto procesy a môže ale nemusí sa spoliehať na dokumentáciu. Zrelosť procesu sa pre úroveň 1 neposudzuje;
  - **Postupy – základná kybernetická hygiena**: úroveň 1 sa zameriava na ochranu FCI (federálne zmluvné informácie) a pozostáva len z postupov, ktoré zodpovedajú základných bezpečnostným požiadavkám;
- **Úroveň 2**
  - **Procesy – zdokumentované**: úroveň 2 vyžaduje, aby organizácia zriadila a zdokumentovala postupy a stratégie, ktoré sa použijú na nasmerovanie implementácie jej úsilia na CMMC. Zdokumentovanie postupov umožňuje

jednotlivcom tieto postupy uskutočňovať opakovane. Organizácie vyvíjajú zrelé spôsobilosti pomocou dokumentovania svojich procesov a následným uplatňovaním týchto procesov ako zdokumentovaných;
- **Postupy – stredná kybernetická hygiena**: úroveň 2 slúži ako prechod z úrovne 1 na úroveň 3 a skladá sa z podskupiny bezpečnostných požiadaviek, ktoré sú špecifikované v NIST SP 800-171, ako aj postupov z iných noriem a referencií;

- **Úroveň 3**
  - **Procesy – riadené**: úroveň 3 vyžaduje, aby organizácia zriadila, udržiavala a zaistila prostriedky pre plán, ktorý ukáže riadenie aktivít pre implementovanie postupu. Plán môže obsahovať informácie o misiách, cieľoch, projektových plánoch, získavaní zdrojov, potrebnom školení a zapojení relevantných zainteresovaných strán;
  - **Postupy – dobrá kybernetická hygiena**: úroveň 3 sa zameriava na ochranu CUI a zahŕňa všetky bezpečnostné požiadavky špecifikované v NIST SP 800-171, ako aj ďalšie postupy z iných noriem a referencie na zmiernenie hrozieb;
- **Úroveň 4**
  - **Procesy – preskúmané**: úroveň 4 vyžaduje, aby organizácia preskúmala a zmerala efektívnosť postupov. Okrem merania efektívnosti postupov môžu organizácie v tejto úrovni podniknúť v prípade potreby opravný krok a opakovane informovať riadenie vyššej úrovne o stave a problémoch;
  - **Postupy – proaktívne**: úroveň 4 sa zameriava na ochranu CUI (regulované neutajené informácie) a zahŕňa podskupinu zlepšených bezpečnostných požiadaviek. Tieto postupy zlepšujú spôsobilosti detekcie a reakcie organizácie pri pomenovaní a prijímaní náročnej taktiky, techník a postupov;
- **Úroveň 5**
  - **Procesy – optimalizačné**: úroveň 5 vyžaduje od organizácie, aby štandardizovala a optimalizovala implementáciu procesu v organizácii a
  - **Postupy – pokročilé/proaktívne**: úroveň 5 sa zameriava na ochranu CUI. Ďalšími postupmi sa prehlbujú spôsobilosti v oblasti kybernetickej bezpečnosti a stávajú sa zložitejšími.

Metóda posudzovania

CMMC je relatívne mladý model, ktorý bol dokončený v prvom štvrťroku 2020. Zatiaľ nebol zavedený v rámci žiadnych organizácií. Napriek tomu dodávatelia DoD očakávajú, že na vykonanie auditov siahnu po certifikovaných kontrolóroch tretích strán. DoD očakáva od svojich dodávateľov, že implementujú osvedčené postupy na podporu kybernetickej bezpečnosti a ochranu citlivých informácií.

A.6 Model zrelosti kybernetickej bezpečnosti spoločenstva (CCSMM)

Model zrelosti kybernetickej bezpečnosti spoločenstva (CCSMM) vyvinulo Centrum pre zaistenie infraštruktúry a bezpečnosti na Texaskej univerzite (University of Texas). Cieľom modelu CCSMM je lepšie definovať metódy na určovanie aktuálneho stavu kybernetickej pripravenosti spoločenstva a poskytnúť spoločenstvám plán, pomocou ktorého budú postupovať vo svojom úsilí pri príprave. Spoločenstvá, na ktoré je model CCSMM zameraný, sú najmä samosprávy alebo vlády štátov. Model CCSMM bol skoncipovaný v roku 2007.

Atribúty/rozmery

Úrovne zrelosti sú definované podľa **6 hlavných rozmerov**, ktoré zahŕňajú rôzne aspekty kybernetickej bezpečnosti v spoločenstvách a organizáciách. Tieto rozmery sú jasne definované pre každú úroveň zrelosti (detailný popis nájdete na obrázku 31: Súhrn rozmerov CCSMM) Týchto 6 rozmerov zahŕňa:

i. pomenované hrozby,
ii. metrika,
iii. poskytovanie informácií,
iv. technológia,
v. školenie a

vi test.

Úrovne zrelosti

CCSMM spočíva na **5 úrovniach zrelosti** na základe hlavných typov hrozieb a aktivít, ktorými sa táto úroveň zaoberá:

- **Úroveň 1: Povedomie o bezpečnosti**
  Hlavnou témou aktivít na tejto úrovni je informovať jednotlivcov a organizácie o hrozbách, problémoch a záležitostiach týkajúcich sa kybernetickej bezpečnosti.
- **Úroveň 2: Vývoj procesu**
  Úroveň určená na pomoc spoločenstvám pri zriaďovaní a zlepšovaní bezpečnostných procesov potrebných na efektívne riešenie problémov kybernetickej bezpečnosti.
- **Úroveň 3: Povolené informácie**
  Navrhnuté na zlepšenie mechanizmov poskytovania informácií v rámci spoločenstva, aby bolo toto schopné efektívne nájsť vzťah medzi zdanlivo nezlučiteľnými informáciami.
- **Úroveň 4: Rozvoj taktiky**
  Táto úroveň je vytvorené na rozvoj lepších a proaktívnejších metód na zisťovanie a reagovanie na útoky. Pri tejto úrovni by mala byť v praxi zavedená väčšina preventívnych metód.
- **Úroveň 5: Plná bezpečnostná prevádzková spôsobilosť**
  Táto úroveň predstavuje tie prvky, ktoré by mali byť zavedené do praxe v každej organizácii, aby sa mohla považovať za plne prevádzkovo pripravenú na riešenie akéhokoľvek typu kybernetickej hrozby.

Obrázok 31: Súhrn rozmerov CCSMM podľa úrovne

	Level 1 Security Aware	Level 2 Process Development	Level 3 Information Enabled	Level 4 Tactics Development	Level 5 Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1 Security Aware	Úroveň 1 Povedomie o bezpečnosti
Level 2 Process Development	Úroveň 2 Vývoj procesu
Level 3 Information Enabled	Úroveň 3 Povolené informácie

Level 4 Tactics Development	Úroveň 4 Rozvoj taktiky
Level 5 Full Security Operational Capability	Úroveň 5 Plná bezpečnostná prevádzková spôsobilosť
Threats Addressed	Pomenované hrozby
Metrics	Metrika
Information sharing	Poskytovanie informácií
Technology	Technológia
Training	Odborná príprava
Test	Test
Unstructured	Neštruktúrované
Governement Industry Citizens	Vláda Priemysel Občania
Information Sharing Committee	Výbor pre poskytovanie informácií
Rosters, GETS, Assess Controls, Encryption	Rozpisy, GETS, kontroly prístupu, šifrovanie
1-day Community Seminar	1-dňový seminár spoločenstva
Dark Screen – EOC	Dark Screen – EOC
Unstructured	Neštruktúrované
Governement Industry Citizens	Vláda Priemysel Občania
Community Security Web site	Webová stránka bezpečnosti spoločenstva
Secure Web Site Firewalls, Backups	Systémy firewall zabezpečenej webovej stránky, zálohy
Conudcting a CCSE	Vykonanie CCSE
Community Dark Screen	Community Dark Screen
Structured	Štruktúrované
Governement Industry Citizens	Vláda Priemysel Občania
Information Correlation Center	Centrum korelácií informácií
Event Correlation SW IDS/IPS	Softvér korelácií udalostí IDS/IPS
Vulnerability Assessment	Posúdenie zraniteľnosti
Operational Dark Screen	Operational Dark Screen
Structured	Štruktúrované
Governement Industry Citizens	Vláda Priemysel Občania
State/Fed Correlation	Štátna/federálna korelácia
24/7 manned operations	Nepretržité operácie s obsluhou
Operational Security	Prevádzková bezpečnosť
Limited Black Demon	Limited Black Demon
Highly Structured	Vysoko štruktúrované
Governement Industry Citizens	Vláda Priemysel Občania
Complete Info Vision	Vízia úplných informácií
Automated Operations	Automatizované operácie
Multi-Discipline Red Teaming	Multidisciplinárny Red Teaming
Black Demon	Black Demon

Metóda posudzovania

CCSMM ako metódu posudzovania majú používať spoločenstvá spolu so vstupnými informáciami od štátnych orgánov a federálnych orgánov presadzovania práva. Jej cieľom je pomôcť spoločenstvám pri definovaní toho, čo je najdôležitejšie, aké sú najpravdepodobnejšie ciele a ktoré potreby je nevyhnutné chrániť (a v akom rozsahu). Pri zobrazí týchto cieľov na vedomie je možné vytvoriť plány, prostredníctvom ktorých sa každý aspekt spoločenstva dostane na potrebnú úroveň zrelosti kybernetickej bezpečnosti. Konkrétne informácie vygenerované

pomocou CCSMM pomôžu definovať ciele rôznych testov a cvičení, ktoré sa môžu použiť na zmeranie efektívnosti programov kybernetickej bezpečnosti.

A.7 Model zrelosti bezpečnosti informácií pre rámec kybernetickej bezpečnosti NIST (ISMM)

Model zrelosti bezpečnosti informácií (ISMM) vyvinula fakulta počítačových vied a inžinierstva na univerzite King Fahd University of Petroleum and Minerals v Saudskej Arábii. Navrhuje nový model zrelosti spôsobilosti na meranie implementácie opatrení kybernetickej bezpečnosti. Cieľom modelu ISMM je umožniť organizáciám na pravidelnej báze merať svoj progres v implementácii v čase pomocou rovnakého nástroja merania, čím sa zaistí udržanie želaného stavu bezpečnosti. Model ISMM vznikol v roku 2017.

Atribúty/rozmery

Model ISMM stavia na existujúcich pomenovaných oblastiach rámca NIST a pridáva rozmer hodnotenia súladu. Na základe toho má model **23 hodnotených oblastí** stavu bezpečnosti organizácie. Týchto 23 hodnotených oblastí sú:

i správa majetku,
ii obchodné prostredie,
iii správa a riadenie,
iv posúdenie rizík,
v stratégia riadenia rizík,
vi hodnotene súladu,
vii kontrola prístupu,
viii informovanosť a odborná príprava,
ix bezpečnosť osobných údajov,
x procesy a postupy ochrany informácií,
xi údržba,
xii ochranná technológia,
xiii anomálie a udalosti,
xiv nepretržité monitorovanie bezpečnosti,
xv procesy detekcie,
xvi plánovanie reakcií,
xvii komunikovanie reakcií,
xviii analýza reakcií,
xix zmiernenie reakcií,
xx zlepšenia reakcií,
xxi plánovanie obnovy,
xxii zlepšenia obnovy a
xxiii komunikovanie obnovy.

Úrovne zrelosti

Model ISMM je založený na **5 úrovniach zrelosti**, ktoré nie sú bohužiaľ v dostupnej dokumentácii detailne popísané.

- **Úroveň 1:** uskutočnený proces,
- **Úroveň 2:** riadený proces,
- **Úroveň 3:** zriadený proces,
- **Úroveň 4:** predvídateľný proces a
- **Úroveň 5:** optimalizačný proces.

Metóda posudzovania

Model ISMM nenavrhuje žiadnu konkrétnu metódu na uskutočnenie hodnotenia pre organizácie.

A.8 Model spôsobilosti vnútorného auditu (IA-CM) pre verejný sektor

Model spôsobilosti vnútorného auditu (IA-CM) vytvorila Výskumná nadácia inštitútu interných audítorov so zámerom vybudovať kapacitu a podporu prostredníctvom sebahodnotenia vo verejnom sektore. Model IA-CM je zameraný na odborníkov v oblasti auditu a poskytuje prehľad samotného modelu s príručkou na používanie, ktorá pomôže pri používaní modelu ako nástroja sebahodnotenia.

Napriek tomu, že sa model IA-CM skôr zameriava na spôsobilosť vnútorného auditu ako na budovanie kapacít v oblasti kybernetickej bezpečnosti, je zostavený ako nástroje sebahodnotenia zrelosti pre subjekty verejného sektora, ktorý je možné použiť globálne na zlepšenie procesov a efektívnosti. Keďže jeho záber nie je zameraný na kybernetickú bezpečnosť, atribúty sa neanalyzujú. Model IA-CM vznikol v roku 2009.

Úrovne zrelosti

Model spôsobilosti vnútorného auditu (IA-CM) zahŕňa **5 úrovní zrelosti**, z ktorých každá popisuje charakteristiky a spôsobilosti činnosti vnútorného auditu na tejto úrovni. Úrovne spôsobilosti v modeli poskytujú podrobný plán na nepretržité zlepšovanie.

- **Úroveň 1: počiatočný**
  Neexistujú žiadne udržateľné, opakovateľné spôsobilosti – závisia od individuálneho úsilia
  - Je ad hoc a neštruktúrovaná.
  - Samostatné jednotlivé audity alebo posúdenia presnosti a súladu dokumentov a transakcií.
  - Výstupy závisia od zručností konkrétnej osoby na danej pozícii.
  - Nie sú vytvorené žiadne odborné postupy ako tie, ktoré poskytnú profesionálne asociácie.
  - Financovanie podľa potreby schvaľuje vedenie.
  - Absencia infraštruktúry.
  - Audítori sú pravdepodobne súčasťou väčšej organizačnej jednotky.
  - Inštitucionálna spôsobilosť neexistuje.
- **Úroveň 2: infraštruktúra**
  Udržateľné a opakovateľné postupy a metódy
  - Kľúčovou otázkou alebo výzvou pre úroveň 2 je to, ako vytvoriť a zachovať opakovateľnosť procesov, a tým opakovateľnosť spôsobilosti.
  - Budujú sa vzťahy nahlasovania vnútorného auditu, infraštruktúra riadenia a správy a profesionálne postupy a procesy (vedenie vnútorného auditu, procesy a postupy).
  - Plánovanie auditu v princípe na základe priorít riadenia.
  - Pokračujúca závislosť od zručností a schopností konkrétnych osôb.
  - Čiastočný súlad s normami.
- **Úroveň 3: integrovaný**
  Jednotne aplikované postupy riadenia a profesionálne postupy
  - Stratégie vnútorného auditu a postupy sú definované, zdokumentované a integrované navzájom a do infraštruktúry organizácie.
  - Riadenie vnútorného auditu a profesionálne postupy sú dostatočne zriadené a jednotne aplikované v rámci činnosti vnútorného auditu.
  - Vnútorný audit začína byť v súlade s podnikaním organizácie a rizikami, ktorým organizácia čelí.
  - Vnútorný audit sa mení z vykonávania len bežného vnútorného auditu a integruje sa ako tímový hráč, ktorý poskytuje rady k výkonu a riadeniu rizík.
  - Pozornosť je zameraná na budovanie tímu a spôsobilosti aktivity vnútorného auditu a jeho nezávislosti a objektivity.
  - Vo všeobecnosti je v súlade s normami.
- **Úroveň 4: riadený**
  Integruje informácie od organizácie na zlepšenie vedenia a riadenia rizík
  - Očakávania vnútorného auditu a kľúčových zainteresovaných strán sa zhodujú.
  - Metrika výkonu je zavedená v praxi a meria a monitoruje procesy a výsledky vnútorného auditu.

- Vnútorný audit je uznávaný ako významný prínos organizácii.
- Vnútorný audit funguje ako neoddeliteľná súčasť vedenia a riadenia rizík organizácie.
- Vnútorný audit je dobre riadená obchodná jednotka.
- Riziká sa merajú a riadia kvantitatívne.
- Uplatňujú sa nevyhnutné zručnosti a schopnosti so spôsobilosťou obnovy a výmeny znalostí (v rámci interných auditov a v rámci organizácie).

▶ **Úroveň 5: optimalizačná**

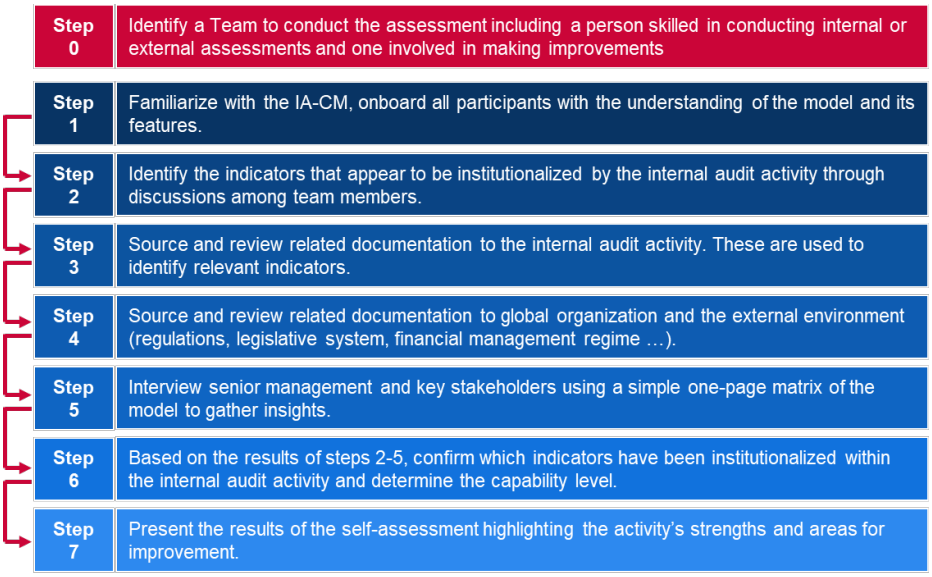
Učenie sa zvnútra a zvonku organizácie s cieľom nepretržitého zlepšovania

- Vnútorný audit je vzdelávajúca sa organizácia s nepretržitým zlepšovaním a inováciou procesu.
- Vnútorný audit používa informácia zvnútra a zvonku organizácie na to, aby prispel k dosiahnutiu strategických cieľov.
- Prvotriedny/odporúčaný výkon/realizovanie osvedčených postupov.
- Vnútorný audit je dôležitou súčasťou riadiacej štruktúry organizácie.
- Vrcholové profesionálne a špecializované zručnosti.
- Individuálne opatrenia, opatrenia v rámci jednotky a opatrenia výkonu organizácie sú plne integrované s cieľom
- podporovať zlepšenia výkonu.

Metóda posudzovania

Model spôsobilosti vnútorného auditu je jasne vytvorený pre sebahodnotenie. Poskytuje podrobné kroky, ktoré je potrebné dodržať na použitie modelu IA-CM a vzorového balíka prezentácie, ktorý je možné prispôsobiť. Pred spustením sebahodnotenia je potrebné určiť konkrétny tím, vrátane minimálne jednej osoby so skúsenosťami s vykonávaním interných alebo externých hodnotení vnútorných auditov a jednej osoby, ktorá bude zapojená do vylepšení v tejto oblasti.

Obrázok 12: Kroky sebahodnotenia modelu IC-AM



Step 0	0. krok
Step 1	1. krok
Step 2	2. krok
Step 3	3. krok
Step 4	4. krok
Step 5	5. krok
Step 6	6. krok
Step 7	7. krok

Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Určenie tímu, ktorý vykoná hodnotenie, vrátane osoby so skúsenosťami s internými a externými hodnoteniami a jednej osoby zapojenej do vytvárania zlepšení.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Oboznámenie sa s modelom IA-CM, zapojenie všetkých účastníkov s vedomosťami o modeli a jeho funkciách.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Identifikovanie ukazovateľov, ktoré sa zdajú byť inštitucionalizované pomocou aktivity vnútorného auditu na základe diskusie medzi členmi tímu.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Zaistenie zdrojov a posúdenie dokumentácie súvisiacej s aktivitou vnútorného auditu. Tie sa používajú na určenie relevantných ukazovateľov.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Zaistenie zdrojov a posúdenie dokumentácie súvisiacej s globálnou organizáciou a externým prostredím (nariadenia, legislatívny systém, režim finančného riadenia…).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Pohovor s vyšším vedením a kľúčovými zainteresovanými stranami prostredníctvom jednoduchej jednostranovej matice modelu a zistenie názorov.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Na základe výsledkov 2. – 5. kroku dôjde k potvrdeniu, ktoré ukazovatele sa v rámci aktivity vnútorného auditu inštitucionalizovali a určenie úrovne spôsobilosti.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Predstavenie výsledkov sebahodnotenia a poukázanie na silné stránky aktivity a oblasti na zlepšenie.

A.9 Globálny index kybernetickej bezpečnosti (GCI)

Globálny index kybernetickej bezpečnosti (GCI) je iniciatíva Medzinárodnej telekomunikačnej únie (ITU) zameraná na posúdenie angažovanosť a situácie kybernetickej bezpečnosti vo všetkých regiónoch ITU: Afrika, Severná a Južná Amerika, Arabské štáty, Ázijsko-pacifický región, Spoločenstvo nezávislých štátov a Európa a upriamenie pozornosti na krajiny s vysokou angažovanosťou a odporučiteľnými postupmi. Cieľom GCI je pomôcť krajinám nájsť oblasti na zlepšenie v odvetví kybernetickej bezpečnosti, ako aj motivovať ich k tomu, aby podnikali kroky na zlepšenie svojho postavenia, a tým pomohli zvýšiť celkovú úroveň kybernetickej bezpečnosti na celom svete.

Keďže CGI je index a nie model zrelosti, nepoužíva úrovne zrelosti, ale skôr bodovanie na určenie pozície a porovnanie celosvetovej angažovanosti v kybernetickej bezpečnosti jednotlivých národov a regiónov.

Atribúty/rozmery

Globálny index kybernetickej bezpečnosti (GCI) je založený na piatich pilieroch globálnej agendy kybernetickej bezpečnosti (GCA). Tieto piliere tvoria päť podindexov GCI a každý z nich obsahuje súbor ukazovateľov. Ide o týchto päť pilierov a ukazovatele:

i **Právny**: opatrenia založené na existencii právnych inštitúcií a rámcov zaoberajúcich sa kybernetickou bezpečnosťou a počítačovou kriminalitou.
- právne predpisy v oblasti kybernetickej bezpečnosti,
- nariadenie o kybernetickej bezpečnosti a

- obmedzenie/potlačenie nevyžiadanej legislatívy.

ii **Technický**: Opatrenia založené na existencii technických inštitúcií a rámcov zaoberajúcich sa kybernetickou bezpečnosťou.
- CERT/CIRT/CSRIT,
- implementačný rámec noriem,
- normalizačná organizácia,
- technické mechanizmy a spôsobilosti použité na riešenie spamu,
- použitie cloudu na účely kybernetickej bezpečnosti a
- mechanizmy ochrany detí na internete.

iii **Organizačný**: Opatrenia založené na existencii koordinačných inštitúcií zásad a stratégií pre vývoj kybernetickej bezpečnosti na národnej úrovni.
- národná stratégia kybernetickej bezpečnosti,
- zodpovedný orgán a
- kybernetická bezpečnosť.

iv **Budovanie kapacít**: Opatrenia založené na existencii výskumu a vývoja, vzdelávacích a školiacich programov, certifikovaných profesionálov a orgánov verejného sektora, ktoré podporujú budovanie kapacít.
- kampane na zvyšovanie informovanosti verejnosti,
- rámec na certifikáciu a akreditáciu profesionálov v oblasti kybernetickej bezpečnosti,
- profesionálne školiace kurzy v oblasti kybernetickej bezpečnosti,
- vzdelávacie programy alebo akademické študijné plány v oblasti kybernetickej bezpečnosti,
- programy výskumu a vývoja kybernetickej bezpečnosti a
- stimulačné mechanizmy.

v **Spolupráca**: Opatrenia založené na existencii partnerstiev, kooperačných rámcov a sietí na poskytovanie informácií.
- bilaterálne dohody,
- multilaterálne dohody,
- účasť na medzinárodných fórach/združeniach,
- verejno-súkromné partnerstvá,
- medziodborové/vnútroodborové partnerstvá a
- osvedčené postupy.

Metóda posudzovania

Index GCI je nástroj na sebahodnotenie vytvorený pomocou prieskumu[30] s použitím binárnych, predbežne stanovených a otvorených otázok. Použitie binárnych odpovedí eliminuje hodnotenia na základe vlastného názoru a všetky prípadné odchýlky smerom k určitým typom odpovedí. Vopred určené odpovede šetria čas a umožňujú presnejšiu analýzu údajov. Jednoduchá dichotomická stupnica okrem toho umožňuje rýchlejšie a komplexnejšie vyhodnotenie, pretože nevyžaduje dlhé odpovede, čím sa zrýchli a zjednoduší proces zadávania odpovedí a ďalšieho hodnotenia. Respondent by mal iba potvrdiť prítomnosť, alebo neprítomnosť, určitých vopred definovaných riešení v oblasti kybernetickej bezpečnosti. Mechanizmus online prieskumu, ktorý sa používa na zhromaždenie odpovedí a nahrávanie relevantných materiálov, umožňuje získanie osvedčených postupov a súboru tematických kvalitatívnych hodnotení panelom expertov.

Celý proces GCI sa implementuje takto:

- Všetci účastníci dostanú pozvánku, ktorá ich informuje o tejto iniciatíve a požiada ich o uvedenie ústrednej osoby na zhromaždenie všetkých relevantných údajov a dokončenie online dotazníka GCI. Počas online prieskumu dostane ústredná osoba oficiálnu pozvánku od ITU, aby dotazník vyplnila;
- Primárne získavanie údajov (pre krajiny, ktoré dotazník nevyplnia):

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

- ITU rozpracuje s využitím verejne dostupných údajov a online prieskumu prvý návrh odpovede na dotazník;
- Návrh dotazníka sa odošle ústredným osobám na posúdenie;
- Ústredné osoby zvýšia presnosť a potom odošlú návrh dotazníka späť;
- Opravený návrh dotazníka sa odošle ústrednej osobe na konečné schválenie a
- Potvrdený dotazník sa použije na analýzu, bodovanie a určenie pozície.

▶ Sekundárne získavanie údajov (pre krajiny, ktoré dotazník nevyplnia);
- ITU identifikuje všetky chýbajúce odpovede, nosné dokumenty, odkazy atď.;
- Ústredná osoba zvýši v prípade potreby presnosť odpovedí;
- Opravený návrh dotazníka sa odošle ústrednej osobe na konečné schválenie a
- Potvrdený dotazník sa použije na analýzu, bodovanie a určenie pozície.

A.10 Index kybernetickej moci (CPI)

Index kybernetickej moci (CPI) vytvoril výskumný program agentúry Economist Intelligence Unit sponzorovaný Booz Allen Hamiltonom v roku 2011. CPI je „dynamický kvantitatívny a kvalitatívny model, […], ktorý meria konkrétne atribúty kybernetického prostredia v rámci štyroch hnacích prvkov kybernetickej moci: právny a regulačný rámec; ekonomický a sociálny kontext; infraštruktúra technológie a priemyselná aplikácia, ktorá skúma digitálny pokrok v kľúčových odvetviach“[31]. Cieľom indexu kybernetickej moci je referenčne porovnať spôsobilosť krajín G20 odolávať kybernetickým úrokom a zavádzať digitálnu infraštruktúru potrebnú pre úspešnú a bezpečnú ekonomiku. Porovnania, ktoré umožňuje CPI, sa zameriava na 19 krajín G20 (okrem EÚ). Index následne poskytuje rebríček krajín pre každý ukazovateľ.

Atribúty/rozmery

Index kybernetickej moci (CPI) je založený na štyroch hnacích prvkoch kybernetickej moci. Každá kategória sa potom zmeria pomocou rôznorodých ukazovateľov a každá krajina dostane konkrétne skóre. Toto sú kategórie a piliere:

i **Právny a regulačný rámec**
- záväzok vlády smerom ku kybernetickému rozvoju,
- zásady kybernetickej ochrany,
- kybernetická cenzúra (alebo jej nedostatok),
- politická účinnosť,
- ochrana duševného vlastníctva.

ii **Ekonomický a sociálny kontext**
- úrovne vzdelávania,
- technické zručnosti,
- otvorenosť obchodu,
- stupeň inovácie v podnikateľskom prostredí.

iii **Infraštruktúra technológie**
- prístup k informačnej a komunikačnej technológii,
- kvalita informačnej a komunikačnej technológie,
- finančná dosiahnuteľnosť informačnej a komunikačnej technológie,
- náklady na informačnú technológiu,
- počet bezpečných serverov.

iv **Priemyselná aplikácia**
- inteligentné siete,
- elektronické zdravotníctvo,
- elektronický obchod,
- inteligentná doprava,
- elektronická verejná správa.

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

Metóda posudzovania

CPI je kvantitatívny a kvalitatívny bodovací model. Hodnotenie vykonáva agentúra Economist Intelligence Unit pomocou kvantitatívnych ukazovateľov z dostupných štatistických zdrojov a v prípade chýbajúcich údajov vytvorí odhady. Hlavnými zdrojmi sú agentúra Economist Intelligence Unit; Organizácia Spojených národov pre vzdelávanie, vedu a kultúru (UNESCO); Medzinárodná telekomunikačná únia (ITU) a Svetová banka.

A.11 Index kybernetickej moci (CPI)

Táto časť sumarizuje hlavné zistenia analýzy existujúcich modelov zrelosti. Tabuľka 5: Prehľad analyzovaných modelov zrelosti poskytuje prehľad hlavných charakteristík každého modelu podľa upraveného Beckerovho modelu. Tabuľka 6 Porovnanie úrovní zrelosti dôležité definície úrovní zrelosti analyzovaných modelov. Tabuľka 7 poskytuje prehľad rozmerov alebo atribútov použitých v každom modeli.

Tabuľka 5: Prehľad analyzovaných modelov zrelosti

Názov modelu	Zdroj inštitúcie	Účel	Cieľ	Počet úrovní	Počet atribútov	Metóda posudzovania	Predstavenie výsledkov
Model zrelosti kapacít v oblasti kybernetickej bezpečnosti pre národy (CMM)	Globálne centrum spôsobilosti kybernetickej bezpečnosti Oxfordská univerzita	Zvýšenie miery a efektívnosti budovania kapacít kybernetickej bezpečnosti na medzinárodnej úrovni	Krajiny	5	5 hlavných rozmerov	Spolupráca s miestnou organizáciou na doladení modelu pred jeho použitím v národnom kontexte	Päťdielny radar
Model zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti (C2M2)	Americké Ministerstvo energetiky (DOE)	Pomoc organizáciami pri hodnotení a zlepšovaní programov kybernetickej bezpečnosti a posilnenie ich digitálnej prevádzkovej odolnosti	Organizácie zo všetkých sektorov, typov a veľkostí	4	10 hlavných aspektov	Metodika sebahodnotenia a súbor nástrojov	Bodovacia karta s kruhovými grafmi
Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry	Národný inštitút pre normy a technológie (NIST)	Rámec zameraný na riadenie aktivít kybernetickej bezpečnosti a riadenie rizík v organizáciách	Organizácie	neuvedené (4 stupne)	5 hlavných funkcií	Sebahodnotenie	-
Katarský model zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti (Q-C2M2)	Fakulta práva na katarskej univerzite	Poskytnutie realizovateľného modelu, ktorý sa môže použiť na referenčné porovnávanie, meranie a vývoj katarského rámca kybernetickej bezpečnosti	Katarské organizácie	5	5 hlavných aspektov	-	-
Certifikácia modelu zrelosti kybernetickej bezpečnosti (CMMC)	Americké Ministerstvo obrany (DOD)	Podpora osvedčených postupov v oblasti kybernetickej bezpečnosti na ochranu informácií	Organizácie sektora priemyselnej základne obrany (DIB)	5	17 hlavných aspektov	Hodnotenie audítormi tretej strany	-
Model zrelosti kybernetickej bezpečnosti spoločenstva (CCSMM)	Centrum pre zaistenie infraštruktúry a bezpečnosti na Texaskej univerzite	Určenie aktuálneho stavu kybernetickej pripravenosti spoločenstva a poskytnutie plánu spoločenstvám, pomocou ktorého budú postupovať vo svojom úsilí pri príprave	Spoločenstvá (samosprávy alebo vlády štátov)	5	6 hlavných rozmerov	Hodnotenie v rámci komunít so vstupnými informácií od štátu a federálnych orgánov presadzovania práva	-
Model zrelosti bezpečnosti informácií pre rámec kybernetickej bezpečnosti NIST (ISMM)	Fakulta počítačových vied a inžinierstva Univerzita King Fahd University of Petroleum and, Minerals, Dhahran, Saudská Arábia	Umožnenie organizáciám merať svoj pokrok pri implementovaní v čase a zaistiť tak udržiavanie želaného stavu bezpečnosti	Organizácie	5	23 hodnotených oblastí	-	-
Model spôsobilosti vnútorného auditu (IA-CM) pre verejný sektor	Výskumná nadácia inštitútu interných audítorov	Vybudovanie spôsobilosti vnútorného auditu a podpora prostredníctvom sebahodnotenia vo verejnom sektore	Organizácie z verejného sektora	5	6 prvkov	Sebahodnotenie	-
Globálny index kybernetickej bezpečnosti (GCI)	Medzinárodná telekomunikačná únia (ITU)	Preskúmanie záväzku s ohľadom na kybernetickú bezpečnosť a situácie a	Krajiny	neuvedené	5 pilierov	Sebahodnotenie	Tabuľka s hodnotením

		pomoc krajinám pri identifikovaní oblastí na zlepšenie v kybernetickej bezpečnosti					
Index kybernetickej moci (CPI)	Agentúry Economist Intelligence Unit a Booz Allen Hamilton	Referenčné porovnanie spôsobilosti krajín G20 odolávať kybernetickým úrokom a zavádzať digitálnu infraštruktúru potrebnú pre úspešnú a bezpečnú ekonomiku.	Krajiny G20	neuvedené	4 kategórie	Referenčné porovnávanie agentúrou Economist Intelligence Unit	Tabuľka s hodnotením

Tabuľka 6 Porovnanie úrovní zrelosti

Model	Úroveň 1	Úroveň 2	Úroveň 3	Úroveň 4	Úroveň 5
Model zrelosti kapacít v oblasti kybernetickej bezpečnosti pre národy (CMM)	**Počiatočná fáza** Buď žiadna zrelosť kybernetickej bezpečnosti, alebo je vo svojej počiatočnej podobe. Môžu existovať prvotné diskusie o budovaní kapacít v oblasti kybernetickej bezpečnosti, ale nepodnikli sa žiadne konkrétne kroky. V tejto fáze chýbajú pozorovateľné dôkazy.	**Formatívna fáza** Niektoré funkcie aspektov začali rásť a nadobúdať formu, ale môžu existovať len pre konkrétny prípad, môžu byť chaotické, nedostatočne definované alebo jednoducho „nové“. Dôkazy o tejto aktivite je však možné jasne preukázať.	**Zriadená fáza** Prvky aspektu sú zavedené v praxi a fungujú. Zohľadnenie relatívneho pridelenia zdrojov však nebolo dobre premyslené. V súvislosti s „relatívnou“ investíciou do rôznych prvkov aspektu došlo k malým obchodným rozhodnutiam. Aspekt je ale funkčný a definovaný.	**Strategická fáza** Pre konkrétnu organizáciu alebo krajinu sa vybrali časti, ktoré sú dôležité a ktoré sú menej dôležité. Strategická fáza reflektuje skutočnosť, že tento výber sa uskutočnil v závislosti od národa alebo okolností organizácie.	**Dynamická fáza** Existujú jasné mechanizmy na zmenu stratégie v závislosti od prevažujúcich okolností, ako napríklad technológia prostredia hrozieb, globálny konflikt alebo významná zmena v oblasti záujmu (napr. počítačová kriminalita alebo súkromie). Dynamické organizácie vyvinuli metódy na jednoduchú zmenu stratégií. Charakteristikou tejto fázy je rýchle rozhodovanie, prerozdelenie zdrojov a neustála pozornosť venovaná meniacemu sa prostrediu.
Model zrelosti spôsobilosti kybernetickej bezpečnosti (C2M2)	**MIL0** Postupy sa nevykonajú.	**MIL1** Prvotné postupy sa vykonajú, ale môžu byť určené pre konkrétny prípad.	**MIL2** Charakteristiky riadenia: Postupy sa zdokumentujú; Sú k dispozícii adekvátne zdroje na podporu procesu; Personál vykonávajúci tieto postupy má adekvátne zručnosti a vedomosti; a Je pridelená zodpovednosť a oprávnenie na vykonávanie postupov. Charakteristika prístupu: Postupy sú kompletnejšie alebo pokročilejšie ako v MIL1.	**MIL3** Charakteristiky riadenia: Aktivity sa riadenia zásadami (alebo inými organizačnými smernicami); Sú zriadenie a monitorujú sa ciele výkonu pre činnosti oblasti sa, aby bolo možné sledovať výsledok; a Zdokumentované postupy činností oblasti sa štandardizujú a zlepšia v rámci celého podniku. Charakteristika prístupu: Postupy sú kompletnejšie alebo pokročilejšie ako v MIL2.	-

Model zrelosti bezpečnosti informácií pre rámec kybernetickej bezpečnosti NIST (ISMM)	**Uskutočnený proces**	**Riadený proces**	**Zriadený proces**	**Predvídateľný proces**	**Optimalizačný proces**
Katarský model zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti (Q-C2M2)	**Iniciovanie** Používa v niektorých oblastiach ad hoc postupy a procesy kybernetickej bezpečnosti.	**Vývoj** Implementované stratégie a postupy na vývoj a zlepšenie aktivít kybernetickej bezpečnosti v oblastiach s cieľom navrhnúť nové aktivity, ktoré sa majú vykonávať.	**Implementovanie** Prijaté stratégie na implementovanie všetkých aktivít kybernetickej bezpečnosti v oblastiach s cieľom dokončiť implementovanie v určitom čase.	**Prispôsobenie** Opätovné navštívenie a preskúmanie aktivít kybernetickej bezpečnosti a prijatie postupov na základe prediktívnych ukazovateľov odvodených z predchádzajúcich skúseností a opatrení.	**Agilita** Pokračovanie v uplatňovaní adaptívnej fázy so zvýšeným dôrazom na agilnosť a rýchlosť pri implementovaní aktivít v oblastiach.
Certifikácia modelu zrelosti kybernetickej bezpečnosti (CMMC)	**Procesy: uskutočnené** Keďže organizácia môže byť schopná uskutočniť tieto procesy len ad hoc spôsobom a môže ale nemusí sa spoliehať na dokumentáciu. Zrelosť procesu sa pre úroveň 1 nehodnotí. **Postupy: základná kybernetická hygiena** Úroveň 1 sa zameriava na ochranu FCI (federálne zmluvné informácie) a pozostáva len z postupov, ktoré zodpovedajú základných bezpečnostným požiadavkám.	**Procesy: Zdokumentované** Úroveň 2 vyžaduje, aby organizácia zriadila a zdokumentovala postupy a stratégie, ktoré sa použijú na nasmerovanie implementácie jej úsilia na CMMC. Zdokumentovanie postupov umožňuje jednotlivcom tieto postupy uskutočňovať opakovane. Organizácie vyvíjajú zrelé spôsobilosti pomocou dokumentovania svojich procesov a následným uplatňovaním týchto procesov ako zdokumentovaných. **Postupy: Stredná kybernetická hygiena** Úroveň 2 slúži ako prechod z úrovne 1 na úroveň 3 a skladá sa z podskupiny bezpečnostných požiadaviek, ktoré sú špecifikované v NIST SP 800-171, ako aj postupov z iných noriem a referencií.	**Procesy: Riadené** Úroveň 3 vyžaduje, aby organizácia zriadila, udržiavala a zaistila prostriedky pre plán, ktorý ukáže riadenie aktivít pre implementovanie postupu. Plán môže obsahovať informácie o misiách, cieľoch, projektových plánoch, získavaní zdrojov, potrebnom školení a zapojení relevantných zainteresovaných strán. **Postupy: dobrá kybernetická hygiena**. Úroveň 3 sa zameriava na ochranu CUI (regulované neutajené informácie) a zahŕňa všetky bezpečnostné požiadavky špecifikované v NIST SP 800-171, ako aj Ďalšie postupy z iných noriem a referencie na zmiernenie hrozieb.	**Procesy: preskúmané.** Úroveň 4 vyžaduje, aby organizácia preskúmala a zmerala efektívnosť postupov. Okrem merania efektívnosti postupov môžu organizácie v tejto úrovni podniknúť v prípade potreby opravný krok a opakovane informovať riadenie vyššej úrovne o stave a problémoch. **Postupy: Proaktívne** Úroveň 4 sa zameriava na ochranu CUI (regulované neutajené informácie) a zahŕňa podskupinu zlepšených bezpečnostných požiadaviek. Tieto postupy zlepšujú spôsobilosti detekcie a reakcie organizácie pri pomenovaní a prijímaní náročnej taktiky, techník a postupov.	**Procesy: Optimalizačné** Úroveň 5 vyžaduje od organizácie, aby štandardizovala a optimalizovala implementáciu procesu v celej organizácii. **Postupy: Pokrok/proaktivita** Úroveň 5 sa zameriava na ochranu CUI (regulované neutajené informácie). Ďalšími postupmi sa prehlbujú spôsobilosti v oblasti kybernetickej bezpečnosti a stávajú sa zložitejšími.
Model zrelosti kybernetickej bezpečnosti spoločenstva (CCSMM)	**Povedomie o bezpečnosti** Hlavnou témou aktivít na tejto úrovni je informovať jednotlivcov a organizácie o hrozbách, problémoch a záležitostiach týkajúcich sa kybernetickej bezpečnosti	**Vývoj procesu** Úroveň určená na pomoc spoločenstvám pri zriaďovaní a zlepšovaní bezpečnostných procesov potrebných na efektívne riešenie problémov kybernetickej bezpečnosti.	**Povolené informácie** Navrhnuté na zlepšenie mechanizmov poskytovania informácií v rámci spoločenstva, aby bolo toto schopné efektívne nájsť vzťah medzi zdanlivo nezlučiteľnými informáciami.	**Rozvoj taktiky** Táto úroveň je vytvorené na rozvoj lepších a proaktívnejších metód na zisťovanie a reagovanie na útoky. Pri tejto úrovni by mala byť v praxi zavedená väčšina preventívnych metód.	**Plná bezpečnostná prevádzková spôsobilosť** Táto úroveň predstavuje tie prvky, ktoré by mali byť zavedené do praxe v každej organizácii, ktorá sa má považovať za plne prevádzkovo pripravenú na

					riešenie akéhokoľvek typu kybernetickej hrozby.
Model spôsobilosti vnútorného auditu (IA-CM) pre verejný sektor	**Počiatočný** Neexistujú žiadne udržateľné, opakovateľné spôsobilosti – závisia od individuálneho úsilia	**Infraštruktúra** Udržateľné a opakovateľné postupy a metódy	**Integrácia** Jednotne aplikované postupy riadenia a profesionálne postupy	**Riadenie** Integruje informácie od organizácie na zlepšenie vedenia a riadenia rizík	**Optimalizácia** Učenie sa zvnútra a zvonku organizácie s cieľom nepretržitého zlepšovania

Tabuľka 7: Porovnanie atribútov/rozmerov

	Model zrelosti kapacít v oblasti kybernetickej bezpečnosti pre národy (CMM)	Model zrelosti spôsobilosti kybernetickej bezpečnosti (C2M2)	Katarský model zrelosti spôsobilosti v oblasti kybernetickej bezpečnosti (Q-C2M2)	Certifikácia modelu zrelosti kybernetickej bezpečnosti (CMMC)	Certifikácia modelu zrelosti kybernetickej bezpečnosti (CMMC)	Model zrelosti bezpečnosti informácií pre rámec kybernetickej bezpečnosti NIST (ISMM)	Rámec pre zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry	Globálny index kybernetickej bezpečnosti (GCI)	Index kybernetickej moci (CPI)
Úrovne	Päť rozmerov rozdelených do niekoľkých faktorov samotných, vrátane viacerých aspektov a ukazovateľov (Obrázok 4)	Oblasti vrátane jedinečného cieľa riadenia a niekoľkých cieľov prístupu (Obrázok 6)	Päť oblastí rozdelených na podoblasti	Sedemnásť oblastí detailne rozdelených do procesov a na jednu z mnohých spôsobilosti, ktoré sa potom detailne rozdelia do postupov (Obrázok 9).	Šesť hlavných rozmerov	Dvadsaťtri hodnotených oblastí	Päť funkcií so základnými kľúčovými kategóriami a podkategóriami (Obrázok).	Päť pilierov vrátane niekoľkých ukazovateľov	Štyri kategórie s niekoľkými ukazovateľmi
Atribúty/ rozmery	i navrhovanie zásad a stratégie v oblasti kybernetickej bezpečnosti, ii podpora zodpovednej kultúry kybernetickej bezpečnosti v spoločnosti, iii rozvoj znalostí o kybernetickej bezpečnosti, iv vytvorenie efektívnych právnych a regulačných rámcov a v riadenie rizík pomocou noriem, organizácií a technológií.	i riadenie rizík, ii riadenie aktív, zmien a konfigurácie, iii riadenie identity a prístupu, iv riadenie hrozieb a zraniteľnosti, v situačná informovanosť, vi reakcie na udalosti a incidenty, vii riadenie dodávateľského reťazca a externých závislostí, viii riadenie pracovnej sily, ix architektúra kybernetickej bezpečnosti, x riadenie programu kybernetickej bezpečnosti.	i pochopenie (výbor pre správu kybernetických záležitostí, riziká a školenie), ii zabezpečenie (bezpečnosť údajov, bezpečnosť technológie, bezpečnosť kontroly prístupu, bezpečnosť komunikácie a bezpečnosť personálu), iii expozícia (monitorovanie, riadenie incidentov, detekcia, analýza a expozícia), iv reakcia (plánovanie reakcií, zmiernenie reakcií a komunikovanie reakcií), v zachovanie (plánovanie obnovenia, riadenia kontinuity, zlepšovanie a externé závislosti).	i kontrola prístupu, ii správa majetku, iii audit a zodpovednosť, iv informovanosť a odborná príprava, v riadenie konfigurácie, vi identifikácia a autentifikácia, vii reakcia na incidenty, viii údržba, ix ochrana médií, x bezpečnosť personálu, xi fyzická ochrana, xii obnova, xiii riadenie rizík, xiv analýza bezpečnosti, xv situačná informovanosť, xvi ochrana systémov a komunikácie, xvii integrita systémov a informácií.	i pomenované hrozby, ii metrika, iii poskytovanie informácií, iv technológia, v odborná príprava, vi test.	i správa majetku, ii obchodné prostredie, iii správa a riadenie, iv posúdenie rizík, v stratégia riadenia rizík, vi hodnotene súladu, vii kontrola prístupu, viii informovanosť a odborná príprava, ix bezpečnosť osobných údajov, x procesy a postupy ochrany informácií, xi údržba, xii ochranná technológia, xiii anomálie a udalosti, xiv nepretržité monitorovanie bezpečnosti, xv procesy detekcie, xvi plánovanie reakcií, xvii komunikovanie reakcií, xviii analýza reakcií, xix zmiernenie reakcií, xx zlepšenia reakcií, xxi plánovanie obnovy, xxii zlepšenia obnovy, xxiii komunikovanie obnovy.	i identifikovanie, ii ochrana, iii odhalenie, iv reakcia, v obnova.	i právny, ii technický, iii organizačný, iv budovanie kapacít, v spolupráca.	i právny a regulačný rámec, ii ekonomický a sociálny kontext, iii infraštruktúra technológie, iv priemyselná aplikácia.

PRÍLOHA B – ZOZNAM LITERATÚRY SEKUNDÁRNEHO PRIESKUMU

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2012) NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. K dispozícii na adrese: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2016) Guidelines for SMEs on the security of personal data processing.

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2017) Handbook on security of personal data processing. K dispozícii na adrese: http://dx.publications.europa.eu/10.2824/569768

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

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

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

Belgická vláda (2012) Cyber Security Strategy. K dispozícii 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

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

Biely dom (2018) Národná kybernetická stratégia Spojených štátov amerických. K dispozícii na adrese: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

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

Bulharská vláda (2015) Národná stratégia kybernetickej bezpečnosti – Bulharsko odolné proti kybernetickým útokom 2020.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) "Cybersecurity Capability Maturity Model (C2M2) Version 2.0. K dispozícii 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 dispozícii 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

Council of Ministers (2019) Portuguese Official Journal, Series 1 — No. 108 - Resolution of the Council of Ministers No. 92/2019. K dispozícii na adrese: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

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

CSIRT Maturity - Self-assessment Tool (neuvedený dátum). K dispozícii 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 dispozícii na adrese: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

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

Dánska vláda – Ministerstvo financií (2018) Dánska stratégia kybernetickej a informačnej bezpečnosti. K dispozícii na adrese: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

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

Darra, E. (no date) 'Welcome to the NCSS Training Tool'.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. K dispozícii 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 dispozícii 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 dispozícii 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 dispozícii 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. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* K dispozícii na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Európska komisia (2012) Nariadenie Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu. K dispozícii na adrese: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52012PC0238&from=SK

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 dispozícii na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Európska únia a Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. K dispozícii na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Galan Manso, C. et al. (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 dispozícii na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) 'Evaluating Business Process Maturity Models', Journal of the Association for Information Systems. K dispozícii na adrese: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Grécka vláda (2017) Národná stratégia kybernetickej bezpečnosti. K dispozícii 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

Hodnotiaci nástroj národných stratégií kybernetickej bezpečnosti (2018). K dispozícii na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Holandská vláda (2018) Národná agenda kybernetickej bezpečnosti. K dispozícii 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

Chorvátska vláda (2015) Národná stratégia kybernetickej bezpečnosti Chorvátskej republiky. K dispozícii na adrese: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Inštitút interných audítorov (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Výskumná nadácia inštitútu interných audítorov.

Írska vláda (2019) Národná stratégia kybernetickej bezpečnosti. K dispozícii na adrese: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

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

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

Lotyšská vláda (2014) Stratégia kybernetickej bezpečnosti Lotyšska. K dispozícii na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Luxemburská vládna rada (2018) Národná stratégia kybernetickej bezpečnosti. K dispozícii 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

Maďarská vláda (2018) Stratégia v oblasti bezpečnosti sietí a informačných systémov. K dispozícii 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

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

Medzinárodná telekomunikačná únia (ITU) (2018) Guide to developing a national cybersecurity strategy. K dispozícii na adrese: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Medzinárodná telekomunikačná únia (ITU) (2018) The Global Cybersecurity Index. K dispozícii na adrese: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Ministerstvo ekonomických záležitostí a komunikácie (2019) Stratégie kybernetickej bezpečnosti – Estónska republika. K dispozícii na adrese: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministerstvo národnej obrany Litovskej republiky (2018) Národná stratégia kybernetickej bezpečnosti

Ministerstvo pre hospodársku súťaž a digitálnu a námornú ekonomiku a ekonomiku služieb (2016) Stratégia kybernetickej bezpečnosti – Malta. K dispozícii 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

Národná stratégia kybernetickej bezpečnosti Spojeného kráľovstva 2016 – 2021 (2016). K dispozícii na adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Národné centrum kybernetickej bezpečnosti (2015) Národná stratégia kybernetickej bezpečnosti Českej republiky. K dispozícii na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Národné stratégie kybernetickej bezpečnosti – Interaktívna mapa (bez dátumu). K dispozícii na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Národný inštitút pre normy a technológie (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Národný inštitút pre normy a technológie. K dispozícii na adrese: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

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

OECD, Európska únia a Spoločné výskumné centrum – Európska komisia (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. K dispozícii na adrese: https://www.oecd.org/sdd/42495745.pdf.

Organizácia pre hospodársku spoluprácu a rozvoj (OECD) (2012) Cybersecurity policy making at a turning point. K dispozícii 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

Predsedníctvo Rady ministrov (2017) Taliansky akčný plán kybernetickej bezpečnosti. K dispozícii 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

Príručka osvedčených postupov Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (2016) NCSS: designing and implementing national cyber security strategies. Heraklion: ENISA.

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

Rumunská vláda (2013) Stratégia kybernetickej bezpečnosti Rumunska. K dispozícii 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

Sarri, A., Kyranoudi, P. and European Union Agency for Cybersecurity (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. K dispozícii na adrese: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Sekretariát Bezpečnostného výboru (2019) Fínska stratégia kybernetickej bezpečnosti 2019. K dispozícii na adrese: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovenská vláda (2015) Koncept kybernetickej bezpečnosti Slovenskej republiky. K dispozícii 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

Smith, R. (2015) Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010

Smith, R. (2016) 'Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010', in Smith, R., Core EU Legislation. London: Macmillan Education. K dispozícii na adrese: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016L1148&from=SK.

Spolková rada (2018) Národná stratégia na ochranu švajčiarska pred kybernetickými rizikami.

Spolkové ministerstvo vnútra (2011) Kybernetická stratégia pre Nemecko. K dispozícii 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

Spolkový kancelár Rakúskej republiky (2013) Rakúska stratégia kybernetickej bezpečnosti. K dispozícii 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

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

Španielska vláda (2019) Národná stratégia kybernetickej bezpečnosti. K dispozícii 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

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

Trimintzios, P., et al. (2011) Cyber Europe Report. K dispozícii na adrese: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. a Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (2013) *National-level risk assessments: an analysis report.* K dispozícii na adrese: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

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

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

Univeruita v Innsbrucku et al. (2009) Understanding Maturity Models.

Úrad francúzskeho premiéra (2014) Francúzska národná digitálna bezpečnostná stratégia. K dispozícii na adrese: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Úrad komisára pre elektronické komunikácie a reguláciu v poštách (2012) Stratégia kybernetickej bezpečnosti – Cyperská republika.

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

Úradný vestník Európskej únie (2008) SMERNICA RADY 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. K dispozícii na adrese: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32008L0114&from=SK

Wamala, D. F. (2011) „ITU National Cybersecurity Strategy Guide“. K dispozícii 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)

PRÍLOHA C – OSTATNÉ SKÚMANÉ CIELE

Ciele, ktoré sú detailne popísané nižšie, boli skúmané ako súčasť fázy sekundárneho prieskumu a rozhovorov uskutočnených agentúrou ENISA. Tieto ciele nie sú súčasťou národného hodnotiaceho rámca spôsobilostí, ale objasňujú témy, ktoré sú hodné prediskutovania. Každá z týchto podkapitol obsahuje vysvetlenie, prečo bol daný cieľ vyradený,

- vývoj stratégií kybernetickej bezpečnosti špecifických pre konkrétny sektor,
- boj proti dezinformačným kampaniam,
- zaistenie pokročilej technológia (5G, AI, kvantová výpočtová technika…);
- zabezpečenie dátovej suverenity a
- poskytnutie stimulov na rozvoj odvetvia poistenia kybernetických rizík.

Vývoj stratégií kybernetickej bezpečnosti špecifických pre konkrétny sektor

Prijatie stratégií špecifických pre konkrétny sektor, ktoré sú zamerané na intervencie a stimuly v tomto sektore, určite predstavuje silnú decentralizovanú spôsobilosť. Je to obzvlášť vhodné pre členské štáty, ktorých prevádzkovatelia základných služieb sa musia zaoberať rôznymi rámcami a nariadeniami a v prípade existencie veľkého množstva závislostí z dôvodu priebežnej povahy kybernetickej bezpečnosti. V niekoľkých členských štátoch je skutočne bežné napočítať desiatky vnútroštátnych orgánov a regulačných orgánov s vedomosťami o špecifickostiach každého sektora, ktoré majú mandát na presadzovanie konkrétneho nariadenia pre každý sektor.

Napríklad Dánsko spustilo šesť cielených stratégií, ktoré pomenúvajú najdôležitejšie snahy v oblasti kybernetickej bezpečnosti a bezpečnosti informácií, aby vytvorilo silnejšiu decentralizovanú spôsobilosť v oblasti kybernetickej bezpečnosti a bezpečnosti informácií. Každá „sektorová jednotka“ prispeje okrem iného k posúdeniu hrozieb na sektorovej úrovni, k monitorovaniu, cvičeniam pripravenosti, zriadeniu bezpečnostných systémov, podeleniu sa o vedomosti a k pokynom. Stratégie špecifické pre konkrétny sektor zahŕňajú tieto sektory:

- energia,
- zdravotná starostlivosť,
- doprava,
- telekomunikácie,
- financie a
- námorné záležitosti.

Ostatné členské štáty vyjadrili záujem o zohľadnenie stratégií kybernetickej bezpečnosti pre konkrétny sektor, aby reflektovali všetky regulačné požiadavky. Je ale potrebné poznamenať, že takýto cieľ nemusí v závislosti od veľkosti, národných stratégií a zrelosti vyhovovať všetkým členským štátom. Veľký problém, ktorý predstavuje zabezpečenie, aby rámec zahŕňal všetky špecifickosti, viedol agentúru ENISA k tomu, aby do rámca tento cieľ nezahrnula.

Boj proti dezinformačným kampaniam

Členské štáty zahŕňajú do svojich stratégií kybernetickej bezpečnosti ochranu základných princípov, ako napríklad ľudských práv, transparentnosti a verejnej dôvery. Toto je veľmi

dôležité najmä keď ide o dezinformácie, ktoré sa šíria tradičnými médiami alebo platformami sociálnych sietí. Kybernetická bezpečnosť je navyše momentálne jednou z najväčších volebných výziev. Aktivity, ako napríklad šírenie nepravdivých informácií alebo negatívna propaganda, boli pozorované v rôznych krajinách počas predvolebného obdobia dôležitých volieb. Táto hrozba môže potenciálne podkopať demokratický proces EÚ. Na európskej úrovni načrtla Komisia akčný plán[32] na zriadenie snáh na boj proti dezinformáciám v Európe: tento plán sa zameriava na 4 kľúčové oblasti (zistenie, kooperácia, spolupráca s online platformami a povedomie) a slúži na vybudovanie spôsobilostí EÚ a posilnenie spolupráce medzi členskými štátmi.

4 z 19 opýtaných krajín vyjadrili svoj zámer popasovať sa s problémom dezinformácií a propagandy vo svojich NCSS.

Napríklad vo francúzskej NCSS[33] sa uvádza, že: „je zodpovednosťou štátu informovať občanov o rizikách vyplývajúcich z metód manipulácie a propagandy, ktoré využívajú podvodní hráči na internet. Napríklad po teroristickom útoku vo Francúzsku v januári 2015 zriadila vláda informačnú platformu o rizikách súvisiacich s islamskou radikalizáciou prostredníctvom elektronických komunikačných sietí: « Stop-djihadisme.gouv.fr ».” Tento prístup by sa mohol rozšíriť o reakcie na iné javy propagandy alebo destabilizácie.

Ďalším príkladom je poľská NCSS na roky 2019 – 2024[34], v ktorej sa hovorí, že: „proti manipulatívnym aktivitám, ako napríklad dezinformačným kampaniam, sú potrebné systémové kroky, ktoré vytvoria u občanov povedomie v kontexte overovania a autentifikácie informácií a reakcie na pokusy na ich skreslenie.“

Počas rozhovorov organizovaných agentúrou ENISA sa niekoľko členských štátov podelilo o názor, že problém neriešia ako kybernetickú hrozbu v rámci svojej NCSS, ale sa s ním zaoberajú na širšej spoločenskej úrovni, napríklad prostredníctvom politických iniciatív.

Zaistenie pokročilých technológií (5G, AI, kvantová výpočtová technika…)

Vzhľadom na neustále rozširovanie oblasti kybernetických hrozieb bude výsledkom vývoja nových technológií pravdepodobne zvýšenie intenzity a počtu kybernetických útokov a diverzifikácia spôsobov, prostriedkov a cieľov aktérov hrozieb. Zatiaľ majú tieto nové technologické riešenia, ktoré majú podobu pokročilých technológií, potenciál stať sa stavebnými kameňmi európskeho digitálneho trhu. Na ochranu rastúcej digitálnej závislosti členských štátov a vzniku nových technológií je potrebné zriadiť stimuly a rozvinuté stratégie, ktoré pomôžu pri bezpečnom a dôveryhodnom vývoji a zavádzaní týchto technológií v EÚ.

Počas fázy sekundárneho prieskumu uskutočnenej v rámci NCSS členských štátov, označili členské štáty záujem o tieto vyspelé technológie: 5G, AI, kvantová výpočtová technika, kryptografia, edge computing, pripojené a autonómne vozidlá, veľké objemy dát a inteligentné dáta, blockchain, robotika a internet vecí (IoT).

Európska komisia konkrétne začiatkom roka 2020 zverejnila komunikačnú výzvu pre členské štáty, aby podnikli kroky na implementovanie súboru opatrní odporúčaných v záveroch súboru nástrojov pre 5G[35]. Súbor nástrojov 5G je následkom odporúčania (EÚ) 2019/534 ku kybernetickej bezpečnosti 5G sietí, ktoré prijala Komisia v roku 2019 a ktoré vyzýva na jednotný európsky prístup k bezpečnosti 5G sietí[36].

[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/SK/TXT/?uri=CELEX%3A32019H0534

Počas rozhovorov vedených agentúrou ENISA sa zdôraznilo, že táto téma je viac interdisciplinárna a je skôr pomenovaná v rámci NCSS ako stanovená ako konkrétny cieľ *sama o sebe*.

Zabezpečenie dátovej suverenity

Kybernetický priestor môže byť na jednej strane vnímaný ako náročný globálny spoločný priestor, ktorý je ľahko prístupný, poskytuje vysoký stupeň pripojiteľnosti a je schopný prinášať výborné príležitosti pre socio-ekonomický rast. Na druhej strane charakterizuje kybernetický priestor jeho slabosť v oblasti právomoci, náročnosť pri priradení krokov, nedostatok hraníc a prepojené sústavy, ktoré môžu byť porézne a ktorých údaje môžu cudzie vlády ukradnúť alebo k nim dokonca získať prístup. Okrem týchto pohľadov sa digitálny ekosystém vyznačuje koncentráciou platforiem online služieb a infraštruktúrou v rukách veľmi malého počtu zainteresovaných strán. Všetky uvedené aspekty vedú členské štáty k podpore technologickej suverenity. Dosiahnutie technologickej suverenity znamená, že občania a podniky sú schopní úplne prosperovať s využitím digitálnych služieb a produktov IKT, ktoré sú dôveryhodné, bez akéhokoľvek strachu o osobné údaje alebo digitálny majetok, ekonomickú autonómiu alebo politický vplyv.

Dátovú suverenitu alebo technologickú suverenitu presadzujú členské štáty na národnej a európskej úrovni. Aj keď sa nezdá že, členské štáty pomenúvajú tento problém ako konkrétny cieľ priamo vo svojich NCSS, riešia ho buď ako interdisciplinárny princíp alebo načrtnú svoj zámer na zaistenie technologickej suverenity na národnej úrovni v *ad hoc* publikáciách zameraním sa na kľúčové technológie. Vo francúzskom strategickom preskúmaní kybernetickej obrany z roku 2018 je napríklad uvedené, že „na zaistenie technologickej suverenity je najdôležitejšie riadenie nasledujúcich technológií: šifrovanie komunikácie, odhaľovanie kybernetických incidentov, profesionálne mobilné bezdrôtové prenášanie signálov, cloud computing a umelá inteligencia“[37].

Na európskej úrovni sa členské štáty aktívne podieľajú na definovaní európskej dátovej stratégie (COM/2020/66 final) a budovaní certifikačného rámca EÚ pre digitálne produkty, služby a procesy IKT, ktoré definuje európsky akt o kybernetickej bezpečnosti (2019/881), aby sa na európskej úrovni zabezpečila strategická digitálna nezávislosť.

Vo fáze rozhovorov s členskými štátmi sa ukázalo, že téma technologickej suverenity sa často považuje za širší problém ako len obmedzenie na kybernetickú bezpečnosť. Členské štáty preto nezahŕňajú túto tému do svojich NCSS a tých niekoľko, ktoré tak spravia, ju nezahrnie ako konkrétny cieľ *per se*.

Poskytnutie stimulov na rozvoj odvetvia poistenia kybernetických rizík

Aktuálny stav odvetvia poistenia kybernetických rizík ukazuje, že globálny trh zaznamenal nesporný rast. Momentálne je ale stále len vo svojich začiatkoch, pretože je potrebné zhromaždiť údaje a stanoviť mnohé precedensy (*napr.* tiché krytie, systematické kybernetické riziká…). Odhadované straty z kybernetických útokov na celom svete sú o niekoľko rádových hodnôt vyššie ako súčasná kapacita krytia odvetvia poistenia kybernetických rizík (Pracovný dokument IMF – kybernetické riziko pre finančný sektor: Rámec pre kvantitatívne posúdenie WP/18/143). Rozvoj odvetvia poistenia kybernetických rizík môže ale určite priniesť výhody a položiť základy poctivých mechanizmov. Mechanizmy poistenia kybernetických rizík môžu skutočne pomôcť pri:

- zvyšovaní informovanosti o kybernetických rizikách v spoločnostiach,

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

- hodnotení expozície kybernetickým rizikám kvantitatívnym spôsobom,
- zlepšovaní riadenia kybernetických rizík,
- poskytovaní pomoci organizáciám, ktoré sú obeťami kybernetických útokov a
- pri pokrývaní škôd (materiálnych alebo iných) spôsobených kybernetickým útokom.

Niektoré členské štáty začali na tejto téme pracovať. Napríklad:

- Estónsko zaviedlo do svojej NCSS prístup „čakaj a uvidíš“: „Na zmiernenie kybernetických rizík v súkromnom sektore vo všeobecnosti sa uskutoční analýza dopytu a ponuky poistenia kybernetických rizík v Estónsku a na základe toho sa dotknuté strany dohodnú na princípoch spolupráce, vrátane poskytovania informácií, prípravy posudzovania rizík atď. Dnes existuje na estónskom trhu len niekoľko poskytovateľov služieb poistenia kybernetických rizík a je potrebné najprv zmapovať, kto čo ponúka. Komplexnosť poistnej ochrany sa často považuje za prekážku pri rozvoji trhu poistenia kybernetických rizík.“
- Luxembursko konkrétne vo svojej NCSS podporuje rozvoj odvetvia poistenia kybernetických rizík: „Cieľ 1: Vytvorenie nových produktov a služieb. Na zhromaždenie rizík a podporu obetí digitálnych kybernetických útokov pri vyhľadávaní pomoci u odborníkov, ktorí dokážu takýto incident zvládnuť a obnoviť systém zasiahnutý škodlivým konaním, budú spoločnosti podporované v tom, aby vytvorili konkrétne produkty pre oblasť poistenia kybernetických rizík.“

Spätná väzba od respondentov bola k tejto téme pomerne rozmanitá: niektoré členské štáty uviedli, že téma poistenia kybernetických rizík sa v poslednom čase stala témou diskusií, zatiaľ čo ostatné štáty vyjadrili názor, že napriek tomu, že je táto téma sľubná, odvetvie nie je ešte dostatočné zrelé. Veľký počet respondentov ale uviedol, že tému nezaradilo ako súčasť NCSS buď preto, že ju považovali za príliš konkrétnu, alebo že nebola v zábere NCSS.

TP-02-21-253-SK-N

O Agentúre Európskej únie pre kybernetickú bezpečnosť

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúra Únie, ktorej úlohou je zabezpečovať vysokú spoločnú úroveň kybernetickej bezpečnosti v Európe. Agentúra EÚ, ktorá bola zriadená v roku 2004 a ktorej postavenie posilnil akt EÚ o kybernetickej bezpečnosti, prispieva k vytváraniu kybernetickej politiky EÚ a pomocou systémov certifikácie kybernetickej bezpečnosti zvyšuje dôveryhodnosť produktov, služieb a procesov IKT, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy v budúcnosti. Agentúra prostredníctvom spoločného využívania vedomostí, budovania kapacít a zvyšovania informovanosti spolupracuje s kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v rámci prepojenej ekonomiky, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zachovať digitálnu bezpečnosť európskej spoločnosti a občanov Európy. Viac informácií nájdete na stránke 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: 978-92-9204-486-2
DOI: 10.2824/978297