EURÓPSKA
KOMISIA

V Štrasburgu 18. 4. 2023
COM(2023) 207 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ (Akadémia zručností v oblasti kybernetickej bezpečnosti)

Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ

(Akadémia zručností v oblasti kybernetickej bezpečnosti)

1. Naliehavá potreba znížiť riziká riešením nedostatku zručností a odstraňovaním medzier v oblasti kybernetickej bezpečnosti

Kybernetická bezpečnosť nie je len súčasťou bezpečnosti občanov, podnikov a členských štátov. Je nevyhnutná aj na zabezpečenie politickej stability EÚ, stability jej demokracií a prosperity našej spoločnosti a podnikov. **Panoráma kybernetickobezpečnostných hrozieb** sa v posledných rokoch výrazne zmenila, pričom znepokojujúcim trendom je rastúci počet kybernetických útokov zameraných na vojenskú a civilnú kritickú infraštruktúru v EÚ. Aktéri hrozieb zlepšujú svoje schopnosti a objavujú sa nové, hybridné a rozvíjajúce sa hrozby, ako napríklad používanie botov a techník založených na umelej inteligencii[1]. Najmä aktéri ransomvérových hrozieb bežne spôsobujú subjektom značnú finančnú ujmu, ako aj poškodenie dobrého mena[2].

Mnoho kybernetických incidentov bolo namierených aj na verejnú správu a vlády v členských štátoch, ako aj na európske inštitúcie, orgány, úrady a agentúry[3]. Neustálym terčom útokov[4] sú aj finančný sektor[5] a zdravotníctvo[6], ktoré sú pilierom spoločnosti a hospodárstva. Geopolitické napätie spojené s útočnou vojnou Ruska proti Ukrajine zvýšilo kybernetické ohrozenie[7] a má potenciál destabilizovať našu spoločnosť. **Bezpečnosť** EÚ nemožno zaručiť bez **najcennejšieho aktíva EÚ: jej obyvateľov.** EÚ naliehavo potrebuje odborníkov so zručnosťami a kompetenciami na predchádzanie kybernetickým útokom proti EÚ vrátane jej najdôležitejších infraštruktúr, ich odhaľovanie, odrádzanie od nich a na ochranu Únie pred týmito útokmi, ako aj na zabezpečenie jej **odolnosti** voči nim.

---

1 ENISA, *Threat Landscape 2022* (Panoráma hrozieb v roku 2022) – ENISA (europa.eu).

2 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021* (Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2021). Títo aktéri vychádzajú z modelu ransomvéru ako služby. Ročné náklady, ktoré podnikom vznikli, presiahli v roku 2022 18,4 miliardy EUR [Cybereason, *2022 Report on the true cost or Ransomware* (Správa o skutočných nákladoch ransomvéru za rok 2022)].

3 Pozri napríklad spoločnú publikáciu agentúry ENISA a tímu CERT-EU JP-23-01 – *Sustained activity by specific threat actors* (Neutíchajúca činnosť konkrétnych aktérov hrozieb), TLP:CLEAR, 15. február 2023.

4 ENISA, *Threat Landscape 2022* (Panoráma hrozieb v roku 2022).

5 Pozri napríklad Nemecko, kde 90 % e-mailových podvodov nahlásených od 1. júna 2021 do 31. mája 2022 tvoril finančný phishing alebo útoky na spoločnosti pôsobiace vo finančnom sektore, pri ktorých bolo infikovaných viac ako 20 000 zariadení zo 125 krajín, *The State of IT Security in Germany in 2022* (Stav IT bezpečnosti v Nemecku v roku 2022), Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. január 2023.

6 Pozri napríklad ransomvérové útoky na verejné zdravotnícke zariadenia vo Francúzsku, napríklad na Centre Hospitalier Sud Francilien, počas ktorých bolo kompromitovaných 11 GB osobných a lekárskych údajov, ako aj údajov týkajúcich sa zamestnancov, ktoré aktér hrozby zverejnil, *Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023*.

7 Pozri aj: CERT-EU – *Russia's war on Ukraine: one year of cyber operations* (Ruská vojna na Ukrajine: jeden rok kybernetických operácií) (europa.eu); Ruské kybernetické operácie proti Ukrajine: vyhlásenie vysokého predstaviteľa v mene Európskej únie, 10. máj 2022; Vyhlásenie vysokého predstaviteľa v mene Európskej únie o škodlivých kybernetických činnostiach hackerov a hackerských skupín v súvislosti s agresiou Ruska voči Ukrajine, 19. júl 2022.

Nedostatok odborníkov v oblasti kybernetickej bezpečnosti ďalej brzdí **konkurencieschopnosť** a **rast** Európy, ktoré vo veľkej miere závisia od rozvoja a zavádzania strategických digitálnych technológií (napr. umelej inteligencie, 5G a cloudu). Kvalifikovaná pracovná sila v oblasti kybernetickej bezpečnosti je potrebná na to, aby si EÚ udržala pozíciu dodávateľa kľúčových vyspelých technológií v globálnom prostredí.

S cieľom pripraviť sa na túto meniacu sa panorámu hrozieb a čeliť jej, ako aj podporiť konkurencieschopnosť EÚ sa v posledných rokoch dosiahol výrazný pokrok v politike EÚ v oblasti kybernetickej bezpečnosti, čo viedlo k prijatiu viacerých iniciatív, ako sú stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde[8], revidovaná smernica o sieťovej a informačnej bezpečnosti (smernica NIS2)[9], odvetvové právne predpisy EÚ v oblasti kybernetickej bezpečnosti[10], politika EÚ v oblasti kybernetickej obrany[11], akt o kybernetickej odolnosti[12] a akt o kybernetickej solidarite predložené Komisiou spolu s týmto oznámením. Bez potrebných kvalifikovaných jednotlivcov, ktorí budú tieto právne predpisy vykonávať, sa však stanovené ciele nedosiahnu. Zatiaľ čo základnými znalosťami širokej populácie o kybernetickej bezpečnosti sa zaoberajú iniciatívy na podporu rozvoja všeobecných zručností potrebných na účasť v spoločnosti[13], **na splnenie uvedených právnych a politických požiadaviek v oblasti kybernetickej bezpečnosti** je nevyhnutná kompetentná pracovná sila vo verejnom aj v súkromnom sektore vrátane normalizačných organizácií, a to na vnútroštátnej úrovni, ako aj na úrovni EÚ.

Bezpečnosť a konkurencieschopnosť EÚ preto závisia od dostupnosti odbornej kvalifikovanej pracovnej sily v oblasti kybernetickej bezpečnosti. EÚ však čelí výraznému nedostatku kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti, čo vystavuje EÚ, jej členské štáty, podniky a občanov riziku kybernetických bezpečnostných incidentov. V roku 2022 sa nedostatok odborníkov v oblasti kybernetickej bezpečnosti v Európskej únii pohyboval v rozmedzí **od 260 000**[14] **do 500 000**[15], zatiaľ čo potreba pracovnej sily v tejto

---

8 Spoločné oznámenie Európskemu parlamentu a Rade Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde, JOIN(2020) 18 final.

9 Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

10 Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (nariadenie DORA) pre finančný sektor.

11 Spoločné oznámenie Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany, JOIN(2022) 49 final.

12 Návrh nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020, COM(2022) 454 final.

13 Medzi príslušné iniciatívy zamerané na všeobecné digitálne zručnosti obyvateľstva patria: Akčný plán na realizáciu Európskeho piliera sociálnych práv a Digitálny kompas, ktorých cieľom je, aby 80 % obyvateľstva získalo do roku 2030 základné digitálne zručnosti, Akčný plán digitálneho vzdelávania na roky 2021 – 2027, nástroj rámca digitálnych kompetencií alebo návrh odporúčania Rady o zlepšení poskytovania digitálnych zručností v rámci vzdelávania a odbornej prípravy.

14 (ISC)² v: *Assessing Cyber Skills on the basis of the ECSF* (Hodnotenie kybernetických zručností na základe európskeho rámca kybernetických zručností), webinár agentúry ENISA, 16. február 2023.

15 Podľa Európskej organizácie kybernetickej bezpečnosti (ECSO), ako sa uvádza v spoločnom oznámení Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany, JOIN(2022) 49 final.

oblasti sa odhadovala na 883 000 odborníkov[16], čo naznačuje nesúlad medzi dostupnými kompetenciami a kompetenciami požadovanými na trhu práce. Pracovná sila v oblasti kybernetickej bezpečnosti ďalej dopláca na mylnú predstavu spojenú s jej technickým imidžom a stále sa jej nedarí prilákať **ženy**, ktoré tvoria 20 % absolventov odboru kybernetickej bezpečnosti[17] a 19 % odborníkov na informačné a komunikačné technológie (IKT)[18]. Na riešenie tohto problému sa v európskom **politickom programe Digitálne desaťročie do roku 2030**[19] stanovil cieľ zvýšiť do roku 2030 počet odborníkov v oblasti IKT o 20 miliónov a zároveň dosiahnuť rovnomernejšie rodové zastúpenie. Vykonávanie novej politiky EÚ si navyše vyžaduje primerane kvalifikovanú a dostatočnú pracovnú silu. Napríklad viac ako 42 % vysokopostavených vedúcich IT pracovníkov v odvetví finančných služieb označilo nedostatok kybernetickobezpečnostných zručností a odborných znalostí za hlavnú výzvu, ktorej ich podnik čelí, pokiaľ ide o kybernetickobezpečnostnú obranu a riadenie incidentov[20], a to práve v čase, keď budú musieť vykonávať odvetvové právne predpisy v oblasti kybernetickej bezpečnosti, ako je napríklad akt o digitálnej prevádzkovej odolnosti (DORA).

Váhavosť zamestnávateľov investovať do ľudského kapitálu a to, že hľadajú už vyškolenú a skúsenú pracovnú silu, ďalej prispieva k obmedzeniam na trhu práce[21]. Týmto nedostatkom trpia všetky typy spoločností vrátane malých a stredných podnikov (**MSP**), ktoré predstavujú 99 % všetkých podnikov v EÚ[22]. Veľkej výzve čelí aj **verejná správa**, ktorú kybernetické incidenty zasahujú v značnej miere a ovplyvňujú najviac[23].

Keďže je ohrozená bezpečnosť a konkurencieschopnosť EÚ, riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti v EÚ je naliehavé.

2. Absencia synergií a koordinovaných opatrení na odstránenie nedostatku kybernetickobezpečnostných zručností

Na európskej a vnútroštátnej úrovni sa darí iniciatívam verejných a súkromných subjektov zameraným na riešenie nedostatku pracovných síl v oblasti kybernetickej bezpečnosti na trhu práce. Sú však ojedinelé a zatiaľ sa nepodarilo dosiahnuť ich kritické množstvo, ktoré by prinieslo skutočnú zmenu.

Na začiatok treba povedať, že v súčasnosti existuje len obmedzená spoločná predstava o zložení pracovnej sily v oblasti kybernetickej bezpečnosti v EÚ a súvisiacich zručnostiach, pričom podobné profily pracovných pozícií v oblasti kybernetickej bezpečnosti by mali zahŕňať rovnaký súbor zručností. Nízka miera zavádzania spoločného **európskeho**

---

16 (ISC)² v: *Assessing Cyber Skills on the basis of the ECSF* (Hodnotenie kybernetických zručností na základe európskeho rámca kybernetických zručností), webinár agentúry ENISA, 16. február 2023.

17 Databáza vysokoškolského vzdelávania v oblasti kybernetickej bezpečnosti (CyberHEAD).

18 Iba 19 % odborníkov na IKT v EÚ tvoria ženy – Index digitálnej ekonomiky a spoločnosti (DESI) za rok 2022 | Formovanie digitálnej budúcnosti Európy (europa.eu). Nie sú k dispozícii žiadne údaje týkajúce sa ženskej pracovnej sily Únie v oblasti kybernetickej bezpečnosti.

19 Rozhodnutie Európskeho parlamentu a Rady (EÚ) 2022/2481 zo 14. decembra 2022, ktorým sa zriaďuje politický program digitálne desaťročie do roku 2030, ktorým sa vytvára mechanizmus monitorovania a spolupráce na dosiahnutie spoločných cieľov a ambícií digitálnej transformácie Európy stanovených v Digitálnom kompase do roku 2030 vrátane oblasti zručností.

20 S-RM, *Cyber Security Insights Report 2022* (Správa o kybernetickej bezpečnosti za rok 2022).

21 *Cybersecurity Skills Development in the EU* (Rozvoj kybernetickobezpečnostných zručností v EÚ), ENISA, december 2019.

22 Definícia MSP (europa.eu).

23 ENISA, *Threat Landscape 2022* (Panoráma hrozieb v roku 2022) – ENISA (europa.eu).

referenčného rámca pre odborníkov v oblasti kybernetickej bezpečnosti príslušnými aktérmi sa prejavuje v absencii komunikačného nástroja medzi zamestnávateľmi, pedagógmi a tvorcami politík a v neschopnosti vykonávať merania a posudzovať nedostatky na trhu práce v oblasti kybernetickej bezpečnosti. Ďalej bráni navrhovaniu učebných plánov vzdelávania a odbornej prípravy a vytváraniu kariérnych možností zodpovedajúcich potrebám politiky a trhu pre tých, ktorí chcú pracovať v tomto sektore. **Zvyšovanie úrovne zručností a rekvalifikácia** pracovnej sily sa vo veľkej miere opierajú o odbornú prípravu a certifikáty v oblasti kybernetickej bezpečnosti, ktoré zvyčajne ponúkajú súkromní poskytovatelia. Pracovníci však majú problémy získať prehľad o kvalite ponúkanej odbornej prípravy v oblasti kybernetickej bezpečnosti a o súvisiacich certifikátoch, ktoré sa vydávajú.

Zatiaľ čo na posilnenie ponuky na trhu práce sú potrebné vzdelávanie a odborná príprava a budovanie kariérnych možností, v súčasnosti sa podceňuje úloha **dopytu** pri odbornej príprave pracovnej sily a prispôsobovaní sa vývoju trhu práce. Zamestnávateľom z daného odvetvia a verejného sektora chýbajú spoločné fóra a miesta, kde by si mohli vymieňať nápady, ako čo najlepšie vzdelávať pracovnú silu, a zaoberať sa tým, ako **lepšie hodnotiť zručnosti**, najmä počas náborového procesu. Najžiadanejšie **odborné zručnosti** síce môžu byť zručnosti súvisiace s kybernetickou bezpečnosťou[24], ako napríklad vývoj softvéru alebo cloud computing[25], no stále sa neodôvodnene ignorujú **prierezové zručnosti**. Medzi skupiny zručností, ktoré sú zamestnávateľmi viac žiadané[26] a ktorých význam do roku 2025 porastie[27], patria kritické myslenie a analýza, riešenie problémov či samoriadenie.

Existuje už mnoho verejných a súkromných iniciatív na investovanie do kybernetickobezpečnostných zručností, pričom EÚ vo veľkej miere **financuje** projekty v rámci rôznych nástrojov[28]. Pretrvávajúci nedostatok zručností v EÚ však vyvoláva otázky, pokiaľ ide o ich viditeľnosť a vplyv, a naznačuje, že nemusia systematicky zodpovedať potrebám trhu, ktoré je na úrovni EÚ potrebné urýchlene zmapovať. Okrem toho viaceré zdroje financovania spôsobujú duplicitu, čím sa stráca príležitosť na rozšírenie a dosiahnutie skutočného vplyvu. Navyše tí, ktorí potrebujú investície, nedokážu vždy určiť najvhodnejšie zdroje pre svoje potreby.

Zainteresované strany sa snažia riešiť zložitý a komplexný problém nedostatku kybernetickobezpečnostných zručností. Agentúra EÚ pre kybernetickú bezpečnosť (ENISA) vyvíja nástroje týkajúce sa profilov úloh alebo vysokoškolského vzdelávania[29], Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej

---

24 LinkedIn, *2023 Most In-Demand Skills: Learn the Skills Companies Need Most* (Najžiadanejšie zručnosti v roku 2023: získajte zručnosti, ktoré spoločnosti najviac potrebujú).

25 Infografika Asociácie auditu a kontroly informačných systémov o stave kybernetickej bezpečnosti v roku 2022.

26 Napríklad nástroj Európskeho strediska pre rozvoj odborného vzdelávania: Skills-OVATE | Európske stredisko pre rozvoj odborného vzdelávania (europa.eu).

27 *The Future of Jobs Report* (Správa o budúcnosti pracovných miest), október 2020, Svetové ekonomické fórum.

28 Napríklad: Aliancia kybernetickobezpečnostných zručností – Nová vízia pre Európu – projekt REWIRE (financovaný z programu Erasmus+); projekty podporujúce centrum kompetencií v oblasti kybernetickej bezpečnosti [ECHO, CONCORDIA, CyberSec4Europe, SPARTA (financované v rámci programu Horizont 2020), projekt Cybersecpro (financovaný z programu Digitálna Európa)].

29 Najmä: Európsky rámec zručností v oblasti kybernetickej bezpečnosti (ECSF); CYBERHEAD – databáza vysokoškolského vzdelávania v oblasti kybernetickej bezpečnosti; platforma pre cvičenia v kybernetickej oblasti (CEP); Európska výzva v oblasti kybernetickej bezpečnosti; Európsky mesiac kybernetickej bezpečnosti.

bezpečnosti (ECCC)[30] sa zaoberá kybernetickobezpečnostnými zručnosťami v rámci osobitnej pracovnej skupiny, Európska akadémia bezpečnosti a obrany (EABO) pracuje na kybernetickobezpečnostných zručnostiach civilnej a vojenskej pracovnej sily v kontexte spoločnej bezpečnostnej a obrannej politiky[31], problém sa snažia riešiť aj súkromné organizácie[32] a odvetvie certifikácie kybernetickej bezpečnosti pripravuje plán a školenia zamerané na nedostatok zručností[33]. Aj členské štáty sa snažia riešiť tento problém prostredníctvom rôznych iniciatív od regulačných[34] až po zriaďovanie akadémií zručností v oblasti kybernetickej bezpečnosti[35] alebo kybernetických kampusov[36] a centier excelentnosti v oblasti boja proti počítačovej kriminalite[37] alebo prostredníctvom verejno-súkromných partnerstiev[38]. Práca všetkých týchto zainteresovaných strán však často nie je dostatočne koordinovaná a synergická a nedosiahla svoj potenciál podstatne zmeniť situáciu na trhu práce, čo dokazuje rastúci nedostatok pracovnej sily v oblasti kybernetickej bezpečnosti v EÚ. Musí sa posilniť aj synergia medzi kybernetickými komunitami, keďže potrebné zručnosti na udržiavanie kybernetickej bezpečnosti, boj proti **počítačovej kriminalite** alebo budovanie reakcií **kybernetickej obrany** sú často podobného charakteru.

EÚ má v súčasnosti obmedzené prostriedky na posúdenie **stavu a vývoja trhu práce v oblasti kybernetickej bezpečnosti** a zručností jeho pracovnej sily. Členské štáty a európske inštitúcie, orgány, úrady a agentúry sa spoliehajú buď na údaje zozbierané súkromnými subjektmi, alebo na širší súbor údajov o odborníkoch v oblasti IKT, ktoré zbiera EÚ, najmä Eurostat[39] a Európske stredisko pre rozvoj odborného vzdelávania (CEDEFOP)[40]. Inými slovami, EÚ má čiastkový a roztrieštený prehľad o svojich potrebách, čo jej bráni vytvoriť si súhrnný obraz o stave trhu práce v oblasti kybernetickej bezpečnosti.

3. Koordinovaná reakcia na úrovni EÚ: Akadémia zručností v oblasti kybernetickej bezpečnosti

3.1. Cieľ

Ako oznámila predsedníčka Európskej komisie vo svojom vyhlásení o zámere v rámci správy o stave Únie za rok 2022, navrhuje Komisia v kontexte Európskeho roka zručností s cieľom

---

30 Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/887 z 20. mája 2021, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier.

31 Najmä platforma pre vzdelávanie, odbornú prípravu, hodnotenie a cvičenia v kybernetickej oblasti.

32 Napríklad pracovná skupina 5 Európskej organizácie kybernetickej bezpečnosti (ECSO) Vzdelávanie, odborná príprava, informovanosť, kybernetické polygóny, ľudský faktor; organizácia DIGITALEUROPE.

33 Napríklad SANS Institute, (ISC)², ISACA.

34 Napríklad v národných stratégiách pre vzdelávanie alebo kybernetickú bezpečnosť.

35 Napríklad C-Academy v Portugalsku.

36 Napríklad kybernetické kampusy vo Francúzsku.

37 Napríklad Litovské centrum excelentnosti pre odbornú prípravu, výskum a vzdelávanie v oblasti počítačovej kriminality v Litve (L3CE).

38 Napríklad iniciatíva spoločnosti Microsoft zameraná na získavanie kybernetickobezpečnostných zručností.

39 *ICT specialists in employment* (Zamestnanosť odborníkov v oblasti IKT) – Štatistika v kocke (europa.eu).

40 Napríklad nástroj Európskeho strediska pre rozvoj odborného vzdelávania: Skills-OVATE | Európske stredisko pre rozvoj odborného vzdelávania (europa.eu).

zvládnuť výzvu riešiť otázky kybernetickobezpečnostných zručností a nedostatku pracovnej sily zriadenie **Akadémie zručností v oblasti kybernetickej bezpečnosti**[41, 42].

Cieľom Akadémie zručností v oblasti kybernetickej bezpečnosti (skrátene „akadémia“) je vytvoriť **miesto jednotného kontaktu a synergií** pre ponuky vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti, ako aj pre možnosti financovania a konkrétne opatrenia na podporu rozvoja kybernetickobezpečnostných zručností. Rozšíri iniciatívy zainteresovaných strán s cieľom dosiahnuť kritické množstvo, ktoré prinesie zmenu na trhu práce, a to aj v oblasti obrany. Na dosiahnutie väčšieho vplyvu by sa tieto činnosti zosúladili podľa spoločných cieľov a kľúčových ukazovateľov výkonnosti.

Akadémia sa zameria na získavanie zručností **odborníkov v oblasti kybernetickej bezpečnosti**. Činnosť akadémie sa premietne do politík EÚ v oblasti kybernetickej bezpečnosti, ale aj do vzdelávania a celoživotného vzdelávania. Dopĺňa dve odporúčania Rady týkajúce sa digitálneho vzdelávania a zručností, ktoré Komisia navrhla v rovnakom čase ako toto oznámenie[43].

Akadémia sa bude opierať o štyri piliere: 1. podpora **budovania znalostí prostredníctvom vzdelávania a odbornej prípravy**, a to prácou na spoločnom rámci pre profily úloh v oblasti kybernetickej bezpečnosti a súvisiace zručnosti, zlepšením európskej ponuky vzdelávania a odbornej prípravy s cieľom uspokojiť potreby, budovaním kariérnych možností a zabezpečením viditeľnosti a prehľadnosti odbornej prípravy a certifikácií v oblasti kybernetickej bezpečnosti s cieľom zlepšiť ponuku na trhu práce; 2. zabezpečenie lepšieho usmerňovania a viditeľnosti dostupných **možností financovania** činností súvisiacich so zručnosťami s cieľom maximalizovať ich vplyv; 3. výzva zainteresovaným stranám, **aby prijali opatrenia**, a 4. definovanie ukazovateľov na **monitorovanie vývoja trhu** a na umožnenie posudzovania účinnosti opatrení.

Zriadenie akadémie bude podporené finančnými prostriedkami vo výške 10 miliónov EUR z programu Digitálna Európa[44].

3.2.Riadenie akadémie

Akadémia by v konečnom dôsledku mohla mať podobu **konzorcia pre európsku digitálnu infraštruktúru (EDIC)**[45], aby poskytla infraštruktúru, ktorá by slúžila ako **jednotné kontaktné miesto** na podporu spolupráce medzi akademickou obcou, poskytovateľmi odbornej prípravy a odvetvím, kde by sa mohli stretávať strany ponuky a dopytu ekosystému kybernetickej bezpečnosti EÚ a kde by sa mohla realizovať príslušná odborná príprava. Tento nástroj by členským štátom umožnil spoločne pracovať na riešení nedostatku kybernetickobezpečnostných zručností, v súlade s ich mandátmi a právomocami úzko spolupracovať s Komisiou, agentúrou ENISA a Európskym centrom kompetencií v oblasti kybernetickej bezpečnosti (ECCC) a zapojiť všetky príslušné zainteresované strany, ako aj

---

41 Správa o stave Únie za rok 2022: Vyhlásenie o zámere predsedníčke Roberte Metsolovej a predsedovi vlády Petrovi Fialovi.

42 Spoločné oznámenie Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany, JOIN(2022) 49 final.

43 Návrhy odporúčaní Rady o kľúčových faktoroch umožňujúcich úspešné digitálne vzdelávanie a odbornú prípravu a o zlepšení poskytovania digitálnych zručností v rámci vzdelávania a odbornej prípravy.

44 Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694 z 29. apríla 2021, ktorým sa zriaďuje program Digitálna Európa a zrušuje rozhodnutie (EÚ) 2015/2240.

45 Konzorciá EDIC boli zriadené článkom 13 a nasl. rozhodnutia Európskeho parlamentu a Rady (EÚ) 2022/2481 zo 14. decembra 2022, ktorým sa zriaďuje politický program digitálne desaťročie do roku 2030.

sústrediť európske, vnútroštátne a súkromné investície na spoločný cieľ. Na tento účel sa zainteresované členské štáty vyzývajú, aby do 30. mája 2023 predložili Komisii predbežné oznámenie o svojej budúcej žiadosti o takéto konzorcium EDIC. Toto dobrovoľné predbežné oznámenie by Komisii umožnilo predložiť včasné pripomienky k návrhu žiadosti o konzorcium EDIC, čím by sa urýchlilo jeho ďalšie rozpracovanie a formálne predloženie. Počas celého procesu a v rozsahu, v akom o to členské štáty požiadajú, bude Komisia ako akcelerátor viacnárodných projektov pomáhať s prípravou žiadosti o konzorcium EDIC. Po kladnom posúdení žiadosti Komisiou a jej schválení výborom pre program Digitálne desaťročie vydá Komisia rozhodnutie o zriadení konzorcia EDIC a následne pomôže koordinovať jeho realizáciu[46].

Kým dôjde k formálnemu zriadeniu konzorcia EDIC, Komisia vytvorí virtuálne jednotné kontaktné miesto zlepšením **platformy Komisie pre digitálne zručnosti a pracovné miesta**[47] s pomocou podporného projektu európskej komunity kybernetickej bezpečnosti (ECCO)[48].

Agentúra **ENISA** bude prispievať k realizácii akadémie v súlade so svojimi cieľmi[49], najmä pokiaľ ide o pomoc pri vzdelávaní a odbornej príprave v oblasti kybernetickej bezpečnosti, a s prihliadnutím na svoje oznamovacie povinnosti podľa smernice NIS2[50]. **Európske centrum kompetencií v oblasti kybernetickej bezpečnosti** bude pri podpore realizácie Akadémie zručností v oblasti kybernetickej bezpečnosti pôsobiť v súlade so svojím strategickým programom. Centrum bude predovšetkým plniť strategický cieľ 3 (kybernetická bezpečnosť) programu Digitálna Európa. Bude využívať podporu Komisie a členských štátov prostredníctvom **národných koordinačných centier**. V relevantných prípadoch sa o pomoc požiada **skupina pre spoluprácu** zriadená podľa smernice NIS2[51]. V neposlednom rade bude na dosiahnutie cieľa akadémie, ktorým je odstránenie nedostatku kybernetickobezpečnostných zručností, potrebné spojiť sily s **príslušným odvetvím** a **akademickou obcou**.

4. Budovanie znalostí a odborná príprava: vytvorenie spoločného prístupu EÚ k odbornej príprave v oblasti kybernetickej bezpečnosti

V rámci piliera budovania znalostí a odbornej prípravy Akadémie zručností v oblasti kybernetickej bezpečnosti sa vypracuje štruktúrovaný prístup s jasným cieľom zvýšiť **počet**

---

46 Tamže, článok 12.

47 Domov | Platforma pre digitálne zručnosti a pracovné miesta (europa.eu).

48 Pozri *European Cybersecurity Competence Centre and Network: new EU-funded project to support the Cyber Community* (Európske centrum kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier: nový projekt financovaný z prostriedkov EÚ na podporu komunity kybernetickej bezpečnosti) (europa.eu). V decembri 2022 podpísala Európska komisia zmluvu na podporu komunity kybernetickej bezpečnosti EÚ v rámci Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti v hodnote 3 miliónov EUR. Tento projekt prispeje k plneniu cieľov EÚ v oblasti budovania komunity a kapacít, pokiaľ ide o výskum, inovácie, širokú akceptáciu a priemyselnú základňu v oblasti kybernetickej bezpečnosti.

49 „Agentúra ENISA podporuje budovanie kapacít a pripravenosť v celej Únii tým, že inštitúciám, orgánom, úradom a agentúram Únie, ako aj členským štátom a verejným a súkromným zainteresovaným stranám pomáha […] pri rozvoji zručností a spôsobilosti v oblasti kybernetickej bezpečnosti.“ Pozri článok 4 ods. 3 aktu o kybernetickej bezpečnosti.

50 Článok 18 smernice NIS2.

51 Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

osôb s kybernetickými zručnosťami v EÚ, lepšie zacieliť odbornú prípravu na **potreby trhu** a zviditeľniť **kariérne možnosti**.

4.1. Hovorme rovnakým jazykom: spoločný prístup k profilom úloh v oblasti kybernetickej bezpečnosti a súvisiacim zručnostiam

Agentúra ENISA už vymedzila profily úloh odborníkov v oblasti kybernetickej bezpečnosti v rámci európskeho rámca kybernetických zručností (**ECSF**)[52]. Na tomto základe by akadémia mala vymedziť a hodnotiť príslušné zručnosti, monitorovať vývoj chýbajúcich zručností a poskytovať informácie o nových potrebách. Pri každej úlohe v oblasti kybernetickej bezpečnosti v európskom rámci kybernetických zručností je ako prvok opisu profilu[53] začlenený súbor platných kompetencií z európskeho rámca elektronických kompetencií[54].

Agentúra ENISA preto preskúma európsky rámec kybernetických zručností a **identifikuje meniace sa potreby a nedostatky, pokiaľ ide o zručnosti** pracovnej sily v oblasti kybernetickej bezpečnosti, a to aj prostredníctvom pokročilých nástrojov (napr. umelej inteligencie, veľkých dát[55], hĺbkovej analýzy údajov). Na tento účel bude agentúra ENISA pracovať pod vedením konzorcia EDIC, keď bude zriadené, Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti, spolu s národnými koordinačnými centrami, Komisiou, projektom ECCO a účastníkmi trhu[56]. Pokiaľ ide o pracovnú silu v oblasti kybernetickej obrany, agentúra ENISA náležite zohľadní prácu Európskej akadémie bezpečnosti a obrany. Podobne aj v oblasti boja proti počítačovej kriminalite bude agentúra ENISA zohľadňovať činnosti Agentúry EÚ pre odbornú prípravu v oblasti presadzovania práva (CEPOL) a Europolu pri vypracúvaní operačnej analýzy potrieb odbornej prípravy[57] v oblasti kybernetických útokov.

Európsky rámec kybernetických zručností sa bude v rámci akadémie v pravidelných dvojročných cykloch dopĺňať a prehodnocovať. Okrem toho Komisia a Európska služba pre vonkajšiu činnosť podľa potreby prispejú k vymedzeniu osobitných profilov a súvisiacich

---

52 Európsky rámec kybernetických zručností (ECSF) – ENISA (europa.eu). Európsky rámec kybernetických zručností pomáha pri identifikácii a formulácii úloh, kompetencií, zručností a znalostí súvisiacich s úlohami európskych odborníkov v oblasti kybernetickej bezpečnosti. Všetky úlohy súvisiace s kybernetickou bezpečnosťou zhŕňa do profilov, ktoré sa jednotlivo analyzujú až na úroveň detailov o ich príslušných zodpovednostiach, zručnostiach, synergiách a vzájomných závislostiach.

53 V tejto súvislosti pozri *User Manual - European Cybersecurity Skills Framework (ECSF)* [Používateľská príručka – Európsky rámec kybernetickobezpečnostných zručností (ECSF)] – september 2022.

54 Európsky rámec elektronických kompetencií | ESCO (europa.eu). Európsky rámec elektronických kompetencií poskytuje konzistentné prepojenia v kontexte kvalifikácií v oblasti IKT a iných rámcov relevantných pre tento sektor vrátane rámca DigComp.

55 Pozri napríklad nástroj Skills-OVATE vyvinutý strediskom Cedefop.

56 Agentúra bude ďalej využívať výsledky iných projektov financovaných z prostriedkov EÚ [napr. REWIRE, dátový priestor pre zručnosti (DS4S), CyberSecPro, Concordia] a metodiky vyplývajúce z podobných iniciatív [napr. *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States* (Budovanie kvalifikovanej pracovnej sily v oblasti kybernetickej bezpečnosti v piatich krajinách: poznatky z Austrálie, Kanady, Nového Zélandu, zo Spojeného kráľovstva a Spojených štátov), správa OECD, vydaná 21. marca 2023], aby sa v budúcnosti zabezpečil aktuálny prehľad potrieb v prostredí s neustále sa vyvíjajúcim dopytom.

57 CEPOL, *Operational Training Needs Assessment (OTNA)* (Operačné posúdenie potrieb odbornej prípravy).

zručností pre jednotlivé sektory, a to s pomocou agentúr a orgánov EÚ, ako sú napríklad Európska akadémia bezpečnosti a obrany[58], Europol a CEPOL[59].

Takisto sa vytvoria prepojenia medzi európskym rámcom kybernetických zručností a príslušnými nástrojmi politiky zamestnanosti EÚ[60]. Predovšetkým sa do **klasifikácie ESCO** začlenia profily pracovných pozícií európskeho rámca kybernetických zručností, ako aj súvisiace zručnosti. Tým sa zlepší klasifikácia povolaní a zručností v oblasti kybernetickej bezpečnosti a prepojenie medzi nimi, čo jednotlivcom uľahčí zvyšovanie úrovne zručností a rekvalifikáciu a podporí zosúladenie pracovných miest na základe zručností a cezhraničnú mobilitu.

4.2. Podpora spolupráce pri tvorbe učebných plánov vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti

Po zriadení konzorcia EDIC by akadémia mala získať podporu členských štátov, aby sa stala **referenčným miestom v Európe pre navrhovanie a poskytovanie odbornej prípravy v oblasti kybernetickej bezpečnosti** zameranej na najžiadanejšie zručnosti a poskytovala príležitosti na odbornú prípravu na pracovisku a stáže pre startupy a MSP, ako aj pre verejnú správu v inovačných kybernetickobezpečnostných spoločnostiach a centrách kompetencií v oblasti kybernetickej bezpečnosti. Konzorcium EDIC by malo pri navrhovaní takejto odbornej prípravy spolupracovať so všetkými príslušnými zainteresovanými stranami vrátane príslušného odvetvia a vychádzať z projektov, ako je napríklad **CyberSecPro**[61] financovaný z programu Digitálna Európa, ktorý spája 17 inštitúcií vysokoškolského vzdelávania a 13 bezpečnostných spoločností zo 16 členských štátov, aby sa stalo príkladom najlepších postupov pre všetky programy odbornej prípravy v oblasti kybernetickej bezpečnosti.

Akadémia bude spolupracovať so všetkými príslušnými zainteresovanými stranami s cieľom **zatraktívniť pre mladé generácie** kariéru v oblasti kybernetickej bezpečnosti. V súlade s návrhom odporúčania Rady o zlepšení poskytovania digitálnych zručností v rámci vzdelávania a odbornej prípravy by členské štáty mali zaviesť a posilniť opatrenia v oblasti náboru a odbornej prípravy špecializovaných učiteľov a školiteľov a uľahčiť získavanie kybernetickobezpečnostných zručností, a to aj prostredníctvom učňovskej prípravy. Malo by sa podporovať začlenenie kybernetickej bezpečnosti do programov vzdelávania a odbornej prípravy a zároveň by sa mala zabezpečiť ich prístupnosť, ďalej rozvíjať ponuka **učňovskej prípravy** a stáží, mali by sa podporovať inovačné prístupy vrátane napríklad vzdelávacích počítačových hier a spoločných simulačných platforiem, organizovať týždne pohrúženia sa do pozícií v oblasti kybernetickej bezpečnosti a vysvetľovať profily netechnických úloh. Takisto by sa mala podporovať účasť ťažko osloviteľných skupín, ako sú mladí ľudia so zdravotným postihnutím, ľudia žijúci v odľahlých alebo vo vidieckych oblastiach a ľudia

---

58 V tejto súvislosti pozri spoločné oznámenie Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany, JOIN(2022) 49 final.

59 V tejto súvislosti sa bude venovať pozornosť práci na rámci kompetencií pre odbornú prípravu v oblasti počítačovej kriminality, ktorý sa v súčasnosti vyvíja.

60 Napríklad Európska klasifikácia zručností, kompetencií, kvalifikácií a povolaní (ESCO), Europass, Európska sieť služieb zamestnanosti (EURES).

61 CyberSecPro. Vykoná sa napríklad analýza programov, kurzov a letných škôl kybernetickej bezpečnosti ponúkaných na univerzitách, ako aj používaných bodovacích tabuliek Európskeho systému prenosu a zhromažďovania kreditov (ECTS), zabezpečí sa zapojenie cieľového počtu viac ako 530 stážistov počas trojročného obdobia, vyškolia sa externí pracovníci z rôznych odvetví a sektorov.

z iných menšinových skupín, na týchto možnostiach vzdelávania v oblasti kybernetickej bezpečnosti.

Komisia bude ďalej podporovať rozvoj mikrocertifikátov, programov odborného vzdelávania a prípravy. V rámci programu Erasmus+ sa budú naďalej financovať najmä **spoločné bakalárske a magisterské študijné programy, spoločné kurzy alebo moduly, ktoré môžu viesť k získaniu mikrocertifikátov**, a **zmiešané intenzívne programy**[62] zamerané na všetky témy vrátane **kybernetickej bezpečnosti**. Podporí sa aj ďalšie zavádzanie **iniciatívy „Európske univerzity“**[63] a **centier excelentnosti odborného vzdelávania a prípravy**[64] s cieľom podporiť intenzívnejšiu spoluprácu medzi inštitúciami vysokoškolského vzdelávania a príslušnými inštitúciami odborného vzdelávania a odbornej prípravy v celej Európe. Tento cieľ hlbšej spolupráce podporia programy financovania z prostriedkov EÚ vrátane programu Erasmus+ a programu Digitálna Európa, ako aj finančné prostriedky EÚ určené na rozvoj **individuálnych vzdelávacích účtov**[65].

S cieľom uľahčiť spoluprácu na vnútroštátnej úrovni medzi akademickou obcou a poskytovateľmi odbornej prípravy v oblasti kybernetickobezpečnostných zručností so zamestnávateľmi zo súkromného a verejného sektora a podporiť synergie medzi verejným a súkromným sektorom sa národné koordinačné centrá vyzývajú, aby preskúmali možnosť zriadenia **kybernetických kampusov** v členských štátoch. Cieľom kybernetických kampusov by bolo vytvoriť centrá excelentnosti na vnútroštátnej úrovni pre komunitu v oblasti kybernetickej bezpečnosti, pričom akadémia by pomohla pri vytváraní sietí a ďalšej koordinácii ich činností.

Agentúra ENISA takisto rozšíri svoju ponuku odbornej prípravy v oblasti kybernetickej bezpečnosti, pričom zosúladí svoj **katalóg kurzov**[66] s profilmi európskeho rámca kybernetických zručností a vypracuje moduly odbornej prípravy podľa jednotlivých profilov, čím sa môže rozšíriť ponuka odbornej prípravy členských štátov. Agentúra ENISA rozšíri aj svoj **program odbornej prípravy školiteľov**[67], ktorý sa zameriava na profesionálne potreby európskych inštitúcií, orgánov, úradov a agentúr, subjektov verejného sektora v členských štátoch a **verejných a súkromných prevádzkovateľov kritických služieb** v rozsahu pôsobnosti smernice NIS2.

Aj ostatné agentúry a orgány EÚ rozšíria svoju ponuku odbornej prípravy v oblasti kybernetickej bezpečnosti. Napríklad **Európska akadémia bezpečnosti a obrany** pri vykonávaní politiky EÚ v oblasti kybernetickej obrany vypracuje nový súbor kurzov kybernetickej bezpečnosti a zosúladí niektoré zo svojich súčasných kurzov s európskym rámcom kybernetických zručností. Tieto kurzy povedú k certifikácii vzdelávacích výstupov[68]. Európska akadémia bezpečnosti a obrany v spolupráci s Komisiou preskúma možnosť integrácie certifikátov do európskej peňaženky digitálnej identity. Európska akadémia

---

62 Zmiešané intenzívne programy kombinujú dištančnú výučbu s krátkym obdobím fyzickej mobility.

63 Iniciatíva „Európske univerzity“ | Európsky vzdelávací priestor (europa.eu).

64 Centrá excelentnosti odborného vzdelávania a prípravy | Erasmus+ (europa.eu).

65 V súlade s odporúčaním Rady zo 16. júna 2022 týkajúcim sa individuálnych vzdelávacích účtov.

66 Kurzy odbornej prípravy – ENISA (europa.eu).

67 Program odbornej prípravy školiteľov – ENISA (europa.eu).

68 V súlade s článkom 20 ods. 4 rozhodnutia Rady (SZBP) 2020/1515 z 19. októbra 2020, ktorým sa zriaďuje Európska akadémia bezpečnosti a obrany a ktorým sa zrušuje rozhodnutie (SZBP) 2016/2382.

bezpečnosti a obrany ďalej preskúma možné mechanizmy hodnotenia zručností, na základe ktorých sa budú vydávať certifikáty. Podobne sa v oblasti boja proti počítačovej kriminalite vyvinie úsilie o úzke prepojenie s **Akadémiou pre počítačovú kriminalitu agentúry CEPOL**[69] s cieľom podporiť synergie a komplementárnosť pri navrhovaní a vykonávaní učebných plánov odbornej prípravy.

4.3. Vytváranie synergií a zviditeľňovanie odbornej prípravy a certifikácie v oblasti kybernetickej bezpečnosti v členských štátoch

Akadémia by sa mala zaoberať otázkou viditeľnosti a synergií odbornej prípravy a certifikácie. Bolo by to prospešné pre kybernetické komunity z občianskej spoločnosti, z oblasti obrany, presadzovania práva a diplomacie, keďže vo všetkých sektoroch sa v mnohých prípadoch vyžadujú rovnaké odborné znalosti založené na podobných učebných plánoch a vzdelávacích výstupoch.

Akadémia by záujemcom o kariéru v oblasti kybernetickej bezpečnosti slúžila ako **jednotné kontaktné miesto**. V krátkodobom horizonte sa to dosiahne zlepšením **platformy Komisie pre digitálne zručnosti a pracovné miesta** s pomocou projektu ECCO. Osobitná časť venovaná kariére v oblasti kybernetickej bezpečnosti sa prepojí s existujúcimi nástrojmi – od programov vysokoškolského vzdelávania cez možnosti odbornej prípravy vrátane kurzov vedúcich k získaniu mikrocertifikátov a programov odborného vzdelávania a prípravy až po pracovné ponuky. Na tento účel sa na platforme budú uvádzať alebo sa do nej integrujú prebiehajúce činnosti a iniciatívy, ako sú činnosti a iniciatívy agentúry ENISA, ktorá v spolupráci s akademickou obcou zaviedla **mapovanie vzdelávacích inštitúcií** poskytujúcich programy kybernetickej bezpečnosti. S podporou národných koordinačných centier sa uskutočnia ďalšie zlepšenia. Okrem toho agentúra ENISA s podporou národných koordinačných centier, Komisie a projektu ECCO a v spolupráci so subjektmi poskytujúcimi certifikácie vytvorí a skonsoliduje **register existujúcich školení z verejného a súkromného sektora a register certifikácií kybernetickej bezpečnosti**, pričom sa bude opierať aj o iné relevantné iniciatívy[70]. Budú integrované aj do jednotného kontaktného miesta platformy digitálnych zručností a pracovných miest. Táto práca bude prínosom aj pre národné koordinačné centrá, ktorých úlohou je najmä propagovať a šíriť vzdelávacie programy v oblasti kybernetickej bezpečnosti[71].

Takisto je potrebné poskytnúť odborníkom záruky, že odborná príprava, ktorú absolvujú, má požadovanú kvalitu. V tejto súvislosti agentúra ENISA vypracuje **pilotný projekt**, v rámci ktorého preskúma vytvorenie európskej schémy osvedčovania kybernetickobezpečnostných zručností.

Okrem toho je nevyhnutné identifikovať zručnosti a školenia a priradiť ich k pracovnému profilu, ale takisto je dôležité zabezpečiť, aby sa služby kybernetickej bezpečnosti

---

69 Akadémia pre počítačovú kriminalitu agentúry CEPOL bola zriadená v roku 2019 s cieľom poskytnúť najmodernejšiu platformu na zlepšenie znalostí o počítačovej kriminalite a kybernetických kapacít v Európe.

70 Napríklad Akadémia W4C – Women4Cyber alebo projekt globálnej certifikácie v oblasti počítačovej kriminality pre orgány presadzovania práva a justičné orgány.

71 „1. Národné koordinačné centrá plnia tieto úlohy: […] g) bez toho, aby boli dotknuté právomoci členských štátov v oblasti vzdelávania, a s prihliadnutím na príslušné úlohy agentúry ENISA spolupracujú s vnútroštátnymi orgánmi, pokiaľ ide o možné príspevky na podporu a šírenie vzdelávacích programov v oblasti kybernetickej bezpečnosti“, článok 7 ods. 1 písm. g) nariadenia o Európskom centre kompetencií v oblasti kybernetickej bezpečnosti. Pozri aj súvisiace odôvodnenie 28.

poskytovali s požadovanými kompetenciami, odbornými znalosťami a skúsenosťami. To platí najmä pre poskytovateľov riadených bezpečnostných služieb v oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. V smernici NIS2 a v návrhu aktu o kybernetickej solidarite sa stanovujú konkrétne úlohy pre takýchto poskytovateľov riadených bezpečnostných služieb. Komisia preto navrhuje aj **cielenú zmenu aktu o kybernetickej bezpečnosti**[72] s cieľom umožniť schémy certifikácie riadených bezpečnostných služieb na úrovni EÚ. Cieľom takýchto schém certifikácie by malo byť okrem iného zabezpečiť, aby tieto služby poskytovali zamestnanci s veľmi vysokou úrovňou technických znalostí a kompetencií v príslušných oblastiach.

Mechanizmy zabezpečovania kvality a uznávania mikrocertifikátov[73] uľahčujú transparentnosť, porovnateľnosť a prenosnosť vzdelávacích výstupov. V súlade s odporúčaním Rady týkajúcim sa európskeho prístupu k mikrocertifikátom[74] sa členské štáty vyzývajú, aby do svojich národných kvalifikačných rámcov zahrnuli mikrocertifikáty v oblasti kybernetickej bezpečnosti. Vďaka tomu by mohli prepojiť mikrocertifikáty v oblasti kybernetickej bezpečnosti s európskym kvalifikačným rámcom[75]. Na vydávanie digitálne podpísaných kvalifikácií a mikrocertifikátov v oblasti kybernetickej bezpečnosti pre jednotlivcov je k dispozícii infraštruktúra európskych digitálnych certifikátov na vzdelávanie. Obsahujú veľké množstvo údajov vrátane údajov o vzdelávacích výstupoch v oblasti kybernetickej bezpečnosti a môžu byť uložené v pripravovanej **európskej peňaženke digitálnej identity**[76].

Opatrenia v rámci akadémie

Členské štáty a príslušné odvetvie

- Zabezpečia podporu rozvoja a uznávania **mikrocertifikátov** vzdelávania v oblasti kybernetickej bezpečnosti v súlade s odporúčaním Rady týkajúcim sa európskeho prístupu k mikrocertifikátom.
- Zahrnú kvalifikácie v oblasti kybernetickej bezpečnosti vrátane mikrocertifikátov do **národných kvalifikačných rámcov**.
- Poskytnú jednotlivcom zapojeným do iniciatív rozvoja kybernetickobezpečnostných zručností **možnosti vzdelávania na pracovisku** prostredníctvom učňovskej prípravy.

Komisia

- V krátkodobom horizonte do konca roka 2023 prostredníctvom **platformy digitálnych zručností a pracovných miest** vytvorí **jednotné kontaktné miesto** pre programy kybernetickej bezpečnosti, existujúce školenia a certifikácie kybernetickej bezpečnosti.

[72] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).

[73] Napríklad záznamy alebo certifikácia vzdelávacích výstupov, ktoré jednotlivci získali po krátkych školeniach.

[74] Odporúčanie Rady týkajúce sa európskeho prístupu k mikrocertifikátom pre celoživotné vzdelávanie a zamestnateľnosť.

[75] Odporúčanie Rady z 22. mája 2017 týkajúce sa európskeho kvalifikačného rámca pre celoživotné vzdelávanie, ktorým sa zrušuje odporúčanie Európskeho parlamentu a Rady z 23. apríla 2008 o vytvorení európskeho kvalifikačného rámca pre celoživotné vzdelávanie.

[76] Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca pre európsku digitálnu identitu.

- S cieľom umožniť certifikáciu poskytovateľov riadenej bezpečnosti navrhne 18. apríla 2023 zmenu **aktu o kybernetickej bezpečnosti**.

Orgány a agentúry EÚ

- Do konca roka 2023 zavedú **európsky rámec kybernetických zručností** ako spoločný prístup k profilom úloh v oblasti kybernetickej bezpečnosti a súvisiacim zručnostiam.
- Agentúra ENISA v druhom štvrťroku 2023 iniciuje vypracovanie pilotného projektu, ktorým sa vytvorí **európska schéma osvedčovania** kybernetickobezpečnostných zručností.
- Agentúra ENISA preskúma svoj **katalóg kurzov** a do konca roka 2023 otvorí **program odbornej prípravy školiteľov** pre verejných a súkromných prevádzkovateľov kritických služieb.
- Do polovice roka 2023 dokončia **zosúladenie učebných plánov Európskej akadémie bezpečnosti a obrany s európskym rámcom kybernetických zručností**.

5. Zapojenie zainteresovaných strán: záväzok vyriešiť nedostatok kybernetickobezpečnostných zručností

V rámci akadémie sa vypracuje koordinovaný prístup k zapojeniu zainteresovaných strán s cieľom riešiť nedostatok kybernetickobezpečnostných zručností. Cieľom bude maximalizovať viditeľnosť a vplyv záväzkov rôznych zainteresovaných strán zameraných na zníženie nedostatku kybernetickobezpečnostných zručností.

Komisia vyzýva zainteresované strany, aby prijali konkrétne záväzky, v ktorých prisľúbia zvýšiť úroveň zručností pracovníkov a rekvalifikovať ich pomocou špecializovaných opatrení, pri ktorých budú v čo najväčšej miere vychádzať zo zisteného nedostatku kybernetickobezpečnostných zručností. Takéto **prísľuby zainteresovaných strán v oblasti kybernetickej bezpečnosti** by sa mali oznamovať na **platforme digitálnych zručností a pracovných miest**, podobne ako ostatné digitálne záväzky, ktoré už možno na platforme nájsť. Komisia ďalej vyzýva zainteresované strany, ktoré na platforme prijmú záväzok v oblasti kybernetickej bezpečnosti, aby sa pripojili k **rozsiahlemu digitálnemu partnerstvu v rámci Paktu o zručnostiach**[77]. Záväzky v oblasti kybernetickej bezpečnosti prijaté v rámci rozsiahleho digitálneho partnerstva sa majú predložiť na platforme digitálnych zručností a pracovných miest. Podobne sa odporúča, aby sa záväzky prijaté v rámci platformy digitálnych zručností a pracovných miest oznamovali v rámci rozsiahleho digitálneho partnerstva Paktu o zručnostiach.

Komisia ďalej vyzýva členské štáty, aby **pokračovali v úsilí o vykonávanie deklarácie o ženách v digitálnom sektore**[78] s cieľom podporiť ženy, aby zohrávali aktívnu a významnú úlohu v sektore digitálnych technológií, a dosiahnuť rovnomernejšie rodové zastúpenie na pozíciách v oblasti kybernetickej bezpečnosti. Komisia takisto vyzýva členské štáty, aby rozvíjali synergie so svojimi programami **Európskeho sociálneho fondu plus** (ESF+), a tak

[77] *New European Partnerships launched to deliver on the EU's ambitions for the Digital Decade* (Vznik nových európskych partnerstiev s cieľom splniť ambície EÚ v digitálnom desaťročí) | Formovanie digitálnej budúcnosti Európy (europa.eu), partnerstvo bolo vytvorené v rámci Paktu o zručnostiach na riešenie nedostatku v oblasti informačných a komunikačných technológií (IKT).

[78] *EU countries commit to boost participation of women in digital* (Krajiny EÚ sa zaviazali zvýšiť účasť žien v digitálnom sektore) | Formovanie digitálnej budúcnosti Európy (europa.eu).

ďalej podporovali cieľ rodovej rovnosti v účasti na trhu práce[79], napríklad prostredníctvom vytvorenia **mentorských programov pre dievčatá a ženy.** Tieto programy môžu uľahčiť vytváranie vzorov, ktoré prilákajú dievčatá do profesií v oblasti kybernetickej bezpečnosti, a zároveň bojovať proti rodovým stereotypom. Podporí sa tým aj zvyšovanie úrovne zručností a rekvalifikácia žien, ako aj rozvoj komunity, ktorá môže podporovať ženy pri vstupe na trh práce v oblasti kybernetickej bezpečnosti alebo ich povýšení na tomto trhu práce.

Členské štáty by mali v rámci **svojich národných stratégií kybernetickej bezpečnosti prijať osobitné opatrenia s cieľom zmierniť nedostatok kybernetickobezpečnostných zručností**[80], identifikovať a lepšie nasmerovať úsilie na odstránenie nedostatku zručností a v konečnom dôsledku zabezpečiť riadne plnenie svojich povinností podľa smernice NIS2.

Niektoré členské štáty využívajú **synergie medzi civilnými iniciatívami, iniciatívami týkajúcimi sa obrany a iniciatívami v oblasti presadzovania práva**. Napríklad rozvíjanie pracovnej sily s využitím povinnej vojenskej služby na vnútroštátnej úrovni alebo využívanie kybernetických záložníkov, čo sú občania s vojenským výcvikom, ktorí v ozbrojených silách zastávajú pozície v oblasti kybernetickej bezpečnosti[81], umožňuje obyvateľstvu, a najmä mladým dospelým, zlepšovať svoje zručnosti v oblasti kybernetickej bezpečnosti a kybernetickej obrany. To isté platí aj v oblasti **boja proti počítačovej kriminalite**, keďže existuje mnoho podobností medzi všeobecnými opatreniami v oblasti kybernetickej bezpečnosti a činnosťami presadzovania práva v reakcii na kybernetické bezpečnostné incidenty. Komisia podporuje diskusie medzi členskými štátmi o takýchto iniciatívach a vyzýva ich, aby posúdili, ako môže kvalifikovaná pracovná sila čo najlepšie slúžiť obranným aj civilným komunitám v oblasti kybernetickej bezpečnosti.

Komisia zváži návrhy, ako vykryť súčasné a očakávané nedostatky zistené pri preskúmaní potrieb európskych inštitúcií, orgánov, úradov a agentúr. Predovšetkým podporí zamestnancov, aby využili pripravované **štipendijný program EÚ a Spojených štátov v oblasti kybernetickej bezpečnosti** zriadený v rámci dialógu medzi EÚ a USA.

Opatrenia v rámci akadémie

Odvetvie

- Od 18. apríla 2023 bude na platforme digitálnych zručností a pracovných miest navrhovať konkrétne **prísľuby v oblasti kybernetickej bezpečnosti**.

Členské štáty

- Zahrnú do **národných stratégií kybernetickej bezpečnosti** konkrétne opatrenia na riešenie nedostatku kybernetickobezpečnostných zručností.

Členské štáty a odvetvie

- Budú vykonávať deklaráciu o ženách v digitálnom sektore a do roku 2030 dosiahnu **rovnomernejšie rodové zastúpenie na pozíciách v oblasti kybernetickej bezpečnosti**.

[79] Článok 4 ods. 1 písm. c) nariadenia Európskeho parlamentu a Rady (EÚ) 2021/1057 z 24. júna 2021, ktorým sa zriaďuje Európsky sociálny fond plus (ESF+) a zrušuje nariadenie (EÚ) č. 1296/2013.

[80] Článok 7 ods. 2 písm. f) smernice NIS2.

[81] *Report – Cyber Conscription: Experience and Best Practice from Selected Countries* (Správa – Kybernetická branná povinnosť: skúsenosti a najlepšie postupy z vybraných krajín), Martin Hurt a Tiia Sõmer, Medzinárodné centrum pre obranu a bezpečnosť, február 2021.

6. Financovanie: budovanie synergií s cieľom maximalizovať vplyv výdavkov na rozvoj kybernetickobezpečnostných zručností

V rámci akadémie sa maximalizuje vplyv investícií do kybernetickobezpečnostných zručností tým, že sa zabezpečí jednotné kontaktné miesto, uľahčí sa lepšie prideľovanie finančných prostriedkov na uspokojenie potrieb trhu a zefektívni sa ich využívanie, pričom sa podporí synergia medzi rôznymi nástrojmi a zároveň sa zabráni duplicite úsilia[82].

6.1. Zosúladenie finančných prostriedkov s potrebami

V rámci akadémie bude Európske centrum kompetencií v oblasti kybernetickej bezpečnosti s podporou Komisie, projektu ECCO a národných koordinačných centier zhromažďovať **informácie o tom, ako sa finančné prostriedky EÚ využívajú na financovanie kybernetickobezpečnostných zručností**, a bude posudzovať, ako finančné prostriedky EÚ prispievajú k znižovaniu nedostatku kybernetickobezpečnostných zručností. S prihliadnutím na tieto súhrnné informácie sa bude Európske centrum kompetencií v oblasti kybernetickej bezpečnosti snažiť zabezpečiť lepšie prideľovanie finančných prostriedkov EÚ na uspokojenie zistených potrieb. Bude financovať opatrenia, ktorými by sa riešili najnaliehavejšie nedostatky pracovnej sily v oblasti kybernetickej bezpečnosti vrátane tých, ktoré súvisia s realizáciou potrieb politiky v tejto oblasti.

6.2. Zviditeľnenie dostupných finančných prostriedkov a partnerských iniciatív pre kybernetickobezpečnostné zručnosti

V krátkodobom horizonte sa **platforma digitálnych zručností a pracovných miest** stane pre zainteresované strany jednotným kontaktným miestom, kde budú k dispozícii všetky informácie o možnostiach financovania kybernetickobezpečnostných zručností.

EÚ investuje do ľudí a ich zručností a využíva partnerstvá, najmä s príslušným odvetvím, na mobilizáciu opatrení zameraných na zvyšovanie úrovne zručností a rekvalifikáciu prostredníctvom niekoľkých nástrojov určených v rámci **Európskeho programu v oblasti zručností**[83], najmä **Paktu o zručnostiach**[84] a **akčného plánu digitálneho vzdelávania**[85]. Z **programu Digitálna Európa** sa financujú príležitosti na získanie kybernetickobezpečnostných zručností, najmä prostredníctvom iniciatív viacnárodných projektov, pričom toto financovanie sa jasne dopĺňa s podporou, ktorú ponúka program Horizont Európa na výskum a inovačné technologické riešenia v oblasti kybernetickej bezpečnosti. Z **Európskeho obranného fondu**[86] sa financuje výskum a vývoj technológií na

---

82 Možnosti financovania (europa.eu). Podporné služby Paktu o zručnostiach poskytujú jednotné kontaktné miesto pre informácie o financovaní zručností, a to aj pre digitálny ekosystém. Podporné služby paktu poskytujú všeobecné informácie o nástrojoch financovania, ktoré nie sú špecificky zamerané na kybernetickobezpečnostné zručnosti, napriek tomu by akadémia mala zohľadniť ich prácu, aby sa zabránilo duplicite.

83 Európsky program v oblasti zručností – Zamestnanosť, sociálne záležitosti a začlenenie – Európska komisia (europa.eu).

84 Finančné nástroje EÚ na zvyšovanie úrovne zručností a rekvalifikáciu – Zamestnanosť, sociálne záležitosti a začlenenie – Európska komisia (europa.eu).

85 Akčný plán digitálneho vzdelávania na roky 2021 – 2027.

86 Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/697 z 29. apríla 2021, ktorým sa zriaďuje Európsky obranný fond a zrušuje nariadenie (EÚ) 2018/1092.

vykonávanie účinných kybernetických operácií vrátane odbornej prípravy a cvičení[87]. **Erasmus+** bude naďalej podporovať takéto iniciatívy, a to aj prostredníctvom zmiešaných intenzívnych programov a projektov spolupráce.

Členské štáty sa vyzývajú, aby mobilizovali finančné prostriedky EÚ, ktoré priamo spravujú, na podporu kybernetickobezpečnostných zručností a pracovných miest. Fondy politiky súdržnosti, ako napríklad **Európsky fond regionálneho rozvoja (EFRR)** a **ESF+**, majú v tomto ohľade významný potenciál synergií[88]. Dôležitú komplementárnosť pri dosahovaní cieľov akadémie prinášajú aj opatrenia v rámci **Mechanizmu na podporu obnovy a odolnosti**[89] a **Programu InvestEU**[90].

Opatrenia v rámci akadémie

Európske centrum kompetencií v oblasti kybernetickej bezpečnosti a agentúra ENISA

- Do konca roka 2024 **preskúmajú** existujúce finančné prostriedky EÚ na kybernetickobezpečnostné zručnosti v porovnaní s potrebami trhu, posúdia **účinnosť** a určia **priority** financovania.

Komisia

- Do konca roka 2023 vytvorí na platforme digitálnych zručností a pracovných miest **jednotné kontaktné miesto** pre možnosti financovania kybernetickobezpečnostných zručností.

7. Meranie pokroku: integrovaná zodpovednosť

V rámci akadémie sa vypracuje **metodika**, ktorá umožní **merať pokrok pri riešení nedostatku kybernetickobezpečnostných zručností**.

7.1. Definovanie ukazovateľov kybernetickej bezpečnosti na monitorovanie vývoja trhu práce v oblasti kybernetickej bezpečnosti

Index digitálnej ekonomiky a spoločnosti (DESI) sumarizuje ukazovatele digitálnej výkonnosti Európy a sleduje pokrok v členských štátoch EÚ. V rámci Akadémie zručností v oblasti kybernetickej bezpečnosti agentúra ENISA v spolupráci s Komisiou a so skupinou

[87] Členské štáty sa zaviazali k spoločnej odbornej príprave a spoločným cvičeniam, napríklad prostredníctvom vytvorenia projektov stálej štruktúrovanej spolupráce (PESCO) v oblasti kybernetickej odbornej prípravy a cvičení a účasti na nich, ako sú Akademické a inovačné centrum EÚ pre kybernetickú oblasť (CAIH EÚ) a Združenie národných kybernetických polygónov.

[88] Článok 3 ods. 1 nariadenia (EÚ) 2021/1058 a článok 4 ods. 1 písm. g) nariadenia (EÚ) 2021/1057.

[89] Napríklad v estónskom pláne obnovy a odolnosti sa predpokladajú investície (10 mil. EUR) do digitálnych zručností, ktoré budú zahŕňať revíziu odbornej prípravy dostupnej pre odborníkov na IKT, financovanie zvyšovania úrovne zručností a rekvalifikácie odborníkov na IKT v oblasti kybernetickej bezpečnosti a prispejú k vypracovaniu pilotného programu na prepracovanie kvalifikačného rámca pre odborníkov na IKT.

[90] Zainteresované strany (napr. poskytovatelia odbornej prípravy a spoločnosti, ktoré chcú navrhnúť alebo zlepšiť svoje vzdelávacie činnosti v oblasti kybernetickej bezpečnosti) sa môžu obrátiť na Poradenské centrum InvestEU, ktoré poskytuje technickú podporu a pomoc vrátane budovania kapacít pre tvorcov projektov a subjekty, a nájsť rôzne informácie na Portáli InvestEU.

pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti[91] vypracuje **ukazovatele** vrátane rodových ukazovateľov na sledovanie pokroku dosiahnutého v členských štátoch EÚ pri zvyšovaní počtu odborníkov v oblasti kybernetickej bezpečnosti, pričom bude uskutočňovať konzultácie aj s príslušnými účastníkmi trhu a národnými koordinačnými centrami. Agentúra ENISA bude vychádzať z metodiky indexu digitálnej ekonomiky a spoločnosti[92] a zabezpečí, aby boli ukazovatele v súlade s európskymi digitálnymi cieľmi týkajúcimi sa odborníkov na IKT a dosiahnutia rovnomernejšieho rodového zastúpenia v oblasti IKT. Komisia bude následne pracovať na začlenení týchto ukazovateľov do indexu digitálnej ekonomiky a spoločnosti, čo umožní každoročné sledovanie stavu kybernetickobezpečnostných zručností a trhu práce.

7.2. Zber údajov a podávanie správ

Agentúra ENISA bude s pomocou projektu ECCO a národných koordinačných centier zbierať údaje o ukazovateľoch. Na základe zozbieraných údajov agentúra ENISA vypracuje **výročnú správu**, ktorá bude príspevkom k správe o stave digitálneho desaťročia[93], ktorá zase bude spolu s indexom digitálnej ekonomiky a spoločnosti podkladom pre analýzu a odporúčania pre jednotlivé krajiny v rámci **európskeho semestra**[94]. Ukazovatele kybernetickobezpečnostných zručností budú okrem toho príspevkom k **dvojročnej správe** agentúry ENISA o stave kybernetickej bezpečnosti v EÚ, ktorá sa predpokladá v smernici NIS2 a ktorá sa bude týkať spôsobilostí, informovanosti a hygieny v oblasti kybernetickej bezpečnosti v celej EÚ.

7.3. Príprava kľúčových ukazovateľov výkonnosti (KPI) pre kybernetickú bezpečnosť

S cieľom riešiť nedostatok odborníkov v oblasti kybernetickej bezpečnosti v Európe agentúra ENISA v úzkej spolupráci s Komisiou a národnými koordinačnými centrami navrhne Komisii kľúčové ukazovatele výkonnosti, pričom bude vychádzať z metodiky politického programu Digitálne desaťročie do roku 2030, ako aj zo skúseností príslušného odvetvia. Agentúra ENISA náležite zohľadní kľúčové ukazovatele výkonnosti, ktoré členské štáty používajú na hodnotenie svojich národných stratégií kybernetickej bezpečnosti[95].

<u>Opatrenia v rámci akadémie</u>

Agentúra ENISA

- Do konca roka 2023 pripraví **ukazovatele a kľúčové ukazovatele výkonnosti** pre kybernetickobezpečnostné zručnosti.
- Bude **zbierať údaje** o ukazovateľoch a podávať o nich správy, pričom prvý zber údajov sa uskutoční do roku 2025.

Komisia

- Bude pracovať na začlenení **ukazovateľov kybernetickej bezpečnosti do indexu**

[91] Pritom sa budú opierať o metodiku, ktorú má pripraviť agentúra ENISA na účely dvojročnej správy agentúry o stave kybernetickej bezpečnosti v Únii podľa článku 18 ods. 3 smernice NIS2, a zároveň túto metodiku dopĺňať.

[92] Pozri metodickú poznámku k indexu digitálnej ekonomiky a spoločnosti (DESI) 2022: Index digitálnej ekonomiky a spoločnosti (DESI) | Formovanie digitálnej budúcnosti Európy (europa.eu).

[93] Rozhodnutie Európskeho parlamentu a Rady (EÚ) 2022/2481 zo 14. decembra 2022, ktorým sa zriaďuje politický program digitálne desaťročie do roku 2030.

[94] Tamže, odôvodnenie 25.

[95] Článok 7 ods. 4 smernice NIS2.

digitálnej ekonomiky a spoločnosti a do **správy o stave digitálneho desaťročia**.

8. Záver

Týmto oznámením sa vytvárajú základy pre revíziu prístupu EÚ k zvyšovaniu kybernetickobezpečnostných zručností odborníkov v EÚ. Cieľom je znížiť nedostatok kybernetickobezpečnostných zručností a vybaviť EÚ potrebnou pracovnou silou, ktorá jej umožní reagovať na neustále sa vyvíjajúcu panorámu hrozieb, vykonávať politiky EÚ zamerané na ochranu EÚ pred kybernetickými útokmi, ale aj posilniť obchodné príležitosti a konkurencieschopnosť. Kvalifikovaná pracovná sila v oblasti kybernetickej bezpečnosti môže byť prínosom pre **komunity občianskej spoločnosti, obrany, diplomacie a presadzovania práva** a uľahčiť ich vzájomné synergie.

Komisia vyzýva členské štáty a všetky zainteresované strany, aby napĺňali ambície Akadémie zručností v oblasti kybernetickej bezpečnosti.