EVROPSKÁ
KOMISE

Ve Štrasburku dne 18.4.2023
COM(2023) 207 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU („Akademie dovedností v oblasti kybernetické bezpečnosti“)

Řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU
(„Akademie dovedností v oblasti kybernetické bezpečnosti“)

1. Naléhavá potřeba snížit rizika řešením nedostatku dovedností a mezer v oblasti kybernetické bezpečnosti

Kybernetická bezpečnost není jen součástí bezpečnosti občanů, podniků a členských států. Je také nutností pro zajištění politické stability EU, stability jejích demokracií a prosperity naší společnosti a podniků. **Situace v oblasti kybernetických hrozeb** v posledních letech zaznamenala intenzivní vývoj a objevil se znepokojivý trend zvyšujícího se počtu kybernetických útoků zaměřených na vojenskou a civilní kritickou infrastrukturu v EU. Aktéři hrozeb zdokonalují své schopnosti a objevují se nové, hybridní a vznikající hrozby, jako je využívání botů a technik založených na umělé inteligenci[1]. Zejména aktéři hrozeb využívající ransomware běžně způsobují subjektům značné škody, a to jak finanční, tak spočívající v poškozování jejich pověsti[2].

Velký počet kybernetických bezpečnostních incidentů cílil také na veřejnou správu a vlády členských států, jakož i na evropské orgány, instituce a jiné subjekty[3]. Soustavným cílem útoků jsou i finanční sektor[4] a zdravotnictví[5], které tvoří páteř společnosti a ekonomiky[6]. Geopolitické napětí spojené s ruskou agresí vůči Ukrajině kybernetickou hrozbu[7] zvýšilo a může destabilizovat naši společnost. **Bezpečnost** EU nelze zaručit bez **nejcennějšího aktiva EU: jejích obyvatel.** EU naléhavě potřebuje odborníky s dovednostmi a kompetencemi, kteří budou předcházet kybernetickým útokům, odhalovat je, odrazovat od nich a budou před nimi bránit EU včetně jejích nejkritičtějších infrastruktur a zajišťovat její **odolnost**.

Nedostatek talentů v oblasti kybernetické bezpečnosti dále brání **konkurenceschopnosti** a **růstu** Evropy, které jsou do značné míry závislé na vývoji a zavádění strategických digitálních technologií (např. umělé inteligence, 5G a cloudu). Aby byla EU nadále schopna v

---

[1] *ENISA Threat Landscape 2022* (Zpráva agentury ENISA o situaci v oblasti hrozeb, 2022), ENISA (europa.eu).

[2] Europol, *Internet Organised Crime Threat Assessment* (Posouzení hrozeb organizované trestné činnosti na internetu) (IOCTA) 2021. Tito aktéři staví na modelu „ransomware-as-a-service“. Roční náklady podniků v roce 2022 přesáhly 18,4 miliardy EUR (Cybereason, *2022 Report on the true cost or Ransomware* (Zpráva o skutečných nákladech spojených s ransomwarem).

[3] Viz například společná publikace agentur ENISA a CERT-EU, JP-23-01 – *Sustained activity by specific threat actors* (Soustavná činnost konkrétních aktérů hrozeb), TLP:CLEAR, 15. února 2023.

[4] Viz například Německo, kde 90 % poštovních podvodů nahlášených od 1. června 2021 do 31. května 2022 představovalo finanční phishing neboli útok na společnost ve finančním sektoru a bylo do nich zapojeno více než 20 000 infikovaných zařízení ze 125 zemí, *The State of IT Security in Germany in 2022* (Stav zabezpečení IT v Německu v roce 2022), *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, 1. ledna 2023.

[5] Viz například Francie, kde ransomwarové útoky na veřejná zdravotnická zařízení, např. na Centre Hospitalier Sud Francilien, při nichž bylo ohroženo a aktérem hrozby zveřejněno 11 GB osobních a zdravotnických dat a údajů souvisejících se zaměstnanci, *Panorama de la cybermenace 2022*, Agence nationale de la sécurité des systèmes d'information (ANSSI), leden 2023.

[6] *ENISA Threat Landscape 2022* (Zpráva agentury ENISA o situaci v oblasti hrozeb, 2022).

[7] Viz také: CERT-EU – *Russia's war on Ukraine: one year of cyber operations* (Válka Ruska proti Ukrajině: rok kybernetických operací) (europa.eu); Ruské kybernetické operace namířené proti Ukrajině: prohlášení vysokého představitele jménem Evropské unie, 10. května 2022; prohlášení vysokého představitele jménem Evropské unie k nepřátelské kybernetické činnosti prováděné hackery a hackerskými skupinami v souvislosti s agresí Ruska vůči Ukrajině, 19. července 2022.

celosvětovém měřítku zajišťovat klíčové pokročilé technologie, potřebuje kvalifikovanou pracovní sílu v oblasti kybernetické bezpečnosti.

S cílem připravit se na tento vývoj hrozeb a čelit mu, jakož i podpořit konkurenceschopnost EU učinila politika EU v oblasti kybernetické bezpečnosti v posledních letech významný pokrok, který vedl k přijetí řady iniciativ, jako jsou strategie kybernetické bezpečnosti EU pro digitální dekádu[8], revidovaná směrnice o bezpečnosti sítí a informací (směrnice NIS 2)[9], odvětvové právní předpisy EU v oblasti kybernetické bezpečnosti[10], politika kybernetické obrany EU[11], akt o kybernetické odolnosti[12] a akt o kybernetické solidaritě, jejichž návrh Komise předkládá spolu s tímto sdělením. Tyto právní předpisy však nedosáhnou svých cílů bez kvalifikovaných pracovníků, kteří je budou uvádět do praxe a uplatňovat. Zatímco základní znalosti obyvatelstva týkající se kybernetické bezpečnosti jsou řešeny v rámci iniciativ podporujících rozvoj obecných dovedností potřebných k zapojení do společnosti[13], **splnění těchto právních a politických požadavků na kybernetickou bezpečnost** vyžaduje kompetentní pracovní síly ve veřejném i soukromém sektoru, na vnitrostátní i unijní úrovni a včetně normalizačních organizací.

Bezpečnost a konkurenceschopnost EU proto závisí na tom, zda bude mít profesionální kvalifikovanou pracovní sílu v oblasti kybernetické bezpečnosti. EU se však potýká s velmi výrazným nedostatkem kvalifikovaných odborníků na kybernetickou bezpečnost, což vystavuje EU, její členské státy, podniky a občany riziku kybernetických bezpečnostních incidentů. V roce 2022 se počet chybějících odborníků na kybernetickou bezpečnost v Evropské unii pohyboval v rozmezí **260 000**[14] **až 500 000**[15] osob, přičemž potřeba pracovních sil v oblasti kybernetické bezpečnosti v EU se odhadovala na 883 000 odborníků[16], což naznačuje nesoulad mezi dostupnými kompetencemi a kompetencemi požadovanými trhem práce. Na pracovní síly v oblasti kybernetické bezpečnosti má vliv i mylná představa přisuzující této činnosti (ryze)? technickou povahu, díky čemuž na tento obor stále nedaří přilákat **ženy**, které tvoří jen 20 % absolventů v oboru kybernetické bezpečnosti[17] a 19 %

[8] Společné sdělení Evropskému parlamentu a Radě, Strategie kybernetické bezpečnosti EU pro digitální dekádu, JOIN(2020) 18 final.

[9] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

[10] Například pro finanční sektor nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (nařízení DORA).

[11] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN(2022) 49 final.

[12] Návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, COM/2022/454 final.

[13] K významným iniciativám zaměřeným na obecné digitální dovednosti obyvatelstva patří: dosažení základních digitálních dovedností u 80 % obyvatelstva do roku 2030, což je cíl Akčního plánu pro evropský pilíř sociálních práv, Digitální kompas, Akční plán digitálního vzdělávání na období 2021–2027, nástroj rámce digitálních kompetencí nebo návrh doporučení Rady o zlepšení poskytování digitálních dovedností ve vzdělávání a odborné přípravě.

[14] (ISC)² v hodnocení kybernetických dovedností na základě rámce ECSF, webinář agentury ENISA, 16. února 2023.

[15] Podle Evropské organizace pro kybernetickou bezpečnost (ECSO), jak je uvedeno ve společném sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN(2022) 49 final.

[16] (ISC)² v hodnocení kybernetických dovedností na základě rámce ECSF, webinář agentury ENISA, 16. února 2023.

[17] Databáze vysokoškolského vzdělávání v oblasti kybernetické bezpečnosti (CyberHEAD).

odborníků v oblasti informačních a komunikačních technologií (dále jen „IKT“)[18]. Ve snaze řešit tento stav stanovil evropský **program Digitální dekáda 2030**[19] cíl zvýšit do roku 2030 počet odborníků v oblasti IKT o 20 milionů a zároveň dosáhnout rovnoměrnějšího genderového zastoupení. Zavádění nové politiky EU navíc vyžaduje dostatek odpovídajícím způsobem kvalifikované pracovní síly. Například více než 42 % vedoucích pracovníků v IT v odvětví finančních služeb upozornilo na nedostatečné dovednosti a odbornost v kybernetické bezpečnosti jako na klíčový problém, kterému jejich obor čelí, pokud jde o obranu a řízení incidentů v oblasti kybernetické bezpečnosti[20], a to v době, kdy budou muset začít uplatňovat odvětvové právní předpisy týkající se kybernetické bezpečnosti, jako je akt o digitální provozní odolnosti (DORA).

K nedostatečné nabídce na trhu práce přispívá i neochota zaměstnavatelů investovat do lidského kapitálu a snaha hledat již vyškolenou a zkušenou pracovní sílu[21]. Tento nedostatek se dotýká všech typů podniků, včetně malých a středních podniků (**MSP**), které představují 99 % všech podniků v EU[22]. Velký problém zaznamenávají i **orgány veřejné správy**, které se obětí kybernetických bezpečnostních incidentů stávají velmi často a se značnými následky[23].

Řešení nedostatku talentovaných odborníků nakybernetickou bezpečnost v EU je proto velmi naléhavé, neboť v sázce je bezpečnost a konkurenceschopnost EU.

2. Chybějící součinnost a koordinovaná opatření k odstranění nedostatku dovedností v oblasti kybernetické bezpečnosti

Existuje nespočet iniciativ na evropské a vnitrostátní úrovni, které provádějí veřejné i soukromé subjekty s cílem řešit nedostatek pracovních sil v oblasti kybernetické bezpečnosti. Jsou však rozptýlené a zatím se jim nepodařilo dosáhnout kritického rozsahu, který by mohl znamenat skutečnou změnu.

Především v současné době existuje jen omezená obecná shoda na skladbě pracovních sil v kybernetické bezpečnosti v EU a souvisejících dovednostech, přičemž podobné pracovní profily v kybernetické bezpečnosti by měly zahrnovat tentýž soubor dovedností. Nízká míra přijetí společného **evropského referenčního rámce pro odborníky v oblasti kybernetické bezpečnosti** příslušnými aktéry vede k tomu, že chybí nástroj komunikace mezi zaměstnavateli, poskytovateli vzdělávání a tvůrci politik a nedostatky na trhu práce v oblasti kybernetické bezpečnosti nelze měřit a posuzovat. Brání to i tvorbě programů vzdělávání a odborné přípravy a vytváření možností profesní dráhy pro osoby se zájmem o tuto profesi, které by odpovídaly potřebám politiky a trhu. **Prohlubování dovedností a změna kvalifikace** pracovních sil se ve velké míře opírají o školení a certifikáty v oblasti kybernetické bezpečnosti, které obvykle nabízejí soukromí poskytovatelé. Pracovní síly však jen obtížně získávají přehled o kvalitě nabízených školení v oblasti kybernetické bezpečnosti a o vydávaných certifikátech.

---

[18] Pouze 19 % odborníků v oboru IKT v EU tvoří ženy Index digitální ekonomiky a společnosti (DESI) 2022 |,Utváření digitální budoucnosti Evropy (europa.eu). Není k dispozici žádný číselný údaj týkající se počtu žen v oboru kybernetické bezpečnosti v Unii.

[19] Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030, který zřizuje mechanismus monitorování a spolupráce pro dosažení společných cílů a úkolů v oblasti digitální transformace Evropy stanovených v Digitálním kompasu 2030, včetně dovedností.

[20] S-RM, *Cyber Security Insights Report 2022* (Zpráva o kybernetické bezpečnosti 2022).

[21] *Cybersecurity Skills Development in the EU* (Rozvoj kybernetických dovedností v EU), ENISA, prosinec 2019.

[22] Definice malých a středních podniků (europa.eu).

[23] *ENISA Threat Landscape 2022* (Zpráva agentury ENISA o situaci v oblasti hrozeb, 2022), ENISA (europa.eu).

Vzdělávání a odborná příprava a budování možností profesní dráhy jsou nezbytné k posílení nabídkové strany trhu práce, úloha **poptávkové strany** v odborné přípravě pracovních sil a přizpůsobování se jejímu vývoji je však v současné době podceňována. Zaměstnavatelé z průmyslu a veřejného sektoru postrádají společná fóra a místa, kde by mohli sdílet náměty na nejlepší odbornou přípravu pracovních sil a řešit, jak **lépe hodnotit dovednosti**, zejména během náboru. Nejžádanějšími **„tvrdými" dovednostmi** jsou sice dovednosti související s kybernetickou bezpečností[24], jako je vývoj softwaru nebo cloud computing[25], stále jsou však neoprávněně opomíjeny **průřezové dovednosti**. Kritické myšlení a analýza, řešení problémů a samostatné fungování jsou skupiny dovedností, které zaměstnavatelé požadují více[26] a jejichž význam s blížícím se rokem 2025 narůstá[27].

V oblasti kybernetické bezpečnosti již existuje mnoho veřejných i soukromých investičních iniciativ, přičemž EU rozsáhle **financuje** projekty v rámci různých nástrojů[28]. Přetrvávající nedostatek dovedností v EU však vyvolává otázky ohledně jejich viditelnosti a dopadu a naznačuje, že tyto projekty možná systematicky nereagují na potřeby trhu, které je třeba na úrovni EU urychleně zmapovat. Kromě toho více zdrojů financování vede k duplicitám a ztrácí se příležitost k rozšíření a dosažení skutečného dopadu. Navíc ti, kteří investice potřebují, nejsou vždy schopni určit nejvhodnější zdroje k pokrytí svých potřeb.

Zúčastněné strany se snaží řešit složitý a mnohostranný problém nedostatku dovedností v oblasti kybernetické bezpečnosti. Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA") vyvíjí nástroje týkající se profilů rolí nebo vysokoškolského vzdělávání[29], Evropské centrum kompetencí pro kybernetickou bezpečnost (dále jen „ECCC")[30] se zabývá dovednostmi v oblasti kybernetické bezpečnosti ve specializované pracovní skupině, Evropská bezpečnostní a obranná škola (dále jen „EBOŠ") se zabývá dovednostmi v oblasti kybernetické bezpečnosti u civilních a vojenských pracovníků v kontextu společné bezpečnostní a obranné politiky[31], tuto problematiku se snaží řešit i soukromé organizace[32] a odvětví certifikace v oboru kybernetické bezpečnosti připravuje plán a školení zaměřená na chybějící dovednosti[33]. Členské státy se rovněž snaží uvedený problém řešit prostřednictvím různých iniciativ, od iniciativ regulačních[34] až po zřizování akademií kybernetických dovedností[35] nebo kybernetických kampusů[36] a center excelence

[24] *LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most* (Nejžádanější dovednosti: získejte dovednosti, které firmy potřebují nejvíce).

[25] Infografika ISACA Stav kybernetické bezpečnosti 2022.

[26] Například nástroj CEDEFOP: Skills-OVATE| CEDEFOP (europa.eu).

[27] *The Future of Jobs Report* (Zpráva o budoucnosti pracovních míst), říjen 2020, Světové ekonomické fórum.

[28] Například: Aliance pro kybernetickou bezpečnost – Nová vize pro Evropu – projekt REWIRE (financovaný z programu Erasmus+); projekty na podporu kompetenčního centra kybernetické bezpečnosti (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (financovaný z programu Horizont 2020), projekt Cybersecpro (financovaný z programu Digitální Evropa).

[29] Zejména: evropský rámec dovedností v oblasti kybernetické bezpečnosti (ECSF); databáze vysokoškolského vzdělávání v oblasti kybernetické bezpečnosti CYBERHEAD – *Cybersecurity Higher Education Database*; *Cyber Exercise Platform* (platforma pro kybernetická cvičení, CEP); *European Cyber Security Challenge* (evropská výzva v oblasti kybernetické bezpečnosti); evropský měsíc kybernetické bezpečnosti.

[30] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

[31] Zejména *Cyber education, training, exercise and evaluation platform* (platforma pro vzdělávání, odbornou přípravu, hodnocení a cvičení v oblasti kybernetické bezpečnosti, ETEE).

[32] Například pracovní skupina 5 Evropské organizace pro kybernetickou bezpečnost (ECSO) „Vzdělávání, odborná příprava, povědomí, kybernetický rozsah, lidské faktory"; organizace DIGITALEUROPE.

[33] Například SANS Institute, (ISC)², ISACA.

[34] Například v národních strategiích pro vzdělávání nebo kybernetickou bezpečnost.

[35] Například C-Academy v Portugalsku.

pro boj proti kyberkriminalitě[37], nebo prostřednictvím partnerství veřejného a soukromého sektoru[38]. Práce všech těchto zúčastněných stran však často postrádá koordinaci a součinnost a nedosahuje svého potenciálu z hlediska podstatné změny situace na trhu práce, jak ukazuje rostoucí nedostatek pracovníků v oblasti kybernetické bezpečnosti v EU. Je také zapotřebí zvýšit součinnost mezi kybernetickými komunitami, protože soubory dovedností potřebné k zajišťování kybernetické bezpečnosti, boj proti **kyberkriminalitě** nebo budování **kybernetické obrany** jsou často podobné povahy.

V neposlední řadě má dnes EU omezené možnosti, jak posoudit **stav a vývoj trhu práce v oblasti kybernetické bezpečnosti** a dovedností příslušných pracovních sil. Členské státy a orgány, instituce a jiné subjekty využívají buď údaje shromážděné soukromými subjekty, nebo širší soubor údajů shromážděných v EU, zejména Eurostatem[39] a Evropským střediskem pro rozvoj odborného vzdělávání (CEDEFOP)[40] o odbornících na IKT. Jinými slovy, EU má o svých potřebách jen částečný a roztříštěný přehled, což jí brání konsolidovat souhrnnou představu o stavu trhu práce v oblasti kybernetické bezpečnosti.

3. Koordinovaná reakce v rámci celé EU: Akademie dovedností v oblasti kybernetické bezpečnosti

3.1 Cíl

K překonání problému, který řešení dovedností v oblasti kybernetické bezpečnosti a odstranění nedostatků na trhu práce představuje, předkládá Komise návrh na zřízení **Akademie dovedností v oblasti kybernetické bezpečnosti**, který oznámila předsedkyně Evropské komise ve svém prohlášení o záměru v rámci projevu o stavu Unie v roce 2022[41, , 42] a v souvislosti s Evropským rokem dovedností.

Cílem Akademie dovedností v oblasti kybernetické bezpečnosti (zkráceně „akademie“) je vytvořit **jednotné místo kontaktu a součinnosti** pro nabídky vzdělávání a odborné přípravy v oblasti kybernetické bezpečnosti, jakož i pro možnosti financování a konkrétní opatření na podporu rozvoje dovedností v oblasti kybernetické bezpečnosti. Posílí iniciativy zúčastněných stran, aby dosáhly kritického množství, které zajistí změnu na trhu práce, včetně oblasti obrany. Tyto činnosti budou sladěny na základě společných cílů a klíčových ukazatelů výkonnosti, aby se dosáhlo většího dopadu.

Akademie se zaměří na kvalifikaci **odborníků na kybernetickou bezpečnost**. Činnost akademie se promítne do politik EU v oblasti kybernetické bezpečnosti, ale také do vzdělávání a celoživotního učení. Akademie doplňuje dvě doporučení Rady týkající se digitálního vzdělávání a dovedností, jejichž návrh Komise předložila současně s tímto sdělením[43].

---

[36] Například Cyber Campus ve Francii.

[37] Například Litevské centrum excelence v odborné přípravě, výzkumu a vzdělávání v oblasti kyberkriminality v Litvě (L3CE).

[38] Například iniciativa společnosti Microsoft zaměřená na zvyšování kvalifikace v oblasti kybernetické bezpečnosti.

[39] Zaměstnanost odborníků na IKT – vysvětlení statistik (europa.eu).

[40] Například nástroj CEDEFOP: Skills-OVATE| CEDEFOP (europa.eu).

[41] Projev o stavu Unie 2022, prohlášení o záměru předsedkyni Robertě Metsolové a premiérovi Petru Fialovi.

[42] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN(2022) 49 final.

[43] Návrhy doporučení Rady o klíčových faktorech umožňujících úspěšné digitální vzdělávání a odbornou přípravu a o zlepšení poskytování digitálních dovedností ve vzdělávání a odborné přípravě.

Akademie se bude opírat o čtyři pilíře: 1) podpora **získávání znalostí prostřednictvím vzdělávání a odborné přípravy**, a to prací na společném rámci pro profily rolí v oblasti kybernetické bezpečnosti a související dovednosti, zlepšováním nabídky evropského vzdělávání a odborné přípravy odpovídající potřebám, budováním možností profesních drah a zajišťováním přehlednosti a jasnosti odborné přípravy a certifikací v oblasti kybernetické bezpečnosti s cílem posílit nabídku pracovních sil; 2) zajišťování lepšího směrování a viditelnosti dostupných **možností financování** pro činnosti související s dovednostmi s cílem maximalizovat jejich dopad; 3) vyzývání zúčastněných stran k **přijetí opatření** a 4) definování ukazatelů, které umožní **sledovat vývoj trhu** a posoudit účinnost opatření.

Realizace akademie bude podpořena finančními prostředky ve výši 10 milionů EUR z programu Digitální Evropa[44].

3.2 Správa a řízení akademie

V konečném důsledku by akademie mohla mít podobu **konsorcia evropské digitální infrastruktury** (dále jen **„konsorcium EDIC“**)[45], aby nabídla infrastrukturu, která bude sloužit jako **jednotné kontaktní místo** na podporu spolupráce mezi akademickou obcí, poskytovateli odborné přípravy a průmyslem, kde by se strany nabídky a poptávky v rámci ekosystému kybernetické bezpečnosti EU mohly setkávat a vzdělávat. Tento nástroj by členským státům umožnil společně pracovat na odstranění nedostatku kybernetických dovedností a úzce spolupracovat s Komisí, agenturou ENISA a Evropským centrem kompetencí pro kybernetickou bezpečnost (ECCC) v souladu s jejich mandáty a pravomocemi a zapojit všechny příslušné zúčastněné strany, ale také směrovat evropské, vnitrostátní a soukromé investice ve prospěch společného cíle. Za tímto účelem se zúčastněné členské státy vyzývají, aby do 30. května 2023 předložily Komisi předběžné oznámení o své budoucí žádosti o účast v takovém konsorciu EDIC. Toto dobrovolné předběžné oznámení Komisi umožní vznést k návrhu žádosti o zřízení konsorcia EDIC včas připomínky, a tím urychlit další vývoj a formální předložení. V průběhu celého procesu a v rozsahu požadovaném členskými státy bude Komise jako akcelerátor projektů pro více zemí usnadňovat přípravu žádosti o zřízení konsorcia EDIC. Poté, co Komise žádost kladně posoudí a výbor pro program digitální dekády ji schválí, vydá Komise rozhodnutí o zřízení konsorcia EDIC a následně pomůže koordinovat jeho provádění[46].

Do té doby a než bude konsorcium EDIC formálně zřízeno, vytvoří Komise virtuální jednotné kontaktní místo tak, že posílí svou **Platformu pro digitální dovednosti a pracovní místa**[47] za pomoci projektu Podpora evropské komunity pro kybernetickou bezpečnost (dále jen „ECCO“)[48].

---

[44] Nařízení Evropského parlamentu a Rady (EU) 2021/694 ze dne 29. dubna 2021, kterým se zavádí program Digitální Evropa a zrušuje rozhodnutí (EU) 2015/2240.

[45] Konsorcia EDIC byla stanovena v článku 13 a násl. rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí Digitální dekáda 2030.

[46] Tamtéž, článek 12.

[47] Hlavní stránka |Platforma pro digitální dovednosti a pracovní místa (europa.eu)

[48] Viz Evropské centrum a síť kompetencí v oblasti kybernetické bezpečnosti: nový projekt na podporu kybernetického společenství financovaný z EU (europa.eu). V prosinci 2022 podepsala Evropská komise smlouvu v hodnotě 3 miliony EUR na podporu kybernetického společenství EU v rámci Evropského centra kompetencí v oblasti kybernetické bezpečnosti. Tento projekt přispěje k cílům EU v oblasti budování společenství a kapacit pro výzkum, inovace, zavádění a průmyslovou základnu v oblasti kybernetické bezpečnosti.

Agentura ENISA bude přispívat k provádění akademie v souladu s cíli agentury[49], zejména pokud jde o pomoc při vzdělávání a odborné přípravě v oblasti kybernetické bezpečnosti, a to s ohledem na své oznamovací povinnosti podle směrnice NIS 2[50]. **Centrum ECCC** bude v souladu se svou strategickou agendou podporovat realizaci Akademie dovedností v oblasti kybernetické bezpečnosti. Centrum ECCC bude zejména provádět strategický cíl 3 (kybernetická bezpečnost) programu Digitální Evropa. Bude využívat podpory Komise a členských států prostřednictvím **národních koordinačních center**. V případě potřeby bude požádána **skupina pro spolupráci** zřízená podle směrnice NIS 2[51]. K dosažení cíle akademie, kterým je odstranění nedostatků v oblasti kybernetických dovedností, bude nezbytné spojit síly s **průmyslem** a **akademickou obcí**.

4. Získávání znalostí a odborná příprava: vytvořit společný přístup EU k odborné přípravě v oblasti kybernetické bezpečnosti

V rámci pilíře Akademie dovedností v oblasti kybernetické bezpečnosti zaměřeného na získávání znalostí a odbornou přípravu bude vypracován strukturovaný přístup s jasným cílem zvýšit **počet** osob s dovednostmi v oblasti kybernetické bezpečnosti v EU, lépe cílit odbornou přípravu na **potřeby trhu** a zajistit přehled o **možnostech profesní dráhy**.

4.1 Hovořit stejným jazykem: společný přístup k profilům rolí v oblasti kybernetické bezpečnosti a souvisejícím dovednostem

Agentura ENISA již pracovala na definování profilů rolí odborníků v oblasti kybernetické bezpečnosti v rámci evropského rámce kybernetických kompetencí (dále jen **„ECSF“**)[52]. Ten by se měl stát základem, na němž bude akademie definovat a posuzovat příslušné dovednosti, sledovat vývoj nedostatků v dovednostech a poskytovat údaje o nových potřebách. [53] Pro každou roli v oblasti kybernetické bezpečnosti v rámci ECSF je jako prvek popisu profilu začleněn soubor příslušného evropského rámce e-kompetencí[54].

Agentura ENISA proto provede přezkum rámce ECSF a **určí vyvíjející se potřeby a nedostatky týkající se dovedností** pracovníků v kybernetické bezpečnosti, a to i pomocí pokročilých nástrojů (např. umělé inteligence, dat velkého objemu[55], vytěžování dat). Za tímto účelem bude agentura ENISA pod vedením konsorcia EDIC, až bude zřízeno, a centra ECCC pracovat s národními koordinačními centry, Komisí, projektem ECCO a účastníky trhu[56]. Pokud jde o pracovníky v oblasti kybernetické obrany, agentura ENISA náležitě

---

[49] „Agentura ENISA podporuje budování a připravenost kapacit v celé Unii tím, že pomáhá orgánům, institucím a jiným subjektům Unie, jakož i členským státům a zúčastněným stranám z veřejného a soukromého sektoru (…) rozvíjet schopnosti a odbornost v oblasti kybernetické bezpečnosti.“ Ustanovení čl. 4 odst. 3 aktu o kybernetické bezpečnosti.

[50] Článek 18 směrnice NIS 2.

[51] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

[52] Evropský rámec dovedností v oblasti kybernetické bezpečnosti (ECSF) – ENISA (europa.eu). Rámec ECSF podporuje identifikaci a formulaci úkolů, kompetencí, dovedností a znalostí souvisejících s rolemi evropských odborníků v oblasti kybernetické bezpečnosti. Shrnuje všechny role související s kybernetickou bezpečností do profilů, které jsou jednotlivě analyzovány do podrobností o jejich odpovídajících odpovědnostech, dovednostech, synergiích a vzájemných závislostech.

[53] V tomto ohledu viz *User Manual – European Cybersecurity Skills Framework (ECSF)* (Uživatelská příručka – Evropský rámec dovedností v oblasti kybernetické bezpečnosti (ECSF)), září 2022.

[54] Evropský rámec e-kompetencí (e-CF) |Esco (europa.eu). Rámec e-CF stanoví konzistentní vazby v kontextu kvalifikací v oblasti IKT a dalších rámců relevantních pro toto odvětví, mezi něž patří i rámec digitálních kompetencí, DigComp.

[55] Viz například nástroj Skills-OVATE vyvinutý střediskem Cedefop.

[56] Agentura bude dále využívat výsledky jiných projektů financovaných z EU (např. REWIRE, Data Space For Skills (DS4S), CyberSecPro, Concordia) a metodiku vycházející z podobných iniciativ (např. „*Building a Skilled Cyber*

zohlední práci EBOŠ. Podobně v oblasti boje proti kyberkriminalitě agentura ENISA zohlední činnosti Agentury Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (dále jen „CEPOL“) a Europolu při přípravě analýzy potřeb operativní odborné přípravy[57] v oblasti kybernetických útoků.

Evropský rámec dovedností v oblasti kybernetické bezpečnosti bude na základě činnosti akademie ve dvouletém cyklu pravidelně doplňován a revidován. Kromě toho Komise a Evropská služba pro vnější činnost podle potřeby přispějí k vymezení konkrétních profilů a souvisejících dovedností pro jednotlivá odvětví, a to za podpory subjektů a institucí EU, jako je Evropská bezpečnostní a obranná škola[58], Europol a Agentura Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva[59].

Bude rovněž vytvořena vazba mezi rámcem ECSF a příslušnými nástroji politiky zaměstnanosti EU[60]. Zejména budou pracovní profily podle rámce ECSF a související dovednosti začleněny do **evropské klasifikace dovedností, kompetencí, kvalifikací a povolání**. Tím se zlepší klasifikace a vazby mezi povoláními a dovednostmi v oblasti kybernetické bezpečnosti, což jednotlivcům usnadní prohlubování dovedností a změny kvalifikace a podpoří se obsazování pracovních míst podle dovedností a přeshraniční mobilita.

4.2 Podpora spolupráce při tvorbě plánů vzdělávání a odborné přípravy v oblasti kybernetické bezpečnosti

Po zřízení konsorcia EDIC by akademie měla získat podporu členských států, aby se stala **referenčním místem v Evropě pro koncipování a realizaci školení v oblasti kybernetické bezpečnosti** zaměřených na nejžádanější dovednosti a zajišťovala profesní přípravu na pracovišti a stáže pro začínající podniky a malé a střední podniky a pro orgány veřejné správy v inovativních společnostech a centrech kompetencí v oblasti kybernetické bezpečnosti. Konsorcium EDIC by mělo při koncipování takových školení spolupracovat se všemi příslušnými zúčastněnými stranami, včetně průmyslu, a vycházet z projektů, jako je **CyberSecPro**[61], financovaný z programu Digitální Evropa, který sdružuje sedmnáct vysokoškolských institucí a třináct bezpečnostních společností ze šestnácti členských států, aby přinesl dobrou praxi pro všechny programy školení v oblasti kybernetické bezpečnosti.

Akademie bude spolupracovat se všemi příslušnými zúčastněnými stranami, aby k profesní dráze v oblasti kybernetické bezpečnosti **přilákala generaci mladých lidí**. V souladu s

---

Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States“ (Budování kvalifikovaných pracovních sil v oblasti kybernetické bezpečnosti v pěti zemích: poznatky z Austrálie, Kanady, Nového Zélandu, Spojeného království a Spojených států), zprávy OECD vydané 21. března 2023), aby v budoucnu zajistila aktuální představu o potřebách v prostředí vyznačujícím se neustálým vývojem poptávky.

[57] *CEPOL Operational Training Needs Assessment* (analýza potřeb operativní odborné přípravy, OTNA).

[58] V této souvislosti viz společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN(2022) 49 final.

[59] V tomto ohledu bude věnována pozornost práci na rámci kompetencí odborné přípravy v oblasti kyberkriminality, který je v současné době připravován.

[60] Například evropská klasifikace dovedností, kompetencí, kvalifikací a povolání (ESCO), Europass, evropská síť služeb zaměstnanosti (EURES).

[61] CyberSecPro. Projekt například provede analýzu programů, kurzů a letních škol v oblasti kybernetické bezpečnosti nabízených na univerzitách a používaných tabulek klasifikace podle evropského systému přenosu a akumulace kreditů (ECTS), zajistí zapojení cílového počtu více než 530 účastníků odborné přípravy během tříletého období a vyškolí externisty z různých odvětví a sektorů.

návrhem doporučení Rady o zlepšení poskytování digitálních dovedností ve vzdělávání a odborné přípravě by členské státy měly zavést a posílit opatření k náboru a odborné přípravě specializovaných učitelů a školitelů a usnadnit získávání dovedností v oblasti kybernetické bezpečnosti, a to i prostřednictvím učňovských stáží. Je třeba podporovat začlenění kybernetické bezpečnosti do programů vzdělávání a odborné přípravy a zároveň zajistit jejich dostupnost, rozvíjet nabídku **učňovské přípravy** a stáží, podporovat inovativní přístupy včetně například vážných her (tzv. „serious games“) a sdílených simulačních platforem, pořádat týdny intenzivní přípravy v oblasti kybernetické bezpečnosti a vysvětlovat profily netechnických rolí. Účast na těchto vzdělávacích příležitostech v oblasti kybernetické bezpečnosti by měla být podporována i u obtížně oslovitelných skupin, jako jsou mladí lidé se zdravotním postižením, mladí lidé žijící v odlehlých nebo venkovských oblastech a mladí lidé z jiných menšinových skupin.

Komise bude i nadále podporovat rozvoj mikrocertifikátů a programů odborného vzdělávání a přípravy. V rámci programu Erasmus+ budou nadále financovány zejména **společné bakalářské a magisterské studijní programy, společné kurzy nebo moduly, které mohou vést k získání mikrocertifikátů**, a **kombinované intenzivní programy**[62] na všechna témata včetně **kybernetické bezpečnosti**. Podporováno bude také další zavádění **iniciativy „Evropské univerzity“**[63] a **center excelence odborného vzdělávání**[64] s cílem povzbudit větší spolupráci mezi vysokoškolskými institucemi a příslušnými institucemi odborného vzdělávání a přípravy v celé Evropě. Tento cíl spočívající v prohloubení spolupráce bude podpořen programy financování z EU, včetně programu Erasmus+ a programu Digitální Evropa, a také fondy EU pro rozvoj **individuálních vzdělávacích účtů**[65].

S cílem usnadnit spolupráci na vnitrostátní úrovni mezi akademickou obcí a poskytovateli odborné přípravy v oblasti kybernetické bezpečnosti a zaměstnavateli ze soukromého a veřejného sektoru a podpořit součinnost mezi veřejným a soukromým sektorem se národní koordinační centra vyzývají, aby prozkoumala možnost zřízení **kybernetických kampusů v** členských státech. Cílem kybernetických kampusů by bylo vytvořit póly excelence na vnitrostátní úrovni pro komunitu kybernetické bezpečnosti, přičemž akademie by napomohla jejich propojení a další koordinaci jejich činností.

Svou nabídku odborné přípravy v oblasti kybernetické bezpečnosti rozšíří rovněž agentura ENISA, přičemž sladí **svůj katalog kurzů**[66] s profily podle rámce ECSF a vypracuje moduly školení pro jednotlivé profily, které mohou rozšířit nabídku členských států v oblasti odborné přípravy. Agentura ENISA rovněž rozšíří svůj **program „školení školitelů“**[67] zaměřený na odborné potřeby orgánů, institucí a jiných subjektů EU a subjektů veřejného sektoru v členských státech a **veřejných a soukromých kritických provozovatelů** v oblasti působnosti směrnice NIS 2.

Kromě toho svou nabídku školení v oblasti kybernetické bezpečnosti posílí i další subjekty a instituce EU. Například v rámci provádění politiky EU v oblasti kybernetické obrany vypracuje **EBOŠ** nový soubor kurzů kybernetické bezpečnosti a sladí některé ze svých

[62] Kombinované intenzivní programy kombinují on-line výuku s krátkým obdobím fyzické mobility.

[63] Iniciativa „Evropské univerzity“ |Evropský vzdělávací prostor (europa.eu).

[64] Centra excelence odborného vzdělávání | Erasmus+ (europa.eu).

[65] V souladu s doporučením Rady ze dne 16. června 2022 o individuálních vzdělávacích účtech.

[66] Vzdělávací kurzy – ENISA (europa.eu)

[67] Program školení školitelů – ENISA (europa.eu)

stávajících kurzů s rámcem ECSF. Tyto kurzy povedou k certifikaci výsledků učení[68]. EBOŠ ve spolupráci s Komisí prozkoumá možnost začlenění certifikátů do peněženky digitální identity EUeID. EBOŠ dále prozkoumá možné mechanismy hodnocení dovedností, na jejichž základě budou certifikáty vydávány. Podobně se v oblasti boje proti kyberkriminalitě bude usilovat o úzké propojení s **akademií CEPOL pro boj proti kyberkriminalitě**[69], aby se podpořila součinnost a doplňkovost při koncipování a zavádění programů odborné přípravy.

4.3 Vytváření součinnosti a zviditelnění školení a certifikace v oblasti kybernetické bezpečnosti ve všech členských státech

Akademie by se měla zabývat otázkou viditelnosti a součinnosti odborné přípravy a certifikace. Z toho by těžily civilní, obranné, donucovací a diplomatické kybernetické komunity, neboť všechny sektory vyžadují v mnoha případech stejné odborné znalosti založené na podobných učebních plánech a výsledcích vzdělávání.

Akademie by pro zájemce o profesní dráhu v oblasti kybernetické bezpečnosti sloužila jako **jednotné kontaktní místo**. V krátkodobém horizontu to bude zajištěno posílením **platformy** Komise **pro digitální dovednosti a pracovní místa** s podporou projektu ECCO. Zvláštní oddíl věnovaný profesní dráze v kybernetické bezpečnosti bude propojen se stávajícími nástroji, od vysokoškolských vzdělávacích programů přes možnosti odborné přípravy, včetně kurzů vedoucích k získání mikrocertifikátů a programů odborného vzdělávání a přípravy, až po nabídky zaměstnání. Za tím účelem budou na platformě uváděny nebo do ní integrovány aktuální činnosti a iniciativy , například iniciativa agentury ENISA, která ve spolupráci s akademickou obcí vytvořila **mapu vzdělávacích institucí** poskytujících programy v oblasti kybernetické bezpečnosti,. Tuto činnost dále posílí podpora ze strany národních koordinačních center. Kromě toho agentura ENISA s podporou národních koordinačních center, Komise a projektu ECCO a ve spolupráci se subjekty, které udělují certifikace, zřídí dvě **úložiště existující nabídky školení z veřejného a soukromého sektoru a certifikace v oblasti kybernetické bezpečnosti** a bude je konsolidovat, přičemž čerpat bude i z dalších důležitých iniciativ[70]. Úložiště budou rovněž začleněna do jednotného kontaktního místa Platformy pro digitální dovednosti a pracovní místa. Z této práce budou těžit i národní koordinační centra, jejichž úkolem je zejména propagovat a šířit vzdělávací programy v oblasti kybernetické bezpečnosti[71].

Je také nutné poskytnout odborníkům záruky, že školení, která absolvují, budou mít požadovanou kvalitu. V tomto ohledu agentura ENISA vypracuje **pilotní projekt**, který prozkoumá možnosti zřízení Evropského systému osvědčování dovedností v oblasti kybernetické bezpečnosti.

Kromě toho je nezbytné určit dovednosti a odbornou přípravu a přiřadit je k pracovnímu profilu, ale je také důležité zajistit, aby služby kybernetické bezpečnosti byly poskytovány s potřebnými kompetencemi, odbornými znalostmi a zkušenostmi. To platí zejména pro

[68] V souladu s čl. 20 odst. 4 rozhodnutí Rady (SZBP) 2020/1515 ze dne 19. října 2020, kterým se zřizuje Evropská bezpečnostní a obranná škola (EBOŠ) a zrušuje rozhodnutí (SZBP) 2016/2382.

[69] Akademie CEPOL pro boj proti kyberkriminalitě byla založena v roce 2019 s cílem poskytnout nejmodernější platformu pro zlepšení znalostí o kyberkriminalitě a kybernetických kapacit v Evropě.

[70] Například W4C Academy – Women4Cyber nebo projekt Global Cybercrime Certification pro donucovací a justiční orgány.

[71] „1. Národní koordinační centra mají tyto úkoly: (…) g) aniž jsou dotčeny pravomoci členských států v oblasti vzdělávání, a s přihlédnutím k příslušným úkolům ENISA, spolupracovat s vnitrostátními orgány ohledně možných příspěvků k podpoře a šíření vzdělávacích programů v oblasti kybernetické bezpečnosti“, čl. 7 odst. 1 písm. g) nařízení, kterým se zřizuje centrum ECCC. Viz také související 28. bod odůvodnění.

poskytovatele řízených bezpečnostních služeb v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Směrnice NIS 2 a návrh aktu o kybernetické solidaritě stanoví pro tyto poskytovatele řízených bezpečnostních služeb konkrétní úkoly. Komise proto také navrhuje **cílenou změnu aktu o kybernetické bezpečnosti**[72], která by umožnila zavedení systémů certifikace řízených bezpečnostních služeb na úrovni EU. Cílem těchto certifikačních systémů by mělo být mimo jiné zajistit, aby tyto služby poskytovali pracovníci s velmi vysokou úrovní technických znalostí a kompetencí v příslušných oblastech.

Mechanismy zajištění kvality a uznávání mikrocertifikátů[73] usnadňují transparentnost, srovnatelnost a přenositelnost výsledků vzdělávání. V souladu s doporučením Rady o evropském přístupu k mikrocertifikátům[74] se členské státy vyzývají, aby do svých vnitrostátních rámců kvalifikací zahrnuly mikrocertifikáty v oblasti kybernetické bezpečnosti. To by jim umožnilo propojit mikrocertifikáty v oblasti kybernetické bezpečnosti s evropským rámcem kvalifikací[75]. Infrastruktura evropských digitálních certifikátů o vzdělání je k dispozici pro vydávání digitálně podepsaných kvalifikací a mikrocertifikátů v oblasti kybernetické bezpečnosti pro jednotlivce. Ty obsahují velké množství dat včetně údajů o výsledcích vzdělávání v oblasti kybernetické bezpečnosti a mohou být uloženy v budoucí **digitální peněžence EUeID**[76].

Akce v rámci akademie

Členské státy a průmysl

- Zajistit podporu rozvoje a uznávání **mikrocertifikátů** o studiu v oblasti kybernetické bezpečnosti v souladu s doporučením Rady o evropském přístupu k mikrocertifikátům.
- Zahrnout kvalifikace v oblasti kybernetické bezpečnosti včetně mikrocertifikátů do **vnitrostátních rámců kvalifikací**.
- Poskytnout lidem, kteří se účastní iniciativ pro rozvoj dovedností v oblasti kybernetické bezpečnosti, **příležitosti k učení na pracovišti** formou stáží.

Komise

- V krátkodobém horizontu vytvořit **jednotné kontaktní místo** pro programy v oblasti kybernetické bezpečnosti, stávající školení a certifikace v oblasti kybernetické bezpečnosti prostřednictvím **Platformy pro digitální dovednosti a pracovní místa**, a to konce roku 2023.
- Dne 18. dubna 2023 předložit návrh změny **aktu o kybernetické bezpečnosti**, která by umožnila certifikaci poskytovatelů řízených bezpečnostních služeb.

Instituce a subjekty EU

[72] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

[73] Například záznamy nebo osvědčení o výsledcích učení, které lidé získali v krátkých školeních.

[74] Doporučení Rady o evropském přístupu k mikrocertifikátům pro celoživotní učení a zaměstnatelnost.

[75] Doporučení Rady ze dne 22. května 2017 o evropském rámci kvalifikací pro celoživotní učení, kterým se zrušuje doporučení Evropského parlamentu a Rady ze dne 23. dubna 2008 o zavedení evropského rámce kvalifikací pro celoživotní učení.

[76] Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu.

- Do konce roku 2023 zavést **rámec ECSF** jako společný přístup k profilům rolí v oblasti kybernetické bezpečnosti a souvisejícím dovednostem.
- Agentura ENISA zahájí ve 2. čtvrtletí roku 2023 vývoj pilotního projektu, kterým se zřídí **evropský systém osvědčování** dovedností v oblasti kybernetické bezpečnosti.
- Agentura ENISA přezkoumá svůj **katalog kurzů** a do konce roku 2023 otevře **program „školení školitelů“** pro veřejné i soukromé kritické provozovatele.
- Do poloviny roku 2023 dokončit **sladění učebních plánů EBOŠ s rámcem ECSF**.

5. Zapojení zúčastněných stran: usilovat o odstranění nedostatku dovedností v oblasti kybernetické bezpečnosti

V rámci akademie bude vypracován koordinovaný přístup k zapojení zúčastněných stran do řešení nedostatku dovedností v oblasti kybernetické bezpečnosti. Cílem bude maximalizovat viditelnost a dopad závazků různých zúčastněných stran zaměřených na snížení nedostatku dovedností v oblasti kybernetické bezpečnosti.

Komise vyzývá zúčastněné strany, aby přijaly konkrétní závazky a zavázaly se k prohlubování dovedností a změnám kvalifikace pracovníků prostřednictvím specializovaných opatření, která budou v co největší míře vycházet ze zjištěných nedostatků dovedností v oblasti kybernetické bezpečnosti. Tyto **závazky zúčastněných stran v oblasti kybernetické bezpečnosti** by měly být oznámeny **Platformě pro digitální dovednosti a pracovní místa**, podobně jako ostatní digitální závazky, které jsou již na platformě viditelné. Komise dále vyzývá zúčastněné strany, které na platformě zveřejní závazek v oblasti kybernetické bezpečnosti, aby se připojily k **digitálnímu partnerství velkého rozsahu v rámci Paktu pro dovednosti**[77]**.** Závazky v oblasti kybernetické bezpečnosti přijaté v rámci digitálního partnerství velkého rozsahu by měly být uvedeny na Platformě pro digitální dovednosti a pracovní místa. Stejně tak se doporučuje, aby závazky přijaté na Platformě pro digitální dovednosti a pracovní místa byly oznámeny v digitálním partnerství velkého rozsahu v rámci Paktu pro dovednosti.

Komise dále vyzývá členské státy, aby **pokračovaly v úsilí o naplňování deklarace o ženách v digitálním světě**[78] s cílem podpořit ženy, aby hrály aktivní a významnou roli v odvětví digitálních technologií, a dosáhnout rovnoměrnějšího genderového zastoupení na pracovních pozicích v kybernetické bezpečnosti. Komise rovněž vybízí členské státy, aby rozvíjely synergie se svými programy v rámci **Evropského sociálního fondu+** (ESF+) s cílem dále podpořit cíl genderově vyvážené účasti na trhu práce[79], například zřizováním **mentorských programů pro dívky a ženy.** Díky nim bude možné snadněji vytvářet vzory, které přilákají dívky k profesím v oblasti kybernetické bezpečnosti, a zároveň budou bojovat proti genderovým stereotypům. Podporuje se také prohlubování dovedností a změny kvalifikace žen a rozvoj komunity, která bude schopna podpořit ženy při jejich vstupu na trh práce nebo kariérním postupu v oblasti kybernetické bezpečnosti.

[77] Zahájení nových evropských partnerství k naplnění ambicí EU v rámci digitální dekády |Utváření digitální budoucnosti Evropy (europa.eu) v rámci Paktu pro dovednosti s cílem řešit nedostatek informačních a komunikačních technologií (IKT).

[78] Země EU se zavázaly významně zvýšit účast žen v digitální oblasti |Utváření digitální budoucnosti Evropy (europa.eu).

[79] Nařízení Evropského parlamentu a Rady (EU) 2021/1057 ze dne 24. června 2021, kterým se zřizuje Evropský sociální fond plus (ESF+) a zrušuje nařízení (EU) č. 1296/2013, čl. 4 odst. 1 písm. c).

Členské státy by měly v rámci **svých národních strategií kybernetické bezpečnosti** přijmout **konkrétní opatření s cílem zmírnit nedostatek dovedností v oblasti kybernetické bezpečnosti**[80], určit a lépe směrovat úsilí o odstranění nedostatků dovedností a v konečném důsledku zajistit řádné plnění svých povinností podle směrnice NIS 2.

Některé členské státy využívají **součinnosti mezi iniciativami v civilním, obranném a donucovacím sektoru**. Například výchova pracovních sil prostřednictvím povinné vojenské služby nebo využití kybernetických záložníků, tedy občanů, kteří absolvovali vojenský výcvik a v ozbrojených silách obsazují pracovní pozice v oblasti kybernetické bezpečnosti[81], umožňuje obyvatelstvu, a zejména mladým dospělým, zvýšit své dovednosti v oblasti kybernetické bezpečnosti a kybernetické obrany. Totéž platí i pro oblast **boje proti kyberkriminalitě**, neboť mezi obecným úsilím o kybernetickou bezpečnost a činností donucovacích orgánů v reakci na kybernetické bezpečnostní incidenty existuje mnoho podobností. Komise vybízí členské státy k diskusi o těchto iniciativách a vyzývá je, aby posoudily, jak mohou kvalifikované pracovní síly nejlépe sloužit komunitě obranné i civilní kybernetické bezpečnosti.

Komise zváží návrhy, jak řešit současné a očekávané nedostatky zjištěné při přezkumu potřeb orgánů, institucí a jiných subjektů EU. Zejména bude podporovat zaměstnance, aby využili plánovaného **stipendia EU a Spojených států amerických v oblasti kybernetické bezpečnosti**, které bude zřízeno v rámci dialogu mezi EU a USA.

Akce v rámci akademie

Průmysl

- Navrhnout konkrétní **závazky v oblasti kybernetické bezpečnosti** v rámci Platformy pro digitální dovednosti a pracovní místa ode dne 18. dubna 2023.

Členské státy

- Zahrnout do **národních strategií kybernetické bezpečnosti** konkrétní opatření k řešení nedostatku kybernetických dovedností.

Členské státy a průmysl

- Naplňovat deklaraci Ženy v digitálním světě a do roku 2030 dosáhnout **rovnoměrnějšího genderového zastoupení na pracovních pozicích v kybernetické bezpečnosti**.

6. Financování: budovat synergie s cílem maximalizovat dopad výdajů na rozvoj dovedností v oblasti kybernetické bezpečnosti

V rámci akademie bude dopad investic do dovedností v oblasti kybernetické bezpečnosti maximalizován zajištěním společného kontaktního místa, usnadněním lepšího směrování finančních prostředků ve vztahu k potřebám trhu a lepšího využívání finančních prostředků, umožněním součinnosti mezi různými nástroji a zároveň předcházením zdvojování úsilí[82].

[80] Směrnice NIS 2, čl. 7 odst. 2 písm. f).

[81] Zpráva – Cyber Conscription:Experience and Best Practice from Selected Countries (Kybernetická branná povinnost: zkušenosti a osvědčené postupy z vybraných zemí), Martin Hurt a Tiia Sõmer, International Centre for Defence and Security, únor 2021.

[82] Možnosti financování (europa.eu). Podpůrné služby v rámci Paktu pro dovednosti nabízejí jednotné kontaktní místo pro informace o financování dovedností, včetně financování digitálního ekosystému. Podpůrné služby paktu poskytují obecné

6.1 Sladění finančních prostředků s potřebami

V rámci akademie bude centrum ECCC s podporou Komise, projektu ECCO a národních koordinačních center shromažďovat **informace o využívání finančních prostředků EU k financování dovedností v oblasti kybernetické bezpečnosti**, a posoudí, jak finanční prostředky EU pomáhají řešit nedostatek dovedností v oblasti kybernetické bezpečnosti. S ohledem na tyto souhrnné informace bude centrum ECCC usilovat o zajištění lepšího směrování finančních prostředků EU na zjištěné potřeby. Bude financovat opatření, která se zaměří na nejpalčivější nedostatky v oblasti kybernetické bezpečnosti včetně těch, které souvisejí s prováděním potřeb politiky kybernetické bezpečnosti.

6.2 Zviditelnění dostupných finančních prostředků a partnerských iniciativ zaměřených na dovednosti v oblasti kybernetické bezpečnosti

V krátkodobém horizontu se **Platforma pro digitální dovednosti a pracovní místa** stane pro zúčastněné strany jednotným kontaktním místem, kde budou k dispozici veškeré informace o možnostech financování dovedností v oblasti kybernetické bezpečnosti.

EU investuje do lidí a jejich dovedností a využívá zejména partnerství s průmyslem k mobilizaci opatření týkajících se prohlubování dovedností a změn kvalifikace prostřednictvím několika nástrojů určených v rámci **Evropské agendy dovedností**[83], zejména **Paktu pro dovednosti**[84] a **Akčního plánu pro digitální vzdělávání**[85]. **Program Digitální Evropa** financuje příležitosti v oblasti kybernetické bezpečnosti, zejména prostřednictvím projektových iniciativ za účasti více zemí, a jasně tak doplňuje podporu výzkumu a inovativních technologických řešení v oblasti kybernetické bezpečnosti, kterou nabízí program Horizont Evropa. **Evropský obranný fond**[86] financuje výzkum a vývoj technologií k provádění účinných kybernetických operací, včetně školení a cvičení[87]. **Erasmus+** bude tyto iniciativy nadále podporovat, a to i prostřednictvím kombinovaných intenzivních programů a projektů spolupráce.

Členské státy se vyzývají, aby mobilizovaly finanční prostředky EU, které spravují v rámci přímého řízení, na podporu dovedností a pracovních míst v oblasti kybernetické bezpečnosti. Významný synergický potenciál mají v tomto ohledu fondy politiky soudržnosti, jako je **Evropský fond pro regionální rozvoj (EFRR)** a **ESF+**[88]. Opatření v rámci **Nástroje pro oživení a odolnost** (RRF)[89] a programu **InvestEU**[90] zahrnují další doplňkové prvky klíčové pro plnění cílů akademie.

---

informace o nástrojích financování, které nejsou konkrétně zaměřeny na dovednosti v oblasti kybernetické bezpečnosti, přesto by však akademie měla jejich práci zohlednit, aby nedocházelo ke zdvojování.

[83] Evropská agenda dovedností – Zaměstnanost, sociální věci a sociální začleňování – Evropská komise (europa.eu).

[84] Nástroje EU, jimiž se financuje prohlubování dovedností a změna kvalifikace – Zaměstnanost, sociální věci a sociální začleňování – Evropská komise (europa.eu).

[85] Akční plán digitálního vzdělávání na období 2021–2027.

[86] Nařízení Evropského parlamentu a Rady (EU) 2021/697 ze dne 29. dubna 2021, kterým se zřizuje Evropský obranný fond a zrušuje nařízení (EU) 2018/1092.

[87] Členské státy se zavázaly ke společné odborné přípravě a cvičením, například vytvořením projektů školení a cvičení v oblasti kybernetické bezpečnosti v rámci stálé strukturované spolupráce (PESCO) a účastí na těchto projektech a cvičeních, k nimž patří například Akademické a inovační středisko EU pro kybernetickou oblast (EU CAIH) a Propojené kybernetické polygony.

[88] Ustanovení čl. 3 odst. 1 nařízení (EU) 2021/1058 a čl. 4 odst. 1 písm. g) nařízení (EU) 2021/1057.

[89] Například estonský plán obnovy a odolnosti předpokládá investice (10 mil. EUR) do digitálních dovedností, které budou zahrnovat revizi školení dostupných pro odborníky v oblasti IKT, budou financovat prohlubování dovedností a změn kvalifikace odborníků na IKT v oblasti kybernetické bezpečnosti a přispějí k rozvoji pilotního programu přepracování rámce kvalifikací pro odborníky v oblasti IKT.

Akce v rámci akademie

Evropské centrum kompetencí v oblasti kybernetické bezpečnosti a agentura ENISA

- Do konce roku 2024 **zmapovat** stávající financování EU kybernetické bezpečnosti s ohledem na potřeby trhu, posoudit **účinnost** a určit **priority** financování.

Komise

- Do konce roku 2023 zřídit na Platformě pro digitální dovednosti a pracovní místa **jednotné kontaktní místo** pro možnosti financování dovedností v oblasti kybernetické bezpečnosti.

7. Měření pokroku: integrovaná odpovědnost

V rámci akademie bude vypracována **metodika**, která umožní **měřit pokrok v odstraňování nedostatku dovedností v oblasti kybernetické bezpečnosti**.

7.1 Definování ukazatelů kybernetické bezpečnosti pro sledování vývoje trhu práce v oblasti kybernetické bezpečnosti

Index digitální ekonomiky a společnosti (dále jen „DESI“) shrnuje ukazatele digitální výkonnosti Evropy a sleduje vývoj v členských státech EU. V rámci Akademie dovedností v oblasti kybernetické bezpečnosti vypracuje agentura ENISA ve spolupráci s Komisí a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací[91] **ukazatele**, včetně ukazatelů rovnosti žen a mužů, aby bylo možné sledovat pokrok dosažený v členských státech EU ve zvyšování počtu odborníků na kybernetickou bezpečnost, přičemž bude konzultovat také příslušné subjekty trhu a národní koordinační centra. Agentura ENISA bude vycházet z metodiky indexu DESI[92] a zajistí, aby ukazatele byly v souladu s evropskými digitálními cíli týkajícími se odborníků v oblasti IKT a rovnoměrnějšího genderového zastoupení v oboru IKT. Komise bude následně pracovat na začlenění těchto ukazatelů do indexu DESI, což umožní každoroční sledování stavu dovedností v oblasti kybernetické bezpečnosti a trhu práce.

7.2 Shromažďování údajů a předkládání zpráv

Agentura ENISA bude s podporou ze strany projektu ECCO a národních koordinačních center shromažďovat údaje o ukazatelích. Na základě shromážděných údajů agentura ENISA vypracuje **každoroční zprávu**, která přispěje ke zprávě o digitální dekádě[93], jež bude společně s indexem DESI dále využita v analýze a doporučeních pro jednotlivé země v rámci **evropského semestru**[94]. Ukazatele týkající se dovedností v oblasti kybernetické bezpečnosti

---

[90] Zúčastněné strany (např. poskytovatelé odborné přípravy a společnosti, které chtějí navrhnout nebo zlepšit své vzdělávací aktivity v oblasti kybernetické bezpečnosti) se mohou obrátit na poradenské centrum InvestEU, které poskytuje technickou podporu a pomoc včetně budování kapacit pro tvůrce a účastníky projektů, a získat informace na portálu InvestEU.

[91] Na základě využití a doplnění metodiky, kterou vypracuje agentura ENISA pro účely zprávy agentury o stavu kybernetické bezpečnosti v Unii podle čl. 18 odst. 3 směrnice NIS 2 vydávané jednou za dva roky.

[92] Viz Metodická poznámka k Indexu digitální ekonomiky a společnosti (DESI) 2022, k dispozici na adrese Index digitální ekonomiky a společnosti (DESI) |Utváření digitální budoucnosti Evropy (europa.eu).

[93] Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030.

[94] Tamtéž, 25. bod odůvodnění.

navíc přispějí ke **dvouleté zprávě** agentury ENISA o stavu kybernetické bezpečnosti v EU podle směrnice NIS 2, která zahrne kapacity, povědomí a hygienu v oblasti kybernetické bezpečnosti v celé EU.

7.3 Příprava klíčových ukazatelů výkonnosti pro oblast kybernetické bezpečnosti

S cílem odstranit nedostatek talentů v oblasti kybernetické bezpečnosti navrhne agentura ENISA v úzké spolupráci s Komisí a národními koordinačními centry Komisi klíčové ukazatele výkonnosti, přičemž bude vycházet z metodiky politického programu Digitální dekáda 2030 i ze zkušeností v odvětví. Agentura ENISA náležitě zohlední klíčové ukazatele výkonnosti, které členské státy používají k hodnocení svých národních strategií kybernetické bezpečnosti[95].

Akce v rámci akademie

Agentura ENISA

- Do konce roku 2023 připravit **ukazatele a klíčové ukazatele výkonnosti** v oblasti kybernetické bezpečnosti.
- **Shromažďovat a vykazovat údaje** o ukazatelích, přičemž první shromažďování údajů bude provedeno do roku 2025.

Komise

- Pracovat na začlenění **ukazatelů kybernetické bezpečnosti do indexu DESI** a do **zprávy o digitální dekádě**.

8. Závěr

Toto sdělení stanoví základ pro přepracování přístupu EU ke zvyšování kvalifikace odborníků v oblasti kybernetické bezpečnosti v EU. Cílem je snížit nedostatek dovedností v oblasti kybernetické bezpečnosti a vybavit EU potřebnou pracovní silou, která jí umožní reagovat na neustále se vyvíjející prostředí hrozeb, provádět politiky EU, jejichž cílem je chránit EU před kybernetickými útoky, ale také navýšit obchodní příležitosti a konkurenceschopnost. Kvalifikovaná pracovní síla v oblasti kybernetické bezpečnosti může být přínosem pro **civilní, obranné, diplomatické a donucovací orgány** a může usnadnit jejich vzájemnou součinnost.

Komise vyzývá členské státy a všechny zúčastněné strany, aby naplnily ambice Akademie dovedností v oblasti kybernetické bezpečnosti.

[95] Ustanovení čl. 7 odst. 4 směrnice NIS 2.