

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Národní centrum kybernetické bezpečnosti



**NÁVRH KONCEPCE
VZDĚLÁVÁNÍ V PROBLEMATICE
KYBERNETICKÉ BEZPEČNOSTI**

OBSAH

ÚVOD A LEGISLATIVNÍ RÁMEC	3
1. OBECNÉ VZDĚLÁVÁNÍ.....	7
2. SPECIFICKÉ VZDĚLÁVÁNÍ.....	20
SEZNAM POUŽITÝCH ZDROJŮ	39

ÚVOD A LEGISLATIVNÍ RÁMEC

Dne 16. února 2015 byla Vládou ČR schválena **Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020** (dále jen „NSKB“), která definuje cíle v kybernetické bezpečnosti (dále jen „KB“). V NSKB stojí, že jedním z klíčových bodů zajišťování KB je potřeba celospolečenské osvěty¹ a vzdělávání. Jednotlivé body Strategie jsou konkrétně rozpracovány v **Akčním plánu** (dále jen „AP“), který byl Vládou ČR schválen 25. května 2015. Ten mimo jiné definuje tři hlavní cíle vzdělávání v oblasti KB:

1. Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků základních a středních škol, studentů vyšších odborných a vysokých škol, tak u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.
2. Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vzdělávat experty na kybernetickou bezpečnost.
3. Vzdělávat a školit zaměstnance veřejné správy působící nejen v oblasti kybernetické bezpečnosti a informační kriminality.

AP dále určuje i jednotlivé body týkající se ochrany národní kritické informační infrastruktury (dále jen „KII“) a významných informačních systémů (dále jen „VIS“). Dnem 1. 1. 2015 nabyl účinnosti **zákon č. 181/2014 Sb., o kybernetické bezpečnosti** (dále jen „ZKB“), který stanovuje systém zajišťování KB včetně povinností pro správce jednotlivých informačních a komunikačních systémů. V rámci této problematiky je vzdělávání a osvěta základem prevence a ochrany důležitých informačních a komunikačních systémů, které mají zásadní vliv na fungování ČR. Tato problematika bude podrobněji rozepsána v části věnované KII a VIS v kapitole specifického vzdělávání.

Záměrem návrhu koncepce vzdělávání v oblasti KB (dále jen „koncepte“) je zmapovat jednotlivé cílové skupiny, analyzovat jejich potřeby a rozpracovat i navrhnout prostředky k realizaci těchto potřeb, tak aby byly naplněny stanovené úkoly vzdělávání, které ukládá AP. Zároveň má pomoci vytvořit síť styčných bodů na národní i mezinárodní úrovni, tak aby byla zajištěna celkově co nejefektivnější spolupráce.

Ambicí dokumentu je předložit ucelený rámec a nástroje pro vzdělávání osob a skupin obyvatel, které přicházejí do styku s - nebo jsou zranitelní - v kybernetickém prostoru. Jedná se o koncepční materiál, který směřuje k průběžnému vzdělávání cílových skupin přímo či nepřímo se podílejících na zvyšování úrovně kybernetické bezpečnosti. NBÚ/NCKB jako národní autorita pro kybernetickou bezpečnost definuje oblasti i skupiny a metodicky spolupracuje s gestory vzdělávání příslušných cílových skupin.

¹ NSKB – hlavní cíl F (v AP dále stanoveno jako úkol F. 1.01)

Co do povahy dokumentu, je jeho cílem usnadnit práci všem níže uvedeným cílovým skupinám. Jedná se o podpůrný materiál, který nemá snahu direktivně úkolovat a vyžadovat plnění úkolů. Jde o metodický návod, který systematicky řadí laickou i odbornou veřejnost do skupin, kterých se problematika KB nějakým způsobem týká, čímž umožňuje snadnější orientaci v tématu a vzdělávacích pramenech. NBÚ/NCKB zde funguje pouze jako zastřešující koordinační orgán, který umožňuje přístup k uceleným, souhrnným informacím a poskytuje vodítko pro jednotlivce i skupiny, které mají zájem získávat nové poznatky v oblasti KB a dále rozvíjet své profesní znalosti.

Tento materiál vznikl v koordinaci s Ministerstvem školství, mládeže a tělovýchovy a jeho přímo řízenou organizací - Národním ústavem pro vzdělávání, Ministerstvem práce a sociálních věcí a Národním centrem bezpečnějšího Internetu. Jeho smyslem není vytvářet duplicitní materiály ani postupy, ale reflektovat účinnost, strukturu a potřeby již existujících strategických materiálů, z nichž stěžejním jsou **Strategie digitálního vzdělávání do roku 2020** (dále jen „SDV“), vydaná Ministerstvem školství, mládeže a tělovýchovy (dále jen „MŠMT“) dne 31. 10. 2014 a **Strategie digitální gramotnosti ČR na období 2015 – 2020** (dále jen „SDG“), vydaná Ministerstvem práce a sociálních věcí (dále jen „MPSV“) a schválená Vládou ČR dne 1. července 2015.

SDV prosazuje rozvoj informatického myšlení (tzv. „computational thinking“) a používání digitálních technologií ve vzdělávání. NCKB se na jejím uskutečňování bude podílet jako podpůrný subjekt pro začlenění problematiky kybernetické bezpečnosti do některých z jejích hlavních cílů, kterými jsou například:

- *podmínky pro rozvoj digitální gramotnosti žáků* – zejména: pravidelná aktualizace rámcových vzdělávacích programů, zdůraznění problematiky funkce a užití digitálních technologií napříč kurikulem a modernizace vzdělávací oblasti ICT v rámcových vzdělávacích programech;
- *podmínky pro rozvoj gramotnosti učitelů* – zejména: zařazení digitálních kompetencí učitele do vzdělávání učitelů, zařazení rozvoje digitální gramotnosti a informatického myšlení žáků do vzdělávání učitelů;
- *budování a obnova digitální vzdělávací infrastruktury* – zejména: připojení škol k internetu;
- *systém podporující rozvoj škol v oblasti integrace digitálních technologií do výuky a života školy* – zejména: koordinace podpory digitálního vzdělávání v resortu školství, rozvoj aktualizace nástroje „Profil Škola²¹“ a zavedení nového nástroje „Profil Učitel²¹“, odborná a metodická podpora rozvoje infrastruktury digitálního prostředí škol pro zřizovatele a vedení škol, metodická podpora začleňování digitálních technologií do výuky a života školy či zřízení sítě ICT metodiků na úrovni kraje/obce a jejich podpora.

SDG prosazuje rozvoj digitální gramotnosti a následné využití potenciálu digitálních technologií k celoživotnímu osobnímu rozvoji občanů ČR. S tím je spojeno zvyšování kvality života občanů a jejich společenské uplatnění ať už na trhu práce, v komunitě nebo ve vztahu k digitalizovaným médiím či informatizující se veřejné správě. NCKB se na plnění strategie bude podílet jako podpůrný subjekt pro začlenění problematiky kybernetické bezpečnosti do některých z jejích prioritních cílů, kterými jsou například:

- *zvýšení schopnosti rodin využívat příležitosti a eliminovat rizika spojená s využíváním digitálních technologií v rámci rodiny i školního a volnočasového prostředí* – zejména: zvyšování povědomí a gramotnosti v otázkách kybernetické bezpečnosti, především bezpečného užívání digitálních technologií a pohybu v internetovém prostředí;
- *budování a obnova digitální infrastruktury ve veřejném sektoru* – zejména: připojení veřejných míst k internetu (knihovny, komunitní centra atd.), digitalizace společnosti;
- *zvýšení efektivity a dostupnosti vhodných forem učení a vzdělávání prostřednictvím digitálních technologií v celoživotní perspektivě* – zejména: tvorba osvětových kampaní, podpora a koordinace činnosti neziskových organizací a sdružení v oblasti vzdělávání a osvěty kybernetické bezpečnosti prostřednictvím dalšího vzdělávání.

Na úrovni EU návrh této koncepce rámcově vychází ze strategického dokumentu **Evropa 2020**², vydaného Evropskou komisí dne 3. 3. 2010, který stanovuje kroky pro inteligentní a udržitelný růst podporující začlenění. Prioritami procesu začlenění jsou podpora vzdělávání, odborné přípravy a digitální společnosti³, kde mezi stěžejní iniciativy patří zlepšení výsledků a mezinárodní atraktivita evropských vysokoškolských institucí⁴ a zajištění udržitelného hospodářského a sociálního přínosu jednotného digitálního trhu⁵.

Koncepce svým zaměřením koresponduje se zahraničními⁶ strategickými materiály, čímž potvrzuje celosvětový trend potřeby vzdělávání a osvěty v oblasti KB. Společným cílem těchto dokumentů je zvýšení informovanosti o rizicích kyberprostoru a rozvoj digitální gramotnosti všech cílových skupin. Zaměřují se především na zvyšování kvality výuky kybernetické bezpečnosti napříč jednotlivými vzdělávacími úrovněmi, ale i v průběhu dalšího vzdělávání. V návaznosti na tuto skutečnost je jednou z priorit například vzdělávání stávajících pedagogů i povinné vzdělávání studentů pedagogických oborů. Většina dokumentů si vzala za cíl zlepšit vzdělávání odborníků technických oborů včetně ICT specialistů a zároveň budovat základnu nové generace expertů v oblasti ICT. Z tohoto tak jasně vyplývá, že podpora vzdělávání a výzkumu v problematice KB se stává jednou z hlavních priorit mnoha států.

² Strategický dokument Evropa 2020 ke stažení: <https://www.mmr.cz/getmedia/7c31b211-1a5a-46a8-b6bd-151b72dc94ec/EU2020-CJ.pdf>

³ Evropa 2020, str. 12

⁴ Evropa 2020, str. 13

⁵ Evropa 2020, str. 14

⁶ Například USA – National Initiative for Cyber Security Education Strategy, EST – HITSA Strategy 2014-2020, HU - (National Cyber Security Strategy of Hungary), SVK - National Strategy for Information Security in the Slovak Republic, UK – Cyber Security Strategy Protecting and Promoting the UK in a Digital World, AT – National ICT Security Strategy, PL – Cyberspace Protection Policy of the Republic of Poland.

STRUKTURA KONCEPCE, PERSONÁLNÍ NÁROKY A NÁPLŇ ČINNOSTI

Základní jednotkou koncepce je stanovení cílových skupin vzdělávání. Ty jsou dle své charakteristiky začleněny do kapitoly 1 - Obecné vzdělávání a kapitoly 2 - Specifické vzdělávání, kam spadá i interní vzdělávání zaměstnanců NBÚ. Každá cílová skupina má následující osnovou:

- zdůvodnění proč byla určena;
- prostřednictvím jakých subjektů by měla být tato cílová skupina vzdělávána;
- jaké nástroje lze při vzdělávání prakticky využít;
- specifická role NBÚ/NCKB - jak může ke vzdělávání přispět a
- subjekty doporučené ke spolupráci s cílem maximalizovat výsledný efekt.

Poslední dva body osnovy jsou pro kapitolu obecného vzdělávání přesunuty na začátek hned po výčtu cílových skupin, jelikož jsou pro všechny tyto skupiny identické. V kapitole specifického vzdělávání jsou řazeny na konec zvlášť ke každé cílové skupině.

Struktura koncepce bude reflektovat uspořádání plánované vzdělávací části portálu GovCERT.CZ⁷.

Doporučený personální nárok pro odpovídající zajištění stanovených úkolů ze strany NCKB jsou minimálně 3 osoby s VŠ vzděláním, z čehož 2 z nich s pedagogicko-technickým vzděláním (zastoupení aprobací pro základní i střední školu).

Návrh na náplň činnosti těchto osob je:

- zabezpečit styčný kontakt pro spolupráci s níže uvedenými zainteresovanými subjekty,
- podílet se na tvorbě informačních materiálů,
- vytvářet osvětové a vzdělávací materiály pro oblast KB pro jednotlivé cílové skupiny,
- vytvářet obsah vzdělávacích programů, sylabů a učebních osnov, práce na modernizaci stávajících rámcových programů na ZŠ a SŠ úrovni⁸,
- připravovat metodická doporučení a materiály usnadňující školám zapracování problematiky KB do školních vzdělávacích programů podle nových rámcových programů⁹,
- pracovat na metodických materiálech pro učitele, průběžně pracovat na tvorbě výchozích učebních materiálů pro žáky a studenty¹⁰,
- sledovat celosvětových trendů v oblasti KB a vzdělávání,
- spolupracovat na tvorbě obsahu e-learningu, prosazování a využívání interaktivních metod výuky, podpora využívání multimediálních prostředků ve vzdělávacích institucích,
- spolupracovat při tvorbě obsahu vzdělávacího portálu GovCERT.CZ.

⁷ AP – úkol F.1.02

⁸ AP – úkol F.2.01

⁹ AP – úkol F.2.02

¹⁰ AP – úkol F.2.03

1. OBECNÉ VZDĚLÁVÁNÍ

Potřeba vzdělávat veřejnost v oblasti digitální gramotnosti a kybernetické bezpečnosti již od nejranějšího věku vzhledem k narůstajícímu počtu využívání prostředků ICT a rizik s tím spojených, neustále sílí. V případě vzdělávání dětí, žáků a studentů je tato koncepce v souladu s již v úvodu zmíněnou Strategií digitálního vzdělávání do roku 2020. Na digitální gramotnost jakožto vůdčí trend současnosti odkazuje rovněž uvedená Strategie digitální gramotnosti ČR na období 2015 - 2020 a další materiály, jako je např. strategický záměr „Digitální vzdělávání Touch your future“¹¹, který je součástí strategie Digitální Česko 2.0 – Usnesení vlády č. 203 ze dne 20. 3. 2013¹².

Neméně významným dokumentem ve vztahu digitálních technologií ke školnímu prostředí je Horizon Report Europe – 2014 Schools Edition. Jeho cílem je přehled stávající situace používání digitálních technologií ve školách s budoucím výhledem propojení formálního i neformálního vzdělávání a potřeby zlepšení výuky komplexního myšlení. Na základě kontinuálně se zvyšujícího používání ICT k výuce či učení prostřednictvím gamifikovaného prostředí, počítačových her a sociálních sítí má u dětí a žáků docházet k logickému propojování virtuálního prostředí s fyzickým, což má zajistit lepší pochopení obou světů. Takovým vlivem však dochází i ke změně úlohy a odborného rozsahu učitelů, což je rovněž při současném stavu systému vzdělávání třeba vzít v potaz. Důležitým prvkem výuky samotné je co nejvíce ji přiblížit evropskému standardu, který doporučuje využívání osvětových projektů, jako je například internetový evropský portál e-Twinning (.cz, .net) sloužící jednak k podpoře a výměně informací pro pedagogy i školy a také k praktickému propojování škol a učitelů různých zemí za účelem realizace vzdělávacích projektů.

Ostatní vyjmenované cílové skupiny této kapitoly se nemusí nutně s ICT technologiemi setkávat přímo z didaktického hlediska, jako s prostředky vlastního procesu učení se, ale coby uživatelé musí být na různých úrovních obeznámeni s jejich možnostmi i úskalími, které s sebou přinášejí.

Definované cílové skupiny obecného vzdělávání:

- a) Děti předškolního věku a žáci 1. stupně ZŠ
- b) Žáci 2. stupně ZŠ
- c) Žáci SŠ
- d) Pedagogičtí pracovníci¹³
- e) Preventisté¹⁴
- f) Sociální pracovníci a pomáhající profesionálové
- g) Odborná a zájmová sdružení
- h) Rodiče
- i) Senioři
- j) Široká veřejnost

¹¹ VLÁDA ČESKÉ REPUBLIKY (2013). USNESENÍ VLÁDY ČESKÉ REPUBLIKY KE STRATEGICKÉMU ZÁMĚRU DIGITÁLNÍ VZDĚLÁVÁNÍ – TOUCH YOUR FUTURE. [online] <http://bit.ly/1qSiIcB>

¹² VLÁDA ČESKÉ REPUBLIKY (2013). DIGITÁLNÍ ČESKO V. 2.0: CESTA K DIGITÁLNÍ EKONOMICE. [online] <http://bit.ly/1qSiIgz>

¹³ Dle § 2 zákona č. 563/2004 Sb., o pedagogických pracovnících a o změně některých zákonů.

¹⁴ Pracovníci prevence, např. pracovníci prevence kriminality v gesci MV ČR a pracovníky prevence rizikových jevů v gesci MŠMT.

Přínos a praktický vstup NCKB:

- Poskytování podpory prostřednictvím konzultací a odborných garancí přímo zainteresovaným subjektům.
- Ve spolupráci s MŠMT a MPSV podpora celorepublikové sítě (kontaktní list) osvětových organizací a projektů z oblasti KB s rozdělením na kraje (seznam organizací, osob, kontaktů, odkaz na webové stránky).
- Průběžně pracovat na tvorbě preventivně informačních materiálů a vytvoření osvětového portálu GovCERT.CZ, jehož jedna část bude věnována veřejnosti a jejíž součástí bude e-learning¹⁵.

Přímo zainteresované subjekty spolupracující s NCKB:

Při realizaci všeobecného vzdělávání výše uvedených cílových skupin je počítáno se spoluprací relevantních subjektů. Klíčovými partnery jsou MŠMT včetně Národního ústavu pro vzdělávání (dále jen „NÚV“), MPSV, Česká školní inspekce, Jednota školských informatiků, Univerzita Palackého v Olomouci – Centrum prevence rizikové komunikace (dále jen „PRVok“), pedagogičtí pracovníci, CESNET, Policie České republiky (dále jen „PČR“), obecní a městská policie (dále jen „OP“, „MP“), Krajské úřady a Kraje pro bezpečný internet (dále jen („KPBI“), Orgán sociálně-právní ochrany dětí (dále jen „OSPOD“) a osvětové organizace, agentury a projekty (např. NCBI, CZ.NIC, Seznam se bezpečně apod.).

Spolupráce NCKB se zainteresovanými subjekty zahrne následující roviny:

1. Strategická – vedení institucí, tvorba synergie mezi NCKB (AP), MŠMT, MPSV.
2. Operační – vytváření a plnění koncepce vzdělávání – sylaby, osnovy, konkrétní výuka.
3. Odborná – analýza a překlad existujících materiálů, vytváření nových, pravidelná aktualizace, informační servis (zranitelnosti, obsahová stránka atd.).
4. Projektová a mediální – realizace konkrétních projektů, pomoc s medializací (poskytovat a distribuovat materiály vytvořené k cílovým skupinám).

¹⁵ AP – úkol F.1.03

a) DĚTI PŘEDŠKOLNÍHO VĚKU A ŽÁCI ZŠ DO 1. STUPNĚ

Zdůvodnění cílové skupiny:

Již od nejranějších let děti užívají základní informační technologie (dále jen ICT) a mobilní komunikační zařízení, a to zejména k hraní her nebo sledování videí. Technologie ICT mají v současnosti nezastupitelnou roli (jsou dnes součástí téměř veškerého lidského fungování) a vzhledem k jejich čím dál snadnější ovladatelnosti, jsou už i malé děti co do technické manipulace samostatnými uživateli. Byť je tato cílová skupina zpravidla ještě pod vysokým dohledem rodičů, svět ICT a Internetu je tak obsáhlý a nekontrolovatelný, že je třeba již těmto dětem vštěpovat základy bezpečného zacházení s digitálními technologiemi.

V osvětě malých dětí mají jednoznačně nezastupitelný podíl jejich rodiče, kteří ne vždy disponují znalostmi reálných úskalí ICT nebo je často spíše podceňují. Osvěta samotných rodičů je tedy souvisejícím, velmi podstatným prvkem, a proto je v této koncepci rodičům věnována vlastní cílová skupina níže.

Doporučený způsob vzdělávání:

Vzdělávání by mělo probíhat formou her a zábavy jednak přímo ze strany rodičů a také ze strany učitelů v MŠ a ZŠ. Na úrovni MŠ a ZŠ by měla s rodiči probíhat na toto téma pravidelná diskuze, zejména na téma využití technických možností zákazu přístupu na vybrané „webové stránky“. Účinnost vzdělávání u této cílové skupiny je přímo úměrná úrovni vzdělání pedagogů, kteří je vyučují. S výše uvedeným je tedy spjata potřeba zvyšování ICT kompetencí těchto pedagogů (souvislost s cílovou skupinou d).

Doporučené vzdělávací nástroje:

Mezi velmi vhodné nástroje pro děti z MŠ patří osvětové audiovizuální a multimediální nástroje vzdělávání (např. pexeso, omalovánky, hry, animovaná videa). Pro první stupeň ZŠ jsou pak vhodnější interaktivní semináře, dílny, tematické soutěže, hry, videa a celkově vštípení dobrých návyků již od začátku při využívání ICT technologií při školní práci. V plánu je modernizace rámcových vzdělávacích programů, respektive podpora při začlenění problematiky KB do RVP. Obě dvě části této skupiny je vhodné vzdělávat prostřednictvím audiovizuálních prostředků (např. OVCE.sk). Další velmi zajímavou možností je využití peer programů, kdy žáci vyšších ročníků vzdělávají žáky (děti) mladší.

b) ŽÁCI 2. STUPEŇ ZŠ

Zdůvodnění cílové skupiny:

ICT a zejména mobilní komunikační zařízení tvoří nedílnou součást každodenního života žáků 2. stupně. Užívají je při studiu i v soukromém životě (nejčastěji sociální sítě, blogy, online komunikace, hry a sledování videí). V rámci výuky jsou ICT prostředky běžně využívány pro různé školní práce a jako výukový nástroj během hodin. I přes schopnost běžně využívat ICT si ještě dostatečně neuvědomují veškerá reálná rizika, proto je třeba na tato rizika upozornit a nabídnout preventivní opatření i následné řešení vzniklého problému. Za účinnou prevenci považujeme názorné příklady a modelové situace spojené s kyberšikanou, sociálním inženýrstvím, neověřenou virtuální identitou, kybergroomingem či sextingem. Tyto jevy mohou být navzájem propojeny a vytvářet tak vzájemnou síť příčin a následků.

Neopatrné používání technologií ICT v kombinaci s nedostatečnou informovaností či ochranou a neetickým jednáním mohou stát zákeřnou zbraní. Z pozice potenciální oběti jsou žáci 2. stupně základních škol nejzranitelnější skupinou a naopak z pozice potenciálního pachatele jsou od věku 15 let trestně stíhatelní. Vedle prohlubování technických znalostí je zde tedy nutno klást zvýšený důraz na etiku, která je v případě diskutované cílové skupiny základem správného užívání prostředků ICT.

Významným prvkem osvěty náctiletých je vytvoření důvěry nezbytné jak pro prevenci, tak pro řešení různých situací. Zároveň je velmi důležité získání dobré praxe – bezpečného chování ve vztahu k sociálním sítím, heslům a sdílení osobních údajů.

Je podstatné prohlubovat u těchto žáků zájem o využívání a znalosti prostředí ICT a motivovat je tím dále k profesnímu i osobnímu rozvoji zaměřeného na práci s žákovými postoji. Pro takový rozvoj zde může pozitivně zapůsobit podpora tematicky zaměřených odbornějších aktivit v oblasti informatiky a výpočetní techniky či různé interaktivní besedy s kvalifikovanými odborníky. Pro zvýšení edukačního prvku lze takové aktivity pojmout interaktivní, potažmo on-line formou (např. sdílené krátké filmy a naučná videa).

Doporučený způsob vzdělávání:

Zde je třeba zapojení MŠMT a včlenění této problematiky do RVP dle jejich zaměření v rámci vzdělávacích oborů (například Informační a komunikační technologie, výchova k občanství, člověk a jeho svět či výchova ke zdraví) a vhodných průřezových témat (například mediální výchovy). Jako velmi vhodné se jeví i vytvoření zcela nového průřezového tématu. Pro získání požadovaného vzdělávacího efektu je důležité společné působení učitelů a rodičů.

Doporučené vzdělávací nástroje:

Vhodnými nástroji jsou prezentace a osvětové semináře poskytované externími odborníky, modelové situace, hry a tematické soutěže, projektová výuka, videa, workshopy, dílny, tablet, debatní kroužky či peer programy. Velmi důležitá je podpora tematicky zaměřených odbornějších aktivit v oblasti informatiky a výpočetní techniky jako je například „Olympiáda“. Podpůrně lze využít e-learningovou výuku a osvětový portál GovCERT.CZ.

c) ŽÁCI SŠ

Zdůvodnění cílové skupiny:

Žáci středních škol jsou velmi širokou skupinou setkávající se s ICT téměř denně a to téměř bezvýhradně v propojení s Internetem. Většina se pohybuje na sociálních sítích a část svého života prožívá virtuálně. Je třeba neustále zdůrazňovat a opakovat rizika s tím spojená. I zde je stále důležitý aspekt etiky, jakožto nedílné součásti bezpečného používání ICT, a i zde je na místě upozorňovat na nebezpečí patologických jevů v podobě kyberšikany, sociálního inženýrství, neověřené virtuální identity, kybergroomingu či sextingu.

Dále jsou na střední škole ICT prostředky hojně využívány i pro školní práce, projekty a prezentace. Je tedy nutné zdůraznit, jak může mít nedostatečná ochrana vlastního zařízení vliv nejen na volnočasové aktivity v prostředí internetu, ale také na studijní výsledky a prospěch, například v podobě ztráty dat, hotových prací či učebního materiálu, stejně jako na „ztrátu“ vlastního soukromí odcizením soukromých „osobních údajů“.

Konkrétní podoba vzdělávání žáků středních škol by měla kopírovat zaměření škol. Rozdílné přístupy tedy budou ve všeobecném vzdělávání a ve vzdělávání odborném dle oborů. Obzvláště důležité je téma KB důkladně přiblížit SŠ s technickým zaměřením a žáky tak motivovat k pokračování studia KB na VŠ, čímž bude docházet k posilování řad odborníků na KB. I zde je tedy jednou ze stěžejních praktických aktivit podpora tematicky zaměřené odbornější činnosti.

Doporučený způsob vzdělávání:

Opět potřeba zapojení MŠMT a včlenění této problematiky do RVP dle jejich zaměření v rámci vzdělávacích oborů (například Informatika a informační a komunikační technologie, oblast vzdělávání Informační a komunikační technologie atd.). Zapojení studentů do tvorby vlastních projektů s tematikou KB, zapojení rodičů.

Doporučené vzdělávací nástroje:

Stejně jako pro ostatní věkové skupiny je vhodné i pro středoškolské studenty využít i jiných metod, než které nabízí frontální výuka. Navrhované metody jsou dobrovolné semináře motivované odměnou či zlepšením prospěchu, debaty s externími odborníky na školách a to jak z řad odborníků na KB, tak z řad policie, která řeší případy kyberšikany a může uvést mnoho názorných příkladů. Dále lze uplatnit projektovou výuku, workshopy, tematické soutěže, videa, tabletop a debatní kroužky. Velmi důležitá je i výše zmíněná podpora tematicky zaměřených odbornějších prací, jako je například Středoškolská odborná činnost („SOČ“) v oblasti informatiky, informační bezpečnosti a ostatních okruhů s ní spojených. Jako podpůrné doplňkové materiály lze opět využít e-learningovou výuku a osvětový portál GovCERT.CZ.

d) PEDAGOGIČTÍ PRACOVNÍCI

Zdůvodnění cílové skupiny:

Pedagogičtí pracovníci jsou hned po rodině ti, kdo mají svůj nezastupitelný podíl při vštěpování dobrých návyků, sociálního chování a zapojení jedinců do společnosti. Učitelé byli vždy právem považováni za základní kámen, potažmo zrcadlo vzdělanosti národa. Vzdělání člověka je faktorem, od něhož se odvíjí jeho další existence a úspěšnost jeho počínání. Vzdělanost je základem civilizované společnosti a předurčuje její další vývoj. Kvalitně vzdělaní učitelé zvyšují možnost kvalitně vzdělávat žáky a pomáhat tak formovat vzdělané občany.

Cílovou skupinu pedagogických pracovníků je nutno rozdělit do podskupin podle stupně a zaměření školy (MŠ, ZŠ, SŠ – technické, netechnické). Tito pracovníci by měli být průběžně informováni o současných běžně využívaných ICT prostředcích, aplikacích a rizicích, která plynou z jejich využívání. Důležitá je schopnost řešit nastalé situace a v případě potřeby vědět, na jaké instituce se obrátit. Tyto informace je nutné efektivně předávat žákům. Z pozice této cílové skupiny je opět vhodné upozorňovat i rodiče na hrozby vyplývající z využívání ICT včetně doporučení pro domácí osvětu (kontakty a informační zdroje z oblasti KB).

Jak již naznačila Strategie digitálního vzdělávání do roku 2020, zásadní pozornosti je potřeba věnovat učitelům, kteří působí na 1. Stupni ZŠ. Formální vzdělávání těchto v problematice ICT je neuspokojivé¹⁶.

Do vzdělávání této cílové skupiny je vhodné zapojit i Českou školní inspekci, která do svých inspekčních priorit může zakomponovat i sledování postupu škol v oblasti bezpečného používání prostředků ICT a tématu kybernetické bezpečnosti.

Doporučený způsob vzdělávání:

Primárním krokem k zajištění odpovídajícího vzdělávání je jeho zefektivnění, což obnáší celkovou modernizaci dosavadního vzdělávání pedagogických pracovníků v oblasti informačních a komunikačních technologií. Výchozím dokumentem pro takový krok je již výše uvedená Strategie digitálního vzdělávání do roku 2020. Základními prvky k úspěšné implementaci uvedené strategie, a tím i zefektivnění celého procesu vzdělávání této cílové skupiny jsou zejména začlenění problematiky KB do digitálních kompetencí učitele¹⁷, spolupráce s VŠ vzdělávajícími učitele a podpora integrace tohoto do profilu absolventa pedagogické VŠ¹⁸ a spolupráce s Národním institutem dalšího vzdělávání - zvláště podpora integrace digitálních kompetencí učitelů do kariérního systému¹⁹. Neméně důležitou roli zastává integrace problematiky KB do pro Studium k výkonu specializovaných činností, integrace problematiky KB pro ředitele škol a školských zařízení a podpora vzniku nových kurzů dalšího vzdělávání pedagogických pracovníků zaměřených na problematiku KB.

Praktickým přínosem zde je zapojení MŠMT ve spolupráci s VŠ vzdělávajícími učitele při tvorbě akreditovaných kurzů pro průběžné další vzdělávání pedagogických pracovníků, které by byly zakončeny obecně uznávaným osvědčením o absolvování. Zároveň je u této cílové skupiny velmi doporučena podpora již výše jmenovaného specializačního studia, a to zejména pro koordinátory a metodiky (např. koordinátoři v oblasti ICT, správci digitální infrastruktury škol, metodici prevence sociálně patologických jevů etc.).

¹⁶ Strategie digitálního vzdělávání do roku 2020 – Současná situace ve školách

¹⁷ Strategie digitálního vzdělávání do roku 2020 – bod 3.1.1

¹⁸ Strategie digitálního vzdělávání do roku 2020 – bod 3.1.2

¹⁹ Strategie digitálního vzdělávání do roku 2020 – bod 3.1.3

Významné jsou i programy dalšího vzdělávání, celoživotní vzdělávání a podpora využívání portálů jako je eTwinning.net, které umožňují kooperaci učitelů a realizaci projektů aktivně využívající ICT napříč Evropskými státy.

Doporučené vzdělávací nástroje:

Vzdělávat pedagogické pracovníky se doporučuje zejména metodou proškolení celých učitelských sborů a to například formou přednášek, prezentací, videí, konferencí, tvorbou a úpravou sylabů, e-learningu, kurzů zakončených obecně uznávaným osvědčením o absolvování, workshopů, tabletopů, seminářů a webinářů, osvětového portálu GovCERT.CZ a prostřednictvím dalších otevřených informačních zdrojů z oblasti KB. Dále pak rovněž pomocí výukových opor a materiálů využitelných přímo v pedagogické praxi jako jsou například pracovní listy, metodické materiály, online tools. Oporou pro integraci KB do školního kurikula a tvorbu a rozvoj školní strategie je mezinárodní projekt národních ministerstev školství eSafety Label (www.esafetylabel.eu). Zároveň je zde pro završení celistvosti vzdělávání této cílové skupiny v příslušné škole či školském zařízení doporučen aktivní kontakt v rámci pedagogického sboru s pedagogem pro oblast informačních a komunikačních technologií.

e) PREVENTISTÉ - PRACOVNÍCI PREVENCE KRIMINALITY, PRACOVNÍCI PREVENCE RIZIKOVÝCH JEVŮ APOD.

Zdůvodnění cílové skupiny:

I zaměstnanci preventivních oddělení, osvětových organizací, projektů a agentur v oblasti KB ke své práci potřebují sledovat trendy v oblasti KB a dále se průběžně vzdělávat v tomto oboru. Pouze tak budou schopní v rámci svých vzdělávacích programů předávat relevantní informace příslušným subjektům, potažmo svým cílovým skupinám.

Rozsah jejich znalostí by měl sahát od preventivních opatření přes návrhy řešení nastalých situací až po znalost toho, kam se případně dál obrátit s žádostí o pomoc. Základní digitální gramotnost je u nich nutným předpokladem a další rozšiřování znalostí v oblasti technologií ICT by mělo být podporováno.

Doporučený způsob vzdělávání:

Vzdělávání je doporučeno zejména prostřednictvím MVČR/PČR, MPSV, akademické sféry, Krajských úřadů včetně KPBI, OSPOD, osvětových organizací a agentur. Specifické dílčí oblasti lze i prostřednictvím NCKB. V tomto ohledu je velmi důležité vzájemné /meziresortní/ vzdělávání a výměna zkušeností v oblasti KB.

Doporučené vzdělávací nástroje:

K vzdělávání preventistů se nejlépe hodí přednášky, workshopy, tabletopy, konference, praktické „zážitkové“ aktivity, pravidelný kontakt a setkávání se svými profesními kolegy a partnery např. ve formě užších neformálních pracovních skupin, e-learning, osvětové portály včetně GovCERT.CZ. Dále pak zpřístupnění informačních zdrojů a kontaktů z oblasti KB.

f) SOCIÁLNÍ PRACOVNÍCI A POMÁHAJÍCÍ PROFESIONÁLOVÉ

Zdůvodnění cílové skupiny:

Pracovníci a dobrovolníci poskytující vlastní intervenci a krizovou pomoc, poradenství či další služby lidem ohroženým elektronickým násilím a kriminalitou jsou vzhledem k odlišnému charakteru profesního zaměření a vykonávané praxe odděleni od pracovníků prevence. Sociální pracovníci a pomáhající profesionálové řeší ve spolupráci s dalšími orgány jako je například Policie ČR již přímo vlastní následky, pracují s oběťmi a způsob jejich vzdělávání je třeba oddělit od pracovníků prevence.

Do této cílové skupiny lze zahrnout například i psychology a právníky poskytující sociálně-právní pomoc v různých neziskových a dobrovolnických organizacích či dalších sociálních a krizových službách. Téma této cílové skupiny se částečně dotýká i cílové skupiny d) zahrnující pedagogické pracovníky, a to speciální pedagogy či pracovníky působící v pedagogicko-psychologických poradnách.

Vzhledem ke skutečnosti, že zatím neexistuje ucelený systém vzdělávání výše uvedených profesionálů, který by zohledňoval kybernetickou bezpečnost a online násilí jako jeden ze zásadních faktorů, který může být předstupněm násilí fyzického, zvyšuje se riziko, že nebudou schopni poskytnout odpovídající pomoc. Jejich pomoc však může být pro oběť zásadní a z tohoto důvodu by měla být i tato cílová skupina patřičně a průběžně vzdělávána a informována o trendech z oblasti ICT technologií a jejich rizicích.

Doporučený způsob vzdělávání:

Pro cílovou skupinu sociálních pracovníků a pomáhajících profesionálů lze v rámci jejich vzdělávání použít obdobný způsob, jako u předchozí cílové skupiny, přičemž je ještě doporučeno zapojit MŠMT.

Doporučené vzdělávací nástroje:

Pro vzdělávání sociálních pracovníků a pomáhajících profesionálů lze použít stejné nástroje jako u cílové skupiny preventistů včetně zpřístupnění informačních zdrojů a kontaktů z oblasti KB (přičemž rozdíl bude v obsahové stránce s důrazem na řešení následků).

g) ODBORNÁ A ZÁJMOVÁ SDRUŽENÍ

Zdůvodnění cílové skupiny:

Odborná a zájmová sdružení patří mezi hlavní strategické hráče v oblasti osvěty kybernetické bezpečnosti a prevence kyberkriminality. Tato sdružení mnohdy nabízejí jak metodickou podporu pedagogům, tak i vlastní vzdělávací aktivity pro žáky, studenty, širokou veřejnost, pedagogy, ale i policisty a sociální pracovníky. Další z činností odborných a zájmových sdružení je zřizování kontaktních center a poraden, které nabízejí pomoc při řešení krizových situací. Není tedy žádným překvapením, že i tato cílová skupina by měla být pravidelně informována a průběžně vzdělávána o nových trendech v oblasti KB.

Vzhledem k širokému záběru poskytovaných služeb těchto sdružení by mělo vzdělávání cílit nejen na problematiku rizik spojených využíváním ICT a pohybem v kyberprostoru, problematiku jednotlivých forem kyberkriminality, ale mělo by také cílit na preventivní opatření, řešení nastalých situací a výčet kontaktů a institucí, na které se v případě problémů obrátit.

Doporučený způsob vzdělávání:

Zde se jeví optimální identický způsob vzdělávání, jako u cílové skupiny sociálních pracovníků a pomáhajících profesionálů.

Doporučené vzdělávací nástroje:

Pro vzdělávání této cílové skupiny lze použít stejné nástroje jako u předchozích dvou včetně zpřístupnění informačních zdrojů a kontaktů z oblasti KB. Zároveň je doporučeno vzájemné bližší povědomí a aktivní udržování kontaktů mezi všemi těmito třemi cílovými skupinami.

h) RODIČE

Zdůvodnění cílové skupiny:

Rodiče jsou primárně odpovědní za výchovu svých dětí. Rodina poskytuje modely chování, které dítě napodobuje a s kterými se identifikuje. Je také zprostředkovatelem sociální interakce a komunikace a seznamuje dítě se zažitými společenskými normami. Nedílnou součástí výchovy by v současnosti měla tvořit i osvěta v oblasti KB včetně toho, jak se na internetu chovat a komunikovat (např. využívání sociálních sítí v běžném životě).

Doporučený způsob vzdělávání:

Vzdělávání a osvěta rodičů je závislá na jejich vlastní iniciativě, například zapojení se do veřejně dostupných e-learningových kurzů. Na tyto kurzy a další možnosti by měli rodiče upozorňovat učitelé (ZŠ, SŠ, MŠ). V současné době narůstají snahy o posílení vazeb mezi školami a rodiči. Doporučují se společné aktivity pro děti a rodiče iniciované školou.

Doporučené vzdělávací nástroje:

Pro potřeby vzdělávání je vhodné využít e-learningové kurzy, vzdělávací a osvětové semináře a kurzy pro rodiče (vedené osvětovými organizacemi), kampaně cílené na osvětu rodičů (rádio, televize, internet), interaktivní semináře, dílny, „tematická odpoledne pro rodiče s dětmi“. Další možností jsou informační materiály pro rodiče i do škol (např. příručky, desatero, doporučení).

i) SENIOŘI

Zdůvodnění cílové skupiny:

Senioři se stále častěji stávají obětí trestných činů v podobě internetových podvodů (tzv. „kyberšmejdi“). Vzhledem k stále rozšířenějšímu používání ICT prostředků všemi věkovými skupinami a značně omezeným znalostem ICT, je tato skupina velmi zranitelná, a proto je třeba ji seznámit s bezpečným používáním nástrojů ICT i online komunikace. Jako velmi vhodné se jeví jim maximálně srozumitelným způsobem sdělit, na co si dát pozor a jakým způsobem se chránit.

Doporučený způsob vzdělávání:

Při vzdělávání této cílové skupiny se nejlépe jeví spolupráce s PČR, MP/ OP, odbornými a zájmovými sdruženími, osvětovými organizacemi a institucemi zaměřenými na práci se seniory. Další možností jsou vzdělávací „webové stránky“. Seniors lze zároveň vzdělávat i prostřednictvím interaktivnějších forem například v rámci škol či odborných a zájmových sdružení jejich vnoučat. Podpora integračních mezigeneračních a obdobných projektů (např. peer programy typu „vnuk učí své prarodiče“), které přinášejí pozitivní didaktický i sociální efekt.

Aktivnějším seniorům lze nabídnout variantu v podobě vzdělávacích modulů „Univerzity třetího věku“, kde by problematika kybernetické bezpečnosti byla zahrnuta v rámci určitého modulu (takovou výuku již poskytuje např. Univerzita Palackého v Olomouci).

Doporučené vzdělávací nástroje:

Doporučované vzdělávací nástroje jsou semináře a workshopy, e-learning, kampaně, help line specializovaná na pomoc seniorům. Integrační peer programy např. v rámci škol či odborných a zájmových sdružení. Jako podpůrné doplňkové materiály lze opět využít e-learningovou výuku a osvětový portál GovCERT.CZ.

j) ŠIROKÁ VEŘEJNOST

Zdůvodnění cílové skupiny:

ICT jsou stále více využívány prakticky všemi občany ČR, kteří nejsou ve většině případů obeznámeni s jejich bezpečným a etickým užíváním, nebo mají tendenci jej podceňovat. Je třeba je upozornit na reálná rizika, dbát na osvojení základních obecně platných preventivních opatření a současně s tím jim nabídnout možnosti řešení v případě, že již došlo ke zneužití ICT.

Doporučený způsob vzdělávání:

Doporučuje se spolupráce s PČR a osvětovými organizacemi, odborná a zájmová sdružení, osvětový portál GovCERT.CZ. Využít lze veřejné knihovny a infocentra. I zde je vítána živá účast na výukových mezigeneračních projektech, kdy se např. rodiče interaktivně učí společně se svými dětmi.

Doporučené vzdělávací nástroje:

Pro potřeby vzdělávání se doporučují semináře, workshopy a kampaně – zejména mediální. Jako podpůrné doplňkové materiály lze využít e-learningovou výuku a osvětový portál GovCERT.CZ.

2. SPECIFICKÉ VZDĚLÁVÁNÍ

Část věnující se specifickému vzdělávání pokrývá subjekty KII a VIS, akademickou sféru, veřejnou správu a soukromý sektor. Téma KII a VIS s odkazem na aplikaci ZKB se prolíná napříč většinou cílových skupin. Zde je třeba vedle klasické osvěty, určené převážně pro běžné uživatele, se věnovat problematice kybernetické bezpečnosti, s ohledem na široké spektrum úrovní odbornosti a potřeb, hlouběji. Stejně jako část obecná i tato následuje NSKB a odráží konkrétní body akčního plánu.

Vzdělávání na vysokých školách by opět mělo vycházet z již uvedeného cíle dokumentu Evropa 2020. Vzdělávání ve veřejné správě²⁰ koresponduje s vybranými body strategie MPSV. Sektor veřejné správy je rovnou konkretizován do cílových skupin, přičemž vzdělávání příslušníků Armády ČR, Policie ČR a státních zástupců/soudců je vzhledem k rozsáhlosti a speciálním potřebám těchto složek dále vyčleněno na samostatné cílové skupiny. Zde je především nutno udržet soulad s organizací jejich vlastních koncepčních materiálů a při komunikaci dodržet standardní postup, stanovený jimi nadřizenými organizačními složkami státu. Ke zvyšování vzdělanosti zaměstnanců veřejné správy v oblasti kybernetické bezpečnosti přispějí moderní výukové metody, jakými jsou například interaktivní přístup a využívání multimediálních či online nástrojů při vlastní výuce²¹.

Definované cílové skupiny:

- a) Správci KII a VIS
- b) Vysoké školy /akademická sféra
- c) Veřejná správa
- d) Policie ČR
- e) Armáda ČR
- f) Státní zástupci /soudci
- g) Soukromý sektor
- h) Pracoviště typu CERT a CSIRT (operátoři, analytici, specialisté)
- i) Administrátoři a bezpečnostní správci systémů a sítí

²⁰ AP – úkol F.3.01, F.3.02

²¹ AP – úkol F.304

a) SPRÁVCI KII A VIS

Zajišťování bezpečnosti subjektů kritické informační infrastruktury (dále jen „KII“) a významných informačních systémů (dále jen „VIS“) patří mezi hlavní priority všech vyspělých států. Téma KII a VIS se prolíná napříč většinou dále uváděných cílových skupin, z důvodu jeho významnosti však bylo určeno samostatně.

Vzhledem k existenci zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který mimo jiné reguluje i tzv. správce KII a VIS, vyžaduje tato cílová skupina zcela individuální přístup. Správcem tzv. prvku KII může být soukromoprávní nebo veřejnoprávní subjekt, správcem VIS může být pouze orgán veřejné moci. Prvek KII může být tvořen informačními systémy, komunikačními systémy nebo jejich kombinací. Zajištění bezpečnosti těchto informačních a komunikačních systémů je tedy zcela klíčové, neboť Jedná se například o informační systémy obsahující důležité databáze včetně osobních údajů obyvatel ČR či průmyslové kontrolní systémy elektráren, přepravních tras důležitých surovin, dopravní infrastruktury a další. Nedostatečné zabezpečení může mnohdy způsobit závažné dopady nejen na obyvatelstvo, ale i na životní prostředí.

Ochrana KII a VIS, včetně povinností správců KII a VIS, vyplývá ze ZKB, je potvrzena v NSKB a Akční plán k této Strategii přímo ukládá jednotlivé úkoly, které musí být naplněny. Vzdělávání v této oblasti je jedním z nich.

Zdůvodnění cílové skupiny

V rámci této cílové skupiny se jedná o důležité informační a komunikační systémy státu a soukromých subjektů, kde narušení jejich ICT bezpečnosti může mít zásadní dopad nejen na samotnou organizaci, ale i na stát. Případný kybernetický útok, nebo závažný kybernetický incident způsobený nedostatečně vzdělaným zaměstnancem, pak může mít za následek ohrožení zdraví a života obyvatel, ohrožení bezpečnosti státu, základních životních potřeb, ekonomiky, potažmo veřejného zájmu.

Cílová skupina zahrnuje zejména zákonem stanovené bezpečnostní role (*výbor pro řízení KB, manažery KB, auditory KB, garanty aktiv, architektury KB*), pracovníky ICT (*CIO, administrátoři, architekti, ISMS specialisté*), ale také bezpečnostní manažery a pracovníky úseku bezpečnosti, běžné uživatele a dále pak také dodavatele systémových řešení, kteří s konkrétními systémy KII a VIS přicházejí do styku. Povinnosti jednotlivých rolí (např. IS KII, KS KII a VIS) přímo stanovuje ZKB. Aby byly osoby zastávající tyto role požadované povinnosti naplňovat, musí mít co nejpřesnější a nejaktuálnější znalosti, musí umět vzájemně kooperovat.

Doporučený způsob vzdělávání

Vzdělávání bude probíhat za podpory NCKB především z pozice metodické podpory a odborného garanta v rámci problematiky KB. Rovněž tak je možná varianta různých školení příslušných specializovaných organizací či agentur (včetně agentur EU).

Doporučené vzdělávací nástroje

Zejména interaktivní metody, kybernetická cvičení a simulace. Pravidelná školení, přednášky, konference, semináře, workshopy, tabletopy, e-learning, kurzy v rámci celoživotního vzdělávání, osvětový portál GovCERT.CZ.

Přínos a praktický vstup NCKB

- tvorba a poskytování podpůrných materiálů a metodik, včetně standardů a osvědčených postupů pro zvládání kybernetických bezpečnostních rizik²²
- styčný bod pro komunikaci s příslušnými kontaktními osobami v rámci veřejné správy i soukromoprávních subjektů
- poskytování konzultací a předávání nejaktuálnějších zásadních informací (*pro subjekty KII/VIS nezbytnost znalosti mezinárodní situace a průběžné sledování trendů v této oblasti*),
- zajišťování kybernetických cvičení, tvorba workshopů, pořádání seminářů, přednášek, konferencí,
- osvětový portál GovCERT.CZ.

Přímo zainteresované subjekty spolupracující s NCKB

Relevantní resorty státní správy dle specifik (MVČR, MOČR atd.), akademická sféra a její vědecká pracoviště (tuzemská i zahraniční), expertní agentury, organizace či konsorcia (působící například v oblasti bezpečnosti sítí, analýzy rizik).

Vzdělávání jednotlivých bezpečnostních rolí v rámci cílové skupiny

V rámci cílové skupiny (správců KII a VIS) jsou zákonem o kybernetické bezpečnosti a jeho prováděcím právním předpisem (vyhláškou o kybernetické bezpečnosti) definovány tzv. bezpečnostní role, jejich práva a povinnosti. Tyto role jsou zmíněny níže.

i. Výbor pro řízení kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti definuje výbor pro řízení kybernetické bezpečnosti, jako organizovanou skupinu tvořenou osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.

Vzdělávání této cílové skupiny (členů výboru) bude zaměřeno především na management (řízení) a jeho obory, např. na projektový management a zejm. na management kybernetické bezpečnosti v jednotlivých organizacích.

ii. Manažeři kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti říká, že manažer kybernetické bezpečnosti je osoba, odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost vyškolená a **prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let.**

Vzdělání této cílové skupiny bude zaměřeno především na problematiku ISMS (zejm. na řadu norem ISO/IEC 27 000) a na relevantní standardy, opomenuto nebude ani na oblasti managementu, projektového managementu a práva v oblasti ICT.

²² AP – úkol C.1.02, C.3.02

iii. Auditoři kybernetické bezpečnosti

Podle vyhlášky o kybernetické bezpečnosti, je auditor kybernetické bezpečnosti osoba provádějící audit kybernetické bezpečnosti, která je pro tuto činnost vyškolená a **prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let**. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a garanta kybernetické bezpečnosti.

Vzdělávání této cílové skupiny se zaměří na znalosti auditu kybernetické bezpečnosti, dále na oblast managementu a práva v oblasti ICT.

iv. Architekti kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti říká, že architekt kybernetické bezpečnosti je osoba zajišťující návrh a implementaci bezpečnostních opatření, která je pro tuto činnost vyškolená a **prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let**.

Vzdělávání této role se zaměří na návrh a implementaci jednotlivých bezpečnostních opatření (organizačních, technických). Přesné vymezení oboru vzdělávání je u této cílové skupiny velmi náročné, neboť se liší specializací organizace, danou technologií apod.

v. Garant aktiva

Vyhláškou o kybernetické bezpečnosti je garant aktiva osoba, určená k zajištění rozvoje, použití a bezpečnosti aktiva.

Vzdělávání této cílové skupiny je závislé od funkce a technologie konkrétního aktiva.

b) VYSOKÉ ŠKOLY / AKADEMICKÁ SFÉRA

Zdůvodnění cílové skupiny

Vysoké školy a akademická sféra jsou zvláště podstatnou cílovou skupinou, jelikož právě akademická půda má za cíl produkovat budoucí odborníky a jejím posláním by mělo být poskytnout svým studentům i pedagogům maximálně erudované zázemí, o které se budou moci opřít v další profesní kariéře i praxi. Pouze prostřednictvím kvalitního zázemí, nejmodernějších přístupů a širokého spektra možností i informačních zdrojů lze podporovat a stimulovat talent²³ studentů, který posléze může vyústit v zásadní praktický přínos. Úspěch jedince zde tak může znamenat prestiž pro příslušnou vzdělávací instituci, potažmo i pro Českou republiku jako celek.

V případě technických oborů je technický aspekt kybernetické bezpečnosti včetně hlubší orientace v této problematice nezbytností a to například i ve strojních či stavebních oborech neboť i tyto již v současné době využívají ke své činnosti sofistikované prostředky ICT.

Pro netechnické obory je KB důležitá například z hlediska právně-legislativního, bezpečnostně strategického či pedagogického a dalších. Zde bude vzdělávání přesně cílit na jednotlivá zaměření. Na jejich základě pak budou vytvořeny vzdělávací osnovy i obsahové stránky sylabů a například i zcela nové předměty či celé obory²⁴.

Pro ucelený přehled stavu vysokoškolského vzdělávání je v první řadě třeba vytvořit kompletní přehled nabízených vysokoškolských programů a oborů zahrnujících téma KB a to u nás i v zahraničí²⁵.

Doporučený způsob vzdělávání

Zapojení učitelů ve spolupráci s pracovníky NCKB, živé vstupy pracovníků NCKB v podobě přednáškové činnosti na akademických institucích. Zapojení projektu C4E, který působí pod Masarykovou univerzitou, a který má personální kapacity a zájem školit a tvořit vzdělávací materiály. C4E může poskytnout prostory k uspořádání školení, kurzů, konferencí a různých osvětových přednášek. Zapojení klíčových partnerů, agentur EU a zahraničních vzdělávacích institucí.

Doporučené vzdělávací nástroje

Přednášky, semináře, prezentace, konference, konzultace, workshopy, tabletop, odborné stáže, e-learning a webináře s certifikátem nebo kreditovou hodnotou pro ukončení předmětu, kvalifikační práce vedené nebo oponované bezpečnostními specialisty z veřejné správy nebo ICT komunity, osvětový portál GovCERT.CZ. Zejména k některým nástrojům bude velmi doporučována forma videokonferencí, webinářů a dalších online aktivit.

²³ AP – úkol F.2.06

²⁴ AP – úkol F.2.08

²⁵ AP – úkol F.2.04

Přínos a praktický vstup NCKB

- NBÚ jakožto odborný garant pro kybernetickou bezpečnost bude hlavní kontaktní institucí pro vysoké školy – pracovníci NCKB vytvoří kontaktní list a komunikační matici s VŠ;
- ve spolupráci s vysokými školami (potažmo MŠMT, NCBI, NÚV atd.) bude vytvořen kompletní přehled oborů či předmětů zabývajících se KB, které jsou v současné době poskytovány v ČR i zahraničí s odkazem na instituci, která dané vzdělávání poskytuje;
- ve spolupráci s výše uvedenými subjekty budou vytvářeny sylaby a přednášky;
- pracovníci NCKB budou poskytovat konzultace k jednotlivým předmětům a vystupovat na vybraných přednáškách v roli přednášejících;
- pracovníci NCKB povedou, budou konzultovat a oponovat vysokoškolské kvalifikační²⁶ práce a projekty v rámci studentské odborné činnosti,
- pracovníci NCKB budou doporučovat literaturu a informační zdroje z ČR i zahraničí;
- pracovníci NCKB budou přispívat svými články do akademických sborníků či odborných publikací;
- NCKB bude poskytovat odborné stáže (pro učitele i pro studenty) a zprostředkovávat stáže v předních organizacích na území ČR i v zahraničí²⁷;
- ve spolupráci s vysokými školami se bude NCKB podílet na přípravě a organizaci odborných konferencí, případně poskytnout oficiální záštitu;
- NCKB bude provozovat osvětový portál GovCERT.CZ.

Přímo zainteresované subjekty spolupracující s NCKB

MŠMT/NÚV, CZ.NIC, CESNET, C4E, styční pracovníci příslušných vysokých škol a jednotlivých fakult.

²⁶ Bakalářské a diplomové.

²⁷ AP – úkol F.2.07

c) VEŘEJNÁ SPRÁVA

Zdůvodnění cílové skupiny

Převážná většina zaměstnanců veřejné správy pro výkon své činnosti využívá takové prostředky ICT, u kterých je ve většině případů znalost bezpečnostních pravidel nezbytná. S novými technologiemi a z nich plynoucími možnými riziky narůstá i potřeba osvěty a odbornějšího vzdělávání, načež pokrývá oblast od běžných uživatelů až například po manažery kybernetické bezpečnosti.

Na základě pracovního zaměření jednotlivých skupin zaměstnanců veřejné správy budou rozděleny úrovně a směr vzdělávání. Některé činnosti vyžadují podstatně sofistikovanější přístup k využívání ICT a praktikování pravidel kybernetické bezpečnosti (např. potřebnou znalostí manažerů kybernetické bezpečnosti je umět rozpoznávat a detekovat anomálie včetně znalosti přesného postupu v případě kybernetického bezpečnostního incidentu – v tomto je důkladné školení zásadní)²⁸.

I zaměstnanci NBÚ, coby součást veřejné správy, potřebují pravidelně udržovat aktuální povědomí o kybernetické bezpečnosti. Zaměstnanci NBÚ budou v rámci profesního vzdělávání v pravidelných intervalech školeni svými kolegy z NCKB.

Pracovníci NCKB navíc v souvislosti se zajišťováním a posilováním kybernetické bezpečnosti ochranou kybernetického prostoru koordinují a spoluzodpovídají za naplňování NSKB a plnění úkolů stanovených Akčním plánem. Tyto úkoly pokrývají strategicko-politickou i technickou rovinu a jejich co nejefektivnější plnění vyžaduje neustálé sebevzdělávání se²⁹.

Doporučený způsob vzdělávání

Prostřednictvím aktivit institucí zabývajících se vzděláváním veřejné správy s podporou NCKB (poskytnutí podkladů, metodik, e-learning, apod.) a též v rámci interních vzdělávacích procesů jednotlivých složek veřejné správy, čímž jsou myšlena například pravidelná školení k aktualizaci znalostí prováděna příslušnými vedoucími pracovníky přímo na pracovišti. Jako další spolupracující školicí středisko by bylo možné využít i C4E pod MU. Dále lze ve vybraných případech využít i ustanovení zákona č. 234/2014 Sb., o státní službě a v rámci úřednické zkoušky státního zaměstnance preferovat i přehled v oblasti ICT.

Pracovníky NCKB je třeba školit prostřednictvím nejrůznějších tuzemských i zahraničních vzdělávacích aktivit a stáží v příslušných specializovaných agenturách, organizacích a institucích³⁰. Tito budou vystupovat rovněž i jako přednášející, poskytovat prezentace na odborných konferencích a účastnit se diskusních panelů v ČR i v zahraničí. NCKB bude mimo výše uvedené i koordinačním bodem a zprostředkovatelem specializovaných školení tuzemských a zahraničních vzdělávacích aktivit (semináře, školení, cvičení kybernetické bezpečnosti apod.) v oblasti KB.

²⁸ AP – úkol F3.02

²⁹ AP – úkol C.6.01

³⁰ AP – úkol C.6.02

Doporučené vzdělávací nástroje

Primárním zdrojem vzdělávání této cílové skupiny budou především e-learningové kurzy a další online aktivity jako jsou například videokonference, webináře, aktivní využívání osvětového portálu GovCERT.CZ apod. Ty budou podrobně rozčleněny na různá zaměření i úrovně a jejich zdárné absolvování bude ukončeno osvědčením či potvrzením od zaměstnavatele³¹, které bude oficiálně uznávaným dokladem (doklad dalšího odborného vzdělání). Dále budou využívány například klasické konference a semináře, odborná setkání, workshopy s praktickým zaměřením na prevenci KB, využívání prostředků ICT v podmínkách veřejné správy či tabletop. Výše jmenované nástroje budou aplikovány v rámci celoživotního vzdělávání a vzdělávání státních zaměstnanců. V případě zaměstnanců pracujících ve strategické či bezpečnostní oblasti je zde možnost různých kybernetických cvičení.

Přínos a praktický vstup NCKB

- tvorba e-learningových a online aktivit pro vzdělávání jednotlivých skupin
- metodická podpora při tvorbě vzdělávacích cyklů a programů s možností lektorské činnosti
- metodická podpora interních školení a e-learningových programů
- metodická podpora školení vedoucích, zejména ICT pracovníků
- osvětový portál GovCERT.CZ

Přímo zainteresované subjekty spolupracující s NCKB

MPSV, ostatní organizační složky státu zabývající se veškerými aspekty kybernetické bezpečnosti, instituce zabývající se vzděláváním veřejné správy, vybrané části akademické sféry (tuzemské i zahraniční), vzdělávací složky jednotlivých resortů či institucí - styční pracovníci veřejné správy, osvětové a odborné organizace či konsorcia (tuzemské i zahraniční).

³¹ AP – úkol F3.03

d) POLICIE ČR

Zdůvodnění cílové skupiny

V současné době pracují s nejrůznějšími prostředky ICT na různých úrovních téměř všechny složky Policie ČR. Policie ČR pokrývá široký záběr vztahů k ICT z metodického i praktického hlediska od běžných uživatelů využívajících ICT prostředky ke své administrativní činnosti, příslušníků/pracovníků preventivně-informačních odborů/oddělení, příslušníků odborů obecné kriminality, potažmo mravnostních oddělení, manažerů bezpečnosti, správců sítí až po specializované útvary zabývající se přímo odhalováním, vyšetřováním a postihováním trestné činnosti či organizovaného zločinu spojeného s kybernetickou kriminalitou. Zvláštní skupinu tvoří zaměstnanci Kriminalistického ústavu Praha a krajských odborů kriminalistických technických expertíz, které jsou expertní podpůrnou složkou PČR z hlediska analýz zajištěných důkazů. Z uvedeného plyne, že i vzdělávání PČR je třeba provádět na několika úrovních dle zaměření a stupně odbornosti.

Vzdělávání Policie ČR v oblasti KB je důležité z hlediska společensko-osvětově-informativního (community policing), bezpečnostního, technického i legislativního - a to pro obecnou prevenci i pro vlastní postihování. Z tohoto důvodu je nezbytné problematiku KB reflektovat v rámcových vzdělávacích programech a plně ji zapojit nejen do výuky ve specializačních kurzech, ale již do výuky v rámci základní odborné přípravy příslušníků Policie ČR. Policisté ve všech úrovních služby musí disponovat základními znalostmi problematiky kybernetické bezpečnosti. Dále pak podle požadovaného stupně odbornosti souvisejícího s výkonem jejich služby mnozí z nich i širšími tak, aby tyto znalosti a dovednosti odpovídaly současným potřebám, včetně znalosti nejnovějších hrozeb a způsobu jak jim čelit. U příslušníků vyčleněných pro boj s kybernetickou kriminalitou je pro efektivní odhalování a vyšetřování tohoto typu trestné činnosti/organizovaného zločinu navíc stěžejní adekvátní technické vybavení³² a důkladná znalost práce s těmito prostředky.

Podstatnou částí kvalitního policejního vzdělávání je i sledování a znalost světových trendů v oblasti kybernetické bezpečnosti a kybernetické kriminality. K tomuto je nepostradatelná živá mezinárodní spolupráce, která je mj. schopna zprostředkovat a zajistit kontinuální expertní vzdělávání na mezinárodní úrovni včetně pravidelných školení českých policistů/policejních důstojníků v mezinárodních organizacích. Mezinárodní policejní vzdělávání prospěšné i pro tak důležité vytváření a utužování sítě kontaktů, která může zásadně pomoci již např. v rámci konkrétních vyšetřování.

Doporučený způsob vzdělávání

Prostřednictvím vlastního resortního vzdělávání, zejména v rámci PA ČR či policejních škol. Podpůrně lze příslušníky PČR vzdělávat rovněž i prostřednictvím NCKB (poskytne zejména podklady a metodické materiály, dílčí expertní školení atd.). Dále prostřednictvím akademické sféry a osvětových organizací. Na mezinárodní úrovni např. prostřednictvím aktivit CEPOL, MEPA, George C. Marshall European Center for Security Studies, Eurojust, ENISA, ENFSI, 2Centre, ECTEG apod. Pro nejužší část policejních odborníků mohou být velmi přínosné aktivity či stáže v rámci INTERPOL a EUROPOL (např. EC3 - European Cybercrime Centre of Excellence).

³² Podpůrný aspekt NBÚ k AP – úkolům G.2.01, G.2.02

Doporučené vzdělávací nástroje

Kurzy základní odborné přípravy a specializační kurzy, kurzy celoživotního vzdělávání i online formou v podobě konferencí, přednášek, workshopů, tabletopů, e-learningu, webinářů, osvětový portál GovCERT.CZ, mezinárodní vzdělávací aktivity, praktické stáže. Interaktivní výuka prostřednictvím modelových situací či simulací. V případě příslušníků vykonávajících svou činnost na strategicko-rozhodovacích nebo technických pozicích lze tyto vzdělávat i prostřednictvím národních i mezinárodních kybernetických cvičení.

Přínos a praktický vstup NCKB

- kontaktní bod pro podporu vytvoření sítě provázanosti PČR s akademickým prostředím³³
- styčný bod pro spolupráci s odbory vzdělávání MV ČR a PP ČR (potažmo resortními vzdělávacími zařízeními) – podpora při tvorbě metodik a obsahové stránky vzdělávacích aktivit³⁴
- podpora tvorby osvětových materiálů PČR
- školení vybraných útvarů PČR přímo zaměstnanci NCKB a poskytování krátkodobých odborných stáží vybraným příslušníkům PČR
- doporučování stáží příslušníků PČR v dalších organizacích
- osvětový portál GovCERT.CZ

Přímo zainteresované subjekty spolupracující s NCKB

MVČR/PPČR, MPSV, MSp, (potažmo státní zástupci/soudci, osvětové organizace, agentury a konsorcia, jako např. C4E (tuzemské i zahraniční), vybrané části akademické sféry a jejich vědecká pracoviště (dle specializace – převážně technici, právníci, bezpečnostní experti), CZ.NIC, apod.

³³ podpůrný aspekt NBÚ k AP – úkolu G.6.01

³⁴ Podpůrný aspekt NBÚ k AP – úkolům G.5.01, G. 5.02, G 5.03

e) ARMÁDA ČR

Zdůvodnění cílové skupiny

Armáda je stěžejní složkou obranyschopnosti a suverenity státu. Vzhledem ke vzrůstajícímu využívání informačních a komunikačních technologií ve všech oblastech lidského působení mají ICT dnes již i podobu zbraní, které mohou být zneužity ke kybernetickým útokům. Kybernetický útok s sebou může přinést zásadní dopad na ekonomiku a základní fungování státu i jeho infrastrukturu, čímž jej může přímo i nepřímo vážně ohrozit. Zajištění kybernetické bezpečnosti a obrany České republiky je proto jedním ze strategických zájmů státu.

Případy kybernetických útoků se zvyšují a s nimi i jejich sofistikovanost a je tedy nutná adekvátní připravenost jím čelit. Proto je třeba vzdělávání Armády ČR věnovat obzvláště patřičnou pozornost a v maximální možné míře spolupracovat na posilování KB jako součásti obranyschopnosti České republiky. V poslední době dochází k významnému nárůstu vojenských kapacit některých států, včetně ofenzivních kybernetických prostředků, proto přestává být samotná defenziva postačující a nejen v rámci mezinárodního fungování je vyžadován průběžný nácvik ofenzivy. Ve vyspělých zemích je tento trénink připravenosti zcela běžný. Defenzivně - ofenzivní aspekt je tedy praktickým markantem pojetí zajišťování KB prostřednictvím ozbrojených sil a pravidelné vzdělávání, školení a cvičení jsou základem pro připravenost.

Tato cílová skupina má organizačně obdobné schéma jako Policie ČR a tedy i rozsah oblastí vzdělávání Armády ČR včetně nezbytnosti mezinárodní spolupráce bude veden v podobném duchu (tzn. od běžného uživatele až po experty přímo zajišťující strategickou obranu). Rovněž tak postup komunikační matice bude probíhat analogicky jako u Policie ČR. Základy kybernetické bezpečnosti je i zde třeba zapojit do školských a rámcových vzdělávacích programů již v rámci základního vojenského výcviku. Technické a strategické specialisty je zapotřebí neustále vzdělávat prostřednictvím nejnovějších poznatků a techniky, kde nejúčinnějšími metodami jsou praktické simulace a nejrůznější kybernetická cvičení.

Konkrétní podoba i obsah vzdělávání budou tedy zohledněny ve vztahu k potřebám jednotlivých složek Armády ČR a dimenzovány dle jejich zaměření i úrovně odbornosti. Význam aktivní mezinárodní spolupráce ve sféře vzdělávání spočívá zejména v aktivním zapojení v rámci NATO, EU a V4.

Doporučený způsob vzdělávání

Prostřednictvím vlastního resortního vzdělávání, kde nejodbornější část vzdělávání může zaštitit Centrum CIRC MO a Univerzita obrany. Podpůrně rovněž prostřednictvím NCKB (NCKB poskytne podklady a metodické materiály), akademické sféry, osvětových organizací a agentur EU jako je např. EDA a ENISA. V případě příslušníků ze strategických a technických pozic se jednoznačně doporučují interaktivní metody, jako jsou kybernetická cvičení a praktické simulace. Na mezinárodní úrovni se jedná zejména o vzdělávací programy pořádané NATO, George C. Marshall European Center for Security Studies apod. Nutnou podmínkou je neustálé sledování nejnovějších trendů v ICT, což znamená rychlou reakci v požírování těchto vyspělých technologií z důvodu seznamování se s nimi a z důvodu jejich využívání pro zabezpečení spravovaného kyberprostoru.

Doporučené vzdělávací nástroje

Kurzy základní vojenské přípravy, specializační a kvalifikační kurzy, kurzy celoživotního vzdělávání i online v podobě konferencí, přednášek, workshopů, tabletopů, e-learningu, webinářů, osvětový portál GovCERT.CZ, praktické stáže, aktivní účast na kybernetických cvičeních.

Přínos a praktický vstup NCKB

- kontaktní bod pro podporu vytvoření sítě provázanosti AČR s akademickým prostředím
- styčný bod pro spolupráci s gestorem KB rezortu MO, odbory vzdělávání MO a GŠ AČR a resortními vzdělávacími zařízeními – podpora při tvorbě metodik a obsahové stránky vzdělávacích aktivit
- styčný bod pro spolupráci s Centrem CIRC MO
- školení vybraných útvarů AČR přímo zaměstnanci NCKB a poskytování odborných krátkodobých stáží vybraným příslušníkům AČR
- doporučování stáží příslušníků AČR v dalších organizacích
- podpora a aktivní spolupráce při kybernetických cvičeních
- školení vybraných útvarů AČR přímo zaměstnanci NCKB
- osvětový portál GovCERT.CZ

Přímo zainteresované subjekty spolupracující s NCKB

MOČR/GŠ AČR, MPSV, CZ.NIC, osvětové organizace, agentury a konsorcia (tuzemské i zahraniční), vybraná část akademické sféry a jejich vědecká zázemí (dle specializace – převážně technici, právníci).

f) STÁTNÍ ZÁSTUPCI/SOUDCI

Zdůvodnění cílové skupiny

Kybernetické prostředí se stává stále pevnější součástí celé společnosti. V této souvislosti se v kyberprostoru odehrává i celá řada právem upravených jednání a událostí. Je proto nutné, aby byl právní řád aplikován institucemi zabývající se ochranou a vymáháním práva s ohledem na jeho specifika. Zejména státní zástupci a soudci, jakožto osoby závislé na správném výkladu a aplikaci právních norem na reálný stav společnosti pro řádný výkon své činnosti, musí disponovat základními informacemi o kybernetickém prostředí, jeho možnostech, bezpečnosti a aktuálních problémech.

Státní zástupci a soudci se ve své praxi dostávají do kontaktu s kybernetickým prostředím stále více a jejich rozhodovací a jiná činnost může být na znalosti problematiky kybernetického prostředí závislá. Aby byli schopni při své práci obsáhnout specifika kybernetického prostoru a posléze s ním dále pracovat tak, aby byla zachována profesionalita a další požadavky kladené na jejich funkce, je nutno se jejich vzdělávání v oblasti kybernetického prostředí zaměřit³⁵. Nutnost vzdělávání soudců a státních zástupců pro řádný výkon jejich funkce i v této oblasti lze dovozovat z požadavku profesionality jejich funkce stanovených v § 82 zákona č. 6/2002 Sb., o soudech a soudcích, respektive v § 24 odst. 3 zákona č. 283/1993 Sb., o státním zastupitelství. Potřebu dalšího vzdělávání zdůrazňují například i dokumenty Rady Evropy³⁶.

Vzdělávání státních zástupců a soudců by se mělo uskutečňovat zejména s přesahem do základních technických specifik, a to zvláště v bodu prolnutí problematiky kybernetické bezpečnosti s kybernetickou kriminalitou (zaměření na důkazní prostředky v kyberprostoru), ale též i v obecných oblastech fungování počítačů a sítí, současných problémech a výzvách kybernetické bezpečnosti a dopadu možných kybernetických hrozeb na společnost.

Doporučený způsob vzdělávání

Pilířem je poskytnutí kvalitního základu znalosti problematiky kybernetické bezpečnosti, potažmo kybernetické kriminality již v rámci vysokoškolského vzdělávání. Pro zajištění vzdělání současných soudců a státních zástupců, jakožto pro udržování profesionality výkonu jejich funkce je pak předpokládáno i vzdělávání čekatelského a při výkonu funkce. Vzdělávat tuto cílovou skupinu je vhodné prostřednictvím akademické sféry a resortu spravedlnosti, za spolupráce NCKB a vědeckých institucí zabývajících se ICT a právem, dále pak zejména u mezinárodních osvětových organizací, institucí a agentur EU vzdělávající orgány činnými v trestním řízení jako jsou např. Eurojust, CEPOL, EUROPOL apod.).

Doporučené vzdělávací nástroje

Aktivity v rámci vysokoškolského vzdělání (tvorba osnov, studijních programů, speciálně zaměřených kurzů či zapojení této problematiky do již existujících kurzů), čekatelského vzdělání a vzdělávání při výkonu funkce (konference, přednášky, školení, workshopy, tabletop cvičení, e-learning, webináře, osvětový portál GovCERT.CZ, praktické stáže, další formy celoživotního vzdělávání a to i online formou).

³⁵ AP – úkol H.4.01

³⁶ Pro více informací viz

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/default_en.asp

Přínos a praktický vstup NCKB

- styčný bod pro spolupráci se subjekty zodpovědnými za resortní vzdělávání
- podpora při tvorbě metodik a obsahové stránky vzdělávacích aktivit
- školení soudců a státních zástupců přímo zaměstnanci NCKB a poskytování krátkodobých odborných stáží
- doporučování stáží státních zástupců a soudců v dalších relevantních organizacích
- osvětový portál GovCERT.CZ

Přímo zainteresované subjekty spolupracující s NCKB

MSp/Justiční akademie, PČR/PAČR, akademická sféra a vědecké instituce technického a právního zaměření (tuzemské i zahraniční), bezpečnostní týmy (tuzemské i zahraniční) osvětové organizace a agentury (tuzemské i zahraniční).

g) SOUKROMÝ SEKTOR

Zdůvodnění cílové skupiny

Potřeba dobré orientace v tématu KB je u této cílové skupiny velmi důležitá především z důvodu naplňování zákona o KB a navyšování povědomí u nepovinných soukromých subjektů se zaměřením na malé a středně velké podniky, které jsou páteří ekonomiky.

Spektrum ochrany firemních sítí je široké. Nejčastěji se může jednat například o identifikační údaje zaměstnanců, vnitřní organizaci, hospodaření a finanční stav firmy, ale například i o údaje o klientech, vlastní pracovní postupy či firemní tajemství a „know how“. Zachování diskrétnosti těchto informací i firemních tajemství má tedy nezpochybnitelný význam a její ztráta pak může mít vliv zejména na soukromí zaměstnanců, ekonomiku či prosperitu dané společnosti, potažmo ČR.

Zapojení ICT téměř do všech činností zaměstnanců soukromého sektoru, zvyšuje riziko ohrožení například v podobě internetových podvodů, krádeží identity a zneužívání různých druhů citlivých firemních informací (sociální inženýrství). Cílovou skupinu soukromého sektoru lze dále rozčlenit podle velikosti firem, počtu zaměstnanců, oboru činnosti a profesionálního zaměření (např. technická - ICT, ISP, bezpečnostní agentury, netechnická). Způsob, obsah a úroveň vzdělávání musí být opět stanoven adekvátně k jednotlivým profesním povahám a úrovním činností.

Doporučený způsob vzdělávání

Prostřednictvím NCKB ve spolupráci s příslušným úsekem nebo pověřenou osobou mající na starosti vzdělávání v dané společnosti. Dále pak prostřednictvím osvětových organizací a expertů z ICT.

Doporučené vzdělávací nástroje

Primárním zdrojem vzdělávání této cílové skupiny se doporučují, podobně jako u veřejného sektoru, především e-learningové kurzy a další online aktivity jako jsou například videokonference, webináře, aktivní využívání osvětového portálu GovCERT.CZ apod. Tyto aktivity by měly být podrobně rozčleněny na různá zaměření i úrovně a jejich zdárné absolvování bude ukončeno osvědčením či certifikátem od zaměstnavatele, popřípadě jiným dokladem, který bude oficiálně uznatelný (doklad dalšího odborného vzdělání). Rovněž budou využívány například klasické konference a semináře, workshopy či tabletop. Výše jmenované nástroje lze nejlépe aplikovat v rámci celoživotního vzdělávání. V případě zaměstnanců pracujících ve strategické či bezpečnostní oblasti je zde možnost i různých praktických simulací či kybernetických cvičení.

Přínos a praktický vstup NCKB

- zprostředkovávání kontaktů na osvětové organizace i expertní vzdělávací instituce z oblasti ICT, případně vytvoření kontaktního listu
- poskytování metodické podpory dle požadavků jednotlivých soukromých subjektů³⁷
- tvorba a podpora informačních kampaní ohledně KB dle konkrétních možností a potřeb soukromých subjektů³⁸
- spolupráce na tvorbě obsahové stránky vzdělávacích aktivit
- podpora vytváření interního e-learningového vzdělávacího systému
- osvětový portál GovCERT.CZ

Přímo zainteresované subjekty spolupracující s NCKB

MPSV, osvětové organizace, agentury a konsorcia (tuzemské i zahraniční), expertní vzdělávací instituce z oblasti ICT (tuzemské i zahraniční).

³⁷ AP – úkol D.4.01

³⁸ AP – úkol D.4.02

h) Pracoviště typu CERT a CSIRT (operátoři, analytici, specialisté)

Zdůvodnění cílové skupiny

Pracovníci bezpečnostních týmů jsou zodpovědní za zvládání, vyhodnocování a analyzování kybernetických hrozeb. Dále pak za koordinaci informací s dalšími týmy a příslušnými organizacemi. K tomuto účelu je nutné, aby měli specifické odborné vysokoškolské vzdělání a patřičný výcvik v oblasti zvládání incidentů. Pro již zavedené týmy je doporučeno udržovat dobré osobní vazby s členy tzv. bezpečnostní komunity tj. ostatních CERT, CSIRT týmů, akademické sféry, správců kritické informační infrastruktury a významných informačních systémů a dalších organizací, které se věnují oblasti kybernetické bezpečnosti.

Tito pracovníci musí disponovat co nejodbornějšími znalostmi a detailní znalostí světových trendů v oblasti kybernetické bezpečnosti. Prostřednictvím patřičných školení si tak neustále zvyšují svou odbornost a jsou tak schopni identifikovat nejnovější hrozby, analyzovat jejich příčiny a poskytovat řešení pro jejich eliminaci, čímž výrazně přispívají k posilování kybernetické bezpečnosti v ČR.

U všech pracovníků je nutné zvyšovat úroveň jejich vzdělání a poskytovat jim aktuální informace a kontakty, aby měli pro svoji práci ty nejlepší podmínky. Každý zaměstnanec by měl být zaměřen na zvládání jiného druhu hrozeb a incidentů. V rámci jednoho pracoviště by měla existovat zastupitelnost. Z toho vyplývá nutnost individuálního přístupu ke vzdělávání jak ze strany zaměstnance tak zaměstnavatele.

Pracovníky vládního CERT týmu je mimoto třeba vzdělávat i s ohledem na povinnosti vyplývající ze zákona o KB. Těmito jsou zejména poskytování metodické podpory a součinnosti orgánům či osobám, jimž byly výše uvedeným zákonem uloženy povinnosti v oblasti kybernetické bezpečnosti, přijímání hlášení o kybernetických bezpečnostních událostech a incidentech, jejich následné vyhodnocování či hodnocení zranitelností. Hodnocení vypracovaná NCKB jsou pak podkladem pro případná bezpečnostní opatření vydaná NBÚ. Zvláště podstatným bodem pro sebevzdělávání vládního CERT týmu je vlastní laboratorní zázemí³⁹.

Doporučený způsob vzdělávání

Pracovníky bezpečnostních týmů je doporučeno vzdělávat prostřednictvím všech existujících nástrojů volených s ohledem na povahu a konkrétní cíle vzdělávání. Velký význam je přikládán interaktivním metodám (např. praktická cvičení, simulace apod.) za využití všech zdrojů ICT technologií a ostatních multimediálních prostředků, v laboratorních a dalších specializovaných zázemích včetně vzájemné podpory jejich budování.

Nezbytným základem je zde akademická sféra zaměřená na výuku technických oborů, dále pak lze bezpečnostní týmy vzdělávat skrze odborníky pro nejrůznější specifické oblasti ICT, tuzemských i mezinárodních vzdělávacích institucí. Stěžejní je pravidelnost a kontinuita průběžného vzdělávání a doplňování aktuálních informací.

Protože je potřeba aktuální informace mezi jednotlivými týmy také sdílet, je velký důraz kladen na spolupráci veřejného a soukromého sektoru (Public Private Partnership). Pro zvýšenou efektivitu vzdělávání, potažmo výkon profese, je zejména přínosné pořádání a absolvování společných vzdělávacích aktivit dohromady s ostatními CERT/CSIRT týmy. Zvláště přidanou hodnotu má budování a udržování osobních kontaktů napříč těmito týmy. Právě tyto mají při jejich práci často klíčový význam.

³⁹ AP – úkol C.3.08

Doporučené vzdělávací nástroje

Expertní školení, přednášky, semináře, e-learningové kurzy, odborné kurzy v rámci celoživotního vzdělávání, osvětový portál GovCERT.CZ. Interaktivní metody s důrazem na praktický aspekt – řešení modelových situací, simulace, kybernetická bezpečnostní cvičení a semináře pořádané expertními národními, mezinárodními vládními i komerčními organizacemi (např. NATO CCDCOE). Z hlediska aktuálnosti informací je vhodná účast na odborných konferencích, a to jak v pozici posluchačů, tak přednášejících. Participace na odborných diskusních panelech a dalších setkáních formálního i neformálního charakteru.

Přínos a praktický vstup NCKB

- zprostředkovávání kontaktů na bezpečnostní týmy, expertní vzdělávací instituce a odborníky, vytvoření a zpřístupnění kontaktního listu
- vytváření a rozesílání tzv. newsletteru (informačního bulletinu, zveřejňování aktuálních informací na stránkách) v rámci bezpečnostní komunity s informacemi o aktuálním dění, aktuálních hrozbách a aktuálních vzdělávacích možnostech

Přímo zainteresované subjekty spolupracující s NCKB

Technická část akademické sféry a její vědecká pracoviště (tuzemská i zahraniční), technická část veřejné správy (NCKB, MOČR, MVČR/PČR) i soukromého sektoru, další CERT/CSIRT týmy – vzájemné vzdělávací aktivity. Na mezinárodní úrovni dále expertní centra, organizace a agentury např. NATO CCD COE, ENISA, Europol, EC3, C4E.

i) ICT ADMINISTRÁTOŘI

Zdůvodnění cílové skupiny

Každá organizace, která je složena z dílčích pracovišť, zaměstnává skupinu osob tvořící tým. Tyto týmy mají dnes veškerou svou agendu vedenu elektronicky, načež některé oblasti bývají propojeny a mohou vytvářet celé databáze fungující v rámci daných počítačových systémů. Obsahem zde zpravidla bývají informace pro interní použití daného týmu, což vyžaduje precizní zabezpečení. Za zajištění bezpečnosti systémů a sítí odpovídají jejich administrátoři a bezpečnostní správci.

Mimo obecných pravidel bezpečnosti, které by měli bez výjimky dodržovat všichni uživatelé (*a měli by v nich být pravidelně proškolení - viz provázanost s dalšími cílovými skupinami koncepce*), musí i samotná síť, potažmo systémy splňovat aktuální bezpečnostní kritéria k zajištění a udržení požadované ochrany.

Kvalitní, funkční a pravidelně aktualizované antivirové programy, firewally a jiné prvky ochrany jsou prvním krokem k zajištění bezpečnosti. Nutno však podotknout, že v celkové bezpečnostní architektuře jde jen o pouhý základ a problematika bezpečnosti systémů a sítí s sebou nese spoustu dalších sofistikovaných úkonů a navazujících odpovědností, které je třeba znát a provádět.

Administrátoři a bezpečnostní správci IS a KS jsou tedy neopominutelnou složkou bezpečnosti a vzhledem k úzké specifice jejich činnosti jsou v tomto dokumentu určeni jako samostatná cílová skupina vyžadující pravidelné odborné vzdělávání.

Doporučený způsob vzdělávání

Prostřednictvím CSIRT týmů, akademické sféry a nejrůznějších expertů a organizací z oblasti ICT. Prostřednictvím NCKB ve spolupráci s pověřenou osobou mající na starosti vzdělávání v daném útvaru. Vybraná, úzce specializovaná školení lze rovněž jednorázově poskytnout přímo pracovníky NCKB.

Doporučené vzdělávací nástroje

Odborná školení, přednášky, semináře, workshopy, e-learning, odborné kurzy v rámci celoživotního vzdělávání, osvětový portál GovCERT.CZ. Interaktivní metody s důrazem na praktický aspekt – řešení modelových situací, simulace. Stěžejní je zde pravidelnost a kontinuita průběžného vzdělávání.

Přínos a praktický vstup NCKB

- zprostředkovávání kontaktů na expertní vzdělávací instituce z oblasti ICT, případně vytvoření kontaktního listu
- poskytování metodické podpory dle požadavků jednotlivých útvarů
- podpora úzce specializovaných vzdělávacích aktivit
- spolupráce na tvorbě obsahové stránky vzdělávání
- podpora vytváření interního e-learningového vzdělávacího systému
- osvětový portál GovCERT.CZ

Přímo zainteresované subjekty spolupracující s NCKB

Technicky orientovaná část akademické sféry a její vědecká pracoviště, CZ.NIC/CSIRT.CZ a další CSIRT týmy, CESNET, expertní vzdělávací organizace a týmy z oblasti ICT (tuzemské i zahraniční), pro veřejnosprávní týmy – např. i instituce zabývající se vzděláváním veřejné správy, MPSV.

SEZNAM POUŽITÝCH ZDROJŮ

Akční plán k Národní strategii kybernetické bezpečnosti na období let 2015 – 2020

Národní strategie kybernetické bezpečnosti na období let 2015 – 2020

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

MŠMT - Strategie digitálního vzdělávání do roku 2020

MŠMT - Strategický záměr „Digitální vzdělávání / Touch your future

Zákon č. 563/2004 Sb., o pedagogických pracovnících a o změně některých zákonů

Evropská komise - Horizon Report Europe – 2014 Schools Edition

Evropská komise – Evropa 2020

Vláda ČR – Digitální Česko 2.0 „Cesta k digitální ekonomice“

Zákon č. 6/2002 Sb., o soudech a soudcích

Zákon č. 283/1993 Sb., o státním zastupitelství

USA – National Initiative for Cyber Security Education Strategy (NICE)

Est – HITSA Strategy 2014-2020

HU- National Cyber Security Strategy of Hungary

SVK - National Strategy for Information Security in the Slovak Republic

UK– Cyber Security Strategy Protecting and Promoting the UK in a Digital World

AT – National ICT Security Strategy

PL – Cyberspace Protection Policy of the Republic of Poland