Kyberbezpečnost a informační bezpečnost na středních školách

JIŘÍ SEDLÁČEK – TOMÁŠ PITNER

Network Security Monitoring Cluster – Masarykova univerzita, Národní centrum kompetence pro kyberbezpečnost

Článek může sloužit jako rychlý orientační materiál pro vedení středních škol a učitele informatiky v tom, jaká jsou východiska výuky kyberbezpečnosti a informační bezpečnosti v dnešní době plné hrozeb pocházejících z online světa, a jak takovou výuku zavést do všech středoškolských RVP a ŠVP v České republice.

Nastíní nově vyvinutý trojúrovňový koncept výuky kyberbezpečnosti a informační bezpečnosti s nejvyšším stupněm v podobě *Juniorních center excelence (JCE)*. V dalším čísle se budeme podrobněji věnovat prvním zkušenostem s JCE a jejich službám pro ostatní školy v rámci daných regionů.

Kyberbezpečnost a informační bezpečnost

V dnešní dynamické době jsme stále častěji konfrontováni s pojmy IoT, IoS, IoP, ..., Průmysl 4.0, chytré domy, chytrá města, cloudové služby, eGovernment, ale také kyberválka, kyberzločin, kyberšikana, kyberšpionáž, kybersabotáž, atd. Závislost dnešní společnosti na elektronických technologiích je stále vyšší a vyšší, stejně tak jako rizika z toho plynoucí.

Dne 1. 1. 2015 vešel v účinnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále ZKB), ve znění pozdějších předpisů. To je v naší legislativě průlomový krok, díky němuž se začal měnit přístup ke kyberbezpečnosti nejen z pohledu organizačních a technických opatření, ale i v právní rovině (povinné subjekty mají zákonnou povinnost řešit kyberbezpečnost) a v oblasti vzdělávání a evangelizace. Počet povinných osob daný §3 ZKB byl v roce 2017, po transpozici evropské směrnice NIS, rozšířen. Obecně velkým strašákem, jakkoli iracionálně, je od 25. 5. 2018 evropské nařízení o ochraně osobních údajů známé pod názvem GDPR (General Data Protection Regulation).

Každý občan bude v osobním životě v kyberprostoru dříve či později řešit komunikaci se státní správou a samosprávou (eGovernment), bezpečnost svou, zabezpečení svého majetku, bezpečnost svých blízkých. Budování bezpečnostního povědomí a znalostní základny je proto nezbytné systematicky zajišťovat nejpozději na středních školách.

Národní strategie kybernetické bezpečnosti a očekávání od středních škol

Národní strategie kybernetické bezpečnosti (NSKB) České republiky na období let 2015–2020 konstatuje, že: *Český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti* NEODPOVÍDÁ *v současné podobě aktuálním požadavkům a trendům. Z tohoto důvodu pak nedostatečně vzdělává a vychovává na základním a středním stupni žáky a také v nedostatečné míře nabízí vysokoškolské programy, které by vytvářely odborníky na kybernetickou bezpečnost. Poptávka po těchto odbornících je přitom vysoká.*

Národní strategie kybernetické bezpečnosti (NSKB) České republiky na období let 2015–2020 předpokládá v části F tato opatření:

F. Podpora vzdělávání, osvěta a rozvoj informační společnosti.

Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.

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.

F.2.01 Modernizovat rámcové vzdělávací programy na základní a středoškolské úrovni.

Z výše uvedeného je zřejmé, že výuka kyberbezpečnosti není ve středním školství na úrovni odpovídající požadavkům rozvinuté informační společnosti. Školy musí ze zákona zajistit výuku studentů a současně chránit *informace o studentech* (zajištění dostupnosti, důvěrnosti a integrity), které jsou mnohdy charakteru *zvláštní kategorie osobních údajů* (viz např. dopady inkluze). Jsou povinny archivovat informace nezbytné k vystavení *opisů studijních dokladů* – dobrým příkladem, ovšem ze školství vysokého, je Masarykova univerzita, která již léta nabízí možnost dálkově ověřit platnost diplomu při znalosti jeho čísla a nově také vydává potvrzení o studiu opatřené *elektronickou pečetí* (Vertéši, 2020).

Principy informační bezpečnosti

V oblasti informační bezpečnosti jsou nezbytné:

- **Systémový přístup.** Každá organizace sestává z *lidí, procesů a technologií*. Problematika IB/KB je proto řešena komplexně.
- **Analytický přístup.** Než jsou přijímána rozhodnutí, je nezbytné danou problematiku podrobit analýze. Jedině tak je možné nasazovat vhodná a ekonomicky přijatelná řešení.
- **Měřitelnost.** IB/KB je postavena na měřitelnosti. Ať už z pohledu zavedených opatření, tak i z pohledu ekonomického, tzn. efektivity a účelnosti vynaložených nákladů.
- **Opakovatelnost a přenositelnost/kompatibilita.** Jak z pohledu času, tak z pohledu peněz je vhodné použít řešení, které je principiálně přenositelné i na ostatní obdobné organizace. Jde jak o kvalitu a ověření řešení, tak o jeho další rozvoj a výměnu zkušeností v komunitě uživatelů, dodavatelů a s akademickou sférou.
- **Standardy.** Tak jako jsou jako norma přijaty v oblasti IB standardy (např. normy řady ISO 27000), stejně tak je nutné tento přístup aplikovat na zvolená technická opatření. Otevřené standardy jsou jedna strana mince, dlouhodobě fungující spolehlivý dodavatel druhá.
- **Udržitelnost.** Nasazená řešení a technologie musejí dlouhodobě splňovat tytéž (nebo vyšší) požadavky na bezpečnost. To lze garantovat za podmínky jejich trvalé udržovatelnosti, dostupnosti bezpečnostních varování, aktualizací, nástrojů pro monitoring a existence komunity s dostatečným know-how. Nezbytnost podmínkou udržitelnosti je rovněž ekonomická stránka – vybudované infrastruktury jak hardwarové, tak systémové a aplikační musejí být nejen nárazově na počátku, ale trvale finančně únosné. Nemá smysl vkládat velké prostředky na pořízení drahého řešení, když nebudou na provoz a údržbu, externí služby atd.
- **Racionalita.** Optimální přístup k řešení problematiky IB je postavený na *racionálních rozhodnutích podložených argumenty a fakty* (objektivně), nikoli dojmy.
- **Dokumentovatelnost.** Veškeré kroky jsou v oblasti IB/KB *dokumentovány*. Důvody jsou auditní (tzn. dohledatelnost, kdo, co jak a proč učinil), ale i udržení know-how (jak a proč se co technicky nastavovalo).
- **Systematičnost.** Souvisí se systémovým přístupem a s vědomím, že bezpečnost celku je odvislá od *bezpečnosti nejslabšího článku*.

- **Metodičnost.** Veškeré zaváděné postupy v IB/KB jsou aplikovány na základě předem stanovených *metodik*. Tedy nespoléhat na improvizaci, ale postupovat systematicky a metodicky; metodiky existují, jen je používat.

Modelová koncepce výuky kyberbezpečnosti na SŠ

V rámci analýzy byly identifikovány 3 typy vzdělávacích programů informační bezpečnosti pro SŠ v ČR:

I. Kategorie základní (KZ).

II. Kategorie ICT (KICT).

III. Kategorie JCE (KJCE).

Základ – KZ

Uvažuje se výuka pro všechny typy RVP, tedy těch, které s ICT nesouvisí, ale i RVP 18-20-M/01 Informační technologie, ŠVP *Kyberbezpečnost*, případně RVP *Kyberbezpečnost* v pilotním ověřování.

Předpokládá se tedy, že tato kategorie pokryje výuku IB/KB na všech školách, které nejsou více na tuto problematiku zaměřeny (specializovány) a dále na školách, které již vyučují RVP 18-20-M/01 *Informační technologie*, ŠVP Kyberbezpečnost, případně RVP KB v pilotním ověřování.

Informační bezpečnost a kyberbezpečnost uvažujeme vyučovat v základním rozsahu. Výuka je koncipována především se zaměřením na pokročilou evangelizaci, aby byli studenti dostatečně připraveni na fungování v rozvinuté informační společnosti. V rámci výuky pro kategorii *Základ* jsou uvažovány oblasti:

- *Úvod do informační bezpečnosti.*
- *Kyberprostor I.*
- *Sociální inženýrství.*
- *Právo v oblasti informační bezpečnosti I.*

Střed – KICT

Uvažuje se výuka v rámci RVP 18-20-M/01 *Informační technologie*, ŠVP *Kyberbezpečnost*, případně RVP *Kyberbezpečnost* v pilotním ověřování.

Předpokládá se tedy, že tato kategorie pokryje výuku IB/KB na všech školách, které již vyučují RVP 18-20-M/01 Informační technologie, ŠVP Kyberbezpečnost, případně RVP Kyberbezpečnost v pilotním ověřování.

Informační bezpečnost a kyberbezpečnost uvažujeme vyučovat ve středním rozsahu v návaznosti na základní rozsah. Školy jsou vybaveny učebnami ICT a mají tedy předpoklady pro výuku informační bezpečnosti a

kyberbezpečnosti nejen v teoretické, ale i v praktické rovině. Technická opatření je možné v počítačových učebnách implementovat a procvičovat dle možností dané školy. V rámci výuky pro KICT jsou uvažovány oblasti:

- *Informační bezpečnost v organizaci I.* (technická opatření u právnických osob nepodléhajících ZKB)

Top – KJCE

Uvažuje se výuka v rámci ŠVP *Kyberbezpečnost*, případně RVP *Kyberbezpečnost* v pilotním ověřování.

Předpokládá se tedy, že tato kategorie pokryje výuku IB/KB na všech školách, které již vyučují ŠVP Kyberbezpečnost, případně RVP Kyberbezpečnost v pilotním ověřování.

Informační bezpečnost a kyberbezpečnost uvažujeme vyučovat v návaznosti na střední a základní rozsah. Zvolené školy jsou excelentními centry s výukou kyberbezpečnosti a aspirující na vytvoření JCSIRT. Technické zázemí škol umožňuje i pokročilou praktickou výuku s možností procvičování vybraných technických opatření dle možností dané školy. Tyto školy mají roli lídra v oblasti IB v kraji. V rámci výuky pro KJCE jsou uvažovány oblasti:

- *Strategická analýza v organizaci.*
- *Integrovaná bezpečnost* (Informační bezpečnost, Kyberbezpečnost, Ochrana osobních údajů).
- *Kybernetický prostor II.*
- *Právo v oblasti informační bezpečnosti II.*
- *Standardy v oblasti informační bezpečnosti.*
- *Informační bezpečnost v organizaci II.*

Závěr

Jak je z výše uvedeného zřejmé, oblasti na sebe navazují. Tento model umožňuje výuku IB/KB na každé SŠ pro každý studijní obor na této SŠ; může nastat situace, že na jednu školu budou aplikovány všechny tři výše uvedené kategorie. Výuka IB/KB tedy nebude nadále doménou pouze pro školy se specializovanými studijními obory, jak tomu bylo doposud.

Literatura

[1] *Veréši, M.*: Potvrzení o studiu na MUNI nově elektronicky a jedním klikem. Magazín M, Masarykova univerzita, Brno.
Dostupné z: https://www.em.muni.cz/student/12394-potvrzeni-o-studiu-na-muni-nove-elektronicky-a-jednim-klikem