GORDIC

Proč je vzdělávání v kybernetické bezpečnosti důležité?

Eliška Bartůšková, MBA – Gordic spol. s r.o.

Nedostatek odborníků

- 40% nárust poptávky po specialistech z oblasti KB
- **ČR postrádá až 30.000 KB odborníků (EU 500-900tis)**
- Veřejná správa ČR postrádá 12.000 KB odborníků

- Očekávaný růst počítačových povolání v USA v letech 2016 – 2026 ve výši 13.5%
- Očekávaný růst kyber. bezpečnostních povolání v letech 2020 – 2030 ve výši 31%

Zdroje: Jirásek (2013, 2020), ISC2 (2020), Ventures (2021), NIST NICE (2021), BLS (2021), Ministry of Labor (2021)

Proč se zabývat kybernetickou bezpečností?

- Téměř 100% závislost moderních společností na ICT
- V roce 2020 státy G20 měly 3 miliardy uživatelů internetu a generovaly 8.000 miliard USD „Internetové ekonomiky“
- „Internetová ekonomika“ v ČR generuje ca. 3.6% HDP
- Požadavky vyplývající z legislativy a regulací (ZoKB, EU NIS2)
- Obchodní příležitost

Role vyplývající ze zákona o KB

- **Manažer kybernetické bezpečnosti**
  zodpovídá za plánování, organizování a řízení realizace opatření, projektů a programů k řízení bezpečnosti informací tak, aby bylo dosaženo stanovených cílů v oblasti kybernetické bezpečnosti, a to ve stanoveném termínu a v rámci stanoveného rozpočtu

- **Architekt kybernetické bezpečnosti**
  zajišťuje návrh implementace bezpečnostních opatření

- **Auditor kybernetické bezpečnosti**
  provádí audit kybernetické bezpečnosti

- **Garant aktiva**
  zajišťuje rozvoj, použití a bezpečnost aktivita (důvěrnost, dostupnost, integrita)

Pracovní pozice v oblasti KB

- Cybersecurity Analyst

  detailně zná podnikovou ICT infrastrukturu a je ji schopen monitorovat

- Cybersecurity Consultant

  chrání ICT infrastrukturu a data před narušením

- Cybersecurity Manager

  řídí kybernetickou bezpečnost organizace

- Software Developer

  vyvíjí aplikace

Pracovní pozice v oblasti KB

- Systems Engineer

  odborník na technologie, který má potřebné dovednosti pro plánování, implementaci a dohled nad počítačovými systémy

- Network Engineer

  odborník na technologie, který má potřebné dovednosti pro plánování, implementaci a dohled nad počítačovými sítěmi

- Penetration & Vulnerability Tester

  provádí simulované kybernetické útoky na počítačové systémy a sítě společnosti

Jak začlenit kybernetickou bezpečnost do výuky?

- **Aktualizace učebních plánů**
  IT předměty by měly zahrnovat obsah věnovaný kybernetické bezpečnosti.
  Osvětové portály (NUKIB, KPBI)

- **Zaměření se na praktické dovednosti**
  Studenti by měli mít možnost vyzkoušet si reálné scénáře útoků a obrany, aby získali praktické zkušenosti s identifikací a řešením bezpečnostních hrozeb.

- **Spolupráce s odborníky a firmami**
  Spolupráce může školám poskytnout přístup k odborným znalostem a zkušenostem, stejně jako k aktuálním trendům a technologiím v oblasti kybernetické bezpečnosti.

- **Soutěže**
  Účast v soutěžích v této oblasti může poskytnout studentům motivaci a uznání za jejich znalosti a dovednosti v oblasti bezpečnosti.

KB znalostní profil studenta

Dle Pracovní skupiny kybernetické bezpečnosti (zpracováno pro MŠMT)

Základní školy – 2. stupeň

- Bezpečné a etické chování v kyberprostoru;
- Rozvoj etického a právního povědomí, práv, povinností a trestní odpovědnosti při využívání kybernetického prostoru;
- Rozvoj znalostí a dovedností důležitých pro bezpečné chování v kyberprostoru;
- Rozvoj schopnosti rychle a správně se rozhodovat, vyhledávat informace a ověřovat si je;
- Rozvoj schopností bezpečné komunikace a rozpoznání indikátorů negativních jevů;
- Ochrana vlastní identity a dat bezpečnosti v kyberprostoru.

Střední škola – IT bez specializace KB

- Rozvoj znalostí a dovedností důležitých pro bezpečné chování v kyberprostoru;
- PDCA a základy ISMS jako východisko pro řízení bezpečnosti informací
- Základy legislativy pro řízení bezpečnosti informací v ČR a EU
- Definice povinností „uživatele“ v prostředí řízení kybernetické bezpečnosti

Střední škola – IT se specializací KB

- Schopnost zavádět systém řízení bezpečnosti v organizaci;
- Schopnost vykonávat povinnosti „garanta aktiva“ a „architekta kybernetické bezpečnosti“;
- Schopnost navrhovat a spravovat podnikovou síť;
- Schopnost diagnostikovat a spravovat personální počítač;
- Schopnost detekovat a analyzovat kybernetické incidenty;
- Znalost a schopnost použití technik kybernetické obrany;
- Znalost legislativy pro řízení bezpečnosti informací v ČR a EU.

VOŠ – IT bez specializace KB

- Základy legislativy pro řízení bezpečnosti informací v ČR a EU
- Základní orientace ve všech oblastech bezpečnosti informací, základní kontext povinností KB u právnických a fyzických osob
- Schopnost aplikace znalostí bezpečnosti informací v podnikovém řízení

VOŠ – IT se specializací KB

- Schopnost navrhovat a řídit bezpečnost informací v organizaci;
- Schopnost auditovat systém řízení bezpečnosti informací;
- Schopnost vykonávat povinnosti „manažera kybernetické bezpečnosti“;
- Znalost a schopnost použití technik kybernetické obrany;
- Schopnost navrhovat nové detekční a forenzní metody;
- Schopnost navrhovat a spravovat rozsáhlé podnikové sítě;
- Znalost legislativy pro řízení bezpečnosti informací v ČR a EU.

Děkuji za pozornost.

eliska_bartuskova@gordic.cz
Tel.: 725 056 390