GORDIC®

Lidský faktor nejen v kybernetické bezpečnosti

Jan Dienstbier

KYBEZ Platforma kybernetické bezpečnosti

- Česko v digitální Evropě
- Informační koncepce ČR
- Koncepce Digitální ekonomika a společnost

Vláda ČR schválila svým usnesením č. 629 dne 3. října 2018 průřezový strategický dokument Digitální Česko, který se týká veškerých dopadů digitalizace na hospodářství a společnost. Jde o soubor koncepcí zajišťující předpoklady dlouhodobé prosperity České republiky. Jeho náplň je možné definovat pojmem: "Strategie koordinované a komplexní digitalizace České republiky 2018+". "Digitální Česko" zastřešuje tři pilíře (dílčí koncepce), které tvoří jeden logický celek. Pokrývá oblasti od interakce České republiky v Evropské unii v digitální agendě, přes digitální veřejnou správu, až po přípravu a interakci společnosti a ekonomiky ČR na digitalizaci.

Česko v digitální Evropě

- Koncepce si klade ambici zajistit jednotný a inovativní přístup ČR k problematice digitální agendy na úrovni Evropské unie, a to v souladu s moderními technologickými trendy a s kritickým respektem k platné regulaci vycházející z EU. Cílem je prosazování priorit, zájmů a národních specifik ČR.
- Tato oblast představuje soubor cílů orientovaných na budování vyjednávacích pozic a jejich využití k získání optimálních přínosů pro českou veřejnost i **výkon veřejné moci na národní úrovni**. Koncepce Česko v digitální Evropě je v **gesci Úřadu vlády**.

Informační koncepce ČR

- Informační koncepce ČR je zaměřena na **digitalizaci v oblasti výkonu veřejné moci na národní úrovni.**
  Je vytvořená na základě pověření zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
- Stanovuje hlavní cíle v oblasti budování informačních systémů veřejné správy a dále stanoví obecné principy správy a provozování informačních systémů veřejné správy. **Jedná se o problematiku známou jako „eGovernment“ ČR.**

Informační koncepce ČR - cíle

1. UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ ON-LINE SLUŽBY PRO OBČANY A FIRMY
2. DIGITÁLNĚ PŘÍVĚTIVÁ LEGISLATIVA
3. ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE
4. ZVÝŠENÍ KAPACIT A KOMPETENCÍ ZAMĚSTNANCŮ VE VEŘEJNÉ SPRÁVĚ
5. EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY

Koncepce Digitální ekonomika a společnost

Koncepce Digitální ekonomika a společnost řeší průřezově problematiku, jejíž části leží mimo přímou gesci veřejné moci. Jedná se zejména o podporu pozitivních aspektů společenských i ekonomických změn souvisejících s digitální revolucí a minimalizaci negativních dopadů (např. na pracovní trh). Do této oblasti spadá řada iniciativ, či potenciálních iniciativ, jako např.

- Elektronické zdravotnictví (eHealth, Health 4.0)
- Elektronické vzdělávání
- Elektronická kultura (eCulture)
- Inovace, výzkum a vývoj 4.0
- Průmysl 4.0
- Stavebnictví 4.0
- Koncept SMART Region/City/Village
- a další.

Koncepce Digitální ekonomika a společnost - cíle

1. EFEKTIVNĚJŠÍ SYSTÉM PŘÍMÉ I NEPŘÍMÉ PODPORY VÝZKUMU, VÝVOJE A INOVACÍ
2. ZRALOST A PŘIPRAVENOST SEKTORŮ EKONOMIKY NA DIGITÁLNÍ TRANSFORMACI
3. PŘIPRAVENOST OBČANŮ NA ZMĚNY TRHU PRÁCE, VZDĚLÁVÁNÍ A ROZVOJ DIGITÁLNÍCH DOVEDNOSTÍ
4. PODPORA KONEKTIVITY A INFRASTRUKTURY DIGITÁLNÍ EKONOMIKY A SPOLEČNOSTI
5. ZAJIŠTĚNÍ BEZPEČNOSTI A DŮVĚRY V PROSTŘEDÍ DIGITÁLNÍ EKONOMIKY A SPOLEČNOSTI
6. LEGISLATIVA PODPORUJÍCÍ VŠECHNY ASPEKTY DIGITÁLNÍ EKONOMIKY A SPOLEČNOSTI
7. OPTIMÁLNÍ SYSTÉM FINANCOVÁNÍ DIGITÁLNÍ EKONOMIKY A SPOLEČNOSTI
8. INSTITUCIONÁLNÍ ZAJIŠTĚNÍ CENTRÁLNÍ KOORDINACE POLITIK NA PODPORU DIGITÁLNÍ EKONOMIKY A SPOLEČNOSTI

digitální ; ČESKO

Budeme se učit užívat technologie, které se ještě neužívají

Musíme na to připravit studenty i celou společnost => celoživotní vzdělávání => znalostní ekonomika => participace průmyslu

Jádrem učitel? Kdo ho připraví? Umělá inteligence?

Dřív jsme se učili vyhledávat informace, dnes vyhodnocovat informace

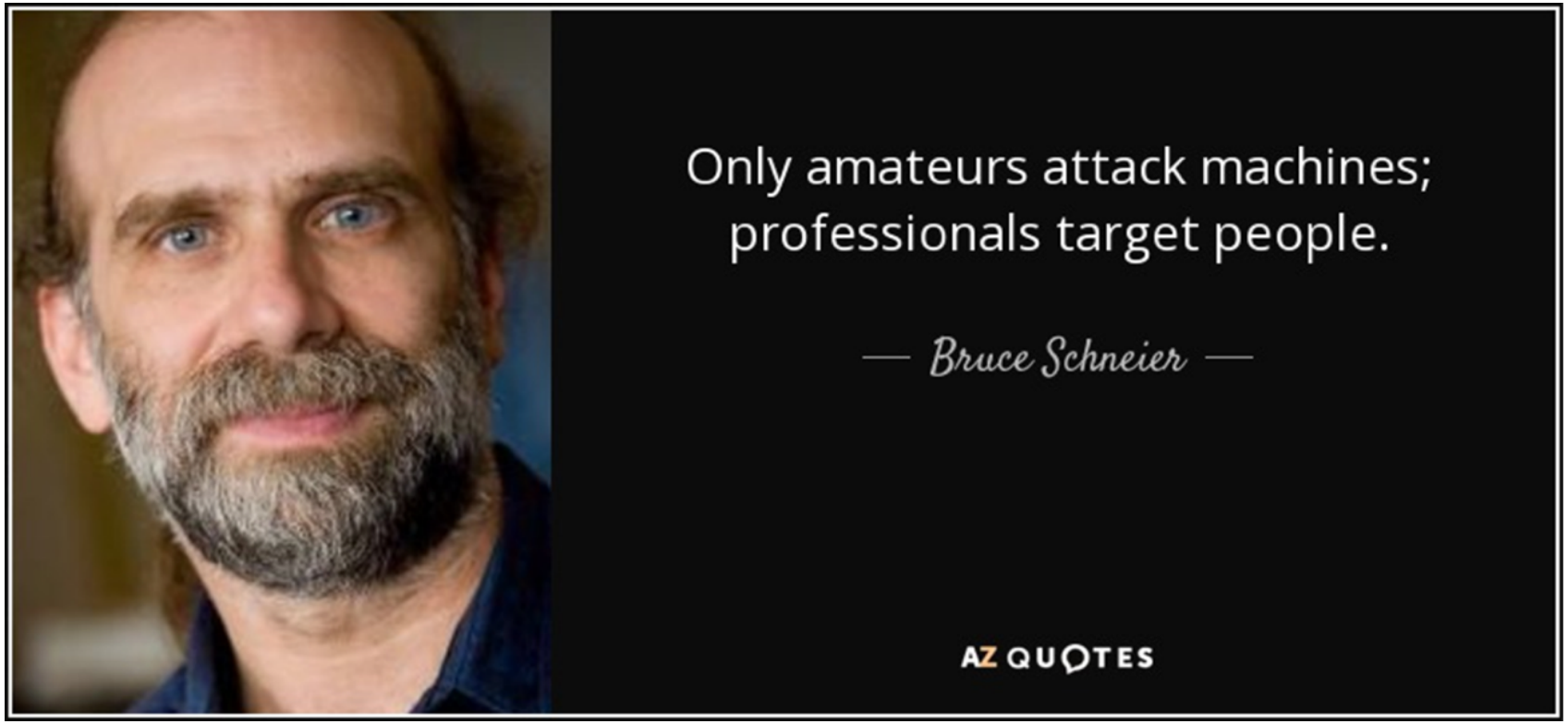
digitální ; ČESKO

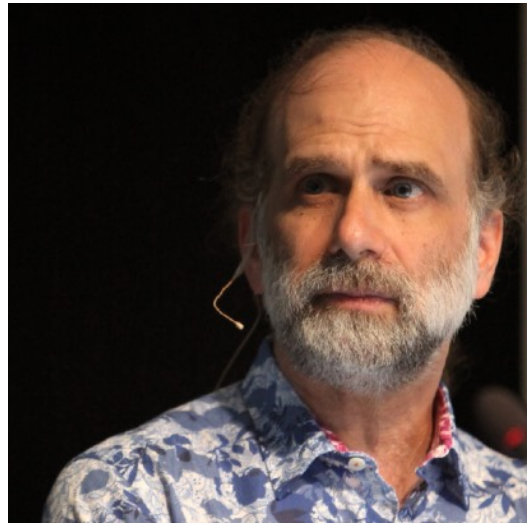
- Schopnost orientace – kritické myšlení – informace x desinformace
- Adaptabilita
- Kreativita – správné odpovědi – nová řešení
- Přesvědčit okolí o užitečnosti kreativního objevu/postupu (empowerment)
- Vedení lidí
- Spolupráce – jazyky, soužití různých skupin „agilní řízení“
- Prodat výsledky

Naučit se jak se v tomto prostředí bezpečně pohybovat by mělo být prvním krokem, stejně jako se děti učí před cestou do školy správně přecházet přes silnici.

Nepůjde to hned, ale začít je třeba dnes, zejména s výukou bezpečného chování.

Proč?





American cryptographer, computer security professional, privacy specialist and writer

Kybernetický ekosystém

Hrozba → Příležitost → Kybernetická ekonomika

Např.: Izrael

Zatím ještě hodně dlouhá cena před námi.

Vzdělávání v kybernetické bezpečnosti

Základní školy?

Střední školy - několik pilotních implementací
- různé iniciativy SSKB, Bezpečný internet, kraje pro bezpečný internet, Policie …

Vysoké školy - denní, postgraduální, MBA …

Vzdělávání seniorů

Vzdělávání v kybernetické bezpečnosti ve státní správě

- Kybernetická gramotnost je nutnou podmínkou digitalizace státní správy a projektů eGovermentu
- Vzdělávání v kybernetické bezpečnosti je jedním z klíčových opatření pro zmírnění části rizik projektu Digitální Česko – tj. vzdělání v kybernetické bezpečnosti musí být startem projektu
- Lze začít okamžitě
- Základy kyberneticko-bezpečnostní gramotnost = Ekvivalent kurzů BOZP nebo požární bezpečnosti
- Budou nabyté znalosti předávat dětem i rodičům

Jak vzdělávat úředníky v kybernetické bezpečnosti?

- **Formou eLearningových kurzů**
- **Obsah kurzů koordinován NUKIB**
- **Časová perioda – 1 rok**

Základy kybernetické-bezpečnostní gramotnosti

Obecné seznámení se základními pojmy ICT a kybernetické bezpečnosti

- **Obsah školení:**
  - seznámení se základními pojmy a uživatelskými technologiemi ICT
  - vysvětlení potřeby kybernetické bezpečnosti
  - seznámení se základními pojmy v oblasti kybernetické a informační bezpečnosti
  - seznámení s hrozbami a typy kybernetických útoků a užívanými technikami útočníků
  - ochrana dat a soukromí (osobních údajů)
  - seznámení s legislativním rámcem ČR (zákon o Kybernetické bezpečnosti....) a prováděcími předpisy ve státní správě

Základy kyberneticko-bezpečnostní gramotnosti

Phishing - seznámení se a rozpoznání útoku na bázi sociálního inženýrství

- **Phishing je jedním ze tří nejčastějších typů kybernetických útoků**
- **Phishingu nelze zcela zabránit technologickou cestou**
- **Sociálně-inženýrský způsob útoku pomocí e-mailu**

- **Doporučený způsob školení:**

  Simulace Phishingových útoků v níž jsou úředníkům každý měsíc rozesílány „falešné“ e-maily v různém čase a z různých adres, pokrývající různé typy scénářů útoků („Spray“ a „Spear Phishing), „odchycené“ uživatele přesměruje systém k výukovým kapslím, jejichž cílem je lépe je naučit rozpoznat phishingový útok

Základy kybernetické bezpečnosti pro IT profesionály ve státní správě

Proč vzdělávat pracovníky IT oddělení v kybernetické bezpečnosti?

- **Základy kybernetické bezpečnosti - jedna ze základních provozních znalostí a dovedností**
- **Být rovnocenným partnerem dodavatelům a poskytovatelům cloudu**
- **Vzdělávání v kybernetické bezpečnosti by mělo být profesní kvalifikací – ekvivalent školení profesionálních řidičů**

Základy kybernetické bezpečnosti pro IT profesionály ve státní správě

Obsah školení:

- podpora dodržování pravidel bezpečnosti dat
- kybernetický prostor – jeho definice a vymezení rolí v něm (zločinci, profesionálové)
- vysvětlení základních pojmů a principů jako např. důvěrnost, integrita, dostupnost
- porovnání jak kybernetické hrozby ohrožují fyzické osoby, firmy/ instituce a státy
- ISO model kybernetické bezpečnosti, ZKB
- kybernetické hrozby (taktika, techniky užívané útočníky)
- typy kybernetických hrozeb jako malware, malicious software, sociální inženýrství a ochrana proti nim
- seznámení s technologiemi, produkty a procesy používané k zajištění důvěrnosti dat
- zajištění integrity dat

Základy kybernetické bezpečnosti pro IT profesionály ve státní správě

Obsah školení pokračování:

- řízení přístupových práv uživatelů
- užití elektronických podpisů a certifikátů
- vysoká dostupnost IT systémů a její zajištění
- zpracování „Disater recovery“ plánů a zvládání incidentů
- ochrana síťové infrastruktury a koncových zařízení uživatelů
- kryptografické techniky

Základy kybernetické bezpečnosti pro IT profesionály ve státní správě

Analytik/ specialista kybernetické bezpečnosti

- **Cíl kurzu:**

získání znalostí a praktických dovedností potřebných k zajištění provozu SOC na pozicích operátora SOC nebo analytika kybernetické bezpečnosti

Závěr

- Koordinovat aktivity – určit koordinátora a dát mu pravomoci NÚKIB, RVIS, MŠ?
- Zapojit i podnikovou sféru
- Kvalitativní i kvantitativní cíle
- Neotálet se začátkem

Děkuji za pozornost