NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

AFCEA

Centrum kybernetické bezpečnosti

Vzdělávání a osvěta v kybernetické bezpečnosti

01.03.2022

Petra Šnoblová

Proč je důležité vzdělávat lidi v kyberbezpečnosti?

- 92 % malware (škodlivého software) je šířeno přes e-mail[1)]
- 85 % případů úniku dat bylo v roce 2021 vinou selhání lidského faktoru[2)]
- V roce 2020 byl oproti 2019 téměř 5násobný nárůst ransomware útoků[3)]
- V první polovině 2021 téměř 3násobný nárůst ransomware útoků oproti 2020[4)]
- Zaměstnanec otevřením přílohy phishing e-mailu způsobil ransomware útok na irskou národní zdravotní službu (HSE, Health Service Executive), celková finanční ztráta se vyšplhala na 100 milionů euro[5)]
- 20 % uživatelů klikne na odkaz, z nich cca 68 % vyplní údaje na podvodné stránce[6)]

Proč je důležité vzdělávat lidi v kyberbezpečnosti?

- Lidé jsou nejslabší a zároveň nejsilnější článek obrany proti kyberútokům
- Útoky cílené na selhání lidského faktoru lze často odvrátit jen obezřetností jednotlivců
- Ne všechny útoky lze zachytit bezpečnostními nástroji
- Lidé musí být konstantně vzděláváni na konkrétních příkladech, musí znát aktuální hrozby a podobu útoků
- Vzděláváním lidí v kyberbezpečnosti se snižuje riziko úspěšného kyberútoku o 70 %[7)]

Proč je důležité vzdělávat lidi v kyberbezpečnosti?

- Zlepšování reakce na kybernetické incidenty
- Zvyšování efektivity aktuálně nasazených bezpečnostních nástrojů
- Zajištění souladu s legislativními požadavky a standardy
  - Obce až na výjimky nespadají pod působnost zákona o kybernetické bezpečnosti (č. 181/2014 Sb.)
  - zákon č. 365/2000 Sb., o informačních systémech veřejné správy **stanovuje požadavek na zajištění bezpečnosti informací v informačních systémech**
  - Návod: **Minimální bezpečnostní standard**

Jak zvyšovat povědomí v kyberbezpečnosti?

- Neformální vzdělávání:
  - pravidelná interní školení, workshopy (např. e-learning na míru, online workshop s odborníkem)
- Všeobecná osvěta:
  - stránka na Intranetu věnovaná kybernetické bezpečnosti – aktuality, bezpečnostní doporučení, základní pravidla bezpečnosti v organizaci
  - Newsletter, pravidelná varování před aktuálními hrozbami
- Vzdělávejte všechny zaměstnance, ne jen IT pracovníky
- Provádějte simulované útoky a testujte účinnost vzdělávání
- Vzdělávání a školení nastavte na pravidelné bázi

Jak zvyšovat povědomí v kyberbezpečnosti?

- Zaměřte se na
  - bezpečnost hesel,
  - zabezpečení zařízení (zejména mobilních) a jejich bezpečné používání,
  - reakci na kybernetickou bezpečnostní událost a incident.
- Zaveďte proces pravidelného varování zaměstnanců před aktuálními hrozbami, např. aktuální phishing kampaně
- Zaměřujte se i na oblast využívání ICT pro soukromé účely (bezpečnost mobilních aplikací, online nakupování, sociální sítě,…)
- Užitečné online kurzy: **Dávej kyber** – online kurz NÚKIB,
  Kybertest.cz

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

- Servisní organizace MV ČR
- Poskytuje služby v oblasti informačních a komunikačních technologií
- mj. konzultační a metodické služby v oblasti informační a kybernetické bezpečnosti

AFCEA

- Česká pobočka mezinárodní neziskové členské asociace
- Podpora rozvoje informačních a komunikačních technologií ozbrojených sil ČR, včetně kybernetické bezpečnosti
- Pracovní skupiny kybernetická bezpečnost, inteligence, ochrana obyvatelstva
- mj. osvětová činnost v kyberbezpečnosti

Centrum kybernetické bezpečnosti

- Od roku 2021 navazuje na práci PSKB AFCEA
- Pořádá Národní soutěž ČR v kybernetické bezpečnosti
- Osvětové a odborné akce pro studenty a učitele
- Metodická podpora ve vzdělávání v kyberbezpečnosti

Zdroje

1) https://purplesec.us/resources/cyber-security-statistics/
2) 2021 Data Breach Investigations Report, Verizon
3) 2020 Consumer Threat Landscape Report, Bitdefender
4) Global Security Report: Rapid Increase in Ransomware Threats Drives Need for Security Controls That Speed the Kill Chain, Venafi
5) The Irish Times
6) Expertinsights.com
7) 2021 KnowBe4, Train employees and cut cyber risks up to 70 percent

Děkuji za vaši pozornost!

Petra Šnoblová
Specialista kybernetické bezpečnosti,
NAKIT, s.p.

Centrum kybernetické bezpečnosti

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.