EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kybernetická bezpečnost jednotlivce

Kyberbezpečnost – úvod

- ✓ Interdisciplinární vědní obor – setkání technické (informatika) a společenskovědní stránky (politologie, bezpečnostní studia, psychologie apod.).
- ✓ Můžeme ji zkoumat na několika úrovních – jednotlivec/organizace/národní/mezinárodní.
- ✓ Silná propojenost úrovní – botnety, organizovaný zločin apod.
- ✓ Při dodržování poměrně jednoduchých zásad (viz následující slidy) jsme schopni se vyhnout většině hrozeb a vše začíná u jednotlivce.

Základní koncepty

- ✓ CIA triáda – chrání ji informační bezpečnost.
  - *Confidentiality* – důvěrnost;
  - *Integrity* – integrita, neporušenost a
  - *Availability* – dostupnost dat.
- ✓ Tři vrstvy kyberprostoru – fyzická (hardware), logická (software), a nejslabší – sociální (uživatel).
- ✓ Vektor útoku – způsob, jakým se útočník dostane do systému – nejčastěji je to uživatel. Útoky za zneužití lidské psychiky jsou tak jedny z nejčastějších.

Vybrané hrozby

- ✓ Sociální inženýrství – soubor technik využívajících psychologickou manipulaci jako vektor útoku.
  - *Nejčastěji – phishing, smishing, vishing.*
- ✓ Malware – obecně jakýkoliv škodlivý program.
  - *Soubor vlastností – např. virus, ransomware – nazývá se podle toho, jaký je jeho účel.*

Kyberšikana

- ✓ Český právní řád tento termín nezná, ale ví, jak postihnout její obsah!
- ✓ Trestní zákoník i legislativa EU (např. GDPR).
- ✓ Poměrně závažná trestná činnost – nebezpečné pronásledování, pomluva, porušení tajemství listin aj. dokumentů uchovávaných v soukromí, účast na sebevraždě apod.
- ✓ Projevy jsou vnímány hůře jak u „klasické“ šikany.

Jak se zabezpečit? - silná hesla

- ✓ Naprostý a často podceňovaný základ, který dokáže velmi dobře ochránit před celou řadou hrozeb.
- ✓ Heslo musí být silné (cca 13 znaků). Velká a malá písmena, znaky, číslovky.
- ✓ A také snadno zapamatovatelné. Ale jak toho dosáhnout?
- ✓ Správce hesel nebo vlastní algoritmus.

Občanský průkaz 4.0

Jak si vytvořit silné heslo? – příklad

1. Zvolíme si kořen slova – hesla - např. „jezevec“.
2. Spousta služeb vyžaduje využití čísel a velkých písmen, proto se základ změní na „j3Z3v3c“.
3. Nyní rozlišení pro každou službu. Přihlašuji se např. na Aliexpress a tak dám za kořen jméno služby pozpátku. Vznikne mi „j3Z3v3csserpxeila“.
4. Pro ještě lepší zabezpečení přidejte číslovku podle počtu použitých znaků v celém heslu: „j3Z3v3csserpxeila17“.

Další zabezpečení a kybernetická hygiena

- ✓ Zabezpečení sítí
  - Domácí vs. Veřejná.
  - VPN vs. proxy!
- ✓ Dvoufaktorová autentizace.
- ✓ Pravidelné aktualizace, časté zálohování, rozpoznání phishingu.
- ✓ Sdílet jen data, u kterých nevadí, že budou existovat už napořád.
- ✓ Ideální stav – automatické návyky.

Doporučená literatura

- Matyáš, Vašek a Jan Krhovják: *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008.
- Švestková, Renata, Ladislav Soldán a Martin Řehka: *Kyberšikana*. České Budějovice: ZSF JU, 2019.
- Zuboff, Shoshana: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.
- *Nástroje a tipy, které vám pomohou zajistit vaše bezpečí na internetu* [online]. Google, 2021. [cit. 2021-12-01]. Dostupné z www: <https://safety.google/security/security-tips/>.
- *Top 10 Secure Computing Tips* [online]. UC Berkeley, 2021. [cit. 2021-12-01]. Dostupné z www: <https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips>.