E-Bezpečí 2025, 10(2): Page 30-33. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=4712

ČLOVĚK – NEJSLABŠÍ ČLÁNEK POČÍTAČOVÉ BEZPEČNOSTI

Kamil KOPECKÝ

Když se řekne „počítačová bezpečnost“, většina lidí si vybaví antiviry, hesla, šifrování nebo složitá technologická řešení. Jenže v praxi selhává celý bezpečnostní systém nejčastěji jinde – na člověku samotném. Technologie se vyvíjejí, útočníci se zdokonalují, ale lidská důvěřivost, spěch, nepozornost a emoční zranitelnost zůstávají stejné.

Útočník už dávno nehledá chybu v systému, ale v nás

Dnešní kybernetické útoky už zdaleka nefungují jen tak, že někdo prolomí heslo nebo najde skulinu v systému. Útočníci jdou jednodušší cestou – **zneužívají lidské chování**. Místo technického prolomení systému se zaměří na to, aby přesvědčili uživatele, že jim má pomoci sám. Ať už jde o e-mail, který se tváří jako zpráva z banky, telefonát od „policisty“ nebo webovou stránku, která napodobuje oficiální portál – cílem je jediné: vyvolat důvěru a přimět člověka k chybě.

Zvláštní kapitolou je tzv. **spoofing**, tedy podvržení identity. Útočník dokáže napodobit telefonní číslo banky, oficiální e-mailovou adresu nebo dokonce hlas konkrétní osoby. Oběť pak skutečně věří, že mluví s bankéřem, příbuzným či kolegou – a právě tato víra bývá začátkem problému. Mnozí se diví, jak je možné, že lidé dokážou uvěřit neznámému člověku, který jim po telefonu říká, že mají okamžitě vybrat všechny své peníze z účtu a

převést je „na bezpečný účet“, nebo je dokonce vybrat a předat osobně pachateli vydávajícímu se za pracovníka bezpečnostní agentury.

Jenže tito pachatelé nejsou amatéři. Jsou to profesionálové, kteří dokonale rozumí lidské psychologii, dovedou vyvolat dojem naléhavosti, hrát na emoce a přimět člověka, aby přestal přemýšlet racionálně. Jsou na to trénováni, dokonce mají k dispozici aplikace, které je vedou rozhovorem s klientem - podobně jako call centra bankovních institucí.

Dezinformace, manipulace a hybridní hrozby

Slabiny lidského uvažování se netýkají jen individuálních podvodů, ale i společnosti jako celku. Dnes už nežijeme jen v éře kyberzločinu, ale i **hybridních hrozeb** – útoků, které kombinují digitální, informační a psychologické nástroje. Dezinformace, konspirační teorie a propagandistické kampaně dokážou rozdělit společnost, ovlivnit volby nebo oslabit důvěru lidí v demokratické instituce.

Lidé si často ani neuvědomují, že se stali terčem hybridní operace. Sdílejí zmanipulovaný obsah, obhajují zločiny režimů, jako je ten ruský, nebo věří informacím, které jsou součástí propagandy. Když se je pak snažíme konfrontovat s fakty, náprava je velmi obtížná – propaganda už zanechala svůj otisk. A bohužel s sebou nese velké množství agrese. Čím déle člověk žije v informační bublině, tím těžší je jeho probuzení.

Když lidé uvěří falešným zprávám, sdílejí je dál a jednají podle nich, problém už není jen individuální. Ohrožuje nejen jednotlivce, ale **celou zemi** – její stabilitu, bezpečnost i schopnost čelit vnějším vlivům. Schopnost rozpoznat manipulaci a bránit se jí se tak stává otázkou národní odolnosti.

Kritické myšlení jako digitální imunitní systém

Nejlepší antivir pro lidskou mysl se jmenuje **kritické myšlení**. Schopnost zastavit se, pochybovat, ověřovat a nenechat se strhnout emocemi je dnes klíčová. Právě ono nám pomáhá odlišit realitu od manipulace, rozpoznat podvod od pravdy, lživý titulek od seriózní informace.

Bohužel, praxe ukazuje, že i v době, kdy máme k dispozici více informací než kdykoli dřív, **mediální gramotnost** zůstává slabá. Ve školách se jí věnuje jen okrajově, a přitom právě tam by měla začínat obrana proti dezinformacím a manipulaci. Mladí lidé sice ovládají technologie, ale často nerozumí tomu, jak s nimi bezpečně pracovat. Učí se psát, číst a počítat – ale méně často ověřovat, přemýšlet a pochybovat.

Umělá inteligence: když nevíme, co je skutečné

S nástupem **umělé inteligence** se situace ještě komplikuje. AI dnes dokáže vygenerovat text, který vypadá jako novinový článek, vytvořit realistické video (deepfake) nebo napodobit hlas skutečné osoby. Vzniká tak nová vlna manipulací, které jsou čím dál těžší k rozpoznání. Falešné e-maily, deepfake videa či hlasové nahrávky se mohou stát běžnou součástí podvodů, politické propagandy i osobních útoků.

V takovém světě už nestačí věřit tomu, co vidíme nebo slyšíme. Je nutné vědět, **jak snadno lze realitu zfalšovat** – a o to víc dávat pozor na zdroje informací a jejich důvěryhodnost.

Když použijeme rozum, máme šanci

Přesto není všechno ztraceno. Pokud se naučíme dodržovat **základní bezpečnostní návyky**, být opatrní při komunikaci, ověřovat informace a nenechat se manipulovat emocemi, dokážeme rizika výrazně snížit. Kritické myšlení, obezřetnost a mediální gramotnost nejsou jen hezké pojmy z výuky občanské

výchovy – jsou to **nástroje přežití** v digitálním světě. Bezpečnost totiž nezačíná v počítači, ale v hlavě. A právě tam se rozhoduje, jestli budeme obětí, nebo člověkem, který rozumí světu kolem sebe a umí se v něm bránit.

Kamil Kopecký
E-Bezpečí, Univerzita Palackého v Olomouci