

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **15** ze dne **17.8.2022**

Pět nejčastějších technik sociálního inženýrství

Naprostá většina úspěšných kybernetických útoků zneužívá nechtěné spolupráce napadeného a stojí na technikách sociálního inženýrství. Ty podle některých odhadů stojí až za 98 % úspěšných kybernetických útoků. Sociální inženýrství využívá – často zákeřným způsobem – lidských emocí k dosažení svých cílů, ať již k získání fyzického přístupu do kanceláří či k online přístupu k firemním systémům.

Sociální inženýrství

Podle průzkumu společnosti PurpleSec se v uplynulém roce setkala s útokem založeným na metodách sociálního inženýrství 43 % IT profesionálů. A shodou okolností stejný podíl (43 %) takovýchto útoků míří na SMB firmy. Bez adekvátní ochrany jim hrozí vysoké riziko napadení, ztráty dat a provozních výpadků.

Podle analýzy společnosti Acronis patří mezi nejčastější techniky sociálního inženýrství:

1. **Vyvolání strachu.** Potenciální oběť dostane například e-mail oznamující exekuci, pokud finančnímu úřadu nezaplatí smyšlený dluh na dani s pomocí přiloženého odkazu.
2. **Brnkání na strunu chamtivosti.** Tou je třeba e-mail či zpráva na Facebook Messengeru oznamující výhru v loterii či nového iPhoneu za poskytnutí osobních informací a údajů k bankovnímu účtu.
3. **Vzbuzení zvědavosti.** Příkladem jsou falešné e-maily od přepravních společností typu DHL či FedEx s oznámením chybné adresy a odkazem k její opravě vedoucím na infikované stránky.
4. **Žádost o pomoc.** Poslaná z ukradeného účtu známého na sociální síti s prosbou o rychlé zaslání finančních prostředků na přiložený účet.
5. **Zneužití empatie či soucitu.** Sociální inženýrství nekvete jen online, ale jeho obětí se člověk může stát i v reálném světě, pokud třeba vyhoví prosbám neznámé osoby o vpuštění do budovy s výmluvou, že si zapomněla vstupní kartu.

Zdroj: AVcentrum ČR