Acta Informatica Pragensia
2(1), 2013, 122–124, DOI: 10.18267/j.aip.18
Online: aip.vse.cz

Sekce / Section:
Knižní recenze / Book reviews

Sociální inženýrství aneb umění klamu

Tomáš Klíma[1]

[1] Katedra systémové analýzy, Fakulta informatiky a statistiky,
Vysoká škola ekonomická v Praze
nám. W. Churchilla 4, 130 67 Praha 3

tomas.klima@vse.cz

Abstrakt: Recenze knihy Umění klamu od Kevina Mitnicka, která nám představuje sociální inženýrství jakožto nástroj, který je v současnosti plnohodnotným doplňkem k technicky založeným prostředkům v arzenálu narušitelů informační bezpečnosti. Na rozdíl od nich však netrpí tak rychlým zastaráváním, proto je pohled na jeho základy od jednoho z nejproslulejších hackerů stále aktuální a má informační hodnotu nejen pro řešitele bezpečnosti, ale i pro běžné uživatele, kterých se probíraná problematika bezpochyby týká.

Klíčová slova: recenze, sociální inženýrství, sociotechnika, informační bezpečnost

Title: Social engineering or the art of deception

Abstract: Review of the Kevin Mitnick´s book Art of deception. This book introduces to us the social engineering as complementary tool to technically-based approaches to penetration of information security of organisations. Unlike these approaches the social engineering doesn´t become obsolete so fast which means this book has a value for the IT security guys as well as for the end users who are the main victims of social engineering.

Keywords: Review, Social engineering, Information security

RECENZE KNIHY

MITNICK, Kevin, SIMON, William. *Umění klamu*. 1. vyd. Gliwice: Helion, 2003. 345 s. ISBN 83-7361-210-6.

Sociální inženýrství neboli sociotechnika je jedním ze způsobů, jak mohou útočníci narušit bezpečnost organizace bez použití technických nástrojů. Spoléhají přitom na nejslabší článek, v tomto případě na lidský faktor, který bývá při řešení bezpečnosti často neprávem opomíjen. Jedním z nejúčinnějších a nejúčelnějších způsobů ochrany je vzdělávání uživatelů a jejich informovanost o metodách, které útočníci využívají. Přitom ovšem řešitelé bezpečnosti narážejí na problém nedostatku kvalitní literatury (zejména v českém překladu), která by byla nejen obsahově kvalitní, ale zároveň i čtivá a pro čtenáře, neznalého IT světa a terminologie, atraktivní.

Monografie Umění klamu od Kevina Mitnicka bezpochyby výše zmíněné požadavky splňuje, navíc je již jméno autora zárukou, že půjde o fundovaný výklad podložený vlastní praktickou zkušeností (která nicméně autora přivedla na řadu let do vězení). Na 345 stranách je v šestnácti kapitolách členěných do čtyř oddílů probráno vše potřebné k pochopení podstaty útoku a obrany proti manipulaci sociálním inženýrem.

První oddíl se věnuje představení slabin informačních systémů a vysvětluje, jak jsou organizace pomocí sociotechniky zranitelné. Druhý pak popisuje, jak sociotechnici využívají ochotu a důvěru uživatelů k poskytnutí požadovaných informací. Vše je demonstrováno na základě "fiktivních historek". Při bližším zkoumání a zběžné znalosti autorovy další tvorby je ovšem zřejmě, že tyto historky jsou často založené na skutečných případech, jen identifikační údaje firem a zaměstnanců jsou z pochopitelných důvodů pozměněny.

V třetím oddíle jsou pak rozvinuty další scénáře, které ukazují možnosti hlubšího průniku do infrastruktury firmy a odcizení citlivých údajů. Také jsou nastíněny motivy útočníků od prosté pomsty propuštěného zaměstnance až po kyberterorismus. Čtvrtý oddíl představuje způsoby možné obrany. Konkrétně se jednotlivé kapitoly tohoto oddílu zaměřují na tvorbu účinného školení a návrh bezpečnostní politiky organizace[1].

V závěru se pak nachází "bezpečnost v kostce", neboli shrnutí klíčových informací formou seznamů a tabulek. Zvláštní pozornost je vhodné mimo jiné věnovat předmluvě, která v krátkosti shrnuje autorův (kontroverzní) život a zdůvodňuje jeho odborné směřování. Pokud by ovšem čtenář chtěl získat o autorovi více informací, je vhodné se obrátit na nezávislé zdroje.

Jazyková úroveň monografie je na slušné úrovni a je třeba vyzdvihnout fakt, že na rozdíl od mnoha konkurenčních titulů v oblasti bezpečnosti informací, či konkrétně bezpečnosti IT, nedošlo při překladu ke zmatení termínů, což je ovšem i částečně dáno netechnickou povahou publikace.

[1] Šestnáctá kapitola obsahuje vzor bezpečnostní politiky firmy, který je možné upravovat "na míru" konkrétní organizaci.

Text je vhodně členěn do krátkých podkapitol dle jednotlivých příkladů a scénářů, což usnadňuje čtení a následně i pochopení. Pokud nepočítáme přílohy, není text doplněn obrázky ani grafy, což lze ovšem vzhledem k povaze textu omluvit.

Vzhledem k faktu, že autor se knihou obrací zejména na koncové uživatele a na řešitele bezpečnosti připravující jejich školení, je zvolena odpovídající úroveň odbornosti textu, který je srozumitelný i bez předchozí znalosti terminologie či teorie bezpečnosti informačních systémů. Osobně bych čekal, že autor v dalších publikacích půjde hlouběji a zaměří se na detaily konkrétních typů sociotechnických útoků[2]. Bohužel tomu tak není a Mitnick dále vesměs zůstáva na povrchu a zkoumání detailů nechává pak na svých následovnících.

Celkově lze tuto knihu (i další díla autora) doporučit pro seznámí s fenoménem sociálního inženýrství, zejména s jednotlivými technikami a postupy, které jsou využívány k oklamání koncových uživatelů a následně k získání patřičných informací (hesla, interní údaje). Pokud s tímto uživatel obeznámen není, existuje zde velké riziko, že při samotném útoku sociotechnika nejenže poskytne požadované informace, ale dokonce ani s odstupem času nedokáže identifikovat, že byl oklamán, a incident tak zůstane nezachycen, což v důsledku znamená, že vyzrazené informace mohou být dále použity k hlubší úrovni průniku do infrastruktury firmy (např. s využitím technických nástrojů).

Přestože se může zdát, že tento typ útoků se v našich zeměpisných šířkách prakticky nevyskytuje a spíše než přímého kontaktu s pracovníky se využívá phishingu (včetně jeho „cílené“ podoby spear phishingu), rozesílání malwaru a dalších technik „hromadného ničení“, opak je pravdou, o čemž svědčí i fakt, že IT bezpečnostní firmy působící na našem území, jmenovitě ESET[3], již do své nabídky penetračního testování (způsob ověřování bezpečnosti systémů organizace) zařadily i testy ve formě fingovaného sociálního inženýrství, ať už se jedná o ověřování reakce pracovníků na přímý osobní, telefonický či mailový kontakt.

Na závěr bych tedy pro ilustraci sofistikovanosti útoků, se kterými se můžeme setkat, použil slova samotného Mitnicka: „Dobrý sociotechnik plánuje svůj útok jako šachovou partii, předvídá otázky, které může oběť klást a připravuje si patřičné odpovědi.“ Kniha, kterou jsme si dnes představili, by nám tedy měla pomoci, aby naše organizace takovou partii lacině neprohrála.

SEZNAM POUŽITÝCH ZDROJŮ

[1] MITNICK, Kevin, SIMON, William. Umění klamu. 1. vyd. Gliwice: Helion, 2003. 345 s. ISBN 83-7361-210-6.

[2] Dnes je zejména populární využívat sociotechniky ve spojení s phishingem, distribucí malware, a dalšími prostředky, k čemuž jsou již dostupné i softwarové nástroje - např. modul SET (Social Engineering Toolkit) dostupný v Metasploitu. Využití tohoto spojení sociotechniky se speciálním softwarem/malwarem stojí za několika významnými datovými úniky z poslední doby (např. RSA). Tento trend je v krátkosti zmíněn v kapitole 7, odkazy na malware a spyware jsou pak na několika dalších místech v knize.

[3] Viz webová stránka: http://www.eset.cz/cz/firmy/eset-services/bezpecnostni-audit/socialni-inzenyrstvi/