Pozor na lidi

Neposkytujte o sobě více informací než je opravdu nutné!

MARTIN IGNJATOVIĆ

Je to právě rok, co do naší země zavítal Kevin Mitnick. Je to člověk, který se proslavil průnikem do mnoha systémů po celém světě. Některé „kousky" jsou mu připisovány neprávem a o jeho schopnostech superhackera se také vedou diskuse, zanechal v dějinách počítačové bezpečnosti nesmazatelnou stopu.

Proslavil se zejména svojí manipulací s lidmi a využíváním jejich nedbalosti. Proto se na techniku, kterou používal, podíváme blíže.

Práce s lidmi souvisí s bezpečností informačních systémů mnohem více, než se všeobecně předpokládá. Tato technika, anglicky zvaná social engineering, je mezi útočníky na počítačové systémy velmi oblíbená. Český ekvivalent se hledá velmi těžko, proto se budeme držet anglického označení SI. Je to totiž jeden z nejsnazších způsobů napadení cílového systému. Od útočníka vyžaduje pouze trochu bystrosti a dobré vyjadřovací schopnosti. Nyní se podíváme na to, jaké techniky a triky se při tomto druhu útoku používají, a řekneme si, jaká lze proti nim použít aktivní opatření.

Cílem tohoto útoku je zpravidla získání citlivých informací či přímo průnik do systému. Útočník se bude snažit zjistit různé informace. Uvedeme zde výčet věcí, které by mohly útočníka zajímat:

- struktura sítě,
- vnitřní a vnější IP adresy,
- IP adresy hraničních firewallů,
- jména a osobní informace o osobách,
- bezpečnostní politika,
- telefonní čísla a adresy,
- programové vybavení,
- hesla.

Jaké triky útočník používá?

Zpravidla se vydává za někoho jiného. Může se například stát, že si útočník zjistí jména správců sítě a pak zavolá nic netušícímu uživateli a chce po něm, aby si změnil heslo nebo změnil nastavení systému. Uživatel v dobré víře opatření provede a bezpečnostní incident je na světě. Rovněž se útočníci mohou vydávat za zástupce poskytovatele připojení a požadovat od správce sítě přenastavení firewallů nebo změnu přístupových hesel. Základním předpokladem úspěchu u tohoto druhu útoku je dobrá znalost místních podmínek a pravidel. Rovněž je užitečná znalost osob, kterých se útok týká. Pokud útočník vzbudí důvěru a prokáže znalost situace, málokdo odmítne udělat to, co požaduje. To od útočníka vyžaduje znalost prostředí. Získá ji z různých míst, ale nejčastěji z informací, které publikuje sama společnost. Zjistit jména správců sítě, registrátorů domén, webmasterů či pracovníků technické podpory dnes není žádný problém. Mnoho takových informací je publikováno na firemních webových stránkách či v propagačních materiálech konkrétních podniků. Ve státní správě je situace ještě mnohem horší. K získání podobných informací však může použít útočník rovněž SI a takzvaně „vytáhnout" tyto informace z pracovníka firmy a následně je použít k dalšímu SI útoku. Může například zavolat na informační linku společnosti a představit se jako zástupce firmy, která se zabývá prodejem softwaru. Bude požadovat jména a telefonní čísla osob, na něž se může se svojí nabídkou obrátit. Triků je opravdu mnoho a záleží jen na útočníkově vynalézavosti a šikovnosti, jaké informace může zjistit. Nejsou výjimkou situace, kdy se útočníkovi podaří zjistit hesla k důležitým systémům a klíčovým serverům. Klamat však nemusí útočník jen po telefonu, ale i přes fax či e-mail. Nyní se podíváme na to, jak snížit riziko podobného průniku.

Zkuste snížit riziko průniku

Základním pravidlem by mělo být utajování informací souvisejících s bezpečností. Měl by být stanoven okruh informací a lidí, kteří k nim mají přístup. Je zbytečné, aby manažeři znali přístupová hesla k hlavním systémům, i když to často vyžadují, spíše kvůli své pozici než ze skutečné nutnosti. Toto riziko lze eliminovat zavedením falešného administrátorského účtu s nízkým oprávněním. Funguje opravdu spolehlivě. Další nutnou věcí je důkladné proškolení všech uživatelů o tom, jaké informace a komu smějí předávat. Není na škodu občas prověřit dodržování takových opatření a směrnic. Rovněž je důležité neposkytovat více informací než je opravdu nutné a všechny informace, které nejsou nezbytně potřebné, vyhledat a stáhnout z veřejných zdrojů. 4 0358/FEL ❑