Bezpečná hesla

aneb Jak vyřešit autentizaci do podnikových systémů a přitom neudělat uživatelům ze života peklo

Petr Šnajdr

Hesla pro přístup do systémů používají lidé velmi dlouho. Dlouho byla jedinou překážkou pro vstup neoprávněné osoby. O bezpečnosti hesel se diskutuje poměrně často, přesto však existuje velké množství uživatelů, pro které je bezpečné heslo synonymem pro složitost, otravu, a dokonce zbytečnou šikanu správců systémů. Přitom správně zvolené bezpečné heslo dokáže téměř zázraky. Minimálně tedy dokáže zásadním způsobem znesnadnit prolomení autentizačních procesů.

Jak jsme se ale v posledních letech přesvědčili, bezpečnost hesel není vždy problémem běžných uživatelů, ale v některých případech i správců systémů. Příkladem byla operace Windigo, při které došlo ke zneužití několika tisíc serverů. Během vyšetřování se následně zjistilo, že obrovské množství správců systémů použilo hesla typu 123456, admin atp. Uvnitř firemní sítě by prosté heslo stačit mohlo. Bohužel pro přístup k firemním datům z internetu prosté heslo nestačí. Uživatel by se totiž k systému mohl přihlásit z jakéhokoli, třeba i z kompromitovaného zařízení, kde by heslo mohlo jednoduše odejít neoprávněné osobě.

Na bezpečnost kritických systémů je kladen důraz dlouhodobě, firmy se čím dál častěji poohlížejí i po dalších bezpečnostních vrstvách, které zamezí neoprávněnému přístupu do sítě ze strany zaměstnanců nebo úplně cizích lidí. To ovšem v době nárůstu práce mimo kancelář a fenoménu BYOD (přines si vlastní zařízení) není zrovna jednoduchý úkol. Častou a efektivní odpovědí na tyto problémy firmy je, že sahají po řešeních pro dvoufaktorovou autentizaci (2FA).

Je třeba si ale uvědomit, že i když tento systém jednoznačně pomáhá předcházet podvodům a útokům ze strany kyberzločinců, rozhodně se nejedná o všelék na všechny hrozby. Mnohé služby 2FA používají dlouhodobě a v daném segmentu se jedná o standard. Přesto jsou tímto způsobem chráněné sítě a data stále zranitelné, o čemž svědčí neustálé a často úspěšné útoky hackerů.

Jak tedy všechny ty uživatele identifikovat? Jak zajistit bezpečnost zařízení a systémů? Zdaleka nejběžnějším příkladem identifikátoru je jméno nebo název účtu. Je to snadný způsob, jak dát vědět počítačovému systému, kdo jste. Tento postup ale samozřejmě nemůže dokázat, že jste to opravdu vy. Proto vám ve většině případů systém nedovolí cokoli měnit nebo používat, dokud nedokážete, že jste skutečně osoba, kterou zná a která má povolení systém používat. Nebudete tak schopni počítač používat, dokud neprokážete vaši identitu prostřednictvím zadání hesla, které byste měli znát pouze vy. Kombinace uživatelského jména a hesla je jedním příkladů bezpečnostního opatření nazývaného autentizace. Lidé mají svá hesla nebo PIN kódy a používají je, aby dokázali, že jsou oprávnění používat něco, k čemu je omezený přístup. Všem je tedy jasné, že může jít například o soukromý prostor, počítačový systém, internetovou službu nebo třeba zašifrovaný dokument. Identifikační údaje bývají často z pohodlnosti založeny na reálném jméně držitele účtu, které se tak dá snadno uhodnout. A někdy není nutné ani hádat: kdykoli s někým komunikujeme z určitého e-mailového účtu, zná téměř vždy i vaše přihlašovací jméno k e-mailové schránce.

V situacích, kdy prostá autentizace nedostačuje potřebám firemní bezpečnosti, přichází již zmíněná dvoufaktorová autentizace. Ta je schopna zajistit uživatelsky jednoduché, přesto bezpečné přihlášení. Je založena na dvou zcela nezávislých faktorech, po jejichž spojení se teprve uživatel řádně přihlásí. Mezi metody přihlášení pak patří nejčastěji kombinace:

- **„Něco vím.“** Něco, co uživatel musí znát. Typická jsou přístupová hesla, správná kombinace znaků, pro bankomaty nebo mobilní telefony PIN kódy, a také správné odpovědi na „bezpečnostní otázky“.
- **„Něco jsem.“** Tato třída zahrnuje využívání biometrických senzorů pro snímání otisků prstů, sítnice a duhovky, nebo algoritmy pro měření charakteristiky chování jako rytmus psaní nebo identifikace hlasu.
- **„Něco mám.“** Něco, co uživatel vlastní. Patří mezi ně fyzické klíče, průkazy totožnosti, a také komunikační zařízení, např. hardwarový token, standardní mobilní telefon nebo smartphone.

V internetových službách kromě „něco vím“ ve formě hesla nastupuje další faktor, nejčastěji v podobě zasílání SMS zpráv na mobilní telefon (něco mám), nebo aplikace pro tvorbu jednorázových hesel ve smartphonech. Hlavní výhoda tohoto systému spočívá v tom, že mobilní telefon vlastní skoro každý, a odpadá tak nutnost koupit si nebo instalovat novou platformu, která by sama o sobě plnila pouze funkci dalšího autentizačního faktoru. U mobilních zařízení se ale dostáváme k dalšímu problému. Taková zařízení musí být chráněná před zneužitím neoprávněnou osobou.

Pokud se tedy chcete přihlásit ke svému profilu, systém předpokládá, že jste to právě vy, kdo má u sebe mobilní telefon, na nějž přijde po zadání přihlašovacího jména a hesla jednorázový PIN. Útočník by pak musel nejen získat vaše heslo, ale také mobil, bez něhož by neměl šanci se k vašemu účtu přihlásit.

Dříve se objevovaly názory, že hackeři dosud nikdy neprolomili webové stránky, do nichž byla implementována dvoufaktorová autentizace. Na webu není nic úplně bezpečné. Stránky zabezpečené dvoufaktorovou autentizací pak hackery lákají vysoce hodnotným obsahem. Implementace 2FA dozajista zvýší

bezpečnost, stále však zůstává celá řada významných slabin. Úroveň zabezpečení se totiž také může u jednotlivých dodavatelů technologie velmi lišit. Potenciální hrozbou může být kromě útočníka také dodavatel služby, jak dokazuje mj. případ hardwarových tokenů SA SecurID z roku 2011. U varianty na bázi SMS, která je zdaleka nejčastější, se bezpečnost liší u jednotlivých mobilních operátorů a je zranitelná, pokud např. změníte telefonní číslo. Kyberzločinci také dokážou nainstalovat malware na mobilní zařízení a sledovat textové zprávy obsahující dvoufaktorový autentizační kód.

Mobilní zařízení jsou oblíbená proto, že je vlastní skoro každý a jsou schopna jednoduše ověřit identitu uživatele propojením skryté informace a zapamatovaného hesla v rámci jednoho přístroje. Aplikaci můžete používat ve spojení s něčím, čím se uživatel může prokázat jako něčím, co má (smartphone) a zároveň zná (např. jednorázové heslo). Tato aplikace pak může uživatele vyzvat k autentizaci a využít k tomu šifrovacích technik.

2FA se vyvíjí zejména v posledních několika letech. Původní varianta využívala technologii hardwarových tokenů, které nabízely jednorázová hesla. V poslední době se začalo využívat častěji zpráv SMS a dalších mobilních technologií. Dnešní dvoufaktorová autentizace typicky využívá mobilních aplikací. Dnes už nespoléhá čistě na jednorázová hesla generovaná aplikací. V rámci usnadnění interakce s uživateli velmi často nabízí řešení pro 2FA i tzv. push notifikace, u kterých může uživatel na obrazovce jen potvrdit přihlášení ke konkrétnímu systému či aplikaci. Zásadně se tak minimalizují stížnosti zaměstnanců na složitost používání bezpečnějších technologií.

Jak tedy splnit požadavky na bezpečnost systémů, a přitom neudělat uživatelům dalšími požadavky z autentizace peklo? Během své dlouholeté praxe jsem se snažil uživatelům vysvětlit, že nejde jen o složitost hesla. Že ruku v ruce s tím musí jít pravidelná obměna hesel, nepoužívat stejná hesla pro několik služeb. Uživatelé si časem zvyknou na používání dvoufaktorové autentizace ve firemním prostředí, protože tvorbu složitých hesel a jejich obměnu si dokáží obejít. Pochopitelně nevystavují riziku jen sebe, ale i firemní data. Přitom dnes existují flexibilní metody autentizace, které uživatelům zajistí pohodlný přístup a zároveň přijatelně nízké riziko. Je samozřejmě nutné si uvědomit, že pokaždé jde o kompromis mezi uživatelským pohodlím a bezpečností. Ve světle nových nařízení

a hrozících pokut správci pravděpodobně rezignují na domluvy, přijmou výčitky a nadávky uživatelů, ale systémy budou bezpečnější. Nikdy nebudou stoprocentně bezpečné, vícefaktorová autentizace však minimalizuje riziko pod kritickou úroveň. ■

Petr Šnajdr

Autor článku pracuje jako business development manager pro značku Trend Micro ve společnosti Veracomp.