

Nebezpečná „bezpečná hesla“, aneb klíče pod rohožkou

Zajistit bezpečnost je snad nejkomplexnější úkol v IT. V praxi často dochází k nevyváženému zabezpečení, čímž mohou být degradovány i dokonalé bezpečnostní systémy. V každém systému se objevuje mnoho různých dat, objektů či aplikací, které jsou chráněny heslem, tedy softwarovým klíčem. Pojďme společně hledat tyto „klíče pod rohožkou“.

Nestavme tento článek jako popis technik profesionálních hackerů. Existuje totiž mnoho profesionálních podvůdků a technik, jak klíče vymámit. My nyní nic mámit nebudeme. Jen sebereme to, co nám uživatel schová pod rohožku. Takový klíč pod rohožkou pak může sebrat i šikovnější uživatel a zneužití pak můžete čekat i od kolegy či „kamaráda“. Tímto způsobem se například dostanou po odhalené fotky z vašeho soukromí do cizích rukou, vaši známí dostanou e-mail odeslaný cizí rukou pod vaši hlavičkou s velmi ztrapňujícím obsahem. Vaše osobní citlivá data zjistí někdo nepatřičný. Někdo zneužije váš bankovní účet nebo registraci v elektronickém obchodě. To samé se pak samozřejmě týká vašich zákazníků, kterým se staráte o jejich IT.

Jednoduchá hesla

Jednoduchá hesla je snadné uhodnout. Ve smyslu tohoto článku je klíčem pod rohožkou heslo uhodnutelné i bez speciálních programů, jako jsou jména dětí, manželek, milenců, rodná čísla, telefonní čísla apod.

Informujte svoje zákazníky, že pokud používají jakékoliv přihlášení do internetových formulářů, jako jsou například e-shopy, volné e-maily apod., že se dříve nebo později pokusí nějaký jejich „kamarád“ přihlásit po nich za ně. Přihlašovací jméno zůstane předvyplněno v prohlížeči. A heslo? Tak co asi vyzkouší...

Hrozba stejných hesel

Hrozba stejných klíčů pro různé účely je trojí. Jednak když už někdo získá klíč, dostane se do dvou místností naráz a udělá dvojnásobnou škodu. Potom také, získat jeden ze dvou stejných klíčů je mnohem snazší, obzvlášť když jsou klíče uloženy a zabezpečeny samostatně. Zvyšuje se pravděpodobnost, že u jednoho z klíčů bude uložení nevhodné.

A za třetí, někdy může být nutné klíč zapůjčit dočasně někomu jinému. Soused, který klíčkem vybírá schránku po dobu dovolené, by

také mohl vybrat sekretář, pokud bude klíček od schránky stejný, jako klíče od domu.

Počítačová praxe

Pokud „kamarád“ zná jediné heslo, věřte, že jej zkusí použít i k přihlášení i do jiných aplikací, které se používají. Zatímco některé aplikace, zpravidla s nevelkým bezpečnostním dopadem, mají velmi nedbale vyřešenou správu hesel, jiné aplikace, jež jsou naopak velmi bezpečnostně citlivé, musejí mít uživatelské údaje, jako jsou klíče, uloženy velmi bezpečně.

Pokud o těchto dvou aplikacích bude stejné heslo, pak tu velmi dobře zabezpečenou aplikaci lze odemknout klíčem druhé aplikace, která jej nechává například v textovém souboru, který se může jmenovat třeba uzivatele.cfg a je čitelný v otevřené podobě.

Nedokonalost dokonalých hesel

A teď z opačného konce. Rozhodnete se u zákazníka nasadit opravdu dokonalá hesla, která nejsou uhodnutelná, jsou tvořena kombinací písmen, číslic, speciálních znaků, jsou dlouhá třeba deset znaků, a doporučíte mu pravidelně a často hesla měnit, používat pro každou aplikaci jiné heslo. Je tato varianta bezpečná? Ve smyslu tohoto článku bezpečná nejsou. Jak odhalil průzkum prováděný firmami Nucleus Research a KnowledgeStorm, zavedení tvrdých požadavků na hesla má jen malý výsledný efekt v navýšení bezpečnosti. Důvodem je totiž vysoká náročnost správy takových hesel.

Představte si pět hesel, třeba do pošty, intranetu, e-shopu, do ceníku, do ekonomického systému, internetového bankovníctví, ICQ, Skype... Pět účtů má asi většina uživatelů IT. Každý čtvrtý pracovní den pak přijde požadavek na změnu hesla. Pokud je patřičně složité, musejí být pro každou aplikaci jiná a nemůže se opakovat, pak je tento systém pro uživatele zatěžující, nemůže si tato hesla pamatovat, a nakonec z toho zapomene i své křestní jméno. Východiskem jsou pak pro něj papírky nalepené na monitoru, zespona klávesnice, v textovém dokumentu na ploše apod. Tak... a zase tu máme klíče pod rohožkou.

Existuje řešení?

Jedním ze způsobů řešení je nepoužívat hesla, ale nějaký jiný způsob ověření, třeba otisky prstů, karty, plovoucí hesla apod. Jenomže co s existujícími aplikacemi? Některé už těžko upravíte, aby se neptaly na heslo, ale na prst nebo na kartu.

Pokud není možné upravit aplikaci, tak lze použít malou lest. Můžete totiž použít software, který je schopen rozpoznat přihlašovací okno do aplikace a zadat heslo za vás. Tento software usnadní život tím, že si uživatel nemusí hesla pamatovat ani nikam zapisovat na papírky apod. Software si pamatuje hesla za něj, ale tak bezpečně, aby se k nim nikdo jiný než on nedostal. K těmto heslům se dostane a nechá automatické přihlašování do aplikací fungovat. Samozřejmě si tento software uživatele přede velmi důkladně ověří. K tomu má mnoho nástrojů, včetně zmíněných čipových karet, otisků prstů apod. Hesla, která si pamatuje, je schopen i automaticky měnit, a pokud je třeba, pak je může i bezpečně synchronizovat s jinými systémy.

Centrální systém

Nejvyšší stupeň řešení zabezpečení přístupu je využití centrálního systému pro řízení přístupu k datům. Toto řešení vyžaduje, aby byla bezpečnostní část aplikace navržena podle otevřených standardů, případně je nutné upravit. Aplikace se vzdá vlastního mechanismu ověření uživatele, tedy zadávání jména a hesla, a přenechá tuto činnost specializovanému softwaru. Ten zajistí bezpečné ověření uživatele. Pokud je již uživatel bezpečně ověřen, není nutné jej opakovaně ověřovat při opětovném přístupu k aplikaci.

Když tento centrální systém přihlášení využívá více aplikací, pak je možné nastavit bezpečnostní skupiny a role pro křížová oprávnění. Takto se mohou například z jedné webové stránky, například jako účetní ve firmě, prokliknout na e-mail, ceník produktů, účetní výkazy, aniž bych byli těmito aplikacemi opakovaně vyzýváni k zadání hesla. Již první zadání hesla nebo projetí kartou, prstem apod. bylo dostatečným důkazem, že jsem to já, účetní.

Nasadte vyspělý systém

V reálném životě, pokud nestavíte na zelené louce, bývá nejčastěji použita kombinace všech těchto uvedených variant řešení. Vyspělé systémy jsou schopny tyto způsoby kombinovat a vzájemně propojit do jednoho celku. Uživatel pak nemusí dávat klíče pod rohožku, ani nosit velké svazky klíčů. ■

Ing. Petr Klabeňš pracuje u distributora Avnet Technology Solutions jako IBM Software Business Development Manager