Obsah

Vážené čtenářky, vážení čtenáři,

není to tak dávno, co nám k přihlášení k naprosté většině internetových služeb postačovalo jméno a heslo. Ta však představují pro obě strany v poslední době značné riziko, zejména kvůli masivním únikům osobních dat.

Navíc kvůli vyžadování poměrně striktních pravidel, co se týče skladby takového hesla, je pro mnohé lidi velice obtížné si je zapamatovat, takže se stále častěji uchylují k tomu, že jedno heslo využívají pro různé účty – a tím se zranitelnost hesel dále znásobuje.

Určitý přelom sice přinesly (pokud pomineme nepohodlné tokeny) softwarové moduly, které pro potvrzení už mohly využít například biometrické ukazatele uživatele, často ale šlo o proprietární řešení, které se vlastně nemohlo použít nikde jinde.

Jako mnohem univerzálnější se pak jeví systémy dvoufaktorové autentizace, které zavedli velcí dodavatele mobilních platforem. Zejména nejnovější aktivita Googlu má velké ambice – nově totiž budou muset všichni jeho uživatelé ve výchozím nastavení používat pro zabezpečení svých účtů dvoufaktorovou autentizaci. To už sice mohli dělat i dříve, avšak na volitelné bázi, nově to bude tzv. defaultní (Google později upřesnil, že tuto možnost bude možné vypnout).

Google tak umožní spravovat přístupy uživatelů do dalších jejich služeb – v podstatě stačí potvrdit zadání uchovaného hesla k příslušnému webu například otiskem prstu, a celý proces autentizace se uskuteční díky řešení Google Authenticator automaticky – v podstatě tak dojde ke sloučení dvou faktorů – toho, který znáte (hesla, jež máte k odpovídající službě), a toho, kterého máte (autorizovaný telefon).

Hesla lze navíc z různých internetových prohlížečů či správců hesel jednoduše importovat do řešení Google Password Manager. Ten také může generovat obtížně prolomitelná hesla pro internetové služby, ke kterým se nově přihlašujete. Přínosná je bezesporu i služba Password Checkup, jež zkontroluje, jestli se některá vaše hesla nestala součástí úniků dat nebo hackerských útoků.

Podmínkou je, abyste měli účet Googlu „správně nakonfigurovaný" – v tomto případě jde především o nastavení telefonního čísla a sekundárního e-mailu – zřejmě jste se s vynucováním těchto údajů už sami setkali.

Google to považuje jen za počátek přechodu od složitých hesel. Nic však není úplně černobílé. Dvoufaktorová autentizace, ač se jeví jako bezpečnější než hesla, má sama také řadu nedostatků a zranitelností, které mohou vést k jejímu prolomení. Jaké to jsou, vám přibližuje jeden z příspěvků v tomto vydání Security Worldu.

A v těchto dnech si také připomínáme páté výročí objevení malwaru Petya a WannaCry, které znamenaly doslova revoluci v pojetí škodlivého kódu. Jejich základní nekalou činností totiž bylo zašifrovat uživatelské soubory a následně po obětech vyžadovat výkupné – ano, v roce 2016 se začal ve větší míře prosazovat ransomware, v současnosti zřejmě největší kybernetická hrozba zejména pro firmy.

Co všechno vám ransomware v moderní podobě může způsobit, jaké jsou ztráty, které vám zapříčiní, a zda je řešením zaplacení výkupného – to vše vám objasní tento Security World.

S přáním příjemně stráveného léta třeba i nad stránkami Security Worldu

Pavel Louda
vedoucí projektu