

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 45 ze dne 5.9.2023

Tipy pro firemní politiku hesel

Netrapte zaměstnance příliš složitými pravidly pro používání hesel, spíše vytvořte černou listinu běžně používaných hesel nebo zvolte další způsoby, jak zvýšit bezpečnost zaměstnaneckých účtů i celé vaší organizace.

Když inženýr Bill Burr z amerického Národního institutu standardů a technologie (NIST) napsal v roce 2003 dokument, který se brzy stal zlatým standardem pro zabezpečení hesel, doporučil lidem a organizacím, aby své účty chránili vymyšlením dlouhých a "chaotických" řad písmen, čísel a znaků a aby je pravidelně měnili. O čtrnáct let později Burr přiznal, že svých rad lituje. *"Lidi to prostě přivádí k šílenství a nevybírají si dobrá hesla, ať děláte, co děláte,"* řekl deníku Wall Street Journal.

Nebo jak to vyjádřil slavný komiks: *"Díky dvacetiletému úsilí jsme všechny úspěšně naučili používat hesla, která jsou těžko zapamatovatelná pro lidi, ale snadno uhodnutelná pro počítače."*

Nejnovější vývoj v tvorbě silných hesel

V dnešní době si průměrný člověk musí pamatovat až 100 hesel, přičemž jejich počet v posledních letech rychle roste. Studie ale zjistily, že lidé si obvykle pamatují jen okolo pěti hesel a ulehčují si práci vytvářením snadno uhodnutelných hesel, která pak recyklují u různých online účtů. Někteří z nich mohou skutečně nahradit písmena číslicemi a speciálními znaky (např. "heslo" se změní na "P4??WØrd"), ale i tak jde o heslo, které je snadno prolomitelné.

V posledních letech přední organizace, jako je The Open Web Application Security Project (OWASP) a samozřejmě i samotný NIST, posunuly své zásady a rady směrem k uživatelsky přívětivějšímu přístupu při současném zvýšení bezpečnosti hesel. Technologičtí giganti, jako je Microsoft a Google, zároveň vyzývají všechny, aby se zcela vzdali hesel a přešli na bezheslové přihlašování.

Pokud však vaše malá nebo střední firma ještě není připravena se s hesly rozloučit, přinášíme vám několik doporučení pro vytvoření firemní politiky hesel, která vám pomůže zvýšit firemní bezpečnost.

Přestaňte zavádět zbytečně složitá pravidla pro vytváření hesel

Jakákoli příliš složitá pravidla pro vytváření hesla (například požadavek, aby uživatelé uváděli velká i malá písmena, alespoň jednu číslici a speciální znak) již nejsou nutností. Jedná se o jednu z nejčastějších chyb při tvorbě požadavků na hesla, která jen málokdy povzbudí uživatele k nastavení silnějších hesel. Místo toho takové pravidlo nabádá k vymyšlení hesel, která jsou slabá a zároveň obtížně zapamatovatelná.

Přejděte na přístupové fráze

Místo kratších, ale složitých hesel používejte heslovou frázi. Takové heslo je delší a složitější, ale stále snadno zapamatovatelné. Může to být například celá věta, která vám z nějakého důvodu utkvěla v hlavě, doplněná velkými písmeny, speciálními znaky nebo emoji. I když není nijak extra složitá, automatickým nástrojem bude její prolomení trvat celou věčnost.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 45 ze dne 5.9.2023

Před několika lety byla minimální délka silného hesla osm znaků a skládalo z malých a velkých písmen, speciálních znaků a čísel. Dnes dokážou automatizované nástroje na prolamování hesel takové heslo uhodnout během několika minut, zejména pokud je zabezpečeno pomocí hashovací funkce MD5. Vyplývá to z testů provedených společností Hive Systems z dubna 2023. Naopak prolomení jednoduchého hesla, které obsahuje pouze malá a velká písmena, ale je dlouhé 18 znaků, trvá mnohem, mnohem déle.

Počet znaků	Pouze čísla	Malá písmena	Malá a velká písmena	Čísla, malá a velká písmena	Čísla, malá a velká písmena, speciální znaky
4	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
5	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
6	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
7	okamžitě	okamžitě	1 s	2 s	4 s
8	okamžitě	okamžitě	28 s	2 min	5 min
9	okamžitě	3 s	24 min	2 h	6 h
10	okamžitě	1 min	21 h	5 dní	2 týdny
11	okamžitě	32 min	1 měsíc	10 měsíců	3 roky
12	1 s	14 h	6 let	53 let	226 let
13	5 s	2 týdny	332 let	3 tis. let	15 tis. let
14	52 s	1 rok	17 tis. let	202 tis. let	1 mil. let
15	9 min	27 let	898 let	12 mil. let	77 mil. let
16	1 h	713 let	46 mil. let	779 mil. let	5 mld. let
17	14 h	18 tis. let	2 mld. let	48 mld. let	380 mil. let
18	6 dní	481 tis. let	126 mld. let	2 bil. let	26 bil. let

Vyžadujte minimálně 12 znaků

Pokyny NIST uznávají délku jako klíčový faktor síly hesla a zavádějí minimální požadovanou délku hesla 12 znaků a maximálně 64 znaků. Důležitým pravidlem pro tvorbu silného hesla tedy je – čím delší, tím lepší.

Povolte různé znaky

Uživatelé by měli mít při nastavování hesla možnost volby ze všech tisknutelných znaků ASCII a UNICODE, včetně emotikonů. Měli by mít také možnost používat mezery, které jsou přirozenou součástí heslových frází.

Omezte opakované používání hesel

Dalším faktorem, který přispívá k bezpečnosti hesla je, aby nebylo opakovaně používáno k různým online účtům, protože prolomení jednoho účtu může snadno vést ke kompromitaci dalších účtů.

To nicméně uživatelé obtížně dodržují a přibližně polovina respondentů studie Ponemon Institute z roku 2019 přiznala, že opakovaně používá v průměru pět hesel ke svým firemním a/nebo osobním účtům.

Nestanovujte pro hesla datum expirace

NIST nedoporučuje vyžadovat pravidelné změny hesel, pokud o to uživatel nepožádá nebo pokud neexistuje důkaz o kompromitaci účtu. Odůvodňuje to tím, že uživatelé nemají mnoho trpělivosti s neustálým vymýšlením nových silných hesel. Nutit je k tomu v pravidelných intervalech, tak může přinést více škody než užitku.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **45** ze dne **5.9.2023**

Mějte na paměti, že se jedná pouze o obecné rady. Pokud zabezpečujete aplikaci, která je pro vaši firmu klíčová a atraktivní pro útočníky, můžete své zaměstnance stále nutit k pravidelné změně hesla.

Vykašlete se na nápovědy a kontrolní otázky

Nápovědy k heslům a ověřovací otázky založené na znalostech o uživateli jsou zastaralé. Sice mohou uživatelům pomoci při hledání zapomenutých hesel, ale zároveň mohou být velmi cenné pro útočníky. Jake Moore několikrát ukázal, jak mohou hackeři zneužít stránku "zapomenuté heslo" k tomu, aby se nabourali do cizích účtů, například na PayPal a Instagramu.

Například otázku typu "Jaké bylo jméno vašeho prvního domácího mazlíčka?" lze s trochou hledání nebo sociálního inženýrství snadno zjistit, a pro automatické nástroje se také nejedná o nekonečné množství možností, které musí projít.

Vytvořte černou listinu běžných hesel

Spíše než spoléhat na to, jak uživatel tvořil minulá hesla, kontrolujte nová hesla vůči "černé listině" nejčastěji používaných a/nebo dříve kompromitovaných hesel.

V roce 2019 Microsoft skenoval účty svých uživatelů a porovnával uživatelská jména a hesla s databází více než tří miliard sad uniklých přihlašovacích údajů. Našel 44 milionů uživatelů s kompromitovanými hesly a vynutil obnovení těchto hesel.

Umožněte používání správce hesel a dalších nástrojů

Vyberte pro uživatele ověřené nástroje pro správu hesel v prohlížeči a externí správce hesel, které jim pomohou zvládnout potíže s vytvářením a uchováváním hesel.

Dejte uživatelům možnost také dočasně zobrazit celé maskované heslo, nebo poslední zadaný znak hesla. Podle pokynů OWASP se tak zvyšuje použitelnost systému při zadávání přihlašovacích údajů, zejména když uživatelé používají delší hesla, heslové fráze a správce hesel.

Nastavte krátkou dobu platnosti pro výchozí hesla

Při zakládání účtu novému zaměstnanci systém zpravidla vygeneruje počáteční heslo nebo aktivační kód, který by měl mít alespoň šest znaků a může obsahovat písmena a číslice. Zajistěte, aby po krátké době vypršela jeho platnost a uživatel ho musel změnit.

Dávejte si pozor na proces obnovy hesla

Proces obnovy by nejen neměl odhalit aktuální heslo, ale ani to, jestli účet skutečně existuje. Jinými slovy, neposkytujte útočníkům žádné informace navíc.

Používejte CAPTCHA a dalších kontroly proti automatizovaným útokům

Používejte kontrolní mechanismy, které sníží riziko útoků hrubou silou (jako prolomení přihlašovacích údajů nebo zablokování účtu). Mezi takové kontroly patří zákaz používání nejčastěji prolamovaných hesel, zablokování účtu po x neúspěšných pokusech o přihlášení, CAPTCHA, zvyšující se prodlevy mezi jednotlivými pokusy o přihlášení, omezení určitých IP adres nebo omezení založená na lokalitě, prvním přihlášení do zařízení, nedávných pokusech o odblokování účtu apod.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 45 ze dne 5.9.2023

Podle aktuálních standardů OWASP by mělo být na jednom účtu zaznamenáno maximálně 100 neúspěšných pokusů o přihlášení za hodinu.

Nespoléhejte se pouze na hesla

Heslo je často jedinou překážkou, která odděluje útočníka od vašich cenných dat. Kde je to možné, zvýšte zabezpečení účtů ještě ověřováním pomocí dalšího faktoru (2FA/MFA).

Dejte ale pozor na to, že ne všechny metody vícefázového ověřování jsou stejně bezpečné. SMS zprávy jsou sice mnohem lepší než žádné 2FA, ale jsou zranitelnější. Bezpečnějšími alternativami je používání hardwarových zařízení a softwarových generátorů jednorázových hesel (OTP), např. zabezpečené aplikace nainstalované v mobilních zařízeních.

Jak zvýšit povědomí zaměstnanců o důležitosti silných hesel?

Vysvětlete kolegům, proč je důležité tvořit silná hesla, na co při tvorbě bezpečných hesel myslet a jak je spravovat. Zvyšujte povědomí o IT bezpečnosti a ověřujte znalost interních politik v rámci pravidelných školení.

Zdroj: AVcentrumCZ