Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-sec-passwords

BEZPIECZEŃSTWO IT

Hasła i MFA, czyli zamek, klucz i drugi ochroniarz

Hotel „Pod Złotym Hasłem” właśnie obchodził otwarcie nowego skrzydła. Trzysta pokoi, trzy windy i jeden Pan Kierownik, który postanowił uprościć system kluczy. Zamówił klucz uniwersalny. Na breloczku wygrawerował „TAJNE”, po czym przypiął go do długopisu na recepcji, żeby nikt go nie zgubił. 🔑🏨🤣

— Panie Kierowniku, dlaczego ten klucz otwiera także sejf? — zapytała pani Agnieszka.

— BO JEST UNIWERSALNY! TO SIĘ NAZYWA OPTYMALIZACJA!

— To dlaczego leży obok księgi gości?

— ŻEBY BYŁ POD RĘKĄ!

Grzesiu przyjrzał się kluczowi.

— Gratuluję. Zrobił pan hasło „123456”, tylko z metalu.

Jeden klucz do wszystkich drzwi

Na recepcji leżał zeszyt. Przy systemie rezerwacji, poczcie, monitoringu i księgowości widniało dokładnie to samo hasło: `Hotel2026!`.

— Ma wykrzyknik! — bronił się Kierownik.

— Złodziej też może go wpisać — zauważyła Agnieszka.

— Jeśli hasło wycieknie z jednej usługi, przestępcy mogą spróbować go w pozostałych — wyjaśnił Grzesiu. — To **credential stuffing**, czyli sprawdzanie skradzionych danych logowania w innych serwisach. Dlatego każde konto powinno mieć **inne, unikalne hasło**.

— TO ILE JA MAM ICH ZAPAMIĘTAĆ?!

— Pan nie pamięta nawet numeru własnego pokoju.

— BO CIĄGLE MI GO ZMIENIACIE!

— Mieszka pan w nim od trzech lat — odpowiedziała księgowa.

Długie, nieprzewidywalne, niekoniecznie z trzema wykrzyknikami

Na drzwiach pokoju 404 wisiał regulamin: „Hasło musi mieć wielką literę, cyfrę, znak specjalny i powodować u użytkownika lekki niepokój”.

— SAM PISAŁEM! — pochwalił się Kierownik.

— Ostatni wymóg spełniliśmy już dawno — westchnęła Agnieszka.

Grzesiu wskazał napis `P@ssw0rd!`.

— Zamiana „a” na małpę czy „o” na zero nie czyni popularnego hasła bezpiecznym. Liczą się **długość, losowość lub trudność przewidzenia oraz unikalność**. Menedżer może generować długie losowe hasła. Do ręcznego wpisywania sprawdza się też długa fraza ze słów wybranych losowo, jeśli usługa ją akceptuje.

— Mam! „Kierownik jest bardzo genialny”!

— Panie Kierowniku, to jest najbardziej przewidywalne zdanie w tym budynku.

— ALE DŁUGIE!

— Długość nie pomoże wystarczająco, jeśli każdy zna pana ulubione zdanie. I nie bierzemy przykładowych haseł z artykułów jako gotowych do użycia.

Recepcjonista, który pamięta tysiąc kluczy

W pokoju obok pracował recepcjonista z ogromną szafą przegródek. Każda miała inny klucz, a cały katalog był zamknięty w sejfie.

— To nasz **menedżer haseł** — powiedział Grzesiu. — Przechowuje dane logowania w chronionym magazynie, generuje unikalne hasła i pomaga je wypełniać. Nie trzeba pamiętać stu różnych ciągów znaków.

— Czyli pamiętam tylko jedno hasło główne? — zapytała Agnieszka.

— Zazwyczaj tak, plus dodatkowe zabezpieczenie konta menedżera, jeśli jest dostępne. Hasło główne powinno być wyjątkowo mocne. Trzeba też wcześniej poznać procedurę odzyskiwania dostępu.

— A kopię klucza trzymamy pod wycieraczką! — zawołał Kierownik.

— Nie. Ani w ogólnodostępnym arkuszu, ani na kartce przy monitorze. Kody awaryjne przechowujemy osobno i bezpiecznie.

— GDZIE DOKŁADNIE?

— Na pewno nie powiem tego przy wszystkich gościach.

Drugi ochroniarz przy windzie

Przy windzie stał ochroniarz. Kierownik pokazał klucz, lecz nie został wpuszczony.

— JAK TO?! PRZECIEŻ MAM KLUCZ!

— Ktoś mógł go panu ukraść — odpowiedział ochroniarz. — Potrzebuję jeszcze potwierdzenia.

— JESTEM KIEROWNIKIEM!

— To akurat mówi tu co drugi człowiek — zauważył Grzesiu.

To jest **MFA — Multi-Factor Authentication**, uwierzytelnianie wieloskładnikowe. Możemy łączyć coś, co znasz, jak hasło; coś, co masz, jak urządzenie lub klucz sprzętowy; i coś, czym jesteś, na przykład cechę biometryczną.

— A dwa hasła to dwa czynniki? — zainteresowała się Agnieszka.

— Nie. To dwie rzeczy z kategorii „wiem”. **Dwa etapy logowania nie zawsze są uwierzytelnianiem dwuskładnikowym.**

— A JA MAM DWA KCIUKI! — oznajmił Kierownik.

Ochroniarz wyjął notes. Zaczął pisać podanie o przeniesienie.

SMS, zegarek w aplikacji i natrętne powiadomienia

Na drugim piętrze przygotowano trzy stanowiska: „SMS”, „Kod z aplikacji” i „Zatwierdź na telefonie”.

— Które jest najlepsze? — zapytała księgowa.

— Zależy od zagrożeń i dostępnych możliwości. **Kod SMS** jest zwykle lepszy niż samo hasło, ale numer telefonu może zostać przejęty, a sam kod wyłudzony. **TOTP**, czyli jednorazowe kody z aplikacji, bazują na sekrecie i czasie. Nie wymagają otrzymania SMS-a, lecz można je wpisać również na fałszywej stronie.

— A powiadomienie z przyciskiem „Zatwierdź”?

— Wygodne, ale potwierdzamy tylko logowanie, które sami rozpoczęliśmy. Oszuści czasem wysyłają dziesiątki powiadomień i liczą, że ktoś w końcu kliknie. To **MFA fatigue**, czyli zmęczenie żądaniami.

Telefon Kierownika zawibrował.

— PROSI O ZATWIERDZENIE!

— Loguje się pan gdzieś?

— NIE!

— Więc proszę odmówić i zgłosić podejrzaną próbę.

Telefon zawibrował drugi raz.

— ALE ON BARDZO PROSI!

— Natręctwo nie jest dowodem tożsamości — powiedziała Agnieszka.

Klucz, który rozpoznaje prawdziwy hotel

Grzesiu postawił obok hotelu niemal identyczną makietę. Na szyldzie zamiast „Złotym” widniało „Zlotym”.

— Prawie ten sam — powiedział Kierownik.

— Właśnie „prawie” robi różnicę. **Klucze FIDO2 i poprawnie wdrożone passkeys** używają kryptografii powiązanej z rzeczywistą witryną. Fałszywa domena nie powinna dostać podpisu przeznaczonego dla prawdziwej.

— Czyli mogę nie wpisywać hasła?

— Tak. Podczas logowania z passkey urządzenie podpisuje wyzwanie kluczem prywatnym; serwer sprawdza podpis kluczem publicznym. Klucz prywatny nie powinien być wysyłany do serwera. PIN lub biometria mogą służyć do odblokowania go lokalnie.

— A mój odcisk palca leci do hotelu? — przeraził się Kierownik.

— Nie w tym modelu. Biometria zwykle zostaje na urządzeniu i potwierdza lokalnie, że wolno użyć klucza.

— CZYLI JUŻ ŻADEN OSZUST NAS NIE DOPADNIE!

— Niestety, nadal można wyłudzić przelew, nadużyć procedury odzyskiwania konta albo przejąć urządzenie. Odporność na **phishing logowania** nie oznacza odporności na wszystkie oszustwa.

Hasła nie powinny leżeć w sejfie zapisane na odwrocie drzwi

— A skąd system wie, że podałam prawidłowe hasło? — zapytała Agnieszka.

— Dobrze zbudowany serwer nie przechowuje haseł w jawnej postaci. Zamiast tego przechowuje **odpowiednio obliczony hash hasła z unikalną solą** i weryfikuje podaną wartość. Do tego stosuje się algorytmy przeznaczone do haseł, takie jak Argon2id, odpowiednio skonfigurowane scrypt lub bcrypt.

— To może zwykłe SHA-256?

— Sam szybki hash to zły pomysł do przechowywania haseł. Atakujący może bardzo szybko sprawdzać kandydatów po wycieku bazy.

— ZROBIĘ TRZY HASHOWANIA! — zaproponował Kierownik.

— Proszę nie projektować własnej kryptografii — odparł Grzesiu.

— CZŁOWIEK CHCE POMÓC I NIGDY MU NIE POZWALAJĄ!

— Dlatego właśnie serwerownia ma osobny zamek.

Co miesiąc zmiana hasła, co miesiąc nowy numerek

Kierownik dumnie pokazał procedurę: „Zmiana hasła co 30 dni. Obowiązkowo”.

— Dzięki temu ludzie wymyślają `Hotel2026!01`, później `Hotel2026!02` — zauważyła Agnieszka.

— **Cykliczne wymuszanie zmiany bez konkretnej przyczyny nie jest uniwersalną dobrą praktyką** — wyjaśnił Grzesiu. — Zmieniamy hasło w razie kompromitacji, podejrzenia ujawnienia lub innego uzasadnionego powodu. Pomagają unikalność, sprawdzanie znanych wyciekłych haseł, ograniczanie prób logowania i MFA.

— A jak zapomnę hasła?

— Potrzebna jest bezpieczna procedura odzyskania. Pytanie „jak ma na imię pies?” bywa łatwe do odgadnięcia.

— MÓJ PIES MA NA IMIĘ TAJNE!

— Już nie jest tajne — powiedziała Agnieszka.

Drzwi awaryjne, przez które złodziej wchodzi pierwszy

Przed zamknięciem hotelu Grzesiu poprosił o kody odzyskiwania i zapasowe klucze.

— Jeśli zgubimy telefon z aplikacją albo sprzętowy klucz, musimy wiedzieć, jak odzyskać konto bez wydawania go przypadkowej osobie. Warto mieć **kody awaryjne w bezpiecznym miejscu, zapasowy klucz lub inną oficjalnie obsługiwaną metodę**.

— TO PO CO TEN DRUGI OCHRONIARZ? — oburzył się Kierownik.

— Bo oszust może udawać gościa, który zgubił klucz. Jeśli recepcja wydaje nowy każdemu, kto głośno płacze, cały system jest dekoracją.

— Czyli weryfikujemy tożsamość również przy odzyskiwaniu konta? — upewniła się Agnieszka.

— Tak. W firmie trzeba też ustalić, kto może zatwierdzić reset i jak to dokumentować.

— Ja przechowuję klucz awaryjny pod doniczką — pochwalił się Kierownik.

— Znowu?!

— ALE DONICZKA JEST W INNYM MIEJSCU!

Wymeldowanie

Nazajutrz hotel miał unikalne klucze do pokoi, menedżera haseł, dodatkowe uwierzytelnianie i procedurę awaryjną. Kierownik zwołał konferencję prasową.

— OD DZIŚ NIKT NIGDY NICZEGO NIE UKRADNIE!

— Nie mówiliśmy tego — przypomniał Grzesiu. — Silne, unikalne hasła, menedżer haseł i MFA utrudniają przejęcie kont. Passkeys i klucze FIDO2 mogą znacznie utrudnić phishing logowania. Ale nadal potrzebujemy aktualizacji, rozsądnych uprawnień i reagowania na incydenty.

— Ja już mam drugi czynnik! — oznajmiła Agnieszka.

— Bardzo dobrze.

— I menedżera haseł!

— Jeszcze lepiej.

— A JA MAM ZAPASOWY KLUCZ! — zawołał Kierownik.

— Gdzie?

Nachylił się konspiracyjnie.

— NIE POWIEM. TO TAJEMNICA.

— Pierwsza rozsądna rzecz, którą pan dzisiaj powiedział — przyznał Grzesiu.

— ALE PODPOWIEM: POD DONICZKĄ!

Agnieszka zamknęła oczy.

— Panie Kierowniku, proszę już niczego nie ułatwiać.

Komunikat hotelu „Pod Złotym Hasłem”: pokoje mają już osobne zamki, sejf ma własnego ochroniarza, a okrzyk „JESTEM KIEROWNIKIEM” nie jest akceptowaną metodą logowania. Podczas audytu doniczki odnaleziono dwa klucze, trzy karteczki z hasłami i nieopłacony rachunek za pizzę. 🔑🏨🤣❤️