Cyberdefence 24

09.03.2021

KPRM REKOMENDUJE UWIERZYTELNIANIE WIELOSKŁADNIKOWE

Hasła nie są już wystarczającym sposobem na ochronę naszych kont przed przejęciem ich przez cyberprzestępców. Warto stosować dodatkową weryfikację. O co w niej chodzi i jak ona działa - wyjaśnia KPRM Cyfryzacja.

Uwierzytelnienie wieloskładnikowe, czyli MFA z ang. *Multi-Factor Authentication* (najczęściej stosowane jako dwuskładnikowe, czyli 2FA – *Two-Factor Authentication*), bo o nim mowa, to skuteczny sposób zabezpieczenia kont e-mail czy profili w mediach społecznościowych. Dzięki niemu - nawet jeśli cyberprzestępca w jakiś sposób pozna nasze hasło - nie dostanie się do konta.

Włącz!

Użytkownicy, którzy korzystają z bankowości elektronicznej wiedzą o co chodzi. Banki mają bowiem prawny obowiązek stosowania uwierzytelnienia dwuskładnikowego. Jeden składnik to najczęściej hasło lub PIN, którym użytkownik loguje się do konta. Drugi – to np. sms z kodem, który trzeba wpisać przy potwierdzaniu przelewu.

Tak samo to działa w przypadku kont e-mail czy profili w mediach społecznościowych. Tam nie jest to jednak zawsze automatyczne ustawienie. Użytkownik musi to zrobić samemu.

"Uwierzytelnienie dwuskładnikowe warto stosować do ważnych kont, czyli tych, na których naprawdę nam zależy, na które włamanie spowodowałoby dla nas największe szkody" – mówi minister Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa. "To np. poczta elektroniczna. Jeśli przestępcy dostaną się do naszej skrzynki odbiorczej – mogą ją wykorzystać do resetowania haseł na innych kontach. Dlatego warto zadbać o dodatkowe zabezpieczenie" – dodaje.

Tak jak już wspominaliśmy - niektóre usługi online będą miały od razu włączone 2FA. Większość jednak nie ma takiej opcji. Użytkownik musi włączyć je samemu. Jeśli opcja włączenia dwuskładnikowego uwierzytelnienia jest dostępna - zwykle znajduje się w ustawieniach zabezpieczeń konta (może być tam nazwana np. „weryfikacją dwuetapową").

Dwa typy

A czym dokładnie jest drugi składnik uwierzytelnienia (pierwszy to hasło)? Opcji jest kilka. Jedną z najpopularniejszych są wiadomości SMS - tłumaczy Cyfryzacja KPRM.

Podczas uruchamiania 2FA użytkownik podaje swój numer telefonu, a usługa – np. przy zmianie hasła lub próbie logowania - wysyła wiadomość zawierającą kod. Dopiero po jego wprowadzeniu użytkownik będzie mógł się zalogować lub zmienić hasło.

Wiadomości tekstowe nie są najbezpieczniejszym typem 2FA, ale nadal oferują znacznie lepszą ochronę niż jego brak.

Co jeśli nie SMS? Cyfryzacja KPRM proponuje listę kodów lub bezpłatne aplikacje generujące kody jednorazowe.

Najpierw lista kodów. Po włączeniu 2FA na niektórych kontach użytkownik otrzyma listę kodów do wykorzystania. Każdy kod będzie działał tylko raz, więc gdy użyjemy wszystkich – będziemy musieli utworzyć kolejne. Kody zapasowe są bardzo przydatne, jeśli musimy się zalogować bez telefonu. Trzeba jednak pamiętać, by trzymać je w bezpiecznym miejscu.

Dużo wygodniejszym i bezpieczniejszym niż listy kodów narzędziami wspierającymi uwierzytelnienie dwuskładnikowe są bezpłatne aplikacje. Najpopularniejsze z nich to Google Authenticator i Microsoft Authenticator generujące kody do najpopularniejszych usług oraz wspierające uwierzytelnienie dwuskładnikowe w logowaniu do zasobów organizacji (np. wewnętrznych portali).

Istnieją jeszcze inne drugie składniki, które oferuje kilka usług. Niektóre aplikacje po zalogowaniu proszą np. o pozwolenie. Inne umożliwiają korzystanie z „kluczy bezpieczeństwa”, czyli małych urządzeń (tokeny), które można dokupić. Czasem można także użyć adresu e-mail jako drugiego składnika, pod warunkiem, że jest to inne konto e-mail niż to użyte do zresetowania hasła.

Jeśli konto oferuje choćby jeden z nich i działa prawidłowo - wszystkie one są dobrymi drugimi czynnikami.

A co jeśli 2FA nie jest dostępne? Wtedy jedynym sposobem na wzmocnienie ochrony konta jest silne i unikatowe hasło.

AK/Cyfryzacja KPRM