Cyberdefence 24

aut. Sylwia Gliwa 26.11.2019

UWIERZYTELNIANIE DWUSKŁADNIKOWE BEZ NUMERU TELEFONU. JAK TWITTER NAS OCHRONI?

Uwierzytelnianie dwuskładnikowe będzie możliwe bez wykorzystywania numeru telefonu - poinformował Twitter za pośrednictwem swojej własnej platformy. Czy jest to reakcja na wpadkę i utratą danych użytkowników?

Twitter o sprawie poinformował za pośrednictwem swojego konta Twitter Safety. Uwierzytelnianie dwuskładnikowe na platformie będzie odbywać się obecnie za pomocą wiadomości tekstowych, aplikacji uwierzytelniającej oraz kluczy uwierzytelniających. Użytkownicy już teraz mogą korzystać z tej możliwości.

Według wielu ekspertów tego typu zabezpieczenia nie stanowią wystarczającego zabezpieczenia przed hakerami. Dużo wcześniej na podobny krok zdecydował się Facebook, który w maju 2018 roku zrezygnował z wymogu korzystania z numeru telefonu przypisanego do konta do celów logowania do swojej platformy.

Trudno określić czy decyzja Twittera jest odpowiedzią na wpadki, które ostatnimi czasy zaliczyła platforma czy raczej jest odpowiedzią na zmiany również na innych platformach. Na początku października Twitter wydał oświadczenie, w którym poinformował użytkowników o dość poważnym incydencie - numery telefonów oraz adresy e-mail wykorzystywane m.in do dwuskładnikowego uwierzytelniania konta zostały użyte w celach reklamowych. Zdarzenie określone jako „błąd" naraziło użytkowników na utratę danych. W oświadczeniu władze platformy nie poinformowały natomiast, ile osób zostało poszkodowanych w wyniku zdarzenia.

O tym, że uwierzytelnianie dwuskładnikowe jest omijane przez hakerów również w październiku br ostrzegało amerykańskie FBI. Aby ominąć ten sposób logowania cyberprzestępcy przejmują kontrolę nad numerem telefonu ofiary. Dość głośny atak z zastosowaniem tej techniki miał miejsce w sierpniu a ofiarą przestępców padł sam szef Twittera Jack Dorsey. Za pośrednictwem przejętego konta Dorseya przez prawie 20 minut wysyłano rasistowskie hasła. Do ataku przyznała się grupa Chuckling Squad. Konto szefa Twittera, posiadało uwierzytelnianie dwuskładnikowe jednak przestępcy prawdopodobnie weszli w posiadanie duplikatu karty SIM milionera.

Po zdarzeniu wybuchły medialne spekulacje odnośnie sposobu zabezpieczenia konta amerykańskiego prezydenta Donalda Trumpa. Washington Examiner w wyniku przeprowadzonego dochodzenia, donosił, że konto amerykańskiego prezydenta jest podatne na atak hakerski „zagranicznej potęgi". Wtedy to „biały haker", a wcześniej cyberprzestępca Kevin Mitnick, wezwał Biały Dom do stworzenia własnego systemu uwierzytelniającego. „Kiedy byłem po drugiej stronie w latach 90, zasadniczo naraziłem na szwank każdą firmę telefoniczną w Stanach Zjednoczonych (…) Gdyby ktoś chciał namierzyć telefon tego faceta… z moją wytrwałością, dostałbym go" – stwierdził w komentarzu Mitnick.

Czytaj też: Jak zhakować konto twitterowe Trumpa? Wystarczą dwa "proste" kroki