Warszawa, 11.06.2021 r.

Informacja prasowa

**Jak doszło do włamania na skrzynkę Michała Dworczyka? Komentarz eksperta: Adam Gładkowski, specjalista ds. bezpieczeństwa IT, ODO 24.**

Szef Kancelarii Prezesa Rady Ministrów Michał Dworczyk z dużym prawdopodobieństwem padł ofiarą ataku, w wyniku którego atakujący mógł pobrać całą zawartość lub uzyskać całkowity dostęp do jego prywatnej skrzynki. Warto zaznaczyć, że na razie brak na to jednoznacznych dowodów, zaś kolejne publikowane materiały wskazują na coraz większe prawdopodobieństwo, że dostępne w sieci zrzuty ekranu wiadomości są spreparowane. Publikowane materiały związane m.in. z poufnymi wiadomościami dotyczącymi uzbrojenia polskiej armii czy informacje o negocjacjach z innymi państwami w zakresie obronności niekoniecznie muszą pochodzić z jego prywatnej skrzynki – brakuje jakiegokolwiek powiązania pomiędzy publikowanymi materiałami, a skrzynką. Włamywacze mogliby w bardzo prosty sposób wykazać prawdziwość posiadanych materiałów publikując pełne źródła wiadomości – rozwiałoby to wszelkie wątpliwości, ale pomimo wielokrotnych próśb nie zdecydowali się na ten ruch.

Jednakże zakładając, że do wycieku danych faktycznie doszło, warto zauważyć, że zdarzenie takie mogło być następstwem różnego rodzaju ataków hakerów bądź zaniedbań ze strony właściciela poczty. Pierwszą, najczęściej wskazywaną w mediach przyczyną jest przełamanie zabezpieczeń, czyli odgadnięcie hasła do skrzynki pocztowej.

W takim przypadku należy zauważyć, że Szef Kancelarii Prezesa Rady Ministrów w celu poprawnego zabezpieczenia swojej korespondencji mógł określić u operatora skrzynki pocztowej autentyfikację dwupoziomową, która uniemożliwiłaby dostęp do skrzynki atakującemu, który znał lub odgadł hasło. Gdyby tak się stało, to do uzyskania dostępu do poczty niezbędny byłby dodatkowy kod wysyłany np. na telefon komórkowy, który nie mógłby trafić w ręce cyberwłamywacza. Jednakże należy zaznaczyć, że w przypadku niektórych operatorów poczty, metoda autentyfikacji dwupoziomowej albo nie jest wspierana, bądź jest mocno ograniczona i rozwiązana w sposób niewygodny w użytkowaniu - nie wspiera innych metod zabezpieczenia konta użytkownika w rodzaju autoryzacji SMS, autoryzacji kluczem sprzętowym zgodnym ze specyfikacją FIDO U2F czy autoryzacji OAuth. Warto również zwrócić uwagę, że niektóre, popularne serwisy pocztowe wykazują się dużą podatnością w zakresie możliwości szybkich prób sprawdzania potencjalnych haseł (umożliwiającą hakerom znającym protokoły sieciowe błyskawiczne i zautomatyzowane weryfikacje wielu haseł – limitu ilościowego po którym następowałaby czasowa blokada IP atakującego), co jest rażącym zaniedbaniem patrząc na współczesne standardy zabezpieczeń.

Innym aspektem sprawy jest kwestia samego hasła. Mogło ono zostać złamane korzystając z niskiego poziomu zabezpieczeń występującego u usługodawcy poczty lub było zbyt proste – np. włamywacz mógł stworzyć w celu ataku listę potencjalnych haseł, złożonych z kombinacji słów powiązanych z osobą Michała Dworczyka (jak imiona czy nazwiska rodziny, znajomych, współpracowników, terminów zawodowych, zwierząt, hobby czy zainteresowań) i liczb (np. data urodzin swoich lub rodziny, rocznice) oraz najpowszechniej używanych „utrudniaczy”, jak wykrzyknik na końcu hasła, bądź cyfra 1. Jest też inna, bardziej niepokojąca możliwość – dość powszechna praktyka używania przez użytkowników takiego samego hasła w wielu miejscach. A niestety faktem jest, że w omawianym przypadku adres i powiązane z nim hasło pojawiło się dotychczas co najmniej w dwóch wyciekach danych. W 2018 r. adres e-mail ministra odnalazł się przynajmniej raz na zbiorczej liście danych wykradzionych z wielu niezidentyfikowanych portali, natomiast w 2012 r. wyciekło jego hasło z portalu LinkedIn.

Warto podkreślić, że niestety zarówno politycy, jak również zwykli obywatele często nie są świadomi zagrożeń wynikających z własnej aktywności w sieci. Nie wszyscy zdają sobie sprawę z ryzyka, które występuje w wypadku, kiedy to nasz adres mailowy przejmie osoba niepożądana i będzie chciała wykorzystać go do osiągnięcia własnych korzyści. Niestety, w przypadku zwykłych osób, które wprawdzie są mniej narażone na ataki niż osoby publiczne, szybkość reakcji służb i skuteczność w odzyskiwaniu dostępu do własnej poczty jest dużo mniejsza. A przecież mamy tam „podpięte” konta bankowe, profile zaufane do komunikacji z urzędami, Internetowe Konta Pacjenta, konta usług chmurowych (Dropbox, Onedrive), portale społecznościowe, ubezpieczenia, faktury elektroniczne, smartfony i inne urządzenia. Na dodatek prywatne skrzynki pocztowe często służą nam niejednokrotnie za archiwum wszelkiej maści historii zakupów, faktur i ogólnie korespondencji, której kopii lokalnej niejednokrotnie nawet nie mamy na swoim komputerze.

**ODO 24 sp. z o. o.** oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z zakresu m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Kontakt dla mediów:

**Triple PR**

**Aneta Gałka**

tel. 570 533 678

aneta.galka@triplepr.pl