Cyberdefence 24

aut. Adam Lelonek 06.09.2017

WYCIEK DANYCH TYSIĘCY PRACOWNIKÓW ARMII I SŁUŻB USA

Amerykańska prywatna firma wojskowa, a zarazem międzynarodowa firma ochroniarska TigerSwan potwierdziła wyciek tysięcy plików zawierających wrażliwe i osobiste informacje pracowników armii i wywiadu USA, które zostały nieumyślnie udostępnione na niezabezpieczonym serwerze firmy Amazon. Sprawa została ujawniona przez pracownika firmy UpGuard Chrisa Vickery'ego, który odkrył, iż przestrzeń do składowania obiektów wchodzących (tj. przestrzeń buforowa służąca do weryfikacji zawartości, ang. *Bucket*) w chmurze Amazon Web Services S3 została przypadkowo skonfigurowana na publiczny dostęp.

Ujawnione zasoby obejmują 9402 dokumenty, datowane od 2009 roku, które zawierały prywatne informacje tysięcy kandydatów do pracy w firmie, spośród których setki miały poświadczenia bezpieczeństwa i dostęp do ściśle tajnych informacji. Wśród nich były informacje o dotychczasowych obowiązkach służbowych, adresy domowe, numery telefonów, adresy mailowe, dane z dokumentów (prawa jazdy, paszporty, ubezpieczenie społeczne itp.). W chmurze znajdywały się dane czynnych pracowników służb specjalnych, Organizacji Narodów Zjednoczonych, byłych żołnierzy służących w Afganistanie, Iraku czy pracowników amerykańskiej bazy w Guantanamo. Ponadto były też osobiste informacje zagranicznych aplikantów, m.in. obywateli Iraku i Afganistanu, współpracujących z siłami USA i agencjami rządowymi.

Ujawnienie danych miało miejsce 20 lipca, lecz nie zostały one zabezpieczone aż do 24 sierpnia br. W oświadczeniu z soboty 2 września firma TigerSwan zakomunikowała, iż baza danych nadsyłanych CV była zarządzana przez zewnętrzną firmę TalentPen. Po zakończeniu okresu trwania ich umowy w lutym 2017 roku, ta ostatnia ustanowiła zabezpieczoną stronę internetową do przekazania plików na serwer TigerSwan. Transfer danych zakończył się 8 lutego br., po czym poinformowano TalentPen, że procedura dobiegła końca. Mimo tego dane nie zostały zabezpieczone i przebywały w publicznym dostępie bucketu w wirtualnej przestrzeni magazynowej aż do sierpnia.

TigerSwan twierdzi, iż nie miała dostępu do strony internetowej podwykonawcy czy utworzonego przez niego bucketu, więc nie mogła być świadoma, że dokumenty pozostają w publicznym dostępie. Firma TalentPen nie udzieliła wcześniej informacji na temat swoich aktywności w tym obszarze zanim nie został skonfrontowana w dniu 31 sierpnia, dokładnie tydzień po tym, jak nie przyznając się do zaistniałej sytuacji usunęła w tajemnicy wspomniane pliki. TigerSwan otworzyła gorącą linię dla potencjalnie poszkodowanych pracowników.

Firma UpGuard zauważa, że zagrożenie dla wrażliwych danych powstało nie wskutek ataku, lecz ludzkiego błędu. W tej sytuacji najbardziej symptomatyczne jest, iż przez miesiąc nie podjęto działań, aby zabezpieczyć tysiące plików. Cała sytuacja jest rezultatem niewłaściwych procedur wewnętrznych firmy, która zajmowała się obsługą i transferem dokumentów. Pokazuje to też, jak duże jest ryzyko wynajmowania zewnętrznych podwykonawców przez firmy pracujące z wrażliwymi danymi, które same mają wysoce rozwinięte zabezpieczenia.

Konsekwencjami zdarzenia mogą być m.in. ataki phishingowe wobec weteranów oraz czynnych pracowników służb, których osobiste dane zostały poznane przez złodziei tożsamości. Otwartym pozostaje też kwestia wartości takich informacji dla zagranicznych służb. W sposób oczywisty może to stanowić zagrożenie dla obywateli Iraku czy Afganistanu, współpracujących z podmiotami z USA.