Cyberdefence 24

aut. Tomasz Fastyn 24.06.2016

KAŻDY WYCIEK DANYCH JEST NIEBEZPIECZNY

Jeśli dane przestają być poufne, to nie są bezpieczne. Przypadek czeski pokazuje zauważalny trend wskazujący, że coraz słabszym ogniwem w bezpieczeństwie teleinformatycznym są ludzie i tzw. „insider threat", czyli zagrożenie ze strony pracowników organizacji - mówi Michał Grzybowski z Fundacji Bezpieczna Cyberprzestrzeń w rozmowie z Cyberdefence24.

Czy kolejne wycieki danych klientów firm pomagają w tworzeniu kampanii phishingowych?

Należy zdawać sobie sprawę, że ciągle najskuteczniejszym sposobem ataku na integralność i poufność danych w cyberprzestrzeni pozostaje przekonanie użytkownika do otwarcia załącznika w poczcie lub odwiedzenia strony internetowej zawierającej złośliwe oprogramowanie. Jeśli przestępca ma dostęp nie tylko do aktualnych adresów poczty elektronicznej ofiar, ale też danych jak imię, nazwisko, numer klienta to zwiększa szansę powodzenia ataku socjotechnicznego.

Ostatni wyciek danych w Czechach był spowodowany działaniem pracownika tamtejszego oddziału T-mobile. Firma uspokaja klientów mówiąc, że nie ma poważnego zagrożenia bezpieczeństwa.

Z informacji ogólnodostępnych wynika, że dane zostały wykradzione przez pracownika firmy, co oznacza, że osoba posiadająca autoryzowany dostęp do danych postanowiła go wykorzystać w nielegalny sposób. Oznacza to, że mogą być one wykorzystane w sposób zagrażający bezpieczeństwu klientów np. stanowić bardzo dobry punkt startowy kampanii mającej na celu wyłudzenie od klientów kolejnych informacji, takich jak dane uwierzytelniające do systemów, czy dane kart kredytowych. Przypadek czeski pokazuje też zauważalny trend wskazujący, że coraz słabszym ogniwem w bezpieczeństwie teleinformatycznym są ludzie i tzw. „insider threat", czyli zagrożenie ze strony pracowników organizacji.

Czy samo źródło bazy danych pozwala na ukierunkowanie ataku phishingowego?

Istnieje takie prawdopodobieństwo. Może to być kampania skierowana do całego grona 1,5 mln klientów np. w formie wiadomości elektronicznej z załączoną sfabrykowaną fakturą do opłacenia lub bardzo ukierunkowany atak. Możemy sobie wyobrazić, że wśród 1,5 mln klientów znajduje się główny księgowy dużego przedsiębiorstwa. Jeśli przestępca przekona go do „kliknięcia" w odpowiedni link, w chwili kiedy pracuje on na służbowym komputerze, spenetrowanie jego zawartości pozostanie formalnością.

Jak powinny wyglądać bezpieczne hasła stosowane przez użytkowników internetu?

To zależy od świadomości użytkownika i jego wyobraźni. Im hasło dłuższe - tym lepsze. Im więcej znaków specjalnych i stosowania różnych wielkości liter - tym lepiej. Należy zdawać sobie sprawę, że krótkie hasło stanowiące "jeden wyraz słownikowy" jest do załamania w kilka godzin. Żeby złamać te

złożone, standardowy komputer dzisiaj musiałby pracować przez dziesiątki lat. Szef Facebooka Mark Zuckerberg nigdy nie był i nie przedstawiał się jako guru od cyberbezpieczeństwa i nie powinniśmy go podawać jako wzór, choć paradoksalnie może być emanacją "średniego" użytkownika FB.

Czy czeski T-mobile zrobił wszystko poprawnie w kwestii komunikacji z klinetami?

Podczas każdej edycji ćwiczeń Cyber-EXE Polska sprawdzamy, jak na ataki cybernetyczne na firmy zareagują ich działy Public Relations. Każda dojrzała organizacja posiada procedury komunikacji na wypadek sytuacji kryzysowej i działa według swojej polityki informacyjnej. Zakres komunikatów przeważnie jest bardzo ogólny. Jeśli dane przestały być poufne, to nie są bezpieczne.

O kradzieży danych przez byłego pracownika T-mobile w Czechach pisaliśmy na początku tego tygodnia.