Ataki socjotechniczne, czyli umysł w niebezpieczeństwie

Cyberprzestępcy wykorzystują nie tylko zaawansowane narzędzia informatyczne i techniki, aby włamać się do komputerów lub na konta użytkowników. Czasem uciekają się do nakłonienia internautów do popełnienia błędu za pomocą metody zwanej socjotechniką. Jak się przed nią obronić, przypominamy w ramach kampanii „Jak chronić się w internecie – nie tylko podczas Europejskiego Miesiąca Bezpieczeństwa", która powstała w Państwowym Instytucie Badawczym NASK na podstawie materiałów SANS Institute.

Atak socjotechniczny polega na tym, że cyberprzestępca podszywa się pod kogoś znanego lub zaufanego – przedstawiciela banku, współpracownika albo firmę zapewniającą wsparcie – aby uzyskać to, co jest mu potrzebne.

Cyberprzestępcy mogą przeprowadzać ataki socjotechniczne, używając różnych metod, np. poczty e-mail, komunikatora, telefonu lub osobistego kontaktu. Aby przyciągnąć uwagę potencjalnej ofiary, używają wielu sztuczek – oferują bezpłatne pobrania, ogłaszają wygraną w konkursie albo twierdzą, że komputer został zainfekowany. Ponadto ataki te często wydają się wiarygodne – dokumenty mają oficjalne logo lub podpis. Jaki jest ich cel? Skłonić użytkownika do udostępnienia informacji (jak hasła) lub podjęcia konkretnych czynności (np. otwarcia zainfekowanego załącznika).

Jak mogą wyglądać ataki?

Może to być np. telefon od osoby podającej się za pracownika urzędu skarbowego. Informuje ona ofiarę, że ma zaległości podatkowe i jeśli nie ureguluje ich w ciągu najbliższych 48 godzin, trafi do więzienia. Następnie objaśnia kroki umożliwiające dokonanie płatności natychmiast, przez telefon, i uniknięcie aresztowania.

Tak naprawdę nie jest to jednak urzędnik państwowy. Mamy tu do czynienia z cyberprzestępcą próbującym wyłudzić pieniądze. Stara się on wywołać strach i przekonać, że sprawa jest pilna, zmuszając do popełnienia błędu, np. podania danych karty kredytowej czy informacji potrzebnych do przelewu.

A teraz inny przykład ataku socjotechnicznego: otrzymanie od szefowej e-maila z informacją, że jest w podróży. Twierdzi ona, że musi natychmiast skontaktować się z kimś z działu HR, ale nie posiada, niestety, ich numeru telefonu. Ponadto jej laptop właśnie się rozładował i nie ma dostępu do firmowej skrzynki pocztowej. W związku z tym prosi o przesłanie na jej prywatny adres w domenie gmail.com firmowej książki telefonicznej.

Nie jest to jednak szefowa użytkownika, ale cyberprzestępca, który próbuje zaatakować go przez e-mail. Przestępca próbuje podstępem zmusić go do przesłania mu listy numerów telefonów, aby później zaatakować inne osoby z organizacji.

Oznaki ataków socjotechnicznych

Najprostszym sposobem obrony przed atakami socjotechnicznymi jest po prostu zdrowy rozsądek. Jeśli coś wydaje się podejrzane albo ma się co do tego złe przeczucia, to może być atak. Częste oznaki ataku socjotechnicznego to:

- wywoływanie wrażenia, że sprawa jest niezwykle pilna. Nacisk, aby podjąć bardzo szybką decyzję.

- prośba o informację, do której ta osoba nie powinna mieć dostępu.
- żądania ominięcia bądź zignorowania zasad lub procedur bezpieczeństwa.
- coś jest zbyt piękne, by było prawdziwe. Typowy przykład stanowi informacja o wygranej na loterii (pomimo braku udziału).

Kilka sposobów ochrony

1. Jeśli istnieje podejrzenie, że ktoś wziął nas na cel, nie należy komunikować się więcej z tą osobą. Najlepiej po prostu odłożyć słuchawkę lub zignorować wiadomość i natychmiast zawiadomić pomoc techniczną lub zespół bezpieczeństwa.

2. Odrzuć pośpiech

Ataki socjotechniczne często sugerują, że sytuacja jest niezwykle pilna. Cyberprzestępcy informują cię, że istnieje ścisły termin i prowokują do popełnienia błędu. Jeśli ktoś naciska, aby ominąć lub zignorować procedury, to zapewne atak.

3. Poznaj sztuczki socjotechniczne

Cyberprzestępcy używają emocji, jak strach, onieśmielenie, ciekawość czy podekscytowanie, aby zmusić cię do czegoś, czego chcą. Jeśli coś wydaje się zbyt piękne, aby było prawdziwe, to zapewne takie jest.

4. Pomyśl, zanim klikniesz

Ataki socjotechniczne prowokują cię do nieuważnego klikania w odnośniki i otwierania załączników. Uważaj: jeden błędny ruch może spowodować infekcję urządzenia i rozprzestrzenienie się jej na inne.

5. Rozważnie pobieraj i podłączaj

Cyberprzestępcy oczekują, że pobierzesz złośliwe oprogramowanie, podłączysz zainfekowany nośnik lub urządzenie. Używaj zatwierdzonego sprzętu i oprogramowania. Jeśli nie wiesz, czy coś zostało zaaprobowane, zapytaj.

6. Pytaj, a jeśli coś jest dziwne lub podejrzane, skontaktuj się z ochroną

Jeśli uważasz, że doświadczasz ataku socjotechnicznego, odłóż słuchawkę (lub nie odpowiadaj na e-mail) i natychmiast skontaktuj się z pomocą techniczną.

Źródło: https://bezpiecznymiesiac.pl/bm/baza-wiedzy/844,Ataki-socjotechniczne-czyli-umysl-w-niebezpieczenstwie.html