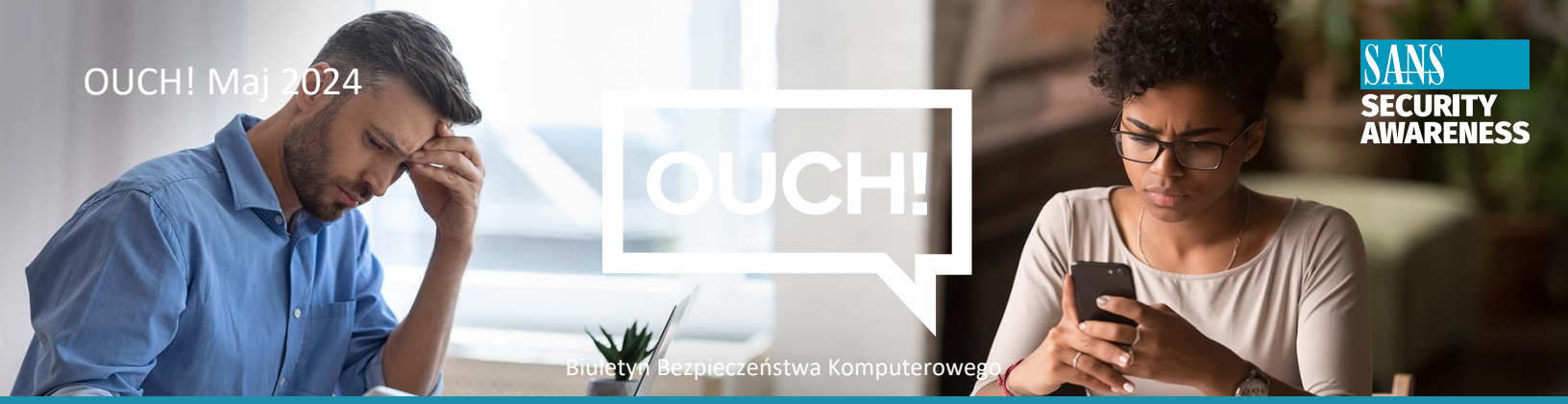

Trzy najczęstsze sposoby ataków

Wstęp

Ataki socjotechniczne, podczas których atakujący nakłaniają ludzi do zrobienia czegoś, czego nie powinieneś robić, to jedna z najpowszechniejszych metod cyberprzestępców. Ta koncepcja była wykorzystywana przez oszustów od tysięcy lat. Nowością jest to, że Internet bardzo ułatwia cyberprzestępcom udawanie kogoś kim nie są i obranie za cel dowolną osobę. Poniżej znajdują się trzy najczęstsze metody socjotechniki.

Phishing

Phishing to najbardziej znany atak wykorzystujący socjotechnikę; ma to miejsce wtedy, gdy cyberprzestępcy wysyłają wiadomość e-mail, próbując nakłonić do podjęcia działania, którego nie powinno się wykonać. Nazywa się to phishingiem, ponieważ przypomina łowienie ryb: Rzucasz wędkę i haczyk, ale nie masz pojęcia, co złapiesz. Taktyka jest prosta. Im więcej e-maili phishingowych wysyłają cyberprzestępcy, tym więcej osób pada ich ofiarą. Ataki phishingowe stały się znacznie bardziej wyrafinowane i ukierunkowane, a przestępcy często dostosowują swoje e-maile phishingowe przed ich wysłaniem.

Smishing

Smishing to phishing oparty na wiadomościach SMS, podczas którego zamiast wiadomości e-mail wysyłana jest wiadomość tekstowa. Cyberprzestępcy wysyłają wiadomości tekstowe również w aplikacjach takich jak iMessage, Google Messages lub WhatsApp. Jest kilka powodów, dla których smishing stał się popularny. Po pierwsze, znacznie trudniej jest odfiltrować ataki za pośrednictwem wiadomości tekstowych niż ataki za pośrednictwem e-maili. Po drugie, wiadomości tekstowe zazwyczaj są krótkie, co znacznie utrudnia ustalenie, czy wiadomość jest wiarygodna, czy nie. Po trzecie, przesyłanie wiadomości jest często bardziej nieformalne, dlatego ludzie są przyzwyczajeni do reagowania na nie szybko. Przede wszystkim ludzie są coraz lepsi w wykrywaniu ataków phishingowych za pośrednictwem wiadomości e-mail, więc cyberprzestępcy po prostu przechodzą na nową metodę – SMSy.

Vishing

Vishing, czyli voice-based phishing, to taktyka wykorzystująca połączenie telefoniczne lub wiadomość głosową. Vishing zajmuje atakującemu znacznie więcej czasu, ponieważ wchodzi z ofiarą w interakcję, bezpośrednio z nią rozmawiając. Tego typu ataki są też znacznie skuteczniejsze, ponieważ przez telefon znacznie łatwiej jest wywołać silne emocje, takie jak poczucie pilności. Jeśli zaczniesz rozmowę z cyberprzestępcą, ten zrobi wszystko, żeby nie zakończyć połączenia, dopóki nie dostanie tego, czego chce.

Wykrywanie i zatrzymywanie ataków

Na szczęście nie ma znaczenia, której z trzech metod użyją przestępcy, wskazówki są uniwersalne:

- **Pilność**:Każda wiadomość, która stwarza presję, ma nakłonić do podjęcia szybkich działań i popełnienia błędu. Przykładem jest wiadomość z Urzędu Skarbowego informująca o niezapłaconym podatku i możliwych konsekwencjach, jeśli nie zapłacisz od razu.

- **Presja**:Każda wiadomość, która nakłania pracownika do zignorowania lub obejścia firmowych zasad i procedur bezpieczeństwa.

- **Ciekawość**: Każda wiadomość, która wzbudza ogromne zainteresowanie lub wydaje się zbyt piękna, aby mogła być prawdziwa, na przykład niedoręczona paczka DHL lub powiadomienie, że otrzymujesz zwrot pieniędzy z Allegro.

- **Ton**: Każda wiadomość, która wydaje się pochodzić od kogoś, kogo znasz, np. współpracownika, ale nie przypomina typowych wiadomości od tej osoby.

- **Twoje dane**: Każda wiadomość zawierająca prośbę o podanie poufnych informacji, takich jak hasło lub dane karty kredytowej.

- **Ogólniki**: Wiadomość pochodząca od zaufanej organizacji, ale zawierająca ogólne zwroty, takie jak „Szanowny Kliencie". Jeśli firma kurierska ma dla Ciebie paczkę lub operator telekomunikacyjny ma problem z rozliczeniem, z pewnością znają Twoje imię i nazwisko.

- **Osobisty adres e-mail**: Każda wiadomość e-mail, która wydaje się pochodzić z podmiotu publicznego, dostawcy usług lub współpracownika, ale zawiera osobisty adres e-mail, taki jak @gmail.com lub @hotmail.com.

Szukając tych typowych wskazówek, możesz znacznie polepszyć swoje bezpieczeństwo.

Redaktor gościnny

Mary Jane Suarez Partain jest dyrektorką programową w Women in CyberSecurity (WiCyS). Jej rola polega na zapewnianiu zasobów, inicjatyw i programów mających na celu rekrutację, utrzymanie i awans kobiet w dziedzinie cyberbezpieczeństwa. Jej pasją jest tworzenie środowiska, w którym wszyscy czują się cenieni, mile widziani i zauważani.

Źródła

Zatrzymaj oszustwa związane z połączeniami telefonicznymi: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
Ataki phishingowe: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier
Działania na emocjach - o tym jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
Shakowali mnie, co teraz: https://www.sans.org/newsletters/ouch/im-hacked-now-what/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz