Biuletyn Bezpieczeństwa Komputerowego

Działania na emocjach - o tym jak cyberprzestępcy oszukują

Wstęp

Cyberprzestępcy nieustannie opracowują innowacyjne sposoby nakłaniania nas do robienia rzeczy, których nie powinniśmy robić, takich jak klikanie w podejrzane linki, otwieranie zainfekowanych załączników, kupowanie kart podarunkowych lub przekazanie atakującym swoich haseł. Ponadto często używają różnych technologii lub platform, aby nas oszukać, takich jak wiadomości e-mailowe, połączenia telefoniczne, wiadomości SMS lub serwisy społecznościowe. Chociaż może to wydawać się przytłaczające, większość z tych ataków łączy jedno: emocje. Znając emocjonalne wyzwalacze, których używają cyberprzestępcy, możesz wykryć ich ataki bez względu na to, jakiej metody użyją.

Chodzi o emocje

Wszystko zaczyna się od emocji. Ludzie zbyt często podejmują decyzje bazując na emocjach, a nie faktach. W rzeczywistości istnieje cały obszar badań, zwany „ekonomią behawioralną", prowadzony przez badaczy takich jak Daniel Khaneman, Richard Thaler i Cass Sunstein. Na szczęście, jeśli znamy wyzwalacze emocjonalne, możemy z powodzeniem wykryć i powstrzymać większość ataków. Poniżej wymieniono najczęstsze wyzwalacze emocjonalne. Zdarza się, że cyberprzestępcy wykorzystują kombinację różnych technik w jednym ataku - dzięki temu jest to znacznie bardziej skuteczne.

Pilność: Pilność jest jednym z najczęstszych wyzwalaczy emocjonalnych. Cyberprzestępcy często wykorzystują strach, niepokój lub zastraszanie, aby zmusić Cię do popełnienia błędu. Na przykład możesz otrzymać wiadomość e-mail od szefa z żądaniem natychmiastowego przesłania poufnych dokumentów, a w rzeczywistości jest to przestępca podszywający się pod szefa. A może otrzymasz SMS-a od kogoś podszywającego się pod pracownika administracji publicznej, który informuje, że masz zaległości w płatności i musisz zapłacić teraz lub poniesiesz konsekwencje.

Złość: Otrzymujesz wiadomość dotyczącą sytuacji politycznej, środowiskowej lub społecznej, która jest Ci bliska – na przykład „Nie uwierzysz, co robi ta grupa polityczna lub firma korporacyjna!"

Zdziwienie / **Ciekawość**: Czasami najskuteczniejsze ataki są najmniej spodziewane. Ciekawość idzie w parze ze zdziwieniem, ponieważ chcemy wiedzieć więcej. To odpowiedź na coś nieoczekiwanego. Na przykład atakujący wysyła wiadomość, że paczka nie została dostarczona i załącza link, gdzie możesz dowiedzieć się więcej o tym zamówieniu, nawet jeśli nie zamówiłeś niczego online. Jesteś zachęcany do odwiedzania podejrzanych linków! Niestety, pod linkiem nie znajdziesz żadnych prawdziwych informacji, tylko szkodliwe treści.

Zaufanie: Atakujący używają nazwy lub logo, które znasz, aby przekonać Cię do podjęcia działania. Na przykład wiadomość udająca, że jest z Twojego banku, znanej organizacji charytatywnej, zaufanej organizacji rządowej, a nawet osoby, którą znasz. Tylko dlatego, że wiadomość e-mail lub wiadomość tekstowa zawiera nazwę organizacji, którą znasz, i jej logo, nie oznacza, że faktycznie pochodzi od tego podmiotu.

Podekscytowanie: Dostajesz wiadomość tekstową od banku lub usługodawcy z podziękowaniem za terminowe dokonywanie płatności. Wiadomość tekstowa zawiera link, w którym możesz odebrać nagrodę – nowy iPhone! Link prowadzi do witryny, która wygląda na prawdziwą, ale prosi o wszystkie dane osobowe lub sugeruje, że musisz podać dane karty kredytowej, aby pokryć niewielkie koszty wysyłki. Jest to oszustwo, które po prostu kradnie pieniądze lub tożsamość.

Empatia/Współczucie: Cyberprzestępcy wykorzystują chęć pomocy. Na przykład, gdy w wiadomościach pojawi się informacja o jakiejś katastrofie, oszuści wyślą tysiące fałszywych wiadomości, podszywając się pod organizację charytatywną pomagającą ofiarom.

Dzięki lepszemu zrozumieniu tych wyzwalaczy emocjonalnych będziesz znacznie lepiej przygotowany do powstrzymywania cyberprzestępców, niezależnie od technologii lub platformy, z której korzystają.

Redaktor gościnny

My-Ngoc Nguyen jest dyrektorem w Secured IT Solutions. Ma 20-letnie doświadczenie w zarządzaniu programów bezpieczeństwa cybernetycznego i zarządzania ryzykiem zarówno dla rządu, jak i sektora prywatnego. Dzieli się tym doświadczeniem jako Certyfikowany Instruktor MGT512.https://www.linkedin.com/in/menop, My-Ngoc Nguyen | SANS Institute @MenopN.

Źródła

Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/
Najpopularniejsze oszustwa w mediach społecznościowych: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Wykryj i zatrzymaj ataki w wiadomościach tekstowych: ttps://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Ataki phishingowe: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz