OUCH! Listopad 2020

SANS SECURITY AWARENESS

Ataki socjotechniczne

Wstęp

Powszechnym błędnym przekonaniem na temat cyberprzestępców jest to, że używają oni wyłącznie wysoce zaawansowanych narzędzi i technik do włamywania się do komputerów lub kont użytkowników. Cyberprzestępcy wiedzą, że najłatwiejszym sposobem na kradzież informacji, zhakowanie konta lub zainfekowanie systemu jest po prostu nakłonienie Cię do zrobienia tego za nich techniką, która nasi nazwę socjotechniki. Dowiedzmy się, jak działają te ataki i co możesz zrobić, aby się chronić.

Czym jest socjotechnika

Socjotechnika to atak psychologiczny, w którym atakujący nakłania Cię do zrobienia czegoś, czego nie powinieneś robić, za pomocą różnych technik manipulacji. Naciągacze i oszuści działają tak samo. Dzisiejsza technologia ułatwia każdemu napastnikowi z dowolnego miejsca na świecie udawanie, że jest kimkolwiek zechce i atakowanie każdego na całym świecie, w tym Ciebie. Spójrzmy na dwa przykłady w rzeczywistym świecie:

Otrzymujesz telefon od osoby, która twierdzi, że dzwoni z Urzędu Skarbowego z informacją, że masz zaległości podatkowe i jeśli ich nie zapłacisz od razu, zostaniesz ukarany grzywną. Następnie naciska, abyś zapłacił przez telefon kartą kredytową, kartą podarunkową lub przelewem, ostrzegając, że jeśli nie zapłacisz, spotkają Cię konsekwencje. Dzwoniący nie jest tak naprawdę z urzędu, tylko przestępcą, który próbuje nakłonić Cię do przekazania mu pieniędzy.

Innym przykładem jest atak zwany phishingiem. Atakujący tworzy wiadomość e-mail, która próbuje nakłonić Cię do podjęcia działania, takiego jak otwarcie zainfekowanego załącznika, kliknięcie złośliwego łącza lub podanie poufnych informacji. Czasami e-maile phishingowe są łatwe do wykrycia. Przykładem mogą być te, które sugerują, że pochodzą z banku. Innym razem e-maile phishingowe mogą być spersonalizowane i ukierunkowane, ponieważ atakujący najpierw sprawdzają swoje cele, na przykład e-mail sugerujący, że pochodzi od szefa lub współpracownika.

Należy pamiętać, że takie ataki socjotechniczne nie ograniczają się do rozmów telefonicznych lub e-maili; mogą się zdarzyć w dowolnej formie, w tym SMS-em, w mediach społecznościowych, a nawet twarzą w twarz. Dobrze wiedzieć na co zwrócić uwagę.

Typowe wskazówki dotyczące ataku socjotechnicznego

Zdrowy rozsądek jest często najlepszym sposobem obrony. Jeśli coś wydaje się podejrzane lub nie wydaje się właściwe, może to być atak. Na co zwrócić uwagę:

- Zachowaj dużą czujność. Atakujący próbują zmusić cię do popełnienia błędu. Im większe poczucie pilności, tym większe prawdopodobieństwo ataku.
- Atakujący naciskają na omijanie lub ignorowanie zasad lub procedur bezpieczeństwa, których masz przestrzegać w pracy.
- Prośby o podanie poufnych informacji, do których nikt nie powinien mieć dostępu, takich jak numery kont.
- E-mail lub wiadomość od znajomego lub współpracownika, którego znasz, ale wiadomość nie brzmi jakby to oni ją wysłali, może okazać się fałszywa - być może sformułowanie jest dziwne lub podpis jest nieprawidłowy.
- E-mail, który wydaje się pochodzić od współpracownika lub legalnej firmy, ale jest wysyłany przy użyciu osobistego adresu e-mail, takiego jak @gmail.com.
- Granie na twojej ciekawości lub czymś zbyt pięknym, aby mogło być prawdziwe. Na przykład otrzymasz powiadomienie, że przesyłka została opóźniona, mimo że nigdy nie zamówiłeś paczki lub że wygrałeś nagrodę w konkursie, w którym nigdy nie uczestniczyłeś.

Jeśli podejrzewasz, że ktoś próbuje cię oszukać, nie kontaktuj się już z tą osobą. Pamiętaj, zdrowy rozsądek jest często najlepszym sposobem obrony.

Redaktor gościnny

Christian Nicholson (@GuardianCosmos) jest instruktorem SANS dla SANS SEC560 i SANS SEC504, a także partnerem/Cyber Leadem w Indelibl (https://indelible.global). Christian specjalizuje się w bezpieczeństwie aplikacji, Purple Teaming i automatyzacji w zakresie bezpiecznej integracji, programowania i inżynierii.

Źródła

Oszustwa Telefoniczne oraz Scam: https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams
Powstrzymać phishing: https://www.sans.org/security-awareness-training/resources/stop-phish
CEO Fraud: https://www.sans.org/security-awareness-training/resources/ceo-fraudbec
Spersonalizowane oszustwa: https://www.sans.org/security-awareness-training/resources/personalized-scams

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz