Phishing i metoda „na wnuczka”

11 marca spotkaliśmy się kolejny raz z seniorami. Tematem tego spotkania były oszustwa phishingu i metodą „na wnuczka”. Na spotkaniu seniorzy dowiedzieli się co to są ataki socjotechniczne, jakie metody mogą stosować oszuści i jak się przed nimi zabezpieczyć. Uczniowie odegrali małe scenki, wcielając się w role oszustów i seniorów. Następnie wspólnie dyskutowaliśmy o tym, czy mimo wszystko warto korzystać z usług Internetu.

Coraz więcej słyszymy ostatnio o socjotechnice, czyli różnych sposobach manipulacji, która polega na wykorzystaniu ludzkich emocji, zachowań i psychologicznych słabości do uzyskania informacji lub wywarcia wpływu na drugą osobę. Oszuści doskonale znają te sztuczki, dlatego tak często stosują je zarówno w internetowych atakach, takich jak phishing, czy w próbach wyłudzeń „w realu”, tzw. metodą „na wnuczka”. W obydwu przypadkach wspólnym mianownikiem jest wywoływanie silnych emocji, chęć sprawienia, by ofiara przestała myśleć racjonalnie i szybciej podjęła decyzje, które mogą prowadzić do wyłudzenia pieniędzy lub danych.
Na dzisiejszym spotkaniu uczestnicy zajęć dowiedzieli się, jak rozpoznać takie oszustwa, jak nie dać się zmanipulować i jak reagować, gdy jesteśmy celem ataku. Nauczyli się też, jak ważne jest zachowywanie zimnej krwi w sytuacji, gdy ktoś próbuje wywierać na nas presję. Okazuje się bowiem, że zdrowy rozsądek i nieuleganie emocjom są potężną bronią w walce z oszustami.

Ataki socjotechniczne

Ataki socjotechniczne to metoda manipulacji, która wykorzystuje ludzkie słabości, aby nakłonić ofiarę do wykonania określonego działania, np. ujawnienia poufnych informacji lub wykonania przelewu pieniędzy.

- Oszuści często grają na emocjach takich jak strach, ciekawość, współczucie czy chęć pomocy. Mogą np. przesyłać alarmujące wiadomości o rzekomym zagrożeniu lub konieczności pilnego działania.
- Atakujący mogą podszywać się pod zaufane osoby lub instytucje (np. pracowników banku, urzędników, przyjaciół) i używać znanych, wiarygodnych nazwisk czy logo.
- Przestępcy mogą wcześniej zebrać informacje o ofierze, korzystając z mediów społecznościowych, co pozwala im na lepsze dopasowanie swoich ataków i wzbudzenie większego zaufania.
- Przykłady: oszustwa związane z fałszywymi ofertami pracy, prośbami o pomoc czy „darmowymi” prezentami lub nagrodami w Internecie.

Phishing

- Jeden z najbardziej popularnych i skutecznych rodzajów ataków w Internecie, polegający na wyłudzeniu danych osobowych lub finansowych.
- Oszuści tworzą fałszywe strony internetowe, e-maile czy wiadomości SMS, które wyglądają jak komunikaty od banków, sklepów internetowych czy innych zaufanych instytucji. Celem jest skłonienie ofiary do kliknięcia w link lub pobrania złośliwego oprogramowania.
- W ramach phishingu przestępcy wysyłają linki do formularzy, w których ofiara zostaje poproszona o podanie swoich danych osobowych, loginów, haseł, numerów kart kredytowych czy innych wrażliwych informacji. Oszuści wykorzystują także inne metody, takie jak SMS-y informujące o konieczności dopłaty do paczki czy telefony od rzekomych pracowników banku.
- Przestępcy często tworzą wrażenie zagrożenia, np. informując ofiarę, że jej konto zostało zablokowane i musi natychmiast podać dane, by je odzyskać.
- Przykłady: e-maile przypominające powiadomienia z banków, z informacjami o rzekomej weryfikacji konta, które prowadzą do fałszywych stron logowania, czy telefony, w których rozmówca wymusza natychmiastowe działanie.

Metoda „Na Wuczka”

- Uwaga! Jeśli znasz lokalne przykłady oszustw, koniecznie o nich opowiedz. Postaraj się też znaleźć informacje statystyczne dotyczące np. kwot, na które okradziono ofiary metodą „na wnuczka” w Twoim regionie (przeszukaj w tym celu stronę internetową lokalnej komendy policji).
- Oszust kontaktuje się z ofiarą, twierdząc, że jest jej wnuczkiem lub innym członkiem rodziny. Mówi, że znalazł się w trudnej sytuacji (np. wypadek, aresztowanie, potrzeba natychmiastowej pomocy finansowej).

- Ofiara jest proszona o przesłanie pieniędzy lub wykonanie przelewu na konto, aby „pomóc” bliskiej osobie. Przestępca może podać fałszywe dane kontaktowe lub numer konta.
- Oszuści umiejętnie grają na uczuciu troski, miłości i chęci pomocy. Często stwarzają poczucie, że ofiara jest jedyną osobą, która może w danej chwili udzielić wsparcia.
- W komunikatach od „wnuczków” często pojawia się presja czasu, oszuści mówią, że trzeba działać „pilnie”, „natychmiast”, „nie można z tym czekać”. Takie słowa zawsze powinny wzbudzić nasze podejrzenia
- Przykłady: telefon od „wnuczka” informującego o wypadku samochodowym, prośba o pomoc w zapłaceniu kaucji czy rzekomych kosztów leczenia.

Jak sobie radzić z oszustami?

- Nie ufaj emocjom. Ataki socjotechniczne i phishing często wykorzystują emocje, takie jak strach, zaskoczenie czy poczucie winy. Jeśli otrzymasz nagłą wiadomość, w której ktoś domaga się pilnego działania lub podania danych osobowych, nie reaguj natychmiastowo. Zawsze daj sobie czas na przemyślenie sytuacji. Zadzwoń też do bliskiej osoby i opowiedz o zdarzeniu. Taka rozmowa może pomóc Ci poradzić sobie z problemem.
- Weryfikuj informacje. Przestępcy często podszywają się pod zaufane instytucje, takie jak banki, firmy kurierskie czy urzędników. Zanim klikniesz w linki w e-mailach czy SMS-ach, sprawdź adresy nadawców oraz weryfikuj informacje na oficjalnych stronach internetowych. Jeśli podejrzewasz, że Twój rozmówca jest oszustem, rozłącz się i zadzwoń na infolinię np. banku, by upewnić się, że rozmawiał z Tobą realny konsultant.
- Nie udostępniaj swoich danych osobowych przez telefon ani w internecie. Nigdy nie przekazuj nikomu danych osobowych ani nie przelewaj pieniędzy bez uprzedniego zweryfikowania sytuacji. Jeśli otrzymasz telefon od kogoś, kto twierdzi, że jest Twoim bliskim, oddzwoń na numer, który masz zapisany w telefonie, lub skontaktuj się z tą osobą w inny sposób (np. na komunikatorze).
- Zawsze sprawdzaj adresy URL. Oszuści tworzą strony internetowe, które wyglądają identycznie jak oficjalne strony banków czy sklepów online. Zanim podasz swoje dane logowania lub dokonasz płatności, sprawdź dokładnie adres strony w poszukiwaniu literówek.
- Uważaj na nieznane numery i wiadomości. W phishingu i metodzie „na wnuczka” oszuści często wykorzystują numer telefonu, który może wyglądać na zaufany, lub nawiązują kontakt przez media społecznościowe. Bądź czujny i nie daj się zwieść!
- Zabezpiecz swoje konta silnymi hasłami. Używaj silnych, unikalnych haseł do różnych kont, aby w razie wycieku danych z jednego serwisu nie doszło do przejęcia innych kont. Korzystaj też z uwierzytelniania dwuskładnikowego i menedżerów haseł. Nie klikaj w linki i nie pobieraj załączników z podejrzanych maili. Możesz w ten sposób pobrać na swoje urządzenie szkodliwe oprogramowanie lub np. trafić na fałszywą stronę płatności.