KONSPEKT

TEMAT SPOTKANIA: Cyberprzestępstwo. *Phishing*

CEL: Budowanie świadomości na temat oszustwa *phishingu* oraz kształtowanie odpowiedzialnych postaw

ZAKRES TREŚCI:

1. Wstęp
2. Definicja *phishingu*
3. Siła socjotechniki
4. Postawy ograniczające bycie ofiarą *phishingu*
5. Przykłady praktyczne - ćwiczenia

WYNIKI:

1. Znajomość różnych form *phishingu*
2. Umiejętność właściwej reakcji, gdy mamy do czynienia z *phishingiem*
3. Kształtowanie dobrych praktyk podczas korzystania z sieci

1. Wstęp

Badanie przeprowadzone przez jedną z firm analitycznych w związku z sytuacją wywołaną pandemią pokazuje, że ruch w sieci zwiększył się w zależności od kraju od 20% do nawet 40%, przy czym w zakresie używania komunikatorów (np. Zoom, Skype) odnotowano wzrost trzykrotny, a w sferze *gamingowej* nawet czterokrotny.

Zwiększony ruch znajduje również odzwierciedlenie w tym, że duża część Polaków rezygnuje z zakupów w sklepach tradycyjnych (a decydując się na zakupy wybiera płatności zbliżeniowe kartami lub urządzeniami) albo decyduje się na zakupy za pośrednictwem oferty *e-commerce*.

W ciągu ostatnich pięciu lat proporcja relacji transakcji gotówkowych do bezgotówkowych zmieniła się z 98% do 2% na 57% do 43%.

Rozpytanie uczniów/uczestników

Na samym początku warto zwrócić uwagę uczestników/uczniów na ich skojarzenia związane z pojęciem *phishingu*. Czy ich wiedza oparta jest wyłącznie o przekaz medialny? Czy bezpośrednio (jako ofiary) lub pośrednio (jako osoby trzecie) spotkali się z jakąkolwiek formą *phishingu*? Z czym związane są takie sytuacje? Czy zbierane przez nich doświadczenia mają wpływ na korzystanie przez nich z sieci? Podane przez uczniów odpowiedzi można zapisać na tablicy.

2. Definicja *phishingu*

Password harvesting fishing lub po prostu *phishing* (jedna z teorii mówi o celowo błędnym zapisie słowa *fishing*) to jedna z metod oszustwa dokonywanego za pośrednictwem sieci, polegająca na

pozyskaniu przez oszusta poufnej informacji osobistej. Z reguły dotyczy to danych wrażliwych pozwalających zidentyfikować naszą osobę, ale także danych służących nam do uwierzytelniania naszej tożsamości dostawcom usług, z których korzystamy na co dzień (login, hasło, sms lub e-mail autoryzujący).

Oszust w oparciu o wybrany model socjotechniki podszywa się pod znaną nam osobę, firmę lub instytucję publiczną i próbuje wyłudzić dotyczące nas wrażliwe informacje, które następnie może wykorzystać do szantażu, zainfekowania naszych urządzeń lub korzystania z przypisanych do nas usług (np. bankowość elektroniczna, skrzynka poczty elektronicznej).

Nie zawsze atak *phishingowy* kończy się dla ofiary szkodą majątkową. Pozyskanie danych umożliwiających zalogowanie się na nasze konto poczty elektronicznej pozwala rozesłać materiał w postaci spamu za pośrednictwem naszej skrzynki do szerszego kręgu odbiorców, co na pozór utożsamia wysyłkę z naszym własnym działaniem. O ile w przypadku prywatnego adresu mailowego nie stanowi to realnego zagrożenia, to już skorzystanie z adresu osadzonego na domenie np. instytucji finansowej i rozesłanie wiadomości do klientów banku stanowi duże niebezpieczeństwo dla wyrządzenia szkody majątkowej.

Phishing to obecnie najpopularniejsze przestępstwo popełniane z użyciem sieci. Od 2018 roku w Polsce obowiązuje ustawa o Krajowym Systemie Cyberbezpieczeństwa, która nakazuje raportować tzw. incydenty – zdarzenia mogące mieć niekorzystny wpływ na cyberbezpieczeństwo, tj. naruszające poufność, integralność, dostępność, autentyczność przetwarzanych danych lub związanych z nimi usług. W 2019 roku polskiego systemu reagowania na incydenty naruszeń (CERT) wpłynęło prawie 6 500 zgłoszeń, z czego ponad połowa dotyczyła właśnie *phishingu*. Warto pamiętać, że liczba ta dotyczy tylko zgłoszonych incydentów i ich realna liczba może być wyższa.

Nie można zaprzeczyć stwierdzeniu, że zintensyfikowanie korzystania z sieci w związku z pandemią z pewnością doprowadzi do wzrostu liczby incydentów w 2020 roku i kolejnych prób *phishingu*.

Obserwując rynek widać, że to właśnie banki i instytucje finansowe prowadzą najwięcej kampanii informacyjnych na temat *phishingu*, gdyż najwięcej spotyka się prób wyłudzenia danych do konta bankowego za pośrednictwem fałszywych platform rozliczeniowych (np. popularne PayU). Efekty są ciągle dalekie od zamierzonych. Z przeprowadzonego w 2019 roku badania na zlecenie jednego z banków wynika, że 30% dorosłych Polaków w ogóle nie zna *phishingu*, a 32% ma wrażenie, że wie, ale nie jest tego pewna.

3. Siła socjotechniki

Posiadanie aplikacji infekującej czy znajomość podstawowych technik manipulacji często nie jest wystarczające do przeprowadzenia skutecznego ataku *phishingowego*, ponieważ dopiero właściwy dobór mechanizmu socjotechniki dostosowanego do konkretnego odbiorcy (lub lekceważące podejście odbiorcy do podsyłanej mu przez oszusta treści) pozwala na udostępnienie mu poufnych informacji.

Dlatego też w trakcie korzystania z sieci i telefonu tak ważna jest nasza świadomość w kontekście podejmowanych działań (wyrażanie zgód, otwieranie maili, przechodzenie odnośnikami na kolejne strony internetowe, odczytywanie sms, instalowanie aplikacji, korzystanie z portali społecznościowych). Zachowaniu tej świadomości z pewnością nie sprzyja tendencja w konstruowaniu witryn i aplikacji, gdzie głównym założeniem jest intuicyjność interfejsu dająca nam możliwość jak najszybszego przejścia do interesującej nas treści.

Okazuje się zatem, że do wyłudzenia naszych prywatnych informacji nie są potrzebne żadne wyspecjalizowane narzędzia lub aplikacje.

Wyobraźmy sobie, że oszust jest w posiadaniu wirusa, którego wprowadzenie do naszego komputera lub telefonu, w którym przechowujemy dane prywatne i informacje wrażliwe doprowadziłoby do ich uszkodzenia, usunięcia lub upublicznienia.

Nasz komputer, telefon i znajdujące się na nich aplikacje są chronione hasłami, posiadamy program antywirusowy i zaporę sieciową, dbamy o aktualizację oprogramowania.

Bez naszej pomocy pozyskanie danych znajdujących się na naszych urządzeniach lub wprowadzenie do nich tego szkodliwego wirusa jest wysoce utrudnione.

Dlatego tak dużą uwagę przywiązuje się w przypadku próby wyłudzenia informacji do socjotechniki, która zajmuje się badaniem różnych technik manipulacji.

Wydarzenia na czasie. Szczególną uwagę należy zachować w wypadku informacji budzących powszechne zainteresowanie, aktualnych. Np. w 2020 roku próby ataków *phishingowych* podejmowano w oparciu o tematykę pandemii, wybory prezydenckie, Euro 2020, mikrorachunek VAT, 13 emeryturę, Black Friday.

Wykorzystanie emocji. Treści przekazywane przez dostawców usług lub podmioty publiczne nie są nacechowane emocjami. Jeżeli przesłana wiadomość zawiera informację wzbudzającą w nas poczucie strachu, przesadnej ekscytacji paniki lub przekonuje nas o konieczności natychmiastowego działania, warto uważniej zweryfikować przesłany materiał.

Osoba trzecia. Prowadzenie korespondencji mailowej lub rozmów w ramach popularnych komunikatorów umożliwia nieostrożnemu użytkownikowi podszycie się pod naszych znajomych, współpracowników lub członków rodziny. Przyjęcie ogólnej zasady, zgodnie z którą nie udostępniamy wrażliwych danych (w tym haseł) poprzez wskazane kanały informacji pozwoli uchronić się przed niebezpieczeństwem omyłkowego ujawnienia tych danych oszustowi.

Rozpytanie uczniów/uczestników

W świetle przedstawionych powyżej informacji kształtują się podstawowe postawy związane z ograniczaniem narażenia na cyberatak *pishingowy*. Czy uczestnicy/uczniowe potrafią wymienić zachowania, które mogłyby ograniczyć stopień ich narażenia na taki atak? Co mogą zrobić w swoim środowisku? Podane przez uczniów odpowiedzi można zapisać na tablicy.

4. Postawy ograniczające bycie ofiarą *phishingu*

- Jeżeli znasz adres strony, unikaj wprowadzania jej w wyszukiwarce
- Przed przejściem na stronę z poziomu wyszukiwarki sprawdź poprawność domeny
- Przed kliknięciem w link korzystaj z opcji podglądu łącza, aby zweryfikować rzetelność przekierowania
- Unikaj przekazywania danych wrażliwych (loginów i haseł) za pośrednictwem poczty elektronicznej, komunikatorów internetowych, telefonu
- Unikaj haseł tworzonych w oparciu o łatwy do odszyfrowania algorytm
- Korzystaj z kilku adresów poczty elektronicznej zapewniając gradację przypisania danych do poszczególnych kont
- Nie otwieraj linków znajdujących się bezpośrednio w wiadomościach
- Wiadomości (e-mail, sms) ocenione jako podejrzane oznaczaj jako spam, aby usprawnić pracę algorytmu
- Unikaj otwierania niechcianych wiadomości wysyłanych za pośrednictwem komunikatora społecznościowego

- Dbaj o aktualizację oprogramowania antywirusowego, zapory sieciowej i aplikacji sieciowych
- Aplikacje na telefon pobieraj z zaufanych źródeł
- Potwierdzaj u dostawców usług wiadomości wysyłane rzekomo od nich

5. Przykłady praktyczne – ćwiczenia

PRZYKŁAD 1

Korzystając z mobilnego dostępu do bankowości elektronicznej dowiadujemy się, że środki na naszym koncie zniknęły bez naszej wiedzy.

Na pierwszy rzut oka może się wydawać, że udostępnienie przez nas danych oszustowi powoduje, że sami jesteśmy sobie winni i odpowiedzialni za utratę środków na naszym koncie bankowym. Sytuacja nie jest jednak taka oczywista. Zawierając umowę rachunku bankowego ustalamy z bankiem, że będzie on prowadził na naszą rzecz (jesteśmy posiadaczami rachunku) określony, wydzielony rachunek oznaczony numerem, na którym będziemy gromadzili środki pieniężne. Wpłacając 100 zł na rachunek i wypłacając 100 zł następnego dnia oczywiście nie otrzymujemy dokładnie tych samych pieniędzy, ponieważ bank prowadząc nasz rachunek m.in. zobowiązał się, że na każde nasze żądanie wypłaci nam wartość w pieniądzu, którą mu wcześniej powierzyliśmy, a nie ten konkretnie wpłacony pieniądz. To prawo żądania wypłaty przez bank środków, które mu powierzyliśmy nazywamy wierzytelnością.

A co w sytuacji, kiedy sprawdzamy stan naszego rachunku i okazuje się, że na koncie znajduje się mniejsza kwota, niż ta, którą powierzyliśmy kilka dni wcześniej bankowi i od tego czasu nie korzystaliśmy z wypłat i płatności z tego rachunku?

Bank nie zabezpieczając dostatecznie swojego systemu (mechanizmy antyfraudowe, analiza ruchów na stronie, danych geolokalizacyjnych logowań, numerów IP, kwoty przelewu) umożliwił wypłatę oszustowi części naszej wierzytelności – zmniejszając ją. W wielu wypadkach to zatem bank ponosi konsekwencje oszustwa. Odpowiedzialność spoczywa na posiadaczu rachunku, jeżeli ujawnione będzie jego wyraźne niedbalstwo w dysponowaniu danymi do rachunku.

Z tego też względu wiele kampanii informacyjnych obecnych w mediach na temat tego oszustwa jest inicjowanych właśnie przez banki. Sprawa nie jest wcale oczywista i jest duża szansa, że w przypadku pozbawienia nas środków wypłaconych przez osoby trzecie posługujące się *phishingiem* bank będzie zobowiązany do zwrotu środków, które znikły z naszego konta. Nawet jeśli postępowanie reklamacyjnie w banku (bez lub z udziałem Rzecznika Finansowego) nie da zamierzonego efektu, możemy poszukać pomocy w sądzie. Oczywiście we wszystkich przypadkach podejrzenia kradzieży środków zawiadamiamy organy ścigania.

PRZYKŁAD 2

Od czasu do czasu korzystamy z popularnego operatora przesyłek pocztowych. Na nasz numer telefonu otrzymaliśmy od nadawcy „INP0ST" wiadomość informującą, że uzyskanie kodu odbioru przesyłki uzależnione jest od pobrania aplikacji operatora, do której link znajduje się poniżej.

Oczywiście po odczytaniu wiadomości nie uruchamiamy odnośnika. W pokazanej sytuacji już na pierwszy rzut oka widać, że wiadomość nie pochodzi od zaufanego dostawcy, ponieważ posługuje się on nazwą INP0ST zamiast INPOST. Literówki lub brak polskich znaków często pojawiają się przy próbach wyłudzenia informacji drogą elektroniczną.

Nie zawsze sytuacja będzie tak oczywista. Na pewno warto przeanalizować, jaki był schemat zachowania operatora pocztowego w wypadku próby doręczenia nam przesyłek w przeszłości. Jak wyglądały wiadomości wysyłane na nasz telefon przez operatora w przeszłości? Czy jeśli korzystamy z aplikacji, to czy zaproponowana forma pobrania nowej/aktualizacji starej aplikacji jest zgodna z dotychczasowym schematem?

Nawet jeśli nasz numer nie został wykradziony z bazy operatora pocztowego, a został uzyskany losowo, to prawdopodobieństwo, że właśnie oczekujemy na doręczenie paczki jest całkiem spore, co zwiększa ryzyko, że odruchowo uruchomimy aplikację, która miałaby zainfekować nasze urządzenie i udostępnić *phisherowi* dane wrażliwe.

PRZYKŁAD 3

Na nasz adres mailowy przychodzi wiadomość od komornika, który działa na zlecenie wierzyciela. Jesteśmy wzywani do natychmiastowej zapłaty na wskazany numer rachunku, a w wypadku jej braku wysokość długu wzrośnie o dodatkowe koszty należne dla komornika. Dodatkowo wiadomość obejmuje wezwanie do podania numeru PESEL oraz adresu zamieszkania celem weryfikacji odbiorcy wiadomości.

Postępowanie egzekucyjne jest uregulowane w kodeksie postępowania cywilnego i co do zasady korespondencja w sprawie egzekucyjnej

powinna być prowadzona pisemnie, a pewnością zawiadomienie o wszczęciu egzekucji powinno być doręczone na adres zamieszkania w formie pisemnej (nie wyłącza to oczywiście kontaktu z komornikiem mailowo na dalszym etapie sprawy).

Komornik przed wszczęciem egzekucji nie podejmuje nieodpłatnie innych czynności zmierzających do wyegzekwowania długu, ponieważ nie ma on w tym żadnego interesu.

Warto zwrócić uwagę na domenę mailową, którą posługuje się nadawca wiadomości. Domena przypisana komornikom jest charakterystyczna i jest związana z domeną Krajowej Rady Komorniczej (komornik.pl).

Komornik egzekwując należność względem dłużnika działa na podstawie orzeczenia z klauzulą wykonalności (tzw. tytułu wykonawczego), które zawiera w swej treści PESEL dłużnika. Adres jest weryfikowany za pośrednictwem bazy PESEL-SAD.

Organy państwowe nie ustalają danych adresowych osób fizycznych za pośrednictwem korespondencji mailowej.