CyberMSME

Cyberbezpieczeństwo dla mikro, małych i średnich firm

Socjotechniki. Kiedy użytkownicy są najsłabszym ogniwem...

Autorzy: CTS Customized Training Solutions i CASE

Erasmus+

Cele i założenia:

Po zakoczeniu tego modułu będziesz potrafił/-a:

- określić, czym są socjotechniki
- rozpoznać i rozróżnić najczęściej używane socjotechniki
- zrozumieć mechanizmy manimulacyjne używane przez sprawców
- zlokalizować potencjalne źródła ataków
- ocenić ryzyko ataku socjotechnicznego na Twoją firmę

Spis Treści

Rozdział 1: Czym są socjotechniki?

Rozdział 2: Metody socjotechniczne

Rozdział3: Przeciwdziałanie socjotechnikom

Rozdział 1: Czym są socjotechniki?

Sekcja 1.1: Definicja

Socjotechnika w kontekście IT jest terminem używanym do opisania różnych złośliwych działań realizowanych poprzez interakcje międzyludzkie. Podstawą jej działania jest manipulacja w sensie psychologicznym. Celem zaś jest nakłonienie użytkownika do popełnienia błędu naruszającego zasady bezpieczeństwa. Innymi słowy, atak socjotechniczny jest możliwy tylko wtedy, gdy użytkownik nie jest świadomy, że sprawca zamierza mu zaszkodzić.

Czy jesteś bezpieczny/-a?

Ataki socjotechniczne mogą uderzyć w Ciebie w każdej chwili, bez względu na to, jak dużą lub małą firmę prowadzisz.

Najsłabsze ogniwo

Najsłabszym ogniwem w całym procesie jest użytkownik: Ty, Twoi pracownicy, Twoi partnerzy biznesowi. Aby zminimalizować ryzyko należy zmaksymalizować świadomość. Jak to zrobić?

Erasmus+

Rozdział 1: Czym są socjotechniki?

Sekcja 1.2: Czym jest atak socjotechniczny?

Zrozumienie ataków socjotechnicznych jest pierwszym krokiem do zwiększenia świadomości Twojej i Twoich pracowników. Przede wszystkim musisz pamiętać, że ataki te organizują cyberprzestępcy i oszuści. Nie zawsze jednak chodzi im o pieniądze. Wystarczającym powodem do złamania przez nich prawa może okazać się każda ilość informacji (np. hasło) lub wrażliwych danych.

Jaki rodzaj danych uważa się za dane wrażliwe?

- dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne
- przynależność do związków zawodowych
- dane genetyczne i biometryczne przetwarzane wyłącznie w celu identyfikacyjnym
- dane dotyczące stanu zdrowia
- dane dotyczące życia seksualnego lub orientacji seksualnej*

*Źródło: European Commission > What personal data is considered sensitive?

Erasmus+

Rozdział1: Czym są socjotechniki?

Sekcja 1.3: Podstawy ataków socjotechnicznych

Zwykle atak socjotechniczny składa się z **3 etapów**...

etap 1: sprawca namierza ofiarę

- identyfikacja ofiary
- zebranie informacji
- wybór metod ataku

etap 2: sprawca zdobywa zaufanie ofiary

- zaangażowanie ofiary w opowieść
- przejęcie kontroli nad interakcją
- zdobycie przewagi

etap 3: sprawca osiąga cel, wykradając dane lub naruszając procedury bezpieczestwa

- przeprowadzenie ataku
- usunięcie śladów
- zniknięcie sprawcy

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 1: Czym są socjotechniki?

Sekcja 1.3: Podstawy ataków socjotechnicznych

W ataku socjotechnicznym sprawca bazuje na manipulacji. Z tego względu jest to większe zagrożenie niż bezpośredni cyberatak na Twój system. Dlaczego? Ponieważ musisz mieć pewność, że Ty i Twoi pracownicy potraficie odróżnić manipulację od klasycznej reklamy. A nie jest to łatwe, gdyż jesteśmy tylko ludźmi.

Co się dzieje podczas ataku?

Sprawca ataku gra na słabościach ofiary. Pomyślmy więc o ataku socjotechnicznym jak o nieczystej grze, w której tylko jedna osoba zna reguły, co więcej, czasem je tworzy! Jak każda gra, ta również posiada pewne ogólne mechanizmy, które mogą zwiększyć Twoją szansę na wygraną.

Większość ataków socjotechnicznych opiera się na 5 zasadach: **autorytet, dowód społeczny, niedostępność, pilność, zażyłość.**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 1: Czym są socjotechniki?

Sekcja 1.3: Podstawy ataków socjotechnicznych

autorytet:
napastnik prezentuje się w roli autorytetu

niedostępność:
napastnik wykorzystuje mechanizm, wedle którego ofiara coś straci, jeśli nie zareaguje

zażyłość:
napastnik przekonuje ofiarę do wykonania określonych kroków, zdobywszy jej zaufanie

dowód społeczny:
napastnik wykorzystuje presję otoczenia, aby zmusić ofiarę do podjęcia działania

pilność:
napastnik stosuje przekonanie, że ofiara straci, jeśli nie zareaguje tak szybko, jak to możliwe

Erasmus+

Rozdział 1: Czym są socjotechniki?

Sekcja 1.4: Kto może paść ofiarą?

Właśnie poznałeś 5 zasad ataków socjotechnicznych. Zasady te związane są z psychologicznymi motywami i motywacjami ludzi. Te, oczywiście, powstają głęboko w naszej podświadomości.

Robert Cialdini, psycholog, mówca i autor książki "Wywieranie wpływu na ludzi: Teoria i praktyka" opisał, w jaki sposób ludzie mogą ulegać wpływom innych. Według Cialdiniego, kluczowymi czynnikami są:

Reguła wzajemności

Ogólnie rzecz biorąc, ludzie czują się zobowiązani do odwdzięczenia się po otrzymaniu pomocy. Ta cecha wydaje się być tak naturalna dla wszystkich kultur, że nie czujemy się skrępowani, gdy ktoś prosi nas o odwzajemnienie przysługi.

Cialdini wspomniał, że tzw. specjaliści ds. zapewnienia zgodności często oferują potencjalnym klientom drobny upominek, aby wykorzystywać to zjawisko. Badania pokazują, że nawet niechciany prezent wpłynie na odbiorcę, aby się odwzajemnić.

Erasmus+

Rozdział 1: Czym są socjotechniki?

Sekcja 1.4: Kto może paść ofiarą?

Reguła konsekwencji

Ludzie często trzymają się swoich przyzwyczajeń i pierwszych wyborów. Pragną, aby ich zachowanie wyglądało na konsekwentne. Cenią sobie również konsekwencję u innych.

Cialdini wspomniał, że ma to także związek z silnym dążeniem ludzi do podtrzymywania podjętych zobowiązań wtedy, gdy są one uzasadnione i umotywowane.

Reguła społecznego dowodu słuszności

Wspomnieliśmy już o tym mechanizmie mówiąc o podstawach ataków socjotechnicznych. Termin "dowód społeczny" oznacza, że ludzie przy podejmowaniu decyzji ufają innym, podobnym do siebie osobom. Uwypukla się to w sytuacjach niepewnych lub niejednoznacznych.

Cialdini wspomniał, że tzw. specjaliści ds. zgodności, wykorzystując tę zasadę, przedstawiają fałszywe informacje o decyzjach innych osób. Na przykład przygotowują wyreżyserowane wywiady, zmyślone dane lub studia przypadków.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 1: Czym są socjotechniki?

Sekcja 1.4: Kto może paść ofiarą?

Reguła lubienia

Cóż, nie jest to tajemnicą — ludzie chcą być lubiani. W myśl tej zasady, ludzie chętniej przystają na oferty osób, które lubią.

Cialdini wspomniał, że lubienie ludzi może przejawiać się na kilka sposobów, np. może mieć wymiar pociągu fizycznego lub sympatii do osób o podobnych cechach.

Reguła autorytetu

Jest to prawdopodobnie najbardziej niebezpieczny element wpływu, dający sprawcy ataku największą władzę. Generalnie, ludzie podążają za tymi, którzy w ich oczach wydają się być najsilniejsi, lepsi, pewni siebie; którzy mają coś, czego nie mają oni sami. Badania pokazują, że ludzie zazwyczaj reagują w sposób zautomatyzowany na polecenia od autorytetu, a nawet na symbole autorytetu (jak drogie samochody, mundury, dyplomy, stopnie naukowe itp.) Dzieje się tak nawet wtedy, gdy instynkt podpowiada, że nie powinniśmy wykonywać takich poleceń.

Rozdział 1: czym są socjotechniki?

Sekcja 1.4: Kto może paść ofiarą?

Reguła niedostępności
Wspomnieliśmy już o tej regule, mówiąc o podstawach ataków socjotechnicznych. Reguła niedostępności odnosi się do chęci posiadania przez ludzi mniej dostępnych rzeczy. To, co mniej dostępne, może być ekskluzywne lub dostępne tylko przez określony czas. Ta cecha pomaga np. reklamodawcom promować towary jako "limitowane" lub "dostępne tylko w ograniczonym okresie".

Kto zatem może paść ofiarą ataku socjotechnicznego?

Ogólnie rzecz ujmując — każdy. To, co jednak ma znaczenie, to profil psychologiczny danej osoby i jej aktualna kondycja psychiczna.

Nigdy nie zapominaj, że socjotechniki bazują na manipulacji.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 2: Metody socjotechniczne

Sekcja 2.1: Wiadomość od przyjaciela

Wyobraź sobie, że jesteś w pracy, piszesz jakieś raporty w Excelu w firmowej chmurze, a w międzyczasie zaglądasz na swoje konta w mediach społecznościowych. W jednej przeglądarce masz więc otwarty zarówno Excel, jak i Facebook. Wypełniasz te nudne wykresy i nagle Twój przyjaciel (nazwijmy go Janek) pisze do Ciebie na Messengerze. Janek napisał, że Twoje nagie zdjęcia są dostępne na załączonej stronie — i oczywiście podesłał Ci link. Klikasz go i...

Prawdopodobnie właśnie straciłeś dostęp do swojego konta na Facebooku i/lub swojej strony firmowej. Być może utraciłeś również część danych przechowywanych na swoim komputerze.

Dlaczego Janek Ci to zrobił?

Cóż, bądźmy szczerzy... **To nie był Janek...**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 2: Metody socjotechniczne

Sekcja 2.1: Wiadomość od przyjaciela

Prawdopodobnie był to bot stworzony w celu kradzieży danych. Twój przyjaciel Janek był ofiarą tak samo jak Ty. Napastnik wykorzystał jego tożsamość (w tym przypadku konto w mediach społecznościowych), aby zdobyć Twoje zaufanie. Ostatecznie znasz Janka bardzo dobrze, razem dorastaliście i jesteście przyjaciółmi. Skąd napastnik mógł to wiedzieć?

Może macie wiele wspólnych zdjęć, dużo rozmawiacie przez Messengera, a może to był zbieg okoliczności — ale zadziałało. Teraz jesteś kolejną ofiarą w długim łańcuchu zwanym phishingiem.

Kiedy mogą Cię zaatakować z użyciem tej metody?

Kiedy korzystasz z social mediów, instant messengerów, czatów, emaili, SMSów itd.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 2: Metody socjotechniczne

Sekcja 2.2: Phishing

Obecnie najpopularniejszą metodą socjotechniczną jest phishing. Phishing to każda kampania z użyciem wiadomości, której celem jest przekierowanie ofiary do konkretnego formularza, strony lub punktu płatności. Sprawca podszywa się pod zaufane źródło (np. znajomego, bank, agencję ubezpieczeniową, fundusze inwestycyjne) i układa wiarygodny scenariusz. W przypadku wątpliwości ofiary, sprawca wykorzystuje element silnie emocjonalny.

Jak może wyglądać taki scenariusz?

jak pilna potrzeba pomocy z Twojej strony

Twój "przyjaciel" utknął za granicą, został okradziony, pobity i jest w szpitalu. Potrzebuje pieniędzy i instruuje Cię, jak zrobić przelew.

ALBO

Twój "przyjaciel" zobaczył Twoje nagie zdjęcia w Internecie i wysłał Ci link.

Erasmus+

Rozdział 2: Metody socjotechniczne

Sekcja 2.2: Phishing

jak działania o pozornie legalnym podłożu

Twój "bank" wysyła Ci SMS z linkiem i z prośbą o potwierdzenie salda.

ALBO

Twój "dostawca usług hostingowych" wysłał Ci email, twierdząc, że zhakowano im serwer danych i że musisz się z nimi skontaktować za pomocą załączonego formularza.

jak prośba o datek na charytatywną zbiórkę pieniędzy itd.

Jakaś ważna osoba prosi Cię o wsparcie w usuwaniu skutków strasznej klęski żywiołowej, w kampanii politycznej lub w akcji charytatywnej.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 2: Metody socjotechniczne

Sekcja 2.3: Vishing

Vishing to odmiana phishingu wykorzystująca technologię głosową, taką jak rozmowa telefoniczna, rozmowa za pośrednictwem komunikatora Messenger/Zoom lub fałszywe wiadomości głosowe. Mechanizmy manipulacji są takie same jak w phishingu, ale sprawca wykorzystuje naglące wiadomości głosowe lub telefony, aby przekonać ofiarę do podjęcia działań.

Jak może wyglądać scenariusz?

wielkie zagrożenie

Po oświadczeniu napastnika o ogromnym niebezpieczeństwie, jak np. włamanie na konto bankowe lub niezapłacone podatki, ofiara czuje presję, aby działać szybko. Pod wpływem emocji, ofiara ujawnia swoje poufne dane i hasła w trakcie rozmowy telefonicznej.

Rozdział 2: Metody socjotechniczne

Sekcja 2.3: Vishing

Kiedy mogą Cię zaatakować z użyciem tej metody?

Kiedy posiadasz publiczny profil/ stronę firmową z numerem telefonu (nie tylko swoim, ale i pracowników), udostępniasz numer telefonu w mediach społecznościowych, korzystasz z komunikatorów i aplikacji z opcją połączeń głosowych itp.

Sekcja 2.4: Baiting

Czasami zamiast niebezpieczeństwa pojawia się ogromna szansa. To Ty jesteś zwycięzcą, szczęściarzem, możesz zainwestować niewielkie pieniądze i w krótkim czasie zamienić je w fortunę! Pamiętaj, że sprawcy ataków często stosują baiting pod przykrywką różnych funduszy europejskich. Mogą cię zaatakować za pomocą formularza online, telefonu, a nawet osobiście.

Rozdział 2: Metody socjotechniczne

Sekcja 2.4: Baiting

Jak może wyglądać scenariusz?

tu jest coś, czego pragniesz →

Sprawca ataku wybiera coś, czego ludzie pragną, np. ściągnięcie nowego filmu. Wiele osób skorzysta z okazji, aby znaleźć coś, czego pragną.

superokazja! →

Sprawca ataku może stworzyć ogłoszenie informujące o niesamowicie korzystnej ofercie w serwisie ogłoszeniowym, na portalu aukcyjnym itp. Zwykle sprawca korzysta z konta sprzedawcy z dobrą oceną, aby zminimalizować Twoje podejrzenia.

Jeśli ofiara chwyci przynętę, to jej urządzenie zostanie zainfekowane złośliwym oprogramowaniem. To z kolei generuje dalsze działania przeciwko ofierze i jej kontaktom.

Rozdział 2: Metody socjotechniczne

Sekcja 2.5: Podsumowanie

Oczywiście, wszystkie wymienione scenariusze są tylko przykładami metod socjotechnicznych. Pamiętaj, że sprawca ataku jest osobą przebiegłą, obeznaną z technologią i znającą techniki manipulacyjne.

Phishing, vishing i baiting mogą mieć nieskończenie wiele scenariuszy. Wszystko zależy od pomysłowości i kreatywności sprawcy ataku.

Aby być na bieżąco, sprawdzaj regularnie doniesienia o najnowszych praktykach socjotechnicznych.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Rozdział 3: Przeciwdziałanie socjotechnikom

Sekcja 3.1: Dobre i złe praktyki

Jak widać, metody socjotechniczne mają wysoką skuteczność i zasięg dzięki wykorzystaniu manipulacji, a także dzięki temu, że ofiary wykazują się słabą świadomością i wiedzą w tym temacie. Warunkiem udanego ataku jest podatność ofiary na wybrane mechanizmy.

Co zatem możesz zrobić, aby zapobiec atakom socjotechnicznym?

Zwiększ świadomość złośliwych działań, zarówno u siebie, jak i u swoich pracowników, partnerów i klientów. Pamiętaj, że metody socjotechniczne zmieniają się w czasie i przestrzeni, dlatego konieczne jest regularne aktualizowanie swojej wiedzy.

Rozdział 3: Przeciwdziałanie socjotechnikom

Sekcja 3.1: Dobre i złe praktyki

Naucz swoich pracowników, partnerów i klientów, jak cenne są hasła i wrażliwe dane. Pamiętaj, że zabawny post na Facebooku, w którym ktoś pyta Cię o datę urodzenia, może zostać wykorzystany przeciwko Tobie. Pomyśl, ile razy użyłeś swojej daty urodzenia w haśle...

Nie przechowuj wszystkich wrażliwych danych i kluczowych informacji w jednym miejscu. Jeśli sprawca ataku zdoła je wykraść je za pomocą jednego zrzutu ekranu, to znaczy, że musisz popracować nad swoim systemem bezpieczeństwa.

Nie klikaj na otrzymane linki i zdjęcia przed sprawdzeniem źródła. Nawet jeśli źródło wygląda znajomo, nie spiesz się. Przyjrzyj się dokładnie adresowi e-mail, IP, linkowi itp.

Rozdział 3: Przeciwdziałanie socjotechnikom

Sekcja 3.1: Dobre i złe praktyki

Przygotuj przejrzyste standardy bezpieczeństwa dla swojej firmy. Zaplanuj protokół na wypadek ataku i naucz swoich pracowników, partnerów i klientów, co mają robić.

Nie wywołuj niepotrzebnego strachu wśród swoich pracowników, partnerów i klientów. Strach pomaga sprawcy ataku w manipulowaniu ludźmi. Z kolei świadomość i wiedza — wręcz przeciwnie.

Jesteś gotowy/-a stawić czoła metodom socjotechnicznym?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bibliografia i przydatne linki

European Commission > **What personal data is considered sensitive**

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Webroot > What is Social Engineering? **Examples & Prevention Tips**

https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Seon > **What is Social Engineering? Attacks, Techniques & Prevention**

https://seon.io/resources/protect-against-social-engineering-attacks/?utm_term=&utm_campaign=%5BS%5D%20Blog%20-%20dynamic%20%5BEMEA%5D&utm_source=google&utm_medium=cpc&hsa_acc=9367189488&hsa_cam=12655034312&hsa_grp=119030291966&hsa_ad=511148698722&hsa_src=g&hsa_tgt=dsa-414755398l3&hsa_kw=&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwvuGJBhB1EiwACU1AibG5GowOFa1Q_FazH8_RDbrb3OEI7k7fQacOcLKrty9ZFQw-b7i_7hoCDWcQAvD_BwE

Imperva > **Social Engineering**

https://www.imperva.com/learn/application-security/social-engineering-attack/

Verizon > Data Breach Investigations Report > **2021 DBIR Master's Guide**

https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

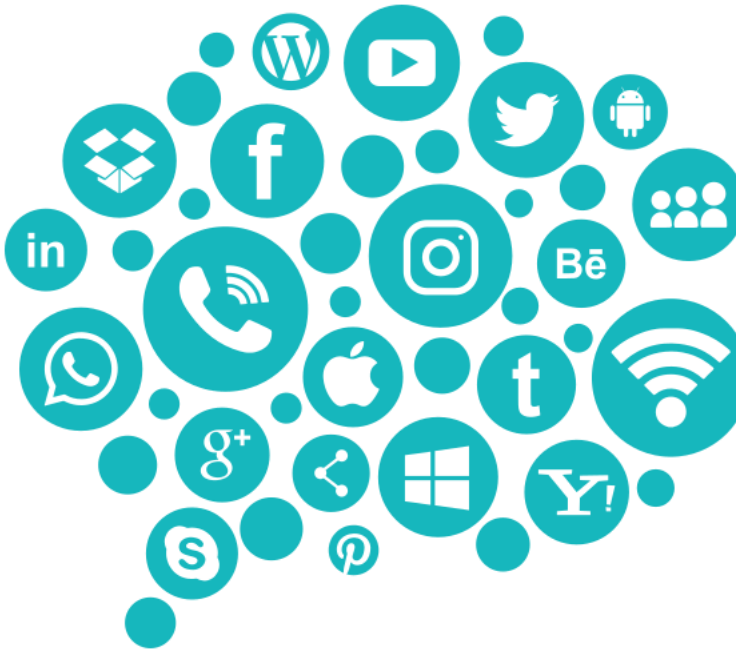
Terranova Security > **9 Examples of Social Engineering Attacks**

https://terranovasecurity.com/examples-of-social-engineering-attacks/

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Dziękujemy za uwagę!



Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.