Inżynieria społeczna

Spis treści

Techniki stosowane w inżynierii społecznej

* W miarę wymyślanie coraz to nowych technologii zabezpieczających, utrudniających znalezienie technicznych luk w systemie, napastnicy będą zwracać się w stronę ludzkich słabości.
    * Czasy się zmieniają, ale ludzie się nie zmieniają

Techniki stosowane w inżynierii społecznej

* Władza -socjotechnik maskuje się za pomocą otoczki władzy, mówiąc, że pracuje w dziale informatyki, jest z zarządu, itp.
* Sympatia -w trakcie rozmowy napastnik dowiaduje się o jakimś hobby lub zainteresowaniu ofiary, po czym sam deklaruje swoje zainteresowanie, entuzjazm. Socjotechnik będzie próbował zachowywać się w sposób podobny do ofiary. Natura ludzka jest tak, że najbardziej lubimy tych, którzy myślą podobnie jak my.

Techniki stosowane w inżynierii społecznej

* Wzajemność -pracownik odbiera telefon od osoby, która przedstawia się, że jest z działu IT, wyjaśnia, że niektóre komputery zostały zainfekowane ransmoware, który nie jest wykrywany przez programy antywirusowe. Problem jest taki, że szkodliwe oprogramowanie może zaszyfrować pliki w komputerze, trudnym do odgadnięcia asymetrycznym kluczem 128 bitowym. Potem proponuje przeprowadzenie rozmówcy przez proces weryfikacji i zapobieżeniu problemowi. Tuż potem napastnik prosi rozmówcę o testy nowej aplikacji… a wiesz, jak już mam Cię na linii, to mam prośbę…

Techniki stosowane w inżynierii społecznej

* Konsekwencja -napastnik kontaktuje się ze młodym pracownikiem w firmie i informuj o wytycznych polityki bezpieczeństwa oraz o konieczności przestrzegania tych zasad. Po omówieniu kilku praktyk bezpieczeństwa rozmówca prosi o podanie swojego hasła do komputera, tak, by sprawdzić, czy spełnia wymogi bezpieczeństwa. Kiedy ofiara podaje swoje hasło, atakujący podaje zalecenia, co do konstrukcji przyszłych haseł w taki sposób, aby sam potrafił je łatwo odgadnąć. Ofiara podporządkowuje się w związku ze swoją wcześniejszą zgodą na dostosowanie się do firmowych praktyk i założeniem, że rozmówca weryfikuje tylko jedynie podporządkowanie regulaminowi

Techniki stosowane w inżynierii społecznej

* Przyzwolenie społeczne -rozmówca twierdzi, że przeprowadza ankietę (jest audytorem z firmy zewnętrznej), a zarazem dla uspokojenia ofiary, podaje nazwiska osób, które wcześniej zdecydowały się odpowiedzieć na pytania. Ofiara wierząc, że zachowanie innych potwierdza wiarygodność prośby, godzi się na udział w ankiecie. Rozmówca zadaje szereg pytań…

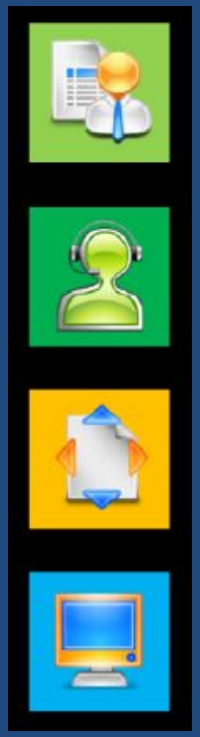
Techniki stosowane w inżynierii społecznej

* Rzadka okazja -napastnik wysyła e-mail oznajmiający, że pierwsze 500 osób, które zarejestruje się na stronie produktu, wygra darmowe bilety na najnowszą premierę filmową. Ofiara niczego nie podejrzewa i dokonuje procesu rejestracji, w trakcie którego proszona jest o podanie adresu e-mail i hasła??? Wiele osób dla wygodny ma tendencję do operowanie jednym loginem i hasłem do wielu witryn i systemów.

Jak się bronić

* Praktyki bezpieczeństwa związane z hasłami dostępowymi
* Procedury ujawniania poufnych informacji lub materiałów
* Procedury i dobre praktyki korzystania z poczty elektronicznej
* Fizyczne wymogi bezpieczeństwa – noszenie identyfikatorów, karty dostępu
* Prawidłowe i bezpieczne sposoby usuwanie poufnych dokumentów, nośników komputerowych i fizycznych,

Dlaczego tak skuteczna



* Polityki bezpieczeństwa są tak silne jak najsłabsze ogniwo, którym najczęściej jest człowiek
* Trudno wykryć, czy to próba ataku socjotechnicznego
* Brak metod określających jednoznacznie atak
* Brak oprogramowania i mechanizmów sprzętowych wykrywających atak

Co powinno wzbudzić naszą czujność?

- Odmowa podania numeru zwrotnego.
  – Nietypowa prośba.
  – Nadmierne okazywanie posiadania władzy.
  – Podkreślanie pilności sprawy.
  – Grożenie konsekwencjami - niepodporządkowanie się prośbie.
  – Okazywanie niechęci w przypadku zadawania pytań.
  – Komplementy lub pochlebstwa.

Fazy ataku socjotechnicznego

1

Research on Target Company

Dumpster diving, websites, employees, tour company, etc.

2

Select Victim

Identify the frustrated employees of the target company

3

Develop Relationship

Develop relationship with the selected employees

4

Exploit the Relationship

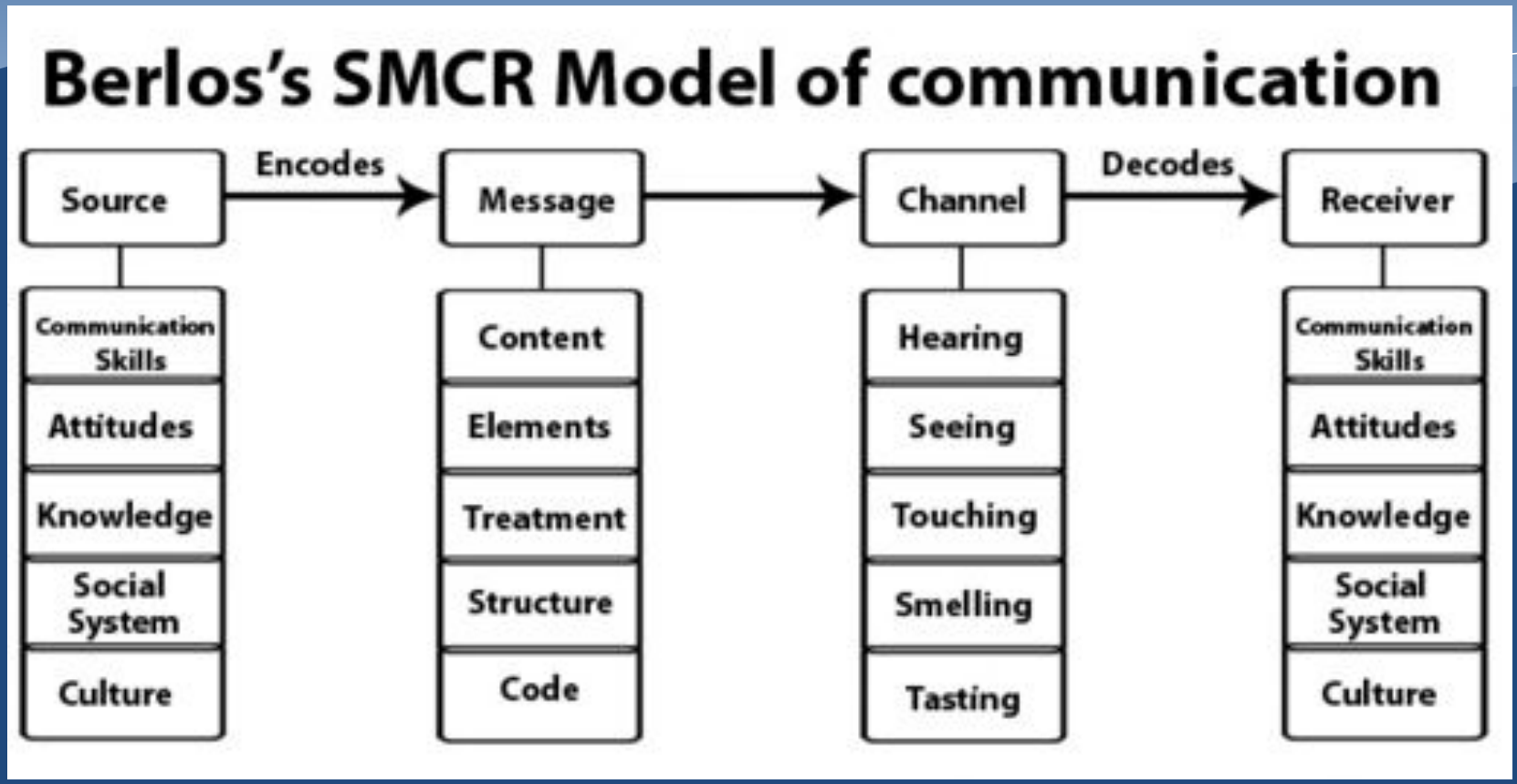
Collect sensitive account information, financial information, and current technologies

„Cele”ataku

Typowe cele atuku socjotechnicznego:

* recepcja, personel helpdesk,
* personel techniczny,
* administratorzy systemów – mimo świadomości posiadają dużą wiedzę na temat organizacji,
* użytkownicy i klienci firmy/organizacji,
* dostawcy /firmy trzecie

Model komunikacji Berlo



Źródło

Aby komunikacja była zrozumiała potrzebne są umiejętności komunikacyjne, które pozwolą innym zrozumieć przekaz.

* **Postawa**
  To wrażenie, jakie wywiera osoba mówiąca oraz jej umiejętności zainteresowania słuchacza.
* **Wiedza**
  klarowność i rzeczowość informacji.
* **System społeczny**
  Uczucia, wartości, przekonania, przekonania religijne i kulturowe drugiej osoby.
* **Kultura**
  Odnosi się do szeroko pojętej kultury, religii oraz tradycji i miejsca gdzie dana informacja jest przekazywana.

Przekaz/komunikat

* **Zawartość**
  Prosty przekaz, który od początku do końca zawiera przekazywaną informację. Staranne dbanie o treść wypowiedzi, by była jasna i sensowna.
* **Elementy**
  Mowa ciała. Wszystko to pomaga przekazać komunikat w sposób wiarygodny, o ile gesty są zgodne ze słowami.
* **Traktowanie**
  To nastawienie z jakim zostaje przedstawiona informacja. Odzwierciedla wiarygodność, tego co mówimy.
* **Struktura**
  Konstruowany przekaz uporządkowany i logiczne przedstawiony.
* **Kod**
  Połączenie języka, gestów, mowy ciała, kultury a nawet innych przekazów jak np. muzyki. Wszystko to składa się na proces przekazywania wiadomości.

Kanał

* słuch
* wzrok
* dotyk
* zapach
* smak

Odbiorca

* W momencie otrzymania informacji odbiorca stara się ją zrozumieć co zostało powiedziane, a następnie na nią odpowiednio reaguje.
* Odbiorca powinien posiadać podobne elementy co nadawca, czyli umiejętności komunikacyjne, postawę, wiedzę, system społeczny. Wtedy komunikacja będzie przebiegała prawidłowo.

Model komunikacji Berlo

Źródło – socjotechnik

Kanał – sposób przekazania komunikatu

Komunikat – co socjotechnik zamierza przekazać odbiorcy/odbiorcom

Odbiorcy – ofiary socjotechnika

Informacja zwrotna – jakie zachowanie socjotechnik chce sprowokować u odbiorcy

Scenariusze

Wiadomość phishingowa skierowana do 25-50 pracowników firmy. Spróbuj ich nakłonić, by odwiedzili stronę o charakterze niebiznesowym, zawierającą złośliwe oprogramowanie, dzięki któremu będziesz mógł włamać się do sieci

Scenariusze

Jedź do firmy i podaj się za potencjalnego kandydata do pracy, który właśnie wylał kawę na swoje CV. Spróbuj przekonać pracownika recepcji, aby wziął od Ciebie pendrive'a, włożył go do swojej stacji i wydrukował dla Ciebie nowy egzemplarz dokumentu…

Scenariusze

Model komunikacji buduje się od końca

Informacja zwrotna – jaką reakcję chcesz wywołać?

Odbiorcy - o ofiarach musisz wiedzieć wszystko

Komunikat -mężczyźni 25-40 lat biorący udział w wirtualnych rozgrywkach piłki nożnej. „*Aby kogoś przekonać, trzeba wskazywać na jego interesy, a nie apelować do rozumu*” – B. Franklin – wskazanie czegoś atrakcyjnego dla adresata

Kanał – email, osobista wizyta

Źródło - Ty

Wywoływanie

* Okazuje się skuteczne z wielu powodów:
  * większość ludzie chce zachowywać się grzecznie w stosunku do obcych,
  * profesjonalistom zależy na wizerunku osoby inteligentnej i dobrze poinformowanej,
  * gdy się kogoś pochwali staje się bardziej wylewny i skłonny wyjawić więcej informacji,
  * większość osób nie będzie kłamać, nie mając ku temu konkretnego powodu
  * większość ludzi reaguje uprzejmością w kontaktach z osobami, które zdają się okazywać im zainteresowanie

Wywoływanie

* Celowe stwierdzenie nieprawdy: „przecież wszyscy wiedzą, że najlepsze oprogramowanie do… robi firma..”
* O: „nieprawda, tak się składa, że nasza firma pracuje nad podobnym zagadnieniem już od 12 lat, od tamtej pory, regularnie osiągamy wyniki o 23% wyższe od innych”

Wywoływanie

* NSA definiuje jako: *„subtelne pozyskiwanie informacji w toku pozornie normalnej i niewinnej rozmowy”*
* Rozmowy mogą odbywać się wszędzie
* Niewielkie ryzyko
* Ofiara nie wie nawet w którym momencie doszło do wycieku informacji

Wchodzenie w rolę

- *„Kluczem do budowania relacji jest szczerość. Jeśli potrafisz ją udawać, sukces murowany”*
- Zasady wchodzenia w rolę:
  - Im lepiej się przygotujesz tym większa szansa na sukces
  - Odwołaj się do własnych zainteresowań -> pewność siebie zależy **zawsze** od zadania i sytuacji
  - Nie lekceważ telefonu
  - Im prostsza rola, tym większa szansa na sukces -> technicy

Wchodzenie w rolę

* Odgrywaj rolę spontanicznie i wiarygodnie
* Przedstaw ofierze logiczny wniosek -> idziesz do lekarza, ten przeprowadza wywiad, ogląda wyniki, coś zapisuje, po czym mówi: „*w porządku do zobaczenia za miesiąc…*”
* *Spece żyją swoją nową tożsamością,*
* *Uwiarygodniają się tworząc profile społecznościowe*
* *Używają stosownych rekwizytów*

Mowa ciała

* http://demotywatory.pl/4415543/15-zdjec-ktore-pokaza-ci-co-mowi-mowa-ciala-o-drugim-czlowieku

Ćwiczenia

* Wykonanie kontrolowanego ataku socjotechnicznego przy pomocy narzędzia SET i Maltego