Cyberbezpieczeństwo
dla zaawansowanych

Skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze

Cesar Bravo
Przedmowa Darren Kitchen, założyciel Hak5

Helion

Tytuł oryginału: Mastering Defensive Security: Effective techniques to secure your Windows, Linux, IoT, and cloud infrastructure

Tłumaczenie: Magdalena A. Tkacz

ISBN: 978-83-283-9833-7

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/cydlza
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

4

ROZDZIAŁ

Łatanie ósmej warstwy

„Środki bezpieczeństwa cybernetycznego często koncentrują się na zagrożeniach pochodzących z zewnątrz organizacji, a nie na zagrożeniach stwarzanych przez niegodne zaufania osoby wewnątrz organizacji. Jednak zagrożenia z wewnątrz są obecnie odpowiedzialne za wiele milionów strat w krytycznej infrastrukturze"

— Ricardo Gazoli — dyrektor wykonawczy ds. informatyki

Użytkownicy są zdecydowanie najbardziej wrażliwym czynnikiem w cyberbezpieczeństwie. Ostatnie badanie ujawniło, że w rzeczywistości ponad 50% ataków jest spowodowanych przez osoby mające dostęp do zasobów firmy (ang. *insider*) — albo przez przypadek (nieumyślnie), albo celowo (złośliwie).

Jednym z powszechnych błędów jest przygotowywanie specjalistów ds. cyberbezpieczeństwa do radzenia sobie z wyzwaniami technicznymi, takimi jak serwery i sieci, a nieprzygotowanie ich do zajmowania się wszystkimi zagrożeniami związanymi z czynnikiem ludzkim wewnątrz organizacji (zarówno działaniami nieumyślnymi, jak i złośliwymi). Wiele osób zgadza się, że zarządzanie użytkownikami jest znacznie bardziej złożone niż zajmowanie się systemami, ponieważ — koniec końców — użytkowników nie można po prostu załatać!

Dlatego zarządzanie użytkownikami jest sztuką; w tym rozdziale pokażę Ci różne wektory ataku skierowane na użytkownika, ale także to, jak możesz opanować wiele technik, metod i narzędzi, aby zapobiec atakom tego rodzaju.

W tym rozdziale zajmiemy się następującymi głównymi tematami:

- Zrozumienie warstwy 8 — zagrożenie wewnętrzne.
- Opanowanie sztuki inżynierii społecznej.
- Obrona przed technikami inżynierii społecznej.
- Obrona przed atakami wykorzystującymi socjotechniki (łatanie warstwy 8).

Warstwa 8 — zagrożenie wewnętrzne

Jak zapewne wiesz, użytkownicy są również nazywani żartobliwie **warstwą 8**, ponieważ znajdują się na szczycie siedmiowarstwowego modelu OSI.

Inaczej, bardziej *profesjonalnie* nazywamy ich **wewnętrznym czynnikiem ludzkim** (ang. *insiders*). Stanowi on poważne zagrożenie: ponieważ znajduje się już wewnątrz sieci, wiele naszych systemów i mechanizmów obronnych (służących do uniemożliwienia użytkownikom dostępu do naszej sieci) ich nie obejmuje.

Teraz zajmiemy się różnymi typami użytkowników, które należy uwzględnić przy tworzeniu strategii bezpieczeństwa cybernetycznego.

Działanie nieumyślne

Z badania przeprowadzonego przez Ponemon Institute wynika, że około 24% naruszeń danych jest spowodowanych przez ludzką *lekkomyślność*. Nazywamy je nieumyślnie popełnionymi błędami, ponieważ są to zazwyczaj błędy popełnione przez użytkownika bez intencji wyrządzenia szkody danym lub systemom.

Wiele osób uważa, że tego typu incydenty są rzadkie lub mają marginalny wpływ. Jednak jak widać na rysunku 4.1, badanie przeprowadzone w 2020 roku przez Ponemon Institute pokazuje zupełnie inną sytuację.

Rysunek 4.1. Koszt zagrożeń wewnętrznych

Podsumowując, najczęstsze pomyłki lub błędy spowodowane lekkomyślnością użytkowników to:

- stosowanie słabych haseł,
- powtarzanie haseł w różnych systemach,
- używanie tego samego hasła do systemów osobistych,
- brak zrozumienia zasad bezpieczeństwa cybernetycznego,
- niewłaściwe użycie lub nadużycie kont uprzywilejowanych,
- pozostawienie urządzenia bez nadzoru,
- nieprawidłowe przetwarzanie danych,

- instalacja nieautoryzowanego oprogramowania,
- nieumyślne przerwanie pracy systemów,
- nieostrożne przeglądanie zasobów Internetu,
- korzystanie z bezpłatnych lub otwartych sieci Wi-Fi,
- zaniechanie przestrzegania zasady „Pomyśl, zanim klikniesz" (czyli klikanie odnośników w załącznikach do wiadomości e-mail lub linkach),
- nieumyślne ujawnienie informacji wrażliwych.

Jak wspomniano wcześniej, są to błędy pojawiające się *przez lekkomyślność*, ale bez intencji wyrządzenia szkody organizacji. Istnieje jednak inny rodzaj zagrożenia, w którym użytkownicy są zmotywowani do przeprowadzenia ataku i są oni znani jako **szkodliwi użytkownicy** (szkodnicy), co omówimy w następnej kolejności.

Szkodliwy użytkownik

Najpierw spróbujmy zrozumieć, jakie rodzaje motywacji mogą spowodować, że użytkownik zmieni się w osobę będącą zagrożeniem:

1. uzyskanie oferty od zewnętrznych napastników na dostarczanie danych lub wykonywanie działań w zamian za pieniądze,
2. brak regulacji dotyczących cyberbezpieczeństwa i sankcji korporacyjnych,
3. brak kontroli,
4. koncentracja władzy,
5. złe zarządzanie,
6. słaby wynik oceny,
7. brak akceptacji i niezgoda na politykę firmy, jej strategie i współpracowników,
8. zwolnienie z pracy.

Rysunek 4.2 pokazuje różnicę w motywacji między złośliwym a lekkomyślnym użytkownikiem.

Rysunek 4.2. Rodzaje zagrożeń wewnętrznych

Jak widać na rysunku 4.2, zrozumienie tych motywacji pomoże Ci współpracować z kierownictwem w celu stworzenia strategii zapobiegających przekształcaniu się użytkowników w *wewnętrznych szkodników*. Dodatkowo wdrożenie strategii szkoleniowej i edukacyjnej będzie Twoim najlepszym sprzymierzeńcem w zapobieganiu błędom *popełnianym* przez *lekkomyślnych użytkowników*.

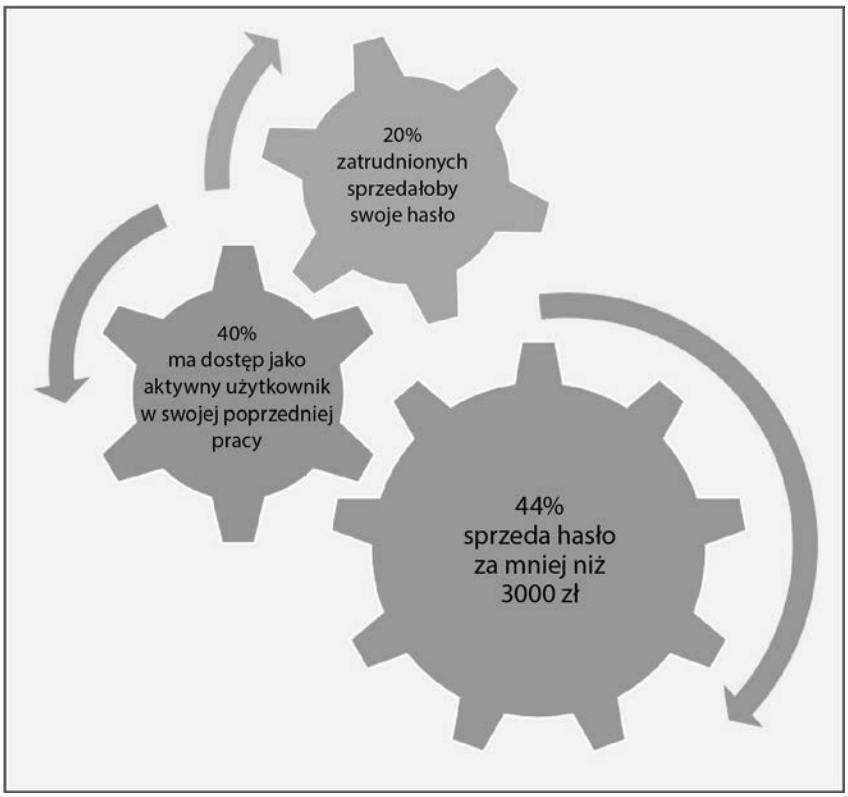
Jak rozpoznać wewnętrznego szkodnika?

Oto lista *zachowań lub działań*, które mogą pomóc w identyfikacji szkodnika, zanim będzie za późno:

- pobranie dużej ilości danych (lub zrzut bazy danych),
- dostęp do systemów i informacji po godzinach pracy,
- eskalacja uprawnień,
- pobieranie informacji wrażliwych bez potrzeby biznesowej,
- tworzenie kont bez przestrzegania ustalonych procesów i kontroli,
- zwiększone przesyłanie danych na nieznane adresy zewnętrzne,
- powtarzające się żądania dostępu do wrażliwych systemów lub danych,
- nieuzasadnione lub częstsze niż zwykle występowanie o wnioski o wyjątki od danej zasady cyberbezpieczeństwa,
- wzrost wykorzystania zewnętrznych urządzeń pamięci masowej,
- pojawienie się nietypowych załączników w wiadomościach e-mail (wykrywanie według rozmiaru lub liczby plików)
- dowody lub oznaki wykorzystania narzędzi hakerskich,
- nieoczekiwana lub zwiększona częstotliwość podłączania urządzeń osobistych do sieci organizacji.

Jeśli uważasz, że nie będziesz miał do czynienia z wewnętrznym szkodnikiem, to zastanów się dwa razy. Z badania opublikowanego przez *inc.com* wynika, że prawie jeden na pięciu pracowników byłby skłonny sprzedać swoje hasło zewnętrznemu napastnikowi, i jak widać na rysunku 4.3, zrobi to za bardzo niską cenę.

Teraz, gdy widzisz, że jest to poważne zagrożenie, rozważmy kilka działań, które możesz wykonać, aby zmniejszyć prawdopodobieństwo i wpływ ryzyka związanego z takimi złośliwymi działaniami.



Rysunek 4.3. Wartość hasła korporacyjnego

Ochrona infrastruktury przed wewnętrznymi szkodnikami

Przyjrzyjmy się narzędziom, systemom i strategiom, które można wdrożyć w celu ochrony przed tym zagrożeniem.

Podział obowiązków

Jest to jedno z podstawowych działań, które *musisz* wykonać w ramach strategii bezpieczeństwa defensywnego. Opiera się na dwóch głównych działaniach (lub czynnościach):

- Pierwsze z nich dotyczy identyfikacji *najbardziej krytycznych zadań w infrastrukturze*. W tym miejscu należy zadać sobie pytanie: jakie są ludzkie działania, które (jeśli zostaną wykonane przez osobę złośliwą) spowodują *znaczny wpływ na systemy i dane*?
- Drugie polega na tym, by po zidentyfikowaniu tych działań zdefiniować mechanizmy kontrolne dające gwarancję, *że pojedyncza osoba nie będzie mogła wykonać tych zadań*.

Rozdzielenie obowiązków jest istotne

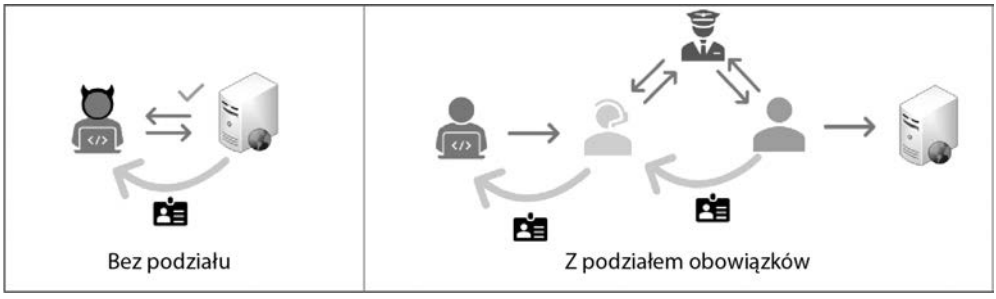
Naukowcy zgadzają się, że największemu włamaniu do platformy mediów społecznościowych (włamaniu na Twittera w 2020 roku) można było zapobiec, gdyby był wprowadzony podział obowiązków.

Teraz spójrzmy na kilka przykładów, jak można wykorzystać i wdrożyć tę strategię.

Przykład podziału obowiązków

Jak widać na rysunku 4.2, zezwolenie administratorowi systemu na tworzenie uprzywilejowanych kont daje wewnętrznemu szkodnikowi możliwość przeprowadzenia niebezpiecznego ataku. Zamiast tego *należy* zaangażować pewne systemy i procesy, aby opracować *przepływ stosowany podczas tworzenia nowych użytkowników*, który wymaga zaangażowania kilku grup, co *zmniejsza prawdopodobieństwo ataku*.

Na rysunku 4.4 widać, że administrator systemu będzie musiał utworzyć zgłoszenie z żądaniem. Następnie żądanie jest wysyłane do zatwierdzenia, a po zatwierdzeniu zostanie wysłane do zespołu **Zarządzania Tożsamością i Dostępem** (ang. *Identity and Access Management*, **IAM**) w celu jego wykonania.



Rysunek 4.4. Podział obowiązków

Zauważ, że filtrowanie całej komunikacji przez helpdesk (w obu kierunkach) jest doskonałym sposobem na uniemożliwienie bezpośredniej komunikacji między złośliwym szkodnikiem a osobą odpowiedzialną za tworzenie kont, co znacznie zwiększa bezpieczeństwo tej metody.

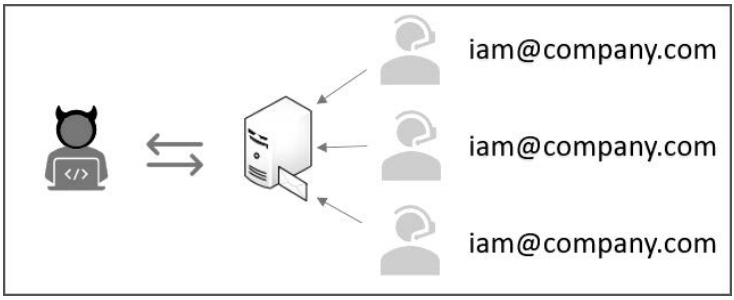
Inny świetny przykład jest związany z kopiami zapasowymi, ponieważ użytkownik działający na szkodę firmy może wiedzieć, że usunięcie niektórych plików nie spowoduje żadnej szkody. Dzieje się tak dlatego, że mogą one zostać odzyskane z kopii zapasowych. W takich przypadkach to kopie zapasowe będą stanowić cel działania, aby zapobiec wszelkim próbom odtworzenia.

Aby zapobiec takiemu niebezpiecznemu scenariuszowi, można użyć podziału obowiązków, aby zagwarantować, że pojedynczy użytkownik nie będzie mógł usunąć kopii zapasowych, ponieważ istnieje określony przepływ (*wspierany przez politykę, procesy i egzekwowany przez system*) niezbędny do wykonania tej czynności.

Korzystanie ze skrzynek pocztowych

Kiedy mamy wdrożony podział obowiązków, szkodnik może próbować namówić lub przekonać inną osobę do pomocy w ataku przez wykonanie pewnych działań.

Aby tego uniknąć, do komunikacji z wysoce wrażliwymi zespołami, takimi jak zespół zatwierdzający żądania, helpdesk czy zespół IAM, możesz użyć **skrzynek pocztowych** (rysunek 4.5). To pozwala uniknąć ujawnienia tożsamości osób zajmujących te stanowiska, co zapobiega wszelkim bezpośrednim próbom ich namawiania lub szantażowania.



Rysunek 4.5. Używanie skrzynek pocztowych

Jak widać na rysunku 4.5, nawet jeśli istnieje bezpośredni kanał komunikacji z zespołami wsparcia (co jest normalne w małych firmach), osoby chcące działać na szkodę firmy nie będą w stanie zidentyfikować, kto jest osobą pracującą nad danym żądaniem.

Rotacja stanowisk pracy

Kolejną dobrą praktyką jest rotacja stanowisk dla pracowników wsparcia IT. Polega ona na stworzeniu reguły, która wymaga od pracowników IT zmiany ról od czasu do czasu. Wymaga to wdrożenia *programów szkoleń wewnętrznych, mentoringu i programów rozwoju umiejętności*, co *jest również motywujące* dla pracowników IT.

Ta prosta zasada daje kilka dodatkowych korzyści, jeśli chodzi o bezpieczeństwo defensywne, między innymi:

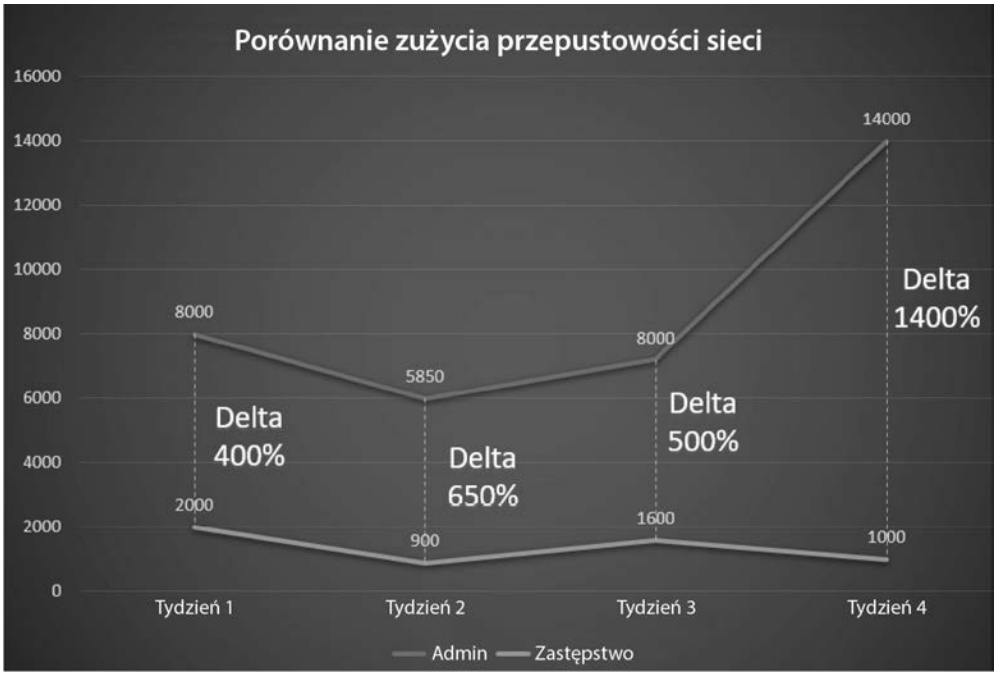
- *Zmniejsza ryzyko przestojów:* Musisz mieć przeszkolonych ludzi, aby uniknąć ryzyka wynikającego z braku umiejętności dotyczących danej technologii. Na przykład: *„Och, będziemy musieli poczekać do następnego tygodnia, ponieważ Maria jest nieobecna, a ona jest jedyną osobą, która zna się na DB2”.*
- *Zmniejsza ryzyko oszustwa:* Kiedy osoba pozostaje „przykuta” na stałe do tej samej roli, może być w stanie ukryć ślady własnych działań (w przypadku jakiejkolwiek nielegalnej działalności). W przypadku ciągłej rotacji istnieje uzasadnione prawdopodobieństwo, że nowa osoba odkryje jakieś anomalie, które mogą ujawnić tę nielegalną działalność.

- *Zmniejsza wpływ ataku:* Poprzez zmniejszenie czasu, przez który dana osoba wykonuje tę samą rolę, zmniejszy się również czas, jaki będzie ona miała na wykonanie nielegalnego działania; dlatego wpływ takiego ataku (na Twoje dane i systemy) będzie mniejszy.

Obowiązkowe urlopy

Działają na tej samej zasadzie co rotacja stanowisk i służą jako sposób na *wykrywanie i zapobieganie oszustwom*. Działa to bardzo prosto: po pierwsze, wiadomo, że osoby mające dostęp do informacji poufnych, popełniające oszustwa, mają tendencję do paranoi przed byciem odkrytym. Dlatego unikają urlopów, aby nie dopuścić do wykrycia ich ukrytej działalności.

Dodatkowo łatwo będzie zidentyfikować deltę w działaniach pomiędzy nowym adminem a poprzednim (będącym teraz na urlopie), która może prowadzić do odkrycia niepożądanej działalności (rysunek 4.6).



Rysunek 4.6. Wykrywanie złośliwej aktywności przez korelację aktywności w sieci z obowiązkowym urlopem

Rysunek 4.6 przedstawia scenariusz, w którym uprzywilejowany użytkownik pobierał ponad 4 GB danych tygodniowo (co było uznawane za *normę*) aż do momentu, gdy został zmuszony do wzięcia urlopu i wykorzystanie pasma spadło o ponad 400%. Potwierdziło to, że użytkownik ten wykorzystywał pasmo korporacyjne w sposób nieautoryzowany.

Analiza i korelacja logów

Nieprzetworzone dane mogą nie spowodować żadnych alarmów, ale jak pokazano w poprzednim przykładzie, gdy odpowiednio je skorelować, mogą pokazać bardzo interesujące informacje.

Logi są kopalnią złota; trzeba jednak kopać stosunkowo głęboko, aby odkryć przydatne informacje. Jednym z najbardziej podstawowych sposobów zbierania tych informacji jest uwzględnienie korelacji między danymi użytkownika i danymi z systemów w celu wykrycia wartości odstających.

Dodatkowo, wykonując analizę, należy określić, które ze zdarzeń są powyżej lub poniżej średniej, i to właśnie im należy poświęcić uwagę.

Istnieje również wiele systemów, które automatyzują analizę logów. Zamiast podawać kilka marek i nazw, zamierzam pokazać typ narzędzi, które pomogą Ci to osiągnąć, abyś sam mógł poszukać i znaleźć rozwiązanie, które najlepiej pasuje do Twojej organizacji. Dodatkowo sugerowałbym, abyś poszukał alternatyw, które wykorzystują algorytmy uczenia maszynowego w celu poprawy wykrywalności i zmniejszenia liczby fałszywie pozytywnych przypadków.

Są to następujące systemy:

- systemy analizy behawioralnej (ang. *behavioral analytics system*),
- systemy inteligentnego wykrywania zagrożeń (ang. *threat intelligence*),
- systemy wykrywania anomalii,
- alerty predykcyjne (ang. *predictive alerts*).

Chcę jednak, abyście wiedzieli, że jeśli nie macie takich systemów, to nie jest to wystarczająca wymówka do marnowania Waszych cennych danych. Pamiętam bardzo ciekawy przypadek, kiedy analizując kilka logów, znaleźliśmy administratora systemu, który nielegalnie wykorzystywał zasoby korporacyjne do *„wydobywania" bitcoinów*.

Jak to znaleźliśmy?

Po prostu sprawdzając logi, odkryliśmy, że kilka niedziałających „na produkcji" systemów i serwerów było włączonych od 22:00 do 4:00 rano w jedynym celu: wydobywania bitcoinów. Dodatkowo logi te zawierały poziom szczegółowości wymagany do *zidentyfikowania* zaangażowanych *użytkowników*, ale także wystarczające dowody, by móc sprawę zgłosić organom ścigania i *wyegzekwować związane z tym kary i sankcje*.

Alerty

Innym świetnym sposobem na zidentyfikowanie złośliwego szkodnika jest skonfigurowanie opcji monitorowania działalności z wyzwalaniem alertów, gdy użytkownik wyłącza system cyberbezpieczeństwa.

Jest to szczególnie przydatne w tych firmach, które dają *prawa administracyjne wszystkim pracownikom*. Pracownicy sądzą, że mogą ominąć mechanizmy bezpieczeństwa (takie jak wyłączenie oprogramowania antywirusowego lub ściany ogniowej); ale nie wiedzą, że jesteś krok przed nimi.

> **Ważna uwaga**
>
> Istnieje kilka sposobów, aby uniemożliwić wyłączenie niektórych zabezpieczeń przez użytkownika; jednak nie wszystkie firmy lub działy IT mają narzędzia, wiedzę lub są zainteresowane tym, aby to zrobić. Dlatego ważne jest, aby dowiedzieć się, jak radzić sobie w takim przypadku.

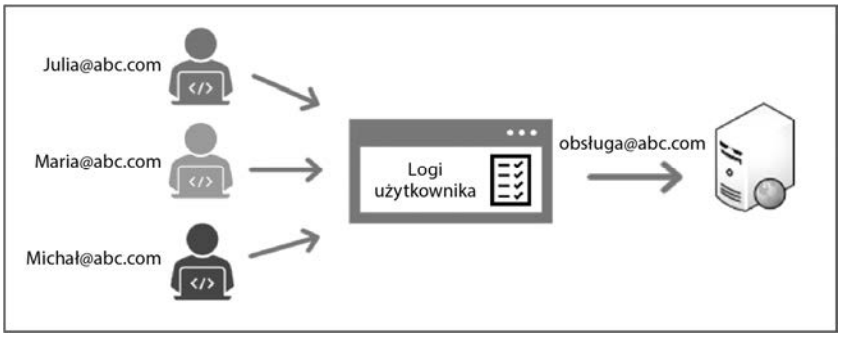
Przyjrzyjmy się teraz jednemu przykładowi bardzo powszechnej praktyki w działach IT, która jest naprawdę złą praktyką z punktu widzenia bezpieczeństwa.

Wspólne dane uwierzytelniające

Domyślnie najlepsza praktyka mówi, że wspólne *dane uwierzytelniające dla kilku osób NIE powinny być dozwolone w Twojej infrastrukturze*. W przypadku gdy jednak są, musisz skonfigurować dodatkowe opcje kontroli, takie jak uwierzytelnienie wieloczynnikowe (ang. *Multifactor Authentication*, **MFA**), kontrola dostępu oparta na rolach (ang. *Role-Based Access Control*, **RBAC**) oraz zarządzanie uprzywilejowanym dostępem (ang. *Privileged Access Management*, **PAM**).

PAM działa poprzez *blokowanie współdzielonych poświadczeń* w repozytorium, do którego dostęp mają tylko uwierzytelnione konta pracowników (ze względu na możliwość ustalenia odpowiedzialności, (ang. *accountability*)). Gdy dane poświadczenie jest używane przez administratora systemu, poświadczenie dla następnego pracownika jest *resetowane*. Chociaż PAM rozwiązuje problem kont współdzielonych, jego wdrożenie jest bardzo kosztowne.

Diagram na rysunku 4.7 przedstawia działanie systemu PAM i pokazuje, że każdy użytkownik loguje się do scentralizowanego systemu (aby wiedzieć, kto dokładnie jest odpowiedzialny za działania na koncie), a następnie stamtąd korzysta ze współdzielonego konta na serwerze.



Rysunek 4.7. Przykład systemu PAM

Audyty

Temat ten został już szczegółowo omówiony w rozdziale 3., „Zasady, procedury, zgodność i audyty"; chciałbym jednak podkreślić, że audyty są *jednym z najskuteczniejszych sposobów wykrywania złośliwych użytkowników działających wewnątrz*, więc upewnij się, że Twoja infrastruktura podlega regularnym audytom (wewnętrznym lub zewnętrznym).

Stosowanie zasad w cyberbezpieczeństwie

Jak to zostało omówione w rozdziale 3, „Zasady, procedury, zgodność i audyty", zasady muszą być dobrze zdefiniowane i przekazane. Dodatkowo *muszą określać powiązane z nimi sankcje — w przypadku ich naruszenia*. Sankcje są doskonałym mechanizmem odstraszającym wewnętrznych, złośliwych użytkowników, dlatego ważne jest upewnienie się, że wszyscy pracownicy je znają.

Mówiliśmy już o dwóch typach zagrożeń z wewnątrz: *lekkomyślnych* i *złośliwych* użytkownikach. Istnieje jednak jeszcze jeden wektor ataku. W tym ataku osoba z *zewnątrz wykorzystuje siłę wpływu i manipulacji psychologicznej, aby przekonać lub namówić pracownika do wykonania zestawu działań mających na celu zakłócenie pracy systemów lub zebranie/modyfikację wrażliwych danych*. Technika ta znana jest jako **inżynieria społeczna** (ang. *social engineering*) — omówimy ją w następnej części.

Doskonalenie sztuki inżynierii społecznej

Inżynieria społeczna jest jednym z najbardziej fascynujących tematów w dziedzinie bezpieczeństwa. Wielu ekspertów definiuje inżynierię społeczną jako *sztukę*: wymaga wielu umiejętności społecznych, umożliwiając napastnikom *uzyskanie dostępu* do umysłu ofiary w celu zebrania informacji osobistych lub nawet przekonania jej do wykonania pewnych działań, które przyniosą korzyść napastnikom.

To trochę jak włamanie się do ludzkiego mózgu w celu odczytania danych użytkownika lub wprowadzenia tam instrukcji, które ofiara ma wykonać.

Jak wspomniałem wcześniej, jest to bardzo ekscytujący i ważny temat, więc postaram się go podsumować, na ile dam radę.

> **Ważna uwaga**
>
> Jako profesjonalista w dziedzinie bezpieczeństwa *musisz* opanować ten temat, ponieważ im lepiej zrozumiesz, jak to działa, tym lepiej będziesz mógł zaplanować obronę.

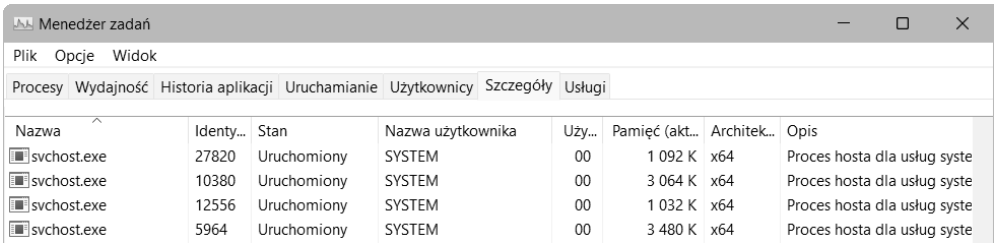
Teraz przyjrzyjmy się atakom, które mają na celu oszukanie użytkownika. Pamiętaj jednak, że chociaż nie wszyscy autorzy zgadzają się co do klasyfikacji tych ataków jako ataków z zakresu inżynierii społecznej, prawda jest taka, że w ich przypadku mamy te same koncepcje i strategie, co w przypadku ataków inżynierii społecznej.

Przebieg ataku w inżynierii społecznej

Istnieje wiele technik, które napastnicy mogą wykorzystać do przeprowadzenia ataku socjotechnicznego, ale aby zwiększyć skuteczność ataku, należy je odpowiednio zaaranżować (rysunek 4.9):

1. *Zbieranie informacji:* Po pierwsze, atakujący zbiera jak najwięcej informacji o osobie lub organizacji będącej celem ataku. Im więcej atakujący wie o organizacji, tym większe ma szanse na sukces. Na przykład atakujący będzie bardzo zainteresowany poznaniem struktury organizacyjnej, procesów i procedur jako danych wejściowych do kolejnych kroków.
2. *Budowanie zaufania:* W tym przypadku atakujący wykorzysta zebrane dane oraz kombinację technik społecznych, aby zdobyć zaufanie. W bardziej skomplikowanych atakach atakujący będzie musiał zdobyć zaufanie wielu osób, aby ominąć dodatkowe warstwy zabezpieczeń przed dotarciem do prawdziwego celu lub ofiary.

   Jak widać na poniższym zrzucie ekranu, napastnik może również wykorzystać pewną wiedzę techniczną, aby zdobyć zaufanie ofiary. Na przykład atakujący może podszyć się pod informatyka, mówiąc użytkownikowi, że jego komputer został zgłoszony jako zainfekowany wirusem, i poprosić użytkownika o sprawdzenie, czy proces Windows `svchost` jest widoczny w Menedżerze zadań (Oczywiście atakujący wie, że taki proces *zawsze będzie* istniał, a więc gdy użytkownik go znajdzie (rysunek 4.8), będzie to uzasadnienie kontaktu ze strony atakującego, zdobycie pełnego zaufania i otwarcie drzwi do kolejnego kroku).



Rysunek 4.8. Proces SVCHOST uruchomiony w systemie Windows

3. *Wywieranie wpływu na ofiarę:* Zdobywszy zaufanie użytkownika, atakujący może zmanipulować ofiarę, aby albo podała pewne informacje uwierzytelniające (takie jak nazwy użytkownika i hasła), albo wykonała pewne działania (takie jak zresetowanie hasła, otwarcie terminala, otwarcie strony internetowej).
4. *Przeprowadzenie ataku:* W tym momencie atakujący może mieć już aktualne dane uwierzytelniające użytkownika, pełną zdalną kontrolę nad komputerem i wiele innych możliwości działania, których może użyć do swojego ostatecznego ataku (takiego jak usunięcie, modyfikacja lub skopiowanie danych uwierzytelniających, uzyskanie dostępu do danego systemu i inne).
5. *Zacieranie śladów:* Po zakończeniu ataku atakujący może chcieć *zatrzeć ślady*, aby uniknąć wykrycia i ścigania, ale także może chcieć zachować dostęp do systemów i danych przez dłuższy czas.

Rysunek 4.9. Cykl życia inżynierii społecznej

Teraz przyjrzyjmy się na szybko niektórym technikom (*socjotechniki*) wykorzystywanym przez napastników do skutecznego przeprowadzenia ataku w inżynierii społecznej.

Socjotechniki

Oto kilka technik, które napastnik może wykorzystać do przeprowadzenia ataku socjotechnicznego:

- **Podszywanie się:** Jedna z najczęstszych technik stosowanych przez napastników: przedstawianie się jako ktoś inny; na przykład jako ktoś mający autorytet, władzę lub reprezentujący renomowaną firmę lub grupę.

  Zazwyczaj jest ona wykorzystywana do zdobycia zaufania ofiary w celu uzyskania informacji lub skłonienia jej do wykonania określonego działania.

  Najczęściej dochodzi do podszywania się pod osobę z branży IT, przedstawiciela rządu, pracownika banku lub renomowanej firmy.

- **Zagrożenie:** Atakujący mogą wykorzystać strach, aby przekonać użytkownika do wykonania danej akcji. Na przykład wyobraź sobie następującą wiadomość e-mail:

  „Twój komputer jest zainfekowany. Kliknij tutaj, aby przeskanować, zanim komputer zostanie pozbawiony możliwości pracy w sieci firmowej, zablokowany i wpisany na czarną listę”.

- **Wzajemność:** Napastnik zrobi coś, co wydaje się korzystne dla ofiary. Dzięki temu ofiara będzie skłonna spełnić prośbę napastnika (o udzielenie pewnych informacji lub wykonanie jakiejś czynności), aby odwdzięczyć się za to.

- **Wykorzystanie chciwości użytkowników:** Ten typ wykorzystuje podstawową ludzką słabość, na przykład:

  „Wygrałeś wakacje — rejs na jachcie! Kliknij tutaj, aby odebrać swoją nagrodę!”.

- **Wykorzystanie ciekawości użytkownika:** W tym scenariuszu atakujący może upuścić kilka złośliwych dysków USB w pobliżu celu, mając nadzieję, że pracownik podniesie je i podłączy. Atakujący może umieścić na USB etykietę, taką jak *Moje fotki* lub *Poufne*, aby sprowokować zaciekawienie, a tym samym wpłynąć na skuteczność ataku.

  Zabawny fakt: większość źródeł uważa, że *Stuxnet* (wirus, który uszkodził irański program nuklearny) został rozprzestrzeniony przez zainfekowane dyski USB.
- **Dowód społecznej słuszności:** Inną taktyką jest wykorzystanie dowodu społecznej słuszności do „wrobienia" ofiary. Na przykład napastnik może powiedzieć, że *„To już zostało sprawdzone i przetestowane przez innych adminów"*, aby uśpić Twoją czujność i dać Ci poczucie pewności, że żądanie jest bezpieczne, ponieważ zostało już wykonane przez innych.
- **Uzasadnienie z wykorzystaniem technicznych szczegółów:** Atakujący mogą używać żargonu technicznego, aby zmylić ofiarę. Zwykle jest stosowane w połączeniu z innymi technikami, takimi jak wywołanie pośpiechu i poczucia zagrożenia. Rysunek 4.8 jest doskonałym przykładem zastosowania tej techniki.
- **Władza:** Atakujący może podszywać się pod osobę sprawującą władzę, aby zmusić Cię do spełnienia danego żądania. W niektórych przypadkach atakujący niekoniecznie będzie podszywać się pod daną osobę, ale będzie twierdzić, że działa w imieniu osoby upoważnionej. Na przykład: *„Jeśli nie zainstalujesz tego oprogramowania, sprawa zostanie skierowana do pana Krzysztofa"*. Zauważ, że w tym przykładzie osoba decyzyjna została nazwana po imieniu (pan Krzysztof) zamiast po tytule (dyrektor), co też wchodzi w skład technik stosowanych przez atakujących.
- **Utrata okazji:** Tutaj atakujący sprawi, że ofiara będzie myślała, że jeśli akcja nie zostanie wykonana szybko, użytkownik (ofiara) może stracić potencjalną nagrodę. Na przykład wyobraź sobie taki e-mail z (rzekomo) działu IT:

  „Mamy 20 nowych MacBooków dostępnych w ramach wymiany starych komputerów. Kliknij tutaj, aby wypełnić formularz. Pamiętaj, że jest ich tylko 20 i otrzyma je pierwszych 20 osób, które wypełnią formularz (kto pierwszy, ten lepszy)."
- **Wywołanie pośpiechu:** Jest klasycznym oszustwem, może wyglądać na przykład tak:

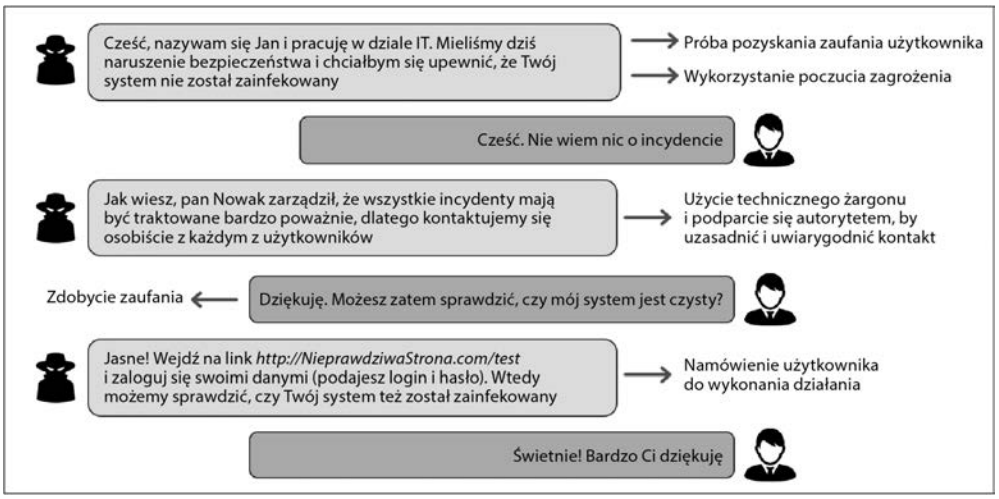
  „Jeśli nie zresetujesz swojego hasła w ciągu najbliższych 30 minut, Twój komputer zostanie zablokowany w sieci".

  „Twój komputer jest zainfekowany, kliknij TU natychmiast, zanim Twoje informacje zostaną skradzione".

Rysunek 4.10 opisuje cały przebieg ataku socjotechnicznego oraz taktykę stosowaną przez napastników.

Wiesz już teraz, jak przebiega typowy atak oraz jakie techniki stosują napastnicy w celu zdobycia zaufania użytkownika i przeprowadzenia ataków.

Teraz czas, abyśmy przyjrzeli się najczęstszym typom ataków socjotechnicznych, w których te techniki są wykorzystywane.



Rysunek 4.10. Przykład ataku socjotechnicznego

Rodzaje ataków wykorzystujących inżynierię społeczną

Tutaj zamierzam podsumować najczęstsze ataki, które są oparte na technikach inżynierii społecznej.

Phishing

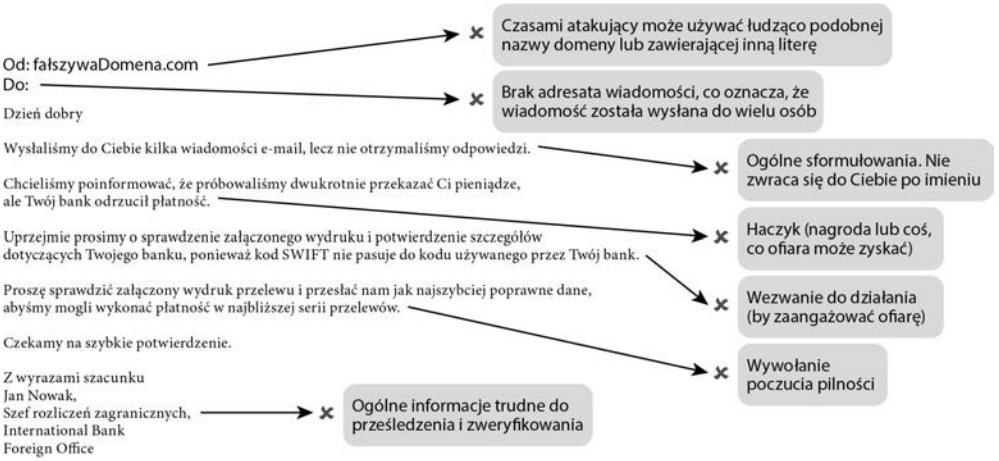
Jak już zapewne wiesz, koncepcja jest bardzo prosta. Napastnik wysyła fałszywy e-mail, próbując podszyć się pod renomowaną osobę lub firmę. Aby zwiększyć swoje szanse na sukces, atakujący najpierw stara się przekonać ofiarę, że e-mail jest legalny (używając logo firmy albo podszywając się pod konto e-mail lub domenę), a następnie prosi użytkownika o podjęcie jakiegoś działania, zwykle o przejście do linku lub otwarcie załączonego pliku PDF.

Zobaczmy kilka przykładów.

Każdy marzy o darmowych pieniądzach i napastnicy o tym wiedzą. Aby wykorzystać to pragnienie, napastnik podszywa się pod firmę, która chce przelać pieniądze na Twoje konto, ale twierdzi, że nie może tego zrobić, ponieważ numer jest nieprawidłowy. Aby *zdobyć* te pieniądze, wystarczy otworzyć *nieszkodliwy plik* PDF, który oczywiście będzie zawierał różnego rodzaju wirusy, od programu rejestrującego naciśnięcia klawiszy w klawiaturze (ang. *keylogger*) po śmiertelnie niebezpieczne oprogramowanie wymuszające okup (ang. *ransomware*).

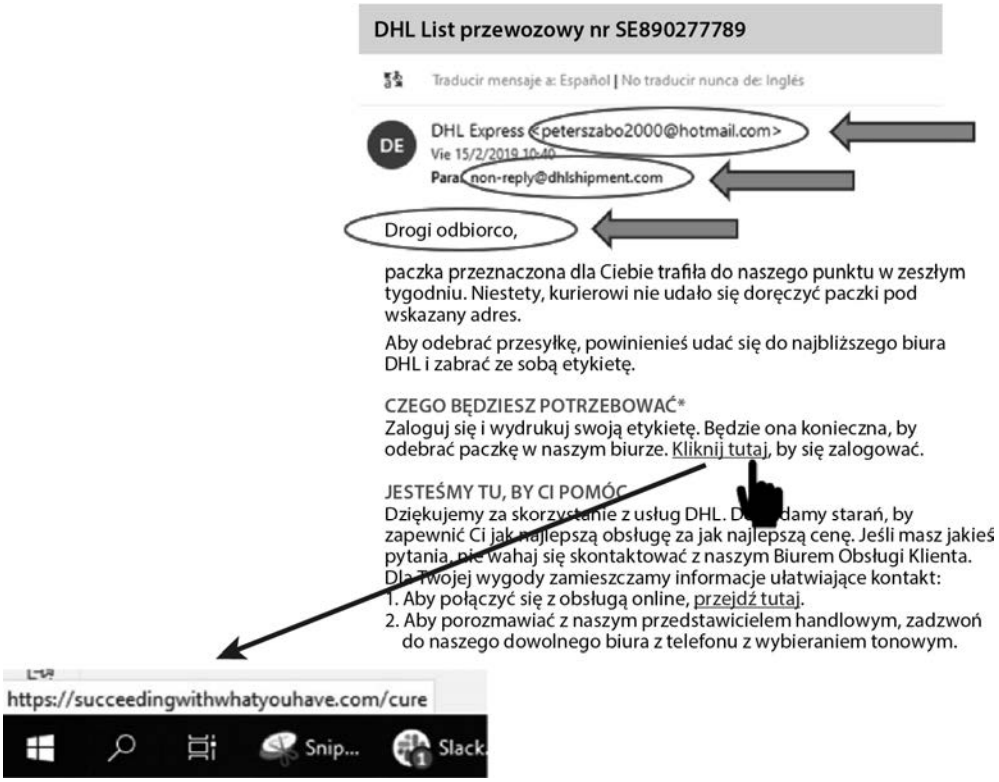
Na rysunku 4.11 wyróżniliśmy wspólne specyficzne cechy, które pomogą Ci zidentyfikować tego typu ataki.

W dzisiejszych czasach każdy robi zakupy online, a prawdopodobieństwo, że spodziewasz się przesyłki, jest bardzo wysokie, więc napastnicy wykorzystują to i masowo wysyłają tego typu wiadomości wyłudzające dane (ang. *phishing*), mając nadzieję, że każdy, kto naprawdę spodziewa się przesyłki, wpadnie w pułapkę.



Rysunek 4.11. Przykład wiadomości wyłudzającej dane typu „darmowe pieniądze"

Na rysunku 4.12 pokazano, jak atakujący podszywa się pod znaną firmę kurierską, ale nadal istnieje kilka elementów, których możesz użyć, aby upewnić się, że jest to e-mail phishingowy.



Rysunek 4.12. Przykład phishingu dotyczącego dostawy paczek

Pierwszym elementem (co może wydawać się bardzo oczywiste) jest to, że adres pochodzi z serwisu Hotmail.

Drugim jest to, że Twój e-mail nie jest wymieniony w polu *Do*.

Trzecim jest użycie ogólnego pozdrowienia. Najważniejszy jest jednak ten dotyczący linku.

Możesz najechać myszką na link, aby zobaczyć, gdzie on wskazuje. W tym przykładzie jest w sposób oczywisty widać, że link nie wskazuje na prawdziwą domenę DHL.

Jak wiadomo, wektory ataku zwykle ewoluują w celu obejścia mechanizmów obronnych, dlatego przyjrzyjmy się niektórym wariantom inżynierii społecznej, które wyewoluowały z ataków phishingowych.

SMishing

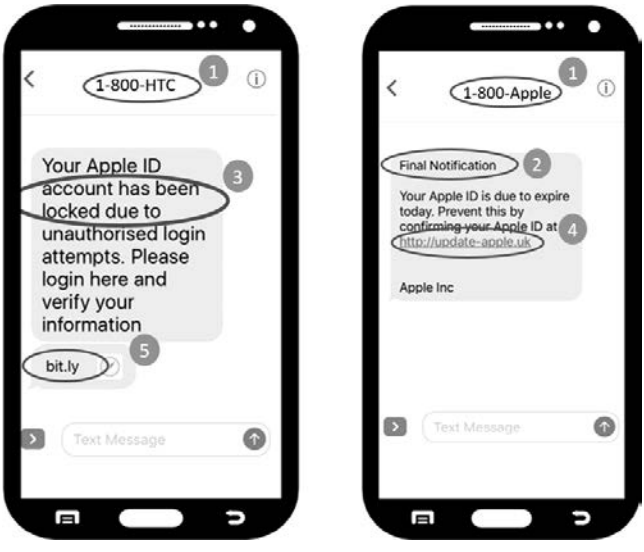
Atak ten posiada te same cechy co atak phishingowy, z tą różnicą, że jest on rozpowszechniany za pomocą **wiadomości SMS** (ang. *Short Message Service*).

Choć może to brzmieć jak niewielka zmiana, jest to jeden z najgroźniejszych wektorów ataku, ponieważ użytkownicy nie kojarzą starych SMS-ów z wirusami, więc mają tendencję do *ufania* tym wiadomościom i wpadania w pułapkę. Jeśli Twoja firma stosuje politykę **Bring-Your-Own-Device** (**BYOD**), to musisz wykonać następujące czynności:

Edukuj użytkowników na temat tego typu zagrożeń.

Wyłączaj funkcje hiperłącza w SMS-ach.

Spójrzmy teraz na rysunek 4.13, aby pokazać, jak łatwo dostrzec te zagrożenia.



Rysunek 4.13. Przykład SMishingu

1. W większości przypadków atakujący użyją losowego numeru, który jest łatwy do zauważenia i zablokowania. Jednak w bardziej rozbudowanych atakach atakujący może użyć niektórych narzędzi (takich jak **BurnerApp** i **SpoofCard**), aby zmanipulować identyfikator dzwoniącego i podszyć się pod bardziej wiarygodny numer.
2. Ponownie kolejnym wspólnym czynnikiem jest wywołanie *wrażenia pilności* wykonania żądanej czynności.
3. Innym wspólnym czynnikiem jest *wykorzystanie lęku*, aby użytkownik uwierzył, że coś złego się stanie, jeśli żądana akcja nie zostanie wykonana.
4. Jak wspomniano wcześniej, tutaj głównym wektorem ataku *jest wysłanie ofiary na złośliwą stronę internetową*, która albo wykradnie dane uwierzytelniające, albo zainfekuje urządzenie złośliwym oprogramowaniem, albo jedno i drugie.
5. W jednym z możliwych scenariuszy atakujący zakupi domenę, która wygląda jak oryginał; jednak w innych sytuacjach atakujący użyje *skracania linków* (ang. *link shortener*), aby zamaskować nazwę strony.

Spear phishing

Jest to atak ukierunkowany, w którym atakujący rozpoczyna od przeprowadzenia dogłębnego badania ofiary i firmy. Następnie wykorzystuje całą tę wiedzę do stworzenia *spersonalizowanego ataku phishingowego*.

Zwykle ataki tego typu są wymierzone w cele o dużej wartości, takie jak menedżerowie, personel finansowy lub administratorzy systemów (ze względu na wartość ich poświadczeń administracyjnych).

Przeanalizujmy teraz prawdziwy przykład spear phishingu (przedstawiony na rysunku 4.14).

Rysunek 4.14. Przykład spear phishingu

Z poprzedzającego zrzutu ekranu możemy rozszyfrować, co następuje:

1. W większości przypadków atakujący *użyje bardzo podobnej domeny, aby oszukać swoją ofiarę*. Jak widać w tym przykładzie, w bardziej rozbudowanych atakach strona może wyglądać na legalną. Jednak jeśli przyjrzysz się dokładnie, zobaczysz, że nazwa firmy jest tylko poddomeną domeny atakującego.
2. Atakujący używa *chwytliwego tematu*, ale z wywołaniem wrażenia pilności (aby zapobiec wykryciu ataku).
3. E-mail będzie skierowany do konkretnej ofiary dzięki *użyciu prawdziwego nazwiska i tytułu* (w niektórych sytuacjach atakujący użyje nawet brzmiących znajomo pseudonimów, aby zmniejszyć podejrzenia).
4. Haczyk ma przyciągnąć uwagę ofiary i przekonać ją do otwarcia pliku z podejrzaną zawartością.
5. Wywoływane jest *wrażenie pilności*, które ma być dla użytkownika motywacją do jak najszybszego wykonania żądanej czynności (na przykład otwarcia załącznika) bez dalszej weryfikacji z kierownictwem lub innym pracownikiem, który mógłby zidentyfikować to jako potencjalny atak.
6. Na koniec pozornie *niewinny PDF* będzie furtką użytą przez atakującego do ostatecznego przeprowadzenia ataku (na przykład zainstalowania określonego oprogramowania wymuszającego okup, otwarcia tylnych drzwi lub zainstalowania aplikacji zapisującej naciśnięcia klawiszy klawiatury).

Vishing

Znany również jako telefoniczna prowokacja lub oszustwo telefoniczne, vishing jest rodzajem phishingu opartym na rozmowie telefonicznej atakującego z ofiarą. W rozmowie tej atakujący próbuje przekonać ofiarę do wykonania serii działań lub do nieumyślnego ujawnienia pewnego rodzaju poufnych danych.

Jest to jeden z najbardziej złożonych ataków z punktu widzenia atakującego, ponieważ wymaga od niego opanowania większości koncepcji inżynierii społecznej, które wcześniej omówiliśmy.

Jednak atakujący może również rozszerzyć niektóre z tych technik, aby ofiara mu uległa. Na przykład napastnik może zadzwonić do działu pomocy technicznej i poprosić o zresetowanie hasła i podanie nowego hasła przez telefon. Jeśli ten odmówi, napastnik może mu zagrozić, że właśnie kończy uzgodnienia potrzebne do sfinalizowania wielomilionowej transakcji, a jeśli hasło nie zostanie przekazane przez telefon, to umowa nie zostanie podpisana, a pracownik zostanie pociągnięty do odpowiedzialności. Ta prosta sztuczka dowodzi, dlaczego ten atak jest preferowanym mechanizmem przez doświadczonych inżynierów społecznych.

> **Phishing w liczbach**
>
> Phishing to najczęstszy rodzaj inżynierii społecznej. *Raport Verizon's Data Breach Investigations Report 2019* wykazał, że ponad 30% potwierdzonych naruszeń danych było związanych z atakami phishingowymi. *Globalne straty z tytułu ataków vishingowych szacuje się na 46 mld dolarów*.

Jak widać, napastnicy są dobrzy w wymyślaniu nowych i sprytnych sposobów na rozszerzenie lub ewolucję swoich ataków, więc musisz być na bieżąco, aby odkryć każdą nową i potencjalną odmianę phishingu, która może mieć wpływ na Twoich pracowników.

Scareware

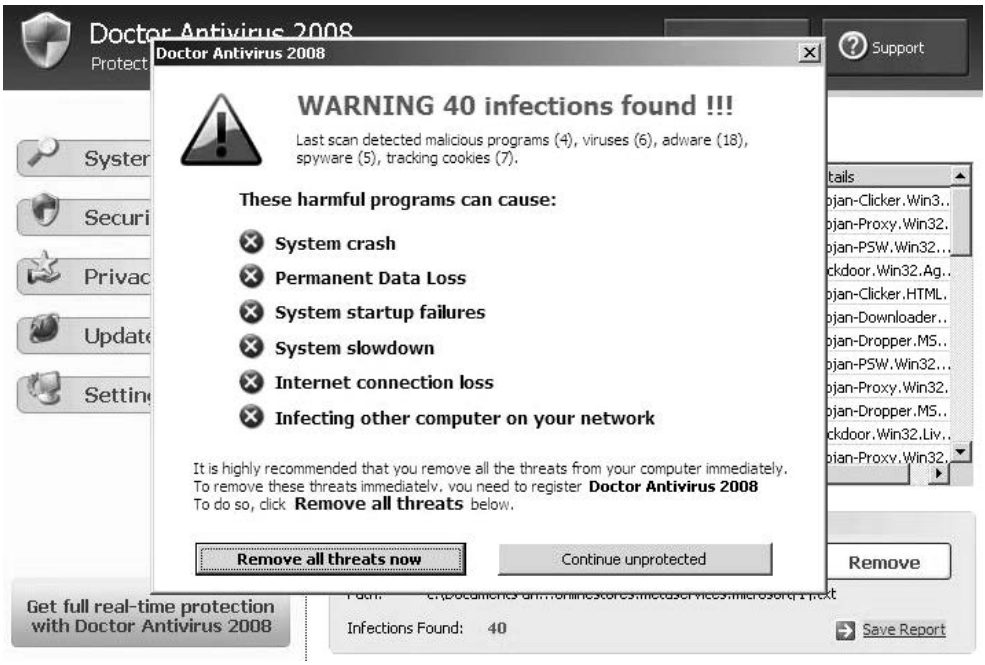
Scareware polega na wprowadzeniu ofiary w błąd, że komputer został zainfekowany wirusem, podczas gdy w rzeczywistości nie jest to prawda. Celem atakującego jest przekonanie ofiary do zainstalowania *oprogramowania antywirusowego* w celu usunięcia tych rzekomych wirusów, ale sugerowane *oprogramowanie antywirusowe* jest fałszywe.

Istnieją dwie główne odmiany tego ataku. Pierwsza z nich opiera się na *„darmowym programie antywirusowym"*, który w rzeczywistości jest wirusem *otwierającym drzwi* dla innych wirusów.

Inny wariant opiera się na sprzedaży oprogramowania *„antywirusowego"*, *„usuwającego" nawet te* wirusy, które nie istnieją (jest to więc w zasadzie oszustwo).

Zwykle pojawia się na kilka sposobów, na przykład:

- wyskakujące okienko ze złośliwej strony internetowej,
- dodatek do legalnej witryny (na przykład YouTube),
- skrypt, który zostanie wykonany przy starcie systemu Windows,
- fałszywy program antywirusowy (rysunek 4.15).



Rysunek 4.15. Przykład scareware

Ten typ zagrożeń był bardzo popularny jakiś czas temu (to znaczy za czasów Windows XP) i pomimo że dziś nie jest już tak często spotykany, nadal jest groźny.

W ostatnich latach wydaje się, że to zagrożenie przeniosło się na inną platformę i obecnie celem są użytkownicy smartfonów.

Jak widać na rysunku 4.16, atak jest bardzo podobny. Aby temu zapobiec, Sklep Play stale blokuje takie aplikacje; jednak one po prostu wciąż pojawiają się pod inną nazwą:

Rysunek 4.16. Scareware na smartfonach

Jednym ze sposobów zapobiegania temu zagrożeniu na korporacyjnych stacjach roboczych jest ograniczenie uprawnień do instalowania aplikacji firm trzecich (co jest tematem, który omówimy w podrozdziale „Obrona przed atakami socjotechnicznymi (łatanie warstwy 8)"). Ograniczenie to dotyczy również smartfonów i *musi* być egzekwowane, jeśli firma pozwala pracownikom na dostęp do swoich systemów za pomocą smartfonów (BYOD).

Doskonałym sposobem na osiągnięcie tego celu jest wykorzystanie systemu **Android Business** umożliwiającemu firmom stworzenie wirtualnego środowiska, w którym mogą zastosować większy nadzór w celu zabezpieczenia swoich danych i kontrolowania, kto ma dostęp do ich sieci, systemów i danych.

Więcej informacji można znaleźć na ich oficjalnej stronie internetowej *https://www.android.com/enterprise/*.

Dodatkowo świetnym pomysłem jest wdrożenie **oprogramowania blokującego reklamy** (ang. *ad blocker*). Można to zrobić na trzech poziomach:

- lokalnie na stacji roboczej,
- korzystając z firmowej ściany ogniowej,
- używając DNS.

> **Tworzenie własnej blokady reklam z użyciem DNS**
>
> W rozdziale 10., „Zabezpieczenia IoT w praktyce", pokażę Ci, jak możesz stworzyć *własną blokadę* reklam z użyciem DNS za mniej niż 50 dolarów, korzystając z *Raspberry Pi*.

Scareware był bardzo popularny w poprzednich wersjach systemu Windows, ale atak ten jest nadal istotny nie tylko jeśli chodzi o ochronę infrastruktury, ale także ze względu na dbałość o finanse poszczególnych osób.

Wabienie

W tej technice napastnik wykorzystuje ciekawość ofiary do wciągnięcia jej w pułapkę. Głównym celem atakującego jest skłonienie ofiary do wejścia na fałszywą stronę internetową, otwarcia zainfekowanego pliku, podania swoich danych uwierzytelniających na fałszywej stronie lub pobrania konia trojańskiego.

Kilka przykładów wabienia (ang. *baiting*) przedstawia poniższy schemat (rysunek 4.17).

Rysunek 4.17. Typowe przykłady przynęt

Istnieje również podtyp tego ataku, zwany **clickbaitem**, który skupia się głównie na przedstawianiu bardzo interesujących fałszywych wiadomości z nadzieją, że użytkownik na nie kliknie. W większości przypadków *clickbait* jest wykorzystywany do generowania ruchu lub zarabiania na reklamach, ale zdarzają się również przypadki wykorzystywania go do infekowania systemu złośliwym oprogramowaniem.

Zaglądanie przez ramię

Być może brzmi to bardzo prosto, ale wiele informacji wycieka przy użyciu tej prostej metody. Zasadniczo polega ona na zaglądaniu przez ramię, aby zebrać wrażliwe informacje, takie jak nazwy użytkowników, hasła i inne.

Jest zwykle wykorzystywana przez osoby z zewnątrz, więc posiadanie silnego systemu bezpieczeństwa fizycznego jest kluczem do zapobiegania tego typu atakom.

Innym zaleceniem dla pracowników, którzy stale podróżują, jest stosowanie *ekranów prywatności*, które uniemożliwiają innym czytanie z Twojego ekranu. Dodatkowo stosowanie *skarbców haseł* również zmniejsza to ryzyko, ponieważ hasła nie muszą być wpisywane, a zatem nie ma ryzyka ich ujawnienia.

Tailgating

Teraz, gdy wspomnieliśmy o bezpieczeństwie fizycznym, nadszedł czas, aby porozmawiać o **tailgatingu** (dosł. siedzenie na ogonie).

Jest to jedna z najczęstszych metod wykorzystywanych przez napastników do uzyskania fizycznego dostępu do zastrzeżonego miejsca.

W tym przypadku napastnik wykorzysta ludzką skłonność do bycia *uprzejmym lub przyjaznym* i przytrzymania otwartych drzwi kolejnej wchodzącej osobie.

Atakujący są bardzo kreatywni i niejednokrotnie będą mieli przy sobie duże pudło z pizzą lub kilka filiżanek pysznej kawy jako wymówkę, aby dostać się do budynku bez użycia identyfikatora — licząc na to, że „dobry człowiek" (czyli lekkomyślny użytkownik) przytrzyma dla nich otwarte drzwi.

Oprócz odpowiednich szkoleń dla użytkowników najlepszym sposobem na zwalczenie tego typu zagrożeń jest wykorzystanie dodatkowych mechanizmów weryfikacji, takich jak kamery do wykrywania osób postronnych. W rzeczywistości kamery mogą być wykorzystywane do wykrywania osób postronnych przy użyciu innych mechanizmów niż rozpoznawanie twarzy. Obejmują one wzorce ruchów, liczenie użytkowników (jeśli wchodzą dwie osoby, ale system odczytuje tylko jeden identyfikator), analizę (opartą na wykrywaniu nietypowych ścieżek) i inne.

Nurkowanie w śmietniku

Nurkowanie w śmietniku (ang. *dumpster diving*) to taktyka rozsławiona przez jednego z najbardziej znanych hakerów, Kevina Mitnicka, będącego zresztą pierwszym *hakerem*, który znalazł się na liście najbardziej poszukiwanych przez FBI (swą technikę bardzo dobrze wyjaśnił w swoich książkach).

Stwierdził, że był w stanie uzyskać wiele informacji, po prostu przetrząsając firmowe śmieci w poszukiwaniu nierozdrobnionych dokumentów zawierających poufne informacje. W niektórych przypadkach atakującemu może się udać znaleźć wrażliwe informacje, takie jak dane uwierzytelniające użytkownika; w innych przypadkach atakujący może zdobyć ważne informacji o firmie, które może z powodzeniem wykorzystać do przeprowadzenia innych ataków (takich jak podszywanie się).

Aby uniknąć tego ataku, *należy stworzyć politykę klasyfikacji i zarządzania danymi*, która jasno definiuje następujące kwestie:

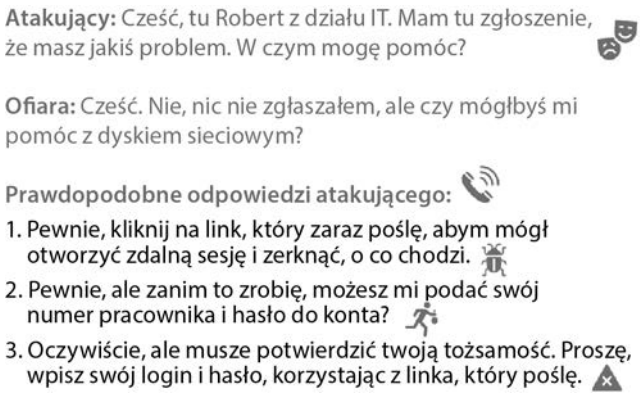
- różne rodzaje dokumentów (takie jak poufne, poufne, publiczne i inne),
- właściwy sposób utylizacji każdego rodzaju dokumentu,
- właściwy sposób pozbywania się dokumentów fizycznych (na przykład notatek, książek, karteczek samoprzylepnych i innych).

Zasady te łatwiej jest egzekwować, gdy użytkownicy przebywają w biurze. Jednak w sytuacji, gdy coraz więcej użytkowników pracuje w domu, musisz zastosować dodatkowe mechanizmy, aby upewnić się, że te zasady są przestrzegane i że użytkownicy mają odpowiednie narzędzia do ich realizacji. Na przykład udostępnij użytkownikom posiadającym wrażliwe informacje niszczarkę lub ogranicz drukowanie wrażliwych dokumentów w domu.

Coś za coś

„Coś za coś" (łac. *quid pro quo*) jest bardzo ciekawym atakiem, w którym atakujący dostarcza ofierze za darmo jakieś korzyści.

Klasycznym przykładem jest sytuacja, gdy atakujący dzwoni do pracowników danej firmy, podszywając się pod osobę z działu IT i twierdząc, że jest to reakcja na otwarte zgłoszenie serwisowe. Jak widać na przykładzie przedstawionym na rysunku 4.18, ofiary z dużym prawdopodobieństwem „*skorzystają*" z połączenia, aby coś załatwić, podczas gdy w rzeczywistości to atakujący ich wykorzysta.



Rysunek 4.18. Atak typu „coś za coś"

Najlepszym sposobem zapobiegania temu atakowi jest wdrożenie (i rozgłoszenie) zasady dotyczącej wsparcia IT, która mówi, co następuje:

- IT nigdy nie zadzwoni do Ciebie z numeru zewnętrznego lub zablokowanego (jeśli to możliwe, przypisz przyjazny numer dla wszystkich połączeń z IT, na przykład 114).
- Pracownicy IT NIGDY nie będą prosić o podanie hasła.
- Nigdy nie podawaj swojego hasła ani przez telefon, ani przez e-mail, ani przez sms — **NIGDY**.

Innym dobrym pomysłem jest ustanowienie *dwukierunkowego mechanizmu oddzwaniania*. Oznacza to, że jeśli użytkownik otrzyma telefon od informatyka, będzie musiał do niego oddzwonić (używając oficjalnego numeru help desk). Takie oddzwonienie będzie służyło jako dodatkowa metoda weryfikacji i dla informatyka, i pracownika.

Okup w mediach społecznościowych

To jeden z najnowszych rodzajów ataków, które mają miejsce. Tutaj atakujący stosuje wiele technik, aby uzyskać dostęp do sieci społecznościowych Twojej firmy (czyli Facebooka, Instagrama i WhatsAppa). Atakujący zadba o to, aby zmienić wszystkie Twoje mechanizmy pozwalające na łatwe przywrócenie konta, więc podczas gdy Ty będziesz kontaktować się z firmą mediów społecznościowych, aby odzyskać do niego dostęp, napastnik będzie miał do niego dostęp do czasu rozwiązania problemu, co może trwać godziny, a nawet dni. Atakujący wiedzą, że wiele firm nie podejmie ryzyka pozostawienia swoich kont społecznościowych pod ich kontrolą (ze względu na szkody dla marki, klientów i osób obserwujących konta, (ang. *follower*)), więc żądają jakiejś zapłaty (zwykle bitcoinów) za oddanie firmie kontroli nad kontem.

Oto kilka wskazówek, jak zapobiec temu groźnemu atakowi:

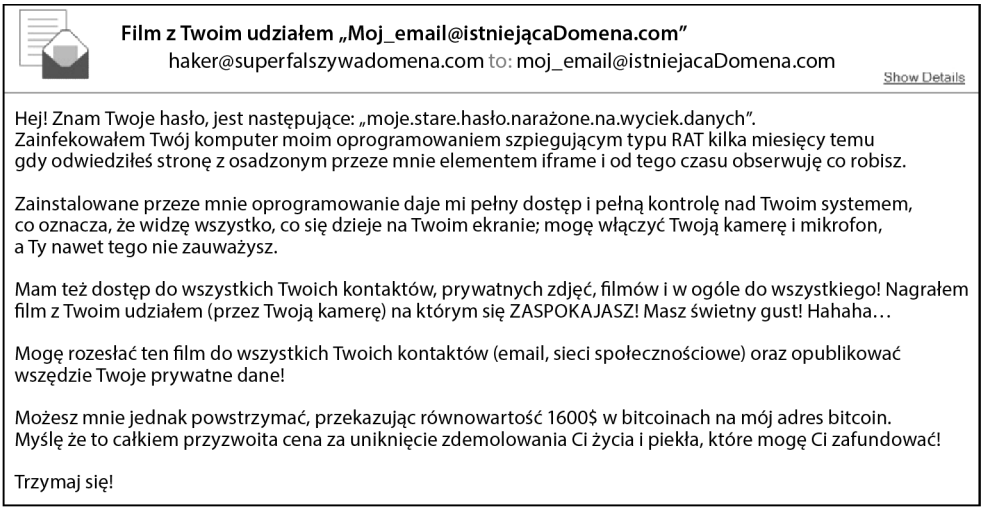
- Zawsze używaj MFA.
- Używaj silnych haseł. Tego typu kontami powinno się zarządzać za pomocą skarbca haseł, więc po co się krępować? Użyj maksymalnej długości, użyj znaków specjalnych i uodpornij je na ataki słownikowe lub siłowe.
- Upewnij się, że każde hasło jest unikalne.
- Często zmieniaj hasło (przynajmniej co 3 miesiące). Hasła i tak są zarządzane przez menedżera haseł, więc wymagany wysiłek to tylko dwa kliknięcia, cztery razy w roku.
- Umożliwiaj dostęp do tych kont jak najmniejszej liczbie osób, aby zmniejszyć ryzyko.

Dodatkowo *upewnij się, że osoby zarządzające tymi kontami* (na przykład menedżerowie mediów społecznościowych) *są dobrze przeszkolone w zakresie cyberbezpieczeństwa* (aby zapobiec tego typu atakom).

Szantaż

W tym scenariuszu napastnik będzie próbował przekonać ofiarę, że jej komputer lub smartfon został zhakowany i że zostaną ujawnione jakieś prywatne lub kompromitujące informacje, jeśli żądania napastnika nie zostaną spełnione w czasie krótszym niż 10 godzin (oczywiście wykorzysta taktykę wywoływania wrażenia pilności).

Jak widać na rysunku 4.19, jedna z metod opiera się na wmówieniu ofierze, że jej komputer został zhakowany, a na dowód tego atakujący wklei do środka e-maila hasło ofiary.



Film z Twoim udziałem „Moj_email@istniejącaDomena.com"
haker@superfalszywadomena.com to: moj_email@istniejacaDomena.com
Show Details

Hej! Znam Twoje hasło, jest następujące: „moje.stare.hasło.narażone.na.wyciek.danych".
Zainfekowałem Twój komputer moim oprogramowaniem szpiegującym typu RAT kilka miesięcy temu gdy odwiedziłeś stronę z osadzonym przeze mnie elementem iframe i od tego czasu obserwuję co robisz.

Zainstalowane przeze mnie oprogramowanie daje mi pełny dostęp i pełną kontrolę nad Twoim systemem, co oznacza, że widzę wszystko, co się dzieje na Twoim ekranie; mogę włączyć Twoją kamerę i mikrofon, a Ty nawet tego nie zauważysz.

Mam też dostęp do wszystkich Twoich kontaktów, prywatnych zdjęć, filmów i w ogóle do wszystkiego! Nagrałem film z Twoim udziałem (przez Twoją kamerę) na którym się ZASPOKAJASZ! Masz świetny gust! Hahaha…

Mogę rozesłać ten film do wszystkich Twoich kontaktów (email, sieci społecznościowe) oraz opublikować wszędzie Twoje prywatne dane!

Możesz mnie jednak powstrzymać, przekazując równowartość 1600$ w bitcoinach na mój adres bitcoin.
Myślę że to całkiem przyzwoita cena za uniknięcie zdemolowania Ci życia i piekła, które mogę Ci zafundować!

Trzymaj się!

Rysunek 4.19. Szantażująca wiadomość e-mail

Jeśli atakujący zna hasło, czy oznacza to, że naprawdę zhakował ofiarę?

Absolutnie nie!

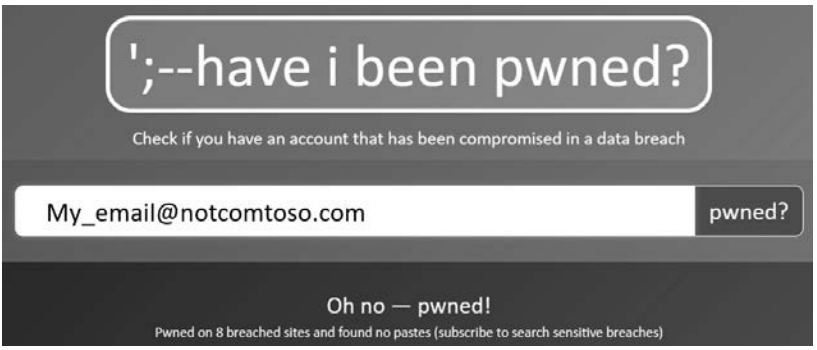
Tutaj atakujący wykorzystują informacje z poprzednich wycieków danych, szukają par e-mail – hasło i wykorzystują to w ataku.

Dlatego też, choć w większości przypadków podawane hasło jest starym hasłem, ofiara rozpoznaje je jako jedno ze swoich haseł i dlatego jest bardzo prawdopodobne, że padnie ofiarą tego oszustwa.

Najlepszym sposobem na zapobieganie tego typu atakowi jest uruchomienie kampanii wyjaśniającej pracownikom, w *jaki sposób napastnicy mogą wejść w posiadanie starych haseł*. Możesz podjąć następujące kroki:

1. Przedstaw krótkie wyjaśnienie, czym jest wyciek danych, i podaj kilka przykładów ostatnich wycieków danych w dużych firmach (na przykład wyciek danych z LinkedIna, wyciek danych z Yahoo i inne).

2. Poproś, aby sprawdzili, czy ich konta zostały skompromitowane w którymś z tych wycieków. Istnieje kilka stron, które to umożliwiają, ale nie wszystkim można zaufać. Jak pokazano na rysunku 4.20, jedną z najbardziej zaufanych/najczęściej używanych stron jest *https://haveibeenpwned.com/*. Witryna ta pokaże Ci, w którym wycieku danych znaleziono Twój adres e-mail, dzięki czemu możesz śmiało zabezpieczyć te konta.
3. Poinformuj, co należy zrobić, jeśli ich konto zostało znalezione w jakimś znanym naruszeniu danych, na przykład zmienić hasło, upewnić się, że nigdzie nie używają wariantu lub podobnego hasła, użyć MFA lub usunąć konto (jeśli nie jest używane):



Rysunek 4.20. Strona internetowa umożliwiająca sprawdzenie, czy dane uwierzytelniające zostały wykradzione

Powinieneś już teraz znać taktyki stosowane w atakach socjotechnicznych, a także najczęstsze typy ataków.

Omówiliśmy niektóre techniki obrony. Teraz nadszedł czas, aby poznać dodatkowe *najlepsze praktyki*, które mają zastosowanie do *wszystkich* tych typów ataków i pomogą Ci zmniejszyć ryzyko związane z tymi zagrożeniami.

Obrona przed atakami socjotechnicznymi (łatanie warstwy 8)

„Firmy wydają miliony dolarów na ściany ogniowe, szyfrowanie i urządzenia bezpiecznego dostępu, ale są to zmarnowane pieniądze, ponieważ żadne z tych działań nie odnosi się do najsłabszego ogniwa w łańcuchu bezpieczeństwa: ludzi, którzy używają, administrują, obsługują i rozliczają systemy komputerowe zawierające chronione informacje”

— Kevin Mitnick

Dowiedzmy się, jak skutecznie chronić swoją firmę przed tymi zagrożeniami.

Tworzenie strategii szkoleń

Jak wiecie, *łatanie* jest jedną z najważniejszych strategii w obronie bezpieczeństwa, a strategia ta może być również zastosowana do ludzi poprzez *edukację i szkolenia*. Dlatego *MUSISZ* zainwestować czas i inne zasoby, aby upewnić się, że masz **silną strategię szkoleń**.

Przyjrzyjmy się kluczowym punktom, które należy wziąć pod uwagę przy tworzeniu własnej strategii przeprowadzania szkoleń:

1. *Spersonalizuj szkolenie*, opierając się na kulturze firmy, istniejących zagrożeniach i rodzaju danych, którymi zarządza firma.
2. W przypadku mniejszych firm można stworzyć jedną sesję szkoleniową, która obejmie wszystkich pracowników, jednak średnie i duże firmy oraz korporacje *MUSZĄ mieć różne rodzaje szkoleń dostosowane do potrzeb*. Szkolenia te mogą być podzielone na grupy w zależności od typu pracownika, poziomu w organizacji, zarządzanych danych lub dostępu do danych.
3. Określ *metody prowadzenia* (na przykład szkolenie na żywo, webinar, filmy, animacje, interaktywne uczenie się przez internet i inne).
4. Określ *częstotliwości odbywania* szkoleń.
5. Określ kryteria konieczne do *zaliczenia* szkolenia, na przykład zdobycie co najmniej 80% punktów w ocenie końcowej.
6. Zdefiniuj *schemat nagradzania*; na przykład zapewnienie cyfrowej odznaki, którą można udostępnić w mediach społecznościowych.
7. Uzyskaj akceptację działu kadr i kierownictwa wyższego szczebla, tak aby *szkolenie było obowiązkowe*.

> **Wskazówka**
>
> Spraw, aby szkolenie było jak najbardziej interaktywne, wykorzystuj aktualne przykłady z życia wzięte, uwzględniaj wszystko (nigdy nie zakładaj, że jakiś temat jest zbyt podstawowy, aby go uwzględnić) i wykorzystaj listę ataków, które właśnie przejrzeliśmy, jako punkt odniesienia, aby upewnić się, że wszystkie główne wektory ataku zostały uwzględnione.

Musisz przekonać wyższe kierownictwo, że edukacja w zakresie cyberbezpieczeństwa nie jest dla organizacji *wydatkiem* pieniędzy, ale *inwestycją* w zabezpieczenie najbardziej wrażliwego czynnika w cyberbezpieczeństwie.

Prawa administratora

Jest to temat kontrowersyjny, ponieważ nie ma zgodności co do tego, czy nadawanie praw administracyjnych wszystkim pracownikom jest praktyką dobrą, czy nie. Jednak *z punktu widzenia bezpieczeństwa nie ma wątpliwości, że nadanie praw administracyjnych wszystkim pracownikom zwiększa liczbę zagrożeń.*

Dlatego zawsze należy dążyć do tego, aby nie nadawać praw administratora wszystkim użytkownikom; jeśli jednak firma zdecyduje się przyznać prawa administratora wszystkim pracownikom, to należy podjąć następujące środki zaradcze:

1. Określić jasne zasady dotyczące instalacji oprogramowania.
2. Utworzyć białą i czarną listę aplikacji, które mogą być zainstalowane.
3. Jeśli to możliwe, utworzyć repozytorium, w którym będzie znajdowało się gotowe do pobrania oprogramowanie z białej listy (zmniejsza to ryzyko zainstalowania przez użytkownika zhakowanej wersji oprogramowania).
4. Ustawić alert, jeśli na służbowej stacji roboczej zostanie zainstalowany program z czarnej listy.

Wdrożenie silnej zasady BYOD

Jeśli pozwalasz pracownikom na korzystanie z ich osobistych urządzeń do pracy, upewnij się, że masz silną politykę BYOD.

Dodatkowo zasada ta *musi* być wspierana przez systemy i oprogramowanie do jej egzekwowania.

Przeprowadzanie losowych ataków inżynierii społecznej

Najlepszym sposobem na ocenę poziomu przygotowania lub narażenia użytkowników na atak socjotechniczny jest przetestowanie ich za pomocą rzeczywistych, kontrolowanych ataków.

Oto jak można to zrobić:

- *Skonfiguruj swoje środowisko:* Wykup domenę, z której będziesz przeprowadzał ataki. Szukaj nazw podobnych do tych, których użyje prawdziwy atakujący, na przykład *suport-companyname.com*.
- *Testuj jeden atak na cykl:* Najpierw należy zdefiniować cykle, na przykład co 3 miesiące, co 6 miesięcy lub 1 rok. Na przykład phishing na początku 2020 roku, baiting pod koniec 2020 roku, coś za coś na początku 2021 roku i szantaż pod koniec 2021 roku.
- *Przeanalizuj wyniki:* Celem kontrolowanych ataków *nie* jest ściganie pracowników i upublicznienie ich wizerunku na „ścianie wstydu". Zamiast tego chodzi o zebranie informacji w celu określenia obszarów wymagających poprawy w ramach nadchodzących szkoleń i edukowania pracowników.
- *Ustanowienie nagród:* Możesz ustanowić system nagród dla tych pracowników, którzy znaleźli *atak* i użyli odpowiednich kanałów, aby zgłosić go do zespołu ds. cyberbezpieczeństwa.
- *Ogłoszenia i komunikaty:* Być może nie chcesz psuć wyników swoich testów poprzez uprzedzenie o tym, że się odbędą. Jednak dobrym pomysłem jest wysłanie komunikatu *po* zakończeniu oceny, aby ludzie byli świadomi tego typu inicjatyw, ale także aby podzielić się z nimi pewnymi istotnymi liczbami (na przykład ile osób padło ofiarą ataku, jakie byłyby potencjalne straty itp.).

Nagrody to nie zawsze pieniądze

Możesz również wykorzystać darmowe fanty, takie jak cyfrowe odznaki, ściana sławy, tytuł „bezpieczny pracownik miesiąca" (możesz chcieć użyć bardziej chwytliwej nazwy, takiej jak *Gwiazdor Cyberbezpieczeństwa*), przyznanie preferencyjnego miejsca parkingowego na miesiąc lub więcej.

Aby uniknąć zakłóceń w działaniu usług, zalecam przeprowadzenie tych kampanii na losowo wybranej grupie osób (w zależności od wielkości firmy może to być od 10% do 60% pracowników). Dodatkowo należy upewnić się, że w tej losowej grupie znajdują się uczestnicy ze wszystkich pionów i działów w firmie (na przykład HR, sprzedaż, IT).

Podsumowanie

W tym rozdziale dowiedziałeś się wszystkiego o użytkownikach — o tym, jak mogą wpłynąć na Twoją strategię obrony, o ich podatnościach i mnogości ataków skierowanych na nich, ale także o wszystkich taktykach, które możesz zastosować, aby zmniejszyć te zagrożenia.

Ten rozdział jest niezwykle ważny, ponieważ zabezpieczając ten wektor ataku, gwałtownie zmniejszysz zakres ataków na Twoją infrastrukturę, systemy i dane.

Teraz przygotuj się na kolejny ekscytujący rozdział, w którym głęboko zanurkujemy w rzeczy bardziej techniczne. W następnym rozdziale znajdziesz informacje o najlepszych narzędziach do testów penetracyjnych, kryminalistyce, sieci i wielu innych technologiach, które musisz opanować, aby stworzyć najlepszą defensywną strategię bezpieczeństwa.

Lektura uzupełniająca

Oto pełny raport The Cost of Insider Threats: 2020: *https://www.ibm.com/security/digital—assets/services/cost—ofinsider—threats/#/*.

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

U

V

W

X

Z

Chroń, co najcenniejsze — przede wszystkim dbaj o zabezpieczenia!

Gra o cyberbezpieczeństwo jest fascynująca i toczy się o wysoką stawkę. W każdej organizacji są dane, które trzeba chronić przed stale rosnącą liczbą zagrożeń. Jeśli to się nie uda, musimy się liczyć z uszczerbkiem na wizerunku, ze stratami finansowymi, a w niektórych wypadkach nawet z utratą zdrowia lub życia człowieka. Dlatego ważne jest, aby koncepcje bezpieczeństwa defensywnego były znane nie tylko inżynierom do spraw bezpieczeństwa, ale także wszystkim specjalistom IT. Jedynie w ten sposób można skutecznie wdrożyć przemyślaną strategię bezpieczeństwa.

To książka przeznaczona dla specjalistów, którzy chcą poszerzyć wiedzę na temat cyberbezpieczeństwa. Opisano tu aktualne koncepcje związane z podatnościami i zagrożeniami bezpieczeństwa, w tym model dojrzałości cybernetycznej. Zaprezentowano narzędzia takie jak Wireshark, DVWA, Burp Suite, OpenVAS i NMAP, a także techniki utwardzania systemów Unix i Windows. Omówiono też bardziej zaawansowane kwestie, w tym bezpieczeństwo fizyczne IT, ochronę urządzeń IoT, aplikacji internetowych i infrastruktury w chmurze. Autor zagłębił się również w takie zagadnienia jak analiza złośliwego oprogramowania, testy penetracyjne, techniki informatyki śledczej i automatyzacja w zapewnianiu bezpieczeństwa IT.

W książce:

- koncepcje związane z bezpieczeństwem defensywnym
- zabezpieczanie najbardziej podatnego czynnika — użytkownika
- konfiguracja najlepszych narzędzi bezpieczeństwa
- techniki utwardzania w środowiskach Windows i Unix
- przygotowywanie i ulepszanie strategii tworzenia zabezpieczeń
- zabezpieczenia urządzeń internetu rzeczy (IoT)
- poprawa bezpieczeństwa aplikacji internetowych i wdrożeń w chmurze

Cesar Bravo jest badaczem i wynalazcą, który ma ponad 100 patentów na wynalazki związane z cyberbezpieczeństwem. Uwielbia dzielić się wiedzą. Prowadził na kilku uczelniach zajęcia z zakresu bezpieczeństwa cybernetycznego na wszystkich poziomach. Chętnie uczestniczy w prestiżowych konferencjach, takich jak TEDx; wygłasza prelekcje na temat cyberbezpieczeństwa i innowacji w Wielkiej Brytanii, Niemczech, Meksyku, USA i Hiszpanii.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-9833-7
9 788328 398337
Cena: 109,00 zł
Packt