TestArmy CyberForces

LEVEL 1.0

POLOWANIE NA GRUBĄ RYBĘ

Ataki hakerskie na Muska, Bezosa, Gatesa,
które mogą spotkać też Ciebie

Spis treści

Kilka słów od nas

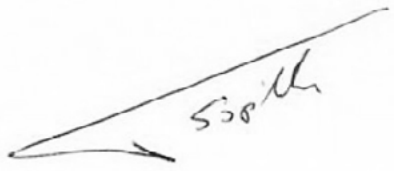
Pracownikowi Tesli zaoferowano milion dolarów za zainfekowanie wirusem sieci firmowej. Za pomocą prostej socjotechniki przejęto kontrolę nad kontem WhatsApp Jeffa Bezosa. Włamano się też na konta m.in. Billa Gatesa, Joe Bidena oraz Elona Muska i użyto ich do wyłudzenia łącznie ponad 100 tysięcy dolarów od użytkowników Twittera.

Jak widać prezesi firm i inne osoby na wyższych szczeblach różnych organizacji (również politycznych) są pod ciągłą obserwacją cyberprzestępców. Nic dziwnego — zwieńczone sukcesem polowanie na grubą rybę owocuje znacznie większym łupem niż nawet wiele udanych ataków na małe firmy. Osoby o najwyższym poziomie dostępu w organizacji to też doskonała furtka do informacji poufnych i innych cennych zasobów przedsiębiorstwa.

Rozwiązanie? Kroków, które należy poczynić w kierunku zapewnienia cyberbezpieczeństwa jest wiele, ale pierwszy z nich to zawsze świadomość. Tylko ktoś świadomy istnienia zagrożenia i tego jakie formy przybiera, jest w stanie opracować skuteczną linię obrony. W tym celu powstał niniejszy e-book: aby pokazać co grozi pracownikom wyższego szczebla i właścicielom firm oraz jak się przed tym bronić. Dodatkowo, naszą publikację okrasiliśmy historiami z życia wziętymi, dotyczącymi prezesów największych światowych firm — jak wiadomo, lepiej uczyć się na cudzych błędach niż popełniać własne.

Przyjemnej lektury!

TOMASZ SZPIKOWSKI,
PREZES ZARZĄDU TESTARMY GROUP



Polowanie na grubego zwierza. Whaling i CEO Fraud

Zacznijmy od najważniejszego. Whaling i CEO Fraud to dwa typy ataków, na które powinny szczególnie uważać osoby piastujące wyższe stanowiska w firmie. Czym są?

WHALING

to atak phishingowy ukierunkowany na osoby decyzyjne wyższego szczebla. Haker podszywa się pod inną osobę lub instytucję (np. kontrahenta, dostawcę) i stara się pozyskać w ten sposób dane od swojej ofiary — prezesa, właściciela firmy itd.

CEO FRAUD

— atak socjotechniczny, podczas którego haker podszywa się pod osobę decyzyjną, np. udając prezesa firmy zleca pracownikom wykonanie pilnego przelewu na podane przez siebie konto.

Po powyższych definicjach od razu widać, że ataki różnią się tym, w kogo są wycelowane. Tak więc, jeśli piastujesz wysokie stanowisko w firmie, lub jesteś jej właścicielem, **powinieneś nie tylko umieć rozpoznać atak typu whaling, ale też edukować swoich pracowników z identyfikowania i właściwego reagowania na CEO Fraud** — i właśnie dlatego CEO Fraud omówimy tu jako pierwsze.

CEO FRAUD

Nic nie zapada w pamięć tak dobrze, jak przykłady konkretnych sytuacji, które miały miejsce w rzeczywistości. Dlatego też, zamiast suchych faktów o CEO Fraud, opowiemy Wam historię ataku na dwie znane wszystkim korporacje — Snapchat i Seagate.

Co mają wspólnego ze sobą Snapchat i Seagate? Obie firmy są duże. Obie funkcjonują w branży technologicznej: Snapchat produkuje oprogramowanie (software) a Seagate – hardware. Od 2016 r. łączy je też fakt, że stały się ofiarą największych wycieków danych uzyskanych metodą CEO Fraud.

Jak doszło do tego, że takiej wielkości firmy nie dały rady uchronić się przed hakerem?

Cóż, w przeciwieństwie do wielu innych typów ataków, CEO Fraud z zasady jest skrupulatnie przygotowany. Już na etapie planowania scenariusza ataku, stara się pozyskać przydatne dla siebie informacje:

- Jaka jest specyfika działalności firmy? Jakie wyglądają poszczególne procesy i jacy ludzie są w nie zaangażowani?
- Ile osób zatrudnia firma? Jak wygląda struktura pracownicza? Kto odpowiada przed kim i w jakich obszarach?
- Z kim współpracuje firma? Kim są jej dostawcy, kontrahenci?
- Jak wygląda firmowa stopka mailowa? Jaki jest ton komunikacji pomiędzy poszczególnymi pracownikami?

Na pierwszy rzut oka mogłoby się wydawać, że nie jest łatwo uzyskać dostęp do takich informacji. W praktyce — można się zdziwić.

Czasem wystarczy, że haker dokładnie przeczesze Internet pod kątem materiałów zawierających wzmianki o przedsiębiorstwie. I tak:

- Na stronie firmowej zobaczy logotypy klientów — wiele firm umieszcza je w ramach social proof;
- W zakładce "O nas" znajdzie zdjęcia i stanowisko każdego z pracowników;
- W social mediach natknie się na wzmiankę o trwających projektach i nowych współpracach;
- Wypowiedzi dla prasy, udzielone np. przez prezesa firmy, pozwolą mu poznać jego styl komunikacji;

- Krótka wymiana maili z działem handlowym umożliwi wgląd w firmową stopkę.

Teraz wystarczy tylko odpowiednio połączyć kropki i scenariusz ataku mamy gotowy. Podszycie się pod nadawcę wiadomości mailowej (mail spoofing) jest technicznie proste do wykonania – w większości sytuacji wystarczy tylko jedna linijka kodu. Jeżeli nie mail spoofing osoby decyzyjnej, można wykorzystać też funkcję wysyłania wiadomości „w imieniu" w Microsoft Outlook, przekonując do współpracy osobę niższego szczebla. Możliwości jest naprawdę wiele.

CZY TO DZIAŁA?

Niestety, tak. Według danych FBI, w latach 2016-2019 wyłudzanie danych od firm metodą BEC (Business Email Compromise, CEO Fraud) wygenerowało **26 miliardów dolarów strat.** Natomiast w ostatnich dwóch latach, czyli pomiędzy rokiem 2018 a 2019, ilość ataków wzrosła o 100%.

CASE STUDY

A CO ZE WSPOMNIANYMI NA POCZĄTKU SNAPCHATEM I SEAGATE? JUŻ ODPOWIADAMY!

W 2016 r. pracownik Seagate został sławny po tym, jak wysłał do hakera rozliczenia finansowe około 10 000 pracowników firmy – od A do Z. Zrobił to na rzekome polecenie prezesa, którym okazał się haker. Mail był na tyle wiarygodny, że umknął czujnemu oku osób księgowości i ominął zabezpieczenia technologiczne.

Tego samego roku Snapchat padł ofiarą identycznego ataku z bardzo podobnym rezultatem. Dział finansów firmy otrzymał maila, w którym hakerzy podali się za prezesa firmy, prosząc o udostępnienie informacji dotyczących wypłat. Dane oczywiście otrzymali.

Zarówno Snapchat, jak i Seagate były zmuszone do publicznego przyznania się do ataku i zadośćuczynienia swoim pracownikom.

WHALING

Główną różnicą pomiędzy metodą CEO Fraud a whalingiem jest cel ataku — zazwyczaj prezes lub inna osoba wyższego szczebla. Samo słowo whaling nawiązuje do "phishingu" (łowienie)
i oznacza wielorybnictwo, a więc łowienie największych.

Ataki typu whaling są stosunkowo trudne do przeprowadzenia, ale przynoszą hakerom największe zyski. Prezesi firm i członkowie zarządu są uprzywilejowani w kwestii dostępu do danych: mają dostęp do praktycznie każdego zasobu firmy i w przeciwieństwie do średniego szczebla pracowników, nie obejmuje ich konteneryzacja informacji. Skompromitowanie urządzenia lub konta prezesa jest więc strzałem w dziesiątkę.

Choć wydawać by się mogło, że przez samą naturę swojej pracy, prezesi firm i osoby decyzyjne powinne być najlepiej chronione przed atakami cybernetycznymi, nie zawsze tak jest. Za przykład może posłużyć sam Jeff Bezos – prezes Amazon, który padł ofiarą ataku socjotechnicznego wykonanego przez komunikator WhatsApp. To właśnie przez sukces tego ataku w 2018 r. wyszło na jaw, że nawet prezesi gigantów technologicznych nie zawsze są adekwatnie zabezpieczeni. Co dokładnie się stało?

CASE STUDY

W 2018 roku, podczas rozmowy przez popularny komunikator WhatsApp, Bezos otrzymał wiadomość od osoby podającej się za księcia koronnego Arabii Saudyjskiej, Mohammeda bin Salmana. Jak donoszą media, wiadomość zawierała klip wideo, w którym znajdowały się dodatkowe linie kodu, pozwalające na import malware'u na urządzenie. Po aktywacji na telefonie Bezosa, malware dostał się do niemal wszystkich zasobów, dając hakerom nieograniczony dostęp do danych z telefonu. W mgnieniu oka okazało się, że prezes jednej z największych firm informatycznych jest tak samo podatny na ataki hakerskie jak przeciętny Kowalski.

Od momentu zhakowania media spekulują, czy istnieje korelacja pomiędzy wyciekiem danych z iPhone'a Jeffa a rychłym rozwodem z MacKenzie Bezos. Nie jest jasne też, czy na wycieku nie ucierpiał sam Amazon. Faktem jest, że malware uzyskał dostęp do wszelkiej komunikacji na urządzeniu, w tym kont mailowych – można więc przypuszczać, że ujawnione zostały również kontakty biznesowe Bezosa.

Hakowanie szefów i rad nadzorczych to naprawdę lukratywny biznes. Nawet gdy pełne przejęcie urządzenia – jak to się wydarzyło u szefa Amazonu – nie jest możliwe, na samym autorytecie zhakowanej osoby można zarobić krocie. Dobrym tego przykładem jest lipcowy hack Twittera, w którym autorytet osób takich jak Elon Musk, Barack Obama czy Joe Biden został wykorzystany, aby w ciągu kilku minut zarobić ponad 100 tysięcy dolarów. Więcej informacji o tym ataku znajdziesz w dalszej części e-booka, tymczasem przejdźmy do tego, jak bronić się przed whalingiem i CEO Fraud.

JAK SIĘ BRONIĆ?

Z pomocą przychodzą zasady i procedury Najlepszą zasadą jest przestrzeganie zasad.

W wypadku ataków typu CEO Fraud, żaden pracownik nie powinien był wysyłać danych, do których prezes teoretycznie już posiadał dostęp, np. poprzez systemy wewnętrzne.

Ponadto praca z danymi poufnymi, szczególnie natury finansowej, powinna być ściśle kontrolowana regulaminem przetwarzania danych. **Dobrą praktyką jest manualna weryfikacja, choćby sprawdzenie telefoniczne, czy prośba o tak dużą ilość danych, faktycznie powinna być zrealizowana.**

W sytuacji whalingu jest bardzo podobnie. Nie istnieją rozwiązania technologiczne, które gwarantują bezpieczeństwo w Internecie. Nawet Jeff Bezos takich nie posiada. Pośpiech i pochopność w działaniu, nawet w sytuacjach awaryjnych, jest najgorszym doradcą. Jeżeli wiadomość, zaproszenie, plik lub informacja choć w najmniejszym procencie wydaje się nietypowa, zawsze można ją przekazać do działu IT do weryfikacji. W przeciwnym wypadku może dojść do tego, co wydarzyło się w Amazonie.

RED TEAMING, WDROŻENIA I AUDYTY

Bezpieczeństwo osób decyzyjnych nie kończy się na zabezpieczeniu infrastruktury i ustaleniu odpowiednich procedur. Procedury, tak jak **zabezpieczenia technologiczne, działają tylko wtedy, gdy są wykorzystywane świadomie.**

Według badań Canona, tylko 17% wycieków danych jest spowodowanych obejściem zabezpieczeń technologicznych (Źródło: ABI Research – Canon, Office of the Future Survey, 2019). Natomiast około 55 do 59% wycieków danych jest spowodowanych przez tak zwany błąd ludzki, czyli niepoprawną konfigurację, podatność na ataki socjotechniczne i zwykłe wypadki przy pracy – choćby takie, jak niezrozumienie lub niestosowanie procedur. Aby wyeliminować te czynniki, firma powinna kompleksowo podejść do polityki bezpieczeństwa danych, korzystając z usług takich jak red teaming, audyty procedur i szkoleń.

Red Teaming to technika ofensywna polegająca na symulacji ataku wymierzonego w pracownika, system, czy oprogramowanie z uwzględnieniem fizycznego wkroczenia do siedziby organizacji, zgodnie z zasadą, że cel uświęca środki (więcej o red teamingu przeczytasz tutaj).

Audyty procedur wewnętrznych polegają na weryfikacji zastanej sytuacji, czyli zasad i słuszności obecnych procedur w firmie, jak i ich przestrzegania. Rezultatem audytów często są optymalizacje procesów.

Szkolenia sprawiają, że pracownicy nie tylko są świadomi, ale rozumieją cele procedur i swoją odpowiedzialność za bezpieczeństwo danych firmy.

PODSUMOWANIE

CEO Fraud i whaling są typami ataków socjotechnicznych, które ilustrują różnicę pomiędzy posiadaniem procedur a ich zrozumieniem i wdrożeniem w życie. Za każdym sukcesem hakerów stoi błąd szefa lub pracownika, który nieświadomie współpracował z przestępcami. Osoby decyzyjne, którym zależy na utrzymaniu wysokiego poziomu odporności na ataki hakerskie powinny traktować bezpieczeństwo kompleksowo, tworząc kulturę bezpiecznej pracy z danymi poufnymi w całej firmie.

Insiderzy, czyli milion dolarów za zainfekowanie sieci firmowej Tesli

Standardowo, gdy mowa o wyciekach danych i atakach cybernetycznych, przedsiębiorcy dopatrują się źródła zagrożenia na zewnątrz — to krążący po sieci wirus zasadza się na bezpieczeństwo firmy lub podstępny haker chce zaatakować przedsiębiorstwo. Mało kto zwraca uwagę również na niebezpieczeństwa, czające się wewnątrz organizacji.

Tymczasem **dwa główne zagrożenia bezpieczeństwa sieci, według badania Canon, to „osoby o złych intencjach, mające dostęp do informacji poufnych (30%) oraz błąd człowieka (25%)”.** Jeden i drugi przypadek możemy podsumować jednym, krótkim określeniem — insider. Kim są wspomniani insiderzy i jak się przed nimi bronić?

KIM JEST INSIDER

Insider to po prostu osoba mająca dostęp do informacji poufnych — i nadużywająca tego dostępu, świadomie bądź nie, z własnej inicjatywy lub zaszantażowana przez hakera.

Jak podaje „Insider Threat. Spotlight report” od AT&T Business, **ponad 75% organizacji szacuje, że koszty usunięcia skutków naruszenia informacji poufnych przez insiderów mogą osiągnąć nawet 500 000 dolarów. 25% uważa, że koszty przekraczają tę kwotę i mogą sięgać nawet milionów.**

Jak widać, przed insiderami warto się bronić — a żeby robić to skutecznie, warto dowiedzieć się o nich nieco więcej. Zacznijmy od typów insiderów.

/ 5 TYPÓW INSIDERÓW

Firma Verizon — autor publikowanego corocznie raportu „Insider Threat Report", pokusiła się o sklasyfikowanie najczęstszych typów insiderów, odpowiadających aż za 34% wszystkich wycieków danych w firmach. Klasyfikacja wygląda następująco:

01. **Nieostrożny pracownik** (The Careless Worker) — to ten, który celowo łamie lub obchodzi politykę bezpieczeństwa firmy. Czasem wynika to z braku wiedzy o konsekwencjach takich działań. Czasem — przyczyną jest faktyczna chęć ominięcia firmowych wytycznych, np. aby zainstalować nielegalne oprogramowanie na służbowym laptopie;

02. **Agent wewnętrzny** (The Inside Agent) — pracownik zrekrutowany nieświadomie lub przekupiony przez cyberprzestępcę w celu przekazywania danych;

03. **Niezadowolony pracownik** (The Disgruntled Employee) — to ktoś, kogo nie należy lekceważyć! Zdarza się, że konflikty na linii pracodawca-pracownik skutkują zniszczeniem danych lub przekazywaniem ich osobom z zewnątrz;

04. **Złośliwy informator** (The Malicious Insider) — pracownik, który nadużywa dostępu do poufnych danych w celu uzyskania własnych korzyści. Motywacją mogą być np. prowizja od okupu lub finansowanie przez konkurencje;

05. **Beztroska trzecia strona** (The Feckless Third-Party) — to pracownik lub kontrahent, który zaniedbując cyberbezpieczeństwo naraża firmę na wyciek danych.

CASE STUDY

PRZYKŁADY INSIDERÓW

Problem insiderów dotknął m.in. Coca Coli. Pracownik jednej ze spółek zależnych firmy odchodząc przywłaszczył dane około 8 tysięcy osób. Coca Cola powiadomiła pracowników, których dane wyciekły oraz zaoferowała im roczny bezpłatny monitoring pod kątem ewentualnych kradzieży tożsamości, realizowany przez firmę zewnętrzną.

Z problemem insiderów zmierzył się też Facebook. Pracownik zatrudniony jako (o ironio) inżynier bezpieczeństwa, za pomocą dostępnych na tym stanowisku uprawnień, pozyskiwał informacje, które następnie wykorzystywał do prześladowania kobiet online.

„Ważne, aby informacje, którymi dzielą się użytkownicy Facebooka, były przechowywane w sposób bezpieczny i gwarantujący prywatność. Zachowujemy ścisłą politykę bezpieczeństwa i ograniczeń technicznych, przez co pracownicy mają dostęp tylko do danych, których potrzebują do wykonywania swojej pracy — na przykład naprawy błędów, obsługi klienta lub odpowiedzi na ważne wnioski prawne. Pracownicy, którzy nadużyją uprawnień, zostaną zwolnieni" — podsumował sytuację Alex Stamos, Chief Security Officer Facebooka.

JAK ZAPOBIEGAĆ? JAK SIĘ BRONIĆ?

/ SPRAWDŹ, KTO MA DOSTĘP DO DANYCH

Zabezpieczanie firmy przed atakami z wewnątrz najlepiej zacząć od ustalenia poziomu dostępu poszczególnych pracowników. Czasem firmy mają co prawda listy uprawnień zatrudnionych przez siebie osób, ale nie są one regularnie aktualizowane (co czyni je właściwie bezużytecznymi).

Tymczasem, w przypadku ataku lub wycieku danych, warto mieć możliwość błyskawicznego ustalenia, kto posiada wgląd w skompromitowane informacje — i to w tym gronie rozpocząć poszukiwanie winnego.

Lista uprawnień pomaga też w przestrzeganiu zasady minimalnych uprawnień (o której kilka słów poniżej). Czasem dostęp do informacji mają pracownicy, którzy ich już nie potrzebują: nie pracują już na danym stanowisku lub nawet całkiem opuścili firmę. Lista pomaga szybko zauważyć takie przypadki.

/ STOSUJ ZASADĘ MINIMALNYCH UPRAWNIEŃ

Po okazji porządków na liście osób posiadających dostęp do najważniejszy danych firmy, proponujemy wdrożenie zasady minimalnych uprawnień. Mowa o tym, aby nadając uprawnienia użytkownikom, brać pod uwagę tylko te, których faktycznie potrzebują oni do wykonywania swojej pracy. Tak więc, np. osobie dodającej artykuły w panelu Wordpress wystarczy konto „Redaktora", nie są jej potrzebne uprawnienia administratorskie. Warto kierować się zdrowym rozsądkiem przy udzielaniu dostępu do różnych danych — im mniej osób cieszy się najwyższym poziomem uprawnień, tym lepiej dla firmy.

/ JASNO OKREŚL ZASADY

Czasem już samo zobrazowanie konsekwencji nielojalności wystarczy, aby ochłodzić zapały nieuczciwego pracownika. Absolutną podstawą jest polityka bezpieczeństwa firmy, jasno określająca jak korzystać z firmowego sprzętu
i otrzymanych uprawnień, oraz jakie działania są wyraźnie zakazane (np. pobieranie nieautoryzowanego oprogramowania).

Nic nie stoi też na przeszkodzie, aby zabezpieczyć się przed trudnymi sytuacjami za pomocą umowy NDA (Non-disclousure agreement), zawierającej też informacje o karze za jej złamanie.

Co ciekawe, nawet jeśli nie zawarłeś z pracownikiem umowy o poufności danych, a on np. przekazywał je konkurencji, wciąż możesz wyciągnąć za to konsekwencje. Wspomina o tym przepis art. 11 ust. 1 ustawy o zwalczaniu nieuczciwej konkurencji: Czynem nieuczciwej konkurencji jest ujawnienie, wykorzystanie lub pozyskanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa.

Oczywiście dochodzenie roszczeń bez zawarcia stosownej umowy jest znacznie trudniejsze, warto więc dmuchać na zimne i nie bać się prosić przyszłego pracownika o parafowanie stosownego pisma. Dla tych, którzy i tak nie planują nadużyć swoich uprawnień, podpisanie standardowej umowy, nie powinno stanowić większego problemu.

/ MONITORUJ GODZINY PRACY

Sygnałem alarmowym wskazującym, że masz do czynienia z insiderem może być nagłe rozpoczęcie przez pracownika korzystania z zasobów firmowych poza godzi-

nami pracy. Warto przyjrzeć się bliżej takim niespodziewanym aktywnościom — niestety mogą zwiastować one kłopoty.

/ NIE ZADZIERAJ Z PRACOWNIKIEM

Rozwścieczony pracownik potrafi nieźle zajść za skórę pracodawcy, zwłaszcza jeśli w swojej opinii nie ma już nic do stracenia (czyli na przykład trwa jego okres wypowiedzenia).Warto na bieżąco pytać pracowników o ich ocenę miejsca pracy, na przykład za pomocą ewaluacji kwartalnej, i rozwiązywać problemy jeszcze zanim urosną do niebotycznych rozmiarów.
To nie tylko kwestia cyberbezpieczeństwa, ale też po prostu zwykłego bycia fair. **Czy to wystarczy?** Niestety nie zawsze. Nikt nie zagwarantuje Ci uczciwości pracownika, nawet jeśli Ty sam traktujesz go jak należy. Niemniej, dbanie o dobre samopoczucie zatrudnionych ludzi, nawet jeśli nie pomoże — na pewno nie zaszkodzi.

PODSUMOWUJĄC

Insiderzy to spore ryzyko dla organizacji — zwłaszcza jeśli zarząd nie zdaje sobie sprawy z ich istnienia. Często uparcie wypatrujemy ataku z zewnątrz, jednocześnie nie zauważając, że oszust podkopuje cyberbezpieczeństwo firmy od środka.

Na początek warto w ogóle dopuścić do siebie myśl, że insiderzy się zdarzają — świadomość zagrożeń to pierwszy krok do ochrony przed nimi. Mamy nadzieję, że ten rozdział był dla Ciebie właśnie takim krokiem — teraz pozostało Ci zachęcić do jego wykonania swoich pracowników. **Powodzenia!**

Socjotechnika, czyli „Proszę pilnie wykonać ten przelew!”

„Jak nie drzwiami to oknem” — tym mottem zdaje się kierować coraz więcej cyberprzestępców i niestety mają w tym sporo racji. Wystarczy, że w miejsce „drzwi” podstawimy zabezpieczenia systemowe, a „okna” — pracowników. W tym rozdziale skupimy się na socjotechnikach, za pomocą których, hakerzy przeprowadzają swoje ataki.

CZYM SĄ SOCJOTECHNIKI I DLACZEGO W OGÓLE POWINNO CIĘ TO OBCHODZIĆ?

Być może sądzisz, że nie grozi Ci atak hakerski. Ba, jeśli prowadzisz biznes, prawdopodobnie zrobiłeś już wiele, aby nie dostał się on w ręce przestępców. Ustawiłeś silne hasła do kont firmowych. Zadbałeś o wysokiej jakości kod źródłowy strony. Zainwestowałeś w oprogramowanie antywirusowe i karty dostępu dla pracowników. Niestety, to wciąż może być za mało.

„Firma może wydać setki tysięcy dolarów na zapory sieciowe, szyfrowanie i inne technologie bezpieczeństwa, jednak jeżeli atakujący znajdzie choć jedną podatną na sugestie osobę wewnątrz organizacji, i osoba ta pozwoli sobą manipulować, wszystkie te pieniądze wyłożone na ochronę będą zmarnowaną inwestycją” – Kevin Mitnick.

System bezpieczeństwa jest więc tak bezpieczny, jak jego najsłabsze ogniwo — nieważne czy jest nim słaba zapora sieciowa, czy manager klikający link, przesłany na jego służbową pocztę przez nigeryjskiego księcia.

Domyślasz się, do czego zmierzam?

Socjotechniki to metody manipulacji człowiekiem, mające na celu nakłonienie go do podjęcia określonych czynności. Nie trudno domyślić się, jakie akcje są na rękę cyberprzestępcom. Podanie danych logowania, wpuszczenie do budynku, pobranie zawirusowanego pliku — przykłady można mnożyć. Łączy je jedno: na końcu haker dostaje dokładnie to, czego chce. Aktualnie najczęstszym celem ataków jest pozyskanie dostępu do zasobów w firmie, w celu ich zaszyfrowania i zażądania okupu.

Wiesz już, czym są socjotechniki i dlaczego musisz bronić przed nimi swoją firmę. Czas dowiedzieć się więcej o tym, z jakich metody korzystają hakerzy.

TYPY ATAKÓW Z WYKORZYSTANIEM SOCJOTECHNIK

Techniki używane przez cyberprzestępców możemy podzielić na wirtualne, fizyczne i mieszane (hybrydowe). Przyjrzymy się po kolei każdej grupie.

Jedną z najpopularniejszych metod wirtualnych jest **phishing**, którego przykłady wymienialiśmy już w poprzednich rozdziałach. Jest to niespersonalizowany, zwykle masowy, atak, najczęściej za pomocą fałszywych e-maili lub przekierowywań na sfabrykowane strony internetowe.

Odmianą phishingu jest **spear phishing**. Jest on atakiem ukierunkowanym na konkretną osobę. Tak, tak. Skojarzenia ze wspomnianym wcześniej **whaling**iem są tu słuszne! Osoby znajdujące się wysoko w biurowej hierarchii, zwykle mają pełen dostęp do interesujących hakera poufnych danych.

Jak przebiega atak phishingowy? Na początek haker wybiera ofiarę, a następnie planuje atak, uwzględniając jej słabości. Może on na przykład wykonać telefon do właściciela firmy z prośbą o wypowiedź odnośnie głośnej afery związanej z jego przedsiębiorstwem. Gdy niepodejrzewająca niczego ofiara dopyta o jakiej aferze mowa, rzekomy dziennikarz bez zająknięcia opowie zmyśloną wcześniej pogłoskę, proponując od razu przesłanie na skrzynkę mailową artykułu opisującego ten przykry news. Tutaj wystarczy spreparowana strona z tekstem o chwytliwym tytule np. „Firma X zamyka oddział w Poznaniu. Szykują się masowe zwolnienia". Po chwili na stronie pojawia się pop-up, zawierający link do wirusa. Ofiara klika, żeby zamknąć go i wznowić lekturę artykułu, a wirus podlinkowany pod przycisk zamknięcia, trafia prosto do jej komputera. Co więcej, jeśli ofiara prześle stronę kolejnym osobom w firmie (na przykład do reszty zarządu, osób odpowiedzialnych za PR itd.), co prawdopodobnie nastąpi, w niedługim czasie wirus obejmie całe przedsiębiorstwo.

Nie zapominajmy też o **deepfake**, czyli sfałszowanych nagraniach audio lub video. Wystarczy, że haker skorzysta z, chociażby, oprogramowania autorstwa Lyrebird, dzięki któremu wystarczy zaledwie minutowa próbka głosu, aby stworzyć jego cyfrowe odwzorowanie. Następnie może wykorzystać je np. do podszycia się pod prezesa firmy, który dzwoni do pracownika z poleceniem wykonania pilnego przelewu ze służbowego konta. To przykład, który wydarzył się naprawdę!

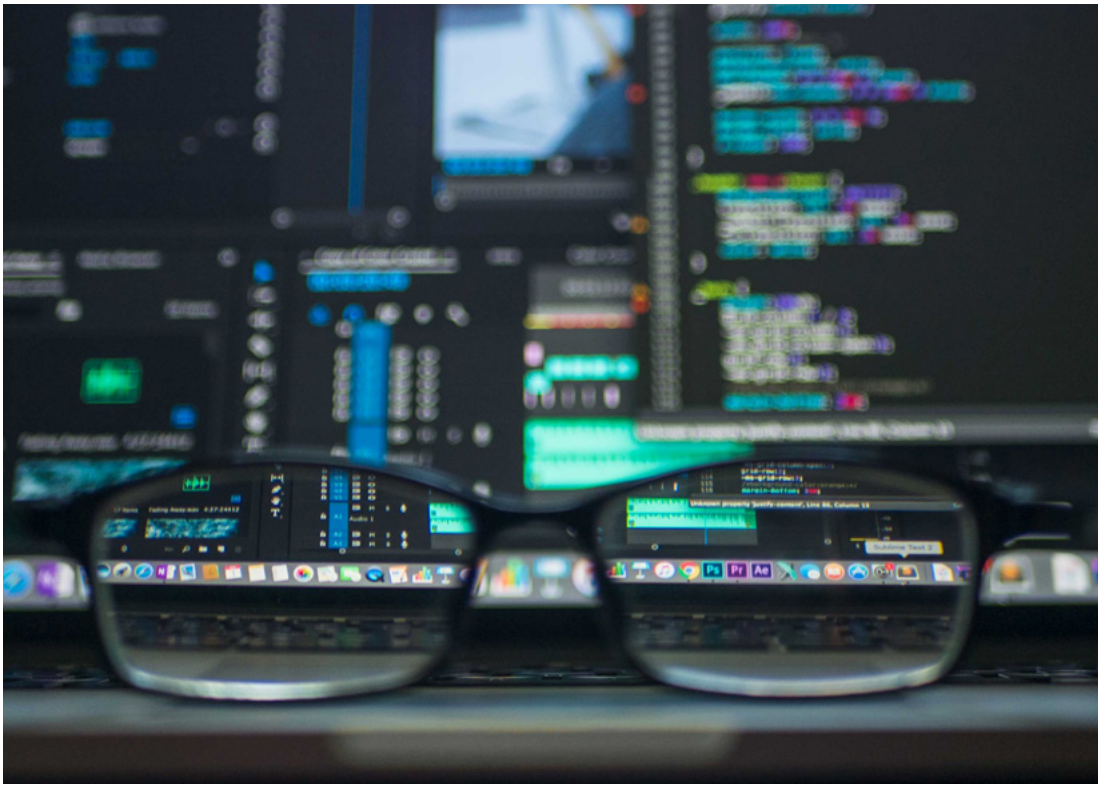
CASE STUDY

Dyrektor generalny brytyjskiej firmy energetycznej myśląc, że rozmawia przez telefon ze swoim szefem, wykonał na polecenie dzwoniącego przelew dla węgierskiego dostawcy. Według firmy ubezpieczeniowej Euler Hermes Group SA, zajmującej się tą sprawą, dzwoniący powiedział, że prośba jest pilna i nakazał zarządowi zapłacić w ciągu godziny. Przelew wykonano.

Innym zagrożeniem jest też pretexting. **Pretexting** to próba pozyskania wrażliwych danych poparta brzmiącym wiarygodnie pretekstem. Haker może na przykład zadzwonić do firmy, podszywając się pod konkretną instytucję (np. bank, w którym prowadzone jest konto firmowe) twierdząc, że ma do przekazania ważne informacje, ale najpierw prosi o potwierdzenie tożsamości. Pozornie to kłamstwo zdaje się mieć krótkie nogi, ale gdy sprawa jest pilna, łatwo stracić głowę i zdradzić poufne informacje przestępcy.

Czy cyberprzestępcy atakują tylko online? Niekoniecznie! Choć kiedy mowa o hakerach, większość z nas wyobraża sobie zakapturzonego mężczyznę, siedzącego w ciemnym pokoju, który rozświetlona tylko blask ekranu komputera, to ten znany z okładek gazet obraz, niekoniecznie odzwierciedla rzeczywistość. Hakerzy działają też w świecie rzeczywistym — i to z sukcesami.

Do ataku socjotechnicznego przestępcy mogą wykorzystać **przebranie**. Haker może pojawić się w firmie, na przykład udając serwisanta znanej firmy usługowej, któremu



rzekomo zlecono zainstalowanie sterowników do drukarki. Wybierze przy tym idealny moment, kiedy w biurze nie ma akurat żadnej osoby, która mogłaby potwierdzić, czy faktycznie wzywano fachowca. W rezultacie, nie chcąc niepokoić pracowników telefonami po godzinach, niejeden manager udostępni serwisantowi komputer celem zainstalowania sterowników — i w pakiecie z nimi otrzyma złośliwe oprogramowanie.

Inną metodą wykorzystywaną podczas ataku socjotechnicznego jest **baiting**. Nazwa pochodzi od angielskiego słowa „bait" — przynęta. Skojarzenie z łowieniem ryb jest tu nieprzypadkowe. Tak jak rybak zawiesza na wędce robaka, tak
i haker może podrzucić do firmy np. zainfekowany pendrive opatrzony intrygującą nalepką: "Wynagrodzenia".

Tailgating to z kolei wejście w dane miejsce osoby do tego nieupoważnionej. Przykładem może być przytrzymanie przez pracownika drzwi do firmy spieszącemu się człowiekowi. Tailgating najczęściej ma miejsce w dużych przedsiębiorstwach, gdzie zatrudnieni nie znają wszystkich współpracowników.

6 REGUŁ CIALDINIEGO

Niezależnie od metody, jaką wybiorą cyberprzestępcy, przeprowadzając atak, często sięgają przy tym po 6 reguł wywierania wpływu, przedstawionych w bestsellerowej książce Roberta Cialdiniego pt. „Wywieranie wpływu na innych". Aby lepiej zobrazować działanie każdej z nich, przygotowaliśmy krótkie podsumowanie:

01. **Reguła wzajemności**

O co chodzi: Kiedy ktoś wyświadcza nam przysługę, czujemy się zobowiązani odpłacić się tym samym.

Jak korzystają z niej hakerzy: Haker może zainscenizować sytuację, podczas której pomoże swojej ofierze, np. pozbierać dokumenty, które wypadły jej z rąk po tym, jak sam ją potrącił („Przepraszam, to mój pierwszy dzień w pracy, niezdara ze mnie…"). Następnie, zdobywszy zaufanie ofiary, poprosi o to, czego chce — przykładowo o możliwość wejścia do firmy („Zostawiłem kartę w biurze, a to mój pierwszy dzień, szef nie może się dowiedzieć…").

02. **Reguła zaangażowania i konsekwencji**

O co chodzi: Ludzie lubią uważać się za konsekwentnych w działaniu. Gdy poświęciliśmy czemuś sporo czasu i energii, podejmowanie kolejnych zobowiązań przyjdzie nam dużo łatwiej, niż wtedy, gdy tego nie zrobiliśmy.

Jak korzystają z niej hakerzy: Pracownik, który zgodził się już na jedną prośbę hakera (np. wpuszczenie do firmy), prawdopodobnie zgodzi się też na kolejne (np. udostępnienie firmowego komputera). Z każdą spełnioną prośbą, rośnie szansa na akceptację kolejnych.

03. Reguła społecznego dowodu słuszności

O co chodzi: Kiedy inni postępują w dany sposób, łatwiej jest nam uwierzyć, że jest on właściwy i podejmować te same działania.

Jak korzystają z niej hakerzy: Gdy jedna osoba zrobi daną rzecz (na przykład pobierze nieautoryzowane oprogramowanie na swój komputer), reszta będzie bardziej skłonna pójść w jej ślady.

04. Reguła sympatii

O co chodzi: Gdy kogoś lubimy, chętniej spełnimy jego prośby.

Jak korzystają z niej hakerzy: Wróćmy do przykładu z podszyciem się pod nowego pracownika, który zapomniał zabrać karty z biura i prosi, żeby go wpuścić („To mój pierwszy dzień, szef nie może się dowiedzieć…"). Tu też zadziała reguła sympatii — wielu pracowników nie odmówi udzielenia pomocy czarującemu niezdarze.

05. Reguła autorytetu

O co chodzi: Chętniej spełniamy prośby osób, mających w naszych oczach autorytet lub władzę.

Jak korzystają z niej hakerzy: Cyberprzestępca może podszyć się pod ważną osobę w firmie (w kontakcie mailowym/telefonicznym) lub kogoś cieszącego się szacunkiem — strażaka, policjanta (korzystając z przebrania).

06. Reguła niedostępności

O co chodzi: To, co rzadkie lub trudne do osiągnięcia, uważamy za cenniejsze.

Jak korzystają z niej hakerzy: Kto z nas choć raz nie otrzymał powiadomienia, że właśnie wygrał smartfona i musi spieszyć się, by go odebrać? No właśnie. To doskonały przykład jak hakerzy wykorzystują regułę niedostępności.

JAK UCHRONIĆ FIRMĘ PRZED ATAKIEM SOCJOTECHNICZNYM?

Oczywiście, wymienione powyżej socjotechniki nie są wszystkimi, z jakich korzystają hakerzy. Z roku na rok pojawiają się nowe metody, tak samo, jak powstają nowe wirusy. Najlepszą obroną przed nimi pozostają czujność i zdrowy rozsądek.

Aby uchronić się przed atakiem socjotechnicznym:

Nie wykonuj czynności automatycznie — wyrób w sobie nawyk przeczytania adresu linku przed jego kliknięciem, dokładnego sprawdzania adresu mailowego nadawcy, porównania danych na wydrukowanych fakturach z danymi z elektronicznej wersji itd.;

Stosuj zasadę ograniczonego zaufania — proś fachowców, którzy przychodzą do firmy o okazanie legitymacji, nie otwieraj drzwi tym, którzy nie mają karty dostępu;

Regularnie aktualizuj system operacyjny oraz oprogramowanie antywirusowe — wymagaj też tego od pracowników pracujących na własnych urządzeniach (zdalnie);

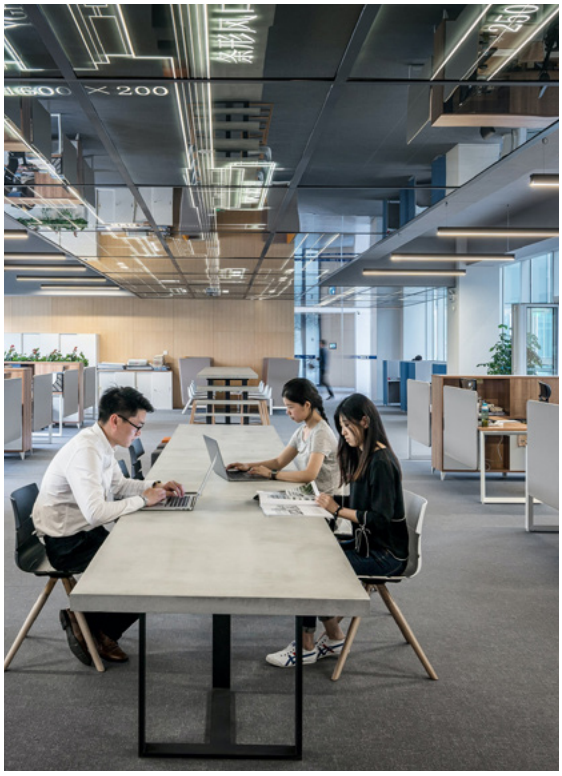
Zadaj sobie pytanie „Dlaczego?" — zanim zdecydujesz się spełnić przekazaną przez nieznajomego, prośbę, zastanów się co za nią stoi. Czy jest uzasadniona? Czy na pewno istnieje dobry powód, aby ją spełnić — i abyś zrobił to właśnie Ty?

Upewnij się, z kim rozmawiasz — jeśli masz wątpliwości co do rozmówcy, wpleć w rozmowę błędne stwierdzenie, które u prawdziwej osoby szybko wywoła zdziwienie. Przykład? Proszę bardzo. Wyobraź sobie, że odbierasz telefon z działu księgowości kontrahenta z prośbą o zmianę numeru konta do przelewów. Możesz zapytać na przykład czy Zosia wróciła już z macierzyńskiego, wiedząc, że w firmie nie pracuje żadna Zosia;

Potwierdzaj informacje u źródła — czasem wystarczy tylko jeden telefon z zapytaniem o przesłaną mailowo prośbę (np. zmianę numeru konta na fakturze), aby uniknąć tragedii.

Uczul swoich pracowników na kwestie bezpieczeństwa — to, że Ty masz świadomość zagrożenia, nie znaczy, że ma ją każdy w Twojej firmie. Hakerzy dobrze o tym wiedzą i często za cel obierają sobie pracowników pozbawionych nawet podstawowej wiedzy o cyberbezpieczeństwie. Nic dziwnego! Przekonanie do podania danych logowania „pani Krysi" z recepcji jest zwykle łatwiejsze niż nakłonienie do tego członka zarządu. Idealnie byłoby, gdyby każdy pracownik Twojej firmy zdawał sobie sprawę z grożących mu niebezpieczeństw i wiedział jak się przed nimi bronić. Na dobry początek możesz podrzucić im ten artykuł (np. w newsletterze wewnętrznym).

PRZEPROWADŹ TESTY SOCJOTECHNICZNE



Słowa mają to do siebie, że szybko ulatują z pamięci. Za to przeżycia, zwłaszcza te powiązane z silnymi emocjami, zostają w niej znacznie dłużej. A czy może być coś bardziej zapadającego w pamięć pracownika, niż odkrycie, że to właśnie z powodu popełnionych przez niego błędów, hakerzy dokonali udanego ataku na firmę?

Na szczęście nie musisz stawiać firmy w obliczu realnego zagrożenia, aby uczulić pracowników na kwestie cyberbezpieczeństwa. Wystarczy symulacja przeprowadzona w ramach testów socjotechnicznych. Jak wyglądają takie testy krok po kroku?

- **Podpisanie umowy o poufności danych** — Firmy przeprowadzające testy socjotechniczne zwykle rozumieją, że „papier to papier" i choć Twoje dane są u nich bezpieczne, nie mają problemu ze sporządzeniem stosownej umowy;
- **Rozmowa o Twojej firmie** — Każdy biznes jest inny. Rozmowa pomoże lepiej zrozumieć strukturę Twojej firmy, jej kluczowe zasoby i pracowników — a następnie dopasować do nich testy;
- **Ustalenie punktów wejścia** — Pentesterzy poszukają luk w Twoich zabezpieczeniach, korzystając przy tym z ogólnodostępnych źródeł (informacji o firmie i pracownikach dostępne w sieci), zweryfikują wektory ataku i ich wykorzystanie;

- **Opracowanie strategii testów** — zostanie przygotowany scenariusz testu. Specjaliści zadbają, aby był on jak najbardziej realistyczny;

- **Testy —** Oto moment, na który czekaliśmy od początku. Teraz okaże się, czy Twoi pracownicy są gotowi, aby odeprzeć atak hakera. Na tym etapie specjaliści przeprowadzą ustalony scenariusz, np. włamanie do siedziby firmy, albo atak zdalny z wykorzystaniem spear phishingu.

- **Ustalenie co dalej** — Po przeprowadzeniu testu, otrzymasz raport, ukazujący zarówno przebieg samego testu (do jakich zasobów uzyskano dostęp, jakie były punkty wejścia), jak i dalsze rekomendacje (jakie obszary należy wzmocnić, jak opracować protokoły postępowania w takich sytuacjach). Jeśli będzie taka potrzeba, firma zaproponuje też przeszkolenie pracowników, aby wiedzieli jak radzić sobie z zagrożeniami w przyszłości.

PODSUMOWUJĄC

Scenariuszy cyberataków jest wiele (i wciąż przybywają nowe!), ale główny sposób na obronę przed nimi się nie zmienia — jest nim zdrowy rozsądek.

Zadbaj, aby nie zabrakło go Tobie i Twoim pracownikom. Jak wspominaliśmy, na początek możesz dać im do przeczytania tego e-booka. Jeżeli czujesz, że to za mało (a prawdopodobnie masz rację), rozważ przeprowadzenie testów socjotechnicznych w swojej firmie.

Ile warte jest Twoje konto na Twitterze?

Do tej pory skupialiśmy się na zagrożeniach wynikających z wysokiego poziomu uprawnień, jakim dysponują właściciele firm i osoby piastujace wysokie stanowiska. Tymczasem to nie tylko dostęp do danych poufnych naraża przedsiębiorców na ataki. Dla cyberprzestępców równie cenny jest sam wizerunek ofiary. Doskonale wiedzą jak wykorzystać go dla swoich celów. Niedawno przekonali się o tym m.in. Barack Obama, Joe Biden, Jeff Bezos i Elon Musk.

O czym mowa? O najprawdopodobniej największym ataku w historii Twittera, do którego doszło w lipcu 2020. Konta Baracka Obamy, Joe Bidena, Jeff Bezosa i Elona Muska zostały przejęte przez hakerów. Cyberprzestępcy nie oszczędzili też kont firmowych, hakując między innymi konta należące do Apple, Uber czy Crash App. Po włamaniu, niektóre opublikowały komunikat o rzekomej akcji charytatywnej: „Wyślij pieniądze w bitcoinach na podany adres, a zwrócimy podwójną sumę! Akcja jest naszym sposobem na pomaganie społeczeństwu (m.in. w dobie COVID-19)".

Zrzut ekranu wiadomości opublikowanej na koncie Apple w ramach serwisu Twitter. Wariantów tej wiadomości było kilka. Tłumaczenie własne. Oryginalny tekst w Tweecie Baracka Obamy „I am giving back to the community due to Covid-19! All bitcoin sent to my address will be sent back doubled. If you send $1,000 I will send you back $2,000! [Adres bitcoina]. Only doing this for the next 30 minutes. Enjoy!".

Przejęcie 130 kont może nie zalicza się do największego ataku, jeśli chodzi o rozmiar utraty danych lub wycieku haseł. Istotne natomiast jest to, że ofiarą ataku padły osoby i instytucje, których opinia wyrażona publicznie, może przyczynić się do wielkich skutków ekonomicznych lub geopolitycznych.

JAK DOSZŁO DO ATAKU

Twitter od dawna pozwala użytkownikom na uwierzytelnienie dwuetapowe (ang. two factor authentication). Mogłoby więc mogłoby się wydawać, że konta na tej platformie są rzetelnie zabezpieczone. Uwierzytelnienie dwuetapowe polega na weryfikacji logowania do konta poprzez drugie urządzenie, np. wprowadzając hasło z SMS-a wysłanego na wcześniej podany numer. W teorii uniemożliwia to łatwe przejęcie konta poprzez skompromitowanie np. jednego urządzenia i używanie hasła do wtórnego zalogowania się na innych.

Mimo to doszło do ataku, który podzielił świat cyberbezpieczeństwa na dwa obozy, o dwóch różnych teoriach co do tego, jak do niego doszło. Przyjrzyjmy się bliżej każdej z nich.

/ SPEKULACJE

Teoria 1.: SIM swap i atak socjotechniczny

Biorąc pod uwagę fakt, że telefon domyślnie służy jako narzędzie do ponownego potwierdzenia tożsamości użytkownika, celem hakerów jest przechwycenie przychodzących wiadomości SMS. Osiągnięcie tego celu jest technicznie bardzo trudne: wymaga specyficznej wiedzy o konteneryzacji i systemach Linux, namierzenia smartfona ofiary i (najczęściej) sprowokowanie jego właściciela do zainstalowania pliku zawierającego złośliwy kod.

Znacznie łatwiejszy jest atak socjotechniczny na firmę świadczącą usługi telefoniczne. Wystarczy poprosić operatora telefonii komórkowej o przekierowanie SMS-ów na inny telefon i… cel osiągnięty! Zabezpieczenie za pomocą weryfikacji dwuetapowej zostało złamane.

Choć wydawać by się mogło, że osiągnięcie tego celu u operatora byłoby trudne ze względu na liczne procedury związane z bezpieczeństwem danych, dużo kont Twittera pada ofiarą właśnie takiego typu ataku. Hakerzy zbierają informacje o swojej ofierze z różnych źródeł, m.in. z mediów społecznościowych, publikacji, wiadomości

i materiałów reklamowych. Czasami istnieje też możliwość zakupienia pewnego zbioru informacji – bazy danych o osobach, gdy są one celebrytami lub zajmują stanowiska eksponowane.

Uzbrojeni w wiedzę i możliwość szybkiego znalezienia dodatkowych informacji, hakerzy dzwonią lub piszą do operatora komórkowego z prośbą o zmianę numeru karty SIM, która obsługuje dany numer telefonu. Podczas rozmowy uwierzytelniają się przez poprawne odpowiadanie na pytania weryfikujące i tłumaczą, że właśnie zgubili swój smartfon i nie chcieliby stracić obecnego numeru telefonu. Operator, mając na uwadze dobro klienta, przychyla się do ich prośby. Numer telefonu zostaje przypisany do nowej karty SIM, którą posiada haker. Ten natomiast szybko resetuje hasła lub adresy mailowe kont, które mogłyby używać SMS-ów do potwierdzenia tożsamości. Gdzie to możliwe, wyłącza też dalszą weryfikację dwuetapową.

Naturalnie, ofiara takiego ataku dość szybko orientuje się, że jej numer telefonu został przypisany innej osobie – telefon po prostu przestaje działać. Niemniej, nawet jedna godzina to wystarczająca ilość czasu, aby dobrze zorganizowani hakerzy zmienili dane dostępu do kont – takich jak Twitter – na inne numery telefonu i inne adresy mailowe.

Teoria 2.: Insiderzy

Drugą metodą włamania się do kont jest zwykłe przekupstwo, o którym wspominaliśmy już w rozdziale o insiderach. ➤

W przypadku lipcowego przejęcia kont Twittera, nie brakowało zwolenników teorii, że mamy do czynienia z agentem wewnętrznym, który został przekupiony przez hakerów w celu udostępnienia loginu do wewnętrznego panelu administracyjnego Twittera. O takim stanie rzeczy mogły świadczyć liczne zrzuty ekranu, opublikowane przez grupę hakerską, przedstawiające coś, co Twitter nazywa Agent Tools lub Twitter Services UI (W związku z tym, że zrzuty ekranu przedstawiają wewnętrzne narzędzia pracowników Twittera, nie publikujemy ich tutaj). Używając panelu administracyjnego, należącego do pracownika Twittera, hakerzy z łatwością mogliby masowo przypisać konta do innych adresów mailowych lub ręcznie ustawić inny numer telefonu do weryfikacji dwuetapowej.

Lekko zmodyfikowana wersja tej teorii głosiła też, że winę ponosi pracownik Twittera, którego dane do logowania zostały wykorzystane przez hakerów — nieumyślnie stał się więc insiderem. Starannie przygotowane ataki socjotechniczne potrafią wprowadzić w błąd nawet osoby, które uważane są za autorytety w dziedzinie IT.

Przejdźmy jednak do najciekawszego — jaka jest prawda?

CAŁA PRAWDA O ATAKU

Rozwiązanie zagadki dostarczył sam Twitter, podając do wiadomości publicznej następujący komunikat:

> **„Osoby atakujące z powodzeniem manipulowały niewielką liczbą pracowników i wykorzystywały ich dane uwierzytelniające, aby uzyskać dostęp do wewnętrznych systemów Twittera, w tym przejść przez nasze dwuetapowe zabezpieczenia. Na razie wiemy, że uzyskali dostęp do narzędzi dostępnych tylko dla naszych wewnętrznych zespołów wsparcia”.**

Wychodzi więc na to, że (jak to zwykle bywa) obie strony miały odrobinę racji. Hakerzy sięgnęli po socjotechniki, jednak zamiast na pracownikach linii komórkowej, użyli ich na tych zatrudnionych przez samego Twittera. Tak czy siak — cyberprzestępcy dopięli swego.

Oto podsumowania ataku w kilku liczbach:

- Cyberprzestępcy zdobyli dostęp do **130 kont** z czego mieli możliwość resetowania haseł i publikowania tweetów na **45** z nich;
- W dniu incydentu giełda kryptowalut Coinbase powstrzymała około **1100 klientów** przed wysłaniem bitcoinów na konta hakerów;
- Około **14 użytkowników** giełdy przekazało łącznie mniej więcej **3 tysięcy dolarów** w bitcoinach na konta hakerów, zanim firma zdołała interweniować;
- Łącznie szacuje się, że przestępcom udało się wyłudzić ponad **100 tysięcy dolarów** (466 tysięcy złotych).

WNIOSEK?

Dbaj o bezpieczeństwo swoich kont w mediach społecznościowych! Choć cyberprzestępcy nie próżnują i co rusz wynajdują nowe podatności oraz metody ataku, wciąż warto ograniczać możliwe zagrożenia. W jaki sposób? Chociażby pogłębiając wiedzę o socjotechnikach, o których wspominaliśmy już w poprzednim rozdziale, ale też praktykując OPSEC — sposób umiejętnego dawkowania informacji dostępnych publicznie tak, aby nie ułatwiać przestępcy podszycia się pod Twój sposób komunikacji (zwróć uwagę jak spersonalizowane były tweety hakerów!). I to właśnie OPSEC będzie głównym tematem kolejnego rozdziału.

OPSEC, czyli sztuka ochrony danych według armii USA

Dostępność informacji w sieci jest dziś tak powszechna, że przy zaangażowaniu często niewielkich nakładów pracy, każdy z użytkowników Internetu, jest w stanie zebrać dowolną ich ilość. Osoby publiczne, menedżerowie wysokiego szczebla czy określone organizacje, nierzadko spotykają się z niechcianym zainteresowaniem, którego wolałyby uniknąć.

Zapewne skuteczną metodą ochrony prywatności byłoby całkowite nieujawnianie publicznie swojego wizerunku, informacji osobistych czy danych związanych z funkcjonowaniem i bieżącą działalnością. Nie każdy jednak chce lub może pozwolić sobie na dobrowolne wykluczenie z obiegu medialnego. Żyjemy w czasach, gdy obecność w mediach często decyduje o istnieniu i sukcesie, a jej brak z góry skazuje na niepowodzenie.

Stare powiedzenie mówi, że „pieniądze lubią ciszę" — i nie tylko one. Prywatność, a nawet (choć pozornie może brzmieć to zaskakująco) popularność, również za nią przepadają. Przekazując informacje o sobie do wiadomości publicznej, warto mieć na uwadze, że inni mogą wykorzystać je do własnych, często niekorzystnych dla nas, działań. Choć więc pozornie dzielenie się znaczną ilością informacji sprzyja budowaniu wizerunku i pomnażaniu majątku (przykładem są influencerzy, celebryci, eksperci wypowiadający się online itd.), jeśli ktoś wykorzysta je przeciwko nam, efekt będzie odwrotny.

Z tego rozdziału dowiesz się więcej o doktrynie OPSEC, czyli bezpieczeństwie operacji — procesie ochrony informacji i świadomego „dawkowania" ich na forum publicznym tak, by maksymalizować korzyści z wyjawiania danych informacji a minimalizować ryzyko utraty kontroli nad innymi.

CZYM JEST OPSEC?

Bezpieczeństwo operacji OPSEC (ang. operations security) to proces oceny i ochrony dostępnych publicznie danych na swój temat, które można zgrupować w celu uzyskania szerszego, logicznego obrazu.

OPSEC identyfikuje krytyczne informacje w celu ustalenia, czy działania podejmowane w dobrej wierze powinny być jawne lub pozostać ukryte, w celu uniknięcia ich użycia w nieprzyjaznym celu. Następnie określa, czy informacje uzyskane przez przeciwników mogą być dla nich przydatne i podejmuje działania, które eliminują lub ograniczają ich wykorzystanie.

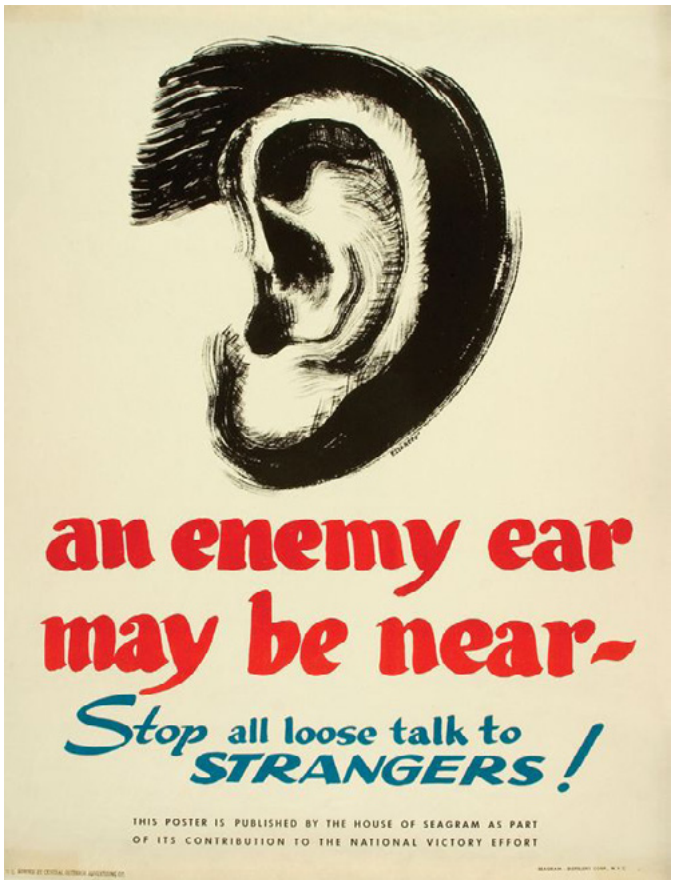
Proces ten skutkuje opracowaniem środków zaradczych, które obejmują metody techniczne i nietechniczne, takie jak:

- korzystanie z oprogramowania szyfrującego,
- zabezpieczanie się przed podsłuchem,
- zwracanie uwagi na udostępniane zdjęcia i elementy w tle,
- brak otwartych wypowiedzi w serwisach społecznościowych o informacjach poufnych, wrażliwych dla działalności osobistej lub biznesowej.

W erze powszechnego dostępu do Internetu, doktryna OPSEC stała się nieodłączną częścią życia instytucji rządowych, prywatnych przedsiębiorstw, jak i każdej osoby publicznej. Można wręcz posunąć się do oceny, że każda organizacja powinna zastanowić się, jakie kroki może podjąć, aby poprawić swoją postawę w kwestii chronienia informacji o sobie.

OPSEC zakłada, że jeśli ktoś wyszukuje informacji na mój temat, to ja powinienem zadbać, aby je otrzymał, ale w takim zakresie, na jaki świadomie pozwolę lub nawet, jaki będę chciał drugiej stronie pokazać (w kontekście: zmanipulować, by myślała, że informacje, które otrzymuje, są tym czego poszukuje, gdy w rzeczywistości są one fałszywe lub celowo wprowadzają w błąd).

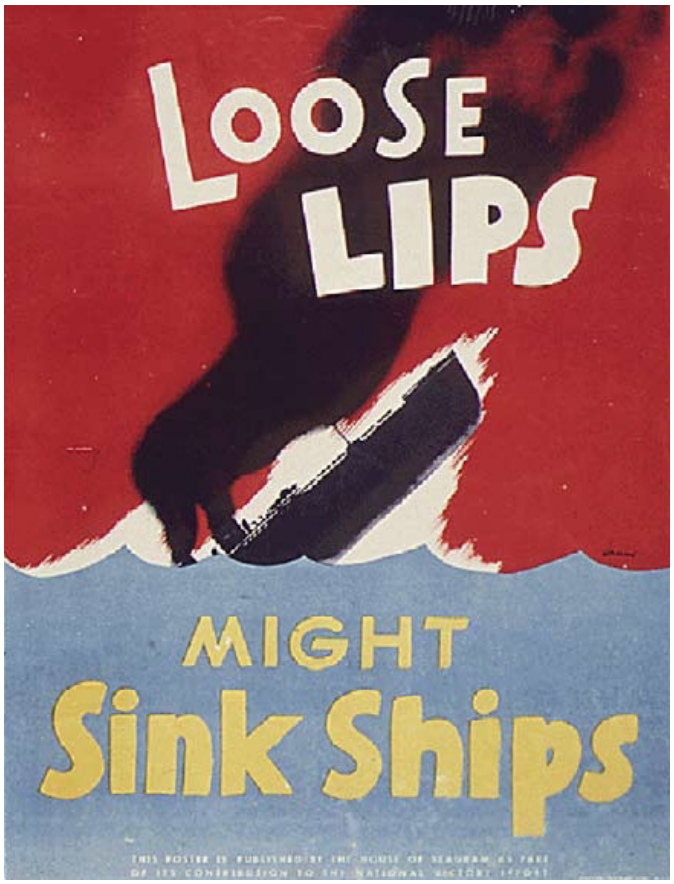
TROCHĘ HISTORII – SKĄD TO SIĘ WZIĘŁO?



Termin „operations security" został po raz pierwszy użyty w armii Stanów Zjednoczonych podczas wojny w Wietnamie. W 1966 r. admirał Stanów Zjednoczonych Ulysses Sharp powołał zespół ds. bezpieczeństwa w celu zbadania niepowodzenia niektórych operacji bojowych. Operacja ta została nazwana Operacją Purpurowy Smok (ang. Operation Purple Dragon) i obejmowała personel Agencji Bezpieczeństwa Narodowego (NSA) i Departamentu Obrony.

W wyniku wysiłków prowadzonych przez zespół Purple Dragon, zwrócono uwagę, że wróg był w stanie przewidzieć strategię i taktykę działań armii USA. Wojsko było pewne, że przeciwnikowi nie udało się odszyfrować amerykańskiej komunikacji i nie dysponowano zasobami wywiadowczymi, które mogłyby gromadzić dane od wewnątrz. Wniosek był taki, że to siły USA nieumyślnie ujawniły wrogowi istotne informacje. Na tej podstawie zespół Purple Dragon opracował pierwszą definicję militarną, będącą prekursorem OPSEC: „zdolność do trzymania wiedzy o naszych mocnych i słabych stronach z dala od wrogich sił".

Po zakończeniu operacji zespół Purple Dragon usystematyzował swoje rekomendacje oraz nadał im oficjalną nazwę OPSEC — Operations Security.
Z biegiem czasu koncepcja spotkała się z szerokim zainteresowaniem i rozprzestrzeniła się z US Army na inne departamenty rządowe oraz przemysł prywatny. Przyjęła się do tego stopnia, że została rozwinięta i dopracowana bardziej szczegółowo, jako jeden z procesów zarządzania bezpieczeństwem.



Z ciekawostek warto jeszcze dodać, że Amerykański Departament Energii, który odpowiada za nadzór nad arsenałem i gospodarką nuklearną kraju, opracował własną definicję OPSEC, która brzmi następująco: „Bezpieczeństwo operacji obejmuje proces określania niesklasyfikowanych lub kontrolowanych informacji krytycznych, które mogą być wskaźnikiem lub drogą do informacji niejawnych wymagających ochrony, niezależnie od tego, czy przez czas ograniczony lub dłuższy".

JAK PRZEPROWADZIĆ ANALIZĘ OPSEC

Analizę OPSEC przeprowadza się w celu oceny zdolności drugiej strony (zazwyczaj o wrogich zamiarach) do uzyskania dostępu do Twoich kluczowych informacji, własności intelektualnych, informacji zastrzeżonych lub danych osobowych. Takie analizy przynoszą bezpośrednie korzyści wszystkim, którzy chcą chronić informacje lub aktywa przed ujawnieniem. Oceny bezpieczeństwa operacji umożliwiają wgląd w przewidywalne wskaźniki, możliwe do wykorzystania procesy i procedury, a jednocześnie przedstawiają konkretne środki przeciwdziałania potencjalnym podatnościom. Oceny mogą być przeprowadzane przez wewnętrznych przedstawicieli z każdego działu lub przez ekspertów zewnętrznych. Zwykle trwają od 1 do 3 tygodni.

Armia Stanów Zjednoczonych ustanowiła pięciostopniowy proces, którego założeniem jest pomoc organizacji w identyfikowaniu informacji wymagających ochrony i środków ich zabezpieczenia. Dzięki niemu, w sposób ustrukturyzowany i normatywny, organizacje mogą oceniać swoje dane i infrastrukturę, by opracowywać plan ich ochrony. Przejdźmy zatem do opisu i wyjaśnienia kolejnych kroków.

1. IDENTYFIKACJA KRYTYCZNYCH INFORMACJI

Krytyczna informacja to informacja, którą przekazujesz w dobrej wierze, mając przyjazne zamiary, zdolności i działania (ang. Capabilities, Activities, Limitations, Intentions), jednak której znajomość pozwala przeciwnikowi zrealizować czynności destabilizujące twoje funkcjonowanie. Musisz zacząć od ustalenia, które dane, jeśli trafią w posiadanie lub zostaną udostępnione przez przeciwnika, wyrządzą szkodę Tobie lub organizacji.

Dane te mogą obejmować:

- informacje od klientów,
- dane finansowe,
- własność intelektualną,
- wewnętrzne dane organizacyjne,
- szczegóły dotyczące środków bezpieczeństwa,
- plany logistyczne,
- wyniki finansowe,
- dane osobowe
- itp.

Są to również wszelkie informacje udostępniane za pomocą mediów społecznościowych, publikowane oferty zatrudnienia czy ogłoszenia o starcie w przetargach.

Rozporządzenie US Army nr 530-1 dzieli informacje krytyczne na cztery kategorie, określane skrótem CALI (ang. Capabilities, Activities, Limitations, Intentions), co w tłumaczeniu oznacza: możliwości, działania, ograniczenia (w tym podatności na zagrożenia) i intencje.

Dzięki wykonaniu identyfikacji informacji krytycznych powstaje lista, która pozwala danej organizacji skoncentrować zasoby na istotnych elementach niejawnych, zamiast próbować chronić wszystkie publicznie dostępne informacje.

2. ANALIZA ZAGROŻEŃ

Zagrożenie pochodzi od przeciwnika,
a im bardziej zdeterminowany jest przeciwnik i im wyższe są jego zdolności, tym większe stanowi zagrożenie.

Pytaniem, które należy sobie zadać, jest: kim są nasi przeciwnicy? Mogą to być zarówno hakerzy, stalkerzy, porywacze, jak i konkurenci biznesowi. Pamiętaj, że różni wrogowie mogą celować w różne dane! W celu zidentyfikowania prawdopodobnych przeciwników i ustalenia stopnia zagrożenia wykorzystuje się wiele źródeł zależnych od kontekstu, takich jak: działania wywiadowcze, działalność organów ścigania i agencji detektywistycznych, jak również testy penetracyjne, mające ujawnić słabe punkty i błędy bezpieczeństwa oprogramowania.

3. ANALIZA PODATNOŚCI

W ramach analizy podatności weryfikujemy informacje, jakie planujemy udostępnić publicznie, w celu zidentyfikowania wektorów zagrożenia, mogących ujawnić dane krytyczne, a następnie porównujemy wyniki z możliwościami gromadzenia danych zidentyfikowanych w punkcie drugim przez przeciwnika. Zagrożenie traktujemy jako siłę przeciwnika, natomiast podatność jako wrażliwy element publikowanych informacji.

Przeprowadzenie pełnego audytu bezpieczeństwa w celu ujawnienia słabych punktów to kluczowy krok, dla zachowania bezpieczeństwa każdej organizacji.

4. OCENA RYZYKA

Na tym etapie analizowane są luki zidentyfikowane w punktach drugim i trzecim, by móc określić możliwe środki zapobiegawcze odrębnie dla każdej z nich.

Na podstawie oceny ryzyka, wykonanej w zależności od obszaru działania przez kierownictwo, przeszkolony personel lub samodzielnie, wybierane są do wprowadzenia konkretne środki bezpieczeństwa.

Ryzyko obliczane jest na podstawie prawdopodobieństwa ujawnienia krytycznych informacji i jego ewentualnych skutków. Prawdopodobieństwo, podobnie jak w punkcie trzecim, dzieli się na poziom zagrożenia i poziom podatności.

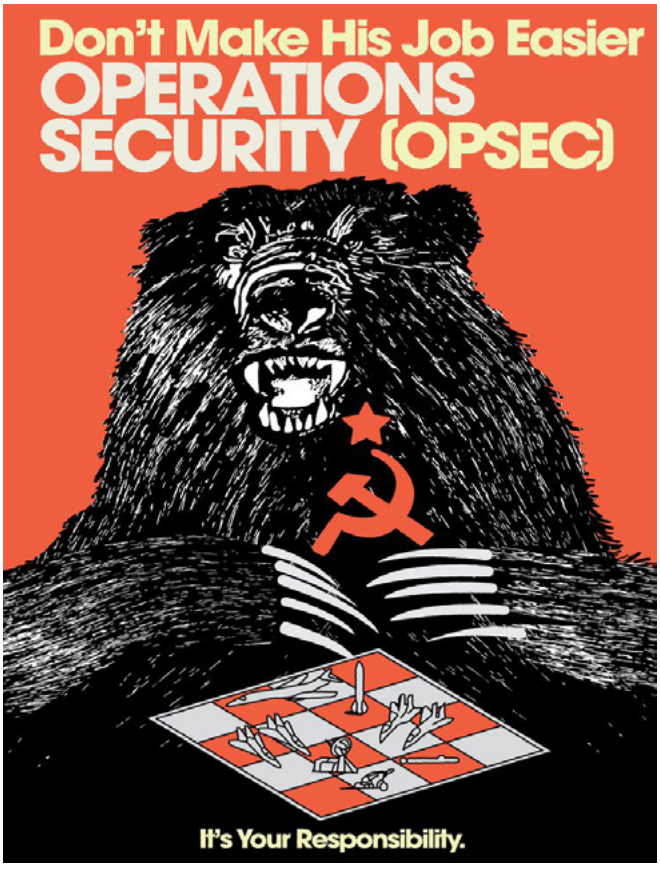
Podstawową zasadą podziału jest reguła, że prawdopodobieństwo wystąpienia zagrożenia jest najwyższe, gdy przeciwnik cechuje się silnym zamiarem i zdolnością realizacji dedykowanego ataku, przy zachowanym wysokim stopniu otwartości organizacji lub osoby narażonej wobec otoczenia.

Dochodzi tutaj do sytuacji, gdy publikując informacje w dobrej wierze, organizacja lub osoba prywatna staje się ofiarą, gdyż atakujący wykorzystuje je z wrogim zamiarem. Należy oszacować i dowiedzieć się, jakie jest prawdopodobieństwo ataku oraz ile szkód może wyrządzić ktoś wykorzystujący podatności.

5. OPRACOWANIE PLANU I ZASTOSOWANIE ODPOWIEDNICH ŚRODKÓW

Mając zebrane w poprzednich czterech punktach wszystkie istotne informacje, kolejnym krokiem jest stworzenie planu eliminacji luk i zapewniania bezpieczeństwa danych. Plan ten wdraża środki zaradcze wybrane do oceny działań związanych z ryzykiem lub w przypadku planowanych przyszłych operacji, obejmuje środki określone według harmonogramu. Środki zaradcze, aby zapewnić stałą ochronę bieżących informacji przed odpowiednimi zagrożeniami, muszą być regularnie monitorowane.

Ostatnim elementem opracowania planu jest formalna ocena wdrożenia procesu wobec zachodzących potrzeb. Warto zaangażować w tym celu zespół ekspertów. Oceny określają wymagania co do nakładów dodatkowych środków i wymaganych zmian w istniejących procedurach. Ponadto, osoby odpowiedzialne za wdrożenie, ściśle współpracując z personelem organizacji, muszą zdefiniować i opracować elementy przyjaznych informacji, stosowane w celu zapobiegania nieumyślnemu ujawnieniu w przyszłości informacji krytycznych lub wrażliwych.



Odniesienie definiujące środki zaradcze w kategorii kontroli działań opisuje wspomniane uprzednio rozporządzenie armii Stanów Zjednoczonych nr 530-1: „Środki zaradcze oraz kontranaliza, jako narzędzia pomagające profesjonaliście bezpieczeństwa operacji w ochronie krytycznych informacji".

DOBRE PRAKTYKI I ŚRODKI BEZPIECZEŃSTWA WEDŁUG OPSEC

Mamy już za sobą techniczną część procesu OPSEC, która dla części czytelników może wydawać się mocno abstrakcyjna i trudna do przyswojenia. Przejdźmy zatem do elementów, które w największym stopniu dotyczą każdego z nas, zarówno w biznesie, jak i prywatnie.

W poniższym akapicie przedstawimy elementy, na które należy zwracać uwagę w planowaniu i realizacji codziennych działań w publicznej przestrzeni cyfrowej. Znajdziesz tutaj szereg dobrych praktyk i środków zapobiegawczych, jakie warto stosować dla własnego bezpieczeństwa lub umiejętnie wykorzystywać je, by odbiorca otrzymywał tylko takie informacje, na jakich nam zależy.

Poniższe rady dość szczegółowo opisują problematykę przeciwdziałania zagrożeniu. Jej zakres jest jednak tak szeroki, że trudno jest mi wyczerpać go w całości. Zalecenia odnoszą się tylko do opisywanego szczególnego rodzaju ryzyka, jakim jest obszar biznesowo-prywatny. Nie wszystkie elementy będą możliwe do wdrożenia w każdej sytuacji, jednak im więcej punktów uda Ci się zrealizować, tym wyższy będzie poziom bezpieczeństwa i kultury OPSEC w Twoim środowisku. Miej na uwadze, by nie traktować poniższych wytycznych, jako uniwersalnego rozwiązania w każdej sytuacji. Warto byś analizował swoją indywidualną sytuację i wyszukiwał nowych potencjalnych podatności, które warto eliminować.

01. **Zanim udostępnisz publicznie jakieś informacje, zadaj sobie pytanie, czy powinny się one tam znaleźć.** Zwracaj uwagę na treści publikowane w social media: czy Twój profil nie ukazuje informacji zbyt osobistych, czy nie przedstawia niejawnych informacji zawodowych, czy w tle zdjęć nie znajdują się nieodpowiednich treści, czy nie publikujesz danych wrażliwych lub innych informacji, które nie powinny trafić do sieci. Pamiętaj o starej zasadzie: „co pojawia się w Internecie, już tam zostaje";

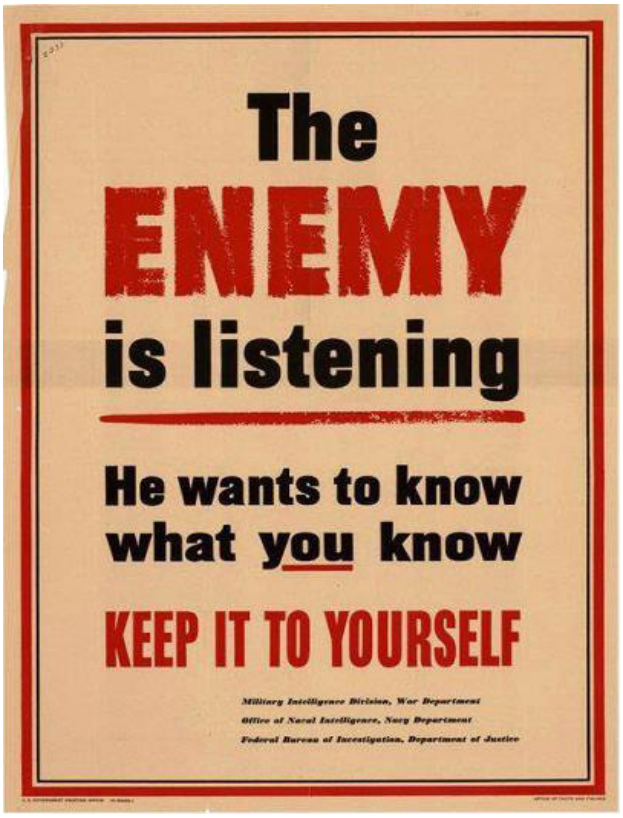
02, **Jeśli to możliwe nie łącz życia prywatnego z zawodowym** i nie chwal się każdemu, co robisz w pracy: z pozoru nieistotne opowieści mogą między wierszami zawierać niejawne, strategiczne lub bardzo osobiste informacje, które nie powinny być przekazywane. Trzymaj się zasady „prywatne – prywatne, służbowe – służbowe". Nie wykorzystuj infrastruktury i urządzeń służbowych w celach prywatnych i odwrotnie, nie używaj prywatnego sprzętu w pracy. W trakcie pracy nie korzystaj z firmowej sieci w celach prywatnych: przede wszystkim nie loguj się w mediach społecznościowych, a jeśli musisz — wyloguj się wcześniej z kont służbowych;

03. **Przeglądarkę internetową uruchamiaj z „czystym" profilem:** używaj trybu prywatnego incognito (według zapewnień producentów nie zapisuje on historii przeglądania stron i nie gromadzi plików cookies), dla pewności po skończonej pracy wyczyść pamięć cache — to samo wykonaj przed kolejnym użyciem przeglądarki, jeśli nie masz pewności, czy nie byłeś jedynym użytkownikiem komputera;

04. **Kontroluj zawartość swoich mediów społecznościowych.** Najlepiej, gdyby profil nie posiadał żadnej historii, wszelka aktywność, jak zdjęcia, polubienia i komentarze były na bieżąco monitorowane, a te, które z czasem uznasz za niewarte dzielenia się z szerszą publicznością — usuwane. Unikaj oznaczania lokalizacji i powiązań rodzinnych. Usuwaj metadane z publikowanych zdjęć;

05. **Zakładaj konta tylko tam, gdzie jest to konieczne.** Jeśli jest taka możliwość, przy rejestracji i użytkowaniu podawaj jak najmniej prawdziwych informacji. Usuń zasoby sieciowe, które nie są Ci już potrzebne;

06. **Używaj oprogramowania VPN, aby ukryć swój adres IP.** Jeśli wyszukujesz lub publikujesz informacje, co do których zależy Ci na anonimowości lub by były odczytane wyłącznie przez określoną grupę odbiorców, nigdy nie podejmuj takich akcji, korzystając z adresu IP, który wskazuje Twoje miejsce pracy, pobytu czy zamieszkania;



07. **Bezwzględnie stosuj się do polityki bezpieczeństwa obowiązującej w Twojej firmie:** jeśli jednoznacznie zabrania ona korzystania z urządzeń prywatnych, to ich nie używaj; jeśli firma funkcjonuje na zasadach BYOD (ang. bring your own device), to przestrzegaj zasad bezpieczeństwa, jakich wymaga od Ciebie dział techniczny;

08. **Jeśli przebywasz na terenie infrastruktury, której obszar nie jest powszechnie jawny, nie używaj urządzeń stosujących funkcję geolokalizacji,** np. telefonu komórkowego z włączoną lokalizacją, smartwatchy, smartbandów, urządzeń GPS. Zwróć uwagę, jakie dane lokalizacyjne przekazuje pojazd, którym się poruszasz;

09. **Powstrzymaj się przed publikowaniem w emocjach,** zwłaszcza jeśli używałeś substancji zmieniających postrzeganie rzeczywistości, jak alkohol czy narkotyki — wtedy najlepiej całkowicie powstrzymaj się od aktywności w mediach publicznych, nic nie komentuj i nie publikuj;

10. Jeśli odpowiadasz za zarządzanie infrastrukturą firmowej sieci, to **stosuj metodę ograniczania dostępu do urządzeń sieciowych** na zasadzie „najpierw się zapoznaj, potem korzystaj". W praktyce oznacza to, że zanim użytkownik otrzyma dostęp do pewnych zasobów, powinien zapoznać się z procedurą lub instrukcją bezpiecznego ich wykorzystania. Stosuj metodę zapewnienia pracownikom minimalnego niezbędnego dostępu do zasobów i przestrzegaj zasady utrzymywania jak najmniejszych uprawnień;

11. **Przeszkol swoich pracowników** w zakresie dobrych praktyk oraz obsługi urządzeń szyfrujących i monitorujących transfer danych;

12. **Zadbaj, by sposób myślenia Twój i ludzi, z którymi współpracujesz, był zgodny z regułami OPSEC.** Postaraj się, aby w Twojej organizacji OPSEC nie funkcjonował jako abstrakcyjny, niewygodny twór, tylko był czymś naturalnym i zrozumiałym. Uświadom swoich ludzi, gdzie znajduje się granica pomiędzy tematami, o których można się swobodnie wypowiadać na zewnątrz firmy, a co jest kategorycznie zabronione. Świadomość personelu, w jakim zakresie obiegu informacji mogą się poruszać, jest niezwykle istotna;

13. **Automatyzuj, gdzie się da.** Jeśli pewne procesy da się zautomatyzować, to warto wdrożyć takie rozwiązanie: pozwoli ono uniknąć ingerencji słabego ogniwa, jakim jest człowiek.

CENNE WSKAZÓWKI

01. Pamiętaj, jeśli tworzysz regulacje OPSEC w swojej organizacji, procedura ta powinna być jawna wobec wszystkich zainteresowanych. Ci, którzy wiedzą, czego strzec, mają większą szansę na ochronę poufnych informacji w przeciwieństwie do osób nieświadomych ich wartości.

02. W pierwszej kolejności skup się na ochronie zasobów, które nie zostały jeszcze ujawnione.

03. Staraj się bazować na wiedzy eksperckiej. Z pewnością część zagrożeń już analizowano i nie ma potrzeby tworzyć całej procedury od podstaw. Zamiast tracić czas i zasoby na samodzielnie przeprowadzane analizy, postaraj się uzyskać dane o zagrożeniach od ekspertów.

04. Proces bezpieczeństwa informacji włącz do procesów planowania i podejmowania decyzji. Jeśli opracowujesz strategię nowego projektu i dysponujesz czasem, nie czekaj na ostatnią chwilę – planuj OPSEC od początku, równolegle z pozostałymi stadiami rozwoju.

05. OPSEC, to nieprzerwany proces, którego przebieg i skala efektywności powinny być mierzalne.

06. Chcąc osiągnąć wyższy poziom kontroli i dopasowywać proces do zmiennych warunków, przeprowadzaj regularne oceny efektywności programu i pozwalaj mu na ewolucję.

07. OPSEC, jest często najtańszym rozwiązaniem w porównaniu z drogimi technologiami, które należałoby wdrożyć, chcąc osiągnąć podobny poziom bezpieczeństwa.

08. Procedurę bezpieczeństwa operacji należy zawsze stosować w zgodzie z porządkiem prawnym i standardami etycznymi.

OPSEC ALARM! PRZYPADKI BŁĘDÓW, GDY PROCEDURA ZAWIODŁA

Życie często pokazuje, że nic nie uczy tak dobrze, jak cudze lub własne błędy. Niestety wielu ludzi, dopóki nie uświadomi sobie zagrożenia na przykładzie rzeczywistych przypadków, nie jest w stanie racjonalnie zrozumieć, a tym bardziej zastosować pewnych rozwiązań — zwłaszcza takich, które ograniczają swobodę działań. Przykładowo, z entuzjazmem zarejestrujemy się w nowym portalu społecznościowym, niestety
z mniejszym entuzjazmem zastosujemy się do wymagań posiadania skomplikowanego hasła i jego regularnej zmiany, weryfikacji dwuetapowej z podaniem numeru telefonu czy kolejnego potwierdzenia captcha, że nie jesteśmy robotem.

Chcąc ułatwić zrozumienie, jak ważne jest wdrożenie i stosowanie procedury OPSEC, przedstawię poniżej kilka przykładów z życia, ukazujących konsekwencje braku przestrzegania podstawowej higieny bezpieczeństwa informacji.

CASE STUDY

ZIELONE LUDZIKI

Według oficjalnego przekazu medialnego, rząd w Moskwie zaprzecza, aby na terenie wschodniej Ukrainy, stacjonowały rosyjskie wojska. Wielokrotnie jednak udowodniono, iż nie jest to prawda. Świadczy o tym m.in. szereg incydentów nieuważnego ujawnienia przez rosyjskich żołnierzy własnych danych geolokalizacyjnych podczas oznaczania lokalizacji w mediach społecznościowych. Publikowane w taki sposób zdjęcia ukazywały dokładną lokalizację żołnierza – w tym stronę granicy, po której się znajduje.

CASE STUDY

UJAWNIENIE KONTA SZEFA FBI

Podczas wywiadu w telewizji, brak czujności ze strony szefa FBI — Jamesa Comeya, przyczyniła się do namierzenia jego tajnego konta w social media. Podczas wystąpienia telewizyjnego, Comey przyznał się, że korzysta z anonimowego konta na Twitterze i Instagramie, które ma 9 osób obserwujących. Już te szczątkowe informacje wystarczyły oglądającej program dziennikarce, Ashley Feinberg, do namierzenia członków rodziny Comeya. Następnie poprzez analizę wzajemnych relacji pomiędzy kontami użytkowników, odnalazła właściwe konto szefa FBI, które faktycznie posiadało 9 obserwujących. Jako uzasadnienie swojej tezy dziennikarka uznała, że nazwa profilu ‚reinholdniebuhr' jest taka sama, jak postać teologa Reinholda Niebuhra, o którym James Comey pisał pracę w trakcie studiów. Jako kolejny krok, pozostało już tylko przeszukać Twitter pod kątem występowania fraz z nazwiskiem teologa, by w wynikach odnaleźć konto @projectexile7, będące własnością Comeya.

CASE STUDY

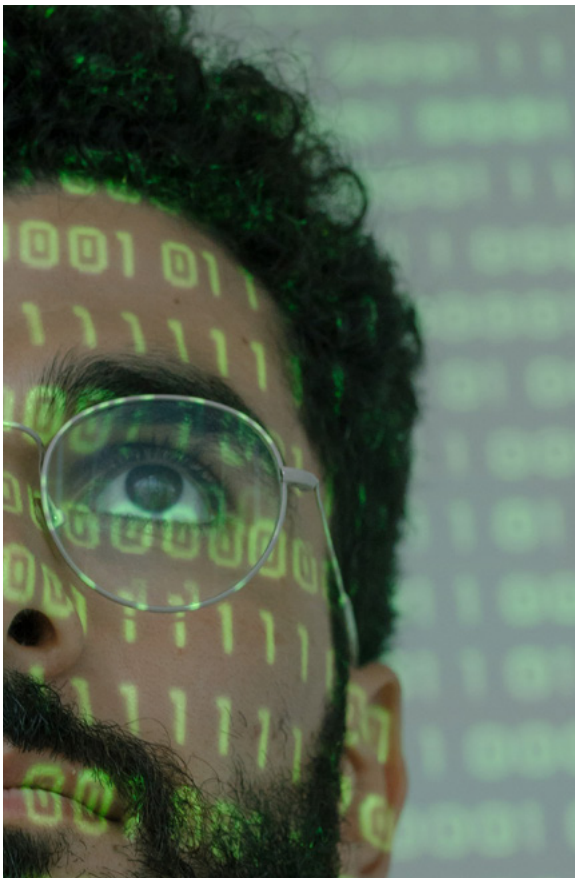
APLIKACJE TRENINGOWE DLA BIEGACZY

Kilka lat temu głośno było o aplikacjach monitorujących aktywność fizyczną: Strava i Endomondo. W oparciu o rejestr lokalizacji urządzeń posiadających zainstalowaną jedną z tych aplikacji można było wyśledzić wizualizacje tras, którymi biegają ich użytkownicy. Okazało się, że obie aplikacje cieszą się sporą popularnością wśród żołnierzy. Ci biegając na terenie swoich baz, nieświadomie publikowali za pośrednictwem aplikacji wyniki przebiegu trasy i dokładną lokalizację. W efekcie, niepozorne i odludne punkty na mapach, w tym obszary pustynne czy gęsto zalesione, okazywały się popularnymi miejscami aktywności sportowych. Dla osób, zorientowanych w celu poszukiwań, był to jasny znak, że w danym miejscu może znajdować się tajny obiekt militarny.

KILKA SŁÓW NA ZAKOŃCZENIE

Wysoki poziom determinacji, posiadanie pewnej wiedzy i umiejętność konsolidowania jej źródeł (tutaj: dane lokalizacyjne, mapa satelitarna, wiedza, że osoba wykonuje określoną funkcję zawodową) ukazują, jak agregacja pozornie nieistotnych szczątków informacji, może pozwolić zbudować klarowny obraz celu. Co istotne, nawet osoby zawodowo związane z bezpieczeństwem mogą nie być świadome pozostawianych śladów. Wobec powyższych przykładów warto również zwrócić uwagę na niski koszt zaangażowanych nakładów – większość informacji cel dostarczył samodzielnie, a rola atakującego wymagała jedynie sprytu i poświęcenia kilku minut, by połączyć elementy układanki.

Pamiętajmy zatem o słynnym powiedzeniu z czasów II Wojny Światowej: „Luźne usta mogą zatopić statki" (ang. „Loose lips might sink ships"). Pojawiało się ono na plakatach propagandowych i ostrzegać miało obywateli, by nie otwierali się nadmiernie podczas rozmów z innymi ludźmi. W ten sposób starano się zapobiegać szerzeniu plotek i informacji, które mogły przedostać się na stronę przeciwnika, by zostać wrogo użyte. Podobnie, jak w opisanej historii zbyt rozmowne usta rozpowszechniały plotki, tak dziś rolę ust w cyfrowym świecie pełnią media społecznościowe. Pamiętaj: zanim zamieścisz coś w internecie, zadaj sobie to kluczowe pytanie: czy na pewno powinno się to tam znaleźć?



Na koniec

Przelew na rachunek bankowy przestępców, wykonany bez mrugnięcia okiem, gdy tylko w słuchawce zabrzmiał znajomy głos szefa. Milion dolarów za zainfekowanie sieci firmowej Tesli. Żołnierze zdradzający swoją pozycję za pomocą aplikacji do mierzenia efektywności treningów.

Przykłady cyber-wpadek można mnożyć – ale lepiej ich nie powielać! Mamy nadzieję, że wyciągnąłeś wnioski z historii opisanych w tym e-booku i dzięki niemu pozostaniesz silnym ogniwem łańcucha cyberbezpieczeństwa w swojej firmie.

Powodzenia i – zostań bezpieczny!

O Digital Innovation Hub

Digital Innovation Hub (pełna nazwa: **Digital Innovation Hub Technologiczna Fabryka Ucząca dla Przemysłu Przyszłości**) to polska inicjatywa, wspierana przez Ministerstwo Rozwoju. Jej celem jest pomoc przedsiębiorstwom w podnoszeniu konkurencyjności rynkowej przez zastosowanie innowacyjnych rozwiązań przemysłu 4.0.

W skład Konsorcjum Digital Innovation Hub wchodzą: TestArmy Group S.A, Politechnika Wrocławska, Uniwersytet Ekonomiczny, Wrocławski Park Technologiczny i firma Balluff. Organizacje wspólnymi siłami wygrały ogólnopolski konkurs „Standaryzacja usług Hubów Innowacji Cyfrowych dla wsparcia cyfrowej transformacji przedsiębiorstw".

Konsorcjanci realizują cele Digital Innovation Hub: oferują firmom w swoim regionie kompleksowy dostęp do najnowszej wiedzy, doświadczenia i technologii. Wspomagają także przedsiębiorców w dostępie do finansowania przedsięwzięć dla transformacji cyfrowej.

W TestArmy, jako część Konsorcjum, odpowiadamy za sektor cyberbezpieczeństwa, automatyzacji i robotyki oraz IoT w projekcie. To właśnie dlatego powstała ta publikacja!

LEVEL 4.0 Digital Innovation Hub Wrocław

Politechnika Wrocławska · Uniwersytet Ekonomiczny we Wrocławiu · WPT Wrocławski Park Technologiczny · BALLUFF

Potrzebujesz wsparcia w cyberbezpieczeństwie?

Skontaktuj się z nami

SZYMON CHRUŚCICKI

BUSINESS DEVELOPMENT DIRECTOR

t: +48 505 372 810

e: szymon.chruscicki@testarmy.com

TestArmy CyberForces Sp. z o.o.

ul. Petuniowa 9/5

53-238 Wrocław