

Cyberbezpieczeństwo dla zaawansowanych

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

```
selector = undefined;  
( fn == null ) {  
  if selector == "string" {  
    s, selector, fn )  
  }  
  defined:  
  s, selector, fn )
```

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

Copyright © Packt Publishing 2022. First published in the English language under the title 'Mastering Defensive Security – (9781800208162)'.

Polish edition copyright © 2023 by Helion S.A.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

O autorze	15
O recenzentach	16
Przedmowa	17
Wstęp	19

Część I. Doskonalenie technik obrony. Podstawy teoretyczne

Rozdział 1. Przypomnienie pojęć związanych z cyberbezpieczeństwem	25
Wymagania techniczne	26
Nurkujemy w samo sedno cyberbezpieczeństwa	26
Triada cyberbezpieczeństwa	26
Rodzaje ataków	28
Zarządzanie legendarnym słabym punktem w cyberbezpieczeństwie — hasła	36
Zdekonspirowane hasła	36
Ataki inżynierii społecznej z wykorzystaniem wykradzionych haseł	38
Ataki siłowe	39
Ataki słownikowe	40
Tworzenie bezpiecznego hasła	41
Zarządzanie hasłami na poziomie przedsiębiorstwa	43
Dodatek	45
Doskonalenie obrony w głąb	46
Czynniki, które należy wziąć pod uwagę przy tworzeniu modeli DiD	46
Identyfikacja aktywów	48
Obrona dzięki warstwom	49
Dodatek	53

Drużyny: niebieskich i czerwonych — porównanie	53
Podsumowanie	56
Lektura uzupełniająca	56
Rozdział 2. Zarządzanie zagrożeniami, podatności i ryzyko	57
Wymagania techniczne	58
Zrozumienie podatności i zagrożeń związanych z cyberbezpieczeństwem	58
Przeprowadzenie oceny podatności na zagrożenia	58
Proces oceny zagrożeń	59
Kiedy należy wykonać sprawdzenie pod kątem podatności?	61
Rodzaje podatności	61
Podatności w zabezpieczeniach USB HID	66
Rodzaje ataków USB HID	67
Fałszywe poczucie bezpieczeństwa	72
Ochrona przed atakami USB HID	75
Zarządzanie ryzykiem związanym z cyberbezpieczeństwem	78
Identyfikacja ryzyka	79
Ocena ryzyka	80
Reakcja na ryzyko	82
Monitorowanie ryzyka	83
Ramy cyberbezpieczeństwa NIST	84
Identyfikacja	84
Ochrona	84
Wykrywanie	84
Reakcja	85
Przywracanie	85
Tworzenie skutecznego planu ciągłości działania (BCP)	86
Tworzenie analizy wpływu na biznes (BIA)	87
Planowanie ciągłości działania (BCP)	91
Wdrażanie najlepszego w swojej klasie DRP	95
Tworzenie DRP	95
Wdrażanie DRP	96
Podsumowanie	98
Lektura uzupełniająca	98
Rozdział 3. Zasady, procedury, zgodność i audyty	100
Tworzenie światowej klasy zasad i procedur dotyczących cyberbezpieczeństwa	101
Zasady związane z cyberbezpieczeństwem	101
Procedury związane z cyberbezpieczeństwem	102
Metoda CUDSE	103
Zrozumienie i osiągnięcie zgodności	108
Rodzaje regulacji	108
Osiągnięcie zgodności	110
Eksplorowanie, tworzenie audytów i zarządzanie nimi	113
Wewnętrzne audyty cyberbezpieczeństwa	114
Zewnętrzne audyty bezpieczeństwa cybernetycznego	114
Zarządzanie danymi podczas audytów	115
Rodzaje audytów cyberbezpieczeństwa	117
Kiedy przeprowadzać audyt?	120

Zastosowanie CMM	120
Cele CMM	120
Charakterystyka dobrego CMM	120
Struktura dobrego CMM	121
Analizowanie rezultatów	123
Zalety CMM	124
Podsumowanie	125
Lektura uzupełniająca	125
Rozdział 4. Łatanie ósmej warstwy	126
Warstwa 8 — zagrożenie wewnętrzne	127
Działanie nieumyślne	127
Szkodliwy użytkownik	128
Jak rozpoznać wewnętrznego szkodnika?	129
Ochrona infrastruktury przed wewnętrznymi szkodnikami	130
Doskonalenie sztuki inżynierii społecznej	136
Przebieg ataku w inżynierii społecznej	137
Socjotechniki	138
Rodzaje ataków wykorzystujących inżynierię społeczną	140
Obrona przed atakami socjotechnicznymi (łatanie warstwy 8)	152
Tworzenie strategii szkoleń	153
Prawa administratora	153
Wdrożenie silnej zasady BYOD	154
Przeprowadzanie losowych ataków inżynierii społecznej	154
Podsumowanie	155
Lektura uzupełniająca	155
Rozdział 5. Technologie i narzędzia w cyberbezpieczeństwie	156
Wymagania techniczne	157
Zaawansowane narzędzia bezprzewodowe dla cyberbezpieczeństwa	157
Obrona przed atakami bezprzewodowymi	157
Narzędzia i metody testów penetracyjnych	163
Metasploit	163
Zestaw narzędzi do inżynierii społecznej	164
exe2hex	168
Stosowanie narzędzi i metod kryminalistycznych	168
Postępowanie z dowodami	169
Narzędzia kryminalistyczne	169
Odzyskiwanie skasowanych plików	173
Jak sobie radzić z APT?	174
Techniki obrony	175
Systemy inteligentnego wykrywania zagrożeń w podnoszeniu poziomu cyberbezpieczeństwa	176
Inteligentne wykrywanie zagrożeń — podstawy	176
Wdrażanie systemu inteligentnego wykrywania zagrożeń	177
Przekształcenie zagrożenia w rozwiązanie	178
Problem	179
Rozwiązanie	179
Podsumowanie	179
Lektura uzupełniająca	180

Część II. Obrona w praktyce

181

Rozdział 6. Zabezpieczanie infrastruktury działającej pod kontrolą systemów Windows

183

Wymagania techniczne	184
Utwardzanie systemu Windows w praktyce	184
Utwardzanie przez zespół ds. infrastruktury	184
Tworzenie listy kontrolnej dla procedur utwardzania	185
Tworzenie strategii instalowania łatek	190
Złożoność łatania	190
Rozdzielanie zadań (łatanie ról i przydziałów)	192
Dystrybucja i wdrażanie poprawek	193
Rodzaje łatek	195
Zabezpieczanie AD w praktyce	198
Bezpieczne hosty administracyjne	200
Dokumentacja dotycząca bezpieczeństwa systemu Windows Server	201
Zabezpieczanie końcówek — stacji roboczych	201
Aktualizacje systemu Windows	201
Dlaczego warto przejść na Windows 10?	201
Bezpieczeństwo fizyczne	202
Programy antywirusowe	203
Zapora ogniowa Windows Defender	203
Kontrola aplikacji	204
Filtrowanie adresów URL	204
Filtrowanie spamu	205
Systemy, do których ma dostęp klient	205
Kopie zapasowe	206
Użytkownicy	206
Zabezpieczanie danych	207
Wykorzystanie szyfrowania	207
Konfiguracja programu BitLocker	208
Podsumowanie	208

Rozdział 7. Utwardzanie serwera Unix

209

Wymagania techniczne	210
Zabezpieczanie usług uniksowych	210
Określ przeznaczenia serwera	210
Skonfiguruj bezpieczny rozruch	211
Zarządzanie usługami	211
Uprawnienia do plików w praktyce	215
Zrozumienie pojęcia „właściciel” i uprawnień	215
Domyślne uprawnienia	218
Uprawnienia w katalogach (folderach)	219
Zmiana domyślnych uprawnień za pomocą umask	220
Hierarchia uprawnień	221
Porównywanie uprawnień do katalogów	222
Zmiana uprawnień i własności pojedynczego pliku	222
Przydatne polecenia do wyszukiwania niechcianych uprawnień	223

Zwiększenie ochrony serwera poprzez ulepszenie kontroli dostępu	224
Przeglądanie ACL	224
Zarządzanie listami ACL	225
Domyślne ACL dla katalogów	225
Usuwanie list ACL	226
Rozszerzona kontrola dostępu	227
Konfiguracja zapory sieciowej	228
Zrozumieć iptables	228
Konfigurowanie iptables	229
Ochrona SSH przed atakami siłowymi przy użyciu iptables	232
Ochrona przed skanowaniem portów za pomocą iptables	233
Zaawansowane zarządzanie dziennikami	233
Wykorzystanie logów	234
Podsumowanie	235
Lektura uzupełniająca	235
Rozdział 8. Zwiększ swoje umiejętności obrony sieci	236
Wymagania techniczne	237
Wykorzystanie eksperckiego narzędzia mapowania sieci — Nmap	237
Fazy cyberataku	238
Nmap	239
Skrypty Nmap	242
Lepsza ochrona sieci bezprzewodowych	246
Podatności w zabezpieczeniach sieci bezprzewodowych	246
Instrukcja bezpieczeństwa użytkownika dla sieci bezprzewodowych	250
Wprowadzenie do programu Wireshark	255
Namierzanie użytkowników korzystających z niezabezpieczonych protokołów	258
FTP, HTTP i inny, nieszyfrowany ruch	263
Wykorzystanie Wiresharka do obrony	264
Praca z IPS i IDS	265
Co to jest IDS?	265
Co to jest IPS?	266
Bezpłatny system IDS/IPS	267
IPS a IDS	267
Podsumowanie	268
Rozdział 9. Nurkujemy w zabezpieczenia fizyczne	269
Wymagania techniczne	270
Zrozumienie zabezpieczeń fizycznych i związanych z nimi zagrożeń	270
Potężny LAN Turtle	270
Podstępny Plunder Bug LAN Tap	271
Niebezpieczny Packet Squirrel	272
Przenośny Shark Jack	273
Niesamowity Screen Crab	273
Zaawansowany Key Croc	275
Zagrożenia związane z USB	276
Kradzież sprzętu	277
Zagrożenia środowiskowe	278
Fizyczne mechanizmy zabezpieczeń	278

Doskonalenie zabezpieczeń fizycznych	280
Zasada czystego biurka	280
Przeglądy zabezpieczeń fizycznych	281
Podsumowanie	282
Lektura uzupełniająca	282

Rozdział 10. Zabezpieczenia IoT w praktyce **283**

Wymagania techniczne	284
Zrozumieć internet rzeczy	284
Ryzyko	285
Podatności	286
Zrozumienie technologii sieciowych w IoT	287
LoRaWAN	287
Zigbee	288
Sigfox	289
Bluetooth	290
Uwagi dotyczące bezpieczeństwa	291
Poprawa bezpieczeństwa IoT	292
Tworzenie sprzętu wspomagającego cyberbezpieczeństwo z wykorzystaniem IoT	295
Wykrywanie fałszywych punktów dostępu	295
Ściana ogniowa i system wykrywania włamań na Raspberry Pi	298
Systemy obrony dla przemysłowych systemów sterowania (SCADA)	299
Bezpieczne kopiowanie z USB na USB	299
Tworzenie przynęty za grosze	300
Zaawansowane monitorowanie aplikacji internetowych i sieci	302
Tworzenie urządzenia blokującego reklamy internetowe	303
Kontrola dostępu i systemy fizycznych zabezpieczeń	303
Dodatkowe informacje: niebezpieczeństwo związane z nieautoryzowanymi urządzeniami IoT	304
Wykrywanie nieautoryzowanych urządzeń IoT	304
Wykrywanie Raspberry Pi	304
Wyłączanie fałszywych urządzeń Raspberry Pi	305
Podsumowanie	306
Lektura uzupełniająca	306

Rozdział 11. Bezpieczne wytwarzanie i wdrażanie oprogramowania w środowisku chmury **307**

Wymagania techniczne	308
Bezpieczna implementacja i wdrożenie aplikacji w chmurze	308
Bezpieczeństwo w różnych modelach chmury	308
Bezpieczeństwo danych w chmurze	310
Zabezpieczanie Kubernetes i API	313
Zabezpieczenia typowe dla chmury	313
Kontrola dostępu do interfejsu API Kubernetes	314
Kontrola dostępu do kubeletu	314
Zapobieganie ładowaniu niepożądanych modułów jądra przez kontenery	314
Ograniczenie dostępu do etcd	315
W systemach produkcyjnych unikaj korzystania z funkcji będących w wersjach alfa lub beta	315
Integracje z elementami innych producentów	315

Zabezpieczanie usług baz danych	316
Testowanie bezpieczeństwa chmury	317
Centrum zabezpieczeń Azure	318
Amazon CloudWatch	318
AppDynamics	319
Nessus — skaner podatności	320
InsightVM	320
Intruder	321
Podsumowanie	322
Lektura uzupełniająca	322
 Rozdział 12. Bezpieczeństwo aplikacji internetowych	 323
Wymagania techniczne	324
Zbieranie informacji o Twojej witrynie/aplikacji internetowej	324
Znaczenie gromadzenia publicznie dostępnych danych	325
Wywiad z wykorzystaniem publicznie dostępnych źródeł	325
Informacje o hostingu	327
Sprawdzanie ekspozycji danych za pomocą Google hacking (dorki)	329
Wykorzystanie DVWA	331
Instalacja DVWA na Kali Linux	332
Przegląd najczęstszych ataków na aplikacje internetowe	336
Badanie ataków XSS	336
Korzystanie z pakietu Burp Suite	338
Wersje Burp Suite	338
Konfiguracja Burp Suite na Kali	339
Atak typu wstrzyknięcie SQL na DVWA	340
Naprawienie często występującego błędu	346
Atak siłowy na hasła w aplikacjach internetowych	347
Analiza wyników	350
Podsumowanie	351
Lektura uzupełniająca	352

Część III. Wyptywamy na szerokie wody obrony **353**

Rozdział 13. Narzędzia do oceny podatności	355
Wymagania techniczne	356
Radzenie sobie z podatnościami	356
Kto powinien szukać podatności?	356
Programy nagród za znalezione błędy	356
Wewnętrzne podatności	357
Narzędzia do badania podatności	358
Użycie skanera podatności (OpenVAS)	360
Testy z uwierzytelnieniem	360
Instalacja OpenVAS	361
Używanie OpenVAS	363
Aktualizowanie swoich kanałów	366

Skaner Nexpose	367
Podsumowanie	369
Lektura uzupełniająca	369
Rozdział 14. Analiza złośliwego oprogramowania	370
Wymagania techniczne	371
Dlaczego warto analizować złośliwe oprogramowanie?	371
Funkcjonalność złośliwego oprogramowania	371
Cele złośliwego oprogramowania	371
Z kim i z czym łączy się złośliwe oprogramowanie	372
Zostawianie furtek	373
Narażone systemy	373
Rodzaje i kategorie analizy złośliwego oprogramowania	373
Statyczna analiza złośliwego oprogramowania	373
Dynamiczna analiza złośliwego oprogramowania	374
Hybrydowa analiza złośliwego oprogramowania	374
Analiza właściwości statycznych	375
Interaktywna analiza zachowania	375
Analiza w pełni zautomatyzowana	375
Inżynieria wsteczna kodu	376
Najlepsze narzędzia do analizy złośliwego oprogramowania	376
Process Explorer	377
Process Monitor	377
ProcDOT	378
Ghidra	379
PeStudio	379
Przeprowadzanie analizy złośliwego oprogramowania	379
Zasady bezpieczeństwa	380
Przeprowadzamy analizę	381
Podsumowanie	384
Lektura uzupełniająca	384
Rozdział 15. Wykorzystanie testów penetracyjnych w taktykach obrony	385
Wymagania techniczne	386
Zrozumienie znaczenia dzienników	386
Pliki dzienników	386
Zarządzanie dziennikami	387
Dlaczego zadbanie o dzienniki jest ważne	388
Poznaj najlepszego przyjaciela swojego przeciwnika — Metasploit	389
Metasploit	390
Wersje frameworka Metasploit	391
Instalacja Armitage	391
Konfiguracja frameworka Metasploit po raz pierwszy	392
Instalacja Armitage (ciąg dalszy)	393
Eksploracja Armitage	394
Rozpoczęcie ataku z Armitage	396
Uruchamianie frameworka Metasploit	400

Inne hakerskie narzędzia do przeprowadzania ataków	403
Searchsploit	404
sqlmap	405
Weevely	405
Podsumowanie	409
Lektura uzupełniająca	410
Rozdział 16. Informatyka śledcza w praktyce	411
Wprowadzenie do kryminalistyki cyfrowej	412
Techniki śledcze w odzyskiwaniu usuniętych lub brakujących danych	412
Metody i techniki kryminalistyki cyfrowej w zabezpieczaniu infrastruktury	416
Kto powinien zajmować się cyfrową kryminalistyką?	416
Proces cyfrowej kryminalistyki	417
Platformy kryminalistyczne	418
CAINE	418
Stacja robocza SIFT	419
PALADIN	420
Znalezienie dowodów	421
Źródła danych	421
Kryminalistyka urządzeń mobilnych	422
Dochodzenie bez urządzenia	423
Ważne źródła danych na urządzeniach mobilnych	425
Transportowanie urządzeń mobilnych	426
Zarządzanie materiałem dowodowym (z perspektywy prawnej)	426
ISO 27037	427
Podręcznik polityki i procedur dotyczących dowodów cyfrowych	427
Przewodnik po polityce FBI dotyczącej dowodów cyfrowych	427
Regionalne Laboratorium Informatyki Śledczej	428
Amerykańska Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury	428
RFC 3227 — wytyczne dotyczące gromadzenia i archiwizacji dowodów	428
Podsumowanie	428
Lektura uzupełniająca	429
Rozdział 17. Automatyzacja zadań związanych z cyberbezpieczeństwem	430
Po co zwracać sobie głowę automatyzacją?	431
Korzyści z automatyzacji	431
Ryzyko związane z ignorowaniem automatyzacji	431
Rodzaje automatycznych ataków	432
Gromadzenie kont	432
Tworzenie kont	432
Oszustwo reklamowe	432
Porażka CAPTCHA	433
Rozszyfrowywanie kart	433
Carding	433
Wypłata gotówki	433
Łamanie danych uwierzytelniających	434
Faszerowanie danymi uwierzytelniającymi	434
Odmowa z magazynu	434

DoS	434
Przyspieszanie	435
Zbieranie odcisków palców	435
Tropienie	435
Scalping	436
Strzał z ukrycia	436
Zbieranie	436
Wypaczanie	436
Spamowanie	436
Rozgryzanie tokenów	437
Skanowanie podatności	437
Automatyzacja narzędzi cyberbezpieczeństwa z wykorzystaniem języka Python	437
Lokalne wyszukiwanie plików	437
Podstawowe zadania kryminalistyki cyfrowej	439
Zbieranie danych ze stron internetowych	441
Automatyzacja zabezpieczania sieci	442
Automatyzacja zadań związanych z cyberbezpieczeństwem z Raspberry Pi	443
Automatyzacja systemu inteligentnego zbierania informacji	
za pomocą przynęty Fail2ban na Raspberry Pi	444
Zautomatyzowany system monitorowania internetu za pomocą Raspberry Pi	445
Podsumowanie	447
Lektura uzupełniająca	447
Rozdział 18. Kompilacja narzędzi eksperta. Przydatne zasoby	448
Darmowe szablony dotyczące cyberbezpieczeństwa	449
Szablony planu ciągłości działania i planu odzyskiwania po awarii	449
Zarządzanie ryzykiem	449
Projektowanie i zarządzanie zasadami i procedurami dotyczącymi cyberbezpieczeństwa	450
Niezbędne zasoby internetowe	450
Mapy zagrożeń cybernetycznych lub ataków cyfrowych	451
Certyfikaty w dziedzinie cyberbezpieczeństwa	452
Wiadomości i blogi dotyczące cyberbezpieczeństwa	453
Narzędzia w cyberbezpieczeństwie	453
Narzędzia związane z hasłami	454
Wiodące najlepsze praktyki branżowe	454
Przepisy i normy	454
Ramy, standardy i inne elementy bezpieczeństwa cybernetycznego	455
Podsumowanie	456
Lektura uzupełniająca	456
Skorowidz	457

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 wyzwaniem 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.

Szkodliwi użytkownik

Najpierw spróbujemy 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 strategię 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 *popelnianym przez lekkomyślnych użytkowników*.

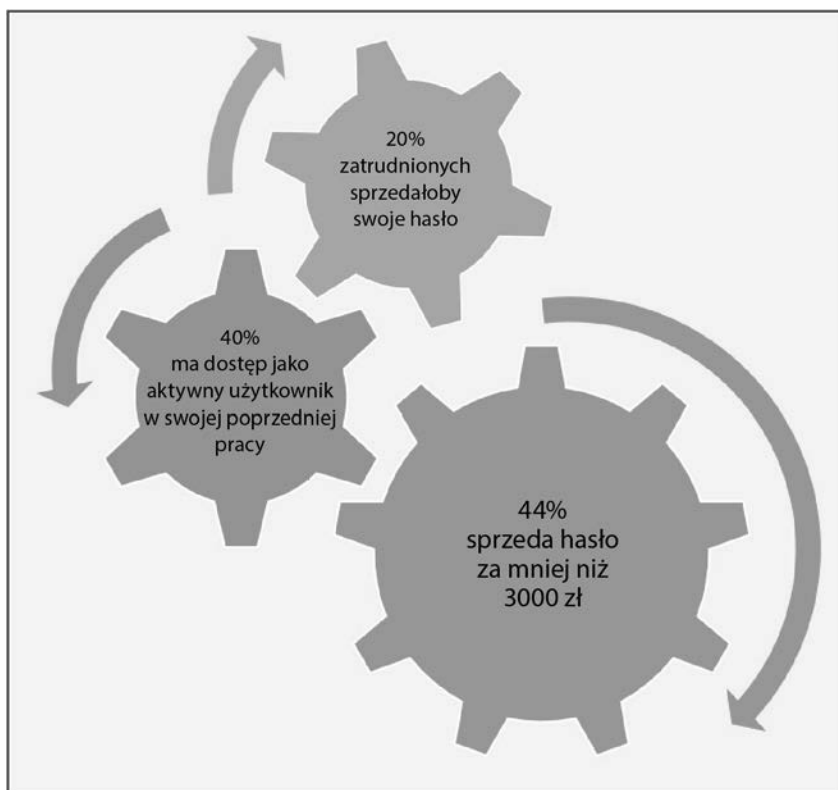
Jak rozpoznać wewnętrznego szkodnika?

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 przysyłanie 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, robi 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

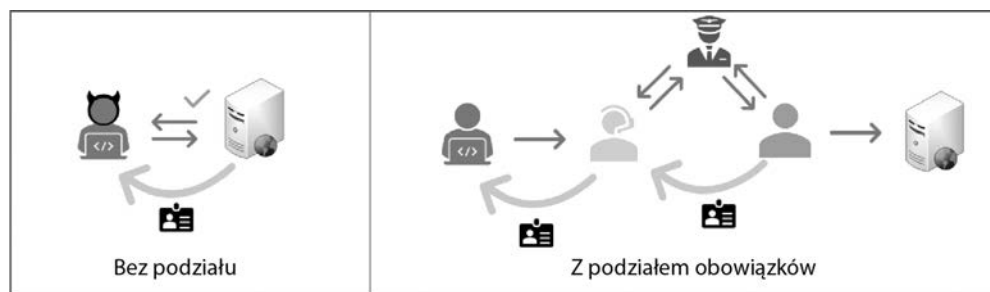
Naukowcy zgadzają się, że największemu włamaniu do platformy mediów społecznościowych (włamaniu na Twittera w 2020 roku) można było zapobiec, gdyby był wprowadzony podział obowiązków.

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.

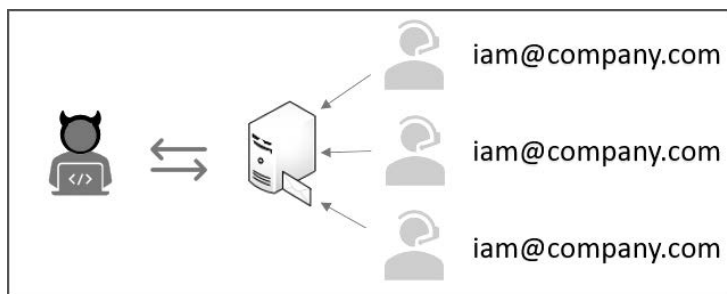
Inny świetny przykład jest związany z kopiami zapasowymi, ponieważ użytkownik działający na szkodę firmy może wiedzieć, że usunięcie niektórych plików nie spowoduje żadnej szkody. Dzieje się tak dlatego, że mogą one zostać odzyskane z kopii zapasowych. W takich przypadkach to kopie zapasowe będą stanowić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

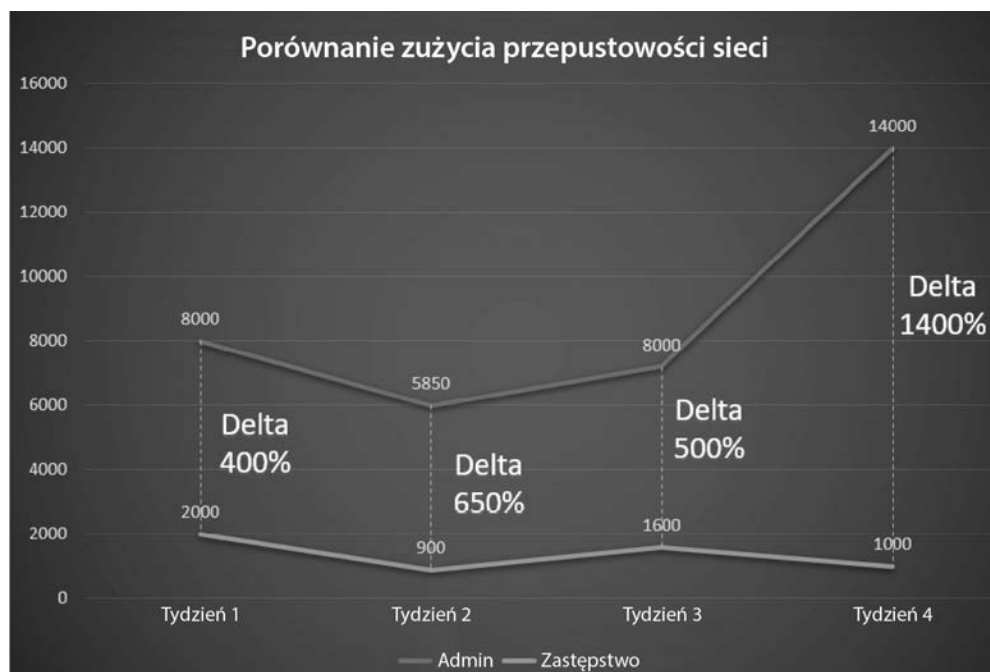
- *Zmniejsza ryzyko przestojów:* Musisz mieć przeszkolonych ludzi, aby uniknąć ryzyka wynikającego z braku umiejętności dotyczących danej technologii. Na przykład: „Och, będziemy musieli poczekać do następnego tygodnia, ponieważ Maria jest nieobecna, a ona jest jedyną osobą, która zna się na DB2”.
- *Zmniejsza ryzyko oszustwa:* Kiedy osoba pozostaje „przykuta” na stałe do tej samej roli, może być w stanie ukryć ślady własnych działań (w przypadku jakiegokolwiek 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.

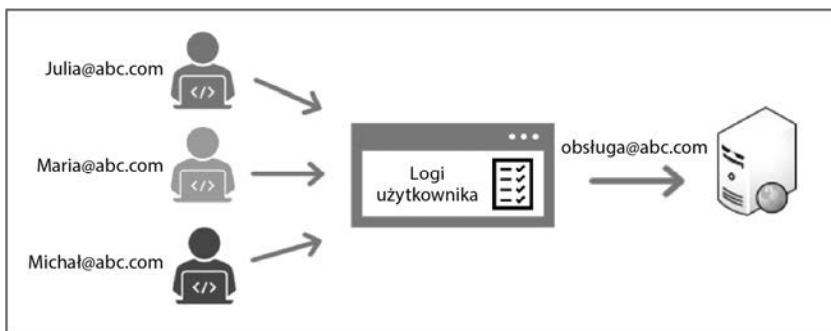
Przyjrzyjmy się teraz jednemu przykładowi bardzo powszechnej praktyki w działach IT, która jest naprawdę złą praktyką z punktu widzenia bezpieczeństwa.

Wspólne dane uwierzytniające

Domyślnie najlepsza praktyka mówi, że wspólne *dane uwierzytniające dla kilku osób NIE powinny być dozwolone w Twojej infrastrukturze*. W przypadku gdy jednak są, musisz skonfigurować dodatkowe opcje kontroli, takie jak uwierzytlnienie 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 uwierzytlnione 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.

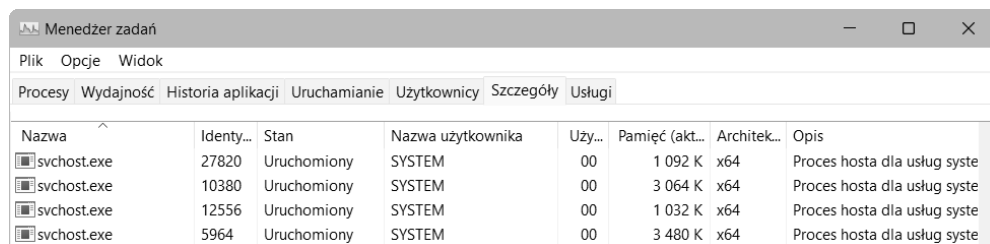
Teraz przyjrzymy się atakom, które mają na celu oszukanie użytkownika. Pamiętaj jednak, że chociaż nie wszyscy autorzy zgadzają się co do klasyfikacji tych ataków jako ataków z zakresu inżynierii społecznej, prawda jest taka, że w ich przypadku mamy te same koncepcje i strategie, co w przypadku ataków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

Przebieg ataku w inżynierii społecznej

Istnieje wiele technik, które napastnicy mogą wykorzystać do przeprowadzenia ataku socjo-technicznego, 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).



Menedżer zadań							
Plik Opcje Widok							
Procesy Wydajność Historia aplikacji Uruchamianie Użytkownicy Szczegóły Usługi							
Nazwa	Identy...	Stan	Nazwa użytkownika	Uży...	Pamięć (akt...	Architek...	Opis
svchost.exe	27820	Uruchomiony	SYSTEM	00	1 092 K	x64	Proces hosta dla usług syste
svchost.exe	10380	Uruchomiony	SYSTEM	00	3 064 K	x64	Proces hosta dla usług syste
svchost.exe	12556	Uruchomiony	SYSTEM	00	1 032 K	x64	Proces hosta dla usług syste
svchost.exe	5964	Uruchomiony	SYSTEM	00	3 480 K	x64	Proces hosta dla usług syste

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 robi coś, co wydaje się korzystne dla ofiary. Dzięki temu ofiara będzie skłonna spełnić prośbę napastnika (o udzielenie pewnych informacji lub wykonanie jakiejś czynności), aby odwdziżyć 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.

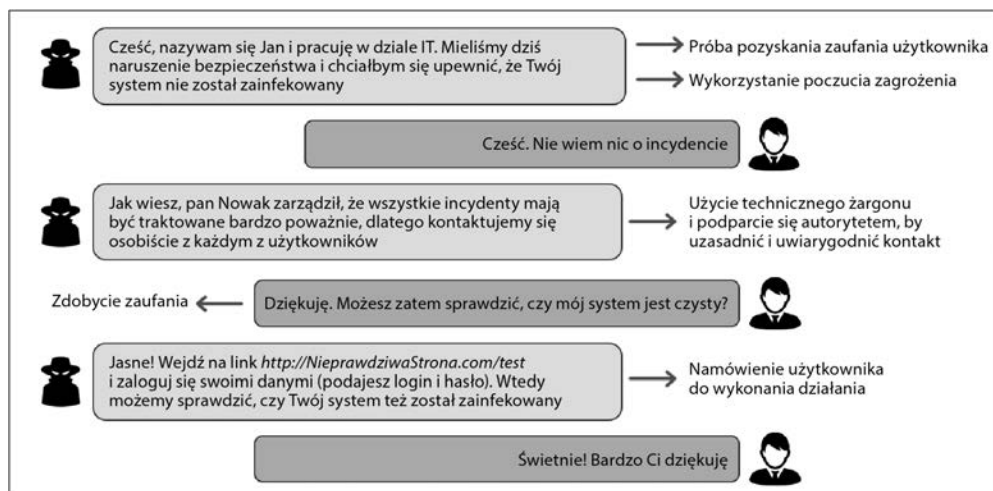
Zabawny fakt: większość źródeł uważa, że *Stuxnet* (wirus, który uszkodził irański program nuklearny) został rozprzestrzeniony przez zainfekowane dyski USB.

- **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 uspić 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 przyjrzeeli 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

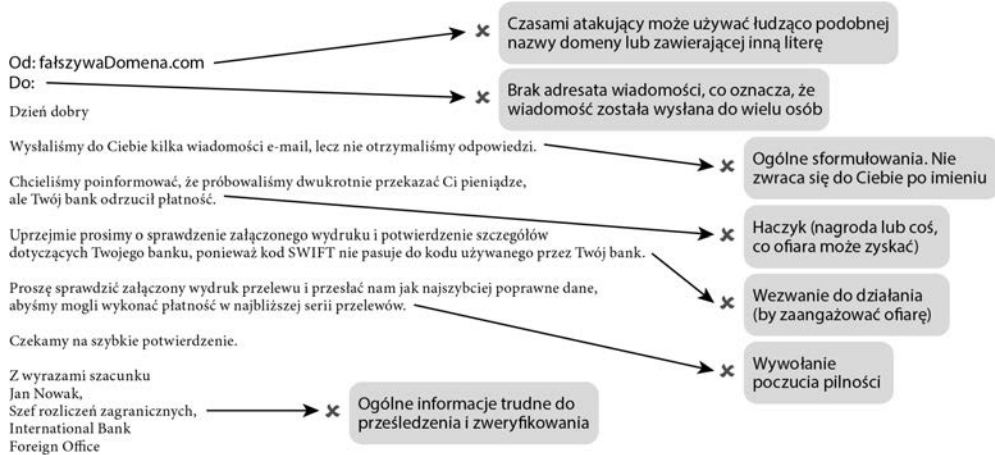
Jak już zapewne wiesz, koncepcja jest bardzo prosta. Napastnik wysyła fałszywy e-mail, próbując podszyć się pod renomowaną osobę lub firmę. Aby zwiększyć swoje szanse na sukces, atakujący najpierw stara się przekonać ofiarę, że e-mail jest legalny (używając logo firmy albo podszywając się pod konto e-mail 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*).

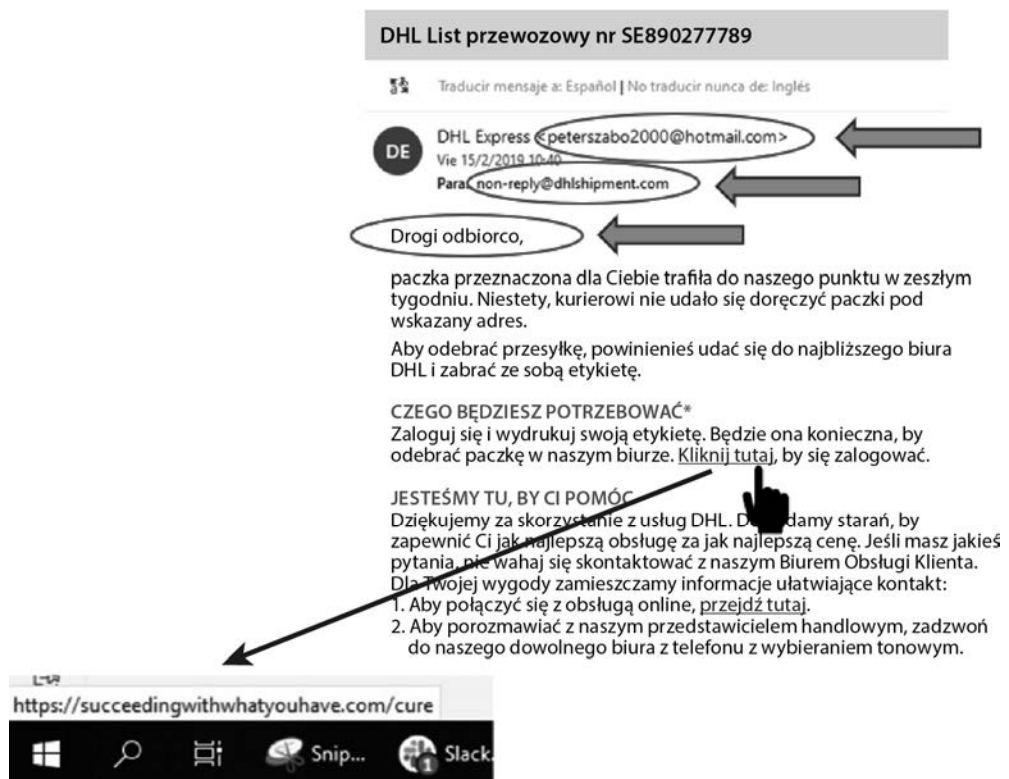
Na rysunku 4.11 wyróżniliśmy wspólne specyficzne cechy, które pomogą Ci zidentyfikować tego typu ataki.

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 wyludzącej dane typu „darmowe pieniądze”

Na rysunku 4.12 pokazano, jak atakujący podszywa się pod znaną firmę kurierską, ale nadal istnieją 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 najeżdzać 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 przyjrzymy się niektórym wariantom inżynierii społecznej, które wyewoluowały z ataków phishingowych.

SMishing

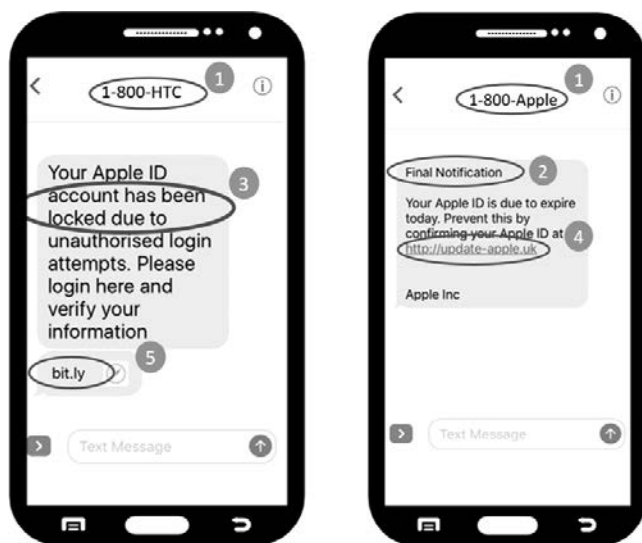
Atak ten posiada te same cechy co atak phishingowy, z tą różnicą, że jest on rozpowszechniany za pomocą **wiadomości SMS** (ang. *Short Message Service*).

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

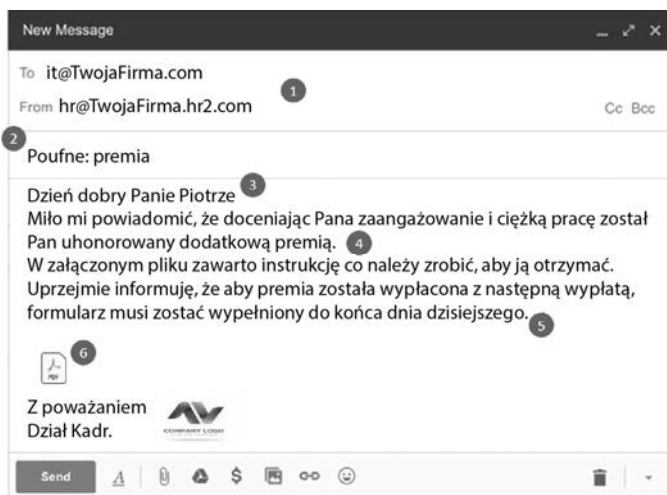
1. W większości przypadków atakujący użyją losowego numeru, który jest łatwy do zauważenia i zablokowania. Jednak w bardziej rozbudowanych atakach atakujący może użyć niektórych narzędzi (takich jak **BurnerApp** i **SpoofCard**), aby zmanipulować identyfikator dzwoniącego i podszyć się pod bardziej 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 *skraccania 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 przyjrzyś 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

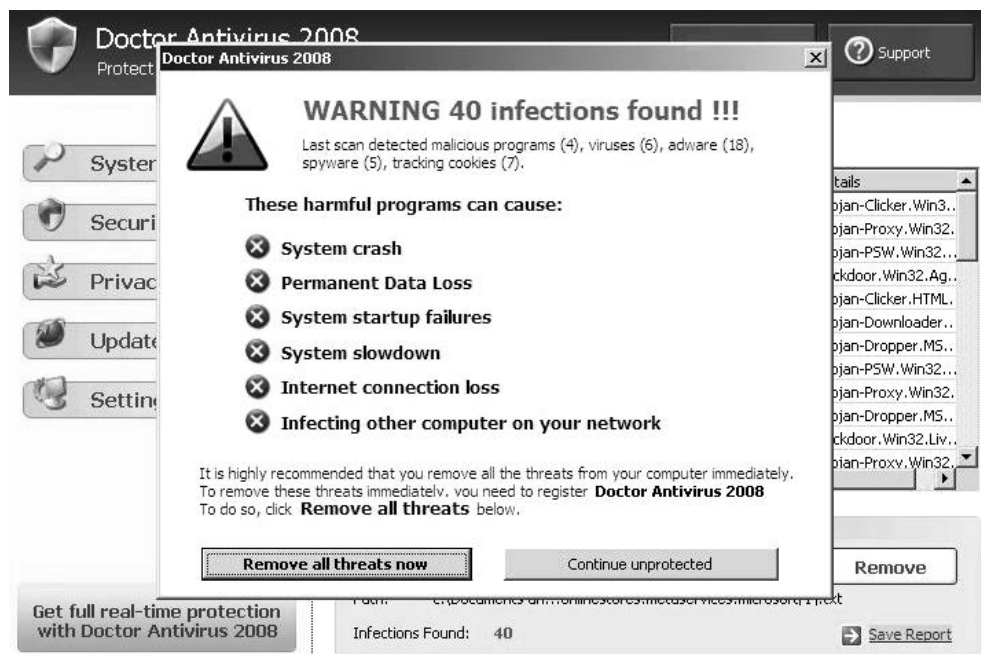
Scareware polega na wprowadzeniu ofiary w błąd, że komputer został zainfekowany wirusem, podczas gdy w rzeczywistości nie jest to prawda. Celem atakującego jest przekonanie ofiary do zainstalowania *oprogramowania antywirusowego* w celu usunięcia tych rzekomych wirusów, ale sugerowane *oprogramowanie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

Zagłądanie przez ramię

Być może brzmi to bardzo prosto, ale wiele informacji wycieka przy użyciu tej prostej metody. Zasadniczo polega ona na zagłądaniu 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 wchodzi 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 rozślawniona 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 niszcarkę 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 wykorzystuje.

Atakujący: Cześć, tu Robert z działu IT. Mam tu zgłoszenie, że masz jakiś problem. W czym mogę pomóc?



Ofiara: Cześć. Nie, nic nie zgłaszałem, ale czy mógłbyś mi pomóc z dyskiem sieciowym?

Prawdopodobne odpowiedzi atakującego:



1. Pewnie, kliknij na link, który zaraz poślę, abym mógł otworzyć zdalną sesję i zerknąć, o co chodzi. 
2. Pewnie, ale zanim to zrobię, możesz mi podać swój numer pracownika i hasło do konta? 
3. Oczywiście, ale muszę potwierdzić twoją tożsamość. Proszę, wpisz swój login i hasło, korzystając z linka, który poślę. 

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:

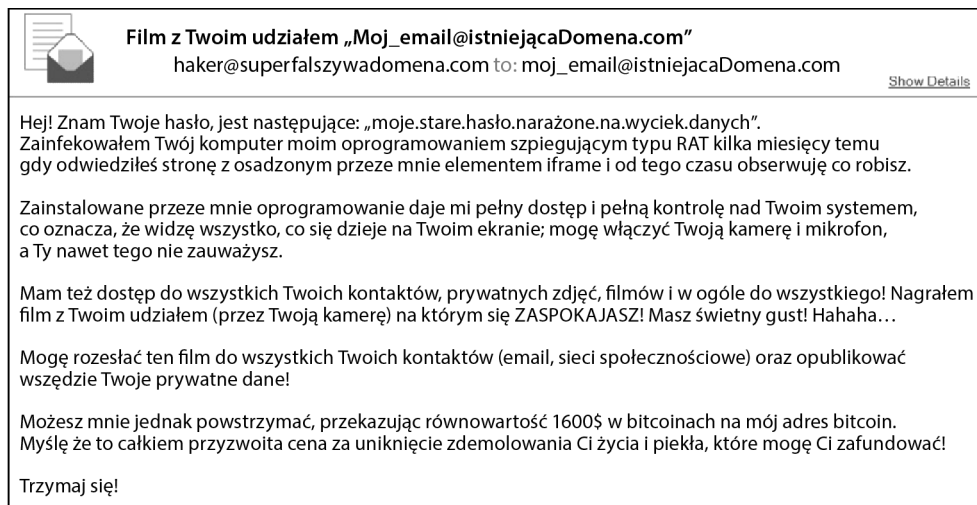
- Zawsze używaj MFA.
- Używaj silnych haseł. Tego typu kontami powinno się zarządzać za pomocą skarbca haseł, więc po co się krępować? Użyj maksymalnej długości, użyj znaków specjalnych i uodpornij je na ataki słownikowe lub siłowe.
- Upewnij się, że każde hasło jest unikalne.
- Często zmieniaj hasło (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.



Rysunek 4.19. Szantażująca wiadomość e-mail

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

Absolutnie nie!

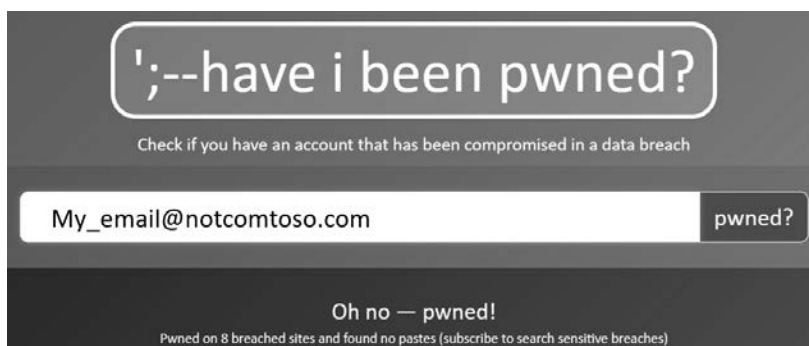
Tutaj atakujący wykorzystują informacje z poprzednich wycieków danych, szukają par e-mail – hasło i wykorzystują to w ataku.

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 *częstotliwość 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 przejrzelismy, 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 *support-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

- ACL, access control list, 224
 - dla katalogów, 225
 - przeglądanie, 224
 - usuwanie list, 226
 - zarządzanie listami, 225
- AD, Active Directory, 198
 - najlepsze praktyki, 200
- adresy IP, 325
- aktualizacja, update, 195
 - definicji, definition update, 195
 - krytyczna, critical update, 195
 - zabezpieczeń, security update, 196
- aktywa
 - identyfikacja, 48
- Amazon CloudWatch, 318
- analiza
 - ilościowa, 81
 - jakościowa, 82
 - logów, 134
 - podatności, 60
 - przyczyn źródłowych, RCA, 60
 - ryzyka, 178
 - wpływu na biznes, BIA, 87, 91
 - złośliwego oprogramowania, 370, 379
- AP, access point, 158
- API
 - kontrola dostępu do interfejsu, 314
- aplikacje internetowe, 323
 - atak siłowy na hasła, 347
 - ataki XSS, 336
 - informacje publiczne, 325
 - używanie Burp Suite, 338
- AppDynamics, 319
- APT, Advanced Persistent Threat, 174
- Armitage, 391
 - ekran główny, 394
 - eksploracja, 394
 - instalacja, 391, 393
 - konsola, 395
 - moduły, 396
 - rozpoczęcie ataku, 396
- ataki, 28, *Patrz także* złośliwe oprogramowanie
 - BadUSB MITM, 72
 - bezwolne, 157
 - exploity dnia zerowego, 32
 - fazy cyberataku, 238
 - HTML, 166
 - internetowe, 165
 - inżynierii społecznej, 30, 137, 140
 - coś za coś, 149
 - nurkowanie w śmietniku, 148
 - okup w mediach społecznościowych, 150
 - phishing, 140
 - scareware, 145
 - SMishing, 142
 - spear phishing, 143
 - szantaż, 151
 - tailgating, 148
 - testowanie, 154
 - vishing, 144
 - wabienie, 147
 - z użyciem hasła, 38
 - zagłębienie przez ramię, 148
- na DNS
 - przejęcie DNS, DNS hijacking, 33
 - router DNS, 33
 - tunelowanie, 35
 - uprowadzanie domeny, 35
 - zatrucie pamięci podręcznej, 34
- na hasła
 - na skróty hasła, 43
 - siłowe, brute-force, 39, 347
 - słownikowe, 40
- SYN flood, 31
- typu
 - człowiek pośrodku, 30, 33
 - DDoS, 285
 - DoS, 325
 - odmowa usługi, DoS, 30
 - restart „na zimno”, 413
 - Stuxnet, 64
 - teardrop, 31
 - wstrzyknięcie SQL, 340
- USB HID, 67
 - Bash Bunny, 69
 - Harpun USB, 71
 - klucze sprzętowe, 71, 78
 - ochrona, 75
 - oparte na smartfonach, 72
 - USB Rubber Ducky, 67
 - USB Samurai, 71
- WiFi Pineapple, 162
- XSS, 336
 - za pomocą kodów QR, 167
- zautomatyzowane, 432
 - carding, 433
 - DoS, 434
 - faszeringowanie danymi uwierzytelniającymi, 434

ataki

- zautomatyzowane
 - gromadzenie kont, 432
 - łamanie danych
 - uwierzytelniających, 434
 - odmowa z magazynu, 434
 - oszustwo reklamowe, 432
 - porażka CAPTCHA, 433
 - przyspieszanie, 435
 - rozgryzanie tokenów, 437
 - rozszyfrowywanie kart, 433
 - scalping, 436
 - skanowanie podatności, 437
 - spamowanie, 436
 - strzał z ukrycia, 436
 - tropienie, 435
 - tworzenie kont, 432
 - wypaczanie, 436
 - wypłata gotówki, 433
 - zbieranie, scrape, 436
 - zbieranie odcisków
 - palców, 435

ATP

- techniki obrony, 175

audyty, 113

- dostępu fizycznego, 118
- IAM, 117
- kodu, 119
- przetwarzania danych, 117
- sieci, 117, 264
- sieci Wi-Fi, 158
- systemów, 117
- wewnętrzne, 114
- zarządzanie danymi, 115
- zasad, 117
- zewnętrzne, 114
- zgodności hasel, 119

automatyzacja, 431

- monitorowania sieci, 445
- zabezpieczania sieci, 442
- zbierania informacji, 444

Autopsy, 170
Azure Security Center, 318
B
Bash Bunny, 69
baza danych

- kontrola dostępu, 316
- Baza Danych Google Hacking, GHDB, 62

BCP, Business Continuity Plan, 86

- aktualizacje i konserwacja, 94
- badania i przeglądy, 94
- bezpieczeństwo pracowników, 93
- kommunikacja, 93
- ocena ryzyka, 92
- określenie celów, 92
- statystyki, 87
- strategie ciągłości działania, 92
- tworzenie BIA, 87, 92

bezpieczeństwo

- aplikacji internetowych, 323
- danych w chmurze, 310
- fizyczne, 202
- przez zastosowanie warstw, 52
- sieci bezprzewodowej, 250, 252
- sieci IoT, 291
- urządzeń IoT, 292
- użytkownika, 250

bezpieczne hasło, 41
BIA, Business Impact Analysis, 87, 91
biała skrzynka, white box, 55
Binwalk, 172
BitLocker, 190

- konfiguracja programu, 208

blogi, 453
blokowanie reklam, 303
Bluetooth, 290
botnet, 31
Bulk Extractor, 173
Burp Suite, 324, 338

- konfiguracja, 339
- przechwytywanie danych, 343
- wersje, 338
- zmiana ID użytkownika, 344

BYOD, Bring-Your-Own-Device, 142, 154
C
CAINE, 418
CAPTCHA, 329, 433
certyfikaty, 452
CFG, control flow guard, 189
chmura, 307

- bezpieczeństwo danych, 310
- centrum zabezpieczeń Azure, 318
- monitorowanie aplikacji, 318
- testowanie bezpieczeństwa, 317

CIRCLearn, 299
CLI, command line interface, 194
clickbait, 148
CMM, Cybersecurity Maturity Model, 100, 120

- analizowanie rezultatów, 123
- cele, 120
- charakterystyka, 120
- struktura, 121
- zalety, 124

CMS, content management system, 238
CUDSE, Create, Update, Distribute, Socialize, Enforce, 100, 103, 450

- aktualizacja, 105
- egzekwowanie, 107
- rozpowszechnianie, 106
- tworzenie, 103

CVE, Common Vulnerabilities and Exposures, 58, 326
cyberbezpieczeństwo NIST, 84
czarna skrzynka, black box, 54
czynnik ludzki, 47, 127
D
DDoS, Distributed Denial-of-Service, 30
DEP, data execution prevention, 189
DiD, Defense in Depth, 46

- czynnik ludzki, 47
- identyfikacja aktywów, 48
- procesy firmy, 48
- tworzenie modeli, 46
- tworzenie warstw, 49
 - na podstawie funkcji, 50
 - na podstawie technologii, 51
 - według typu, 50

DNS

- ataki, 32
- hijacking, 33
- wyszukiwanie, 325

docelowy

- czas przywrócenia, RTO, 87
- punkt przywrócenia, RPO, 88

domeny, domains, 121
dorki Google, 329
DoS, 434

dostęp
 do etcd, 315
 do routera, 250

dostępność, 28
 serwisu, 89

dowody, 169
 zarządzanie, 426
 związane z atakiem, 421
 źródła danych, 421

DRP, Disaster Recovery Plan, 95
 tworzenie, 95
 wdrażanie, 96

DuckHunt, 77

DuckHunter HID, 72

Ducky Scripts, 68

DVWA, Damn Vulnerable Web Application, 62, 323, 331
 ekran logowania, 335
 instalacja, 332
 interfejs internetowy, 335
 obniżanie poziomu
 zabezpieczeń, 407
 testowanie ataku siłowego,
 347
 wstrzyknięcie SQL, 340
 wyświetlanie skrótów hasel,
 345
 zmiana poziomu
 bezpieczeństwa, 342

dysk
 SSD, 416
 twardy, 415

dzienniki, 386
 w systemie Windows, 386
 zarządzanie, 387
 zabezpieczeń Windows, 75

E

ECM2, Enterprise Cybersecurity Maturity Model, 101, 121–123

ESP32, 303

exe2hex, 168

exploits, 189, 401
 dnia zerowego, 32

F

falszywe
 poczucie bezpieczeństwa, 72
 punkty dostępu, 295

falszywką, hoax, 38

falszywy
 ekran aktualizacji, 69
 SSID, 162

filtrowanie
 adresów URL, 204
 spamu, 205

Fing, 254

FragmentSmack, 31

framework
 Metasploit, 163
 Wifipumpkin3, 296

FTP, 263

funkcje urządzenia mobilnego, 53

G

GDPR, 108
 generator infekującego nośnika,
 166

GHDB, Google Hacking Database, 62

Ghidra, 379

Google hacking, 329

GPO, Group Policy Object, 168

H

harpun USB, 71

hasło, 36
 administratora, 251
 ataki siłowe, 39, 347
 audyt zgodności, 119
 bezprzewodowe
 wstrzykiwanie, 45
 do sieci bezprzewodowej, 252
 skradzione, 38
 tworzenie, 41
 zarządzanie, 43, 454
 zdekonspirowane, 36

HTTP, 263

I

IaaS, Infrastructure as a Service, 309

IAM, Identity Access Management, 103

ICS, Industrial Control Systems, 63, 64

identyfikacja, identyfik, 84
 aktywów, 48
 podatności, 60
 ryzyka, 79

IDS, 265

informacje
 o aplikacji internetowej, 324
 o hostingu, 327
 o witrynie, 324
 publiczne, 325
 związane z DNS, 325

infrastruktura jako usługa, IaaS, 309

InsightVM, 320, 368

integralność, 27

inteligentne wykrywanie
 zagrożeń, 176
 wdrażanie systemu, 177

interfejs
 programowania aplikacji, API, 314
 wiersza poleceń, CLI, 194

internet rzeczy, IoT, 284

Intruder, 321

inżynieria społeczna, social engineering, 30, 136
 przebieg ataku, 137

IoT, Internet of Things, 63, 284
 bezpieczne kopiowanie, 299
 inteligentne domy, 285
 kontrola dostępu, 303
 podatności, 286
 poprawa bezpieczeństwa, 292

Raspberry Pi, 295

technologie sieciowe, 287

tworzenie przynęty, 300

urządzenia nieautoryzowane, 304
 urządzenie blokujące reklamy, 303
 wdrożenia, 285

IPS, 266

iptables, 228
 konfigurowanie, 229
 ochrona przed skanowaniem portów, 233
 ochrona SSH, 232

J

język Python, 437

K

Kali Linux, 237

Key Croc, 275

keylogger, 275

klatka Faradaya, 426
 klonowanie strony, 165
 klucze sprzętowe USB, 71
 konto gościa, 253
 kontrola dostępu, access control, 278
 dla gości, 279
 do interfejsu API, 314
 do kubeletu, 314
 oparta na rolach, RBAC, 135
 kopie zapasowe, 206
 kryminalistyka
 cyfrowa, 412, 417
 urządzeń mobilnych, 422
 Kubernetes, 308
 zabezpieczanie, 313

L

LAN Turtle, 270
 Linux, *Patrz* Unix
 lista
 kontroli dostępu, ACL, 224
 podatności, 326
 zabronionych IP, blacklist, 329
 logi, 234
 analiza i korelacja, 134
 LoRaWAN, 287

Ł

łatanie
 ósmej warstwy, 126
 ról i przydziałów, 192
 starszych systemów, 191

M

macierz
 odpowiedzialności za
 wsparcie OS, 192
 ryzyka, 82
 zasad cyberbezpieczeństwa, 113
 malware, *Patrz* złośliwe
 oprogramowanie
 mapowanie sieci, 237
 mapy zagrożeń, 451
 maszyna
 wirtualna, 210, 396

mechanizm skryptowy Nmap, NSE, 243
 Metasploit, 163, 389
 dostęp zdalny, 403
 informacje o exploitach, 402
 konfiguracja, 392
 uruchamianie frameworka, 400
 wersje, 391
 Metasploitable, 396
 Meterpreter, 390
 metoda CUDSE, 100, 103, 450
 metody
 kryminalistyczne, 168
 testów penetracyjnych, 163
 MFA, Multifactor
 Authentication, 135
 MFT, Master File Table, 414
 struktura tabeli, 415
 Microsoft
 COFEE, 412
 Defender, 76
 model
 dojrzałości
 cyberbezpieczeństwa firmy, ECM2, 101, 121–123
 dojrzałości
 cyberbezpieczeństwa, CMM, 100, 120
 modele
 DiD, 46
 warstwowe, 52
 monitor internetu, 302, 446
 monitorowanie
 aplikacji internetowych, 302
 ryzyka, 83
 sieci, 302
 MTBF, mean time between failures, 89
 MTTR, mean time to repair, 89

N

najlepsze praktyki branżowe, 454
 narzędzia
 bezprowadowe, 157
 do analizy
 złośliwego oprogramowania, 376
 do badania podatności, 358
 do inżynierii społecznej, 164
 do oceny podatności, 355, 358
 do pozyskiwania danych, 328
 do tunelowania DNS, 36

eksperta, 448
 kryminalistyczne, 169
 związane z hasłami, 454
 narzędzie

 Armitage, 391
 Binwalk, 172
 BitLocker, 190, 208
 Bulk Extractor, 173
 Burp Suite, 324
 debug.exe, 168
 DVWA, 62, 323, 331
 exe2hex, 168
 Fing, 254
 Ghidra, 379
 InsightVM, 320, 368
 Intruder, 321
 Kismet, 304
 Microsoft COFEE, 412
 Nessus, 118, 320
 Nexpose, 367
 Nmap, 118, 239
 OpenVAS, 360
 PeStudio, 379
 PineAP, 162
 ProcDOT, 378
 Process Explorer, 377
 Process Monitor, 377
 RPI Hunter, 305
 Scapy, 442
 Searchsploit, 404
 sqlmap, 405
 Weeveily, 405
 WiFi Pineapple, 158
 Wifiphisher, 296
 Wireshark, 118, 255
 nazwa SSID, 252
 NEMS, 302
 Nessus, 320, 359
 Nethunter, 72
 Nexpose, 367
 NFC, 255
 Nmap, 239
 skrypty, 242
 NSE, Nmap Scripting Engine, 243

O

obliczanie dostępności serwisu, 89
 obrona
 obwodowa, 46
 przed atakami
 bezprowadowymi, 157

przed atakami
 socjotechnicznymi, 152
 w głąb, DiD, 46
 obszary, controls, 121
 ocena
 podatności, 58
 ryzyka, 60, 80
 zagrożeń, 59
 ochrona, protect, 84
 infrastruktury
 alerty, 134
 analiza logów, 134
 audyty, 136
 obowiązkowe urlopy, 133
 podział obowiązków, 130
 rotacja stanowisk pracy, 132
 stosowanie zasad, 136
 używanie skrzynek
 pocztowych, 132
 wspólne dane
 uwierzytelniające, 135
 przed atakami USB HID, 75
 blokada USB, 77
 DuckHunt, 77
 dzienniki zabezpieczeń, 75
 Microsoft Defender, 76
 przed exploitami, 189
 przed skanowaniem portów,
 233
 przepływu sterowania, CFG,
 189
 serwera Unix, 224
 sieci bezprzewodowych, 246
 SSH, 232
 odcisk palca przeglądarki, 329
 odmowa z magazynu, 434
 odzyskiwanie
 cyfrowe, 414
 danych z pamięci nieulotnej,
 414
 danych z pamięci RAM, 412
 fizyczne, 414
 skasowanych plików, 173
 OpenVAS, 360
 aktualizowanie swoich
 kanałów, 366
 instalacja, 361
 struktura skanowania sieci, 360
 testy z uwierzytelnieniem, 360
 używanie, 363
 oprogramowanie jako usługa,
 SaaS, 308

Orange Pi, 303
 OSINT, Open Source
 Intelligence, 325

P

PaaS, Platform as a Service, 309
 Packet Squirrel, 272
 pakiet
 funkcji, feature pack, 197
 serwisowy, service pack, 197
 PALADIN, 420
 PAM, Privileged Access
 Management, 135
 pamięć
 nieulotna, 412
 ulotna, 412
 PeStudio, 379
 phishing, 140
 pieprz, 44
 Pi-hole, 303
 planowanie, 111
 ciągłości działania, BCP, 86, 91
 odzyskiwania po awarii, DRP,
 95
 platforma
 Autopsy, 170
 jako usługa, PaaS, 309
 platformy kryminalistyczne, 418
 pliki dzienników, 386, 421
 Plunder Bug LAN Tap, 271
 podatności, 58
 analiza, 60
 dostawców, 65
 fizyczne, 62
 identyfikacja, 60
 IoT, 63, 286
 klienta, 65
 narzędzia do oceny, 355, 358
 procedur postępowania, 65
 ręczna ocena, 358
 sieci WWW, 62
 sprawdzanie, 61
 usuwanie, 60
 w Joomla, 59
 w oprogramowaniu, 61
 w systemach SCADA/ICS, 64
 w zabezpieczeniach
 Bluetooth, 290
 LoRaWAN, 288
 sieci bezprzewodowych, 246
 Sigfox, 290
 Telnetu, 258

USB HID, 66
 Zigbee, 288
 wewnętrzne, 357
 zautomatyzowane skanery, 359
 związane z użytkownikami, 62
 pojedynczy punkt awarii, 90
 polecenie
 chmod, 222
 getfacl, 224
 nmap -A, 241
 nmap, 240
 systemd, 213
 umask, 220
 poufność, 27
 PowerShell, 168
 prawa administratora, 47, 153
 PRF, Probe Request Frames, 158
 priorytet aktywów, 49
 ProcDOT, 378
 procedury, 102, 450
 proces SVCHOST, 137
 Process
 Explorer, 377
 Monitor, 377
 program nagród za znalezione
 błędy, 356
 programy antywirusowe, 203
 protokół
 FTP, 263
 HTTP, 263
 Telnet, 258
 TLS, 314
 USB, 74
 przemysłowy system kontroli,
 ICS, 63
 przepisy
 krajowe, 108
 regionalne, 108
 wewnętrzne, 110
 przynęta, 329
 Canary, 300
 Cowrie, 301
 Fail2ban, 444
 SNARE, 301
 przywracanie, recover, 85
 punkt dostępu, AP, 158
 nieautoryzowany, 160
 fałszywy, 159, 296
 Python, 437
 biblioteka BeautifulSoup, 441
 biblioteka Pillow, 440
 lokalne wyszukiwanie plików,
 437
 menedżer pakietów pip, 441

Python

- metadane z plików PDF i Word, 439, 440
- narzędzie Scapy, 442
- zbieranie danych ze stron internetowych, 441

R

- ramki PRF, 158

- Raspberry Pi, 295, 443

- automatyzacja monitorowania, 445
 - automatyzacja zbierania informacji, 444
 - Pi Finder, 304
 - Pi Zero, 70, 303
 - ściana ogniowa, 298
 - wykrywanie włamań, 298

- RBAC, Role-Based Access Control, 135

- RCA, Root Cause Analysis, 60

- reagowanie, respond, 85
 - na incydenty, 178

- regulacje, 108

- dotyczące klientów, 109
 - rynkowe/branżowe, 109

- RODO, 108

- rodzaje

- analizy
 - złośliwego oprogramowania, 373

- ataków, 28
 - automatycznych, 432
 - inżynierii społecznej, 140
 - USB HID, 67

- audytów, 117

- łatek, 195

- podatności, 61

- regulacji, 108

- Rpi-AWAPS, 297

- RPO, Recovery Point Objective, 88

- RTO, Recovery Time Objective, 87
- ryzyko, 78

- analizowanie, 178

- identyfikacja, 79

- monitorowanie, 83

- ocena, 60, 80

- analiza ilościowa, 81

- analiza jakościowa, 82

- reakcje, 82

- zarządzanie, 449

S

- SaaS, Software as a Service, 308

- SCADA, 64, 299

- Scapy, 442

- scareware, 145

- Screen Crab, 273

- Searchsploit, 404

- Security Onion, 267

- serwer linuksowy, 210

- SET, Social Engineering Toolkit,

- 164

- główne menu, 165

- moduł ataku sieciowego, 166

- moduł Spearphishing, 165

- Shark Jack, 273

- Shodan, 63

- sieci bezprzewodowe, 246

- dostęp do routera, 250

- hasło administratora, 251

- hasło do sieci, 252

- identyfikator SSID, 252

- konto gościa, 253

- LPWAN, 287

- PAN, 288

- Sigfox, 290

- tryb bezpieczeństwa, 252

- użytkownik admin, 252

- zdalny dostęp, 253

- Zigbee, 288

- SIEM, Security Information and Event Management, 234

- Sigfox, 289

- skaner podatności, 359

- InsightVM, 368

- Intruder, 321

- Nessus, 320

- Nexpose, 367

- OpenVAS, 360

- skanowanie, 237

- skrót, hash, 43

- skrypt

- DuckHunt, 77

- Ducky Scripts, 68

- inicjujący MySQL, 212

- vulners, 243, 244

- vulscan, 244, 245

- skrypty

- międzywitrnowe, XSS, 336

- USB Rubber Ducky, 68

- słownik, 40

- SMishing, 142

- Snort, 267

- SOC, Security Operations Centers, 178

- socjotechniki, 138

- sól, 44

- spear phishing, 143

- sqlmap, 405

- SSID, 252

- stacja robocza SIFT, 419

- sterownik, driver, 196

- sterowniki HID, 66

- system

- antybotowy CAPTCHA, 329

- ICS, 63, 64

- IDS/IPS, 267

- SCADA, 64

- zarządzania treścią, CMS, 238

- szablon

- planu ciągłości działania, 449

- planu odzyskiwania po awarii, 449

- szantaż, 151

- szara skrzynka, gray box, 54

- szkolenia, 153

- szyfrowanie, 207

- program BitLocker, 208

- wymagania, 207

- dysku, 190

- EFS, 190

Ś

- średni

- czas między awariami, MTBF, 89

- czas naprawy, MTTR, 89

T

- tablica typu kanban, 49

- tailgating, 148

- Telnet, 258

- klient, 258

- serwer, 259

- test penetracyjny, 54

- testowanie podatności, 358

- bez uwierzytelnienia, 360

- narzędzia, 360, 367, 368

- z uwierzytelnieniem, 360

- testy

- penetracyjne jako usługa, 55

- penetracyjne, 163, 385

- tęczowe tabele, rainbow tables, 43

TLS, Transport Layer Security, 314
 triada CIA, 26, 27
 tryb „dochodzenie”, 169
 tunelowanie DNS, 35
 tworzenie
 analizy wpływu na biznes, BIA, 87
 bezpiecznego hasła, 41
 listy kontrolnej, 185
 modeli DiD, 46
 przynęty, 300
 strategii szkoleń, 153
 warstw obrony, 49
 na podstawie funkcji, 50
 na podstawie technologii, 51
 według typu, 50

U

Unix, 209
 konfiguracja zapory sieciowej, 228
 kontrola dostępu, 224
 lista usług, 211
 uprawnienia do plików, 215
 zabezpieczanie usług, 210
 zarządzanie dziennikami, 233
 zarządzanie usługami, 213
 UPnP, 249, 253
 uprawnienia
 do plików, 215
 domyślne, 218
 hierarchia, 221
 użytkownika, 204
 w katalogach, 219
 w trybie numerycznym, 217
 wyszukiwanie, 223
 zmienianie, 220, 222
 urządzenia mobilne
 dochodzenie bez urządzenia, 423
 transportowanie, 426
 źródła danych, 425
 urządzenie
 BadUSB, 71
 wstrzykujące WHID, 70
 USB
 bezpieczne kopiowanie, 299
 Harpoon, 71
 HID, 66
 Rubber Ducky, 67

Samurai, 71
 skrypty, 68
 usługa
 Active Directory, 183
 mysql, 213
 usługi
 uniksowe, 210
 uruchamianie, 213
 usuwanie, 214
 WSUS, 193
 wyłączanie, 214
 usuwanie podatności, 60
 utwardzanie
 lista kontrolna, 185
 serwera Unix, 209
 systemu Windows, 184
 uwierzytelnianie
 wieloczynnikowe, MFA, 37, 135
 wieloetapowe, 37
 za pomocą hasła, 45
 użytkownicy, 126, 206

V

vishing, 144
 VPN, virtual private network, 191

W

wabienie, baiting, 147
 WAF, Web Application Firewall, 328
 warstwa 8, 127
 warstwowy model
 bezpieczeństwa, 52
 warstwy
 bezpieczeństwa, 51
 obrony, 49
 Weevely, 405, 409
 WHID, 70
 WHOIS, 326
 Wi-Fi, 250
 WiFi Pineapple, 158, 162
 dodawanie modułów, 163
 mapa 3D, 162
 Windows
 aktualizacja sterowników, 196
 aktualizacje, 195, 201
 Defender, 185, 203
 funkcje systemu, 199

instalowanie latek, 190
 jako usługa, 201
 lista kontrolna, 185, 189
 monitorowanie, 188
 opcje bezpieczeństwa, 202
 porty i protokoły, 186
 Server
 dokumentacja, 201
 usługi i funkcje, 185
 utwardzanie systemu, 184
 wdrażanie poprawek, 193
 wspierane wersje, 185
 zabezpieczanie AD, 198
 zabezpieczanie stacji
 roboczych, 201
 zarządzanie użytkownikami, 187
 Wireshark, 255
 aktywne interfejsy, 256
 audyt sieci, 264
 ekran początkowy, 256
 przechwytywanie danych
 Telnet, 258
 wyniki nasłuchiwania, 257
 wirtualna sieć prywatna, VPN, 191
 WPS, 253
 dane, 248
 implementacje, 246
 połączenie hybrydowe, 247
 WPS, Wi-Fi Protected Setup, 246
 wstrzykiwanie
 hasel z klawiatury, 45
 WHID, 70
 WSUS, Windows Server Update Services, 193
 graficzny interfejs
 użytkownika, 194
 instalacja, 193
 wykrywanie, detect, 84
 wywiad OSINT, 325
 informacje o hostingu, 327
 narzędzia do pozyskiwania
 danych, 328
 wpisy w WHOIS, 326
 wyszukiwanie DNS, 325

X

XSS, Cross-Site Scripting, 336

Z

- zaawansowane nieuchronne
 - zagrożenie, APT, 174
- zabezpieczanie
 - AD, 198
 - danych, 207
 - podczas przesyłania, 310
 - w stanie spoczynku, 310
 - w użyciu, 311
 - infrastruktury, 416
 - Kubernetes, 313
 - stacji roboczych, 201
 - usług baz danych, 316
 - usług uniksowych, 210
- zabezpieczenia fizyczne
 - IoT, 283
 - kontrola dostępu, 278
 - odstraszające, 278
 - prewencyjne, 278
 - przeglądy, 281
 - typowe dla chmury, 313
 - USB HID, 66
 - wykrywające, 278
 - zasada czystego biurka, 280
- zabezpieczenie
 - kognitywne, 53
 - warstwowe, 51
- zagrożenia fizyczne
 - Key Croc, 275
 - kradzież sprzętu, 277
 - LAN Turtle, 270
 - Packet Squirrel, 272
 - Plunder Bug LAN Tap, 271
 - Screen Crab, 273
 - Shark Jack, 273
 - związane z USB, 276
- zagrożenie wewnętrzne, 127
 - działanie nieumyślne, 127
 - ochrona infrastruktury, 130
 - rozpoznawanie wewnętrznego
 - szkodnika, 129
 - szkodliwy użytkownik, 128
- zapobieganie wykonywaniu
 - danych, DEP, 189
- zapora sieciowa
 - dla aplikacji, WAF, 328
 - iptables, 228
- zarządzanie
 - dziennikami, 233, 387
 - hasłami, 43, 454
 - listami ACL, 225
 - ryzykiem, 78, 449
 - tożsamością i dostępem, IAM, 103
 - uprzywilejowanym dostępem, PAM, 135
 - usługami, 211, 213
 - zagrożeniami, 57
- zasady, 101, 102, 450
 - integracja, 104
 - obiektów grupy, GPO, 168
- zasoby internetowe, 453
- zatrucie pamięci podręcznej
 - DNS, 34
- zbiórca pakiet aktualizacji, 197
- zespół
 - ds. infrastruktury, 184
 - ds. zgodności, 112
- zgodność
 - z przepisami, 110
 - z regulacjami, 110
- Zigbee, 288
- złośliwe oprogramowanie, malware, 29
 - analiza, 370, 381–384
 - dynamiczna, 374
 - hybrydowa, 374
 - interaktywna zachowania, 375
 - statyczna, 373
 - właściwości statycznych, 375
 - zautomatyzowana, 375
- cele, 371
- funkcjonalność, 371
- inżynieria wsteczna kodu, 376
- narzędzia do analizy, 376
- zasady bezpieczeństwa, 380
- zostawianie furtek, 373

PROGRAM PARTNERSKI

— GRUPY HELION —



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion 

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.

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

Packt