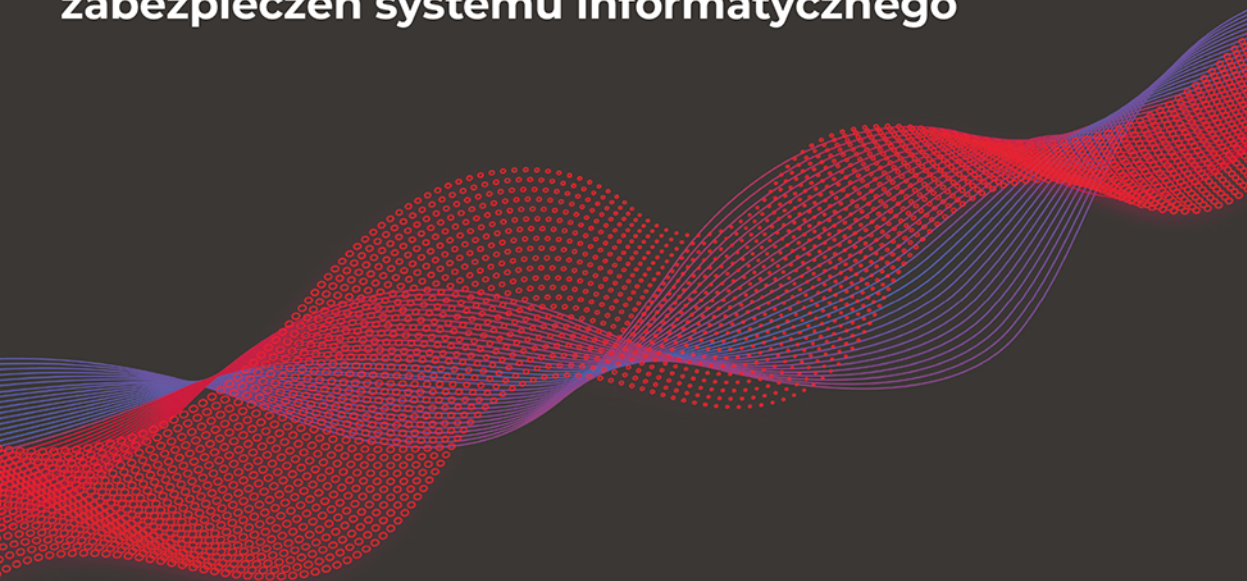


Wydanie III

# Cyberbezpieczeństwo

## Strategie ataku i obrony

Jak osiągnąć najwyższy możliwy stan  
zabezpieczeń systemu informatycznego



**Yuri Diogenes**  
**Erdal Ozkaya**



Helion 

Packt

Tytuł oryginału: Cybersecurity - Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system, 3rd Edition

Tłumaczenie: Lech Lachowski

ISBN: 978-83-8322-421-3

Copyright © Packt Publishing 2022. First published in the English language under the title 'Cybersecurity – Attack and Defense Strategies – Third Edition – (9781803248776)'

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/cybstr>

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](mailto: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 |

|                         |           |
|-------------------------|-----------|
| <b>O autorach .....</b> | <b>15</b> |
|-------------------------|-----------|

|                                         |           |
|-----------------------------------------|-----------|
| <b>O korektorze merytorycznym .....</b> | <b>16</b> |
|-----------------------------------------|-----------|

|                    |           |
|--------------------|-----------|
| <b>Wstęp .....</b> | <b>17</b> |
|--------------------|-----------|

## **ROZDZIAŁ 1**

|                                |           |
|--------------------------------|-----------|
| <b>Stan zabezpieczeń .....</b> | <b>21</b> |
|--------------------------------|-----------|

|                                                                |    |
|----------------------------------------------------------------|----|
| Dlaczego higiena bezpieczeństwa powinna być priorytetem? ..... | 21 |
|----------------------------------------------------------------|----|

|                                 |    |
|---------------------------------|----|
| Obecny krajobraz zagrożeń ..... | 23 |
|---------------------------------|----|

|                                              |    |
|----------------------------------------------|----|
| Ataki z wykorzystaniem łańcucha dostaw ..... | 26 |
|----------------------------------------------|----|

|                  |    |
|------------------|----|
| Ransomware ..... | 28 |
|------------------|----|

|                                                      |    |
|------------------------------------------------------|----|
| Poświadczenia — uwierzytelnianie i autoryzacja ..... | 33 |
|------------------------------------------------------|----|

|                 |    |
|-----------------|----|
| Aplikacje ..... | 35 |
|-----------------|----|

|            |    |
|------------|----|
| Dane ..... | 36 |
|------------|----|

|                                              |    |
|----------------------------------------------|----|
| Wyzwania dotyczące cyberbezpieczeństwa ..... | 37 |
|----------------------------------------------|----|

|                                          |    |
|------------------------------------------|----|
| Stare techniki i szersze rezultaty ..... | 38 |
|------------------------------------------|----|

|                                  |    |
|----------------------------------|----|
| Zmiana krajobrazu zagrożeń ..... | 39 |
|----------------------------------|----|

|                                      |    |
|--------------------------------------|----|
| Poprawianie stanu zabezpieczeń ..... | 41 |
|--------------------------------------|----|

|                                      |    |
|--------------------------------------|----|
| Architektura zerowego zaufania ..... | 43 |
|--------------------------------------|----|

|                                                 |    |
|-------------------------------------------------|----|
| Zarządzanie stanem zabezpieczeń w chmurze ..... | 45 |
|-------------------------------------------------|----|

|                                |    |
|--------------------------------|----|
| Środowisko wielochmurowe ..... | 47 |
|--------------------------------|----|

|                                     |    |
|-------------------------------------|----|
| Zespoły czerwone i niebieskie ..... | 49 |
|-------------------------------------|----|

|                                            |    |
|--------------------------------------------|----|
| Zakładanie naruszenia bezpieczeństwa ..... | 52 |
|--------------------------------------------|----|

|                    |    |
|--------------------|----|
| Podsumowanie ..... | 53 |
|--------------------|----|

|                          |    |
|--------------------------|----|
| Materiały źródłowe ..... | 54 |
|--------------------------|----|

## **ROZDZIAŁ 2**

|                                             |           |
|---------------------------------------------|-----------|
| <b>Proces reagowania na incydenty .....</b> | <b>57</b> |
|---------------------------------------------|-----------|

|                                      |    |
|--------------------------------------|----|
| Proces reagowania na incydenty ..... | 57 |
|--------------------------------------|----|

|                                          |    |
|------------------------------------------|----|
| Dlaczego należy wdrożyć proces IR? ..... | 58 |
|------------------------------------------|----|

|                                                 |    |
|-------------------------------------------------|----|
| Tworzenie procesu reagowania na incydenty ..... | 61 |
|-------------------------------------------------|----|

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| Zespół reagowania na incydenty .....                                      | 63 |
| Cykl życia incydentu .....                                                | 64 |
| Obsługa incydentu .....                                                   | 65 |
| Lista kontrolna dla obsługi incydentów .....                              | 68 |
| Działania po zdarzeniu .....                                              | 69 |
| Scenariusz 1. ....                                                        | 70 |
| Wnioski ze scenariusza 1. ....                                            | 71 |
| Scenariusz 2. ....                                                        | 72 |
| Wnioski ze scenariusza 2. ....                                            | 75 |
| Kwestie związane z reagowaniem na incydenty w chmurze .....               | 76 |
| Aktualizacja procesu IR w celu uwzględnienia charakterystyki chmury ..... | 77 |
| Odpowiedni zestaw narzędzi .....                                          | 78 |
| Proces IR z perspektywy dostawcy rozwiązań w chmurze .....                | 78 |
| Podsumowanie .....                                                        | 79 |
| Materiały źródłowe .....                                                  | 79 |

## ROZDZIAŁ 3

|                                                                                                             |           |
|-------------------------------------------------------------------------------------------------------------|-----------|
| <b>Czym jest cyberstrategia? .....</b>                                                                      | <b>81</b> |
| Jak zbudować cyberstrategię? .....                                                                          | 81        |
| 1. Zrozumienie organizacji .....                                                                            | 82        |
| 2. Zrozumienie zagrożeń i ryzyka .....                                                                      | 82        |
| 3. Odpowiednia dokumentacja .....                                                                           | 83        |
| Dlaczego trzeba budować cyberstrategię? .....                                                               | 84        |
| Najlepsze cyberstrategie ataku .....                                                                        | 86        |
| Strategie testowania zewnętrznego .....                                                                     | 86        |
| Strategie testowania wewnętrznego .....                                                                     | 87        |
| Strategia testowania ślepego .....                                                                          | 87        |
| Strategia testowania ukierunkowanego .....                                                                  | 87        |
| Najlepsze cyberstrategie defensywne .....                                                                   | 88        |
| Obrona w głąb .....                                                                                         | 88        |
| Obrona wszczepiona .....                                                                                    | 89        |
| Korzyści z posiadania proaktywnej strategii cyberbezpieczeństwa .....                                       | 90        |
| Najlepsze strategie cyberbezpieczeństwa dla firm .....                                                      | 92        |
| Szkolenie pracowników w zakresie zasad bezpieczeństwa .....                                                 | 93        |
| Ochrona sieci, informacji i komputerów przed wirusami, złośliwym kodem i oprogramowaniem szpiegującym ..... | 93        |
| Stosowanie firewalla dla wszystkich połączeń internetowych .....                                            | 94        |
| Aktualizowanie oprogramowania .....                                                                         | 94        |
| Korzystanie z kopii zapasowych .....                                                                        | 94        |
| Zaimplementowanie ograniczeń fizycznych .....                                                               | 94        |

|                                                |    |
|------------------------------------------------|----|
| Zabezpieczanie sieci wi-fi .....               | 95 |
| Rotacja haseł .....                            | 95 |
| Ograniczenie dostępu dla pracowników .....     | 95 |
| Stosowanie unikatowych kont użytkowników ..... | 95 |
| Podsumowanie .....                             | 96 |
| Dalsza lektura .....                           | 97 |

## ROZDZIAŁ 4

### **Łańcuch niszczenia cyberzabezpieczeń ..... 98**

|                                                                                                            |     |
|------------------------------------------------------------------------------------------------------------|-----|
| Łańcuch niszczenia cyberzabezpieczeń .....                                                                 | 99  |
| Rekonesans .....                                                                                           | 99  |
| Uzbrajanie .....                                                                                           | 101 |
| Dostarczanie .....                                                                                         | 102 |
| Eksploracja .....                                                                                          | 102 |
| Instalowanie .....                                                                                         | 106 |
| Dowodzenie i kontrola .....                                                                                | 106 |
| Działania na celach .....                                                                                  | 106 |
| Maskowanie .....                                                                                           | 108 |
| Mechanizmy kontroli bezpieczeństwa stosowane<br>do przerywania łańcucha niszczenia cyberzabezpieczeń ..... | 111 |
| UEBA .....                                                                                                 | 113 |
| Świadomość bezpieczeństwa .....                                                                            | 113 |
| Zarządzanie cyklem życia zagrożeń .....                                                                    | 116 |
| Gromadzenie danych kryminalistycznych .....                                                                | 117 |
| Wykrywanie .....                                                                                           | 118 |
| Kwalifikowanie .....                                                                                       | 118 |
| Dochodzenie .....                                                                                          | 118 |
| Neutralizacja .....                                                                                        | 119 |
| Odzyskiwanie sprawności .....                                                                              | 119 |
| Obawy dotyczące łańcucha niszczenia cyberzabezpieczeń .....                                                | 120 |
| Ewolucja łańcucha niszczenia .....                                                                         | 121 |
| Narzędzia używane w łańcuchu niszczenia cyberzabezpieczeń .....                                            | 122 |
| Metasploit .....                                                                                           | 122 |
| Twint .....                                                                                                | 124 |
| Nikto .....                                                                                                | 124 |
| Kismet .....                                                                                               | 126 |
| Sparta .....                                                                                               | 127 |
| John the Ripper .....                                                                                      | 128 |
| Hydra .....                                                                                                | 129 |
| Aircrack-ng .....                                                                                          | 130 |

|                                               |     |
|-----------------------------------------------|-----|
| Airgeddon .....                               | 131 |
| Deauther Board .....                          | 132 |
| HoboCopy .....                                | 133 |
| EvilOSX .....                                 | 134 |
| Platforma Dragon rozwiązania Comodo AEP ..... | 135 |
| Podsumowanie .....                            | 141 |
| Dalsza lektura .....                          | 142 |
| Materiały źródłowe .....                      | 143 |

## ROZDZIAŁ 5

|                                                                |            |
|----------------------------------------------------------------|------------|
| <b>Rekonesans .....</b>                                        | <b>145</b> |
| Rekonesans zewnętrzny .....                                    | 146        |
| Skanowanie mediów społecznościowych celu .....                 | 146        |
| Nurkowanie w śmietnikach .....                                 | 148        |
| Inżynieria społeczna .....                                     | 149        |
| Rekonesans wewnętrzny .....                                    | 157        |
| Narzędzia używane do rekonesansu .....                         | 158        |
| Narzędzia do rekonesansu zewnętrznego .....                    | 159        |
| Narzędzia rekonesansu wewnętrznego .....                       | 177        |
| Airgraph-ng .....                                              | 177        |
| Wardriving .....                                               | 187        |
| Hak5 Plunder Bug .....                                         | 188        |
| Porównanie rekonesansu pasywnego i rekonesansu aktywnego ..... | 191        |
| Metody walki z rekonesansem .....                              | 191        |
| Metody zapobiegania rekonesansowi .....                        | 192        |
| Podsumowanie .....                                             | 193        |
| Materiały źródłowe .....                                       | 194        |

## ROZDZIAŁ 6

|                                              |            |
|----------------------------------------------|------------|
| <b>Włamywanie się do systemów .....</b>      | <b>196</b> |
| Analizowanie aktualnych trendów .....        | 197        |
| Ataki z wymuszeniem .....                    | 197        |
| Ataki z manipulowaniem danymi .....          | 201        |
| Ataki na urządzenia IoT .....                | 204        |
| Backdoory .....                              | 206        |
| Hakowanie urządzeń codziennego użytku .....  | 208        |
| Hakowanie chmury .....                       | 209        |
| Phishing .....                               | 220        |
| Ekspluotowanie luki w zabezpieczeniach ..... | 222        |
| Zero-day .....                               | 224        |

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| Wykonywanie kroków mających na celu złamanie zabezpieczeń systemu .....  | 232 |
| Wdrażanie ładunków .....                                                 | 232 |
| Włamywanie się do systemów operacyjnych .....                            | 236 |
| Włamywanie się do systemu zdalnego .....                                 | 239 |
| Włamywanie się do systemów internetowych .....                           | 241 |
| Ataki na urządzenia mobilne z systemami iOS i Android .....              | 248 |
| Exodus .....                                                             | 249 |
| SensorID .....                                                           | 251 |
| Zhakowanie iPhone'ów przez Cellebrite .....                              | 252 |
| Man-in-the-disk .....                                                    | 253 |
| Spearphone (przechwytywanie danych głośnika na Androidzie) .....         | 254 |
| Tap 'n Ghost .....                                                       | 254 |
| Narzędzia zespołów czerwonych i niebieskich dla urządzeń mobilnych ..... | 256 |
| Podsumowanie .....                                                       | 258 |
| Dalsza lektura .....                                                     | 260 |
| Materiały źródłowe .....                                                 | 260 |

## ROZDZIAŁ 7

|                                                               |            |
|---------------------------------------------------------------|------------|
| <b>W pogoni za tożsamością użytkownika .....</b>              | <b>263</b> |
| Tożsamość to nowe granice .....                               | 263        |
| Poświadczenia i automatyzacja .....                           | 266        |
| Strategie hakowania tożsamości użytkownika .....              | 267        |
| Uzyskanie dostępu do sieci .....                              | 268        |
| Zbieranie poświadczeń .....                                   | 269        |
| Hakowanie tożsamości użytkownika .....                        | 271        |
| Brute force .....                                             | 271        |
| Inżynieria społeczna .....                                    | 273        |
| Pass the hash .....                                           | 279        |
| Kradzież tożsamości za pośrednictwem urządzeń mobilnych ..... | 282        |
| Inne metody hakowania tożsamości .....                        | 282        |
| Podsumowanie .....                                            | 283        |
| Materiały źródłowe .....                                      | 283        |

## ROZDZIAŁ 8

|                                     |            |
|-------------------------------------|------------|
| <b>Ruch boczny .....</b>            | <b>285</b> |
| Infiltracja .....                   | 286        |
| Mapowanie sieci .....               | 286        |
| Przeskanuj, zablokuj i napraw ..... | 289        |
| Blokowanie i spowalnianie .....     | 291        |

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| Wykrywanie skanów Nmapa .....                                                         | 292 |
| Wykorzystanie sprytnych sztuczek .....                                                | 293 |
| Wykonywanie ruchu bocznego .....                                                      | 295 |
| Etap 1. — zhakowany użytkownik (działanie użytkownika) .....                          | 295 |
| Etap 2. — dostęp administratora stacji roboczej (użytkownik =<br>administrator) ..... | 296 |
| Myśl jak haker .....                                                                  | 297 |
| Unikanie alertów .....                                                                | 298 |
| Skanowanie portów .....                                                               | 299 |
| Sysinternals .....                                                                    | 300 |
| Udziały plików .....                                                                  | 302 |
| Windows DCOM .....                                                                    | 304 |
| Pulpit zdalny .....                                                                   | 305 |
| PowerShell .....                                                                      | 307 |
| Windows Management Instrumentation .....                                              | 309 |
| Zaplanowane zadania .....                                                             | 311 |
| Kradzież tokenów .....                                                                | 311 |
| Skradzione poświadczenia .....                                                        | 312 |
| Nośniki wymienne .....                                                                | 313 |
| Skażone treści udostępniane .....                                                     | 313 |
| Rejestr zdalny .....                                                                  | 313 |
| TeamViewer .....                                                                      | 314 |
| Wdrażanie aplikacji .....                                                             | 315 |
| Sniffing sieci .....                                                                  | 315 |
| Spoofing ARP .....                                                                    | 315 |
| AppleScript i IPC (OS X) .....                                                        | 316 |
| Analiza zhakowanego hosta .....                                                       | 317 |
| Centralne konsole administracyjne .....                                               | 317 |
| Plądrowanie poczty elektronicznej .....                                               | 317 |
| Usługa Active Directory .....                                                         | 318 |
| Udziały administratora .....                                                          | 320 |
| Pass the Ticket .....                                                                 | 320 |
| Pass-the-Hash (PtH) .....                                                             | 320 |
| Winlogon .....                                                                        | 322 |
| Proces lsass.exe .....                                                                | 322 |
| Podsumowanie .....                                                                    | 326 |
| Dalsza lektura .....                                                                  | 326 |
| Materiały źródłowe .....                                                              | 327 |

**ROZDZIAŁ 9**

|                                                                                              |            |
|----------------------------------------------------------------------------------------------|------------|
| <b>Podnoszenie poziomu uprawnień .....</b>                                                   | <b>328</b> |
| Infiltracja .....                                                                            | 329        |
| Poziome podnoszenie uprawnień .....                                                          | 329        |
| Pionowe podnoszenie uprawnień .....                                                          | 331        |
| Jak działa podnoszenie poziomu uprawnień? .....                                              | 331        |
| Eksplatacja poświadczeń .....                                                                | 332        |
| Błędne konfiguracje .....                                                                    | 333        |
| Luki w zabezpieczeniach i eksploity podnoszenia uprawnień .....                              | 334        |
| Inżynieria społeczna .....                                                                   | 336        |
| Złośliwe oprogramowanie .....                                                                | 337        |
| Unikanie alertów .....                                                                       | 337        |
| Podnoszenie uprawnień .....                                                                  | 339        |
| Eksplatacja niezaktualizowanych systemów operacyjnych .....                                  | 341        |
| Manipulacja tokenami dostępu .....                                                           | 342        |
| Eksplatacja funkcjonalności ułatwień dostępu .....                                           | 344        |
| Shimming aplikacji .....                                                                     | 346        |
| Omijanie kontroli konta użytkownika .....                                                    | 349        |
| Luka w zabezpieczeniach podnoszenia uprawnień i ucieczki<br>z kontenera (CVE-20220492) ..... | 352        |
| Wstrzyknięcie biblioteki DLL .....                                                           | 352        |
| Zhakowanie kolejności przeszukiwania bibliotek DLL .....                                     | 354        |
| Przejęcie biblioteki dynamicznej .....                                                       | 355        |
| Eksploracja luk w zabezpieczeniach .....                                                     | 355        |
| Demon startowy .....                                                                         | 357        |
| Praktyczny przykład podnoszenia uprawnień<br>w docelowym systemie Windows .....              | 358        |
| Zrzucanie pliku SAM .....                                                                    | 360        |
| Rootowanie Androida .....                                                                    | 361        |
| Korzystanie z pliku /etc/passwd .....                                                        | 361        |
| Wstrzyknięcie EWM .....                                                                      | 362        |
| Stosowanie zaczepów .....                                                                    | 362        |
| Zaplanowane zadania .....                                                                    | 363        |
| Nowe usługi .....                                                                            | 364        |
| Elementy startowe .....                                                                      | 364        |
| Buforowanie sudo .....                                                                       | 365        |
| Dodatkowe narzędzia do podnoszenia uprawnień .....                                           | 365        |
| Oxsp Mongoose v1.7 .....                                                                     | 366        |
| Oxsp Mongoose RED dla systemu Windows .....                                                  | 367        |
| Hot Potato .....                                                                             | 367        |

|                          |     |
|--------------------------|-----|
| Wnioski .....            | 368 |
| Podsumowanie .....       | 369 |
| Materiały źródłowe ..... | 369 |

## ROZDZIAŁ 10

|                                                                                       |            |
|---------------------------------------------------------------------------------------|------------|
| <b>Reguły bezpieczeństwa .....</b>                                                    | <b>371</b> |
| Przegląd reguł bezpieczeństwa .....                                                   | 371        |
| Przesunięcie w lewo .....                                                             | 373        |
| Edukacja użytkownika końcowego .....                                                  | 375        |
| Wytyczne dla użytkowników w zakresie bezpieczeństwa<br>mediów społecznościowych ..... | 375        |
| Szkolenie w zakresie świadomości bezpieczeństwa .....                                 | 377        |
| Egzekwowanie reguł .....                                                              | 378        |
| Reguły w chmurze .....                                                                | 380        |
| Biała lista aplikacji .....                                                           | 382        |
| Zwiększanie zabezpieczeń .....                                                        | 385        |
| Monitorowanie zgodności .....                                                         | 387        |
| Automatyzacja .....                                                                   | 389        |
| Ciągła poprawa stanu zabezpieczeń dzięki regułom bezpieczeństwa .....                 | 390        |
| Podsumowanie .....                                                                    | 392        |
| Materiały źródłowe .....                                                              | 393        |

## ROZDZIAŁ 11

|                                                         |            |
|---------------------------------------------------------|------------|
| <b>Bezpieczeństwo sieciowe .....</b>                    | <b>394</b> |
| Obrona w głąb .....                                     | 394        |
| Infrastruktura i usługi .....                           | 395        |
| Przesyłane dokumenty .....                              | 397        |
| Punkty końcowe .....                                    | 399        |
| Mikrosegmentacja .....                                  | 399        |
| Fizyczna segmentacja sieci .....                        | 400        |
| Wykrywanie sieci za pomocą narzędzia do mapowania ..... | 402        |
| Zabezpieczanie zdalnego dostępu do sieci .....          | 404        |
| VPN site-to-site .....                                  | 406        |
| Segmentacja sieci wirtualnej .....                      | 407        |
| Sieć zerowego zaufania .....                            | 409        |
| Planowanie wdrożenia sieci zerowego zaufania .....      | 411        |
| Bezpieczeństwo sieci hybrydowej w chmurze .....         | 412        |
| Widoczność sieci w chmurze .....                        | 414        |
| Podsumowanie .....                                      | 418        |
| Materiały źródłowe .....                                | 418        |

**ROZDZIAŁ 12**

|                                                         |            |
|---------------------------------------------------------|------------|
| <b>Aktywne czujniki .....</b>                           | <b>419</b> |
| Funkcjonalności wykrywania .....                        | 419        |
| Wskaźniki naruszenia bezpieczeństwa .....               | 420        |
| System wykrywania włamań .....                          | 425        |
| System zapobiegania włamaniom .....                     | 428        |
| Wykrywanie na podstawie reguł .....                     | 428        |
| Wykrywanie na podstawie anomalii .....                  | 429        |
| Analityka behawioralna w infrastrukturze lokalnej ..... | 429        |
| Umieszczenie urządzenia .....                           | 433        |
| Analityka behawioralna w chmurze hybrydowej .....       | 433        |
| Microsoft Defender for Cloud .....                      | 434        |
| Analityka dla obciążeń roboczych PaaS .....             | 436        |
| Podsumowanie .....                                      | 438        |
| Materiały źródłowe .....                                | 439        |

**ROZDZIAŁ 13**

|                                                                          |            |
|--------------------------------------------------------------------------|------------|
| <b>Analiza zagrożeń .....</b>                                            | <b>440</b> |
| Analiza zagrożeń .....                                                   | 440        |
| Narzędzia do analizy zagrożeń udostępniane na licencji open source ..... | 445        |
| Bezpłatne źródła informacji o zagrożeniach .....                         | 449        |
| MITRE ATT&CK .....                                                       | 452        |
| Analiza zagrożeń oferowana przez Microsoft .....                         | 458        |
| Microsoft Sentinel .....                                                 | 458        |
| Podsumowanie .....                                                       | 461        |
| Materiały źródłowe .....                                                 | 461        |

**ROZDZIAŁ 14**

|                                                                                     |            |
|-------------------------------------------------------------------------------------|------------|
| <b>Badanie incydentu .....</b>                                                      | <b>462</b> |
| Ustalanie zakresu problemu .....                                                    | 462        |
| Kluczowe artefakty .....                                                            | 463        |
| Badanie włamania do systemu lokalnego .....                                         | 469        |
| Badanie włamania do systemu w chmurze hybrydowej .....                              | 473        |
| Integracja Defender for Cloud z systemem SIEM<br>w celu przeprowadzania badań ..... | 479        |
| Proaktywne badanie (polowanie na zagrożenia) .....                                  | 482        |
| Wnioski .....                                                                       | 485        |
| Podsumowanie .....                                                                  | 486        |
| Materiały źródłowe .....                                                            | 486        |

**ROZDZIAŁ 15**

|                                                                            |            |
|----------------------------------------------------------------------------|------------|
| <b>Proces odzyskiwania sprawności .....</b>                                | <b>487</b> |
| Plan odzyskiwania sprawności po katastrofie .....                          | 488        |
| Proces planowania odzyskiwania sprawności po katastrofie .....             | 489        |
| Wyzwania .....                                                             | 493        |
| Odzyskiwanie sprawności bez przestojów .....                               | 494        |
| Planowanie awaryjne .....                                                  | 495        |
| Proces planowania awaryjnego IT .....                                      | 496        |
| Narzędzia zarządzania ryzykiem .....                                       | 502        |
| Plan ciągłości działania .....                                             | 504        |
| Planowanie ciągłości działania .....                                       | 505        |
| Jak opracować plan ciągłości działania? .....                              | 506        |
| Siedem kroków do utworzenia skutecznego planu ciągłości działania .....    | 507        |
| Najlepsze praktyki w zakresie odzyskiwania sprawności po katastrofie ..... | 509        |
| Najlepsze praktyki lokalne .....                                           | 510        |
| Najlepsze praktyki w chmurze .....                                         | 510        |
| Najlepsze praktyki w środowisku hybrydowym .....                           | 511        |
| Podsumowanie .....                                                         | 512        |
| Dalsza lektura .....                                                       | 512        |
| Materiały źródłowe .....                                                   | 513        |

**ROZDZIAŁ 16**

|                                                                                             |            |
|---------------------------------------------------------------------------------------------|------------|
| <b>Zarządzanie lukami w zabezpieczeniach .....</b>                                          | <b>514</b> |
| Tworzenie strategii zarządzania lukami w zabezpieczeniach .....                             | 515        |
| Inwentaryzacja zasobów .....                                                                | 516        |
| Zarządzanie informacjami .....                                                              | 517        |
| Ocena ryzyka .....                                                                          | 519        |
| Ocena luk w zabezpieczeniach .....                                                          | 524        |
| Raportowanie i śledzenie procesu remediacji .....                                           | 525        |
| Planowanie reagowania .....                                                                 | 526        |
| Elementy strategii zarządzania lukami w zabezpieczeniach .....                              | 528        |
| Różnice między zarządzaniem lukami w zabezpieczeniach<br>a przeprowadzaniem ich oceny ..... | 529        |
| Najlepsze praktyki zarządzania lukami w zabezpieczeniach .....                              | 530        |
| Strategie usprawniające zarządzanie lukami w zabezpieczeniach .....                         | 533        |
| Narzędzia do zarządzania lukami w zabezpieczeniach .....                                    | 535        |
| Narzędzia do inwentaryzacji zasobów .....                                                   | 536        |
| Narzędzia do zarządzania ryzykiem .....                                                     | 538        |
| Narzędzia do oceny ryzyka .....                                                             | 541        |
| Narzędzia do oceny luk w zabezpieczeniach .....                                             | 541        |

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| Narzędzia do raportowania i śledzenia remediacji .....                                    | 543 |
| Narzędzia do planowania reagowania .....                                                  | 543 |
| Intruder .....                                                                            | 544 |
| Patch Manager Plus .....                                                                  | 545 |
| Windows Server Update Services (WSUS) .....                                               | 546 |
| Platforma Comodo Dragon .....                                                             | 547 |
| InsightVM .....                                                                           | 548 |
| Azure Threat and Vulnerability Management .....                                           | 548 |
| Implementowanie zarządzania lukami w zabezpieczeniach<br>za pomocą narzędzia Nessus ..... | 549 |
| OpenVAS .....                                                                             | 556 |
| Qualys .....                                                                              | 556 |
| Acunetix .....                                                                            | 558 |
| Wnioski .....                                                                             | 559 |
| Podsumowanie .....                                                                        | 559 |
| Dalsza lektura .....                                                                      | 560 |
| Materiały źródłowe .....                                                                  | 560 |

## ROZDZIAŁ 17

|                                                                              |            |
|------------------------------------------------------------------------------|------------|
| <b>Analiza dzienników .....</b>                                              | <b>562</b> |
| Korelacja danych .....                                                       | 562        |
| Dzienniki systemów operacyjnych .....                                        | 564        |
| Dzienniki systemu Windows .....                                              | 564        |
| Dzienniki systemu Linux .....                                                | 566        |
| Dzienniki firewalla .....                                                    | 567        |
| Dzienniki serwera WWW .....                                                  | 569        |
| Dzienniki platformy AWS .....                                                | 570        |
| Dostęp do dzienników AWS z poziomu usługi Microsoft Sentinel .....           | 572        |
| Dzienniki Azure Activity .....                                               | 574        |
| Dostęp do dzienników Azure Activity z poziomu usługi Microsoft Sentinel .... | 575        |
| Dzienniki platformy GCP .....                                                | 577        |
| Podsumowanie .....                                                           | 579        |
| Materiały źródłowe .....                                                     | 580        |

|                        |            |
|------------------------|------------|
| <b>Skorowidz .....</b> | <b>581</b> |
|------------------------|------------|



# Czym jest cyberstrategia?

## Rozdział 3

Cyberstrategia to udokumentowane podejście do różnych aspektów cyberprzestrzeni. Jest opracowywana głównie w celu zaspokojenia potrzeb cyberbezpieczeństwa określonego podmiotu przez zdefiniowanie sposobu ochrony danych, sieci, systemów technicznych i ludzi. Skuteczna cyberstrategia jest zwykle powiązana ze stopniem ryzyka naruszenia cyberbezpieczeństwa podmiotu. Obejmuje wszystkie możliwe wektory ataków, które mogą być wykorzystywane przez złośliwe strony zewnętrzne.

W większości cyberstrategii centralne miejsce zajmuje cyberbezpieczeństwo, gdyż zagrożenia cybernetyczne stają się coraz bardziej zaawansowane, w miarę jak dla aktorów zagrożenia stają się dostępne coraz lepsze narzędzia i techniki eksploatacji. W związku z tymi zagrożeniami zaleca się organizacjom opracowanie cyberstrategii, które zapewnią ochronę ich infrastruktury cybernetycznej i zmniejszą ryzyko.

W tym rozdziale zostaną omówione następujące tematy:

- budowanie strategii marketingowej;
- cele budowania cyberstrategii;
- najlepsze strategie cyberataków;
- najlepsze strategie cyberobrony;
- korzyści z posiadania proaktywnej strategii cyberbezpieczeństwa;
- najlepsze strategie cyberbezpieczeństwa dla firm.

Zacznijmy od omówienia podstawowych elementów potrzebnych do zbudowania cyberstrategii.

## Jak zbudować cyberstrategię?

W VI w. p.n.e. Sun Tzu powiedział: „Jeśli znasz siebie i swego wroga, przetrwasz pomyślnie sto bitew.

Jeśli nie poznasz swego wroga, lecz poznasz siebie, jedną bitwę wygrasz, a drugą przegrasz. Jeśli nie poznasz ni siebie, ni wroga, każda potyczka będzie dla ciebie zagrożeniem”.

Ten cytat wciąż ma zastosowanie do cyberstrategii i wyjaśnia, dlaczego tak ważne jest zrozumienie zarówno swojej firmy, jak i zagrożeń, jakie stwarzają dla niej cyberprzestępcy — będzie to stanowić podstawę silnej cyberstrategii, która pomoże chronić Twoją firmę przed atakiem.

Do zbudowania cyberstrategii będziesz potrzebować trzech głównych filarów, dzięki którym utworzysz solidne fundamenty. Pokazaliśmy to na rysunku 3.1.



Rysunek 3.1. Podstawy cyberstrategii

Te trzy komponenty mają kluczowe znaczenie dla zrozumienia, co zapewnia skuteczność cyberstrategii.

## 1. Zrozumienie organizacji

Im więcej wiesz o swojej firmie, tym lepiej możesz ją zabezpieczyć. Bardzo ważne jest, aby poznać cele i zadania swojej organizacji, ludzi, z którymi się pracuje, branżę i jej aktualne trendy, a także ryzyko, jakie grozi firmie, oraz jej apetyt na ryzyko i najcenniejsze aktywa. Posiadanie kompletnego spisu aktywów jest niezbędne do ustalenia priorytetów planów strategicznych na podstawie ryzyka i wpływu ataku na te aktywa. Wszystko, co robimy, musi odzwierciedlać wymagania biznesowe zatwierdzone przez kierownictwo wyższego szczebla.

## 2. Zrozumienie zagrożeń i ryzyka

Nie jest łatwo zdefiniować ryzyko, ponieważ słowo „ryzyko” jest używane na wiele różnych sposobów. Chociaż istnieje wiele definicji tego terminu, norma ISO 31000 definiuje ryzyko jako „wpływ niepewności na cele”, gdzie wpływ określa pozytywne lub negatywne odchylenie od stanu oczekiwanego. W tym przypadku posłużymy się definicją ryzyka z normy ISO.

Słowo „ryzyko” łączy w sobie trzy elementy: zaczyna od potencjalnego zdarzenia, a następnie łączy jego prawdopodobieństwo z jego potencjalną dotkliwością. W wielu szkoleniach na temat zarządzania ryzykiem ryzyko jest definiowane następująco (zobacz rysunek 3.2):

$$\text{Ryzyko (potencjalna strata)} = \text{zagrożenie} \cdot \text{podatność} \cdot \text{aktywa}$$



Rysunek 3.2. Ilustracja definicji ryzyka

Trzeba zrozumieć, że nie do wszystkich zagrożeń warto stosować środki zaradcze. Jeśli środki zaradcze będą kosztowniejsze niż wdrożenie albo ryzyko nie będzie poważne, może ono zostać zaakceptowane.

### 3. Odpowiednia dokumentacja

Dokumentacja działa jako rodzaj normalizacji różnych procesów, która zapewnia, że wszyscy w organizacji pracują w ten sam sposób i dążą do tego samego wyniku. Jest to kluczowy aspekt każdej strategii i odgrywa szczególnie ważną rolę, jeśli chodzi o zapewnienie ciągłości działania firmy. Dokumentowanie planu cyberstrategii zapewni wydajność, spójność i spokój ducha wszystkim zaangażowanym stronom. Dokumentacja nie powinna być jednak traktowana jako działanie jednorazowe, ponieważ nawet po spisaniu planu cyberstrategii nadal będzie wymagała aktualizowania w celu odzwierciedlania zmian w krajobrazie cyberbezpieczeństwa.

Na rysunku 3.3 pokazaliśmy przykład tego, co powinna uwzględniać dobra dokumentacja cyberstrategii.

Możemy podsumować, że cyberstrategia to plan zarządzania ryzykiem bezpieczeństwa organizacyjnego zgodnie z firmową definicją tolerancji ryzyka z zamiarem realizacji celów biznesowych i organizacyjnych. Cyberstrategia powinna być w pełni zgodna ze strategią biznesową, a także z czynnikami i celami biznesowymi. Po zapewnieniu tej zgodności można budować aspekty techniczne i zwiększać poziom bezpieczeństwa cyberstrategii w cyberprzestrzeni. Omówimy te aspekty dalej w rozdziale, ale teraz, gdy znasz już podstawy opracowywania cyberstrategii, poświęćmy chwilę na omówienie korzyści, jakie przynosi jej wdrożenie.



Rysunek 3.3. Elementy, które powinien uwzględniać plan cyberstrategii

## Dlaczego trzeba budować cyberstrategię?

Organizacje stale zmagają się z zagrożeniami, jakimi są ataki przeprowadzane przez zatwardziały profesjonalnych cyberprzestępców. Smutna rzeczywistość jest taka, że wiele włamań przeprowadzają państwa narodowe, cyberterroryści i potężne grupy cyberprzestępcze. Istnieje czarny rynek dla hakerów, który ułatwia zakup lub wynajem narzędzi, technik i personelu do dokonywania włamań, a ponadto umożliwia pranie pieniędzy pozyskanych z udanych ataków. Nierzadko atakujący mają znacznie większą wiedzę techniczną w zakresie cyberbezpieczeństwa niż przeciętny pracownik działu IT. Dlatego atakujący mogą wykorzystać swoją zaawansowaną wiedzę, aby łatwo ominąć wiele narzędzi cyberobrony skonfigurowanych przez działy IT w wielu organizacjach.

Wymaga to zatem przededefiniowania sposobu, w jaki organizacje powinny radzić sobie z zagrożeniami cybernetycznymi i aktorami zagrożeń, gdyż pozostawienie tych zadań działowi IT nie jest wystarczające. Chociaż jeszcze kilka lat temu zwiększanie poziomu zabezpieczenia systemów i instalowanie większej liczby narzędzi bezpieczeństwa mogło się sprawdzać, dziś organizacje potrzebują dobrze przemyślanej cyberstrategii, która będzie kierować działaniami z zakresu cyberobrony. Oto niektóre z powodów, dla których cyberstrategie są niezbędne:

- Cyberstrategie dostarczają szczegółowych informacji na temat taktyki bezpieczeństwa — określają ogólne taktyki zapewnienia bezpieczeństwa organizacji. Taktyki te dotyczą procesów reagowania na incydenty, planów przywracania sprawności po katastrofie i ciągłości biznesowej oraz reakcji behawioralnych na ataki, aby pomóc dodatkowo uspokoić interesariuszy. Mogą być pomocne w informowaniu interesariuszy o gotowości organizacji do radzenia sobie z cyberatakami.
- Cyberstrategie odchodzą od założeń — niektóre defensywne mechanizmy cyberbezpieczeństwa stosowane obecnie w organizacjach opierają się na założeniach przyjmowanych przez dział IT lub konsultantów ds. cyberbezpieczeństwa. Zawsze istnieje jednak ryzyko, że te założenia mogą być mylące i być może dostosowane tylko do określonego celu, takiego jak zapewnianie zgodności z normami. Natomiast cyberstrategie to świadome plany działania obejmujące różne zagrożenia cybernetyczne i związane z nimi ryzyko. Ponadto ich opracowywaniu przyświeca wspólny cel końcowy: dostosowanie celów bezpieczeństwa do celów biznesowych.
- Cyberstrategie poprawiają działanie organizacji — zapewniają scentralizowaną kontrolę i podejmowanie decyzji w sprawach dotyczących cyberbezpieczeństwa, ponieważ są budowane we współpracy z różnymi interesariuszami. Gwarantuje to, że różne działy w organizacji mogą pracować w koordynacji, aby osiągnąć wspólny zestaw celów bezpieczeństwa. Menedżerowie liniowi mogą na przykład instruować młodszych pracowników, aby nie udostępniali danych logowania, co może zapobiec phishingowi. Zgodnie z cyberstrategią taki niewielki wkład różnych działów firmy pomaga poprawić ogólny stan zabezpieczeń organizacji.
- Cyberstrategia dowodzi długoterminowego zaangażowania w bezpieczeństwo — zapewnia, że organizacja będzie podejmować znaczące wysiłki i angażować istotne zasoby w celu zagwarantowania bezpieczeństwa. Takie zaangażowanie jest dobrym sygnałem dla interesariuszy, że organizacja pozostanie bezpieczna podczas ataków.
- Cyberstrategia upraszcza kwestie cyberbezpieczeństwa dla interesariuszy — pomaga zrozumieć złożone zagadnienia z zakresu cyberbezpieczeństwa. Informuje wszystkich interesariuszy o ryzyku i zagrożeniach w cyberprzestrzeni, a następnie wyjaśnia, w jaki sposób są one łagodzone za pośrednictwem zestawu niewielkich osiągalnych celów.

Możemy podsumować, że bez cyberstrategii nie zoptymalizujesz swojej inwestycji, nie nadasz priorytetu potrzebom firmy, a ogólny stan zabezpieczenia stanie się znacznie bardziej złożony.

Cyberstrategie mogą przyjmować dwa podejścia do kwestii bezpieczeństwa: perspektywę defensywną lub perspektywę ataku. W perspektywie defensywnej cyberstrategia koncentruje się na informowaniu interesariuszy o strategiach defensywy, które organizacja wdrożyła w celu ochrony przed zidentyfikowanymi zagrożeniami. Natomiast cyberstrategie przyjmujące perspektywę ataku mogą koncentrować się na udowodnieniu skuteczności istniejących zabezpieczeń, aby znaleźć wady i je naprawić. Dlatego strategie ataku mogą w szerokim zakresie obejmować różne metody, które będą wykorzystywane do testowania gotowości organizacji na atak. Niektóre strategie mogą być połączeniem tych dwóch perspektyw, uwzględniając testowanie i wzmacnianie istniejących mechanizmów defensywnych. Wybrane podejście będzie zależało od dostępnych zasobów i celów biznesowych. W następnych podrozdziałach omówimy niektóre powszechnie stosowane cyberstrategie ataku i defensywy.

## Najlepsze cyberstrategie ataku

Jednym z najlepszych sposobów zabezpieczania organizacji jest myślenie z perspektywy hakera i podejmowanie prób naruszenia bezpieczeństwa organizacji przy użyciu tych samych narzędzi i technik, których użyłby przeciwnik.

Strategie defensywne można testować przez wykonywanie zewnętrznych testów spoza sieci lub testów wewnętrznych. Te procesy testowe mają na celu zapewnienie, że zaimplementowana strategia bezpieczeństwa będzie skuteczna i zgodna z celami procesów biznesowych.

W kolejnych punktach przedstawimy niektóre z najlepszych cyberstrategii ataku, jakie organizacje powinny wziąć pod uwagę podczas testowania swoich systemów.

## Strategie testowania zewnętrznego

Te strategie testowania obejmują próby naruszenia bezpieczeństwa organizacji z zewnątrz, czyli spoza jej sieci. W takim przypadku w celach testowych cyberataki będą kierowane na publicznie dostępne zasoby. Można zaatakować firewall na przykład za pomocą ataku DDoS, aby uniemożliwić przepływ do sieci organizacji dozwolonego ruchu. Ataki kieruje się także na serwery pocztowe w celu zablokowania komunikacji e-mailowej w organizacji. Celem ataków mogą być również serwery WWW, na których można potencjalnie znaleźć niewłaściwie umieszczone pliki, takie jak poufne informacje przechowywane w publicznie dostępnych folderach. Do innych popularnych celów należą m.in. serwery nazw domenowych (ang. *Domain Name Server* — DNS) i systemy wykrywania włamań (ang. *Intrusion Detection System* — IDS), które zwykle są udostępniane publicznie. Poza systemami technicznymi zewnętrzne strategie testowania obejmują także ataki skierowane na personel lub użytkowników. Takie

ataki mogą być przeprowadzane za pośrednictwem platform mediów społecznościowych, e-maili i połączeń telefonicznych. Najczęściej stosowaną metodą ataku jest inżynieria społeczna, w której cele są przekonywane do dzielenia się poufnymi informacjami lub wysyłania pieniędzy, aby opłacić nieistniejące usługi, zapłacić okup itd., dlatego zewnętrzne strategie testowania powinny naśladować te ataki.

## Strategie testowania wewnętrznego

Obejmują one ataki przeprowadzane w obrębie organizacji w celu naśladowania zagrożeń wewnętrznych, które mogą próbować złamać zabezpieczenia organizacji. Tego rodzaju zagrożenia mogą stanowić niezadowoleni pracownicy i goście ze złośliwymi intencjami. Wewnętrzne testy naruszenia bezpieczeństwa zawsze zakładają, że przeciwnik ma standardowe uprawnienia dostępu, zna miejsce przechowywania poufnych informacji i może uniknąć wykrycia, a nawet wyłączyć niektóre narzędzia bezpieczeństwa.

Celem testów wewnętrznych jest wzmocnienie zabezpieczeń systemów udostępnianych regularnym użytkownikom, aby utrudnić włamanie się do nich. Niektóre z technik stosowanych w testach zewnętrznych mogą być stosowane także w testach wewnętrznych, ale wewnątrz sieci ich wydajność często wzrasta, gdyż mają one do dyspozycji więcej celów.

## Strategia testowania ślepego

Jest to strategia testowa, która ma na celu zaskoczenie organizacji. Testowanie odbywa się to przy ograniczonym informowaniu działu IT, aby jego pracownicy mogli potraktować je jako prawdziwy atak. Testowanie ślepe polega na atakowaniu narzędzi bezpieczeństwa, wykonywaniu prób złamania zabezpieczeń sieci i obieraniu za cel użytkowników, aby uzyskać od nich poświadczenia lub poufne informacje. Takie testowanie jest często kosztowne, ponieważ zespół testerów nie otrzymuje żadnej formy wsparcia ze strony działu IT, aby uniknąć ostrzegania go o planowanych atakach. Jednak często prowadzi do odkrycia wielu nieznanych luk w zabezpieczeniach.

## Strategia testowania ukierunkowanego

Ten typ testów izoluje tylko jeden cel i przeprowadza na nim wiele ataków, aby odkryć te, które mogą się powieść. Jest to bardzo skuteczne podczas testowania nowych systemów lub określonych aspektów cyberbezpieczeństwa, takich jak reagowanie na incydenty związane z atakami wymierzonymi w kluczowe systemy. Jednak ze względu na wąski zakres testy ukierunkowane nie dają pełnych informacji na temat podatności na ataki całej organizacji.

# Najlepsze cyberstrategie defensywne

Cyberbezpieczeństwo często sprowadza się głównie do systemów defensywnych wdrożonych przez organizację. Istnieją dwie strategię defensywne powszechnie stosowane przez organizacje: obrona w głąb i obrona wszcz.

## Obrona w głąb

Obrona w głąb (ang. *defense in depth*) jest również określana jako zabezpieczanie warstwowe i obejmuje zastosowanie warstwowych mechanizmów defensywnych, aby utrudnić atakującym włamanie się do organizacji. Ponieważ stosuje się wiele warstw zabezpieczeń, po złamaniu jednego poziomu zabezpieczeń atakujący napotyka jedynie kolejny poziom. Ze względu na tę redundancję próba włamania się do systemów staje się złożona i kosztowna dla hakerów.

Strategia obrony w głąb wydaje się atrakcyjna dla organizacji, które uważają, że żadna pojedyncza warstwa zabezpieczeń nie jest odporna na ataki. Dlatego zawsze stosuje się wiele systemów defensywnych w celu ochrony systemów, sieci i danych. Organizacja, która chce chronić na przykład swój serwer plików, może wdrożyć w swojej sieci system wykrywania włamań i firewall. Może również zainstalować na serwerze program antywirusowy dla punktów końcowych i jeszcze lepiej szyfrować jego zawartość. Ponadto może wyłączyć zdalny dostęp i zastosować uwierzytelnianie dwuskładnikowe dla każdej próby logowania. Każdy haker próbujący uzyskać dostęp do poufnych plików na serwerze będzie musiał skutecznie złamać wszystkie te warstwy zabezpieczeń. Szanse na powodzenia są bardzo małe, ponieważ każda warstwa bezpieczeństwa ma własną złożoność. Oto typowe komponenty podejścia obrony w głąb:

- **Bezpieczeństwo sieci** — ponieważ sieci są najbardziej narażonymi powierzchniami ataku, pierwsza linia obrony ma zwykle na celu ich ochronę. Dział IT może zainstalować firewall, aby zablokować złośliwy ruch, a także uniemożliwić użytkownikom wewnętrznym wysyłanie złośliwego ruchu lub odwiedzanie złośliwych sieci.

Ponadto w sieci wdrażane są systemy wykrywania włamań, które pomagają wykrywać podejrzone działania. Ze względu na powszechne stosowanie przeciwko firewallom ataków DDoS zaleca się organizacjom kupowanie firewalli, które mogą wytrzymać takie ataki w sposób ciągły.

- **Ochrona hostów** (bezpieczeństwo komputerów i serwerów) — w ochronie urządzeń komputerowych przed zainfekowaniem złośliwym oprogramowaniem są niezbędne systemy antywirusowe. Nowoczesne systemy antywirusowe są wyposażone w dodatkowe funkcjonalności, takie jak wbudowane firewalle, które można wykorzystać do dalszego zabezpieczenia hosta w sieci.

- **Szyfrowanie** — jest często najbardziej zaufaną linią obrony, gdyż opiera się na złożoności matematycznej. Organizacje decydują się na szyfrowanie poufnych danych, aby zapewnić dostęp do nich wyłącznie upoważnionemu personelowi. Kiedy takie dane zostaną ukradzione, nie będzie to duży cios dla organizacji, ponieważ większość algorytmów szyfrowania nie jest łatwa do złamania.
- **Kontrola dostępu** — kontrola dostępu jest stosowana jako metoda ograniczania za pomocą uwierzytelniania zakresu osób, które mogą uzyskiwać dostęp do określonych zasobów w sieci. Organizacje często łączą fizyczne i logiczne mechanizmy kontroli dostępu, aby utrudnić potencjalnym hakerom ich złamanie. Fizyczne mechanizmy kontroli obejmują stosowanie zamków i ochroniarzy, aby uniemożliwić fizyczny dostęp do wrażliwych obszarów, takich jak serwerownie. Natomiast logiczne mechanizmy kontroli wiążą się z użyciem uwierzytelniania, które chroni systemy przed nieautoryzowanym dostępem. Tradycyjnie używano tylko kombinacji nazwy użytkownika i hasła, ale ze względu na zwiększoną liczbę naruszeń bezpieczeństwa zaleca się uwierzytelnianie dwuskładnikowe.

Zabezpieczenia warstwowe są najczęściej stosowaną cyberstrategią defensywną. Staje się to jednak coraz bardziej kosztowne i nieefektywne. Hakerzy nadal są w stanie ominąć kilka warstw zabezpieczeń przy użyciu technik ataków takich jak phishing, w których atakowany jest bezpośrednio użytkownik końcowy. Ponadto wiele warstw zabezpieczeń to większe koszty instalacji i utrzymywania, co stanowi spore wyzwanie dla małych i średnich przedsiębiorstw (MŚP). Z tego powodu rośnie liczba organizacji rozważających podejście typu obrona wszерz.

## Obrona wszерz

Obrona wszерz (ang. *defense in breadth*) to nowa strategia defensywna, która łączy tradycyjne podejście do bezpieczeństwa z nowymi mechanizmami zabezpieczeń. Jej celem jest zapewnienie bezpieczeństwa w każdej warstwie modelu OSI. Do warstw modelu OSI należą następujące warstwy: fizyczna, łącza danych, sieciowa, aplikacji, prezentacji, sesji i transportowa. Dlatego gdy hakerom udaje się obejść konwencjonalne narzędzia bezpieczeństwa, są powstrzymywani przez inne strategie defensywne stosowane na kolejnych warstwach modelu OSI. Ostatnią warstwą zabezpieczeń jest zazwyczaj warstwa aplikacji. Rośnie popularność tzw. **firewalli aplikacji internetowych** (ang. *Web Application Firewall* — WAF), które są bardzo skuteczne w atakach ukierunkowanych na określone aplikacje. WAF może udaremnić przeprowadzony atak i można utworzyć regułę, aby zapobiec podobnym atakom w przyszłości, dopóki nie zostanie zastosowana poprawka. Oprócz tego programiści świadomi kwestii bezpieczeństwa używają podczas tworzenia aplikacji metod projektu **OWASP** (ang. *Open Web Application Security Project*). Metody te kładą nacisk na tworzenie aplikacji, które zapewniają

standardowy poziom bezpieczeństwa i rozwiązują problemy związane z typowymi lukami w zabezpieczeniach. W przyszłości dostarczane będą prawie w pełni zabezpieczone aplikacje. Będą one zatem w stanie udaremniać lub wytrzymywać ataki samodzielnie, bez polegania na innych systemach defensywnych.

Kolejną koncepcją stosowaną w defensywie wszcz jest automatyzacja zabezpieczeń. Polega ona na tym, że systemy są opracowywane z funkcjonalnościami wykrywania ataków i automatycznego stosowania środków defensywnych. Funkcjonalności te opierają się na uczeniu maszynowym, w którym systemy uczą się swoich stanów pożądanых i normalnych ustawień środowiska. Gdy występują anomalie w ich stanie lub środowisku, aplikacje mogą przeprowadzać skanowanie w poszukiwaniu zagrożeń i stosować środki zaradcze. Technologia ta jest już stosowana w aplikacjach bezpieczeństwa w celu poprawy ich efektywności. Istnieją firewalle oparte na sztucznej inteligencji i programy antywirusowe oparte na hostach, potrafiące obsługiwać incydenty naruszenia bezpieczeństwa bez potrzeby udziału czynnika ludzkiego. Obrona wszcz jest jednak wciąż nową strategią i wiele organizacji obawia się jej stosowania.

Bez względu na to, czy organizacja wykorzystuje obronę wszcz (w celu zapewnienia bezpieczeństwa wszystkich sektorów organizacji), obronę w głąb (aby zapewnić określonego sektorowi wiele warstw zabezpieczeń) czy nawet kombinację obu rodzajów obrony, warto, aby ogólna strategia cyberbezpieczeństwa organizacji była proaktywna.

## Korzyści z posiadania proaktywnej strategii cyberbezpieczeństwa

Samo wdrożenie strategii cyberbezpieczeństwa przestaje już być wystarczające. Biorąc pod uwagę potencjalne negatywne skutki incydentu naruszenia bezpieczeństwa, aby strategia cyberbezpieczeństwa przynosiła największe korzyści, musi funkcjonować proaktywnie. Proaktywna strategia bezpieczeństwa zasadniczo koncentruje się na przewidywaniu zagrożeń i stosowaniu środków zaradczych, zanim dojdzie do jakiegokolwiek incydentu. Oto niektóre z korzyści płynących z proaktywnego podejścia do cyberbezpieczeństwa:

- Podejście proaktywne jest mniej kosztowne w porównaniu do podejścia reaktywnego. Reaktywne podejście do cyberbezpieczeństwa oznacza opracowywanie systemów i reguł, które koncentrują się na reagowaniu na incydenty naruszenia bezpieczeństwa po ich wystąpieniu. Ryzykowność takiego podejścia polega na tym, że jeśli organizacja stanie w obliczu nowego rodzaju zagrożenia, może nie być w pełni przygotowana do radzenia sobie z jego konsekwencjami. Będzie to prawdopodobnie bardziej kosztowne niż podejście proaktywne.

- Proaktywne podejście do zarządzania ryzykiem pozwala być o krok przed aktorami zagrożeń. Wyprzedzanie potencjalnych napastników to wymarzona sytuacja dla każdego zespołu ds. bezpieczeństwa. Oznacza to, że zespół ds. bezpieczeństwa opracowuje środki ochrony organizacji, które powstrzymają atakujących. Przy zastosowaniu takiego podejścia aktorzy zagrożeń będą mieli trudności z opracowaniem jakiegokolwiek znaczącego ataku na systemy, a w przypadku incydentu naruszenia bezpieczeństwa można się spodziewać tylko niewielkiego negatywnego efektu.
- Proaktywne podejście zwiększa przejrzystość. Zapewnia zespołowi ds. bezpieczeństwa i całej organizacji środki reagowania na incydenty naruszenia bezpieczeństwa i na wszelkie potencjalne zagrożenia związane z takimi incydentami. Dostarcza jasnego planu, który określa, w jaki sposób organizacja będzie wykonywała działania w razie wystąpienia ewentualnych zagrożeń. W przypadku stosowania reaktywnego podejścia do kwestii bezpieczeństwa zamieszanie będące następstwem incydentu związanego z naruszeniem bezpieczeństwa może doprowadzić do dalszych strat i dalszych opóźnień w przywracaniu sprawności systemów organizacyjnych.
- Proaktywne podejście utrudnia atakującym przeprowadzanie ataków. Atakujący nieustannie poszukują w organizacjach słabych punktów do eksploatacji. W proaktywnym podejściu organizacja sama stosuje podobne taktyki, stale oceniając swoje systemy w celu zidentyfikowania możliwych do eksploatacji luk w zabezpieczeniach systemu. Po znalezieniu takich luk w zabezpieczeniach organizacja podejmuje działania w celu ich wyeliminowania, zanim zostaną wykorzystane przez aktorów zagrożeń atakujących organizację. Dlatego proaktywne podejście pomaga zapobiegać znajdowaniu luk w zabezpieczeniach przez cyberprzestępców i eksploatacji tych luk ze szkodą dla organizacji.
- Proaktywne podejście pozwala dostosować strategię cyberbezpieczeństwa do wizji organizacji. Dobrze zaplanowane i proaktywne podejście do zarządzania ryzykiem i cyberbezpieczeństwa jest niezbędne, aby pomóc organizacji w dopasowaniu jej planów cyberstrategii do własnej wizji. Niezaplanowana cyberstrategia może mieć niekorzystny wpływ na działalność biznesową i plany organizacji zarówno w perspektywie krótko-, jak i długoterminowej. Jednak dzięki proaktywnemu podejściu organizacja może mieć pewność, że strategia będzie dostosowana do jej długoterminowej wizji, a planowanie budżetu i implementowanie strategii będzie dopasowane do wizji prowadzonej działalności.
- Proaktywne podejście rozwija kulturę świadomości kwestii związanych z bezpieczeństwem. Każdy członek organizacji ma kluczowe znaczenie dla wdrożenia strategii cyberbezpieczeństwa. Pracownicy, podobnie jak zasoby informacyjne w organizacji, mogą być atakowani jako słabe ogniwa

w systemie bezpieczeństwa, a następnie wykorzystywani do uzyskania dostępu do systemu organizacji. Dlatego rozwój kultury świadomości bezpieczeństwa przynosi ogromne korzyści w zakresie bezpieczeństwa organizacji i zwiększa jej zdolność do powstrzymywania atakujących.

- Proaktywne podejście pomaga organizacji wyjść poza zapewnianie wyłącznie zgodności z regulacjami. Często organizacje opracowują strategię cyberbezpieczeństwa, która odpowiada wymogom zgodności, aby uniknąć problemów z prawem. W większości przypadków te wymagania dotyczące zgodności wystarczą do ochrony organizacji przed wieloma zagrożeniami, zwłaszcza tymi powszechnymi. Strategia cyberbezpieczeństwa mająca na celu spełnienie minimalnych wymogów prawnych nie pozwala jednak zapobiegać najniebezpieczniejszym atakom, które często są przeprowadzane, aby bardziej zaszkodzić organizacji.
- Proaktywne podejście do opracowywania cyberstrategii sprawia, że organizacja w równym stopniu inwestuje w trzy fazy cyberbezpieczeństwa: zapobieganie, wykrywanie i reagowanie. Wszystkie te trzy fazy są istotne dla zaimplementowania skutecznej strategii bezpieczeństwa. Skupienie się na jednym obszarze przy jednoczesnym zaniedbaniu innego prowadzi do powstawania nieefektywnych strategii, które nie przynoszą organizacji pełnych korzyści lub nie obsługują odpowiednio incydentów naruszenia bezpieczeństwa, jeśli takie wystąpią.

Jak widać, korzystanie z proaktywnej cyberstrategii ma wiele zalet i jest wiele powodów, dla których Twoja firma powinna z niej skorzystać. Ponadto istnieje wiele konkretnych strategii cyberbezpieczeństwa, które możesz zastosować w celu zapewnienia bezpieczeństwa swojej organizacji.

## Najlepsze strategie cyberbezpieczeństwa dla firm

Ostatnimi czasy odnotowano wzrost liczby incydentów naruszenia bezpieczeństwa i wiele firm padło ofiarą cyberprzestępców atakujących ich dane lub inne zasoby informacyjne.

Jednak dzięki starannemu rozwojowi strategii cyberbezpieczeństwa nadal możliwe jest zapewnienie firmie wystarczającego bezpieczeństwa w tych trudnych czasach. Oto jedno z najlepszych strategii cyberbezpieczeństwa, które możesz wdrożyć w celu poprawy bezpieczeństwa swojej organizacji:

- szkolenie pracowników w zakresie zasad bezpieczeństwa;
- ochrona sieci, informacji i komputerów przed wirusami, złośliwym kodem i oprogramowaniem szpiegującym;
- stosowanie firewalla dla wszystkich połączeń internetowych;
- aktualizowanie oprogramowania;
- korzystanie z kopii zapasowych;
- zaimplementowanie ograniczeń fizycznych;
- zabezpieczanie sieci wi-fi;
- rotacja haseł;
- ograniczenie dostępu dla pracowników;
- stosowanie unikatowych kont użytkowników.

Poszczególne strategie omówimy szerzej w kolejnych punktach tego podrozdziału.

## **Szkolenie pracowników w zakresie zasad bezpieczeństwa**

Pracownicy są niewątpliwie istotnym aspektem strategii cyberbezpieczeństwa. W wielu przypadkach aktorzy zagrożeń atakują pracowników lub słabości spowodowane zachowaniem pracowników, aby uzyskać dostęp do systemów firmy. Zespół ds. bezpieczeństwa musi opracować podstawowe praktyki bezpieczeństwa, które muszą być przestrzegane przez wszystkich pracowników w miejscu pracy i podczas przetwarzania danych związanych z pracą. Ponadto informacje na temat tych praktyk i reguły bezpieczeństwa muszą być odpowiednio przekazywane pracownikom za każdym razem, gdy są one ustanawiane lub wprowadzane są w nich jakiegokolwiek zmiany. Pracownicy powinni znać kary za nieprzestrzeganie tych zasad bezpieczeństwa. Kary powinny być jasno określone, pomaga to bowiem w kultywowaniu kultury bezpieczeństwa wśród pracowników.

## **Ochrona sieci, informacji i komputerów przed wirusami, złośliwym kodem i oprogramowaniem szpiegującym**

Aktorzy zagrożeń najprawdopodobniej będą atakować wymienione w tytule zasoby organizacji. Do infiltracji systemów będą używać złośliwego kodu, wirusów i oprogramowania szpiegującego, gdyż są to najczęściej używane metody nielegalnego uzyskania dostępu do dowolnego systemu. Dlatego organizacja musi zapewnić ochronę swoich komputerów, informacji i sieci przed takimi taktykami infiltracji. Można to osiągnąć m.in.

przez zainstalowanie skutecznych systemów antywirusowych i regularne ich aktualizowanie w celu zwalczania wirusów i innego złośliwego kodu. Zaleca się automatyczne sprawdzanie aktualizacji zainstalowanych systemów antywirusowych, aby mieć pewność, że system jest aktualny i może zwalczać wszelkie nowe ataki.

## **Stosowanie firewalla dla wszystkich połączeń internetowych**

Połączenia internetowe są obecnie najbardziej prawdopodobną opcją, którą atakujący mogą wykorzystywać do atakowania systemów. Dlatego zapewnienie bezpieczeństwa połączeń internetowych jest ważnym i skutecznym sposobem zapewnienia bezpieczeństwa systemów. Firewall to zestaw programów, które pomogą uniemożliwić osobom postronnym dostęp do danych przesyłanych w sieci prywatnej. Firewalle powinny być zainstalowane na wszystkich komputerach, również na tych, których pracownicy mogą używać w celu uzyskiwania dostępu do sieci organizacji z domu.

## **Aktualizowanie oprogramowania**

Wszystkie aplikacje i systemy operacyjne wykorzystywane w organizacji powinny być aktualizowane. Aby mieć pewność, że system działa na bieżącej i zaktualizowanej wersji oprogramowania, co zmniejsza ryzyko wykrycia i eksploatacji przez cyberprzestępców luk w zabezpieczeniach starych systemów, zweryfikuj, czy w organizacji obowiązuje reguła pobierania i instalowania aktualizacji dla wszystkich używanych w niej aplikacji i programów. Aktualizacje powinny być skonfigurowane tak, aby były wykonywane automatycznie. W celu zapewnienia efektywności tego procesu aktualizacji należy go stale monitorować.

## **Korzystanie z kopii zapasowych**

Organizacja powinna zawsze przechowywać kopie zapasowe wszystkich ważnych informacji i danych biznesowych. Procesy tworzenia kopii zapasowych należy uruchamiać regularnie, codziennie lub co tydzień, dla każdego komputera używanego w organizacji. Przykładami poufnych danych, które mogą wymagać tworzenia kopii zapasowych, są dokumenty programu Word i bazy danych.

## **Zaimplementowanie ograniczeń fizycznych**

Ograniczenie fizycznego dostępu jest skuteczną strategią utrzymywania intruzów z dala od systemu. W wielu przypadkach intruzi próbują uzyskać fizyczny dostęp do jednych systemów, aby uzyskać dostęp do innych. Niektóre zasoby informacyjne, takie

jak laptopy, są szczególnie podatne i gdy nie są używane, powinny być przechowywane pod kluczem. Kradzieży mogą dokonać nawet pracownicy, dlatego konieczne są fizyczne ograniczenia, aby zapewnić bezpieczeństwo wszystkich aktywów organizacji.

## **Zabezpieczanie sieci wi-fi**

Pamiętaj o zabezpieczaniu i ukrywaniu sieci wi-fi przed złośliwymi osobami. Punkty dostępu bezprzewodowego można skonfigurować w taki sposób, aby nazwa sieci nie była rozgłaszana. Ponadto można użyć szyfrowania i haseł, dzięki którym tylko uwierzytelnione osoby będą upoważnione do uzyskania dostępu do systemów.

## **Rotacja haseł**

Hakowanie haseł jest jednym z najprostszych sposobów na uzyskanie dostępu do dowolnego systemu. Pracownicy powinni zostać poinstruowani, aby zmieniać swoje hasła i nie używać wspólnych haseł. Zapobiega to wykorzystywaniu przez atakujących długotrwanie stosowanego hasła, które może być współdzielone przez współpracowników.

## **Ograniczenie dostępu dla pracowników**

Wprowadzanie ograniczeń i przyznawanie uprawnień w korzystaniu z systemu organizacji powinno opierać się na rozpoznaniu potrzeb pracowników. Pracownicy powinni mieć dostęp tylko do tych zasobów w systemie, których potrzebują do swojej pracy, a dostęp ten może być ponadto ograniczony do określonych przedziałów czasu zgodnych z godzinami pracy. Ograniczenie możliwości instalowania oprogramowania podczas korzystania z systemów firmowych gwarantuje, że personel nie będzie mógł zainstalować złośliwego oprogramowania przypadkowo lub w inny sposób.

## **Stosowanie unikatowych kont użytkowników**

Organizacje powinny dopilnować, aby pracownicy korzystali z unikatowych kont użytkowników, przy czym poszczególni użytkownicy powinni mieć indywidualne konta. Gwarantuje to, że każdy użytkownik będzie odpowiedzialny za swoje konto użytkownika i będzie mógł zostać pociągnięty do odpowiedzialności za zaniedbania lub złośliwe działania na tym koncie. Wszystkich użytkowników należy także poinstruować, aby pamiętali o używaniu silnych haseł do swoich kont użytkowników w celu zapewnienia bezpieczeństwa i uniknięcia zhakowania. Ponadto uprawnienia dla tych kont użytkowników należy ustalać na podstawie stażu pracy pracownika i jego potrzeb dotyczących korzystania z systemu. Uprawnienia administracyjne powinny być przyznawane wyłącznie dla zaufanego personelu IT, który będzie pociągany do odpowiedzialności za wszelkie nadużycia i nieprawidłowości związane z korzystaniem z takich uprawnień.

Użytkownicy stanowią takie samo, a być może nawet większe zagrożenie dla systemu jak luki w zabezpieczeniu oprogramowania, ponieważ wiadomo, że atakujący wykorzystują słabości użytkowników, aby uzyskać dostęp do systemów docelowych. Z tego względu w poprzednich punktach uwzględniliśmy zarówno aspekty behawioralne, jak i kwestie techniczne związane z działaniami użytkowników, które możesz zaimplementować w różnych strategiach cyberbezpieczeństwa, jakie zdecydujesz się wybrać dla swojej organizacji.

## Podsumowanie

W tym rozdziale omówiliśmy cyberstrategie, powody wskazujące na konieczność ich stosowania oraz podejścia, które można zastosować podczas ich opracowywania. Jak wyjaśniliśmy, cyberstrategia to udokumentowane podejście organizacji do różnych aspektów cyberprzestrzeni. Jednak głównym problemem w większości cyberstrategii jest bezpieczeństwo. Cyberstrategie są niezbędne, gdyż zapobiegają przyjmowaniu przez organizacje określonych założeń, pomagają scentralizować podejmowanie decyzji dotyczących cyberbezpieczeństwa, dostarczają szczegółów na temat taktyk stosowanych w celu radzenia sobie z kwestiami związanymi z cyberbezpieczeństwem, zapewniają długoterminowe zaangażowanie w bezpieczeństwo i upraszczają złożoność zagadnień cyberbezpieczeństwa. W tym rozdziale przedstawiliśmy dwa główne podejścia stosowane w opracowywaniu cyberstrategii — ofensywne i defensywne.

Cyberstrategie pisane z perspektywy ataku koncentrują się na technikach testowania bezpieczeństwa, które będą wykorzystywane do znajdowania i usuwania luk w zabezpieczeniach. Natomiast cyberstrategie pisane z perspektywy defensywnej szukają sposobów zapewnienia jak najlepszej obrony organizacji. W tym rozdziale opisaliśmy również dwie główne strategie defensywne: obronę w głąb i obronę wszecz. Obrona w głąb koncentruje się na stosowaniu wielu redundantnych narzędzi bezpieczeństwa, podczas gdy obrona wszecz ma na celu ograniczanie ataków na różnych warstwach modelu OSI. W dążeniu do poprawy stanu cyberzabezpieczeń organizacja może zdecydować się na wykorzystanie defensywnej strategii bezpieczeństwa, ofensywnej strategii bezpieczeństwa albo obu tych strategii.

Rozdział ten zawiera również przykłady najlepszych strategii cyberbezpieczeństwa, które mogą być skutecznie wykorzystywane przez organizacje do zabezpieczania prowadzonej działalności.

W następnym rozdziale postaramy się przybliżyć zagadnienie łańcucha niszczenia cyberzabezpieczeń oraz jego znaczenie w kontekście stanu zabezpieczeń organizacji.

## Dalsza lektura

Oto lista materiałów źródłowych, które możesz wykorzystać do poszerzenia swojej wiedzy w zakresie tematów omówionych w tym rozdziale:

- Strategia cyberbezpieczeństwa Stanów Zjednoczonych: [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf).
- Strategia cyberbezpieczeństwa Australii: <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.
- Strategia cyberbezpieczeństwa Banku Kanady: <https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf>.
- *Developing a National Strategy for Cybersecurity* (Microsoft): <https://www.microsoft.com/en-us/cybersecurity/content-hub/developing-national-strategy-for-cybersecurity>.
- Narodowa Strategia Cyberbezpieczeństwa Rządu Wielkiej Brytanii: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>.
- Narodowe Strategie Cyberbezpieczeństwa agencji ENISA: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>.
- *Achieving Productivity without Exposing the Endpoint*: <https://www.comodo.com/endpoint-protection-strategy.php>.
- *Top 10 Cybersecurity Trends*: <https://www.simplilearn.com/top-cybersecurity-trends-article>.
- Wybór artykułów na temat cyberbezpieczeństwa: <https://www.erdalozkaya.com/category/cybersecurity/>.
- Hacker Combat — materiały, które pomogą Ci przyjąć nastawienie hakera: <https://hackercombat.com/>.
- Global CISO Forum — witryna, w której możesz rozwijać swoje umiejętności związane z pracą na stanowisku dyrektora ds. bezpieczeństwa informacji (ang. *Chief Information Security Officer* — CISO): <https://www.globalcisoforum.com>.
- Erdal Ozkaya, *Cybersecurity Leadership Demystified*: <https://www.packtpub.com/product/cybersecurity-leadership-demystified/9781801819282>.



# Skorowidz |

## A

- Active Directory, 270, 318
- Acunetix, 558
- AEP, Advanced Endpoint Protection, 136
- Aircrack-ng, 130
- Airgeddon, 131
- Airgraph-ng, 177
- aktor zagrożeń, 21, 30
- alerty, 432
- alternatywne lokalizacje, 500
- analityka
  - behawioralna
    - w chmurze hybrydowej, 433
    - w infrastrukturze lokalnej, 429
  - dla obciążeń roboczych PaaS, 436
  - zachowania użytkowników i podmiotów, UEBA, 113, 430
- analiza
  - behawioralna, 41
  - bezpłatne źródła, 449
  - cyberzagrożeń, CTI, 442
  - dzienników, 562
  - kodu źródłowego, 229
  - MITRE ATT&CK, 452
  - narzędzia, 445
  - oferowana przez Microsoft, 458
  - wpływu na działalność, BIA, 490, 497, 498
  - zagrożeń, TI, 440
  - zhakowanego hosta, 317
- anatomia cyberataku, 197
- Androguard, 257
- anomalie, 429
- aplikacje
  - firmowe, 35
  - kryptograficzne, 324
  - osobiste, 35
- AppleScript, 316
- APT, Advanced Persistent Threat, 99
- architektura zerowego zaufania, ZTA, 43
- Armitage, 235
- ARP, Address Resolution Protocol, 315
- atak
  - brute force, 271
  - DDoS, 23, 204, 247
  - fingerprinting, 251
  - man-in-the-middle, 37
  - pass-the-hash, PtH, 269, 270, 325
  - wstrzyknięcie kodu, 242
  - XSS, 245
- ataki
  - Comodo, 249
  - dzienniki, 67
  - fazy, 99
  - na chmurę, 211, 218
  - na łańcuchy dostaw, 26, 27, 39
  - na sieć korporacyjną, 207
  - na urządzenia IoT, 204
  - na urządzenia mobilne, 248
    - Exodus, 249
    - hakowanie iPhone'ów, 252
    - man-in-the-disk, 253
    - SensorID, 251
    - Spearphone, 254
    - Tap 'n Ghost, 254
  - socjotechniczne, 27, 149, 273, 336
  - ukierunkowane, 38
  - z manipulowaniem danymi, 201
    - przeciwdziałanie, 203
  - z wykorzystaniem maskowania, 109
  - z wymuszeniem, 197
  - za pomocą ransomware'u, 31, 201
- audyt bezpieczeństwa, 182
- automatyzacja, 266
  - przepływu pracy, 389
- autoryzacja, 33
- Azure
  - Activity, 574
  - Security Center, 435
  - Threat and Vulnerability Management, 548

**B**

backdoory, 206  
badanie  
  incydentu  
    ustalenie zakresu problemu, 462  
  proaktywne, 482  
  włamania do systemu  
    lokalnego, 469  
    w chmurze hybrydowej, 473  
baza  
  danych domeny Active Directory, 323  
  danych SAM, 323  
BCP, Business Continuity Plan, 504  
beaconing, 296  
bezpieczeństwo, 21  
  aplikacji, 35  
    fizyczna segmentacja, 400  
    hybrydowej w chmurze, 412  
  mediów społecznościowych, 375  
  sieci, 394  
    obrona w głąb, 394  
    segmentacja sieci wirtualnej, 407  
    sieć zerowego zaufania, 409  
    zabezpieczanie zdalnego dostępu, 404  
  świadomość personelu, 113  
  w chmurze, 217, 380, 412  
BIA, Business Impact Analysis, 490, 497  
biała lista aplikacji, 382  
biały wywiad, OSINT, 27, 169  
blog Erdala, 159  
blokowanie, deny, 111, 291  
błędne konfiguracje, 333  
boty skanujące GitHub, 211  
brute force, 27, 271  
buforowanie sudo, 365

**C**

C2, Command and Control, 40, 106, 112, 296  
Cain and Abel, 185  
CATT, Cast All The Things, 189  
CCE, Common Configuration Enumeration, 386  
centra danych, 297  
centralne konsole administracyjne, 317  
centrum  
  operacji bezpieczeństwa, SOC, 441  
  operacji sieciowych, NOC, 441

**chmura**

  bezpieczeństwo sieci hybrydowej, 412  
  najlepsze praktyki odzyskiwania  
    sprawności, 510  
  reguły bezpieczeństwa, 380  
  widoczność sieci, 414  
  zalecenia dotyczące bezpieczeństwa, 217  
  hybrydowa  
    analityka behawioralna, 433  
    włamanie do systemu, 473

**ciągła**

  integracja i ciągłe dostarczanie, CI/CD, 374  
  poprawa stanu zabezpieczeń, 390  
ciągłe monitorowanie bezpieczeństwa, 41  
CloudTracker, 215  
Cobalt Strike, 73  
COM, Component Object Model, 304  
CredMan, Credential Manager, 270  
Crontab, 289  
cross-site scripting, XSS, 245  
CSP, Cloud Solution Provider, 78  
CSPM, Cloud Security Posture Management, 46, 390  
  egzekwowanie reguł, 47  
  identyfikacja ryzyka, 47  
  integracja DevSecOps, 47  
  monitorowanie operacyjne, 47  
  ocena zgodności, 47  
  ochrona przed zagrożeniami, 47  
  zalecenia, 48  
CTI, Cyber Threat Intelligence, 442  
CVE, Common Vulnerability and Exposure, 386  
cyberbezpieczeństwo, 37  
cyberprzestępca, 442  
cyberstrategia, 81  
  ataku, 86  
  defensywna, 88  
  dla firm, 92  
  dokumentacja, 83  
  korzyści, 90  
  planowanie, 84  
  zrozumienie organizacji, 82  
  zrozumienie zagrożeń i ryzyka, 82  
cyberszpieg, 442  
cyberzabezpieczenia, *Patrz* łańcuch niszczenia  
  cyberzabezpieczeń  
Cycrypt, 257

## cykl

- dochodzenie, 118
  - gromadzenie danych kryminalistycznych, 117
  - kwalifikowanie, 118
  - neutralizacja, 119
  - odzyskiwanie sprawności, 119
  - wykrywanie, 118
  - życia incydentu, 64
  - życia zagrożeń, 116
- czyszczenie dysków, 109

**D**

## dane, 36

- eksfiltracja, 107
- kryminalistyczne, 117
- stan, 37
- środki zaradcze, 37
- zagrożenia, 37

## dashboard Hunting, 483

## DCOM, Distributed Component Object Model, 304

## DDoS, Distributed Denial-of-Service, 23, 204

## Deauther Board, 132

## Defender for Cloud, 435, 436

- adaptacyjne zabezpieczanie sieci, 417
- funkcjonalność Network Map, 414
- integracja z systemem SIEM, 479
- plany wykrywania zagrożeń, 437
- skoroszyt, 417
- wyszukiwanie alertów, 480
- zalecenia dotyczące sieci, 413

## degradowanie, degrade, 111

## demon startowy, launchd, 357

## DevSlop, 215

## DNSdumpster, 174

## DNSRecon, 171

## dodatkowa pamięć okna, EWM, 362

## dokumentowanie planu cyberstrategii, 83

## dostawca

- rozwiązań w chmurze, CSP, 78
- tożsamości, 45
- usług zarządzanych, MSP, 491

## dostęp

- do dzienników AWS, 572
- do dzienników Azure Activity, 575
- do poczty elektronicznej, 317
- do zasobów, 318
- zdalny do sieci, 404

## dowodzenie i kontrola, C2, 40, 106, 112, 296

## Dragon

- faza aktywnego naruszenia bezpieczeństwa, 140
- faza przygotowania, 136
- faza wtargnięcia, 137

## dyrektor ds. bezpieczeństwa informacji, 23

## działanie

- na celach, 106, 112
- UEBA, 430

## dzienniki

- Azure Activity, 574
- do identyfikacji ataków, 67
- firewalla, 567
- platformy AWS, 570, 572
- platformy GCP, 577
- serwera WWW, 569
- systemu Linux, 566
- systemu Windows, 564

**E**

## egzekwowanie reguł bezpieczeństwa

- biała lista aplikacji, 382
- w chmurze, 380
- zwiększanie zabezpieczeń, 385

## eksfiltracja danych, 107

## eksploatacja, 102, 112

- funkcjonalności ułatwień dostępu, 344
- luki w zabezpieczeniach, 222
- konfiguracji, 27

- niezaktualizowanych systemów operacyjnych, 341
- poświadczeń, 332

## eksploity

- podnoszenia uprawnień, 334
- zero-day, 224, 230

## eksploracja luk w zabezpieczeniach, 355

## elementy startowe, 364

## e-mail phishingowy, 470

## Enterprise Security Manager, 537

## enumeracja, 100

- typowych konfiguracji, CCE, 386

## etapy łańcucha niszczenia cyberzabezpieczeń

- dostarczanie, 102, 112
- dowodzenie i kontrola, 40, 106, 112, 296
- działanie na celach, 106, 112
- eksploatacja, 102, 112

etapy łańcucha niszczenia cyberzabezpieczeń

instalowanie, 106, 112

maskowanie, 108

rekonesans, 99, 111

uzbrajanie, 101, 112

ETTD, Estimated Time To Detection, 52

ETTR, Estimated Time To Recovery, 52

EvilOSX, 134

EWM, Extra Window Memory, 362

Exodus, 249

Exploit-DB, 158

## F

fałszowanie adresu MAC, 409

fazy ataku, 99

FIM, File Integrity Monitoring, 203

firewall, 567

fIAWS, 213

FOCA, Fingerprinting Organizations with  
Collected Archives, 167

footprinting, 100

Forward DNS, 215

framework

Metasploit, 123, 233

MITRE ATT&CK, 29

OSINT, 169, 171

Windows Application Compatibility, 346

WMI, 309

FraudGuard, 445

Frida, 257

funkcjonalności

IDS-u, 426

UEBA, 431

wykrywania, 419

fuzzing, 228

## G

generowanie istotnych alertów, 421

GPO, Group Policy Object, 378

graf, 297

CAPR, 178

CPG, 178

Graylog, 192

## H

Hak5 Plunder Bug, 188

hakowanie

chmury, 209

dostęp do sieci, 268

iPhone'ów, 252

kolejności przeszukiwania bibliotek DLL, 354

tożsamości użytkownika, 267, 271, 282

zbieranie poświadczeń, 269

urządzeń codziennego użytku, 208

haktywista, 442

Harmonogram zadań, 290

HIDS, Host-based Intrusion Detection Systems,  
288, 426

higiena bezpieczeństwa, 21

Hiren's BootCD, 236

HoboCopy, 133

Hot Potato, 367

Hunting, 483

Hydra, 129

## I

IaaS, Infrastructure as a Service, 25, 76

IDA Pro, 229

IDS, Intrusion Detection System, 39, 425

funkcjonalności, 426

określanie lokalizacji, 427

IDS, Intrusion Defense System, 288

incydent

cykl życia, 64

działania po zdarzeniu, 69

obsługa, 65, 68

określenie priorytetu, 62, *Patrz także*

proces reagowania na incydenty

infiltracja, 286, 329

infrastruktura jako usługa, IaaS, 25, 76

InsightVM, 548

instalacja złośliwego oprogramowania, 106,  
112, 296

interfejs DPAPI, 324

internet rzeczy, IoT, 23, 117, 204

Intruder, 544

inwentaryzacja zasobów, 516

narzędzia, 536

inżynieria społeczna, 27, 149, 273, 336

IoA, Indicator of Attack, 60, 483  
IoC, Indicator of Compromise, 60, 420, 442  
iOS Implant Teardown, 255  
IoT, Internet of Things, 23, 117, 204  
IPC, Inter-Process Communication, 316  
IPS, Intrusion Prevention System, 428  
IR, Incident Response, 57  
IT and Cyber Risk Management, 504

## J

jednostka organizacyjna, OU, 378  
John the Ripper, 128

## K

Keepnet Labs, 176  
Kismet, 126  
klucz, 464  
Knock Subdomain Scan, 215  
komponenty ZTA, 44  
komunikacja międzyprocesowa, IPC, 316  
Kon-Boot, 236  
konto użytkownika, 31  
kontrola  
dostępu do sieci, NAC, 405  
konta użytkownika, UAC, 349  
kontroler domeny, DC, 433  
kopie zapasowe, backupy, 33, 499  
KPI, Key Performance Indicator, 390  
kradzież  
dywersyjna, 151  
poświadczeń, 263, 312  
tokenów, 311  
tożsamości za pośrednictwem urządzeń mobilnych, 282

## L

LANDesk Management Suite, 536  
linki Canarytokens, 190  
Linux Live CD, 237  
lista kontroli dostępu, ACL, 409  
LolrusLove, 212  
LSA, Local Security Authority, 270  
LSASS, Local Security Authority Subsystem, 270

## luka

podnoszenia uprawnień, 352  
w systemie Windows, 228  
w zabezpieczeniach  
aplikacji WhatsApp, 226  
przeglądarki Chrome, 226  
usług pulpitu zdalnego, 306  
luki w zabezpieczeniach, 27, 222, 296, 334  
najlepsze praktyki zarządzania, 530  
narzędzia do zarządzania, 535  
narzędzia do oceny, 541  
strategie zarządzania, 515, 529  
elementy, 528  
etapy, 515  
inwentaryzacja zasobów, 516  
ocena luk, 524  
ocena ryzyka, 519, 529  
planowanie reagowania, 526  
raportowanie, 525  
śledzenie procesu remediacji, 525  
usprawnianie, 533  
zarządzanie informacjami, 517

## Ł

łamanie zabezpieczeń  
systemu internetowego, 241  
wstrzyknięcie SQL, 242  
systemu operacyjnego, 236  
Linux Live CD, 237  
narzędzia, 236, 239  
preinstalowane aplikacje, 238  
systemu zdalnego, 239  
wdrażanie ładunków, 232  
łańcuch niszczenia cyberzabezpieczeń,  
cybersecurity kill chain, 98  
dostarczanie, 102, 112  
dowodzenie i kontrola, 40, 106, 112, 296  
działania na celach, 106, 112  
eksploatacja, 102, 112  
ewolucja, 121  
instalowanie, 106  
maskowanie, 108  
obrona AEP, 136  
rekonesans, 99, 111  
ruch boczny, 295  
uzbrajanie, 101, 112  
używane narzędzia, 122  
wady, 120

## M

macierz ryzyka, 490  
 magazyn CredMan, 324  
 maksymalny dopuszczalny czas przestoju, MTD, 490, 493  
 manipulacja tokenami dostępu, 342  
 mapowanie topologii sieci, 182, 286, 403  
 maskowanie, 108  
 Masscan, 184  
 maszyna wirtualna, 415  
 MDM, Mobile Service Management, 25  
 mechanizm IDS, 426  
 mechanizmy kontroli bezpieczeństwa, 111  
 menedżer przełączników wirtualnych, 409  
 Metasploit, 122, 233  
   interfejs, 123  
   ładunki, 123  
   omijanie kontroli UAC, 350  
 MFA, Multi-Factor Authentication, 33, 406  
 Microsoft  
   Application Compatibility Toolkit, 347  
   Defender for Cloud, 29, 387, 390, 434  
   Defender for Endpoint, MDE, 423  
   Sentinel, 431, 458, 482  
 Mimikatz, 280, 319  
 MITRE  
   ATT&CK Navigator, 457  
   ATT&CK, 26, 30, 73, 137, 431, 452  
 modyfikowanie dzienników, 109  
 monitorowanie  
   integralności plików, FIM, 203  
   zgodności reguł, 387  
 MSP, Managed Services Provider, 491  
 MTD, Maximum Tolerable Downtime, 490, 493  
 MTTC, Mean Time To Compromise, 50  
 MTTP, Mean Time To Privilege escalation, 50

## N

NAC, Network Access Control, 405  
 narzędzia  
   do analizy zagrożeń, 445  
   do hakowania chmury, 211  
   do inwentaryzacji zasobów, 536  
   do oceny luk w zabezpieczeniach, 541  
   do oceny ryzyka, 541  
   do planowania reagowania, 543  
   do podnoszenia uprawnień, 365

do raportowania i śledzenia remediacji, 543  
 do rekonesansu, 158, 159  
 do zarządzania lukami w zabezpieczeniach, 535  
 do zarządzania ryzykiem, 502, 538  
 do mapowania, 402  
 dostępu zdalnego, RAT, 362  
 eksploatacji, 274  
 Microsoft Security Compliance Toolkit, 380  
 Pass-The-Hash, 269  
 rekonesansu wewnętrznego, 177  
 SET, Social-Engineer Toolkit, 273  
 sniffingowe, 179  
 Sysinternals, 300  
 narzędzie  
   0xsp Mongoose RED, 367  
   0xsp Mongoose v1.7, 366  
   Acunetix, 558  
   Aircrack-ng, 130  
   Airedragon, 131  
   Airgraph-ng, 177  
   Androguard, 257  
   Azure Threat and Vulnerability Management, 548  
   Cain and Abel, 185  
   CATT, 189  
   CloudTracker, 215  
   Crontab, 289  
   Cycrypt, 257  
   Deauther Board, 132  
   Defender for Cloud, 413  
   DevSlop, 215  
   DNSDumpster, 174  
   DNSRecon, 171  
   Dragon, 135  
   Enterprise Security Manager, 537  
   EvilOSX, 134  
   f1AWS, 213  
   FOCA, 167  
   Frida, 257  
   Graylog, 192  
   Hak5 Plunder Bug, 188  
   Hiren's BootCD, 236  
   HoboCopy, 133  
   Hot Potato, 367  
   Hydra, 129  
   IDA Pro, 229  
   InsightVM, 548  
   Intruder, 544

## narzędzie

IT and Cyber Risk Management, 504  
John the Ripper, 128  
Keepnet Labs, 176  
Kismet, 126  
Kon-Boot, 236  
LANDesk Management Suite, 536  
LolrusLove, 212  
Masscan, 184  
Microsoft Defender for Cloud, 387, 434  
Microsoft Sentinel, 431, 458  
Microsoft Sentinee, 482  
Mimikatz, 280, 319  
msinfo32, 465  
Nessus, 186, 549  
Nikto, 125  
Nimbusland, 212  
Nishang, 305  
Nmap, 180  
OpenVAS, 556  
Ophcrack, 239  
OTX Pulse, 448  
Patch Manager Plus, 545  
PDF Examiner, 279  
PhoneInfoga, 168  
Policy Viewer, 380  
PowerShell, 75, 307  
Prismdump, 179  
Prowler 2.1, 212  
PsExec, 280  
PsExec, 303  
Qualys, 556  
RiskNAV, 503  
SAINT, 159  
Scanrand, 184  
Seatbelt.exe, 159  
Shodan, 175  
SIEM, 458  
Snoopydroid, 256  
Sparta, 127  
SpiderFoot, 175  
SQL Injection Scanner, 243  
SQLi Scanner, 245  
tcpdump, 180  
TeamViewer, 314  
theHarvester, 168  
Twint, 124  
VirusTotal, 73  
Vulnerability Management Qualys, 557

Webshag, 166  
Wireshark, 183, 316  
WMImplant, 310  
WSUS, 546  
Nessus, 186, 549  
eksportowanie wyników, 555  
interfejs internetowy, 551  
konfiguracja skanowania, 552  
luki w zabezpieczeniach, 554  
tworzenie konta, 550  
NIDS, Network-based Intrusion Detection System, 288, 426  
Nikto, 124  
Nimbusland, 212  
Nishang, 305  
Nmap, 180  
funkcjonalności narzędzia, 182  
skanowanie otwartych portów, 287  
wyszukanie informacji o gościu, 287  
zalety narzędzia, 182  
NMS, Network Management System, 28  
NOC, Network Operations Center, 441  
nośniki wymienne, 313  
NTLM, New Technology LAN Manager, 269

## O

obiekt zasad grupy, GPO, 378  
obiektywny model komponentów, COM, 304  
obrona  
sieci, 291  
w głąb, 88, 394  
infrastruktura i usługi, 395  
mikrosegmentacja, 399  
punkty końcowe, 399  
warstwy, 395  
warstwy ochrony dla danych, 397  
wszerz, 89  
obsługa  
incydentów, 65  
lista kontrolna, 68  
wyjątków ustrukturyzowanych, SEH, 231  
obszar  
operacyjny, 444  
strategiczny, 444  
taktyczny, 444  
techniczny, 444

- ocena
    - luk w zabezpieczeniach, 524
    - ryzyka, 489, 519
  - ochrona
    - danych, 36
    - obwodowa, 120
    - wielowarstwowa tożsamości, 34
    - zaawansowana punktów końcowych, AEP, 136
  - odzyskiwanie sprawności, 487, 488
    - bez przestojów, 494
    - najlepsze praktyki, 509
      - lokalne, 510
      - w chmurze, 510
      - w środowisku hybrydowym, 511
    - ocena ryzyka, 489
    - opracowanie strategii, 491, 499
    - testowanie planu, 492
    - ustalenie priorytetów dla procesów i operacji, 490
    - utrzymywanie planu, 493
    - utworzenie planu odzyskiwania, 491
    - utworzenie zespołu, 489
    - wyzwania, 493
    - zatwierdzenie planu, 492
    - zebranie danych, 491
  - omijanie kontroli konta użytkownika, 349
  - OpenVAS, 556
  - Ophcrack, 239, 240
  - oprogramowanie
    - jako usługa, SaaS, 25, 76, 265
    - szpiegujące, 251
  - OSINT, open-source intelligence, 27, 169
  - osłona
    - DHCP, 409
    - routera, 409
  - OTX Pulse, 448
  - OU, Organizational Unit, 378
- P**
- PaaS, Platform as a Service, 436
  - Packet Storm Security, 159
  - pass the hash, PtH, 279, 320
  - pass the ticket, 320
  - Patch Manager Plus, 545
  - PAW, Privileged Access Workstation, 325
  - PDF Examiner, 279
  - phishing, 154, 220
    - profilowany, 155
    - telefoniczny, vishing, 156
  - PhoneInfoga, 168
  - plan
    - ciągłości działania, BCP, 504
    - cyberstrategii, 84
      - opracowanie, 506
    - odzyskiwania sprawności, 488
  - planowanie
    - awaryjne IT, 495, 496
      - identyfikacja środków zapobiegawczych, 499
    - narzędzia zarządzania ryzykiem, 502
    - opracowanie reguł, 497
    - przeprowadzanie analizy BIA, 497
  - reagowania, 526
    - narzędzia, 543
  - platforma
    - AWS, 570
    - Comodo Dragon, 547
    - CSPM, 390
    - Dragon, 135
    - GCP, 577
    - jako usługa, 436
    - Open Threat Exchange, 446
  - plik
    - /etc/passwd, 361
    - SAM, 360
  - poczta elektroniczna, 31
  - podatność na ataki, 120
  - podejście proaktywne, 90
  - podnoszenie
    - dotatkowe narzędzia, 365
    - poziomu uprawnień, 102, 227, 328, 331
      - pionowe, 103, 331
      - poziome, 104, 329
    - schemat, 339
    - uprawnień w systemie Windows, 227, 358
  - PoE, Power over Ethernet, 188
  - polecenie
    - Get-GPOReport, 379
    - Get-ItemProperty, 463
    - wmic process, 309
  - Policy Viewer, 380
  - poświadczenia, 33, 266, 269, 321
    - eksploatacja, 332
  - PowerShell, 75, 307
  - PowerSploit, 308

- poziom uprawnień w Windows, 227, 358
- pretexting, 151
- Prismdump, 179
- proaktywne
  - badanie, 482
  - strategie cyberbezpieczeństwa, 90
- proces
  - lsass.exe, 322
  - odzyskiwania sprawności, 487
  - planowania awaryjnego IT, 496
  - reagowania na incydenty, 57
    - aktualizacja, 77
    - na osi czasu zdarzeń, 58
    - tworzenie, 61
    - w chmurze, 76
    - z perspektywy CSP, 78
    - zestaw narzędzi, 78
  - remediacji, 525
  - tworzenia kopii zapasowej, 500
- program bezpieczeństwa, 373
  - edukacja użytkownika końcowego, 375
  - egzekwowanie reguł, 378
- programy pulpitu zdalnego, RDP, 300
- protokół
  - ARP, 315
  - UDP, 292
  - uwierzytelniania NTLM, 269
- Prowler 2.1, 212
- przechowywanie poświadczeń, 321
- przejęcie biblioteki dynamicznej, 355
- przepełnienie bufora, 230
- przesunięcie w lewo, shift left, 373
- przynęta, 153
- PsExec, 280, 303
- pulpit zdalny, 305
- punkty końcowe, 31

## Q

- Qualys, 556
- Quid Pro Quo, 153

## R

- RaaS, Ransomware-as-a-Service, 29
- ransomware, 28, 31, 201
  - jako usługa, RaaS, 29
  - Petya, 422
- RAT, Remote Access Tools, 362

- RCE, Remote Code Execution, 226
- RDP, Remote Desktop Program, 300
- reagowanie na incydenty, IR, 57
- reguły
  - bezpieczeństwa, 371
    - ciągła poprawa stanu zabezpieczeń, 390
    - egzekwowanie, 378
    - monitorowanie, 387
  - blokowania, 291
  - grup zabezpieczeń sieci, 416
- rejestr
  - ARIN, 172
  - zdalny, 313
- rejestrowanie aktywności, 204
- rekonesans, 99, 111
  - aktywny, 191
  - metody walki, 191
  - metody zapobiegania, 192
  - pasywny, 191
- wewnętrzny, 157
  - narzędzia, 158, 177
  - wardriving, 187
- zewnątrzny, 146
  - inżynieria społeczna, 149
  - narzędzia, 159
  - nurkowanie w śmietnikach, 148
  - skanowanie mediów społecznościowych, 146
- RiskNAV, 503
- rootowanie Androida, 361
- routing cebulowy, 109
- rozproszony obiektowy model komponentów, DCOM, 304
- RPO, Recovery Point Objective, 490
- RTO, Recovery Time Objective, 493
- ruch boczny, 269, 285
  - dostęp administratora stacji roboczej, 296
  - wykonywanie, 295
  - zhakowany użytkownik, 295
- ryzyko, 82, 490, 502, 519
  - narzędzia do oceny, 541
  - narzędzia do zarządzania, 538

## S

- SaaS, Software as a Service, 25, 76, 265
- SAINT, 159
- SAM, Security Accounts Manager, 270, 323, 360

- SAS, Secure Attention Sequence, 322
- Scanrand, 184
- scenariusz BYOD, 36
- schemat podnoszenia uprawnień, 340
- Seatbelt.exe
  - kontrola oprogramowania antywirusowego, 162
  - skanowanie komputera, 164
  - uruchamianie narzędzia, 161
  - wyszukiwanie połączeń TCP, 163
  - wyszukiwanie zainstalowanych programów, 162
  - zdalne uruchamianie, 165
- Seebug, 159
- segmentacja sieci
  - fizyczna, 400
  - na podstawie VLAN-ów, 401
  - wirtualnej, 407
- SEH, Structured Exception Handling, 231
- SensorID, 251
- serwer WWW, 569
- serwis VirusTotal, 471
- shimming aplikacji, 346
- Shiotob, 40
- Shodan, 175
- sieci VPN typu site-to-site, 406
- sieć zerowego zaufania, 409
- SIEM, Security Information and Event Management, 453, 458, 479, 482, 572, 575
- skanowanie, 73, 179, 289
  - luk w zabezpieczeniach, 101, 232
  - mediów społecznościowych, 146
  - portów, 101, 299
  - proaktywne, 289
  - sieci, 101
- skażone treści udostępniane, 313
- skrót
  - hasła, 133, 269, 322
  - pliku, 74
- SLA, Service-Level Agreement, 64
- sniffing, 179
  - sieci, 315
- Snoopdroid, 256
- Snort, 428
- SOC, Security Operations Center, 441
- Social-Engineer Toolkit, 273
- Sparta, 127
- Spearphone, 254
- SpiderFoot, 175
- SPN, Service Principal Name, 319
- spoofing ARP, 315
- spowalnianie skanera Nmapa, 293
- sprawdzanie integralności, 203
- SQL Injection Scanner, 243
- SQLi Scanner, 245
- stan zabezpieczeń, security posture, 21
  - ochrona, 41
  - reagowanie, 41
  - w chmurze, 45
  - wykrywanie, 41
- standard PCI DSS, 386
- steganografia, 108
- strategie
  - cyberbezpieczeństwa dla firm, 92
  - proaktywne, 90
  - testowania
    - ślepego, 87
    - ukierunkowanego, 87
    - wewnętrznego, 87
    - zewnętrznego, 86
- Sysinternals, 300
- system
  - obrony przed włamaniami, IDS, 288
  - wykrywania włamań, IDS, 39, 425
    - oparty na hostach, HIDS, 288, 426
    - oparty na sieci, NIDS, 288, 426
  - zapobiegania włamaniom, IPS, 428
  - zarządzania siecią, NMS, 28
- systemy alarmowe, 41
- szacowany czas
  - do odzyskania sprawności, ETTR, 52
  - do wykrycia, ETTD, 52
- szkolenie, 377
- szyfrowanie, 108, 397
  - danych, 204

## Ś

- średni czas
  - do naruszenia bezpieczeństwa, MTTC, 50
  - do podniesienia uprawnień, MTTP, 50
- środowisko wielochmurowe, 47
- świadomość bezpieczeństwa, 113

**T**

tailgating, 154  
Tap 'n Ghost, 254  
tcpdump, 180  
TeamViewer, 314  
technika wodopoju, 152  
theHarvester, 168  
TI, Threat Intelligence, 440  
tokeny  
    manipulacje, 342  
tożsamość użytkownika, 263  
trojan Duqu, 423  
tunelowanie, 109  
Twint, 124  
tworzenie  
    kopii zapasowej, 500  
    planu ciągłości działania, 507  
    strategii zarządzania lukami, 515

**U**

UAC, User Account Control, 349  
uczenie maszynowe, ML, 41, 431  
UDP, User Datagram Protocol, 292  
udziały  
    administratora, 320  
    plików, 302  
UEBA, User and Entity Behavior Analytics, 113, 430  
    działanie, 430  
    funkcjonalności, 431  
    określanie lokalizacji, 433  
ułatwienia dostępu, 344  
umowa poziomu usług, SLA, 64  
unikanie alertów, 298, 337  
uprawnienia  
    podnoszenie poziomu, 102, 227, 328, 331  
    pionowe, 103, 331  
    poziome, 104, 329  
usługa  
    Active Directory, AD, 318  
    Azure AD, 45  
    Azure Policy, 381  
    Defender for Cloud, 437  
    FraudGuard, 445  
    Microsoft Sentinel, 575  
    VSS, 133

**usługi**

    Microsoft Sentinel, 572  
    nielegalne, 364  
    RaaS, 29  
uwierzytelnianie, 33  
    domeny, 318  
    uszkodzone, 246  
    wieloskładnikowe, MFA, 33, 406  
uzbrajanie, 101, 112  
użycie skradzionych poświadczeń, 265  
użytkownicy  
    domowi, 264  
    korporacyjni, 264

**V**

VLAN, Virtual Local Area Network, 400  
VPN site-to-site, 406  
Vulnerability Management Qualys, 557

**W**

walidacja danych wejściowych, 204  
wardriving, 187  
warstwy ochrony dla danych, 397  
wdrażanie aplikacji, 315  
Webshag, 166  
weryfikacja adresu URL, 471  
WhatsApp  
    generator RCE, 226  
    instalowanie oprogramowania  
        szpiegującego, 226  
    kradzież informacji, 255  
wiaderko, bucket, 216  
widoczność punktu końcowego, 203  
Windows  
    Application Compatibility, 346  
    DCOM, 304  
    Management Instrumentation, WMI, 309  
    Server Update Services, WSUS, 546  
Winlogon, 322  
Wireshark, 183, 316  
wirtualne sieci lokalne, VLAN, 400  
wizualizacja sieci, 408  
włamanie  
    do systemu w chmurze hybrydowej, 473  
    do systemu lokalnego, 469

wskaźnik  
  ataku, IoA, 60, 483  
  IoC, 424  
  naruszenia bezpieczeństwa, IoC, 60, 420, 442, 483  
  wydajności KPI, 390  
wstrzyknięcie  
  biblioteki DLL, 352  
  dodatkowej pamięci okna, 362  
  SQL, 242  
wykonywanie ruchu bocznego, 295  
wykrywanie, detect, 111  
  na podstawie anomalii, 429  
  na podstawie reguł, 428  
  sieci, 402  
  skanów Nmapa, 292  
  systemów operacyjnych, 182  
  usług, 182  
wyszukiwanie skrótu pliku, 74  
wyszukiwarka urządzeń Shodan, 175

## Z

zaawansowane zagrożenia długotrwałe, APT, 99  
zabezpieczanie  
  się przed backdoorami, 208  
  urządzeń IoT, 205  
zaczepy  
  procedur, 363  
  tablicy adresów importów, 363  
  wstawiane, 363  
zagrożenia, 23, 39, 82  
  zarządzanie, 116  
zakładanie naruszenia bezpieczeństwa, 52  
zakładany  
  czas przywracania, RTO, 493  
  punkt przywracania, RPO, 490  
zakłócanie, disrupt, 111  
zalecenia dotyczące Pth, 325

zaplnowane zadania, 311, 363  
zapobieganie  
  ataków ransomware'owym, 31  
  eskalowaniu ataków, 32  
zarządzanie  
  chmurą hybrydową, 434  
  cyklem życia zagrożeń, 116  
  informacjami bezpieczeństwa i zdarzeniami, SIEM, 453  
  informacjami, 517  
  lukami w zabezpieczeniach, 514, 535  
  ryzykiem, 502, 538  
  stanem zabezpieczeń, 29  
  stanem zabezpieczeń w chmurze, CSPM, 46  
  urządzeniami mobilnymi, MDM, 25  
zdalne wykonywanie kodu, RCE, 226  
zdalny dostęp do zasobów firmy, 31  
zdarzenia związane z bezpieczeństwem, 465–468  
zero-day, 224  
zerowe zaufanie, 43, 409  
zespół  
  czerwony, 49  
  narzędzia dla urządzeń mobilnych, 256  
  zadania, 50  
niebieski, 49  
  narzędzia dla urządzeń mobilnych, 256  
  zadania, 51  
  reagowania na incydenty, 63  
złośliwe  
  oprogramowanie, 27, 337  
  Emotet, 424  
  Exodus, 249  
  w sklepie Google Play, 250  
  pliki PDF, 279  
zrzucanie pliku SAM, 360  
ZTA, Zero Trust Architecture, 43  
zwođenje, deceive, 111

# 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**

## Nie daj się zinfiltrować! Poznaj tajniki cyberbezpieczeństwa!

Przyspieszenie transformacji cyfrowej oznacza również uelastycznienie zasad pracy zdalnej. W takim środowisku zapewnienie cyberbezpieczeństwa jest trudniejsze, a złośliwe operacje stają się częstsze. Standardowy zestaw zabezpieczeń już nie wystarcza. Organizacje muszą przemyśleć swoje polityki bezpieczeństwa i dostosować je do nowych warunków. Na tym polu przewagę zyskuje się dzięki łączeniu taktyk defensywnych z ofensywnymi.

Ta książka jest skierowana do specjalistów z zakresu bezpieczeństwa IT, pentesterów, konsultantów do spraw bezpieczeństwa lub tych, którzy chcą działać jako etyczni hakerzy. Do pracy z nią przyda się znajomość sieci komputerowych, chmury obliczeniowej i systemów operacyjnych. Dzięki lekturze zdobędziesz aktualne informacje o kluczowych aspektach oceny zagrożeń i stanu systemu bezpieczeństwa, a także o zasadach utrzymywania właściwego stanu zabezpieczeń. Dowiesz się też, jak powinien wyglądać proces reagowania na incydenty. Zapoznasz się z taktykami zespołu czerwonego oraz zespołu niebieskiego, jak również z zasadami ich współdziałania. Znajdziesz tu dogłębne omówienie wzorców rozpoznawania nieregularnych zachowań w organizacji, technik analizy sieci i radzenia sobie ze złośliwym oprogramowaniem. Ten wyczerpujący przewodnik pozwoli Ci na ustalenie, jakich mechanizmów kontroli bezpieczeństwa potrzebujesz, jak je wdrożyć, wreszcie jak przeprowadzać poszczególne etapy procesu reagowania na incydenty.

### W książce:

- łagodzenie skutków incydentów i odzyskiwanie sprawności systemu
- ochrona obciążeń roboczych i kwestie zerowego zaufania
- najlepsze narzędzia, takie jak Nmap i Metasploit i framework MITRE ATT&CK
- bezpieczeństwo tożsamości i egzekwowanie reguł
- integracja systemów wykrywania zagrożeń z rozwiązaniami SIEM

## Yuri Diogenes

Menedżer w zespole Microsoft Cloud Security. Napisał ponad 20 książek dotyczących bezpieczeństwa informacji i technologii Microsoftu. Zdobył wiele certyfikatów branżowych IT/security.

## Erdal Ozkaya

Profesor cyberbezpieczeństwa Charles Sturt University w Australii. Jest też przedsiębiorcą, a także autorem lub współautorem ponad 10 książek na temat bezpieczeństwa informacji i technologii Microsoftu. Posiada liczne certyfikaty branżowe IT/security.

|                                                                                                                                                                                       |                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Helion</b>                                                                                      | <b>KOD KORZYŚCI</b><br>Sięgnij po więcej! ➤  |
|  <b>helion.pl</b>                                                                                  | ISBN 978-83-8322-421-3                                                                                                          |
|  <b>HELION SA</b><br>ul. Kościuszki 1c<br>44-100 Gliwice<br>tel.: 32 230 98 63<br>helion@helion.pl | <br>9 788383 224213                          |
| <b>Cena: 119,00 zł</b>                                                                                                                                                                |                                                                                                                                 |

**Packt** 