
Spis treści

Przedmowa	xi
Rozdział 1. Zasady i pojęcia	1
Najmniejsze uprzywilejowanie	1
Bezpieczeństwo od podstaw	2
Potencjalni atakujący, diagramy i granice zaufania	2
Model świadczenia usługi w chmurze	6
Model współodpowiedzialności w chmurze	6
Zarządzanie ryzykiem	10
Rozdział 2. Zarządzanie zasobami danych i ich ochrona	13
Identyfikacja i klasyfikacja danych	13
Przykładowe poziomy klasyfikacji danych	14
Istotniejsze wymagania branżowe i prawne	15
Zarządzanie zasobami danych w chmurze	17
Oznaczanie zasobów w chmurze	18
Ochrona danych w chmurze	20
Tokenizacja	20
Szyfrowanie	20
Podsumowanie	27
Rozdział 3. Zarządzanie zasobami danych i ich ochrona	29
Różnice w stosunku do tradycyjnego IT	29
Rodzaje zasobów w środowisku w chmurze	30
Zasoby obliczeniowe	31
Zasoby pamięci	37
Zasoby sieciowe	42

Pipeline zarządzania zasobami	43
Wycieki podczas wyboru usługi	44
Wycieki wynikające z przetwarzania	45
Wycieki wynikające z wykorzystania narzędzi	46
Wycieki wynikające z zaniedbania ryzyka	46
Oznaczanie zasobów w chmurze	47
Podsumowanie	48
Rozdział 4. Zarządzanie tożsamością i dostępem	51
Różnice w stosunku do tradycyjnego IT	53
Cykl życia dla tożsamości i dostępu	53
Żądanie	55
Zatwierdzanie	56
Utwórz, usuń, udziel lub odwołaj	56
Uwierzytelnianie	56
Tożsamości IAM w chmurze	57
Relacje firma-klient i firma-pracownik	58
Uwierzytelnianie wielopoziomowe	59
Hasła i klucze API	61
Współdzielone tożsamości	63
Tożsamość federacyjna	63
Pojedyncze logowanie	63
Metadane instancji i dokumenty tożsamości	66
Zarządzanie sekretami	67
Autoryzacja	71
Scentralizowana autoryzacja	72
Role	73
Przedłużanie ważności	74
Połączenie wszystkiego w przykładowej aplikacji	75
Podsumowanie	77
Rozdział 5. Zarządzanie podatnościami	79
Różnice w stosunku do tradycyjnego IT	80
Zagrożone obszary	82
Dostęp do danych	82
Aplikacje	83

Oprogramowanie pośredniczące	85
System operacyjny	86
Sieć	87
Infrastruktura wirtualna	87
Infrastruktura fizyczna	87
Znajdowanie i naprawianie podatności	87
Skanery podatności na zagrożenia sieciowe	89
Skanery bezagentowe i zarządzanie konfiguracją	91
Skanery agentowe i zarządzanie konfiguracją	92
Narzędzia zarządzania bezpieczeństwem od dostawcy chmury	93
Skanery kontenerów	93
Dynamiczne skanery aplikacji (DAST)	94
Statyczne skanery aplikacji (SAST)	95
Skanery analizy składu oprogramowania (SCA)	95
Interaktywne skanery aplikacji (IAST)	96
Runtime Application Self-Protection Scanners (RASP)	96
Ręczne sprawdzenie kodu	96
Testy penetracyjne	97
Raporty użytkowników	98
Przykładowe narzędzia do zarządzania podatnościami i konfiguracją	98
Procesy zarządzania ryzykiem	101
Mierniki zarządzania podatnościami	102
Zakres narzędzi	102
Średni czas naprawy	102
Systemy/aplikacje z niezależnymi podatnościami	103
Odsetek wyników fałszywie pozytywnych	104
Odsetek wyników fałszywie negatywnych	104
Mierniki powtarzalności podatności	104
Zarządzanie zmianami	105
Połączenie wszystkiego w przykładowej aplikacji	105
Podsumowanie	109
Rozdział 6. Bezpieczeństwo sieci	111
Różnice w stosunku do tradycyjnego IT	111
Pojęcia i definicje	113
Białe i czarne listy	113

Strefy DMZ	114
Proxy	114
Sieci definiowane programowo	115
Wirtualizacja funkcji sieciowych	115
Sieci nakładkowe i enkapsulacja	116
Prywatne chmury wirtualne	116
Network Address Translation	117
IPv6	118
Połączenie wszystkiego w przykładowej aplikacji	119
Szyfrowanie w trakcie przesyłania	120
Zapory i segmentacja sieci	123
Zezwalanie na dostęp administracyjny	129
Zapora sieciowa aplikacji internetowych i RASP	133
Anty-DDoS	135
Systemy wykrywania i zapobiegania włamaniom	136
Filtrowanie ruchu wychodzącego z sieci	137
Zapobieganie utracie danych	139
Podsumowanie	140
Rozdział 7. Wykrywanie, reagowanie i odzyskiwanie po incydentach bezpieczeństwa ...	143
Różnice w stosunku do tradycyjnego IT	144
Co monitorować	145
Dostęp użytkownika uprzywilejowanego	147
Dzienniki narzędzi defensywnych	148
Dzienniki i mierniki usług w chmurze	152
Dzienniki i mierniki systemu operacyjnego	153
Dzienniki oprogramowania pośredniczącego	153
Serwer sekretów	154
Twoja aplikacja	154
Jak monitorować?	154
Agregacja i zatrzymywanie	155
Parsowanie	156
Wyszukiwanie i korelacja	157
Alarmowanie i automatyczna reakcja	158
Informacje o bezpieczeństwie i menedżerowie zdarzeń	159
Threat Hunting	161

Przygotowanie do incydentu	161
Zespół	161
Plany	163
Narzędzia	165
Reagowanie na zdarzenie	167
Cyber Kill Chains	167
Pętla OODA (Obserwacja-Orientacja-Decyzja-Akcja)	168
Forensic w chmurze	170
Blokada nieautoryzowanego dostępu	170
Zatrzymywanie ekstrakcji danych oraz komunikacji z serwerami C&C	171
Odzyskiwanie	171
Ponowne instalowanie systemów informatycznych	171
Powiadomienia	171
Zdobytą wiedza	172
Przykładowe mierniki	172
Przykładowe narzędzia do wykrywania, reagowania i odzyskiwania	172
Połączenie wszystkiego w przykładowej aplikacji	173
Monitorowanie systemów ochronnych	175
Monitorowanie aplikacji	175
Monitorowanie administratorów	176
Zrozumienie infrastruktury audytu	177
Podsumowanie	178
Indeks	179