

Zdążyć przed hakerem : jak przygotować firmę na cyberatak / Jakub Bojanowski. – Wydanie pierwsze. – Warszawa, 2022

Spis treści

Wstęp	11
Podziękowania	17
 Rozdział 1	
Menedżer w obliczu cyberincydentu	21
Zaklinanie rzeczywistości	23
Deprecjonowanie skali incydentu	24
Poszukiwanie łatwych rozwiązań	25
Trudności w analizie zdarzenia	26
Straty wizerunkowe i chaos komunikacyjny	27
Słabe programy szkoleniowe dla pracowników	28
Prywatne i służbowe zasoby informatyczne	29
Poleganie na fachowcach	32
 Rozdział 2	
Typowy scenariusz cyberataku	35
Etap rozpoznania	39
Etap uzbrojenia	41
Etap dostarczenia	41
Etap wykorzystania	43
Etap instalacji	45
Etap dowodzenia i kontroli	46
Etap działania	47
MITRE ATT&CK®, czyli kill chain dla zaawansowanych	48
 Rozdział 3	
Cyberprzestępcy	51
Aktorzy i ich motywy	51
Pozyskiwanie środków z cyberprzestępczości	53
Kierunki i narzędzia ataku	54
Phishing	56
Ransomware	57
Ataki na aplikacje internetowe	59
Denial of Service	59
Błędy ludzkie	61
Działania na szkodę pracodawcy	63
Podsumowanie	64
 Rozdział 4	
Aktywa informacyjne	67
Sieć, urządzenia sieciowe	69

Usługi sieciowe, serwery aplikacyjne	70
Serwery w sieci wewnętrznej, systemy operacyjne, kontroler domeny	72
Bazy danych i repozytoria danych	75
Systemy przemysłowe	77
Komputery osobiste, urządzenia mobilne i przenośne nośniki danych	79
Zasoby w chmurze obliczeniowej	80
Skrzynki poczty elektronicznej	82

Rozdział 5

Uwierzytelnienie	85
Silne uwierzytelnienie	89
Silne uwierzytelnienie z perspektywy hakera	94

Rozdział 6

Bezpieczeństwo informacji	97
----------------------------------	-----------

Rozdział 7

Bezpieczeństwo informacji z perspektywy kierownictwa	107
Poufność	110
Integralność	112
Dostępność	113
Podsumowanie - profil ryzyka	115

Rozdział 8

Profil ryzyka cybernetycznego - studium przypadku	117
Pierwsze wnioski	121
Perspektywa audytora finansowego (biegłego rewidenta)	122
Perspektywa rady nadzorczej	124
Perspektywa dyrektora finansowego	125
Perspektywa szefa IT	125
Perspektywa zarządu	125
Perspektywa audytora bezpieczeństwa	126
Analiza scenariuszowa	127
Ocena dostępnych informacji	128
Sceptycyzm zawodowy i zasada ograniczonego zaufania	130
Podsumowanie	132

Rozdział 9

Współpraca z CISO	135
Organizacja w „pułapce cyberbezpieczeństwa”	138
CISO jako gatekeeper	138
Zawężenie perspektywy	139
Blindspot	140
Realistyczne oczekiwania wobec CISO	141
Raporty na temat bezpieczeństwa	144
Model referencyjny	147
Ekspert od bezpieczeństwa jako konsultant	149
Incydent u dużego klienta	150

Kradzież komputera z salonu	152
Konkurencja cenowa	153
Rozdział 10	
Zarządzanie bezpieczeństwem - kanon dobrej praktyki	157
Zakres ISO 27000	158
Dostosowanie ISO do potrzeb instytucji	161
Przypisanie odpowiedzialności a szczegółowość procedur	162
Ścieżka rewizyjna	163
Rutynowa ocena bezpieczeństwa	165
Rozwój oprogramowania	166
Obsługa urządzeń mobilnych	166
Rozdział 11	
Polityka bezpieczeństwa informacji	169
Polityka bezpieczeństwa informacji	169
Polityka bezpieczeństwa a procedury	171
Aktualizacja polityki	172
Rozdział 12	
Organizacja zarządzania bezpieczeństwem	175
Komitet bezpieczeństwa teleinformatycznego	175
Skład komitetu	175
Statut i tryb pracy komitetu	176
Zespół (szef) ds. bezpieczeństwa informacji	178
Zadania innych menedżerów związane z zapewnieniem bezpieczeństwa	178
Podległość służbowa zespołu ds. bezpieczeństwa	179
Bezpieczeństwo w „pionie prezesa”	180
Bezpieczeństwo w strukturach IT	180
Barьеры prawne	181
Korzystanie z zasobów zewnętrznych	182
Rozdział 13	
Klasyfikacja informacji	187
Klasyfikacja informacji a uprawnienia systemowe	188
Użytkownicy specjalni	190
Klasyfikacja informacji - podejście teoretyczne	192
Klasyfikacja informacji - podejście pragmatyczne	193
Klasyfikacja informacji - podejście superpragmatyczne	195
Klasyfikacja informacji a informacje niejawne	196
Rozdział 14	
Od bezpieczeństwa informacji	
do cyberbezpieczeństwa	199
Krytyczne spojrzenie na ISO 27000	200
Model NIST	203
Program poprawy cyberbezpieczeństwa według modelu NIST	206

Podsumowanie	208
Rozdział 15	
Ryzyko innowacji	209
Poszerzenie bazy użytkowników	210
Elektroniczny pieniądz	211
Przygotowanie do e-biznesu	214
<i>Case study</i> - ujednolicenie handlu elektronicznego	216
Rozdział 16	
Bezpieczeństwo kart kredytowych	219
Wymagania PCI DSS	220
Rozdział 17	
Ochrona płatności internetowych	225
Rozdział 18	
Potwierdzanie tożsamości w internecie	231
Inne wykorzystanie usług zaufania	236
Rozdział 19	
Zagrożenia dla prywatności	239
Rozdział 20	
Ochrona danych osobowych	247
Identyfikacja informacji	251
Wybór środków ochrony	253
Podejście oparte na analizie ryzyka	255
Podsumowanie	257
Rozdział 21	
Zapobieganie cyberincydentom	259
Obrona przed phishingiem	260
Data Leakage Protection	263
Systemy automatycznego wykrywania zdarzeń	265
Dalsza rozbudowa SIEM	268
Rozdział 22	
<i>Security Operations Center</i>	271
CSIRT	274
Rozdział 23	
Zarządzanie kryzysowe podczas cyberincydu	277
Jak dobre praktyki mogą pomóc w cyberkryzysie	281
Realna ocena cyber zagrożeń	281
Współpraca z ekspertami	283
Polityka bezpieczeństwa i zasady eksploatacji systemów	284
Bezpieczna konfiguracja techniczna	285

Szkolenie dla pracowników	286
Kompleksowy program budowy świadomości cyberzagrożeń	287
Monitorowanie zagrożeń	288
Rzetelna ocena skali incydentu	290
Dodatek A	
Protokoły sieciowe	293
Perspektywa użytkownika	293
Architektura warstw, protokoły komunikacyjne	295
Model referencyjny ISO OSI	296
Poziomy fizyczny i łączy danych	298
Poziom sieci - internet	300
Poziom transportu	303
Poziom sesji - usługi sieciowe	305
Poziomy prezentacji i aplikacji	307
Dodatek B	
Adresy sieciowe	309
Adresy IP	309
Adresy alfanumeryczne	312
<i>Firewall</i>	313
Rozszerzenia funkcjonalności zapory sieciowej	315
Jak oszukać zaporę sieciową	316
VPN	317
Dodatek C	
Podstawy kryptografii	321
Szyfrowanie	322
Szyfrowanie symetryczne	325
Kryptografia asymetryczna	327
Porównanie kryptografii symetrycznej i asymetrycznej	328
Funkcja skrótu	332
Kwestia tożsamości - trzecia strona zaufania	335
<i>Blockchain</i>	340
Dodatek D	
Modelowe zarządzanie uprawnieniami	347
Bibliografia	353
Słownik	357