Wstęp ... **11**

1. Zagrożenia związane z funkcjonowaniem systemów e-mail ... **13**

1.1. Wstęp – klasyfikacja zagrożeń ... 14

1.1.1. Bezpieczeństwo systemów ... 14

1.1.2. Bezpieczeństwo danych ... 14

1.1.3. Odpowiedzialność prawna ... 15

1.1.4. Utrata reputacji ... 15

1.1.5. Produktywność ... 15

1.2. Ryzyko utraty danych ... 16

1.2.1. E-mail jednym z głównych źródeł wycieku danych ... 16

1.2.2. Zaniedbania ... 17

1.2.3. Świadome działania pracowników ... 18

1.2.4. Zagrożenia zewnętrzne – byli pracownicy, pracownicy kontraktowi, współpracownicy ... 18

1.2.5. Szpiegostwo przemysłowe i „państwowe” ... 19

1.2.6. Zagrożenie dla użytkowników indywidualnych ... 21

1.3. Odpowiedzialność prawna ... 22

1.4. Reputacja ... 23

1.5. Produktywność ... 24

1.6. Analiza ryzyka i koszty zabezpieczenia ... 26

1.7. Złośliwy kod – klasyfikacja ... 28

1.7.1. Wirusy ... 28

1.7.2. Robaki ... 29

1.7.2.1. Struktura robaka ... 30

1.7.2.2. The Internet Worm – robak Morrisa ... 30

1.7.2.3. Wektory ataków ... 32

1.7.2.4. Zdalne przejęcie kontroli nad maszyną – ataki *smash the stack* i pokrewne ... 33

1.7.2.5. Inne znane robaki ... 34

1.7.2.6. Zbieranie adresów e-mail ... 35

1.7.2.7. Wykaz ważnych i groźnych robaków ... 36

1.7.3. Trojan i spyware ... 37

1.7.4. Przykład – Sobig ... 38

1.7.5. Sterowanie trojanami i połączenia zwrotne ... 38

1.7.6. *Addware*, *scareware* i inne „…-*ware*” ... 39

1.7.6.1. *Addware* ... 40

1.7.6.2. *Scareware* ... 40
1.7.6.3. *Hoax* ... 40
1.7.7. Rootkity ... 41
1.7.8. Złośliwy kod (*mallware*) ... 43
1.7.9. Motywacje tworzenia złośliwego kodu ... 47
1.7.10. Botnety ... 48
1.7.11. Zaufanie i jego brak ... 49

2. Architektura systemów poczty – protokół SMTP i standard MIME ... 53

2.1. Wprowadzenie ... 54
2.2. Sesja SMTP ... 56
2.3. Polecenia SMTP ... 58
2.4. Kody odpowiedzi SMTP ... 59
2.5. Obsługa błędów SMTP przez klienta ... 60
2.6. Raportowanie statusu operacji i reakcja serwera na błędy ... 61
2.6.1. Scenariusze obsługi błędów ... 61
2.6.2. Backscatter jako efekt uboczny powiadomień o błędach ... 61
2.6.3. Rozszerzone kody odpowiedzi ... 62
2.7. Ruting poczty ... 63
2.7.1. Ogólny algorytm rutingu SMTP ... 63
2.7.2. Rekordy MX ... 63
2.7.3. Zapasowe serwery MX i bezpieczeństwo ... 65
2.8. Pola nagłówkowe SMTP ... 66
2.8.1. Przykład i analiza przesyłki ... 66
2.8.2. Nagłówki śledzenia wiadomości – modyfikowane przez serwer MTA ... 67
2.8.2.1. Nagłówki *Return-Path* i *Received* ... 67
2.8.2.2. Zapętlenie poczty ... 68
2.8.3. Grupa pól związana z nadawcą ... 68
2.8.4. Grupa pól związana z odbiorcą ... 69
2.8.6. Pola *Resent* i przekierowanie (*forward*) poczty ... 69
2.8.7. Grupa pól identyfikujących wiadomość ... 70
2.8.8. Grupa pól informacyjnych ... 71
2.8.9. „Eksperymentalne" pola nagłówka ... 71
2.8.10. Listy wysyłkowe ... 73
2.8.10.1. Wprowadzenie ... 73

2.8.10.2. Adresowanie ... 73
2.8.10.3. Zwrotki z list wysyłkowych ... 74
2.8.10.4. Pola nagłówka list wysyłkowych ... 75
2.9. Rozszerzenia ESMTP ... 76
2.9.1. Wstęp i przykład ... 76
2.9.2. Przegląd możliwości wprowadzonych w ESMTP ... 77
2.9.2.1. ESMTP – powitanie EHLO i opcje ... 77
2.9.2.2. DSN – potwierdzenie dostarczenia wiadomości ... 78
2.9.2.3. Funkcja śledzenia wiadomości – MTRK ... 79
2.9.2.4. Rozszerzenia związane z transmisją kodów ośmiobitowych ... 82
2.9.2.5. Przesyłanie dużych wiadomości: CHUNKING i BDAT ... 83
2.10. Autoryzacja w SMTP ... 83
2.10.1. Zakres autoryzacji ... 83
2.10.2. Metody bazujące na nazwie użytkownika i haśle (PLAIN i LOGIN) ... 85
2.10.3. Metoda *Challenge-Response* ... 86
2.10.4. Autoryzacja za pomocą metod SASL i GSSAPI ... 86
2.10.5. Inne metody autoryzacji w SMTP ... 87
2.10.6. Autoryzacja i TLS ... 87
2.11. Przepływ poczty – raz jeszcze ... 89
2.12. Rozszerzone mechanizmy autoryzacji SMTP ... 90
2.12.1. *Sender Policy Framework* ... 91
2.12.1.1. Zasada działania SPF ... 91
2.12.1.2. Testy zgodności SPF ... 92
2.12.1.3. *Sender ID* ... 94
2.12.1.4. Problemy z SPF i przyszłość standardu ... 95
2.12.2. *Domain Keys Identified Mail* (DKIM) ... 96
2.12.2.1. Zasada działania DKIM ... 96
2.12.2.2. Podpis DKIM ... 97
2.12.2.3. Uzyskiwanie kluczy DKIM z DNS ... 98
2.12.3. Porównanie SPF z DKIM, cechy wspólne ... 99
2.13. Zaszłości i niebezpieczne cechy protokołu SMTP ... 101
2.13.1. Polecenia VRFY i EXPN ... 101
2.13.2. Polecenia TURN i ETRN ... 102
2.14. Załączniki w poczcie elektronicznej – standard MIME ... 103

2.14.1. MIME – podstawy ... 103
2.14.2. Typy MIME ... 105
2.14.2.1. Proste typy MIME ... 105
2.14.2.2. Złożone typy MIME – *multipart/mixed* ... 106
2.14.2.3. Inne złożone typy MIME ... 107
2.14.3. Nagłówki i kodowania MIME ... 109
2.14.3.1. Nagłówek *Content-Disposition* ... 109
2.14.3.2. Nagłówek *Content-Transfer-Encoding* ... 110
2.14.3.3. Kodowanie *base64* ... 110
2.14.3.4. Kodowanie *quoted-printable* ... 111
2.14.2.5. Nagłówek *Content-ID* ... 111
2.14.4. MIME w nagłówkach wiadomości ... 112

3. Protokoły *maildrop* i konstrukcja PO ... 115

3.1. Wprowadzenie ... 116
3.2. Protokół POP3 ... 116
3.3. Protokół IMAP4 ... 118
3.3.1. Wprowadzenie ... 118
3.3.2. Sesja IMAP4 ... 118
3.3.3. Foldery IMAP4 i operacje na nich ... 119
3.3.4. Pobieranie wiadomości ... 120
3.3.5. Zapisywanie i modyfikacja wiadomości ... 122
3.3.6. Wyszukiwanie wiadomości ... 123
3.4. Lokalne dostarczenie poczty – protokół LMTP ... 124
3.5. Konstrukcja urzędu pocztowego (PO) ... 125
3.5.1. Rola urzędu pocztowego ... 125
3.5.2. Format *mbox* (*mailbox*) ... 126
3.5.3. Format *maildir* ... 127
3.5.4. Format plikowo-indeksowy stosowany przez Sun Java System Messaging Server ... 128
3.6. Limity wielkości skrzynek pocztowych ... 130
3.6.1. Cele i efekty zastosowania limitów ... 130
3.6.2. Implementacja limitów ... 130
3.7. Bezpieczeństwo serwisów *maildrop* ... 132
3.7.1. Bezpieczeństwo danych w systemie *maildrop* ... 132
3.7.2. Bezpieczeństwo PO związane z możliwością eskalacji uprawnień ... 133

4. Serwisy katalogowe ... 135
4.1. Wprowadzenie ... 136
4.2. Funkcje i cechy serwisu katalogowego ... 136
4.3. Serwis LDAP ... 137
4.3.1. Wstęp ... 137
4.3.2. Organizacja katalogu LDAP ... 137
4.3.2.1. Wpisy ... 137
4.3.2.2. Drzewo katalogowe ... 138
4.3.3. Protokół LDAP ... 140
4.3.4. Przykładowe schematy danych ... 141
4.3.4.1. Schematy i klasy ... 142
4.3.4.2. Atrybuty ... 143
4.3.5. Przykładowe schematy danych do obsługi poczty ... 143
4.3.6. Rozszerzenia schematu dla systemów e-mail ... 145
4.3.7. Grupy adresów i listy wysyłkowe ... 148
4.3.8. Współpraca z serwerami e-mail ... 150
4.3.8.1. Wysyłka SMTP przez użytkownika lokalnego i obsługa *maildrop* ... 150
4.3.8.2. Przyjmowanie przesyłek SMTP ... 150
4.3.9. Uwierzytelnianie i bezpieczeństwo ... 151
4.3.9.1. Rola bezpieczeństwa LDAP ... 151
4.3.9.2. Metody uwierzytelnienia LDAP ... 151
4.3.9.3. Listy kontroli dostępu ... 152
4.3.9.4. Hasła ... 153
4.3.10. Zaawansowane możliwości LDAP ... 153
4.4. Inne realizacje usług katalogowych ... 154
5. Bezpieczna poczta: S/MIME i PGP ... 157
5.1. Wprowadzenie ... 158
5.2. Cechy bezpiecznej poczty ... 159
5.3. Rys historyczny ... 160
5.4. S/MIME ... 161
5.4.1. Wprowadzenie ... 161
5.4.2. Wiadomość podpisana ... 161
5.4.3. Wiadomość zaszyfrowana ... 168
5.4.4. Zaawansowane mechanizmy S/MIME ... 169

5.4.4.1. Wiadomość „potrójnie opakowana” ... 169
5.4.4.2. Podpisane zwrotki ... 169
5.4.5. Podsumowanie ... 170
5.4.6. Standardy S/MIME ... 171
5.5. PGP ... 171
5.5.1. Wstęp i historia ... 171
5.5.2. Możliwości PGP ... 172
5.5.3. Wiadomości w formacie PGP ... 173
5.5.3.1. Format PGP „ASCII armour” ... 174
5.5.3.2. Format PGP/MIME ... 177
5.5.4. Certyfikaty PGP ... 181
5.5.5. Zaufanie w PGP – *Web of trust* ... 182
5.5.6. Wersje PGP ... 184
5.5.7. Przykłady wykorzystania programu klienckiego ... 185
5.5.8. Porównanie PGP i S/MIME ... 185
5.6. Wykorzystanie S/MIME i PGP w bramce SMTP ... 187
5.7. Podstawowe pojęcia i terminologia kryptograficzna ... 189
5.7.1. Wprowadzenie do terminologii ... 189
5.7.2. Certyfikaty cyfrowe i PKI ... 191
5.7.2.1. Certyfikat cyfrowy ... 191
5.7.2.2. Zaufanie i Centra Certyfikacji (CA) ... 193
5.7.2.3. PKI ... 195
5.7.3. Standardy PKCS i CMS ... 196
5.7.4. Język ASN.1 i kodowanie BER ... 197
6. Walka ze spamem ... 201
6.1. Wprowadzenie ... 202
6.2. Miejsca filtracji spamu ... 202
6.3. Ocena jakości filtrowania ... 204
6.4. Metody „naiwne” ... 204
6.4.1. Czarna lista adresów nadawców (*black list*) ... 204
6.4.2. Biała lista adresów nadawców (*white list*) ... 206
6.4.3. Szare listy (*grey list*) i metoda *tarpit* ... 207
6.4.4. Proste metody słownikowe i filtracja URL (SURBL) ... 210
6.4.5. Filtrowanie według pól nagłowka ... 213

6.5. Autoryzacja nadawcy ... 215
6.6. Metody statystyczne ... 216
6.6.1. Leksemy i określenie prawdopodobieństw cząstkowych ... 216
6.6.2. Klasyfikowanie wiadomości ... 218
6.6.3. Lepsze metody obliczania prawdpodobieństw leksemów ... 219
6.6.4. Więcej o wydzielaniu leksemów ... 220
6.6.5. Inne metody statystyczne ... 221
6.6.6. Jak oszukać klasyfikację statystyczną? ... 222
6.6.7. Problemy z klasyfkacją centralną ... 227
6.7. Skróty wiadomości ... 228
6.8. Metody wykrywania spamu obrazkowego ... 229
6.9. Łączenie metod wykrywania spamu ... 229
6.10. Porównanie metod filtracji ... 232
6.11. Metody „nietechniczne" ... 233
6.12. Podsumowanie ... 234
7. Walka z wirusami w poczcie ... 235
7.1. Wprowadzenie ... 236
7.2. Drogi infekcji ... 236
7.3. Techniki wykrywania złośliwego kodu ... 238
7.4. Reakcja na wykrycie wirusa ... 239
7.5. Integracja modułu AV z systemem poczty ... 239
7.6. Podsumowanie ... 243
8. Filtrowanie treści ... 245
8.1. Wprowadzenie ... 246
8.2. Analiza załączników ... 247
8.3. Analiza leksykalna ... 249
8.3.1. Wstęp ... 249
8.3.2. Wyrażenia regularne ... 251
8.3.3. Wyrażenia regularne – definicje i przykłady ... 251
8.3.4. Praktyczne przykłady zastosowania wyrażeń regularnych do kontroli zawartości ... 253
8.4. Akcje reguł dopasowania ... 253
8.5. Zamiast podsumowania – wytyczne dla systemu filtracji ... 255

9. Architektura serwerów e-mail 257

9.1. Wprowadzenie 258

9.2. Warianty architektury 258

9.2.1. Wydzielony serwer brzegowy i serwery bezpieczeństwa 258

9.2.2. Oddzielne serwery brzegowe dla ruchu wchodzącego i wychodzącego 259

9.2.3. Skalowanie PO i serwisów *maildrop* 260

9.3. Replikacja serwisu LDAP 262

9.4. Przykładowe środowisko dostawcy usług 262

9.5. Skalowanie 263

9.6. Monitorowanie 265

9.7. Bezpieczeństwo „w chmurze” a e-mail 266

9.8. Podsumowanie 267