MỤC LỤC

Lời nói đầu 3

Chương 1. Tổng quan về an ninh mạng 5

1.1. Tình hình an ninh mạng trên thế giới 5

1.1.1. Chiến tranh mạng 5

1.1.2. Xây dựng đội an ninh mạng 7

1.2. Tình hình an ninh mạng tại Việt Nam 10

1.2.1. Hiện trạng công tác đảm bảo an toàn thông tin trong các cơ quan nhà nước 10

1.2.2. Mã độc tràn lan tại Việt Nam 11

1.2.3. Tin nhắn rác 13

1.2.4. Lừa đảo, trộm cắp trên mạng viễn thông và Internet 15

1.2.5. Lợi dụng mạng viễn thông và Internet cho các hoạt động phá hoại 15

1.2.6. Trộm cắp và mua bán thông tin cá nhân 16

1.3. Một số nguy cơ gây mất An toàn thông tin 16

1.3.1. Tấn công từ chối dịch vụ với quy mô lớn 16

1.3.2. Các vụ tấn công mạng mà đứng sau là các quốc gia 18

1.3.3. Nguy cơ với các thiết bị di động thông minh 20

1.4. An ninh mạng và các yếu tố cần bảo vệ 22

1.5. Các tiêu chí đánh giá mức độ an ninh an toàn mạng 23

1.5.1. Đánh giá trên phương diện vật lý 23
1.5.2. Đánh giá trên phương diện logic 24
1.6. Các hiểm họa chính đối với an toàn hệ thống mạng 26
1.6.1. Các hiểm họa không có cấu trúc 27
1.6.2. Các hiểm họa có cấu trúc 28
1.6.3. Các hiểm họa từ bên trong 29
1.6.4. Các hiểm họa từ bên ngoài 30

Chương 2. Một số hành vi vi phạm thường gặp trên mạng Internet 31
2.1. Lừa đảo trên mạng xã hội 31
2.2. Giả mạo tổ chức cá nhân trên mạng xã hội 40
2.3. Phát tán thư rác, mã độc trên mạng xã hội 44
2.4. Vi phạm bản quyền trên Internet 45

Chương 3. Một số hình thức tấn công mạng phổ biến 46
3.1. Hình thức tấn công APT 46
3.1.1. Tấn công APT có chủ đích 46
3.1.2. APT diễn ra như thế nào? 47
3.1.3. Một ví dụ điển hình về tấn công APT 48
3.1.4. Đánh giá về tấn công APT 49
3.1.5. Chống lại APT 50
3.2. Hình thức tấn công lừa đảo Phishing 52
3.2.1. Lừa đảo trực tuyến 53
3.2.2. Địa chỉ giả 55
3.2.3. Chống lừa đảo trực tuyến 58
3.2.4. Đối mặt với Phishing 60

3.3. Hình thức tấn công khác 61
3.3.1. Tấn công theo kiểu thăm dò 61
3.3.2. Tấn công truy cập 64
3.3.3. Tấn công từ chối dịch vụ (DoS) 66
3.3.4. Tấn công thao tác dữ liệu 74

Chương 4. Bảo vệ máy tính người dùng 79
4.1. Những thói quen sử dụng máy tính gây mất an toàn thông tin 79
4.2. An toàn thông tin khi sử dụng mạng không dây 83
4.2.1. Những việc cần làm khi truy cập Internet bằng mạng không dây công cộng 84
4.2.2. Kỹ năng phòng chống mã độc 87
4.3. Một số cách phòng chống mã độc 89
4.3.1. Sử dụng thư điện tử thận trọng 89
4.3.2. Cẩn thận khi truy cập các website trên mạng Internet 89
4.3.3. Không sử dụng phần mềm bẻ khóa, không bản quyền 90
4.3.4. Sử dụng phần mềm diệt virus 91
4.4. Hướng dẫn nhận biết, phòng chống thư rác, thư giả mạo, tin nhắn rác 92
4.5. Hướng dẫn sử dụng mạng xã hội an toàn 94
4.5.1. Các rủi ro khi sử dụng mạng xã hội 94
4.5.2. Hướng dẫn thiết lập chế độ an toàn cho tài khoản Facebook 96

Chương 5. Thiết lập an toàn cho hệ thống mạng 98
5.1. Phân vùng hệ thống mạng 98
5.1.1. Lựa chọn mô hình phân vùng mạng 99

5.1.2. Phân vùng mạng dựa vào trách nhiệm theo lĩnh vực công việc 99
5.1.3. Phân vùng mạng dựa vào mức độ đe dọa và rủi ro về an toàn 101
5.2. Thiết lập an toàn cho hệ điều hành mạng 102
5.2.1. Thiết lập các kiểm soát truy cập 102
5.2.2. Xác định các quyền truy cập 113
5.2.3. Kiểm soát truy cập dựa vào vai trò 116
5.2.4. Thiết lập các công cụ nền tảng cho kiểm soát truy cập 117
5.3. Thiết lập nền tảng xác thực an toàn 127
5.3.1. Thiết lập mật khẩu an toàn 128
5.3.2. Các phương pháp xác thực mạnh 142
5.3.3. Thiết lập các dịch vụ xác thực 143
5.3.4. Sử dụng các phương pháp xác thực đa nền tảng 145
Chương 6. Phòng chống các vi phạm trên mạng Internet 147
6.1. Xây dựng kế hoạch và chính sách an toàn thông tin mạng 147
6.1.1. Xây dựng và ban hành văn bản pháp luật 147
6.1.2. Hợp tác quốc tế 149
6.1.3. Nâng cao năng lực và nhận thức 150
6.1.4. Xây dựng tiêu chuẩn, hướng dẫn kỹ thuật 151
6.1.5. Nghiên cứu, phát triển 152
6.1.6. Đầu tư trang thiết bị 154
6.1.7. Theo dõi, giám sát 154
6.1.8. Phối hợp xử lý sự cố 155

6.2. Thiết kế các cơ chế an toàn 155
6.2.1. Cơ chế an toàn vật lý 155
6.2.2. Cơ chế xác thực 156
6.2.3. Cơ chế cấp quyền 156
6.2.4. Cơ chế kiểm toán 157
6.2.5. Mã hóa dữ liệu 157
6.3. Xây dựng quy trình quản lý mạng an toàn 158
6.3.1. Quản lý lỗi 158
6.3.2. Quản lý cấu hình 160
6.3.3. Quản lý kiểm toán 160
6.3.4. Quản lý hiệu suất 161
6.3.5. Quản lý an toàn 163
6.4. Các phương pháp chọn lọc Spam 166
6.4.1. Sử dụng bộ lọc phòng, ngăn chặn Spam 166
6.4.2. Thay đổi thói quen người sử dụng 172
6.4.3. Các phương pháp chọn lọc Spam 174
6.5. Phòng chống mã độc 179
6.5.1. Bảo vệ hệ thống khỏi Virus và Spyware 179
6.5.2. Phòng chống sâu mạng 183
6.5.3. Bảo vệ ứng dụng Web từ các tấn công 190
6.6. Hệ thống giám sát An ninh mạng 195
6.6.1. Các yếu tố cơ bản của giám sát 196
6.6.2. Các giải pháp công nghệ giám sát an toàn mạng 196

6.6.3. Giải pháp quản lý và phân tích sự kiện an ninh 197
6.6.4. Thành phần quản trị tập trung 199
6.6.5. Các thành phần khác 199
Chương 7. Xử lý sự cố khi xảy ra mất ATTT mạng 200
7.1. Diễn tập an toàn thông tin hàng năm 200
7.2. Quy trình phát hiện và xử lý sự cố mã độc 202
7.2.1. Quy trình phát hiện và xử lý sự cố mã độc 202
7.2.2. Xây dựng và phát triển các kỹ năng liên quan đến mã độc 204
7.2.3. Nâng cao khả năng điều phối 205
7.2.4. Thu thập công cụ và tài nguyên 205
7.2.5. Các dấu hiệu nhận biết sự cố mã độc hại 207
7.2.6. Xác định các đặc điểm sự cố mã độc hại 214
7.2.7. Phản ứng sự cố ưu tiên 216
7.2.8. Ngăn chặn 217
7.2.9. Ngăn chặn thông qua sự hợp tác người dùng 218
7.2.10. Ngăn chặn thông qua phát hiện tự động 219
7.2.11. Ngăn chặn thông qua vô hiệu hóa dịch vụ 220
7.2.12. Ngăn chặn thông qua ngắt kết nối 220
7.2.13. Khuyến cáo ngăn chặn 221
7.2.14. Xác định các máy chủ bị nhiễm 221
7.2.15. Xử lý triệt để 225
7.2.16. Phục hồi 227

Chương 8. Chính sách an toàn thông tin cho người dùng và tổ chức 228
8.1. Chính sách an toàn thông tin cho người dùng 228
8.1.1. Phân loại người dùng 228
8.1.2. Chính sách chấp nhận người dùng 239
8.1.3. Phân mức quyền truy nhập 240
8.1.4. Chính sách nhận thức an toàn 241
8.2. Chính sách an toàn thông tin cho tổ chức 242
8.2.1. Chính sách an toàn cơ sở hạ tầng công nghệ thông tin 242
8.2.2. Các chính sách miền hệ thống/ứng dụng 261
8.2.3. Các chính sách viễn thông 263
8.3. Chính sách phân loại và quản lý dữ liệu, và chính sách quản lý rủi ro 265
8.3.1. Chính sách phân loại dữ liệu 265
8.3.2. Chính sách quản lý dữ liệu 270
8.3.3. Các loại rủi ro liên quan đến hệ thống thông tin 272
8.3.4. Chính sách phân tích tác động các hoạt động trong tổ chức 273
8.3.5. Chính sách đánh giá rủi ro 273
8.3.6. Chính sách lên kế hoạch duy trì liên tục các hoạt động 274
8.3.7. Chính sách khắc phục thảm họa 276
8.4. Chính sách xử lý sự cố 277
Phụ lục 279
Tài liệu tham khảo 292