Inhaltsverzeichnis

1. Vorwort 1

1.1. Warum gibt es brand-wand? . . . 2
1.2. Der etwas andere Weg... . . . 2
1.3. Zielgruppe . . . 3
1.4. Danksagung . . . 3

2. Wer ist Admina? 5

2.1. Der Start in einen neuen Lebensabschnitt . . . 6
2.2. Steckbrief . . . 6
2.3. Foto unserer Protagonistin . . . 7

3. Von 0 auf 100 in 90 Tagen 9

3.1. Der erste Arbeitstag . . . 10
3.2. TransLKW AG . . . 10
3.3. Das IT-Team . . . 10
3.4. Der Platz im Team . . . 11
3.5. Erstens kommt es anders, zweitens als man denkt . . . 12
3.6. Und da waren's nur noch drei . . . 12

4. Geschichtsunterricht 13

4.1. Lernstoff statt Brennstoff . . . 14
4.2. Die Geschichte des Internets . . . 14
4.3. Morris Wurm . . . 15
4.4. Die ersten Firewalls . . . 16
4.4.1. Access Control List . . . 17
4.4.2. Der Klassiker: Paketfilter . . . 17

4.4.3. Huhn oder Ei? . . . 19

5. Die nötigen Netzwerkgrundlagen 21
5.1. Und wo steht Admina? . . . 22
5.2. Vorgehensplan für die Technik . . . 23
5.3. ISO/OSI Modell . . . 25
5.3.1. Zusammenfassung der sieben Layer . . . 28
5.4. IPv4 und IPv6 . . . 29
5.4.1. IPv4 kurz und knapp . . . 29
5.4.2. Subnetzmaske . . . 29
5.4.3. IPv4 und Subnetzmaske . . . 31
5.4.4. IPv4 und die Adressknappheit . . . 32
5.4.5. IPv6 kurz gestreift . . . 33
5.5. Was sind Ports? . . . 34
5.6. TCP- und UDP-Verbindungsaufbau . . . 37
5.7. Wie wird im Netzwerk kommuniziert . . . 41
5.8. Was muss man wissen? . . . 43

6. Firewall Grundlagen 45
6.1. Das Mittagessen mit Stefan . . . 46
6.2. Was ist eine Firewall . . . 48
6.3. Was ist eine DMZ . . . 50
6.4. Firewall-Slang . . . 52
6.5. Die Vierfaltigkeit der Firewall . . . 53
6.6. Firewall Philosophie . . . 54
6.6.1. Deny Filter - Verbotsfilter . . . 54
6.6.2. Pass Filter - Erlaubnisfilter . . . 55
6.7. Das Firewall Regelset . . . 55
6.7.1. Aufbau einer Policy . . . 55
6.7.2. Und wer sendet von wo? . . . 57
6.7.3. Der "First match, first win"-Grundsatz . . . 57
6.7.4. Ein erstes Policy-Beispiel . . . 58
6.7.5. Sägen Sie nie den Ast ab, auf dem Sie sitzen . . . 60
6.8. Die Grenzen einer Firewall . . . 61
6.9. Was muss man wissen? . . . 63

7. Firewalltypen 65
7.1. Paketfilter . . . 66
7.1.1. Wo wird geprüft? . . . 68
7.1.2. Statische Paketfilter . . . 69
7.1.3. Dynamische Paketfilter . . . 69
7.1.4. Vergleich statische und dynamische Paketfilter . . . 70

7.1.5. Beispiele von Paketfiltern . . . 71
7.2. Proxy Firewall . . . 72
7.2.1. Wo wird geprüft? . . . 73
7.2.2. Protokollkonformität . . . 75
7.2.3. Paketfilter und Proxy-Firewall im Vergleich . . . 75
7.3. Application Level Firewall . . . 76
7.3.1. Wo wird geprüft? . . . 76
7.3.2. Paketfilter, Proxy- und ALF im Vergleich . . . 78
7.4. Information zu den drei Firewalltypen . . . 78
7.5. Die Entwicklung geht weiter... . . . 79

8. Firewall Architekturen 81
8.1. Einfache Internetverbindung . . . 82
8.2. Einfache Internetverbindung mit DMZ . . . 83
8.3. Internetverbindung mit hoher Sicherheit . . . 84
8.4. Hochverfügbarkeit . . . 85
8.4.1. Anbindung mit einem Router . . . 85
8.4.2. Anbindung mit zwei Routern . . . 86
8.5. Lastverteilung auf der Firewall . . . 87
8.6. Multinationales Firmennetzwerk . . . 87
8.7. Zusammenarbeit mit Partner . . . 88
8.7.1. Anbindung an Firewall . . . 88
8.7.2. Anbindung an dedizierter Firewall . . . 89
8.8. Zusammenfassung der Architekturen . . . 90

9. Angriffe und Firewalls 91
9.1. DoS - Denial of Service . . . 92
9.2. DDoS - Distributed Denial of Service . . . 93
9.3. Brute Force - die rohe Gewalt . . . 94
9.4. IP-Spoofing . . . 95
9.4.1. Smurf . . . 96
9.4.2. SYN-Flood . . . 96
9.5. Erkennt eine Firewall einen Angriff? . . . 97
9.5.1. Intrusion Detection System . . . 98
9.5.2. Intrusion Prevention System . . . 98
9.6. Fazit Angriffe . . . 98

10. Admina und die Firewall 101
10.1. Admina wird langsam fit . . . 102
10.2. Die Policies von TransLKW . . . 105
10.3. Analyse der Policies . . . 106
10.4. Verbesserungsmöglichkeiten . . . 107

11. Grundlagen des Managements 109
11.1. Warum Management . . . 110
11.2. Der PDCA-Zyklus . . . 111
11.3. Grundlegender Lösungsansatz . . . 112
11.4. So viel wie nötig, so wenig wie möglich . . . 113
11.5. Ist die IT-Verfügbarkeit ein Risiko? . . . 115
11.6. Rund ums Risiko . . . 117
11.6.1. Definition Risiko . . . 117
11.6.2. Risiken im Geschäftsalltag . . . 117
11.6.3. Risiken versus Standards . . . 118
11.6.4. Das Restrisiko . . . 121
11.6.5. Service Level Agreement . . . 122

12. Dokumentation 125
12.1. Was gehört alles in eine Dokumentation . . . 126
12.2. Dokumentation kurz und knapp . . . 130
12.3. Admina und das liebe Management . . . 131
12.4. Praktische Anwendung von PDCA . . . 132
12.5. Das fehlende Feedback . . . 135

13. Evaluation, Kauf & Implementierung 137
13.1. Die Struktur einer Evaluation . . . 138
13.1.1. Fundament erarbeiten . . . 139
13.1.2. Durchführung . . . 140
13.1.3. Resultate . . . 142
13.2. Nur zertifizierte Firewalls? . . . 142
13.3. Kauf einer neuen Firewall . . . 144
13.4. Implementierung . . . 147
13.4.1. Vorbereitungen für die Implementierung . . . 147
13.4.2. Die Testphase . . . 148
13.4.3. Die Implementierung . . . 149

14. Management Querbeet 151
14.1. Für was brauche ich Management bei Firewalls? . . . 152
14.2. Wie argumentieren Sie für eine neue Firewall? . . . 152
14.3. Gewisse Spannungsfelder gelten als gegeben . . . 155
14.4. Hat die Unternehmensgrösse Einfluss auf meine Management-Instrumente? . . . 156

15. Grundlagen des Rechts 159
15.1. Das Recht in seinen Grundzügen . . . 160
15.1.1. Das Privatrecht . . . 160
15.1.2. Das öffentliche Recht . . . 160
15.1.3. Dispositives & zwingendes Recht . . . 161

15.1.4. Die Obligation . . . 162
15.1.5. Auflösung eines Vertrages . . . 164
15.1.6. Zusammenfassung Grundlagen . . . 165

16. Die Gesetze 167
16.1. Schweizerisches Zivilgesetzbuch . . . 168
16.2. Obligationenrecht . . . 168
16.3. Bundesgesetz über den Datenschutz . . . 168
16.4. Bundesgesetz über das Urheberrecht . . . 169
16.5. Schweizerisches Strafrecht . . . 169
16.6. Zusammenfassung Gesetze . . . 170

17. Praxisfragen im Bezug auf Firewall 177
17.1. Eindringen in ein Datenverarbeitungssystem . . . 178
17.2. Erschleichen einer Leistung . . . 181
17.3. Wer haftet bei Peer-2-Peer? . . . 182
17.4. Hilfe, ich bin ein SPAMER . . . 184
17.5. Wie stark darf ich meine Mitarbeiter loggen? . . . 186

18. Firewall im Eigenbau 189
18.1. Welche Firewall-Software? . . . 191
18.2. Die Hardware . . . 192
18.3. Vorbereitungsarbeit und Zusammenbau . . . 193
18.4. Die Installation von PFSense . . . 195
18.5. Grundkonfiguration von PFSense . . . 198
18.6. Konfiguration von PFSense . . . 201
18.7. Das Firewall-Ruleset PFSense . . . 203
18.8. Fazit PFSense . . . 205

A. Beispiel einer Firewall Dokumentation 207

B. Kontrollblatt für Firewallpolicies 219

C. Beispiel einer Richtlinie für die Internetnutzung 221

D. Glossar 223