

Table of Contents

Introduction	ix
Chapter 1. An Ordinary Day in the Life of Mr. Rowley, or the Dangers of Virtualization and Mobility	1
1.1. A busy day	1
1.2. The ups and downs of the day	3
1.3. What actually happened?	3
Chapter 2. Threats and Attacks	7
2.1. Reconnaissance phase	9
2.1.1. Passive mode information gathering techniques	10
2.1.2. Active mode information gathering techniques	14
2.2. Identity/authentication attack	22
2.2.1. ARP spoofing	22
2.2.2. IP spoofing	22
2.2.3. Connection hijacking	29
2.2.4. Man in the middle	29
2.2.5. DNS spoofing	30
2.2.6. Replay attack	31
2.2.7. Rebound intrusion	31
2.2.8. Password hacking	32
2.2.9. The insecurity of SSL/TLS	34
2.3. Confidentiality attack	38
2.3.1. Espionage software	39
2.3.2. Trojans	41
2.3.3. Sniffing	43
2.3.4. Cracking encrypted data	44

2.4. Availability attack	49
2.4.1. ICMP Flood	50
2.4.2. SYN Flood	50
2.4.3. Smurfing	52
2.4.4. Log Flood	52
2.4.5. Worms	53
2.5. Attack on software integrity	55
2.6. BYOD: mixed-genre threats and attacks	57
2.7. Interception of GSM/GPRS/EDGE communications	61
Chapter 3. Technological Countermeasures	65
3.1. Prevention	66
3.1.1. Protection of mobile equipment	67
3.1.2. Data protection	71
3.2. Detection	81
3.2.1. Systems of intrusion detection	81
3.2.2. Honeypot	88
3.2.3. Management and supervision tools	91
3.3. Reaction	95
3.3.1. Firewall	95
3.3.2. Reverse proxy	102
3.3.3. Antivirus software	104
3.3.4. Antivirus software: an essential building block but in need of completion	107
3.4. Organizing the information system's security	108
3.4.1. What is security organization?	109
3.4.2. Quality of security, or the attraction of ISMS	110
Chapter 4. Technological Countermeasures for Remote Access	113
4.1. Remote connection solutions	114
4.1.1. Historic solutions	115
4.1.2. Desktop sharing solutions	115
4.1.3. Publication on the Internet	116
4.1.4. Virtual Private Network (VPN) solutions	118
4.2. Control of remote access	137
4.2.1. Identification and authentication	139
4.2.2. Unique authentication	155
4.3. Architecture of remote access solutions	157
4.3.1. Securing the infrastructure	157
4.3.2. Load balancing/redundancy	161
4.4. Control of conformity of the VPN infrastructure	162
4.5. Control of network admission	166

4.5.1. Control of network access	166
4.5.2. ESCV (Endpoint Security Compliancy Verification)	167
4.5.3. Mobile NAC	170
Chapter 5. What Should Have Been Done to Make Sure Mr Rowley’s Day Really Was Ordinary	173
5.1. The attack at Mr Rowley’s house	173
5.1.1. Securing Mr Rowley’s PC	173
5.1.2. Securing the organizational level	174
5.1.3. Detection at the organizational level	175
5.1.4. A little bit of prevention.	175
5.2. The attack at the airport VIP lounge while on the move	176
5.3. The attack at the café	176
5.4. The attack in the airport VIP lounge during Mr Rowley’s return journey	178
5.5. The loss of a smartphone and access to confidential data	180
5.6. Summary of the different security solutions that should have been implemented	181
Conclusion	187
APPENDICES	189
Appendix 1.	191
Appendix 2.	197
Bibliography.	223
Index.	233