Inhalt

	Editorial	**3**
1	**Ratgeber und Praxis**	**8**
1.1	**So erkennen Sie Hacker auf Servern**	**8**
1.1.1	Server auf verdächtige Prozesse untersuchen	8
1.1.2	Bots und Rootkits entfernen	9
1.1.3	Offenes Relay auf dem E-Mail-Server	10
1.1.4	Verdächtigen Netzwerkverkehr finden	11
1.1.5	Geöffnete Ports analysieren	12
1.1.6	Einbrüche in Active Directory erkennen	14
1.1.7	DEFT Linux 8.2 – Sicherheits-Live-CD für Administratoren	15
1.2	**DNS-Attacken – Typen und Sicherheitsvorkehrungen**	**16**
1.2.1	Angriffe, um DNS-Dienste zu unterbrechen	16
1.2.2	Angriffe, um über das DNS Unternehmen auszuspähen	19
1.2.3	DNS-Angriffen vorbeugen	19
1.2.4	Fazit	20
1.3	**Verschlüsselung – was ist noch unknackbar?**	**21**
1.3.1	Von wo die Gefahr droht	21
1.3.2	Was ist heute noch sicher?	23
1.3.3	Fazit	25
1.4	**TLS/SSL – Fragen und Antworten**	**26**
1.4.1	Wie funktioniert Verschlüsselung?	26
1.4.2	Welche Verschlüsselungsmethoden kommen im Internet zum Einsatz?	26
1.4.3	Was sind die Aufgaben von SSL beziehungsweise TLS?	27
1.4.4	Was hat Verschlüsselung mit Zertifikaten zu tun?	27
1.4.5	Welche Anwendungen verwenden SSL-Zertifikate?	27
1.4.6	Wie verläuft ein typischer SSL-Verbindungsaufbau?	27
1.4.7	Schützen Zertifikate vor Datendiebstahl?	28
1.4.8	Welche digitalen Zertifikate gibt es?	28
1.4.9	Sind alle Zertifikate gleich sicher?	28
1.4.10	Wer garantiert die Vertrauenswürdigkeit von Zertifikaten?	29
1.5	**BadUSB: So groß ist die Gefahr wirklich**	**30**
1.5.1	BadUSB – was ist eigentlich das Problem?	31
1.5.2	Wie hoch ist aktuell die reelle Gefahr?	31
1.5.3	Gibt es Schutz vor dieser Bedrohung?	32
1.5.4	Was können Anwender und Firmen tun?	33
1.5.5	Fazit: Mehr Vorsicht denn je ist geboten	36
1.6	**Wirksame E-Mail-Verschlüsselung mit S/MIME**	**38**
1.6.1	S/MIME in der Kürze	38
1.6.2	Wie kompatibel ist M/MIME?	38
1.7	**Die sichere E-Mail im Mittelstand**	**40**
1.7.1	E-Mail-Appliance oder doch „nur“ Software?	40
1.7.2	Die Hardwarelösung: alles in einer Appliance	41
1.7.3	Appliance ohne Hardware: die Lösung für Virtualisierungs-Profis	42
1.7.4	Barracuda mit Auswahl: Appliance, virtuell im RZ oder Cloud	42
1.7.5	Zwei Welten vereinigt: Managed Appliance von antispameurope	44
1.7.6	Alle E-Mail-Daten aus der Cloud?	45
1.7.7	E-Mail-Lösungen aus der Cloud: Angebote von vielen Providern	46
1.7.8	Fazit sichere E-Mail: Die Lösung muss passen	48

1.8	**Perfect Forward Secrecy – was ist das?**	**49**
1.8.1	Öffentlich und privat	49
1.8.2	Was ist bei PFS anders?	50
1.8.3	PFS nutzen	50
1.9	**Cyber-Spionage in der Praxis**	**52**
1.9.1	Schwarzmarkt für Zero-Day-Exploits	52
1.9.2	Staaten mischen kräftig mit	53
1.9.3	Angreifer gehen methodisch vor	53
1.9.4	Die Folgen eines Angriffs	54
1.9.5	Pro und Contra Meldepflicht	55
1.9.6	Empfehlungen: Datenspionage verhindern	55
1.10	**Gehört die Bremse bald dem Hacker?**	**57**
1.10.1	Höhere Risiken	57
1.10.2	Datenschutz	58
1.10.3	Interoperabilität ist Trumpf	58
1.10.4	Gelernte Lektionen	59
1.10.5	Wie kommt der Erfolg?	60
2	**Tipps und Tools**	**61**
2.1	**Tipps für den IT-Notfall**	**61**
2.2	**So vermeiden Sie IT-Ausfälle im Unternehmen**	**64**
2.2.1	Die Werkzeuge im Krisenfall	65
2.2.2	Krisenmanagement – von A wie Alarmierung …	65
2.2.3	… bis Z wie zentrales Power-Management	65
2.2.4	Typische Fehler bei Disaster-Recovery-Szenarien	66
2.2.5	Umfassende IT-Security ist Pflicht	67
2.3	**Windows zuverlässig vor Angriffen schützen**	**68**
2.3.1	Erweiterter Schutz mit Microsoft Enhanced Mitigation Experience Toolkit (EMET)	68
2.3.2	EMET produktiv nutzen	69
2.3.3	Security TechCenter – My Security Bulletins Dashboard	71
2.3.4	Windows 7 sicherer machen – Microsoft Enterprise Hotfix-Rollup	71
2.4	**Mehr Sicherheit für Windows – die besten Tipps und Tools**	**72**
2.4.1	Mehr Sicherheit im Browser	72
2.4.2	Regelmäßig Windows-Updates installieren, auch für andere Microsoft-Programme	72
2.4.3	Virenscanner von Drittherstellern installieren und automatisiert aktualisieren	73
2.4.4	Lassen Sie Rechner regelmäßig mit Kaspersky-Rettungs-CD scannen	74
2.4.5	AdwCleaner installieren und verwenden	75
2.4.6	Microsoft-Windows-Tool zum Entfernen bösartiger Software verwenden	75
2.4.7	Spybot Antispyware herunterladen und System immunisieren	75
2.4.8	Autostart-Programme im Blick behalten	76
2.5	**Die 10 besten Security-Tools für den PC**	**77**
2.5.1	AVG Antivirus Free	77
2.5.2	Zone Alarm Free Firewall	77
2.5.3	KeePass Password Safe	78
2.5.4	K9 Web Protection	78
2.5.5	Malwarebytes Anti-Malware	79
2.5.6	McAfee Labs Stinger	80
2.5.7	Virus Total	80
2.5.8	SpyBot – Search & Destroy	81
2.5.9	Avast Free Antivirus	81
2.5.10	Paragon Backup und Recovery	81
2.6	**Spurensuche: Der Surf-Check**	**82**
2.6.1	Cookies: So funktioniert der Netzwerk-Trick	82
2.6.2	So machen Sie die Cookies einer Website sichtbar	83

2.6.3	Bestimmte Werbung nicht mehr anzeigen lassen	84
2.6.4	Abwägung: Vor- und Nachteile personalisierter Werbung	84
2.6.5	So geht's: personalisierte Werbung abschalten	85
2.6.6	Wer es spartanisch mag: Cookies löschen, immer ausloggen	86
2.6.7	Bremsklötze finden: So analysieren Sie eine Website	86
2.7	**Spezielle Linux-Distributionen für die Datenrettung**	**88**
2.7.1	Parted Magic	88
2.7.2	Parted-Magic-Werkzeuge	90
2.7.3	Trinity Rescue Kit	91
2.7.4	Virenjagd mit TRK	92
2.7.5	SystemRescueCd	93
2.7.6	Tipp: eine eigene Datenrettungs-Distribution basteln	94
2.7.7	Fazit	96
2.8	**Linux-Distributionen für die Netzwerksicherheit**	**97**
2.8.1	Firewall und Router: Endian	97
2.8.2	Devil Linux: von Admins für Admins	98
2.8.3	Mit Vyatta das Netzwerk schützen	100
2.8.4	Abbild unter 25 MByte: m0n0wall	100
2.8.5	Auf FreeBSD basierend: pfSense	102
2.8.6	Die Netzpolizei: IPCop	104
2.8.7	Übersichtlich: SmoothWall Express	105
2.8.8	Fazit	106
3	**Sicherheit im Unternehmen**	**107**
3.1	**Woran der Datenschutz im Unternehmen krankt**	**107**
3.1.1	Datenschutz in Deutschland und Europa	107
3.1.2	Unnötiges Risiko	108
3.1.3	Kosten für die Umsetzung	108
3.1.4	Was ist zu tun?	109
3.2	**Cyber-Kriminalität: Wann zahlt die Versicherung?**	**110**
3.2.1	Das Krisenmanagement entscheidet	111
3.2.2	Wo die Versicherung ins Spiel kommt	111
3.2.3	Beispiel: Cyber Risk Management by Hiscox	112
3.2.4	Im Ernstfall	113
3.2.5	Und danach?	114
3.3	**Cyber-Forensiker sind die digitale Feuerwehr**	**115**
3.3.1	Die Ghost-Busters unter den ITlern	115
3.3.2	Anomalien jagen gehen	115
3.3.3	Hände aus der Keksdose	116
3.3.4	Die Master-Forensiker	117
3.3.5	Vor Gericht verwertbar	117
3.3.6	Quereinsteiger und Künstler	118
3.4	**Warum Nutzername und Passwort nicht mehr schützen**	**119**
3.4.1	Remote-Zugriff ist jetzt die Norm	119
3.4.2	Über die Entwicklung von Hacker-Angriffen	119
3.4.3	Welcher Schutz ist am besten?	120
3.4.4	Multi-Faktor-Authentifizierung neu gedacht	121
3.4.5	Ein Blick in die Zukunft	122
3.5	**Wie Home Office sicher wird**	**123**
3.5.1	Security ist mehr als eine Pflichtübung	124
3.5.2	Risiken des mobilen Arbeitens	125
3.5.3	Schwachstelle Endgeräte	126
3.5.4	Der Faktor Mensch	127
3.5.5	Gutes Passwort?	127

3.5.6	Flexibilität braucht ein ISMS	127
3.5.7	Wie kann gutes Mobile Working aussehen?	129
3.5.8	Praxisbeispiel: Mobile Office im täglichen Einsatz	130
3.6	**Die Psychologie der E-Mail-Scams**	**131**
3.6.1	Ein lukratives Geschäft	131
3.6.2	Der Erfolg scheint sicher	132
3.6.3	Der Mensch, das immergleiche Risiko	132
3.6.4	Wer klickt?	133
3.6.5	Auf was?	134
3.6.6	Wer ist Ziel?	135
3.6.7	Die Kunst des Marketings	135
3.6.8	Ein Problem für die Zukunft	135
3.6.9	Wie sich Unternehmen schützen können	136
3.7	**Unternehmen wollen vor Geheimdiensten nicht kapitulieren**	**137**
3.7.1	Technologie braucht Sicherheit	137
3.7.2	Wer früh erkennt, schützt besser	137
3.7.3	„Revival des Endpoint“	139
3.8	**Mehr Sicherheit dank Open Source**	**140**
3.8.1	Community – die objektive Instanz	140
3.8.2	Schnelle Aufdeckung komplexer Bedrohungen	141
3.8.3	Sicherheitslücken schließen	142
3.8.4	Intelligentere Lösungen	142
4	**Security in der Cloud**	**143**
4.1	**Verschlüsselung in der Praxis**	**143**
4.1.1	Die gängigsten Krypto-Arten	143
4.1.2	Symmetrische Kryptografie	144
4.1.3	Asymmetrische Kryptografie	146
4.1.4	Vergleich beider Verfahren	147
4.1.5	Zertifikate	147
4.1.6	SSL/TLS-Verbindungen im Alltag	148
4.1.7	Verschlüsselung in der Cloud	149
4.1.8	Fazit	150
4.2	**SaaS-Sicherheit: Fünf wichtige Punkte, die Kunden beachten sollten**	**151**
4.2.1	SSL ist ein absolutes Muss	152
4.2.2	Regelmäßige Backups sind Pflicht	153
4.2.3	Doppelt gut: redundante Systeme	153
4.2.4	Zertifizierungen und Gütesiegel	154
4.2.5	Verschlüsselung wird immer wichtiger	155
4.3	**Community Cloud – eine Wolke für besondere Sicherheitsansprüche**	**156**
4.3.1	Cloud Management als sichere Brücke zur Community	157
4.3.2	Erhöhtem Sicherheitsbedarf leichter entgegenkommen	158
4.3.3	Verbindliche Sicherheitsrichtlinien für alle Teilnehmer	159
4.3.4	Zugangsberechtigung nur mit dem richtigen Zertifikat	159
4.3.5	Gemeinsam definierte Standards erleichtern Zusammenarbeit	160
	Impressum	**162**