

Lars Behrens

**WEKA**

# IT-Sicherheit

So schützen Sie Ihr Unternehmen  
vor Systemstörungen und Risiken

**B BOOKS**  
BUSINESS BOOKS

*Ein Problem? Kein Problem!*

CIP-Kurztitelaufnahme der deutschen Bibliothek

## IT-Sicherheit

Autor: Lars Behrens

Projektleitung: Petra Schmutz

WEKA Business Media AG, Schweiz

© WEKA Business Media AG, Zürich, 2013

Alle Rechte vorbehalten, Nachdruck – auch auszugsweise – nicht gestattet.

Die Definitionen, Empfehlungen und rechtlichen Informationen sind von den Autoren und Verlag auf deren Korrektheit in jeder Beziehung sorgfältig recherchiert und geprüft worden. Trotz aller Sorgfalt kann eine Garantie nicht übernommen werden. Eine Haftung der Autoren bzw. des Verlags ist daher ausgeschlossen. Der Einfachheit halber und zwecks besserer Lesbarkeit wurden meist die männlichen Formen verwendet. Die weiblichen Formen sind dabei selbstverständlich mitgemeint.

WEKA Business Media AG

Hermetschloostrasse 77, CH-8048 Zürich

Telefon 044 434 88 88, Telefax 044 434 89 99

[www.weka.ch](http://www.weka.ch)

Zürich • Kissling • Paris • Amsterdam • Wien

---

ISBN 978-3-297-02063-0

1. Auflage 2013

Druck: Auble Druck GmbH, Layout: Dimitri Gabriel, Satz: Peter Jäggi



*Ein Problem? Kein Problem!*

# Inhaltsverzeichnis

## Inhaltsverzeichnis

<b>1.</b>	<b>Grundlagen der IT-Sicherheit</b> .....	<b>9</b>
1.2	Bedrohung der IT-Sicherheit .....	11
1.2.1	Bedrohungen durch organisatorische Fehler .....	11
1.2.1.1	Verantwortlichkeiten .....	12
1.2.1.2	Verwaltung der Betriebsmittel.....	13
1.2.1.3	Zutritt, Zugang und Zugriff.....	13
1.2.2	Bedrohungen durch das Personal .....	13
1.2.2.1	Neue Mitarbeiter .....	14
1.2.2.2	Alte Mitarbeiter und «vergessene» Accounts.....	14
1.2.2.3	Schulungen und Sensibilisierungen .....	14
1.2.2.4	Checkliste: Private Nutzung und Überwachung von E-Mail und Internet .....	15
1.2.2.5	Beispiel: Weisung zum Gebrauch von Informatikinstrumenten und zur Benutzung von elektronischen Kommunikationseinrichtungen (technische Betriebsmittel) .....	16
1.2.3	Bedrohungen durch technische Mängel .....	22
1.2.3.1	Sicherheitslücken und Exploits .....	22
1.2.3.2	Malware: Verbreitung auch ohne Sicherheitslücke .....	23
1.2.4	Checkliste: Keine Gegenmassnahme ohne bekannte Bedrohung .....	24
1.3	Risikoabschätzung und Wirtschaftlichkeitsbetrachtungen .....	24
1.3.1	Entwicklung eines Risikobewusstseins .....	25
1.3.2	Risiken und Schadensfälle .....	25
1.3.2.1	Verstoss gegen Gesetze oder Vorschriften.....	26
1.3.2.2	Beeinträchtigung der persönlichen Unversehrtheit.....	27
1.3.2.3	Beeinträchtigung der Aufgabenerfüllung .....	27
1.3.2.4	Negative Aussenwirkung.....	27
1.3.2.5	Finanzielle Auswirkungen.....	28
1.3.2.6	Umgang mit dem Risiko .....	28
1.3.3	Wirtschaftlichkeitsbetrachtungen .....	29
1.3.3.1	IT-Sicherheitsrisiken und IT-Investment .....	29
1.3.3.2	Beispiel einer Kosten-Nutzen-Rechnung.....	30
1.4	Anforderungen an die IT-Sicherheit .....	31
1.4.1	Einflussfaktoren .....	31
1.4.2	Katalog der Anforderungen .....	33
1.4.2.1	Vertraulichkeit .....	33
1.4.2.2	Verhinderung einer Verkehrsfluss-Analyse.....	33
1.4.2.3	Erkennung der Datenunversehrtheit.....	34
1.4.2.4	Authentifizierung des Kommunikationspartners.....	34
1.4.2.5	Authentifizierung des Ursprungs der Daten .....	35
1.4.2.6	Zugangs- und Zugriffskontrolle .....	35
1.4.2.7	Urhebernachweis .....	36
1.4.2.8	Empfängernachweis.....	36

1.4.2.9	Aufrechterhaltung des Betriebs.....	36
1.5	Aufbau eines CERT .....	36
1.5.1	Organisation und Personal .....	37
1.5.2	Aufgaben .....	37
<b>2.</b>	<b>Management und Organisation von IT-Sicherheit.....</b>	<b>39</b>
2.1	IT-Sicherheits-Management.....	41
2.2.1	Grundsätzliche Ansätze .....	41
2.2.1.1	Controlling-bezogenes Sicherheits-Management .....	41
2.2.1.2	Benutzerbezogenes Sicherheits-Management.....	42
2.2.1.3	Ganzheitlicher Ansatz im Sicherheits-Management .....	42
2.2.2	Strukturen und Verantwortlichkeiten.....	42
2.2.3	Standards .....	42
2.2.4	Werkzeuge zum Sicherheits-Management .....	43
2.2.4.1	Enterprise Security Management ESM .....	43
2.2.5	Outsourcing von Sicherheit .....	44
2.2.5.1	Zertifizierung und Normierung .....	45
2.2.5.2	Vertragsgestaltung .....	46
2.2.5.3	Beispiel: Outsourcing-Vertrag.....	47
2.3	Sicherheit als Prozess .....	54
2.3.1	Modell der Sicherheit .....	55
2.3.2	Der Regelkreis der Sicherheit.....	55
2.3.3	Unterstützung durch Standards.....	58
2.4	Prüfung der Sicherheit.....	58
2.4.1	Messung der Sicherheit .....	58
2.4.2	Vorbereitung .....	60
2.4.2.1	Festlegung des Umfangs der Arbeiten .....	60
2.4.2.2	Beschaffung des Ausgangsmaterials .....	60
2.4.2.3	Werkzeuge zur Datensammlung.....	60
2.4.2.4	Festlegung der Prüfstrategie .....	61
2.4.3	Durchführung .....	62
2.4.3.1	Interviews.....	62
2.4.3.2	Begehungen .....	62
2.4.3.3	Security-Scans .....	63
2.4.3.4	Penetrationstest .....	63
2.4.3.5	Auswertung von Logdateien .....	63
2.4.4	Auswertung.....	64
2.4.4.1	Erstellung des Berichts .....	64
2.4.4.2	Präsentation der Ergebnisse.....	65
2.5	Checkliste: Datensicherheit .....	65
2.6	Checkliste: Datenschutzvertrag .....	68
2.7	Mustervertrag: Sicherstellung des Datenschutzes .....	69
<b>3.</b>	<b>Wichtige Elemente der IT-Sicherheit.....</b>	<b>73</b>
3.1	Verschlüsselung.....	75
3.1.1	Symmetrische Verfahren.....	75
3.1.1.1	Vorteil symmetrischer Verfahren.....	75
3.1.1.2	Nachteile symmetrischer Verfahren .....	75

3.1.1.3	Data Encryption Standard (DES) .....	76
3.1.1.4	International Data Encryption Algorithm (IDEA) .....	76
3.1.1.5	RC4 .....	76
3.1.1.6	Advanced Encryption Standard (AES) .....	77
3.1.2	Asymmetrische Verfahren .....	77
3.1.2.1	Digitale Signatur .....	77
3.1.2.2	Vorteile asymmetrischer Verfahren .....	78
3.1.2.3	Nachteile asymmetrischer Verfahren .....	78
3.1.2.4	Diffie-Hellman .....	78
3.1.2.5	RSA .....	78
3.1.2.6	Die elliptische Kurvenkryptographie (ECC) .....	79
3.1.3	Hash-Funktionen .....	80
3.1.3.1	Message-Digest 4 (MD4) .....	80
3.1.3.2	Message Digest 5 (MD5) .....	81
3.1.3.3	Secure Hash Algorithm (SHA) .....	81
3.1.4	Hybride Verschlüsselungstechnik .....	81
3.2	Authentifizierung .....	82
3.2.1	Passwörter .....	82
3.2.1.1	Wiederverwendbare Passwörter .....	83
3.2.1.2	Einmalpasswörter .....	83
3.2.2	Smartcard (Token) .....	84
3.2.2.1	Aufbau einer Smartcard .....	84
3.2.2.2	Aktivierung der Smartcard .....	85
3.2.3	Biometrie .....	85
3.2.4	Steganografie .....	86
3.2.4.1	Technik .....	86
3.3	Autorisierung .....	87
3.3.1	Rollenbasierte Autorisierung .....	88
3.3.2	Ressourcenbasierte Autorisierung .....	88
3.3.3	Checkliste: Strategie zur Authentifizierung und Autorisierung .....	88
3.4	Abgesicherte Netzwerkprotokolle .....	89
3.4.1	Sicherungsverfahren im Netzwerk-Stack .....	89
3.4.2	Secure Socket Layer (SSL) .....	90
3.4.2.1	Arbeitsweise .....	91
3.4.2.2	Risiken von SSL .....	91
3.4.3	IPsec und IKE .....	91
3.4.3.1	Arbeitsweise .....	92
3.4.3.2	Schlüsselaustausch .....	92
3.4.3.3	Risiken bei IPsec und IKE .....	93
3.5	Computer-Forensik .....	94
3.5.1	Aufgaben der Computer-Forensik .....	94
3.5.1.1	Fragestellungen .....	95
3.5.1.2	Anforderungen .....	95
3.5.1.3	Techniken .....	96
3.5.2	Die Beweissicherung .....	97
3.5.2.1	Verhaltensregeln .....	97

3.5.2.2	Wunsch und Wirklichkeit .....	98
3.5.3	Die Analyse.....	98
3.5.3.1	Vorarbeiten .....	99
3.5.3.2	Auswertungen.....	99
3.5.3.3	Protokollierung.....	100
3.5.4	Empfehlenswerte Produkte für die forensische Analyse von IT-Systemen.....	101
<b>4.</b>	<b>IT-Sicherheit in Netzwerken .....</b>	<b>103</b>
4.1	Alles auf eine Karte? Suisseld, soziale Netzwerke und Sicherheit .....	107
4.1.1	Digitale Kommunikation.....	108
4.1.1.1	Schnell, einfach, tückisch?.....	108
4.1.1.2	Rolle der elektronischen Medien wird überschätzt.....	108
4.1.1.3	Soziale Medien verschlingen (Büro-)Zeit .....	110
4.1.1.4	Fazit: präsent sein mit Distanz.....	111
4.1.2	E-Government .....	111
4.1.2.1	E-Government ist in Unternehmen angekommen.....	111
4.1.2.2	Suisseld: ein elektronisches Angebot unter vielen.....	112
4.1.2.3	Praktische Anwendungen .....	113
4.1.2.4	Aktueller Stand der Umsetzung der Suisseld .....	113
4.1.3	Suisseld: privat oder geschäftlich? .....	114
4.1.3.1	Suisseld und E-Commerce.....	114
4.1.3.2	Gesicherter, personalisierter Zugang .....	115
4.1.3.3	Digitale Authentifizierung ersetzt Username/Passwort.....	115
4.1.3.4	Sicherheitsklassen: Kartenleser ist nicht gleich Kartenleser.....	116
4.1.4	Updates und Upgrades tun not .....	117
4.1.4.1	Verschiedene Identifizierungsverfahren.....	117
4.1.4.2	Tokentechnik .....	117
4.1.4.3	Biometrische Verfahren .....	118
4.1.5	Identitätsdiebstahl als reales Problem.....	118
4.1.6	Unsicheres Internet .....	118
4.1.6.1	Transportwege sind offen .....	118
4.1.6.2	Wege im Internet sind verknüpft, aber nicht vorhersagbar .....	119
4.1.6.3	Exkursion: Traceroute .....	120
4.1.6.4	Standleitungen: unsicher, etwas weniger und noch weniger unsicher.....	123
4.1.6.5	«Das Böse lauert immer und überall!».....	124
4.1.6.6	Verschlüsselung tut not.....	125
4.1.7	Sichere Kommunikation.....	125
4.1.7.1	Verschlüsselt, authentifiziert und unverfälscht .....	125
4.1.7.2	Verschlüsselung ist nicht per se sicher .....	126
4.1.7.3	Beispiel WLAN-Verschlüsselung.....	126
4.1.7.4	Wichtige Regel: Sichere Passwörter verwenden!.....	127
4.1.8	Eine Frage des Vertrauens .....	128
4.1.8.1	Authentifizierung .....	128
4.1.8.2	Verschiedene Möglichkeiten der Authentifizierung .....	129
4.2	Von Männern in der Mitte und gefälschten Namen .....	129
4.2.1	DNS-Spoofing und DNS-Poisoning .....	129
4.2.2	ARP-Poisoning.....	130

4.2.3	Man-in-the-Middle-Angriffe .....	131
4.2.4	Zusätzliche Identifikationsmethoden nutzen! .....	132
4.2.5	Phishing .....	132
4.2.6	Social Engineering.....	133
4.2.7	Replay-Angriffe .....	133
4.3	Firewall-Konzepte.....	134
4.3.1	Firewalls alleine geben keinen ausreichenden Schutz .....	134
4.3.2	Basis-Topologien .....	135
4.3.3	Einsatz von einfachen Paketfiltern.....	135
4.3.4	Zustandlos oder «stateless»?.....	137
4.3.5	Serverschutz: Umleitungen per Firewall.....	137
4.3.6	Nichts Pazifistisches: die DMZ .....	138
4.3.7	Eine schwierige Paarung: Firewalls und Serverdienste.....	139
4.3.8	Authentifizierung an der Firewall .....	140
4.3.8.1	Proxy-Firewalls .....	141
4.3.9	Hintereinanderschaltung von Firewalls.....	141
4.3.10	Mehrere Firewalls parallel .....	141
4.3.10.1	Aufteilung von Diensten.....	141
4.3.10.2	Lastverteilung.....	141
4.3.11	Dual-homed-Firewall .....	142
4.3.12	Circuit-Level-Gateways: bitte keine Einzelhaltung.....	142
4.3.13	Entscheidungskriterien .....	142
4.3.14	Zusätzliche Aspekte.....	143
4.3.15	Intrusion Detection und Firewalls .....	144
4.3.16	Content Security.....	144
4.3.17	Segmentierung von Netzwerken zur Erhöhung der Sicherheit.....	144
4.4	BYOD – der Feind im eigenen Haus? .....	145
4.4.1	Bedrohung von Innen? .....	145
4.4.2	BYOD geht überwiegend von Mitarbeitern aus .....	145
4.4.3	Pro oder Contra BYOD? .....	146
4.4.4	WILB – steigert privates Surfen die Produktivität? .....	146
4.4.5	Generation Y, «Milleniums» und «Always-On»: BYOD ist nicht aufzuhalten .....	147
4.4.5.1	Lascher Umgang mit Sicherheit des Unternehmens .....	147
4.4.6	Gewinner Android und Apple, Verlierer Microsoft.....	148
4.4.7	Mobile Device Management .....	148
4.4.8	Gesicherter Zugang zum Netzwerk unabdingbar .....	149
4.4.8.1	VPNs .....	150
4.4.9	Türsteher: Zugangskontrolle auch im Firmennetz.....	150
4.4.9.1	Proprietäre Softwarelösungen .....	151
4.4.9.2	Bewährte Hausmittel.....	151
4.4.9.3	Desktop-Virtualisierung.....	152
4.4.9.4	Ein fahrlässiger Umgang mit Geräten kann sich rächen.....	152
4.5	IT-Security-Konzept.....	152
4.5.1	Dokumentierte Sicherheit ist besser als «gemarkte» Sicherheit .....	152
4.5.2	Anforderungen an ein Sicherheitskonzept.....	153
4.5.3	Erstellung eines Sicherheitskonzepts.....	153

4.5.3.1	Aufgabe und Zielsetzung definieren.....	153
4.5.3.2	Einsatzzweck und -ort spielen eine wichtige Rolle.....	153
4.5.3.3	Zusammenarbeit von IT-Abteilung und Management.....	153
4.5.3.4	IT-Systemerfassung/Strukturanalyse.....	154
4.5.3.5	Schutzbedarfs-Feststellung.....	154
4.5.3.6	Basis-Sicherheitscheck.....	154
4.5.3.7	Modellierung nach IT-Grundschatz.....	154
4.6	Realisierung eines IT-Sicherheitskonzepts.....	154
4.6.1	IT-Strukturanalyse.....	155
4.6.1.1	Netzplan als Grundlage.....	155
4.6.1.2	Netzwerk visualisieren.....	155
4.6.2	Gruppenbildung.....	158
4.6.3	Liste der IT-Anwendungen.....	158
4.6.4	Schutzbedarfsfeststellung.....	159
4.6.4.1	Schutzbedarf konkretisieren.....	159
4.6.4.2	Schutzbedarf ermitteln.....	159
4.6.4.3	Schutzbedarf der IT-Systeme nach dem Maximum-Prinzip!.....	159
4.6.4.4	Kritische und nicht-kritische Kommunikationsverbindungen.....	159
4.7	Fazit.....	160
<b>5.</b>	<b>Sicherheit im LAN – das Ende der Firewalls?</b> .....	<b>161</b>
5.1	Netzwerksicherheit – Firewalls, Intrusion Detection.....	164
5.1.1	Netzangriffe erkennen – und abwehren!.....	164
5.1.2	Bedrohungen von Netzwerken.....	164
5.1.3	Internetkriminalität lauert selten am Übertragungsweg.....	165
5.1.4	Datenleitungen sind nicht per se «sicher»!.....	166
5.2	Firewall: Blick ins «Reich des Bösen».....	166
5.2.1	Logs beobachten!.....	167
5.2.2	Manuelle Beobachtung ist schwierig.....	168
5.2.3	Detektivarbeit.....	168
5.2.3.1	Checkliste: Systematisch Vorgehen bei Ports, Dienste, Logs und Telnet.....	168
5.2.3.2	Fachwissen ist erforderlich.....	170
5.2.4	Firewall kann Datenverkehr regeln.....	171
5.2.5	Abgestuftes Sicherheitssystem als bestmöglicher Schutz.....	172
5.3	Social Engineering.....	172
5.3.1	Schweigen ist Gold.....	172
5.3.2	Risiko soziale Netzwerke.....	173
5.3.3	Informationen nicht unbedacht herausgeben.....	173
5.4	Angriffe verhindern, erkennen, abwehren.....	173
5.4.1	Systemen nicht blind vertrauen.....	174
5.4.2	Firewalls – «konventioneller» Schutz.....	174
5.4.3	Firewall und NAT können Probleme verursachen.....	175
5.4.4	Firewalls und MZ – «erweiterter» Schutz.....	175
5.4.5	VPN «untertunneln» Firewalls.....	176
5.4.6	Firewalls müssen nicht routen!.....	177
5.4.7	Hilft Verstecken im Internet?.....	179
5.4.7.1	Privat oder öffentlich?.....	179



5.4.7.2	Netzwerkinfos lassen sich nur bedingt verstecken .....	179
5.4.7.3	Kaum noch Netze ohne NAT .....	180
5.4.7.4	IPv6? .....	181
5.4.7.5	«Security by Obscurity» – auch ohne NAT.....	181
5.4.8	ICMP als Türklingel.....	181
5.4.8.1	ICMP: Überprüfungsfunktionen .....	182
5.4.8.2	Ping ist nicht gleich ICMP! .....	182
5.4.8.3	ICMP: standardisiertes Protokoll für Netzwerksysteme .....	182
5.4.9	Checkliste: Fehlersuche mittels ICMP .....	183
5.4.10	Wer pingt denn da?.....	185
5.4.11	Reale Bedrohung durch ICMP .....	186
5.4.11.1	ICMP Redirects .....	187
5.4.11.2	ICMP Unreachable .....	187
5.4.11.3	Informationen «ausspionieren» mittels ICMP .....	188
5.4.11.4	«Überfluten» eines Systems als verbreitete ICMP-Angriffsart .....	188
5.4.11.5	Weitere Angriffsformen .....	191
5.4.11.6	Path-MTU-Discovery.....	191
5.4.12	ICMP-Angriffe abwehren.....	192
5.4.13	Also doch: Security by Obscurity?.....	193
5.4.13.1	Verzögerung statt Verhinderung.....	194
5.4.13.2	Ports scannen .....	194
5.4.14	Sind Firewalls noch zeitgemäß? .....	195
5.4.15	Sind Personal Firewalls Hexenwerk oder Lachnummer? .....	196
5.4.15.1	Personal Firewalls: Wie sinnvoll ist deren Einsatz? .....	197
5.4.15.2	Musterknaben ohne Firewalls: Mac OS X und Linux.....	198
5.4.15.3	Überwachen statt verhindern .....	198
5.4.15.4	Personal Firewalls: unnützlich und potenziell gefährlich .....	199
5.4.15.5	Sinnvoller als Personal Firewalls: Systeme aktuell halten .....	200
5.4.16	Gern übersehene Binsenweisheit: Keine Software ist frei von Fehlern! .....	202
5.4.17	Virenschutz.....	203
5.5	Angriffsszenarien: (Hinter)gründe .....	204
5.5.1	Ursprünge und Gründe für Angriffe .....	204
5.5.2	Es geht ums Geld .....	204
5.5.3	Anonyme Proxies .....	205
5.5.4	Gemeinsam sind sie stark: Botnetze.....	205
5.5.5	NAC und Firewalls bieten nur unzureichenden Schutz .....	206
5.6	«Das Reich des Guten» – Abwehr gegen Bedrohungen der IT .....	207
5.6.1	Gefahr erkannt – Gefahr gebannt? .....	207
5.6.2	Intrusion Detection .....	207
5.6.2.1	Angriffsmuster erkennen .....	207
5.6.2.2	Hostbasierte Intrusion-Detection-Systeme .....	208
5.6.2.3	Netzwerkbasierende Intrusion-Detection-Systeme.....	208
5.6.3	Verschiedene Lösungen.....	209
5.7	Snort .....	212
5.7.1	Sensoren .....	212
5.7.2	Implementierung Snort .....	213

5.7.3	Szenario: Snort im praktischen Beispiel.....	214
5.7.3.1	Anforderungen.....	214
5.7.3.2	Hardware.....	214
5.7.3.3	Open oder Closed Source?.....	214
5.7.3.4	Überlegung zur Umsetzung: Virtualisierung und Standby?.....	215
5.7.3.5	Lastenheft.....	216
5.7.3.6	Anforderungen an die Sensorik.....	216
5.7.3.7	Pflichtenheft.....	216
5.7.3.8	Eingreifen in die Verbindungen im Bedarfsfall.....	217
5.7.3.9	Bandbreitenminimierung.....	217
5.7.3.10	Anforderungen an die Sensorik.....	217
5.7.3.11	Rate-Limiting.....	217
5.7.3.12	Sicherheitskonzept Grundsystem.....	217
5.7.4	GUIs.....	218
5.7.4.1	BASE.....	218
5.7.4.2	Snorby.....	219
5.7.5	Sicherungskonzept.....	220
5.8	Paketquellen.....	221
5.9	Übersicht: über das enthaltene Regelwerk.....	222
5.9.1	Zeitplan: für die Umsetzung eines Snort-IDPS.....	223
5.10	Fazit.....	223
5.11	Wichtige Links.....	224
5.12	Literaturverzeichnis.....	224
<b>Autor</b>	.....	<b>225</b>

## 1.

# Grundlagen der IT-Sicherheit

<b>1.2</b>	<b>Bedrohung der IT-Sicherheit</b> .....	11
1.2.1	Bedrohungen durch organisatorische Fehler.....	11
1.2.1.1	Verantwortlichkeiten.....	12
1.2.1.2	Verwaltung der Betriebsmittel.....	13
1.2.1.3	Zutritt, Zugang und Zugriff.....	13
1.2.2	Bedrohungen durch das Personal.....	13
1.2.2.1	Neue Mitarbeiter.....	14
1.2.2.2	Alte Mitarbeiter und «vergessene» Accounts.....	14
1.2.2.3	Schulungen und Sensibilisierungen.....	14
1.2.2.4	Checkliste: Private Nutzung und Überwachung von E-Mail und Internet.....	15
1.2.2.5	Beispiel: Weisung zum Gebrauch von Informatikinstrumenten und zur Benutzung von elektronischen Kommunikationseinrichtungen (technische Betriebsmittel).....	16
1.2.3	Bedrohungen durch technische Mängel.....	22
1.2.3.1	Sicherheitslücken und Exploits.....	22
1.2.3.2	Malware: Verbreitung auch ohne Sicherheitslücke.....	23
1.2.4	Checkliste: Keine Gegenmassnahme ohne bekannte Bedrohung.....	24
<b>1.3</b>	<b>Risikoabschätzung und Wirtschaftlichkeitsbetrachtungen</b> .....	24
1.3.1	Entwicklung eines Risikobewusstseins.....	25
1.3.2	Risiken und Schadensfälle.....	25
1.3.2.1	Verstoss gegen Gesetze oder Vorschriften.....	26
1.3.2.2	Beeinträchtigung der persönlichen Unversehrtheit.....	27
1.3.2.3	Beeinträchtigung der Aufgabenerfüllung.....	27
1.3.2.4	Negative Aussenwirkung.....	27
1.3.2.5	Finanzielle Auswirkungen.....	28
1.3.2.6	Umgang mit dem Risiko.....	28
1.3.3	Wirtschaftlichkeitsbetrachtungen.....	29
1.3.3.1	IT-Sicherheitsrisiken und IT-Investment.....	29
1.3.3.2	Beispiel einer Kosten-Nutzen-Rechnung.....	30

<b>1.4</b>	<b>Anforderungen an die IT-Sicherheit.....</b>	<b>31</b>
1.4.1	Einflussfaktoren .....	31
1.4.2	Katalog der Anforderungen.....	33
1.4.2.1	Vertraulichkeit.....	33
1.4.2.2	Verhinderung einer Verkehrsfluss-Analyse .....	33
1.4.2.3	Erkennung der Datenunversehrtheit .....	34
1.4.2.4	Authentifizierung des Kommunikationspartners .....	34
1.4.2.5	Authentifizierung des Ursprungs der Daten .....	35
1.4.2.6	Zugangs- und Zugriffskontrolle .....	35
1.4.2.7	Urhebernachweis .....	36
1.4.2.8	Empfängernachweis.....	36
1.4.2.9	Aufrechterhaltung des Betriebs.....	36
<b>1.5</b>	<b>Aufbau eines CERT .....</b>	<b>36</b>
1.5.1	Organisation und Personal .....	37
1.5.2	Aufgaben .....	37

# 1. Grundlagen der IT-Sicherheit

Dieses Kapitel beschäftigt sich mit den grundlegenden Bedrohungen der IT-Sicherheit, die sich aus organisatorischen, personellen und technischen Problemen zusammensetzen. Für die Bewertung der Gefahren, die von diesen Problemen ausgehen, sind eine Risikoabschätzung und gegebenenfalls eine Wirtschaftlichkeitsbetrachtung von Massnahmen zur IT-Sicherheit notwendig.

Sicherheit ist ein Prozess, der sich mit einer häufig ändernden Infrastruktur sowie mit täglich neuen Sicherheitslücken auseinandersetzt. Daraus ergeben sich bestimmte Anforderungen an die Einführung und Kontrolle der IT-Sicherheit selbst und an das Krisenmanagement im Notfall.

## 1.2 Bedrohung der IT-Sicherheit

Heutige IT-Strukturen sind meist recht komplexe Gebilde. Deshalb ergeben sich zahlreiche Möglichkeiten, Systeme oder Netzwerke zu stören, zu manipulieren oder unbefugt Daten zu lesen. Die IT-Sicherheit ist immer dann bedroht, wenn durch organisatorische, personelle oder technische Fehlleistungen Risiken entstehen und dadurch im ungünstigsten Fall Probleme auftreten.

Bedrohung der IT-Sicherheit		
Organisation	Personal	Technik

Abbildung 1: Bedrohung der IT-Sicherheit

Auf die Organisationsstruktur und die Auswahl des Personals hat ein Unternehmen einen entscheidenden Einfluss, während bei technischen Fehlern oft das Gefühl von Ohnmacht und Stochern im Nebel bleibt. Vielleicht ist das ein Grund dafür, dass zur Suche nach technischen Fehlern oft teure Security-Scanner angeschafft werden, dass aber offensichtliche personelle und organisatorische Probleme nur zögerlich angegangen werden.

Die Erfahrung zeigt, dass die grössten Risiken im personellen oder organisatorischen Bereich liegen. Hier lohnt sich die Suche nach Sicherheitslücken also am meisten.

### 1.2.1 Bedrohungen durch organisatorische Fehler

Die Organisation der Arbeitsabläufe in einem Unternehmen oder einer Behörde ist oft über Jahrzehnte gewachsen. Da wird man manchmal betriebsblind gegenüber Mängeln.

## BEISPIELE



Das Rechenzentrum ist durch eine teure Anlage vor unbefugtem Zutritt gesichert. Der Zugang durch die anliegende Druckerei ist leider nicht Bestandteil der Zutrittskontrolle.

Für die Zutrittskontrolle werden Chipkarten mit drei unterschiedlichen Berechtigungsstufen vergeben. Der Pförtner teilt die Karten an externe Personen nach der «Wichtigkeit» der Gäste aus und nicht nach deren Aufgaben.

Das Papierlager für die IT-Drucker befindet sich im selben Brandschutzabschnitt wie das Rechenzentrum.

Risiken durch organisatorische Fehler können die Existenz einer Firma bedrohen, besonders in Kombination mit personellen Problemen.

Um organisatorische Risiken aufzuspüren, sind regelmässige Prüfungen aller Abläufe nötig, z.B. in Form eines Security Audits.

## 1.2.1.1 Verantwortlichkeiten

Vermutlich werden die meisten Fehler in der Organisation durch eine falsche Zuordnung von Verantwortungen zu den einzelnen Aspekten der IT-Sicherheit gemacht.

## BEISPIELE



Der Administrator eines IT-Systems kontrolliert gleichzeitig die Log-Dateien.

Der Programmierer eines Programms ist auch gleichzeitig der Tester.

Vergib die Verantwortung nach dem Motto «Teile und herrsche», sodass sich das System selbst kontrolliert. Andernfalls entstehen immer Sicherheitslücken, die nur schwer aufzudecken sind.

## PRAXISTIPP



Auf keinen Fall miteinander vereinbar sind folgende Funktionen:

- Rechteverwaltung und Revision
- Netzadministration und Revision
- Programmierung und Test bei selbst erstellter Software
- Datenerfassung und Zahlungsanordnungsbefugnis
- Revision und Zahlungsanordnungsbefugnis

### 1.2.1.2 Verwaltung der Betriebsmittel

Ein weiterer Punkt in der Organisation, wo besonders schnell Sicherheitslücken entstehen, ist die Verwaltung der Betriebsmittel. Dabei geht es weniger darum, ob ein Mitarbeiter eine Tintenpatrone oder ein paar Disketten «mitgehen» lässt, sondern vor allem um den Einsatz von Instrumenten zur Vergrößerung der Sicherheit der IT-Systeme wie:

- Firewalls
- Viren-Scanner
- Produkte zur Content-Security

Der praktische Einsatz dieser Hilfsmittel ist natürlich technischer Natur. Die Organisation hat jedoch für die Randbedingungen eines vollständigen und effektiven Gebrauchs zu sorgen, damit sich keine offenen Flanken zeigen.

### 1.2.1.3 Zutritt, Zugang und Zugriff

Diese Begriffe stehen für die Arbeit des Personals mit den IT-Ressourcen, die vielfältigen Einschränkungen unterliegen:

- Zutritt zu Räumlichkeiten
- Zugang zu IT-Systemen
- Zugriff auf Dateien, Drucker, E-Mail etc.

Die Organisation von Zutritt, Zugang und Zugriff fängt bei der Verwaltung von Schlüsseln an und hört bei der Vergabe von Dateirechten auf.

Wenn die organisatorischen Vorgaben hier kein lückenloses Gebilde ergeben, entstehen Risiken, bei denen Personen auf nicht zugelassene Ressourcen zugreifen können.

## 1.2.2 Bedrohungen durch das Personal

Grundsätzlich kommt jede Person als potenzieller Angreifer in Betracht, die Zugang zu einem IT-System hat oder sich diesen verschaffen kann:

- Berechtigte User können im Rahmen ihrer Autorisierungen zugreifen.
- Unberechtigte User sind interne oder externe Benutzer, die unter Ausnutzung von Sicherheitsmängeln IT-Systeme nutzen.
- Eigene oder externe Systemprogrammierer haben eine Vielzahl von Rechten auf den von ihnen betreuten IT-Systemen.
- Service-Technikern wird für die Zeit der Wartungstätigkeiten ebenfalls eine Vielzahl von Rechten eingeräumt.
- Operateure sorgen für den ordnungsgemässen Ablauf des Systems, fahren Backups usw. Sie arbeiten als Administratoren und haben daher alle Möglichkeiten, die ihnen das System bietet.

- Putzpersonal oder Handwerker können aufgrund ihrer Tätigkeiten in die Nähe von IT-Systemen gelangen und unter Ausnutzung von Sicherheitsmängeln zugreifen.
- Software-Hersteller haben die Möglichkeit, intelligente Manipulationen wie Trojaner, Computerviren usw. in ihre Software einzubauen.
- Hardware-Hersteller sind in der Lage, ihre Hardware so zu konzipieren, dass sie zu einem bestimmten Ereignis oder zu einer bestimmten Uhrzeit gezielt oder zerstörerisch Manipulationen im System vornimmt.

### Vollständige Überprüfung unmöglich

Besonders das Beispiel der Hersteller zeigt, dass eine Institution praktisch nicht in der Lage ist, alle am Arbeitsprozess beteiligten Personen zu überprüfen. Einzig der Teil des Personals, der sich in den eigenen Betriebsräumen aufhält, kann durch organisatorische Massnahmen daran gehindert werden, unberechtigt zuzugreifen.

#### 1.2.2.1 Neue Mitarbeiter

Die Auswahl neuer Mitarbeiter ist unter dem Aspekt der IT-Sicherheit ein ganz kritischer Punkt. Dabei kann es allerdings nicht darum gehen, ein ungerechtfertigtes Misstrauen an den Tag zu legen. Doch sollte sich jeder Abteilungsleiter genau überlegen, wann er einem als Netzwerk-Administrator eingestellten Mitarbeiter den gesamten Satz an Schlüsseln und Passwörtern zur Verfügung stellt. Beim heutigen Mangel an Fachkräften ist es eher die Regel, dass neue Administratoren häufig sofort den vollen Zugang haben, ohne zunächst eine Vertrauensbasis zu schaffen.

Ähnliche Überlegungen gelten für die Einweisung bzw. Einarbeitung neuer Mitarbeiter. Sicherheitsprobleme entstehen nicht nur durch Böswilligkeit, sondern auch durch mangelndes Know-how und Erfahrung.

#### 1.2.2.2 Alte Mitarbeiter und «vergessene» Accounts

Auch für ausscheidende Mitarbeiter müssen genaue Vorgaben existieren, was mit ihren Zugangsberechtigungen, Accounts und Daten zu geschehen hat.

#### WICHTIG

In der Hektik des Alltags wird gern vergessen, alte Accounts zu löschen und die dazugehörigen Daten an den Nachfolger bzw. die Kollegen zu verteilen. Das schafft Lücken, über die oft noch nach Jahren Zugriffe auf IT-Systeme möglich sind.



#### 1.2.2.3 Schulungen und Sensibilisierungen

Besonders im recht komplexen IT-Bereich entstehen viele Sicherheitslücken durch Unkenntnis von Mitarbeitern. Das bedeutet für die Institution, eine meist beträchtliche Summe Geldes für Schulungsmassnahmen auszugeben.



### Sicherheit geht alle an

Dabei ist es wichtig, dass nicht nur die Administratoren von IT-Systemen auf Schulungen zum Thema Sicherheit geschickt werden.

#### WICHTIG

Wenn nicht alle Mitarbeiter regelmässig auf die aktuellen Gefahren hingewiesen werden, entstehen durch Unkenntnis L cher, durch die dann vielleicht trotz aller technischen Massnahmen ein Wurm oder Trojaner ins eigene Netz schl pfen kann.



#### 1.2.2.4 Checkliste: Private Nutzung und  berwachung von E-Mail und Internet

erf�llt	Massnahme
	Nutzungs- und �berwachungsreglement erstellen; Ziel: Klarheit und Sicherheit �ber die Rechte und Pflichten des Mitarbeiters im Umgang mit E-Mail und Internet sowie Klarheit �ber die M�glichkeit der �berwachung und Sanktionen
	Reglement den Nutzern zur Kenntnis bringen; den Erhalt des Reglements quittieren lassen
	Verbot der privaten E-Mail- und Internetnutzung am Arbeitsplatz theoretisch m�glich; praktisch meist unverh�ltnism�ssig, daher massvolle Nutzung erlauben (allenfalls auf Randzeiten verlegen)
	Anonymisierte �berwachungen/Auswertungen vornehmen; personenbezogene �berwachungen und Auswertungen erst nach Feststellung des Missbrauchs durch Mitarbeiter durchf�hren
	Vor der Durchf�hrung personenbezogene �berwachungen und Auswertungen den Mitarbeitern ank�ndigen
	Verzicht auf eine st�ndige personenbezogene �berwachung (eine solche �berwachung ist widerrechtlich)
	�berwachungen sind von �bergeordneter Stelle anzuordnen und von spezialisiertem Personal vorzunehmen

## E-Mail

erfüllt	Massnahme
	Uneingeschränkter Schutz privater E-Mails, wenn als solche erkennbar (idealerweise als solche kennzeichnen bzw. in Ordner ablegen)
	Kontrolle von geschäftlichen E-Mails erlaubt (Leistungs- und Geschäftskontrolle)
	Bei Verdacht einer strafrechtlichen Handlung via E-Mail: Beweissicherung erlaubt (Abspeichern des E-Mails). Einsicht in das E-Mail ist nicht erlaubt und hat durch die Strafverfolgungsbehörden zu erfolgen
	Stellvertretungsregelungen für Abwesenheiten aufstellen
	Regelung bei Austritt aus dem Unternehmen vorsehen

### 1.2.2.5 Beispiel: Weisung zum Gebrauch von Informatikinstrumenten und zur Benutzung von elektronischen Kommunikationseinrichtungen (technische Betriebsmittel)

#### Präambel

Das Unternehmen stellt den Mitarbeitern zur Erbringung ihrer Arbeitsleistung Informatikinstrumente (insb. PC) und elektronische Kommunikationseinrichtungen (E-Mail, Internet) zur Verfügung. Nebst den vielen Vorteilen (rasche Kommunikation, einfache Informationsbeschaffung usw.) bietet die Nutzung von Computer, E-Mail und Internet während der Arbeit auch wesentliche Gefahren und Nachteile für das Unternehmen und den einzelnen Mitarbeiter: die übermässige private Nutzung von Internet und E-Mail, Ausbleiben der erwarteten Arbeitsleistung, Sicherheitsrisiken für die Informatik des Unternehmens, Internetsucht usw.

Diese Weisung soll Klarheit bezüglich der Rechte und Pflichten der Mitarbeiter im Umgang mit den zur Verfügung stehenden Informatikinstrumenten und elektronischen Kommunikationseinrichtungen liefern und aufzeigen, wie und wann das Unternehmen Kontrollen zur Einhaltung der Weisung vornimmt.

Die Vereinbarung ist in 4 Bereiche aufgeteilt:

- **Allgemeines**, insb. Grundsatz, Regelung des persönlichen Geltungsbereichs und der Verbindlichkeit (Ziff. 1).
- **Informatikinstrumente und Sicherheit im eigenen Netzwerk**, insb. die Beschaffung von Hard- und Software und der Einsatz von privaten Informatikinstrumenten, Vorgaben für das An- und Abmelden am Informatiksystem, Umgang mit Passwörtern und der Einsatz des Virenschutzes (Ziff. 2).
- **Nutzung von elektronischen Kommunikationseinrichtungen (E-Mail und Internet)**, insb. die private Nutzung sowie die Kontrolle und Überwachung des Nutzerverhaltens unter bestimmten Voraussetzungen (Ziff. 3).
- Die Sanktionierung von Verstössen (Ziff. 4).

## **1. Allgemeines**

### **1.1 Grundsatz**

Die Benutzung der Informatikinstrumente und elektronischen Kommunikationsmittel hat in direktem Zusammenhang mit der Tätigkeit des Arbeitgebers zu stehen. Sie soll dazu dienen, die unternehmerischen Ziele werkzeuggestützt und effizient zu erreichen.

Eine massvolle, gelegentliche private Benutzung dieser Betriebsmittel ist unter bestimmten, im Folgenden ausgeführten Voraussetzungen erlaubt.

### **1.2 Geltungsbereich**

Der persönliche Geltungsbereich dieser Weisung umfasst alle Arbeitnehmer des Unternehmens, auch Praktikanten, Temporär- und Aushilfspersonal.

### **1.3 Verbindlichkeit**

Diese Weisung ist für alle betroffenen Personen verbindlich. Sie räumt den Mitarbeitern Rechte und Pflichten ein, deren nicht Beachtung sanktioniert werden können.

## **2. Informatikinstrumente und Sicherheit im Unternehmensnetzwerk**

### **2.1 Informatikinstrumente des Unternehmens**

#### **Beschaffung**

Die Beschaffung von Informatikinstrumenten erfolgt zentral durch den internen Informatikdienst («IT-Abteilung»). Beschaffungen für das Unternehmen durch den Mitarbeiter sind nicht gestattet. Die Informatikinstrumente sind Eigentum des Unternehmens.

#### **Hardware**

Der jeweilige Benutzer ist für die sorgfältige Benutzung von PCs, Notebooks, Bildschirmen, Arbeitsplatzdrucker und andere Peripheriegeräten verantwortlich.

Datei- und Datenbankserver, Netzwerkkommunikationsgeräte und Netzwerk- sowie Sicherheitseinrichtungen dürfen nur von Mitarbeitern der IT-Abteilung oder von bezeichneten Dritten (externe Berater und Fachkräfte) bedient werden.

#### **2.1.1 Software**

Es gelangen nur Programme zum Einsatz, die von der IT-Abteilung getestet und freigegeben wurden und für welche das Unternehmen die entsprechenden Lizenzen erworben hat.

#### **2.1.2 Installationen**

Sowohl Hardware- wie auch Software-Installationen werden durch Mitarbeiter der IT-Abteilung vorgenommen. Dies gilt auch im Falle von Bürowechseln. Ohne Rücksprache mit der IT-Abteilung ist das Installieren von peripheren Geräten wie z.B. Drucker, Scanner, Modems untersagt.

Das Installieren und Benutzen von Fremdsoftware durch den Mitarbeiter ist untersagt.

## 2.2 Private Informatikinstrumente

Private Informatikinstrumente wie Scanner, Notebooks etc. dürfen grundsätzlich nicht im Firmennetz eingesetzt werden. Ausnahmen werden durch die IT-Abteilung bewilligt. Es besteht kein Anspruch auf finanzielle Vergütung. Auch die Versicherung solcher Geräte ist Sache des Eigentümers.

## 2.3 Private Daten auf dem Dienstcomputer

Mit im Unternehmen vorhandenen Programmen erstellte private Dateien sind ausschliesslich auf dem zu privaten Zwecken vorgesehenen Laufwerk H des Dienstcomputers zu speichern. Das Laufwerk H ist auf eine Speicherkapazität von 100 MB beschränkt.

Stösst das Unternehmen bei legitimen Kontrollen auf dem Dienstcomputer des Mitarbeiters (ausserhalb des Laufwerks H) auf Dateien, die möglicherweise privaten Charakter haben, so wird der Mitarbeiter über die Natur des Dokuments befragt. Deklariert der Arbeitnehmer die Daten sodann als privat, so hat dieser die Daten ins Laufwerk H zu verschieben. Stattdessen kann das Unternehmen diese Daten auch löschen (lassen).

## 2.4 An- und Abmelden am Informatik-System

### 2.4.1 Benutzerauthentisierung

Die Anmeldung erfolgt über eine benutzerspezifische Authentisierung. Über diese Authentisierung werden die Zugriffsberechtigungen auf die einzelnen Bereiche des Netzwerks sowie der Programme geregelt. Die Verantwortung für die dem Benutzer zugewiesenen Authentisierungsmittel (Benutzername und Passwort) trägt jeder Benutzer selbst. Sie sind persönlich, nicht übertragbar und dürfen anderen (Dritten oder Mitarbeiter) nicht zugänglich gemacht werden.

### 2.4.2 Abmeldung vom System

Wird der Arbeitsplatz für mehr als 5 Minuten verlassen, muss die Arbeitsstation vor unberechtigtem Zugriff gesichert werden. Die Dienstcomputer inkl. Bildschirme und lokale Arbeitsplatzdrucker müssen bei längerer Abwesenheit, vor allem über Nacht und am Wochenende, abgeschaltet werden.

## 2.5 Passwort

### 2.5.1 Passwortwechsel und Kreieren von Benutzerpasswörtern

Ein Passwortwechsel wird vom System alle 6 Monate verlangt. Während 4 Passwortwechseln kann dasselbe Passwort nicht erneut verwendet werden.

Passwörter dürfen nie in unmittelbarem Zusammenhang mit dem Benutzer stehen (z.B. Name des Kindes oder Partners, Geburtsdatum, Telefonnummer, Autokennzeichen). Grundsätzlich gilt, je komplexer ein Passwort ist, desto sicherer ist es.

### 2.5.2 Passwort-Sperre

Aus Sicherheitsgründen wird das Benutzer-Konto nach sechsmaliger Fehleingabe des Passworts automatisch gesperrt. Das Entsperren des Kontos wird durch die IT-Abteilung vorgenommen.

## 2.6 Virenschutz

Auf den Servern der IT-Abteilung sind alle Benutzer durch den Virenschutz des Unternehmens geschützt. Die im Netzwerk des Unternehmens gespeicherten Dokumente werden laufend geprüft. Des Weiteren befindet sich auf jeder Arbeitsstation ein lokales Virenschutzprogramm, welches automatisch und periodisch mit den neusten Virensignaturen versorgt wird. Das Virenschutzprogramm darf nie ausgeschaltet werden. Mobile Geräte, welche sporadisch ins Unternehmensnetzwerk angeschlossen werden, müssen zwingend mit einem Virenschutzprogramm mit aktualisierten Virensignaturen versehen sein.

### **3. Nutzung von elektronischen Kommunikationseinrichtungen**

#### **3.1 E-Mail**

##### **3.1.1 Generelles**

Das elektronische Mail-System des Unternehmens dient dem geschäftlichen Informations- und Datenaustausch mit internen und externen Geschäftspartnern. Die angemessene, private Benutzung ist unter den folgenden Voraussetzungen erlaubt.

##### **3.1.2 Private Benutzung**

Die massvolle, gelegentliche Nutzung der E-Mail vorname.nachname@firma.ch (Mitarbeiter-E-Mail) zu privaten Zwecken während der Arbeitszeit ist erlaubt, sofern dadurch die Arbeitsleistung und die technischen Ressourcen der IT-Abteilung nicht beeinträchtigt werden. Nicht zu privaten Zwecken benützt werden dürfen Team-E-Mail-Adressen (z.B. einkauf@firma.ch, info@firma.ch). Die Kommunikation über diese E-Mails kann von allen Mitarbeitern des jeweiligen Teams eingesehen werden.

Private E-Mails sind im Betreff als solches zu kennzeichnen (Betreff: Privat) und in einem privaten Ordner (Ordner «private Korrespondenz») abzulegen oder zu löschen.

Von allen Mailboxen auf dem Server werden nächtliche Backups erstellt. Der Benutzer hat private Mails auf einen anderen Datenträger zu speichern, wenn er diese Sicherung der privaten E-Mails nicht wünscht.

##### **3.1.3 Generell nicht erlaubt sind**

- das Verwenden der geschäftlichen E-Mail-Adresse zur Registrierung für private Dienstleistungen
- das Versenden von privaten E-Mails an den internen Mailverteiler (und damit Zustellung an alle Mitarbeiter des Unternehmens)
- das Versenden von privaten E-Mails, die grösser als 2 MB sind
- das Öffnen, Versenden und Weiterleiten von Mail-Beilagen wie z.B. ausführbare Programme (z.B. Dateierweiterungen .exe oder .vbs), Spiele, Kettenbriefe etc.
- das Versenden und Weiterleiten von Witzen, Comics, Fun-Videos und dergleichen
- das Versenden und Weiterleiten von unsittlichen und strafrechtlich relevanten Inhalten
- die Belästigung anderer Personen und Mobbing per E-Mail
- das Antworten auf Spam- oder Phishing-Mails (als Spam- oder Phishing-Mail erkennbare E-Mails sind ungeöffnet zu löschen)
- das Versenden von Geschäftsgeheimnissen an Unberechtigte

##### **3.1.4 Maximale Grösse von E-Mails inkl. Anhänge**

Die Grösse von E-Mails inklusive allfälliger Anhänge ist auf 6 MB beschränkt. Grosse Dateien sind über das Programm WinZip zu komprimieren.

##### **3.1.5 Mailarchivierung**

Gesetzliche Auflagen verpflichten das Unternehmen, geschäftsrelevante ein- und ausgehende E-Mails inkl. Anhängen während 10 Jahren aufzubewahren. Das eingesetzte Mailarchivierungs-Tool macht keinen Unterschied zwischen geschäftlichen und privaten E-Mails, d.h. es wird alles archiviert. Der Mitarbeiter erklärt sich mit dieser Archivierung einverstanden. Für das Öffnen privater E-Mails, die im Mailarchiv gespeichert sind, gilt die Regelung in Ziff. 3.3.4 und 3.3.5.

### 3.1.6 E-Mail-Account des Mitarbeiters, der das Unternehmen verlässt

Der Mitarbeiter muss alle privaten Elemente aus seinem Postfach löschen. Die geschäftlichen E-Mails, die weiterhin benötigt werden oder noch in Bearbeitung sind, hat er an seinen Stellvertreter, zuständigen Vorgesetzten oder Nachfolger weiterzuleiten oder entsprechend abzulegen. Nach dem letzten Arbeitstag des betreffenden Angestellten wird sein E-Mail-Postfach von der IT-Abteilung blockiert.

## 3.2 Internet

### 3.2.1 Nutzungsbestimmung

Das Internet dient der geschäftlichen Informationsbeschaffung für den Mitarbeiter. Die massvolle, gelegentliche Nutzung zu privaten Zwecken während der Arbeitszeit ist erlaubt, sofern dadurch die Arbeitsleistung sowie die technischen Ressourcen der IT-Abteilung nicht beeinträchtigt und die folgenden Regeln beachtet werden.

### 3.2.2 Generell nicht erlaubt sind:

- das Herunterladen und Installieren von Browser Plug-Ins und Programmen
- die Verwendung von Online-Spielen
- das Erstellen oder Verbreiten von schädlichen Programmcodes (z.B. Viren, Trojaner, Würmer)
- der Zugriff auf rassistische, pornographische, extremistische oder (andere) widerrechtliche und unsittliche Inhalte

### 3.2.3 Nicht erlaubt, falls dies nicht in geschäftlichem Auftrag erfolgt, sind:

- die Teilnahme an Börsenforen und das Online-Handeln (z.B. Aktien, Fonds, Wertpapiere, Güter) und E-Banking
- das Verschieben von Dateien über das FTP-Protokoll (File Transfer Protocol)
- die Teilnahme an Online-Auktionen und Versteigerungen (z.B. ebay)
- die Benutzung von Internet-Radiostationen oder Internet-Fernsehen
- die Benutzung von sozialen Internetplattformen, wie facebook.com, xing.com
- die Teilnahme an Newsgroups (Diskussionsforen), Blogs, Twitter

## 3.3 Aufzeichnungen und Kontrolle

### 3.3.1 Aufzeichnung des Internetverkehrs

Aus Sicherheitsgründen wird der Internetverkehr laufend von den Firewall-Servern des Unternehmen aufgezeichnet und protokolliert (Log-Files). Die Protokollierungen werden nach 7 Tagen automatisiert gelöscht. Im Rahmen der personenbezogenen Überwachung oder Strafverfolgungen werden die Protokollierungen bis zur Beendigung der Verfahren aufbewahrt.

Heruntergeladene Webseiten verbleiben im Zwischenspeicher des Browsers und des unternehmensinternen Proxy-Servers. Die Inhalte sämtlicher Zwischenspeicher werden nach 30 Tagen automatisch gelöscht. Der Mitarbeiter kann den Browserverlauf über die entsprechenden Funktionen des verwendeten Browsers jederzeit selber löschen.

### 3.3.2 Überprüfung der Log-Files

Bei Störungen und Ausfällen prüft die IT-Abteilung die nach Ziff. 3.3.1 angefallenen Daten. Die Log-Files werden dabei nicht mit einem bestimmten Computer (IP-Adresse) oder einer bestimmten User-ID (Passwort) eines Mitarbeiters verknüpft.

Besteht aufgrund der getätigten Überprüfung der Verdacht auf Missbrauch der elektronischen Kommunikationseinrichtungen, informiert die Geschäftsleitung die Informatik-Anwender, dass Missbräuche vorgekommen sind und dass die IT-Abteilung mit einer zeitlich befristeten, personenbezogenen Auswertung des Internetverhaltens der Mitarbeiter ab dem Folgetag der Information beauftragt wird.

Der Leiter der IT-Abteilung übergibt die Auswertungsergebnisse der Geschäftsleitung. Bei fehlbaren Mitarbeitenden sperrt die IT-Abteilung auf Anordnung der Geschäftsleitung den Zugang vorsorglich. Zudem werden verdächtige Informationen zur späteren Auswertung durch die Anwaltschaft oder den Richter sichergestellt.

### 3.3.3 Aufzeichnung des E-Mail-Verkehrs

Von den Mailboxen auf dem Server werden Backups erstellt (vgl. Ziff. 3.1.2). Zudem werden E-Mails (vgl. Ziff. 3.1.5) archiviert. Versandte E-Mails werden zusätzlich in der Ausgangsbox des Benutzers gespeichert.

### 3.3.4 Überprüfung von E-Mails

Das Unternehmen kann die Nutzung von Team-E-Mails (info@...ch; sales@...ch; usw.) jederzeit kontrollieren.

Bei der individualisierten Geschäfts-E-Mail (vorname.nachname@firma.ch) kann das Unternehmen (bzw. der Vorgesetzte) die geschäftlichen E-Mails des Mitarbeiters einsehen. Die Einsichtnahme dient einerseits der Geschäftskontrolle, andererseits, um bei Abwesenheiten des Mitarbeiters auf geschäftsrelevante E-Mails zugreifen zu können.

Auf als «Privat» gekennzeichnete E-Mails bzw. E-Mails, die im separaten Ordner «private Korrespondenz» abgelegt sind, darf das Unternehmen nur im Einzelfall mit vorgängiger, ausdrücklicher Zustimmung des Mitarbeiters für diesen Einzelfall zugreifen. Dasselbe gilt für E-Mails, die noch nicht im privaten Ordner abgespeichert sind, jedoch anhand des Betreffs als privat erkennbar sind.

### 3.3.5 Beweissicherung, Einsicht bei begründetem Verdacht

Falls konkrete Anhaltspunkte für eine Straftat unter Verwendung von E-Mails bestehen, hat das Unternehmen das Recht, entsprechendes Beweismaterial zu sichern. Die Geschäftsleitung beauftragt die IT-Abteilung zur Beweissicherung.

Die Geschäftsleitung kann die privaten E-Mails des Mitarbeiters einsehen, falls dies zwingend notwendig ist, um den Verdacht besser zu begründen oder zu zerstreuen. Dazu braucht das Unternehmen jedoch die vorgängige schriftliche Einwilligung des Arbeitnehmers ins Öffnen der privaten E-Mails. Für die Beweisaufnahme werden die entsprechenden staatlichen Untersuchungsbehörden beigezogen.

## 4. Sanktionen

Eine weisungswidrige Benutzung der Informatikinstrumente und elektronischen Kommunikationseinrichtungen können arbeitsrechtliche Sanktionen bis hin zur fristlosen Entlassung sowie strafrechtliche Untersuchungen zur Folge haben.

Die Geschäftsleitung kann insbesondere folgende Sanktionen erheben:

- Verwarnung gegen die fehlbaren Personen
- Schadenersatzforderungen
- Einreichung einer Strafanzeige
- (fristlose) Kündigung oder Freistellung

Die fristlose Kündigung kann ausgesprochen werden, wenn dem Arbeitgeber nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann. Das ist z.B. bei schwerwiegenden Fällen, wie bei wiederholtem Missbrauch trotz Verwarnung oder bei verhärtetem Verdacht auf Begehen einer Straftat der Fall.

## 5. Verpflichtung/Unterschrift

Der Mitarbeiter bestätigt per Unterschrift den Erhalt dieser Weisung, anerkennt die darin enthaltenen Bestimmungen und verpflichtet sich zu deren Einhaltung. Der Mitarbeiter akzeptiert er ausdrücklich, dass alle (auch privaten) E-Mails archiviert werden.

[Ort], Datum

Name, Vorname (Blockschrift)

Unterschrift

### 1.2.3 Bedrohungen durch technische Mängel

Die durch den technischen Zustand von Hard- und Software entstehenden Risiken lassen sich in mehrere Kategorien einteilen. Bei der Hardware hängt es oft vom Alter der Systeme und den regelmässigen Wartungsintervallen ab, ob Probleme entstehen können oder nicht. Schlechter in den Griff zu bekommen sind Bedrohungen, auf die das Unternehmen bzw. die Behörde gar keinen Einfluss hat:

- Die eingesetzte Software enthält Programmierfehler in Form von Sicherheitslücken, über die ein gezielter Angriff möglich ist. Die dazugehörigen Angriffsprogramme werden auch als «Exploit» bezeichnet.
- Von aussen kommt Software in das eigene Netzwerk, die den Angriff enthält. Viren, Würmer und Trojanische Pferde gehören zu dieser Kategorie, die oft vereinfachend als «Malware» bezeichnet wird.

Eine Sicherheitslücke wird im täglichen Gebrauch oft auch als «Vulnerability» bezeichnet.

#### 1.2.3.1 Sicherheitslücken und Exploits

Die vielen bisher bekannt gewordenen Angriffe unter Ausnutzung von Sicherheitslücken können wie folgt eingeteilt werden: