Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 174
D-50735 Köln
Telefon: (0221) 77 66 0; E-Mail: verlag@vds.de

Copyright by VdS Schadenverhütung GmbH. Alle Rechte vorbehalten.

VdS-Richtlinien für die Informationsverarbeitung

Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Um eine Beeinträchtigung des Textverständnisses zu vermeiden, verwendet VdS Schadenverhütung durchweg das generische Maskulinum. Eine Bevorzugung oder anderweitige Wertung des männlichen, weiblichen oder sonstigen Geschlechts geht damit ausdrücklich nicht einher.

INHALT

1 Allgemeines ... 7
1.1 Einleitung ... 7
1.2 Anwendungshinweise ... 7
1.3 Anwendungs- und Geltungsbereich ... 7
1.4 Gültigkeit ... 8
2 Normative Verweisungen ... 8
3 Begriffe und Abkürzungen ... 8
3.1 Begriffe ... 9
3.2 Abkürzungen ... 14
4 Organisation der Informationssicherheit ... 14
4.1 Grundlagen ... 14
4.2 Verantwortlichkeiten ... 15
4.2.1 Anforderungen ... 15
4.2.2 Zuweisung und Dokumentation ... 15
4.2.3 Funktionstrennungen ... 15
4.2.4 Zeitliche Ressourcen ... 15
4.2.5 Delegieren von Aufgaben ... 15
4.3 Topmanagement ... 16
4.4 Informationssicherheitsbeauftragter ... 16
4.5 Informationssicherheitsteam ... 16
4.6 IT-Verantwortliche ... 17
4.7 Administratoren ... 17
4.8 Vorgesetzte ... 17

4.9 Mitarbeiter ... 17
4.10 Projektverantwortliche ... 17
4.11 Externe Personen ... 17
5 Leitlinie zur Informationssicherheit (IS-Leitlinie) ... 18
5.1 Grundlagen ... 18
5.2 Allgemeine Anforderungen ... 18
5.3 Inhalte ... 18
6 Richtlinien zur Informationssicherheit (IS-Richtlinien) ... 18
6.1 Grundlagen ... 18
6.2 Allgemeine Anforderungen ... 18
6.3 Inhalte ... 19
6.4 Aufbau und Funktionsweise des ISMS ... 19
6.5 Regelungen für Nutzer ... 19
6.6 Weitere Richtlinien ... 20
7 Mitarbeiter ... 20
7.1 Grundlagen ... 20
7.2 Vor Aufnahme der Tätigkeit ... 21
7.3 Aufnahme der Tätigkeit ... 21
7.4 Beendigung oder Wechsel der Tätigkeit ... 21
8 Wissen ... 21
8.1 Grundlagen ... 21
8.2 Aktualität des Wissens ... 21
8.3 Schulung und Sensibilisierung ... 22
9 Identifizieren kritischer IT-Ressourcen ... 22
9.1 Grundlagen ... 22
9.2 Prozesse ... 23
9.3 Kritische Informationen ... 23
9.4 Kritische IT-Ressourcen ... 24
10 IT-Systeme ... 24
10.1 Grundlagen ... 24
10.2 Inventarisierung ... 24
10.3 Lebenszyklus ... 25
10.3.1 Beschreibung ... 25
10.3.2 Inbetriebnahme und Änderung ... 25
10.3.3 Ausmusterung und Wiederverwendung ... 25
10.4 Basisschutz ... 25
10.4.1 Funktionalitäten und Maßnahmen ... 25
10.4.2 Software ... 26
10.4.3 Beschränkung des Netzwerkverkehrs ... 26
10.4.4 Protokollierung ... 26
10.4.5 Externe Schnittstellen und Laufwerke ... 27
10.4.6 Schadsoftware ... 27
10.4.7 Starten von fremden Medien ... 27
10.4.8 Authentifizierung ... 27
10.4.9 Zugänge und Zugriffe ... 28
10.5 Zusätzliche Maßnahmen für mobile IT-Systeme ... 28
10.5.1 Grundlagen ... 28
10.5.2 IS-Richtlinie ... 28
10.5.3 Schutz der Informationen ... 28
10.5.4 Verlust ... 29

10.6 Zusätzliche Maßnahmen für kritische IT-Systeme ... 29
10.6.1 Grundlagen ... 29
10.6.2 Risikomanagement ... 29
10.6.3 Notbetriebsniveau ... 29
10.6.4 Robustheit ... 29
10.6.5 Externe Schnittstellen und Laufwerke ... 29
10.6.6 Änderungsmanagement ... 30
10.6.7 Dokumentation ... 30
10.6.8 Datensicherung ... 30
10.6.9 Überwachung ... 30
10.6.10 Ersatzsysteme und -verfahren ... 30
10.6.11 Kritische Individualsoftware ... 31
11 Netzwerke und Verbindungen ... 31
11.1 Grundlagen ... 31
11.2 Netzwerkplan ... 31
11.3 Aktive Netzwerkkomponenten ... 31
11.4 Netzübergänge ... 31
11.5 Basisschutz ... 32
11.5.1 Grundanforderungen ... 32
11.5.2 Netzwerkanschlüsse ... 32
11.5.3 Segmentierung ... 32
11.5.4 Fernzugang ... 32
11.5.5 Netzwerkkopplung ... 33
11.6 Zusätzliche Maßnahmen für kritische Verbindungen ... 33
12 Mobile Datenträger ... 33
12.1 Grundlagen ... 33
12.2 IS-Richtlinie ... 33
12.3 Schutz der Informationen ... 33
12.4 Zusätzliche Maßnahmen für kritische mobile Datenträger ... 34
13 Umgebung ... 34
13.1 Grundlagen ... 34
13.2 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen ... 34
13.3 Datenleitungen ... 34
13.4 Zusätzliche Maßnahmen für kritische IT-Systeme ... 34
14 IT-Outsourcing und Cloud Computing ... 35
14.1 Grundlagen ... 35
14.2 IS-Richtlinie ... 35
14.3 Vorbereitung ... 35
14.4 Vertragsgestaltung ... 35
14.5 Zusätzliche Maßnahmen für kritische IT-Ressourcen ... 36
15 Zugänge, Zugriffs- und Zutrittsrechte ... 37
15.1 Grundlagen ... 37
15.2 Verwaltung ... 37
15.3 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen ... 37

16 Datensicherung 37
16.1 Grundlagen 37
16.2 IS-Richtlinie 38
16.3 Verfahren 38
16.4 Weiterentwicklung 39
16.5 Basisschutz 39
16.5.1 Basisschutz-Maßnahmen 39
16.5.2 IT-Systeme für die Datensicherung und -wiederherstellung 39
16.5.3 Speicherorte 39
16.5.4 Server 39
16.5.5 Aktive Netzwerkkomponenten 39
16.5.6 Mobile IT-Systeme 40
16.6 Zusätzliche Maßnahmen für kritische IT-Systeme 40
16.6.1 Datensicherung 40
16.6.2 Risikoanalyse 40
16.6.3 Verfahren 40
17 Sicherheitsvorfälle 40
17.1 Vorbereitung auf Sicherheitsvorfälle 40
17.2 IS-Richtlinie 40
17.3 Erkennen 41
17.4 Reaktion 41
17.5 Zusätzliche Maßnahmen für kritische IT-Systeme 42
17.5.1 Anforderungen 42
17.5.2 Wiederanlaufpläne 42
17.5.3 Abhängigkeiten 42
Anhang A Verfahren und Risikomanagement 43
A.1 Verfahren 43
A.2 Risikomanagement 43
A.2.1 Definitionen und Analysen 43
A.2.2 Methodik 43
A.2.3 Risikoidentifikation 44
A.2.4 Risikoanalyse 44
A.2.5 Risikobehandlung 44
A.2.6 Wiederholung und Anpassung 44
Anhang B Änderungen zur Vorversion 45