Ein ITQ-Produkt

Basisprüfung ITQ

Geprüfte Infrastruktur -Anforderung Mittelstand

Basis ITQ-Kriterienkatalog ITQ13 v05

Geprüftes Unternehmen

Schuber + Söhne Fertigungs GmbH

Inhalt

Audit Facts 6
Vorwort 7
Disclaimer 8
Einleitung 9
- Ziel der Prüfung 9
- Informationssicherheitsmanagement 9

Prüfungsumgebung 10
Management Summary 11
- Übersicht der durchgeführten Arbeiten 11
- Genutzte Auditierungsmethoden 11
- Nächste Schritte und Entscheidungshilfen 12
- Erfüllungsgrad Basisprüfung ITQ 13

Risikobewertung gesamt 14
Fazit 15
Maßnahmenempfehlungen 16
Prüfgruppen und Prüfpunkte 19
- 1. IT-Sicherheitsmanagement 19
  - 1.1 Sicherheitsleitlinie 19
  - 1.2 Sicherheitskonzept 20
  - 1.3 Rechtliche Vorgaben 20
  - 1.4 Sicherheitsbeauftragter 20
  - 1.5 Datenschutzbeauftragter 20
  - 1.6 Datenschutzkonzept 21
  - 1.7 Schutzbedarf 21
  - 1.8 Routineaufgaben 21
  - 1.9 Verwaltung von ungenutzten Zugängen 22
  - 1.10 Stellvertretung 22
  - 1.11 Umgang mit Passwörtern 23
  - 1.12 Mitarbeiter-Eintritt und -Austritt 23
  - 1.13 Security Awareness 23
  - 1.14 Aufbewahrung von Informationen 24
  - 1.15 Richtlinie zur IT-Nutzung 24
  - 1.16 Mitnahme von IT-Komponenten 25
  - 1.17 Richtlinie zum Informationsaustausch 25
  - 1.18 Revision 25
- 2. Schutz vor Schadprogrammen 27
  - 2.1 Virenschutz auf dem Internet Gateway 27
  - 2.2 Virenschutzprogramme 28

2.3 Regelmäßige Untersuchung auf Viren 28
2.4 Virenschutz auf dem E-Mail-Server 29
2.5 Gefahren durch HTML-Inhalte und Anhänge 29
2.6 Automatische Warnungen bei Vireninfektion 29
2.7 Verhalten bei Virenbefall 29
2.8 Statusprüfung der Virenschutzprogramme 30
2.9 Aktualität der Signaturen 30
3. Sicherheit von IT-Systemen 31
3.1 Umgang mit Standardpasswörtern 31
3.2 Rechte- und Rollenkonzept 31
3.3 Vergabe sowie Entzug von Zugangsberechtigungen 32
3.4 Bedarfsgerechte Zugriffe 32
3.5 Getrennte Administratorenprofile 33
3.6 Personen mit Administratorrechten 33
3.7 Sicherheitsrichtlinie für Server 33
3.8 BIOS-Einstellungen 34
3.9 Nicht benötige Software 34
3.10 Systemdokumentationen 35
3.11 Monitoring 35
3.12 Wartungs- und Garantieverträge 35
3.13 Zugriff auf Wechselmedien 36
4. Vernetzung und Internetanbindung 37
4.1 Externe Netzzugänge 37
4.2 Konfiguration Sicherheits-Gateway 38
4.3 Personal Firewall auf Notebooks 38
4.4 Penetrationstests und Schwachstellenanalyse 39
4.5 Sicherheitseinstellungen Browser 39
4.6 Beschriftung der Netzwerkkomponenten 40
4.7 Dokumentation der Verkabelung 40
4.8 Betrieb von Routern und Switches 40
4.9 Sicherheit der WWW-Server 41
5. VPN & WLAN 42
5.1 Zugriffe via VPN-Verbindungen 42
5.2 Internetzugriffe via VPN-Client 43
5.3 Kryptografische Verfahren 43
5.4 Sicherheit der VPN-Installation 44
5.5 VPN-Dokumentation 44
5.6 WLAN-Sicherheitsrichtlinie 44
5.7 Schutz von WLAN-Verbindungen 45
5.8 Trennung von LAN und WLAN 45
5.9 Hotspot zur LAN-Verbindung 46
5.10 Updates für WLAN-Komponenten 46
6. Inhaltssicherheit 47
6.1 Filterung von Web-Inhalten 47

6.2 Schutz gegen unerwünschte E-Mails 48
6.3 Richtlinie zur E-Mailnutzung 48
7. Beachtung von Sicherheitserfordernissen 49
7.1 Herausgabe von Datenträgern 49
7.2 Sicherheitsregeln bei Wartungsarbeiten 50
7.3 Datenlöschung 50
7.4 Umgang mit Zugängen bei Wartungen 51
7.5 Datenträgerlöschung 51
7.6 Außerbetriebnahme von IT-Systemen 52
7.7 Freigabeprozess für Software 52
7.8 Identifikation bei Fernwartung 52
8. Software- und Systemaktualität 54
8.1 Patch Management-Strategie 54
8.2 Patch-Status der Server 55
8.3 Patch-Status der Clients 55
8.4 Patch-Status sonstige Netzwerkkomponenten 55
8.5 Bekanntgabe von Patch-Terminen 56
8.6 Testverfahren Patches und Updates 56
8.7 Roll Back Patches und Updates 56
9. Passwörter und Verschlüsselung 57
9.1 Übertragung von vertraulichen Informationen 57
9.2 E-Mail-Verschlüsselung 57
9.3 Passwortschutz 58
9.4 Richtlinien und Komplexitätsanforderungen 58
9.5 Passwortwechsel 58
9.6 Bildschirmsperre 58
10. Notfallvorsorge 59
10.1 Notfallmanagemenstrategie 59
10.2 Identifizierung kritischer Geschäftsprozesse 60
10.3 Notfallpläne 60
10.4 Behandelte Notfallsituationen 60
10.5 Zugriff auf die Notfalldokumentation 61
10.6 Notfälle testen 61
11. Datensicherung 62
11.1 Datensicherungskonzept 62
11.2 Abgleich mit den Verfügbarkeitsanforderungen 62
11.3 Kontrolle 63
11.4 Bestandsverzeichnis 63
11.5 Sicherung tragbarer Computer 63
11.6 Datenrücksicherungstests 64
11.7 Dokumentation der Sicherungs- und Rücksicherungsverfahren 64
11.8 Schutz der Datensicherungsmedien 64
12. Infrastruktursicherheit 65

12.1 Physischer Schutz der IT-Systeme 65
12.2 Einbruchschutz 65
12.3 Handfeuerlöscher 66
12.4 Wasserleitungen 66
12.5 USV 66
12.6 Rauchmelder 67
12.7 Zutritts- und Aufsichtsregelung 67
12.8 Umgang mit Arbeitsunterlagen 67
12.9 Software- und Hardware-Inventar 68
12.10 Lizenzkontrolle 68
13. Mobile Endgeräte 69
13.1 Sicherheitskonzept für mobile Endgeräte 69
13.2 Management von mobilen Endgeräten 69
13.3 MDM Software 70
13.4 Datenübertragung 70
13.5 Zugriff auf das interne Netz 71
13.6 Trennung von privaten und geschäftlichen Daten 71
14. Nutzung externer IT-Leistungen 72
14.1 Übersicht der externen IT-Leistungen 72
14.2 Vertragliche Grundlage 72
14.3 Richtlinien und Vorgaben 73
15. Externes Arbeiten 74
15.1 Richtlinie zum externen Arbeiten 74
15.2 Häuslicher Arbeitsplatz 74
15.3 Sicherstellung der Administration 75
16. Cloud 76
16.1 Cloud-Inventar 76
16.2 Datenhoheit 76
16.3 Rechtskonformität 77
16.4 Richtlinie zur Cloud-Nutzung 77
16.5 Anforderungsprofil 78
16.6 Redundanzen 78
16.7 Multi-Faktor-Authentifizierung 78
Anhänge 79
Firmenprofile und Kontakt 80
Übergabebestätigung 81
Risiko-Matrix 82

Audit Facts

Geprüftes Unternehmen	Schuber + Söhne Fertigungs GmbH
Ansprechpartner	Max Muster / mm@mm.de / 00000012347
Prüfzeitraum	13.03.2023 - 14.03.2023
Berichtsnummer	B387.516
ITQ-Partner	ITQ GmbH
Auditor	Jutta Brunn
Auditor-Kennung	A484.134
Verteiler	Wirtschaftsprüfer, Prüfer
Audit-Typ	Ist-Analyse
Prüforte	Schuber + Söhne Fertigungs GmbH Poststraße 1 12345 Posthausen

Vorwort

Herzlichen Glückwunsch!

Sie sind den ersten wichtigen Schritt gegangen, um den Standard der Informationssicherheit in Ihrem Unternehmen erheblich zu verbessern und Ihre wichtigsten Unternehmenswerte sowie Geschäftsprozesse zu schützen. Sie haben bestätigt, dass ein Sicherheitsprozess initiiert wurde und können dies mit dem „Gütesiegel Basisprüfung ITQ“ nachweisen.

Im weiteren Verlauf des Prüfberichtes werden wir Ihnen aufzeigen, was die nächsten Schritte sind und welche Empfehlungen wir aussprechen bezüglich der Vorgehensweise. Auf Wunsch stehen wir Ihnen während des gesamten Verfahrens prozessbegleitend zur Seite.

Auf eine gute Zusammenarbeit!

Disclaimer

Die ITQ hat ein allgemeines Anforderungsprofil mit Voraussetzungen erstellt, die für den sicheren IT-Betrieb erforderlich sind. Wir weisen ausdrücklich darauf hin, dass auf Grund besonderer Umstände und individueller Eigenschaften Ihres Unternehmens, eventuell weitere Anforderungen gestellt werden müssten, um ein angemessenen Sicherheitsniveau zu erreichen.

Grundlage der Ermittlung, inwieweit Anforderungen erfüllt sind oder nicht vorliegen, sind neben persönlichen Gesprächen, auch übersendete Unterlagen. Die Vollständigkeit und Richtigkeit von Aussagen bzw. Unterlagen kann von uns nicht überprüft werden. Insofern können wir keine Haftung für die ganzheitliche Vollständigkeit oder Richtigkeit des Berichtes bzw. der Maßnahmenempfehlungen übernehmen.

Einleitung

Ziel der Prüfung

Die Basisprüfung ITQ wurde von Experten mit jahrelanger Erfahrung auf dem Gebiet der Informationssicherheit entwickelt. Es wurde ein allgemeines Anforderungsprofil für kleine und mittlere Unternehmen erstellt, dass speziell auf deren Bedürfnisse zugeschnitten ist. Auf Basis dieses Anforderungsprofils wurden die maßgeblichen informationssicherheitsrelevanten Voraussetzungen herausgearbeitet und ein individueller Prüfungskatalog für mittelständische Unternehmen erstellt.

Ziel der Prüfung ist es einen einfachen Einstieg in die Informationssicherheit zu ermöglichen und ein angemessenes Sicherheitsniveau für Ihren Betrieb zu schaffen, auf dessen Basis der sichere IT-Betrieb gewährleistet ist.

Informationssicherheitsmanagement

Informationssicherheit ist keine einmalige Aufgabe, sondern muss als Prozess verstanden werden, indem kontinuierlich an der Verbesserung, Aufrechterhaltung und Kontrolle der Sicherheitsmaßnahmen gearbeitet wird.

Um dieser Aufgabe fachgerecht nachkommen zu können, bieten wir an, binnen eines Zeitraumes von 12 Monaten nach der Basisprüfung, einen Folgebericht zu erstellen. Diese Anschlussprüfung stellt nicht nur das vorherige Prüfungsergebnis dem aktuellen Resultat der Informationssicherheit gegenüber, sondern ist auch ein Kontrollwerkzeug, ob eingeleitete Maßnahmen greifen oder neue Risiken entstanden sind.

Betreiben Sie erfolgreich ein Informationssicherheitsmanagementsystem und wurde der überwiegende Teil der ITQ-Anforderungen erfüllt, kann und sollte im nächsten Schritt eine Zertifizierung angestrebt werden.

Nähere Informationen finden Sie unter dem Link: www.itq-institut.de

Prüfungsumgebung

Das Unternehmen wird an einem Hauptstandort in Posthausen betrieben Daneben gibt es einige kleinere Nebenbüros mit bis zu 10 Mitarbeitern, die ebenfalls von der IT-Abteilung verwaltet werden. Insgesamt beschäftigt das Unternehmen 100 Mitarbeiter.

Die technische Infrastruktur besteht im Wesentlichen aus 6 physikalischen Server, 100 virtuellen Maschinen und weiteren Netzwerkkomponenten, wie Switches, Firewalls, etc.

Zudem wird die Cloud genutzt für das ERP-System und M365-Produkte. Der Webserver wird aktuell gehostet über den Provider MS Azure.

Management Summary

Übersicht der durchgeführten Arbeiten

Im Rahmen der Basisprüfung ITQ wurde durch unterschiedliche Auditmethoden, in der Prüfungsumgebung aus „Audits Facts“, **der aktuelle Stand der Informationssicherheit** ermittelt.

Maßstab für die Bestimmung des Sicherheitsniveaus ist ein Anforderungskatalog, der von der ITQ für kleine und mittlere Unternehmen entwickelt wurde und insgesamt 126 Fragen umfasst, die 16 unterschiedlichen Prüfgruppen zugeordnet wurden. Die jeweiligen Ergebnisse der Prüffragen können dem Diagramm **„Erfüllungsgrad“** entnommen werden.

Es wurde für alle festgestellten Mängel oder Sicherheitslücken eine Liste mit **Maßnahmenempfehlungen** erstellt, nach deren Erledigung eine Risikobeseitigung oder -reduzierung auf einen angemessenen Grad sichergestellt ist. Der Empfehlungskatalog priorisiert zwar einzelne Maßnahmen, wenn der geprüfte Bereich ein erhöhtes Risiko für die Informationssicherheit ausweist, gleichwohl sollte die Reihenfolge nicht als verbindlich betrachtet werden.

Eine detaillierte Übersicht der **Prüfungsergebnisse zu den einzelnen Fragen** kann dem beigefügten Bericht entnommen werden. Inhaltlich werden der ermittelte IST-Zustand sowie die Folgen der Nichterfüllung beschrieben. Die ITQ hat zudem nach eigenem Ermessen eine erste **Risikoabschätzung** vorgenommen und das Ergebnis als Orientierungshilfe zu Verfügung gestellt.

Abschließend wird in einem **Fazit** eine Gesamtbewertung der unternehmerischen IT Infrastruktur vorgenommen und der Stand der Informationssicherheit auf Basis des Erfüllungsgrades bewertet.

Genutzte Auditierungsmethoden

Dokumentationsprüfung	Aktivitätsanalyse	Messdatenanalyse
Ansichtsnahme	**Befragung**	**Unterlagensichtung**

Nächste Schritte und Entscheidungshilfen

Die Maßnahmenempfehlung ist als erster unverbindlicher Umsetzungsplan zu verstehen und soll einen Überblick verschaffen, welche Aufgaben es zu erfüllen gilt.

Zunächst sollte eine Einteilung in technische und organisatorische Maßnahmen erfolgen, um eine Zuweisung zu den jeweiligen Fachbereichen zu erleichtern.

Im nächsten Schritt ist der jeweilige personelle, finanzielle und organisatorische Ressourcenaufwand zu bestimmen und die Reihenfolge der Umsetzung festzulegen, wobei wir folgende Empfehlungen und Hinweise geben möchten:

Nächste Schritte und Entscheidungshilfen

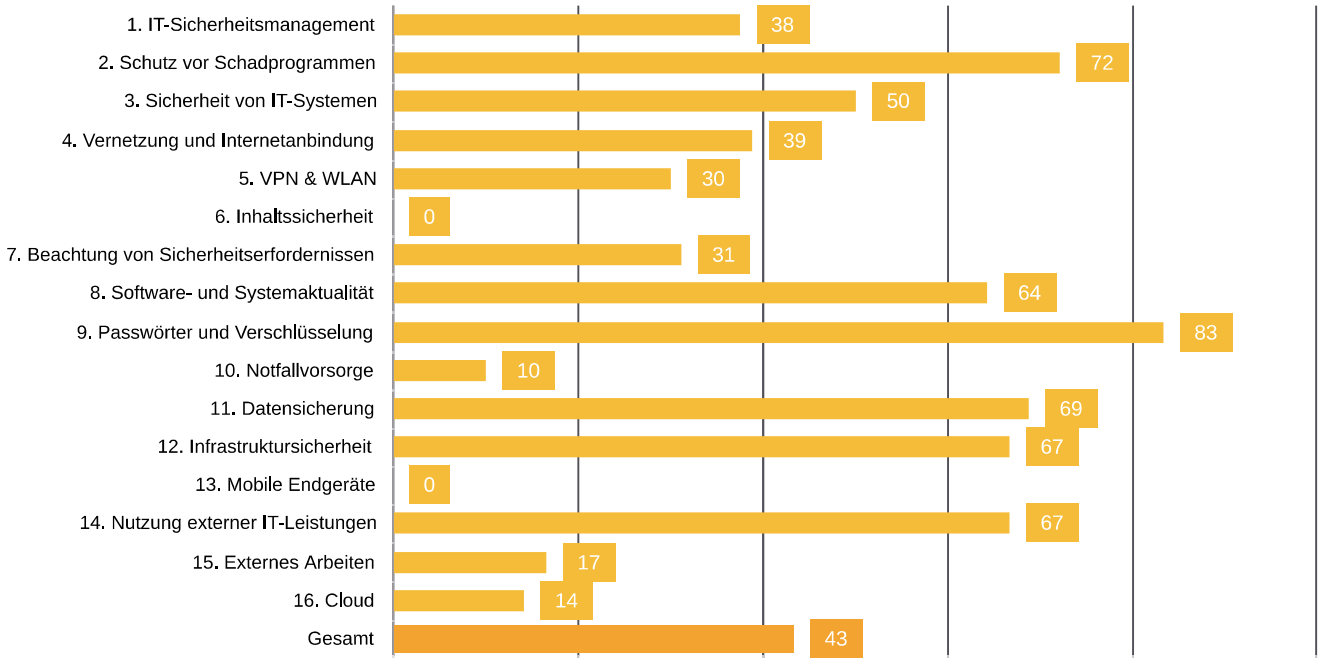
- ✓ Maßnahmen mit Flächenwirkung, d.h. es werden gleichzeitig mehrere Anforderungen erfüllt
- ✓ Maßnahmen, die ein hohes Risiko abstellen
- ✓ Maßnahmen im organisatorischen Bereich sind kurzfristig und günstig zu erledigen
- ✓ Maßnahmen für Bereiche mit auffallend vielen Mängeln
- ✓ Maßnahmen, die zur Erfüllung einer anderen erforderlich sind

Bei der Budgetierung sollte beachtet werden, dass Informationssicherheit als Prozess zu verstehen ist und Maßnahmen mitunter kontinuierlich wiederholt werden müssen.
Statistisch gesehen wird jeder zweite Sicherheitsvorfall durch einen eigenen Mitarbeiter verursacht, sei es durch Fahrlässigkeit oder mangelndes Problembewusstsein. Wir empfehlen daher insbesondere Schulungen und Sensibilisierungsmaßnahmen einzuleiten, um somit einen wichtigen Punkt auf der Liste kostengünstig abzuhaken.

Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung!

Erfüllungsgrad Basisprüfung ITQ

Nachfolgend erhalten Sie eine grafische Übersicht der geprüften Unternehmensbereiche, unterteilt in Prüfgruppen. Der Erfüllungsgrad wird in Prozent angegeben, **100% entsprechen einer vollständigen Erfüllung** der jeweiligen Prüfgruppe.



Risikobewertung gesamt

Bitte beachten Sie:
Bei der Risikobewertung handelt es sich um eine vom ITQ-Gremium erstellte Ermessensentscheidung. Grundlage der Bewertung ist die „Risiko-Matrix“, die Sie unter „Anhänge“ in diesem Dokument finden können. Selbstverständlich können Sie Risiken nach eigenem unternehmerischem Ermessen neu bewerten und zu einer anderen Entscheidung kommen, indem die individuellen Umstände des Betriebes berücksichtigt werden.

6798

Wurde im Rahmen der Basisprüfung ITQ mindestens ein Problem mit sehr hohem Risikograd festgestellt, fällt die Risikobewertung in ihrer Gesamtheit „sehr hoch“ aus. Probleme mit hohem Risikograd sollten unternehmensseitig bei der Umsetzung besonders berücksichtigt und die korrespondierenden Maßnahmen vorrangig umgesetzt werden.

Fazit

Das Unternehmen erreicht insgesamt einen leicht unterdurchschnittlichen Erfüllungsgrad von65% der gestellten Anforderungen aus der Basisprüfung ITQ.

Klare Defizite konnten in der Dokumentation von Arbeitsprozessen, Sicherheitsrichtlinien und Handlungsanweisungen für den Umgang mit IT-Komponenten festgestellt werden. Entweder existieren keine oder es liegen lediglich veraltete Unterlagen vor. Daneben sind einzelne Verantwortlichkeiten nicht klar definiert und werden von den Mitarbeitern nach eigenem Ermessen wahrgenommen. Es wurde nicht schriftlich definiert, welche Anforderungen an den Schutz einzelner IT-Systeme, Informationen und Geschäftsprozesse gestellt werden. Eine solche Schutzbedarfsanalyse ist eine grundlegende Basis, um Entscheidungen für Schutzmaßnahmen zu treffen und den Umfang bestimmen zu können. Mitarbeiterschulungen zur Sensibilisierung, zum Thema Informationssicherheit, finden nicht statt, insbesondere die Gefahren in Zusammenhang mit der E-Mailnutzung sollten ausführlich geschult werden.

Um einen umfassenden Schutz vor Schadprogrammen gewährleistet zu können, müssen Mitarbeiter geschult werden, was zu tun ist, wenn ein Verdacht und ein tatsächlicher Virenbefall vorliegen, speziell welche Sofortmaßnahmen zu ergreifen sind. Zudem sind die mobilen Endgeräte nicht hinreichend geschützt.
Verbesserungswürdig ist zudem das Patchmanagement, indem bislang keine Vorgaben definiert wurden, wann welche Komponenten zu aktualisieren sind. Zudem ist der Status einiger Server und der Clients veraltet, wodurch Sicherheitslücken entstanden sind.
Im Bereich des Notfallmanagements wurden bislang überhaupt keine Maßnahmen getroffen und es sind weder ein Notfallhandbuch vorhanden noch entsprechende Notfallpläne, sodass es beim Eintritt eines Notfalles zu erheblichen Verzögerungen kommen kann, bis dieser behoben wurde.

Im Datensicherungsmanagement fehlt es an einer klaren Definition der Geschäftsleitung, in welchen Intervallen Daten gesichert werden müssen. Ferner sollten Datenrücksicherungstests und Kontrollen der Datensicherung durchgeführt werden.

Auf Grund der Verlagerung vieler Arbeitsplätze in den externen Bereich, müssten Regelungen getroffen werden, die ein sicheres Arbeiten außerhalb des Unternehmens definieren und dem Arbeitgeber zudem ein Kontrollrecht einräumt, die Konformität der Heimarbeitsplätze prüfen zu können.

Es sollte dringend ein Cloud-Konzept für die bevorstehende Nutzung erarbeitet werden, da hier ganz wesentliche Punkte noch nicht berücksichtigt wurden.

Eine datenschutzkonforme Löschung der ausrangierten IT-Systeme und Festplatten ist bislang nicht gewährleistet, da Daten bislang lediglich manuell gelöscht und damit wiederherstellbar sind.

Maßnahmenempfehlungen

Die Maßnahmenempfehlungen sind - unabhängig ihrer Zugehörigkeit zu Prüfpunkten und Prüfgruppen - gemäß des Risikogrades des jeweiligen Problems aufgelistet, wobei innerhalb des Risikogrades keine weitere Sortierung stattfindet. Die Liste ist als erster Umsetzungsplan zu betrachten, kann jedoch auch individuell an das Unternehmen angepasst werden.

Probleme mit **hohem Risikograd** sind rot gekennzeichnet.
Probleme mit **mittlerem Risikograd** orange.
Probleme ohne Farbkodierung weisen einen **niedrigeren Risikograd** auf.

Kennung	Bezeichnung	Prüfpunkt
A07	Durchführen einer Schutzbedarfsanalyse	1.7
A11	Passworthinterlegung regeln	1.11
A13	Regelmäßige Mitarbeiterschulungen durchführen	1.13
A15	Verfassen einer Richtlinie zur IT-Nutzung	1.15
A16	Verfassen einer Richtlinie zur Mitnahme von IT-Komponenten	1.16
A17	Erstellen einer Richtlinie zum Informationsaustausch	1.17
B02	Inbetriebnahme eines zentral verwalteten Antivirussystems	2.2

O02	Sicherheitskonforme Arbeitsplätze schaffen	15.2
O03	Fernverwaltung sicherstellen	15.3
P02	Verschlüsselung von Daten in der Cloud	16.2
P04	Richtlinie zur Cloud-Nutzung	16.4
P07	Multi-Faktor-Authentifizierung einführen	16.7

Kennung	**Bezeichnung**	**Prüfpunkt**
A06	Erstellen eines Datenschutzkonzeptes	1.6
A09	Zeitnahe Deaktivierung inaktiver Benutzerkonten	1.9
A10	Stellvertretungsregelungen definieren	1.10
A12	Ein- und Austrittsprozess von Mitarbeiter	1.12
A14	Bereitstellen von verschließbaren Behältnissen	1.14

J06	Einführung von Notfalltests	10.6
K05	Datensicherungsverfahren erweitern	11.5
K07	Dokumentation des Sicherungsverfahrens	11.7
L08	Umgang mit Arbeitsunterlagen regeln	12.8
L10	Lizenzmanagement	12.10
M02	Verantwortungen für mobile Endgeräte definieren	13.2
M03	Mobile Device Management einführen	13.3
M06	Trennung von privaten und geschäftlichen Daten	13.6
N02	Verträge für IT-Dienstleistungen	14.2
N03	Anforderungsprofil für externe Dienstleister	14.3
O01	Erstellen einer Richtlinie zum externen Arbeiten	15.1
P01	Erstellen einer White List für Cloud-Dienste	16.1
P03	Rechtskonformität der Datenübertragung	16.3
P05	Anforderungsprofil für Cloud-Anbieter	16.5

Kennung	**Bezeichnung**	**Prüfpunkt**
A08	Routineaufgaben definieren	1.8
A18	Jährliche Revision des Sicherheitsstatus	1.18
E05	Dokumentation der VPN-Konfiguration	5.5
G01	Erfassung der Herausgabe von Datenträgern	7.1

Prüfgruppen und Prüfpunkte

Es folgt eine detaillierte Aufführung der geprüften Bereiche, sowie der konkreten Maßnahmen zur Beseitigung von Nichtkonformitäten. Die Reihenfolge der Abschnitte stellt keine Priorisierung dar, sondern orientiert sich an den jeweiligen geprüften Themenbereichen. Daher sollte jedes Unternehmen, die für Sie zutreffenden Maßnahmen identifizieren und entsprechend eigenständig priorisieren, hinsichtlich der Umsetzungsreihenfolge.

1. IT-Sicherheitsmanagement

Zunehmende Technisierung und Digitalisierung von Geschäftsprozessen lassen den Stellenwert der Informationstechnik weiter steigen und sind für ein modernes Unternehmen nicht mehr wegzudenken. Unabhängig von der Größe der Organisation, ist ein Arbeiten ohne IT-Systeme nicht mehr denkbar und teilweise sogar unmöglich. Infolgedessen steigen die Anforderungen an die jederzeitige Verfügbarkeit der Systeme und die Verantwortung der Geschäftsleitung, entsprechende Maßnahmen zu treffen, um die kontinuierliche Funktionalität zu gewährleisten. Ein sorgloser Umgang mit dem Thema Informationssicherheit, fehlende Arbeitsanweisung und Prozesse, sowie mangelnde Sensibilisierungsmaßnahmen für Mitarbeiter, können dazu führen, dass hohe Schäden drohen, wenn die IT ausfällt. Es gehört zu den ordentlichen Pflichten eines Geschäftsführers, etwaige Schäden vom Unternehmen fern zu halten und Schutzmaßnahmen zu implementieren. Fehlt es an einem ordnungsgemäßen Informationssicherheitsmanagement, kann es schnell zu einer persönlichen Haftung der Geschäftsführer kommen – man spricht vom sogenannten Organisationsverschulden. Vor diesem Hintergrund erklärt sich auch der Umfang der Prüfgruppe IT-Sicherheitsmanagement und die Bandbreite der gewählten Prüfelemente. Unabdingbar sind neben Sicherheitskonzepten, Richtlinien und personellen Ressourcen, auch eine regelmäßige Schulung der Mitarbeiter sowie eine kontinuierliche Prüfung des Sicherheitsmanagements. Organisatorische Maßnahmen sind ebenso wichtig, wie die Firewall zum Schutz des internen Netzwerkes, daher sollte festgestellte Mängel aus dem Audit besondere Beachtung finden, um einen ganzheitlichen Schutz der Informationen zu gewährleisten.

1.1 Sicherheitsleitlinie

Ist-Zustand

In der Informationssicherheitsleitlinie sind alle wesentlichen Inhalte aufgeführt, wie beispielsweise die Sicherheitsziele und der Stellenwert der Informationssicherheit, zudem ist sie allen Mitarbeiter bekannt.

1.2 Sicherheitskonzept

Ist-Zustand

Es existiert ein aktuelles IT-Sicherheitskonzept, dass alle sicherheitsrelevanten Bereiche des Unternehmens umfasst und jedem Mitarbeiter bekannt ist.

1.3 Rechtliche Vorgaben

Ist-Zustand

Es gibt eine schriftliche Übersicht mit allen relevanten gesetzlichen Vorgaben, die von den Mitarbeitern zu beachten sind bei der täglichen Ausübung ihrer Arbeit. Die Inhalte werden regelmäßig aktualisiert und berücksichtigen Veränderungen der Gesetzeslage.

1.4 Sicherheitsbeauftragter

Ist-Zustand

Ein Sicherheitsbeauftragter ist schriftlich bestellt worden und seine Aufgaben sind detailliert beschrieben.

1.5 Datenschutzbeauftragter

Ist-Zustand

Es wurde ordnungsgemäß ein Datenschutzbeauftragter bestellt bzw. eine Person, die für den Datenschutz zuständig ist.

1.6 Datenschutzkonzept

Ist-Zustand

Ein Datenschutzkonzept ist vorhanden, allerdings ist dieses veraltet bzw. nicht allen Mitarbeitern bekannt. Analog zum Sicherheitskonzept beschreibt ein Datenschutzkonzept verbindliche Vorgaben zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten (u.a. technische und organisatorische Maßnahmen).

Maßnahmenempfehlung (A06)
Sprechen Sie mit Ihrem Datenschutzbeauftragten über die Notwendigkeit eines Datenschutzkonzeptes. Leiten Sie entsprechende Maßnahmen ein.

1.7 Schutzbedarf

Ist-Zustand

Es bestehen keine Vorgaben der Leitungsebene in welchem Maße Prozesse, Systeme und Informationen zu schützen sind. Anforderungen an die IT, hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität von Informationen und Systemen, müssen klar dokumentiert und definiert werden. Andernfalls ist ein ordnungsgemäßer IT-Betrieb nicht möglich.

Maßnahmenempfehlung (A07)
Es muss eine Schutzbedarfsanalyse durchgeführt werden, die den Schutzbedarf der wichtigsten Anwendungen und Systeme in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität einstuft. Das Ergebnis muss durch die Unternehmensleitung bestätigt werden.

1.8 Routineaufgaben

Ist-Zustand

Es wurde damit begonnen relevante IT-Aufgaben festzulegen, allerdings sind nicht alle notwendigen und erforderlichen Aufgaben erfasst bzw. die Zeitfenster müssten wesentlich kürzer sein, um einen angemessenen Schutz zu erreichen.

Anhänge

Übergabebestätigung
Risiko-Matrix

Firmenprofile und Kontakt

ITQ GmbH Institut für Technologiequalität

Das Institut für Technologiequalität hat sich die Optimierung der IT-Qualität und -Sicherheit in kleinen und mittelständischen Unternehmen zum Auftrag gemacht. Hierzu setzt die ITQ GmbH ein spezialisiertes Verfahren der IT-Sicherheit zum Vorteil von Kunden und Partnern ein.
Ausgewählte, qualifizierte IT-Sicherheitsexperten garantieren die Fachkompetenz des Instituts, eine ausgewogene Partnerlandschaft bietet KMU im gesamten deutschsprachigen Raum die Möglichkeit zur Umsetzung geforderter Sicherheitsstandards in der Informationstechnologie.
Mit IT-Zertifikaten der ITQ GmbH beweisen Unternehmen, dass sie den Anforderungen ihrer Kunden nach sicherer IT und geschützten Informationen nachdrücklich gerecht werden wollen.
Die auf die Anforderungen kleiner und mittelständischer Unternehmen speziell angepassten Zertifikate erfüllen in besonderem Maße die Forderung nach einem verlässlichen Standard in einer immer stärker vernetzten und immer mehr von sicheren IT-Systemen abhängigen Geschäftswelt.

ITQ GmbH

Übergabebestätigung

Mit meiner Unterschrift bestätige ich, in meiner Rolle als Auditor, nach bestem Wissen und Gewissen und unter Ausnutzung aller mir zu Verfügung stehenden Möglichkeiten sämtliche Prüfpunkte der Basisprüfung ITQ wahrheitsgemäß bearbeitet zu haben.

Ort, Datum, Unterschrift

Auditor	Jutta Brunn
Partner	ITQ GmbH

Mit meiner Unterschrift bestätige ich den Erhalt des vollständigen Berichtes. Über die Inhalte wurde ich informiert.

Ort, Datum, Unterschrift

Ansprechpartner

Risiko-Matrix

Risikoeinstufung **OHNE** GERING MITTEL HOCH SEHR HOCH

Ohne Einstufung

Risikoeinstufung OHNE GERING MITTEL HOCH SEHR HOCH

Die geforderte Maßnahme wurde umgesetzt

Risikoeinstufung OHNE **GERING** MITTEL HOCH SEHR HOCH

Umgesetzte Maßnahmen bieten möglicherweise hinreichenden Schutz

Risikoeinstufung OHNE GERING **MITTEL** HOCH SEHR HOCH

Umgesetzte Maßnahmen reichen möglicherweise nicht aus

Risikoeinstufung OHNE GERING MITTEL **HOCH** SEHR HOCH

Umgesetzte Maßnahmen sind unzureichend - gravierender Schaden droht

Risikoeinstufung OHNE GERING MITTEL HOCH **SEHR HOCH**

Umgesetzte Maßnahmen sind unzureichend - nicht tolerabler Schaden droht