Inhalt

Audit Facts

Geprüftes Unternehmen	Schuber + Söhne Fertigungs GmbH
Ansprechpartner	Henry Schuber
Prüfzeitraum	30.06.2017 - 04.07.2017
Berichtsnummer	020.1.17
Versionsnummer Software	AuditQ 16.2.6.0
ITQ-Partner	Am Brühl 25 12345 Musterstadt Fon +49 6024 3579-0 Fax +49 6024 3579-99 Info@formacom www.formacom.de
Partner-Kennung	**p.020.26**
Auditor	**Max Musterman** 0160787878787| 069 565656565 mmustermann@formacom.de
Auditor-Kennung	**a0012.13**
Verteiler	**Henry Schuber | Geschäftsführung** **Peter Langer | Rechtsanwalt**
Audit-Typ	**Erstzertifizierung**
Prüforte	**Schuber + Söhne Fertigungs GmbH** **Beispiel Str. 23 | 0000 Musterstadt**

Disclaimer

Die in diesem Bericht enthaltenen Informationen sind ausschließlich für den Gebrauch des, auf der vorangegangenen Seite unter **Audit Facts** angegebenen, geprüften Unternehmens (der Kunde) sowie der im oben angegebenen Verteiler aufgeführten Instanzen bestimmt und enthalten unter Umständen vertrauliche, schutzwürdige und nicht offen zu legende Informationen. Falls der Empfänger dieses Berichts nicht der Kunde ist, ist es diesem Empfänger streng verboten, den Bericht oder seine Inhalte zu lesen, zu kopieren, zu verbreiten oder in irgendeiner Form anderweitig zu verwenden.

Einleitung

Gütesiegel Basisprüfung ITQ

Herzlichen Glückwunsch! Mit der Durchführung der Basisprüfung ITQ gehen Sie den ersten wichtigen Schritt in Richtung hoher und nachweisbarer IT-Sicherheit für Ihr Unternehmen.

Beheben Sie innerhalb eines Zeitraums von 6 Monaten nach Durchführung der Basisprüfung ITQ im Rahmen dieser Prüfung festgestellte Mängel teilweise oder vollständig, so haben Sie die Möglichkeit, diesen Einsatz zur Festigung Ihrer IT-Sicherheit über weitere Prüfungen bestätigen oder zertifizieren zu lassen.
Details finden Sie unter www.itq-institut.de/zertifizierung.

Zielsetzung Basisprüfung ITQ

Das Ziel der Prüfung ist eine allgemeine Überprüfung des Sicherheitsniveaus und der Konfiguration des Netzwerkes zur Bestimmung der Ist-Situation. Auf dieser Grundlage sollen Handlungsempfehlungen ausgesprochen werden.

Bei der Überprüfung wird eine allgemeine Inspektion des Netzwerkes vorgenommen und durch ein Audit-Gespräch eine Überprüfung auf Basis von Teilen des BSI-Grundschutz und einem von der ITQ GmbH erstellten Prüfkatalog durchgeführt.

Die Ausarbeitung und der erstellte Katalog an Maßnahmenempfehlungen sollen der Geschäftsleitung als Werkzeug dienen, um notwendige Maßnahmen der IT zu erkennen, zu verstehen, zu steuern und zu überwachen.

Technische Zusammenfassung der Kundenumgebung

Das lokale Netzwerk des Unternehmens Schuber + Söhne Fertigungs GmbH besteht aus ca. 100 vernetzten Arbeitsplatzrechnern und 38 Servern, davon 4 Hardware Server, 3 Virtualisierungs-Hosts und 31 virtuelle Maschinen. Zur Virtualisierung ist VMware im Einsatz. Die Clients sind über 2 Cisco Switches an das Netzwerk angebunden, die wiederum über die beiden Netgear Core Switches die Verbindung zu den Servern herstellen. Die Drucker stellen die Verbindung zu den Core Switches über einen Switch des Herstellers HP her.

Die Gebäudeteile ‚Produktion', ‚Produkt-Design', ‚Verwaltung' sowie das Bürogebäude des Tochterunternehmens sind jeweils mit Glasfaserkabeln an die Core Switches angebunden. Im Server-Raum und in jedem Verteilerschrank befinden sich LWL Ethernet-Wandler. In den jeweiligen Verteilerschränken befinden sich Switches, die die jeweils in dem Gebäude(teil) befindlichen Ge-räte mit dem Netzwerk verbinden.

Die Internet-Verbindung über Telekom Company Connect ist über einen Lancom Router an das Netzwerk angeschlossen.

Management Summary

Übersicht der durchgeführten Arbeiten

Im Rahmen der **Basisprüfung ITQ** wurde im Stammsitz des Unternehmens die IT-Infrastruktur auf IT-Sicherheit geprüft.

Auf Basis eines **Audit-Gesprächs** wurden in 14 Prüfgruppen insgesamt 96 Prüfpunkte bewertet und bezüglich Ihres Risikobildes eingestuft.

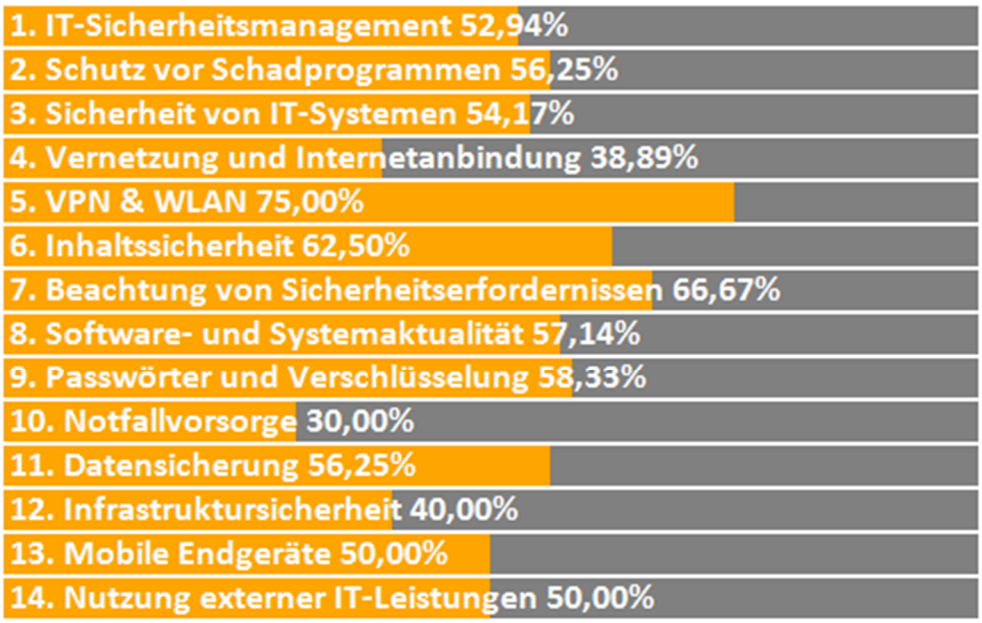
Für jeden festgestellten Mangel wurden **Maßnahmen** formuliert, deren Erledigung eine einhundertprozentige Beseitigung des Mangels sicherstellen.

Im Zuge der Durchführung der Basisprüfung ITQ wurden folgende Audit-Methoden angewendet

Dokumentationsprüfung	Analyse Messdaten	Befragung
Ansichtsnahme	Unterlagensichtung	Aktivitätsanalyse

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 von ITQ-Standards abgeleitete Einschätzung. Anhand des, diesem Bericht im Bereich ‚Anhänge' beigelegten Dokumentes **Risiko-Matrix** können Sie einzelne Probleme selbstständig bewerten und entsprechend einstufen.

Risikoeinstufung 6088

Wurde im Rahmen der **Basisprüfung ITQ** mindestens ein Problem mit hohem Risikograd festgestellt, fällt die Risikobewertung in ihrer Gesamtheit ‚Sehr Hoch' aus. Probleme mit hohem Risikograd sollten unternehmensseitig **umgehend beseitigt** werden.

Fazit

Der erreichte Gesamterfüllungsgrad der Anforderungen von 53,44% erscheint im ersten Moment sehr niedrig. Tatsächlich ist dies ein Ergebnis, welches wir in vergleichbaren Unternehmen häufig feststellen.

In mittelständischen Unternehmen mit bis zu einhundert PC-Arbeitsplätzen ist in der Regel eine Person als Administrator für die Betreuung der IT-Systeme zuständig. Gerade diese Konstellation ist für das Unternehmen ein Risiko. Eine qualifizierte Vertretung ist in der Regel nicht gewährleistet. Wird der IT-Verantwortliche krank, ist er im Urlaub oder fällt er für längere Zeit aus, kann ein Dritter ihn nur nach zeitintensiver Einarbeitung vertreten. Noch deutlicher wird das Risiko beim Ausscheiden des IT-Verantwortlichen aus dem Unternehmen: In der Regel besteht keine Dokumentation der IT-Infrastruktur und Anwendungen. Das Unternehmen ist in einem Maße vom Administrator abhängig, wie es weder sinnvoll noch notwendig ist.

Ein einziger IT-Mitarbeiter hat aber noch ein weiteres Problem: Er kann immer nur eine Aufgabe nach der anderen erledigen. Bei Belastungsspitzen entstehen Wartezeiten, die teilweise auch Produktivitätsverluste bedeuten. In dieser Situation der latenten Überforderung wird ein interner IT-Administrator darüber hinaus eines nicht machen: Ernsthaft an der IT-Strategie arbeiten. Er ist voll ausgelastet mit der Abarbeitung der Anforderungen von Geschäftsleitung und Kollegen. Dabei könnte die Entwicklung der Rahmenbedingungen die Arbeit deutlich erleichtern. Moderne Service-Ansätze wie zentrales IT Monitoring oder der Aufbau hochverfügbarer Strukturen sparen mittelfristig Zeit. Zuvor allerdings benötigen sie Zeit … Zeit, die der IT-Administrator nicht hat.

Früher reichte es aus, einen Allrounder zu beschäftigen, der die wesentlichen Geräte, Betriebssysteme und Anwendungen halbwegs beherrscht. Diesen Allrounder gibt es heute nicht mehr: Die IT-Welt wird mit rasender Geschwindigkeit so viel komplexer, dass kein einzelner Mensch alle Lösungen überschauen oder umsetzen kann. Dies wird der interne Mitarbeiter allerdings kaum zugeben. Wahrscheinlicher ist, dass das Unternehmen sich mit

Kompromiss-Lösungen zufriedengeben muss: Es werden nur die Anwendungen eingesetzt, die der Administrator auch beherrscht. Nicht die sinnvollste Lösung, sondern limitierte Fähigkeiten entscheiden dann über strategische IT-Fragen. Dieses Szenario treffen wir häufig in kleinen und mittleren Unternehmen an. Das Problem kann allerdings auch struktureller Natur sein: Manche Anwendungen sind für einzelne Unternehmen schlicht zu teuer. In beiden Fällen hilft eine externe IT-Abteilung - durch breiteres Fachwissen und die Aufteilung von Lizenzkosten auf mehrere Unternehmen.

Einige dieser Probleme, die wir immer wieder feststellen, treffen auch im Unternehmen Schuber + Söhne Fertigungs GmbH zu. Die niedrige Erfüllungsquote ist in großen Teilen nicht Ursache von Mängeln in der Administration, sondern ein Konstrukt der vergangenen Jahren, welches mit der aktuellen Konstellation kaum anders hätte entstehen können.

Nachfolgend erhalten Sie einen Überblick sämtlicher bei der Durchführung der Basisprüfung ITQ festgestellten Probleme sowie entsprechende Maßnahmenempfehlungen zur Beseitigung dieser Probleme.

Maßnahmenempfehlungen

Die Maßnahmenempfehlungen sind - unabhängig ihrer Zugehörigkeit zu Prüfpunkten und -gruppen - gemäß des Risikograde des jeweiligen Problems aufgelistet.

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

Kennung	**Maßnahmenempfehlung**	Verweis Prüfpunkt
A10	Durchführen einer Schutzbedarfsanalyse	1.7
A17	Ungenutzte aktive Benutzerkonten deaktivieren	1.9
A16	Erstellen von Mitarbeiter-Eintritts- und Austritts-Prozessbeschreibungen	1.12
A02	Büro-Arbeitsplätze mit verschließbaren Behältnissen ausstatten	1.14
A01	Datei-Übertragung und Nachrichtenaustausch regeln	1.17
C04	Inbetriebnahme eines zentral verwalteten Antivirus-Systems	2.1
C07	Antivirus-Full Scan aktivieren	2.3
E08	Standard-Passwörter gegen sichere tauschen	3.1
E05	Dokumentation der Rechtestruktur	3.4
E06	Einführung personalisierter und dienstbasierter Administratorkonten	3.5
E01	Ungenutzte Software deinstallieren	3.9
K07	Sicherheitseinstellungen der Browser aktivieren	4.5
K09	Netzwerk-Topologieplan erstellen	4.7
K08	Regelmäßige Prüfung der Web Server auf Sicherheitslücken	4.9
H01	Regulierung der privaten Nutzung von Internet und e-Mail	6.4
G03	Außerbetriebnahme und Entsorgung von Datenträgern regeln	7.5
M01	Patch-Aktualisierungsintervalle anpassen	8.3
M02	Definition eines Testkonzepts, Einrichtung einer Testumgebung	8.6
I01	Passwort-Wechsel	9.5
J03	Notfall-Management-Strategie erstellen	10.1
D06	Tägliche Prüfung der Datensicherungsvorgänge	11.3

D02	Einführung von Datenrücksicherungstests	11.6
N02	Einbruchschutz	12.2
N06	Rauchmelder installieren	12.6
N07	Zutritts- und Aufsichtsregelung für IT-Räume	12.7
N10	Lizenz-Management	12.10
B06	Mobile Device Management einführen	13.3
B03	Trennung von privaten und geschäftlichen Daten	13.6
F02	Regulierung jeglicher eingesetzter externer IT-Leistung durch vertragliche Grundlagen	14.2

A06	Erstellen einer IT-Sicherheitsleitlinie	1.1
A18	Erstellen eines Datenschutzkonzepts	1.6
A07	Erweitern der IT-Sicherheitsmaßnahmen	1.10
A03	Erstellen einer Regelung zum Hinterlegen von Passwörtern	1.11
A04	Einführen einer Software zur Passwort-Verwaltung	1.11
A15	Verfassen eine Richtlinie zur IT-Nutzung	1.15
A11	Verfassen einer Richtlinie zur Mitnahme von Datenträgern und Komponenten	1.16
C03	Inbetriebnahme einer Gateway-Antivirus-Lösung	2.2
C09	Gefährliche HTML-Inhalte und Anhänge einschränken.	2.5
C05	Routineaufgabe zur regelmäßigen Überprüfung der Viren-Schutzprogramme	2.8
E09	Die Ausgabe bzw. den Entzug von Zugangsmitteln dokumentieren	3.3
E07	Zugriff auf Wechselmedien regeln	3.13
K04	Erstellen eines Konzepts zur Freigabe von Firewall Ports	4.2
K10	Penetrationstest	4.4
K03	Beschriften der Netzwerkkomponenten	4.6
K02	Erstellen einer Sicherheitsrichtlinie für Router und Switches	4.8
L03	Aktualisierung der eingesetzten VPN-Verschlüsselungsverfahren	5.3
L08	Dokumentation der VPN-Konfiguration	5.5
L05	WLAN-Authentifizierung und -Verschlüsselung verbessern	5.7
L11	Nutzungsbedingen für die Hotspot-Nutzung erstellen	5.10
H03	Erstellen einer Richtlinie zum Umgang mit SPAM	6.3
G05	Erstellen einer Richtlinie ‚Löschung und Vernichtung von Daten‘	7.4
G06	Regelung zur Außerbetriebnahme von IT-Systemen	7.6
M01	Patch-Aktualisierungsintervalle anpassen	8.2
M07	Informationsfluss bei Update Roll Outs	8.5
I06	Vertrauliche Informationen sicher übertragen	9.1
I04	Einführung einer Lösung zur Verschlüsselung von e-Mails	9.2
I03	Automatische Bildschirmsperre einrichten	9.6
J01	Speicher- und Ablageorte der Notfallpläne prüfen	10.5
D04	Abgleich mit den Verfügbarkeitsanforderungen	11.2

D01	Sicherungskonzept für tragbare Computer	11.5
D03	Sichere Aufbewahrung von Datensicherungsmedien	11.8
N01	Prüfung der Räume mit IT-Komponenten	12.1
N04	Prüfung der Dichtigkeit	12.4
N05	USVs einsetzen	12.5
N09	Asset Management (Inventarisierung) einführen	12.9
B01	Verantwortungen für mobile Endgerät definieren	13.2
B04	Trennung von Netzwerken für mobile Endgeräte vom Unternehmens-netzwerk	13.5
F03	Erstellen einer Richtlinie zur Nutzung externer IT-Leistungen	14.3
E03	BIOS-Sicherheitseinstellungen an Arbeitsplatzrechnern überarbeiten	3.8
L04	Zugriffe via VPN einschränken	5.1
J02	Einführung von Notfalltests	10.6

Prüfgruppen und Prüfpunkte

1. IT-Sicherheitsmanagement

IT-Sicherheit hat sich von einem rein technischen Thema mit untergeordneter Auswirkung auf die Führung eines Unternehmens zu einer strategisch zentralen Verantwortung mit direkter persönlicher Haftung für die Geschäftsleitung entwickelt. Die immer intensivere Durchdringung der Geschäftsabläufe und Wertschöpfungsprozesse mit Informationstechnologie und die mittlerweile unumgängliche Anbindung an öffentliche Netze haben die Bedeutung von IT für die Führung und Steuerung eines Unternehmens, egal welcher Größe, in nur wenigen Jahren grundlegend verändert. Vor diesem Hintergrund erklärt sich auch der Umfang der Prüfgruppe IT-Sicherheitsmanagement und die Bandbreite der gewählten Prüfelemente: Alle nachfolgenden Prüfgruppen sind, durch die „Governance-Brille“ gesehen, direkt abhängig von einem existierenden aktiven Sicherheitsbewusstsein auf der Geschäftsleitungsebene. Ignoriert die Firmenleitung die persönliche Verantwortung für eine sichere IT und den Schutz der im Unternehmen vorhandenen eigenen oder fremden Datenbeständen, wird sich diese Haltung direkt in den Ergebnissen der folgenden, mehr technisch-inhaltlich orientierten Prüfgruppen mit eher negativen Ergebnissen kenntlich machen. Die Übersetzung des Willens zur sicheren IT auf Seiten der Unternehmensleitung lässt sich für den Auditor an Hand der Art, des Umfanges und der Aktualität der im Unternehmen vorhandenen verpflichtenden dokumentierten und kommunizierten Sicherheitsregeln festmachen. Die Reichweite der Regelungen z.B. im Bereich des Aufnehmens oder des Ausscheidens von Mitarbeitern gibt einen tiefen Einblick in die Sicherheitskultur des auditierten Unternehmens. Grundsätzlich gilt: Der Anspruch an das Vorhandensein eines Sicherheitsbewusstseins ist unabhängig von der Größe, der Branche oder der Struktur eines Unternehmens. Dieses sollte immer vorhanden sein und sich in einer für die jeweils spezifische Unternehmenssituation passende und geeignete Form ausdrücken und im Rahmen des Audits belegen lassen.

1.1 Sicherheitsleitlinie

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **80**
Schadenspotential: **Katastrophe**

Ist-Zustand	Es existiert eine Leitlinie,allerdings ist diese veraltet. Weder der Stellenwert der Informationssicherheit, noch die Ziele der Organisationsstruktur sind festgelegt. Es ist nicht sichergestellt, dass neue Mitarbeiter über die Leitlinie ausreichend informiert werd

Kennung	Maßnahmenempfehlung
A06	**Erstellen einer IT-Sicherheitsleitlinie** Gemeinsam mit der Firmenleitung muss eine Leitlinie zur Informationssicherheit verfasst werden, die zusammengefasst die angestrebten Sicherheitsziele bzw. das angestrebte Sicherheitsniveau für alle Mitarbeiter beschreibt. Diese Leitlinie muss im Namen der Firmenleitung veröffentlicht und bei allen Mitarbeitern bekanntgemacht werden.

1.2 Sicherheitskonzept

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **0**
Schadenspotential: **Katastrophe**

Ist-Zustand	Es existiert ein aktuelles Sicherheitskonzept über alle Bereiche des Unternehmens. Jeder Mitarbeiter ist darüber informiert.

1.3 Sicherheitsbeauftragter

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **0**
Schadenspotential: **Katastrophe**

Ist-Zustand	Ein Sicherheitsbeauftragter ist bestellt. Seine Position und seine Aufgaben sind schriftlich dokumentiert.

1.4 Rechtliche Vorgaben

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **0**
Schadenspotential: **Katastrophe**

Ist-Zustand Es ist ein Dokument mit der Übersicht über alle für das Unternehmen relevanten rechtlichen Vorgaben vorhanden. Verantwortlichkeiten und Zuständigkeiten für die Einhaltung der rechtlichen Vorgaben sind definiert.

1.5 Datenschutzbeauftragter

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **0**
Schadenspotential: **Katastrophe**

Ist-Zustand Es wurde ein Datenschutzbeauftragter bestellt.

1.6 Datenschutzkonzept

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **80**
Schadenspotential: **Katastrophe**

Ist-Zustand Ein Datenschutzkonzept ist vorhanden, allerdings ist dieses veraltet. Es ist nicht sichergestellt dass neu eingestellte Mitarbeiter darüber unterrichtet sind. Analog zum Sicherheitskonzept beschreibt ein Datenschutzkonzept die für eine datenschutzrechtliche Beurteilung notwendigen Informationen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten (u.a. technische und organisatorische Maßnahmen).

Kennung	Maßnahmenempfehlung
A18	**Erstellen eines Datenschutzkonzepts** Sprechen Sie mit Ihrem Datenschutzbeauftragten über die Notwendigkeit eines Datenschutzkonzepts. Leiten Sie entsprechende Maßnahmen ein.

1.7 Schutzbedarf

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **100**
Schadenspotential: **Katastrophe**

Ist-Zustand Es bestehen keine Vorgaben der Firmenleitung bzw. der Haftungsträger in welchem Maße Prozesse, Systeme und Informationen zu schützen sind. Die Administration handelt somit nach bestem Gewissen, Ärger und unerwartete Schäden sind vorprogrammiert. Sicherheits-Entscheidungen sind subjektiver Natur. Deshalb sollten die Haftungsträger zwingend an der Risikobewertung von Systemen bzw. Unternehmensprozessen beteiligt sein. Anforderungen an die IT hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität von Informationen und Systemen müssen klar dokumentiert werden. Nur dann können angemessene Maßnahmen abgeleitet werden und nur dann ist ein zielführender IT-Betrieb gegeben.

Kennung	Maßnahmenempfehlung
A10	**Durchführen einer Schutzbedarfsanalyse** 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

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **0**
Schadenspotential: **Katastrophe**

Ist-Zustand Es ist bei allen IT-Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen. Die Aktivitäten des Administrators können ausreichend kontrolliert werden.

1.9 Verwaltung von ungenutzten Zugängen

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **100**
Schadenspotential: **Katastrophe**

Ist-Zustand Zum Zeitpunkt der Prüfung wurden ungenutzte administrative Konten und/oder Benutzerkonten im Netzwerk festgestellt. Dies ist in der Regel auf eine fehlende Routineaufgabe oder lückenhafte Mitarbeiter-Eintritts- und Austritts-Prozesse zurückzuführen. Ungenutzte aktive Konten können leicht unbemerkt missbraucht werden.

Kennung	Maßnahmenempfehlung
A17	**Ungenutzte aktive Benutzerkonten deaktivieren** Passen Sie Prozesse entsprechend an, um ungenutzte Konten bzw. Netzwerkzugänge jeglicher Art zeitnah zu löschen oder zu deaktivieren. Beachten Sie dabei u.a. den Weggang eines Mitarbeiters, den Wechsel in eine andere Abteilung oder längere Abwesenheiten jeglicher Art.

1.10 Zuständigkeiten und Verantwortlichkeiten

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **80**
Schadenspotential: **Schwer**

Ist-Zustand Es sind für IT-Sicherheitsmaßnahmen Zuständigkeiten, Verantwortlichkeiten und Vertretungsregelungen festgelegt, allerdings sind diese nicht vollständig. Es ist nicht sichergestellt, dass neuen Mitarbeitern die Regelungen bekanntgegeben werden. Sollten daraus resultierend Sicherheitsmaßnahmen unbemerkt unbearbeitet bleiben, können vermeintlich präventiv vorgebeugte Schäden dennoch eintreten. Sollten Schäden eintreten, zeigt sich in der Praxis oftmals, dass - neben der nicht zu unterschätzenden Haftungsfrage - Aufgaben ohne klare Verantwortlichkeiten tendenziell stiefmütterlich behandelt werden. Dies will man an dieser Stelle vermeiden.

Kennung	Maßnahmenempfehlung
A07	**Erweitern der IT-Sicherheitsmaßnahmen** Erweitern Sie die IT-Sicherheitsmaßnahmen, sodass für jede eine klare Zuständigkeit, Verantwortung und Vertretung definiert ist. Stellen Sie sicher, dass die Regelungen allen Mitarbeitern bekannt sind.

1.11 Umgang mit Passwörtern

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **80**
Schadenspotential: **Katastrophe**

Ist-Zustand Es existiert eine Regelung zur Hinterlegung von Passwörtern, allerdings ist diese unvorständig und veraltet. Die Unternehmensleitung muss sicherstellen, dass gerade die Administratoren über die Vorgaben und Werkzeuge verfügen, um das Hinterlegen sicherer Passwörter zu gewährleisten, damit eine Vertretung jederzeit möglich ist. Es besteht ansonsten die Gefahr, dass Daten und Zugriffe unwiderruflich verloren gehen.

Kennung	Maßnahmenempfehlung
A03	**Erstellen einer Regelung zum Hinterlegen von Passwörtern** Erstellen Sie eine schriftliche Regelung welche sicherstellt, dass alle Mitarbeiter wichtigste Passwörter in der dafür vorgesehenen Software hinterlegen. Prüfen Sie deren Einhaltung regelmäßig.
A04	**Einführen einer Software zur Passwort-Verwaltung** Führen Sie eine Software ein, welche das sichere Hinterlegen von Passwörtern zulässt. Achten Sie neben der Sicherheit der Software auf eine anwenderfreundliche Bedienung, um die Akzeptanz seitens des Personals sicherzustellen.

1.12 Mitarbeiter-Eintritt und -Austritt

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **100**
Schadenspotential: **Katastrophe**

Ist-Zustand Es existieren keine dokumentierten Prozesse, die den Mitarbeiter-Eintritt und -Austritt regeln. Diese Prozesse sind häufig komplex, da sie die enge Zusammenarbeit mehrerer Abteilungen voraussetzen. Bei nachgiebiger Entwicklung und Überwachung dieser Prozesse können Datenzugriffe, Firmengeheimnisse, der Zutritt zu kritischen Räumen sowie der Zugriff auf IT-Geräte wie Laptops oder USB Sticks langfristig unbemerkt bestehen bleiben (häufig noch lange nach Beendigung des Arbeitsverhältnisses). Lücken werden dann nur noch zufällig festgestellt - im schlimmsten Fall, wenn bereits ein Schaden eingetreten ist.

Kennung	Maßnahmenempfehlung
A16	**Erstellen von Mitarbeiter-Eintritts- und Austritts-Prozessbeschreibungen** Es müssen Prozesse beschrieben werden, welche Maßnahmen ergriffen werden müssen, wenn ein Mitarbeiter in das Unternehmen eintritt oder dieses verlässt. Die Abarbeitung dieser Prozesse muss je durchgeführtem Vorgang schriftlich und nachvollziehbar dokumentiert werden.

1.13 Mitarbeitersensibilisierung

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **0**
Schadenspotential: **Katastrophe**

Ist-Zustand Mitarbeiter werden regelmässig hinsichtlich der Tragweite und der Notwendigkeit von IT-Sicherheit geschult. Mitarbeitern sind die Sicherheitsmaßnahmen bekannt, die sie in ihrer täglichen Arbeit zu beachten haben.

1.14 Aufbewahrung von Datenträgern

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **100**
Schadenspotential: **Schwer**

Ist-Zustand An den Büro-Arbeitsplätzen sind unzureichend verschließbare Behältnisse bzw. Schränke verfügbar, um vertrauliche Datenträger und Unterlagen zu verstauen. Überall da, wo mit personenbezogenen Daten oder sonstigen Betriebsgeheinissen gearbeitet wird, sollten diese in ausreichender Menge zur Verfügung stehen. Um das Ausspähen oder das Verschwinden von Datenträgern und Unterlagen zu verhindern, sollten Mitarbeiter zum sorgfältigen Umgang klar verpflichtet werden; jedoch benötigen sie auch die Mittel, um die Anforderungen erfüllen zu können.

Kennung	Maßnahmenempfehlung
A02	**Büro-Arbeitsplätze mit verschließbaren Behältnissen ausstatten** Installieren Sie verschließbare Behältnisse überall dort, wo mit sensiblen Daten gearbeitet wird. Es sollte den Mitarbeitern so einfach wie möglich gemacht werden, sich am Schutz der Unternehmenswerte zu beteiligen.

1.15 Richtlinie zur IT-Nutzung

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **80**
Schadenspotential: **Katastrophe**

Ist-Zustand Es gibt eine verfügbare Richtlinie zur IT_Nutzung, allerdings ist veraltet und unvollständig. Mitarbeiter sind nicht hinreichend informiert. Mitarbeiter müssen verstehen, welche Verpflichtungen für sie mit der Bedienung der IT-Arbeitsgeräte einhergehen. Ohne klar kommunizierte Verantwortungen können Verstöße nicht geahndet werden. Dies kann dazu führen, dass Mitarbeiter leichtfertig mit Systemen umgehen und somit geschäftskritische Daten gefährden.

Kennung	Maßnahmenempfehlung
A15	**Verfassen eine Richtlinie zur IT-Nutzung** Erstellen Sie eine Richtlinie, die den Umgang mit IT-Systemen klar regelt. Die Richtlinie zur IT-Nutzung hat sich zudem als Werkzeug zur Mitarbeiter-Sensibilisierung bewährt und ist eine einfache und kosteneffektive Maßnahme, um einigen erheblichen Risiken zu begegnen. Führungskräfte erhalten zudem die Grundlage, um Verstöße ahnden zu können.

1.16 Mitnahme von Datenträgern und Komponenten

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **80**
Schadenspotential: **Schwer**

Ist-Zustand Es gibt Regelungen für die Mitnahme von Datenträgern und Komponenten, allerdings sind diese unvollständig. Verlust, Defekt, Missbrauch oder Diebstahl können somit unbemerkt bleiben. Mitarbeiter müssen verstehen, welche Gefahren die Mitnahme von Datenträgern und Komponenten mit sich bringt und welche Verhaltensweisen einzuhalten sind.

Kennung	Maßnahmenempfehlung
A11	**Verfassen einer Richtlinie zur Mitnahme von Datenträgern und Komponenten** Sensibilisieren Sie betroffenes Personal für die Risiken der Mitnahme von Datenträgern und Komponenten. Legen Sie Verhaltensregeln und Verantwortungen fest. Definieren Sie zudem Meldewege und Ansprechpartner bei Ausfall, Verlust, Defekt, Zerstörung oder Diebstahl.

1.17 Nachrichtenaustausch mit externen Kontakten

Eintrittswahrscheinlichkeit: **Hoch** Risikoeinstufung **100**
Schadenspotential: **Katastrophe**

Ist-Zustand Es bestehen keine Regelungen zu Datei-Übertragung und Nachrichtenaustausch mit externen Kontakten. Wo überall geschäftskritische Daten vorzufinden sind, könnte Sie überraschen. Es besteht die Gefahr, dass Mitarbeiter nicht vertrauenswürdige Portale oder Medien nutzen und geschäftskritische Daten versehentlich im Internet veröffentlichen.

Kennung	Maßnahmenempfehlung
A01	**Datei-Übertragung und Nachrichtenaustausch regeln** Legen Sie - neben technischen Maßnahmen - organisatorisch fest, welche Daten zu welchem Zweck wohin übertragen werden. Sind die genutzten Portale bzw. Medien dem Schutzbedarf der Daten angemessen? Regeln Sie klar wer was wohin übertragen soll und stellen Sie vor allem sicher, dass die genutzten Medien dem Schutzbedarf gerecht werden.

Anhänge

Übergabebestätigung

Risiko-Matrix

Angebot

Firmenprofile und Kontakt

FormaCOM

Am Brühl 25
12345 Musterstadt
Fon +49 6024 3579-0
Fax +49 6024 3579-99
Info@formacom
www.formacom.de

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.

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
Max Musterman Auditor
FormaCOM

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

Ort, Datum, Unterschrift
Henry Schuber
Schuber + Söhne Fertigungs GmbH

Risiko-Matrix