BASISPRÜFUNG ITQ

geprüfte IT-Infrastruktur auf Basis des ITQ-Kriterienkatalogs ITQ13 v04

1 ZIELSETZUNG

Das Ziel ist eine allgemeine Überprüfung des Sicherheitsniveaus und der Konfiguration des Netzwerkes zur Bestimmung der Ist-Situation. Auf dieser Grundlage werden Handlungsempfehlungen ausgesprochen. Bei der Überprüfung wird eine allgemeine Inspektion des Netzwerkes vorgenommen und durch ein Audit-Gespräch eine Überprüfung auf Basis von Teilen des BSI-Grundschutzes und eines vom Institut für Technologiequalität (ITQ GmbH) erstellten Prüfkatalogs durchgeführt.

2 SIEGEL

Mit der Durchführung der Basisprüfung ITQ gehen Unternehmen den ersten wichtigen Schritt in Richtung hoher und nachweisbarer IT-Sicherheit. Nach erfolgreich absolvierter Basisprüfung erhält das Unternehmen das ITQ-Basissiegel zur Verwendung, z.B. auf der Homepage oder auf Geschäftspapieren.

3 INHALT DER PRÜFUNG

Im Rahmen der Basisprüfung ITQ wird im Stammsitz des Unternehmens die IT-Infrastruktur auf IT-Sicherheit geprüft. Auf Basis eines Audit-Gesprächs werden in 14 Prüfgruppen insgesamt über 100 Prüfpunkte bewertet und bezüglich Ihres Risikobildes eingestuft.
Für jeden festgestellten Mangel werden Maßnahmen formuliert. Im Zuge der Durchführung der Basisprüfung werden folgende Audit-Methoden angewendet: Dokumentationsprüfung, Befragung, Ansichtsnahme, Unterlagensichtung und Aktivitätsanalyse

Prüfgruppen und Prüfpunkte:

1. IT-Sicherheitsmanagement

1.1 Sicherheitsleitlinie
1.2 Sicherheitskonzept
1.3 Sicherheitsbeauftragter
1.4 Rechtliche Vorgaben
1.5 Datenschutzbeauftragter
1.6 Datenschutzkonzept
1.7 Schutzbedarf
1.8 Routineaufgaben
1.9 Verwaltung von ungenutzten Zugängen
1.10 Zuständigkeiten und Verantwortlichkeiten
1.11 Umgang mit Passwörtern
1.12 Mitarbeiter-Eintritt und –Austritt

1.13 Mitarbeitersensibilisierung
1.14 Aufbewahrung von Datenträgern
1.15 Richtlinie zur IT-Nutzung
1.16 Mitnahme von Datenträgern und Komponenten
1.17 Nachrichtenaustausch mit externen Kontakten

2. Schutz vor Schadprogrammen

2.1 Viren-Schutzproramme
2.2 Virenschutz auf dem Internet Gateway
2.3 Regelmäßige Untersuchung auf Viren
2.4 Virenschutz auf dem E-Mail Server
2.5 Gefahren durch HTML-Inhalte und Anhänge
2.6 Automatische Warnungen der Viren-Schutzprogramme
2.7 Verhalten bei Virenbefall
2.8 Statusprüfungen der Viren-Schutzprogramme

3. Sicherheit von IT-Systemen

3.1 Umgang mit Standard-Passwörtern
3.2 Rollen- und Rechtekonzept
3.3 Vergabe sowie Entzug von Zugangsberechtigungen
3.4 Bedarfsgerechte Zugriffe
3.5 Getrennte Administratorenprofile
3.6 Personen mit Administrator-Rechten
3.7 Sicherheitsrichtlinien für Server
3.8 BIOS-Einstellungen
3.9 Nicht benötige Software
3.10 Systemdokumentationen
3.11 Monitoring
3.12 Wartungs- und Garantieverträge
3.13 Zugriff auf Wechselmedien

4. Vernetzung und Internetanbindung

4.1 Externe Netzzugänge
4.2 Konfiguration Sicherheits-Gateway
4.3 Personal Firewall auf Notebooks
4.4 Penetrationstests
4.5 Sicherheitseinstellungen Browser
4.6 Beschriftung der Netzwerkkomponenten
4.7 Dokumentation der Verkabelung
4.8 Betrieb von Routern und Switches
4.9 Sicherheit der WWW-Server

5. VPN & WLAN

5.1 Zugriffe via VPN-Verbindungen
5.2 Internet-Zugriffe via VPN Client
5.3 Kryptographische Verfahren
5.4 Sicherheit der VPN-Installation
5.5 VPN-Dokumentation
5.6 WLAN-Sicherheitsrichtlinie
5.7 Schutz von WLAN-Verbindungen
5.8 Trennung von LAN und WLAN
5.9 Hotspot zur LAN-Verbindung
5.10 Nutzungsbedingungen Hotspot
5.11 Updates für WLAN Accesspoints und Repeater

6. Inhaltssicherheit

6.1 Filterung von Web-Inhalten
6.2 Schutz gegen unerwünschte E-Mails
6.3 Umgang mit SPAM E-Mails
6.4 Regelung der geschäftlichen und privaten E-Mail-Nutzung

7. Beachtung von Sicherheitserfordernissen

7.1 Herausgabe von Datenträgern
7.2 Sicherheitsregeln bei Wartungsarbeiten
7.3 Umgang mit Zugängen bei Wartungen
7.4 Datenlöschung
7.5 Außerbetriebnahme und Entsorgung von Datenträgern
7.6 Außerbetriebnahme von IT-Systemen

8. Software- und Systemaktualität

8.1 Patch Management-Strategie
8.2 Patch-Status der Server
8.3 Patch-Status der Clients
8.4 Patch-Status sonstige Netzwerkkomponenten
8.5 Informationsfluss Roll Out Patches und Updates
8.6 Testverfahren Patches und Updates
8.7 Roll Back Patches und Updates

9. Passwörter und Verschlüsselung

9.1 Übertragung von vertraulichen Informationen
9.2 E-Mail-Verschlüsselung
9.3 Passwortschutz
9.4 Richtlinien und Komplexitätsanforderungen
9.5 Passwort-Wechsel
9.6 Bildschirmsperre

10. Notfallvorsorge

10.1 Notfall-Management-Strategie
10.2 Identifizierung kritischer Geschäftsprozesse
10.3 Behandelte Notfallsituationen
10.4 Notfallpläne
10.5 Zugriff auf die Nofalldokumentation
10.6 Notfälle testen

11. Datensicherung

11.1 Datensicherungskonzept
11.2 Abgleich mit den Verfügbarkeitsanforderungen
11.3 Kontrolle
11.4 Bestandsverzeichnis
11.5 Sicherung tragbarer Computer
11.6 Datenrücksicherungstests
11.7 Dokumentation der Sicherungs- und Rücksicherungsverfahren
11.8 Schutz der Datensicherungsmedien

12. Infrastruktursicherheit

12.1 Physischer Schutz der IT-Systeme
12.2 Einbruchsschutz
12.3 Handfeuerlöcher
12.4 Wasserleitungen
12.5 USV
12.6 Rauchmelder
12.7 Zutritts- und Aufsichtsregelung
12.8 Umgang mit Arbeitsunterlagen
12.9 Software- und Hardware-Inventar
12.10 Lizenzkontrolle

13. Mobile Endgeräte

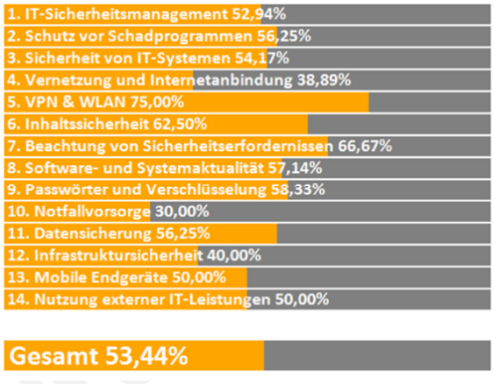
13.1 Sicherheitskonzept für mobile Endgeräte
13.2 Management von mobilen Endgeräten
13.3 MDM Software
13.4 Datenübertragung
13.5 Zugriff auf das interne Netz
13.6 Trennung von privaten und geschäftlichen Daten

14. Nutzung externer IT-Leistungen

14.1 Übersicht der externen IT-Leistungen
14.2 Vertragliche Grundlage
14.3 Richtlinien und Vorgaben

4 ERFÜLLUNGSGRAD

Im Anschluss erhält das geprüfte Unternehmen eine grafische Übersicht der geprüften Unternehmensbereiche, unterteilt in Prüfgruppen. Der Erfüllungsgrad wird in Prozent angegeben, 100% entsprechen dabei einer vollständigen Erfüllung der jeweiligen Prüfgruppe.



5 RISIKOBEWERRTUNG

Bei der Risikobewertung handelt es sich um eine auf Basis von ITQ-Standards abgeleitete Einschätzung. Anhand dieser können einzelne Probleme selbstständig bewertet und entsprechend eingestuft werden.

Risikoeinstufung 6088