Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Ärzteversorgung Westfalen-Lippe
Scharnhorststraße 44
48151 Münster

für das IT-System

MiPor

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ), Version 10.0
Security Assurance Level SEAL-3

der TÜV Informationstechnik GmbH. Die Prüfanforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 6 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Security TÜViT® 2017 Trusted Site

Certificate ID: 9555.17

Zertifikat gültig bis
31.05.2019

Essen, 06.11.2017

Dr. Anja Wiedemann
stellv. Leiterin Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.tuvit.de

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Produktzertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.0 vom 24.08.2015, TÜV Informationstechnik GmbH

Prüfbericht

- „Sicherheitstechnische Qualifizierung MiPor, Version 1.0 vom 26.10.2017, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ) der TÜV Informationstechnik GmbH“, Version 10.0 vom 21.03.2011, TÜV Informationstechnik GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist die Internet Portallösung „Mitglieder-Portal“ (MiPor) der Ärzteversorgung Westfalen-Lippe. MiPor bietet registrierten Endkunden die Möglichkeit gespeicherte Datensätze (bspw. Adressdaten) einzusehen und zu ändern. Eine detaillierte Beschreibung des IT-Systems ist im Prüfbericht hinterlegt.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-3 für IT-Systeme sind erfüllt.
- Der Prüfgegenstand erfüllt die systemspezifischen Sicherheitsanforderungen.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifischen Sicherheitsanforderungen lagen der Zertifizierung zugrunde und wurden überprüft.

1 Authentisierung und Zugriffskontrolle

- Schützenswerte Daten, Dienste und Funktionen werden von der Webanwendung wirksam vor unbefugten Zugriffen geschützt.
- Die Zugangsdaten werden von der Webanwendung sicher geändert, verarbeitet und gespeichert, so dass die Vertraulichkeit und Integrität der Zugangsdaten geschützt wird.

2 Verwaltung von Benutzersitzungen (Session Management)

- Die von der Webanwendung verwendeten Sitzungsinformationen werden sicher generiert, verwaltet und gelöscht, so dass die Vertraulichkeit und Integrität der Sitzungsdaten geschützt wird.
- Die Sitzungsinformationen werden von der Webanwendung vertraulich behandelt.

3 Validierungen von Ein- und Ausgabedaten

- Alle Ein- und Ausgabedaten werden von der Webanwendung vor der Verarbeitung validiert, so dass keine schadhaften Daten von der Webanwendung verarbeitet und ausgegeben werden. Dabei werden Daten von und zu allen Systemkomponenten (z. B. Browser oder Datenbank) von der Webanwendung geprüft.
- Die Validierung aller Ein- und Ausgabedaten wird serverseitig umgesetzt.

4 Datensicherheit

- Von der Webanwendung werden keine vertraulichen Informationen über die interne Struktur der Anwendung preisgegeben.
- Die Übertragung vertrauenswürdiger Daten sowie der Zugriff auf die Webanwendung erfolgt über gesicherte Verbindungen, welche die Integrität und Vertraulichkeit schützen.
- Die Zwischenspeicherung sensibler Daten wird vermieden.
- Vertrauliche Daten (z. B. Zugangsdaten) werden verschlüsselt gespeichert. Dabei werden Algorithmen verwendet, die dem Stand der Technik entsprechen.

5 Anwendungslogik

- Die Webanwendung bietet nur betrieblich notwendige Funktionen an. Die angebotenen Funktionen der Webanwendung können nicht missbräuchlich verwendet werden (z. B. Ausbrechen aus einem definierten Ablauf).

6 Systemhärtung

- Die vom Internet erreichbaren Komponenten und Serverprozesse weisen keine bekannten, ausnutzbaren Schwachstellen auf.

Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 10.0

1 Technische Sicherheitsanforderungen

Die technischen Sicherheitsanforderungen müssen dokumentiert, widerspruchsfrei und überprüfbar sein. Die Spezifikation muss in Anlehnung an ISO/IEC 17007 erfolgen. Des Weiteren müssen die technischen Sicherheitsanforderungen im Rahmen einer individuellen Bedrohungs- und Risikoanalyse hergeleitet sein, sie müssen aus bereits definierten Schutzprofilen hergeleitet sein, oder sie müssen konform zu veröffentlichten Sicherheitsanforderungen anerkannter Autoritäten oder Gremien der IT-Sicherheit sein. Weiterhin müssen sie für den Einsatzzweck des IT-Systems angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Architektur und Design

Das IT-System muss sinnvoll und verständlich strukturiert sein. Seine Komplexität darf keinen Einfluss auf die Sicherheit haben. Die Härtungs- und Schutzmaßnahmen müssen angemessen und wirkungsvoll sein. Es darf keine konzeptionellen Schwachstellen enthalten, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können.

3 Installation und Betrieb (ab SEAL-4)

Die vorhandenen Überwachungsmaßnahmen müssen wirkungsvoll sein. Die überwachten Ereignisse müssen geeignet sein, Sicherheitsvorfälle zuverlässig und zeitnah zu erkennen. Die Administration erfolgt über einen vertrauenswürdigen Pfad hinsichtlich Vertraulichkeit und Integrität. Die Dokumentation muss verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

4 Schwachstellenanalyse und Penetrationstests

Die Sicherheitsmaßnahmen des IT-Systems müssen einer Überprüfung durch Penetrationstests standhalten. Es darf nicht möglich sein, Sicherheitsmaßnahmen zu brechen oder zu umgehen. Das IT-System muss sicher konfiguriert sein, darf keine ausnutzbaren Schwachstellen haben und muss alle definierten technischen Sicherheitsanforderungen erfüllen.

5 Änderungsmanagement (ab SEAL-5)

Das Patch-Management muss dokumentiert und für das IT-System geeignet sein. Das Vorgehen bei Änderungen am IT-System muss klar definiert und geeignet sein. Die beteiligten Personen müssen damit vertraut sein. Verantwortlichkeiten müssen eindeutig geregelt sein. Änderungen dürfen nicht zu einer Reduzierung des erreichten Sicherheitsniveaus führen.

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Prüfkriterien für IT-Systeme. Eine Zertifizierung eines IT-Systems ist möglich ab Level SEAL-3.

Security Assurance Level / Prüfkriterien	SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Technische Sicherheits-anforderungen	X	X	X	X	X
Architektur und Design			X	X	X
Installation und Betrieb				X	X
Schwachstellenanalyse und Penetrationstests		X	X	X	X
Änderungsmanagement					X

Tabelle: Prüfkriterien und Security Assurance Level für IT-Systeme