Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

symmedia GmbH
Turnerstraße 27
33602 Bielefeld

für die Remote Service Portal-Software

symmedia SP/1, Version 9

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 Product

Certificate ID: 6134.17

19

Zertifikat ist gültig bis 31.05.2019

Essen, 06.06.2017

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

Zertifizierungsprogramm

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

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

Prüfbericht

- „Prüfbericht Sicherheitstechnische Qualifizierung, symmedia SP/1, Version 9“, Berichtsversion 1.4 vom 18.05.2017, TÜV Informationstechnik GmbH

Prüfanforderungen

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

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist die Remote Service Portal-Software „symmedia SP/1, Version 9“, der symmedia GmbH. Dieser ist im Prüfbericht detailliert beschrieben.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-3 sind erfüllt.

- Die produktspezifischen Sicherheitsanforderungen sind erfüllt.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

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

1 Identifizierung & Authentifizierung

Das IT-Produkt muss den Benutzer eindeutig identifizieren und authentifizieren. Die Authentisierungsdaten müssen hinreichend stark sein, um gängigen Angriffen ausreichend lange standzuhalten. Des Weiteren müssen vorgetäuschte Authentisierungsdaten erkannt und deren Missbrauch verhindert werden. Dies gilt für folgende Kommunikationsbeziehungen:

Benutzer und Systeme:

- Bediener am Site Control Server
- Servicetechniker am Site Control Server
- Servicetechniker am Central Server

Systeme und Systeme:

- Site Control Server am Central Server

2 Zugriffskontrolle

Das IT-Produkt muss Funktionen bereitstellen, die es ermöglichen, die Zugriffrechte des Benutzers einzuschränken. Einem Benutzer darf es mit vertretbarem Aufwand nicht möglich sein, seine Rechte unbefugt zu erweitern.

3 Transportverschlüsselung

Die Kommunikation über unsichere Netze muss über einen vertrauenswürdigen Pfad erfolgen, der die Vertraulichkeit der übertragenen Daten sicherstellt. Dies gilt insbesondere für die Kommunikation zwischen

- Central Server und Site Control Server,
- Servicetechniker und Site Control Server sowie
- Servicetechniker und Central Server.

4 Datenflusskontrolle

Das IT-Produkt muss sicherstellen, dass nur betrieblich notwendige Verbindungen möglich sind. Dies gilt für die Verbindungen zwischen

- Site Control Server und Central Server sowie
- Servicetechniker und Central Server.

5 Logging

Sicherheitsrelevante Ereignisse müssen protokolliert werden. Für das Prologging (ein Loggingverfahren, bei dem die Log-Einträge mit Hash-Einträgen versehen werden) ist eine Manipulation der Log-Einträge gegenüber dem Standardlogging (Logging ohne Hashing) erschwert.

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

1 Technische Sicherheitsanforderungen (ab SEAL-1)

Die technischen Sicherheitsanforderungen müssen dokumentiert, widerspruchsfrei und überprüfbar sein. Die Spezifikation muss in Anlehnung an ISO/IEC 17007 erfolgen. Des Weiteren müssen die technischen Sicherheitsanfor-

derungen 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-Produkts angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Architektur und Design (ab SEAL-3)

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

3 Entwicklungsprozess (ab SEAL-3)

Die Entwicklung des IT-Produkts muss im Rahmen eines definierten Development Life Cycle erfolgen, der mindestens die Phasen Planung, Analyse, Design, Implementierung, Test, Deployment und Maintenance berücksichtigt. Die Maintenance Phase des Development Life Cycle muss Schwachstellen berücksichtigen und beseitigen, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können. Im Rahmen der Test Phase des Development Life Cycles müssen Tests bezogen auf die Sicherheitsfunktionalität des IT-Produkts berücksichtigt werden.

4 Betriebsvorgaben (ab SEAL-4)

Die Dokumentation bestehend aus den sicherheitsrelevanten Vorgaben an die Betriebsumgebung des IT-Produkts, den Handbüchern zur Installation und Administration sowie den Handbüchern für die Endbenutzer muss gut verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

5 Schwachstellenanalyse und Penetrationstests (ab SEAL-2)

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

6 Sourcecode-Analyse (ab SEAL-4)

Der Sourcecode darf keine Verwundbarkeiten, Fehler oder Inkonsistenzen enthalten, wie beispielsweise undokumentierte Befehle, Parameter oder Testfunktionen.

7 Änderungsmanagement (ab SEAL-5)

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

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Prüfkriterien. Ein Zertifikat kann erteilt werden, wenn ein IT-Produkt die Prüfung erfolgreich durchlaufen und mindestens den Level SEAL-3 erreicht hat.

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
Entwicklungsprozess			X	X	X
Betriebsvorgaben				X	X
Schwachstellenanalyse und Penetrationstests		X	X	X	X
Sourcecode-Analyse				X	X
Änderungsmanagement					X

Tabelle: Prüfkriterien und Security Assurance Level für IT-Produkte