Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin

für das IT-System

BDrive v. 2.0.51.4

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 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Security TÜViT® 2018 Trusted Site

Certificate ID: 9558.18

Zertifikat gültig bis 31.10.2020

Essen, 30.10.2018

Dr. Christoph Sutter
Leiter 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 Qualifikation BDrive v. 2.0.51.4 der Bundesdruckerei GmbH“, Version 1.5 vom 22.10.2018, 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 das IT-System BDrive v. 2.0.51.4, der Bundesdruckerei GmbH.

BDrive v. 2.0.51.4 ist eine Plattform zur sicheren Speicherung und Weitergabe von vertraulichen Daten. Die Daten werden hierbei in Fragmente zerlegt und redundant auf unterschiedliche Cloud-Anbieter-Speicher verteilt, die nicht zwangsläufig Bestandteil der BDrive-Plattform sind. Geschützt werden die Daten durch Verschlüsselungsmechanismen auf dem Client, so dass

die Daten ausschließlich auf dem Client entschlüsselt vorliegen.

Darüber hinaus können einzelne Ordner mit anderen BDrive-Teilnehmern geteilt werden.

Außerdem besteht die Möglichkeit Dateien über einen Shared-Link als Download für nicht BDrive-Teilnehmer freizugeben. Bei der Droppad-Funktion besteht die Möglichkeit Dateien in den BDrive-Ordner eines Benutzers hochzuladen. Sowohl bei der Shared-Link als auch bei der Droppad Funktion besteht die Möglichkeit, ein Passwort zu vergeben, um den Zugang zu der jeweiligen Funktion zu beschränken.

Detaillierte Beschreibungen zu den Funktionen sind im Prüfbericht enthalten.

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 Authentifizierung

- Für das Speichern und Teilen von Dateien sowie Ordnern über die BDrive-Dienste ist eine initiale Registrierung bzw. Freigabe der Anwender durch den Administrator (Company Admin) notwendig. Ausgenom-

men davon sind die Droppad Funktion sowie Shared-Link Funktion.

- Die Authentifizierung der bei BDrive registrierten Anwender und deren Geräte erfolgt über starke Authentifizierungsmechanismen unter Verwendung von Zertifikaten. Zusätzlich ist eine Authentifizierung mittels Passwort bei jedem Start des BDrive-Clients notwendig.

2 Zugriffskontrolle

- Der Zugriff auf Daten, welche über die Shared-Link Funktion freigegeben werden können, sowie die Nutzung der Droppad Funktion kann zeitlich begrenzt werden. Nach Ablauf der angegebenen Zeit ist ein Zugriff nicht mehr möglich.
- Anwender eines Unternehmens können nicht auf Daten von Anwendern anderer Unternehmen zugreifen. Ausgenommen ist die explizite Verknüpfung von Unternehmen (Trusted-Company Funktion), welche es erlaubt, Dateien zwischen vorher festgelegten Unternehmen auszutauschen.
- Anwender können Dateien in BDrive-Ordnern miteinander teilen. Hierzu können durch Anwender Zugriffsberechtigungen auf eigene Ordner an weitere Anwender vergeben werden. Anwender ohne Berechtigung können auf diese Ordner nicht zugreifen.
- Schützenswerte Daten, Dienste und Funktionen werden vor unbefugten Zugriffen geschützt.

3 Datensicherheit

- Schützenswerte Dateien werden in einem BDrive-Ordner auf dem IT-System, auf dem die BDrive-Client-Software

installiert ist, abgelegt. Sie sind nur dort unverschlüsselt gespeichert. Vor der Übertragung dieser Dateien an externe Cloud-Speicher wird jede Datei mit einem eigenen Dateischlüssel verschlüsselt, integritätsgeschützt und anschließend in Fragmente zerteilt. Diese verschlüsselten Dateifragmente werden in verschiedenen, externen Cloud-Speichern gespeichert.

- Die Übertragung schützenswerter Dateien sowie der Zugriff auf die BDrive-Dienste erfolgt über gesicherte Verbindungen, welche die Vertraulichkeit und Integrität sicherstellen.

4 Kryptographie

- Zur Authentisierung, Verschlüsselung und Datenübertragung werden kryptographische Algorithmen verwendet, die dem Stand der Technik genügen.

5 Verwaltung von Benutzersitzungen

- Die von den BDrive-Diensten verwendeten sicherheitsrelevanten Sitzungsmerkmale werden sicher generiert und invalidiert, so dass die Vertraulichkeit und Integrität der Sitzungsdaten geschützt werden.

6 Validierung von Ein- und Ausgabedaten

- Alle Ein- und Ausgabedaten werden von den Webschnittstellen der BDrive-Dienste vor der Verarbeitung validiert, so dass keine Daten, die das System schädigen können, verarbeitet und ausgegeben werden.

7 Systemhärtung

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

- Von den eingesetzten Systemen und Anwendungen werden keine vertraulichen Informationen über die interne Struktur und Komponenten preisgegeben.

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