BDRIVE SICHERHEIT
WHITEPAPER

13. Juni 2018

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin

Inhaltsverzeichnis

Aufgrund der besseren Lesbarkeit wird in diesem Text nur die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer mit eingeschlossen.

1. Einleitung

Mit Bdrive, der Cloud-Lösung der Bundesdruckerei, können Sie Daten teilen und gemeinsam bearbeiten – sowohl innerhalb Ihres Unternehmens als auch im Austausch mit Partnern. Dabei bleiben die Daten jederzeit unter Ihrer Kontrolle, weder Dritte noch die Bundesdruckerei als Betreiber von Bdrive können Ihre Daten einsehen oder manipulieren. Die Bundesdruckerei hat bei der Entwicklung von Bdrive sowohl die Sicherheit als auch die Benutzbarkeit in den Mittelpunkt gestellt. In enger Kooperation mit renommierten Forschungseinrichtungen in diesen Bereichen ist es uns gelungen, eine hochsichere Cloud-Lösung zu entwickeln, die sich darüber hinaus einfach in Ihre Unternehmens-IT integrieren lässt.

Als Hochsicherheitsunternehmen mit Staatsaufgaben kennen wir uns nicht nur mit Sicherheitsstandards aus, sondern ebenso mit der Einhaltung rechtlicher Vorschriften im nationalen und internationalen Geschäftsverkehr. Diese Kompetenz spiegelt sich in all unseren Produkten wider. Bdrive ist komplett compliance-sicher.

In diesem Dokument geben wir ausführliche Informationen über die in Bdrive umgesetzten Sicherheitsmaßnahmen und den aktuellen Stand der externen Sicherheitsevaluierungen. Damit können Sie entscheiden, ob unsere Lösung mit den in Ihrem Unternehmen geltenden Sicherheitsrichtlinien kombinierbar und damit einsetzbar ist.

Das Dokument ist in die folgenden Bereiche unterteilt:

- Bdrive Cloud: Kryptographische Verfahren und Protokolle zur Sicherung der in Bdrive freigegebenen Dateien
- Linkshares und Droppads: Kryptographische Verfahren und Protokolle zur Sicherung der via Linkshares und Droppads übertragenen Dateien
- Netzwerksicherheit: Absicherung der Kommunikation zwischen allen Beteiligten inklusive Identitätsmanagement und gegenseitige Authentisierung
- Plattformsicherheit: Maßnahmen zur Absicherung der Plattformen Bdrive und D-Trust
- Sicherheitsmanagement: Vorgehen zur Umsetzung des Informationssicherheitsmanagementsystems
- Sicherheitsevaluierung: Stand der Sicherheitsevaluierung des Gesamtsystems Bdrive (Bdrive Bdrive Client, Bdrive Service, D-Trust und Cloud-Speicher-Services)
- Wissenschaftliche Begleitung: Vorstellung der beteiligten wissenschaftlichen Einrichtungen

2. Bdrive Cloud

Alle in Bdrive genutzten kryptographischen Verfahren werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen (siehe [3] und [4]). Darüber hinaus sind die in Bdrive eingesetzten kryptographischen Verfahren in einem Kryptokonzept beschrieben, das nach Vorgaben des BSI erarbeitet wurde.

Ziel ist es, durch kryptographische Verfahren Ende-zu-Ende-Sicherheit umzusetzen. Ende-zu-Ende-Sicherheit bedeutet, dass weder Dritte noch die Bundesdruckerei als Betreiber von Bdrive Ihre Daten lesen oder manipulieren können. Bdrive sorgt lediglich für das Management der von den Nutzern verwendeten Schlüssel und der verschlüsselten Daten.

Umgesetzt werden die in diesem Abschnitt beschriebenen Sicherheitsfunktionalitäten von der von Bdrive für die Endgeräte der Nutzer bereitgestellte Software Bdrive Client. Diese Software wird zurzeit für das Windows-Betriebssystem bereitgestellt. Ab Sommer 2018 wird auch macOS unterstützt. Versionen für iOS und Android sind in Planung.

2.1 Dateiverschlüsselung und -authentisierung

Dateien werden zusammen mit dem Namen und dem Hashwert der Datei auf dem Endgerät des Nutzers verschlüsselt. Zum Einsatz kommt das Verschlüsselungsverfahren AES im Counter-Mode mit einer Schlüssellänge von 256 Bit. Um auch die Authentizität der Daten zu garantieren, wird aus den verschlüsselten Daten eine Prüfsumme mit dem Verfahren HMAC-Sha256 erzeugt. Auch hier werden Schlüssel der Länge 256 Bit genutzt.

Die eingesetzten Schlüssel werden auf den Endgeräten der Nutzer erzeugt, sind für jede Datei verschieden und werden zusätzlich neu generiert, wenn die Datei aktualisiert wird. Zur Berechnung der Schlüssel wird ein sicherer Zufallszahlengenerator eingesetzt (siehe auch Abschnitt 2.5). Gleiches gilt für die benötigten Initialisierungsvektoren für den genutzten Counter-Mode.

Alle Nutzer von Bdrive besitzen RSA-Schlüsselpaare, mit denen die Schlüssel zur Dateiverschlüsselung und -authentisierung verschlüsselt werden (hier setzen wir RSA-EME-OAEP ein). Die RSA-Schlüsselpaare werden ebenfalls vom Bdrive Client auf Basis des sicheren Zufallszahlengenerators erzeugt und haben eine Länge von 4.096 Bit. RSA-EME-OAEP ist ein probabilistisches Verschlüsselungsverfahren und benötigt daher Zufallswerte, die ebenfalls von dem in Abschnitt 2.5 beschriebenen Zufallszahlengenerator zur Verfügung gestellt werden.

Damit nicht nur die Inhaber der Daten, sondern auch von ihnen autorisierte Personen auf diese Daten zugreifen können, werden die Dateiverschlüsselungs- und -authentisierungsschlüssel zusätzlich auch mit den öffentlichen RSA-Schlüsseln dieser Personen verschlüsselt.

Um sicherzustellen, dass die Schlüssel für Dateiverschlüsselung und -authentisierung tatsachlich nur autorisierten Personen zugänglich sind, erhalten alle in Bdrive genutzten öffentlichen RSA-Schlüssel ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (siehe Abschnitt 5.1). Damit ist es möglich, die öffentlichen RSA-Schlüssel eindeutig dem Schlüsselinhaber zuzuordnen.

Die AES- und HMAC-Schlüssel können also nur von denjenigen Personen entschlüsselt werden, die dafür von den Inhabern der Daten autorisiert wurden. Damit ist auch eine Entschlüsselung der Dateien nur für diese Personen möglich. Das heißt, dass selbst die Bundesdruckerei als Betreiber von Bdrive keinen Zugang zu den entschlüsselten Dateien hat.

2.2 Verfügbarkeit der Daten

Bei der Nutzung nur eines Cloud-Speicherdienstes kann es zu einem Verlust der Verfügbarkeit kommen, wenn dieser Dienst ausfällt. Um eine sehr hohe Verfügbarkeit zu gewährleisten, nutzt Bdrive daher mehrere unabhängige Cloud-Speicherdienste, um Ihre Daten bereitzustellen.

Die verschlüsselten Daten werden zusammen mit der Prüfsumme mittels eines Erasure-Coding-Verfahrens in mehrere Fragmente zerteilt, so dass nur wenige Fragmente für eine Wiederherstellung ausreichend sind. Beispielsweise können vier Fragmente so erzeugt werden, dass nur zwei Fragmente benötigt werden, um die verschlüsselte Datei inklusive Prüfsumme zu rekonstruieren.

Die erzeugten Fragmente werden auf unabhängige Cloud-Speicherdienste hochgeladen. Fällt einer (oder mehrere) dieser Dienste aus, ist die Datei trotz der dann fehlenden Fragmente wiederherstellbar. Die Anzahl der erzeugten Fragmente kann, abhängig von ihren benötigten Verfügbarkeitsanforderungen, angepasst werden.

Allein die Verfügbarkeit der verschlüsselten Dateifragmente umzusetzen, reicht nicht aus. So können bei Abhandenkommen des Schlüsselpaars zur Ver- und Entschlüsselung der symmetrischen Schlüssel die entsprechenden Daten nicht mehr entschlüsselt werden. Um die Verfügbarkeitsanforderungen umzusetzen, erzeugt jede teilnehmende Institution ein Schlüsselpaar und lässt den öffentlichen Schlüssel ebenfalls, wie bei den regulären Schlüsselpaaren der Nutzer, zertifizieren. Die jeweiligen symmetrischen Schlüssel zum Verschlüsseln von Daten der Mitarbeiter des Unternehmens werden zusätzlich auch mit dem öffentlichen Unternehmensschlüssel (Master Key) verschlüsselt.

Dieser private Schlüssel muss entsprechend geschützt werden. Wir empfehlen die Verwendung des Shamir Secret-Sharing-Verfahrens, um Schlüsselteile auf vier Personen zu übertragen, von denen zwei den geheimen Unternehmensschlüssel zusammensetzen können (Vier-Augen-Prinzip). Die vier Schlüsselteile sollten auf externen Speicherbereichen (z.B. USB-Sticks) abgelegt und sicher hinterlegt werden.

Darüber hinaus muss auch die Verfügbarkeit der Metadaten gewährleistet sein (siehe hierzu Abschnitt 2.3).

2.3 Absicherung der Metadaten von Dateien

Um das Management der Dateien auf der Seite von Bdrive zu gewährleisten, werden Informationen über die Fragmente der Dateien zentral in Bdrive gespeichert. Diese Informationen, auch Metadaten genannt, werden auf den Endgeräten der Nutzer erzeugt und bestehen aus:

- Größe in Bytes (Ausgangsdatei, verschlüsselte Datei, Fragmente)
- lokale Ordnerstruktur über Ordner- und Datei-IDs
- Änderungszeitstempel
- Sha256-Checksumme der Fragmente der verschlüsselten Datei
- Parameter des Erasure Coding
- Speicherkoordinaten in den Cloud-Speicherdiensten

- Verschlüsselte symmetrische Schlüssel (für alle autorisierten Nutzer) mit entsprechenden Nutzer-IDs
- Initialisierungsvektor

Die Metadaten enthalten keinerlei Informationen über den Inhalt der Datei (weder den Namen der Datei und der Ordner und Unterordner, aus denen sich eventuell Rückschlüsse auf den Dateiinhalt schließen ließen). Ordner- und Datei-IDs sind Werte, die bei der Erstellung der Datei zufällig vergeben werden. Nutzer-IDs werden im Rahmen der Registrierung für den Dienst Bdrive vergeben und identifizieren die Nutzer eindeutig.

Nach der Erzeugung der Metadaten auf den Endgeräten der Nutzer werden diese TLS-gesichert (es findet immer eine gegenseitige Authentisierung statt, siehe auch Abschnitt 5.2) in die sichere Umgebung des Bdrive Services hochgeladen und dort verschlüsselt und integritätsgesichert in Datenbanken gespeichert. Um auch die Verfügbarkeit der Daten zu gewährleisten, werden zwei redundante Datenbanken genutzt. Die Inhalte der Datenbanken werden zusätzlich täglich auf unabhängigen Speichermedien gespeichert.

2.4 Sichere Schlüssellöschung und -speicherung

Flüchtige Schlüssel, wie z.B. die für die Verschlüsselung der Dateien, deren Namen und Hashwerte benötigten symmetrischen Schlüssel, werden sofort nach ihrer Verwendung im Bdrive Client gelöscht. Das gleiche gilt für die für den Aufbau der TLS-Verbindung verwendeten geheimen Parameter und Schlüssel.

Im Bdrive Client müssen aber nichtflüchtige Geheimnisse sicher gespeichert werden. Diese sind:

- Der interne Zustand des deterministischen Zufallszahlengenerators
- Der private Schlüssel des RSA-Schlüsselpaars zur Ver- und Entschlüsselung der symmetrischen Schlüssel (siehe Abschnitt 2.1)
- Der private Schlüssel des RSA-Schlüsselpaars zur Authentisierung der Nutzer[1] (siehe Abschnitt 5.3).

Die sichere (d.h. verschlüsselte und integritätsgesicherte) Speicherung dieser Geheimnisse basiert auf einem Passwort. Bei der Verwendung von Authentisierungzertifikaten müssen Nutzer ein Gerätepasswort für die Verwendung des Bdrive-Clients vergeben. Im Fall der Nutzung der GoID Card setzt sich das Passwort aus zwei Teilen zusammen: Ein Teil wird auf dem Endgerät der Nutzer gespeichert. Der zweite Teil wird sicher im Bdrive Service gespeichert und nach der erfolgreichen Anmeldung der Nutzer über die etablierte TLS-Verbindung an den Bdrive Client übertragen.

Für die Verschlüsselung dieser Geheimnisse wird das Password-based Encryption Scheme 2 (PBEC2) und für die Authentisierung der Schlüssel das Password-based MAC 1 (PBMAC1) eingesetzt (siehe [6]). In beiden Fällen wird aus dem Passwort und einem Salt zunächst ein Schlüssel mittels einer sogenannten Key Derivation Function (wir nutzen PBKDF2 ebenfalls aus [6]) der Länge 256) abgeleitet. Wir nutzen für die Ableitung des Schlüssels innerhalb der Key Derivation

[1] Bdrive ermöglicht auch die Nutzung der von der bdr ausgegebenen GoID Card für die Authentisierung gegenüber Bdrive. In diesem Fall werden keine Authentisierungszertifikate benötigt.

Function 100.000 Iterationen. Dies macht Brute-Force-Angriffe auf das Gerätepasswort praktisch unmöglich.

Die Salts sind jeweils verschieden (d.h. verschiedene Salts zur Erzeugung der Verschlüsselungsschlüssel und der Authentisierungsschlüssel), haben eine Länge von 100 Bit und werden (einmalig) zufällig vom in Abschnitt 2.5 beschriebenen Zufallszahlengenerator gewählt.

2.5 Zufallszahlengeneratoren

Die Sicherheit der genutzten kryptographischen Verfahren und Protokolle hängt maßgeblich von der Entropie (einfach gesprochen von der Unvorhersagbarkeit) der eingesetzten Schlüssel und der weiteren kryptographischen Parameter ab. Bdrive nutzt zur Erzeugung dieser Werte Zufallszahlengeneratoren, die von offiziellen Stellen, wie z.B. dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem National Institut for Standard and Technology (NIST) für den Einsatz in hochsensiblen Bereichen empfohlen werden.

Für die Erzeugung der benötigten Zufallswerte wird der deterministische Zufallszahlengenerator (Deterministic Random Number Generator, DRNG) HMAC-DRNG aus [7] genutzt. Die genutzte Funktion HMAC basiert auf Sha256. DRNGs benötigen einen sogenannten Seed, aus denen sie Zufallswerte berechnen können. Dieser muss, um eine hohe Entropie der ausgegebenen Zufallswerte zu erhalten, ebenfalls eine hohe Entropie aufweisen.

Zur Erzeugung des Seed nutzt der Bdrive Client verschiedene Werte: Nutzerinteraktionen (z.B. Zeitpunkte bei verschiedenen Aktionen und zwischen Tastaturanschlägen, Mauspositionen, Systemzustände, Netzwerkverkehr usw.). Die Güte dieser Zufallswerte wird in der externen Sicherheitsevaluierung nachgewiesen.

Der Bdrive Service nutzt einen physikalischen Zufallszahlengenerator zur Erzeugung der Seeds, der vom BSI für diesen Einsatzzweck hinsichtlich Sicherheit analysiert und zertifiziert wurde.

3. Linkshares und Droppads

Mit Bdrive können nicht nur Dateien innerhalb und zwischen Mitarbeitern von Unternehmen, die unseren Service nutzen, sicher ausgetauscht werden, sondern auch Personen nicht beteiligter Unternehmen sicher Dateien zur Verfügung gestellt (über Linkshares) oder von diesen sicher übermittelt werden (über Droppads).

3.1 Linkshares

Mit Linkshares können auch Dateien an Personen sicher übertragen werden, deren Unternehmen nicht an Bdrive beteiligt sind. Hierzu muss zunächst ein Passwort gewählt werden, aus dem ein Verschlüsselungs- und ein Authentisierungsschlüssel abgeleitet wird.

Die Datei wird dann mit diesen Schlüsseln verschlüsselt und authentisiert und die verschlüsselte Datei zusammen mit einem Initialisierungsvektor, der Prüfsumme und einem Salt-Wert sicher in der Bdrive Cloud abgelegt. Die Empfänger der Datei erhalten einen Link, mit dem diese Daten heruntergeladen werden können. Die Verbindung zwischen Browser und Bdrive Cloud ist TLS-gesichert. Mittels des Passwortes kann die Datei dann entschlüsselt und deren Authentizität geprüft werden. Dabei findet die Entschlüsselung und Prüfung der Authentisierung vollständig im Browser statt.

Auch hier verwenden wir AES im Counter-Mode für die Verschlüsselung und HMAC-Sha256 für die Datenauthentisierung. Beide Schlüssel haben eine Länge von 256 Bit und werden mittels der Key Derivation Function PBKDF2 aus [6] mit zusätzlichem Salt aus dem gewählten Passwort abgeleitet. Um Brute-Force-Angriffe praktisch zu verhindern, nutzen wir 100.000 Iterationen innerhalb der Key Derivation Function. Alle benötigten Zufallswerte (Initialisierungsvektor und die beiden Salt-Werte) werden mit dem in Abschnitt 2.5 beschriebenen Zufallszahlengenerator erzeugt.

Das Passwort kann über einen sicheren Weg (z.B. sichere Instant Messengers wie Telegram oder Signal) übertragen werden.

3.2 Droppads

Eine weitere Funktionalität sind Droppads, mit denen auch Personen nicht an Bdrive beteiligter Unternehmen sicher Daten an Bdrive Nutzer übermitteln können. Hierfür werden die Dateien auf Basis der für Bdrive Kunden ausgestellten Verschlüsselungszertifikate gesichert.

Im Browser der Nutzer werden zwei Schlüssel (zur Verschlüsselung und Authentisierung der Datei) sowie der Initialisierungsvektor für die Verschlüsselung generiert. Beide Schlüssel werden mit dem im Verschlüsselungszertifikat enthaltenen öffentlichen Schlüssel verschlüsselt und alle Daten (verschlüsselte Datei, Prüfsumme, verschlüsselte Schlüssel und Initialisierungsvektor) sicher in die Bdrive Cloud hochgeladen. Die Datei erscheint dann im Droppads-Ordner der Bdrive Nutzer.

Verschlüsselung und Authentisierung der Datei erfolgen wieder mittels der Verfahren AES im Counter-Mode und HMAC-Sha256. Für die Verschlüsselung der beiden benötigten Schlüssel nutzen wir, wie schon in Abschnitt 2.1, das asymmetrische Verschlüsselungsverfahren RSA-EME-OAEP.

4. Netzwerksicherheit

Für eine sichere Umsetzung des Bdrive Dienstes müssen nicht nur die einzelnen Systeme, wie z.B. Bdrive Client, Bdrive Service, Zertifizierungsdiensteanbieter und Cloud-Services, abgesichert sein, sondern im besonderen Maße auch die Kommunikation zwischen den einzelnen Systemen. Hierzu gehört neben der Verschlüsselung der Kommunikation über TLS auch die Authentisierung der Kommunikationspartner.

4.1 Identitätsmanagement

Grundlage für den sicheren Austausch von Daten ist, dass sich die Kommunikationspartner jederzeit sicher sein müssen, mit wem sie die Daten teilen. Um diese Anforderung in Bdrive umzusetzen, erhalten alle Nutzer Authentisierungs- und Verschlüsselungszertifikate. In den Zertifikaten sind neben den öffentlichen Schlüsseln der Nutzer auch der Name, das Unternehmen, die Nutzer-ID und die ausstellende Certification Authority enthalten.

Authentisierungszertifikate werden genutzt, um sich gegenüber Bdrive zu authentisieren (siehe auch Abschnitt 5.3). Verschlüsselungszertifikate dienen dazu, die symmetrischen Schlüssel zur Dateiverschlüsselung und -authentisierung für Personen, die Zugriff auf diese Dateien erhalten sollen, zu verschlüsseln (siehe Abschnitt 2.1).

An das Ausstellen dieser Zertifikate müssen also hohe Sicherheitsanforderungen gestellt werden. Alle Zertifikate werden von D-Trust, einem etablierten und sicheren Zertifizierungsdiensteanbieter (siehe auch Abschnitt 8.3) ausgestellt. Damit die Zertifikate auch den Nutzern zugeordnet werden können, müssen diese im Rahmen des Ausstellungsprozesses eindeutig identifiziert werden. Diese Aufgabe übernimmt das jeweilige Unternehmen, bei dem die Nutzer angestellt sind.

4.2 Sichere Kommunikationskanale

Zur Umsetzung der Schutzziele Vertraulichkeit und Authentizitat während der Übersendung der Metadaten zwischen Nutzern und Bdrive werden diese mittels Transport Layer Security (TLS) gesichert. Die Daten werden also sowohl verschlüsselt als auch authentisiert. Zum Einsatz kommt die Cipher-Suite DHE RSA WITH AES 256 CBC SHA256.

Beide Kommunikationspartner müssen sich im Rahmen des Aufbaus der TLS-Verbindung authentisieren. Bdrive authentisiert sich gegenüber der Nutzer über Server-Authentisierungszertifikate, die ebenfalls von D-Trust ausgestellt werden. Nutzer haben mehrere Möglichkeiten, sich gegenüber Bdrive zu authentisieren (siehe Abschnitt 5.3).

4.3 Nutzerauthentisierung

Bdrive authentisiert sich gegenüber den Nutzern mittels Server- Authentisierungszertifikate. Zur Authentisierung von Nutzer gegenüber Bdrive sind derzeit zwei Möglichkeiten vorgesehen:

- Mittels des ausgestellten Authentisierungszertifikats
- Mittels der von der Bundesdruckerei ausgestellten GoID Card

Unternehmen können selbst entscheiden, welches Authentisierungsverfahren sie für den Bdrive Service nutzen wollen und so das eingesetzte Verfahren an ihr benötigtes Sicherheitsniveau anpassen.

5. Plattformsicherheit

Bdrive verarbeitet die Metadaten der Dateifragmente, aus denen sich zwar keine Ruckschlüsse auf die Dateiinhalte, aber darauf, welche Nutzer zusammen an den Dateien arbeiten, ziehen lassen. Diese Informationen müssen also hinsichtlich Vertraulichkeit geschützt werden. Darüber hinaus muss die Plattform auch sicherstellen, dass die Metadaten nicht unbemerkt manipuliert (Schutzziel Authentizität) oder gelöscht (Schutzziel Verfügbarkeit) werden können.

Ein weiteres wichtiges Element von Bdrive ist das Identitätsmanagement. Nutzer müssen sich zu jeder Zeit sicher sein, mit wem sie ihre Daten austauschen. Daher ist die Plattform des Zertifizierungsdiensteanbieters D-Trust entsprechend geschützt, um zu verhindern, dass Angreifer durch Eindringen in das System Authentisierungs- und Verschlüsselungszertifikate fälschen können.

5.1 Intrusion Detection und Prevention

Bdrive und D-Trust nutzen Virenscanner und Firewalls verschiedener Anbieter, um sich vor Angriffen von außen zu schützen. Virensignaturen und Konfigurationen werden regelmäßig aktualisiert und an die aktuelle Sicherheitslage angepasst.

Diese Maßnahmen allein reichen nicht aus, um die Plattform entsprechend zu schützen. So werden z. B. sogenannte Zero-Day Exploits (Sicherheitslücken, die bisher nicht bekannt waren) hierdurch nicht erkannt. Um auch auf aktuelle Angriffe reagieren zu können, haben wir in allen Plattformen verschiedene Intrusion-Detection- und Intrusion-Prevention-Systeme implementiert, die Angriffe über Anomalieerkennung detektieren können und entsprechende Gegenmaßnahmen einleiten.

Zusätzlich werden alle Aktivitäten erfasst und gespeichert und regelmäßig von unseren Sicherheitsexperten mit Hilfe etablierter Tools hinsichtlich Auffälligkeiten untersucht, sodass auch eine manuelle Überprüfung der Sicherheit des Systems gewährleistet ist.

5.2 Softwarequalität und Penetrationstest

Bei der Entwicklung von Software legen wir großen Wert auf deren Qualität, um Sicherheitslücken, die sich aus Softwarefehlern ergeben, zu minimieren. Unsere Software muss vor Einsatz in das bestehende System mehrere Qualitätssicherungstests durchlaufen.

Besonderen Wert legen wir hier auf die Verhinderung von Angriffen durch Code Injection. Alle Eingabefelder sind klar spezifiziert und werden nur dann vom System weiterverarbeitet, wenn die Inhalte der Spezifikation entsprechen. So verhindern wir, dass über solche Eingabefelder Schadsoftware in das System eingespielt und die Sicherheit gefährdet wird.

Aber selbst mit intensiven Tests und klaren Spezifikationen können Fehler nicht vollständig ausgeschlossen werden. Aus diesem Grund lassen wir regelmäßig Penetrationstests durchführen, um Sicherheitslücken frühzeitig erkennen und beheben zu können.

5.3 Hosting

Alle benötigten IT-Komponenten (Server, Datenbanken) sind in speziell abgesicherten Bereichen innerhalb der D-Trust untergebracht. Zugang zu den Räumlichkeiten haben nur die Administratoren von Bdrive nach dem Vier-Augen-Prinzip, d.h. es müssen sich zwei Personen mittels personalisierter Chipkarten und PIN gegenüber den gesicherten Türen authentisieren, um Zutritt zu erhalten. Jeder Zutritt wird revisionssicher protokolliert und regelmäßig vom Sicherheitsteam von Bdrive analysiert.

Die Räumlichkeiten (Türen und Fenster) sind mit Alarmanlagen ausgestattet, sodass Einbrüche zu jeder Zeit erkannt und an das zuständige Sicherheitsteam weitergeleitet werden.

6. Sicherheitsmanagement

Neben dem Einsatz kryptographischer Algorithmen zur Absicherung der Daten müssen auch weitere technische sowie organisatorische und personelle Maßnahmen für den sicheren Betrieb von Bdrive umgesetzt werden.

Die notwendigen Sicherheitsmaßnahmen werden nicht nur von unseren kompetenten Mitarbeitern mit Unterstützung renommierter Forschungseinrichtungen entwickelt und umgesetzt, sondern auch extern auf Vollständigkeit und Wirksamkeit evaluiert (siehe hierzu Abschnitt 7).

Die Erarbeitung der notwendigen umzusetzenden Sicherheitsmaßnahmen erfolgt nach etablierten Vorgehensmodellen. Hierzu gehören neben der Umsetzung aktueller Sicherheitsmaßnahmen auch Aktivitäten zur Aufrechterhaltung im laufenden Betrieb (z. B. Notfallmanagement, Vorgehen bei Sicherheitsvorfällen und Anpassungen der Maßnahmen hinsichtlich der aktuellen Sicherheitslage).

6.1 Sicherheitsteam

Unser Sicherheitsteam besteht aus einem Informationssicherheitsbeauftragten und mehreren Sicherheitsexperten. Aufgaben des Sicherheitsteams sind, neben der Erarbeitung personeller, organisatorischer, technischer und infrastruktureller Sicherheitsmaßnahmen, auch die Umsetzung dieser Maßnahmen und die Aufrechterhaltung im laufenden Betrieb. Hierfür müssen nicht nur alle Mitarbeiter regelmäßig geschult werden, sondern auch Anpassungen an die aktuelle Sicherheitslage vorgenommen und auf eventuell auftretende Sicherheitsvorfälle reagiert werden.

Die Sicherheit von Bdrive wird laufend verbessert. Dabei unterstützen uns renommierte Forschungseinrichtungen, wie das Hasso-Plattner-Institut der Universität Potsdam und die Arbeitsgruppe Identitätsmanagement der Freien Universität Berlin.

6.2 Zuverlässigkeitsüberprüfungen bei Mitarbeitern

Alle Mitarbeiter werden vor Einstellung hinsichtlich ihrer Qualifikation für die von ihnen verantworteten Aufgaben eingehend untersucht.
Dabei prüfen wir die Ausbildung und vorhergehende Anstellungen an Hand von Ausbildungs- und Arbeitszeugnissen. Personen, die in hochsensiblen Bereichen eingesetzt werden, müssen zudem ein polizeiliches Führungszeugnis vorlegen.

6.3 Sicherheitsschulungen

Die Bundesdruckerei führt regelmäßig Sicherheitsschulungen durch, um für das Thema IT-Sicherheit und Datenschutz zu sensibilisieren. Schulungen sind nicht nur für das technische Personal (z.B. Systemadministratoren und Entwickler) verpflichtend, sondern auch für die Mitarbeiter der Verwaltung und werden an die jeweiligen Zielgruppen angepasst. In den Schulungen werden alle relevanten Themen der IT-Sicherheit und des Datenschutzes, von aktuellen Bedrohungen über Vorgehen von Angreifern (auch Social Engineering), Folgen erfolgreicher Angriffe und Methoden zur Risikominimierung behandelt.

Darüber hinaus laden wir im Rahmen unserer jährlich stattfindenden Campus-Week renommierte Forscher ein, die über aktuelle Themen aus ihren Arbeiten vortragen und deren Ergebnisse mit uns diskutieren. So erhalten wir Einblick in innovative Technologien und können unsere Lösung laufend verbessern.

6.4 Schwachstellenmanagement und Vorgehen bei Sicherheitsvorfällen

Software kann Fehler haben. Einige dieser Fehler können auch zu Sicherheitslücken führen. Das gleiche gilt für alle umgesetzten Sicherheitsmaßnahmen, seien sie personeller, organisatorischer, technischer oder infrastruktureller Natur. Trotz Evaluierung dieser Maßnahmen hinsichtlich Sicherheit können sich Sicherheitslücken ergeben, die im Rahmen der Evaluierung nicht erkannt wurden.

Unser Sicherheitsteam prüft daher regelmäßig die Wirksamkeit der umgesetzten Maßnahmen, auch indem wir eigene Angriffe simulieren (Hacking, aber auch z.B. Phishing-Angriffe) und so die Wirksamkeit unserer Sicherheitsmaßnahmen und Sicherheitsschulungen testen.

Sollten sich Sicherheitslücken zeigen, z.B. durch eigene Beobachtungen oder aus tatsächlichen Angriffen, sind wir hierauf vorbereitet. Unser Sicherheitsteam hat bereits mögliche Angriffsszenarien durchgespielt und entsprechende Gegenmaßnahmen vorbereitet. Diese können von kurzfristiger Abschaltung sicherheitskritischer Dienste bis hin zur Abschaltung von Bdrive führen, bis die Sicherheit wieder hergestellt ist.

Darüber hinaus beobachten wir regelmäßig die aktuelle Sicherheitslage und informieren uns, z. B. über das Computer Emergency Response Team des Bundesamtes für Sicherheit in der Informationstechnik über aktuelle Sicherheitslücken und Angriffe und leiten entsprechende Gegenmaßnahmen ein.

7. Sicherheitsevaluierung

Alle Bestandteile der Bdrive Infrastruktur sind nach etablierten Vorgehensmodellen evaluiert und zertifiziert. Dabei wird nicht nur überprüft, ob für alle Sicherheitsrisiken entsprechende Sicherheitsmaßnahmen umgesetzt sind, sondern auch, wie wirksam diese Maßnahmen sind (d. h. ob sie die Risiken geeignet minimieren). Diese Evaluierung bezieht sich sowohl auf den aktuellen Stand der Umsetzung als auch darauf, ob geeignet auf Sicherheitsvorfälle oder aktuelle Entwicklungen hinsichtlich Angriffe reagiert werden kann.

7.1 Bdrive Client

Der Bdrive Client ist eine Software, mit der Nutzer Bdrive verwenden können. Diese Software setzt wesentliche Sicherheitsfunktionalitäten um, wie z. B. Schlüsselgenerierung, Ver- und Entschlüsselung, Authentisierung der Dateien usw. Hierfür streben wir eine Zertifizierung nach Common Criteria EAL 4 an.

EAL steht für Evaluation Assurance Level, also die umgesetzte Vertrauenswürdigkeitsstufe. EAL 4 bedeutet dabei, dass die App methodisch entwickelt, getestet und durchgesehen wird und damit die behauptete Sicherheitsfunktionalität mit sehr hoher Wahrscheinlichkeit erfüllt.

7.2 Bdrive Service

Die Bundesdruckerei strebt für das Gesamtsystem Bdrive eine Zertifizierung nach SEAL-3 (Sicherheitstechnische Qualifizierung, Security Assurance Level 3) an. Geplant ist der Abschluss der Zertifizierung Ende 2018, die danach regelmäßig für neue Releases wiederholt wird.

Die Zertifizierung wird von der TüV Informationstechnik GmbH durchgeführt.

7.3 Zertifizierungsdiensteanbieter

Die in Bdrive genutzten Zertifikate sind der Sicherheitsanker für den sicheren Datenaustausch. Alle Zertifikate werden vom Zertifizierungsdiensteanbieter D-Trust ausgestellt. D-Trust ist eine einhundertprozentige Tochter der Bundesdruckerei und seit vielen Jahren etabliert in diesem Bereich. So stellt D-Trust fortgeschrittene und qualifizierte Zertifikate nach dem deutschen Signaturgesetz aus. Hierfür werden alle Prozesse zum Ausstellen von Zertifikaten sicherheitsevaluiert und die Evaluierung von der Bundesnetzagentur auf Basis eines BSI-Zertifikats bestätigt.

7.4 Cloud Services

Bdrive arbeitet ausschließlich mit unabhängigen und ISO-zertifizierten Anbietern von Cloud-Speichern zusammen, deren Rechenzentren in Deutschland betrieben werden. Das bedeutet: Die Daten – oder besser, die verschlüsselten und authentisierten Datenfragmente – liegen ausschließlich auf deutschen Servern.

8. Wissenschaftliche Begleitung

Bdrive wird ständig weiterentwickelt und hinsichtlich Sicherheit untersucht. Dabei unterstützen uns zwei renommierte Forschungseinrichtungen: die Arbeitsgruppe ID-Management an der Freien Universität Berlin unter Leitung von Prof. Dr. Margraf und das Hasso-Plattner-Institut an der Universität Potsdam unter Leitung von Prof. Dr. Meinel.

8.1 AG ID-Management der Freie Universität Berlin

Die Arbeitsgruppe ID-Management an der Freien Universität Berlin beschäftigt sich mit dem Entwurf, der Erstellung und Bewertung benutzbarer und sicherer Software und IT-Systeme. Die Forschungsschwerpunkte der Arbeitsgruppe sind: Physical Unclonable Functions, Kryptoanalyse, Usable Security, IT-Sicherheitsmanagement sowie Security Management as a Service.

8.2 Hasso-Plattner-Institut

Das Hasso-Plattner-Institut (HPI) ist einmalig in der deutschen Universitätslandschaft: Es bietet die einzigartigen praxis- und innovationsorientierten Studiengänge IT-Systems Engineering mit den Abschlüssen Bachelor bzw. Master of Science sowie ein Zusatzstudium in der Innovationsmethode Design Thinking. Akademisch verfasst als eigenständige Digital-Engineering-Fakultät der Universität Potsdam vereint das HPI exzellente Forschung und Lehre genauso wie die Vorteile eines privatfinanzierten Instituts und einem gebührenfreien Studium.

Glossar

AES: Symmetrischer Verschlüsselungsalgorithmus, der in Bdrive zur Verschlüsselung von Dateien und Metadaten genutzt wird

Authentisierungszertifikat: von einer CA ausgestelltes Zertifikat, das mit einem asymmetrischen Schlüsselpaar zur Authentisierung verknüpft ist

Bdrive Cloud: die in Bdrive genutzte Infrastruktur zur sicheren Speicherung von Dateien und Metadaten

Bdrive Client: Software, die ein Company-Administrator bzw. ein Bdrive Nutzer auf einem Endgerät installiert und die von diesen als clientseitige Schnittstelle zum Dienst Bdrive genutzt wird

Bdrive Kunde: Unternehmen, das mit dem Dienst Bdrive einen Vertrag zur Nutzung des Dienstes abgeschlossen hat

Bdrive Nutzer: Mitarbeiter eines Bdrive Kunden, der den Dienst Bdrive nutzt und sich zu diesem Zweck beim Dienst registriert hat

Certification Authority (CA): vertrauenswürdige Instanz, die Zertifikate herausgibt, mit denen die Bindung zwischen kryptographischen Schlüsseln und Schlüsselinhaber geprüft werden kann

Droppads: verschlüsselte Dateien, die von Mitarbeitern nicht beteiligter Unternehmen an Bdrive Kunden übermittelt werden können

GoID Card: von der Bundesdruckerei herausgegebener Identitätsnachweis für Mitarbeiter eines Unternehmens, der es erlaubt, den Karteninhaber sicher zu identifizieren

Linkshares: verschlüsselte Dateien, die von Bdrive Kunden auch an Mitarbeiter nicht beteiligter Unternehmen übermittelt werden können

MAC/HMAC: Verfahren zur Authentisierung von Daten

Neuer Personalausweis: Identitätsnachweis für deutsche Staatsangehörige, der es erlaubt, den Ausweisinhaber sicherer zu identifizieren und der für Online-Dienstleistungen verwendet werden kann (Nutzung der Online-Ausweisfunktion)

RSA: asymmetrisches Verschlüsselungsverfahren, mit dem in Bdrive symmetrische Verschlüsselungs- und Authentisierungsschlüssel verschlüsselt werden

Transport Layer Security (TLS): hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet

Verschlüsselungszertifikat: von einer CA ausgestelltes Zertifikat, das mit einem asymmetrischen Schlüsselpaar zum Verschlüsseln von Daten verknüpft ist

Zertifikat: digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann

Literatur

[1] T. Bray: *The JavaScript Object Notation (JSON) Data Interchange Format*, Request for Comments (RFC): 7159.

[2] BSI: *IT-Grundschutzkataloge*, Bundesamt für Sicherheit in der Informationstechnik.

[3] BSI: *TR 02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen*, Version 2016-01, 15. Februar 2016, Bundesamt für Sicherheit in der Informationstechnik.

[4] BSI: *TR 02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 - Verwendung von Transport Layer Security (TLS)*, Version 2016-01, Bundesamt für Sicherheit in der Informationstechnik.

[5] D. Hardt: *The OAuth 2.0 Authorization Framework*, Internet Engineering Task Force (IETF), Request for Comments (RFC): 6749

[6] B. Kaliski: *PKCS#5: Password-Based Cryptography Specification Version 2.0*, Request for Comments (RFC): 2898.

[7] NIST *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Special Publication 800-90A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 01/2012

[8] FIPS: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4