BKT-001 – Digitale Identitäten

Überprüfte Komponenten

MODUL	KOMPONENTE
BASIS-ID	SSI Issuer
	Aries Agent
	Tails Server
CHECK-IN	Aries Agent
	Hotel Frontend
	Hotel Controller
	Database
	Integration Service
WALLET	Mediation Agent
	Wallet-App

Vorgehen der Sicherheitsüberprüfung

Die durchgeführte Sicherheitsüberprüfung orientiert sich an etablierten Standards, wie z.B. von OWASP, dem BSI oder dem CIS. In der Durchführungsphase wird das Zielsystem in einzelne Kern- und Funktionskomponenten gegliedert, die iterativ sowohl einzeln als auch im Gesamtkontext des Zielsystems auf Sicherheitslücken untersucht werden.

Hierbei hat die SSE die Mobile Anwendung „Wallet-App“ sowie die Web Anwendung „Hotel Frontend“ in einem ersten Schritt betrachtet und Penetrationstests vorgenommen, um ein Verständnis der Funktionsweise der Anwendung aus Sicht eines Benutzers zu gewinnen.

Im weiteren Verlauf wurde der Fluss der Daten innerhalb der Anwendung nachvollzogen und gezielt die Verarbeitung an den einzelnen Komponenten betrachtet.

Identifizierte Schwachstellen

Risiko	Beschreibung
Mittel	Keine Verifikation der Hotel Endpunkte. Ein Angreifer kann durch eine eigenen Endpunkt Daten eines sich registrierenden Benutzers erlangen. Die Überprüfung ist derzeit durch eine einfache Anzeige der URL dem Benutzer überlassen. Da ein Benutzer hier aber keinen Vergleich zu einer korrekten URL hat, kann diese nur schwer von einem Benutzer überprüft werden.
Niedrig	Durch eine Informationen Disclosure durch die eingesetzte Ausweis2-SDK liegen Informationen zu Zugriffen zu Endpunkten nach einem Crash der Applikation auf dem Endgerät.
Info	Die Hyperledger Infrastruktur sollte von außen nicht Zugreifbar sein, bzw. ein Zugriff nur durch Allowlist für die einzelnen Beteiligten Unternehmen (Hotels und Unternehmen) erfolgen.

Die gezeigten Schwachstellen und ihr Risiko Status sind vorläufig zu betrachten. Im Laufe der Berichterstellung können Schwachstellen neu bewertet werden, oder weitere Hinzukommen. Hierbei handelt es sich dann meistens um Mittlere und Niedrigere Schwachstellen, oder Informationelle Empfehlungen, um die Sicherheit zu verbessern.