Anlage 4

Datensicherheitskonzept

Einleitung

Die Softwarelösung PrivacyPilot wird auf Basis der LowCode-Plattform OutSystems (www.outsystems.com/de-de/company/) realisiert, welche in einem Hochsicherheitsrechenzentrum gehostet wird.

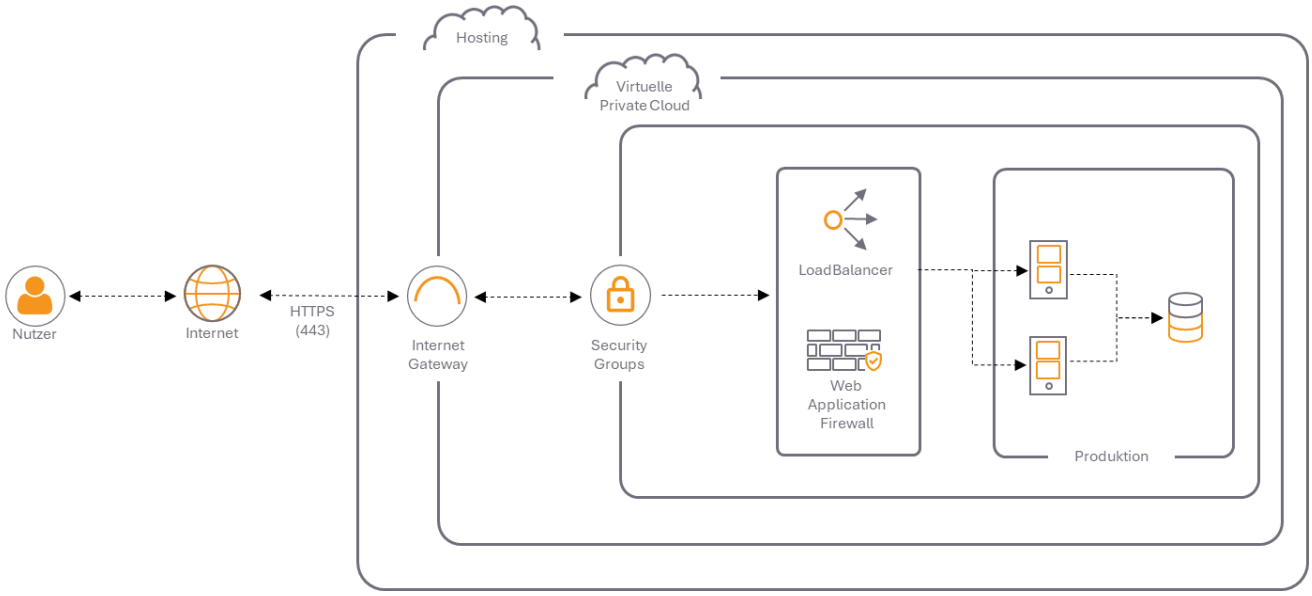
1. Plattformbetrieb

Outsystems ist als Platform-as-a-Service-Betreiber umfassend zertifiziert, unter anderem nach

- ISO 27001 (Sicherheitsstandard für Informationssicherheit),
- ISO 27017 (Sicherheitsstandard für Cloud Service Provider),
- ISO 9001 (Standard für das Qualitätsmanagement),
- SOC 2 (Kriterienkatalog für die sichere Serviceerbringung der AICPA[1]) und
- CSA STAR (Sicherheits- und Datenschutzkontrollen nach CSA STAR[2]).

Alle Zertifikate und Sicherheitsmaßnahmen können im OutSytems Trust Center (https://security.outsystems.com) nachvollzogen werden.

Der PrivacyPilot ist auf einer dedizierten, virtuellen Infrastruktur errichtet und ist als Virtual Private Cloud logisch vom Internet und anderen Netzwerken isoliert. Übergabepunkte zum Internet werden durch verschiedene technische Sicherheitsmaßnahmen wie Web Application Firewalls und Verschlüsselungen überwacht und abgesichert:



[1] American Institute of Certified Public Accountants.
[2] Security, Trust, Assurance and Risk der Cloud Security Alliance.

OutSystems als Plattformbetreiber ergreift unterschiedliche technische und organisatorische Maßnahmen für ein hohes Maß an Verfügbarkeit, Integrität und Vertraulichkeit, wie beispielsweise:

- Physische Anlagen von OutSystems werden durch technische Maßnahmen wie Videoüberwachungsanlagen sowie durch organisatorische Maßnahmen wie Sicherheitspersonal überwacht. Der Zugang zu den Anlagen ist nur autorisiertem Personal gestattet.
- OutSystems verfügt über Richtlinien und Verfahren für die Verwaltung von Schwachstellen und Patches, um sicherzustellen, dass Schwachstellen erkannt, nach Priorität geordnet und beseitigt werden.
- OutSystems verfügt über eine Reihe von definierten Richtlinien und Verfahren für die Softwareentwicklung und das Änderungsmanagement, die sich an internationalen Standards und Best Practices der Branche orientieren. Dies dient der Gewährleistung, dass alle Änderungen in Übereinstimmung mit den Sicherheitsverpflichtungen und -anforderungen genehmigt, konzipiert, entwickelt, konfiguriert, dokumentiert, getestet, freigegeben und implementiert werden.
- OutSystems-Entwickler sind im Bereich der IT-Sicherheit und der sicheren Anwendungsentwicklung geschult.
- Mitarbeiter des Outsystems-Supportteams sind gesondert zur Verschwiegenheit verpflichtet und werden mindestens jährlich neben generellen Schulungen zur Datensicherheit spezifisch hinsichtlich ihrer Security Awareness geschult.
- OutSystems betreibt ein eigenes Security Operations Center für den Plattformbetrieb.
- Die OutSystems-Plattform wird regelmäßigen Penetrationstests durch eine externe Sicherheitsfirma unterzogen.

Mehr zu den Sicherheitsmaßnahmen von OutSystems finden Sie unter Security Overview | Evaluation Guide | OutSystems (www.outsystems.com/de-de/evaluation-guide/security/).

2. Hosting

OutSystems hostet seine Plattform in einem Rechenzentrum in Deutschland[3], das unter anderem nach BSI C5[4] testiert sowie nach ISO 27001, ISO 27017 und ISO 27701 zertifiziert ist. Sicherheitsmaßnahmen des Rechenzentrums sind beispielsweise:

- Der physische Zugang zum Rechenzentrum ist nur autorisierten Personen möglich. Das Rechenzentrum wird dauerhaft durch qualifiziertes Sicherheitspersonal überwacht. Zugangsberechtigungen werden regelmäßig überprüft und angepasst.
- Der physische Zugang wird durch technische Maßnahmen wie Zugangskontrollen durch Multi-Faktor-Authentifizierung, Videoüberwachung und verschiedene Alarmsysteme wie bspw. ein System zur Erkennung von Eindringlingen kontrolliert und protokolliert.
- Technische Maßnahmen wie Notstromversorgung, Klimatisierung, Brandmelde- und -bekämpfungsanlagen oder Wasserleckerkennung gewährleisten ein hohes Maß an Verfügbarkeit.
- Maßnahmen zur Business Continuity ermöglichen die Aufrechterhaltung des Betriebs bei Notfällen, bspw. redundanter Einsatz von Hardwarekomponenten.
- Die eingesetzte Hardware wird kontinuierlich überwacht und von qualifiziertem Personal gewartet.
- Der Hoster führt regelmäßige interne und externe Security Audits durch.
- Der Hoster betreibt ein eigenes Security Operations Center.

3. Verschlüsselung und Schlüsselmanagement

In der Softwarelösung PrivacyPilot werden diverse Verschlüsselungstechniken auf dem Stand der Technik angewandt.

Alle Daten werden gemäß der Empfehlung des Bundesamts für Sicherheit in der Informationstechnik in seiner Technischen Richtlinie BSI TR-02102-1 per Data-At-Rest-Verschlüsselung gemäß dem Industriestandard AES-256 verschlüsselt.

Die Verschlüsselung umfasst den zugrunde liegenden Speicher für Datenbankserver-Instanzen sowie seine automatisierten Sicherungen und Snapshots. Zudem ist auch die Datenkommunikation zwischen den OutSystems-Komponenten verschlüsselt.

Sensible Daten wie beispielsweise API-Keys und die zur Verschlüsselung verwendeten Encryption Keys werden in C5-testierten Management Services gespeichert.

Die Mitarbeiter des Hosters haben keinen Zugriff auf die Encryption Keys, auch nicht auf die Wiederherstellungsschlüssel.

4. Entwicklung

Die Entwicklung des PrivacyPilot wird durch den Auftragnehmer und seinem nach ISO 27001 zertifizierten Entwicklungsdienstleister durchgeführt.

---

[3] www.outsystems.com/evaluation-guide/deploying-outsystems/cloud/.

[4] Der Cloud Computing Compliance Criteria Catalogue (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) spezifiziert Mindestanforderungen für sicheres Cloud Computing. Die Einhaltung der C5-Kriterien kann nur durch Wirtschaftsprüfer geprüft und ein C5-Testat nur durch diese ausgestellt werden.

Der Entwicklungsprozess umfasst unter anderem

- ein kontrolliertes und standardisiertes Anforderungsmanagement,
- eine mit stetigem Blick auf die Informations- und Datensicherheit durchgeführte Entwicklung,
- umfangreiche Testverfahren, wie bspw. Entwickler- und Anwendertests, insbesondere auch im Hinblick auf Sicherheitstests, sowie
- ein standardisiertes Änderungs-, Release- und Deploymentverfahren, inklusive zugehöriger Genehmigungs- und Freigabeprozesse.

Der Auftragnehmer unterhält ein eigenes Ticketingsystem zur Nachverfolgung jeglicher Änderungen sowie von Fehlern. Auftraggeber werden über relevante Änderungen am System informiert.

Die Zugriffsberechtigungen auf Systemkomponenten und Daten für alle Mitarbeiter des Auftragnehmers und seiner Entwicklungsdienstleister werden rollenbasiert gesteuert. Die Berechtigungen werden regelmäßig geprüft und angepasst.

Alle Mitarbeiter des Auftragnehmers sowie Mitarbeiter seines Entwicklungsdienstleisters sind gesondert zur Verschwiegenheit verpflichtet und werden mindestens jährlich im Bereich der Datensicherheit geschult.

5. Tenant-Aufbau

Die Tenants einzelner Auftraggeber und die darin befindlichen Daten und Nutzer sind logisch voneinander getrennt, so dass nur Nutzer innerhalb eines Tenants auf die Daten ihres Tenants zugreifen können. Eine Ausnahme davon bilden solche Daten, die im Rahmen des Marktplatzes explizit durch den Auftraggeber anderen angeboten werden.

Jeder Tenant hat seine eigene, individuelle Nutzerverwaltung. Alle Nutzer sind immer genau einem Tenant zugeordnet, so dass Nutzer bereits ab dem Login lediglich Zugriff auf die Daten des eigenen Tenants nehmen können.

6. Datenzugriff im Supportfall

Grundsätzlich dürfen Mitarbeiter des Auftragnehmers und Mitarbeiter seiner Dienstleister nicht auf Klardaten der Auftraggeber zugreifen. Ein Zugriff ist ausschließlich in den folgenden Fällen gestattet:

1. Im Fall eines vom Auftraggeber aufgegebenen Supportfalls dürfen Mitarbeiter des Auftragnehmers sowie Mitarbeiter seines Entwicklungsdienstleisters auf die Klardaten des Auftraggebers zugreifen, soweit dies für die Bearbeitung des Supportfalls erforderlich ist.
2. Mitarbeiter von OutSystems dürfen nur im Fall eines vom Auftragnehmer erstellten Tickets im Supportfall für eine technische Fehlerbehebung auf die Klardaten auf Datenbankebene zugreifen, soweit dies für die Bearbeitung des Supportfalls erforderlich ist. Der Zugriff ist auf das OutSystems-Supportteam beschränkt.

Durch die Verschlüsselung der Datenbanken und der Backups haben Mitarbeiter des Hosters zu keinem Zeitpunkt Zugriff auf Klardaten der Softwarelösung.