baramundi

Informationen zur Datensicherheit und zum Datenschutz

baramundi
Argus Cockpit

baramundi
Argus Experience

Empower your IT

Liebe Leser:innen,
beim Einsatz von Cloud Lösungen steht vor allem der Schutz der erfassten Daten im Vordergrund. Strenge Unternehmensrichtlinien zur Einhaltung der Cloud Governance sowie gesetzliche Vorgaben wie die EU-DSGVO müssen beim Einsatz derartiger Lösungen eingehalten werden. Die baramundi software GmbH legt bei der Entwicklung und dem Betrieb seiner Cloud Lösungen größten Wert auf Datensicherheit und stellt sicher, dass Sie die erforderlichen Richtlinien einhalten können. Das folgende Dokument gibt Antworten auf die häufigsten Fragen, die sich in diesem Zusammenhang ergeben und gibt einen Überblick über die eingesetzten Technologien und Sicherheitsmechanismen.

Frank Heider
Director R&D Argus Cloud

© 2023 baramundi software GmbH
Änderungen vorbehalten - DocID: ARGUS-230100-INFO-231001-DE

Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information.

1 Inhalt

2 Infrastruktur und Service Provider 4
2.1 Microsoft Azure 4
2.2 MongoDB Inc. 4
2.3 RapidMail GmbH 4
2.4 SoftwareONE Deutschland GmbH 4
3 Datenverarbeitung und Datensicherheit 5
3.1 Microsoft Azure Infrastruktur und Ressourcen 5
3.1.1 Vorratsdatenspeicherung 5
3.1.2 Zugriffsberechtigung 5
3.1.3 Datenschutzerklärungen der baramundi Argus Module 5
3.2 Datenbank MongoDB Atlas 6
3.2.1 Vorratsdatenspeicherung 6
3.2.2 Zugriffsberechtigung 6
3.2.3 Datenspeicherung 6
3.2.4 Datenbank-Backups 6
3.3 Datenerfassung nach Modul 7
3.3.1 baramundi Argus Cockpit 7
3.3.2 baramundi Argus Experience 10
3.4 Verschlüsselung 10
3.5 Multifaktorauthentifizierung (MFA) 10

2 Infrastruktur und Service Provider

Der Betrieb der baramundi Cloud-Anwendungen wird ausschließlich über die Infrastruktur von Microsoft Azure sichergestellt. Darüber hinaus werden einige Serviceprovider eingesetzt, auf die im Folgenden näher eingegangen wird.

2.1 Microsoft Azure

baramundi Argus wird in Microsoft Azure betrieben und verteilt sich wie folgt:

- Die baramundi Argus Anwendungsmodule werden in der **Azure Region Western Europe (Niederlande)** gehostet.
- Das verwendete Azure Active Directory B2C, zur Registrierung und Verwaltung autorisierter Benutzer, wird in der Azure Region Europe gehostet.

Weitere Informationen finden Sie unter:
Region availability and data residency - Azure AD B2C

2.2 MongoDB Inc.

Die eingesetzten MongoDB Atlas Datenbanken werden von MongoDB Inc. in der Azure Region **Western Europe** (Niederlande) für alle baramundi Argus Module gehostet.

2.3 RapidMail GmbH

Der Versand von Benachrichtigungen in baramundi Argus Cockpit erfolgt per Mailversand über den Service Provider „RapidMail“. Das Rechenzentrum von RapidMail befindet sich in Deutschland.

Weitere Informationen finden Sie unter:
DSGVO und Datensicherheit bei Newslettern - rapidmail Wissen & Hilfe

2.4 SoftwareONE Deutschland GmbH

Die SoftwareONE GmbH ist als Service Provider für die Abrechnung der Microsoft Azure Infrastruktur gegenüber der baramundi software GmbH verantwortlich.

3 Datenverarbeitung und Datensicherheit

3.1 Microsoft Azure Infrastruktur und Ressourcen

3.1.1 Vorratsdatenspeicherung

Das **Azure AD B2C** Überwachungsprotokoll zeichnet die Dienste- und Benutzeranmeldungen bis zu 7 Tage auf.

Weitere Informationen finden Sie unter: *AAD B2C Überwachungsprotokoll*

Die *Log Analytics Workspaces* von Microsoft Azure verfügen über die Option *Data Retention*, welche die Laufzeit der Vorratsdatenspeicherung einstellt. Diese Einstellung ist auf die Mindestlaufzeit von **90 Tagen** eingestellt. Darüber hinaus kann die maximale Menge an aufgezeichneten Daten über die Option *Daily cap* begrenzt werden. Diese Begrenzung liegt derzeit bei **2.0 GB pro Tag**.

Weitere Informationen finden Sie unter: *Activate Azure Log Analytics Manually*

3.1.2 Zugriffsberechtigung

Sowohl die Konsolenausgabe zur Laufzeit als auch die aufgezeichneten Log- und Monitoring-Daten können lediglich **durch berechtigte Administratoren der baramundi software GmbH** eingesehen werden. Die aufgezeichneten Log- und Monitoring-Daten werden darüber hinaus im Bedarfsfall von Entwicklungs- und Support-Mitarbeitern in Zusammenarbeit mit den berechtigten Administratoren gesichtet, um Anwendungsfehler zu analysieren. Darüber hinaus verfügt SoftwareONE im Zuge des Kostenmonitorings und des Kostenreportings Zugriff auf die Ressourcen der Azure Infrastruktur. Durch den Einsatz der Customer Logbox haben Microsoft Mitarbeiter keinerlei Zugriff auf Daten innerhalb der Azure Ressourcen ohne Zustimmung unserer verantwortlichen Administratoren bei baramundi. Die verfügbaren Accounts innerhalb der Microsoft Azure Infrastruktur sind entsprechend konfiguriert, nur die minimal nötigen Rechte zu besitzen (Azure RBAC). Privilegierte administrative Rechte können nur über das eingesetzte Azure AD PIM erlangt werden.

Weitere Informationen finden Sie unter:
Azure Role-Based Access Controll (RBAC)
Was ist Privileged Identity Management?

3.1.3 Datenschutzerklärungen der baramundi Argus Module

- Datenschutzerklärung Argus Cockpit: *baramundi Argus Cockpit*
- Datenschutzerklärung Argus Experience: *baramundi Argus Experience*

3.2 Datenbank MongoDB Atlas

3.2.1 Vorratsdatenspeicherung

MongoDB Atlas bewahrt die Logs und Systemereignis-Meldungen der letzten **30 Tage** für jedes Tier in einem Cluster auf. Die Logs des Performance Advisors werden maximal **7 Tage** für jeden Cluster aufbewahrt.

Weitere Informationen finden Sie unter:
View and Download MongoDB Logs

3.2.2 Zugriffsberechtigung

Die aufgezeichneten Log- und Monitoring-Daten können **lediglich durch berechtigte Administratoren der baramundi software GmbH** eingesehen werden. Die aufgezeichneten Log- und Monitoring-Daten werden darüber hinaus im Bedarfsfall von Entwicklungs- und Support-Mitarbeitern in Zusammenarbeit mit den berechtigten Administratoren gesichtet, um Anwendungsfehler zu analysieren. Der Zugriff auf Kundendaten durch MongoDB Mitarbeiter kann nur mit Zustimmung unserer verantwortlichen Administratoren erfolgen.

3.2.3 Datenspeicherung

Die Anwendungsdaten der baramundi Argus Module werden in einem Azure Storage mit laufender MongoDB Atlas mit **256-bit AES** Verschlüsselung gespeichert. **FIPS 140-2** Compliance wird sowohl durch MongoDB Atlas, als auch durch Microsoft Azure in der Region Western Europe sichergestellt. Die Schlüsselverwaltung der verwendeten Schlüssel erfolgt durch Platform Managed Keys (PMKs), im Falle von baramundi Argus per **Azure Key Vault.**

Weitere Informationen finden Sie unter: *Key Vault | Microsoft Azure*
Storage Engine and Cloud Backup Encryption — MongoDB Atlas

3.2.4 Datenbank-Backups

Datenbankbackups werden in verschiedenen Zeitintervallen erstellt, um im Desaster Fall eine zügige Wiederherstellung der Daten gewährleisten zu können. Die maximale Vorhaltezeit der Datenbankbackups beträgt **90 Tage.** Backups werden sowohl in einem Azure Storage, als auch in einer dedizierten Infrastruktur bei baramundi mit einer 256-bit AES Verschlüsselung vorgehalten und gesichert.

Weitere Informationen finden Sie unter:
Key Vault | Microsoft Azure
Storage Engine and Cloud Backup Encryption — MongoDB Atlas

3.3 Datenerfassung nach Modul

Im Folgenden erfahren Sie, welche Daten von den jeweiligen baramundi Argus Modulen zur Laufzeit erfasst und übertragen werden.

3.3.1 baramundi Argus Cockpit

Die Übermittlung der Daten von der baramundi Management Suite (bMS) zu baramundi Argus Cockpit (bAC) erfolgt über Cloud Connectoren. Dabei handelt es sich um Windows Dienste, die relevante Daten aus der bMS über baramundi bConnect auslesen und autorisiert und authentifiziert in die Cloud übertragen. Die folgenden Daten werden dabei synchronisiert.

3.3.1.1 baramundi Cloud Connector Server State

Dieser Cloud Connector übermittelt Informationen zum BMS Server und dessen Systemzustand und umfasst folgende Werte:

- Server
  - GUID
  - Name

- Serverdienste:
  - Name
  - Ausführungszustand

3.3.1.2 baramundi Cloud Connector Job Information

Dieser Cloud Connector übermittelt Informationen zu Jobs, Jobinstanzen und deren Ausführungszustand, die für die Übertragung an bAC freigegeben wurden und umfasst folgende Werte:

- Jobdefinition
  - GUID
  - Anzeigename
  - Beschreibung
  - Name

- Jobinstanz
  - GUID
  - Endpunkt GUID
  - Endpunkt Name
  - Zeitpunkt der letzten Aktion
  - BMS Ausführungszustand
  - Statustext

3.3.1.3 baramundi Cloud Connector Dynamic Groups

Dieser Cloud Connector übermittelt Informationen über die Endpunkte, die zum Zeitpunkt der Übertragung den Kriterien der universellen dynamischen Gruppen (UDG) entsprochen haben. Dabei werden folgende Informationen eines Endpunkts übertragen:

- Allgemein
  - GUID
  - Typ
  - Anzeigename
  - Hostname
  - Domäne
  - Locale ID
  - Informationen zum Betriebssystem und Version
  - Version des Internet Explorers
  - Kennung der verwendeten Boot-Umgebung
  - Letzte Bootzeit
  - Verwendetes Energieschema

- Informationen zur Hardware
  - Seriennummer
  - Hersteller
  - Modell
  - Primäre MAC Adresse
  - MAC Adressliste
  - Logische MAC Adresse
  - Größe des Arbeitsspeichers
  - CPU – Informationen
  - Liste der vorhandenen Speichermedien mit zugehörigen Details, wie
    - Volume ID
    - Größe
    - Freier Speicher
    - Dateisystem
    - Dateisystemtyp
    - Partitionierungstyp
    - Laufwerksbuchstabe
    - Kennung
    - Informationen zu Bitlocker (s. Bitlocker)

- baramundi Management Agent
  - Version des Agenten
  - Status des Agenten
  - Informationen zum Verwaltungsmodus (IEM) des Clients
  - Letzte Aktivität des Agenten
  - Letzte Änderung des Agenten
  - Zuletzt gesehen Datum des Agenten

- Informationen zum Patchmanagement
  - Informationen zur Patch-Konfiguration
  - Informationen zur konfigurierten Updatequelle
  - Datum der letzten Updateinventur
  - Anzahl fehlender Patches nach verschiedenen Kategorien

- Informationen zum Systemzustand
  - Informationen zum Verwaltungszustand
  - Informationen zum Compliance-Zustand und zur Compliance-Konfiguration
  - Informationen zum Virus- und Bedrohungszustands
  - Informationen zur Inventur und Inventurkonfiguration
  - Informationen zum Aktivierungszustand von SecureBoot
  - Informationen und Status des TPM-Moduls
  - Status der automatischen Updates
  - Status des Firewall- und Netzwerkschutzes
  - Status des App- und Browserschutzes
  - Status des Windows Security Dienstes
  - Status des Benutzerkontenschutzes

- Informationen zu Bitlocker
  - Status der Bitlocker Aktivierung
  - Status der Startup-Pin Aktivierung
  - Status des Network-Unlocks
  - Status der Startup-USB Key Aktivierung
  - Pro Laufwerk:
    - Status der Konvertierung
    - Verschlüsselungsgrad in Prozent
    - Bitlockerversion
    - Status des Laufwerkschutzes
    - Status der Sperrung eines Laufwerks
    - Anzahl der Reboots vor Reaktivierung von Bitlocker

- Informationen zu Microsoft Defender
  - Status aller Defender Engines und Module
  - Alle Versions- und Definitionsinformationen der Defender Engines und Module
  - Datum des letzten vollen Scans
  - Ende des letzten vollen Scans
  - Aktive Bedrohungen
  - Gelöste Probleme und Bedrohungen
  - Höchste Severity

- Informationen zu Industrial Endpoints
  - Typ des verwendeten Gateways
  - Datum der letzten Inventur
  - Informationen zum CPU
  - Informationen zu Firmware- und Hardwareversion
  - Standort des Geräts
  - Laufzeit

- Informationen zu mobilen Endgeräten
  - Typ des Android Enterprise Verwaltungsmodus (bei Android)
  - Typ des Apple Verwaltungsmodus (bei Apple)
  - Updateverfügbarkeit von Apple (bei Apple)

3.3.1.4 Typische Zwecke

Diese o.g. Daten sind erforderlich, um den Gesamtstatus, der von der bMS verwalteten Umgebung, erfassen zu können. Durch die Konfiguration von Universellen Dynamischen Gruppen lässt sich individuell pro Umgebung festlegen, welche der o.g. Daten ausgewertet werden sollen. Dem IT-Admin

oder anderen Rollen im Unternehmen wird es damit ermöglicht, Auffälligkeiten in der IT-Umgebung zu erkennen.

3.3.2 baramundi Argus Experience

Die Übermittlung der Daten zu baramundi Argus Experience erfolgt per Agenten der auf den verwendeten Endgeräten installiert ist. Nur authentifizierte und autorisierte Clients können eine Verbindung zu baramundi Argus aufbauen.

3.3.2.1 baramundi Argus Experience Agent

- Letzter Kontakt des Agenten (Datum)
- Angemeldeter Benutzername
- Hostname des Endgerätes
- IP-Adresse des Endgerätes
- Protokollierte Prozessabstürze
- Protokollierte Prozesshänger
- Informationen zum Betriebssystem, Architektur und Version
- Dateipfad der auffälligen Applikationen

3.3.2.2 Typische Zwecke

Diese o.g. Daten sind erforderlich, um die Ergebnisse kritischer Auffälligkeiten der IT-Umgebungen den entsprechenden Endgeräten zuordnen und passende Lösungen zielgerichtet durch den IT-Verantwortlichen initiieren zu können. Machine Learning Algorithmen und künstliche Intelligenz können aus dieser – dafür anonymisierten - Datenbasis dann Vorhersagen für die Stabilität, Performance und Konnektivität der IT-Umgebung ableiten. Das erleichtert den IT-Verantwortlichen die End User Zufriedenheit nachhaltig zu fördern.

3.4 Verschlüsselung

Alle Komponenten und Endgeräte kommunizieren asymmetrisch verschlüsselt per **TLS 1.2 bzw. TLS 1.3** auf allen Kommunikationskanälen. Die dabei verwendeten SSL Zertifikate entsprechen aktuellen Sicherheitsstandards und setzen neben dem Hash-Algorithmus **SHA256** auf eine Schlüssellänge von **2048 Bit**. Alle aktiven Kommunikationsschnittstellen sind mit SSL Zertifikaten versehen. Die entsprechenden Webserver besitzen über ein A+ Rating.

3.5 Multifaktorauthentifizierung (MFA)

Derzeit wird noch keine MFA unterstützt.

baramundi

Wir freuen uns, Sie kennenzulernen!

Kontaktieren Sie uns!

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

+44 2071 93 28 77
request@baramundi.com
www.baramundi.com

+48 735 91 44 54
request@baramundi.com
www.baramundi.com

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

+43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

+39 340 8861886
request@baramundi.com
www.baramundi.com

+41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

+1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com