baramundi

# Informationen zur Datensicherheit und zum Datenschutz der baramundi Proactive Hub Produkte, sowie Argus Cockpit

*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 Product Development Proactive Solutions

# 1 Inhalt

# 2 Infrastruktur und Service Provider

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

## 2.1 Microsoft Azure

Der baramundi Proactive Hub, sowie Argus Cockpit wird in Microsoft Azure betrieben und verteilt sich wie folgt:

- Die baramundi Proactive Hub Produkte, sowie Argus Cockpit werden in der **Azure Region Western Europe (Niederlande)** gehostet. Das gilt für alle Kunden, deren Firmensitz in Europa liegt.
- Die baramundi Proactive Hub Produkte, sowie Argus Cockpit werden in der **Azure Region East US** gehostet. Das gilt für alle Kunden, deren Firmensitz in den USA liegt.
- Das verwendete Azure Active Directory B2C zur Registrierung und Verwaltung autorisierter Benutzer wird von Microsoft über global replizierte Services zur Verfügung gestellt.

*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 Proactive Hub Produkte, sowie Argus Cockpit gehostet. Das gilt für alle Kunden, deren Firmensitz in Europa liegt.
- Die eingesetzten MongoDB Atlas Datenbanken werden von MongoDB Inc. in der Azure Region **Azure Region East US** für alle baramundi Proactive Hub Produkte, sowie Argus Cockpit gehostet. Das gilt für alle Kunden, deren Firmensitz in den USA liegt.

## 2.3 Rapidmail GmbH

Der Versand von Benachrichtigungen per Mailversand erfolgt für die Produkte des baramundi Proactive Hub, sowie für Argus Cockpit über den Service Provider „Rapidmail“. Das Rechenzentrum von Rapidmail befindet sich in Deutschland.

*Weitere Informationen finden Sie unter:*
*https://www.rapidmail.de*

## 2.4 SoftwareONE Deutschland GmbH

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

## 2.5 Cloudflare Germany GmbH

Zur Verbesserung der Anwendungssicherheit als auch zum Schutz vor verschiedenen Angriffsarten werden verschiedene Dienste, wie DDos-Protection und Web Application Firewall, des Service Providers Cloudflare eingesetzt. Der Schutz umfasst sowohl die Infrastruktur und Produkte des baramundi Proactive Hub als auch Argus Cockpit.

## 2.6 Hetzner Online GmbH

Für die Inbetriebnahme von Argus Cockpit wird ein kundenindividuelles Konfigurationspaket benötigt. Diese Pakete werden über einen passwortgeschützten Download Service von Hetzner mit kundenindividuellen Downloads zur Verfügung gestellt.

## 2.7 MicroNova AG

Für das Monitoring und die Bereitstellung einer Website zur Verfügbarkeitskontrolle des baramundi Proactive Hub, sowie Argus Cockpit wird Site24x7 von ManageEngine eingesetzt, stellvertretend durch die MicroNova AG in Deutschland.

# 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.

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**.

### 3.1.2 Zugriffsberechtigung

#### *3.1.2.1 Microsoft*

Sowohl die Konsolenausgabe zur Laufzeit als auch die aufgezeichneten Log- und Monitoring-Daten der Azure Umgebung 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. Durch den Einsatz der Customer Logbox haben Microsoft Mitarbeiter keinerlei Zugriff auf Daten innerhalb der Azure Ressourcen ohne Zustimmung unserer verantwortlichen IT-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.

#### *3.1.2.2 SoftwareONE*

SoftwareONE verfügt im Zuge des Kostenmonitorings und des Kostenreportings eingeschränkten Zugriff auf die Ressourcen der Azure Infrastruktur. Im Support-Fall ist für weitreichendere Rechte eine Genehmigung durch die Administratoren der baramundi software GmbH erforderlich.

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

### 3.1.3 Datenschutzerklärungen der baramundi Proactive Hub Produkte und Argus Cockpit

- Datenschutzerklärung baramundi perform2work: *baramundi perform2work*
- Datenschutzerklärung Argus Cockpit: *Argus Cockpit*

# 3.2 Datenbank MongoDB Atlas

## 3.2.1 Vorratsdatenspeicherung

MongoDB Atlas bewahrt die Logs und Systemereignis-Meldungen der letzten **30 Tage** für jeden Rang 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 innerhalb der eingesetzten MongoDB Atlas Datenbanken durch MongoDB Mitarbeiter kann nur mit Zustimmung unserer verantwortlichen Administratoren erfolgen.

## 3.2.3 Datenspeicherung

Die Anwendungsdaten der baramundi Proactive Hub Produkte, sowie von Argus Cockpit 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) 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

Datenbank-Backups werden in verschiedenen Zeitintervallen erstellt, um im Ernstfall eine zügige Wiederherstellung der Daten gewährleisten zu können. Die maximale Vorhaltezeit der Datenbankbackups beträgt **4 Wochen.** Backups werden sowohl in einem Azure Storage als auch in einer dedizierten Infrastruktur bei baramundi mit einer 256-bit AES-Verschlüsselung vorgehalten und gesichert. Auf Band werden die Backups maximal **12 Monate** vorgehalten.

***Weitere Informationen finden Sie unter:***
*Storage Engine and Cloud Backup Encryption — MongoDB Atlas*

# 3.3 Rapidmail Germany nach Modul

## 3.3.1 Vorratsdatenspeicherung

Im Rahmen des E-Mailversands erfolgt eine Protokollierung der versendeten E-Mails. Die Protokollierung ist auf 500 E-Mails limitiert. Im Rahmen dieser Protokollierung werden alle im Zusammenhang mit dem Versand einer E-Mail stehenden Informationen erfasst, u.a. die E-Mail-Adresse des Empfängers. Personenbezogene Daten werden im Rahmen der DSGVO-EU Vorschriften konform und fristgerecht gelöscht.

***Weitere Informationen finden Sie unter:***
*Datenschutzerklärung - Rapidmail*

## 3.3.2 Zugriffsberechtigung

Sowohl Rapidmail als Versanddienstleister der E-Mails, als auch die Administratoren der baramundi software GmbH haben Zugriff auf diese Log-Protokolle.

# 3.4 Datenerfassung nach Produkten und Modulen

Im Folgenden erfahren Sie, welche Daten von den jeweiligen baramundi Proactive Hub Produkten, sowie von Argus Cockpit zur Laufzeit erfasst und übertragen werden.

## 3.4.1 baramundi perform2work

Die Übermittlung der Daten zu baramundi perform2work erfolgt über den baramundi Proactive Agent, der auf den verwendeten Endbenutzergeräten installiert ist. Nur authentifizierte und autorisierte Clients können eine Verbindung zum baramundi Proactive Hub und den damit verbundenen Produkten aufbauen.

### *3.4.1.1 Typische Zwecke*

Erfasst werden Daten, die erforderlich sind, 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 über die Stabilität, Performance und Konnektivität der IT-Umgebung ableiten. Das erleichtert den IT-Verantwortlichen die End User Zufriedenheit nachhaltig zu fördern.

## 3.4.2 Argus Cockpit

Die Übermittlung der Daten von der baramundi Management Suite zu Argus Cockpit erfolgt über Cloud Connectoren. Dabei handelt es sich um Windows Dienste, die relevante Daten aus der

baramundi Management Suite über unsere Schnittstelle baramundi bConnect auslesen und autorisiert und authentifiziert in die Cloud übertragen.

#### *3.4.2.1 Typische Zwecke*

Erfasst werden Daten, um den Gesamtstatus der von der baramundi Management Suite verwalteten Umgebung überwachen zu können. Durch die Konfiguration von Universellen Dynamischen Gruppen lässt sich individuell pro Umgebung festlegen, welche Daten ausgewertet und an Argus Cockpit übermittelt werden sollen. Dem IT-Admin oder anderen Rollen im Unternehmen wird es damit ermöglicht, Auffälligkeiten in der IT-Umgebung zu erkennen.

## 3.5 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 ein A+ Rating.

## 3.6 Multifaktorauthentifizierung (MFA)

Es gibt in allen baramundi Proactive Hub Produkten, sowie in Argus Cockpit die Möglichkeit, zusätzlich zum Benutzer-Passwort eine zweite Sicherheitsebene hinzuzufügen.

Die Optionen für die Multi-Faktor-Authentifizierung:

- **E-Mail**: Benutzer erhalten einen Sicherheitscode per E-Mail, den sie bei der Anmeldung eingeben müssen.
- **Authenticator App**: Benutzer generieren einen Sicherheitscode über eine App wie z.B. Google Authenticator, die sie auf ihrem Smartphone installieren können.

Wir empfehlen die Nutzung der Authenticator App, da diese Methode selbst dann Schutz bietet, wenn der Zugriff auf E-Mails kompromittiert ist. Die Aktivierung der Multi-Faktor-Authentifizierung kann direkt vom Company Admin im Administrationsbereich vorgenommen werden.

Ferner hat der Umgebungsadministrator die Möglichkeit, die MFA für einzelne Benutzer zurückzusetzen, beispielsweise im Fall eines Geräteverlusts oder bei Änderung der E-Mail-Adresse.