

baramundi
Proactive Hub

Informationen zur Datensicherheit und zum Datenschutz

baramundi Proactive Hub

baramundi

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

© 2026 baramundi software GmbH
Änderungen vorbehalten - DocID: PROACTIVEHUB-260200-INFO-261007-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
2.5 CLOUDFLARE GERMANY GMBH 5
2.6 PINEAPPLE TECHNOLOGY LTD. 5
2.7 CYBER INSIGHT GMBH 5

3 DATENVERARBEITUNG UND DATENSICHERHEIT 6

3.1 MICROSOFT AZURE INFRASTRUKTUR UND RESSOURCEN 6
3.1.1 Vorratsdatenspeicherung 6
3.1.2 Zugriffsberechtigung 6
3.1.3 Datenschutzerklärung des baramundi Proactive Hub 6
3.2 DATENBANK MONGODB ATLAS 7
3.2.1 Vorratsdatenspeicherung 7
3.2.2 Zugriffsberechtigung 7
3.2.3 Datenspeicherung 7
3.2.4 Datenbank-Backups 7
3.3 RAPIDMAIL GERMANY 8
3.3.1 Vorratsdatenspeicherung 8
3.3.2 Zugriffsberechtigung 8
3.4 DATENERFASSUNG 8
3.4.1 baramundi Proactive Hub 8
3.4.2 Cyber Insight 8
3.5 VERSCHLÜSSELUNG 10
3.6 MULTIFAKTORAUTHENTIFIZIERUNG (MFA) 10

2 Infrastruktur und Service Provider

Der Betrieb der baramundi-eigenen Cloud-Anwendungen erfolgt über die Infrastruktur von Microsoft Azure. Darüber hinaus werden externe Service Provider eingesetzt, die teilweise eigene Cloud- und Rechenzentrumsinfrastrukturen nutzen. Diese werden im Folgenden näher beschrieben.

2.1 Microsoft Azure

Der baramundi Proactive Hub wird in Microsoft Azure betrieben und verteilt sich wie folgt:

- Der baramundi Proactive Hub wird in der **Azure Region Western Europe (Niederlande)** gehostet. Das gilt für alle Kunden, deren Firmensitz in Europa liegt.
- Der baramundi Proactive Hub wird 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 den baramundi Proactive Hub 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 den baramundi Proactive Hub gehostet. Das gilt für alle Kunden, deren Firmensitz in den USA liegt.

2.3 Rapidmail GmbH

Der Versand von Benachrichtigungen per Mail erfolgt für den baramundi Proactive Hub 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.

2.6 Pineapple Technology Ltd.

Für das Monitoring und die Bereitstellung einer Website zur Verfügbarkeitskontrolle des baramundi Proactive Hub wird incident.io von Pineapple Technology Ltd. eingesetzt. Das primäre Rechenzentrum befindet sich in Belgien.

Weitere Informationen finden Sie unter:
Terms and Conditions | incident.io

2.7 Cyber Insight GmbH

Für die Schwachstellenanalyse im baramundi Proactive Hub wird der Dienst von Cyber Insight eingesetzt. Cyber Insight verarbeitet die vom Proactive Hub übermittelte Softwareinventarisierung, um installierte Softwareversionen bekannten Schwachstellen und zugehörigen CVEs zuzuordnen.

Die Kundendaten werden in der Google Cloud Platform (Region europe-west3, Frankfurt am Main) gespeichert und verarbeitet. Eigene Machine-Learning-Modelle sowie das selbst gehostete Large Language Model von Cyber Insight laufen auf eigener Infrastruktur in einem Rechenzentrum von envia TEL in Leipzig. Sämtliche Endkundendaten verbleiben innerhalb der EU.

Google Firebase Authentication wird ausschließlich zur Authentifizierung genutzt. Der Dienst wird von Google aus US-Rechenzentren bereitgestellt; dort werden jedoch keine Endkundendaten verarbeitet. Kundendaten werden nicht außerhalb der EU übertragen.

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 30 Tage auf.

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 Datenschutzerklärung des baramundi Proactive Hub

- Datenschutzerklärung baramundi Proactive Hub: *baramundi proactive* hub

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 des baramundi Proactive Hub 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

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

Im Folgenden erfahren Sie, welche Daten vom baramundi Proactive Hub zur Laufzeit erfasst und übertragen werden.

3.4.1 baramundi Proactive Hub

Die Übermittlung der Daten zum baramundi Proactive Hub erfolgt über den baramundi Proactive Hub 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 Cyber Insight

Zur Identifikation und Bewertung von Schwachstellen übermittelt der baramundi Proactive Hub die Softwareinventarisierung der verwalteten Geräte an Cyber Insight. Übertragen werden die Geräteliste,

die installierte Software und die jeweiligen Softwareversionen sowie die für die Identifikation von Schwachstellen und zugehörigen CVEs erforderlichen Daten. Geräte- und Firmennamen werden vor der Übertragung durch baramundi gehasht. Cyber Insight besitzt keinen Schlüssel und keine Zuordnung, mit der diese Hashwerte auf die ursprünglichen Geräte- oder Firmennamen zurückgeführt werden könnten. Die Hashwerte werden von Cyber Insight weder analysiert noch aufgelöst. Cyber Insight erhält keine Benutzernamen, keine Hostnamen im Klartext und keine Netzwerkkonfigurationen. Die IP-Adresse des anfragenden Systems wird technisch im API-Gateway protokolliert, von Cyber Insight nicht verwendet und nach 30 Tagen automatisch gelöscht.

3.4.2.1 Zugriff, Speicherung und Sicherheit

Cyber Insight hat keinen Zugriff auf die Kundenumgebung und verarbeitet ausschließlich die vom Proactive Hub übermittelten Daten. Die Übertragung erfolgt verschlüsselt über HTTPS/TLS; gespeicherte Daten in Google Cloud Storage und Cloud SQL sind mit von Google verwalteten Schlüsseln verschlüsselt. Der Zugriff ist auf einen kleinen Kreis autorisierter Mitarbeiter des Cyber-Insight-Entwicklungsteams beschränkt; aktuell handelt es sich um drei Personen. Administrative Zugriffe sind auf das interne Netzwerk von Cyber Insight beschränkt und werden über Google-Cloud-Audit-Logs protokolliert. Die Plattform wird zusätzlich durch Firewalls geschützt. Cyber Insight weist darauf hin, dass innerhalb des Dienstes keine technische Datentrennung zwischen Kunden besteht. Das Unternehmen betreibt ein nach **ISO/IEC 27001** zertifiziertes Informationssicherheits-Managementsystem und verfügt über dokumentierte Backup-, Business-Continuity- und Disaster-Recovery-Verfahren. Die erfolgreiche Durchführung von Backups sowie die Wiederherstellbarkeit werden regelmäßig überprüft und getestet. Für relevante Systeme bestehen definierte Recovery-Ziele einschließlich RTO und RPO.

3.4.2.2 Künstliche Intelligenz

Cyber Insight verwendet eigene, intern entwickelte Machine-Learning-Modelle sowie das Open-Weight-Modell Mistral-Small-Instruct-2409 als selbst gehostetes Large Language Model. Das LLM wird auf eigener Infrastruktur in Leipzig betrieben; externe LLM-Dienste oder andere AI-Provider werden nicht eingesetzt. Kundendaten werden weder zum Training der Modelle noch für Statistiken, Benchmarks oder Marketing verwendet und nicht an Drittanbieter von KI-Diensten weitergegeben.

3.4.2.3 Datenlebenszyklus und Datenschutz

Kundendaten werden nur so lange aufbewahrt, wie dies für den vereinbarten Geschäftszweck sowie aufgrund gesetzlicher oder vertraglicher Anforderungen erforderlich ist. Bei Vertragsende können Daten im Rahmen der vertraglichen Vereinbarungen exportiert werden; anschließend werden sie nach Ablauf etwaiger Aufbewahrungs- oder Übergangsfristen sicher gelöscht, sofern keine weitere Aufbewahrungspflicht besteht. Für diesen Dienst werden keine personenbezogenen Daten benötigt oder verarbeitet; ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO ist daher aus Sicht von Cyber Insight grundsätzlich nicht erforderlich. Entsprechende Anfragen werden im Einzelfall geprüft.

3.5 Verschlüsselung

Die Komponenten und Endgeräte des baramundi Proactive Hub 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 **4096 Bit**. Alle aktiven Kommunikationsschnittstellen sind mit SSL-Zertifikaten versehen. Die entsprechenden Webserver besitzen ein **A Rating**.
Die Datenübertragung zu Cyber Insight erfolgt über verschlüsselte HTTPS/TLS-Verbindungen. Bei Cyber Insight gespeicherte Daten in Google Cloud Storage und Cloud SQL sind mit von Google verwalteten Schlüsseln verschlüsselt.

3.6 Multifaktorauthentifizierung (MFA)

Es gibt im baramundi Proactive Hub 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.

baramundi

Kontaktieren Sie uns.

Wir freuen uns auf Sie!

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com

+43 1 928 0136 0010
request@baramundi.com

+41 77 280 49 79
request@baramundi.com

+39 340 8861886
request-italia@baramundi.com

+48 735 91 44 54
request@baramundi.com

+44 2071 93 28 77
request@baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com

+49 821 56708-390
request@baramundi.com

