Building Technologies

NEXOSPACE

Sicherheits- und Datenschutz-konzept für digitale Services im Brandschutz

August 2026

Inhalte

Einleitung

NEXOSPACE ist eine digitale Suite aus integrierten, vernetzten und intelligenten Services für das moderne Gebäudemanagement.

Die Plattform basiert auf einer skalierbaren Microservice-Architektur und kombiniert moderne Cloud-Technologien mit umfassenden Sicherheitsmechanismen nach höchsten Standards. Ziel ist der durchgängige Schutz sensibler Gebäudedaten über den gesamten Lebenszyklus hinweg – von der Erfassung über die Verarbeitung bis zur Speicherung und Übertragung.
Dieses Dokument beschreibt die grundlegenden Sicherheits- und Datenschutzprinzipien der Microservice-basierten Architektur von NEXOSPACE für die Services im Brandschutz. Es dient als Leitfaden für die eingesetzten technischen und organisatorischen Maßnahmen und stellt dar, wie Datenschutz, Informationssicherheit und Compliance systematisch in der Plattform verankert sind.
Im Fokus stehen dabei die folgenden Kernbereiche: die sichere und regelkonforme Cloud-Infrastruktur auf Basis europäischer Datenhoheit, ein durchgängiger sicherheitsorientierter Entwicklungs- und Betriebszyklus, moderne Verschlüsselungs- und Authentifizierungsmechanismen, ein strukturiertes Schwachstellen- und Incident-Management sowie umfassende technische Schutzmaßnahmen über den gesamten Plattformbetrieb hinweg.
Durch die konsequente Umsetzung dieser Prinzipien gewährleistet NEXOSPACE ein hohes, nachhaltig betriebenes Sicherheitsniveau und schafft die Grundlage für vertrauenswürdige digitale Gebäudeservices in komplexen, vernetzten Umgebungen.

Übersicht Datenfluss

1. Cloud-Infrastruktur & Compliance

Die Basis für NEXOSPACE bildet ein Fundament aus geprüfter Sicherheit und europäischer Datenhoheit.

Das Hosting der gesamten Plattform erfolgt ausschließlich innerhalb der EU auf Microsoft Azure, wodurch die Einhaltung europäischer Datenschutzstandards gewährleistet ist. Der Betrieb der Cloud-Umgebung orientiert sich an den strengen Empfehlungen des BSI C5:2020-Katalogs des Bundesamtes für Sicherheit in der Informationstechnik. Zudem ist unsere Infrastruktur gezielt nach der Norm DIN 50710 aufgebaut. Zudem ist unsere Infrastruktur für ausgewählte Systeme gemäß der DIN EN 50710 zertifiziert.

Die zugrunde liegende Microsoft Azure-Plattform selbst verfügt über umfangreiche internationale Sicherheitszertifizierungen, die die Sicherheit des Plattformbetriebs im Rahmen des Shared-Responsibility-Modells belegen.

Zu den wichtigsten gehören:

- **ISO/IEC 27001:2022**: international anerkannter Standard für Informationssicherheitsmanagementsysteme
- **ISO/IEC 27017**: spezifische Sicherheitskontrollen für Cloud-Services

2. Sicherer Entwicklungs- und Betriebszyklus

Die Entwicklung und der Betrieb unserer NEXOSPACE Cloud-Services folgen einem streng strukturierten und sicherheitsorientierten Prozess, der auf dem Bosch Building Technologies Product Engineering Process sowie dem Bosch Building Technologies Security Engineering Process basiert.

Im Rahmen dieses Ansatzes wird bereits in der Entwicklungsphase für jeden Service eine detaillierte Bedrohungs- und Risikoanalyse durchgeführt, um potenzielle Angriffsvektoren frühzeitig zu identifizieren. Während des gesamten Lebenszyklus werden unsere Anwendungen durch kontinuierliche Schwachstellenprüfungen überwacht, wobei erkannte Risiken in einem definierten Prozess bewertet und behandelt werden. Zur Validierung unserer Sicherheitsmaßnahmen führen wir zusätzlich regelmäßige Penetrationstests durch externe, unabhängige Sicherheitspartner durch.

3. Datenverschlüsselung

Der Datenschutz hat oberste Priorität. Wir setzen daher durchgängig auf Verschlüsselungsverfahren nach dem aktuellen Stand der Technik, sowohl bei der Übertragung als auch bei der Speicherung.

Datenübertragung:
Jede Form der Datenkommunikation wird ausschließlich über sichere, kryptographisch abgesicherte Kanäle abgewickelt. Externe Schnittstellen, wie unsere APIs, werden per HTTPS mit robuster TLS-Verschlüsselung geschützt und zusätzlich durch ein Azure Application Gateway mit integrierter Web Application Firewall (WAF) abgeschirmt, um Angriffe auf Anwendungsebene abzuwehren. Die Anbindung von Edge-Geräten erfolgt über sichere Endpunkte wie den Azure IoT Hub unter Nutzung verschlüsselter Protokolle wie MQTT over TLS. Für die sichere Standortvernetzung kommen bewährte VPN-Verbindungen auf Basis von IPSec oder OpenVPN über TLS zum Einsatz.
Bei Daten mit besonders hohem Schutzbedarf gehen wir noch einen Schritt weiter und implementieren eine zusätzliche End-to-End-Verschlüsselung direkt auf Anwendungsebene. Dadurch wird sichergestellt, dass ausschließlich autorisierte Kommunikationspartner Zugriff auf die Klartextdaten erhalten.
Das Fundament für diese sichere Kommunikation bilden vertrauenswürdige Public-Key-Infrastrukturen (PKI). Wir setzen hierbei ausschließlich auf Zertifizierungsstellen und Vertrauensdienste, die von den Bosch-Sicherheitsverantwortlichen sorgfältig geprüft und explizit freigegeben wurden.

Daten im Ruhezustand:
Alle Daten, die auf den Microsoft Azure Platform Services gespeichert werden, sind ausnahmslos und standardmäßig verschlüsselt (Encryption at Rest), beispielsweise durch Azure Storage Encryption. Für die sichere Aufbewahrung und Verwaltung der kryptographischen Schlüssel nutzen wir den Azure Key Vault. Für Anwendungsfälle mit erhöhten Sicherheitsanforderungen setzen wir auf Managed HSM. Um unseren Kunden maximale Kontrolle zu ermöglichen, bieten wir je nach Schutzbedarf auch den Einsatz von durch Bosch Building Technologies verwalteten Schlüsseln an. Die gesamte Handhabung der Schlüssel folgt dabei streng definierten Bosch-Prozessen. Der komplette Lebenszyklus eines Schlüssels – von der sicheren Erzeugung über die Verteilung, Rotation und Sperrung bis hin zur unwiderruflichen Löschung – ist durch klare organisatorische und technische Maßnahmen geregelt und wird lückenlos umgesetzt.

4. Authentifizierung & Zugriffs-kontrolle

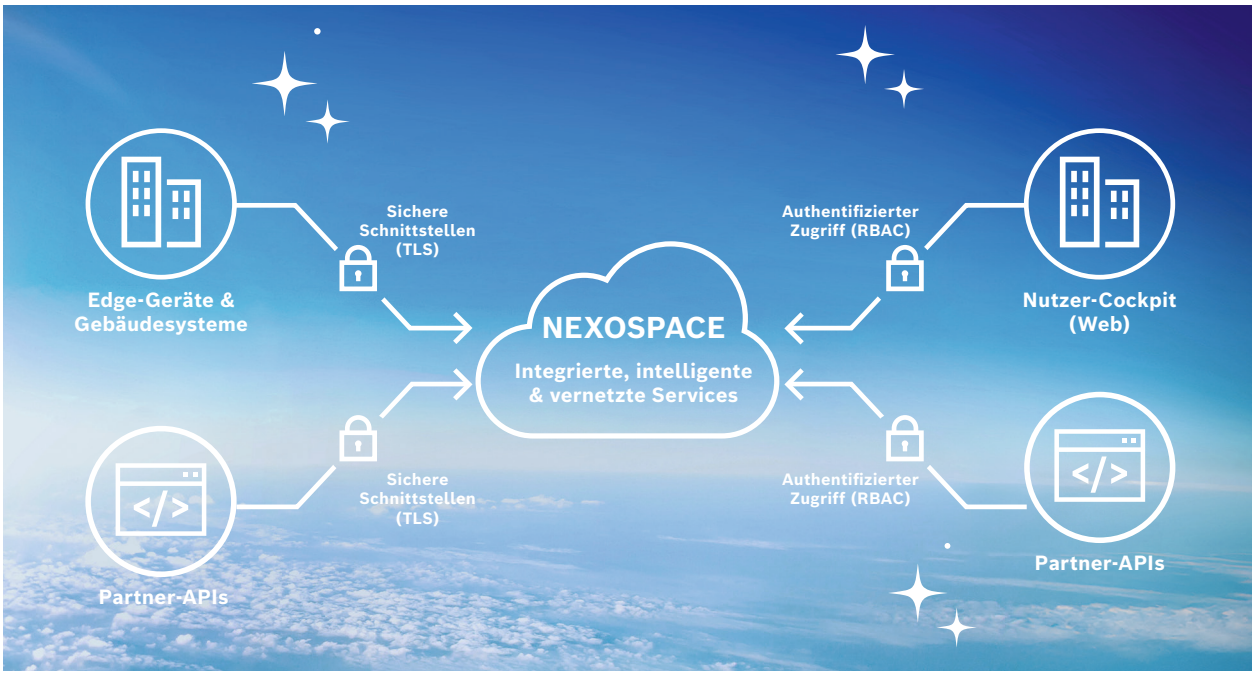
Der Zugriff auf Systeme und Dienste erfolgt ausschließlich über personalisierte Benutzerkonten gemäß den Bosch IT-Standards.

Die Vergabe von Berechtigungen basiert konsequent auf dem Prinzip der minimalen Rechtevergabe (Least Privilege) sowie der Funktionstrennung (Separation of Duties). Die Verwaltung der Zugriffsrechte erfolgt rollenbasiert (RBAC), wobei Berechtigungen mittels Infrastructure-as-Codes (IaC) kontrolliert bereitgestellt, versioniert und nachvollziehbar verwaltet werden.

Auf Ebene der Cloud-Infrastruktur kommen etablierte Sicherheitsmechanismen von Microsoft Azure zum Einsatz. Hierzu zählen insbesondere Privileged Identity Management (PIM) zur kontrollierten und zeitlich begrenzten Vergabe privilegierter Berechtigungen in sicherheitskritischen Bereichen sowie Azure Bastion für einen abgesicherten Zugriff auf Infrastrukturressourcen, beispielsweise innerhalb von AKS-Clustern.

Für die Authentifizierung zwischen Cloud-Services werden ausschließlich Managed Identities verwendet, um eine sichere, schlüssellose Service-zu-Service-Kommunikation sicherzustellen. Die Benutzerauthentifizierung erfolgt über OAuth-2.0-basierte Verfahren unter Nutzung freigegebener Identity Provider wie Microsoft Entra ID oder Bosch SingleKey ID. Bei Bedarf können zusätzlich kundeneigene Identity Provider integriert werden.

Der Zugriff auf Anwendungen erfolgt tenant-spezifisch und rollenbasiert auf Grundlage definierter Berechtigungskonzepte. Die Kommunikation zwischen Gateways, Cloud-Diensten und Endgeräten erfolgt ausschließlich über verschlüsselte und gegenseitig authentifizierte Verbindungen. Der gesamte Lebenszyklus von Identitäten und Berechtigungen – einschließlich Vergabe, Änderung und Entzug von Zugriffsrechten – wird durch definierte organisatorische Prozesse gesteuert, regelmäßig überprüft und revisionssicher dokumentiert.



5. Schwachstellen- & Incident-Management

Das Management von Schwachstellen und Sicherheitsvorfällen erfolgt gemäß den etablierten Prozessen und Richtlinien des Bosch CERT.

Veröffentlichte Sicherheitsmeldungen sowie neu bekannt gewordene Schwachstellen werden kontinuierlich analysiert und hinsichtlich möglicher Auswirkungen auf die NEXOSPACE Service-Produkte sowie die zugrunde liegende Cloud-Infrastruktur bewertet. Identifizierte Risiken werden risikobasiert priorisiert, dokumentiert und im Rahmen definierter Vulnerability- und Patch-Management-Prozesse behandelt.

Die eingesetzten Cloud-Services werden fortlaufend mit Microsoft Defender for Cloud überwacht. Sicherheitsrelevante Ereignisse, Fehlkonfigurationen und identifizierte Schwachstellen werden analysiert und zeitnah behoben. Ergänzend erfolgt eine unabhängige Sicherheitsüberwachung der Cloud-Infrastruktur durch interne Bosch Security-Teams (Bosch BD), um zusätzliche Kontroll- und Eskalationsmechanismen sicherzustellen.

Auf Anwendungsebene werden Sicherheitsprüfungen sowohl während des Softwareentwicklungsprozesses als auch im laufenden Betrieb durchgeführt. Dazu gehören automatisierte Sicherheits- und Compliance-Prüfungen innerhalb der CI/CD-Pipelines, einschließlich der Analyse von Softwareabhängigkeiten, Container-Images und verwendeten Bibliotheken. Container sowie Laufzeitumgebungen werden regelmäßig überprüft. Erkannte Schwachstellen – beispielsweise in Base Images, Frameworks oder Drittanbieterkomponenten – werden im Rahmen definierter Update- und Patch-Management-Prozesse zeitnah behoben.
Sicherheitsvorfälle werden gemäß den etablierten Incident-Response-Prozessen des Bosch CERT erfasst, bewertet und behandelt. Dies umfasst die strukturierte Dokumentation, Ursachenanalyse sowie die Ableitung und Umsetzung geeigneter Gegenmaßnahmen, um potenzielle Auswirkungen zu minimieren und zukünftige Risiken nachhaltig zu reduzieren.

6. Spezifische Sicherheits-maßnahmen

Zur Absicherung der bereitgestellten NEXOSPACE Services werden umfassende technische und organisatorische Sicherheitsmaßnahmen umgesetzt.

Externe Schnittstellen sowie Benutzerzugänge (APIs und Cockpits) werden durch eine Web Application Firewall (WAF) sowie Azure DDoS Protection gegen Angriffe und Überlastungsszenarien geschützt.

Die gesamte Cloud-Infrastruktur ist vollständig als Infrastructure as Code (IaC) modelliert, einschließlich aller sicherheitsrelevanten Konfigurationen und Zugriffskontrollen. Deployments erfolgen ausschließlich automatisiert über CI/CD-Agents im Rahmen etablierter DevOps-Prozesse; manuelle Änderungen durch Betriebsteams sind ausgeschlossen. Der Zugriff auf privilegierte Infrastrukturressourcen wird zentral über Microsoft Privileged Identity Management (PIM) gesteuert und zeitlich sowie kontextbezogen begrenzt.

Alle Azure-Ressourcen werden gemäß den geltenden Bosch-Sicherheitsvorgaben kontinuierlich durch Microsoft Defender for Cloud überwacht. Der Betrieb der Services erfolgt auf Basis eines Bosch Implementation Guides für sichere Cloud-Betriebsmodelle und definierte Best Practices.

Zur Absicherung der Software-Lieferkette werden Open-Source- und Drittanbieterabhängigkeiten automatisiert analysiert und überwacht. In jedem Build-Prozess werden verwendete Bibliotheken geprüft, eine Software Bill of Materials (SBOM) erstellt und ausschließlich freigegebene Komponenten aus einer definierten Allowlist verwendet. Darüber hinaus werden Container-Images sowie Laufzeitumgebungen kontinuierlich auf bekannte Schwachstellen überprüft und entsprechend der Risikobewertung zeitnah aktualisiert.

In jedem DevOps-Team ist ein Security Responsible benannt, die sicherheitsrelevanten Anforderungen innerhalb der Entwicklungs- und Betriebsprozesse koordiniert. Diese Rolle wird durch eine zentrale Sicherheitsorganisation unterstützt, die den bereichsübergreifenden Austausch, die Weiterentwicklung von Sicherheitsstandards sowie Schulungs- und Awareness-Maßnahmen verantwortet.

Durch die Kombination aus technischen Schutzmaßnahmen, automatisierten Sicherheitsprüfungen und klar definierten Verantwortlichkeiten wird ein durchgängiger Security-by-Design- und DevSecOps-Ansatz umgesetzt. Sicherheitsanforderungen werden über den gesamten Lebenszyklus der Services – von der Entwicklung über das Deployment bis hin zum Betrieb – konsequent berücksichtigt. Alle Maßnahmen folgen einem risikobasierten Ansatz und werden kontinuierlich überprüft sowie im Sinne einer fortlaufenden Verbesserung des Sicherheitsniveaus weiterentwickelt.

7. Zusammenfassung

NEXOSPACE wurde mit dem Ziel entwickelt, digitale Gebäudeservices bereitzustellen, die höchste Anforderungen an Informationssicherheit, Datenschutz und Verfügbarkeit erfüllen.

Die in diesem Dokument beschriebenen Maßnahmen zeigen, wie Sicherheitsanforderungen konsequent in Architektur, Entwicklungsprozesse und Betriebsabläufe integriert werden. Von der europäischen Cloud-Infrastruktur über moderne Verschlüsselungs- und Authentifizierungsverfahren bis hin zu einem strukturierten Schwachstellen- und Incident-Management verfolgt NEXOSPACE einen ganzheitlichen Security-by-Design-Ansatz. Sicherheit verstehen wir dabei nicht als einmalige Maßnahme, sondern als kontinuierlichen Prozess. Technologische Entwicklungen, neue Bedrohungsszenarien und steigende regulatorische Anforderungen werden fortlaufend bewertet und in die Weiterentwicklung unserer Plattform integriert. So stellen wir sicher, dass unsere Kunden auch künftig von einer sicheren, skalierbaren und zukunftsfähigen Lösung profitieren.

Sie möchten die digitalen Services von NEXOSPACE für den Brandschutz im Detail kennenlernen?

Erfahren Sie auf unserer Website mehr und kontaktieren Sie uns für ein persönliches Gespräch. Gemeinsam gestalten wir die sichere Digitalisierung Ihrer Brandmeldeanlagen.

DEUTSCHLAND:

NEXOSPACE Fire System Analyzer
Mit dem Brandschutz-Dashboard behalten Sie überall und zu jeder Zeit den Überblick über Ihre Brandmeldeanlagen.

Jetzt entdecken

DEUTSCHLAND:

NEXOSPACE Fire System Observer
Die 24/7-Cloud-Observation überwacht Ihre Melder kontinuierlich und sorgt für einen ungestörten Geschäftsbetrieb dank digitaler Instandhaltung.

Jetzt entdecken

INTERNATIONAL:

NEXOSPACE Fire System Explorer
Maximale Kundenzufriedenheit durch intelligente, rund um die Uhr überwachte Brandmeldeanlagen.

Jetzt entdecken

Performance built on Partnership

Ihr Gebäude kann mehr – mit unseren smarten Lösungen.

Seit über 100 Jahren verbinden wir technisches Know-how mit Leidenschaft, um Menschen und ihre Umgebung zu schützen.

Als einer der weltweit führenden Systemintegratoren bieten wir maßgeschneiderte Lösungen für Gebäudesicherheit, Brandschutz, Gebäudeautomation und Energieeffizienz. Neben unseren eigenen Brandschutztechnologien und digitalen Services setzen wir dabei auf die besten Produkte am Markt.

Von der Beratung bis zum Service begleiten wir Sie über den gesamten Gebäudelebenszyklus – immer an Ihrer Seite.

Bosch Building Technologies

Fritz-Schäffer-Straße 9
81737 München | DEUTSCHLAND

Telefon Deutschland 0800 7000 444
boschbuildingtechnologies.de
buildingtechnologies.el@bosch.com