Sicherheitserklärung

Stand: Januar 2024

Inhaltsübersicht

1. Unser Unternehmen und unser Produkt

Wir sind ein IT-Unternehmen aus Krakau, das 2017 gegründet wurde. Wir haben das innovative QRmaint CMMS -System entwickelt und verbessern es bis heute kontinuierlich mit praktischen Tipps von vielen unserer Kunden.

Unser Ziel ist es, CMMS-Systeme in Produktionsanlagen und in der breit verstandenen Instandhaltung weiter zu verbreiten. Wir konzentrieren uns auf einfache und wirksame Lösungen, die für alle zugänglich sind.

Das QRmaint CMMS-Produkt wird als Software-as-a-Service (SaaS)-Modell angeboten. Die Lösung ist für unsere Kunden über eine Webanwendung, eine Mobile Applikation oder über Application Programming Interfaces (APIs) verfügbar.

2. QRmaint Sicherheit und Risikomanagement

Das oberste Sicherheitsziel von QRmaint ist der Schutz der Daten unserer Kunden und Nutzer. Dies ist einer der Gründe, warum unser Unternehmen in eine angemessene Infrastruktur und andere Ressourcen investiert hat, um ein Höchstmaß an Sicherheit zu gewährleisten. Unser Schwerpunkt liegt auf der Definition neuer und der Verbesserung bestehender Kontrollmechanismen, der Verwaltung der Sicherheitsstruktur von QRmaint und ihrer kontinuierlichen Weiterentwicklung.

3. Unsere Ziele im Bereich Sicherheit und Risikomanagement

Wir haben unsere Sicherheitsrahmen auf der Grundlage bewährter Verfahren in der SaaS-Branche entwickelt. Unsere Hauptziele sind:

- Kundenvertrauen - wir bieten unseren Kunden stets Produkte und Dienstleistungen von höchster Qualität und schützen gleichzeitig die Privatsphäre und Vertraulichkeit ihrer Daten.
- Verfügbarkeit und Geschäftskontinuität - wir sind uns bewusst, wie wichtig es für unsere Kunden ist, dass unsere Anwendung und andere Dienste kontinuierlich verfügbar sind. Daher minimieren wir Sicherheitsrisiken, die die Kontinuität der Dienste gefährden, zu jeder Zeit.
- Einhaltung von Standards - wir implementieren Prozesse und Kontrollen, die den aktuellen internationalen Vorschriften und den Best-Practice-Richtlinien der Branche entsprechen. Wir haben unser Sicherheitsprogramm in Übereinstimmung mit den besten Richtlinien bezüglich der Cloud-Sicherheit entwickelt.

4. Sicherheitskontrolle

4.1.1. Sicherheit von Datenzentrum

QRmaint lagert das Infrastruktur-Hosting seiner Produkte an einen führenden Cloud-Infrastruktur-Anbieter aus. Das sind die Amazon Web Services (AWS). Diese Lösung bietet ein Höchstmaß an physischer und Netzwerksicherheit. Derzeit befinden sich die Cloud-Server-Instanzen von QRmaint in Deutschland. Das Datenzentrum erfüllt die Anforderungen von SOC 2 und ISO 27001 -Normen. Die Qualität der Sicherheit des AWS-Datenzentrums wird durch

die Tatsache belegt, dass große US-Banken ihre Datenzentren zu Amazon AWS verlagern, da sie ein so hohes Sicherheitsniveau nicht erreichen können.

Dieser Infrastrukturanbieter von Weltrang verwendet die fortschrittlichsten Gebäudeinfrastrukturtechnologien für Stromversorgung, Netzwerk und physische Sicherheit. Eine Betriebszeit von 99,95 % bis 100 % wird garantiert, und die Einrichtungen bieten mindestens einen N+1-Überschuss für die Strom-, Netzwerk- und HVAC-Infrastruktur. Der Zugang zu den Datenzentren ist sowohl auf den physischen als auch auf den elektronischen Zugang strikt über öffentliche Netze (Internet) und private Netze (Intranet) beschränkt, um unerwünschte Unterbrechungen des Dienstes auszuschließen.

Die physischen, ökologischen und infrastrukturellen Sicherheitsvorkehrungen, einschließlich der Kontinuitäts- und Wiederherstellungspläne, wurden durch die Zertifizierung nach SOC 2 Typ II und ISO 27001 validiert. Die Zertifizierungen sind auf der Website verfügbar: AWS Cloud-Einhaltung

4.1.2 Netzsicherheit

Die QRmaint-Produktinfrastruktur wurde mit Blick auf die Sicherheit bei der Bereitstellung von Diensten über das Internet entwickelt. Die Netzsicherheit soll insbesondere den unbefugten Zugriff auf das Netz von außerhalb und innerhalb der internen Infrastruktur des Produkts verhindern. Zu diesen Sicherheitsmechanismen gehören Routing der Enterprise Klasse und Firewall-Netzzugangssicherheit (Damm). Diese Technologien blockieren standardmäßig unbeabsichtigten Datenverkehr, und der gesamte Netzwerkverkehr wird protokolliert und zur Information für unsere Überwachungssysteme verwendet. Netzzugangsregeln ermöglichen eine präzise Kontrolle des Netzverkehrs aus dem öffentlichen Netz. Innerhalb der Infrastruktur ermöglichen interne Netzbeschränkungen einen abgestuften Ansatz, um sicherzustellen, dass nur die geeigneten Gerätetypen kommunizieren können.

4.1.3 Konfigurationsmanagement

Die Infrastruktur von QRmaint ermöglicht eine Skalierung gemäß den Bedürfnissen unserer Kunden Die Infrastruktur des Produkts ist eine Umgebung, die ihre Kapazität und Fähigkeiten bei Bedarf flexibel erweitern kann.

4.1.4 Zugang zur Infrastruktur

Ein gut durchdachtes Zugangskontrollmodell verhindert potenzielle Sicherheitsvorfälle. Daher ist der Zugang zu QRmaint-Systemen streng kontrolliert. Die Mitarbeiter von QRmaint erhalten den Zugriff auf die Produktinfrastrukturdienste des Unternehmens auf der Grundlage ihrer Arbeit unter Anwendung des rollenbasierten Zugangskontrollmodells. Der Zugang zu Infrastruktur-Tools, Servern und ähnlichen Dienstleistungen ist nur denjenigen vorbehalten, deren Arbeit es erfordert.

4.2 Schutz von Applikationen

4.2.1 Schutz von Web- und mobilen Applikationen

Alle Kundeninhalte, die auf der Plattform gehostet werden, sind automatisch geschützt. Die Regeln zur Erkennung und Blockierung von bösartigem Datenverkehr stimmen mit den Richtlinien bezüglich der bewährten Verfahren überein, die im Projekt Open Web Application

Security Project (OWASP) dokumentiert sind. Der Schutz vor Distributed Denial of Service (DDoS)-Angriffen ist ebenfalls enthalten, um die kontinuierliche Verfügbarkeit der QRmaint-Dienste und -Produkte zu gewährleisten. Diese Tools überwachen proaktiv den Datenverkehr auf der Anwendungsebene in Echtzeit, was die Warnung vor bösartigem Verhalten und dessen Ablehnung aufgrund der Art und Häufigkeit ermöglicht.

Der Schutz der Daten unserer Kunden hat für uns oberste Priorität, daher ist die Sicherung unseres Dienstes von entscheidender Bedeutung. Das Sicherheitsteam arbeitet ständig an der Verbesserung der Sicherheitsmechanismen, einschließlich CSRF, XSS, SQLi, Sitzungsmanagement, URL-Umleitung und Clickjacking.

4.2.2 Neues Versionsmanagement

Eine der größten Stärken von QRmaint ist das sich schnell entwickelnde Funktionsangebot und die ständige Verbesserung des Produkts durch einen modernen Ansatz zur kontinuierlichen Softwarebereitstellung. Ein neuer Code wird mehrfach getestet, validiert, zusammengeführt und eingeführt. Code-Reviews zur Qualitätssicherung werden von spezialisierten Teams von Ingenieuren durchgeführt, die über fundierte Kenntnisse der QRmaint-Plattform verfügen. Nach der Freigabe wird der Code automatisch in die QRmaint-Umgebung hochgeladen, wo er kompiliert, verpackt und getestet wird. Wenn alle Anforderungen erfüllt sind, wird der neue Code automatisch in der Anwendungsschicht bereitgestellt.

4.3 Schutz von Kundendaten

4.3.1 Vertrauliche Informationen

QRmaint ist ein Produkt, das die Wartungsprozesse von Anlagen und Geräten in Unternehmen unterstützt. In Übereinstimmung mit den Allgemeinen Geschäftsbedingungen und der Datenschutzerklärung stellen die Kunden sicher, dass sie nur relevante Informationen zur Unterstützung ihrer Wartungsprozesse speichern. QRmaint-Produkte werden nicht verwendet, um sensible Daten wie Zahlungskartennummern, persönliche Bankkontoinformationen, PESEL-Nummern, Reisepassnummern, Führerscheinnummern oder ähnliche Dokumente oder Informationen zu Beschäftigung, Finanzen oder Gesundheit zu sammeln oder zu speichern.

4.3.2 Schutz von Kreditkartendaten

Viele QRmaint-Kunden zahlen für die Dienstleistungen per Kreditkarte. QRmaint speichert, verarbeitet oder sammelt keine Kreditkarteninformationen, die uns von Kunden zur Verfügung gestellt werden. Wir arbeiten mit vertrauenswürdigen und PCI-konformen Zahlungsdienstleistern (DotPay) zusammen, um sicherzustellen, dass die Kreditkartendaten unserer Kunden sicher und in Übereinstimmung mit den einschlägigen Vorschriften und Branchenstandards verarbeitet werden.

4.3.3 Verschlüsselung

Alle Interaktionen mit QRmaint-Produkten (z.B. API-Aufrufe, Logins, authentifizierte Sitzungen zum Kundenportal, etc.) werden während der Übertragung mit TLS-Schlüsseln 1.0, 1.1, 1.2 oder 1.3 und 2048 Bit oder besser verschlüsselt.

QRmaint verwendet mehrere Technologien, um die Verschlüsselung der gespeicherten Daten

zu gewährleisten. Die physischen und virtualisierten Festplatten, die von den Serverinstanzen des QRmaint-Produkts verwendet werden sowie Langzeitspeicherlösungen wie AWS S3 verwenden AES-256-Verschlüsselung.

4.4 Datenschutz

Der Schutz der Daten unserer Kunden ist einer der Hauptaspekte, auf die wir uns bei QRmaint konzentrieren. Wie in unserer Datenschutzrichtlinie beschrieben, geben wir Ihre persönlichen Daten niemals an Dritte weiter. Die in diesem Dokument beschriebenen Sicherheitsvorkehrungen und andere von uns eingeführte Schutzmaßnahmen sollen sicherstellen, dass Ihre Daten vertraulich bleiben und nicht verändert werden. QRmaint wurde mit Blick auf die Bedürfnisse der Kunden und den Schutz der Privatsphäre entwickelt und gebaut. Unser Datenschutzprogramm berücksichtigt bewährte Methoden, die Bedürfnisse der Kunden und ihrer Ansprechpartner sowie die gesetzlichen Anforderungen.

4.4.1 Politik der Datenaufbewahrung

Die Kundendaten werden so lange aufbewahrt, wie lange Sie unser aktiver Kunde bleiben. Die QRmaint-Plattform bietet aktiven Kunden die Möglichkeit, ihre Daten nach eigenem Ermessen zu löschen. Die Daten ehemaliger Kunden werden auf schriftlichen oder elektronischen Antrag des Kunden oder nach Ablauf einer bestimmten Frist nach Beendigung aller Verträge aus den aktiven Datenbanken gelöscht. Die Daten von kostenlosen Testkunden Free trial werden gelöscht, wenn das Portal nicht mehr aktiv genutzt wird, und die Daten ehemaliger zahlender Kunden werden 90 Tage nach Beendigung aller Beziehungen gelöscht. In Repliken, Snapshots und Backups gespeicherte Informationen werden nicht aktiv gelöscht, sondern altern ganz natürlich in den Repositoria mit dem Fortschreiten des Datenlebenszyklus.

4.5 Kontinuität von Geschäftsprozessen und Datenwiederherstellung

QRmaint kümmert sich um die Entwicklung von Prozessen, die die Geschäftskontinuität und Wiederherstellungspläne nach einem Ausfall sicherstellen, und konzentriert sich dabei sowohl auf die Vorbeugung von Ausfällen als auch auf schnelle Wiederherstellungsstrategien bei Verfügbarkeits- oder Leistungsproblemen. Wann immer Situationen auftreten, die Kunden betreffen, ist es das Ziel von QRmaint, das Problem schnell und transparent zu isolieren und zu lösen.

4.5.1 Ersatzkopien (Backups)

Wir erstellen täglich Sicherheitskopien der Daten unserer Kunden und speichern diese auf separaten Servern. Die Aufbewahrungsfrist der Backups hängt von der Art der Daten ab.

5. Geltungsbereich und Anwendung des Dokuments

QRmaint legt Wert auf Transparenz in der Art und Weise, wie wir unseren Kunden Lösungen anbieten. Dieses Dokument wurde unter dem Gesichtspunkt der Transparenz erstellt. Wir arbeiten ständig an der Verbesserung der bereits eingeführten Sicherheitsvorkehrungen. Die Daten in diesem Dokument sind nicht dazu gedacht, eine verbindliche oder vertragliche Verpflichtung zwischen QRmaint und anderen Parteien zu schaffen, noch ändern sie eine bestehende Vereinbarung zwischen den Parteien.