Standard-Richtlinien und Verfahren

Datensicherheit

Quinyx

Inhalt

Quinyx Datensicherheit

Dieses Dokument beschreibt, wie Quinyx die Sicherheit und Integrität in Bezug auf die Bereitstellung des Workforce Management Services verwaltet.

Hosting-Partner

Quinyx hat Amazon AWS als Hosting-Partner ausgewählt. Primärregionen sind Frankfurt (EU) und North Virginia (US), die über mindestens zwei Verfügbarkeitszonen pro Region verteilt sind. Sekundäre Regionen sind Irland (EU) und Oregon (USA).

Jeder interne Dienst ist in mindestens zwei Verfügbarkeitszonen aktiv und über Proxies lastverteilt. Alle Dienste können den Ausfall einer einzelnen Zone bewältigen. Quinyx bietet eine hochredundante und skalierbare Plattform.

Systemsicherheit

Physische Sicherheit

Die Quinyx Hosting-Umgebung ist eine vollständig redundante und skalierbare Lösung gehostet in AWS-Hosting-Umgebung. Sie erfüllt ISO 27001 für Sicherheitsanforderungen, ISO 27017 für Cloud-Sicherheit und ISO 27018 für Cloud Datenschutz, was die Einhaltung der DSGVO gewährleistet.

(Lesen Sie mehr über die physische Sicherheit und den Zugriff der AWS-Hosting-Umgebung unter: https://aws.amazon.com/compliance/, insbesondere AWS Security White Paper Physical and Environmental Security).

Betriebssystem-Sicherheit

Wir haben eine konservative Upgrade-Richtlinie, bei der wir Sicherheitshinweise erhalten, diese analysieren und entscheiden, ob sie für uns oder unsere Kunden vor dem Upgrade einen verwertbaren Angriffsvektor darstellen. Auf allen Servern werden Linux-Betriebssysteme eingesetzt, die für die Nutzung des jeweiligen Servers ausgelegt sind.

Anwendungssicherheit

Der Zugriff auf die Anwendung und die gespeicherten Daten ist unabhängig von der Benutzerrolle durch eine persönliche Kennung wie E-Mail-Adresse oder Login-ID und Passwort gesichert. Daten, die für den Zugang zum Kunden genutzt werden können und Benutzerdaten, wie z.B. Passwörter, werden in verschlüsseltem Format gespeichert. Der Kunde kann seinen Nutzern eine erhöhte Passwortsicherheitsstufe auferlegen, welche erfordert, dass Passwörter

- mindestens 8 Zeichen lang sind und mindestens zwei numerische Zeichen und zwei alphabetische Zeichen enthalten.
- mindestens einmal alle drei Monate geändert werden und während eines Zeitraums von 30 Monaten oder 10 aufeinander folgenden Monaten nicht wieder verwendet werden.

Zugriff auf den vollständigen Datensatz erhalten nur die Vertreter von Quinyx, die ihn unbedingt zur Durchführung ihrer Arbeit benötigen. Quinyx überprüft diesen Zugang routinemäßig, um festzustellen, ob je nach den aktuellen Bedürfnissen des Vertreters Gründe für einen Widerruf vorliegen.

Alle Quinyx-Vertreter unterliegen Vertraulichkeitsvereinbarungen und werden im Rahmen ihrer Einweisung in Best-Practice-Datensicherheitsverfahren geschult. Alle digitalen Arbeitsumgebungen werden mit einem zentralen Authentifizierungsmechanismus gesichert, der sicherstellt, dass die Benutzer nur auf die Daten in der jeweiligen Softwareanwendung zugreifen können, die für die Erfüllung der Vereinbarung von Quinyx mit dem Kunden benötigt wird.

Die Anwendung wird durch serverseitige Validierungen bewacht, die auf der tatsächlichen und gespeicherten Rolle und den Zugriffsrechten des Benutzers basieren. Nur Daten, die für den angegebenen Benutzer gültig und erlaubt sind, werden an die Client-Anwendungsschicht übertragen, um sicherzustellen, dass keine Daten verloren gehen. Die gesamte Kommunikation zwischen der Client-Software und den Anwendungen von Drittanbietern wird mit SSL unter Verwendung von SHA-256 (512 Bit) mit RSA-Verschlüsselung verschlüsselt.

Mobile Sicherheit

Der Zugriff auf die mobile Anwendung wird zusätzlich zu den oben genannten Anwendungssicherheitsmaßnahmen durch TLS (Transport Level Security) und Anwendungssicherheit geschützt. Die Anwendungssicherheit mobiler Anwendungen basiert auf den neuesten Sicherheitsstandards für die Authentifizierung und Autorisierung des Benutzerzugriffs. Die Authentifizierungsregeln sind wie oben beschrieben anwendbar. Die Autorisierung basiert auf dem OAuth2-Standard in Kombination mit JWT (Json-Web-Token). Alle Autorisierungsdetails, die über das Netzwerk weitergegeben werden, sind:

- digital signiert (JWS) mit SHA-256 (2048 Bit RSA-Algorithmus-Schlüssel)
- und verschlüsselt (JWE mit 256 Bit AES-Algorithmus-Schlüssel).
- All dies erfolgt zusätzlich zum Schutz auf Transportebene durch die oben genannten Verschlüsselungsmethoden.

API Sicherheit

Einer der von Quinyx bereitgestellten Datenkanäle ist der Zugriff über API. Der API-Zugriff ist hochgradig gesichert und verfügt über mehrere Schutzebenen, darunter TLS, Netzwerksicherheit, Anwendungssicherheit und Sicherheits-Gateways. Effiziente Komponenten einer solchen Architektur garantieren ein hohes Maß an Kundendaten-

Sicherheit. Die Implementierung der API-Sicherheit basiert auf den neuesten Sicherheitsstandards.

API-Authentifizierungskontrollen

Die API-Sicherheit erfordert strengere Richtlinien bezüglich der Länge und Komplexität (mindestens 2 Mal stärker) der Berechtigungsnachweise als die oben im Abschnitt Anwendungssicherheit beschriebenen. Die Anmeldedaten des Kunden (API-Integrators) werden in den Systemen von Quinyx niemals als Klartext gespeichert, sondern mit Hilfe von starken Hashing-Techniken gehasht - was die Möglichkeit eines unbefugten Zugriffs von internen Quinyx-Systemen ausschließt.

API-Berechtigungskontrollen

Zur Unterstützung der Verwaltung des Zugriffs gibt es strenge Kontrollen der API-Zugriffsberechtigungen, so dass der Zugriff effizient aktiviert und bei Bedarf widerrufen werden kann. Die API-Autorisierung verwendet verschiedene Techniken, einschließlich des OAuth2-Standards in Kombination mit JWT. In diesem Szenario sind die Berechtigungsdetails:

- digital signiert (JWS) mit SHA-256 (2048 Bit RSA-Algorithmus-Schlüssel)
- und verschlüsselt (JWE mit 256 Bit AES-Algorithmus-Schlüssel).
- All dies erfolgt zusätzlich zu Verschlüsselungsmethoden, die oben im Abschnitt Anwendungssicherheit aufgeführt sind.

API-Sicherheits-Gateways

API-Gateways bieten eine zusätzliche Sicherheitsebene in Kombination mit anderen Maßnahmen, wie z.B. Netzwerksicherheit. API-Gateways unterstützen die sichere Weiterleitung von autorisiertem Datenverkehr an die internen Dienste, so dass die internen Systeme von Quinyx nicht gefährdet werden. Diese garantieren auch den zusätzlichen Schutz der gesamten API-Schicht, wodurch ein wirksamer Schutz vor unerwarteter Last (Leistungsschalter, Durchsatzgrenzen) gewährleistet wird - was den Gesamtstatus der Abwehrmechanismen der API-Schicht verbessert.

Netzwerk-Sicherheit

Quinyx verwendet einen zentralisierten Authentifizierungsmechanismus für alle Server einschließlich der Testumgebungen. Er ist gruppenbasiert mit minimalen Rechten für die Benutzer, die nach Bedarf gewährt werden.

Kundendaten-Sicherheit

Datenbank

Der Zugriff auf die Datenbank ist nur Systemadministratoren gestattet, um ihre obligatorischen Aufgaben zu erledigen. Der Lese-Zugriff ist nur dann erlaubt, wenn die Vertreter für Zwecke wie Fehlersuche und Support über eine entsprechende Grundlage verfügen.

Daten auf Blockebene

Daten im Ruhezustand werden mit Hilfe von Mechanismen verschlüsselt, die in die Plattform des Hosting-Providers eingebaut sind, und zwar mit Schlüsseln auf einem HSM (Hardware-Sicherheitsmodul), zu denen der Provider nicht mehr als physischen und log-Zugang hat.

Trennung von Umgebungen

Entwicklungs-, Test-, Staging- und Produktionsumgebungen sind auf verschiedenen Servern und Netzwerksegmenten getrennt und nicht logisch miteinander verbunden. Alle aufgeführten Umgebungen werden mit den gleichen Sicherheitsstufen gehostet, als ob es sich um eine Produktionsumgebung handeln würde.

Protokollierung von Datenänderungen

Alle Änderungen an kritischen Anwendungsdaten wie Zugriffsrechten, Vereinbarungsvorlagen, individuellen Vereinbarungen, Benutzern, Planungseinheiten, Zeitplan und Zeitstempeln werden protokolliert, unabhängig davon, ob sie von Quinyx-Vertretern im Namen des Kunden oder von den Benutzern des Kunden selbst durchgeführt wurden.

Allgemeine Sicherheitsprüfung

Jedes Jahr lädt Quinyx ein externes

Sicherheitsunternehmen ein, unsere Umgebungen zu prüfen und Penetrationstests durchzuführen.

Diese Audits und Tests werden in Berichten zusammengefasst, in denen eventuelle Schwachstellen aufgezeigt werden, die in einem solchen Fall sofort behoben werden.

Backup

Quinyx führt alle drei Stunden vollautomatische Backups von Konfiguration, Code und Daten sowohl auf einem lokalen Speicher als auch auf einem sekundären Standort durch. Die Daten werden außerdem in Echtzeit auf eine Datenbank an einem sekundären Standort kopiert, um im unwahrscheinlichen Fall eines vollständigen Ausfalls in beiden Verfügbarkeitszonen des Hauptstandorts keine Daten zu verlieren. Dies gibt uns ein aktuelles RPO (Recovery Point Objective) von maximal drei Stunden. Backups werden mindestens 30 Tage gespeichert.

Wiederherstellung im Katastrophen- und Eventualfall

Das Hosting wird über mindestens zwei verschiedene Verfügbarkeitszonen am Primärstandort gemeinsam genutzt, und alle Komponenten der Umgebung verfügen über mindestens eine Instanz in jeder Verfügbarkeitszone. Im unwahrscheinlichen Fall einer vollständigen Fehlfunktion in beiden Verfügbarkeitszonen am Primärstandort führt Quinyx den Quinyx Disaster Recovery-Prozess durch. Die Zeit für die Wiederherstellung im Katastrophenfall wird derzeit auf maximal 24 Stunden geschätzt.

Verfügbarkeit

Service-Level-Vereinbarung

Quinyx bietet eine hochgradig redundante und skalierbare Plattform und ein hochgradig skalierbares Produkt. Die Serviceverfügbarkeit ist sehr hoch und beträgt garantiert mindestens 99,5% über 24 Stunden, 7 Tage die Woche, außerhalb der geplanten Wartungsfenster. Die historische Verfügbarkeit beträgt 99,98%. Quinyx aktualisiert die Plattform und das Produkt mindestens alle 30 Tage, und alle Kunden werden mindestens sieiben Tage vor Wartungsfenstern, die die Serviceverfügbarkeit stören könnten, benachrichtigt.