Signals

Whitepaper Sicherheit

Klassifizierung: öffentlich

mazars

Inhaltsübersicht

mazars

Versionskontrolle

Datum	*Version*	*Beschreibung der Änderungen*	*Verantwortlich*
23-11-2021	1.0	Erste Fassung	Vincent Roodenburg
18-03-2022	2.0	Hyperlinks aktualisiert/korrigiert Abschnitt „Sicherheit im Entwicklungsprozess“ hinzugefügt	Vincent Roodenburg
26-05-2022	2.01	Deutsche Überarbeitung (DE-Version)	Andreas Janoschek
31-05-2022	3.0	Aktualisierter Link zur Datenschutzerklärung	Vincent Roodenburg
13-02-2023	4.0	Enthaltener Link zum OKTA-Sicherheits-Whitepaper	Cor van de Merwe

mazars

Einführung in die Signals-Plattform von Mazars

Allgemein

Signals ist die digitale Kollaborationsplattform von Mazars. Mazars Signals ist eine cloudbasierte Plattform, die vollständig responsiv ist und auf Desktop-, Tablet- und Mobilgeräten genutzt werden kann. Die Plattform wird von Mandanten und Mazars-Mitarbeitern für die Online-Zusammenarbeit genutzt. Die wichtigsten Funktionen sind:

- Informationen von unseren Mandanten über „Lieferanfragen“ anzufordern
- Freigabe von Aufgaben durch Workflows
- Einreichen von Steuererklärungen bei lokalen Behörden

Mazars' Signals ist Teil eines Cloud-basierten Systems und fungiert als „Eingangstür“ für alle unsere Mandanten, um mit Mazars zu interagieren. Durch diese Tür können sich die Mandanten bei anderen (Cloud-)Anwendungen anmelden.

Angebotsanfrage

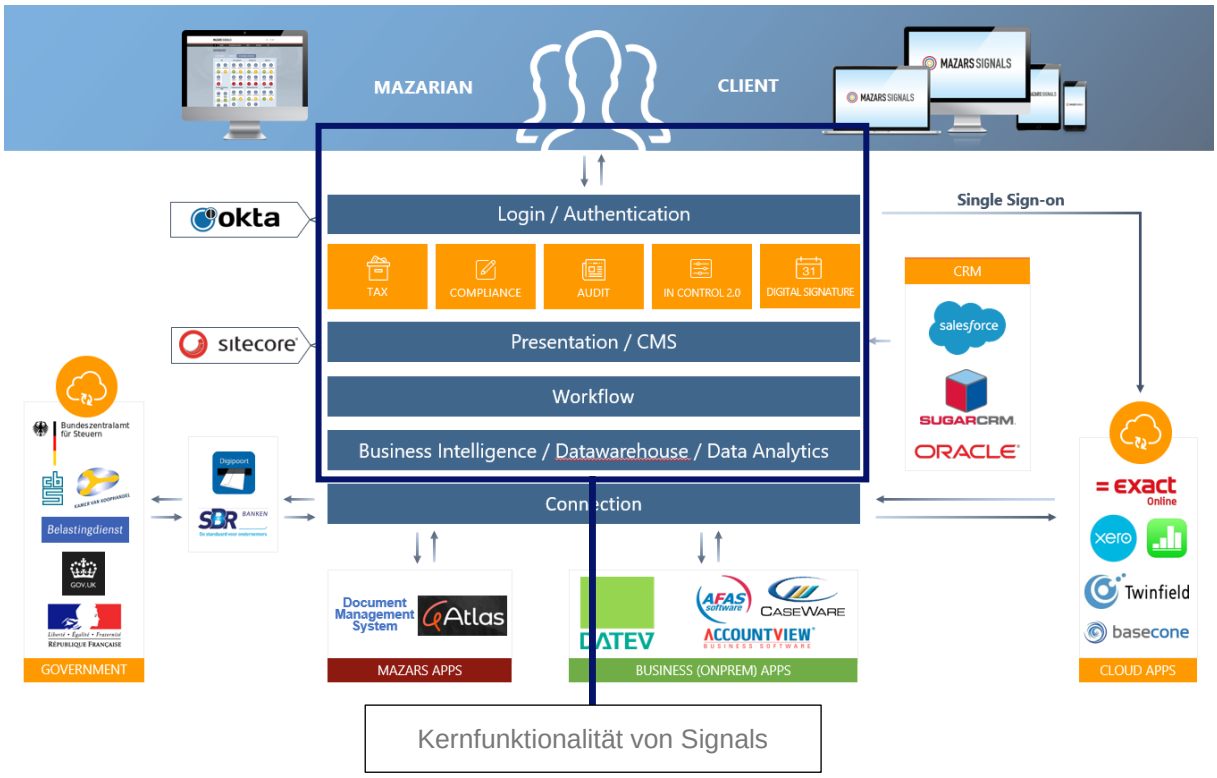
Mazars erstellt eine Anfrage in Signals, um die notwendigen Informationen und Dokumente für die Erbringung von Dienstleistungen anzufordern. Die Mandanten müssen sich in Signals einloggen und die angeforderten Dokumente hochladen. Wenn alle Informationen vorliegen, markiert der Mandant die Anfrage als vollständig und sendet sie an Mazars. Nachdem Mazars die Lieferanfragen genehmigt hat, werden alle Dokumente in Back-Office-Anwendungen gespeichert. Alle Vorgänge im Zusammenhang mit den Lieferanfragen werden in einem Prüfpfad gespeichert.

Arbeitsabläufe und Steuererklärungen

Mazars präsentiert seinen Mandanten die vorbereiteten Arbeiten (Jahresberichte, Steuererklärungen) über Signals. Die Berichte und Steuererklärungen werden in Back-Office-Systemen erstellt und dann in Signals hochgeladen. Die Mandanten können Aufgaben und Erklärungen einreichen, die in einem automatisierten Prozess direkt an die Steuerbehörden weitergeleitet werden. Alle Aktionen, die von Mandanten und Mitarbeitern im Zusammenhang mit den Erklärungen durchgeführt werden, werden in einem vollständigen Prüfpfad gespeichert.

Platform

Diese Abbildung zeigt den Status des Systems um Mazars Signals:



Verschlüsselung

Sowohl ruhende als auch übermittelte Daten werden nach Industriesstandards verschlüsselt. Alle Verschlüsselungsmaßnahmen werden durchgeführt, um die Vertraulichkeit und Integrität der Daten innerhalb von Signals zu gewährleisten.

Datenverwaltung und Einhaltung der Vorschriften

Alle zugehörigen Systeme von Mazars Signals befinden sich in den Niederlanden und Irland (Microsoft Azure West-Europe). Die Datenverarbeitung erfolgt gemäß den Gesetzen und Vorschriften der EU. Um die DSGVO-Anforderungen zu erfüllen, werden keine personenbezogenen Daten (Personally Identifiable Information; PII) über die EU-Grenzen hinaus übertragen. Die Daten unserer Mandanten werden gemäß den gesetzlichen Aufbewahrungsfristen (maximal 10 Jahre) gespeichert.

Seit November 2020 wendet Microsoft zusätzliche Datenschutzmaßnahmen mit der Bezeichnung „Defending your data“ an, um Mandantendaten zu schützen, wie in diesem Artikel beschrieben: New Steps to Defend Your Data - Microsoft On the Issues.

Um mehr über Microsofts zusätzliche Schutzmaßnahmen, insbesondere zu Standardvertragsklauseln, zu erfahren, ist es relevant, das folgende Dokument zur Kenntnis zu nehmen: REFERENCE-COPY-Additional-Safeguards-Addendum-to-Standard-Contractual-Clauses-.pdf (microsoft.com).

(Microsoft's Additional Safeguards Addendum to Standard Contractual Clauses).

Betriebszeit und Zuverlässigkeit

Wir überwachen ständig die Leistung unseres Dienstes und verfügen über automatische Benachrichtigungen, um eine schnelle Reaktion auf mögliche Dienstunterbrechungen zu gewährleisten. Alle Code-Änderungen werden überprüft und genehmigt, bevor sie auf Produktionsservern eingesetzt werden. Wir verfolgen aufmerksam die Aktualisierungen der Sicherheitsgemeinschaft und aktualisieren unsere Systeme sofort, wenn neue Sicherheitslücken entdeckt werden.

Infrastruktur

Hosting

Alle Serversysteme werden in Microsoft Azure in der Region „Westeuropa“ gehostet, mit Amsterdam als primärem Standort und Dublin als sekundärem Standort. Die Rechenzentren von Microsoft erfüllen mehrere Zertifizierungen. Bitte besuchen Sie https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance für alle Details.

Patching-Prozess

Alle zugehörigen Serversysteme werden regelmäßig (mindestens monatlich) gepatcht, um die höchstmöglichen Sicherheitsstandards zu gewährleisten.

Überwachung

Alle zugehörigen Serversysteme werden rund um die Uhr überwacht, um die höchstmögliche Betriebszeit zu gewährleisten. Die Techniker erhalten automatische Warnungen, wenn es zu Störungen kommt, die eine Unterbrechung eines Produktionssystems zur Folge haben könnten.

Sicherheitsmaßnahmen

Bitte informieren Sie sich unter https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security über alle (physischen) Sicherheitsmaßnahmen, die in den Einrichtungen des Microsoft Azure-Rechenzentrums gelten.

Anwendung

Identifizierung, Authentifizierung und Autorisierung

Nur verifizierte Benutzer- und (Mazars-)Mitarbeiterkonten haben Zugang zu Mandantendaten innerhalb der Signals-Plattform von Mazars.

Mandanten authentifizieren sich über die Okta-Plattform, auf der die Multi-Faktor-Authentifizierung (MFA) obligatorisch ist und über die Okta-Verify-App, die für Android und iOS verfügbar ist, angewendet wird. Weitere Informationen über die für die Okta-Plattform geltenden Sicherheitsmaßnahmen finden Sie unter https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/

Mazars-Mitarbeiter, die sich innerhalb des Mazars-Netzwerks anmelden, nutzen die bereits bestehende Anmeldung (Single Sign-on ;SSO) für den Zugriff auf Signals. Abhängig von ihrer Rolle haben Mazars-Mitarbeiter nur Zugriff auf bestimmte Mandantendaten. Funktionale und technische Administratorrollen sind innerhalb der Mazars-Organisation begrenzt. Diese Art von Privilegien werden nur dann gewährt, wenn zusätzliche Hintergrundprüfungen durchgeführt und verifiziert wurden.

Verwaltung

Der Zugang zur Systemverwaltung und Anwendungsentwicklung ist auf eine begrenzte Anzahl von Systemadministratoren und Anwendungsentwicklern beschränkt. Die diesbezüglichen Geheimhaltungs- und Vertraulichkeitsvereinbarungen werden von jedem Systemadministrator und Entwickler, der mit der Durchführung von Systemverwaltungs- und Entwicklungsaufgaben betraut ist, unterzeichnet.

Der Zugang zur Funktionsverwaltung ist auf eine begrenzte Anzahl von Funktionsadministratoren und Mandanten-/Beziehungsmanagern beschränkt. Die entsprechenden Geheimhaltungs- und Vertraulichkeitsvereinbarungen werden von jedem Funktionsadministrator unterzeichnet, der mit der Durchführung von Aufgaben der Funktionsadministration betraut ist.

Entwicklungsprozess

Der Entwicklungsprozess wird auf agile Weise durchgeführt. Mazars stellt den Product Owner, der in einem agilen Entwicklungsprozess eine Schlüsselfunktion einnimmt.

Sicherheit im Entwicklungsprozess

Wir führen Programmcodeprüfungen durch und verwenden statische Codeanalysen, um Sicherheitsrisiken zu ermitteln. Die identifizierten Risiken werden dann bewertet und gegebenenfalls behoben. Wir wenden die folgenden Praktiken aus dem Security Development Lifecycle von Microsoft an:

Verwalten des Sicherheitsrisikos bei der Verwendung von Drittanbieterkomponenten

Wir haben Übersichten darüber erstellt, welche Komponenten von Drittanbietern wir verwenden, und sind dabei, diese Bestandsaufnahme zu automatisieren.

Wir bewerten auch regelmäßig solche Abhängigkeiten, zum Beispiel im Hinblick auf ein nahendes „End-of-Life“-Datum einer solchen Komponente.

Durchführen von Sicherheitstests mit statischer Analyse (SAST)

Wir verwenden SonarCloud zur Identifizierung und Analyse von Sicherheitslücken.

Penetrationstests durchführen

Wir führen Sicherheitstests durch, bevor wir eine neue Anwendung für die Produktion freigeben, und führen mindestens einmal im Jahr einen Penetrationstest durch.

Rollout

Mazars arbeitet mit einem monatlichen Einsatzplan. Jeden Monat ist ein Deployment geplant, in der Regel zwischen dem 14. und dem 20. des Monats. Der Scrum Master entscheidet zusammen mit den Produkteigentümer (Product Owner), welche Arbeiten, die in den 1-2 vorangegangenen Sprints als erledigt markiert wurden, als Inkrement für die Produktionsumgebung freigegeben werden. Das Rollout-Verfahren läuft wie folgt ab:

1. Auswahl der fertiggestellten Storys, die für die Produktionsumgebung freigegeben werden müssen
2. Zusammenführen der Storys aus unserem Entwicklungszweig mit dem Hauptzweig
3. Stellen Sie die Storys in der Haupttestumgebung bereit.
4. Alle Storys werden in der Haupttestumgebung getestet und die gesamte Umgebung wird einem Regressionstest unterzogen.
5. Bereitstellung aller Storys in der Akzeptanzumgebung
6. Die Akzeptanzumgebung wird vollständig regressionsgetestet.
7. Bereitstellung aller Stories in der Produktionsumgebung
8. Nach der Bereitstellung werden Sanity Checks durchgeführt, um die Bereitstellung zu überprüfen. In den Tagen nach der Bereitstellung überprüft das Entwicklungsteam aktiv die Überwachungs- und Protokolldateien.

Nach dem Sprint-Review entscheidet der Product Owner, ob er das neue Inkrement in die Produktionsumgebung einführen will.

Produktfahrplan und langfristige Einschätzungen

Für eine längerfristige Vision gibt es eine Produkt-Roadmap. Der Product Owner ist zusammen mit seinen Stakeholdern der wichtigste Treiber hinter der Produkt-Roadmap. Die Entwickler spielen auch eine Rolle bei der Unterstützung von Mazars bei der Erstellung dieser Roadmap auf strategischer Ebene. Die Produkt-Roadmap sollte die Richtung aufzeigen, in die sich das Produkt entwickelt, und den Wert, den es für Mazars und seine Mandanten haben wird.

Eine Produkt-Roadmap besteht aus „Epics“. Dabei handelt es sich um hochrangige Aufgaben, die zu umfangreich sind, um zusammenhängend bearbeitet zu werden, und die daher in mehrere Abschnitte unterteilt werden, z. B.: digitale Unterzeichnung von Jahresabschlüssen. Für die Roadmap kann das Team zusammen mit dem Product Owner Einschätzungen auf hoher Ebene vornehmen. Diese Schätzungen werden in der Regel schnell vorgenommen, da nicht versucht werden soll, alle Anforderungen im Voraus zu erfüllen. Stattdessen werden High-Level-Einschätzungen vorgenommen, um den erwarteten Umfang der Entwicklung eines Epics anzugeben.

Sobald die Entwicklung beginnt, werden diese Einchätzungen schwanken, da die Storys verfeinert werden und die erforderlichen Ergebnisse für die Storys klarer werden. Es ist immer gut, diese Schwankungen bei der Planung im Auge zu behalten.

Weitere Sicherheitsmaßnahmen

Zusätzlich wird Signals durch Sicherheitskontrollen auf der Anwendungsebene geschützt.

Sicherheitsprüfung

Die Signals-Plattform von Mazars wird regelmäßig von einer unabhängigen Partei auf Sicherheitsschwachstellen getestet, um Objektivität zu gewährleisten. Die Behebung möglicher Schwachstellen wird stets in der Reihenfolge ihrer Kritikalität durchgeführt.

Schutz der Integrität des Audit-Protokolls

Die Protokolldateien und Prüfprotokolle von Signals werden auf virtuellen Festplatten gespeichert, auf denen eine Verschlüsselung der Daten im Ruhezustand angewendet wird. Der Zugriff auf Protokolldateien und Prüfpfade ist auf eine begrenzte Anzahl von Systemadministratoren beschränkt.

Organisation

Privacy

Wir nehmen die Sicherheit und den Schutz der Daten unserer Mandanten sehr ernst und behandeln sie als wichtige Messgröße. Mazars' Signals hält sich an die DSGVO-Vorschriften. Für Länder außerhalb der EU beachten Sie bitte die dort geltenden Datenschutzbestimmungen und, falls zutreffend, zusätzliche Standardvertragsklauseln für Datenübertragungen zwischen EU- und Nicht-EU-Ländern. Einen vollständigen Überblick über unsere Datenschutzpolitik finden Sie unter https://www.mazarssignals.com/en/privacy-statement.

Sicherheitsrichtlinien

Alle Mitarbeiter unterliegen dokumentierten Sicherheitsrichtlinien, welche die zulässige Nutzung, den Umgang mit vertraulichen Daten usw. regeln.

Disaster Recovery (Datensicherung und -wiederherstellung)

Anwendungs- und Mandantendaten werden redundant in mehreren Verfügbarkeitszonen gespeichert, wobei Datensicherungen für die Wiederherstellung im Katastrophenfall verfügbar sind.

Management von Sicherheitsvorfällen

Im Falle einer bestätigten Sicherheitsverletzung, bei der Mandantendaten kompromittiert wurden, wird Sie unser Team umgehend benachrichtigen. Sollten Sie für die Untersuchung eines Vorfalls, von dem Ihr Unternehmen betroffen ist, zusätzliche Protokolle benötigen, wird unser Sicherheitsbeauftragter diese bei Bedarf zur Verfügung stellen.

Zentrale Anlaufstelle für Sicherheit

Um Fragen zu diesem Dokument zu beantworten, senden Sie bitte Ihre Fragen an security@mazars.nl.