Signals

Libro blanco de seguridad

Clasificación: pública

mazars

Índice de contenidos

mazars

Control de versiones

Date	*Versión*	*Descripción de los cambios*	*Responsable*
23-11-2021	1.0	Versión inicial	Vincent Roodenburg
18-03-2022	2.0	- corrección de hipervínculos - Se ha añadido la sección "Seguridad en el proceso de desarrollo".	Vincent Roodenburg
31-05-2000	3.0	Enlace actualizado a la declaración de privacidad	Vincent Roodenburg
13-02-2023	4.0	Enlace incluido al documento técnico de seguridad OKTA	Cor van de Merwe

mazars

Introducción a la plataforma Signals de Mazars

Genérico

Signals es la plataforma de colaboración digital de Mazars. Mazars Signals es una plataforma basada en la nube, totalmente responsiva y que puede utilizarse en ordenadores de sobremesa, tabletas y dispositivos móviles. La plataforma es utilizada por clientes y empleados de Mazars para trabajar juntos en línea. Las principales características son:

- solicitar información a nuestros clientes a través de "solicitudes de suministro
- aprobar tareas a través de flujos de trabajo
- presentar declaraciones de impuestos a las autoridades locales

Mazars' Signals forma parte de un ecosistema basado en la nube y funciona como una "puerta de entrada" para que todos nuestros clientes interactúen con Mazars. A través de esta puerta los clientes pueden acceder a otras aplicaciones (en la nube).

Solicitud de suministros

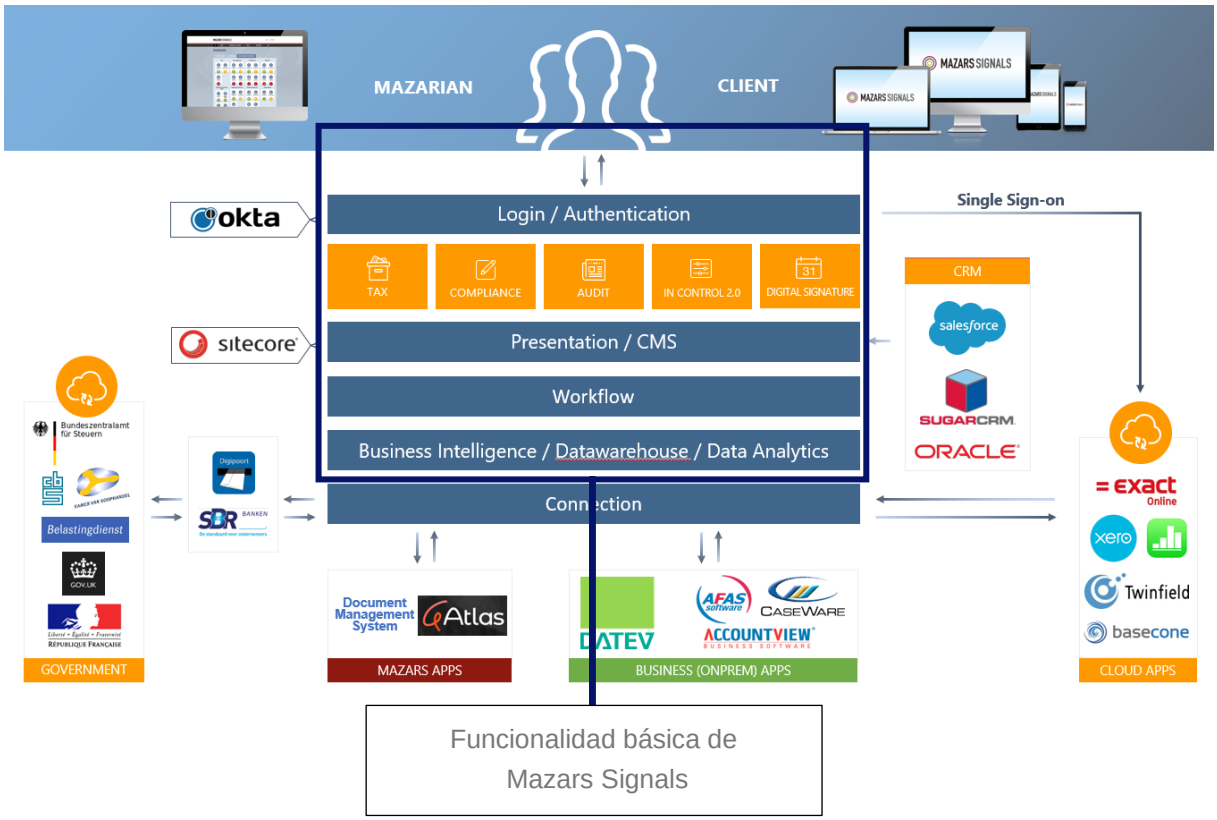
Mazars preparará una solicitud de suministro en Signals para pedir la información y los documentos necesarios para prestar sus servicios. Los clientes tienen que iniciar sesión en Signals y cargar los documentos solicitados. Una vez que se haya proporcionado toda la información, el cliente marcará la solicitud de suministro como completa y la enviará a Mazars. Después de que Mazars apruebe las solicitudes de suministro, todos los documentos se guardarán en su(s) aplicación(es) de back-office. Todas las acciones relacionadas con las solicitudes de suministro se almacenan en un registro de auditoría.

Flujos de trabajo y declaraciones fiscales

Mazars presenta el trabajo preparado (informes anuales, declaraciones de impuestos) a nuestros clientes utilizando Signals. Los informes y las declaraciones fiscales se preparan en los sistemas de back-office y luego se cargan en Signals. Los clientes pueden presentar el trabajo y sus declaraciones, que se enviarán directamente a las autoridades fiscales a través de un proceso automatizado. Todas las acciones relacionadas con las declaraciones realizadas tanto por los clientes como por los empleados se almacenan en una pista de auditoría completa.

Plataforma

Esta figura representa el estado del ecosistema de Mazars Signals:



Encriptación

Tanto los datos en reposo como los datos en tránsito se encriptan utilizando los estándares de encriptación de la industria. Todas las medidas de encriptación se implementan para garantizar la confidencialidad e integridad de los datos dentro de Mazars Signals.

Gestión de datos y cumplimiento de la normativa

Todos los sistemas relacionados de Mazars Signals están situados en los Países Bajos e Irlanda (Microsoft Azure West-Europe). El procesamiento de datos se lleva a cabo de acuerdo con las leyes y regulaciones de la UE. Para cumplir con los requisitos del GDPR, no se transfiere ninguna información personal identificable (PII) fuera de las fronteras de la UE. Los datos de los clientes se conservan de acuerdo con el cumplimiento de los períodos de retención legales (con un máximo de 10 años).

Desde noviembre de 2020, Microsoft ha aplicado protecciones de privacidad adicionales denominadas "Defender sus datos", para proteger los datos de los clientes como se describe en este artículo: New Steps to Defend Your Data - Microsoft On the Issues.

Para conocer las Salvaguardas Adicionales a las Cláusulas Contractuales Estándar de Microsoft, es pertinente tomar conocimiento del siguiente documento: REFERENCE-COPY-Additional-Safeguards-Addendum-to-Standard-Contractual-Clauses-.pdf (microsoft.com).

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

Tiempo de actividad y fiabilidad

Supervisamos constantemente el rendimiento de nuestro servicio y disponemos de notificaciones automáticas para garantizar una respuesta rápida ante posibles interrupciones del servicio. Todos los cambios de código se verifican y aprueban antes de desplegarlos en los servidores de producción. Seguimos de cerca las actualizaciones de la comunidad de seguridad y actualizamos inmediatamente nuestros sistemas cuando se descubren nuevas vulnerabilidades.

Infraestructura

Hosting

Todos los sistemas de servidores están alojados en Microsoft Azure, dentro de la región de Europa Occidental, con Ámsterdam como ubicación principal y Dublín como ubicación secundaria. Los centros de datos de Microsoft cumplen con varias certificaciones. Por favor, compruebe https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/ para todos los detalles.

Proceso de parcheo

Todos los sistemas de servidores relacionados se parchean con regularidad (al menos mensualmente) para mantener los más altos estándares de seguridad posibles.

Monitorización

Todos los sistemas de servidores relacionados se supervisan las 24 horas del día para garantizar el mayor tiempo de actividad posible. Los ingenieros reciben alertas automáticas cuando hay una posible interrupción de cualquier sistema de producción.

Medidas de seguridad

Consulte en https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security todas las medidas de seguridad (físicas) aplicables en las instalaciones del centro de datos de Microsoft Azure.

Aplicación

Identificación, autenticación y autorización

Solo las cuentas de usuarios y empleados (de Mazars) verificados tienen acceso a datos específicos de clientes dentro de la plataforma Signals de Mazars.

Los usuarios de clientes se autentican aplicando la plataforma Okta, donde la autenticación multifactor (MFA) es obligatoria y se aplica a través de la aplicación Okta Verify, disponible para Android e iOS. Consulte https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/ para obtener más información sobre las medidas de seguridad aplicables a la plataforma Okta.

Los empleados de Mazars que inician sesión dentro del área de red de Mazars, utilizan SSO para acceder a Signals. Dependiendo de su rol, los empleados de Mazars sólo tienen acceso a datos específicos de clientes. Los roles de administrador funcional y técnico están limitados dentro de la organización de Mazars. Este tipo de privilegios sólo se permiten cuando se cumplen y verifican los controles de antecedentes adicionales.

Administración

El acceso a las tareas de administración del sistema y desarrollo de aplicaciones está restringido a un número limitado de administradores del sistema y desarrolladores de aplicaciones. Cada administrador del sistema y cada desarrollador asignado a las tareas de administración del sistema y de desarrollo firman los correspondientes acuerdos de no divulgación y confidencialidad.

El acceso para fines de administración funcional está restringido a un número limitado de administradores funcionales y gestores de clientes/relaciones. Cada administrador funcional asignado para realizar tareas de administración funcional firma los acuerdos correspondientes de no divulgación y confidencialidad.

Proceso de desarrollo

El proceso de desarrollo se realiza de forma ágil. Mazars ofrece el propietario del producto, que es una función clave en un proceso de desarrollo ágil.

Seguridad en el proceso de desarrollo

Realizamos revisiones de código y utilizamos el análisis estático de código para identificar los riesgos de seguridad. Los riesgos identificados se evalúan y se resuelven cuando es necesario. Llevamos a cabo las siguientes prácticas del ciclo de vida de desarrollo de seguridad de Microsoft:

Gestione el riesgo de seguridad que supone el uso de componentes de terceros:
Hemos creado resúmenes de los componentes de terceros que utilizamos y estamos en proceso de automatizar este inventario.

También evaluamos periódicamente esas dependencias, por ejemplo, en relación con la proximidad de la fecha de fin de vida de un componente.

Realizar pruebas de seguridad de análisis estático (SAST)
Utilizamos SonarCloud para la identificación y el análisis de los puntos conflictivos de seguridad.

Realizar pruebas de penetración
Realizamos pruebas de seguridad antes de lanzar una nueva aplicación a producción y realizamos una prueba de penetración al menos una vez al año.

Rollout

Mazars trabaja con un calendario de despliegue mensual. Hay un despliegue programado cada mes, normalmente entre el 14 y el 20 del mes. El scrum master decidirá, junto con los propietarios del producto, qué trabajo que se ha marcado como realizado en los 1-2 sprints anteriores se lanzará como un incremento al entorno de producción. El procedimiento de lanzamiento es el siguiente

1. Seleccionar las historias finalizadas que deben ser liberadas al entorno de producción
2. Fusionar las historias de nuestra rama de desarrollo a la rama principal
3. Desplegar las historias en el entorno principal de pruebas
4. Todas las historias se prueban en el entorno de pruebas principal y todo el entorno se somete a pruebas de regresión
5. Despliegue de todas las historias en el entorno de aceptación
6. El entorno de aceptación se somete a una prueba de regresión completa
7. Despliegue de todas las historias en el entorno de producción
8. Después del despliegue se realizan comprobaciones de cordura para verificar el despliegue.

Durante los días posteriores al despliegue, el equipo de desarrollo comprobará activamente la monitorización y los archivos de registro.

Después de la revisión del sprint, el propietario del producto decide si quiere desplegar el nuevo incremento en el entorno de producción.

Hoja de ruta del producto y estimaciones a largo plazo

Para tener una visión a más largo plazo, existe una hoja de ruta del producto. El propietario del producto, junto con las partes interesadas, es el principal impulsor de la hoja de ruta del producto. Los desarrolladores también desempeñan un papel de asistencia a Mazars en la creación de esta hoja de ruta a nivel estratégico. La hoja de ruta del producto debe mostrar la dirección de crecimiento del producto y el valor que aportará a Mazars y a sus clientes.

Una hoja de ruta del producto se compone de conceptos épicos. Se trata de trozos de trabajo de alto nivel que son demasiado grandes para trabajar en ellos de forma independiente y que se dividirán en varios almacenes, por ejemplo: la firma digital de los informes de fin de año.

Para la hoja de ruta, el equipo puede hacer estimaciones de alto nivel junto con el propietario del producto. Estas estimaciones suelen hacerse rápidamente, ya que el objetivo no es tratar de resolver todos los requisitos por adelantado. En cambio, las estimaciones de alto nivel se dan para indicar el alcance esperado del desarrollo de una epopeya.

Una vez que comience el desarrollo, estas estimaciones fluctuarán a medida que las historias se refinen y los resultados requeridos para las historias se vuelvan más claros. Siempre es bueno tener en cuenta estas fluctuaciones a la hora de planificar.

Medidas de seguridad adicionales

Además, Mazars Signals está protegido por controles de seguridad de la capa de aplicación.

Pruebas de seguridad

La plataforma de Señales de Mazars se somete a pruebas periódicas para detectar vulnerabilidades de seguridad por una parte independiente para garantizar la objetividad. La mitigación de las posibles vulnerabilidades se realiza siempre por orden de su criticidad.

Protección de la integridad del registro de auditoría

Los archivos de registro y los registros de auditoría de Mazars Signals se almacenan en discos virtuales, donde se aplica el cifrado en reposo. El acceso a los archivos de registro y a los registros de auditoría está restringido a un número limitado de administradores del sistema.

Organización

Privacidad

Nos tomamos muy en serio la seguridad y la privacidad de los datos de nuestros clientes y los tratamos como una métrica importante. Signals de Mazars cumple con la normativa GDPR/UE. Para los países fuera de la UE, por favor, consulte las regulaciones locales de privacidad y, en su caso, consulte las cláusulas contractuales estándar adicionales para las transferencias de datos entre los países de la UE y fuera de la UE. Puede consultar un resumen completo de nuestra política de privacidad en https://www.mazarssignals.com/en/privacy-statement.

Políticas de seguridad

Todos los empleados se rigen por políticas de seguridad documentadas que cubren el uso aceptable, el manejo de datos confidenciales, etc.

Recuperación de desastres / copias de seguridad

Los datos de las aplicaciones y de los clientes se almacenan de forma redundante en múltiples zonas de disponibilidad con copias de seguridad disponibles para recuperarse en caso de desastre.

Gestión de incidentes de seguridad

En caso de que se confirme una violación de la seguridad en la que los datos de los clientes se vean comprometidos, nuestro equipo se lo notificará rápidamente. En caso de que su equipo de seguridad necesite registros adicionales para su investigación de un incidente que se determine que afecta a su organización, nuestro responsable de seguridad se coordinará de forma responsable para proporcionarlos según sea necesario.

Punto de contacto único para la seguridad

Para responder a las preguntas sobre este documento, envíe sus preguntas a security@mazars.nl.