CS INSTRUMENTS

CS Leak Reporter Cloud Solution
Sicherheitskonzept der Cloud Datenspeicherung

CS INSTRUMENTS GmbH & Co. KG

Geschäftsstelle Süd/ Sales Office South
Zindelsteiner Straße 15
D-78052 VS-Tannheim
Tel.: +49(0)7705 97899-0
Fax: +49(0)7705 97899-20
Mail: info@cs-instruments.com
Web: http://www.cs-instruments.com/de

Geschäftsstelle Nord/ Sales Office North
Gewerbehof 14
D-24955 Harrislee
Tel.: +49(0)461 807150-0
Fax: +49(0)461 807150-15
Mail: info@cs-instruments.com
Web: http://www.cs-instruments.com/de

1 Inhalt

2 Vorwort

Die Leak-Reporter Cloud Anwendung besteht aus einer Reihe von Softwarekomponenten, welche die Verwaltung von Leckage Daten durch mehrere Nutzer möglich machen. Die Komponenten teilen sich dabei in Backend Komponenten / Services auf, die auf dem Server laufen und mit der Datenbank kommunizieren, sowie den Frontend Anwendungen, die von einem Webserver zur Verfügung gestellt werden und im Browser ausgeführt werden. Somit kann der Benutzer die Anwendung einfach über den Browser nutzen und es muss keine Anwendung auf dem System (PC, Tablet,…) installiert werden.

Die Installation der Komponenten kann auf einem Server des Kunden erfolgen (on Premise). Zum anderen bietet CS INSTRUMENTS aber den wesentlich moderneren Ansatz einer Cloud Lösung an, bei dem die Anwendung auf Servern von CS INSTRUMENTS läuft (Cloud). Siehe Abb. 1.

Abbildung 1: Multi-User Leckage Verwaltung mit der CS Instruments Cloud oder der On Premise Installation der Leak-Reporter Software Komponenten.

3 Cloud Lösung

CS Instruments hat die Komponenten auf einer Cloud Plattform installiert und bietet diese Kunden zur Nutzung an. Das Benutzen der CS Instruments Infrastruktur hat den Vorteil, dass der Kunde keinerlei Aufwand für die Installation und Wartung des Systems hat. Zudem liegt die Verantwortung zur Pflege der Software-Infrastruktur bei CS Instruments.

- Updates zur Fehlerbehebung oder zur Bereitstellung erweiterter Funktionen werden zentral auf den Cloudservern installiert und stehen den Endnutzern zeitnah zur Verfügung.
- Außerdem wird die Cloud Lösung in Zukunft um weitere Anwendungen und Features erweitert werden.
- Durch die Speicherung aller Daten auf mehreren Cloud-Servern führen lokale Hardware- und Software-Probleme außerdem seltener zu Datenverlusten und bietet eine höhere Verfügbarkeit.

4 Datensicherheit

Die Software wird von allen Kunden genutzt und die Daten werden zentral abgespeichert. Selbstverständlich kann ein Kunde nicht die Daten eines anderen Kunden sehen. Dies wird über das integrierte Identitäts- und Rechtemanagement sichergestellt.

Darüber hinaus sind auch die APIs öffentlich verfügbar (und damit angreifbar) und der Server steht nicht unter der Kontrolle des einzelnen Kunden. Dementsprechend ist Datenschutz und Datensicherheit von extremer Wichtigkeit.

Im Folgenden sind deshalb wichtige Punkte im Hinblick auf den Schutz der Daten aufgeführt:

4.1 CS INSTRUMENTS Garantie

CS INSTRUMENTS garantiert vertraglich, dass keine Daten an dritte weitergeleitet werden und nur im Fehlerfall benutzt werden, um Fehler zu beheben und das Produkt so für alle Benutzer kontinuierlich zu verbessern.

4.2 Bewährte Cloud Infrastruktur

Die Software setzt auf die Infrastruktur eines erfahrenen Cloud Anbieters (Microsoft Azure) mit entsprechenden Sicherheitsmaßnahmen auf. Die Daten werden in West-Europa entsprechend den geltenden Europäischen Datenschutzrichtlinien gespeichert.

4.3 State of the Art Identity and Access Management

- Die Authentifizierung und Autorisierung erfolgt über ein weitreichend verwendetes open-source IAM System, welches regelmäßig aktualisiert wird.

- Nur der aus dem Passwort des Benutzers entsprechend PBKDF2 abgeleitet Schlüssel wird in der Nutzerdatenbank gespeichert (es gibt keine Möglichkeit das Passwort zu rekonstruieren).

- Ein Login kann nur durch die von IAM bereitgestellte Login-Seite erfolgen (was Phishing Angriffe mit nachgeahmten Login Seiten erschwert). Für die Authentifikation wird openid-connect mit dem Autorisation-Code Flow verwendet (https://openid.net/connect/). Der Nutzer/Client (Browser) enthält daraufhin ein Access und Refresh Token (siehe https://oauth.net/2/). Die Tokens die im Browser (als Cookies) gespeichert werden (für Single Sign On) enthalten keine Zugangsdaten und sind nur begrenzte Zeit gültig (Inaktivitätssperrung).

4.4 Zugriff auf Daten nur über geschützte Service APIs

Die mit Nutzername und Passwort gesicherte Datenbank ist nicht von außen (öffentliche Netzwerke) zugreifbar. Die Daten werden vielmehr von Services, die mit den Datenbanken zusammen in Kubernetes ausgeführt werden über APIs zur Verfügung gestellt. Um die Berechtigungen des Nutzers zu überprüfen, muss vom Client das vom IAM erhaltene Access Token mitgeschickt werden. Dieses wird vom Backend Service auf Gültigkeit überprüft (Signatur des Tokens und Public Key des IAM) und anschließend die Autorisierung für die gewünschten Daten vom IAM abgefragt.

4.5 Isolation von Daten in Organisation / Realms

Über das IAM wird sichergestellt, dass Nutzer nur die Daten (andere Nutzer und Leckage Daten) innerhalb Ihrer Organisation (Realms) sehen. Die Daten einer anderen Organisation können nicht eingesehen werden.

4.6 Fein granulare Zugriffsberechtigungen innerhalb der Organisation

Innerhalb der Organisation können von den Nutzern selbst (ausgehend vom Organisations-Administrator) individuelle Zugriffsrechte auf Daten konfiguriert und vergeben werden. So kann zum Beispiel auch externen Nutzern das Ansehen (und ggf. Bearbeiten) bestimmter Daten ermöglicht werden über einen (temporären) Zugang über deren E-Mail-Adresse. Erteilte Berechtigungen können mit sofortiger Wirkung jederzeit durch den Administrator entzogen werden.

4.7 Moderne Softwarearchitektur

Die Anwendung wurde in Form einer Microservice Architektur implementiert. Dies erlaubt es die Komplexität einzelner Komponenten zu reduzieren und dadurch die Sicherheit zu steigern. Außerdem wurden Technologien verwendet die z.B. SQL-Injections unmöglich machen.

4.8 Minimale Anzahl an Service Account

Der Zugriff auf Kubernetes sowie die Azure APIs / Portal ist nur wenigen Service Accounts (Personen) möglich. Dies gilt auch für die in Azure gespeicherten Datenbank Backups und Log-Dateien.

4.9 Regelmäßige Überprüfung der Logs

Unregelmäßigkeiten, die auf potenzielle Angriffe oder unerlaubte Zugriffe hindeuten, werden frühzeitig erkannt und notwendige Gegenmaßnahmen können schnellstmöglich ergriffen werden.

4.10 Zugriff nur über https (TLS)

Zugriff mit http ist nicht möglich. Die komplette Kommunikation zwischen Client und Server ist verschlüsselt, Datenintegrität wird sichergestellt und Man-in-the-Middle-Angriffe sind nicht möglich.

4.11 Daten Sparsamkeit

- Es werden lediglich die für die Anwendung notwendigen Daten gespeichert. Dazu gehören die Nutzerdaten sowie die Leckage-Daten.
- Die Datenbank-Backups und Log-Dateien werden nur für einen gewissen Zeitraum gespeichert und dann vollständig gelöscht.
- Es werden keinerlei Trackingdaten der Nutzer erhoben.

Das grobe Softwaretechnische Zugriffs- und Sicherheitskonzept, dass für die CS Cloud Lösung implementiert wurde, ist in **Abbildung 2** skizziert:

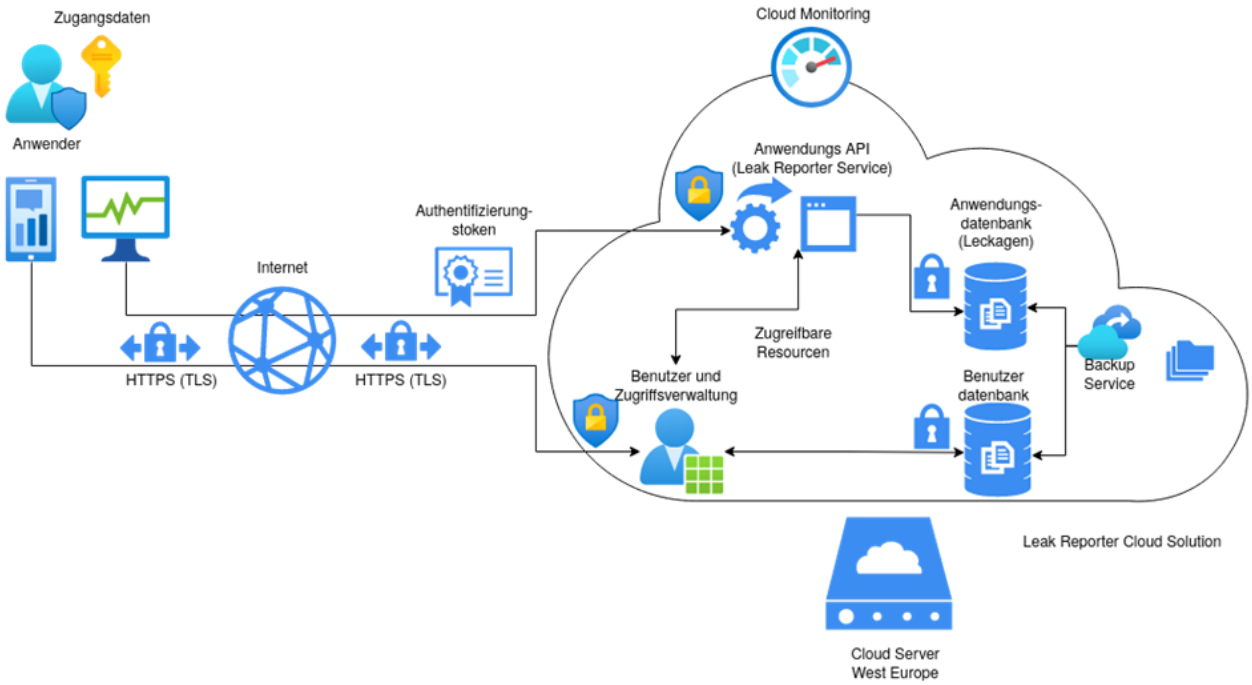

Abbildung 2: *Skizze der CS Cloud Lösung im Hinblick auf Sicherheit. Vor allem über die integrierte Indentitäts- und Rechte-/Zugriffsverwaltung wird sichergestellt das jeder Nutzer nur die für ihn bestimmten Daten zu sehen bekommt.*

4.12 On Premise Lösung (Installation durch den Kunden)

Die von CS Instruments bereitgestellten Softwarekomponenten werden bei der On-Premise Lösung vom Kunden installiert. CS Instruments bietet dafür eine kompakte Vorgehensweise in Form einer Docker-Compose Datei, nichtsdestotrotz erfordert die Installation und Konfiguration einen großen Zeitaufwand und verlangt umfangreiches IT-Know-How vom Kunden.

Dies gilt umso mehr, wenn die Installation in einem Kubernetes Cluster (direkt beim Kunden oder bei einem Cloud Anbieter) erfolgen soll. Der Kunde bzw. dessen IT muss sich zum Beispiel um verschlüsselte Kommunikation (https) oder Backup Mechanismen kümmern. Des Weiteren muss dieser die Wartung und das Einspielen von Updates übernehmen.

CS INSTRUMENTS hält für Entwicklung, Betrieb und Wartung große personelle Ressourcen vor und kann somit die anfallenden Aufgaben in der Cloud Lösung schneller erledigen als Mitarbeiter der firmeneigenen IT-Abteilung, die oft parallel andere dringende Projekte weiterverfolgen und priorisieren müssen.

4.13 Gegenüberstellung

In der folgenden Tabelle sind einige Merkmale der Ansätze gegenübergestellt:

Tabelle 1: *Vergleich verschiedener Merkmale bei der Verwendung der CS Cloud Lösung und einer On Premise Installation.*

Merkmal	**CS Cloud Solution**	**On Premise (Installation durch den Kunden)**	
		Individuelle Cloud	**Server im Firmennetz**
Besitz der verwendeten Server	✗	✗	✓
Sicherheit	Hoch	Hoch	Extrem Hoch
Verfügbarkeit/Redundanz	Hoch (Kubernetes)	Gering – Hoch möglich	Gering
Überall Zugreifbar	✓	✓	✗
Kooperation mit externen Dienstleistern oder Kunden	✓	✓	✗
Installationsaufwand	-	Hoch	Hoch
Initiale Kosten	Gering	Hoch	Hoch
Wartungsaufwand	-	Hoch	Mittel
Laufende Kosten	Gering	Hoch	Mittel