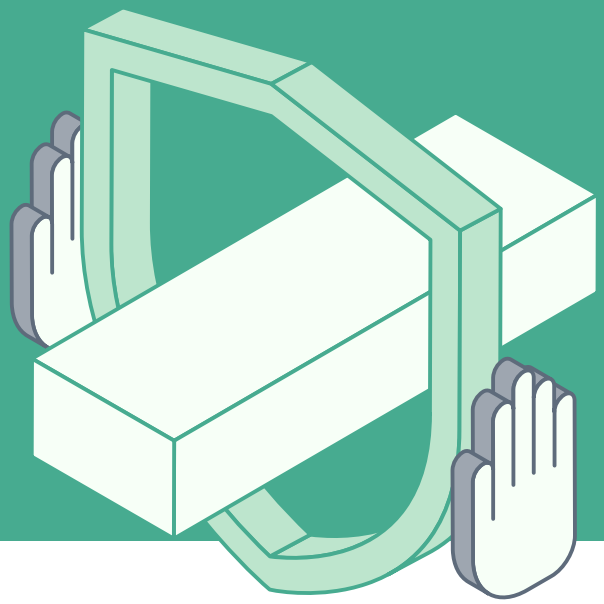
CLOUDYRION

Big Data Security in der Tech-Branche

Ein Unternehmen aus der Tech-Branche mit Fokus auf Telekommunikation wollte große Mengen kundenbezogener Daten aus unterschiedlichen Ressourcen möglichst kostengünstig in eine zentrale Umgebung transferieren. Für die Migration und den anschließenden Zugriff wurde ein IT-Sicherheitskonzept benötigt. Mit der Umsetzung nach Maßgabe des Security-by-Design-Ansatzes betraute der Tech-Anbieter die Experten für ganzheitliche IT-Sicherheit von Cloudyrion.



AUSGANGSLAGE

Private und Enterprise-Kunden von Telekommunikationsanbietern erwarten heutzutage Tarife, die möglichst kosteneffizient auf ihren individuellen Bedarf zugeschnitten sind. Um seinen Bestandkunden Tarifanpassungen auf Basis einer Business Intelligence (BI)-Analyse anzubieten und die Performance einzelner Kunden zu erfassen und zu bewerten, hat sich das Tech-Unternehmen entschlossen, fortschrittliche Big Data Analytics- und Machine Learning-Prozesse zu etablieren. Das Ziel: Eine Basis für Analysen zu schaffen, die Benefits sowohl für die Kunden als auch den Anbieter beinhalten.

Eine große Herausforderung bestand darin, ein zentrales Daten-Repository einzurichten, das den hohen Anforderungen an die Sicherheit kritischer Daten gerecht wird. Welcher Cloud-Anbieter ist der richtige? Welcher erfüllt die Kriterien in Hinblick auf Privacy sowie Security und bietet die Infrastruktur, um die gewünschte Architektur richtig umzusetzen? Um diese sicherheitsrelevanten Fragen unter Wahrung der gültigen Compliance-Vorgaben zu beantworten, begab sich das Tech-Unternehmen auf die Suche nach einem qualifizierten Partner für IT-Sicherheit. Durch Empfehlungen aus dem eigenen Netzwerk wurde die Company auf Cloudyrion aufmerksam und nahm Kontakt zu den IT-Security-Spezialisten auf. Die großen Pluspunkte im Marktauftritt der Düsseldorfer Sicherheitsexperten: umfassende Beratung, technologische Expertise und lösungsorientierte, pragmatische Hilfestellungen aus einer Hand.

CHALLENGE

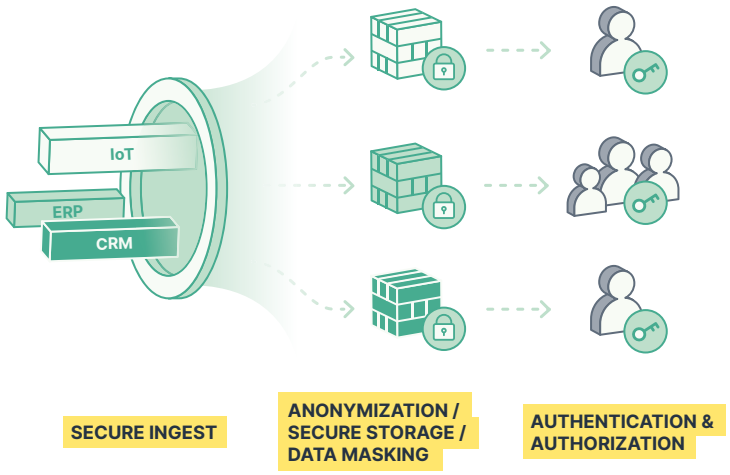
Zwar existierte bereits eine Big Data-Umgebung, für die sich das Unternehmen entschieden hatte, allerdings war sie noch nicht sicherheitstechnisch auf den Prüfstand gestellt worden. Benötigt wurde daher ein systematischer Reverse-Engineering-Ansatz, mit dem sich gewährleisten ließ, dass die drei zentralen sicherheitsrelevanten Bereiche im Segment Big Data Analytics effektiv adressiert und abgedeckt wurden:

- **Minimierung der Angriffsflächen durch Konfigurations- und Schwachstellen Analyse**
- **Sichere Datenübetragung (data-in-transit encprytion)**
- **Sichere Daten Speicherung (data-at-rest encrpytion)**

Verschlüsselung der Daten

Im Fokus standen dabei unter anderem Zugriffsberechtigungen, die Verschlüsselung der Daten, während sie verschickt werden, sowie Datenintegrationsmuster (Data Integration Patterns), in denen standardisiert ist, welche Daten wo rein- und rausgehen dürfen und wer Zugriff auf die Data Lakes (cold/warm storage) sowie die BI-Tools hat. Einen praktikablen Rahmen für die Umsetzung eines sicheren Rollenmanagements sollte das sogenannte „Need to know"-Prinzip setzen. Demnach erhält jeder, der operativ mit den Daten arbeitet, nur Sicht und Zugriff auf das, was er für seine konkrete Aufgabe benötigt. In der Regel tendiert das Management von Zugriffsberechtigungen in Big Data-Umgebungen zur Unübersichtlichkeit – ein durchaus gefährlicher Umstand.

Über die rechtlichen Vorgaben hinaus, die beispielsweise in der EU-DSGVO verankert sind, ist Datensicherheit grundsätzlich ein hoher Wert. Sobald Verstöße, Nachlässigkeiten und Sicherheitsvorfälle an die Öffentlichkeit dringen, entsteht ein Imageschaden für die betroffene Marke, der kaum zu reparieren ist. Hinzu kommt, dass das Kompromittieren besonders sensibler Datenbestände das Kerngeschäft des Unternehmens empfindlich schädigen und im Extremfall sogar den Fortbestand gefährden kann. Mit einem eindeutigen Fokus auf Sicherheit mit Unterstützung durch Cloudyrion sollte daher im Bereich des Rollenmanagements und damit mit Blick auf Datensicherheit und Compliance Klarheit geschaffen werden. Der gesteckte Zeitrahmen für das Projekt erstreckte sich auf sechs Monate. Während der Umsetzung sollte die Hochverfügbarkeit der Daten für berechtigte User zu jeder Zeit sichergestellt bleiben.



LÖSUNG

Zu Beginn der Projektarbeit definierte Cloudyrion gemeinsam mit dem Unternehmen die Datenintegrationsmuster für die Big-Data-Umgebung. Dabei ging es im Kern um die Logik hinter den eingesetzten Dashboards und wer die Berechtigung erhält, sie bei Bedarf zu verändern. Die Sicherheitsexperten berieten unter anderem bei folgenden Themen:

- **Herstellung von Datentransparenz mittels Data Asset Inventory / Data Catalogue (Missing Data Discovery and Mapping)**
- **Datenklassifizierung (Data Classification) auf vier Ebenen von C1 bis C4**
- **Schutz der Daten (Data Leakage/Loss Prevention)**
- **Sichere Datenquellenintegration und Datenvalidierung**
- **Absicherung von Data Lakes (ETL und ML pipelines)**
- **Maskierung oder Anonymisierung von Datensätzen**
- **Erstellung eines Asset-Inventars in Form eines Datenkatalogs**
- **Datenhaltung (Data Retention)**
- **Sicheres Daten-Backup**
- **Identitätsmanagement (Identity Access Management)**

Beim letzten Punkt standen Fragen zur Rollenvergabe an die Anwender im Zentrum: Welche Rollen gibt es? Wie werden sie vergeben, entzogen und freigegeben? Wie lässt sich das Ganze auditieren? Dabei war zu beachten, dass sämtliche Prozesse, die gemäß dem oben genannten Methodeninventar überprüft und nötigenfalls angepasst wurden, Compliance-relevant für das Unternehmen waren.

Darüber hinaus identifizierten die Experten Schwachstellen und Fehler in der bereits implementierten Live-Umgebung und korrigierten diese nachträglich iterativ. Dazu führten sie konkrete Audits sowie Penetration Tests durch, um Angriffsflächen zu finden und Lücken zu schließen. Dieser Prozess wurde mittels Reverse Engineering schrittweise rückwärts durch alle Ebenen bis zum ursprünglichen Design der Lösung vollzogen. Diese erhielt auf Basis der bis dahin erzielten Findings entsprechend eine Anpassung gemäß dem Security-by-Design-Ansatz.

Um die Hochverfügbarkeit der Daten und Data Lakes dauerhaft zu gewährleisten, wurde die Big-Data-Lösung ursprünglich in einer Multi-Cloud-Umgebung aufgesetzt. Die meisten gängigen Cloud Service Provider unterstützen dies strukturell, allerdings weisen ihre Sicherheitstools eine relativ hohe Rate an False-Positive-Meldungen auf, wenn es um die Identifizierung korrekter Datenmuster geht – eine Herausforderung, mit der das gesamte Team dank Unterstützung durch Cloudyrion umzugehen lernte.

AUSBLICK ZUKUNFT

Nach der Erreichung des für nach sechs Monaten festgesetzen Meilensteins, beauftragte das Unternehmen Cloudyrion damit, die Umsetzung der Security-by-Design und die Einhaltung der damit einhergehenden Prinzipien auch über den ersten Projektzeitraum hinaus weiter voranzutreiben und zu monitoren. Dadurch vertiefte sich die vertrauensvolle Zusammenarbeit zwischen den Teams auf Auftraggeberseite und Beratern. Im Ergebnis erhöhte sich die allgemeine Awareness im Unternehmen für Security-Themen signifikant. Dazu tragen auch unangekündigte Audits bei, die Cloudyrion immer wieder in unregelmäßigen Abständen innerhalb der weiter gewachsenen Systemumgebung durchführt, um Schwachstellen kontinuierlich aufzuspüren und zu schließen. Parallel dazu steht Cloudyrion für den Support bei besonders kniffligen Fragen zur Verfügung.

NUTZEN UND BEURTEILUNG

In der praktischen Umsetzung erwies es sich als Herausforderung, den Anwendern das notwendige Skill-Set zu vermitteln, damit sie souverän mit dem System arbeiten können. Die erzielte Lernkurve zeigt indessen, dass sich dieser Aufwand gelohnt hat. „Sicherheitsrelevante Fehler durch Mitarbeiter geschehen in aller Regel nicht mit Absicht, sondern unbewusst. Ziel muss es allerdings sein, dass diese Fehler niemals in die Produktivumgebung gelangen“, erklärt Okay Güler, Founder & IT Security Consultant von Cloudyrion. „Unser Kunde und seine Belegschaft schätzen daher besonders unsere lösungsorientierte Vorgehensweise und Flexibilität, mit der wir die Leute vor Ort dabei unterstützen, Security-Know-how im Big Data-Kontext zu entwickeln, ihnen zu vermitteln und nachhaltig in den Prozessen zu verankern.

Zentrale Ergebnisse im Überblick

- **Sichere Speicherung und sicherer Zugriff auf Daten**
- **Einhaltung der internen Firmen-Policies**
- **EU-DSGVO-Compliance**
- **Implementierung von „What good looks like”-Datenintegrationsmustern**
- **Weitaus schnellere Prozesse**
- **Validierung eingehender Daten unter dem Sicherheitsaspekt**
- **Aufbau von Know-how in der Belegschaft**
- **Klare Zuweisung von Aufgaben und Rollen für Anwender**

Sie suchen nach einem verlässlichen Partner, der Ihr Team dabei unterstützt, ehrgeizige und sicherheitskritische IT-Projekte erfolgreich umzusetzen und langfristige Verfügbarkeit zu gewährleisten? Kontaktieren Sie uns – wir helfen gern.