COMPLIANCE IST PRÄVENTION VOR BEKANNTEN UND UNBEKANNTEN RISIKEN

Suchtechnologien spüren Passwörter im Source Code auf

AUF EINEN BLICK:

- Branche: Finanzdienstleister
- Ziel: Non-Compliance aufdecken
- Lösung: Enterprise Search
- Technologie: Apache Solr

ÜBER DEN KUNDEN:

Der Finanzdienstleister ist ein deutsches Finanzinstitut, das international mit einem umfassenden Portfolio tätig ist.

HERAUSFORDERUNG:

Die internationale Abteilung des Finanzdienstleisters, die für Compliance zuständig ist, reagierte sofort: Bei einem Audit wurde sie auf Passwörter und Private Keys aufmerksam, die in dem Source Code von Anwendungen in ein Versionsverwaltungs-System eingecheckt wurden; betroffen waren auch Admin Accounts und die Zugangsdaten zu Servern, auf denen die Programme bereitgestellt wurden. Daraufhin suchte sie nicht nur eine Lösung, um diese zu entfernen, sondern führte auch eine interne Regelung ein, die diese Praxis künftig untersagte.

Die Programmierer hatten die Zugangsdaten sicherlich nicht mit krimineller Absicht abgelegt, sondern aus Bequemlichkeit für spätere Tests oder aus Unwissenheit über die damit verbundenen Risiken. Diese waren aber denjenigen bewusst, die für die Compliance verantwortlich sind, so dass sie diese Form der Autorisierung nicht dulden konnten und umgehend handelten.

Eine Versionsverwaltungs-Software ist in der Regel sehr vielen Mitarbeitern frei zugänglich. Falls unberechtigte Personen Zugangsdaten in Erfahrung bringen, stellt dies ein hohes Risiko dar. Ohne Kenntnis des Finanzdienstleisters hätten unberechtigte Personen beispielsweise Informationen zu Kreditkarten und Kundendaten mit Hilfe der dafür ausführbaren Programme und deren Passworte einsehen oder sogar die Software manipulieren können. Noch bevor es zu einem Missbrauch kam, mussten daher alle Verstöße zunächst aufgespürt werden, um sie dann zu entfernen.

LÖSUNG UND UMSETZUNG:

Da der Finanzdienstleister mit der SHI bereits in anderen Projekten gut zusammenarbeitete, beauftragte er die Experten für Suchtechnologien damit, die Passwörter im plain Text sowie die Private Keys ausfindig zu machen. Zusammen mit dem Projektteam, das der Finanzdienstleister dafür etablierte, dem Leiter „Search“ und dem Audit Board legten diese im ersten Schritt den Workflow fest. Dazu gehörten beispielsweise, welche Projekte und Datenquellen durchsucht werden sollten, die Fehlertoleranz und die Anzahl der Suchdurchläufe.

Zu den Aufgaben der SHI gehörte es auch, einen Algorithmus zu erstellen, um damit die sensiblen Daten zu erkennen. Die betroffene Datenmenge war nämlich für Menschen nicht überschaubar. Die Daten waren außerdem unstrukturiert und betrafen ganz unterschiedliche Dateiformate. Die Zugangscodes konnten sich in Back-ups, Datenbanken-Schemata oder auch in angehängten PDF-Dokumenten befinden.

Die Experten der SHI indizierten daraufhin die Inhalte der in dem Versionsverwaltungs-System hinterlegten IT-Projekte und -Programme. Für die Volltextsuche setzten sie die Open-Source Software Apache Solr ein, um die sensiblen Daten zu finden. Eine besondere Herausforderung war dabei, dass diese beispielsweise aus einer beliebigen Abfolge unterschiedlicher Zeichen oder aber aus einem sinnvollen Satz bestanden, der nicht augenscheinlich als Passwort zu erkennen war.

ERGEBNIS:

Die IT-Projekte aller Geschäftsbereiche wurden international nach Passwörtern im plain Text sowie nach Private Keys durchsucht, und SHI erstellte einen Bericht über die Ergebnisse der Queries. Der Finanzdienstleister forderte daraufhin die IT-Entwickler auf, die entsprechenden Passwörter zu entfernen. Stattdessen sollten sie ausschließlich das bereits etablierte Passwort-Verwaltungstool nutzen – und damit konform mit der internen Richtlinie handeln.

Anschließend führte SHI einen Rescan durch und überprüfte, ob die Programmierer die Anforderung durchgeführt hatten. Mit Hilfe der Versionierungs-Informationen prüfte SHI, welche Mitarbeiter zuletzt in den relevanten Systemen sensible Daten eingecheckt hatten und ob diese anschließend entfernt wurden.

Im Ergebnis wurden Passwörter im Source Code und Private Keys, bis auf ein Restrisiko, entfernt. Die Mitarbeiter des Finanzdienstleisters programmieren seitdem alle IT-Projekte konform zu einer internen Richtlinie, so dass die Verantwortlichen die Kontrolle darüber haben, wer zu welchen Informationen Zugang hat. Damit wurde eine potentielle Sicherheitslücke, soweit möglich, geschlossen, und ein Missbrauch der Daten unterbunden.

Michael Marheineke, bei der SHI verantwortlich für Search– und Analytics-Lösungen:

„Wer in seinem Unternehmen für die Compliance verantwortlich ist, hat mit Suchtechnologien das entscheidende Hilfsmittel zur Hand. Diese sind nämlich darauf spezialisiert, auch die Inhalte unstrukturierter Daten aus heterogenen Quellen zu standardisieren und in einem zentralen System zu integrieren. Dadurch kann ein Missbrauch von Daten aufgeklärt und durch Prävention ein Data Leakage verhindert werden.“