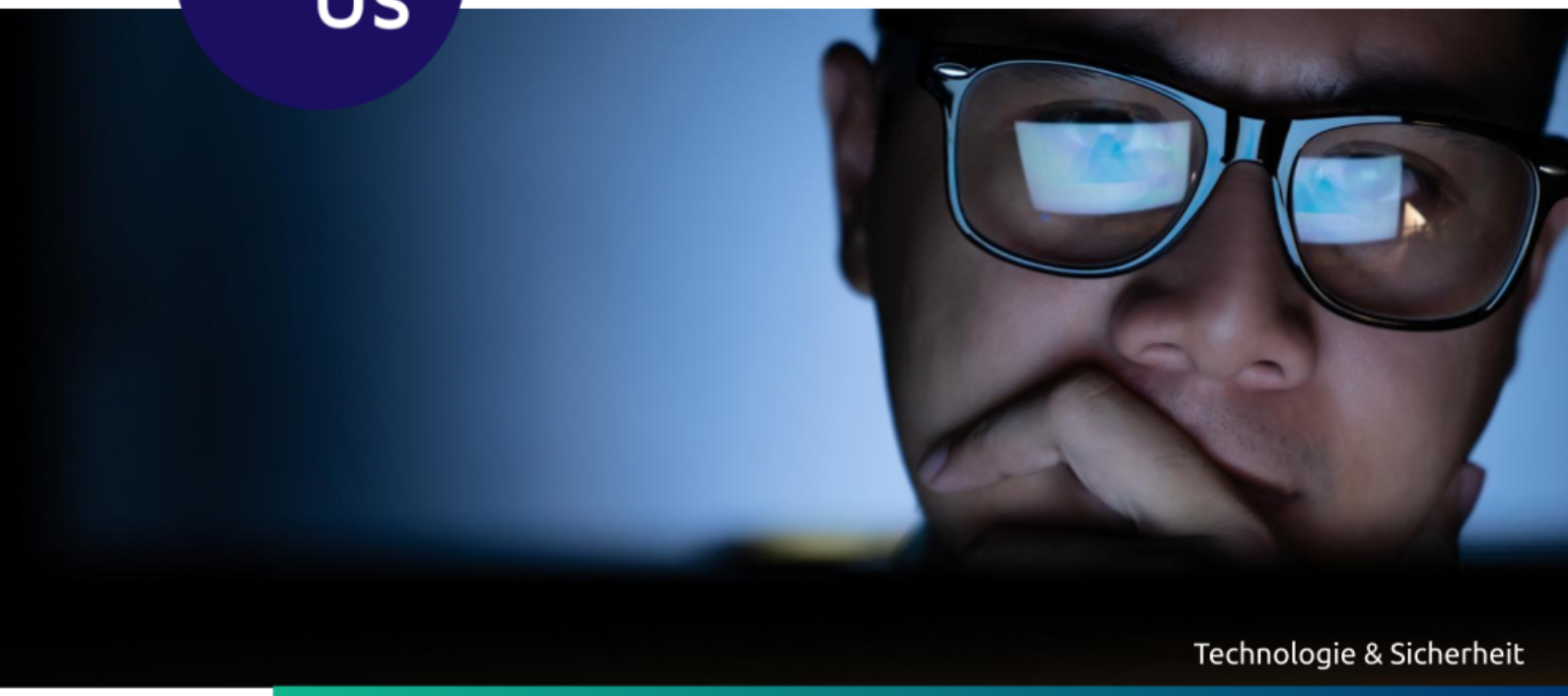

Technologie & Sicherheit

Audit-Protokollierung

Nutzeraktivitäten einfach zurückverfolgen und Ungereimtheiten schnell aufklären

https://innus.de

Inhalt

Unerwartetes erwarten

Audit-Protokollierung ist ein Werkzeug der Qualitätssicherung und dient der Kontrolle und Aufzeichnung von Änderungen, die in einem System vorgenommen werden. Dabei liegt der Fokus auf der Überwachung aller Ereignisse, die zu einer Zustandsänderung führen. Hierzu zählen:

- Erfolgreiche und fehlerhafte Authentifizierungen
- Anlegen, Bearbeiten und Löschen von Ressourcen
- Zustandsübergänge innerhalb eines Prozessablaufs

Neben der Möglichkeit, Ereignisse zu rekonstruieren, Angreifer zu erkennen und Leistungsengpässe zu identifizieren, können auch auffällige Aktivitäten verfolgt werden.

Auf diese Weise hilft die Audit-Protokollierung dabei, die IT-Sicherheit eines Unternehmens zu stärken.

Sequenz von Ereignissen

Jedes Modul der innus Banksuite speichert für alle bereitgestellten Ressourcen eine Sequenz von Ereignissen. Dabei werden alle Informationen einer Änderung festgehalten.

Zusätzlich zum eigentlichen Ereignis werden weitere Metadaten gesammelt. Diese Informationen beinhalten die Quelle der Änderung, die Kennung des authentifizierten Benutzers, einen Zeitstempel und einen Kommentar. Dadurch ist eine lückenlose Verfolgung aller Ereignisse innerhalb der innus Banksuite sichergestellt.

Neben der lückenlosen Verfolgung und Auswertbarkeit von Ereignissen ist es auch möglich, Ereignisse zu extrahieren und schrittweise in ein separates System einzuspielen. Somit ist es möglich, den Zustand des Systems zu einem bestimmten Zeitpunkt zu rekonstruieren und weitergehend zu analysieren.

Audit Service

Mit innus.AUD stellt die innus Banksuite eine Komponente bereit, die eine zentrale Auswertung aller Ereignisse ermöglicht. Eine eigene Rechteverwaltung stellt sicher, dass ein Zugriff nur berechtigten Benutzern möglich ist. Auch ist es möglich, nur die

Nutzung von innus.AUD freizugeben und den Zugriff auf weitere Komponenten zu beschränken.

Auswertung

Ein zentraler Bestandteil jedes Audit-Protokolls ist die regelmäßige Überwachung und Auswertung. Das Audit-Protokoll kann durch die Anwendung von Filtern bei der Suche begrenzt werden, wobei folgende Filteroptionen zur Verfügung stehen:

- Zeitraum
- Komponente
- Benutzer

Das Ergebnis der Suche wird als Liste dargestellt und beinhaltet folgende Informationen:

Spalte	Beschreibung	Beispiel
Komponente	Komponente, in der das Ereignis auftrat	IAM
Ressource	Betroffenes Objekt	Token
Ereignis	Nutzdaten des Ereignisses	{ “identifier”:“user”}
Quelle	Aufrufender Prozess	innus.BOA
Benutzer	Kennung des Benutzers	user
Kommentar	Kommentar zum Ereignis	Nach interner Prüfung freigegeben
Zeitstempel	Zeitpunkt des Ereignisses	2019-10-01T10:23:54

Benachrichtigung

Der Audit Service überwacht bestimmte Ereignisse intern und kann auf Basis standardisierter Regeln Benachrichtigungen versenden. Diese Benachrichtigungen werden immer an das eigene Portal gesendet und stehen direkt nach der Anmeldung zur Verfügung.

Wenn eine E-Mail-Adresse hinterlegt wurde, werden alle Benachrichtigungen sofort weitergeleitet, um eine schnelle Reaktion auf kritische Ereignisse zu gewährleisten.

Die folgenden Ereignisse werden überwacht:

Ereignisse	Regel	Standardwert
Anmeldung	Falsches Passwort	Anzahl: >= 3
Anmeldung	Falsche Anmeldedaten innerhalb eines Zeitraums	Anzahl: >= 10 Zeitraum: 60 Sekunden
Token	Keine Autorisierung gefunden	
Token	Signatur verletzt	
Token	Fingerabdruck ungültig	
Token	Aufruf durch eine unbekannte Quelle	

!EMPFEHLUNG! Bei Erhalt einer Benachrichtigung zu Ereignissen im Bereich Token sollten aus Sicherheitsgründen alle derzeit verwendeten Token zurückgesetzt werden.

Neben der Konfiguration einer E-Mail-Adresse zum Erhalt von Benachrichtigungen können die bereitgestellten Standardwerte der jeweiligen Regeln kundenspezifisch angepasst werden.

!HINWEIS! Die Anpassung der Standardwerte sollte mit Bedacht vorgenommen werden, um einerseits Falsch-Positiv Ereignisse zu vermeiden, aber auch tatsächliche Verletzungen nicht zu unterdrücken.

innus GmbH
Behringstraße 28a
22765 Hamburg
+49 40 303 77 40-0
info@innus.de