LogRhythm
The Security Intelligence Company

User and Entity Behaviour Analytics
Schützen Sie Ihr Unternehmen von innen heraus

In jedem Unternehmen gibt es interne Bedrohungen.

Bei der Suche nach Bedrohungen und deren Bekämpfung konzentrieren sich viele Unternehmen vorwiegend auf potenzielle Sicherheitsverletzungen durch externe Angreifer. In Wahrheit liegt jedoch die größte Sicherheitsbedrohung für ein Unternehmen oft im eigenen Netzwerk.

In 63 Prozent der Fälle gehen Sicherheitsverstöße von derzeitigen oder ehemaligen Mitarbeitern aus.[1]

Technologien sind ein Grundpfeiler jedes Unternehmens, doch diese Technologien werden immer noch von Menschen gesteuert und verwaltet. Vertrauenswürdigkeit ist eine unerlässliche Voraussetzung dafür, dass ein Netzwerk geschützt bleibt, sowohl intern als auch extern. Die Mitarbeiter müssen tagtäglich auf wichtige und sensible Daten zugreifen, um ihre Aufgaben erfüllen zu können, und genau wie die Sicherheitsbedrohungen selbst sind auch die Mitarbeiter nicht statisch. Sie kommen und gehen, nehmen Urlaub und gehen in Rente. Und bei der Arbeit tauschen sie ständig Informationen aus.

Die meisten Unternehmen sehen die Lösung für dieses Problem einfach darin, mittels Passwörtern oder Schlüsselkarten die Zugriffe zu kontrollieren. Die Zugriffe müssen aber auch überwacht werden, um Überblick über die Aktivitäten der Mitarbeiter zu haben und zu wissen, wie sie mit sensiblen Daten umgehen. Und hier versagen viele Unternehmen.

Die Risiken durch interne Bedrohungen

Wenn die Zahl der Beschäftigten wächst, nimmt die Anfälligkeit eines Unternehmens für interne Bedrohungen dramatisch zu. Böswillige Personen, die Zugriff auf sensible Daten haben, könnten diese stehlen, löschen oder veröffentlichen. Genauso gut können Schäden oder Diebstähle aber auch auf schlichte Unachtsamkeit zurückgehen oder die Folge einer erfolgreichen Phishing-Attacke sein.

Durchschnittlich 49 Prozent aller Benutzer geben zu, ihr Netzwerk-Passwort an mindestens einen anderen Benutzer weitergegeben zu haben.[2]

Zudem können Insider-Bedrohungen die langfristigsten Schäden verursachen – 70 Prozent der Vorfälle werden erst nach Monaten oder noch später erkannt.[3] Um echte Sicherheit zu gewährleisten, brauchen Unternehmen deshalb eine geeignete Methode, die nicht nur die Kontrolle, sondern auch die Überwachung der Zugriffe ermöglicht. Diese Methode kann auch als Grundlage dienen, um Informationen und Zugriffsrechte über das gesamte Unternehmen hinweg auf sichere Weise weiterzugeben und so das inhärente Risiko für interne Bedrohungen zu verringern.

Wie kann sich Ihr Unternehmen vor Insider-Bedrohungen schützen?

Um interne Bedrohungen zu verhindern und zu bekämpfen, brauchen Unternehmen zunächst einen vollständigen Überblick über ihre Netzwerke. Traditionell beschränkt sich dieser allerdings meist auf den Netzwerkperimeter, der überwacht wird, um sich vor externen Bedrohungen und Sicherheitsverletzungen zu schützen. Mittels erweiterter interner Sicherheitskontrollen kann ein Unternehmen einen umfassenderen Überblick gewinnen, um sich auch gegen interne Bedrohungen verteidigen zu können.

Wenn Sie diese Kontrollen implementiert haben, wie können Sie dann unternehmensweite Transparenz gewährleisten?

Eine Lösung, die sich dafür anbietet, ist **User and Entity Behaviour Analytics (Analyse des Verhaltens von Benutzern und Systemen, UEBA).**

[1]The Global State of Information Security Survey 2016, S. 24. [2]From Brutus to Snowden: A Study of Insider Threat Personas, S. 3. [3]Verizon Data Breaches Investigation Report 2016, S. 42.

User and Entity Behaviour Analytics
Schützen Sie Ihr Unternehmen von innen heraus

LogRhythm
The Security Intelligence Company

Was ist UEBA, und welche Bedeutung hat sie für Ihren Sicherheitsstatus?

Gartner definiert UEBA als eine Software, die „erfolgreich bösartige und missbräuchliche Aktivitäten entdeckt, die andernfalls nicht bemerkt würden, und Sicherheitswarnungen von anderen Systemen wirksam koordiniert und priorisiert“.[4]

UEBA ist ein leistungsstarkes Instrument, um Bedrohungen durch interne Benutzer zu erkennen und auf sie zu reagieren. Eine UEBA-Lösung hilft Unternehmen nicht nur, Bedrohungen aufzuspüren. Sie hilft auch, die Bedrohungen effektiv zu priorisieren und zu neutralisieren, da sie sämtliche Aktionen aller Benutzer verfolgt. Damit geht UEBA mehrere Schritte über alles hinaus, was die meisten Log-Systeme heute aufzeichnen.

Mittels maschinellem Lernen und anspruchsvollen Analysen erstellt UEBA Zug um Zug eine Baseline der Benutzer-Netzwerk-Interaktionen, die als normal angesehen werden. So kann die Lösung Warnungen ausgeben, wenn irgendwelche Abweichungen auftreten. Allerdings können Warnsignale auf alles Mögliche hinweisen, von einer Benutzeranmeldung an einem neuen Ort bis hin zu nicht autorisierten Datentransfers an eine externe Instanz. Deshalb ist es äußerst wichtig, dass eine UEBA-Lösung Bedrohungen bewerten und priorisieren kann.

Decken Sie blinde Flecken in Ihrem Unternehmen auf: mit der UEBA-Lösung von LogRhythm.

Von Kontoübernahmen bis hin zum Missbrauch privilegierter Accounts – UEBA ist die Lösung Nummer Eins zur Erkennung, Priorisierung und Entschärfung interner Bedrohungen. Die UEBA-Lösung von LogRhythm geht dabei noch einen Schritt weiter und verbindet die Benutzeranalyse mit der Analyse von Endpunkten und Netzwerken, um eine einheitliche, integrierte Sicht auf die Sicherheit zu gewährleisten. Damit bietet sie Ihrem Unternehmen nicht nur den nötigen Überblick, um interne wie auch externe Bedrohungen zu bekämpfen, bevor sie Schaden anrichten, sondern verkürzt auch die Amortisierungszeit und spart Ressourcen.

Wir möchten Unternehmen befähigen, Bedrohungen zu erkennen, abzuwehren und zu neutralisieren, bevor Schaden entsteht. Wenn Sie Ihr Risiko senken und umfassende Übersicht über Ihre Sicherheit gewinnen möchten, kontaktieren Sie LogRhythm.

[4] https://www.gartner.com/doc/3134524/market-guide-user-entity-behavior

Über LogRhythm

LogRhythm, ein führender Anbieter von Security Intelligence und Sicherheitsanalysen, unterstützt Unternehmen weltweit dabei, gefährliche Cyber-Bedrohungen schnell aufzuspüren, abzuwehren und zu entschärfen. Die patentierte, preisgekrönte Plattform des Unternehmens vereint auf einzigartige Weise SIEM der nächsten Generation mit Log-Management, Netzwerk- und Endpunktüberwachung, User Entity and Behaviour Analytics (UEBA), Automatisierung und Orchestrierung von Sicherheitsmaßnahmen sowie fortschrittlichen Sicherheitsanalysen. LogRhythm schützt die Kunden nicht nur vor den Risiken in Zusammenhang mit Cyber-Bedrohungen, sondern bietet darüber hinaus einzigartige Funktionalitäten zur Automatisierung und Gewährleistung der Compliance sowie erweiterte IT-Intelligence.

Die marktführende Rolle von LogRhythm spiegelt sich auch in zahlreichen Auszeichnungen. Das Unternehmen ist im Magic Quadrant-Bericht von Gartner zum Thema SIEM seit fünf Jahren in Folge als „Leader“ positioniert und wurde im SIEM Vendor Landscape-Bericht 2014/15 der Info-Tech Research Group als „Champion“ ausgezeichnet. SC Labs hat 2016 in seinem SIEM- und UTM-Produkttest eine 5-Sterne-Kaufempfehlung für LogRhythm ausgesprochen, und Frost & Sullivan hat dem Unternehmen den Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award 2015 verliehen.

LogRhythm hat seinen Hauptsitz in Boulder, Colorado, und verfügt über Niederlassungen in Nord- und Südamerika, Europa und der Region Asien-Pazifik.

www.logrhythm.com

www.logrhythm.com I +49 89 919292 - 200

© 2017 LogRhythm, Inc. Alle Rechte vorbehalten. Balanstraße 73 - Haus 7, 81541 München, Germany.