Advertorial

Wirksamer Schutz vor Insider-Bedrohungen

Laut des «2020 Verizon Data Breach Investigation Report» sind 30 Prozent aller Datenschutzverletzungen auf Insider zurückzuführen. Dank Insider Threat Management (ITM) von Proofpoint können Security-Teams Insider-Bedrohungen frühzeitig aufdecken, Untersuchungen beschleunigen und Datenverluste verhindern.

Bedrohungen durch Insider nehmen kontinuierlich zu – dies sowohl bezogen auf die Anzahl der Vorfälle als auch hinsichtlich der daraus entstehenden Folgeschäden. Nebst kriminellen oder böswilligen Motiven werden die meisten Insider-Vorfälle durch Unachtsamkeit, Unwissen oder fahrlässiges Verhalten von eigenen Mitarbeitenden oder Auftragnehmern ausgelöst.

In der herkömmlichen Sicht auf die Cybersicherheit herrscht eine Fokussierung auf von aussen gegen das Unternehmen gerichtete Bedrohungen. Doch um Bedrohungen durch Insider wirksam entgegenwirken zu können, bedarf es anderer Lösungen.

Insider-Vorfälle werden in der Regel lange nicht erkannt und oft reagieren Unternehmen erst dann, wenn der Schaden angerichtet bzw. der Datenverlust erfolgt ist. Zudem konzentrieren sie sich immer noch mehrheitlich darauf, stattgefundene Vorfälle zu analysieren und mit den daraus gewonnenen Erkenntnissen Massnahmen zu erarbeiten, die helfen sollen, künftige Vorfälle zu verhindern. Dabei handelt es sich um eine rein reaktive Vorgehensweise. Kommt hinzu, dass die Analyse der stattgefundenen Insider-Vorfälle oft auf der Auswertung von Logfiles basiert. Dies erfordert Spezialwissen und ist ausgesprochen zeitaufwendig. Zudem ist es schwierig, Kausalzusammenhänge aus den unterschiedlichen Logfile-Quellen herauszulesen.

Insider-Bedrohungen aufdecken

Einen anderen, richtungsweisenden Weg geht die innovative Insider-Threat-Management-(ITM-)Lösung von Proofpoint. Sie erkennt Risiken von internen Sicherheitsvorfällen durch kontextbezogene Informationen. Dazu sammelt Proofpoint ITM Daten über User-Rollen, User-Aktivitäten, Alarme/Events von Drittsystemen sowie von Datenveränderungen bzw. Datenverschiebungen und korreliert diese. Dank den mitgelieferten Regelwerken wird schnell erkannt, ob ein auffälliges Verhalten stattfindet. Ist dies der Fall, werden das Security-Team sowie der entsprechende User darüber informiert – noch bevor Schaden entsteht. Bei bereits erfolgten Insider-Vorfällen bietet die Lösung fallbezogene Informationen an, um eine rasche Aufklärung zu ermöglichen. Dazu liefert Proofpoint schnell Antworten mit dem nötigen Kontext über das «Wer, was, wo, wann und warum», ohne dass hierzu Wissen über die Interpretation von Logfiles benötigt wird.

Proofpoint ITM sammelt über unterschiedliche Quellen die Daten für das User Monitoring. Dazu werden Agents auf den Endgeräten und Servern installiert und ein dedizierter Server analysiert die Zugänge von externen Auftragnehmern. Mehrere vorgefertigte Schnittstellen ermöglichen es, Daten von bestehenden SIEM-Lösungen wie Splunk, QRadar, McAfee oder LogRhythm einlesen zu können. Zudem lassen sich mit der vorhandenen Restful API weitere Security-Drittsysteme integrieren. Die gesammelten Daten werden alsdann auf der Proofpoint ITM-Konsole aufbereitet, korreliert und für das Security-Team übersichtlich dargestellt.

Bei der Entwicklung von Proofpoint ITM, das aus der Übernahme von ObserveIT hervorging, wurde grosser Wert auf die Einhaltung des Daten- bzw. Mitarbeiterschutzes gelegt. So berücksichtigt die Lösung sämtliche DSVGO-Vorgaben. Zudem werden die Mitarbeitenden aktiv informiert, wenn ein Fehlverhalten festgestellt wird – noch bevor ein Schaden zu beklagen ist. Hinzu kommt, dass die Mitarbeiterdaten anonymisiert dargestellt bzw. nur wenn notwendig (z. B. bei mutmasslichen Insider-Vorfällen) mittels 4-Augen-Prinzips deren Personendaten sichtbar werden.

Proofpoint Insider Threat Management (ITM) schützt Unternehmen vor Datenverlusten, schädlichen Aktionen und Markenschädigung, die durch böswillig, fahrlässig oder unbewusst falsch handelnde Insider entstehen.

Proofpoint ITM: die Highlights

- Identifizierung von Benutzerrisiken
- Vorbeugung und rasche Aufklärung von Insider-Vorfällen
- Unterbindung unautorisierten Datenabflusses (Data Loss Prevention)
- Einhaltung des Daten- und Mitarbeiterschutzes
- Rasche Inbetriebnahme dank mehr als 350 mitgelieferten Regelwerken
- Kein Security-Spezialwissen für die Anwendung notwendig
- On-Prem-Installation

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch