Improve and automate Account Security by Identity Analytics

Studiengang: MAS | Vertiefung: MAS Information Technology

Heutige Security-Komponenten wie Firewalls, Intrusion Detection Systems, etc. schützen zuverlässig gegen Angriffe, welche von ausserhalb des Perimeters erfolgen. Doch was passiert, wenn der Angreifer mittels kompromittierten Accounts oder als legitimer Insider agiert?

Ausgangslage

Das schwächste Glied in der Cyber Defence Chain ist heutzutage der Mensch. Eine Phishing Attacke, gezielt oder auf gut Glück, verspricht die grösseren Erfolgschancen, als ein frontaler Hackerangriff auf Security-Systeme.
Attacken auf Benutzer und deren Accounts stellen somit einen der grössten Angriffsvektoren unserer Zeit dar. Hinzu kommen andere Bedrohungen, wie zum Beispiel Insider Threats, welche durch die eigenen Mitarbeiter ausgelöst werden. Sei dies bewusst und mit Motiv, oder unbewusst durch Fehlverhalten.

Ziel der Arbeit

Das Ziel dieser Arbeit als erste durch die SBB-IT durchgeführte Studie ist die neuen Entwicklungen in den Bereichen Adaptive Authentication und Identity Analytics zu beleuchten und dessen Potential für die Unternehmung abzuklären. Diese Technologien werten Benutzerattribute wie Login-Zeit, Geoposition und gewünschten Zugriff des Benutzers über eine bestimmte Zeitspanne aus. Daraus wird versucht, abzuleiten, ob der Login-Versuch tatsächlich von der autorisierten Person stammt. Je nach Befund können vordefinierte Aktionen ausgelöst werden.
Das Ergebnis der Masterarbeit soll als Grundlage zur weiteren Evaluierung im Bereich Identity Analytics zum Abschwächen von Insider Threats und Social Attacks bei den Bundesbahnen dienen.

Umsetzung

Im Rahmen einer explorativen Studie wurde nach einem Vier-Phasen-Prinzip vorgegangen:
In einer ersten Phase wurde das Thema durch die Recherche von Fachliteratur und Marktforschungsberichten sowie das Durchführen von Interviews und das Besuchen von Fachmessen aufgearbeitet. Die zweite Phase beinhaltete das Erfassen und Kategorisieren des Ist-Zustands der Authentisierungssysteme in der SBB-IT Landschaft. Anhand dieser Informationen wurden Teil-Systeme definiert, mit dem Ziel, auf der operationellen Logging-Plattform Splunk einen Identity Analytics Proof of Concept mittels realer Login Daten durchzuführen.
Die dritte Phase umfasste die Erarbeitung des PoC, die Interpretation sowie eine Risikobewertung der Resultate. Bezugnehmend auf das Erarbeitete wurden Vorteile, aber auch Limitationen der Anwendungsfälle dargestellt. In der vierten und letzten Phase schliesslich wurden die gesammelten Informationen und Erkenntnisse konsolidiert, eine SWOT Analyse zum Einsatz von Identity Analytics erstellt und eine Empfehlung abgegeben, wie man dieses Mittel zur Detektierung von account-bezogenen Gefahren bei den SBB einsetzen könnte.

Ergebnis

Abschliessend lässt sich sagen, dass die Identity & Access Management (IAM) Systemlandschaft bei den SBB die Voraussetzungen für Identity Analytics grundsätzlich erfüllt. Der Proof of Concept konnte auf bereits bestehenden Systemen durchgeführt werden und liefert Erkenntnisse für das weitere Vorgehen.
User Behavior & Identity Analytics stellen in naher Zukunft wichtige Security-Faktoren im Identity & Access Management-Umfeld dar. Für deren Einsatz sind jedoch noch technische und rechtliche Herausforderungen zu meistern.

Philipp Bretscher