WHITE PAPER | MÄRZ 2017

Security für Unternehmensdaten: Grundlagen zur Analyse des Anwenderverhaltens

ca technologies

Inhaltsverzeichnis

Kurzfassung

Berichte über Cyberangriffe sind immer wieder in den Schlagzeilen. Während die bekanntesten Angriffe – darunter die großen Datenschutzverletzungen bei J.P. Morgan, Anthem und Slack – von außerhalb der betroffenen Unternehmen durchgeführt wurden, nehmen Diebstahl und Datenmissbrauch durch privilegierte Anwender zu.

Tatsächlich gaben 69 % der Security-Experten in Unternehmen an, dass sie bereits Diebstahl oder Beschädigungen von Unternehmensdaten durch Insider, denen sie vertraut hatten, erlebt haben.[1] Es gibt auch Fälle, in denen Auftragnehmer, Zulieferer oder Partner eines Unternehmens für Datenschutzverletzungen in seinem Netzwerk verantwortlich waren, sei es durch böswilliges oder unachtsames Verhalten.

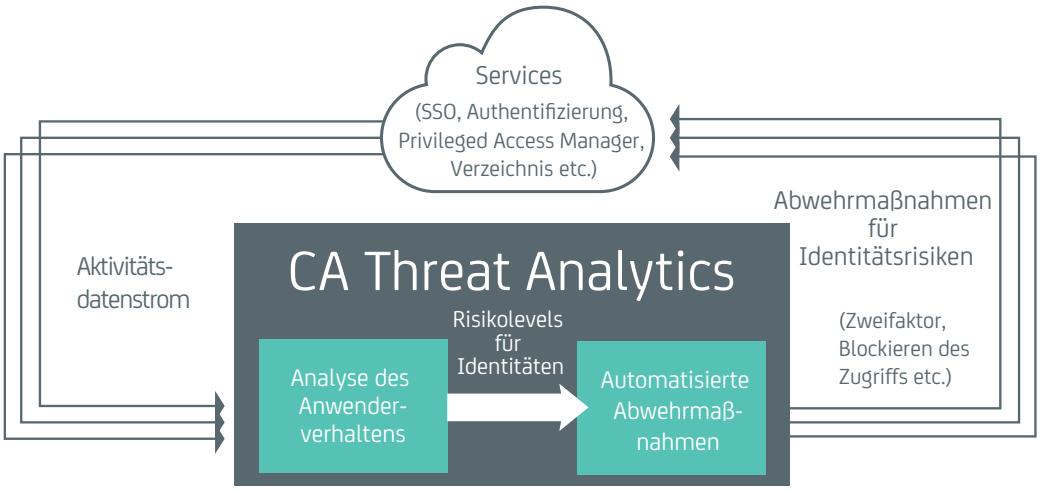
Wenn wir aus solchen Ereignissen irgendetwas gelernt haben, dann, dass der Schutz privilegierter Zugriffe für Unternehmen aller Größen weiterhin ein dringendes Anliegen ist. Doch trotz dieses Wissens und einer Vielzahl erhältlicher Security-Produkte sind viele IT-Systeme weiterhin anfällig für Angriffe.

Das Problem liegt darin, dass herkömmliche Kontrollmechanismen für das Identity and Access Management (IAM) zwar umfangreich, aber statisch sind. Sobald böswillige Anwender Zugang erhalten, können sie das System im Rahmen der festgelegten Berechtigungen des betreffenden Accounts ausnutzen.

Durch Bereitstellung eines identitätsbezogenen Security-Ansatzes, der die Analyse des Anwenderverhaltens und die Erkennung von Anomalien zu einem Modell maschinellen Lernens vereint, können Unternehmen risikoreiche Aktivitäten jedoch schnell erkennen und automatisch Kontrollmechanismen zur Abwehr auslösen, um den Schaden für das Unternehmen zu begrenzen.

CA Threat Analytics

CA Threat Analytics schützt Unternehmensdaten auf die gleiche Weise, in der Kreditkarten Geld schützen. Während diese Formulierung die richtigen Vorstellungen vermittelt – nämlich, dass dauerhaftes Monitoring sowie der Einsatz von Analyseverfahren dazu dient, Risiken zu ermitteln und Asset-Diebstahl zu verhindern – gibt sie kaum Aufschluss darüber, wie dies erreicht wird. In diesem White Paper wird beschrieben, wie CA Threat Analytics Unternehmensdaten mithilfe von zwei miteinander in Beziehung stehenden Lösungen schützt: Analyse des Anwenderverhaltens und automatisierte Abwehrmechanismen.



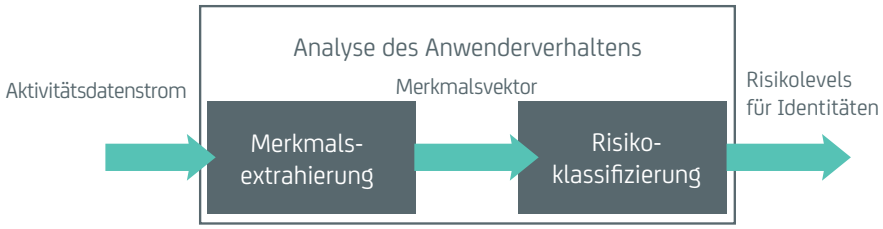
Mit der Analyse des Anwenderverhaltens kann das Unternehmen Risiken kontinuierlich bewerten und böswillige Maßnahmen schnell erkennen. Bei der Analyse des Anwenderverhaltens wird ein Datenstrom als Input verwendet, der Informationen dazu enthält, wie eine bestimmte Identität oder Gruppe von Identitäten mit Services oder Anwendungen interagiert. Auf dieser Grundlage wird für jede Identität im Unternehmen ein Risikolevel angegeben.

Mithilfe automatisierter Abwehrmaßnahmen kann das Unternehmen automatisch Maßnahmen ergreifen, die Risiken mindern und erkannte böswillige Aktivitäten stoppen. Außerdem verändern sie die Access Control für einzelne Identitäten anhand der Risikobewertung, die die Analyse des Anwenderverhaltens ausgibt. Ein einfaches Beispiel für eine automatisierte Abwehrmaßnahme ist die automatische Blockierung des Zugriffs einer risikoreichen Identität auf eine hoch vertrauliche Anwendung oder ein besonders sensibles Daten-Repository.

Während sowohl die Analyse des Anwenderverhaltens als auch die automatisierten Abwehrmaßnahmen integrale Bestandteile von CA Threat Analytics sind, liegt der Schwerpunkt dieses White Papers gezielt auf der Analyse des Anwenderverhaltens. In den folgenden Abschnitten werden die Einzelteile des oben gezeigten Analyseverfahrens für das Anwenderverhalten aufgezeigt. Dann werden diese Teile im Einzelnen detailliert erläutert. Aus Gründen der Einfachheit bezieht sich die Erläuterung zunächst auf den Schutz einer einzelnen Identität, die einen einzelnen Service verwendet. Nachdem die Grundlagen der verwendeten Techniken vorgestellt wurden, wird erörtert, wie diese Ideen für die Arbeit mit einer Vielzahl von Identitäten und unterschiedlichen Services erweitert werden können.

Grundlagen

Konzeptionell besteht die Analyse des Anwenderverhaltens aus zwei Komponenten: der Merkmalsextrahierung und der Risikoklassifizierung.



Die Merkmalsextrahierungskomponente verarbeitet einen Aktivitätsdatenstrom und extrahiert einen Satz relevanter Merkmale. Die relevanten Merkmale beschreiben eine einzelne Identität und wurden im Laufe der Zeit beobachtet, wie beispielsweise:

- Die Identität verwendet ein unbekanntes Mobile Device.
- Die Identität agiert von einem dezentralen Standort aus.
- Die Identität agiert über eine verdächtige IP-Adresse.
- Die Identität ist Mitglied einer privilegierten Gruppe.
- Die Identität hat den Service X außerhalb ihrer normalen Arbeitszeit verwendet.

Die Merkmalsextrahierung ist komplizierter als sie erscheint, weil es nicht einfach nur darum geht, Eigenschaften einer aktuellen Transaktion zu extrahieren. Obwohl ein Aktivitätsdatenstrom als eine Abfolge einzelner Ereignisse ankommt, erhält man den gesamten, von Beginn an aufgezeichneten Aktivitätsdatenstrom. So können Sie die gesamten Nutzungs- und Verhaltensdaten zu jeder Identität verstehen. Ohne die Möglichkeit, das vollständige Aktivitätsprotokoll untersuchen zu können, müssten Sie das Risiko rein anhand jedes einzelnen Ereignisses bewerten.

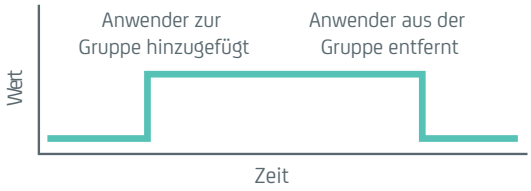
Um ein Beispiel zu einem der aufgeführten Merkmale zu verwenden: Welchen Wert hat die normale Arbeitszeit im Kontext eines einzelnen Ereignisses? Damit CA Threat Analytics wichtige Merkmale wie dieses verwenden kann, muss die Lösung auch Einblicke in Protokolldaten erhalten und diese mit einberechnen können.

CA Threat Analytics untersucht den gesamten Aktivitätsdatenstrom und liefert dem Unternehmen so wesentlich mehr Erkenntnisse als zuvor für die Risikobewertung und die Erkennung böswilliger Maßnahmen verfügbar waren. Das Unternehmen kann Risiken jetzt anhand vergangener Maßnahmen und spezifischer Informationen zu einzelnen Identitäten bewerten. Dies ist vorteilhaft, erfordert jedoch auch die Verarbeitung einer großen Menge an Daten, von denen viele redundant sind. Glücklicherweise wird jedoch mithilfe der Merkmalsextrahierung die Dimensionalität der Daten reduziert. Sie eliminiert oder fasst redundante Daten zusammen und kennzeichnet zugleich die Informationen, die für den zweiten Teil der Analyse des Anwenderverhaltens erforderlich sind: die Risikoklassifizierung.

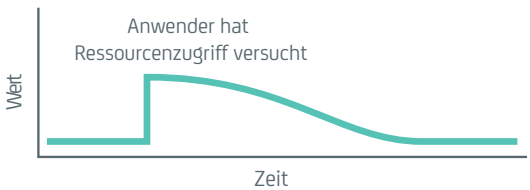
Ermitteln von Wert im Kontext der Zeit

Sehen wir uns zunächst ein interessantes Detail der Merkmale an, die im Laufe der Zeit beobachtet werden. Da sie verändert werden, wenn Maßnahmen stattfinden, sind sie streng genommen Teil der Zeitebene. Dies bedeutet einfach, dass sich die Werte im Laufe der Zeit verändern. Wenn ein Merkmal beobachtet wird, modelliert CA Threat Analytics die Beobachtung in Abhängigkeit der Zeit. In anderen Worten: Wenn eine stattfindende Maßnahme zur Aktivierung eines Merkmals führt, ist es möglich, dass der „Wert“ des Merkmals zum Zeitpunkt der Maßnahme maximal ist und sich im weiteren Zeitverlauf verändert.

Die tatsächliche Veränderung des Werts kann je nach extrahiertem Merkmal ganz unterschiedlich ausfallen. Einige sind völlig binär. Das bedeutet: Wenn das Merkmal beobachtet wird, bleibt es auf seinem höchsten Wert, bis es, wie im Folgenden, abgeschwächt wird.



Ein Beispiel ist die Mitgliedschaft in einer sensiblen Gruppe. Dieses Merkmal behält während des gesamten Zeitraums, in dem die Identität zu der Gruppe gehört, seinen höchsten Wert. Andere Merkmale werden als abfallende Impulse modelliert. Wenn ein Merkmal dieser Art beobachtet wird, ist der Wert am höchsten und fällt danach, wie im Folgenden zu sehen, im Laufe der Zeit ab.



Ein Beispiel ist ein Anwender, der versucht, auf eine Ressource zuzugreifen, ohne dazu berechtigt zu sein. Während dieses Merkmal heute für den Risikolevel der Identität relevant ist, ist es in einer Woche viel weniger relevant, und in einem Monat noch einmal weniger. Indem angenommen wird, dass die Merkmalswerte im Laufe der Zeit abfallen, stellt CA Threat Analytics sicher, dass sie bestmöglich zum Risikowert beitragen.

Risikoklassifizierung

Die Risikoklassifizierung ist ein Analyseverfahren, das den Merkmalsvektor in drei einzelne Risikolevels umwandelt:

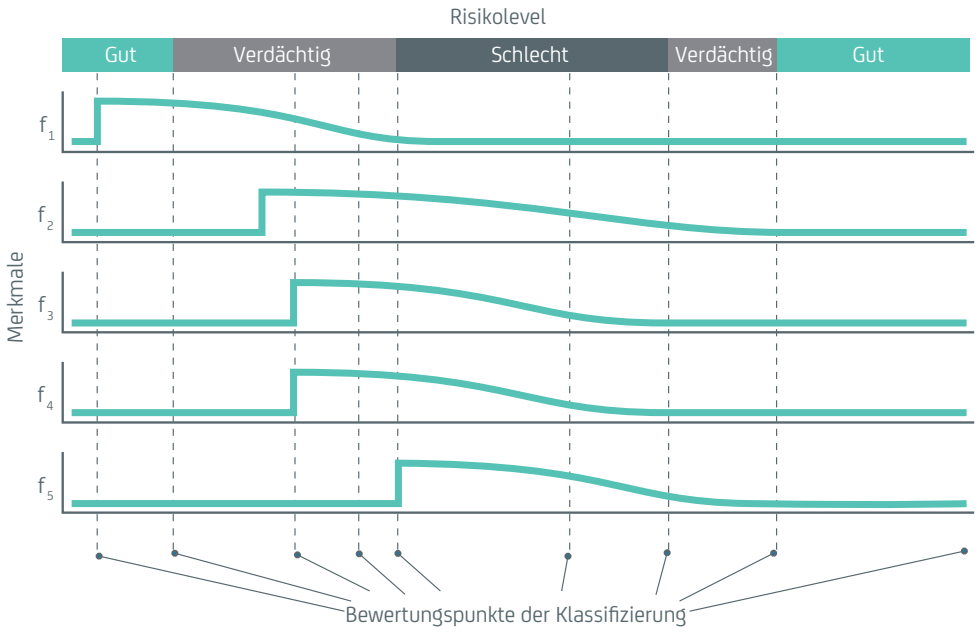
- **Gut**: Die Identität stellt ein minimales Risiko dar.
- **Verdächtig**: Die Identität wurde mit Ereignissen oder Maßnahmen in Verbindung gebracht, die ein Risiko darstellen. Dieses Risiko erfordert jedoch keine unmittelbare Reaktion. Das System wird diese Identität genauer überwachen und abhängig von der Unternehmensrichtlinie möglicherweise anfängliche automatisierte Abwehrmaßnahmen anwenden.
- **Schlecht**: Die Identität wir als hohes Risiko angesehen und bedarf sofortiger Aufmerksamkeit. Das System wendet automatisierte Abwehrmaßnahmen und Warnungen gemäß der Unternehmensrichtlinie an.

Die Risikoklassifizierungsfunktion arbeitet mit einem Vektor von Merkmalswerten und ermittelt eines der obigen Levels.

$$\text{Klassifizierung}(\overrightarrow{\text{Merkmale}(t)}) \longmapsto \{\text{gut, verdächtig, schlecht}\}$$

Wie oben erörtert, sind die Merkmale zeitabhängig, sodass die Risikoklassifizierungsfunktion ebenfalls in der Zeitebene arbeitet. Die Risikoklassifizierung wird an kritischen Entscheidungspunkten angewendet. Im Allgemeinen ist dies eine Reaktion auf wesentliche Änderungen an den Werten des Merkmalsvektors. Wenn der Risikolevel für einen bestimmten Zeitpunkt von der Risikoklassifizierung berechnet wird, werden alle Merkmalsfunktionen dieser Identität oder Einheit in diesem Moment ausgewertet. Der vollständige Satz an Merkmalen, die für die Einheit in diesem Moment aktiv sind, bildet den tatsächlichen Merkmalsvektor, der von der Risikoklassifizierung zur Bestimmung des Risikos verwendet wird.

In der folgenden Abbildung sind die einzelnen Punkte gekennzeichnet, an denen die Risikoklassifizierung wahrscheinlich durchgeführt würde. Wie bereits angemerkt, werden die Bewertungen durchgeführt, wenn der Wert eines Merkmals steigt oder unter einen Schwellenwert fällt. Die an die Risikoklassifizierung übergebenen Werte entsprechen dem Wert jedes Merkmals zu dem Zeitpunkt, zu dem seine Bewertung in Bezug zu den senkrechten Linien oben ausgelöst wurde. Natürlich führt nicht jeder Durchlauf der Risikoklassifizierung zu einem neuen Risikolevel. Es gibt sogar viel mehr Auswertungspunkte als dargestellt. Sie entsprechen Veränderungen an Merkmalswert, Systemaktivität und Bedrohungsinformationen. Im Allgemeinen wird die Risikoklassifizierung jedes Mal aktiviert, wenn eine Änderung des Risikolevels möglich ist.



Wie lässt sich die Risikoklassifizierung nun also genau definieren? Wie überführt sie einen Merkmalsvektor in eines der Risikolevel? Es ist hilfreich, erst einmal festzuhalten, was die Risikoklassifizierung nicht ist. Risikoklassifizierungen von CA Threat Analytics sind keine einfachen Regeln, die spezifische Merkmale überprüfen, wie etwa: „Wenn Merkmal X aktiv ist, dann „Schlecht" angeben". Dies ist ein naiver Ansatz, der von vielen herkömmlichen Security-Produkten verwendet wird. Dieser Ansatz ist völlig ungeeignet, weil er viele Fehlalarme produziert, fragil und leicht zu überwinden ist. Außerdem nutzt er die Informationen nicht, die entscheidend sind, um böswillige Aktivitäten zu erkennen und das System für legitime Anwender nutzbar zu machen.

Die Lösungen von CA Threat Analytics sind weitaus robuster. Die Risikoklassifizierung von CA Threat Analytics untersucht Merkmale nicht in einem Vakuum, sondern im Kontext aller verfügbaren Merkmale. Mit diesem Ansatz können mehrere Merkmale, die einzeln keine Auswirkungen auf den Risikolevel haben, kombiniert werden, um ein Risiko angemessen zu bewerten. Außerdem bezieht CA Threat Analytics Feedback von bereitgestellten Systemen ein, um die im Laufe der Zeit getroffenen Entscheidungen zu optimieren. Darunter fallen Aspekte einzelner Anwender und Veränderungen in der Identitätengruppe. Das Ergebnis ist ein System, das flexible Anpassungen an neue Bedrohungen und Bereitstellungsszenarien ermöglicht.

Gruppen und Services

Wie bereits erwähnt, wurden für die obige Erörterung mehrere praktische Details vereinfacht. Erstens: Was sind Gruppen von Identitäten? Vor allem in der Unternehmensumgebung gibt es Aspekte der Gruppe von Identitäten, die für den Risikolevel einer bestimmten Identität relevant sind. Ein paar Beispiele:

- Zugreifen auf Ressourcen mit mehr Geräten als für das Unternehmen üblich
- Arbeiten außerhalb des normalen Betriebsstandorts der Gruppe
- Zugehörigkeit zu einer unangemessenen Anzahl an Gruppen

Das Grundverhalten der zu erwartenden Maßnahmen ist für jedes Unternehmen anders. Hierzu gehören Faktoren wie die normale Anzahl an Geräten, die einem Anwender zugeordnet sind, die Betriebsstandorte des Unternehmens und die passende Anzahl an Gruppen. Indem Sie statt isolierter Identitäten eine Gruppe von Identitäten betrachten, können Sie ein hohes Maß an nützlichen Gruppenstatistiken erhalten, mit denen Sie die einzelnen Identitäten vergleichen können. Dies hat natürlich auch seinen Preis. Statt nur den gesamten Aktivitätsdatenstrom für eine Identität zu verarbeiten, ist die Durchführung einer Merkmalsextrahierung für das gesamte Aktivitätsprotokoll des gesamten Unternehmens erforderlich.

In ähnlicher Weise bietet die Erweiterung der Analyse eines einzelnen Service auf eine Gruppe von Services einen anderen Nutzen. Durch die Untersuchung der Aktionen, die eine Identität für unterschiedliche Services ausführt, können wir Merkmale extrahieren, um Modelle typischer Zugriffsmuster zu erstellen und sie intelligent anzuwenden, um Security für alle Services bereitzustellen. Mithilfe dieser Informationen kann CA Threat Analytics unregelmäßiges und inkonsistentes Verhalten erkennen, das eine Bedrohung für diese Identität oder für das Unternehmen darstellt.

Fazit

In diesem White Paper wurde einführend beschrieben, wie CA Threat Analytics Unternehmensdaten mithilfe der Analyse des Anwenderverhaltens schützt. Während die Grundideen leicht zu erklären sind, liegen die praktischen Aspekte der Merkmalsextrahierung und der Risikoklassifizierung weit außerhalb des Rahmens dieses White Papers. Viele der praktischen Anforderungen, die unser Team motivieren, wurden noch nicht einmal erwähnt. Dazu zählen die Unterstützung der Entscheidungsfindung in Echtzeit, das Sicherstellen der Systemgenauigkeit im Laufe der Zeit und die Gewinnung echter Erkenntnisse zu Risikoentscheidungen für Systemadministratoren.

Wenn Sie mehr über diese Motivationen erfahren möchten und dazu, wie Ihr Unternehmen von ihnen profitieren kann, klicken Sie auf diesen Link: CA Threat Analytics for PAM.

1 Accenture und HfS Research, „The State of Cyber Security and Digital Trust 2016“, Juni 2016: https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf#zoom=50

CS200-259092