# Die Daten-Detektive

**IT-SICHERHEIT** – Selbstlernende Systeme, welche **alle Vorgänge im IT-System der Unternehmen beobachten und analysieren,** sind ein entscheidender Beitrag zu mehr IT-Sicherheit. Blick auf drei Techniken mit unterschiedlichen Schwerpunkten.

**Bozen** – Bis vor wenigen Jahren assoziierte man mit den Begriffen Big Data und Künstliche Intelligenz eher theoretische Zukunftsszenarien als praktische Anwendungen. Das uneingeschränkte Sammeln, Speichern und Zusammenführen von Unmengen von Informationen jeder Art sowie die Analyse dieser Daten mit neuen technischen Methoden und Algorithmen sollten ganz neue Erkenntnisse und Lösungsmethoden für bestehende Probleme bringen. Aus diesem Hype um Big Data sind mittlerweile handfeste Anwendungen geworden, welche auf den verschiedensten Gebieten zum Einsatz kommen. Dazu zählen etwa die medizinische Diagnostik, die Vorhersage von Epidemien, die Kriminalanalytik und Terrorbekämpfung, der nachhaltige Umgang mit ökologischen Ressourcen und die Onlinewerbung.

Aber auch auf dem Gebiet der IT-Sicherheit hat Big Data schon Einzug in die Praxis gehalten. Die IT-Landschaft eines modernen Unternehmens besteht aus einer Vielzahl von Endgeräten, Servern, Netzwerkkomponenten, Datenbanken und Applikationen, meist auch aus Anwendungen in der Cloud. Bei digitalisierten Produktionsbetrieben gesellen sich noch die Sensorik und Robotik dazu. All diese Systeme erzeugen im laufenden Betriebe eine erhebliche Menge an technischen Daten. Diese Daten wurden in der Vergangenheit als wertlos eingestuft. Nun wird versucht, aus diesen Rohdaten mit neuen Analysemethoden wertvolle Erkenntnisse über den Zustand des Gesamtsystems zu gewinnen, etwa hinsichtlich Sicherheit oder für die Ressourcenoptimierung.

Diese Vorgehensweise wird von verschiedenen Produkten zur IT-Sicherheit eingesetzt. Drei Produktkategorien werden in der Folge etwas näher betrachtet.

### Ein SIEM stellt Ausnahmesituationen fest und löst Alarm aus

Das Kürzel **SIEM** steht für **„Security Information and Event Management"** und bedeutet so viel wie das Verwalten von sicherheitsrelevanten Informationen und Ereignissen. Ein SIEM ist darauf spezialisiert, alle sicherheitsrelevanten Ereignisse der Systeme im IT-Verbund in Echtzeit an einer zentralen Stelle zu erfassen. Ein charakteristisches Merkmal eines SIEMs ist die Fähigkeit, die verschiedenen Ereignisse plattformübergreifend intelligent zu interpretieren und zu klassifizieren. Damit eröffnet sich die Möglichkeit, Einzelereignisse in der gesamten IT-Landschaft miteinander zu korrelieren und daraus ganz neue Erkenntnisse zu gewinnen. So sind etwa sporadische fehlgeschlagene Logins auf unterschiedlichen Systemen für sich betrachtet ganz physiologisch, wenn allerdings darin ein bestimmtes Muster erkannt wird, so kann dies ein Hinweis auf einen ausgeklügelten Angriffsversuch sein.

Wird durch das SIEM eine Anomalie detektiert, so wird ein Alarm ausgelöst, und die gesamte relevante Information zum Vorfall wird bereitgestellt. Bei eindeutig gefährlichen Situationen kann ein SIEM auch automatisiert darauf reagieren.

Moderne SIEMs sind selbstlernend und können nach einiger Zeit selbstständig einschätzen, ob die aktuelle Situation normal ist, oder ob es signifikante Abweichungen vom Normalen gibt.

### UEBA-Systeme erkennen Abweichungen vom Normalverhalten

Maschinengestütztes Lernen ist auch eine besondere Spezialität von sogenannten **„User and Entity Behavior Analytics"-Systemen (UEBA).** Der Name bedeutet die Analyse und das kontinuierliche Überwachen des Benutzer- und Systemverhaltens. Liegt bei einem SIEM der Schwerpunkt der Analyse auf den einzelnen Sicherheitsereignissen, so sind es bei einem UEBA-System ganz allgemeine Parameter wie etwa die Anzahl der Datenbankzugriffe, die Anzahl der gelesenen oder modifizierten Dateien, die übertragene Datenmenge, die Netzwerkzugriffe oder die Zeiten des An- und Abmeldens. Aus all diesen Werten ergibt sich ein Bild, wie die Benutzer im Normalfall die IT-Systeme verwenden. Diese Parameter werden von einem UEBA-System kontinuierlich analysiert, und nach einer angemessenen Lernphase können damit auch subtile Abweichungen von Normalverhalten festgestellt werden.

> Wenn Anmeldungen zu unüblichen Zeiten stattfinden, so könnte dies ein Hinweis auf ein kompromittiertes Konto eines Anwenders sein.

Eine erhöhte Anzahl von Dateizugriffen könnte etwa darauf hinweisen, dass ein böswilliger Insider versucht, Daten aus dem Unternehmen abzuleiten; und wenn zusätzlich noch Anmeldungen zu unüblichen Zeiten stattfinden, so könnte dies ein Hinweis auf ein kompromittiertes Konto eines Anwenders sein.

Die UEBA-Systeme enthalten schon eine Vielzahl von Analysemethoden, um gängige Bedrohungen zu erkennen. Sie bieten aber auch die Möglichkeit, neue Methoden festzulegen, und der Fantasie sind dabei keine Grenzen gesetzt.

Der Einsatz eines UEBA-Systems ist für Hochsicherheitsbereiche im Unternehmen absolut anzuwenden, wenn nicht sogar verpflichtend. Wenn man allerdings bedenkt, wie rasch die Digitalisierung voranschreitet und dass nach wie vor die größte Gefahr zur IT-Sicherheit nachweislich aus dem Inneren des Unternehmens kommt, so ist es sicher angebracht, solche Systeme unternehmensweit zur Vorbeugung und zum Erkennen von Bedrohungen einzusetzen.

### NAC-Produkte helfen, dass nur berechtigte Geräte zum Netzwerk zugreifen

Auf einen anderen spezifischen Themenbereich der IT-Sicherheit sind die NAC-Produkte (**N**etwork **A**ccess **C**ontrol) zugeschnitten: auf das Netzwerk. Zu jedem Zeitpunkt muss garantiert sein, dass nur berechtigte Geräte mit konformen Einstellungen und authentifizierten Benutzern auf die Informationen des Unternehmens zugreifen können. Durch die enorme Verbreitung von Smartphones und Tablets, durch den selbstverständlichen Einsatz von WLANs und durch die Vernetzung der Objekte im Internet der Dinge gestalten sich dies als wahre Herausforderung. Und hierbei unterstützen die NAC-Produkte, deren Kernaufgabe darin besteht, die Geräte, welche sich mit dem Netzwerk verbinden, vorab zu überprüfen und die Rechtmäßigkeit der Verbindung einzuschätzen.

Für die Überprüfung eines Verbindungsversuches können ganz unterschiedliche Entscheidungskriterien zum Einsatz kommen, und die innovativen NAC-Produkte erledigen viele Aufgaben mit eigener Intelligenz und selbstlernenden Fähigkeiten, gestützt auf Big Data. Erfüllt ein Gerät die Bedingungen für den Zugang nicht, so wird es aus dem Netzwerk ausgesperrt oder in einen Bereich zur Normalisierung verschoben. Wird die Verbindung zum Netzwerk hingegen erlaubt, so wird das Verhalten des Gerätes laufend überprüft, und im Falle eines Regelverstoßes wird die Verbindung sofort wieder getrennt.

Ein wichtiger Nebeneffekt beim Einsatz eines NAC-Produktes ist die erlangte Sichtbarkeit auf das gesamte Netzwerk. In vielen Fällen ist dies allein schon der ausschlaggebende Grund, ein NAC-Produkt einzusetzen.

Der Fokus der drei betrachteten Techniken ist unterschiedlich, aber alle werden mit dem Ziel eingesetzt, die IT-Sicherheit im Gesamten zu verbessern.

**Martin Gallor**

**DER AUTOR** ist Verantwortlicher für Datenschutz und -sicherheit beim IT-Dienstleister Konverto, der im Mai aus der Fusion von RUN (Raising Unified Network) und ROL (Raiffeisen OnLine) hervorgegangen ist.