Sicher digitalisieren ohne Silos

Ein Security Information Event Monitoring (SIEM) bewährt sich für die IT-Security. Doch für durchgängige Sicherheit über Abteilungen hinweg braucht es ein Digital Operating Center (DOC), das alle Quellen einbezieht und Incidents in ihrem Impact auf Business-Prozesse sichtbar macht.

Ein Security Information Event Monitoring schafft Visibilität über relevante sicherheitsbezogene Ereignisse auf den IT/OT-Geräten eines Firmennetzwerks, die gesammelt, korreliert und komprimiert werden. Bei Gefahr wird Alarm ausgelöst. Doch funktioniert ein SIEM nur isoliert im Hinblick auf Security-Vorfälle, ebenso wie die Netzwerktechniker in ihren Network Operation Centers (NOC) und viele weitere «Operation Centers» im Unternehmen in ihren eigenen Silos befangen sind. Eine Firma ist jedoch mehr als die Summe ihrer Abteilungen. Daher etabliert sich mehr und mehr die Idee eines DOC – eines Digital Operating Centers, das bereichsübergreifend Ereignisse aus dem täglichen Betrieb zusammenführt, auswertet und zielgerichtet die richtige Sicht für die jeweiligen Stakeholder zur Verfügung stellt.

Bereichsübergreifende Sicht auf Prozesse statt Events

In einem Unternehmen steht eine Vielzahl von Daten zur Verfügung, aus deren Analyse Erkenntnisse über bereichsübergreifende Risiken gewonnen werden können. Indem alle Quellen eingebunden werden, wird ein Mapping auf die geschäftsrelevanten Prozesse möglich, sodass der Impact eines Incidents direkt in dessen Verlauf veranschaulicht werden kann. Daten aus den diversen Operating Center können um eine Vielzahl an Businessdaten angereichert werden. Grundsätzlich sollte ein DOC in der Lage sein, jegliche Art von Informationen zu verarbeiten und zu korrelieren.

Prozessüberwachung im DOC am Beispiel einer Bank

Ein Credit Card Operating Center ist fähig, eine betrügerische Finanztransaktion anhand der Korrelation von Standort- und Zeitangaben bei Bargeldbezug am Bankomaten aufzudecken. Zusätzlich wird ggf. der Bankomat auf Sicherheitsprobleme überprüft. Das IT-Asset Bankomat muss anschliessend in einen Zusammenhang mit der Kreditkarte gestellt werden. Entsprechend muss die Bank die für Kreditkarten verantwortliche Abteilung mit derjenigen für IT-Security vernetzen. Da die Bankomaten zumeist von Drittanbietern betrieben und gewartet werden, wird die IT-Security-Abteilung den Partner in die Verantwortung nehmen. In einem DOC hingegen würde der Blick nicht mehr nur auf ein singuläres Ereignis gerichtet. Vielmehr wäre das Gerät aufgrund seines verdächtigen Verhaltens als Sicherheitsrisiko erkannt und es könnten Schritte eingeleitet werden, bevor es überhaupt zum Kreditkartenmissbrauch kommt. Ein zentrales Reporting und Alerting wäre demzufolge wünschenswert und ist heute auch machbar.

Kein Snapshot, sondern ein konsistenter Report

Im DOC wird aus allen verfügbaren Security-Informationen ein konsistenter Report erstellt, der nicht nur einen «Snapshot» auf das SIEM liefert, sondern alle Ereignisse in geschäftskritischen Prozessen erfasst und so der Geschäftsleitung vorgelegt werden kann. Hierzu werden in der Analysephase die Anforderungen an das Reporting/Alerting definiert, sodass die entsprechenden Datenquellen integriert werden können. Ob statische oder dynamische Daten, ist irrelevant; es werden vielmehr Data Lakes mit einer Reporting- und Alert-fähigen Software verknüpft. Ein solches Security-Reporting kann beispielsweise den CISO entlasten, indem die Sicherheitslage in einem Ampelsystem visualisiert wird. In späteren Ausbauphasen kann das DOC vervollständigt werden, indem weitere Data Lakes, etwa aus dem NOC oder einem GRC (Governance, Risk, Compliance) Center, eingebunden werden, was die ganzheitlich abgebildete Prozesshaftigkeit steigert. Damit empfiehlt sich ein DOC für jedes Unternehmen, das Wert auf abteilungs- und prozessübergreifende Sicherheit legt. ■

T-Systems Schweiz AG, CH-3052 Zollikofen
Ronny Fischer
Security Chief Technology Officer
✆ +41 (0)848 11 22 11, 🖷 +41 (0)848 11 22 12
contact@t-systems.ch, www.t-systems.ch