Security Incident and Event Management-System

Studiengang: MAS Information Technology

Die aktuelle Bedrohungslage in der IT-Sicherheit verlangt einen zentralisierten, systemischen Blick auf die ICT-Infrastruktur der Unternehmung. Mit Hilfe eines Security Incident und Event Management-Systems (SIEM) können sicherheitsrelevante Informationen rasch und zuverlässig gesammelt, ausgewertet und entsprechende Massnahmen ergriffen werden.

Umfeld

Bei der betrachteten Organisation handelt es sich um ein öffentliches Unternehmen mit rund 2500 Mitarbeitenden. Sie erbringt dabei Dienstleistungen für die internen Mitarbeitenden sowie für weitere Partnerorganisationen auf lokaler, nationaler und internationaler Ebene. Die ICT-Umgebung ist geografisch stark verteilt und besteht aus einem komplexen Verbund verschiedenster ICT-Umgebungen, welche eine hohe Verfügbarkeit aufweisen müssen.

Problemstellung

Obwohl die Organisation über ein gutes Sicherheitsverständnis verfügt und Vorkehrungen getroffen hat, um die IT-Sicherheit strategisch abdecken zu können, sind im operativen Geschäft nur wenige Kernindikatoren verfügbar, um effizienter auf sicherheitsrelevante Vorfälle reagieren und diese nachverfolgen zu können.

Lösungskonzept und Realisierung

Das Lösungskonzept betrachtet die gesamte ICT-Organisation und wie sich ein SIEM Tool organisatorisch und technisch in die Umgebung einpassen lässt. Dabei werden sowohl System- wie auch Produktziele definiert, um die von der Organisation geforderte Funktionalität abdecken zu können. Das Vorhaben ist auf die ICT-Strategie abgestimmt und unterstützt die Umsetzung von entsprechend darin formulierten Zielen.
Im Rahmen der Produktevaluation wurde Splunk Enterprise als geeignetes Instrument evaluiert und ausgewählt, weil es die geforderten Funktionalitäten und Ziele abdecken kann und auch für weitere Anwendungsfälle einen strategischen Mehrwert im Gesamtunternehmen bietet.
Der Kern des Lösungsdesigns beruht auf Use Cases. Diese definierten Anwendungsfälle beschreiben, welche Informationen das System verarbeitet, wie diese dargestellt und welche Aktionen allenfalls ergriffen werden sollen.

Dabei wurden zwei Kernelemente aufgegriffen, um die Funktionalität exemplarisch aufzeigen zu können:

Malware – Infektion

Dieser Use Case deckt ein Bedürfnis ab, das für die Organisation wichtig ist. Es geht darum, aktuelle Generationen von Malware mit geeigneten Indikatoren zu erkennen, einzudämmen und deren Ursprünge zurückverfolgen zu können. Anhand dieses Anwendungsfalls kann der Nutzen eines SIEM für Entscheidungsträger sehr gut aufgezeigt werden.

Data Extraction / First Contact

Dieser Use Case konzentriert sich hauptsächlich auf die Namensauflösungsmechanismen (DNS). Hierbei werden die Namensauflösungsanfragen aus der ICT-Umgebung nach Mustern durchsucht, welche aufzeigen, dass Informationen abfliessen oder ungewöhnliche Anfragen durchgeführt werden. Das System wird so dimensioniert, dass es einerseits leistungsfähig genug ist, um auch höhere Datenaufkommen verarbeiteten zu können, die Komplexität aber möglichst zu beschränken. Die Applikationskonfiguration wird zentral verwaltet und die Konfigurationsinformationen automatisch auf die Umsysteme verteilt. Die Informationen sollen zielgruppengerecht dargestellt werden können.

Schlussbetrachtung

Die Problemstellung und der gewählte Lösungsansatz erweisen sich als Materie, welche sowohl in der Breite wie auch Tiefe sehr umfassend sind. Um den Nutzwert des Systems weiter zu erhöhen, sind dabei vor allem den Quelldaten, deren Korrelation und Visualisierung in Form von erweiterten Use Cases besondere Aufmerksamkeit zu schenken. Begleitende Faktoren, wie ISDS-Aspekte oder die Produktbeschaffung, welche im Rahmen dieses Projekts bereits erörtert wurden, müssen in weiteren Phasen ebenfalls vertieft ausgearbeitet werden. Die Weiterentwicklung und Verfeinerung des Gesamtsystems führt zu einem vielschichtigen, interessanten aber auch sehr arbeitsintensiven Projekt. Die Umsetzung erfolgt unterteilt in verschiedenen Schritten und wird sich über eine längere Zeitspanne hinziehen.

Michael Hurst