*/ Der Vorteil des Use-Case-Ansatzes besteht darin, dass es möglich ist, sehr schnell und einfach aus der großen Anzahl täglicher Events potenzielle sicherheitsrelevante Vorfälle herauszufiltern.

*/ Dieser Ansatz hat jedoch Nachteile bei der Erkennung von neu auftretenden, weiterentwickelten Cyberangriffen wie APTs oder Zero-Day-Attacken, für die zum Zeitpunkt des Auftretens noch kein Use Case formuliert werden konnte.

Ausgereifte technische Basis für wirtschaftlichen SOC-Betrieb

SIEM as a Service

Warum Use Cases bei der Erkennung von Cybergefahren helfen und trotzdem keinen ausreichenden Schutz bieten.

Der Schutz vor Cybergefahren ist für die meisten Unternehmen heute keine Frage des »ob«, sondern des »wie«. Viele Unternehmen setzen auf Security Information & Event Management (SIEM)-Lösungen, um vorhandene Informationen auf Cybersecurity-relevante Hinweise zu durchsuchen und auszuwerten. Allerdings setzen die Einrichtung und der Betrieb von SIEM-Lösungen tiefes Fachwissen und Erfahrung sowohl bei der Erkennung von Cybergefahren als auch in der Formulierung und Implementierung der notwendigen Erkennungsmechanismen voraus. Zudem verfügen IT-Abteilungen oftmals nur unzureichend über das erforderliche Know-how oder sind nicht in der Lage, das vorhandene Wissen permanent aktuell zu halten. SIEM-Lösungen in Form von Managed Services können hier eine sinnvolle Alternative darstellen.

SIEM-Systeme verwenden üblicherweise sogenannte Use Cases als Grundlage zur Erkennung von Ereignissen. Bei einem Use Case handelt es sich einfach gesagt um eine permanente Suchabfrage, die erkennt, ob und wann ein zuvor definiertes Ereignis eingetreten ist. Im Rahmen von Cybersecurity werden dabei zwei Arten von Use Cases unterschieden:

1. Compliance-getriebene Use Cases.

Unter Compliance-getriebenen Use Cases sind Basis-Use-Cases zu verstehen, die Verstöße gegen Compliance-Richtlinien erkennen oder Auffälligkeiten in Systemprotokollierungen beziehungsweise Logdaten feststellen, die eventuell auf Security Incidents hindeuten. Diese Use Cases stellen eine Basisüberwachung sicher, eignen sich jedoch nicht zur vollständigen Erkennung möglicher Cybergefahren. Zur Einrichtung dieser Use Cases sind normalerweise Standard-Logquellen (etwa Active Directory-, Firewall-, VPN-, Proxy-Logs) ausreichend.

Professionelle »SIEM as a Service«-Anbieter verfügen meistens über Use-Case-Kataloge, aus denen der Kunde die für seine Anforderungen geeigneten Use Cases auswählen kann. In der Regel basieren die Use Cases auf »Best Practices« der jeweiligen Anbieter. Hierunter fallen unter anderem fehlgeschlagene Logins, Logins zu unüblichen Zeiten, gleichzeitige Logins desselben Benutzers von unterschiedlichen Standorten, Anlage oder Veränderung von privilegierten Konten sowie Deaktivierung von Protokollierungen.

Zusätzlich lassen sich kundenspezifische Use Cases abbilden, um beispielsweise das Eintreten von Risiken zu erkennen, die im Risikokatalog des Kunden festgehalten sind oder zuvor mit einer Schutzbedarfsanalyse ermittelt wurden.

2. Cybersecurity-getriebene Use Cases.

Bei Cybersecurity-getriebenen Use Cases liegt der Fokus auf der Erkennung von Cybergefahren beziehungsweise Cyberangriffen. Hier wird versucht, die typischen Angreifer-Techniken in den unterschiedlichen Phasen eines Cyberangriffs über die Auswertung der entsprechenden Logdaten zu erkennen.

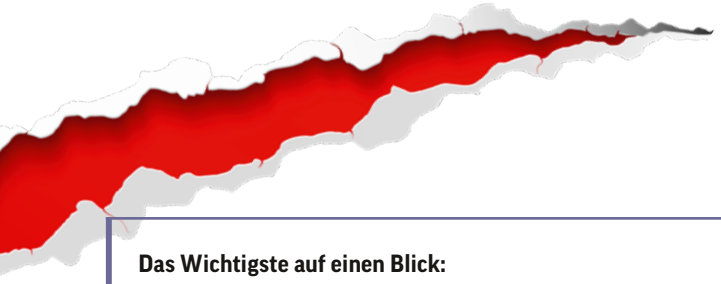
Cybersecurity-Use-Cases sind erheblich komplexer als Basis-Use-Cases und erfordern bei der Formulierung ein sehr profundes Verständnis der Angreifer-Techniken und -Vorgehensweisen sowie Erfahrung bei der individuellen Anpassung an die Kundenumgebung. Zudem sind erweiterte Logquellen wie Sysmon- oder Powershell-Logs erforderlich. Auch für diesen Typ von Use Case verfügen Managed SIEM-Anbieter üblicherweise über einen Use-Case-Katalog, der sich zum Beispiel am MITRE-ATT&CK-Modell orientiert. Diese für unterschiedliche IT-Umgebungen verfügbaren Matrizen beschreiben die wichtigsten tatsächlich genutzten Angreifer-Techniken und -Vorgehensweisen und lassen sich somit als Bewertungskriterium für die Vollständigkeit der Erkennungsmechanismen heranziehen.

Vor- und Nachteile des Use-Case-Ansatzes. Der Vorteil des Use-Case-Ansatzes besteht darin, dass es möglich ist, sehr schnell und einfach aus der großen Anzahl täglicher Events poten-

zielle sicherheitsrelevante Vorfälle herauszufiltern. Dieser Ansatz hat jedoch Nachteile bei der Erkennung von neu auftretenden, weiterentwickelten Cyberangriffen wie APTs oder Zero-Day-Attacken, für die zum Zeitpunkt des Auftretens noch kein Use Case formuliert werden konnte. Außerdem besteht die Gefahr, dass ein nur leicht verändertes Angreiferverhalten nicht erkannt wird, bis eine entsprechende Anpassung erfolgt. Dieses Fine Tuning des SIEM-Systems kann bereits in der Implementierungsphase einen erheblichen Zeitaufwand in Anspruch nehmen und verursacht darüber hinaus im laufenden Betrieb nennenswerten Aufwand und folglich Kosten.

KI-basierte Ansätze zur Anomalieerkennung. Um dem Anspruch einer möglichst vollständigen Erkennung von Cybergefahren gerecht zu werden, ist es ratsam, neben dem beschriebenen SIEM-Ansatz nach heutigem Stand der Technik auch KI-basierte Ansätze zur Anomalieerkennung ergänzend zu berücksichtigen. Diese Lösungen basieren auf Untersuchungen des Netzwerkdatenverkehrs oder des Benutzerverhaltes, nicht auf der Auswertung von Logdaten. Im Rahmen dieser verhaltensbasierten Analysen wird das übliche Kommunikationsverhalten kontinuierlich ermittelt und daraus eine entsprechende Kommunikationsübersicht erstellt (Base Lining). Erfolgt nun eine vom Normalzustand abweichende Kommunikation, kann es sich um ein Indiz dafür handeln, dass schädliches Verhalten vorliegt, das umgehend korreliert und eingehender untersucht wird.

Darüber hinaus werden aber auch Dateien und Verknüpfungen daraufhin überprüft, welches Verhalten sie während der Ausführung oder des Öffnens zeigen, welche Kommandos abgesetzt werden, wie die Interaktion mit dem Betriebssystem aussieht und welche Dateizugriffe erfolgen. Diese Verhaltensweisen lassen sich mit bekannten Informationen zu Malware-Bestandteilen, maliziösen IP-Adressen und Domainnamen, sogenannter Threat Intelligence, abgleichen. In Verbindung mit der oben beschriebenen Netzwerk-Anomalie-Erkennung ergeben sich Kommunikations- und



Das Wichtigste auf einen Blick:

- Managed SIEM Services ergänzen präventive Sicherheitsmaßnahmen durch die aktive Erkennung von Cybergefahren.
- Die Kombination verschiedener Erkennungsmechanismen erhöht die Erkennungsraten und reduziert die Gefahr von Fehlalarmen.
- Je hochwertiger die eingesetzte Erkennungsplattform, umso wirtschaftlicher lässt sich der SOC-Betrieb erbringen.

*/ Um dem Anspruch einer möglichst vollständigen Erkennung von Cybergefahren gerecht zu werden, ist es ratsam, neben dem beschriebenen SIEM-Ansatz nach heutigem Stand der Technik auch KI-basierte Ansätze zur Anomalieerkennung ergänzend zu berücksichtigen.

Verhaltensmuster, die bei marktführenden Systemen mit einer sehr geringen Fehlerrate hinsichtlich des Gefahrenpotenzials bewertet werden können. Solche Analysen auch nur ansatzweise mit Logdaten-basierten Use Cases abzubilden, wäre dagegen neben dem erheblichen Implementierungsaufwand auch mit einer wesentlich höheren Fehlerrate verbunden. Hierbei handelt es sich sowohl um sogenannte False Positives (Fehlalarme) als auch um False Negatives (nicht erfolgte Alarme trotz vorliegenden Gefährdungssituationen).

Beide Ansätze, also Use Cases und KI-basierte Technologien, haben gleichermaßen ihre Berechtigung im Einsatz gegen Malware und Cybergefahren und werden von professionellen Managed-SIEM-Anbietern gerne in Kombination eingesetzt. Allerdings ersetzt auch eine solch ausgereifte technische Basis mit sicherer Erkennung von Cybergefahren nicht die anschließende manuelle Bewertung der erkannten Incidents durch ausgebildete Security-Analysten. Sie ist aber eine wesentliche Grundlage für den wirtschaftlichen Betrieb eines Security Operating Centers, da die Qualität erheblichen Einfluss darauf hat, wie viele Events noch manuell überprüft werden müssen und wie hoch die False-Positive-Rate ist.

Managed-SIEM-Anbieter wie Controlware bieten ihre Cyber Defense Services in der Regel als modulare Pakete an. Der Kunde hat somit die Möglichkeit, die gewünschten Erkennungsmodule mit den entsprechenden Analyseleistungen aus dem Service-Katalog auszuwählen und nach individuellem Bedarf zu kombinieren. Installation, Konfiguration und Betrieb der SIEM-Plattform und des Security Operating Centers übernimmt der Service Provider. Ein weiterer Vorteil besteht darin, dass der Service Provider – im Gegensatz zum Eigenbetrieb – zusätzlich auf Erkenntnisse aus anderen Kundenumgebungen zurückgreifen kann. Somit ist er in der Lage, erstens schneller auf Incidents zu reagieren und zweitens Maßnahmen vorzuschlagen, die sich in anderen Security-Vorfällen als sinnvoll erwiesen haben, um den Eintritt eines Schadens bereits präventiv zu verhindern.

Christian Bohr, Head of Managed Services, Controlware GmbH

www.controlware.de