Der Weg zu einer bedarfsgerechten SIEM Use-Case-Entwicklung

Worauf es in einem Cyber Defense Center ankommt

Sicherheitsvorfälle können in der Komplexität moderner IT-Infrastrukturen oft nur sehr aufwendig analysiert werden. Eine große Hilfe dabei sind Security-Information-and-Event-Management-(SIEM-)Tools. Die Wirksamkeit eines SIEM-Tools hängt von der implementierten Korrelationslogik ab. Zur Konfiguration dieser Logik helfen Use Cases, wobei so ein Anwendungsfall jeweils ein zu überwachendes Bedrohungsszenario beschreibt.

Ein Use Case Framework bündelt alle denkbaren Sicherheitsszenarien. Es ist eine vom Cyber-Defense-Center-(CDC-)Team verwendete Methode zur Ermittlung und Organisation technischer und organisatorischer Anforderungen. Ziel ist das Monitoring dieser Szenarien. Bestimmte Bedrohungen können so leichter erkannt und Gegenmaßnahmen frühzeitig eingeleitet werden. Das Framework hilft dabei, die richtigen Sicherheitsszenarien zu entwickeln und Antworten auf folgende Fragen zu liefern:

- Was ist passiert?
- Welche Systeme sind betroffen?
- Wie hoch ist das Risiko?
- Welcher Schaden ist entstanden beziehungsweise kann noch entstehen?
- Wie muss reagiert werden?

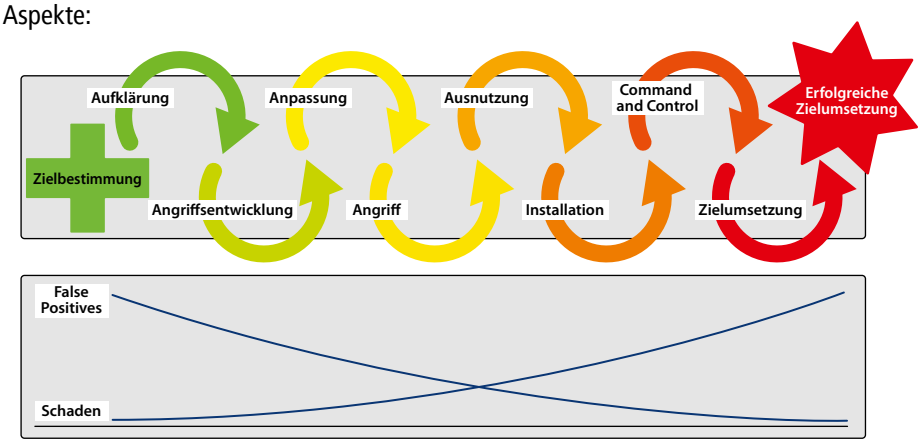
Entwicklung der Use Cases

Es empfiehlt sich die Umsetzung eines Use Case Frameworks auf Basis des Unternehmens-ISMS. Dabei geht es um die praxisgerechte Erfassung der jeweiligen Cyber Kill Chain mithilfe der Entwicklungsmethode Top-Down-Bottom-Up-Middle-Out (TDBUMO).

Aus dem Information Security Management System (ISMS) des Unternehmens lassen sich generelle Bedrohungen bezüglich der Geschäftsprozessen ableiten. Diese werden unter Zuhilfenahme der Cyber Kill Chain in unterschiedliche Bedrohungsszenarien aufgeteilt, welche durch die eingesetzte SIEM-Lösung grundsätzlich verarbeitet werden können. Um Ganzheitlichkeit zu erreichen, muss nun die vorliegende IT-Umgebung mit einbezogen werden. TDBUMO ist eine weit verbreitete Design-Methode, die dazu dient, generelle Anforderungen konkretisiert umsetzen zu können. Im Kontext von SIEM Use Cases bedeutet das die Erfassung folgender Aspekte:

- Welche Bedrohungen existieren und welche Informationen werden benötigt, um das tatsächliche Auftreten dieser Risiken durch aktives Monitoring zu erkennen? (Top-Down)
- Welche Logs kommen auf welchem Weg in das SIEM und welche Informationen sind in den einzelnen Logs enthalten? (Bottom-Up). Im Ergebnis erhält man konkrete SIEM Use Cases, welche die eigene IT-Umgebung vollständig berücksichtigt (Middle-Out)

Legt man nun die definierten SIEM Use Cases über die Ergebnisse aus der Bottom-



Cyber Kill Chain

Bild: © depositphotos.com/yesman

Up-Phase, erhält man konkrete (spezifische) SIEM-Regeln.

Operationell muss das SIEM Use Case Framework mit den Handlungsanweisungen für die Mitarbeiter, die beim Eintreten von Sicherheitsvorfällen ausgeführt werden müssen (Playbooks) verzahnt werden. Dazu empfiehlt sich die Verwendung eines einheitlichen Vokabulars, zum Beispiel in Form einer Adaption des VERIS-Frameworks (Vocabulary for Event Recording and Incident Sharing). VERIS bietet über ein einheitliches Vokabular hinaus die Möglichkeit, Security Events und Security Incidents strukturiert zu erfassen, zu bearbeiten und zu dokumentieren.

VERIS kennt sieben Security-Incident-Kategorien. Diese Security-Incident-Kategorien lassen sich wiederum dazu nutzen, die Anzahl der zu erstellenden Playbooks auf ein Minimum zu reduzieren. Im Idealfall beginnt die Use-Case-Entwicklung mit einer formellen Beschreibung der Entwicklungsmethodik und beruht auf den Prinzipien, dass SIEM Use Cases

- bedrohungsorientiert,
- die IT-Umgebung ganzheitlich abdecken müssen, und
- durch die SIEM-Lösung zu verarbeiten sein müssen.

Zu diesem Zweck hat sich die Etablierung und Implementierung eines SIEM Use Case Frameworks bewährt, das sich an den zuvor genannten Prinzipien orientiert und zusätzlich sicherstellt, dass

- Use Cases unabhängig von der verwendeten SIEM-Lösung entwickelt werden können,
- die „Übersetzung" des formellen Use Cases in die SIEM-spezifische Korrelationslogik vereinfacht wird („Build once – use many")
- die definierten Use-Cases den Compliance-Anforderungen des Unternehmens entsprechen,
- Use Case flexibel an die jeweilige, aktuelle Bedrohungslage angepasst werden können.

Use Case Framework

Ein Use Case Framework muss mindestens folgende Bedingungen erfüllen:

- Die Regelerstellung für die Korrelierungslogik muss vom SIEM-Tool unabhängig dokumentiert werden können und einen kompletten Use-Case-Lebenszyklus unterstützen.
- Die Use Cases müssen über das SIEM-Regelwerk hinaus auch die Playbooks für die Security-Analysten bereithalten. ■

NORBERT BOOK,
Geschäftsführer bei ConSecur

STEPHAN ILIC,
Senior Berater Cyber Defense bei ConSecur