Use Cases für die Cybersicherheit in Unternehmen

Mit Auswahl und Feintuning das SIEM effizient gestalten

Use Cases sind das essenzielle Herzstück eines jeden Security Information and Event Managements (SIEM). Anhand der Use Cases werden Bedrohungen erkannt und in den Meldungen des SIEM ausgegeben. Doch eine zu hohe Anzahl oder die Auswahl der falschen Use Cases für das jeweilige Unternehmen führen häufig zu Fehlmeldungen und dazu, dass tatsächliche Bedrohungen entweder nicht erkannt werden oder aber in einer Masse aus Alarmmeldungen untergehen. Es gilt deswegen, Use Cases so auszuwählen und auf das jeweilige Unternehmen so anzupassen, dass sie mit einer möglichst geringen Anzahl viele Bedrohungsszenarien mit wenig Aufwand abdecken können. Dabei ist es sinnvoll, sich an den bekannten Angriffsvektoren und damit an einem Framework zu orientieren. Wichtig ist außerdem das Tuning, die Anpassung der Use Cases, an die bestehende IT.

Ein Security Information and Event Management (SIEM) sammelt Meldungen, Ereignisse und Logfiles der Systeme in Unternehmen. Mit diesen Daten werden zu Bedrohungen und Cyberangriffen in Echtzeit Alarme ausgegeben, damit Analysten auf diese schnellstmöglich und angemessen reagieren können. Die Basis hierfür stellen zuvor definierte Use Cases. Das SIEM erkennt damit die relevanten Ereignisse in den großen Datenmengen: Sie beschreiben Szenarien mit verdächtigem Verhalten, z.B. ungewöhnliche Anmeldeaktivitäten, das Hinzufügen neuer User oder eine untypische Verwendung von Ports. Im Hinblick darauf muss das Ziel darin bestehen, die geringstmögliche Anzahl von Use Cases auszuwählen, mit der man gleichzeitig die größtmögliche Abdeckung relevanter Angriffsszenarien erzielt. Das gelingt mit der Orientierung an bekannten Angriffsvektoren, wie sie z.B. das MITRE&ATT&CK Framework vorgibt – Use Cases sollten hieraus die wichtigsten Techniken und Taktiken abbilden und berücksichtigen. Im MITRE&ATT&CK Framework werden aus forensischer Sicht zahlreiche verschiedene Ansätze dargestellt und mit Beispielen versehen. Es stellt damit die optimale Basis zur Ableitung von Use Cases dar; IT-Sicherheitsverantwortliche müssen daher nicht Hunderte Use Cases selber bauen, um alle möglichen Szenarien abzudecken, sondern können die für sie sinnvollsten auswählen. IT-Sicherheitspartner wie SECUINFRA verfügen zudem idealerweise über eine eigene Use Case Library. Entwickelt von ihren Cyber Defense Experten, wird so beim Kunden eine maximale Effektivität von Use Cases bei hoher Effizienz gewährleistet. Der Einsatz von monetären und zeitlichen Ressourcen wird damit so gering wie

möglich gehalten. Bei der Auswahl der Use Cases bietet sich außerdem eine enge Abstimmung mit dem Sicherheits- bzw. IT-Risikomanagement an, um aus der Praxis zu erfahren, welche Bereiche das SIEM des jeweiligen Unternehmens abdecken muss.

Parallel dazu ist es sinnvoll, Betriebssysteme, Server und Clients mit der Benutzer- und Rechteverwaltung zu überwachen. Sie sind die zentralen Punkte im Unternehmen und eignen sich als Ausgangspunkt, da die meisten Cyberangriffe auf User, Clients und Server abzielen. Darüber hinaus müssen Überlegungen angestellt werden, wie IT-Systeme mit Eigenentwicklungen überprüft werden können, so dass auch dort keine sicherheitsrelevanten Anomalien auftreten. Je größer das Unternehmen, desto wahrscheinlicher ist es, dass solche Eigenentwicklungen abseits des Frameworks existieren.

Das Tuning der Use Cases

Die ausgewählten Use Cases müssen dann unter Berücksichtigung der Unternehmensspezifika implementiert und anschließend auf diese abgestimmt werden – sie benötigen Tuning. Dabei werden sie vor allem um False Positives, also um Fehlalarme bereinigt. Im Rahmen dessen werden Regelwerke angepasst, die die Logmeldungen auswerten. Außerdem werden Whitelists zu standardmäßig Alarm-auslösenden Events für den Fall integriert, dass diese Events unkritisch erfolgen. Beispiel: Erfolgt eine Datenauslesung, kann dieses Event bereits einen Alarm auslösen und auf einen Cyberangriff hindeuten. Erfolgt dies jedoch durch einen autorisierten Systembenutzer im Unternehmen, ist der Vorgang unkritisch – und der Alarm wäre ein False Positive. Ein anderes Beispiel hierfür ist der Zugriff auf sensible Daten einer Datenbank, der jedoch nicht durch Angreifer von außerhalb verursacht wird, sondern von Administratoren ausgeht. Wird dann in der Analysephase festgestellt, dass es zu viele False Positives gibt, wird durch die Optimierung das Regelwerk mit White- und Blacklists angepasst.

Auch wenn in der ersten Optimierung so effektiv wie möglich vorgegangen wird, kann nicht sofort eine 100-prozentige Lösung erreicht werden. Es ist mittels Tests zu prüfen, ob im Fall einer Anomalie die Regelung auch zukünftig weiterhin greift. Erfahrungsgemäß nimmt es bis zu drei Monate in Anspruch, bis keine oder nur sehr wenige False Positives verursacht werden. In selteneren Fällen können auch Prozesse, die nur alle paar Monate laufen, Fehlalarme auslösen. Das Feintuning der Use Cases stellt also eine fortlaufende, durchaus aufwändige Aufgabe dar. Denn jeder Use Case muss über die gesamte Laufzeit auf dessen Funktion und False Positives überwacht werden. Der Aufwand lässt sich jedoch durch eine geschickte Vorauswahl minimieren.

Tuning als Daueraufgabe umsetzen

Hinzu kommt: Ein SIEM ist ein lebendes System. Ändert sich etwas in der Infrastruktur, indem z.B. Betriebssysteme der Log-Quellen aktualisiert werden, kann das dazu führen, dass ursprünglich angepasste Regeln nicht mehr optimal greifen. Änderungen in der Systemumgebung können neue False Positives erschaffen, wenn ein altes Regelwerk nicht mehr greift, sich Logmeldungen mit einem Update verändert haben oder das Regelwerk, das die Meldungen prüft, zu viel loggt - oder gar nicht mehr. Das macht ein kontinuierliches Nachjustieren notwendig. Der Kreislauf erstreckt sich damit von Analyse, Befund, Optimierung, Tests, Einspielen und Änderungen der Use Cases erneut zurück zur Analyse, so dass der Prozess fortlaufend neu umgesetzt werden muss.

Das Tuning läuft am effizientesten ab, wenn die Teams des Use Case Tunings und der Analysten zusammenarbeiten und gemeinsam das beste Setup finden. Es braucht daher ein Zusammenspiel aus Implementierung, Auswertung und Rücksprache mit den Fachabteilungen.

Gezieltes Tuning sowie die Optimierung tragen daher maßgeblich zur Wirtschaftlichkeit des Security Monitorings bei, da es die Arbeitsbelastung der Security-Analysten deutlich senkt und entsprechend weniger Personalaufwand notwendig macht. Eine Einstellung, die z.B. 90% False Positives auswirft, erfordert hohe Manpower, da alle Fälle einzeln bewertet werden müssen, um tatsächliche Bedrohungen herauszufiltern - schließlich könnte ein echter Angriff hinter einer Meldung stecken. Das Tuning macht manuellen Aufwand dieser Art jedoch weitgehend obsolet und entlastet Unternehmen von der Notwendigkeit, ein zu hohes Alert-Aufkommen bewältigen zu müssen. Hinzu kommt, dass suboptimal implementierte Regelwerke mehr Ressourcen der Systeme benötigen. Sie sind weniger performant, wodurch die Belastung des SIEM steigt – letztendlich macht es einen deutlichen Unterschied, ob für das SIEM fünf oder 20 Server betrieben werden müssen, wenn die Regelwerke entsprechend hohe Lasten verursachen.

Kommunikation ist das A und O

Von SIEM Use Cases bzw. den abgebildeten Szenarien ist häufig eine Personengruppe besonders betroffen: die Belegschaft des Unternehmens – also der einzelne Mitarbeiter. Auf Personalebene entsteht so häufig das Bedenken, dass anwenderbezogene Use Cases vermeintliche Vehikel zur Mitarbeiterüberwachung darstellen könnten. Zwar sind Betriebsrat oder Personalvertretung bei der Auswahl der Use Cases nicht mit involviert, dennoch ist es sinnvoll zu kommunizieren, dass das SIEM nicht dazu zweckentfremdet wird, Auswertungen über die Leistung von Mitarbeitern zu erstellen oder sie auf Personalleiterebene gewissermaßen zu tracken. Es muss klar sein, dass das SIEM nur sicherheitsrelevante Anomalien aufspürt und nicht meldet, dass ein Mitarbeiter vermeintlich zu langsam arbeitet.

Use Cases mit spezialisierten IT-Sicherheitspartnern implementieren

Die Unterstützung durch externe Partner ist bei der Auswahl von SIEM Use Cases unabdingbar, da der gesamte Vorgang Know-how und Erfahrung verlangt, die in Unternehmen meist nicht vorhanden sind und auch nicht in der Kürze der Zeit aufgebaut werden können. Ist ausreichend Personal vorhanden, kommt es häufig jedoch trotzdem nicht mit der Menge an Aufgaben zurecht, die ein SIEM mit sich bringt – es ist mit dessen Implementierung oder dem Aufbau des SOC (Security Operation Center) mehr als ausgelastet und hat keine Zeit für die Auswahl und Implementierung von Use Cases.

Ein erfahrener IT-Sicherheitspartner kann hingegen effizienter und effektiver arbeiten. Es entfällt somit die langwierige Suche nach in der Regel teurem Personal, zudem kann das Unternehmen auch von einem Wissenstransfer profitieren.

Trotz der großen Erfahrung, die ein externer Partner mitbringt, ist eine Zusammenarbeit mit dem Sicherheits- und IT-Risikomanagements des Unternehmens unerlässlich, da diese das Verständnis für den organisatorischen Kontext der Use Cases haben. Denn klar ist: Der Dienstleister benötigt diese interne Unterstützung, etwa um auf die Logmeldungen, Events und Alarme des SIEM-Systems korrekt reagieren zu können. Deswegen ist es wichtig, früh in die Kommunikation zu gehen. So bieten sich zum Beispiel Kickoff-Termine mit Fachabteilungen an, um alle involvierten Parteien abzuholen, Plan und Ziel darzulegen und Unterstützung einzuholen. Kennen sich die beteiligten Teams und Entscheidungsträger, gestaltet sich die Zusammenarbeit zudem harmonischer und Missverständnisse sowie Probleme können schnell ausgeräumt werden.

Wenig hilfreich ist es dagegen, sofort in den Alarmmodus zu wechseln, wenn erste Hürden auftauchen. Sind zum Beispiel erste Regelwerke verfasst, die Systeme aber nicht angebunden oder die Log- und Event-Erzeugung auf Systemen nicht im benötigten Umfang konfiguriert, ist eine frühzeitige Bewertung nicht sinnvoll. Stattdessen sollte eine professionelle Kommunikation etabliert werden, die alle Beteiligten abholt und Lösungswege aufzeigt.

Fazit

Für ein effizient arbeitendes SIEM ist neben der Auswahl der geeigneten Use Cases vor allem deren Feintuning unabdingbar. Ansonsten führt ein falsches und gehäuftes Alarm-Aufkommen schnell zu einem ineffizient arbeitenden System, das das Unternehmen mehr lähmt als unterstützt. Notwendig dafür sind Know-how und Expertise - bei der Auswahl und Implementierung der Use Cases für das SIEM profitieren Unternehmen daher von der Unterstützung durch externe Partner. Denn oft können sie die Aufgabe weder personell noch inhaltlich eigenständig

stemmen. Zudem stellen Auswahl und Feintuning der Use Cases keine einmalig zu erledigenden Aufgaben dar, denn bereits kleine Änderungen an der IT können Nachjustierungen erforderlich machen. Des Weiteren treten fortwährend neue Bedrohungsszenarien auf, denen ggf. mit Anpassungen an bestehende oder der Entwicklung von neuen Use Cases begegnet werden muss. Mit der einmal erfolgten Wahl passender Szenarien allein ist es also nicht getan, die Use Cases benötigen fortlaufendes Anpassen und Feintuning. Indem das SIEM auf diesem Weg als ein quasi lebendes System begriffen wird, entsteht hier ein Kreislauf der ständigen Optimierung.

Autor: Jan Kilby, Senior Cyber Defense Consultant

SECUINFRA

Weitere Informationen: https://www.secuinfra.com/de/services/siem-consulting/

Pressekontakt: SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Deutschland

Tel. +49 (0) 160 921 633 44

svenja.koch@secuinfra.com