SIEM – Technik allein ist keine Lösung

Daniel Mahrenholz · Ralf Schumann · Alexander Brügmann

rt-solutions.de GmbH
{mahrenholz | schumann | bruegmann}@rt-solutions.de

Zusammenfassung

Verschiedene Statistiken zeigen, dass finanziell motivierte, mit umfangreichen Ressourcen ausgestattete professionelle Angreifer mit immer schnelleren und komplexeren Angriffen eine zunehmende Gefahr für die IT-Systeme und den wirtschaftlichen Erfolg von Unternehmen darstellen. Der Einsatz von Security Information and Event Management (SIEM)-Systemen kann eine sehr effektive Maßnahme sein, um derartige Angriffe zu erkennen und Schäden zu minimieren. Kritiker hingegen sehen SIEM-Systeme als ein weiteres Datengrab, das Ressourcen verbraucht, Kosten verursacht und keinen Nutzen erbringt. Den Nutzen realisieren und die Kritikpunkte vermeiden ist nicht allein durch Technik möglich sondert erfordert die Etablierung verschiedener Prozesse und Bereitstellung von angemessenen Personalressourcen für eine nachhaltige Anpassung und Pflege des SIEM-Systems sowie die zeitnahe Reaktion auf erkannte Sicherheitsvorfälle. Die wesentlichen Prozesse und die Risiken einer unzureichenden Umsetzung werden in diesem Beitrag beschrieben. Aus der praktischen Erfahrung heraus werden Empfehlungen dargestellt, wie die Prozesse unter Berücksichtigung der betrieblichen Realität möglichst gut ausgestaltet werden können.

1 Einleitung

Ein SIEM-System verarbeitet eine Menge von Eingabedaten und liefert eine Menge von Ausgaben. Ob die Eingabedaten für den Anwendungszweck geeignet sind, um die gewünschten Ausgaben zu erhalten und ob diese Ausgaben geeignet genutzt werden, um z.B. Sicherheitsvorfälle zu behandeln, kann ein SIEM-System nicht beeinflussen. Hinzu kommt der Faktor Zeit. Veränderungen in der IT-Landschaft müssen im SIEM-System abgebildet werden, um „blinde Flecken“ in der Sichtbarkeit zu vermeiden. Auf die Meldungen des SIEM-Systems muss umgehend reagiert werden, um Schwachstellen rechtzeitig schließen und den Schaden von Vorfällen minimieren zu können. Dies führt in der Praxis oft zu Interessenskonflikten – einerseits erfordern kurze Reaktionszeiten einen signifikanten Personaleinsatz unabhängig von der konkreten Arbeitslast und andererseits erfordern effektive Maßnahmen Befugnisse über klassische Zuständigkeitsgrenzen hinweg. Hinzu kommt das typische Empfinden, dass SIEM-Systeme einen Störfaktor darstellen, da sie Aufgaben in anderen Abteilungen generieren und somit dort die Arbeitslast steigern. In diesem Beitrag soll dargestellt werden, welchen Beitrag ein SIEM-System beim Umgang mit aktuellen Bedrohungen leisten kann, und welche Prozesse dafür wesentlich sind. Dabei sollen die praktischen Erfahrungen im Vordergrund stehen und Empfehlungen für eine effektive und effiziente Umsetzung der Prozesse auf Basis umfangreicher Lessons Learned dargestellt werden.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 1-12.

2 Aktuelle Bedrohungen und der Faktor Zeit

Unternehmen und Organisationen sind einer Vielzahl von internen und externen Bedrohungen ausgesetzt. Durch die starke Verknüpfung von Systemen, Applikationen und Geschäftsprozessen ergibt sich eine große Angriffsfläche und entsprechend vielfältige Angriffsvektoren [HPCR13, SOTR13, MSIR13]. Auch wenn sich die Angriffe in den letzten Jahren weiterentwickelt haben, so ist die deutlichste Veränderung in der Motivation und den Taktiken der Angreifer auszumachen. Angreifer machen sich zunehmend die Komplexität der Systeme zunutze, indem sie versuchen, über schwächer gesicherte Seitenkanäle (z.B. Partnerunternehmen, kompromittierte Hardware) einzudringen und sich dann zu den eigentlichen Zielen vorzuarbeiten. Zunehmend werden dabei auch Systemgrenzen übersprungen, die früher natürliche Grenzen darstellten – waren früher der PC, das Telefon und die Klimaanlage komplett voneinander getrennt, so befinden sich heutzutage der Laptop, das Smartphone und die komplette Gebäudeautomatisierung oft in einem Netzwerk wieder. Erschwerend kommt hinzu, dass Angreifer zunehmend zielgerichtet und finanziell motiviert agieren. Täter aus dem Bereich der organisierten Kriminalität verfügen über umfangreiche Ressourcen und vor allem eine gut ausgebildete Verwertungskette für Unternehmensinformationen [RAND14]. Hinzu kommen die Angreifer, die durch staatliche Organisationen finanziert werden und meist sehr zielgerichtet ausgewählte Opfer angreifen.

Im Kalenderjahr 2012 wurden 25% aller erfolgreichen Angriffe als zielgerichtet eingestuft, die Mehrheit davon (19% absolut) als staatlich gelenkt [DBIR13]. Die übrigen 75% waren sogenannte opportunistische Angriffe, d.h. Angreifer sind z.B. durch automatische Scanner per Zufall auf eine Schwachstelle gestoßen. Zielgerichtete Angriffe bedeuten insbesondere, dass sich die Angreifer nicht davon abschrecken lassen, dass sie keine Zufallserfolge erzielen. Sie werden über einen potentiell sehr langen Zeitraum versuchen, in die Systeme einzudringen und verlassen sich zudem nicht auf einzelne Schwachstellen, sondern versuchen mehrere parallel auszunutzen, um einen zuverlässigen Zugang zu erhalten. Dabei finden oft sogenannte Zero-Day-Exploits Anwendung, d.h. Angriffe auf bisher unveröffentlichte Schwachstellen. Diese werden zunehmend als Handelsware kommerziell verwertet oder gar individuell entwickelt [IBMX14, RAND14].

2.1 Schritte eines erfolgreichen Angriffs

Abhängig vom Ziel eines Angreifers (z.B. Sabotage, Spionage) müssen verschiedene Schritte für einen erfolgreichen Angriff durchlaufen werden. Für die Spionage sind dies:

1. Zugang verschaffen – Ausnutzen einer Schwachstelle, um Zugriff auf mind. ein System im Unternehmensnetz zu erlangen
2. Zugang sichern – auf dem Zielsystemen festsetzen, um jederzeit ohne Ausnutzung der Schwachstelle wieder auf die Systeme zugreifen zu können (z.B. Hintertüren einrichten)
3. Erkunden und Ausbreiten – Infrastruktur und Informationsbestände erkunden und ggf. in weiteren Systemen festsetzen
4. Sammeln – Zugang zu wertvollen Informationen beschaffen, sammeln und aggregieren
5. Herausbefördern – gesammelte Informationen aus dem Unternehmensnetz übertragen

Die Statistiken in [DBIR13] zeigen, dass ca. 25% aller Angriffe innerhalb von weniger als einer Stunde erfolgreich waren, ca. 85% in weniger als einem Tag. War der Zugang erreicht, erreichten 33% innerhalb einer weiteren Stunde ihr Ziel, d.h. begannen mit dem Datenabzug. Innerhalb

eines Tages stieg diese Rate auf 69% an. 18% der Angriffe begannen dagegen frühestens nach einem Monat – ob gewollt oder nicht, lässt sich aus den Daten nicht ermitteln.

2.2 Lebenszyklus eines Vorfalls aus Sicht des Opfers

Aus Sicht des Opfers dauert der Vorfall bis zu seiner vollständigen Behandlung an. Hier ergeben sich die folgenden Phasen:

1. Kompromittierung – alle Aktivitäten bis zum ersten Eindringen in die Systeme
2. Erkunden, Sammeln und Herausbefördern – alle weiteren Aktivitäten bis die ersten Daten den eigenen Perimeter verlassen
3. Erkennen – Zeit von der Kompromittierung bis zur Erkennung des Vorfalls bzw. einer ausgenutzten Schwachstelle (kann sich mit 1 und 2 überlappen)
4. Behandeln – Zeit vom Erkennen bis zur Eindämmung des Vorfalls (Blockierung der Zugangswege, Beseitigung der Schwachstellen, Stopp des Datenabflusses)

Vergleicht man die Zeitrahmen aus Sicht des Angreifers mit der Sichtweise des Opfers [DBIR13], so zeigt sich, dass innerhalb einer Stunde nach der Kompromittierung nur 1% der Angriffe erkannt wurden und nur 10% innerhalb eines Tages – die meisten zudem durch externe Partner oder Behörden. 66% der Angriffe wurden dagegen erst nach einem Monat oder später erkannt. Nach der Erkennung wurden 22% der Vorfälle innerhalb eines Tages behandelt, innerhalb einer Woche immerhin 63%. Für 22% dauerte es aber länger als einen Monat.

2.3 Lebenszyklus einer Schwachstelle

Eine Schwachstelle durchläuft die folgenden Stadien:

1. Erzeugung – die Schwachstelle entsteht
2. (optional) Erkennung – die Schwachstelle wird erkannt
3. (optional) Exploit verfügbar – ein Angriff auf die Schwachstelle steht bereit
4. Beseitigung – die Schwachstelle wird entfernt

Eine Software-Schwachstelle wird meist durch die Anbieter der Software erkannt und beseitigt. Die Existenz wird dem potentiellen Opfer in vielen Fällen meist gar nicht bewusst. Einige Schwachstelle, wie unsichere Konfigurationen können durch nachfolgende Konfigurationen beseitigt werden, ohne dass sie jemals erkannt worden sind. Professionelle Angreifer forschen zunehmend aktiv selbst nach Schwachstellen. Wird einem Angreifer eine Schwachstelle bekannt, so ist typischerweise auch innerhalb kurzer Zeit ein Exploit verfügbar. Ab diesem Zeitpunkt besteht eine konkrete Gefahr für das Opfer.

Für Schwachstellen lassen sich keine allgemeinen zeitlichen Statistiken angeben, da der Zeitpunkt der Erzeugung nur in Einzelfällen bekannt ist und unerkannte Schwachstellen naturgemäß nicht vermessen werden können. Einige Indikatoren zeigen aber die Größenordnungen. Betrachtet man Software-Schwachstellen und Fehlkonfigurationen, so zeigt sich, dass hier Monate oder Jahre zwischen der Erzeugung und Beseitigung vergehen können. Software-Schwachstellen werden oftmals in aktuellen Versionen der Software gefunden, sind aber auch in älteren Versionen vorhanden, d.h. sie wurden schon vor Jahren erzeugt. Nach der Behebung vergeht weitere Zeit, da die Softwarehersteller Korrekturen oft in periodischen Abständen bereitstellen, deren Anwendung sich durch Test- und Freigabeprozesse sowie fehlende Automatismen weiter

verzögern kann. Konfigurationsfehler fallen oft erst im Rahmen von Audits oder Schwachstellenscans auf, die selten häufiger als einmal im Quartal durchgeführt werden.

2.4 Lebenszyklus von Angriffsspuren

Spuren eines Angriffs können vielfältig sein, hierzu zählen primär Einträge in Protokolldateien, Verbindungsdaten, aber auch laufende Programme eines Systems oder Beobachtungen eines Nutzers hinsichtlich eines ungewöhnlichen Systemverhaltens.

Auch Spuren eines Angriffs durchlaufen verschiedene Stadien:

1. Entstehung – die Spur wird erzeugt
2. (optional) Verfälschung – die Spur wird so verändert, dass sie eine andere Aussage vermittelt
3. Beseitigung – die Spur wird entfernt bzw. verschwindet

Werden diese Spuren nicht zentral erfasst und für einen definierten Zeitraum aufbewahrt, verschwinden sie meist schon nach kurzer Zeit. Menschliche Beobachtungen geraten am schnellsten in Vergessenheit oder werden zumindest sehr schnell verfälscht. Protokolle technischer Geräte werden meist nur solange lokal gespeichert, bis definierte Pufferspeicher erschöpft sind. Erfolgt dabei keine Integritätssicherung, können sie in dieser Phase auch jederzeit verfälscht oder gelöscht werden.

2.5 Konsequenzen und Anforderungen an ein SIEM

Betrachtet man die verschiedenen Abläufe in Kombination, so ergeben sich die folgenden Zeitfenster, in denen unterschiedliche Reaktionen möglich sind:

1. Entstehung einer Schwachstelle bis zur Verfügbarkeit eines Exploits – kann die Schwachstelle in dieser Zeit erkannt werden, so kann sie geschlossen werden, bevor die Möglichkeit zur Ausnutzung besteht. Dies wäre optimal.
2. Verfügbarkeit eines Exploits bis zur Kompromittierung – auch in dieser Zeit können erkannte Schwachstellen geschlossen werden, ohne dass ein Schaden entsteht.
3. Kompromittierung bis zum Herausbefördern der Daten – in dieser Zeit kann ein Angreifer noch erfolgreich aufgehalten werden, bevor er einen wesentlichen Schaden anrichten kann. Es entstehen aber bereits Schäden, die in den einzelnen Schritten anwachsen, da immer mehr Systeme betroffen sind, die bereinigt werden müssen.
4. Herausbefördern der Daten bis zum Beseitigen der Spuren – in dieser Zeit kann der angerichtete Schaden zwar nicht mehr begrenzt werden, es besteht aber noch die realistische Chance, das Vorgehen des Angreifers zu verstehen, um die Schwachstellen schließen und eine Wiederholung vermeiden zu können.

Moderne SIEM-Systeme können in allen Phasen hilfreich sein. Hierfür müssen sie Informationen aus unterschiedlichen Quellen wie z.B. Schwachstellenscans, Netzwerk-Flows, Firewall-Ereignisse und Applikationsprotokolle korrelieren. Da die Angriffe sehr schnell ablaufen können, müssen die Korrelation und die Alarmierung in Echtzeit erfolgen. Sie können sich aber auch über längere Zeiträume hinziehen. SIEM-Systeme müssen deshalb in der Lage sein, Vorgänge mit geringer Intensität über längere Zeiträume verfolgen zu können, d.h. Korrelationen über große Datenmengen ermöglichen.

Die Behandlung von Schwachstellen ist originär Teil des technischen Schwachstellenmanagements – dafür müssen die Schwachstellen dem Betreiber eines Systems aber bereits bekannt sein. Ein SIEM-System hilft dabei, ungewöhnliches Kommunikations- und Systemverhalten zu erkennen, das auf die Anwendung eines Zero-Day-Exploits und somit unbekannte Schwachstellen hinweist. Im weiteren Angriffsverlauf kann das SIEM-System das weitere Ausforschen der Infrastruktur, das Einnisten in weitere Systeme sowie das Sammeln von Informationen erkennen. Zudem kann es dabei auch alle Systemveränderungen protokollieren, was eine spätere Bereinigung signifikant vereinfacht. Wichtig hierfür ist, dass das SIEM-System die Infrastruktur möglichst vollständig überwacht und die Protokolle in Echtzeit übermittelt werden. War der Angriff erfolgreich, so unterstützt ein SIEM-System primär bei der Beweissicherung und ggf. bei der Strafverfolgung, da es die technischen Spuren für eine spätere Analyse sichern und diese durch entsprechende Such- und Analysemethoden unterstützen kann.

2.6 Fallbeispiel: Target-Hack

Im Dezember 2013 wurde der US-Einzelhändler Target Opfer eines zielgerichteten Angriffs, in dessen Folge ca. 40 Millionen Kreditkarten-Datensätze sowie ca. 70 Millionen sonstige Kundendatensätze kopiert wurden. Der Angriff erfolgte mehrstufig – nach einem erfolgreichen Angriff auf einen Dienstleister für die Kühltechnik wurden dessen Zugangsberechtigungen genutzt, um in das Target-Netz einzudringen. Dort arbeiteten sich die Angreifer bis zu den Kassenterminals vor, auf denen eine Malware installiert wurde, die die Kreditkartendaten an der Quelle kopierte und periodisch auf einem Server im Target-Netz sammelte. Von dort wurden die Daten (ca. 11 GB) auf verschiedene externe FTP-Server transferiert. Obwohl das Security-Team über die Schwachstellen in den Kassenterminals, die Existenz eines entsprechenden Exploits und entsprechender Malware sowie nachfolgend sogar über Funde der Malware im eigenen Netz informiert war, erfolgten keine Gegenmaßnahmen. Hier haben zum einen die Prozesse versagt, zum anderen fehlte die Sichtbarkeit für die Dringlichkeit des Problems. In der Menge von Meldungen verschiedener Systeme sowie von externen Warnungen z.B. des US-CERT erhielten die einzelnen Vorgänge nicht die notwendige Priorität. Ein SIEM-System hätte diese Indizien (Existenz der Schwachstelle, externe Warnung vor einem passenden Exploit sowie passender Malware, Fund entsprechender Malware-Samples) korrelieren und vor allem priorisieren können, um sie deutlich aus dem Grundrauschen zu heben. Auch die forensische Untersuchung, die klar den Abfluss der Daten in den vorhandenen Logdateien zeigte, wäre durch ein SIEM-System signifikant vereinfach wurden.

2.7 Fallbeispiel: AP-Twitter-Hack

Ein zeitlich sehr gut dokumentierter Fall eines Angriffs ist die Übernahme mehrerer Twitter-Accounts der Associated Press (AP). Die Angreifer der Syrian Electronic Army (SEA) erlangten im Rahmen einer breit angelegten Kampagne gegen amerikanische Medienunternehmen Zugriff auf die Twitter-Konten der AP und verbreiteten am 23.04.2013 die Falschmeldung „*Breaking: Two Explosions in the White House and Barack Obama is injured*“. Die Meldung wurde innerhalb von wenigen Minuten dementiert, der amerikanische Bösenindex Dow Jones verlor dabei aber kurzfristig rund 1,5% an Wert. Im Detail lief der Angriff zeitlich wie folgt:

[12:12] Phishing-Mail an die Mitarbeiter der AP mit angeblichem Link auf einen Artikel der Washington Post, tatsächlich eine gefälschte Seite im Stil des AP-Intranets mit der Aufforderung zur Eingabe von Nutzername/Passwort („Proxy-Anmeldung“)

[12:29] Mail der IT-Abteilung mit Warnung vor der Phishing-Mail

[19:05] Falsche Twitter-Nachricht

[19:10] Dementi der Twitter-Nachricht

[20:10] Sperrung aller AP-Twitter-Accounts

Die Reaktion der IT-Abteilung kam sehr schnell, allerdings beruhte sie nur darauf, dass man dort ebenfalls die Phishing-Mail erhalten hatte. Es wurde niemandem bewusst, dass a) mehrere Mitarbeiter die verlinkte Seite aufgerufen und ihre Zugangsdaten angegeben hatten und b) die erbeuteten Zugangsdaten gegen die öffentlich bekannten Twitter-Accounts getestet wurden, um Zugang zu erlangen. Ein SIEM-System hätte diese zeitliche Häufung und inhaltliche Übereinstimmung von Phishing-Mails und Webseitenaufrufen erkennen können. Selbst ohne eine Alarmierung hätte die IT-Abteilung die Möglichkeit gehabt zu ermitteln, welche Nutzer den kritischen Link aufgerufen und somit potentiell ihre Zugangsdaten preisgegeben hatten.

3 SIEM-Prozesse

Für den Einsatz, den Betrieb und die Nutzung eines SIEM-Systems sind verschiedene Prozesse relevant. Diese sollen im Folgenden kurz beschrieben und die Anforderungen an die Prozesse sowie die Konsequenzen der Nichteinhaltung dieser Anforderungen diskutiert werden. Die Darstellung fokussiert sich dabei auf die Herausforderungen bei der praktischen Umsetzung und stellt entsprechende Lösungsansätze und Empfehlungen dar.

3.1 SIEM Program Management

Seit jeher gilt in der IT-Sicherheit, dass Sicherheit kein Zustand sondern ein Prozess ist. Dies gilt insbesondere für SIEM-Systeme, die nur durch eine kontinuierliche Anpassung ihre optimale Wirkung entfalten können. Der Einsatz von SIEM-Systemen ohne klar definierte Anwendungsfälle ist nicht sinnvoll und zudem hoch riskant. Die richtigen Eingabedaten müssen in der richtigen Art verarbeitet werden, um die gewünschten Ausgaben zu erhalten. Diese Ausgaben müssen den richtigen Personen zur Verfügung stehen, die daraus geeignete Maßnahmen ableiten und umsetzen. Hinzu kommt, dass ein SIEM-System aus Sicht des Datenschutzes und diverser Mitbestimmungsrechte ein hoch kritisches System darstellt. Eine genaue Planung vor der Implementierung ist somit unerlässlich. Aber keine Planung wird jemals vollständig und auf Dauer gültig sein. Das SIEM Program Management hat deshalb die Aufgabe, den SIEM-Einsatz zu überwachen und zu steuern, um den Nutzwert fortlaufend zu optimieren. Dazu gehört, die generelle Strategie des SIEM-Einsatzes sowie die definierten Anwendungsfälle regelmäßig zu überprüfen und ggf. anzupassen, die Umsetzung der Prozesse zu überwachen und auch den Personaleinsatz und die damit verbundenen Kosten zu steuern.

Risiken:

- Ohne eine klare Definition der Analyseregeln sind die erzeugten Alarme oft nur schwer zu interpretieren und Zweifel an der Zuverlässigkeit einer kritischen Meldung sorgen ggf. für eine verspätete oder inkonsequente Umsetzung von Gegenmaßnahmen
- Ohne angemessene Personalausstattung insbesondere für das Incident Management besteht ein hohes Risiko, dass Sicherheitsvorfälle unbeachtet bleiben.
- Ohne eine genaue Planung und Zweckbindung besteht in hohes Risiko, mit dem SIEM-Einsatz gegen geltende Datenschutzvorschriften zu verstoßen.

- Eine schlechte Auswahl und Planung von Informationsquellen sorgt ggf. für „blinde Flecken“, d.h. kritische Vorgänge werden nur unzureichend überwacht und Sicherheitsvorfälle werden somit übersehen und ein falsches Gefühl von Sicherheit erzeugt.
- Ohne eine kontinuierliche Anpassung an geänderte geschäftliche Anforderungen und gesetzliche Vorgaben verliert das System über die Zeit an Effektivität und kann nachträglich rechtliche Probleme erzeugen.

Herausforderungen der Praxis:

- SIEM-Systeme werden sehr oft noch als technische Sicherheitslösungen verstanden, die wie ein Virenfilter zeitnah nach der Installation einen sichtbaren Effekt bieten. Die gründliche Planung eines SIEM-Systems dagegen erfordert Zeit und Ressourcen.
- SIEM-Systeme werden sehr häufig mit aktiven Sicherheitssystemen wie IPS-Systemen oder Schadcodefiltern gleichgesetzt und intern auch so kommuniziert, was speziell auf Managementebene dazu führt, dass der hohe Personalbedarf nicht nachvollziehbar wird und somit die Personalausstattung unzureichend ausfällt.
- SIEM-Systeme liefern speziell zum Beginn des Einsatzes oft sehr viele False-Positives. Werden diese mangels Personal nicht bearbeitet und durch Tuning nachfolgend vermieden, bleiben tatsächliche Vorfälle oft unerkannt. Zudem wird eine negative Wahrnehmung der SIEM-Fähigkeiten erzeugt, was im Extremfall zu einer Aufgabe des Vorhabens mit Verlust der Investitionskosten führt.

Lösungsansätze und Empfehlungen:

- Im Zuge der Planung eines SIEM-Systems sollten alle relevanten Personen in Workshops vorbereitet werden, um eine realistische Erwartungshaltung zu schaffen. Dabei ist insbesondere das Bewusstsein für den Personalaufwand zu schaffen. Es ist auch kritisch zu hinterfragen, ob wirklich SIEM-Funktionen benötigt werden oder ob die Anforderungen auch durch klassisches Log Management erfüllt werden können. Im Zweifel sollte hiermit gestartet und die SIEM-Funktionen erst später nachgerüstet werden.
- Die Planung sollte von Beginn an alle Datenschutzfragen berücksichtigen und den Datenschutzbeauftragten sowie den Betriebsrat frühzeitig einbinden. In der Planung sind der Einsatzzweck, die erhobenen Daten, die Art der Verarbeitung, Speicherung und Auswertung sowie allgemeine Sicherheitsmaßnahmen wie Zugriffsrechte festzulegen.
- Die Planung des SIEM-Systems sollte ausgehend von den gewünschten Ergebnissen und den zu überwachenden Systembereichen die notwendigen Informationsquellen und Verarbeitungsschritte definieren, um sowohl die Vollständigkeit der Überwachung als auch das Datenschutzziel der Datensparsamkeit zu erreichen. Dabei sind zwingend die Prozesse, Verantwortlichkeiten und Ressourcen festzulegen.
- Um möglichst schnell vorzeigbare Ergebnisse liefern zu können, sollten die geplanten Anwendungsfälle zunächst grob skizziert und dann priorisiert werden. Die Detailplanung sollte dann nur für ausgewählte, am besten nur einen, Anwendungsfälle erfolgen, um zeitnah mit einer Implementierung starten zu können.
- Jährlich ist ein Review vorzusehen, in dem die allgemeine SIEM-Strategie, die definierten Anwendungsfälle, Vorgaben und Anforderungen überprüft werden, um ggf. Anpassungsmaßnahmen zu initiieren. Dabei ist jeweils auch der Personaleinsatz zu überprüfen und geeignet anzupassen.

3.2 Betrieb und Überwachung der SIEM-Plattform

Ein SIEM-System stellt selber ein kritisches System dar, das gepflegt und überwacht werden muss. Praktisch unterscheidet es sich dadurch nicht von anderen Systemen, trotzdem sind besondere Eigenarten, insbesondere bei der Überwachung, zu beachten.

Risiken:

- Administratoren des SIEM-Systems können durch ihre Berechtigungen selektiv Überwachungsmaßnahmen deaktivieren, um so unberechtigte Aktivitäten auf anderen Systemen zu verschleiern.
- Durch die Zentralisierung der Protokollierung kann die Zerstörung des Systems zu sehr weitrechender Zerstörung der Protokollinformationen führen.

Zeitliche Anforderungen:

- Da auch ein SIEM-System ein Angriffsziel darstellen kann, müssen Änderungen oder die Deaktivierung seiner Einstellungen in Echtzeit überwacht werden.

Herausforderungen:

- Die Überwachung eines SIEM-Systems erfolgt am effizientesten auf dem System selber. Jedoch ist dies für Manipulationen der beteiligten Administratoren anfällig.
- Praktisch ist es kaum umsetzbar, ein SIEM-System durch ein zweites SIEM-System mit getrenntem Betriebspersonal überwachen zu lassen.
- Aufgrund der gespeicherten Datenmengen ist es oft sehr schwierig oder kostenintensiv, ein vollständiges Backup durchzuführen.

Lösungsansätze und Empfehlungen:

- Alle Möglichkeiten eines SIEM-Produktes zur Integritätssicherung der gespeicherten Informationen sollten auch dafür genutzt werden, Manipulationen durch die zuständigen Administratoren zu erkennen.
- Audit-Logs und andere wesentliche Protokolle des SIEM-Systems sollten in Echtzeit auf einen externen Speicher geschrieben werden, auf den die SIEM-Administratoren keinen Zugriff besitzen. Das Review dieser Aufzeichnung kann auf dem System selber erfolgen, wenn vorab (z.B. durch Checksummen und Reports) die Übereinstimmung beider Kopien überprüft werden kann.
- Regelmäßig sollte eine externe Auditierung der SIEM-Systems erfolgen.
- Kritische Konfigurationsänderungen sollten nach dem 4-Augen-Prinzip erfolgen. Wird diese Funktion nicht durch die Produkte angeboten (der Normalfall), so können die Änderungen direkt an ein externes Ticket-System gemeldet werden, wo sie nachträglich durch eine zweite Person bestätigt werden müssen.
- Wenn vollständige Backups nicht möglich sind, so sollten zumindest die erzeugten Reports sowie Daten zur Nachverfolgung von Vorfällen extern gespeichert werden.

3.3 Konfiguration von Quellen und Datenerfassung

Damit Informationen der Quellen verarbeitet werden können, müssen die Quellen und die Datenerfassung, -übertragung, und -aufnahme zunächst geeignet konfiguriert werden. Dies ist eine kontinuierliche Aktivität, in die verschiedene Fachgruppen eingebunden werden müssen:

- Administratoren der Quellsysteme zur Einrichtung der Quellen
- Netzwerk- und Firewall-Administratoren zur Freigabe der Verbindung mit dem SIEM
- SIEM-Administratoren zur Einrichtung von Empfang und Verarbeitung der Daten

Risiken:

- Werden neue oder geänderte Systeme nicht geeignet an das SIEM-System angebunden, entstehen „blinde Flecken“, d.h. sicherheitskritische Vorgänge werden ggf. nicht erkannt und Vorgaben zur Protokollierung nicht umgesetzt.

Zeitliche Anforderungen:

- Sobald Systeme aktiv sind, können sie Ziel eines Angriffs werden. Sie müssen also von Beginn an in die Protokollierung eingebunden werden.

Herausforderungen:

- Die Anpassung der Quellen bedeutet Mehrarbeit für die jeweiligen Administratoren, ohne dass dem ein direkter Mehrwert gegenüber steht. Subjektiv wird das SIEM-System dadurch zu einem Störfaktor und provoziert entsprechende Widerstände.

Lösungsansätze und Empfehlungen:

- Zusammen mit der SIEM-Einführung muss das Bewusstsein im Unternehmen geschaffen werden, dass das Thema abteilungsübergreifend ist. Hierfür ist es sehr empfehlenswert, das SIEM-Team eigenständig zu organisieren und nicht z.B. dem Netzwerk-Betrieb zu unterstellen nur weil dort z.B. Firewalls und IPS-Systeme eingeordnet sind.
- Bei der Planung der Anwendungsfälle sollte berücksichtigt werden, ob und wie mit den gesammelten Informationen auch operative Aufgaben (z.B. Troubleshooting über Abteilungsgrenzen hinweg) unterstützt werden können, um einen Mehrwert jenseits der Sicherheitsaspekte liefern zu können.
- Bereits bei der Planung des SIEM-Systems sind der Aufwand auf Seite der Datenlieferanten zu planen und Möglichkeiten für die Automatisierung zu untersuchen. Des Weiteren sollte das SIEM-Team die Fachgruppen durch Bereitstellung von Konfigurationsvorlagen und Personal für die Incident-Analyse unterstützen.
- Durch das Change Management der Quellsysteme ist die Anpassung der Logging-Konfiguration sowie eine Benachrichtigung des SIEM-Teams sicherzustellen.

3.4 SIEM-Tuning und -Customization

Ein SIEM-System muss kontinuierlich angepasst werden. Hierzu zählen vor allem das Regelwerk für die Alarmierung, aber auch das Kontextwissen (z.B. Asset-Datenbank, Risikodefinitionen), das zur Bewertung von Ereignissen und Vorgängen genutzt wird.

Risiken:

- Durch unzureichende Anpassung des Regelwerkes und Pflege der Kontextinformationen werden sicherheitskritische Vorgänge nicht erkannt, es werden viele False-Positves erzeugt bzw. Vorgänge falsch bewertet.
- Fehlerhafte Bewertung von Vorfällen kann zu einer fehlerhaften Eskalation im Incident Management führen, wodurch kritische Vorfälle nicht angemessen behandelt werden.

Zeitliche Anforderungen:

- Werden neue Systeme oder Anwendungen eingeführt, so müssen diese umgehend im Regelwerk bzw. dem Kontextwissen abgebildet werden.

Herausforderungen:

- Für die Bewertung des Normalverhaltens von Servern ist ein detailliertes Asset-Inventar notwendig, das in den meisten Fällen nicht gegeben ist. Zur Bewertung von Vorfällen sind zudem Risikobewertungen von Systemen notwendig.
- Das Tuning von Regelwerken erfordert viel Erfahrung über das Verhalten der Quellsysteme und Anwendungen sowie den Aufbau des Regelwerkes.

Lösungsansätze und Empfehlungen:

- Anwendungsfälle sollten immer einzeln hintereinander umgesetzt werden, ggf. auch für einzelne Teile der Infrastruktur getrennt, und danach Zeit für das Tuning eingeplant werden, um nicht von der Menge der False-Positives überfordert zu werden.
- Liegt kein Asset-Inventar vor, so kann das SIEM-System initial zur Asset-Discovery genutzt werden. Später kann diese Funktion zur Gegenprüfung des Inventars bzw. Erkennung unzulässiger Systeme und Dienste genutzt werden.
- Verfügen die Systeme über keine Risikoeinschätzung, kann ersatzweise eine Basiseinstufung nach Netzwerkzonen (Endanwender, RZ, …), Diensten bzw. der Exponierung bzgl. externer Zugriffe (DMZ, Systeme in öffentlichen Räumen, …) genutzt werden.

3.5 Incident Management

Die Behandlung von Vorfällen ist einer der wichtigsten Prozesses überhaupt. Da das SIEM-System passiv ist, müssen alle Vorfallsmeldungen durch die Mitarbeiter der IT-Sicherheit ausgewertet und in Maßnahmen übertragen, umgesetzt und nachverfolgt werden.

Risiken:

- Werden Vorfallsmeldungen nicht rechtzeitig bearbeitet, so können Schäden weder vermieden noch begrenzt werden.
- Durch den Verlust von Spuren kann der Angriffsweg nicht nachvollzogen und somit die entsprechenden Schwachstellen nicht geschlossen werden.
- Erzeugt das System viele False-Positives, so werden hierdurch unnötig Personalressourcen gebunden und die Bearbeitung tatsächlicher Vorfälle verzögert. Zudem sinkt dadurch schnell die Akzeptanz einer SIEM-Lösung.

Zeitliche Anforderungen:

- Da die Mehrzahl der erfolgreichen Angriffe innerhalb eines Tages bereits zu einem Datenabfluss führt, müssen Reaktionen jederzeit, d.h. im 24x7-Betrieb, und mit möglichst kurzer Verzögerung (< 1h) erfolgen.

Herausforderungen:

- Die Bereitstellung eines spezialisierten SIEM-Teams im 24x7-Betrieb erfordert einen hohen Personaleinsatz, um die Verfügbarkeit sicherstellen zu können, der sich mit dem anfallenden Arbeitsaufwand meist nicht rechtfertigen lässt.

- Die kurzfristige Umsetzung von Gegenmaßnahmen erfolgt nicht, da negative Nebenwirkungen befürchtet werden und keine Mitarbeiter für eine Freigabe oder Anweisung derartiger Maßnahmen zur Verfügung stehen.
- Die Vermeidung von False-Positives erfordert einen hohen Tuning-Aufwand, um dabei nicht gleichzeitig auch wichtige Ereignisse auszublenden.

Lösungsansätze und Empfehlungen:

- Vor der Einführung eines SIEM-Systems sollte unbedingt auch die Einrichtung eines Security Operation Centers (SOC) [EYSO13] geprüft werden, in dem das SIEM-Team mit anderen Mitarbeitern der IT-Security gebündelt wird.
- Zur Verringerung des Personalbedarfs kann die Analyse von Vorfällen zweistufig erfolgen, wenn z.B. bereits ein 24x7-Betriebsteam existiert. Dieses nimmt die Erstannahme vor und analysiert die Vorfallsmeldung nach einem fest vorgegebenen Schema (z.B. Checkliste) mit dem Ziel, den Schweregrad zu bestimmen und nach vorab definierten Regeln zu eskalieren (z.B. Aktivierung eines SIEM-Mitarbeiters in Rufbereitschaft) bzw. die Bearbeitung auf den nächsten Arbeitstag zu verschieben. Dieser Schritt sollte nach Möglichkeit durch das SIEM-System durch entsprechende Einstufungshilfen unterstützt werden. Alternativ kann diese Tätigkeit auch über Managed Services durch einen Dienstleister erbracht werden.
- Parallel kann die Auslastung des SIEM-Teams dadurch verbessert werden, dass die Umsetzung von neuen Anwendungsfällen nicht als Projekt sondern als kontinuierliche Weiterentwicklung erfolgt, um langfristig die Arbeitszeit auszufüllen, die nur für die Sicherstellung der Verfügbarkeit benötigt wird.
- Parallel zur Einführung eines SIEM-Systems sollte der Incident Response Plan angepasst bzw. erstellt werden, in dem die wesentlichen und vor allem ersten Schritte formal dargestellt werden. Allein diese Formalisierung sorgt praktisch zu einer deutlichen Reduktion vorfallbedingter Kosten [PDBS13, GTIR14].
- Für möglichst viele Arten von Vorfällen sollten technische Gegen- oder Notfallmaßnahmen vorab erarbeitet, geprüft und freigegeben werden, um z.B. Systeme im Verdachtsfall ohne Zeitverzug isolieren oder zumindest von externen Netzen abtrennen zu können. So wird Zeit für weitere Analysen gewonnen und einem Angreifer die Möglichkeit zur Exfiltration der Informationen genommen.

4 Fazit und Ausblick

Die Praxis zeigt, dass SIEM-Systeme sehr effektiv darin sein können, Bedrohungen, Angriffe oder erfolgte Kompromittierungen zu erkennen und dabei sehr viele Einzelinformationen zu wenigen, handhabbaren Vorfallsmeldungen zu aggregieren. Der finanzielle Nutzen eines SIEM-Systems ist oft schwer zu bestimmen. Rein statistisch zeigt sich, dass der Einsatz eines SIEM-Systems die direkten und indirekten Kosten durch Angriffe auf die IT-Systeme um ca. 25% reduziert (1,4 Mio € von 5,67 Mio € pro Jahr) [PCCS13]. Da die Statistik nur den Durchschnitt abbildet, ist davon auszugehen, dass Unternehmen mit effektiven Prozessen einen überdurchschnittlichen Nutzwert des SIEM-Systems erzielen.

Langfristig stellt sich auch im SIEM-Bereich die Frage nach der Beherrschung der Komplexität. Mit der Zeit wachsen neben den überwachten Systemen auch die Anforderungen und die tech-

nischen Möglichkeiten. Identitätsinformationen z.B. sind eine wertvolle Datenquelle, langfristig aber nur dann effizient zu nutzen, wenn sie unternehmensweit in einem Identity Management System gepflegt und von dort automatisch auf allen Systeme und dem SIEM konfiguriert werden. Auch andere Systemverwaltungswerkzeuge werden erst durch unternehmensweiten Einsatz und Automatisierung wirklich effizient im SIEM-Kontext. Hinzu kommt die Frage nach der wachsenden Geschwindigkeit der Angriffe. Die Technik wird sich entsprechend weiterentwickeln, aber die entsprechenden Prozesse können nicht endlos beschleunigt werden. Auch hier helfen Integration und Automatisierung. Verschiedene Anbieter verfolgen dabei das Ziel, aus dem SIEM-System heraus verdächtige IP-Geräte durch Firewalls bzw. Anwender über IDM-Systeme automatisch zu isolieren, um mehr Zeit für die Incident-Analyse zu erhalten und akute Gefahren automatisch zu bekämpfen. Dieser Trend wird sich sicher verstärken.

Literatur

[HPCR13] HP Development Company: Cyper Risk Report 2013 (2013). http://info.hpenterprisesecurity.com/register_hpenterprisesecurity_cyber_risk_report_2013

[SOTR13] Sophos: Security Thread Report 2013 (2013). http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

[MSIR13] Microsoft: Security Intelligence Report (Vol. 15) (2013). http://www.microsoft.com/security/sir/default.aspx

[IBMX14] IBM: X-Force Thread Intelligence Quarterly 1Q 2014 (2014). http://www-03.ibm.com/security/xforce

[RAND14] RAND Corporation: Markets for Cybercrime Tools and Stolen Data (2014). http://www.rand.org/pubs/research_reports/RR610.html

[TGSR13] Trustwave: 2013 Glocal Security Report (2013). http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

[DBIR13] Verizon: The 2013 Data Breach Investigations Report (2013). http://www.verizonenterprise.com/DBIR/2013/

[PDBS13] Ponemon Institute: 2013 Cost of Data Breach Study: Global Analysis (2013). http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

[EYSO13] Ernst & Young: Security Operations Centers against cybercrime (2013). http://www.ey.com/Publication/vwLUAssets/EY_Security_Operations_Centers_against_cybercrime/$FILE/EY-SOC-Oct-2013.pdf (2013)

[GTIR14] NTT Innovation Institute: Global Thread Intelligence Report (2014). http://www.solutionary.com/_assets/pdf/research/2014-gtir.pdf

[PCCS13] Ponemon Institute: 2013 Cost of Cyber Crime Study: Germany (2013). http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports