Incident Response im SIEM-Kontext – Ein Erfahrungsbericht

Daniel Mahrenholz · Ralf Schumann

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

Zusammenfassung

Unternehmen und Organisationen aller Größen sind ständig den verschiedensten Angriffen auf IT-Systeme ausgesetzt, die zunehmend zielgerichtet durch professionelle Angreifer mit klaren finanziellen Absichten erfolgen. Die Angriffe erfolgen mit zunehmender Geschwindigkeit, jedoch vergeht zwischen dem ersten Eindringen in das Netzwerk bis zur Exfiltration der wertvollen Informationen Zeit, in der der Angreifer oft eine Vielzahl einzelner Spuren hinterlässt. Security Information and Event Management (SIEM)-Systeme erlauben es, aus diesen Spuren Sicherheitsvorfälle und laufende Angriffe in nahezu Echtzeit zu erkennen. Durch umgehend und konsequent ausgeführte Gegenmaßnahmen lassen sich Schwachstellen schließen, laufende Angriffe stoppen und der resultierende Schaden effektiv begrenzen. Optimal wäre ein 24x7-Betrieb, den die meisten Unternehmen wegen des notwendigen Personaleinsatzes scheuen und eher vollständig auf den Einsatz eines SIEM-Systems und den daraus resultierenden Sicherheitsgewinn verzichten. Durch verschiedene technische und organisatorische Maßnahmen wie die Mitnutzung bestehender 24x7-Betriebsmitarbeiter, Managed Services und Automatisierung ausgewählter Gegenmaßnahmen lässt sich der Personalbedarf jedoch soweit reduzieren, dass die Idealvorstellung annähernd erreicht werden kann. Eine Zusammenstellung von Maßnahmen, die sich in verschieden Projekten in verschiedenen Industriebereichen als wirksam erwiesen haben sowie beispielhafte Darstellungen automatisierter Gegenmaßnahmen mit „Bordmitteln“ stellen den Gegenstand dieses Beitrags dar.

1 Einleitung

Durch den Einsatz von Security Information and Event Management (SIEM)-Systemen können Sicherheitsvorfälle in nahezu Echtzeit erkannt werden. Da ein Angreifer meist das Ziel hat, Zugriff auf wertvolle Informationen zu erhalten, sind nach dem ersten Eindringen in das Unternehmensnetz typischerweise weitere Schritte notwendig, um an die Informationen zu gelangen und diese aus dem Netz zu exfiltrieren. Hierdurch ergibt sich ein Zeitfenster, in dem ein Angriff Spuren hinterlässt, durch die er erkannt und durch zeitnahe und konsequente Umsetzung von Gegenmaßnahmen unterbunden und der resultierende Schaden wirksam begrenzt werden kann. Bedingt durch die Geschwindigkeit der Angriffe und den nahezu durchgängigen Geschäftsbetrieb wäre ein Incident-Response-Team mit entsprechenden Fähigkeiten für die Analyse und Behandlung von Sicherheitsvorfällen im 24x7-Betrieb ideal – eine Anforderung, die selbst große Unternehmen vor signifikante Herausforderungen stellt. Kleine und mittlere Unternehmen können dies in der Regel nicht leisten und verzichten aus diesem Grund eher auf den Einsatz von SIEM-Systemen. Die Mehrzahl der Unternehmen gibt den Mangel an Personal bzw. die Schwierigkeiten der Besetzung offener Stellen als den Hauptgrund für ihre Entscheidung an, Sicherheitsmaßnahmen nicht umzusetzen [PoIn14].

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 345-356.

In diesem Beitrag sollen verschiedene Strategien und Implementierungsansätze betrachtet werden, um durch technische und organisatorische Maßnahmen den Personalbedarf so weit zu senken, dass man der Zielvorstellung einer 24x7-Erkennung und -Behandlung von Sicherheitsvorfällen möglichst nah kommen kann. Die dargestellten Strategien und Techniken kombinieren die Erfahrungen verschiedener SIEM-Projekte aus unterschiedlichen Industriesegmenten. Die grundlegende Kosten-Nutzen-Betrachtung von SIEM-Systemen sowie weitere Prozesse beim SIEM-Betrieb sollen in diesem Beitrag nicht betrachtet werden (siehe hierfür [MaSB14]).

2 Zeitliche Aspekte aktueller Bedrohungen

Unternehmen und Organisationen aller Größen 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 (s. [HPSR15], [SoSe14], [Msft14]). In zunehmendem Maße haben es Unternehmen und andere Organisationen mit zielgerichteten und professionellen Angreifern zu tun, die klare finanzielle Motive für ihre Taten (z.B. Betrug, Erpressung, Spionage, Sabotage) haben. Täter aus dem Bereich der organisierten Kriminalität verfügen inzwischen über umfangreiche fachliche und finanzielle Ressourcen und vor allem eine gut ausgebildete Verwertungskette für Unternehmensinformationen [RAND14]. Hinzu kommen die Angreifer, die durch Staaten oder Organisationen finanziert werden und meist sehr zielgerichtet ausgewählte Opfer angreifen. Eine wesentliche Eigenschaft zielgerichteter Angriffe ist dabei, 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. Zielgerichtete Angriffe 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 (s. [IBMX14], [RAND14, [InIn14]). Diese Art der Angriffe machen inzwischen über 25% aller erfolgreichen Angriffe aus [Veri13]. Dass Angriffe potentiell über eine sehr lange Zeit laufen, bedeutet nicht, dass man sich mit Gegenmaßnahmen ebenfalls Zeit lassen kann. Sobald Angreifer Zugriff auf die Zielsysteme oder –Informationen erlangen können, erfolgt ein Datenabzug meist innerhalb sehr kurzer Zeit. Immerhin 25% aller (statistisch erfassten) Angriffe war innerhalb einer Stunde erfolgreich, d.h. zwischen dem ersten technisch erkennbaren Zugriffsversuch (z.B. Datenpaket über eine Firewall, Zustellung einer Email mit Schadcode) und der Kompromittierung eines internen Systems vergingen weniger als 60 Minuten. Innerhalb eines Tages waren immerhin 85% der Angriffe erfolgreich. 33% der Angriffe erlangten innerhalb der ersten Stunde nach der Kompromittierung bereits auch schon ihr Ziel, d.h. sie begannen mit dem Datenabzug. Nach einem Tag lag die Rate bereits bei 69% (weitere Details siehe [Veri13], [MaSB14]).

Ein zielgerichteter Angriff erfordert typischerweise intensive Vorbereitungen z.B. in Form von Recherchen in sozialen Netzwerken oder der Entwicklung und Testung von Schadcode. Diese Vorbereitungen sind im Normalfall für das Opfer aber nicht erkennbar. Unternehmen haben somit nur die Chance, die öffentliche Verfügbarkeit kritischer Informationen über die Infrastruktur zu vermeiden und proaktiv an der Vermeidung und Behandlung von Schachstellen zu arbeiten. Dieser Aspekt soll in dieser Arbeit aber nicht weiter betrachtet werden.

Verschafft sich ein Angreifer Zugriff auf das Unternehmensnetz, ist es essentiell, den Vorfall schnell und konsequent zu behandeln. Die Statistik zeigt, dass innerhalb der ersten Stunde nach

der Kompromittierung nur 1% der Angriffe erkannt wurden und nur 10% innerhalb eines Tages. 66% der Angriffe wurden dagegen erst nach einem Monat oder später erkannt – die Mehrzahl davon wurden dem Opfer durch externe Stellen mitgeteilt. 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 [Veri13]. Die jeweiligen Angreifer hatten somit ausgiebig Zeit, die gewünschten Informationen zu exfiltrieren, ihre Spuren zu verwischen und sich ggf. tief in den internen Systemen einzunisten, um in Zukunft noch einfacher an kritische Informationen zu gelangen.

3 SIEM-Betrieb und Incident-Response-Prozess

Am Betrieb eines SIEM-Systems sind typischerweise eine oder mehrere Personen in unterschiedlichen Rollen beteiligt. Hierzu zählen der SIEM-Plattformadministrator, der sich um die Wartung und Pflege des technischen SIEM-Systems und seiner Komponenten kümmert, der SIEM-Anwendungsadministrator, der sich um die Konfiguration von Regeln, Reports, Kontextinformationen sowie der Verarbeitungslogik innerhalb des SIEM-Systems kümmert, und die Administratoren der Datenquellen, die dafür sorgen, dass die geeigneten Log-Informationen erhoben und an das SIEM-System übertragen werden.

Im Zuge der Vorfallsbehandlung (Incident Response) kommen weitere Rollen hinzu. Der SIEM-Analyst untersucht Alarmmeldungen des SIEM-Systems und zeigt ausgenutzte Schwachstellen und Angriffswege auf, um diese in Zusammenarbeit mit den Administratoren, Entwicklern oder Architekten der verschiedenen Systeme und Anwendungen beseitigen zu können. Handelt es sich um einen Fehlalarm (False Positive), unterstützt er den SIEM-Anwendungsadministrator bei der Anpassung des Regelwerkes (False Positive Tuning), um eine Wiederholung des Fehlalarms zu vermeiden.

4 Strategien für eine zeitnahe Incident Response

Der Erfolg von Gegenmaßnahmen, d.h. die Begrenzung des Schadens eines erfolgreichen Angriffs, hängt maßgeblich davon ab, einen Angriff frühzeitig zu erkennen, das ganze Ausmaß (z.B. alle bisher kompromittierten Systeme) zu verstehen und die Gegenmaßnahmen schnellstmöglich und vollständig umzusetzen. Hierbei ergeben sich in der Praxis in eine Reihe von Problemen, die im Folgenden näher betrachtet werden sollen.

4.1 Der Prozess unter idealen Bedingungen

Geht man davon aus, dass Personen mit allen notwendigen Fähigkeiten ständig für einen 24x7-Betrieb zur Verfügung stehen, ist dies trotzdem keine Garantie für eine zeitnahe Vorfallsbehandlung, d.h. Analyse von Alarmmeldungen des SIEM-Systems, Entscheidung über Gegenmaßnahmen sowie deren Umsetzung. Folgende Probleme ergeben sich häufig in der Praxis:

- Mehrere Vorfallsmeldungen treten parallel auf, wodurch sich die Bearbeitung verzögert (ein klassisches Queueing-Problem).
- Die Bearbeitung kritischer Probleme wird durch die Analyse von Falschmeldungen verzögert.
- Die Einleitung von Gegenmaßnahmen (insbesondere Änderungen an kritischen Systemen) erfordern eine Freigabe durch Personen, die nicht ständig verfügbar sind.

Das Problem parallel auftretender Alarmmeldungen kann praktisch, auch durch einen massiven Personaleinsatz, nicht gelöst werden, da sich immer Fälle konstruieren lassen, in denen mehr Alarme ausgelöst werden, als Personen zur Bearbeitung verfügbar sind. Dass diese Fälle selten auftreten, macht einen massiven Personaleinsatz zudem extrem ineffizient. In der Praxis muss es deshalb das Ziel sein, wichtige Alarme (hohe Risiken) bevorzugt zu behandeln und für Ausnahmesituationen eine höhere Personalreserve verfügbar zu machen. Die wichtigste Maßnahme zur bevorzugten Behandlung wichtiger Meldungen ist die Priorisierung. Optimal wird bereits durch das SIEM-System eine Priorisierung vorgenommen, z.B. auf Basis der Wichtigkeit betroffener Systeme und Informationen für das Geschäft (klassische Risikobewertung) oder nach der Art der erkannten Bedrohung (z.B. Erkundung oder potentieller Datenabfluss). In vielen Fällen lässt sich diese Priorisierung nicht automatisch erstellen. Hier hilft es, die Vorfallsanalyse in mind. zwei Schritte aufzuteilen. Im ersten Schritt werden streng nach einer Checkliste verschiedene Kriterien überprüft und danach eine Priorisierung vorgenommen. Diese Zweiteilung bietet noch weitere Vorteile. Das Abarbeiten der Checkliste (Erstanalyse) erfordert deutlich geringere Analysefähigkeiten bzw. kann komplett in einer Arbeitsanweisung dokumentiert werden. Die Tätigkeit kann somit ggf. auch durch andere IT-Mitarbeiter durchgeführt werden, wodurch die zeitliche Verfügbarkeit und Arbeitskapazität der Mitarbeiter der Erstanalyse erhöht und damit die Durchlaufzeit reduziert wird. Des Weiteren kann die Erstanalyse so innerhalb fester Zeitschranken (im Bereich von 5-10 Minuten) durchgeführt werden. Bei Bedarf kann dann die bereits laufende, weiterführende Analyse anderer Vorfälle unterbrochen werden, wenn die Priorität des neuen Vorfalls dies erfordert.

Ein SIEM-System arbeitet typischerweise mit eine Reihe von Heuristiken oder Regeln mit Schwellwerten, wodurch Fehlalarme nie ausgeschlossen werden können. Auch hier kann die mehrstufige Vorfallsanalyse Vorteile schaffen. Die Erstanalyse muss deshalb auch darauf ausgelegt sein, Fehlalarme mit hoher Wahrscheinlichkeit zu erkennen. Des Weiteren ist es essentiell, Fehlalarme konsequent nachzuverfolgen, um das Regelwerk anpassen zu können, damit sie in Zukunft möglichst nicht wieder auftreten. Hier ist es sogar von Vorteil, die Nachverfolgung erst mit einigem zeitlichen Abstand durchzuführen, um grundlegende Probleme im Regelwerk (z.B. bei vielen ähnlichen Fehlalarmen) erkennen und beheben zu können.

Wurde ein Sicherheitsvorfall oder ein anderes kritisches Systemverhalten erkannt, so sollte es selbstverständlich sein, unverzüglich mit effektiven Gegenmaßnahmen darauf zu reagieren. Praktisch zeigen sich hier die größten Probleme. Die wichtigsten Gründe hierfür sind:

- Angst vor negativen Auswirkungen auf den Geschäftsbetrieb
- Fehlendes Vertrauen in Aussagekraft des SIEM-Systems / Uneinheitliches Verständnis über die potentiellen Auswirkungen eines Sicherheitsvorfalls
- Fehlende Entscheidungsbefugnisse / lange Entscheidungswege zur Umsetzung von Gegenmaßnahmen

Sehr häufig wird Informationssicherheit als rein technisches Problem der IT betrachtet und die Fachabteilungen nur wenig eingebunden bzw. in diesen hat sie nur eine untergeordnete Priorität. Da die Wahl von Gegenmaßnahmen aber immer auch eine Interessensabwägung zwischen geschäftlichen Aspekten und Sicherheitsaspekten bedeutet, kommen beide Seite sehr leicht zu unterschiedlichen Einschätzungen, mit dem Ergebnis, dass die Fachabteilungen als Eigner der Systeme die Umsetzung von Gegenmaßnahmen verhindern. Oft wird dabei auch das Argument der Verlässlichkeit der SIEM-Meldungen eingebracht, d.h. Fachabteilungen zweifeln oft an, dass eine Vorfallsmeldung überhaupt valide ist. Der IT bleibt in diesen Fällen nur der Weg über

eine entsprechende Eskalation, was oft viel Zeit kostet und innere Widerstände fördert. Erschwerend kommt hinzu, dass insbesondere Gegenmaßnahmen, die kritische Systeme betreffen, einer besonderen Freigabe bedürfen und die entsprechenden Personen nicht 24x7 zur Verfügung stehen. Abhilfe können hier zwei Maßnahmen bieten. Zum ersten müssen die Fachabteilungen bereits bei der Planung eines SIEM-Systems konsequent eingebunden werden, um in der Zusammenarbeit zu klären, welche Informationen zu welchem Zweck protokolliert und wie sie verarbeitet werden sollen, damit die Fachabteilungen den kompletten Weg zwischen den Protokollen ihrer Systeme und den Alarmmeldungen des SIEM-Systems verstehen und den Alarmen vertrauen können. Zudem wird dabei das Bewusstsein der durch das SIEM-System adressierten Risiken und Bedrohungen gestärkt. Zum zweiten sollten in der Planungs- und in der Betriebsphase mögliche Vorfälle und geeignete Gegenmaßnahmen betrachtet werden, um die Nebenwirkungen für die Geschäftsprozesse vorab in Ruhe bewerten zu können. Die bewerteten Notfallmaßnahmen sollten dann als ein Maßnahmenkatalog mit allen Randbedingungen dokumentiert und freigegeben werden. Dadurch wird die Balance zwischen geschäftlichen Aspekten und Sicherheitsaspekte gewahrt, das Bewusstsein für die Risiken gestärkt und vor allem im Ernstfall Zeit eingespart.

4.2 Praktische Umsetzung mit begrenzten Ressourcen

In der Praxis stehen die meisten Unternehmen in zwei Bereichen vor der Herausforderung, mit eingeschränkten Personalressourcen umgehen zu müssen. Zum ersten wird Personal benötigt, um ein SIEM-System 24x7 zu betreiben und Vorfallsmeldungen zu analysieren. Zum zweiten müssen die für die Gegenmaßnahmen notwendigen Personen bzw. Personen mit entsprechenden Fähigkeiten 24x7 zur Verfügung stehen. Im Folgenden sollen für verschiedene Szenarien mögliche Optionen und Strategien betrachtet und die sich daraus ergebenen Einschränkungen diskutiert werden.

4.2.1 Betrieb des SIEM-Systems und Vorfallsanalyse

Steht nicht genügend Personal zur Verfügung, um das Arbeitsvolumen des SIEM-Betriebes abzubilden, so stehen vier Optionen zur Verfügung:

1. Reduzierung des Anwendungsbereiches, d.h. der Menge der überwachten Systeme
2. Anpassung der Reaktionszeiten
3. Auswahl eines Produktes mit geringerem Betriebsaufwand
4. Nutzung von SIEM als Managed Service

Die Reduktion des Anwendungsbereiches macht nur dann Sinn, wenn die wesentlichen Risiken auch weiterhin durch das SIEM-System abgedeckt werden. Oft macht es dagegen viel mehr Sinn, die angestrebten Reaktionszeiten zu hinterfragen und entsprechend anzupassen. Hier sollte primär betrachtet werden, ob jederzeit, d.h. auch nachts, am Wochenende oder an Feiertagen, gleichermaßen reagiert werden soll. Eine Möglichkeit wäre, in der Kernarbeitszeit (z.B. 8x5) auf alle Vorfälle zu reagieren, in den Randzeiten (z.B. werktäglich 06:00-22:00) zumindest auf signifikante und in allen anderen Zeiten nur auf hochkritische Vorfälle. Dies sollte nach klaren Risikoaspekten für den Einzelfall diskutiert und im Rahmen des Einsatzkonzeptes vorab definiert werden.

Die verschiedenen am Markt verfügbaren Produkte können sich je nach Anwendungsgebiet in ihrem Betriebsaufwand signifikant unterscheiden. Dies sollte bei der Auswahlentscheidung im-

mer berücksichtig werden und am besten Erfahrungen anderer vergleichbarer Anwender eingeholt werden. Die Nutzung von Managed Services für Teile oder den kompletten Betrieb ist in vielen Fällen die bevorzugte Variante, da man hierbei von der Erfahrung der Anbieter und von Skaleneffekten profitieren kann. Im Gegenzug ist aber eine besondere Sorgfalt bei der Ausgestaltung der verschiedenen Prozesse sowie beim Thema Datenschutz dringend notwendig.

Steht genug Personal für das Arbeitsvolumen des SIEM-Betriebes aber nicht für einen 24x7-Betrieb zur Verfügung, können die folgenden Optionen verfolgt werden:

1. Rufbereitschaft in Kombination mit einer Erstanalyse durch eine bestehende 24x7-Betriebsgruppe (nicht Security)
2. Rufbereitschaft in Kombination mit einer automatisierten Priorisierung
3. Rufbereitschaft in Kombination mit SIEM als Managed Service

Wird die Vorfallsanalyse mehrstufig gestaltet, so kann die erste Stufe auch durch IT-Mitarbeiter ohne besondere Security-Kenntnisse oder externe Mitarbeiter ohne besondere Kenntnisse über interne Systeme durchgeführt werden. Bis zu einem gewissen Grad ist auch eine Automatisierung der Erstanalyse möglich. Grundvoraussetzung in allen Fällen ist, dass die Schritte der Erstanalyse sowie die Kriterien für die Bewertung und Eskalation von Vorfallsmeldungen formalisiert vorliegen. Eine mehrstufige Vorfallsanalyse lässt sich auch sehr gut mit abgestuften Reaktionszeiten kombinieren, um eine möglichst gute Risikoabdeckung zu erzielen.

In Einzelfällen ergibt sich die Situation, dass hinreichend Personal für den 24x7-Betrieb bereitgestellt werden könnte, dies sich aber nicht durch das Arbeitsvolumen des SIEM-Betriebes rechtfertigen lässt. Hier können folgende Strategien verfolgt werden:

1. Verlagerung des initialen Implementierungsaufwandes in den Betrieb
2. Übertragung anderer 24x7-Betriebstätigkeiten

Es ist generell empfehlenswert, SIEM-Systeme schrittweise einzuführen, um die Komplexität reduzieren und interne Prozesse entsprechend angleichen zu können. So kann auch die Erfahrung der Mitarbeiter mit dem System wachsen. Ein Einführungsprojekt kann dabei auch in viele kleinere Umsetzungsschritte aufgegliedert werden, die dann mit nachrangiger Priorität durch die Betriebsmitarbeiter umgesetzt werden, um diese besser auszulasten. Hiermit werden Projektkosten in Betriebskosten verlagert, die Gesamtkosten bleiben gleich. Oft können sie sogar geringer ausfallen, wenn die Erfahrungen der ersten Ausbaustufen und ggf. erkannte Planungsfehler in den weiteren Ausbaustufen berücksichtigt werden. Im Gegenzug darf die Qualitätskontrolle nicht vernachlässigt werden, da sich bei einer nebenläufigen Umsetzung von Erweiterung leichter Flüchtigkeitsfehler einschleichen können, wenn die Arbeiten zur Betriebsaufgaben unterbrochen werden. Wenn ein Betriebsteam einmal für den 24x7-Betrieb bereitsteht, dann kann dessen Auslastung auch durch die Übertragung anderer Betriebsaufgaben optimiert werden. Hier bieten sich insbesondere die Überwachung von Systemen und Anwendungen an, was eine starke Gemeinsamkeit mit dem Security-Monitoring aufweist.

4.2.2 Incident Response / Umsetzung von Gegenmaßnahmen

Für die vollständige Umsetzung von Gegenmaßnahmen werden je nach Komplexität der IT-Landschaft viele Personen mit sehr unterschiedlichen Fähigkeiten benötigt. Deshalb ist es in den meisten Fällen unrealistisch, diese im 24x7-Betrieb vorzuhalten. Da im Ernstfall die Eindämmung eines Vorfalls bzw. die Begrenzung des Schadens die höchste Priorität hat, sind nicht alle Fähigkeiten gleich wichtig. Je nachdem, wie weit ein Angriff fortgeschritten ist, besteht der

Fokus darin, den Angreifer vom Zugriff auf kompromittierte Systeme abzuschneiden, eine weitere Ausbreitung bzw. den Abfluss von Informationen zu verhindern. Alle Aktivitäten, um Systeme zu bereinigen, Schwachstellen zu schließen und ggf. neue Sicherheitsmaßnahmen umzusetzen, haben eine nachrangige Bedeutung.

Die wichtigste Strategie zur zeitnahen Umsetzung von Gegenmaßnahmen ist die Automatisierung. Steht kein Firewall-Administrator zur Verfügung, um bei Bedarf Regeln anzupassen, um einen Angreifer oder die externe Erreichbarkeit eines kompromittierten Systems zu blockieren, so kann dies bei entsprechender Vorbereitung auch automatisiert erfolgen. Hierbei wird das Expertenwissen des Administrators, d.h. wie das Regelwerk anzupassen ist, als Programmcode bereitgestellt. Das SIEM-Team mit dem Wissen über die Angreifer könnte dann bei Bedarf die Gegenmaßnahme selber einleiten. Nach dem Grad der Automatisierung der Vorfallsanalyse können die Maßnahmen ggf. auch durch das SIEM-System selber ausgelöst werden. Praktisch ist hierfür aber eine Reihe von Vorbedingungen zu erfüllen:

1. Die Maßnahmen müssen vorab geplant und unter Berücksichtigung des verbundenen Risikos freigegeben werden.
2. Die Automatismen zur Umsetzung der Maßnahmen müssen regelmäßig gepflegt und getestet werden. Sie müssen zudem gegen missbräuchliche Nutzung gesichert werden.
3. Alle durch die Automatismen vorgenommenen Änderungen müssen nachvollziehbar sein, um sie bei Bedarf zurücknehmen zu können.

Die Angst vor negativen Auswirkungen einer Gegenmaßnahme auf den Geschäftsbetrieb ist oft ein wesentlicher Hinderungsgrund für deren zeitnahe und konsequente Umsetzung. Dies gilt insbesondere für Automatismen, weshalb eine gründliche Vorabplanung unter Einbeziehung der Fachabteilungen und Systemeigner unerlässlich ist. Die technische Umsetzung der Automatismen ist bei wesentlichen Änderungen der gesteuerten Systeme zu überprüfen und ggf. anzupassen, um die korrekte Funktion sicherstellen zu können. Bei der Umsetzung ist auch darauf zu achten, dass die Veränderungen dokumentiert werden, so dass sie bei Bedarf rückgängig gemacht werden können. Wurde z.B. eine Firewall-Regel zum Blockieren einer Angreifer-IP-Adresse erzeugt, muss diese dokumentiert bzw. geeignet markiert werden, um die spätere Entfernung zu vereinfachen. Es ist bei der Umsetzung der Automatismen auch streng darauf zu achten, dass die entsprechenden Programme nur durch berechtigte Nutzer oder Systeme gestartet werden können, da sonst ein derartiges Programm bzw. die im Zielsystem dafür eingerichtete Schnittstelle für einen Denial-of-Service-Angriff genutzt werden kann und dann mehr Schaden als Nutzen anrichtet.

4.3 Automatisierung von Gegenmaßnahmen in der Praxis

Wichtigstes Ziel der automatisierten Gegenmaßnahmen ist es, Angreifern die Kontrolle über kompromittierte Systeme zu nehmen, eine weitere Ausbreitung und den Datenabfluss zu verhindern. Hierfür bieten sich verschiedene technische Maßnahmen an. Über Firewall-/IPS-Systeme kann die Kommunikation von kompromittierten Systemen begrenzt werden. Über die Berechtigungsvergabe können Nutzer in ihren Zugriffsmöglichkeiten und Rechten beschnitten werden, hierzu zählt auch die Möglichkeit für Fernzugriffe. Einzelne Systeme können ggf. über die Konfiguration von Switches oder über eingesetzte NAC (Network Access Control)-Systeme physisch isoliert werden.

Die Vorzüge einer Automatisierung von Gegenmaßnahmen haben auch bereits die Hersteller verschiedener SIEM-Systeme erkannt und versuchen dies durch eine Integration von SIEM-,

IPS- und IAM-Systemen zu erreichen. Die Kombination mit einem IPS (Intrusion Prevention System) stellt für viele Unternehmen eine realistische Option dar, wogegen die Kombination mit einem IAM (Identity and Access Management)-System eher theoretischer Natur ist, da IAM-Systeme kaum verbreitet sind und die Einführung typischerweise selber ein sehr umfangreiches Projekt darstellt, somit alleine für diesen Anwendungsfall unwirtschaftlich ist.

Unternehmen und Organisationen sollten sich nicht von der Komplexität und der Funktionsvielfalt kommerzieller Lösungen abschrecken lassen. Eine Automatisierung von Gegenmaßnahmen kann auch mit vergleichsweise geringem Entwicklungsaufwand selber realisiert werden. Hierbei sollte der Fokus darauf liegen, wie sich zeitkritische, manuelle Tätigkeiten, die man ohnehin als Reaktion auf einen Vorfall durchführen würde, automatisieren lassen. Das Vorgehen soll im Folgenden bespielhaft dargestellt und die Umsetzung beschrieben werden. Eine gute Basis für die Überlegung stellt die kritische Nachbetrachtung tatsächlicher Vorfälle dar. Dabei sollte geklärt werden, wie der Angriff, die Kompromittierung, der Datenabzug sowie die Exfiltration erfolgten. Danach sollte geprüft werden, wie man die jeweiligen Aktivitäten erkennen und ggf. hätte unterbinden können. Auch die eigenen Reaktionen nach der Erkennung des Vorfalls sollten kritisch betrachtet werden, um zu klären, was sinnvoll bzw. hilfreich war, wo und weshalb die meiste Zeit verbraucht wurde und ob es technische oder organisatorische Hemmnisse gab.

5 Implementierung ausgewählter Gegenmaßnahmen

Zur Demonstration des Vorgehens wurden verschiedene automatisierte Gegenmaßnahmen in einer Produktivumgebung umgesetzt. Dabei wurde darauf geachtet, dass die Maßnahmen so implementiert werden, dass die Administratoren der dabei aktiven Systeme die Hoheit über die Änderungen besitzen, d.h. sie sorgen für die Durchführung der Maßnahmen, das SIEM-System meldet nur verdächtige Systeme und Nutzer. Die Umsetzung ist darauf ausgelegt, verdächtige Systeme und Nutzer solange in ihren Möglichkeiten zu beschränken, ihnen insbesondere die Möglichkeit zur Exfiltration von Daten oder zum Verbreiten im internen Netz zu nehmen, bis der Vorfall durch einen Mitarbeiter untersucht werden kann, der die Beschränkungen dann wieder aufheben kann. Die Implementierungsumgebung ist in Abbildung 1 schematisch dargestellt.

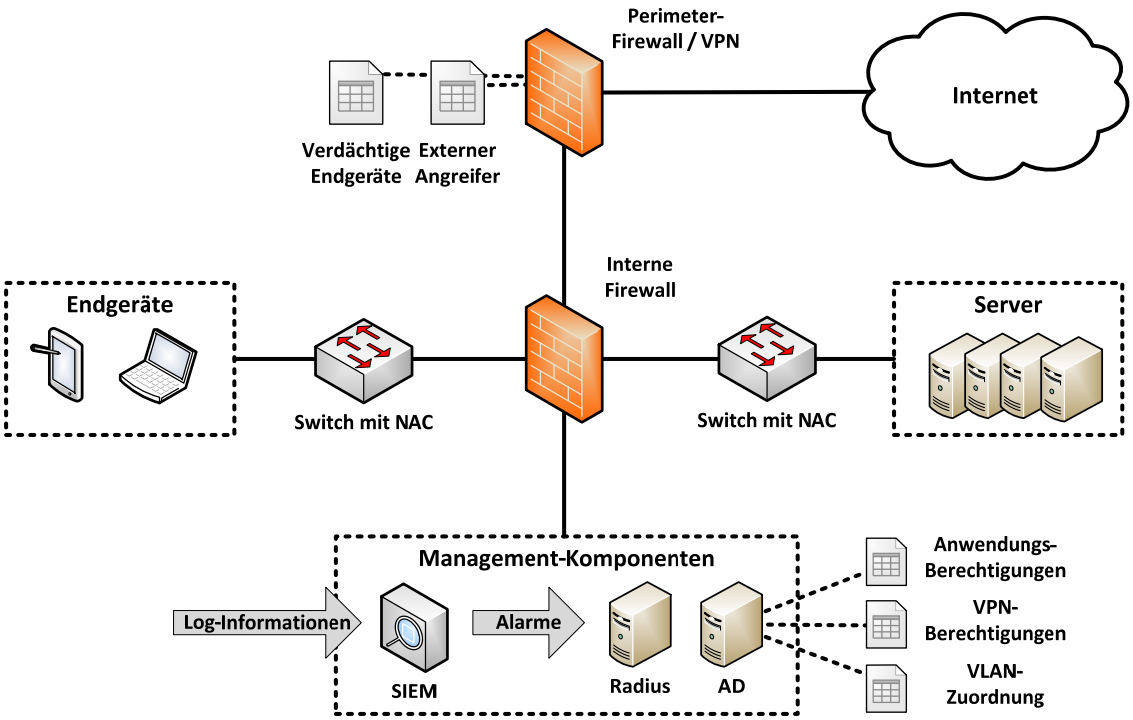

Abb. 1: Schema der Beispielumgebung

Als Komponenten werden Next-Generation-Firewalls (FortiGate) mit den üblichen Funktionen wie Schadcode-, Web-, Reputations- und GeoIP-Filter und SSL-Inspection sowohl am Perimeter als auch intern verwendet. Dazu Netzwerk-Switches mit sFlow-Monitoring und Network Access Control (NAC), ein Microsoft Active-Directory-Server mit Radius-Funktionalität (NPS, Network Policy Server) und als SIEM-System ein kommerzielles Produkt (IBM/QRadar) sowie eine Lösung auf Basis von Open-Source-Komponenten (ElasticSearch, Logstash, nxlog).

5.1 Sperren / Beschränken von auffälligen Nutzern

Verhält sich ein Nutzer auffällig bzw. werden unter den einem Nutzer zugeordneten Nutzerkennungen verdächtige Aktivitäten vorgenommen, so ist es eine gängige Reaktion, die Rechte des Nutzers einzuschränken bzw. den Nutzer komplett für die Anmeldungen an Systemen zu sperren. Dies ist eine Erweiterung des heute schon weit verbreiteten Systemverhaltens, Nutzer nach mehreren falschen Anmeldungen zu sperren. Ein SIEM-System ist darüber hinaus eine Vielzahl weiterer Auffälligkeiten zu erkennen. Hierzu zählen z.B.:

- Mehrere fehlgeschlagene Anmeldungen über verschiedene Systeme hinweg (möglicherweise systematisches Ausprobieren bekannter Zugangsinformationen)
- Mehrere erfolgreiche Anmeldungen an unterschiedlichen Systemen in kurzer Zeit (möglicherweise Ausnutzen bekannter Zugangsinformationen)
- Erfolgreiche Anmeldung nach mehrfach falscher Anmeldung
- Parallele Anmeldung an verschiedenen Systemen via VPN und lokal
- Parallele Anmeldung an verschiedenen Systemen von verschiedenen Quellsystemen (möglichweise geteilte Nutzung einer Zugangskennung)
- Anmeldung zu ungewöhnlichen Tageszeiten / während des Urlaubs

Als Datenquellen werden alle Server und Netzwerkgeräte genutzt. Diese protokollieren an das SIEM alle erfolgreichen An- und Abmeldungen sowie alle erfolglosen Anmeldeversuche. Wird ein Fehlverhalten erkannt, werden die Nutzerrechte wie folgt beschränkt:

- Alle privilegierten Rechte werden entzogen
- Der Zugriff per VPN wird gesperrt
- Alle Intranet-Dienste mit Ausnahme von Email werden gesperrt

Der Nutzer hat danach effektiv noch die Möglichkeit, sich an einem Arbeitsplatzrechner anzumelden und eine E-Mail zu versenden. Hierdurch bleibt die Möglichkeit bestehen, eine fehlerhafte Sperrung an den Support / HelpDesk zu berichten. Der Zugriff auf interne Daten und Dienste, insbesondere mit privilegierten Rechten wird aber verhindert.

Technisch wurde die Automatisierung über PowerShell-Skripte realisiert. Diese sind auf dem Domain Controller gespeichert und werden durch das SIEM ausgelöst, das die Nutzerkennung als Parameter übermittelt, d.h. alle Aktivitäten werden im Skript durch den Domänenadministrator implementiert und sind extern nicht veränderbar. Die Möglichkeit zum Aufruf ist auf das SIEM-System beschränkt. Parallel wird eine E-Mail an das Ticket-System gesendet, in dem die Vorfallsbehandlung nachverfolgt wird. Das Skript führt folgende Aktionen aus:

- Backup der aktuell zugewiesenen Berechtigungen (zum Zwecke der Wiederherstellung durch einen Administrator)
- Entfernen aller Berechtigungen (Zugehörigkeit zu AD-Gruppen)
- Setzen vordefinierter Berechtigungen

Da durch den Entzug der Zugehörigkeit zu AD-Gruppen werden automatisch der Zugang zu internen Systemen und Diensten sowie der VPN-Zugang gesperrt. Die Sperrung bleibt bestehen, bis der Vorfall untersucht werden konnte und die Nutzer manuell freigegeben wird.

5.2 Isolation von auffälligen / kompromittierten Endgeräten

Die Isolation auffälliger Endgeräte erfolgt sehr ähnlich. Wird durch das SIEM erkannt, dass sich ein Endgerät auffällig verhält oder Anzeichen einer Kompromittierung zeigt, so erzeugt das SIEM-System einen Alarm, der die Ausführung eines vorab hinterlegten Skriptes startet. Zeichen für eine mögliche Kompromittierung bzw. auffälliges Verhalten sind z.B.:

- Ein Schadcodefund auf dem System bzw. im vom System ausgehenden Datenstrom
- Bereitstellung neuer Dienste bzw. Nutzung neuer Kommunikationsprotokolle
- Verbindungsaufbau zu bekannten Command & Control (C2)-Servern
- Direkte Anfragen an externe DNS-Server, Umgehung von vorgesehenen Proxy-Systemen

Die typische Vorgehensweise für kompromittierte Endgeräte ist, diese abzuschalten, ggf. forensisch zu untersuchen, zu bereinigen bzw. neu aufzusetzen und dann wieder in Betrieb zu nehmen. Das Skript trägt das System über seine MAC-Adresse in eine spezielle AD-Gruppe ein, wodurch es im Netzwerk (durch die Nutzung von NAC mit 802.1X) in ein anderes VLAN verschoben wird. Dort ist es von anderen Systemen im LAN isoliert und kann nur sehr eingeschränkt und intensiv überwacht auf ausgewählte interne Dienste zugreifen. Dieses Vorgehen ist vergleichbar mit der Microsoft Network Access Protection (NAP), bei der ein Endgerät erst nach Prüfung seines Systemzustandes (z.B. aktuelle AV-Signaturen und Patches) vollen Zugang zum Netzwerk erhält, jedoch kommt es ohne Agenten aus und ist wesentlich einfacher zu implementieren. Darüber hinaus trägt das Skript die MAC-Adresse des Endgerätes in eine Liste

auf der Perimeter-Firewall ein. Die Liste wird dann in verschiedenen fest hinterlegten Regeln genutzt, um den Zugriff auf externe Dienste auf wenige freigegebene zu beschränken.

Durch die Isolation wird einem eingeschleusten Schadcode die Möglichkeit genommen, mit seinen C2-Servern zu kommunizieren, andere interne Systeme anzugreifen bzw. zu erkunden sowie Daten zu exfiltrieren. Zudem werden die versuchten Aktivitäten sehr genau aufgezeichnet, um auf dieser Basis den Angriff besser nachvollziehen zu können und ggf. historische Log-Informationen nach Anzeichen unerkannte Kompromittierungen durchsuchen zu können. Die Isolation bleibt bestehen, bis das System überprüft und manuell freigegeben wurde.

5.3 Sperren externer Angreifer

Unternehmensnetzwerke sind permanent Angriffen aus dem Internet ausgesetzt. In vielen Fällen der letzten Jahre werden Unternehmen aber auch über zuvor kompromittierte (weniger gesicherte) Partnerunternehmen oder Zulieferer angegriffen, denen oft mehr Freiheiten beim Zugriff auf das Netzwerk gestattet werden. Erkennt das SIEM-System ungewöhnliches oder schädliches Verhalten, so wird die externe IP-Adresse für eine festgelegte Zeitdauer am Perimeter komplett blockiert, d.h. weder eingehende noch ausgehende Kommunikation wird zugelassen. Beispiele für ein derartiges Verhalten sind:

- Brute-Force-Angriffe auf Authentifizierungen
- Aggressives Scanning der Infrastruktur
- Senden von Schadcode / Versuch eines Exploits

Typischerweise kann gegen externe Angreifer nichts unternommen werden. Die Blockierung sollen deshalb vor allem aggressive Angreifer, die einen negativen Einfluss auf die Performance der Zielsysteme haben, treffen, um so die Last auf den Zielsystemen zu reduzieren. Gleichzeitig soll so der Zeitaufwand für das systematische Scanning der Infrastruktur bzw. der öffentlichen Dienste signifikant erhöht werden, um zumindest die Mehrzahl der opportunistischen Angreifer abzuschrecken. Zielgerichtete, professionelle Angreifer werden durch diese Maßnahme nicht gestoppt. Eine ähnliche Vorgehensweise wird z.B. durch das HIPS fail2ban für einzelne Server angewendet, durch die Kombination mit dem SIEM-System auf das gesamte Netzwerk ausgeweitet.

Die technische Realisierung ähnelt den beiden anderen Beispielen. Wird eine externe IP-Adresse durch das SIEM-System als Angreifer klassifiziert, so wird ein Alarm erzeugt, der die Ausführung eines Skriptes startet. Dieses Skript trägt die IP-Adresse in eine interne Datenbank ein. Nach einer definierten Zeit wird die IP-Adresse wieder aus der Datenbank entfernt, d.h. eine manuelle Aktion ist nicht notwendig. Der Inhalt der Datenbank wird nach jeder Änderung mit einer Liste auf der Perimeter-Firewall synchronisiert. Diese Liste wird dann wiederum im fest vorgegebenen Regelwerk verwendet, um die IP-Adressen zu blockieren. Gehört die IP-Adresse zu einem Partnernetzwerk, so wird zusätzlich auch eine E-Mail an das Ticket-System gesendet, da in diesen Fällen auch wirksam gegen die Quelle des Angriffs (ein System im Partnernetzwerk) vorgegangen werden kann.

6 Ausblick

SIEM-Systeme bieten eine Vielzahl von Möglichkeiten, Schwachstellen, Bedrohungen, Angriffe oder erfolgte Kompromittierungen zu erkennen und effektiv zu analysieren. Moderne SIEM-Systeme sind zudem darauf ausgelegt, Log-Informationen aus Umgebungen mit sehr

vielen Systemen in nahezu Echtzeit zu analysieren, um mit der zunehmenden Geschwindigkeit und Komplexität heutiger Angriffe Schritt halten zu können. Sie übernehmen die für Menschen besonders schwierigen und zeitaufwändigen Tätigkeiten, können sie aber nie vollständig ersetzen. Insbesondere das Problem, dass für einen 24x7-Betrieb eine Mindestmenge von Personal notwendig ist, können SIEM-Systeme nicht lösen. Durch die Automatisierung vorab definierter Gegenmaßnahmen kann bei Angriffen ein Zeitfenster geschaffen werden, in dem eine angemessene Reaktion erfolgt, aber kein Personal bereitstehen muss. Bisher liefern kommerzielle SIEM-Anbieter hierfür keine zufriedenstellenden Lösungen. Es bleibt abzuwarten, ob sich Protokolle wie das von der Trusted Computing Group spezifizierte IF-MAP (Interface for Metadata Access Points) am Markt Verbreitung finden, um auf dieser Basis Automatisierungsaufgaben herstellerübergreifend implementieren zu können. Wie im Beitrag gezeigt, können individuelle Lösungen aber auch mit geringem Aufwand selbst entwickelt werden. Ein anderer Weg zur Lösung des Verfügbarkeitsproblems ist die Nutzung von Managed Services. Hierfür finden sich erste Angebote am Markt, die sich aber noch stärker auf die Bedürfnisse kleiner und mittlerer Unternehmen sowie den Anforderungen des Datenschutzes ausrichten müssen. Langfristig müssen sich Unternehmen der Aufgabe stellen, Sicherheit im täglichen Betrieb stärker zu berücksichtigen, z.B. indem auf unterschiedliche Bereiche verteilte Security-Aufgaben gebündelt, mit dem allgemeinen Betrieb kombiniert oder als eigenständiges Security Operations Center (SOC) ausgebaut werden. Die Nutzung bestehender Betriebsmitarbeiter für eine Erstanalyse von SIEM-Alarmmeldungen kann ein erster Schritt in diesem Transformationsprozess sein.

Literatur

[HPCR15] HP Security Research: Cyber Risk Report 2015, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability (2015)

[SoSe14] Sophos: Security Thread Report 2014, http://www.sophos.com/en-us/medialibrary/pdfs/other/sophos-security-threat-report-2014.pdf (2014)

[Msft14] Microsoft: Security Intelligence Report (Vol. 17), https://www.microsoft.com/en-us/download/details.aspx?id=44937 (2014)

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

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

[InIn14] Infosec Institute: Pricing Policies in the Cyber Criminal Underground, http://resources.infosecinstitute.com/pricing-policies-cyber-criminal-underground/ (2014)

[MaSB14] D. Mahrenholz, R. Schumann, A. Brügmann: SIEM – Technik allein ist keine Lösung, In: P. Schartner, P. Lipp. „DACH Security 2014“, syssec (2014)

[Veri13] Verizon: The 2013 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2013/ (2013)

[PoIn14] Ponemon Institute: Understaffed and at Risk: Today’s IT Security Department, http://www.ponemon.org/library/understaffed-and-at-risk-today-s-it-security-department (2014)