

White Paper

Security Information and Event Management (SIEM)



NIIT IT-Sicherheit



Inhaltsverzeichnis

1. Die Herausforderung	2
2. Security Information and Event Management – Geschichte.....	3
2.1 Physische Zugangskontrolle – Gates, Guns & Guards.....	3
2.2 Elektronische Zugangskontrolle – Perimeter-Schutz.....	3
2.3 Die nächste Generation – strategische Sicherheitsprozesse	3
3. Gründe für die Investition in ein SIEM-System	4
4. Security Information Management (SIM) – Logarchivierung	5
5. Security Event Management (SEM) – Reaktion in Echtzeit.....	6
5.1 Intrusion Detection	7
5.2 Intrusion Prevention	9
5.3 Intrusion Management.....	9
5. Der SIEM-Prozess.....	10
5.1 Überwachung	11
5.2 Unterdrückung & Verwaltung.....	12
5.3 Untersuchung & Reaktion.....	12
6. Fazit	14

Abbildungsverzeichnis

Abbildung 1: Aufbau der Sicherheitsinformationen.....	2
Abbildung 2: Screenshot: Trendanalyse mit archivierten Logdaten im NetIQ SM	5
Abbildung 3: Screenshot: Forensischer Report aus archivierten Logdaten im NetIQ SM	6
Abbildung 4: Effektivität und Komplexität der unterschiedlichen IDS-Arten	8
Abbildung 5: SIEM-Prozess	10
Abbildung 6: Zuordnung Sicherheitsinformationen zu Prozessschritten	10

1. Die Herausforderung

Moderne Netzwerke sind stark heterogen: Sie vereinen zahlreiche unterschiedliche Betriebssysteme, Kommunikationstechnologien und Anwendungen – darunter auch IT-Security-Komponenten. Alle diese Bestandteile sammeln zur Dokumentation ihrer Aktivitäten eine Unmenge von Ereignisdaten. Diese Daten sinnvoll auszuwerten und so einen Überblick über die Geschehnisse im Netzwerk zu erlangen, ist aber mit traditionellen Mitteln oder auf manuellem Wege unmöglich. Dies verhindern die nahezu unendliche Anzahl der Daten sowie die vielen unterschiedlichen Formate, in denen sie vorliegen.

Um die vom Netzwerk gesammelten Daten auswerten zu können, ist intelligentes Management dieser Informationen von Nöten, das die Daten zentralisiert sammelt, in ein einheitliches Format überträgt und verdichtet, und das außerdem die sicherheitsrelevanten Informationen herausfiltert und in den richtigen Kontext stellt.

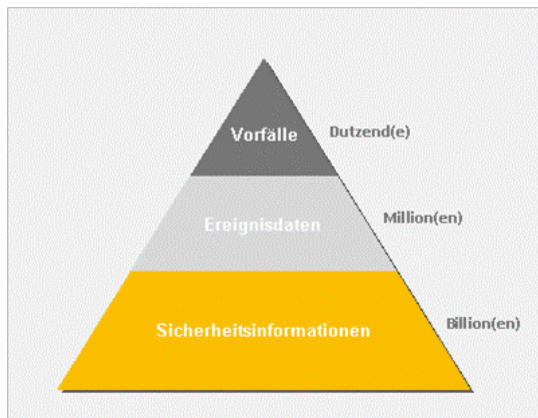


Abbildung 1: Aufbau der Sicherheitsinformationen

Eine durchdachte Lösung für Security Information and Event Management (SIEM) muss nach Gartner zwei Hauptaufgaben erfüllen:

- Security Information Management (SIM): Sammeln und Aufbereiten von Informationen von Betriebssystemen, Anwendungen und IT-Security-Komponenten zur späteren Analyse. SIM ermöglicht so forensische Reports nach sicherheitsrelevanten Vorfällen.
- Security Event Management (SEM): Sammeln und Aufbereiten von

Informationen aus Betriebssystemen, Netzwerkeinheiten und IT-Security-Komponenten, sofortige Auswertung nach vorab definierten Kriterien und gegebenenfalls Alarmierung des verantwortlichen Administrators – so ermöglicht SEM die Reaktion auf interne und externe Gefahren in Echtzeit.

Man kann somit zwischen einer kurzfristigen und einer langfristigen Komponente beim SIEM unterscheiden.

Wie eine intelligente SIEM-Lösung genau beschaffen ist und arbeitet, beschreibt dieses White Paper. Um den heutigen Stand des SIEM zu verstehen, bedarf es einer kurzen Betrachtung der Entwicklung bis dato.

2. Security Information and Event Management – Geschichte

2.1 Physische Zugangskontrolle – Gates, Guns & Guards

Die erste Stufe des Security Information and Event Managements setzte sich auf breiterer Front in den 80er Jahren durch, vor allem in Form physischer Zugangskontrollen. Eingeführt wurden beispielsweise auf Systemebene die RACF für Hosts und für die /36 Maschinen das Objektmodell mit dedizierter Berechtigungssteuerung. Nachteile waren hier die langsamen Reaktionszeiten und der limitierte Schutz vor elektronischen Angriffen.

2.2 Elektronische Zugangskontrolle – Perimeter-Schutz

Die nächste Stufe des SIEM stellen die Perimeter-Schutz Mechanismen dar. Dies sind Firewalls, Anti-Viren Software und Netzwerk Intrusion Detection Systeme. Nachteilig ist bei diesen Lösungen, dass hauptsächlich nur vor bekannten Gefahren geschützt wird und die Lösung meistens aus Komponenten mehrerer Hersteller mit unterschiedlichen Konsolen besteht, wodurch es schwierig wird, den Überblick zu behalten.

2.3 Die nächste Generation – strategische Sicherheitsprozesse

Die nächste Generation des SIEM sind strategische Sicherheitsprozesse, die der IT Governance dienen. Mit den strategischen Sicherheitsprozessen wird die IT-Security von einer projektgetriebenen Abwicklung hin zu einer prozessgesteuerten Realisierung

geführt. Dabei kristallisieren sich zur Zeit im Wesentlichen die folgenden Themengebiete innerhalb der IT-Security heraus:

- Risk Management
- Policy & Compliance Management
- Identity & Access Management
- Configuration & Vulnerability Management
- Security Information and Event Management

3. Gründe für die Investition in ein SIEM-System

SIEM bietet die Möglichkeit, Nutzeraktivitäten und Änderungen an kritischen Daten und Systemeinstellungen nachvollziehen und auch nach einer gewissen Zeit noch revisionssicher nachweisen zu können. Durch SIEM wird der Sicherheitsverantwortliche in die Lage versetzt, in Echtzeit auf sicherheitsrelevante Vorfälle zu reagieren und so akuten Bedrohungen sofort zu begegnen. Eine SIEM-Lösung unterstützt also die IT-Security-Verantwortlichen und erhöht den Sicherheitsstatus des Unternehmens maßgeblich.

Zudem fordern viele aktuelle Standards den Einsatz eines SIEM-Systems. Zu nennen wäre hier an erster Stelle das Bundesdatenschutzgesetz (BDSG), das in der Anlage zu §9 Absatz 1.5 verlangt, dass bei Eingabe, Änderung oder Entfernung personenbezogener Daten im Nachhinein überprüfbar sein muss, wer diese Maßnahme durchgeführt hat und wann.

Auch der Kreditkartenstandard PCI DSS listet in Anforderung 10 die "Verfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten" mit besonderer Betonung der Notwendigkeit von Systemaktivitätsprotokollen für eine gründliche Nachverfolgung bei Gefährdungen.

Der Best Practice-Standard ISO 27001 führt ebenfalls unter A 10.10 das Monitoring als Anforderung an die IT-Security, mit dem Ziel, unautorisierte Aktivitäten aufzudecken an. Hier wird ebenfalls das Sammeln und Archivieren von Daten zu Nutzeraktivitäten und sicherheitsrelevanten Vorfällen für spätere Analysen als Aufgabe genannt.

Es sprechen reichlich Gründe für ein SIEM-System. Wie dieses beschaffen ist, entscheidet das Unternehmen. Es empfiehlt sich jedoch eine Lösung, die SIEM nach

individuell definierten Parametern automatisiert durchführt – anders ist der enormen Datenflut in modernen Netzwerken nicht Herr zu werden.

4. Security Information Management (SIM) – Logarchivierung

Ein SIM-System sammelt und zentralisiert alle sicherheitsrelevanten Informationen und Ereignisdaten aus dem Netzwerk, bringt sie in ein einheitliches Format und archiviert sie zur späteren Auswertung. Dabei ist eine wesentliche Anforderung an die Lösung, dass diese Vorgänge automatisch und auch revisionssicher erfolgen müssen.

Die gesammelten Daten ermöglichen zum einen forensische Analysen zur Beweisführung, sei es nach einem kriminellen Angriff oder zur Entlastung des Unternehmens bei einem nicht-intentionalen Schaden. Zum anderen ermöglicht das Informationsarchiv auch Trendanalysen, die wertvolle Erkenntnisse über die Entwicklung der Bedrohungen oder Schwachstellen im eigenen Netzwerk liefern.

Durch regelmäßige Auswertungen kann sich der IT-Security-Verantwortliche einen guten Überblick über die Vorgänge und den Status des Unternehmensnetzwerks verschaffen und zudem Abweichungen vom Normalen schnell und einfach erkennen.

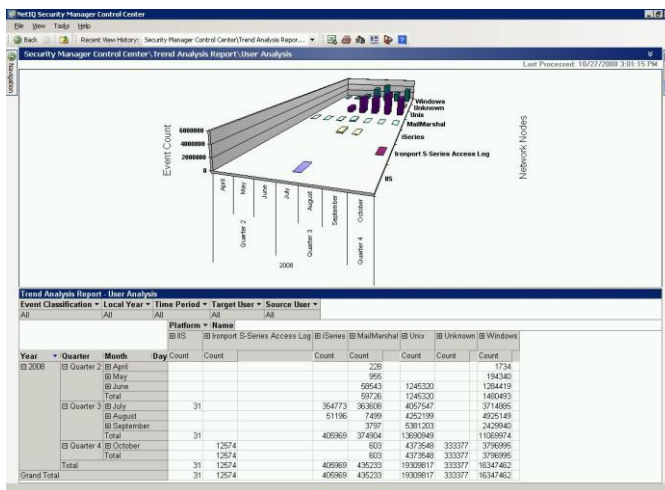


Abbildung 2: Screenshot: Trendanalyse mit archivierten Logdaten im NetIQ SIM

5.1 Intrusion Detection

Intrusion Detection ist der Vorgang, um verdächtige oder unautorisierte, digitale und elektronische Aktivitäten zu identifizieren. Im Netzwerk-Sicherheitsbereich liefern Intrusion Detection Systeme (IDS) eine weitere Sicherheitsebene, indem sie den Netzwerkverkehr laufend auf verdächtige Codes und Angriffe absuchen. Intrusion Detection Systeme laufen permanent im Hintergrund und überprüfen den ein- und ausgehenden Netzwerkverkehr eines Computers. IDS suchen nach verdächtigem, vom normalen abweichenden Datenverkehr oder gleichen ihn mit einer bekannten Bedrohung ab. Wenn das IDS ein verdächtiges Muster erkennt, alarmiert es den Anwender oder startet vorher festgelegte Abwehrmaßnahmen. Idealerweise konfiguriert der IT-Administrator Art und Grad der spezifischen Auffälligkeiten, die als gefährlich angesehen werden und legt für jede Auffälligkeit richtlinienbasierte Reaktionen fest. Ähnlich einem Haus-Sicherheitssystem, das verdächtige Aktivitäten mit Kameras und anderen Geräten kontrolliert, alarmiert das IDS die zuständigen Mitarbeiter bei möglichen Einbrüchen in das Netzwerk. Ein Intrusion Detection System lässt sich leicht in eine bestehende IT-Infrastruktur implementieren.

Netzwerkbasierte IDS

NIDS überprüfen sämtliche Pakete, die über ein Netzwerk übertragen werden. Ein typisches netzwerkbasiertes IDS besteht aus einem oder mehreren Sensoren, die die Daten sammeln und analysieren und einer Konsole, die diese abbildet. Durch heutige hohe Netzlast ist allerdings das Sammeln aller Datenpakete nur schwer möglich. Aufgrund von Fehlerkennungen (false-positives) können netzwerkbasierte IDS auch fälschliche Warnmeldungen erzeugen, so dass ein tatsächlicher Angriff nur schwer erkennbar ist. Moderne NIDS Systeme bieten des Weiteren schon Analysen des Netzwerkverkehrs auf Applikationsebene, so können z. B. schon SQL Datenströme oder http-Traffic auf Anomalien untersucht werden.

Hostbasierte IDS

HIDS überprüfen die Prozesse innerhalb des Hosts und überwachen dabei Protokolldateien und Daten auf verdächtige Aktivitäten. Einige hostbasierte IDS arbeiten unabhängig von anderen Systemen. Es gibt aber auch Systeme, in denen dezentrale hostbasierte IDS ihre Daten an ein Master-System senden. Da dieses Master-System

die zentrale Verwaltung der Auswertungs- und Reaktionsmechanismen übernimmt, wird diese Lösung eher in großen Unternehmensumgebungen eingesetzt. Wie bei den meisten hostbasierten Lösungen ist deren Verwaltung aufgrund der Plattformverfügbarkeit und -abdeckung nicht ganz einfach. Zudem können diese Systeme keine Netzwerkangriffe erkennen, da hostbasierte IDS keine Paketprüffunktionen vorsehen.

Application Shielding

Anwendungs-Intrusion-Detection oder Applikation Shielding überwacht Applikationen wie Webserver und Datenbanken. Die dazu notwendigen Systeme überwachen dabei die Protokolldateien und die Zugriffe auf die Applikationen.

Ein Sonderfall des Application Shielding sind Web Application Firewalls (WAF). Sie schützen Web-Anwendungen vor Angriffen über das http-Protokoll, beispielsweise SQL Injection oder Cross-Site Scripting.

Kernel Shimming

Beim Kernel Shimming wird der Kernel des Betriebssystems gehärtet. Dies ist die sicherste Art der Intrusion Detection, jedoch auch die komplexeste.

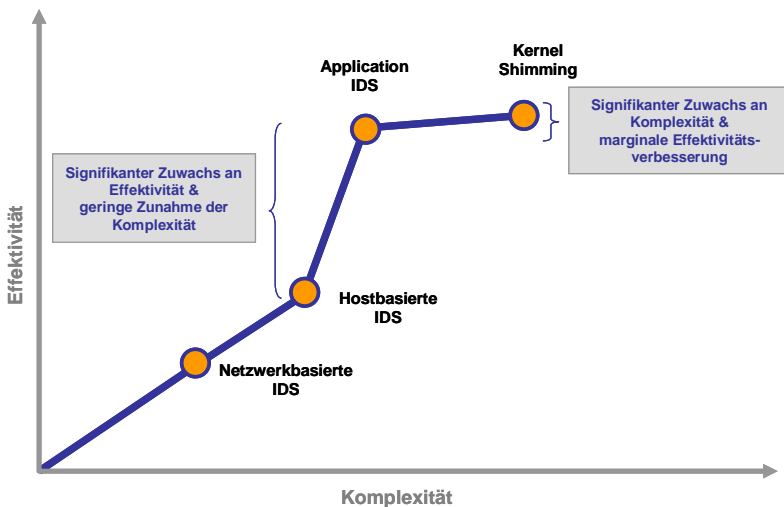


Abbildung 4: Effektivität und Komplexität der unterschiedlichen IDS-Arten

Die effektivste Art ist eine Kombination aus hostbasiertem und applikations-basiertem IDS, welches durch Netzwerk-IDS-Systeme ergänzt werden kann. Aufgrund der geringeren Komplexität ist dies dem Kernel Shimming vorzuziehen.

5.2 Intrusion Prevention

Intrusion Prevention Systeme blocken Angriffe in Echtzeit bevor sie Schaden anrichten können. Es gibt drei Arten von Intrusion Prevention:

perimeterbasierte, host- und applikationsbasierte und an das Netzwerk angepasste (als Gegenpol zu Intrusion Detection-Sensoren und IDS). Der Vorteil von Intrusion Prevention besteht darin, dass aufgespürte Angriffe abgefangen werden, bevor sie ins Netz gelangen und so kein Schaden entsteht, der wieder behoben werden müsste. Es gibt aber auch Nachteile, besonders wenn die Intrusion Prevention-Technology als transparentes Gateway direkt in die Netzwerkverbindung implementiert wird. Alle Intrusion Detection-Technologien liefern Fehlerkennungen. Ein Inline Intrusion Prevention-Produkt wird bei einer Fehlerkennung das System sperren und so auch den legitimierte Geschäftsverkehr behindern. Bei Netzwerk-basierter Intrusion Prevention kann es passieren, dass Fehlalarme ganze Netzwerksegmente außer Betrieb setzen. Auch die Installation und Verwaltung von Intrusion Prevention-Produkten gestaltet sich unter Umständen komplizierter als bei Intrusion Detection-Produkten. Der Einsatz von Intrusion Prevention Systemen muss mit großer Sorgfalt abgewägt werden.

5.3 Intrusion Management

Das Intrusion Management sammelt die Informationen der unterschiedlichen Intrusion Detection Systeme. Diese werden im Intrusion Management aggregiert und korreliert. Aus den gesammelten Ereignisdaten werden dann die Vorfälle abgeleitet und priorisiert.

5. Der SIEM-Prozess

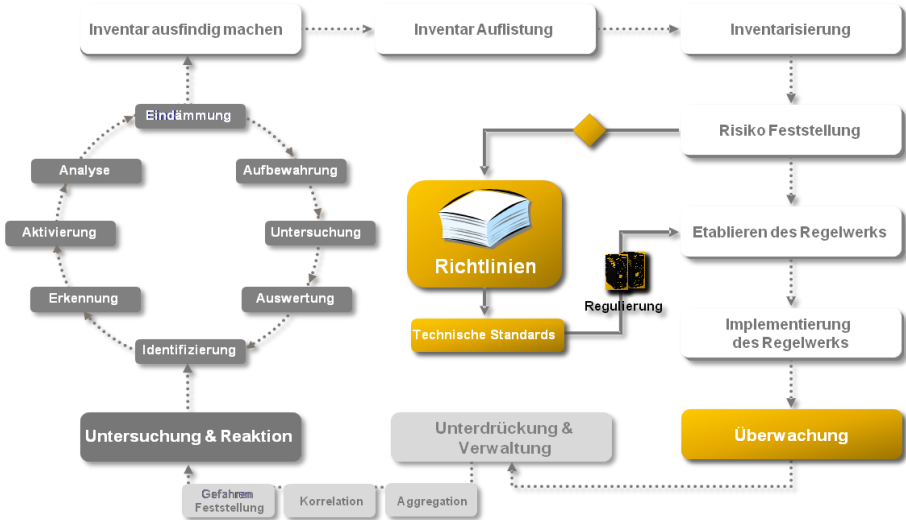


Abbildung 5: SIEM-Prozess

Security Information and Event Management ist ein Ineinandergreifen von unterschiedlichen Aufgaben. Dabei ist es entscheidend, dass jeder dieser Schritte richtliniengesteuert ist. Die einzelnen Schritte bauen aufeinander auf.



Abbildung 6: Zuordnung Sicherheitsinformationen zu Prozessschritten

Die Schritte Überwachung, Unterdrückung & Verwaltung und die Untersuchung und Reaktion auf Vorfälle (Incidents) werden als SIEM-Kernthemen im Folgenden näher betrachtet.

5.1 Überwachung

- **Endpunkt Verwaltung**
Im ersten Schritt werden die zu überwachenden Endpunkte festgelegt.
- **Normalisierung**
Die Daten der unterschiedlichsten Quellen wie Betriebssystemen, Anwendungen und Netzwerkkomponenten kommen in einer Vielzahl von Formaten im Intrusion Management System an. Deshalb müssen im ersten Schritt die Daten im Intrusion Management System normalisiert und in ein einheitliches Format gebracht werden, um sie im nächsten Schritt zu verarbeiten.
- **Datenfilterung**
Entscheidend ist angesichts der Flut an sicherheitsrelevanten Informationen, bedeutende von unbedeutenden zu trennen. Dabei sollte man nicht nach dem Prinzip „Trial and Error“ vorgehen, sondern zu Anfang den Fokus auf eine eher kleine Auswahl der wesentlichsten Daten legen. Nachdem sich der Prozess eingespielt hat und im Zuge des Vulnerability Managements die Vorfälle minimiert wurden, können weitere Informationen in den Fokus aufgenommen werden. Als wesentlich erkannte Informationen werden an das Intrusion Management System weitergeleitet. Das Intrusion Management System muss dabei:
 - die Filterung der Eventdaten in den Kontrollpunkten vornehmen, um eine hohe Netzwerkbelastung zu vermeiden,
 - offene Schnittstellen besitzen, um Informationen von nicht im Standard
 - unterstützten Anwendungen und Systemen trotzdem verarbeiten zu können,
 - die Wahrung der Integrität der Eventdaten sicherstellen,
 - die Speicherung und Archivierung der Eventdaten für forensische Analysen
 - sicherstellen.

5.2 Unterdrückung & Verwaltung

- Aggregation
 - Gleiche Events zusammenfassen (aggregieren, verdichten)
In diesem Schritt erfolgt die Zusammenfassung von gleichen Ereignisdaten über einen definierten Zeitraum, z. B. x fehlgeschlagene Anmeldeversuche innerhalb von 30 Minuten
 - false-positives ausblenden
Die Ausblendung von false-positives ist möglich, z.B. wenn ein Benutzer sein eigenes Kennwort ändert.
- Korrelation
Hier werden die Kombinationen von Events korreliert und als ein Vorfall eskaliert. Nehmen Sie an, es werden an mehreren Maschinen über einen längeren Zeitraum fehlgeschlagene Anmeldeversuche für das Administrationskonto von derselben internen IP-Adresse gemeldet. Ohne die Event-Korrelation würden Sie mehrere Tickets/Alarmer bekommen, obwohl es sich um ein und dasselbe Problem handelt. Mit der Korrelation wird die Vielzahl von Ereignissen der entsprechenden Server zu einem Vorfall (Incident) zusammengefasst, bzw. erst ab einer gewissen Anzahl gemeldet, um false-positives zu verhindern.
- Gefahrenaufstellung
Bei der Gefahrenfeststellung wird anhand der in den beiden vorhergehenden Schritten, dem Aggregieren und Korrelieren von Events nun entschieden, ob ein Event oder eine gewisse Anzahl an Events innerhalb einer bestimmten Zeit oder eine Abfolge von Events eine Gefahr darstellen. Wird ein Event als gefährlich eingestuft, wird ein Incident (Vorfallicket) erstellt, welches in der nachfolgenden Stufe bearbeitet wird.

5.3 Untersuchung & Reaktion

Der Prozess zur Untersuchung von Vorfällen mit den daraus resultierenden Ergebnissen dient als Information zur Schließung von Schwachstellen und zur Verfolgung von Verstößen und Angriffen. Die linke Hälfte der Schritte (Aufbewahrung bis Auswertung, siehe Bild SIEM-Prozess) ist für die Feststellung der Beweismittel, um gegebenenfalls weitere rechtliche oder disziplinarische Maßnahmen ergreifen zu können.

- **Identifizierung**

Während der Identifizierung wird der Vorfall festgestellt. Dabei muss es möglich sein, über eine History oder Firmen-Knowledge-Base schon Verknüpfungen zu gleichen oder ähnlichen Vorfällen in der Vergangenheit herzustellen, um dem bearbeitenden Personal eine Hilfestellung zu bieten. Dieser Schritt sollte weitestgehend automatisiert erfolgen.
- **Klassifizierung**

Die Klassifizierung eines Vorfalles sollte nun, wie die Identifizierung, weitestgehend automatisch erfolgen und dabei gleichzeitig dem bearbeitenden Personal die Möglichkeit bieten, die Klassifizierung zu einem späteren Zeitpunkt manuell zu verändern. Die Kategorisierung des Vorfalles sollte dabei auf den folgenden Kriterien basieren:

 - den betroffenen Systemen, Netzwerken, Anwendungen und Daten
 - der Art des Vorfalles
- **Mobilisierung**

Die Mobilisierung der Ressourcen für die Analyse muss nun anhand der Klassifizierung erfolgen. Dies sollte auch weitestgehend automatisch durch die gewählte Softwarelösung basierend auf der Klassifizierung erfolgen. Best-Practices zeigen, dass es aus Kostengründen sinnvoll ist, zuerst einen Sicherheitsspezialisten mit der Analyse des Vorfalles zu betrauen. Kann dieser den Vorfall nicht bis zum Schritt der Eindämmung lösen, so sollte anschließend je nach Struktur der Firma ein Sicherheitsmanager mit der Eskalation betraut werden und als letzter Schritt ein entsprechendes Incident Response Team in Abhängigkeit des Vorfalles zusammengerufen werden.
- **Analyse**

In der Phase der Analyse wird der Vorfall auf seinen Ursprung und seine Auswirkungen hin untersucht.
- **Eindämmung**

Während der Eindämmung wird die Auswirkung des Vorfalles und die daraus möglicherweise resultierenden Schäden minimiert, bzw. der Ursprung des Vorfalles behoben oder dessen Behebung veranlasst. Dies wird zum Beispiel bei einem fehlenden Sicherheitsupdate für ein Betriebssystem oder bei falschen Berechtigungen für einen Benutzer der Fall sein.
- **Aufbewahrung**

In den nun folgenden Schritten wird die Sicherstellung von Informationen für die Verfolgung von Vorfällen sichergestellt – dieses Sammeln und Archivieren von Daten hat revisionssicher zu erfolgen. Bei der Aufbewahrung werden alle Beweismittel, die für eine weitere rechtliche oder disziplinarische Verfolgung des Vorfalls notwendig sind, sichergestellt. Im Regelfall sind das die entsprechenden Eventdateien von den betroffenen Geräten und ggf. sogar Festplatten von entsprechenden Rechnern.

- **Untersuchung**

Bei der Untersuchung wird der Vorfall geprüft. In diesem Schritt wird in Abhängigkeit der Schwere des Vorfalls untersucht, ob genügend Beweismaterial vorliegt, um weitere Schritte einzuleiten.

- **Auswertung**

Während der Auswertung werden der Vorfall und die Ergebnisse der Analyse und der Untersuchung dokumentiert. Die Ergebnisse der Auswertung werden dann mit den getroffenen Maßnahmen wiederum in die Knowledgebase übernommen und dort gepflegt. Im Laufe des Betriebs entsteht so eine umfangreiche Datenbank mit bereits getroffenen Maßnahmen für die Mitarbeiter, welche zur effizienteren Abarbeitung der Vorfälle zur Verfügung steht. In der Auswertung wird festgehalten, was für Änderungen an den Richtlinien vorzunehmen sind oder in welcher Weise das Regelwerk modifiziert werden muss, um einen solchen Vorfall in Zukunft zu unterbinden.

6. Fazit

Ein professionelles Security Information and Event Management ist für ein größeres Unternehmen oder ein Unternehmen, das unterschiedlichen regulatorischen Vorgaben unterliegt, unabdingbar.

Bei der Auswahl der Software zur Implementierung eines Security Information Management Prozesses muss die Software

- es ermöglichen, die Prozesse auch mit einem hohen Grad an Automatisierung abzubilden
- offene Schnittstellen besitzen, um diese zum einen für ein Wachstum der Infrastruktur offen zu halten und zum anderen um die gesamte Infrastrukturinformationen auf Bedarf zu integrieren

- eine eigene Unternehmens-Knowledge-Base integriert haben, in der die Ergebnisse und Erkenntnisse von vorhergegangenen Vorfällen gepflegt werden können, um so bei erneuten Vorfällen das erarbeitete Wissen verfügbar zu machen
- eine eingebaute Datenbank mit „best practices“ zur Verfügung stellen
- die Möglichkeit bieten, forensische und Trend-Analysen auf Basis der gesammelten Events zu ermöglichen
- eingebaute Korrelation und Aggregation für bekannte Vorfälle von Betriebssystemen und Anwendungen bieten
- flexible Möglichkeit bieten, die Korrelation und Aggregation zu modifizieren bzw. auf eigene Gegebenheiten anzupassen
- eine automatisierte Reaktionsmöglichkeit auf Vorfälle bieten, (Intrusion Prevention System)
- granulare Einstufungsmöglichkeiten für Vorfälle basierend auf Servergruppen und Art des Ereignisses bieten
- automatische Eskalationsstufen bei Vorfällen anhand von SLAs bieten

Eine SIEM-Lösung sollte neben den bisher aufgeführten Eigenschaften für die Verarbeitung des Echtzeit-Incident-Management-Prozesses die Möglichkeit bieten, alle Log-Informationen der überwachten Systeme zu sammeln, zu archivieren und auszuwerten. Somit ist es möglich mit einer Lösung Sicherheitsinformationen in Echtzeit und historisch durch entsprechende forensische Analysen zu bearbeiten. Dies ermöglicht im Ergebnis einen guten Durchblick in der bestehenden Infrastruktur um so stets den Überblick zu behalten.

NIIT Technologies

Die NIIT Technologies GmbH hat sich auf Services rund um Anwendungsentwicklung und -Management, IT-Security, IT-Infrastruktur und Managed Services spezialisiert und begleitet Kunden individuell von der strategischen Ausrichtung bis hin zur operativen Umsetzung. NIIT Technologies gehört zu den führenden Outsourcing-Anbietern weltweit. Neben unseren Kunden bestätigen das auch die Black-Book Studie 2009 und das Ranking der IAOP 2009.

Kontakt

NIIT Technologies GmbH

Zettachring 6 | 70567 Stuttgart

Tel: +49 7 11 71917 – 0

michael.eisenmann@niit-tech.de

www.niit-tech.de

NIIT Technologies GmbH

Deutschland
Zettachring 6
70567 Stuttgart
Tel: +49 7 11 71917 - 0
Fax: +49 7 11 71917 - 150

Delitzscher Straße 9
40789 Monheim
Tel: +49 21 73 16 75 - 0
Fax: +49 21 73 16 75 - 150

info@niit-tech.de
www.niit-tech.de

NIIT Technologies GmbH

Österreich
Kandlgasse 18/4/9
1070 Wien
Tel: +43 1 729 62 62
Fax: +43 1 729 62 62-90

info@niit-tech.at
www.niit-tech.at

NIIT Technologies AG

Schweiz
Tribtschenstraße 9
6005 Luzern
Tel: +41 41 360 48 77
Fax: +41 41 360 21 64

info@niit-tech.ch
www.niit-tech.ch

