management

IT-SICHERHEIT – Mit der Einführung eines ISMS, also eines Informationssicherheits-Managementsystems, gilt es, eine Vielzahl an Maßnahmen umzusetzen. Durch ein Security Incident and Event Management können Sicherheitsvorfälle zielgerichteter und schneller behandelt werden.

DER WÄCHTER

Jeder Strom- und Gasnetzbetreiber ist nach dem IT-Sicherheitskatalog verpflichtet, ein Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 einzuführen. Dabei gibt es zahlreiche Maßnahmen innerhalb der Norm, zu deren Umsetzung ein Security Information and Event Management (SIEM) wirksam beiträgt. Vor allem innerhalb des Maßnahmenbereiches Logging und Monitoring (A.12) ist ein SIEM-System eine ideale Umsetzung dieser Anforderungen.

Eine wichtige Maßnahme ist das sogenannte Event-Logging. Es fordert, dass Eventlogs, in denen Benutzeraktivitäten, Fehler und Informationssicherheitsvorfälle registriert werden, gesammelt und regelmäßig ausgewertet werden müssen. Bei mehreren Millionen Ereignissen täglich ist es schwer, die Übersicht zu bewahren. Ein SIEM-Tool automatisiert diese Übersicht.

Es sammelt die Eventlogs von unterschiedlichen Systemen und legt sie zentral ab. Darüber hinaus werden die Ereignisse von dem SIEM-Tool regelbasiert auf Anomalien untersucht. Bei einem Match, also einem Hinweis auf einen Angriff, wird automatisch ein Alarm generiert und entsprechende Gegenmaßnahmen können durch die Security-Analysten eingeleitet werden.

AKTIVITÄTEN UNTER BEOBACHTUNG

Der zweite wichtige Punkt in der Maßnahmenliste, bei dem ein SIEM-System unterstützen kann, ist das Schützen von Protokollinformationen. Alle gesammelten Logs werden nicht nur auf den jeweiligen Systemen gespeichert, sondern zentral innerhalb des Tools manipulationsgeschützt und revisionssicher gespeichert.

Bild: Ian Sherriffs/fotolia.de

Eine weitere Anforderung ist das Erfassen, Schützen und Überprüfen von Systemadministrator- und Systembetreiber-Aktivitäten. Auch dies erledigt das SIEM durch das automatische Auswerten und manipulationssichere Speichern. Durch die zentrale, systemübergreifende Auswertung können Aktivitäten erkannt werden, die durch eine Betrachtung auf dem einzelnen System nicht erkennbar sind. So kann beispielsweise ein SIEM-Tool erkennen, dass ein Administrator, der große Mengen Daten von einer Datenbank exportiert, diese auf das Nutzerlaufwerk C:\ ablegt und anschließend auf einen USB-Stick exportiert.

SECURITY INCIDENT MANAGEMENT

Ein weiterer Themenbereich innerhalb der Maßnahmen ist zum Beispiel das Information Security Incident Management (A.16). Um sicherheitsrelevante Vorfälle frühzeitig erkennen zu können, bedarf es einer definierten Vorfallsanalyse und -behandlung. In diesem Kontext kommt das SIEM zum Einsatz. Ein SIEM sucht nach festgelegten Angriffskriterien und generiert Alarme, die dann vom Security Incident Management weiterverfolgt werden.

Sofern ein Informationssicherheitsereignis eingetreten ist, muss dieses bewertet und hinsichtlich seiner Relevanz eingestuft werden. Das SIEM generiert in diesem Fall einen Alarm, der die wichtigsten Informationen zu dem Ereignis zusammenfasst. Weitere Informationen können innerhalb des SIEM-Tools gesucht werden. Dadurch lässt sich innerhalb kürzester Zeit ein klares Bild über die Auswirkungen auf die Informationssicherheit ableiten.

Bei erkannten Informationssicherheitsvorfällen muss schnellstmöglich eine Reaktion erfolgen. Mithilfe eines SIEM findet eine ständige, automatisierte Log- und Eventüberwachung der Systeme auf sicherheitsrelevante Vorfälle statt. Somit können potenzielle Vorfälle bereits vor und während eines Angriffes erkannt werden. Bereits geeignete Gegenmaßnahmen können eingeleitet werden, bevor ein größerer Schaden entstehen kann. Dadurch können die Schäden verringert werden.

Ein wichtiger Punkt im Rahmen der ISO 27001 und des Sicherheitsgesetzes ist das Melden von Informationssicherheitsereignissen. Dies setzt voraus, dass Vorfälle auch zuverlässig erkannt und bewertet werden. Es ist nahezu unmöglich, aus einer großen Menge dezentral gespeicherter Logs Informationssicherheitsereignisse schnell zu erkennen und notwendige Informationen zur Meldung zu ermitteln. Ein SIEM ermöglicht innerhalb kurzer Zeit, notwendige Informationen über einen Vorfall zu sammeln und zu analysieren, um bewerten zu können, inwiefern der Vorfall melderelevant ist.

EINFÜHRUNG IN DREI SCHRITTEN

Der erste Schritt bei der Einführung einer SIEM-Lösung besteht darin, herauszufinden, welche Daten und welche IT-Funktionen als kritisch für das Geschäft zu bewerten sind.

Der zweite Schritt ist es, diese Werte durch eine gute und effiziente IT-Sicherheitsarchitektur zu schützen. Hier kommen alle präventiven Maßnahmen, wie Anti-Viren-Systeme, Firewalls, Intrusion-Prevention-Systeme, Zugriffsschutz und Rollenkonzepte, zum Einsatz. Dieser Schritt ist ein Teilbereich der Risikobehandlung und innerhalb des Risikomanagements durchzuführen.

Präventiver Schutz ist niemals lückenlos, zumal die Angreifer fortlaufend neue Methoden entwickeln, um Angriffe durchzuführen, neue Schwachstellen in den vorhandenen IT-Systemen entdeckt werden oder die Mitarbeiter als Einfallstor in das Unternehmen genutzt werden. Letzteres geschieht etwa in zunehmenden Maße durch gut gemachte Phishing-E-Mails, welche nicht mehr einfach zum Beispiel aufgrund ihrer schlechten Grammatik erkannt werden können. Hier setzt im dritten Schritt SIEM an: Alle IT-Geräte werden so konfiguriert, dass die Ereignisse, die Hinweise auf Angriffe geben, aufgezeichnet und an das SIEM zur Auswertung weitergeleitet werden.

Jennifer Lüken (Consecur)

www.consecur.de

WISSEN KOMPAKT

Was ist ein Security Information and Event Management?

Ein SIEM ist eine Management-Lösung, mit der Unternehmen und Organisationen Gefährdungen und Angriffe auf ihre IT-Systeme entdecken und abwehren, idealerweise bevor ein Schaden die Geschäfte beeinträchtigen oder zum Erliegen bringen kann. Im laufenden Betrieb verbessert sie kontinuierlich und regelbasierend die Standards für Sicherheit, Compliance und Qualität der IT-Systeme.

Das SIEM-System sammelt alle Aktivitäten innerhalb der IT-Landschaft und wertet diese nach Angriffskriterien aus. Das können sowohl Protokolldaten von Netzkomponenten, wie Router, Switche und Firewalls, aber auch von IT-Systemen und Anwendungen sein. Diese werden vom System anhand eines Regelwerkes ausgewertet und schlagen Alarm, sobald eine verdächtige Kombination von Ereignissen erkannt worden ist.

Quelle: Consecur