Systeme überwachen – Vorbeugen vor dem Ereignis

Angriffe auf Systeme haben einen neuen Höchststand erreicht. Praktisch kein Tag vergeht, ohne eine Schlagzeile über ein gehacktes System oder gestohlene Daten. Diese Daten werden zur Informationsspionage verwendet, im Internet verkauft oder weitere Systeme angegriffen. Auch die Erpressung, zum Beispiel via Ransomware ist sehr beliebt bei den Hackern. Dabei wird das eigene System infiziert, alle Daten verschlüsselt und Lösegeld zur Wiederherstellung gefordert.

Doch ein Angriff auf ein Unternehmen ist nicht in einer Nacht durchgeführt. Es gilt zuerst Schwachstellen zu identifizieren, die dann in einem späteren Schritt ausgenutzt werden können. Dabei werden Spuren an verschiedenen Stellen hinterlassen.

Diese sind in diversen Log-Dateien der Systeme zu finden. Nur wenn diese regelmässig, idealerweise täglich oder gar in Echtzeit, ausgewertet werden, können genügend früh (Gegen-)Massnahmen ergriffen werden.

Log-Aufzeichnung

Protokoll-Daten helfen, Fehler zu erkennen und vorbeugende Massnahmen zu ergreifen. Auch in der ISO 27001 A.12.4 wird verlangt: «Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.» (siehe auch Maschinenbau 2019/8: Lebenszyklus von Systemen). Dies können Meldungen von Servern, Netzwerkgeräten, Störungen, Alarme, Zugriffe, (Konfigurations-) Änderungen, Nutzung von privilegierten Programmen, usw. sein, die idealerweise zentral gesammelt und regelmässig ausgewertet werden. Darin enthalten sollten mindestens sein: Datum/Uhrzeit, Benutzer und/oder System und/oder IP-Adresse sowie die entsprechende Aktivität.

Damit eine Korrelation der verschiedenen Daten überhaupt sinnvoll möglich ist, müssen die Systemzeiten auf allen Systemen korrekt konfiguriert sein. Dazu stehen im Internet diverse Zeitserver zur Auswahl. Eine gute Anlaufstelle ist www.pool.ntp.org/zone/ch.

Zu beachten gilt auch, dass die Zeitstempel nicht bei allen Systemen identisch sind. Einige Beispiele dafür:

- OLE 2.0 Datum und Uhrzeit (8 Byte, beginnend ab 30.10.1899),
- ANSI SQL Datum und Uhrzeit (8 Byte, beginnend ab 17.11.1858),
- Macintosh HFS+ Datum und Uhrzeit (4 Byte, beginnend ab 1.1.1904),
- Java Datum und Uhrzeit (8 Bytes, beginnend ab 1.1.1970)

Auch die Zeitzonen sind sehr unterschiedlich konfiguriert. Auf linux-basierten Systemen ist die Zeitzone in der Datei timezone im Verzeichnis usw. gespeichert.

Für die Korrelation von Logdaten wird als Normzeitzone die Greenwich Mean Time (GMT) Zone benutzt, zu welcher in westlicher Richtung die Stunden addiert (GMT+X) und von welcher in östlicher Richtung die Stunden (GMT-X) abgezogen werden müssen.

Des Weiteren gilt es, eventuelle Sonderzeiten, wie zum Beispiel die Sommerzeit (engl. Daylight Savings Time) zu berücksichtigen, um eine Aussage über die tatsächliche Zeit in einem System und den von ihm erstellten Objekten treffen zu können. Windows sammelt die Ereignisse in den Eventlogs (Bild 1).

Zu den protokollierten Ereignissen können beispielsweise fehlgeschlagene Anmeldeversuche, Statusänderungen der Netzwerkverbindungen, Warnungsmeldungen über die Systemsicherheit und Fehler bei der Einrichtung von Treibern oder beim Starten von Diensten gehören. Zu jedem Ereignis werden die Art des Ereignisses, die Ereignisquelle sowie Datum und Uhrzeit festgehalten.

Ort	Verwendung
/var/log/messages	Generelle Meldungen, inklusive System
/var/log/auth.log	Authentifizierung
/var/log/kern.log	Kerlen
/var/log/cron.log	Cron Jobs
/var/log/maillog	Mail Server
/var/log/httpd/	Apache Zugriff und Fehlermeldungen
/var/log/boot.log	System Boot Informationen
/var/log/mysqld.log	MySQL Datenbank-Meldungen

Bild 2: Linux-Logdaten.

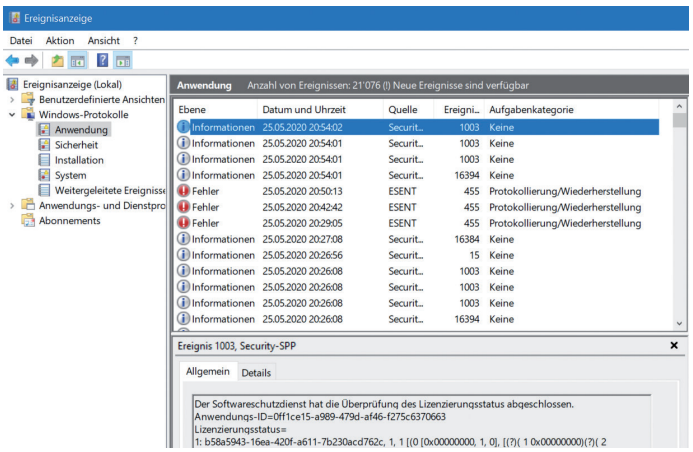

Bild 1: Eventlog, Windows 10.

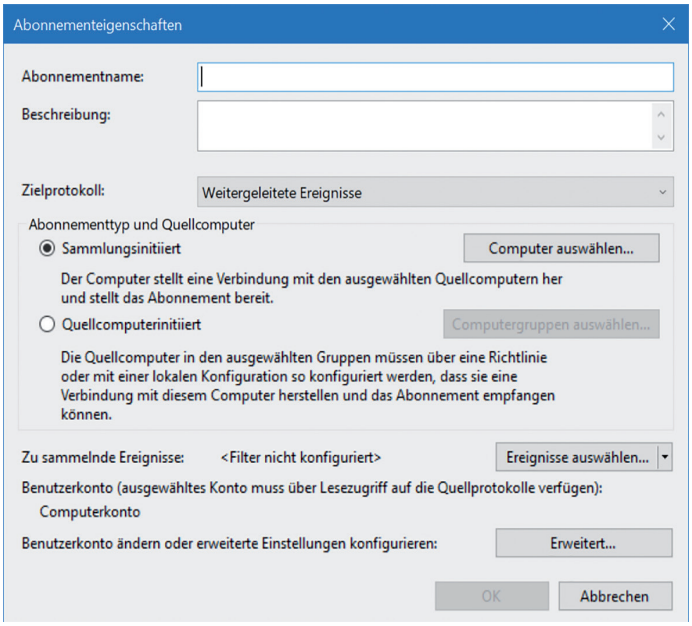

Bild 3: Windows Logweiterleitung.

Auch unter Linux werden selbstverständlich Log-Daten geführt. Praktisch alle Daten werden in das Verzeichnis /var/log abgelegt. Mit den entsprechenden Tools können diese angezeigt werden. Als Werkzeuge kommen beispielsweise less, more, cat, tail oder grep zur Verwendung. Bild 2 zeigt klassische Logs.

Idealerweise werden Logdaten nicht einzeln pro System erfasst und regelmässig ausgewertet, sondern zentral gesammelt. Unter Windows kann dies von einem Collector gesammelt oder vom Server direkt an einen zentralen Ort weitergeleitet werden (Bild 3).

Unter Linux kommt unter anderem das Netzwerk-Protokoll syslog zum Einsatz. Es übermittelt die entsprechenden Logdaten auf einen definierten Rechner und verwendet dabei den UDP-Port 514 oder verschlüsselt TCP 6514. Eine entsprechende Meldung enthält den Selektor (Priorität, teilt zum Beispiel mit, dass es sich um einen Emergency, Alert, Critical, Error, Warnung oder Notice handelt), einen Header (Name und IP-Adresse des Absenders) und den Inhalt.

Monitoring

Am Zielsystem selbst gilt es die Daten auszuwerten und entsprechend darzustellen. Hier gibt es eine Vielzahl von kostenlosen und kommerziellen Produkten.

Sehr beliebt ist die Open-Source-Lösung Graylog (www.graylog.org/products/open-source). Die Daten werden ebenfalls gesammelt, können gefiltert und auf Dashboards dargestellt werden. Diverse Suchfilter ermöglichen die Suche nach Fehlern (Bild 4).

Auswertung

Ein Security Information and Event Management System (SIEM) sammelt Meldungen und Logfiles relevanter Systeme und wertet diese aus. Somit können Ereignisse, welche nicht der Baseline entsprechen, in Echtzeit erkannt werden.

Essenziell bei einem SIEM ist, dass sämtliche Daten an einem zentralen Punkt gesammelt werden. Spezifizierte Analysen und Muster helfen dann, Trends und gefährliche Aktivitäten in Echtzeit zu erkennen und zu alarmieren. Zu den verschiedenen Analyse-Methoden gehören nebst einfachen Regeln auch Korrelations-Modelle, maschinelles Lernen und künstliche Intelligenz. Diese helfen, Beziehungen und Abhängigkeiten zwischen verschiedenen Einträgen herzustellen und potenziell gefährliche Trends und Einträge in Echtzeit zu erkennen und aufzuzeigen.

Data Aggregation

Logdaten verschiedener Systeme werden zusammengezogen und ausgewertet. Dies können Netzwerkgeräte, Firewalls, Server, Datenbanken und Applikationen sein.

Correlation

Die vorhandenen Daten werden zueinander in Beziehung gesetzt und es wird versucht, Verbindungen oder Abhängigkeiten zu erkennen.

Filter

Nur was für das Unternehmen relevant ist, wird weiterverarbeitet. Diese Filter können durch den Lösungsanbieter vorkonfiguriert und durch das Unternehmen angepasst werden.

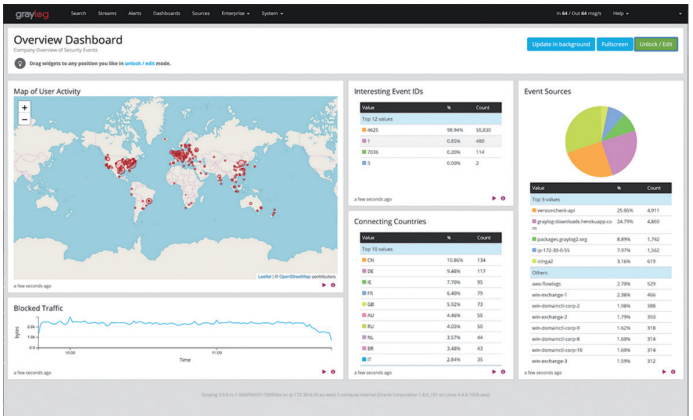

Bild 4: Logauswertung mit Graylog.

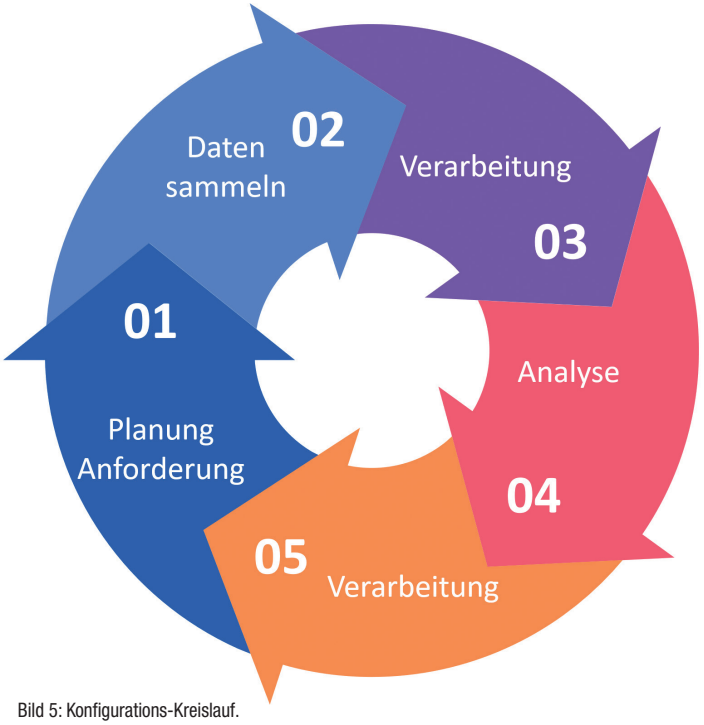

Bild 5: Konfigurations-Kreislauf.

Weitere sollte ein SIEM in der Lage sein, Informationen über einen längeren Zeitpunkt zu sammeln und zu visualisieren, um beispielsweise eine immer länger dauernde Antwortzeiten einer Datenbank festzustellen. Dies kann auch sehr hilfreich sein, wenn ein Hackerangriff erfolgreich war und genauer untersucht wird. Die verschiedenen Daten gilt es auszuwerten und zu bewerten. Zwar kommen die Systeme mit einem Grundset an Regeln. Zwar kann damit schon optimal gestartet werden, aber die Sensoren müssen an die eigene Umgebung angepasst werden. Dies ist eine ständige Aufgabe des Administrators. Ändern sich Elemente im Netzwerk, kommen neue Systeme und Applikationen dazu oder verändern sich die Anforderungen, gilt es die Systeme entsprechend anzupassen (Bild 5).

Gerade Systeme, die auf Anomalien reagieren, können sehr sensitiv reagieren. Solche Abweichungen können beispielsweise Veränderungen in der Bandbreite, Protokollen oder Ports sein.

Damit schnell reagiert werden kann, gilt es die Resultate optimal darzustellen. Eine Ergänzung zum erwähnten Graylog kann hier Icinga sein (Download unter https://icinga.com/). Auch hier gilt es, das Dashboard nach und nach an die eigenen Bedürfnisse anzupassen.

Fazit

Systeme erzeugen an vielen Stellen diverse Logdaten. Mit diesen Daten können Schwachstellen, mögliche Fehler oder Angriffe frühzeitig erkannt und Gegen-Massnahmen ergriffen werden. In der Regel genügt es aber nicht, die Daten auf den Systemen einzeln auszuwerten. In heutigen Umgebungen agieren die Systeme mit vielen anderen. Diese isoliert zu betrachten zeigt kein vollständiges Bild. Ein SIEM sammelt die Daten, bringt diese in einen Zusammenhang und wertet sie aus. Übersichtlich dargestellt bringen die Logdaten einen Mehrwert für jedes Unternehmen. Mit etwas Zeit und Geduld können unerwartete Ereignisse vermieden oder mindestens die Folgen reduziert werden.

INFOS | KONTAKT

goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch