SIEM – Protokollierung und Überwachung

Monitoringsysteme zur Überwachung der Verfügbarkeit und schneller Reaktion auf Probleme sind heutzutage bei allen Unternehmen im Einsatz. Systeme, die die IT-Sicherheit und Policy-Verletzungen überwachen, sind hingegen selten anzutreffen. Die ISO 27001 fordert im Kapitel A.12.4 «Protokollierung» entsprechende Vorgaben. Dieser Artikel gibt eine Einführung in das Thema SIEM und Protokollierung.

Dass eine Firewall, VPN, Antiviren-/Antispam sowie ein grundlegendes Monitoring des Netzwerkes und der Server notwendig sind, weiss jedes Unternehmen und verfügt über die entsprechenden Systeme. Lösungen, die die internen Gefahren im Detail untersuchen, bilden dabei eher die Ausnahme. Gerade bei KMU, wo häufig entsprechende Fachpersonen fehlen oder der administrative Aufwand zu hoch erscheint, fehlen weitergehende Applikationen. Bekannt ist aber allen, dass viele Gefahren nicht nur von aussen kommen, sondern viele werden – absichtlich, unwillentlich oder versehentlich – von innen ausgelöst.

Einen ersten Schritt zur Kontrolle des internen Netzwerks bilden Intrusion Detection/Prevention Systeme (IDS/IPS). Dabei wird ein Sensor im Netzwerk platziert, evtl. auch auf einem Server/Client, und alle Pakete, die über das Netzwerk transportiert werden, werden auf allfällige Abweichungen untersucht. Wird ein schädliches Muster erkannt, wird ein Alarm ausgelöst (IDS) und gegebenenfalls automatisierte Gegenmassnahmen wie das Blocken der Verbindung eingeleitet (IDP). Was sich einfach liest, ist es aber nicht. Solche Systeme müssen aufwendig trainiert werden. Zu Beginn werden viele Fehlermeldungen angezeigt, die gar keine Angriffe sind. Nach einigen Wochen läuft das System dann aber zufriedenstellend. Doch jede Änderung am Netzwerk bedingt eine erneute Anpassung der Sensoren.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

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

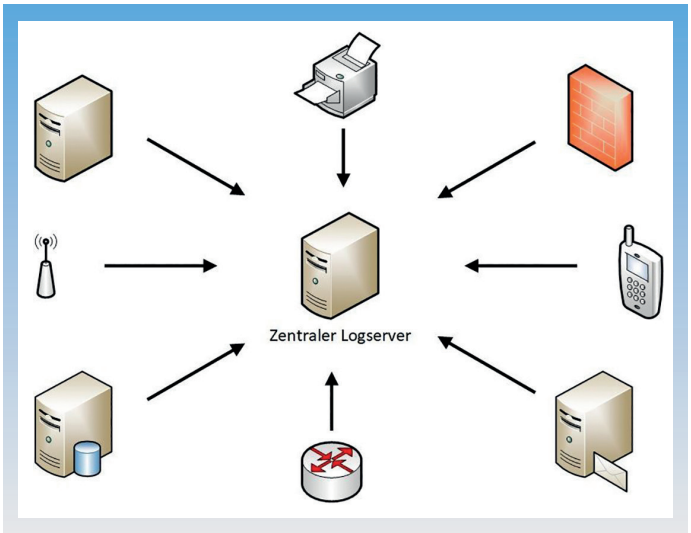

Bild 1: Alle Logdaten müssen zwingend verschlüsselt auf den zentralen Logserver übermittelt werden.

Die nächste Erhöhung der Sicherheit bilden Network-Access-Control-Systeme (NAC). Damit wird verhindert, dass sich unbekannte Geräte am Netzwerk anmelden können. Bei bekannten Geräten werden beim Anmeldeprozess diverse Kontrollen ausgeführt, beispielsweise der Stand des Antivirenprogramms, der Patch-Stand und weitere Richtlinienkonformitäten. Schlägt eine Kontrolle fehl, kann sich das Gerät nicht verbinden und muss zuerst aktualisiert werden. Trotz dieser Möglichkeiten ist dies kein Allheilmittel gegen beliebige Sicherheitsprobleme – unerwünschtes Nutzerverhalten oder Angriffe auf Applikationsebene können damit nicht erkannt werden.

SIEM – Auswerten der Logdaten

Security Information and Event Managementsysteme (SIEM) sammeln relevante Protokoll-, Log- und Ereignisdaten aus verschiedenen Quellen und Bereichen. Das können Netzwerk-Geräte, Server, aber auch Anwendungen sein, weitere typische Quellen sind Firewalls, IDS/IPS, Malware-Software, Web-Server und viele weitere. Die anfallenden Daten werden aggregiert (Verbindung zwischen Daten oder Objekten herstellen, Erstellen von Metadaten) und korreliert (Kombination einzelner Funktionen und Parametern) und danach in Echtzeit analysiert, um mögliche Sicherheitsprobleme zu erkennen und Ereignisse hinsichtlich ihrer Bedeutung einzuordnen.

Bei den SIEM-Systemen gibt es Erweiterungen, die nachfolgend kurz erwähnt sind:

- Security Orchestration, Automation and Response (SOAR): analog von SIEM werden Daten aus verschiedenen Quellen korreliert. Ein SOAR berücksichtigt auch externe Informationen wie Threat-Meldungen von Sicherheitssoftware-Anbietern. Diese Daten ermöglichen ein Gesamtbild darzustellen. Beim SIEM muss der Administrator beim Auftreten eines Alarms selbst entscheiden, welche Schritte einzuleiten sind. Beim SOAR werden die notwendigen Arbeitsabläufe als Reaktion auf bestimmte Sicherheitsvorfälle automatisiert ausgelöst.
- Endpoint (Threat) Detection and Response (DER/ETDR): durch maschinelles Lernen werden die Bedrohungen und Analysen verfeinert. Ebenso werden Schnittstellen wie USB geschützt.
- Extended Detection and Response (XDR): die lokalen Daten werden mit Datenquellen zum Beispiel aus der Cloud kombiniert. Bei einem Angriff kann so ein vollständigeres Bild geliefert und so schneller erkannt und blockiert werden. Weiter kann ein solches System den Angriff zurückverfolgen und diesen nachträglich rekonstruieren. Damit können zentralisierte Konfigurations- und Härtungsfunktionen geplant werden.

Funktionsweise

Jedes System, egal ob Windows, Linux oder Appliance speichert die auftretenden Ereignisse lokal. Diese Daten sollten hier für mindestens drei Wochen aufbewahrt werden. Die Loggrösse muss daher so eingestellt werden, dass ein Überschreiben erst nach dieser Zeit erfolgt. Gleichzeitig wird eine Weiterleitung auf das zentrale SIEM-Tool eingerichtet. Wichtig ist, dass das SIEM bemerkt, wenn über eine bestimmte Zeit keine Daten mehr angeliefert werden und in diesem Fall einen Alarm auslöst. So kann verhindert werden, dass ein Hacker oder Administrator die Logweiterleitung deaktiviert, um unerkannt zu bleiben (Bild 1)

Eine wichtige Voraussetzung ist auch die gemeinsame Systemzeit. Für alle Systeme muss ein zentraler NTP-Dienst verwendet werden. Dieser holt sich die aktuelle Zeit beispielsweise von den Servern ch.pool.ntp.org. Es muss auch darauf geachtet werden, dass die identische Zeitzone, inkl. Sommer-/Winterzeit (Daylight

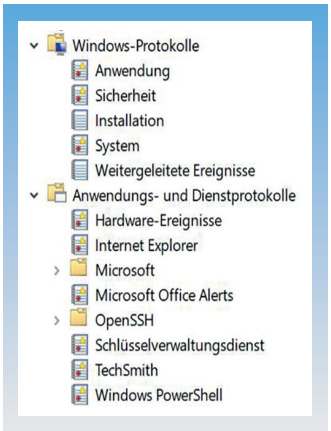

Bild 2: Ereignisanzeige der Logdaten.

Savings Time) verwendet wird. Ansonsten wird die Auswertung unnötig erschwert.

Einmal wöchentlich sind die Log-Daten zu sichten und zu beurteilen. Es müssen Stichproben gemacht werden, um die Richtigkeit der Zugriffe zu bestätigen und mögliche Unregelmässigkeiten zu erkennen. Bei einem allfälligen Sicherheitsvorfall müssen sofort sämtliche Log-Daten gesichert werden.

Logdaten

Windows sammelt seine Logdaten in den sogenannten Eventlogs. Mit der Ereignisanzeige können diese angeschaut werden. Immer mehr Applikationen nutzen ebenfalls diesen Speicherort (Bild 2).

Linux legt praktisch alle Ereignisse in das Verzeichnis /var/log ab. Mit den entsprechenden Tools können diese angezeigt werden. Als Werkzeuge kommen beispielsweise less, more, cat, tail oder grep zur Anwendung. Klassische Log-Daten sind in Bild 3 aufgelistet.

Weitere Orte sind beispielsweise unter https://wiki.ubuntu-users.de/Logdateien/ nachzulesen.

Jede Appliance, wie eine Firewall, ein Router oder ein Switch speichern die Ereignisse je nach Entwickler unterschiedlich ab. Es wird auf das entsprechende Handbuch verwiesen.

Weiterleitung

Für die Weiterleitung von Windows-Log-Daten auf einen anderen Windows-Server können die internen Microsoft-Tools benutzt werden. Für andere Lösungen ist in der Regel eine Zusatzsoftware zu installieren. Diese wird direkt vom Anbieter der SIEM-Lösung angeboten.

Unter Linux kommt 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. Rsyslog ist eine Erweiterung und setzt RELP (Reliable Event Logging Protocol) ein. RELP baut auf TCP auf und ist daher auch mit TLS benutzbar. Eine wichtige Erweiterung von Rsyslog gegenüber Syslog ist, dass es lokale Nachrichten puffern kann, falls der entfernte Server nicht empfangsbereit ist.

Bei Appliances ist dies abhängig von der entsprechenden Applikation und Anbieter.

SIEM-Konfiguration

Die genauen Filter und Baseline Werte müssen in einem separaten Dokument festgehalten werden. Wie die Konfiguration des Filters/Triggers ist auch die Notwendigkeit zu beschreiben.

Wichtig ist es, die Konfiguration über das Backup zu sichern. Änderungen an der Konfiguration des SIEM müssen stets in der Konfigurationsdokumentation nachgeführt werden.

Die gesamte Konfiguration des SIEM muss unmittelbar nach jeder Änderung gesichert werden. Die Aufbewahrung hat gemäss den Vorgaben im Backup-Konzept zu erfolgen. Zusätzlich muss unmittelbar vor einem Update eine Sicherung durchgeführt werden. Das Vorgehen bei einer Wiederherstellung muss in einem Notfallplan dokumentiert werden.

Ort	Verwendung
/var/log/messages	Generelle Meldungen, inkl. System
/var/log/auth.log	Authentifizierung
/var/log/kern.log	Kernel
/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 3.

Bild 4: Folgende Schritte durchlaufen die Logdaten.

Funktionsweise

Die Logdaten durchlaufen, wie bereits weiter oben beschrieben folgende Schritte (Bild 4):

- Aggregation: Logdaten verschiedener Systeme werden zusammengezogen und ausgewertet. Dies können Netzwerkgeräte, Firewalls, Server, Datenbanken und Applikationen sein.
- Korrelation: Die vorhandenen Daten werden zueinander in Beziehung gesetzt und es wird versucht, Verbindungen oder Abhängigkeiten zu erkennen.
- Filtern: Nur was für das Unternehmen relevant ist, wird weiterverarbeitet. Diese Filter können durch den Lösungsanbieter vorkonfiguriert und durch das Unternehmen angepasst beziehungsweise erweitert werden.
- Reports I Dashboard: Die automatische Auswertung löst einen Alarm aus. Dies kann auf ein Dashboard oder auch per E-Mail usw. erfolgen.

Neben kostenpflichtigen Lösungen gibt es auch kostenlose Alternativen. So hat sich Graylog https://www.graylog.org/ einen guten Namen gemacht. Die obenstehenden Anforderungen können damit umgesetzt werden. Nach etwas Einarbeitungszeit steht ein mächtiges Werkzeug zur Auswertung von Logdaten und schneller Reaktion zur Verfügung.

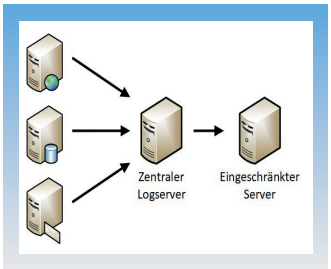

Bild 5: Auf den eingeschränkten Server dürfen die Administratoren keinen Zugriff haben.

Schutz der Logdaten

Administratoren benötigen auf dem zentralen Logserver erweiterte Rechte, um das System zu unterhalten und die Regeln zu erweitern und anzupassen. Damit die Anforderungen aus ISO 27001 A.12.4.3 (Tätigkeiten von Systemadministratoren und Systembedienern werden aufgezeichnet und die Protokolle sind geschützt und werden regelmässig überprüft) ebenfalls erfüllt werden können, ist ein zusätzliches eingeschränktes System notwendig (Bild 5).

Auf den eingeschränkten Server dürfen die Administratoren keinen Zugriff haben. Idealerweise wird der Zugriff nur dem CISO erlaubt, welcher auf dem zentralen Logserver maximal Leserechte besitzt.

Fazit

Unternehmen haben erkannt, dass der Schutz der eigenen Infrastruktur wichtig ist. Firewalls, Antiviren-Lösung, Anti-Spam, wie auch ein Monitoring-System sind praktisch überall vorhanden. Ein SIEM ist eine wichtige Erweiterung, um bereits kleinste Anomalien zu erkennen und schnell reagieren zu können. Weiterentwicklungen wie SOAR und XDR ermöglichen den Einbezug von externen Datenbanken, um automatisierte Gegenmassnahmen einzuleiten. Auch wenn der Initialaufwand hoch ist, sollte sich jedes Unternehmen mit SIEM auseinandersetzen.