Cyber Monitoring

Daten sind Grundlage für Sicherheit

Schlagzeilen wie «Webseite von Genfer Schifffahrtsgesellschaft gehackt» häufen sich: Die digitale Wirtschaft wird zum Ziel von Kriminellen. Die Schäden übersteigen oftmals die Kosten des Schutzes.

→ VON MATHEW THEKKEKARA

DER AUTOR

Mathew Thekkekara
ist Teamleiter für Log-Management und Cyber Security bei Securix.
→ www.securix.ch

Sicherheitsvorkehrungen haben typischerweise ein Ziel: Die Daten, die ein Unternehmen nicht nur über seine Kunden, sondern auch über den Zustand der eigenen IT-Systeme sammelt. Diese Informationen geben meist auch Auskunft darüber, ob Hacker am Werk waren oder sind. So bildet das sorgfältige Erfassen dieser Daten die Grundlage für das Cyber Monitoring sowie für die dazu gehörenden Abwehr- und Schutzmassnahmen.

Ähnlich wie die Videoaufzeichnung für die Gebäudesicherheit eignet sich das Log-Management für die Sicherheit der IT-Infrastruktur. Beim Log-Management geht es um die Aufzeichnung und Aufbewahrung von Ereignissen aus der IT-Umgebung. Ohne diese Überwachungsgrundlage kann keine Aussage zur effektiven Sicherheit der Umgebung getroffen werden.

HERSTELLERNEUTRAL UND SKALIERBAR

Idealerweise werden die gesammelten Daten innerhalb der Organisation für verschiedene Analysezwecke bereitgestellt. Je grösser ein Unternehmen, desto wahrscheinlicher ist die Verwendung unterschiedlicher Applikationen für Analysen. Bei Tausenden von Applikationen für Datenanalysen ist dies auch keine Überraschung. Damit sollte die zentrale Log-Aufbewahrungsstelle eine einfache Möglichkeit bieten, Applikationen anzubinden und die Daten daraus zu benutzen. Da diese zentrale Stelle letztendlich eine wichtige Rolle für die Cybersicherheit übernimmt, sollten die Herstellerunabhängigkeit und Skalierbarkeit nicht vernachlässigt werden. Die Herstellerunabhängigkeit kann durch den Einsatz von Open-Source-Technologien, die weltweit genutzt und über offene Dokumentationen verfügen, verringert werden. Auch die Sicherheitsgewährleistung an weit genutzten Open-Source-Technologien sind höher, weil ihr Quellcode öffentlich einsehbar ist und so die Fehler schneller gemeldet und behoben werden können. Bei der Skalierbarkeit sollte der Fokus einerseits auf der zentralen Stelle liegen, die mehr Daten in Zukunft aufbewahren kann, andererseits aber auch bei den Consumern und Producern, welche die Daten liefern und nutzen. Nur so können potenzielle Engpässe beim Sammeln von Protokollen aus der Quelle und beim Verbinden mit unterschiedlichen Analyseanwendungen vermieden werden.

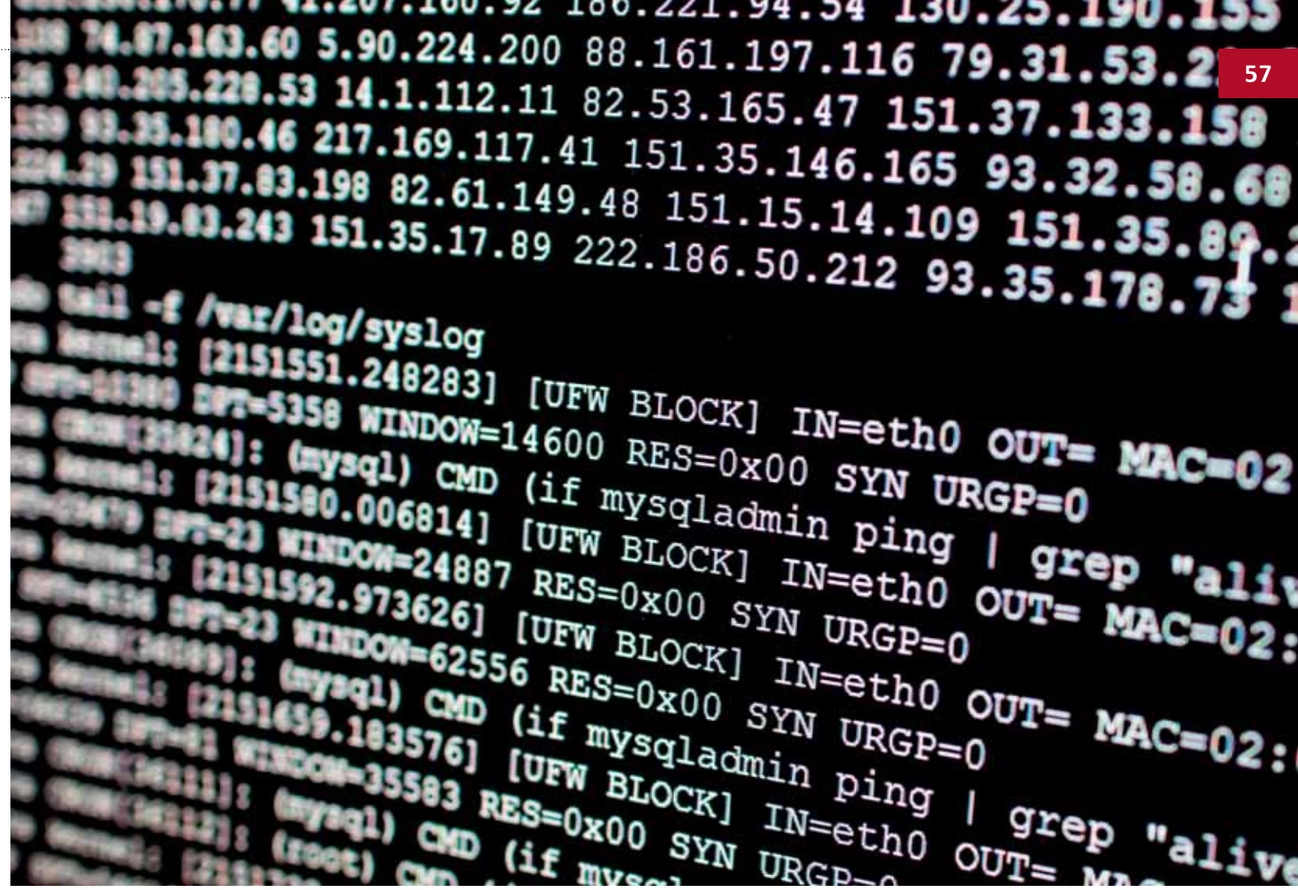
> «Log-Daten geben Auskunft darüber, ob Hacker am Werk waren oder sind»
>
> Mathew Thekkekara

FORENSISCHE ARBEITEN

Bei der Log-Forensik geht es um die Nachvollziehbarkeit. Dies dient nicht nur dazu, einen Schuldigen zu finden, sondern schafft auch Entlastung. Der Schwerpunkt liegt auf der Untersuchung von Angriffsmethoden und Betroffenheit. Nach einem Angriff ist es essenziell zu erfahren, wie dieser sich ereignete. Wichtig ist es dabei, auf eine leistungsfähige Analysemöglichkeit zählen zu können, welche die Wartezeiten reduziert und das Benutzer-Feeling verbessert. Nur so können alle Log-Daten, die zu diesem Zeitpunkt aufgezeichnet wurden und zu diesem Angriff gehören, in einer Timeline abgebildet werden. So kann der Vorfall einer Schritt-für-Schritt-Analyse unterzogen werden, um die Angriffstaktiken nachzuvollziehen. Dadurch kann eine korrekte Sicherheitsoptimierung durchgeführt werden, um die Verbesserung der IT-Security zu gewährleisten.

SIEM FÜR CYBER MONITORING

Beim Security Information und Event Management (SIEM) geht es um eine aktive Cyber-Security-Überwachung aller aktuell gesammelten Daten. Dabei werden die Daten aus den unterschiedlichen Quellen korreliert, um eine ganzheitliche Sicht auf die gesamte IT-Infrastruktur und deren Sicherheit zu erhalten. Nun können komponenten- und produktübergreifende Checks durchgeführt werden, die ohne Korrelationen der unterschiedlichen Quellen nicht möglich wären. Die bereits vorhandenen Standardüberwachungen liefern eine gute Basis, um fortgeschrittene Gefahrenmuster aufzuspüren und die jeweiligen Verantwortlichen zu alarmieren. Zusätzlich können umgebungsspezifische Überwachungen eingerichtet werden, um einen detaillierten Sicherheitsüberblick zu erhalten. Es gibt nur sehr wenige Situationen, in denen nur eine Überwachung zur gleichen Zeit einen Alarm auslöst. Daher sollten Warnungen nach ihrer Kritikalität kategorisiert und den Verantwortlichen zur weiteren Analyse zur Verfügung gestellt werden. Nun kann der Analyst die Indikatoren hinter den Alarmen analysieren und entsprechende Massnahmen vornehmen. Ein wichtiger Teil zum SIEM ist der 24/7-Betrieb dieser Lösung. Denn Gefahren existieren auch ausserhalb der Bürozeiten. Der Betrieb einer SIEM-Lösung wird dadurch oft auch innerhalb eines externen SOC übergeben.



Anhand der Log-Daten analysieren Firmen allfällige Cybervorfälle in ihrem Netz

XDR UNTERSTÜTZT CYBERSPEZIALISTEN

Zu den bereits überlasteten Analysten kommt noch die Tatsache dazu, dass ein Mangel an Cyber-Security-Spezialisten besteht. An dieser Stelle kommt das «Extended Detection and Response» (XDR) zum Einsatz. Das XDR macht an der Stelle weiter, wo SIEM die Analyse beendet und den Alarm den Cyberspezialisten meldet. Sobald die von SIEM generierten Alerts verfügbar sind, kann die XDR Abwehroptionen anzeigen, Analysten eine Entscheidungsgrundlage liefern oder Abwehrmechanismen direkt auslösen. Durch Massnahmen wie das Stoppen von Prozessen oder Blockieren von Benutzern kann die Gefahr eingedämmt und der Normalzustand wiederhergestellt werden. Die zusätzlichen Optionen für die Verteidigung und auch das direkte Ausführen der Abwehr unterstützen somit die Cyberspezialisten bei der Ausübung ihrer Arbeit. Für eine nachträgliche Kontrolle werden die getätigten Defence-Aktivitäten protokolliert und den Analysten zur Verfügung gestellt.

KI-HILFE IN DER CYBERSECURITY

Immer mehr Überwachungssysteme profitieren von wissenschaftlichen Fortschritten in der Forschung im Bereich der künstlichen Intelligenz (KI). Die zu analysierende Datenmenge nimmt exponentiell zu und die Methoden der Cyberangreifer werden immer komplexer. Eine KI unterstützt, indem sie den Normalzustand erkennt und bei Abweichungen Alarme auslöst. Diese können zusätzlich zu den vorhandenen Überwachungen, auf Basis von Angriffsmethoden, auch Gefahren erkennen, deren Methoden noch unbekannt sind. Weiterhin können auch Applikationen wie CuriX genutzt werden, um auf Basis von KI Analysen zu erstellen und anschliessend auch Gegenmassnahmen einzuleiten. Dann sprechen wir bereits von der Responsefähigkeit der Umgebung.

ZUSAMMENFASSUNG

Oft schaffen es attackierte Firmen nicht, nach Angriffen rasch zu reagieren und die betroffenen Kundinnen und Kunden zu informieren. Grund sind oftmals die nicht rechtzeitig erfassten Daten. Durch die Aufzeichnung und Aufbewahrung der Log-Daten können die notwendigen Informationen für eine überlegene Cyberabwehr gelegt werden. Diese Daten können zur forensischen Analyse der Angriffe und für laufende Cyberüberwachungen genutzt werden.

Und die Zukunft wird zweifellos noch mehr Daten bringen. Es ist die Aufgabe der IT-Sicherheitsspezialisten, diese zu analysieren und die notwendigen Schlüsse daraus zu ziehen. Nur so können die richtigen Gegenmassnahmen zur Aufrechterhaltung der Daten- und Infrastruktursicherheit eingeleitet werden. ←

Bilder: Shutterstock/Paolo De Gasperis, Securix