Was Security-Monitoring heute können muss

Das Monitoring der IT-Sicherheit ist ein wichtiger Eckpfeiler in der Security-Strategie jeden Unternehmens. Richtig aufgesetzt, erlaubt es nicht nur unberechtigte Zugriffe und Angriffe zeitnah zu erkennen, auch Compliance-Anforderungen lassen sich damit schnell und einfach prüfen. Doch trotz fortschrittlicher Technologie und professioneller Sicherheitslösungen bleibt das Monitoring eine große Herausforderung für viele Unternehmen. Zu oft reißen lückenhafte Überwachung und mangelnde Verknüpfung von Sicherheitsinformationen blinde Flecken in die Kontrolle. Worauf ist also bei der Auswahl einer Monitoring-Lösung zu achten?

Von Stefan Mutschler, freier Fachjournalist für AMPEG

Die IT-Systeme in Unternehmen werden immer komplexer und vernetzter. Neue Technologien wie Cloud-Computing, mobile Geräte und das Internet of Things (IoT) stellen neue Anforderungen an das Monitoring der IT-Sicherheit. Es wird zunehmend schwieriger, sämtliche Ereignisse im Netzwerk zu erfassen und zu analysieren. Die steigende Anzahl an Datenquellen und -formaten erschwert die Integration und Korrelation von Informationen.

It doesn't matter until you measure it. And if it doesn't matter, you shouldn't measure it.

Ein weiteres Problem beim Monitoring der IT-Sicherheit ist die fehlende Integration von Sicherheit und Compliance. Viele Unternehmen sehen die Einhaltung gesetzlicher Vorschriften als separate Aufgabe an, die nichts mit der IT-Sicherheit zu tun hat. Das führt dazu, dass Sicherheitsmaßnahmen oft nur auf die Einhaltung von Compliance-Vorgaben ausgerichtet sind und nicht auf die tatsächlichen Sicherheitsrisiken. Auch mit der Cloud kommen häufig unterschätzte Risiken ins Unternehmen. Oft fehlt es an Transparenz und Kontrolle über die Cloud-Infrastruktur und die Daten, die in der Cloud gespeichert werden. Das macht es schwierig, eine umfassende Sicht auf die Sicherheitslage des Unternehmens zu bekommen.

Sicherheitsstatus kontinuierlich im Griff: SLM statt SIEM

Mit kontinuierlichem Monitoring können CISOs, beziehungsweise IT-Teams den Sicherheitsstatus von IT-Netzwerken jederzeit überprüfen und sicherheitsrelevante Fehlkonfigurationen in Echtzeit erkennen. Das macht die operative Sicherheit zu einer messbaren und steuerbaren Größe. Somit lassen sich Sicherheitslücken und Handlungsbedarfe zeitnah identifizieren. Diese Sicherheitsmaßnahmen können langfristig analysiert und aktiv gesteuert werden, um dem Risikoappetit des Unternehmens gerecht zu werden. Dieses Verfahren wird als Security-Level-Management (SLM) bezeichnet.

SLM unterscheidet sich von reaktiven Security-Information-and-Event-Management-(SIEM)-Lösungen, die durch die Korrelation von zentral gesammelten Log-Daten Sicherheitsvorfälle nachträglich erkennen und den IT-Betrieb beim Troubleshooting unterstützen. Im Gegensatz dazu erkennt SLM mögliche Abweichungen von Vorgaben und Sicherheitslücken proaktiv, bevor ein Sicherheitsvorfall eintritt. Dadurch kann die Angriffsfläche rechtzeitig minimiert werden. Korrekturmaßnahmen lassen sich mittel- bis langfristig umsetzen. SLM passt perfekt zu den einschlägigen Standards und Normen wie PCI DSS (Anforderungen 5 und 6), BSI Kriterienkatalog C5 (OPS und PSS) und der ISO 27001, die auf dem Plan-Do-Check-Act-Zyklus basieren. Mit seinem Ansatz, Abweichungen und Sicherheitslücken aufzuzeigen, bietet SLM eine umfassende und präventive IT-Sicherheitslösung.

Schneller Überblick über die Sicherheitslage

Die Fragen, die Unternehmen zur Feststellung der Sicherheitslage in ihrer IT haben, folgen einer typischen Charakteristik. Vieles sind Standardfragen, die sich häufig

wiederholen. Daher ist es sehr hilfreich, wenn ein Monitoringsystem eine möglichst große Zahl der entsprechenden Auswertungen gleich mitbringt, etwa in Form von Landkarten, Listen und Diagrammen. Sie liefern direkt Antworten auf wichtige Fragen, wie zum Beispiel wo aktuell das größte Risiko im Netz besteht, welche Lokationen oder Geschäftsbereiche regelkonform arbeiten oder eben nicht, welchen Sicherheitsstatus kritische Systeme haben, ob Schwachstellen erfolgreich geschlossen wurden und ob sich die Sicherheitslage langfristig verbessert hat.

Die Liste der Auswertungen lässt sich beliebig erweitern. Weitere typische Analysen stellen etwa fest, welche mobilen Geräte nicht regelkonform eingerichtet sind, wie gut das Sicherheitsniveau der Systeme aus der Produktion ist, welche Netzwerkgeräte eine veraltete Firmware-Version haben, welche Updates auf welchen Systemen noch nicht installiert wurden und welche Schwachstellen aus dem CVE-Catalogue davon betroffen sind sowie vieles mehr. Wenn das System die ermittelten Daten über einen längeren Zeitraum speichert, lassen sich Langzeitanalysen durchführen, idealerweise über mehrere Jahre. Das erleichtert die Optimierung von Prozessen enorm.

Ein großer Pool an Standardauswertungen erlaubt es, Analysen ohne manuelles Einstellen von Sicherheitsinformationen zu starten. Die Analyse des Sicherheitsstatus etwa kann so durch das Hinzufügen der Auswertungen an der Managementkonsole sofort beginnen. Individuelle Anpassungen sollten durch die Anpassung von Grenz- und Schwellenwerten, Kategorien, Filtern und Unternehmensstandorten möglich sein. Damit wird der Aufwand zur Erstellung von detaillierten Auswertungen minimiert. Ein zentrales Management-Dashboard erleichtert die Aufgabe zusätzlich.

Der Nutzen wird auch schnell deutlich, wenn beispielsweise Wirtschaftsprüfer sich ankündigen, um einen Blick auf das Sicherheitsniveau eines Unternehmens zu werfen. Wo früher Hektik und Nervosität ausbrach, können Sicherheitsteams die gefragten Informationen sofort und in anschaulicher Form anbieten. Auch Reports lassen sich schnell und zielgruppengerecht erstellen. All dies erleichtert Audits erheblich. Auf europäischer Ebene wird besonders durch die NIS-2-Richtlinie (IT-SiG 2.0) auf die Auswertung des Sicherheitsstatus auf Basis der Erfassung aller technischen Komponenten hingewiesen.

Wie system- und herstellerübergreifende Korrelation funktioniert

Wichtig ist, dass die Analysen übergreifende und herstellerunabhängige Informationen aus verschiedenen Sicherheitsbereichen bieten. Dadurch können Korrelationen zwischen diesen Informationen hergestellt werden, um eine übergreifende Aussage zum Stand des Sicherheitsniveaus zu erhalten. Damit das gelingen kann, ist es wichtig, dass möglichst viele Hersteller von Sicherheitssystemen mit dem Monitoring verbunden sind. Praktischerweise werden dafür Konnektoren oder Kollektoren eingesetzt. Sie speisen die Informationen in das Monitoring ein. Großer Vorteil solcher Kollektoren: Flexibel je nach Bedarf ergänzt, können blinde Flecken im Monitoring ausgemerzt werden.

Die gesammelten Informationen aus verschiedenen Bereichen werden für das übergreifende Monitoring und Reporting sowie für die Datenkorrelation verarbeitet. Ein Beispiel: Sind das Active Directory (AD), ein Update-Management, ein Virenschutz und ein Schwachstellenscanner an das Monitoring angebunden, können durch die Korrelation der Informationen unter anderem jene Rechner ermittelt werden, die entweder keinen Virenschutz besitzen oder nicht in das Update-Management integriert sind.

Globale Sicht: Vogelperspektive mit Lupenfunktion

Was im Monitoring keinesfalls fehlen sollte: ein Regelwerk, das den Sicherheitsstatus nach den individuellen Vorgaben des Unternehmens bewertet. Die Darstellung des ermittelten Sicherheitsstatus erfolgt am einfachsten mittels einer Ampelfunktion. Neben Tortendiagrammen, die durch Listen ergänzt werden, ist eine Übersichtslandkarte, welche die Sicherheitsinformationen in einer geografischen Darstellung präsentiert, eine sinnvolle Ergänzung. Eine Sicherheitsinformationskarte ermöglicht es, Schwachpunkte im Netzwerk schnell und effektiv zu identifizieren. Ein Klick auf eine geografische Region oder einen Standort zeigt detaillierte Informationen zum aktuellen Status des Netzwerks an. Die Karte trägt ebenfalls dazu bei, die Wirksamkeit der IT-Sicherheit zu erhöhen.

Fazit

Das Monitoring der IT-Sicherheit ist ein unverzichtbarer Bestandteil des Sicherheitsmanagements in Unternehmen. Es dient dazu, mögliche Angriffspunkte zu erkennen, zu analysieren und zu bekämpfen. Unternehmen, die auf ein professionelles Monitoring der IT-Sicherheit setzen, können wirtschaftliche Schäden vermeiden und gesetzliche Anforderungen erfüllen. ■