Wie kontinuierliches Security-Monitoring die Cyberverteidigung stärkt

Die Abwehr von Cyberbedrohungen steht im Fokus der Security-Strategie jedes Unternehmens. Ein effektives Monitoring der IT-Sicherheit sollte dabei eine zentrale Rolle spielen. Eine wirksame Erhöhung der Widerstandsfähigkeit des gesamten Netzwerks ist jedoch nur möglich, wenn die Monitoring-Lösung eine umfassende Informationsbasis herstellt und die gewonnenen Sicherheitsinformationen intelligent verknüpft.

Von Stefan Mutschler, freier Fachjournalist aus Bad Endorf

Nichts ist bedrohlicher als das Unbekannte. Das gilt ganz besonders auch für Cyberangriffe – Unternehmen, die keinen umfassenden Überblick haben, was in ihrem Netzwerk passiert, sind ein leichtes Opfer und können immer nur reaktiv tätig werden. Proaktive Cyberabwehr erfordert kontinuierliches Monitoring aller Assets, um über alle Vorgänge im Netzwerk umfassend im Bilde zu sein. Nur so können Chief Information Security Officers (CISOs) und SOC-Teams den Sicherheitsstatus von IT-Netzwerken jederzeit im Blick behalten und Schwachpunkte in Echtzeit erkennen. Kontinuierliches Monitoring macht die operative Sicherheit mess- und steuerbar, indem es Sicherheitslücken und Handlungsbedarf zeitnah identifiziert und langfristig analysiert.

It doesn't matter until you measure it.

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

Was kontinuierliches Security-Monitoring ausmacht

Kontinuierliches Monitoring ist ein umfassender Ansatz zur Optimierung der Cybersicherheit, der verschiedene essenzielle Aspekte umfasst. Zunächst einmal beinhaltet es das Sammeln von Sicherheitsinformationen. Das bedeutet, dass kontinuierlich Daten über den Zustand von Systemen, Netzwerken und Anwendungen in einem zentralen Pool zusammenlaufen – angesichts der Vielfalt an Datenquellen und -formaten eine anspruchsvolle Aufgabe. Diese Informationen werden dann intelligent ausgewertet, um Abweichungen vom erforderlichen Sicherheitsniveau zu identifizieren.

Dies führt zum zweiten Kernaspekt des kontinuierlichen Monitorings – die Erkennung von Schwachpunkten im Netzwerk. Für eine wirkungsvolle Cyberabwehr ist es unerlässlich, potenzielle Abweichungen von Sicherheitsstandards und Lücken zu erkennen, bevor ein Sicherheitsvorfall auftritt. Sichtbarkeit und Transparenz der Schwachpunkte im Netzwerk wiederum bilden die Voraussetzung für den dritten Faktor eines zeitgemäßen Monitorings – die Umsetzung proaktiver Maßnahmen, um potenzielle Risiken zu minimieren. Dies kann die Isolierung von betroffenen Systemen, das Patchen von Sicherheitslücken oder andere Abwehrmaßnahmen umfassen.

Schließlich zielt kontinuierliches Monitoring darauf ab, das Schutzschild zu stärken, um die Angriffsfläche zu reduzieren. Dabei geht es um die fortlaufende Verbesserung von Sicherheitsmaßnahmen und -richtlinien, um die Widerstandsfähigkeit des gesamten Netzwerks gegenüber potenziellen Bedrohungen zu erhöhen. Auf diese Weise ist kontinuierliches Monitoring essenzieller Baustein von Sicherheitsarchitekturen, wie sie durch einschlägige Standards und Gesetze (PCI DSS, BSI Kriterienkatalog C5, ISO 27001, NIS2 etc.) gefordert werden.

Wichtig: system- und herstellerübergreifende Korrelation

Ziel des Monitorings ist es also, umfassende Informationen aus verschiedenen Sicherheitsbereichen zu sammeln und zu analysieren, um eine ganzheitliche Aussage über das Sicherheitsniveau zu ermöglichen.

Ein entscheidender Punkt ist dabei, dass die Analysen herstellerunabhängige Informationen aus unterschiedlichen Sicherheitsbereichen bieten sollen. Das bedeutet, dass die Sichtbarkeit nicht auf Produkte eines bestimmten Herstellers beschränkt ist, sondern verschiedene Sicherheitssysteme einbezieht. Dies ermöglicht die Korrelation von Informationen, um ein umfassendes Bild des Sicherheitszustands zu erhalten.

Damit das effektiv funktioniert, ist es wichtig, dass möglichst viele Hersteller von Sicherheitssystemen mit dem Monitoring verbunden sind. Hier kommen Konnektoren oder Kollektoren ins Spiel. Diese Tools dienen dazu, Informationen von verschiedenen Sicherheitssystemen in das Monitoring-System einzuspeisen. Ein großer Vorteil solcher Kollektoren liegt in ihrer Flexibilität, da sie je nach Bedarf ergänzt werden

können, um eventuelle „blinde Flecken“ im Monitoring zu beheben.

Die gesammelten Informationen aus verschiedenen Sicherheitsbereichen werden dann für das übergreifende Monitoring und Reporting sowie für die Datenkorrelation verarbeitet. Ein Beispiel: Sind das Active Directory (AD), ein Update-Management, ein Endpoint-Detection-and-Responce-(EDR)-System und ein Schwachstellenscanner an das Monitoring angebunden, können durch die Korrelation der Informationen unter anderem jene Rechner ermittelt werden, die entweder keinen EDR-Agent besitzen oder nicht über die aktuellen Updates verfügen.

Übergreifendes Monitoring der IT-Sicherheit bietet also einen umfassenden Einblick in den Sicherheitsstatus eines Systems oder Netzwerks, indem es verschiedene Sicherheitsaspekte integriert und miteinander in Beziehung setzt. Dies trägt dazu bei, Schwachpunkte zu identifizieren, Sicherheitsrisiken zu minimieren, um die Angriffsfläche zu verkleinern.

Was Auswertungen für die Cyberdefense bedeuten

Königsdisziplin im Monitoring ist eine aussagekräftige Auswertung aller Daten. Die Auswertungen eines kontinuierlichen Monitorings sind vielfältig. So lässt sich beispielsweise feststellen, wo aktuell das größte Risiko in Netz besteht, welche Lokationen oder Geschäftsbereiche regelkonform arbeiten oder eben nicht, welchen Sicherheitsstatus kritische Systeme haben, welche mobilen Geräte nicht konform eingerichtet sind, wie sicher die Systeme in der Produktion sind, welche Netzwerkgeräte veraltete Firmware verwenden, welche Updates fehlen oder welche Schwachstellen aus dem CVE-Katalog betroffen sind. Ein längerfristiges Speichern der erfassten Daten ermöglicht Langzeitanalysen über Jahre hinweg, was die kontinuierliche Verbesserung von Sicherheitsprozessen enorm unterstützt.

Ein breites Spektrum an Standardauswertungen erlaubt Analysen ohne manuelles Erstellen von Sicherheitsinformationen. Anwender können sofort mit der Analyse des Sicherheitsstatus beginnen, wenn entsprechende Auswertungen einem Security-Dashboard hinzugefügt werden. Darüber hinaus sollte das System individuelle Anpassungen ermöglichen, beispielsweise durch Anpassung von Grenzwerten, Filtern und Kategorien, um detaillierte Auswertungen zu erstellen und den Aufwand hierfür zu minimieren.

Die praktische Relevanz zeigt sich auch, wenn Wirtschaftsprüfer einen Blick auf das Sicherheitsniveau eines Unternehmens werfen. Mit einem gut aufgestellten Monitoring-System können Sicherheitsteams geforderte Informationen sofort und ansprechend präsentieren, was Audits erheblich erleichtert. Die NIS2-Richtlinie auf europäischer Ebene betont insbesondere die Bewertung des Sicherheitsstatus anhand der Erfassung aller technischen Komponenten.

Die Darstellung machts

Die Darstellung des ermittelten Sicherheitsstatus gestaltet sich am einfachsten durch die Integration einer Ampelfunktion. Diese visuelle Darstellungsweise ermöglicht es, auf einen Blick den aktuellen Sicherheitszustand zu erfassen. Parallel dazu bieten sich ergänzende Darstellungsformen an, wie zum Beispiel simple Tortendiagramme, die durch listenbasierte Informationen erweitert werden. Eine besonders sinnvolle Ergänzung stellt zudem eine Übersichtslandkarte dar, welche die Sicherheitsinformationen in einer geografischen Darstellung präsentiert.

Die Einführung einer Sicherheitsinformationskarte ist in diesem Zusammenhang äußerst empfehlenswert, da sie es erlaubt, Schwachpunkte im Netzwerk auf eine schnelle und effektive Weise zu identifizieren. Durch einen einfachen Klick auf eine geografische Region oder einen spezifischen Standort erhält man detaillierte Informationen zum aktuellen Status des Netzwerks. Diese kartografische Darstellung trägt nicht nur zur effizienten Identifikation von Schwachstellen bei, sondern fördert auch die Transparenz und Verständlichkeit der Sicherheitslage.

Durch diese visuellen Hilfsmittel wird eine schnelle sowie eine präzise Bewertung des Sicherheitsstatus ermöglicht, was letztendlich dazu beiträgt, die Cyberverteidigung und die Gesamtsicherheit des Unternehmens zu stärken.

Fazit

Der maßgebliche Wert eines kontinuierlichen Security-Monitorings für die Cyberverteidigung besteht nicht nur darin, bereits erfolgte Angriffe zu detektieren, sondern vor allem präventiv mögliche Schwachpunkte und Sicherheitslücken zu erkennen. Durch die kontinuierliche Beobachtung von Netzwerken, Systemen und Datenströmen ermöglicht das Monitoring der IT-Sicherheit eine proaktive Herangehensweise, um Schwachstellen im Netzwerk frühzeitig zu identifizieren und effektive Gegenmaßnahmen zu ergreifen.

Damit verbessert das Monitoring der IT-Sicherheit nicht nur den Schutzschild gegen potenzielle Bedrohungen, sondern leistet auch einen entscheidenden Beitrag zur wirtschaftlichen Stabilität und rechtlichen Konformität von Unternehmen. In einer zunehmend vernetzten und digitalisierten Geschäftswelt ist ein ganzheitlicher Ansatz für die IT-Sicherheit von grundlegender Bedeutung, und das kontinuierliche Monitoring spielt dabei eine Schlüsselrolle. ■