Automatisierte Bedrohungserkennung mit ScanBox

Die Umsetzung der NIS-2-Richtlinie ist oft komplex und ressourcenintensiv. Die ScanBox von DECOIT bietet eine einfache, skalierbare Lösung zur Angriffserkennung. Sie erleichtert die Einhaltung der Vorgaben durch intelligente Analyse und Expertenunterstützung.

Von Michael Schulte, freier Redakteur in München

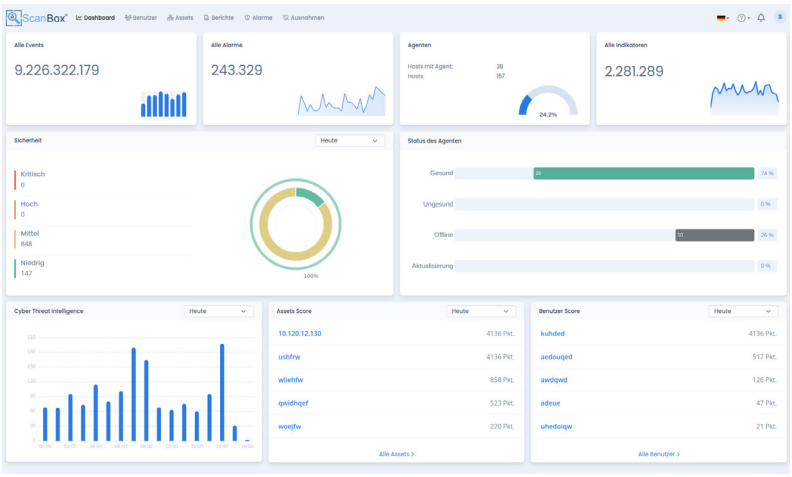
Die NIS-2-Richtlinie stellt eine umfassende Erweiterung der bisherigen Cybersicherheitsvorgaben dar. Die Umsetzung der Richtlinie verläuft vielerorts schleppend, auch in Unternehmen der kritischen Infrastruktur. Gründe sind unter anderem der hohe Zeitaufwand, die komplexen Anforderungen und der Fachkräftemangel. Vor diesem Hintergrund setzen viele Unternehmen auf technische Lösungen, die sie bei der Einhaltung der Vorgaben unterstützen.

Eine Möglichkeit zur Umsetzung der NIS-2-Anforderungen sind automatisierte Systeme zur Angriffserkennung und Netzwerküberwachung. Die ScanBox von DECOIT ist ein Beispiel für ein solches Werkzeug. Sie analysiert Netzwerkverkehr und Systemprotokolle, um Sicherheitsvorfälle frühzeitig zu erkennen.

„Die ScanBox wurde als unkompliziertes, skalierbares System zur Angriffserkennung entwickelt und nutzt als Basis aktuelle Bedrohungsdaten, um verdächtige Muster und Anomalien frühzeitig zu identifizieren“, zeigt Geschäftsführer Prof. Dr. Kai-Oliver Detken auf. Eine proaktive Verteidigung durch die schnelle Bedrohungserkennung und geeignete Gegenmaßnahmen werden ermöglicht. Durch die Anomalie-Erkennung werden Compliance-Abweichungen identifiziert und die Anzahl an „False Positives“ erheblich reduziert. Die zentrale Benutzeroberfläche der ScanBox (www.scanbox-product.de) ermöglicht proaktives Handeln ohne tiefergehendes Sicherheits- oder Clustermanagementwissen. Die Kombination aus benutzerfreundlicher Web-App und direktem Zugang zu Security-Analysten stellt ein Alleinstellungsmerkmal dar und ermöglicht eine erhebliche Zeit- und Personalentlastung.

Die ScanBox braucht nicht permanent an einen Mirror-Port angeschlossen werden, da die Switches zu sehr belastet werden und wertvolle Analysedaten verloren gehen können. Dafür wird bei der Netzwerkanalyse auf das Protokoll NetFlow gesetzt. Bei der Logfile-Analyse werden entsprechende Agenten auf den Client- und Serversystemen ausgerollt, die zusätzlich einen Anti-Viren-Schutz mitbringen. Die Kombination verschiedener Datenquellen verschafft ein Gesamtbild der Bedrohungslage. Ein Experten-Team steht immer direkt und persönlich zur Verfügung.

Die Umsetzung der NIS-2-Richtlinie stellt Unternehmen vor organisatorische und technische Herausforderungen. Analysewerkzeuge wie die ScanBox können eine Möglichkeit darstellen, die Einhaltung der gesetzlichen Vorgaben zu erleichtern und gleichzeitig Sicherheitsrisiken zu minimieren. Die ScanBox ist gerade für solche Unternehmen attraktiv, die keine High-End-Lösungen benötigen, aber die gesetzlichen Anforderungen der NIS-2-Richtlinie erfüllen müssen. ■



Das Dashboard zeichnet sich durch Benutzerfreundlichkeit und Übersichtlichkeit aus. Per Alarmfunktion wird der IT-Administrator unverzüglich über Anomalien unterrichtet. (Bild: DECOIT GmbH & Co. KG)