Cybersicherheit für KRITIS

NIS-2-Richtlinie bedeutet hohen finanziellen Aufwand zur Erfüllung der gesetzlichen Vorgaben, neues Analysetool bietet vereinfachte und kostengünstigere Alternative.

Die neue NIS-2-Richtlinie stellt die Erweiterung der bisherigen Cybersicherheitsvorgaben dar und stellt Unternehmen vor große Herausforderungen. © Adobe Stock / DECOIT GmbH & Co. KG

DECOIT GmbH & Co. KG
info@decoit.de
www.decoit.de

Effiziente Angriffserkennung bei gleichzeitiger Entlastung des Personals: Für viele IT-Abteilungen stellt mittlerweile die Aufrechterhaltung der Sicherheit des Unternehmens-Netzwerkes gegenüber Angriffen von außen eine der wichtigsten Aufgaben dar. Nicht nur, dass Kommunikations- oder Produktionsprozesse unterbrochen, sondern auch komplette Unternehmensnetzwerke lahmgelegt werden können. Öffentliche Einrichtungen bzw. sicherheitsrelevante Unternehmen sind mittlerweile ebenfalls vermehrt Gegenstand von Cyberangriffen.

Strengere Cybersicherheitsstandards

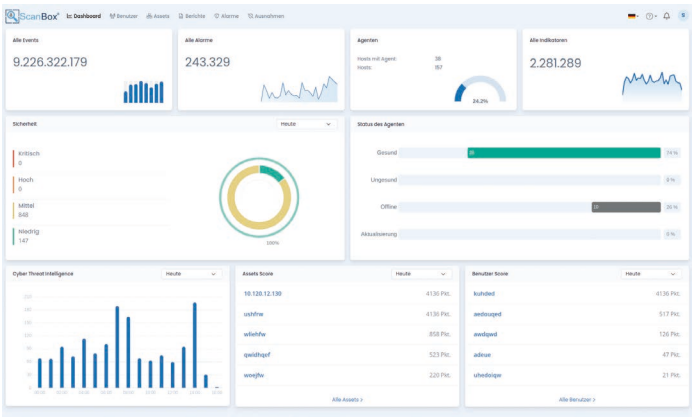
Die neue NIS-2-Richtlinie, welche am 17.10.2024 in Kraft getreten ist, legt hierzu strengere Cybersicherheitsstandards fest, die vorher nur durch KRITIS-Unternehmen erfüllt werden mussten. Was in erster Linie als ein weiterer Schritt zur gesteigerten Cybersicherheit zu verstehen ist, stellt die betroffenen Unternehmen vor nicht unerhebliche Herausforderungen. Die Erfüllung der Richtlinien erfordert sowohl hohe finanzielle Aufwendungen als auch umfangreichen personellen Einsatz, welcher oftmals nicht vorhanden ist. Die Decoit bietet hierfür mit der ScanBox eine passende, bedienerfreundliche Lösung zur Analyse und Dokumentation von Cyberangriffen.

Erweiterung der bisherigen Cybersicherheitsvorgaben

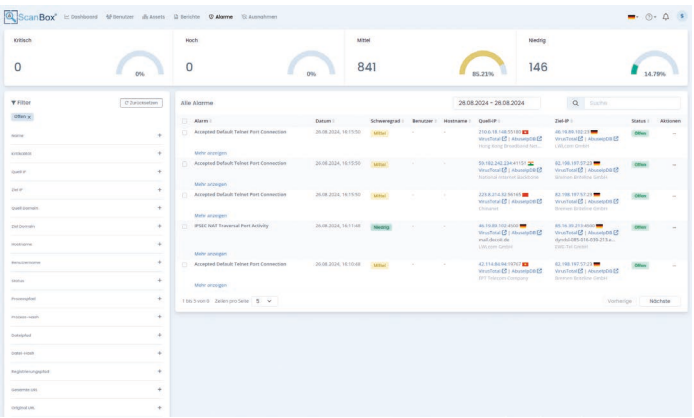
Die Richtlinie stellt eine umfassende Erweiterung der bisherigen Cybersicherheitsvorgaben dar und verpflichtet Unternehmen und Institutionen mit kritischer IT-Infrastruktur zu strengeren Maßnahmen sowie zur Meldung erfolgter Sicherheitsvorfällen. Sie regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen innerhalb der EU. Diese sind verpflichtet, ein umfassendes Risikomanagement zu implementieren. Beinhaltet sind unter anderem regelmäßige Sicherheitsanalysen, Absicherung kritischer Systeme durch geeignete technische und organisatorische Maßnahmen sowie die kontinuierliche Überwachung und Reaktion auf sicherheitsrelevante Ereignisse.

Strenge Meldepflichten

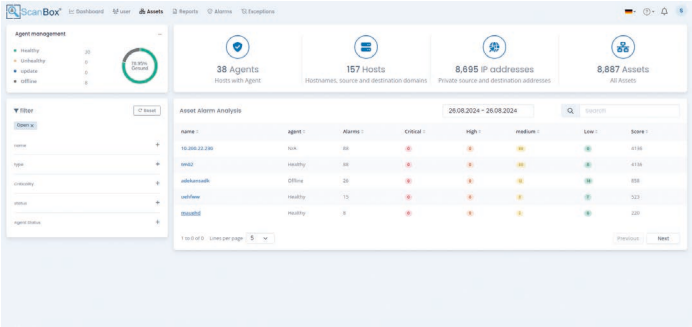
Zudem unterliegen sie strengen Meldepflichten für Sicherheitsvorfälle,



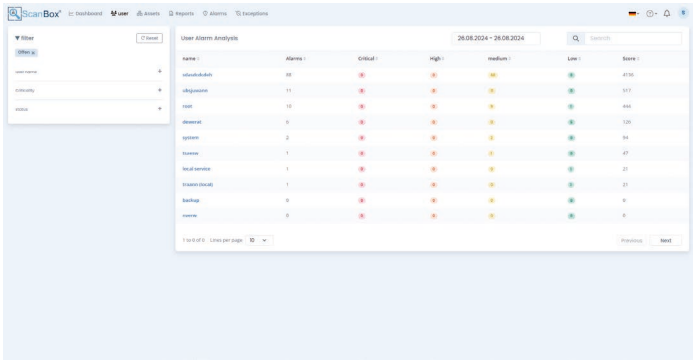
Das Dashboard zeichnet sich durch Benutzerfreundlichkeit und Übersichtlichkeit aus. Alle weiteren Bilder: © DECOIT GmbH & Co. KG



Per Alarmfunktion wird der IT-Administrator unverzüglich über Anomalien unterrichtet.



Die ScanBox bietet detaillierte Sicherheitsanalysen für Assets und Alarme an, wodurch Sicherheitslücken schneller erkannt und behoben werden können.



Detaillierte Sicherheitsanalysen für Benutzer und Alarme

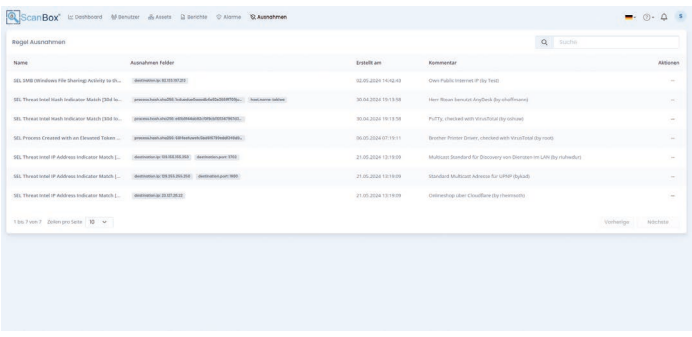
um eine frühzeitige Reaktion und Schadensbegrenzung zu gewährleisten. Betroffen sind neuerdings unter anderem KMUs aus den Bereichen Abfall- und Wasserwirtschaft, Produktion und Verarbeitung und Verwalter von IKT-Diensten ab 50 Mitarbeitern und 10 Mio. Euro Umsatz. Energieversorger, Gesundheitswesen und Finanzdienstleistungen waren bereits seit 2016 betroffen. Bei einer Missachtung der Richtlinie kann dies zu erheblichen Sanktionen führen; darunter hohe Geldstrafen, Einschränkungen im Geschäftsbetrieb und in besonders schweren Fällen sogar zur persönlichen Haftung von Geschäftsführern und Vorständen.

Verzögerungen bei der Umsetzung

Gleichwohl kommt es bei der Umsetzung der NIS-2-Richtlinie in Deutschland wie auch in weiteren EU-Staaten vielfach zu Verspätungen. Selbst KRITIS-Unternehmen befinden sich oftmals noch mitten im Umsetzungsprozess. Der Grund hierfür liegt zum einen in dem hohen zu investierenden Zeitaufwand, der Komplexität der Aufgabe aber auch den fehlenden Personalkapazitäten in den Unternehmen. Genau dies stellt den Ansatzpunkt der von der Decoit GmbH & Co. KG entwickelten ScanBox dar, welche als kostengünstige und effektive Lösung für die IT-Sicherheitsüberwachung und das -management für KMUs und andere KRITIS-Unternehmen entwickelt wurde und als systemunabhängige Lösung positioniert ist.

Lösung: ScanBox

Die ScanBox ist ein einfaches und skalierbares System zur Angriffserkennung. „Die ScanBox von der Decoit wurde als ein unkompliziertes, skalierbares und zuverlässiges System zur Angriffserkennung entwickelt. Sie nutzt als Basis aktuelle Bedrohungsdaten, um verdächtige Muster und Anomalien frühzeitig zu identifizieren“, zeigt Geschäftsführer Prof. Dr. Kai-Oliver Detken auf. Dadurch wird eine proaktive Verteidigung ermöglicht, indem Bedrohungen schneller erkannt und geeignete Gegenmaßnahmen eingeleitet werden.



Durch die sofortige Erkennung von Anomalien unterstützt die ScanBox die schnelle Reaktion auf potenzielle Sicherheitsbedrohungen. Regeln für Ausnahmen können definiert werden.

Anomalie-Erkennung

Die Anomalie-Erkennung nutzt regelbasierte Mechanismen, um Abweichungen von der Compliance zuverlässig zu identifizieren. Dadurch wird die Anzahl an Fehlalarmen („False Positives“), die bei rein KI-gestützten Systemen häufig auftreten, erheblich reduziert. Diese Effizienz ermöglicht es somit auch kleinen und mittelständischen Unternehmen von einem fortschrittlichen SIEM-System zu profitieren – einer Technologie, die durch deren Komplexität und hohem Kostenaufwand bislang eher Großunternehmen vorbehalten war.

Intuitive Benutzeroberfläche

Die intuitive Benutzeroberfläche der ScanBox ermöglicht proaktives Handeln, ohne dass tiefgehendes Wissen in Sicherheits- oder Clustermanagement erforderlich ist. Die Kombination aus einer benutzerfreundlichen Web-App und direktem Zugang zu Security-Analysten ist einzigartig und ein Alleinstellungsmerkmal. IT-Administratoren profitieren von einer erheblichen Entlastung, während gleichzeitig eine professionelle Sicherheitsüberwachung gewährleistet wird – selbst ohne umfassendes internes Know-how in den Bereichen SIEM und Cyber-Operation. Die ScanBox braucht dabei im Gegensatz zu anderen Lösungen nicht mehr permanent an einen Mirror-Port der internen Switches angeschlossen werden, um passive Scans in regelmäßigen Abständen durchzuführen. Denn dieses kann die Switches zu sehr belasten und wertvolle Analysedaten können verloren gehen.

NetFlow

Stattdessen 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. So können verschiedene Datenquellen miteinander kombiniert werden, um ein Gesamtbild der Bedrohungslage zu erhalten. Die Betreuung erfolgt durch ein spezialisiertes, eingespieltes Team aus Experten – direkt, persönlich und aus einer Hand. Die ScanBox stellt daher eine attraktive Lösung gerade für solche Unternehmen dar, welche keine High-End-Lösungen benötigen, aber die gesetzlichen Anforderungen der NIS-2-Richtlinie erfüllen müssen.

Link

Weitere Informationen unter: www.scanbox-product.de

Prof. Dr. Kai-Oliver Detken erklärt die ScanBox.
© Kadet68 - Eigenes Werk, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=144496242