Angriffserkennung mit der ScanBox

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

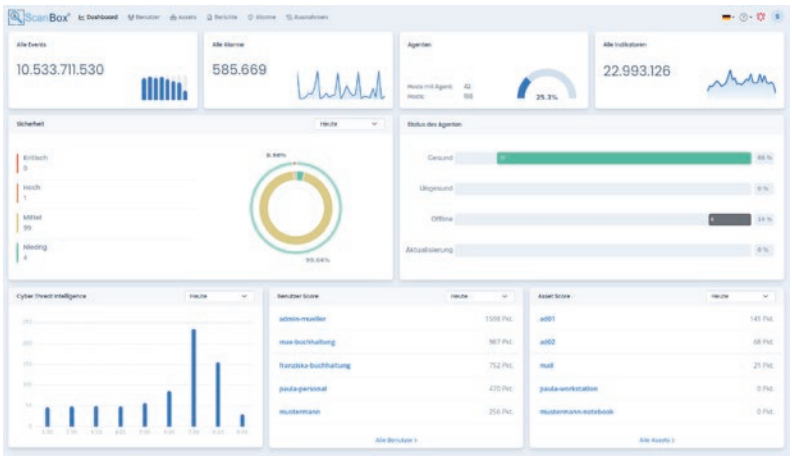
Von Prof. Dr. Kai-Oliver Detken, DECOIT GmbH & Co. KG

Die NIS-2-Richtlinie der Europäischen Union (EU) zur Verbesserung der Cyber- und Informationssicherheit für Unternehmen und Institutionen ist am 17. Oktober 2024 in Kraft getreten. Sie erweitert die Cybersicherheitsanforderungen auf mehr Sektoren und Unternehmen und führt strengere Mindeststandards, Meldepflichten bei Sicherheitsvorfällen sowie höhere Strafen ein für mittlere und große Unternehmen ein, die bestimmte Schwellenwerte bei Mitarbeiterzahl und Umsatz überschreiten. Eine Umsetzung in nationales Recht ist im ersten Quartal 2026 in Deutschland geplant. Spätestens jetzt sollten sich also Unternehmen Gedanken über die Erweiterung ihrer Strategie zur Cybersicherheit machen, um gegen Angriffe von außen und innen sich besser zu schützen oder schlichtweg die Gesetzesvorgaben zu erfüllen.

Zentraler Bestandteil der NIS-2-Richtlinie sind die durchzuführenden Sicherheitsmaßnahmen, die über den bisherigen Stand der Technik hinausgehen. So werden Firewalls als Schutz von äußeren Einflüssen nicht mehr ausreichend angesehen und sollten durch Intrusion-Detection-Systeme (IDS) und Verschlüsselungstechnologien ergänzt werden. Eine kontinuierliche Schwachstellenanalyse sollte durch ein IT-Sicherheitsmonitoring eingeführt werden, um Sicherheitslücken frühzeitig erkennen zu können. Hier kommen sogenannte Security-Information-and-Event-Management-(SIEM) Systeme ins Spiel, die Sicherheitsdaten aus verschiedenen Unternehmensquellen sammeln, analysieren und quasi nahe Echtzeit auswerten. Das Ziel ist es, Bedrohungen und Sicherheitsverstöße frühzeitig zu erkennen, die Einhaltung von Vorschriften zu überwachen und eine schnelle Reaktion zu ermöglichen.

Allerdings fehlt häufig in mittelständischen Unternehmen das entsprechende Fachpersonal, um Sicherheitslücken erkennen und damit umgehen zu können. Dies wird von vielen SIEM-Systemen nicht adressiert. Sie sind für Sicherheitsfachleute in Security Operation Centern (SOC) entwickelt worden. Hinzu kommt, dass meistens nach volumenbasierten Tarifen abgerechnet wird. Das heißt, es wird nach dem tatsächlich anfallenden Datenverkehr der Preis eines solchen Systems ermittelt, wodurch eine feste Planbarkeit der Kosten sich für Unternehmen schwierig gestaltet.

Die DECOIT hat diese Problematik erkannt und ein SIEM-System mit dem Namen ScanBox (https://scanbox-product.de) entwickelt, welches ein einfach zu verstehendes Dashboard für den IT-Systemadministrator enthält und nach der Anzahl der zu überwachenden Assets fest tarifiert wird. Es passt sich daher speichermäßig, als auch preislich der Firmengröße an. Zudem ist es „Made in Germany". Durch die integrierte Cyber-Threat-Intelligence-Korrelation werden aktuelle Bedrohungsdaten genutzt, um verdächtige Muster zu erkennen, Angriffe auszumachen und schnell entsprechende Gegenmaßnahmen einleiten zu können. Auf einen Blick kann so der Administrator erkennen, ob eine problematische Sicherheitslücke vorhanden ist, auf die er sofort reagieren muss, oder die Schwachstellbehebung noch warten kann. Bei technischen Fragen kann er sich nach Bedarf an ein externes SOC wenden, dass die Sicherheitslücke ebenfalls analysiert und ihm Lösungsvorschläge unterbreitet. So ist er gut auf zukünftige Bedrohungen vorbereitet. ■



Das ScanBox Security-Dashboard bietet einen umfassenden Überblick über die IT-Sicherheitslage mit Echtzeit-Kennzahlen zu Events, Alarmen und Agentenstatistiken. (Bild: DECOIT GmbH & Co. KG)