Verfügbarkeit ist nicht alles

Netzmonitoring mit Sicherheitsüberwachung

Kai-Oliver Detken

Heutige Monitoringsysteme sind auf die Überwachung der Verfügbarkeit von IT-Systemen spezialisiert. Sie gehören heute zum Stand der Technik, da jedes Unternehmen auf seine IT-Infrastruktur angewiesen ist. Immer wichtiger werden aber auch Monitoringsysteme, die die IT-Sicherheit überwachen und Alarm schlagen - mit wachsender Notwendigkeit..

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Die Notwendigkeit, seine Systeme zu schützen, wird immer größer. Das beweisen aktuelle Verschlüsselungstrojaner oder MS-Exchange-Sicherheitslücken. Praktisch wäre daher ein Netzmonitoring, das automatisiert Sicherheitschecks vornimmt, die Sicherheitsrichtlinien überprüft, Verstöße meldet und verständliche Handlungsempfehlungen für den IT-Administrator zur Verfügung stellt. Allerdings gibt es auf der einen Seite eine Vielfalt von solchen Systemen und zum anderen auch unterschiedlichste Funktionalitäten in Einklang zu bringen.

Der Markt der IT-Sicherheitssysteme ist von einer großen Vielfalt, aber auch Unübersichtlichkeit geprägt. Typische Lösungen wie z.B. UTM-Firewalls (UTM–Unified Threat Management, ein UTM-System vereint unterschiedliche

IDS/IPS-Systeme analysieren das interne Netzverhalten, erkennen Agriffe durch Muster und leiten automatisierte Gegenmaßnahmen ein. Hier unterscheidet man zwischen host- und netzbasierten IDS-Lösungen (Divya Gupta, Pixabay)

Sicherheitsaufgaben auf einer Plattform, wie Firewall, VPN-Gateway, Virusschutz, Spamschutz, Content-Filter, IDS, Endpoint Protection, Authentifizierung, Quality of Service, Reporting) bieten heutzutage keinen ausreichenden Schutz mehr, da auch viele Angriffe aus dem internen Netz kommen. Um interne Netz- und Serverzugriffe wirksam schützen zu können, sind daher neue Systeme entwickelt worden, die sich wie folgt benennen lassen:

- Intrusion & Prevention Detection System (IDS/IPS);
- Network Access Control (NAC);
- Security Information and Event Ma-

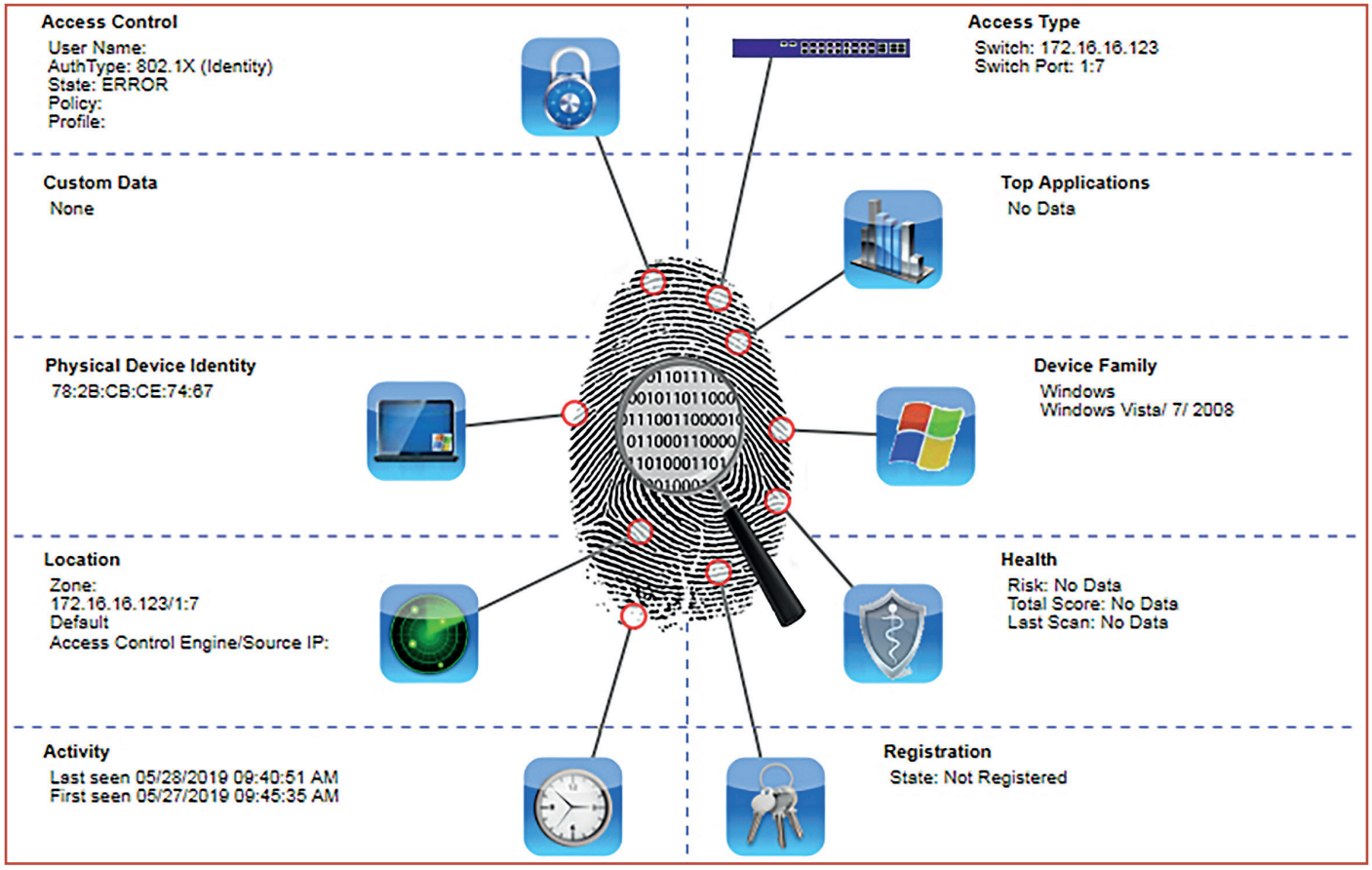

Bild 1: Der NAC-Ansatz ist auf Mitarbeiter und Endgeräte fokussiert und führt während des Anmeldeprozesses eine Richtliniensteuerung durch (Quelle: https://www.extreme-networks.com/product/extremecontrol/)

nagement (SIEM);
- Security Orchestration Automation and Response (SOAR);
- Endpoint Detection and Response (EDR);
- Extended Detection and Response (XDR).

IDS/IPS-Systeme versuchen das interne Netzverhalten zu analysieren, Angriffe durch Muster zu erkennen und ggf. automatisierte Gegenmaßnahmen einzuleiten. Hier unterscheidet man zwischen host- und netzbasierten IDS-Lösungen, die auch in Kombination eingesetzt werden können. Das hostbasierte IDS schützt das Betriebssystem eines Server- oder Client-Rechners und analysiert Log- und Kernel-Daten sowie andere Systemdaten, wie z.B. Datenbanken. Das netzbasierte IDS zeichnet hingegen den Netzverkehr auf und gibt Alarm bei verdächtigen Aktivitäten. Es wird versucht, ein Angriffsmuster zu erkennen und dieses mit den bekannten Mustern abzugleichen. Durch immer schnellere Netze und der entstehenden Datenflut, ist der IT-Administrator aber oftmals überfordert.

Um sich gegen Viren, Würmer und nichtautorisierte Zugriffe auf Serversysteme zu schützen, kann ebenfalls eine sog. Zugangskontrolle (Network Access Control – NAC) eingeführt werden. Der NAC-Ansatz ist auf Mitarbeiter und Endgeräte fokussiert und kontrolliert diese während des Anmeldungsprozesses auf Richtlinienkonformität (Bild 1). Ein typisches Szenario ist es, wenn bei der Authentifizierung die Aktualität des Virenscanners bzw. seiner musterbasierten Datenbank abgefragt wird. Ist diese auf dem neuesten Stand, wird entsprechend der Nutzerrichtlinie der Zugriff gewährt. Ist hingegen der Virenscanner veraltet, wird das Endgerät in die Quarantänezone geschoben. Dort hat es nur Zugriff auf das öffentliche Internet sowie den Update-Server. Ist das Endgerät wieder auf einem Sicherheitsstand, der den Sicherheitsrichtlinien entspricht, kann er auf das Unternehmensnetz wie gewohnt zugreifen. Die erforderlichen Funktionen verteilen sich auf verschiedene Netzkomponenten wie Router, WLAN-APs und Switche oder entsprechende Appliances, die gebündelt die Funktionalität anbieten. Falsches Nutzerverhalten und Angriffe auf Applikationsebene können allerdings nicht erkannt werden.

SIEM-Lösungen stellen hingegen eine Kombination aus ehemals unterschiedlichen Produktkategorien dar: Security Information Management (SIM) und Security Event Management (SEM). Die SIEM-Technik ermöglicht die Echtzeitanalyse von Security-Alarmen, die von Netzkomponenten oder Anwendungen generiert werden. SIEM-Lösungen kann

es als reine Softwaresysteme geben, aber auch Appliances und Managed Services sind möglich. Durch die Analyse von Log-Informationen können zusammenhängende Reports generiert werden, die man auch für Compliance-Zwecke verwenden kann. Eine Kombination mit NAC-Systemen ist dabei durchaus erwünscht, da sich beide Sicherheitssysteme gegenseitig ergänzen können.

SIEM-Lösungen sammeln relevante Protokoll-, Log- und Ereignisdaten aus verschiedensten Quellen aus Bereichen wie z.B. Security, Netz, Server oder auch Anwendungen (Bild 2). Typische Beispiele für Quellen sind Firewalls, IDS/IPS-Systeme, Antimalwaresoftware oder auch Web-Content-Gateways. Die aus diesen Quellen aggregierten Daten werden dann von der SIEM-Lösung in Echtzeit analysiert, um etwaige Sicherheitsprobleme zu erkennen. Da man mehrere Datenquellen analysiert, erkennt das SIEM-System Bedrohungen, indem es Informationen aus mehr als einer Quelle korreliert. Dabei ordnet es die Ereignisse hinsichtlich ihrer Bedeutung ein, indem KI-Methoden zum Einsatz kommen. Security-Admins obliegt dann die Aufgabe, die verschiedenen Vorfälle durchzusehen, um die Quelle der Bedrohung aufzuspüren und das Problem zu beheben. Auf diese Weise lernt die SIEM-Lösung zunehmend besser zu erkennen, was eine echte Bedrohung ist und welche Ereignisse nur verdächtig erscheinen.

Security Orchestration Automation and Response (SOAR) korreliert ähnlich wie SIEM ebenfalls Sicherheitsdaten aus verschiedenen Quellen, aber Herkunft und Menge der bezogenen Informationen unterscheiden sich. Bei SOAR kommen aber noch weitere Faktoren hinzu. So werden beispielsweise externe Informationen wie „Threat Intelligence Feeds“ von Anbietern von Sicherheitssoftware oder anderen externen Drittanbietern mitberücksichtigt. Diese Informationen werden

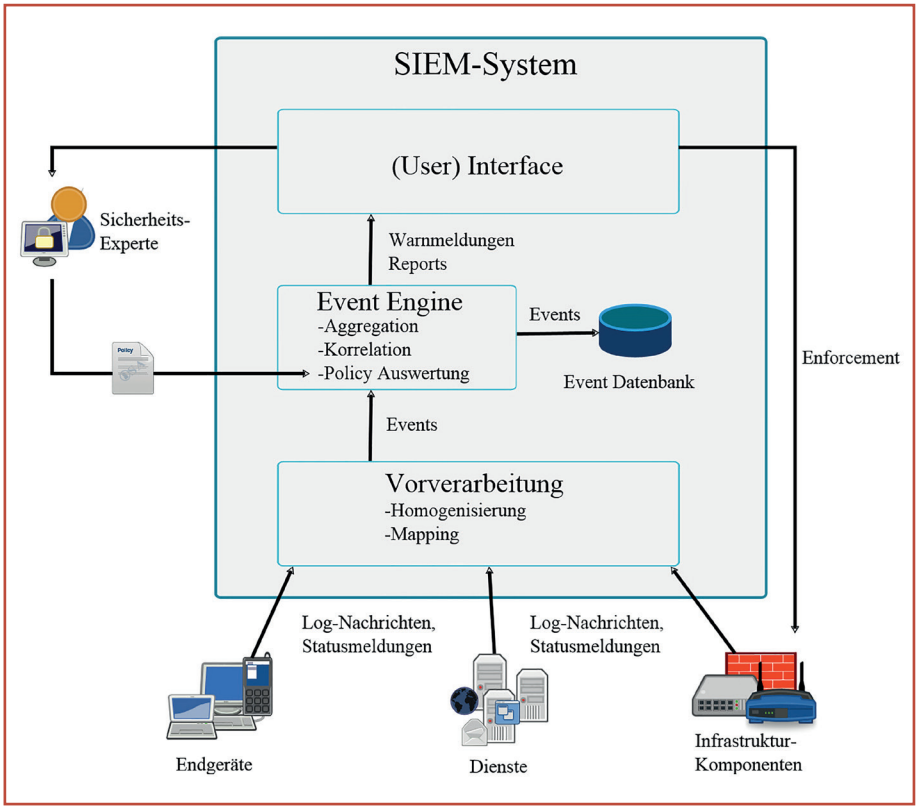

Bild 2: Aufbau eines SIEM-Systems zur Aggregation relevanter Protokoll-, Log- und Ereignisdaten aus verschiedensten Quellen aus Bereichen wie z.B. Security, Netz, Server oder auch Anwendungen

miteinbezogen, um ein besseres Gesamtbild der Sicherheitslandschaft innerhalb und außerhalb des Unternehmensnetzes zu erhalten. Anschließend können die notwendigen Reaktionen auf bestimmte Sicherheitsvorfälle automatisiert umgesetzt werden, ohne einen zusätzlichen Security-Administrator.

Zusätzlich versuchen Hersteller die Kommunikationsendpunkte durch Endpoint-Protection-Lösungen besser abzusichern. Für gezielte Attacken auf bestimmte Rechnersysteme ist daher Endpoint Detection and Response (EDR) entwickelt worden. Diese Systeme bieten präventiven Bedrohungsschutz, intelligente Analysen durch maschinelles Lernen und koordinierte Abwehrprozesse. Das Rechnerbetriebssystem wird nicht nur geschützt, sondern auch seine Schnittstellen (z.B. USB). Als Weiterentwicklung von EDR wird Extended Detection and Response (XDR) gehandelt. XDR kombiniert Daten aus verschiedenen Quellen, wie z.B. den Endpoints, dem Netz, der Cloud und Log-Daten mit allgemeinen Bedrohungsinformationen. Das heißt, es werden lokale Bedrohungsdaten mit externen Datenquellen kombiniert. Dadurch soll ähnlich wie bei SOAR ein vollständigeres Angriffsbild geschaffen werden.

Übersicht über SIEM-Lösungen

An dieser Stelle soll ein Überblick über vorhandene SIEM-Systeme am Markt gegeben werden, die das Monitoring von IT-Sicherheitsvorfällen am besten abdecken. Die Tabelle gibt einen Überblick über die entsprechenden Hersteller mit ihren Lösungen, wobei keine Vollständigkeit aufgrund des dynamischen Marktes garantiert werden kann.

Bei der Bewertung von SIEM-Lösungen sollte dabei folgende Fragestellungen bez. der unterstützten Leistungsmerkmale mit einbezogen werden:

- Integrationsmöglichkeit mit anderen Sicherheitslösungen: Ist das SIEM-

System in der Lage, andere Security-Produkte zu veranlassen, Aktionen auszuführen, Angriffe zu verhindern oder zu stoppen?

- künstliche Intelligenz (KI): Kann das SIEM-System durch maschinelles Lernen (ML) oder Deep Learning (DL) seine Erkennungsgenauigkeit von Vorfällen automatisch verbessern?
- Threat Intelligence Feeds: Lassen sich beliebige Bedrohungs-Feeds an das System anbinden oder muss man einen bestimmten Feed verwenden?
- Reporting: Können vorgefertigte Berichtsvorlagen für gängige Compliance-Anforderungen verwendet werden? Lassen sich Reports anpassen oder neue Berichte erstellen?
- forensische Fähigkeiten: Kann das System zusätzliche Informationen über Vorfälle erfassen, die zur nachträglichen Analyse herangezogen werden können?

Fazit

Die Unternehmen haben heute mehrheitlich begriffen, dass IT-Sicherheit ein elementarer Bestandteil ihrer Geschäftsprozesse sein muss, um sich gegenüber Angreifern abzusichern. Allerdings werden dabei unterschiedliche Aufwände betrieben. Während das Monitoring der Verfügbarkeit auch bei klein- und mittelständischen Unternehmen (KMU) zum Stand der Technik gehört, fehlt es noch an vergleichbaren Systemen zum Monitoring der IT-Sicherheit. Diese Lücke kann durch intelligente SIEM-Systeme gefüllt werden, was aber bisher durch die Kosten oder Komplexität problematisch war. Intrusion Detection Systeme (IDS) scheiterten in der Vergangenheit bereits an dem Auswerte- und Konfigurationsaufwand, was man nun bei SIEM tunlichst vermeiden möchte. NAC-Systeme werden ebenfalls immer noch viel zu wenig eingesetzt (bisher nur 30 % der Unternehmen in Deutschland), obwohl diese gerade im Zusammenspiel mit SIEM sinnvoll sind. Weiterentwicklungen wie SOAR und XDR ermöglichen nun die Einbeziehung von externen Wissensdatenbanken oder Sicherheitsexperten, automatisierte Gegenmaßnahmen und Einbeziehung von Cloud-Systemen. Auch diese Systeme werden inzwischen teilweise in SIEM-Systeme integriert, um das Analysieren von SIEM-Berichten nicht selbst, sondern durch externe Security Operation Center (SOC) vornehmen zu lassen. Allerdings sind solche Funktionen oftmals bei deutschen Unternehmen aus Datenschutzgründen nicht erwünscht, wofür dann allerdings auch das entsprechende Fachpersonal verfügbar sein sollte. Hier muss man das Für und Wider entsprechend abwägen. Eines ist aber auf jeden Fall sicher: Ohne ein Sicherheitsmonitoring sollte ein Unternehmen heute nicht mehr auskommen.

Hersteller/Anbieter	Produktname	URL-Adresse
Alienvault	USM Anywhere	www.alienvault.com
Darktrace	OSSIM	www.alienvault.com
Darktrace	Enterprise Immune System	www.darktrace.com
Decoit	ScanBox	www.scanbox-product.de
	CLEARER	www.clearer-product.de
Elastic	ELK Stack	www.elastic.co
	Elastic-SIEM	www.elastic.co
Exabeam	Security Management Platform	www.exabeam.com
Fireeye	Helix Security Platform	www.fireeye.com
Fortinet	FortiSIEM	www.fortinet.com
Hansight	Enterprise	en.hansight.com
Hewlett Packard Enterprise (HPE)	ArcSight User Behavior Analytics (UBA)	www.hpe.com
	ArcSight ThreatDetector	www.hpe.com
Huawei	HiSec Insight	www.huawei.com
IBM	QRadar SIEM	www.ibm.com
	QRadar User Behavior Analytics (UBA)	www.ibm.com
Logpoint	SIEM	www.logpoint.com
Logrythm	NextGen SIEM Platform	www.logrhythm.com
	User and Entity Behavior Analytics (UEBA)	www.logrhythm.com
	CloudAI	www.logrhythm.com
Manageengine	ADAudit Plus	www.manageengine.com
	EventLog Analyzer	www.manageengine.com
	Log360	www.manageengine.com
Mcafee	Enterprise Security SIEM	www.mcafee.com
Micro Focus	ArcSight Enterprise Security Manager	www.microfocus.com
	ArcSight Logger	www.microfocus.com
Microsoft	Azure Sentinel	www.microsoft.com

Dies ist eine Übersicht über die derzeit im Markt vorhandenen SIEM-Lösungen sowie die einzelnen Hersteller. Darüber hinaus sind die entsprechenden Webseiten aufgeführt. Die Tabelle erhebt aber keinen Anspruch auf Vollständigkeit