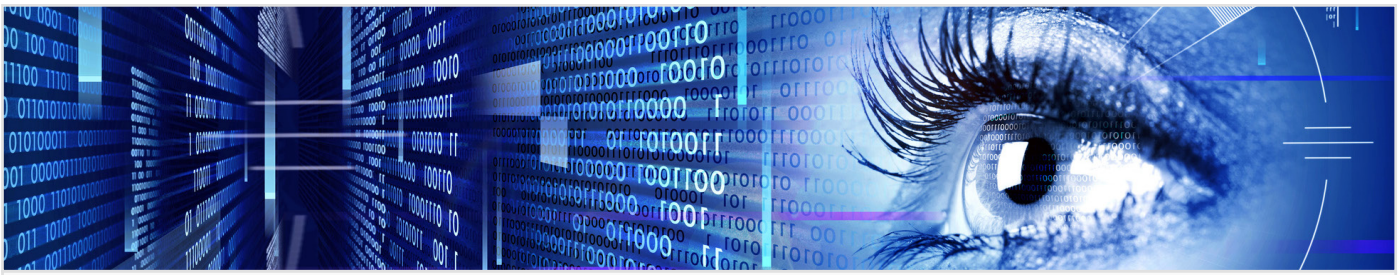

Bild: Fotolia.com: © Kurhan

CLEARER - SIEM-Funktionalität für NAC

Überwachung der Zugangskontrolle und Endgeräte-Dokumentation durch sog. Network Access Control (NAC) Systeme sind notwendig, um unerwünschten oder unbekannten Endgeräten den Zugang zu den Firmennetzwerken zu versperren. Fremde Systeme werden erkannt, auf Richtlinienkonformität überprüft, installierte Programme und Sicherheitsupdates gescannt, Zugangsberechtigungen erteilt/verweigert und aufgrund der Richtlinien werden Systeme in bestimmte Netzwerke verschoben. Bei Security Information and Event Management (SIEM) geht es um die Überwachung der IT-Sicherheit und Korrelation der Ereignisse (Vorfälle). Hier wird eine Gesamtübersicht über den Sicherheitsstatus des Netzwerkes geboten, indem sicherheitsrelevante Informationen im Netzwerk gesammelt, bewertet und dann priorisiert werden. Das System gibt Meldungen über eine kritische Sicherheitslage aus und stellt Handlungsempfehlungen bereit.

Die Produkterweiterung CLEARER bietet dem Administrator SIEM-Funktionalitäten. Dadurch kann das NAC-System nicht nur Geräte/IP-Adressen/Netzwerke isolieren, sondern erhält die Fähigkeit bestehende und neue Geräte auf diverse Sicherheitsrisiken zu untersuchen. CLEARER fragt in regelmäßigen Intervallen den Datenbestand der IP-Adressen im NAC-System ab, vervollständigt damit die eigene Übersicht über alle Adressen, um diese zum Schutz des Systems miteinander bestehenden abzugleichen. Dabei können Anomalien von den Sensoren identifiziert und dann vom System in Handlungsempfehlungen umgewandelt werden. Auf diese Art erhält der NAC-Administrator nicht nur die Information, dass eine IP-Adresse oder ein Netzwerk isoliert werden sollte, sondern auch warum es eine Sicherheitsschwachstelle darstellt.

Integration von macmon NAC mit CLEARER

Um die volle Funktionalität von CLEARER nutzen zu können, ist die Anbindung an das macmon NAC vorgesehen. macmon NAC muss nicht separat konfiguriert werden. Der Austausch zwischen beiden Systemen geschieht über die Rest-API-Schnittstelle. Dafür wurde ein NAC-Actuator in CLEARER integriert.

Haben Sie macmon NAC im Einsatz und sind an der Produkterweiterung CLEARER interessiert?
Gern stellen wir Sie Ihnen persönlich vor. Wir freuen uns auf Ihre Anfrage.

Kontaktdaten

DECOIT® GmbH E-Mail: clearer@decoit.de URL: www.clearer-product.de

Funktionen und Features im Überblick

- Überwachung des Netzwerkverkehrs
  - Mirrorports an den Switchen
  - Aufnahme aller Netzwerkverbindungen
  - Überwachung von Quelle und Zeit, abhängig von Tageszeit und Wochentag
  - Alarm bei unerwünschtem Netzwerkverkehr
  - Regeln für den Netzwerkverkehr zwischen verschiedenen Netzen
  - Sonderregeln für einzelne IP-Adressen

- Scan auf Schwachstellen
  - Umfangreiche Konfigurationsmöglichkeit der zu scannenden Netzwerke und Geräte
  - Automatisierte und manuelle netzwerkweite Scans auf Schwachstellen
  - Aktualisierung der Schwachstellen-Prüfroutinen (VTs) über das Internet
  - Erstellen von Schwachstellen-Tickets zu jeder gefundener Schwachstelle inkl. aktueller CVE (Common Vulnerabilities and Exposures) Informationen
  - Überprüfung der Behebung der Schwachstellen durch erneuten Scan
  - Compliance-Verletzung bei weiterhin offener Schwachstelle

- Bedienung und interne Features
  - Zugang über Web-Browser
  - Anlegen von mehreren Benutzern
  - komplett verschlüsselte Kommunikation der Komponenten
  - automatische Erneuerung der Zertifikate
  - Anschluss an macmon secure NAC für Enforcement
  - Einstufen der Bedrohungslevel (Risikoklasse niedrig/mittel/hoch)
  - Internes Ticketsystem für die Abarbeitung der gefundenen Vorfälle
  - Nachverfolgbarkeit der getätigten Arbeiten

- Konfiguration und Installation
  - Installation aus einem Repository
  - Konfigurationsoberfläche für die komplette Komponentenumgebung
  - Zertifikatsverwaltung für alle Komponenten

Über DECOIT® GmbH

Als Bremer IT-Systemintegrator verfügen wir über mehr als 15 Jahre Erfahrung im Bereich IT-Sicherheit. Individuell auf Kundenwünsche zugeschnittene Lösungen bilden die Kerntätigkeit der DECOIT® in allen Abteilungen, so dass CLEARER aus der Notwendigkeit erhöhter Sicherheit in der Netzwerkabsicherung im Rahmen eines Forschungsprojekts entstanden ist.

Beim Thema Sicherheit ist der ganzheitliche Ansatz besonders wichtig, um alle Schwachstellen zu identifizieren und zu schließen. Die DECOIT® erarbeitet individuelle Sicherheitskonzepte auf Basis von BSI-Empfehlungen, die neben den technischen Komponenten, auch organisatorische Regelungen mit beinhaltet. So ist CLEARER zusammen mit dem NAC-System ein Teil des ganzheitlichen Sicherheitskonzepts.

Kontaktdaten

DECOIT® GmbH E-Mail: clearer@decoit.de URL: www.clearer-product.de