IT-Security Speakers Corner:

Sicherheitsmonitoring-Lösungen für Klein- und Mittelständische Unternehmen

Prof. Dr. Kai-Oliver Detken
DECOIT GmbH & Co. KG
Fahrenheitstraße 9, D-28359 Bremen
https://www.decoit.de
info@decoit.de

Open Source. Open Solutions. Open Strategies.

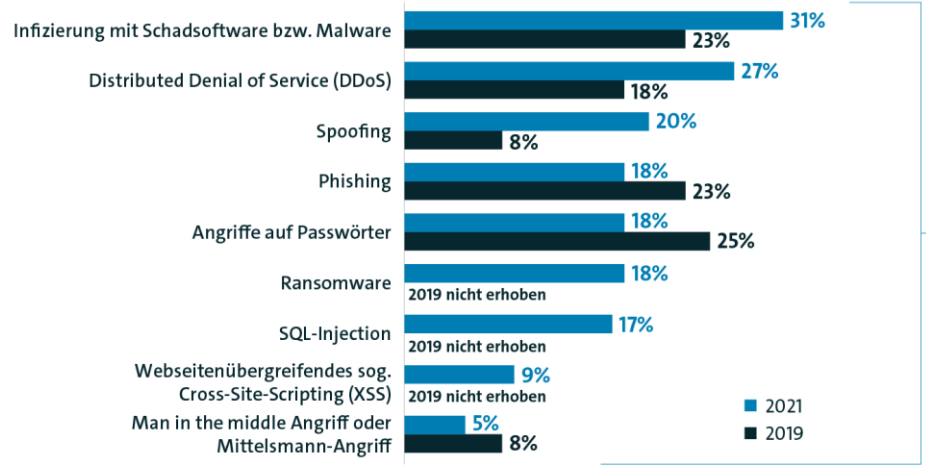
Firmenkurzvorstellung

- **IT-Consulting:** ganzheitliche sowie herstellerneutrale Beratung
- **System Management:** Optimierung technischer Arbeitsabläufe, Integration von Hersteller- oder Open-Source-Lösungen in vorhandene Umgebungen
- **Software-Entwicklung:** Entwicklung von Individualsoftware, Anpassung bestehender Open-Source-Software an Kundenbedürfnisse
- **IT-Forschungsprojekte:** innovative neue IT-Lösungen
- **Produktentwicklung:** innovative Produkte auf Basis von F&E-Projekten

Zunehmende Internet-Attacken

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

86%

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

bitkom

Erste Gegenmaßnahmen

- Zur Absicherung wurden Access Control Lists (ACL) auf den Routern und Switches eingerichtet
- Statische Filter ließen sich allerdings nicht pflegen, weshalb diese später verbindungsabhängig (Stichwort: Stateful Inspection) in Firewalls umgesetzt wurden
- Application Ports wurden gesperrt, ohne den Datenverkehr zu analysieren
- Zur Anomalie-Erkennung wurden Intrusion Detection Systems (IDS) versucht einzuführen, ohne den administrativen Aufwand zu berücksichtigen
- Anti-Viren- und Anti-Spam-Systeme sind auf Basis von reiner Musterkennung im Einsatz

Ausgangssituation bei KMUs

- KMU besitzen kein ausreichendes Fachpersonal, welches sich hinreichend mit Bedrohungspotenzialen auskennt
- Generelle IT-Kenntnisse werden bei KMU den Spezialkenntnissen vorgezogen
- IT-Sicherheit wird daher normalerweise vernachlässigt und nicht als integraler Geschäftsprozess gesehen
- Monitoring und Bewertung von Netzwerk- und Informations-Sicherheit haben aber heute Auswirkungen auf das Rating und den Wert von Unternehmen
- Gesetzgeberische und regulatorische Vorgaben erzwingen regelmäßige Kontrollen und Transparenz des vorhandenen Sicherheitsstandards
- IT-Sicherheit im Produktionsumfeld hinkt der Büroumgebung um ca. 10 Jahre hinterher

IT-Sicherheitsgesetz 2.0

- Mit dem IT-Sicherheitsgesetz (IT-SiG 2.0) sind zahlreiche Änderungen im BSI-Gesetz in Kraft getreten und damit die Anforderungen an die Cybersicherheit verschärft worden
- Gemäß § 8a Absatz 1a BSIG sind KRITIS-Betreiber sowie Unternehmen im besonderen öffentlichen Interesse verpflichtet, ab dem 1. Mai 2023 ein System zur Angriffserkennung umzusetzen
- Wie dieses System im Detail aussehen soll (IDS, IPS, SIEM, XDR, SOAR) wird offen gelassen
- Es gibt aber einen Maßnahmenkatalog, der beschreibt was ein solches Angriffserkennungssystem erfüllen sollte
- Die Anomalie-Erkennung wird als Methode genannt, aber nicht weiter spezifiziert

IT-SiG 2.0-Umsetzungen

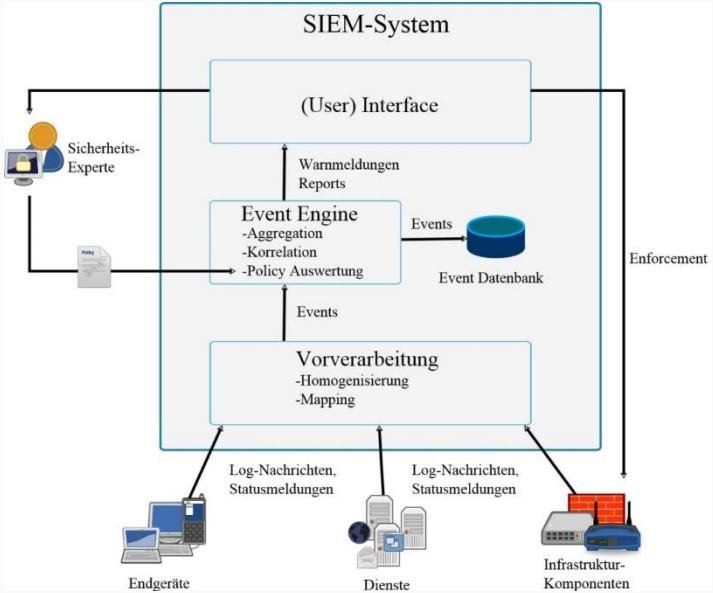
- Um das IT-Sicherheitsgesetz (IT-SiG 2.0) zu erfüllen lassen sich verschiedene Strategien beschreiben
  - Einsatz eines SIEM/SOAR-Systems mit eigenem Fachpersonal
  - Einsatz eines SIEM/SOAR-Systems mit Unterstützung eines Security Operation Centers (SOC) des Anbieters
  - Einsatz eines SIEM/SOAR-Systems mit KI-basierter Angriffserkennung und automatisierten Gegenmaßnahmen
- Die letztgenannte Möglichkeit ist in OT-Netzen nicht umsetzbar

Einsatz von Überwachungssystemen

- Evolution der Überwachungs- und Regulierungssysteme:
  - **Netzmonitoring**: Überwachung der Verfügbarkeit und Netztopologie-Darstellung zur Dokumentation
  - **Network Access Control (NAC)**: Überwachung der Zugangskontrolle und Endgeräte-Dokumentation
  - **Security Information and Event Management (SIEM)**: Überwachung der IT-Sicherheit und Korrelation der Ereignisse (Vorfälle)
  - **Security Orchestration, Automation and Response (SOAR)**: Kombination aus unterschiedlichen Datenquellen und automatische Reaktionen ohne menschliche Eingriffe

SIEM-Schwerpunkte

- Überwachung von
  - Benutzerdiensten und -privilegien
  - Verzeichnisdiensten
  - Systemkonfigurationen
  - Netzwerkverkehr
- Korrelation unterschiedlicher Log- und Netzdaten für bessere Gesamtübersicht
- Erkennung von Anomalien
  - Arbeiten mit regelbasierter oder KI-basierter Anomalie-Erkennung
  - Reagieren automatisch auf Anomalien oder erfordern ein manuelles Eingreifen
- Aber: diese Systeme sind bisher auf IT-Netze spezialisiert worden!

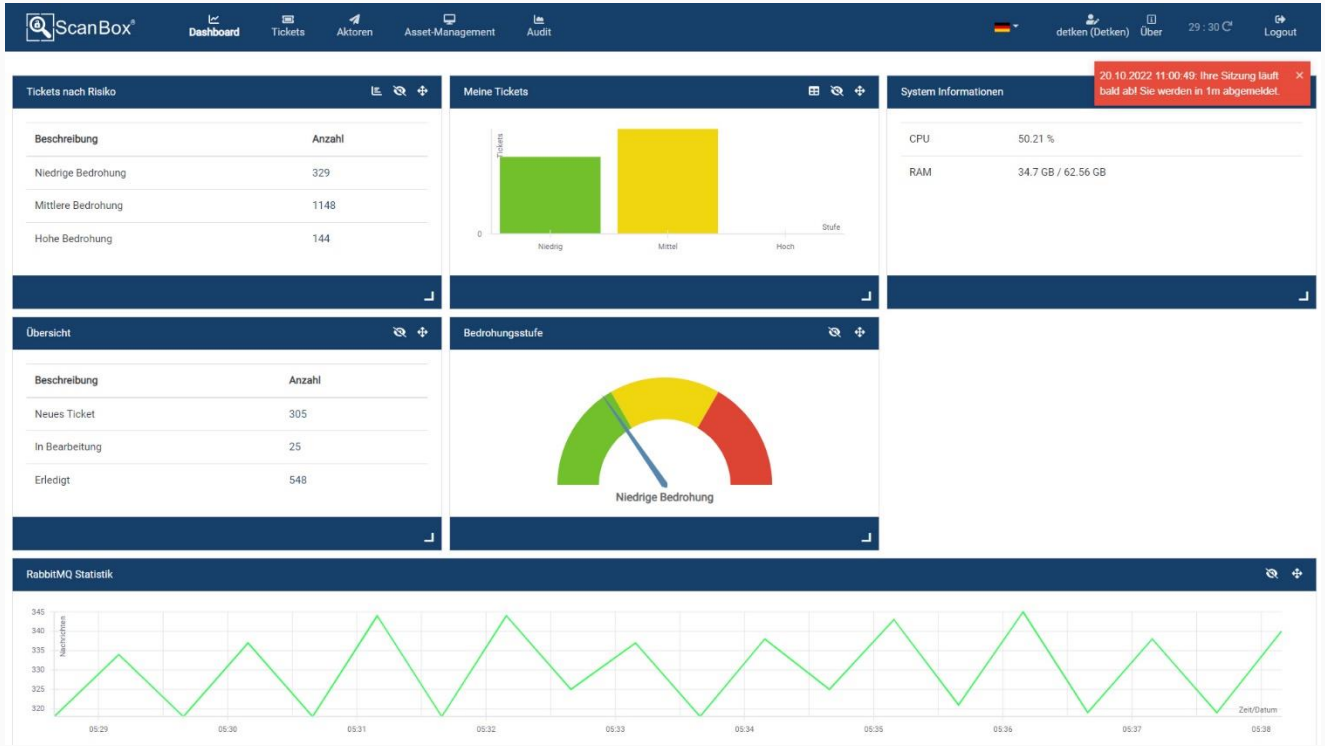


ScanBox®-Lösungsansatz

- Die Monitoring- und Security-Analyse-Appliance ScanBox ist in der Lage aktive sowie passive Scans durchzuführen
- Dadurch lässt sie sich gleichermaßen in IT- als auch in OT-Umgebungen einsetzen
- Es wird nach Schwachstellen gesucht und diese im Dashboard angezeigt
- IT-Nutzer erhalten konkrete Handlungsempfehlungen
- Jeder Vorfall wird in einem integrierten Ticketsystem aufgenommen und wird darüber bearbeitet
- Die Vorfälle lassen sich als Reports archivieren
- Anbindung zu Drittsystemen: NAC-System von macmon secure und IRMA von Achtwerk

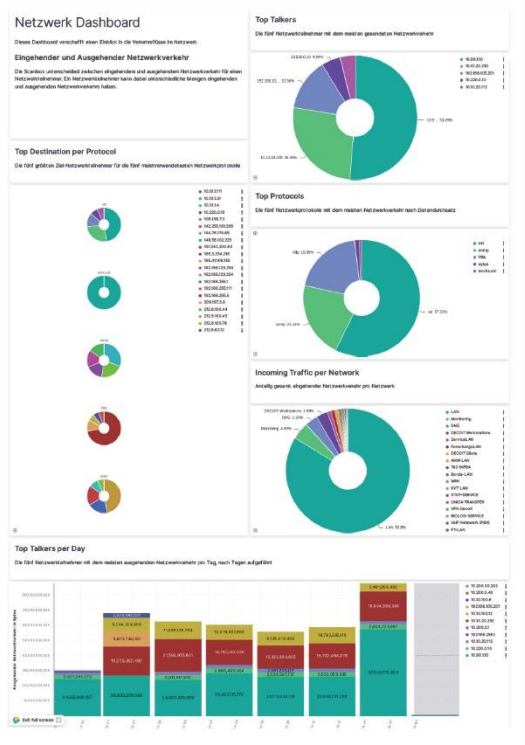
www.scanbox-product.de

ScanBox® SIEM-GUI



ScanBox® Dashboard

- Es werden wöchentliche Dashboard-Reports mit den wichtigsten Ereignissen an den Administrator geschickt :
  - Netzwerk (Top Talkers, Protocols, Incoming Traffic)
  - Performance (Events pro Agent)
  - Events (Alarme pro Kategorie)
- Die Reports sind anpassbar



Funktionsumfang

- Funktionalität:
  - Mit den Sensoren werden Netzwerk- und Serverdaten gesammelt
  - Die Daten werden ausgewertet und reale Vorfälle entdeckt
  - Anschließend erfolgt die Zuordnung zu bekannten CVE-Schwachstellen
  - Handlungsempfehlungen werden daraus abgeleitet
  - Eine kontinuierliche Risikobewertung findet statt
  - Integriertes Ticketsystem zur Vorfallbearbeitung
  - Produkt ist geeignet für IT- und OT-Umgebungen
  - OT-Protokolle können mittels des Aktors IRMA erkannt werden
- Voraussetzungen:
  - Switch-Mirror-Port für Netzüberwachung
  - Konfiguration der Netzregeln
  - Konfiguration der Szenarien

Umsetzung

- Eine Datenvolumengrenze muss angegeben werden aufgrund begrenztem Speicherplatz auf der Appliance
- Zur Erweiterung kann ein externes Storage genutzt werden oder auf einen leistungsfähigeren Server ausgewichen werden
- Ein Vorprojektierung ist erforderlich, um alle Rahmenbedingungen abzuklären (z.B. welche Protokolle, Netze, Komponenten überwacht werden sollen)
- Anhand der gesammelten Anforderungen wird eine Basiskonfiguration erstellt und die ScanBox ausgeliefert
- Support kann per E-Mail oder/und Service-Vertrag beauftragt werden
- Die Anomalie-Erkennung wird regelbasiert über Playbooks (Use Cases) zur Verfügung gestellt

Zusammenfassung

- Die ScanBox® ermöglichen es, dass das interne Netz kontinuierlich auf Schwachstellen analysiert werden kann
- Dabei wird zwischen IT- und OT-Netzen unterschieden (aktive/passive Scans)
- Die enthaltene regelbasierte Anomalie-Erkennung wird kontinuierlich erweitert
- Weiterentwicklungen (neue Leistungsmerkmale) werden durch Maintenance-Verträge kostenfrei zur Verfügung gestellt
- Durch passive Scans und den IRMA-Aktor kann die ScanBox® auch in OT-Netzen zum Einsatz kommen
- Mit dem Sicherheitsgesetz 3.0 werden auch mittlere Unternehmen gezwungen werden sich mit dieser Thematik auseinanderzusetzen

Besuchen Sie uns am Stand D04(5)

DECOIT GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de