Unternehmensschutz:

IT-Monitoring und Security Information and Event Management (SIEM) für den Mittelstand

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

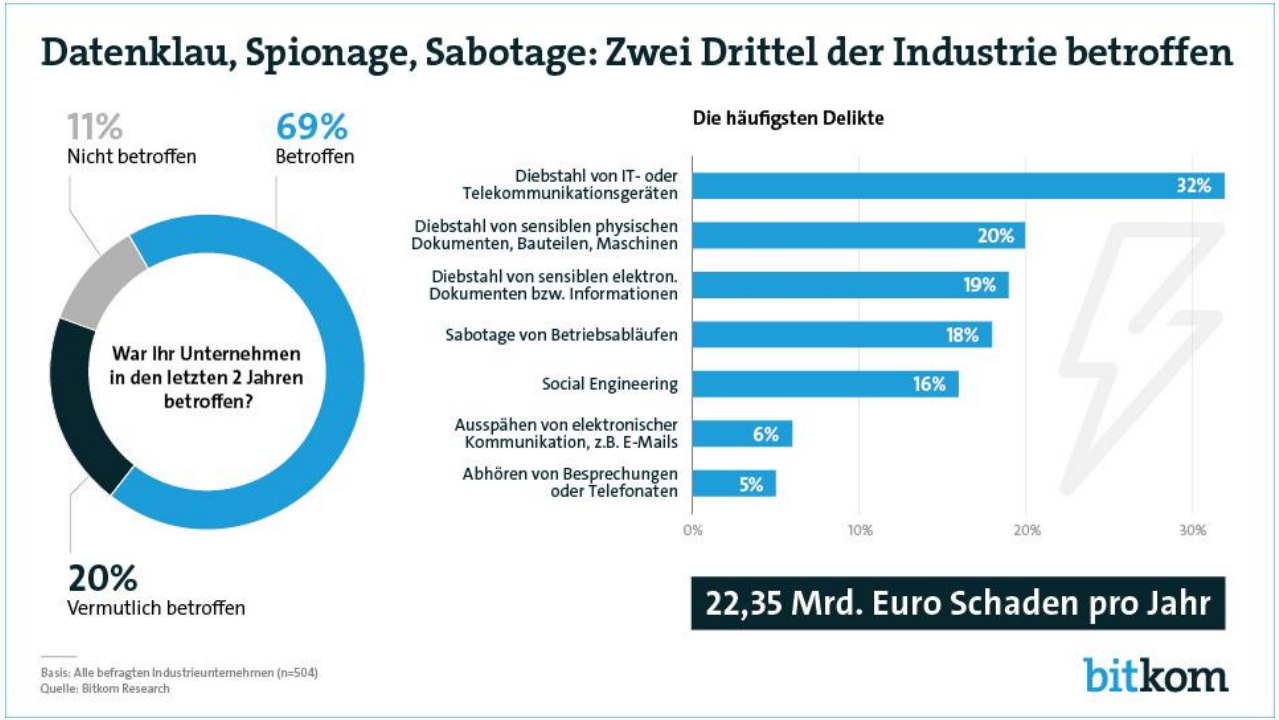
© DECOIT GmbH

Bremer Systemintegrator und Softwarehaus

- **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 IT-Lösungen
- **Produktentwicklung**: innovative Produkte auf Basis von F&E-Projekten

© DECOIT GmbH

Status Internet-Attacken



© DECOIT GmbH

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

© DECOIT GmbH

Einsatz von Überwachungssystemen

- Evolution der Überwachungs- und Regulierungssysteme:
  - **Netzmonitoring**: Überwachung der Verfügbarkeit und Netzdokumentation
  - **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)

© DECOIT GmbH

Netzmonitoring

- Ziel: Überwachung von Services und Serversystemen sowie Sammeln von Verfügbarkeitsstatistiken
- Aufgaben:
  - Einbindung von Netzwerk- und Serverkomponenten
  - Überwachung von Services (Diensten)
  - Eskalationsmanagement bei Alarmmeldungen (SMS, E-Mail)
  - Zusammenfassung von Alarmmeldungen
  - Unterscheidung unterschiedlicher Prioritäten

© DECOIT GmbH

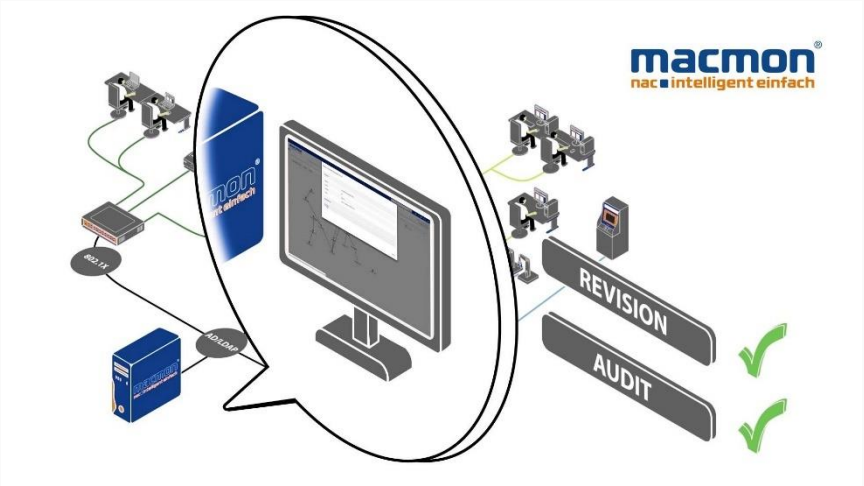
Netzmonitoring-Lösungen

- Nagios:
  - Quasistandard heutiger Monitoring-Lösungen
  - Bietet eine Sammlung von Modulen zur Überwachung des Netzwerks, der Hosts und bestimmter Dienste an
- Icinga:
  - Löste sich im Jahr 2009 als Fork von Nagios
  - Grund war die schleppende Entwicklung und fehlender Support
  - Die Weboberfläche wurde u.a. modernisiert
- Check_MK:
  - Ursprünglich seit 2009 reines Add-On für Nagios
  - Heute eigener leistungsfähiger Core (komplette Monitoring-Lösung)
  - Wesentlich skalierbarer, performanter und einfacher zu konfigurieren

© DECOIT GmbH

Network Access Control (NAC)

- Ziel: Zugangskontrolle von Systemen und Benutzern in Netzwerke
- Aufgaben:
  - Fremde Systeme erkennen
  - Auf Richtlinienkonformität überprüfen
    - Scan der installierten Programme
    - Scan der Sicherheitsupdates
  - Zugangsberechtigung erteilen oder verweigern
  - Verschieben von Systemen in bestimmte Netzwerke aufgrund der Richtlinien



© DECOIT GmbH

NAC-Lösungen

- macmon secure:
  - BSI-zertifizierte NAC-Lösung
  - Herstellerunabhängig
  - Mischbetrieb mit und ohne 802.1X
  - Ermöglicht Compliance-Regeln einzusetzen
- PacketFence:
  - Open-Source-Lösung ohne Lizenzkosten
  - Ähnlich leistungsfähig wie Herstellerlösungen
  - Erkennen von Netzanomalien, proaktive Scans, Isolierung von problematischen Endgeräten

© DECOIT GmbH

Security Information and Event Management (SIEM)

- Ziel: Gesamtübersicht über den Sicherheitsstatus des Netzwerkes bieten
- Aufgaben:
  - Sammeln sicherheitsrelevanter Informationen im Netzwerk
  - Bewerten dieser Informationen
  - Priorisierung der bewerteten Informationen
  - Meldungen über kritische Sicherheitslage geben
  - Handlungsempfehlungen bereitstellen

© DECOIT GmbH

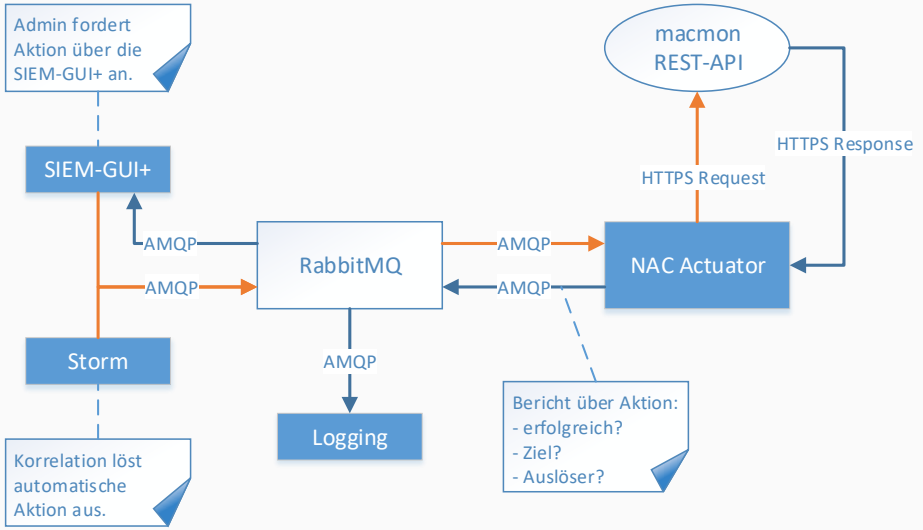
SIEM-Lösungen

- LogRhythm:
  - Effizientes Pattern Matching
  - Dashboard ist anpassbar
  - Wahrscheinlichkeit für „False Positives“ ist angebbar
- OSSIM:
  - Ist als Open-Source-Lösung entwickelt worden
  - Wurde vom Hersteller AlienVault übernommen
  - Integriert andere Open-Source-Lösungen: OpenVAS, Snort, Nagios, Munin etc.

© DECOIT GmbH

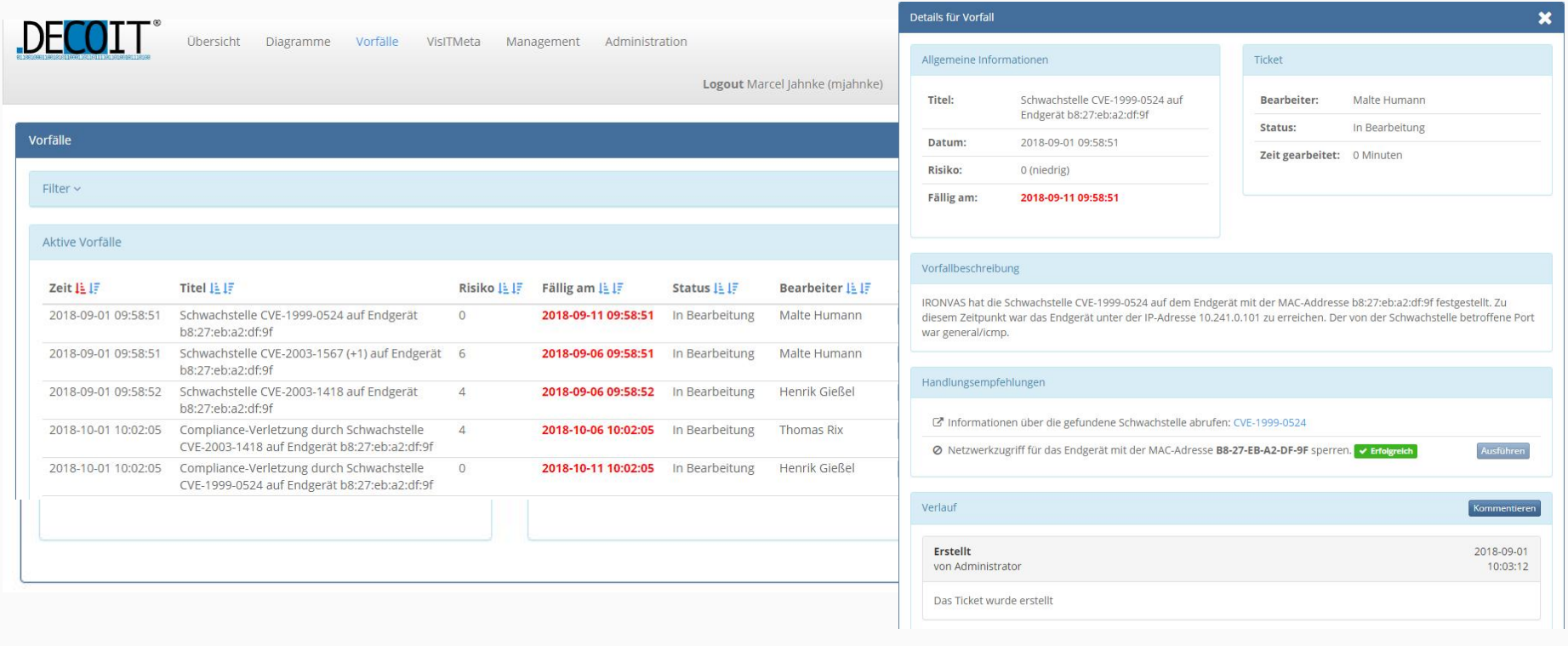
Ausblick: CLEARER mit SIEM-GUI+

- Koppelt NAC-Systeme und SIEM über REST-API-Schnittstelle miteinander
- Kommunikation in beide Richtungen: Infrastrukturdaten lassen sich holen und ein Enforcement-Befehl zurücksenden
- Anzeige der wesentlichen Vorfälle
- Ereigniskorrelation und -bewertung
- Verständliche Handlungsempfehlungen
- Schließt die Lücke der Nachweisbarkeit des Sicherheitsstatus



© DECOIT GmbH

Dashboard der SIEM-GUI+



© DECOIT GmbH

IT-Sicherheit baut auf Open Source!

- Viele proprietäre Hersteller von IT-Sicherheitsprodukten nutzen heute Open-Source-Lösungen
- In manchen Bereichen haben sich dabei die Open-Source-Lösungen sogar durchgesetzt (Quasistandard)
  - VPN: OpenVPN
  - Firewall: pfSense / OPNsense
  - Anti-Viren-/Anti-Spam-Schutz: ClamAV / Rspamd
  - Proxy: Squid
  - Intrusion Detection Systeme: Snort / Suricata
  - Monitoring: Nagios / Icinga / Check_MK

© DECOIT GmbH

Fazit zu Open Source Software

- Keine Hintertüren im Source Code vorhanden
- Fehler (Bugs) werden kommuniziert und können schnell behoben werden
- Kann flexibel eingesetzt und bei Bedarf angepasst werden
- Keine Hersteller-Sackgasse (Vendor Lock-In) bei der Nutzung
- Oftmals keine Lizenzkosten, sondern Maintenance-Kosten
- Genauso leistungsfähig wie oder sogar leistungsfähiger als proprietäre Software

© DECOIT GmbH

Vielen Dank für die Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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

© DECOIT GmbH