KI-Angriffserkennung:

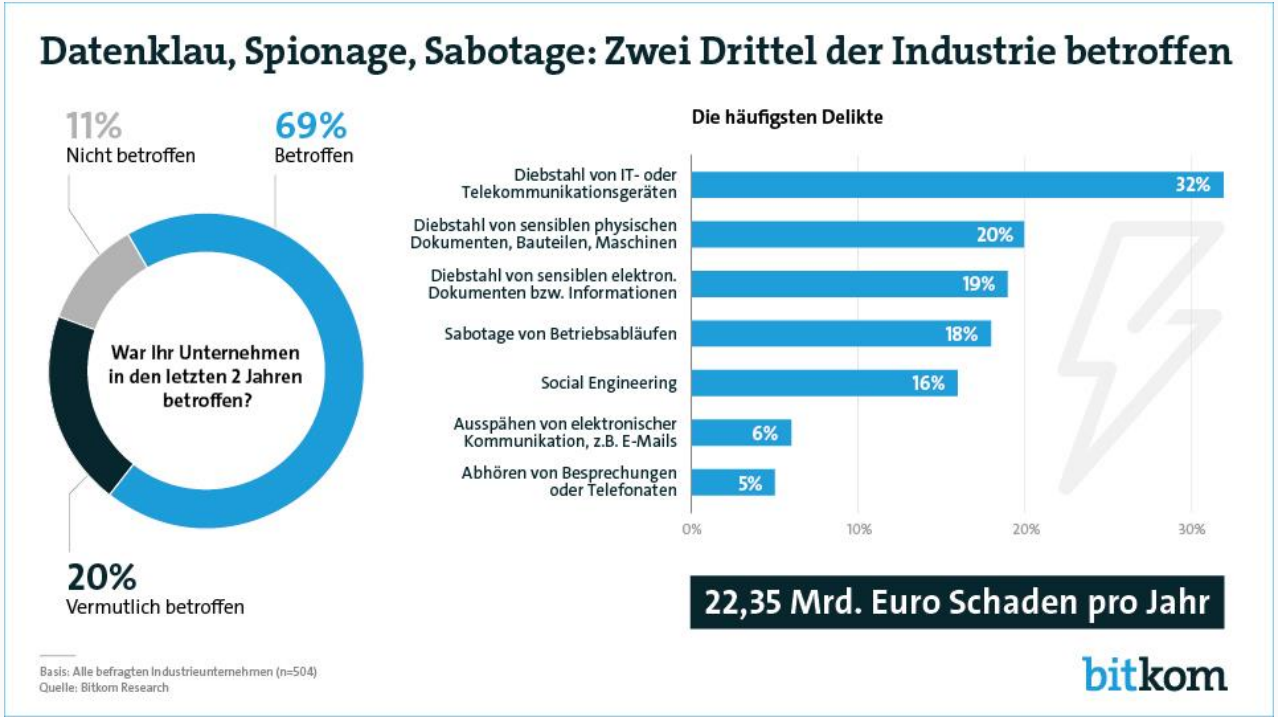
Mit künstlicher Intelligenz und Machine-Learning Angriffe aufspüren

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

Bremer Systemintegrator und Softwarehaus

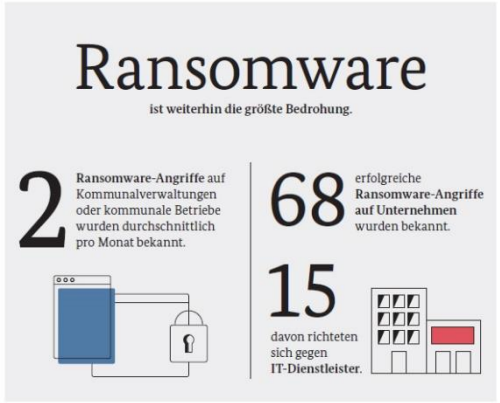
- **IT-Consulting**: ganzheitliche sowie herstellerneutrale Beratung
- **System Management**: Optimierung technischer Arbeitsabläufe, Integration von Hersteller- oder Open-Source-Lösungen in vorhandene Umgebungen
- **Software-Entwicklung**: Entwicklung von Individualsoftware, Anpassung bestehender Open-Source-Software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

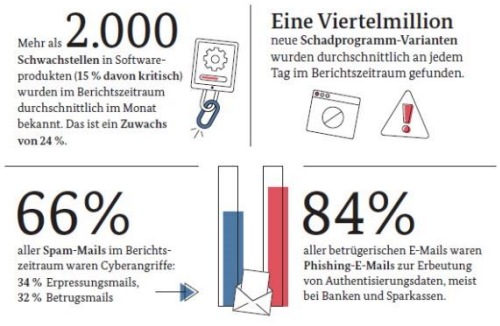
Status von Cyberangriffen

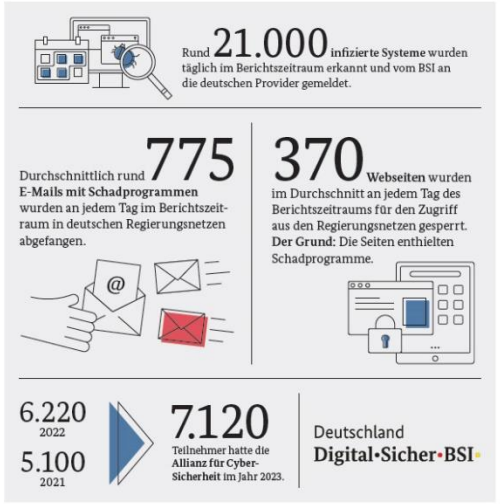


Quelle: https://ap-verlag.de/industrie-im-visier-von-cyberkriminellen-und-nachrichtendiensten/20754/

BSI-Lagebericht 2023







- Die Bedrohungslage im Bereich der Cyber-sicherheit ist weiterhin von einer hohen Dynamik geprägt
- Die rasante Entwicklung im Bereich der Künstlichen Intelligenz zeigt, wie schnell technische Neuerungen fortschreiten können
- Nach wie vor bleiben Angriffe mit Ransomware die größte Bedrohung für die Cybersicherheit

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

Einsatz von Überwachungssystemen

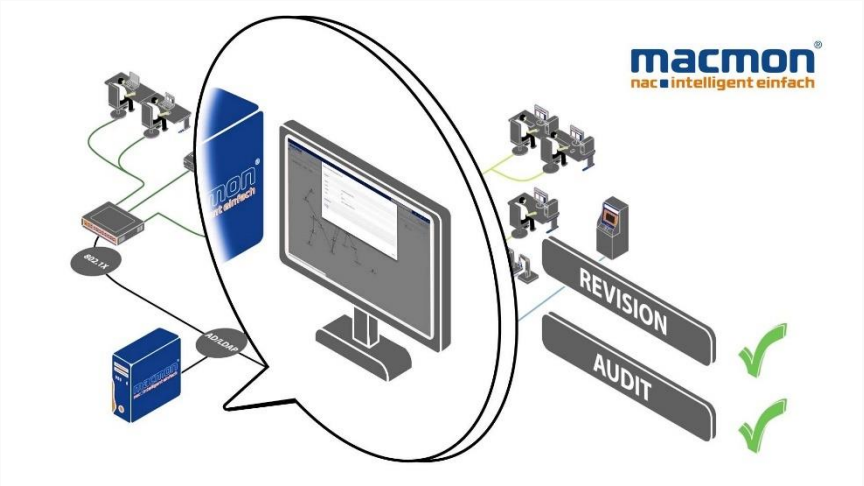
- Evolution der Überwachungs- und Regulierungssysteme:
  - **Netzmonitoring**: Überwachung der Verfügbarkeit und Netzdokumentation
  - **Network Access Control (NAC)**: Überwachung der Zugangskontrolle und Endgeräte-Dokumentation
  - **Security Information and Event Management (SIEM)**: Überwachung der IT-Sicherheit und Korrelation der Ereignisse (Vorfälle)
  - **Endpoint Detection and Response (EDR)**: Überwachung von Endgeräten bzgl. IT-Sicherheit und Anomalien (AV-Weiterentwicklung)

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

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



Security Information and Event Management (SIEM)

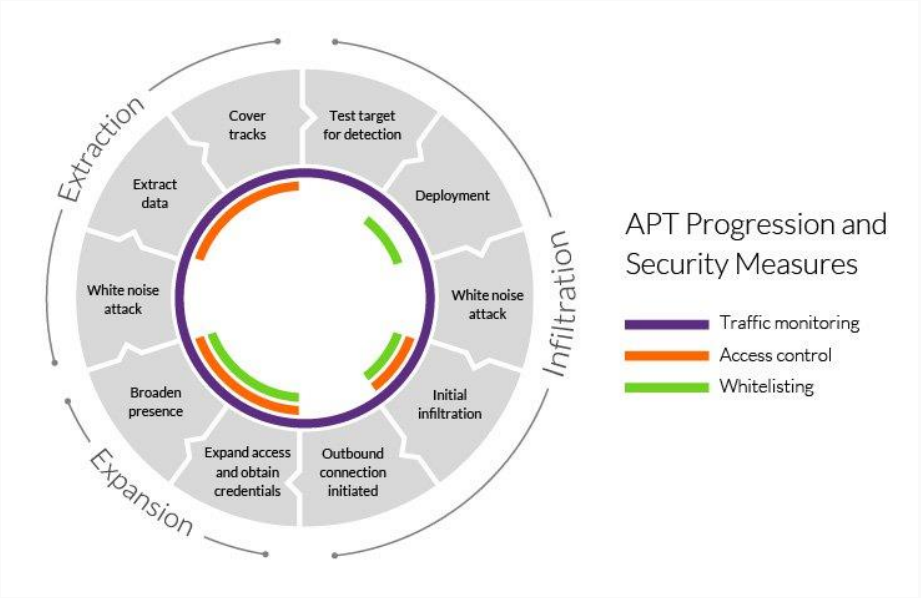
- Ziel: Gesamtübersicht über den Sicherheitsstatus des Netzwerkes bieten
- Aufgaben:
  - Sammeln sicherheitsrelevante Informationen im Netzwerk
  - Bewerten dieser Informationen
  - Priorisierung der bewerteten Informationen
  - Meldungen über kritische Sicherheitslage geben
  - Handlungsempfehlungen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

Endpoint Detection and Response (EDR)

- Ziel: Überwachung von Endgeräten im Hinblick auf verdächtige Aktivitäten
- Aufgaben:
  - Konsolenbenachrichtigungen und -berichte
  - Leistungsfähige Analyse- und Reaktionsfunktionen
  - Sicherheitslücken auf Endgeräten erkennen und melden
  - Managed Services: Weitergabe an ein Security Operation Center (SOC)
  - Schutz gegen Advanced Persistent Threats (APT)

Advanced Persistent Threat (APT)

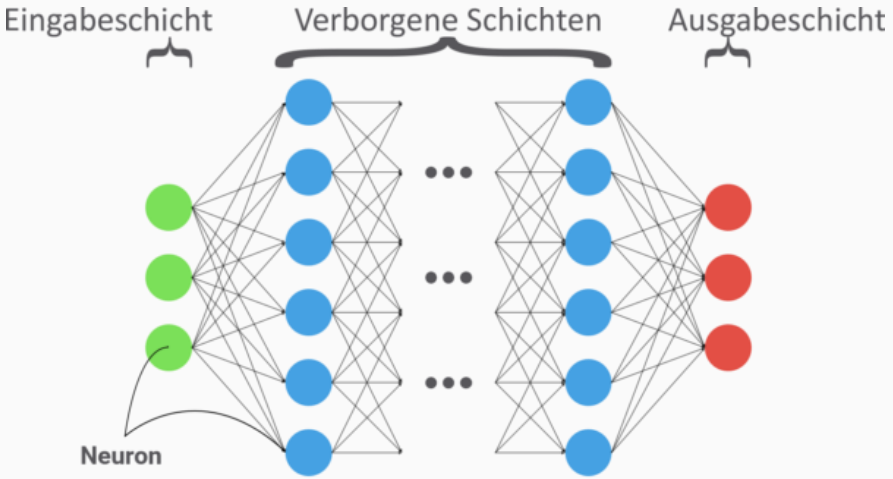
- APT ist ein komplexer, zielgerichteter Cyber-Angriff
- Der Angriff ist darauf ausgelegt über einen längeren Zeitraum hinweg unbemerkt im Zielsystem zu bleiben
- Schwachstellen des Zielsystems sollen auskundschaftet werden
- APTs sind schwer zu erkennen, da sie keinen unmittelbaren Alarm in Sicherheitssystemen auslösen
- Sie lassen sie sich durch die Nutzung von KI einfacher enttarnen, als durch den Sicherheitsexperten



Quelle: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

Was bedeutet KI überhaupt?

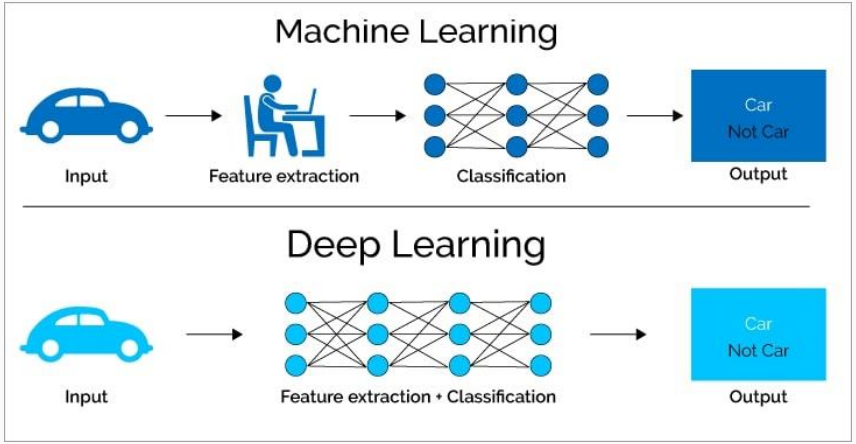
- Generell spricht man bei Machine Learning (ML) von Verfahren, die es erlauben anhand bestimmter Merkmale Dinge zu klassifizieren und zu erwartende Ergebnisse zu extra- bzw. interpolieren
- Dafür werden Neuronale Netze (NN) verwendet, die es erlauben aus dem Dateninput über Synapsen-artige Verschaltungen wahrscheinliche Ergebnisse vorherzusagen
- Dabei gilt: je kleiner der Datensatz ist, umso unwahrscheinlicher ist die NN-Ausgabe korrekt!
- Das NN besteht aus einem Algorithmus, dem ein Entscheidungsbaum antrainiert werden kann (z.B. TensorFlow)
- Sie bilden die Grundlage für das Deep Learning



Quelle: https://nativdigital.com/neuronale-netze/

Deep Learning

- Deep Learning ist eine spezielle Art des maschinellen Lernens, um Muster und Zusammenhänge in großen Datenmengen zu erkennen
- Deep Learning wird zunehmend in der Cybersicherheit eingesetzt, um fortschrittliche Angriffe wie APT-Angriffe zu erkennen, zu analysieren und abzuwehren:
  - Erkennen von Anomalien
  - Malware-Erkennung
  - Verhaltensanalyse
  - Vorausschauende Bedrohungsinformationen
  - Automatisierung von Sicherheitsmaßnahmen



Quelle: https://levity.ai/blog/difference-machine-learning-deep-learning

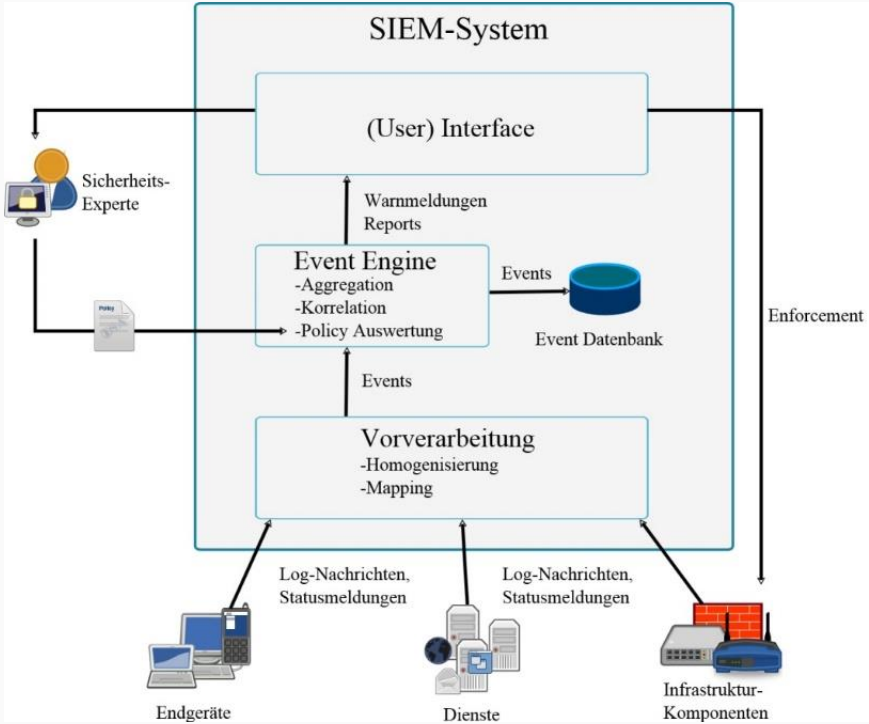
TensorFlow

- TensorFlow ist eine Open-Source-Plattform für maschinelles Lernen und Deep Learning, die von Google entwickelt wurde
- Sie bietet eine umfassende Sammlung von Tools, Bibliotheken und Ressourcen, die es Entwicklern ermöglichen, maschinelle Lernmodelle zu erstellen, zu trainieren und bereitzustellen
- TensorFlow wurde für eine Vielzahl von Anwendungen entwickelt, darunter Bild- und Spracherkennung, Natural Language Processing (NLP), Zeitreihenanalyse etc.
- SIEM-Systeme basieren hauptsächlich auf TensorFlow

Nutzung von KI-Algorithmen

- SIEM-Systeme nutzen KI-Algorithmen auf verschiedene Weise, um Angriffe zu erkennen:
  - **Verhaltensanalyse:** SIEM-Systeme können KI-Algorithmen verwenden, um das normale Verhalten von Benutzern, Geräten und Anwendungen in einem Netzwerk zu modellieren.
  - **Bedrohungsintelligenz:** KI-Algorithmen können dabei helfen, große Mengen von Bedrohungsdaten zu analysieren, um relevante Informationen zu identifizieren.
  - **Automatisierung von Reaktionen:** Moderne SIEM-Systeme integrieren oft automatisierte Reaktionen auf Bedrohungen.
  - **Erkennung von unbekannten Bedrohungen:** KI-Algorithmen sind auch in der Lage, Anomalien zu erkennen, die auf bislang unbekannte Bedrohungen hinweisen könnten.
- Grundsätzlich werden nicht verschiedene Algorithmen genutzt, sondern verschiedene Datensätze verwendet.

Funktionsweise eines SIEM-Systems



- Log- und Netzwerkdaten sammeln (Big Data)
- Homogenisieren der Daten zu einer Datenbasis
- Aggregation verschiedener Events
- Trainieren des Normalverhaltens, um Anomalien mittels KI zu erkennen
- Bewerten der Vorfälle anhand eines Sicherheitsexperten und mittels KI

Cyber Threat Intelligence (CTI)

- Durch die CTI-Nutzung können potenzielle Gefahren erkannt und abgewendet werden
  - CTI beinhaltet die kontinuierliche Sammlung von Informationen über potenzielle Cyberbedrohungen aus verschiedenen Quellen
  - Die gesammelten Daten werden analysiert und bewertet
  - Schwachstellen und Angriffsmuster sollen besser erkannt werden
  - CTI-Plattformen erstellen Bedrohungsmeldungen, die von SIEM-Systemen eingelesen werden können (sog. Threat-Feeds)
- Die CTI-Datenbank dient dazu, bereits bekannte Bedrohungsindikatoren von außerhalb zu erhalten, um neue interne Angriffe besser identifizieren zu können
- Die gewonnenen Erkenntnisse werden in verständlicher Form zusammengefasst → Handlungsempfehlungen

Fazit

- Auch leistungsfähige SIEM-Systeme sind nur so gut wie ihre Datenbasis
  - Ab wann ist ein Normalverhalten erreicht?
  - Wurden zum Anlernen des KI-Algorithmus echte Daten verwendet?
  - Schickt der Hersteller regelmäßig Threat-Feeds?
  - Ist ein Security Operation Center (SOC) vorgesehen?
- KI-Verfahren können helfen die Datenmenge zu beherrschen und die relevanten Informationen herauszufiltern
- Automatisierte Reaktionen sind allerdings in manchen Umgebungen mit Vorsicht einzusetzen

Vielen Dank für die Aufmerksamkeit!

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

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