TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

Berlin, 01.07.2025

Aktueller Stand der KI-Unterstützung in IT-Security-Produkten

Michael Kynast, DCSO

Motivation

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Warum wird künstliche Intelligenz in der IT-Sicherheit benötigt?

Steigende Angriffsgeschwindigkeit:

- Dauer der Angriffe von Erstzugriff bis Datenexfiltration (PAN)
  - 2021: 9 Tage
  - 2025: 2 Tage (in einem von fünf Fällen weniger als 1 Stunde)

Steigende Angriffsqualität

- Automatisierte Aufklärungsarbeit
- KI-gestützte Phishing-Angriffe / personalisierte Angriffe
- Echtzeit-Anpassung zur Umgehung von Abwehrmaßnahmen

Umfang der gesammelten Ereignisse und Alarme

- Durchschnittlicher Anstieg um ca. 250% pro Jahr[2]
- 22% der Unternehmen erstellen täglich 1 TByte oder mehr an Logs[2]

Überlastung von Security-Analysten

- 70% der SOC-Teams fühlen sich durch das Volumen der Sicherheitswarnungen überfordert (Trend Micro[3])

KI-gestützte Angriffe erfordern
KI-gestützte Verteidigung

[1] https://www.paloaltonetworks.com/blog/2025/05/unit-42-develops-agentic-ai-attack-framework

[2] https://chronosphere.io/learn/observability-log-data-trends/?utm_source=chatgpt.com

[3] https://newsroom.trendmicro.com/2021-05-25-70-Of-SOC-Teams-Emotionally-Overwhelmed-By-Security-Alert-Volume

KI-gestützte Verteidigung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Welche Stärken bringt KI in die IT-Sicherheit?

- Verarbeitung großer Datenmengen in Echtzeit (Konsolidierung, Kontextualisierung, Korrelation)
- Erkennung ungewöhnlicher Datenmuster und unüblichen Verhaltens (Anomaly Detection)
- Vorhersage potenzieller Bedrohungen auf Basis historischer Daten und extrapolierter Trends

Wie trägt künstliche Intelligenz zur Verbesserung der IT-Sicherheit bei?

- Angriffserkennung und –alarmierung nahezu in Echtzeit
- Alarmaufbereitung mit Datenkorrelation, -kontextualisierung und – konsolidierung, Klassifizierung und Priorisierung
- Automatisierte Reaktion
- Zusammenfassung und Reporterstellung zu Security-Zwischenfällen
- Einfachere Produktnutzung durch das Verstehen natürlicher Sprache (Chat-Interface)

Kann KI IT-Security-Analysten ersetzen?

Marktsituation: KI-Arten und –konzepte

Große Bandbreite bei Verwendung von KI

- Generative KI für allgemeine Zwecke wie Sprachübersetzung, Zusammenfassungen und Reports
  - „Übersetzungswerkzeug“ für Datenbankabfragen
- ML/DL
  - Verschiedene Methoden des Machine Learning/Deep Learning, zur Erkennung ungewöhnlicher Daten und Verhaltensweisen
- Sicherheitsspezifische ML/DL/Gen AI/Predictive AI
  - Speziell trainierte Modelle für Sicherheitsanwendungsfälle mit vom Anbieter gesammelten Daten

- **Agentic AI**
  - Spezialisierte KI-Agenten, die mit Hilfe externer Tools selbstständig einzelne Aufgaben eines komplexen Szenarios ausführen
- **NEU: Model Context Protocol (MCP)**
  - Als offener Standard soll MCP dafür sorgen, dass KI-Modelle verschiedene Tools (SOAR, EDR, SIEM, TI usw.) mit derselben "Sprache" verwenden können
  - MCP könnte die bevorzugte Kommunikationsmethode für KI-Agenten werden und komplexe Integrationen über APIs ersetzen
  - Noch im Aufbau und wenig genutzt

Marktsituation: Auswirkungen

- **Shadow AI**
  - Verlust sensitiver Unternehmensdaten durch unkontrollierte Nutzung externer KI
- **Wiederbelebung und Weiterentwicklungvon DLP-Produkten**
  - Kontrolle der LLM-Eingaben (ggf. auch Blockierung) und Datenübertragungen an externe KI-Anbieter
  - Nutzung von KI für automatische Klassifizierung von Dokumenten und Monitoring von Datenquellen

- KI ist ein allgemeines Marketing-Schlagwort, auch für bekannte, ältere ML/DL –Techniken
- Mehrheit der Anbieter überlässt Gegenmaßnahmen menschlichen Analysten – einige bieten aber auch automatisierte Response-Schritte

Marktsituation: Lizenzierung & Kosten

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Abrechnungsmodelle

1. Kosten sind in der Lizenz enthalten und damit vorhersehbar/planbar (z. B. Palo Alto Networks)
2. Verbrauchsabhängige Abrechnung (z. B. Microsoft, CrowdStrike)

KI-Kosten vs. Kosten menschlicher Analysten

- Beispiel Phishing-Attacke
  - Volle Bearbeitung mit KI-Assistenten: (13 Prompts): 280 €
  - Unterstützung durch KI-Assistenten (3 Prompts): 65 €
  - Werkstudent als 1st-Level-Analyst: 15 € pro Stunde

Strategien zur Senkung der KI-Kosten

- Verwendung lokaler Zwischenspeicher für wiederkehrende Abfragen (Prompts)
- Aufgabenspezifische Small Language Models (SLMs) anstelle von großen generativen Allzweck-LLMs

Zusammenfassung & Ausblick

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Nahe Zukunft:**
  - Integrierte und auf IT-Security spezialisierte KI mit natürlichsprachigem Interface
  - Agentic AI, die das Model Context Protocol (MCP) zur Kommunikation mit anderen Agenten und internen sowie externen Datenquellen einsetzt.

- **Kann KI IT-Security-Analysten ersetzen?**
  - Aktuell aus Kosten- und Qualitätsgründen noch nicht. In naher Zukunft könnte KI die Arbeit von 1st-Level-Analysten übernehmen. Erfahrene Security-Analysten werden auch in Zukunft benötigt, ihre Effizienz aber durch KI gesteigert.

- **Mit der Weiterentwicklung von KI sind vollautomatisierte, sehr schnell ablaufende KI-basierte Attacken zu erwarten. Das erfordert eine vollautomatisierte KI-gestützte Abwehr, inklusive Reaktion.**

-> Autonomes SOC

Vollautomatische KI-gestützte Angriffe erfordern
vollautomatische KI-gestützte Verteidigung