CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Neue und zukünftige Gefahren

Ausblick

- Technischer Fortschritt gewinnt zunehmend an Geschwindigkeit
  - Rasche Anpassung an damit einhergehende Gefahren erschwert
- Voraussagen und Einschätzung immer schwere zu treffen, aufgrund hochkomplexer, bereichsübergreifender Phänomene
  - Künstliche Intelligenz, Quantencomputing, etc.
- Informations- und Lernressourcen hinken Fortschritt hinterher
- APT-Akteure mit Vorsprung gegenüber industrieller Defensive, dank direktem Zugang zu neuesten Entwicklungen

Definition Künstliche Intelligenz

Künstliche Intelligenz (KI), auch artifizielle Intelligenz (AI), englisch artificial intelligence, ist ein Teilgebiet der Informatik, es umfasst alle Anstrengungen, deren Ziel es ist, **Maschinen intelligent** zu machen. Dabei wird Intelligenz verstanden als die Eigenschaft, die ein Wesen befähigt, **angemessen und vorausschauend in seiner Umgebung zu agieren**; dazu gehört die Fähigkeit, Umgebungsdaten wahrzunehmen, d. h. Sinneseindrücke zu haben und darauf zu reagieren, **Informationen aufzunehmen**, zu **verarbeiten** und als **Wissen zu speichern**, **Sprache** zu **verstehen** und zu **erzeugen**, **Probleme** zu **lösen** und **Ziele** zu **erreichen**.

Positive Auswirkungen von KI auf die Netzwerksicherheit

Erkennung von Anomalien:

- KI-Systeme können durch kontinuierliches Lernen und Mustererkennung ungewöhnliche Verhaltensweisen oder Aktivitäten im Netzwerk identifizieren, die auf Sicherheitsverletzungen hinweisen könnten.

Vorhersage von Sicherheitsbedrohungen:

- KI kann zukünftige Bedrohungstrends vorhersagen, indem sie große Mengen an Sicherheitsdaten analysiert und Muster identifiziert, die auf aufkommende Bedrohungen hinweisen.

Positive Auswirkungen von KI auf die Netzwerksicherheit

Automatisierte Reaktionen auf Bedrohungen:

- KI kann automatisierte Maßnahmen zur Eindämmung oder Behebung von Sicherheitsvorfällen einleiten, was eine schnellere Reaktion als manuelle Eingriffe ermöglicht.

Verbesserte Phishing-Erkennung:

- KI-basierte Systeme können fortschrittliche Phishing-Angriffe erkennen, indem sie E-Mail-Inhalte, Absenderinformationen und andere Merkmale analysieren, die für Menschen schwer zu erkennen sind.

Positive Auswirkungen von KI auf die Netzwerksicherheit

Netzwerksicherheitsmanagement:

- KI kann die Komplexität der Netzwerküberwachung reduzieren, indem sie Verkehrsmuster analysiert und potenzielle Sicherheitsrisiken identifiziert.

Verbesserung der Passwortsicherheit:

- KI kann zur Entwicklung sichererer Authentifizierungsmethoden beitragen, indem sie Verhaltensbiometrie und andere fortschrittliche Techniken nutzt, um die Identität von Benutzern zu verifizieren.

Erweiterte Angriffsmethoden durch KI

Automatisierte Angriffe:

- KI-Systeme können Netzwerksicherheitslücken schneller identifizieren und ausnutzen.

Soziale Manipulation:

- Einsatz von KI in Phishing-Angriffen, um glaubwürdigere und gezieltere Betrugsversuche zu erstellen.

Anpassungsfähige Malware:

- KI kann Malware entwickeln, die sich dynamisch an Sicherheitsmaßnahmen anpasst.

Schwächung der traditionellen Sicherheitsmechanismen

Bypass vorhandener Sicherheitslösungen:

- KI-Methoden können bestehende Sicherheitssysteme wie Firewalls und Antivirenprogramme anhand dynamischer Anpassung umgehen.

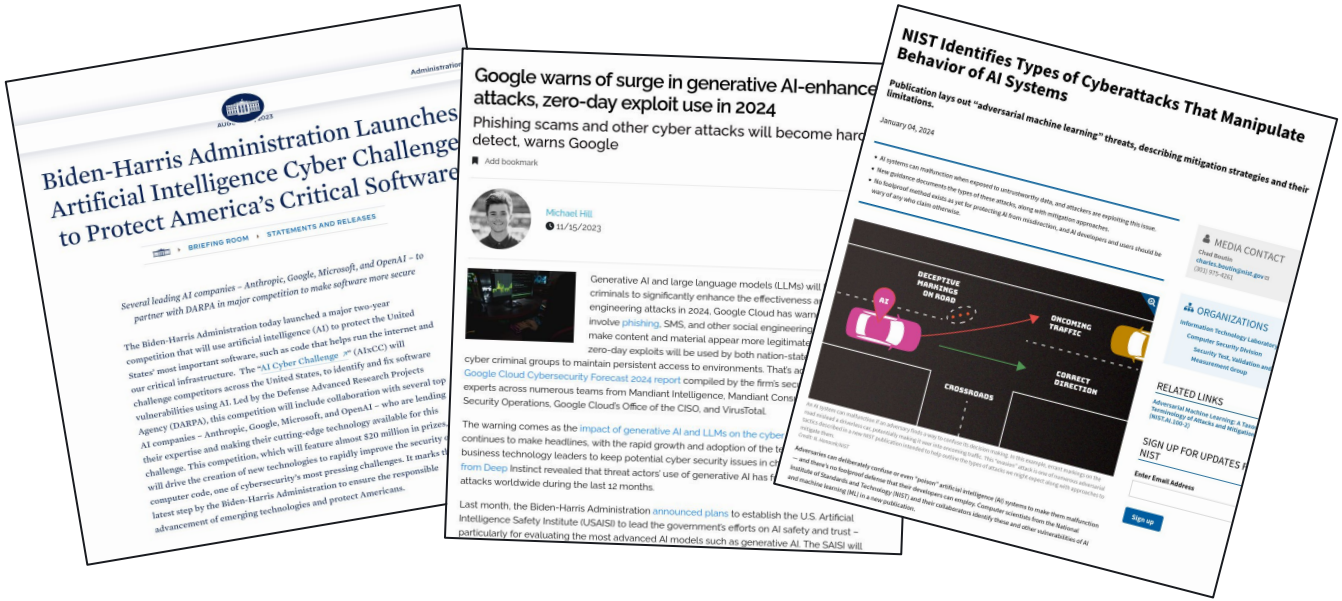
Unvorhersehbare Angriffsmuster:

- Traditionelle Sicherheitssysteme, die auf bekannten Mustern basieren, können von KI-gesteuerten Angriffen leicht überwunden werden.

Risiko der KI-Übernahme:

- Potenzielle Gefahr, dass KI-Systeme von Angreifern übernommen und gegen das eigene Netzwerk eingesetzt werden.

Beispielhafte Aktuelle Meldungen



Definition Quantencomputer

Quantencomputing ist ein **multidisziplinäres Gebiet**, das Aspekte der Informatik, Physik und Mathematik umfasst und die Quantenmechanik nutzt, um **komplexe Probleme schneller als auf klassischen Computern** zu lösen. Das Gebiet des Quantencomputings umfasst Hardwareforschung und Anwendungsentwicklung. Quantencomputer sind in der Lage, bestimmte Arten von Problemen schneller zu lösen als klassische Computer, indem sie sich quantenmechanische Effekte wie **Überlagerung und Quanteninterferenz** zunutze machen. Anwendungen, bei denen Quantencomputer eine solche Beschleunigung ermöglichen, sind Machine Learning (ML), Optimierung und die Simulation physischer Systeme.

Gefahren durch Quantencomputer für Verschlüsselung

Brechen von Public-Key-Kryptographie:

- Quantencomputer können Algorithmen wie RSA und ECC, die heute für die sichere Datenübertragung verwendet werden, effektiv brechen.

“Harvest now, decrypt later”:

- Aktuelles Sammeln verschlüsselter Informationen, um sie später via Zugriff auf Quantencomputing zu entschlüsseln

Notwendigkeit quantensicherer Algorithmen:

- Dringender Bedarf an der Entwicklung und Implementierung von quantenresistenten Verschlüsselungsverfahren.
    - Post-Quantum Cryptography (PQC)

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm