KI durch Cybersicherheit

Beschreibung: Die Technologie wächst rasant und die Welt wird von neuen Trends und Möglichkeiten geprägt. Spannende Entwicklungen finden im gesamten Spektrum von Technologien wie künstlicher Intelligenz (KI), Internet der Dinge (IOT), Cloud Computing, Augmented Reality und so weiter statt. Diese neuen Technologien haben ihre eigenen Vorteile und Herausforderungen. Schauen wir uns an, wie KI durch Cybersicherheit angetrieben wird.

Cybersicherheit (CS)

Cybersicherheit ist ein Prozess zum Schutz, zur Verhinderung und zur Erkennung unerwünschter Angriffe oder unbefugter Zugriffe. Cybersicherheit ist eine Kombination aus Menschen, Richtlinien, Prozessen und Technologien, die von Unternehmen zum Schutz ihrer Cyber-Assets eingesetzt werden. Die Cybersicherheit wird auf ein vom Unternehmen definiertes Niveau optimiert, wobei die Ressourcenanforderungen mit der Benutzerfreundlichkeit/Verwaltbarkeit und dem Grad der Risikokompensation in Einklang gebracht werden (Gartner-Glossar). Mit zunehmender Abhängigkeit und Nutzung von Technologie nehmen auch die Auswirkungen von Cyberbedrohungen und -angriffen zu. Cybersicherheitspraktiken schützen vor Bedrohungen wie Phishing, Denial-of-Service (DOS), Malware-Angriffen et.al. die ihren Ursprung intern oder extern in einem Geschäftsbereich oder sogar persönlich haben.

Darüber hinaus gibt es laut dem Bericht des digitalen Magazins Atos (2023) verschiedene Kategorien von Cyberbedrohungen, zum Beispiel:

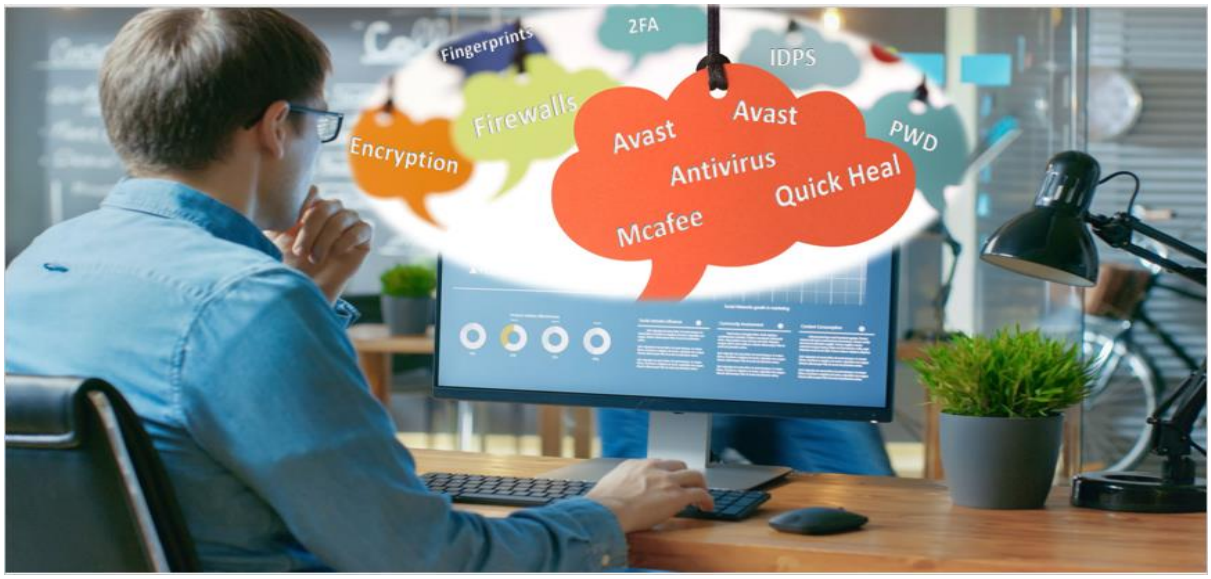
Ransomware-Bedrohungen: Es handelt sich um eine Art von bösartiger Software, die entwickelt wurde, um die Dateien des Opfers zu verschlüsseln und eine Zahlung für den Entschlüsselungsschlüssel zu verlangen.

Bedrohungen der Lieferkette: Sie zielt auf die Netzwerke und Systeme von Lieferanten und Anbietern ab, die Zugriff auf die Computersysteme und Daten eines Unternehmens haben. Diese Bedrohungen können zu Datenverlusten, finanziellen Verlusten und Reputationsschäden führen.

Cloud-Bedrohungen: Es zielt auf Cloud-Computing-Umgebungen ab, die aus der Speicherung, Verarbeitung und dem Zugriff auf Daten und Anwendungen auf Servern von Drittanbietern mit Internetzugang bestehen.

Mobile Bedrohungen: Es zielt auf mobile Geräte ab, auf denen sensible Daten gespeichert sind und die sowohl für private als auch für berufliche Zwecke verwendet werden.

Mit der Weiterentwicklung der Technologie und der zunehmenden Verbreitung in unserem täglichen Leben steigt auch die Wahrscheinlichkeit von Cyberangriffen. Die Technologiespezialisten entwickelten daraufhin Möglichkeiten, sich gegen Cyberangriffe zu verteidigen. Diese Cybersicherheitslösungen können nach ihrer Funktionalität klassifiziert werden, z. B. Netzwerksicherheit, Datensicherheit, Anwendungssicherheit, Cloud-Sicherheit, Zugriffsverwaltung usw. Diese Lösungen schützen sensible Informationen und wahren gleichzeitig die Vertraulichkeit der Daten.



Künstliche Intelligenz (KI)

Künstliche Intelligenz ist ein Schlagwort, das viel Lärm verursacht, sei es in der Wirtschaft, in der Forschung oder im Bildungswesen. Nach NIST-Definition ist KI ein Zweig der Informatik, der sich auf die Erstellung von datenverarbeitenden Systemen konzentriert, die Aktivitäten wie Denken, Lernen und Selbstverbesserung ausführen können, die typischerweise mit menschlicher Intelligenz in Verbindung gebracht werden. Es kann als ein System zusammengefasst werden, das Aufgaben wie wahrnehmungsbasierte Entscheidungsfindung und Verarbeitung natürlicher Sprache ausführt, die normalerweise den menschlichen Intellekt erfordern würden. Lassen Sie mich Ihnen ein Beispiel geben: Wenn Sie Bilder auf Facebook hochladen, können Sie beobachten, dass das System Gesichter erkennt und automatisch Personen im Bild markiert. Das System scannt die verfügbaren Daten mithilfe von Algorithmen des maschinellen Lernens, um Gesichter zu erkennen und Muster zu erkennen, die es ermöglichen, Gesichter genau Menschen zuzuordnen. Facebook verwendet eine KI-gesteuerte Gesichtserkennungstechnologie, die mit Deep-Learning-Algorithmen arbeitet, um die Gesichtsmuster der Personen erkennen zu können.

Welchen Beitrag leistet künstliche Intelligenz im Bereich der Cybersicherheit?

Kurz gesagt können wir sagen, dass KI ein Enabler für die Cybersicherheit ist. KI hat das Potenzial, Cyberangriffe zu erkennen, zu verhindern und darauf zu reagieren, wodurch die Effektivität von Cybersicherheitslösungen verbessert wird. Zum Beispiel:

- KI-Algorithmen helfen dabei, Datensätze zu analysieren und Trends zu finden, die auf potenzielle Cyberangriffe hindeuten;

- Es analysiert auch die Verhaltensmuster eines Schadsoftware-Virus und bewertet die Risiken;

- KI hat das Potenzial, Authentifizierungsverfahren zu verbessern;

- KI kann Reaktionen auf wahrscheinliche Angriffe automatisieren und die Reaktionszeit und den Schaden reduzieren, während sie gleichzeitig zukünftige Angriffe vorhersagt.

uf der anderen Seite nutzen Hacker oder Cyberkriminelle auch KI, um die Wirkung ihrer Angriffe zu erhöhen. Cyberkriminelle verwenden KI-gesteuerte Methoden, um komplexe Techniken zu entwickeln, um sich der Erkennung zu entziehen und Computersysteme und Netzwerke zu infiltrieren.

In der Zwischenzeit nimmt die Cyberkriminalität kontinuierlich zu, da wir immer mehr Technologie einsetzen. Security Operations Analysten (SOAs) konzentrieren sich auf KI, um potenzielle Angriffe zu erkennen. Darüber hinaus bemühen sie sich um eine Anpassung, um einzigartige Eigenschaften zu integrieren, die die Reaktionszeit auf solche Angriffe erheblich

minimieren. Wir wissen, dass KI Cybersicherheitslösungen unterstützt. Lassen Sie uns beleuchten, ob Cybersicherheit besser ist als KI.

Auf der einen Seite bietet die Cybersicherheit jedoch Lösungen oder Strategien zum Schutz von Systemen, und KI erstellt intelligente Muster, um diese Lösungen effektiv anzuwenden und ein besseres Ergebnis zu erzielen. CSET (Center for Security and Emerging Technology) arbeitet an einem Projekt namens CyberAI. Ziel des Projekts ist es, Cyberoperationen und -prävention mithilfe von KI zu automatisieren. Laut einem Beitrag von Deloitte Insights (Tech Trends, 2022) können Unternehmen mithilfe von CyberAI möglicherweise schneller reagieren als ein Angreifer. Es kann ihnen auch helfen, den nächsten Schritt eines Angreifers vorherzusagen und eine sofortige Reaktion vorzubereiten. CyberAI-Tools und -Technologien befinden sich noch in der Anfangsphase der Einführung. Darüber hinaus heißt es in dem Beitrag, dass KI als Multiplikator fungieren kann, der Tech-Profis dabei unterstützt, zeitintensive Aufgaben zu automatisieren und die Eindämmung und Reaktion zu beschleunigen.

Das Hauptziel der Cybersicherheit ist der Schutz von Systemen, Netzwerken, Daten usw., und KI kann zur Stärkung der Cybersicherheitsabwehr eingesetzt werden. Daher sind sowohl Cybersicherheit als auch KI wichtig, um die sich entwickelnden Cyberbedrohungen zu bewältigen.

Verweise

CNBC Business. (2022, Sep13). Künstliche Intelligenz spielt eine größere Rolle in der Cybersicherheit, aber die bösen Jungs können am meisten profitieren. AI has bigger role in cybersecurity, but hackers may benefit the most (cnbc.com)

Deloitte Insights. (2022). CyberAI : Echte Verteidigung. The future of cybersecurity and AI | Deloitte Insights

Gartner-Glossar, Definition of Cybersecurity - Gartner Information Technology Glossary

NIST-Definitionsglossar, Labor für Informationstechnologie, Ressourcenzentrum für Computersicherheit, CSRC Topics - artificial intelligence | CSRC (nist.gov)

PWC-Publikation. (2021). Ausgleich von Macht und Schutz: KI in der Cybersicherheit und Cybersicherheit in der KI. pwc-balancing-power-protection-ai-cybersecurity.pdf

Bedrohungsprognosen für -2023. (2023). The top 10 cybersecurity threats for 2023 - Atos