Cybersicherheitsagentur Baden-Württemberg
(CSBW)

Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: **KI-gestützte Cyberangriffe und Verteidigungsstrategien**

Wie kann KI für und gegen Cyberangriffe eingesetzt werden?

Der Einsatz von Künstlicher Intelligenz (KI) in der Cybersicherheit verändert die Bedrohungslandschaft erheblich. Dabei ermöglicht KI sowohl leistungsfähigere Angriffe als auch effektivere Verteidigungsmethoden. Diese Entwicklung führt zu einer Transformation der gesamten Cybersicherheitslandschaft.[1]

Wie kann KI für Cyberangriffe genutzt werden?

Social Engineering-Angriffe:
KI ermöglicht die Erstellung täuschend echter Inhalte für Phishing-Angriffe. Deepfakes und KI-gesteuerte Chatbots können personalisierte und überzeugend echte Nachrichten generieren.[2] Außerdem können KI-Tools das Internet (insbesondere Soziale Medien) durchsuchen, um möglichst viele Informationen für Phishing zu sammeln.[3]

Inhaltsgeneration durch Sprachmodelle (LLMS):
Große Sprachmodelle können plausible Fake-Websites und überzeugende Texte für Desinformationskampagnen erstellen.

KI-basierte Schadcodegenerierung:
KI ermöglicht die Erstellung komplexer Malware (Schadsoftware) und die dynamische Anpassung von Schadprogrammen, um Erkennungsmechanismen wie z.B. Virenschutz-Programme zu umgehen.

Kompromittierung von Zugangsdaten:
KI-Algorithmen können wahrscheinlich gewählte Passwörter basierend auf dem Benutzerverhalten und psychologischen Profilen der Nutzenden vorhersagen.

Desinformation und Fake-News:[4]
KI-Systeme können durch die Analyse von Benutzerverhalten und Präferenzen auf eine Zielgruppe zugeschnittene Falschinformationen generieren. Eine Verbreitung

von Fehlinformationen über verschiedene Plattformen hinweg ist für KI-Algorithmen ebenfalls leicht möglich.

Echtzeit-Exploitation:
KI-gesteuerte Scans können Sicherheitslücken in Echtzeit identifizieren und ausnutzen.

Jailbreaks:
Ausgeklügelte Eingabesequenzen können Sicherheitsfilter in KI-Systemen umgehen und sie zur Generierung von Schadcode oder anderen unerwünschten Inhalten manipulieren.

Wie kann KI zur Verteidigung vor Angriffen eingesetzt werden?[5]

Bedrohungserkennung:
KI-Systeme erkennen Anomalien im Netzwerkverkehr und analysieren Benutzerverhalten in Echtzeit.

Identifikation von Schwachstellen:
KI-Tools führen ständige Analysen der IT-Infrastruktur durch, um Schwachstellen zu identifizieren und deren Behebung zu priorisieren.

Erweitertes Penetration Testing:
KI-Systeme simulieren komplexe Angriffsszenarien.

Automatisierte Incident Response:
KI-gesteuerte Systeme können bei erkannten Angriffen sofortige Gegenmaßnahmen einleiten.

Prädiktive Sicherheitsanalysen:
KI-Systeme analysieren globale Bedrohungsdaten, um potenzielle zukünftige Angriffsvektoren vorherzusagen.

Worauf sollten Sie achten?

1. Achten Sie auf typische Merkmale von Phishing-E-Mails (nachzulesen in dem CSBW-Factsheet „Phishing-E-Mails“) und seien Sie vorsichtig im Umgang mit E-Mails von unbekannten Absendern.
2. Achten Sie auf typische Merkmale von Fake-Websites bevor Sie mit einer Website interagieren.
3. Gehen Sie sparsam mit personenbezogenen und vertraulichen Daten um und geben Sie nur die unbedingt erforderlichen Daten ein.

4. Informieren Sie sich regelmäßig über neue Angriffsmethoden, auch in Bezug auf Angriffe mit Hilfe von KI-Tools.
5. Schützen Sie Ihre Geräte und Online-Konten mit starken Passwörtern, aktueller Sicherheitssoftware und Multi-Faktor-Authentifizierung.

Ausführliche Informationen finden Sie in der Broschüre „KI-gestützte Cyberangriffe und Verteidigungsstrategien“. Dieses Factsheet ist eine Zusammenfassung der zentralen Punkte der Broschüre.

Quellen:

[1] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240430_Paper_Einfluss_KI_Cyberbedrohungslage.html

[2] https://digitalagentur-niedersachsen.de/social-engineering-im-zeitalter-von-ki/

[3] https://www.security-insider.de/ki-auswirkungen-auf-cyberkriminalitaet-und-ransomware-2024-a-3d0b55403e6d2b139ea222bd11ab0303/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876

[4] https://www.security-insider.de/sicherheitsbehoerden-wegen-zunahme-von-cyberangriffen-durch-ki-besorgt-a-7a86498a41f8f30ab4bcb602d85fbcf9/?cmp=nl-dd8677e7-3d55-4684-9757-84c3e76ddfb1

[5] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240430_Paper_Einfluss_KI_Cyberbedrohungslage.html

Weitere CSBW-Factsheets unter folgendem Link:
Wissen kompakt: Factsheets | Cybersicherheitsagentur

Oder QR-Code scannen:

www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 12.2024
Kontakt: schulungen@cybersicherheit.bwl.de