

KI in der Cyberkriminalität: Die doppelte Rolle als Waffe und Schutzschild

In den nächsten Jahren wird es einen regelrechten KI-Krieg geben. Auf der einen Seite stehen die verbesserten Möglichkeiten zur Erkennung und Abwehr von Angriffen, auf der anderen Seite die zunehmende Angriffsmenge und Raffinesse durch KI-optimierte Angriffsmethoden.

Künstliche Intelligenz als Waffe

Der Einsatz von KI-basierten, automatisierten Innovationen macht Cyberangriffe deutlich schneller, koordinierter und effizienter.

1. Next Level Phishing-Angriffe

Eine der größten Gefahren liegt im KI-gestützten Social Engineering. Cyberkriminelle nutzen E-Mails und Verhaltensmuster zur Erstellung täuschend authentischer Phishing-E-Mails. Die KI-basierten Systeme lernen zudem von jedem Angriff und verbessern ihre Taktiken mit jedem Phishing-Angriff.

2. KI-as-a-Service

Im Darknet bieten Cyberkriminelle KI-basierte Systeme als „KI-as-a-Service“ an. Diese vorgefertigten IT-Lösungen

ermöglichen es kriminellen Hackern, auch ohne umfassende Kenntnisse im Umgang mit KI auf komplexe Technologien zuzugreifen.

3. KI-gestützte Datenanalyse

Cyberkriminelle nutzen leistungsstarke KI-Systeme, um zielgerichteter Informationen über potenzielle Opfer zu sammeln. Als Folge davon teigen weltweit BEC-Attacken (Business Email Compromise).

4. Deepfake-Technologie

Neben Phishing-E-Mails kommen zunehmend Deepfakes zum Einsatz, die in manipulierten Audio- oder Video-Calls das Aussehen oder die Stimme einer Person perfekt simulieren.

5. Intelligente Malware

KI wird nicht nur zur Erstellung, sondern auch zur automatisierten Anpassung von Malware eingesetzt, um Erkennungsmethoden zu umgehen.

6. Detektion von Schwachstellen

KI spielt eine entscheidende Rolle, um automatisiert Schnittstellen in IT-Systemen auf Schwachstellen zu

untersuchen. Damit verbunden ist die Gefahr von Ransomware-Angriffen, da Täter effizienter vorgehen können.

7. Automatisierte Passwörterkennung

Die fortschreitende Entwicklung KI-gestützter Systeme ermöglicht bereits heute eine automatisierte Passwörterkennung durch maschinelles Lernen.

Künstliche Intelligenz als Schutzschild

KI-Sicherheitslösungen ermöglichen Echtzeit-Überwachung und gezielte Bedrohungsanalyse.

Das Security Team von CYBERCONTACT bietet als MSSP – Managed Security Service Provider einen 360°-Ansatz, der künstliche Intelligenz, Cyber Intelligence Taktiken, Verhaltensanalysen und Risikoeinschätzungen in einer einzigen Lösung vereint. Mehr dazu auf cybercontact.at

Mehr dazu auf cybercontact.at
Email: info@cybercontact.at

cyber [contact]



WERO

Lifesaving products

Mit Kompetenz, hoher Flexibilität und spezialisierten Notfallprodukten unterstützen wir Organisationen und Personen, bei der Versorgung lebensbedrohlicher Verletzungen.

WERO GmbH & Co. KG · D-65232 Taunusstein · Phone 0 61 28 / 97 57 0 · Fax 0 61 28 / 97 57 50 · medx@wero.de · www.wero.de



SOS-Kinderdorf bedankt sich für die kostenlose Einschaltung!

DU WIRST PAT'IN UND ICH WERDE ASTRONAUTIN

www.sos-kinderdorf.at

SOS KINDERDORF



© mihailomilovanovic/canva

Entspannen Sie sich, mit uns sind Ihre E-Mails sicher!

Europa ist globaler Vorreiter des digitalen Datenschutzes und lehnt sich gegen BigTechs und Desinformation auf. Gesicherte Informationen sind deswegen wichtiger denn je. Woher kommt die Information und wurde diese am Weg verändert sind Fragen, die es sich im Alltag bei allen digitalen Informationen zu stellen gilt. SEPPmail kann ganz einfach Ihre E-Mails absichern. Die Absenderidentität und die E-Mail werden auf dem Versandweg gegen Veränderung geschützt.

www.seppmail.com/at/