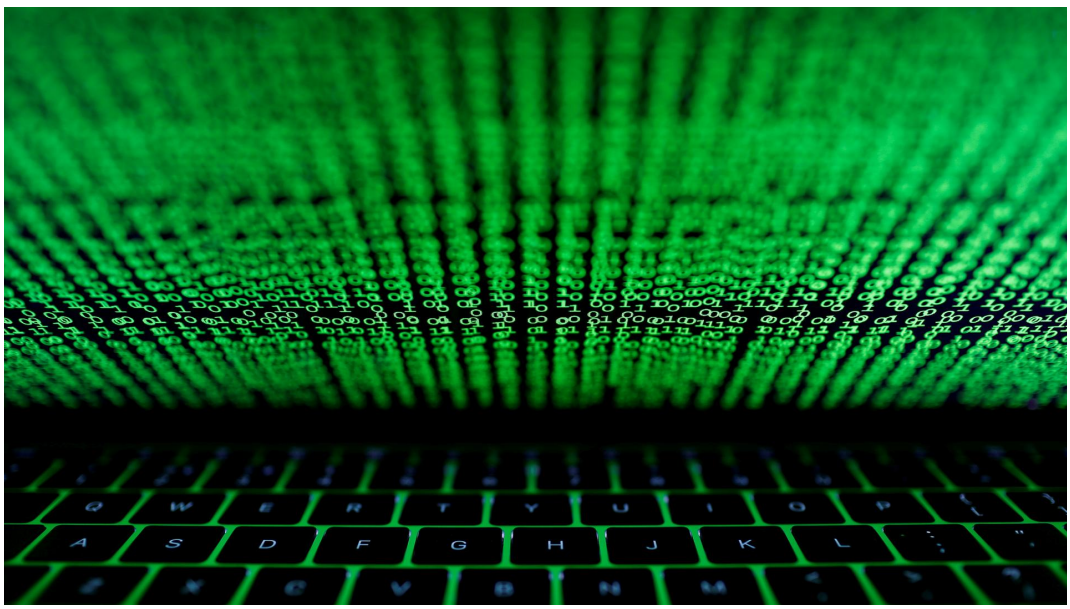
zdf.de

Cyberangriffe: Virtuelle Kampfmaschinen - ZDFmediathek

Sicherheitsspezialist Nikolai Grebennikov

10-12 minutes

Künstliche Intelligenz wird nun auch für Angriffe auf Computersysteme genutzt. Sicherheitsforscher wollen die KI-Algorithmen in Schutzsysteme einbauen. Ein rasanter Wettlauf.



KI-Systeme können jetzt zielgerichtete Programme schreiben. Quelle: reuters

Woran Cybermilitärs viele Jahrzehnte geforscht haben, das ist jetzt einsatzbereit: ein System Künstlicher Intelligenz, das vollkommen autonom Sicherheitslücken von

Computersystemen aufspüren und dafür zielgerichtete Angriffsprogramme schreiben kann. "Das System simuliert digitale Angriffe, lernt aus Misserfolgen und erfolgreichen Angriffen und entwickelt so für eine bestimmte Attacke auf ein Netzwerk oder einzelne Rechner konkrete Angriffsstrategien", erläutert Adrian Janotta, Sicherheitsberater aus Schweinfurt. Er hat selbst ein solches System mitentwickelt.

Dafür verwenden solche KI-Angriffssysteme bisher vor allen Dingen Methoden maschinellen Lernens und Software für die Mustererkennung. Diese Methoden Künstlicher Intelligenz werden bereits zur Früherkennung und Abwehr von digitalen Angriffen eingesetzt. "Häufig laufen Attacken auf Computersysteme nach einem bestimmten Muster ab", erklärt der russische Sicherheitsspezialist Nikolai Grebennikov. Er hat neuronale Netze darauf trainiert, solche Muster schon sehr früh zu erkennen.

Abwehrsysteme nutzen schon KI

> Je eher das Diagnosesystem dann solch ein typisches Angriffsmuster erkennt, desto besser kann es abgewehrt werden.

"Je eher das Diagnosesystem dann solch ein typisches Angriffsmuster erkennt, desto besser kann es abgewehrt werden", berichtet Grebennikov. Dafür hat er das System alle Detaildaten von vielen tausend Angriffen lernen lassen. Auch wie erfolgreich diese Angriffe im Einzelfall waren und was sie genau bewirkt haben, hat das KI-System gelernt.

So konnte das System dann nach der Lernphase genau prognostizieren, wo gerade ein digitaler Angriff aufgebaut wird und gegen wen er sich richten wird. "Dafür müssen allerdings auch die Daten sehr vieler Messpunkte im Internet ständig ausgewertet werden", erläutert Grebennikov. Die Technik gilt inzwischen als Abwehrstandard in der Sicherheitsforschung.

"Der methodische Lernweg bei den KI-Angriffssystemen sieht etwas anders aus", meint Sicherheitsberater Adrian Janotta. Zum Aufspüren von Sicherheitslücken setzen diese Angriffsalgorithmen nicht nur Mustererkennung ein, sondern auch traditionelle Suchmethoden wie Fuzzing. Fuzzing-Software erzeugt zufällige Daten und gibt sie an das zu untersuchende Zielsystem weiter. Eine zeitgleich mitlaufende Monitoring-Software überwacht und protokolliert, wie das zu untersuchende System auf die zufällig generierten Daten reagiert.

So wird beispielsweise ständig der Verbrauch an Rechenzeit, der Speicherbedarf oder der Abbruch eines Algorithmus überwacht. "Das gesamte Laufzeitverhalten eines Computerprogramms wird genau nachverfolgt", erläutert Professor Hartmut Pohl vom Sicherheitsunternehmen Softscheck in Sankt Augustin. Auffälligkeiten im Programmverhalten zeigen dann Sicherheitslücken an. Findet das KI-Angriffssystem eine solche Sicherheitslücke, wählt es entsprechende Angriffsprogramme aus. Adrian Janotta hat dafür auf typische Hacker-Werkzeugsammlungen wie Metasploit

zurückgegriffen. "Diese Werkzeuge hat das Angriffssystem gelernt und kann nun entscheiden, welches Werkzeug bei einer gefundenen Sicherheitslücke sich am ehesten für einen erfolgreichen Angriff eignet", sagt Adrian Janotta.

Sicherheitsforscher setzt auf das Immunsystem

> Wir müssen die KI-Angriffsalgorithmen in unsere operative Software, insbesondere in die Betriebssysteme, einbauen.
>
> Sicherheitsberater Adrien Jottta

Bisher können KI-Angriffssysteme sehr erfolgreich Computersysteme mit kombinierten Hacker-Werkzeugen angreifen. Auch sehr einfache Angriffsprogramme können sie schreiben. "Hochkomplexe Angriffssoftware setzt aber Supercomputer mit Billiarden von Rechenoperationen in der Sekunde voraus", meint Adrian Janotta. Weil solche Höchstleistungsrechner aber noch nicht so weit verbreitet sind, führen die KI-Systeme bisher eher schlichtere Angriffe aus. Doch das könnte sich bald ändern. Und dagegen hilft nur ein Mittel, ist sich Adrian Janotta sicher: "Wir müssen die KI-Angriffsalgorithmen in unsere operative Software, insbesondere in die Betriebssysteme, einbauen."

Janotta vergleicht das gern mit dem Immunsystem des Menschen. Die KI-Angriffsprogramme würden das eigene Betriebssystem in einer Simulation angreifen. Das würde den Angriff lernen und so immun dagegen werden. "Doch bis dahin liegt noch furchtbar viel Arbeit vor uns", urteilt Adrian Janotta. Und diese Arbeit müsse schnell getan werden. Denn der Wettlauf zwischen den KI-

Angriffsprogrammen und den Abwehrsystemen ist in vollem Gange.