Intelligente Abwehr

◢ Das Schlagwort **künstliche Intelligenz** (KI) ist in aller Munde. Durchbrüche bei der Rechenpower von Chips machen maschinelles Lernen sowie die Simulation neuronaler Netze möglich. Das hat zur Folge, dass KI in immer mehr IT-Bereichen zum Einsatz kommen kann – auch in der **IT-Sicherheit** gibt es interessante Szenarien. ›

◢ Die Frage, wie KI im Securitykontext funktionieren kann, ist nicht leicht zu beantworten. Es beginnt schon mit dem Problem einer korrekten KI-Definition. Die Auslegungen sind unterschiedlich und hängen vor allem von den Interessen des Definitionsgebers ab. „Es gibt einen Marketing-Hype. Zu vieles wird als KI bezeichnet, obwohl es auf programmierten Algorithmen beruht. Für mich ist es ein Wesensmerkmal der KI, dass sie selbst entscheidet“, sagt Rüdiger Trost, Cybersicherheitschef beim Virenschutzanbieter F-Secure für die DACH-Region. Im engeren Sinn gehören maschinelles Lernen und neuronale Netze zur KI. Beide Technologien werden bereits von Sicherheitsanbietern genutzt. So hilft maschinelles Lernen im Netzwerk von Unternehmenskunden in der Verhaltenserkennung, das heißt beim Aufspüren von Anomalien im Nutzerverhalten, die auf Angriffe schließen lassen. Dazu braucht das KI-System die Ausgangsdaten für normales Verhalten und für Angriffe und muss vom Hersteller anhand von Millionen gutartiger und bösartiger Dateien trainiert werden. Neuronale Netze erkennen Schadsoftware auf dem Endgerät. Sie benötigen keine Signaturen, die klassische Erkennungsmethode von Virenschutzherstellern, und sind im Vergleich dazu schneller. „Ihr Nachteil ist, dass es oft Monate dauert, bis ein neues Update kommt. Das eröffnet Hackern ein langes Zeitfenster“, sagt Stefan Strobel, Geschäftsführer des IT-Sicherheits-Beratungshauses Cirosec. Generell produziere KI aufgrund der besseren technischen Erkennung weniger Falschmeldungen als traditionelle Systeme, so Strobel. Auch betriebswirtschaftlich rät er zu den modernen Methoden, denn sie haben niedrigere Betriebskosten als die traditionellen Abwehrmittel.

Künstliche und natürliche Intelligenz ergänzen sich sehr gut. So sind Menschen oft schlicht zu langsam, um Attacken schnell genug zu verhindern. KI-Systeme, die lernen und die kleinsten Veränderungen in der Umgebung erkennen, können viel schneller reagieren, um neuartige Attacken zu erkennen und abzufangen. Der Sicherheitsanbieter Kaspersky entdeckt nach eigenen Angaben täglich 323 000 neue Schadsoftwarevarianten. „Es gibt keine Möglichkeit, mit einer solch großen Anzahl von Bedrohungen umzugehen, ohne maschinelles Lernen einzusetzen. Zudem ermöglicht es den Cybersicherheitsspezialisten, das Risiko menschlicher Fehler zu beseitigen“, teilt Kaspersky-Pressesprecher Stefan Rojacher mit. KI kann außerdem Lücken füllen, die der grassierende Fachkräftemangel hinterlässt, und den menschlichen „Kollegen“ entlasten. Der Schwachpunkt der Maschinen ist allerdings ihre (noch) fehlende Kreativität. „Menschliches Wissen ist notwendig, um zu erkennen, wie groß die Tragweite einer identifizierten Gefahr ist. Außerdem können nur Menschen einen Plan entwickeln, wie auf diese Szenarien reagiert werden muss, sich einen Überblick verschaffen und mit der KI zusammen an der perfekten Lösung arbeiten“, schreibt F-Secure in seinem Blog. Die neuen Technologien sind schlicht noch nicht reif genug, um raffinierte und gezielte Angriffe eigenständig bekämpfen zu können. Und so arbeiten Mensch und Maschine in modernen Systemen Seite an Seite, um mit ihren jeweiligen Stärken die Gesamtsicherheit zu verbessern. Einen Blick in die Zukunft warf der Wettbewerb „Cyber Grand Challenge“ der DARPA, einer Forschungseinrichtung des US-Verteidigungsministeriums. Er demonstrierte mit Experimentalprojekten das Fernziel: Computer suchen selbstständig nach Sicherheitslücken und schließen sie eigenhändig. Einige autonom agierende und nur untereinander vernetzte Rechner übten sich gleichzeitig in Angriff und Verteidigung. Sie waren unter anderem dazu in der Lage, ihre eigene Systemsoftware zu reprogrammieren. In diese Richtung könnte sich die IT-Sicherheit entwickeln: Autonome Systeme mit KI-Unterstützung schließen eigenständig Lücken. Die Zeitspanne zwischen dem Erkennen einer Schwachstelle und ihrer Reparatur mit einem Patch wäre deutlich kürzer als heute – und KI in der IT-Sicherheit endgültig mehr als nur ein Hype.

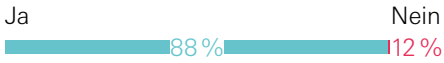
Autor: Ulrich Hottelet

◢ Schlaue Angreifer.
Bläst KI zum Angriff?

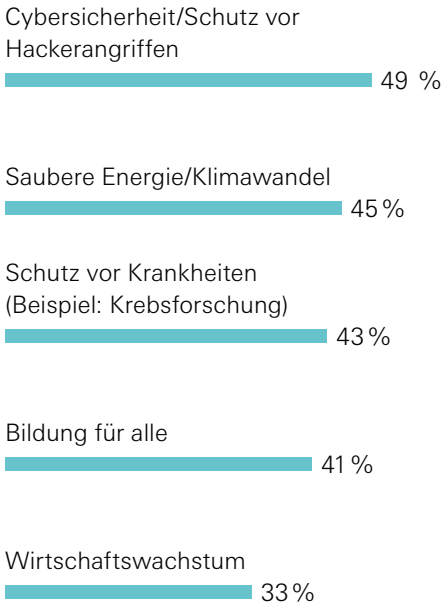
Während KI in der IT-Sicherheit zur Verteidigung bereits eingesetzt wird, ist ihre Nutzung zu Angriffszwecken zumindest in der Breite noch eher Zukunftsmusik. Fachleute halten das aber für möglich. Schließlich haben dieses Jahr die Würmer NoPetya und WannaCry, die Schwachstellen suchen und sich im Netz ausbreiten, große Schäden verursacht und zur angreifenden KI ist es von dort nur noch ein gradueller Schritt. Die Budgets von Staaten, Geheimdiensten und organisierter Kriminalität sind ausreichend groß, um ausgefeilte KI-Systeme zu entwickeln. Für viele Hacker wird es aber schwierig werden, sich die zugrunde liegende riesige Datenbasis zu verschaffen. KI gegen KI ist also durchaus denkbar.

◢ KI – die Antwort auf all unsere Probleme?

Hilft künstliche Intelligenz, zukünftige Herausforderungen zu meistern?



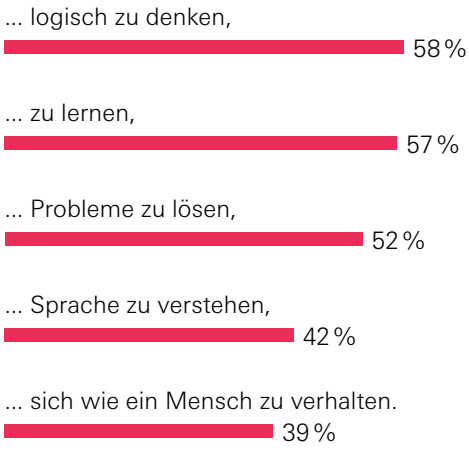
Künstliche Intelligenz kann in folgenden Bereichen eine Hilfe sein:



Quelle: PwC

◢ Was glauben Sie, macht künstliche Intelligenz aus?

Die Fähigkeit von Geräten und Software,



Quelle: Pegasystems

Fotos: Shutterstock/Phonlamai Photo, Shutterstock/Liu zishan