FATA MORGANA SICHERHEIT

Der Glaube an Technik ist unerschütterlich: Künstliche Intelligenz soll jetzt auch Informationstechnik und Daten sichern. Doch bei ihrem Einsatz werden viele ungelöste Probleme übersehen und die Technik überschätzt.

CYBERSICHERHEIT /// AUTOMATISIERUNG /// MACHINE LEARNING

VON DR. AMIR ALSBIH

Das Interesse, Sicherheitsmaßnahmen zu automatisieren, steigt. Einer Untersuchung von Research and Markets zufolge sollen smarte Sicherheitssysteme bis 2023 ein Marktvolumen von rund 18,2 Milliarden US-Dollar erreichen. Künstliche Intelligenz (KI) kann IT-Sicherheit verbessern helfen. Allerdings besteht die Gefahr eines Wettrüstens, das mehr Probleme schafft.

Ob KI im Sicherheitsbereich sinnvoll eingesetzt wird, hängt davon ab, ob ihre Möglichkeiten verstanden werden. Die Geschichte zeigt, dass der Glaube an Technik nur schwer zu erschüttern ist: Die Titanic galt als unsinkbar. Angeblich sollen dank Algorithmen Finanzkrisen der Vergangenheit angehören. Doch oft ist der automatisierte Aktienhandel für plötzlichen Kursverfall verantwortlich. KI wird zurzeit sehr optimistisch gesehen und kommt daher auch bei der IT-Sicherheit zum Einsatz. Wird dabei aber zu stark auf die Kraft der Daten vertraut, entsteht eine Fata Morgana – ein trügerisches Bild von Sicherheit. KI ist allenfalls ein Hilfsmittel, ein Allheilmittel ist sie nicht.

18,2

Mrd. US-Dollar weltweit sollen im Jahr 2023 für smarte Sicherheit ausgegeben werden.

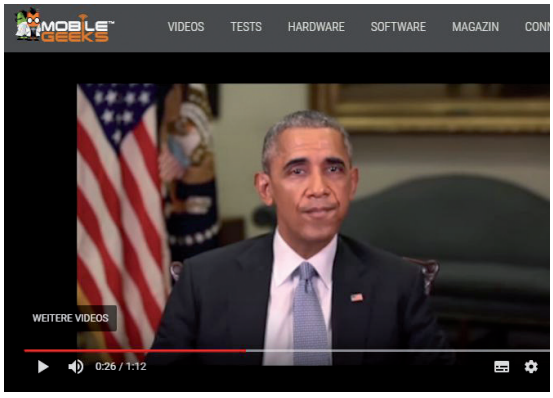
Quelle: Alsbih

Während Sicherheitsteams fieberhaft an Abwehrmaßnahmen gegen Cyberangriffe feilen, arbeiten Hacker ebenfalls mit Algorithmen und KI, um Lücken in IT-Systemen aufzuspüren. Auf dieses Risiko weist der Bericht „The Malicious Use of Artificial Intelligence“ hin. Hier stellen 26 Wissenschaftler fest: Die Ausbreitung von KI führe zu deutlich mehr Datendiebstählen oder Angriffen auf Netzwerke. Wie raffiniert lernende Programme Sicherheitsmaßnahmen überwinden können, zeigt zudem ein Beispiel aus den USA: Dort kreierten Techniker mit Hilfe eines Algorithmus einen künstlichen Fingerabdruck, um Smartphones zu entsperren. Rund 65 Prozent ihrer Versuche funktionierten.

MANIPULATION UND FÄLSCHUNG

Es könnte noch schlimmer kommen: Deep Fakes, Fotos, Video- und andere Mediendateien, die von KI erstellt werden und falsche Informationen enthalten, ergänzen die Risiken. Mit Hilfe von Morphing-Techniken lassen sich Gesichter in Pornofilme integrieren, die unbeteiligten Menschen ähneln. Das Nachrichtenportal Buzzfeed demonstrierte das mit einem Video, in dem Vorgänger Barrack Obama den US-Präsidenten Trump beleidigt. Stimme, Mimik und Gestik ergeben eine perfekte Illusion. Verfälschte Nachrichten manipulieren nicht nur Jugendliche, auch Profis fallen darauf herein. Erpressung und Verleumdung finden so neue Spielarten. In der IT-Security könnten folglich ganz neue Formen des Social Engineering entstehen: etwa, wenn der Chef plötzlich per Videobotschaft nach den Zugangsdaten fragt.

Deterministische Algorithmen kommen in vielen Programmen zum Einsatz. Bei identischem Input gibt es immer ein identisches Ergebnis. Ist von KI-Systemen die Rede, ist damit meistens maschinelles Lernen gemeint. Dabei bekommt ein System eine ganze Menge Daten als Input und lernt, daraus Muster zu erkennen. Damit kann es für verschiedene Aufgaben eingesetzt werden: zur Klassifizierung



ALLES FAKE: Die Trump-Schelte von Barrack Obama per Video wurde technisch produziert. Das Video findet sich hier: https://www.mobilegeeks.de/video/deepfake-falscher-obama-beschimpft-trump/

SICHER IST SICHER

Unsichere Passwörter: Logins mit Authentifizierung über einen Faktor sind nicht sicher. Eine Zwei- oder Multi-Faktor-Authentifizierung schafft mehr Optionen zur Sicherung digitaler Identitäten.

Zugänge regeln: Das Identity- und Access-Management regelt den Zugriff auf Programme und Daten .

Patch-Management: Regelmäßige Software-Updates in kurzen Abständen verhindern, dass Einfallslücken länger offenbleiben.

Informieren: Mitarbeiter sollten Teil des Sicherheitskonzeptes werden. Schulungen und Regeln helfen beim Durchsetzen von Vorgaben.

Analyse: Es gibt keine absolute Sicherheit. Die Analyse von Anwendungsfehlern und Attacken verbessert die Schutzmaßnahmen.

von Daten etwa, zum Clustern von Ähnlichkeiten bei Produkten. Da das System auf Grundlage von Daten lernt, nimmt es auch die darin enthaltenen Fehler auf: Microsofts Chatbot Tay wurde als selbst lernende Software gepriesen und musste vom Netz genommen werden, weil sie auf Sprache zunehmend menschenfeindlich reagierte. Auch in der Strafverfolgung orientiert sich KI oft an der Hautfarbe – und diskriminiert. Autonome Fahrzeuge bauen Unfälle, weil die Systeme Schilder falsch klassifizieren, nach kleinen Manipulationen erkennt KI heute kein Gesicht mehr. Das alles zeigt: Die Kontrolle digitaler Identitäten zu automatisieren, ist noch alles andere als ratsam.

Laut Ponemom-Studie wendet ein Security-Team mehr als 20.000 Stunden im Jahr für die Durchsicht von Warnungen auf. Unternehmen erhoffen sich hier von der KI enorme Entlastung. Doch smarte Systeme lernen je nach Umgebung unterschiedliche Dinge, ihre Entscheidungen sind daher unvorhersehbar. Außerdem können sie einen Angriff oder ein Schadprogramm als gut einstufen. Hält sich eine Führungskraft zum Beispiel im Ausland auf, verändern sich damit oft Einlog- oder Zugriffszeiten. Das dürfte eine KI verwirren: Verweigert sie dann den Zugriff und meldet sie die Abweichung?

AUSNAHMEN ÜBERFORDERN KI

Wo aber für viele Situationen Ausnahmen erstellt werden müssen, wird KI unsicher. Der Mehrwert von maschinellem Lernen ist bei der Erkennung von Krebszellen unbestritten, in der IT-Sicherheit verursacht sie immer noch mehr Nachteile. Denn hier setzen nur wenige Unternehmen aktuelle Technik ein: Regelmäßige Software-Updates in kurzen Abständen gehören nicht überall zum Standard, auch die Identifizierung von Berechtigten mit mehreren Faktioren nicht. Eine Kombination dieser Maßnahmen reduziert jedoch das Risiko eines Angriffs um mehr als 80 Prozent.

KI kann in der IT-Sicherheit helfen, große Datenmengen zu analysieren oder als Spürhund Anomalien aufzudecken. Wie diese aber zu bewerten sind, sollten noch Menschen entscheiden. Ein Blick auf die wichtigsten Sicherheitslücken zeigt, dass smarte Systeme dagegen wenig ausrichten können: Laut Verizon sind gestohlene Zugangsdaten die Hauptursache für Datendiebstahl. 73 Prozent der Attacken kamen von außen, 28 Prozent von innen. Und 96 Prozent aller Datendiebstähle werden erst nach Monaten entdeckt.

96%

der Daten-Diebstähle werden erst nach Monaten entdeckt.

Quelle: Verizon

Passwörter müssen außerdem auch nicht erst erraten oder gestohlen werden. Sie lassen sich durch falsche Telefonate und Fake-Mails in Hektik und Stress leicht vom Nutzer erpressen oder auch im Darknet ersteigern. Es ist also an der Zeit, die wahren Probleme anzugehen und KI als das zu begreifen was sie in Sicherheitsfragen ist: ein Assistenztool.

DER AUTOR

DR. AMIR ALSBIH

führt die Geschäfte von KeyIdentity. Das Unternehmen bietet Identity- und Access-Management-Lösungen an. Info: www.keyidentity.de