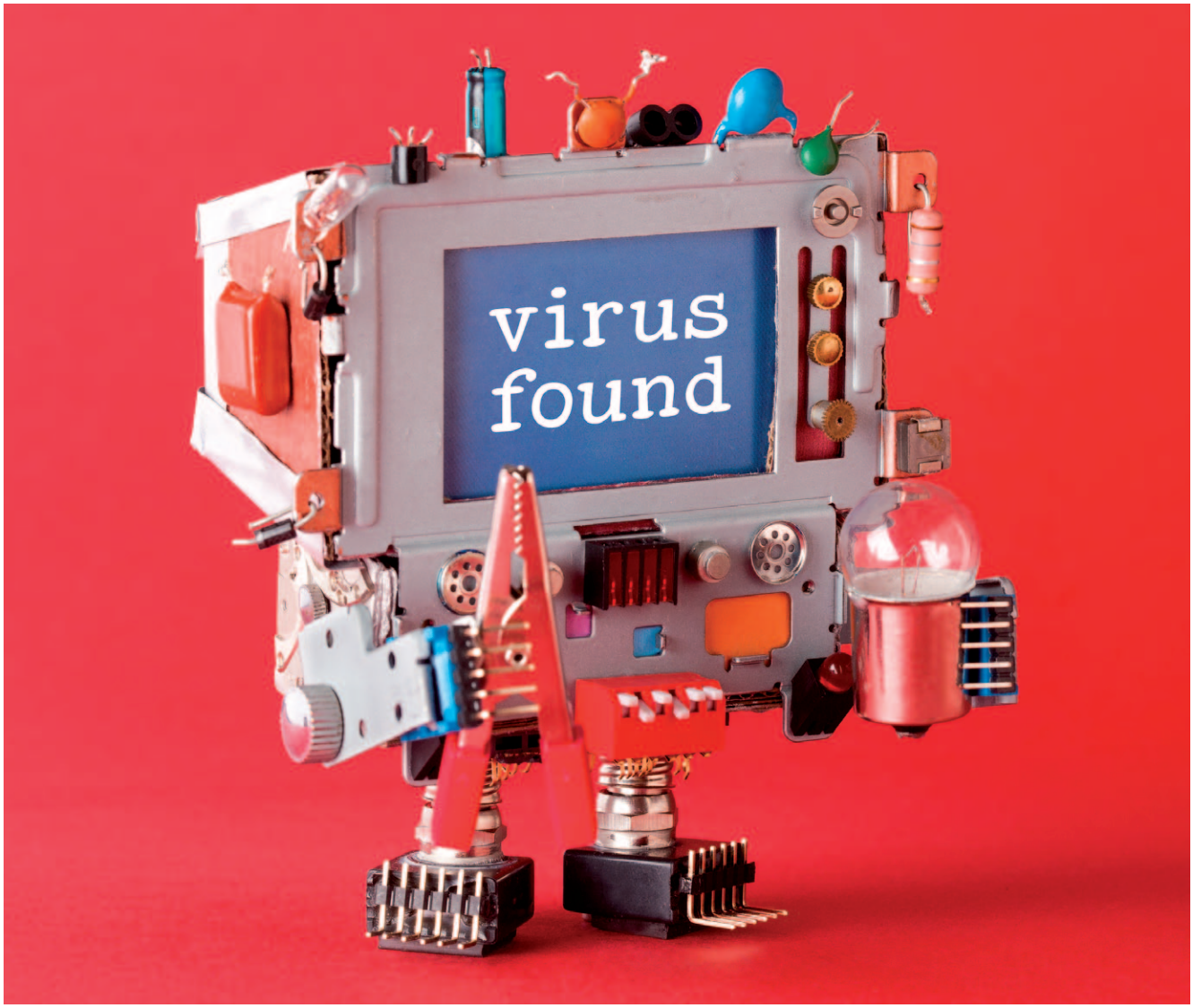

Künstliche Intelligenz in der IT-Security

Intelligente Helfer aus dem Labor

Der Einsatz künstlicher Intelligenz kann die IT-Sicherheit erhöhen, da die raren Experten entlastet werden. Wunder darf man aber keine erwarten. **Von Jens Stark**

Spezialisten für IT-Security werden regelrecht mit Sicherheitsmeldungen bombardiert: Jedes einzelne Unternehmen verzeichnet gemäss dem «IBM X-Force Threat Intelligence Index 2017» durchschnittlich 54 Millionen Vorkommnisse pro Jahr. Die Security-Teams müssen also einer unvorstellbaren Menge automatisch generierter Hinweise aus den diversen Komponenten wie Firewalls und Intrusion-Detection-Systemen nachgehen. Dabei handelt es sich oft um Fehlalarme. 20 000 Stunden pro Jahr verplempern hoch qualifizierte Fachkräfte damit, diesen sogenannten «False Positives» nachzujagen, rechnet IBM vor.

Da die Cyberangriffe immer komplexer werden und die Hacker mit allerlei Verschleierungstaktiken operieren, kann aus einem einzelnen «Event», den ein Überwachungssystem

Bild: Shutterstock/Besjunior

meldet, noch nicht ausgeschlossen werden, ob es sich tatsächlich um einen Angriff handelt. Erst die geschickte Kombination verschiedener Ereignisse lässt den geschulten Experten die eigentliche Attacke erkennen.

Besserung ist nicht zu erwarten – im Gegenteil, die Angriffsfläche weitet sich ständig aus. Reichte es früher aus, dass sich Security-Teams um die Sicherheit im Netzwerk und an den Endpunkten kümmerten, sind mittlerweile Applikationen, Cloud-Dienste und mobile Geräte hinzugekommen. Ganz zu schweigen von der bevorstehenden Lawine an sicherheitsrelevanten Vorkommnissen, die das Internet der Dinge in den nächsten Jahren lostreten wird.

Hoffnungsträger KI

Es ist daher kaum verwunderlich, dass gerade die IT-Security grosse Hoffnungen in Systeme setzt, die auf künstlicher Intelligenz (KI) basieren. Methoden wie maschinelles Lernen und intelligente Mustererkennung sollen dazu führen, dass IT-Security-Teams bei leidigen Routineaufgaben entlastet werden, zumal es kaum eine Branche gibt, die unter einem derart grossen Fachkräftemangel leidet.

«Allgemein wird es darum gehen, die immensen Datenmengen, die heute im Sicherheitsbereich anfallen, überhaupt bewältigen zu können und dabei die Erkennung auch von noch unbekannten Gefahren zu verbessern», umschreibt Reto Häni, Partner und Leiter Cybersicherheit bei PwC Digital Services, das primäre Einsatzgebiet von künstlicher Intelligenz in der IT-Security.

Laut Dario Tizianel, Security Business Unit Leader bei IBM Schweiz, werden KI-Systeme darüber hinaus auch für die Überbrückung von Wissenslücken in der Vorfallsanalyse und als Entscheidungshilfe bei der Behandlung von Vorfällen verwendet. «Wir wollen unsere Sicherheitslösungen durch kognitive Systeme erweitern. Um Systeme also, die in der Lage sind zu verstehen, zu schlussfolgern und zu lernen», erklärt Tizianel.

Erst am Anfang der Entwicklung

Allerdings steht man beim Einsatz künstlicher Intelligenz in der IT-Security noch ziemlich am Anfang, gibt Jan Alsenz zu bedenken. Alsenz ist bei Oneconsult, einem Schweizer Spezialisten für Penetration Testing, als Chief Research Officer tätig. «Aktuell werden überwiegend auf Regeln und Binärmustern basierende Technologien eingesetzt», berichtet er und betont, dass auch die meisten Systeme, die in Kürze auf den Markt kämen, hierauf aufbauten. Auf einer grossen Datenbasis werde einerseits der komplette Netzwerkverkehr überwacht oder das Verhalten von Programmen und Nutzern analysiert. Andererseits würden statistische und heuristische Analysen der Daten durchgeführt, um Anomalien zu erkennen. Fast alle bekannten Security-Systeme wie Antiviren-Software, Spam-Erkennungslösungen und Systeme zur Erkennung und Abwendung von Einbruchsversuchen ins Netzwerk verwendeten diese Komponenten. So gibt es ihm zufolge seit Kurzem verhaltensbasierte Malware-Erkennung oder es könnten Anomalien im Netzwerk festgestellt werden.

«In Zukunft wird der Mensch die Zusammenhänge analysieren und Kreativität einbringen, während die KI die Routineaufgaben übernimmt»

Reto Häni
PwC Digital Services

Theoretisch wäre mit künstlicher Intelligenz noch weit mehr möglich. Doch «Systeme, die über die Fähigkeit verfügen, Schlussfolgerungen zu ziehen, die über statistische Korrelationen oder vorgegebene semantische Beziehungen hinausgehen, existieren aktuell für keinen Bereich», sagt Alsenz. Das heisse nicht, dass die aktuellen Lösungen schlecht seien. Aber: «Sie bringen derzeit nur für bestimmte Nischen einen Nutzen und müssen teilweise noch mit erheblichem Aufwand ‹angelernt› werden.»

Grosses Potenzial

Entsprechend gross ist das Potenzial von KI-Methoden. Letztlich wird an Systemen gefeilt, welche die Effektivität von Cybersecurity-Spezialisten erhöhen sollen. «Stellen Sie sich vor, dass uns nicht nur Siri, Cortana oder Alexa unterstützen, sondern, dass wir dereinst eine persönliche KI zur Seite gestellt bekommen. Diese lernt unsere Art des Arbeitens, entlastet uns von Routine und bereitet uns Informationen so auf, dass wir die Zusammenhänge einfacher und schneller erkennen können», skizziert Häni von PwC seine Zukunftsvision. «Von diesem Szenario sind wir zwar noch ein paar Jahre entfernt, aber die Forschung macht hier grosse Fortschritte.»

Alle derzeit entwickelten Lösungen sind daher noch in einer Lernphase. IT-Security-Spezialisten beurteilen die Ergebnisse der Systeme und füttern diese wieder mit ihren Erkenntnissen. Im Grunde passiert derzeit im Security-Bereich nichts anderes, als was man aus anderen KI-Anwendungen kennt. So fütterten Google und Facebook ihre Bild- und Gesichtserkennungssysteme jahrelang mit dem Feedback ▶

der Anwender, bevor erste Automatismen zu greifen begannen. Und selbst danach sind die KI-Systeme noch auf den Input des Menschen angewiesen, etwa um eine falsche Zuordnung zu korrigieren, wenn ein Bild einer falschen Person zugewiesen wird.

KI entdeckt Schwachstellen

Mit KI lassen sich nicht nur IT-Systeme und Netzwerke besser absichern. Entsprechende Techniken können auch zur Auffindung von Schwachstellen genutzt werden. Demonstriert wurde dies im letzten Jahr an der Cyber Grand Challenge, die von der Darpa (Defense Advanced Research Projects Agency), dem Forschungsarm des Pentagons, ausgetragen wurde. Sieben KI-Systeme traten dabei gegeneinander an und stellten unter Beweis, dass sie in der Lage sind, Sicherheitsschwachstellen aufzufinden. Gewinner des Wettbewerbs wurde das an der Carnegie Mellon University entwickelte System «Mayhem», das trotz zeitweisem Ausfall die Konkurrenz deplatzierte.

Zu viel Euphorie ist allerdings auch hier fehl am Platz. So seien die Testbedingungen an der Darpa-Challenge streng kontrolliert gewesen, kommentiert Alsenz den Wettbewerb. «Die zu findenden und zu behebenden Fehler waren im Wesentlichen auf Speicherfehler begrenzt», sagt er. Im Gegensatz zu logischen oder semantischen Fehlern seien diese vergleichsweise einfach durch automatische Analysen zu er-

«Aktuelle Systeme können noch keine Schlussfolgerungen jenseits von statistischen Korrelationen oder vorgegebenen semantischen Analysen ziehen»

Jan Alsenz
Oneconsult

Konkrete KI-Lösungen in der IT-Security

Es passiert derzeit viel im Bereich IT-Security und künstliche Intelligenz. Kaum eine Woche vergeht, in der nicht ein Start-up eine neue Lösung präsentiert. Aber auch Branchenriesen wie IBM, Google, Microsoft und Amazon forschen, entwickeln und präsentieren laufend Produkte, die KI für eine verbesserte IT-Security nutzen.

Watson for Cyber Security: Bereits seit einiger Zeit füttert IBM seine Plattform für kognitive Intelligenz mit Dokumenten zur IT-Sicherheit. Dabei wurde dem System sukzessive das nötige Security-Wissen antrainiert, indem die Texte zunächst von menschlichen Experten analysiert und mit Anmerkungen versehen wurden. Beispielsweise wurde Watson beigebracht, was ein Virus oder ein Wurm im Security-Kontext bedeutet. So geschult, konnte Watson sodann weitere Dokumente selbstständig analysieren und eine Wissensdatenbank aufbauen, die ständig durch die Konsultation einschlägiger Security-Blogs und -Webseiten erweitert wird. Mittlerweile greifen Produkte wie «QRadar Advisor with Watson» auf die Wissensdatenbank zu und erleichtern IT-Security-Researchern die Arbeit bei der Analyse von Bedrohungen. Der Schweizer Finanzdienstleister Six will ein Security Operations Center (SOC) auf Basis des kognitiven Systems von IBM auf die Beine stellen und künftig den Bankensektor mit entsprechenden Services beliefern.

Secure Terrain von PwC: Zapft Googles immense Cloud-Rechenleistung an und verwendet KI-Techniken, um grosse Volumen von strukturierten und unstrukturierten Daten zu analysieren. Diese vergleicht es mit entsprechenden Erkenntnissen zu bestehenden Angriffen und nimmt eine Priorisierung möglicher Antworten auf die Gefahr vor.

SlashNext: Das Start-up SlashNext wurde von einem ehemaligen Mitarbeiter von FireEye gegründet. Die Lösung von SlashNext soll sogar Angriffe mit Social-Engineering-Methoden erkennen können. So soll sie Phishing-Attacken identifizieren, indem sie analytisch wie ein Mensch vorgeht und erkennen kann, dass beispielsweise die vorgegaukelte Webseite eine falsche URL aufweist.

Deep Instinct: Das israelische Start-up Deep Instinct hat nach eigenen Angaben eine KI-Engine entwickelt, die auf jedem Endpoint, also auch auf Laptops und Smartphones, zum Einsatz kommen kann und diese so absichert. Das Herzstück der Lösung, D-Brain, wird zentral gehostet und ständig anhand frisch entdeckter Malware-Samples trainiert. Es liefert die Updates an gestauchte Versionen des KI-Systems auf den Clients. Da diese Appliances auch selbstständig Analysen durchführen können, müssen sie nicht dauernd mit der Zentrale in Verbindung stehen.

AI²: Die kürzlich präsentierte Plattform AI² soll laut den Wissenschaftlern am MIT (Massachussetts Institute of Technology) bereits 85 Prozent der Cyberangriffe erkennen und voraussagen können. Das System basiert nicht nur auf KI (englisch «AI» für artificial intelligence), sondern auch auf «Analysten-Intuition», daher auch der Name «AI im Quadrat». Konkret lässt man bei der Lösung das System diverse Sicherheitsanalysen selbstständig vornehmen. Nach einer gewissen Zeit werden dann aber die Ergebnisse einem Spezialisten aus Fleisch und Blut präsentiert. Dieser entscheidet sodann, bei welchen Erkenntnissen des Systems es sich tatsächlich um Angriffe oder Bedrohungen handelt, und füttert damit das System von Neuem.

Bilder: PD; CW/Jens Stark

fassen. «Nichtsdestotrotz haben die Systeme Erstaunliches geleistet», so Alsenz. So hat ihm die Leistung des Bots «Mechanical Phish» von Shellphish imponiert. Diesem sei es «als einzigem System gelungen, einen Speicherfehler aufzuspüren und auszunutzen, der in einer komplexen State Machine ‹versteckt› war».

Krieg der Bots

Vor einem vollautomatisierten Cyberkrieg, bei dem sich Armeen von KI-Bots gegenseitig angreifen, stehen wir indes noch nicht. Dies zeigt der «Capture the Flag»-Wettbewerb der letztjährigen IT-Sicherheitskonferenz Defcon. An der Veranstaltung treten Teams von IT-Security-Spezialisten gegeneinander an, indem sie einerseits ihre eigene Rechnerumgebung effizient schützen, andererseits die Systeme der anderen Gruppen angreifen müssen. Erstmals war hier auch der Mayhem-Bot aus der Cyber Grand Challenge mit von der Partie. Er hatte gegen seine menschlichen Opponenten keinen Stich. Mit der geringsten Punktzahl landete die KI-Lösung auf dem letzten Platz.

Auch wenn die Cyberbots noch nicht allzu intelligent sind, könnte eine Entwicklung in Gang kommen, die auch völkerrechtlich weiterverfolgt werden müsste, wie Häni von PwC Schweiz findet. Wichtig sei, dass die Politik hier die Diskussion führe, was für Arten und Mittel von Cyberangriffen künftig toleriert werden könnten. «Aus meiner Sicht ist hier die Zeit reif, im Rahmen einer ‹Digitalen Genfer Konvention› klare Richtlinien und Regeln zu definieren», schlägt Häni vor.

Vollautomatische Sicherheit?

Bleibt die Frage, ob KI jemals die Unternehmen ganz autonom vor Cyberattacken schützen kann. Wohl kaum, lautet der Tenor, zumal auch die Gegenseite aufrüsten und sich der KI-Techniken behändigen wird. «Somit wird es immer ein komplexes Zusammenspiel von Systemen, Prozessen und Menschen bleiben», glaubt Hannes Lubich, der als Professor am Institut für Mobile und Verteilte Systeme der Fachhochschule Nordwestschweiz tätig ist. «Wer diesen Mix am besten beherrscht, hat zumindest einen temporären Vorsprung», ist er überzeugt.

54 Mio.

Sicherheitsmeldungen pro Jahr muss ein Unternehmen im Schnitt bearbeiten

Quelle: IBM

Häni von PwC kann sich aber durchaus vorstellen, dass in gewissen Bereichen die Prozesse vollautomatisch laufen, wobei «der Mensch in Zukunft hauptsächlich die Zusammenhänge analysiert und die Kreativität einbringt, während die Routinearbeiten und -analysen weitgehend oder vollkommen von KI-Systemen übernommen werden». Auch KMU könnten von dieser Entwicklung profitieren. «Viele kleinere Firmen, die heute überhaupt keine Cybersecurity-Spezialisten einsetzen, könnten dann auch – zumindest vor normalen Angriffen – vollständig von KI geschützt werden», hofft Häni.

Dauerthema Fachkräftemangel

Eigentlich wäre es vorteilhaft, wenn mit mehr KI der akute Fachkräftemangel im Cybersecurity-Umfeld gelindert werden könnte. Denn nach Prognosen des jüngsten «Global Information Security Workforce Study»-Berichts des Konsortiums (ISC)² fehlen bis 2022 weltweit 1,8 Millionen IT-Sicherheitsspezialisten, das sind nochmals 20 Prozent mehr, als in einer früheren Studie für das Jahr 2020 vorausgesagt wurde.

«KI kann das Risiko vermindern, das zurzeit durch Personalmangel in den SOC entsteht»

Dario Tizianel
IBM

Viel Hoffnung besteht trotz KI nicht. «Wir haben im Bereich der Cybersecurity heute einen so grossen Mangel an Talenten, dass KI diesen kaum beheben kann, obwohl sich damit die Effektivität und Effizienz des Personals erhöhen lässt», erklärt Häni. Immerhin gibts einen Lichtblick: «Die Kombination von KI und der generellen Entwicklung zu Managed Security Services kann aber helfen, den Mangel zu reduzieren.» Wie Dario Tizianel von IBM anfügt, könne der Einsatz von KI zumindest das Risiko vermindern, das zurzeit durch Personalmangel in den Security Operation Center entstehe.

Fazit: kein Allheilmittel

Der Einsatz künstlicher Intelligenz in der IT-Security ist in Zukunft bestimmt hilfreich und kann einen Beitrag zu sichereren IT- und Netzwerkumgebungen in Firmen leisten. Wundertaten darf man davon aber nicht erwarten, auch wenn viele Werbebotschaften von Herstellern entsprechender Systeme diese suggerieren. In etwas fernerer Zukunft ist das Potenzial der KI zwar gross – dieses würde dann aber auch von der Gegenseite genutzt werden, sprich: Hacker würden dank KI noch bessere Angriffs-Tools erhalten. ■

Jens Stark
ist Redaktor bei Computerworld:
www.computerworld.ch