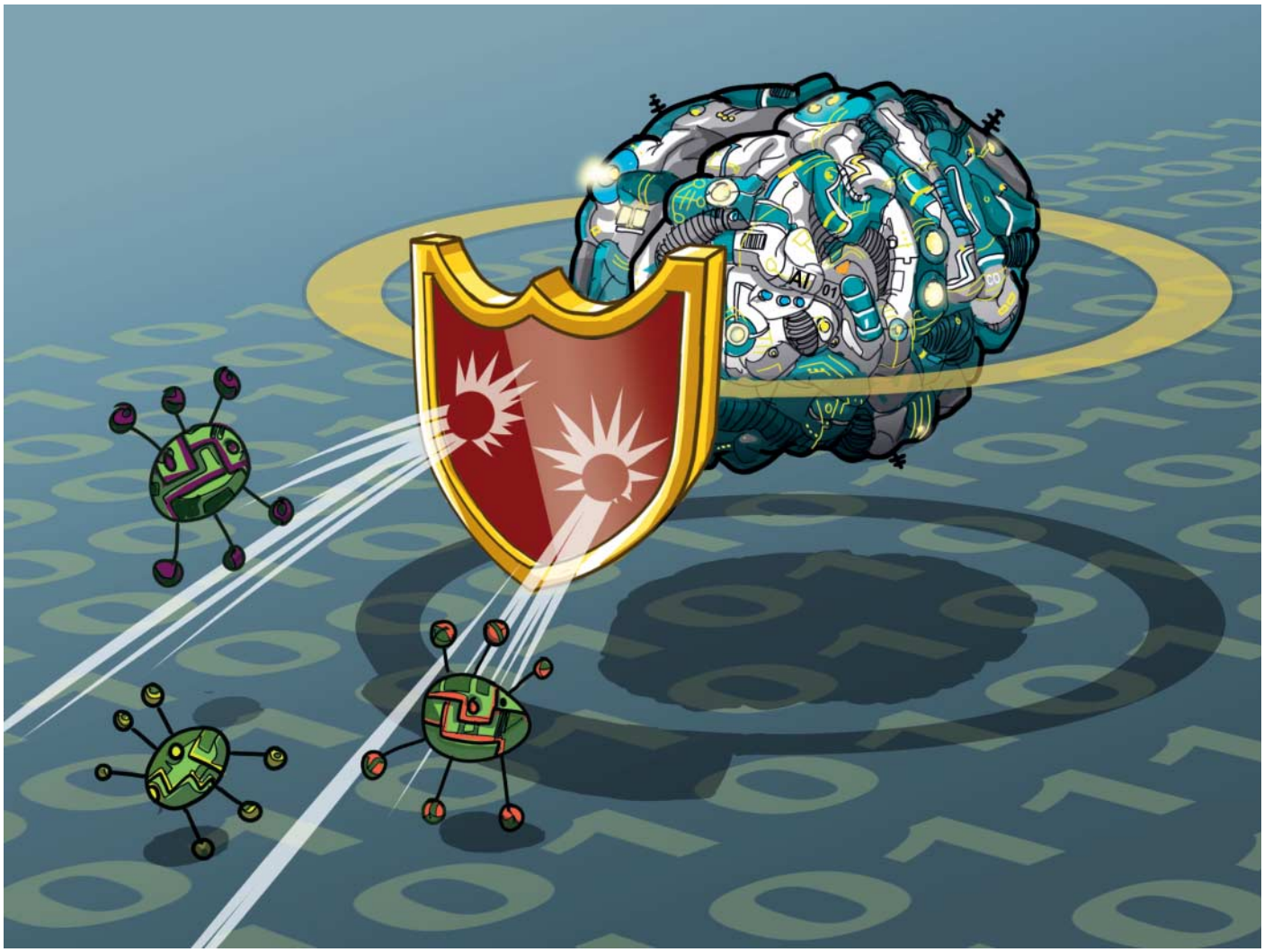


Bild: Thorsten Hübner

Intelligenteres Abwehrschild

Wie künstliche Intelligenz PCs sicherer machen will

Künstliche Intelligenzen haben menschliche Profi-Spieler im Schach, beim Brettspiel Go und dem Strategie-Computerspiel Starcraft 2 geschlagen. Doch kann es KI auch mit Profi-Hackern aufnehmen?

Von Stefan Strobel

Immer mehr Anbieter von Antiviren-Software versprechen, dass ihre Produkte dank künstlicher Intelligenz und maschinellem Lernen noch robusteren Schutz vor Hacker-Attacken bieten. Problematisch ist dabei, dass die Begriffe oft nicht klar definiert sind und in der Praxis sehr beliebig verwendet werden. Im Kern geht es fast immer darum, dass Techniken nicht auf statischen Regeln basieren, sondern einen angeblich intelligenten Erkennungsmechanismus verwenden. Der häufigste Anwendungsfall des maschinellen Lernens in der IT-Sicherheit ist die Erkennung von Malware beziehungsweise Einbrüchen und Kompromittierung von Systemen.

Bessere Erkennungsraten

Eine typische Variante ist maschinelles Lernen zur Erkennung von Malware vor ihrer Ausführung auf Endgeräten von An-

wendern. Bislang setzen die Hersteller von AV-Software auf das Vergleichen von Dateiinhalten mit Signaturen und riesigen Listen von Mustern bekannter Malware. Das wollen sie nun durch KI-Mechanismen ergänzen oder sogar ablösen.

Dafür setzen einige auf neuronale Netze. Das Training des neuronalen Netzes findet beim Hersteller statt, wo er Millionen von bekannten Malware-Samples und ebenso viele gutartige Dateien für die Ausbildung verwendet. Da die zum Lernen verwendeten Daten bekannt und klassifiziert sind, spricht man hier von „Supervised Learning“. Das trainierte neuronale Netz kann man als ein mathematisches Modell betrachten. Beim Kunden findet kein Lernen mehr statt, sondern das neuronale Netz klassifiziert neue unbekannte Dateien vor dem Öffnen oder Starten als gut- oder bösartig und gibt gegebenenfalls Warnungen aus. Die Erkennungsrate ist dabei vor allem bei neuer Malware meist höher als bei klassischen Verfahren und auch die Belastung der CPU ist geringer. Doch gänzlich neue Malware-Ansätze mit bis dato unbekannten Methoden und Praktiken werden allerdings auch einem solchen System Probleme bereiten.

Einschränkungen

Bei einigen AV-Produkten in diesem Bereich kann der KI-Mechanismus bislang nur EXE-Dateien einschätzen. Modelle für weitere Dateitypen sind meist noch in Arbeit. Das führt dazu, dass der Mehrwert einer solchen Technik oft gering ausfällt, wenn bereits Mailsysteme ausführbare Programme aus Nachrichten entfernen oder eine Whitelisting-Lösung, wie beispielsweise unter Windows 10 AppLocker, auf Endgeräten fremde Programme an der Ausführung hindern.

Ein typisches Problem von KI zur Erkennung von Malware ist auch, dass man es in der IT-Sicherheit mit Gegnern zu tun hat, die kein Interesse an einer Enttarnung ihres Schadcodes haben. Die Erkennungs- und Lernmechanismen wurden aber ursprünglich meist für Objekte entwickelt, die sich nicht wehren. Ein neuronales Netz, das Malware von harmlosen Dateien unterscheiden soll, hat daher Probleme, die es bei der Unterscheidung von Äpfeln oder Bananen auf Bildern nicht gibt. Um die Erkennung zu erschweren oder sogar zu verhindern, muss sich ein Malware-Autor lediglich gängige AV-Produkte mit KI-Schutzmechanismen anschauen und seine Malware so lange optimieren und offline testen, bis sie nicht mehr erkannt wird. Ein Profi, der sich einen eigenen EXE-Packer schreiben kann, kommt damit beispielsweise an den heutigen KI-AV-Produkten leicht vorbei. Die Wirksamkeit solcher KI-Techniken gegen professionelle beziehungsweise gezielte Angriffe ist deshalb noch begrenzt.

Erschwerend gesellt sich noch ein zunächst positiver Aspekt von KI-AV auf Basis neuronaler Netze hinzu: Updates für bessere Erkennungsraten gibt es aufgrund des lange andauernden Lernprozesses meist nur nach mehreren Wochen oder sogar Monaten. Für den Schutz vor breit gestreuter Malware ist dies erfreulich, denn das ständige Updaten von Signaturlisten ist hier nicht nötig.

Taucht im Netzwerksystem aber ein Schädling auf, der sich erfolgreich tarnt, kann man die KI-Anti-Viren-Anwendung nicht mal eben durch ein Update des neuronalen Netzes für den Trojaner fit machen. Maschinelles Lernen und neuronale Netze sind also keine Allheilmittel für IT-Security, sondern nur ein weiterer Baustein von vielen innerhalb einer Schutzlösung.

Intelligente Cloud-Analyse

Viele AV-Hersteller statten ihre Cloud-Services mit KI basierten Erkennungsmethoden aus, um klassische Verfahren zu ergänzen. Auf Endgeräten laufen Agenten, die entweder verdächtige Dateien oder nur bestimmte Metadaten wie beispielsweise die PE-Header von ausführbaren Programmen in die Cloud von AV-Anbietern zur Analyse hochladen. Das hat jedoch den Nachteil, dass diese Ansätze nur verfügbar sind, wenn Endgeräte eine dauerhafte Verbindung zur Cloud haben. Solange keine Internet-Verbindung besteht, ist der Virenschutz zurückgestutzt.

Eine weitere Variante sind KI-Sicherheitssysteme, die zwar auch auf einem Endgerät installiert sind, aber nicht Dateien vor dem Öffnen klassifizieren, sondern nach dem Starten von Programmen das Verhalten des Codes beobachten. Auch hier kommt oft maschinelles Lernen beim

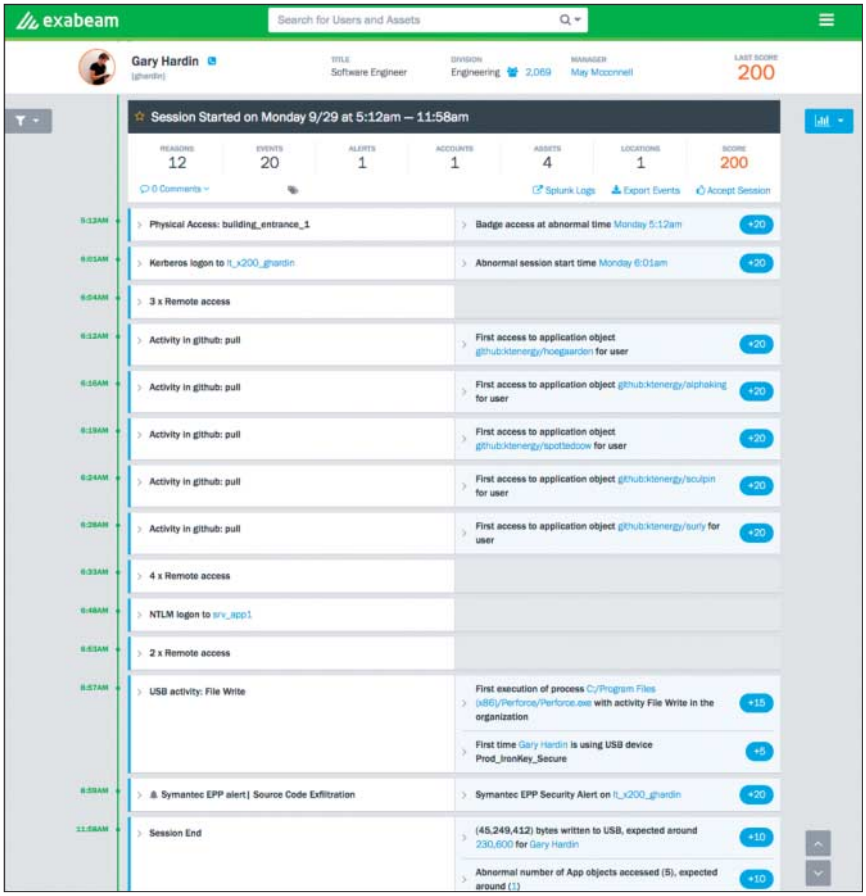


Bild: Exabeam

„Advanced Analytics“ von Exabeam analysiert auf KI-Basis das Verhalten von Mitarbeitern, um daraus normale und bösartige Handlungen abzuleiten. Hierzulande ist das aus Datenschutzgründen problematisch.

Hersteller zum Einsatz, sodass bösartiges Verhalten nicht nur anhand von klaren Regeln, sondern auch mithilfe des KI-Systems erkannt werden kann.

Besonders hilfreich an diesem Ansatz ist der Kontext, den ein solches System im Fall eines Alarms anzeigt. Meist findet man äußerst detaillierte und grafische Darstellungen vor, welcher Prozess auffälliges Verhalten an den Tag legt, auf welche Ressourcen er zugegriffen hat, wo er herkam und noch vieles mehr. Derartige Schutzlösungen sind deshalb fast immer eine sinnvolle Ergänzung zu anderen präventiven Malware-Schutztechniken. Auch diesen Ansatz gibt es als Cloud-Variante.

Gewiefte Netzwerküberwachung

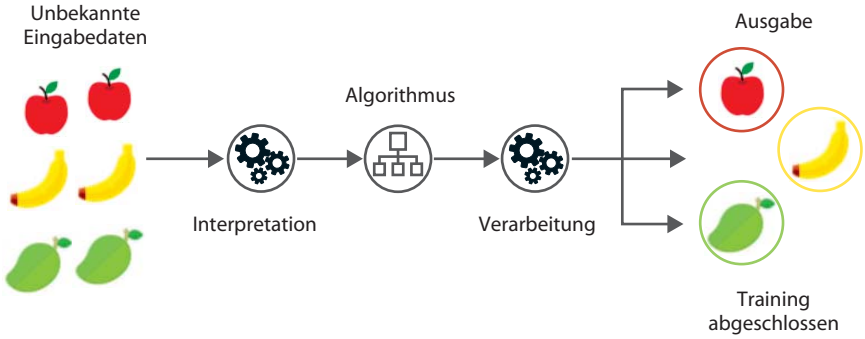
Eine andere Art von KI und maschinellem Lernen in der IT-Sicherheit findet man in Systemen, die sich eher auf den Datenverkehr im Netzwerk konzentrieren. Diese Konzepte erfassen den Datenverkehr von Arbeitsplatz-PCs und Servern untereinander und mit dem Internet.

Mithilfe von maschinellem Lernen wird dann versucht, die Kommunikation von Malware beziehungsweise das Voranschreiten einer Kompromittierung im Netzwerk („Lateral Movement“) zu erkennen. Dabei setzen die Verfahren meist nicht nur auf Supervised Machine Learning, sondern auch auf „Unsupervised Machine Learning“. Damit findet das Lernen vor Ort beim Kunden statt. Die Systeme versuchen so zu lernen, welche Kommunikation im Netzwerk eines Kunden „normal“ ist und wann etwas Ungewöhnliches beziehungsweise eine Anomalie („Anomaly Detection“) vorliegt.

Problematisch dabei ist, dass so auch bösartiges Verhalten, das bereits bei der Inbetriebnahme der Lösung vorzufinden war, als gutartig gelernt werden könnte. Außerdem funktioniert das Lernen solcher Systeme nicht besonders gut, wenn das Netzwerk vergleichsweise klein ist. Mehr als tausend Endgeräte sollten es schon sein, damit das Lernen effizient vonstatten geht. Durch die Kombination der beiden unterschiedlichen Arten von Machine Learning versuchen die AV-Hersteller, dem entgegenzuwirken. Beispielsweise sollte der bereits beim Hersteller trainierte Teil des Produktes dann Alarm schlagen, wenn im Netzwerk bereits Malware kommuniziert. So wollen sie verhindern, dass Malware-Kommunikation als normal gelernt wird.

Lernprozess von KI

In diesem Modell lernt eine KI zwischen Äpfeln, Bananen und Birnen zu unterscheiden. Doch die IT-Security ist vielschichtiger als dieses Beispiel und ein gewiefter Hacker könnte eine KI unter Umständen dahingehend umerziehen, etwas Böses als gut einzustufen ist.



Neben dem Schutz von einzelnen Computern und Netzwerken kann man KI auch für die Suche nach Sicherheitslücken einsetzen. So setzen zum Beispiel Werkzeuge zur Analyse von Quellcode immer mehr auf KI-Techniken, um Software-Schwachstellen zu identifizieren, die ein Angreifer für eine Attacke ausnutzen könnte. Auch beim „Fuzzing“ – also Softwaretests – kommt KI zum Einsatz, um Eingabedaten so zu wählen, dass möglichst alle Code-Teile ausgeführt und eventuelle Schwachstellen ausgelöst werden.

Psycho-Analyse von Nutzern

Eine vor allem in Deutschland noch problematischere Art von KI und Machine Learning in der IT-Security findet man bei Herstellern, die nicht die Kommunikation im Netz oder das Verhalten von Programmen, sondern das Verhalten von Anwendern analysieren.

Als Ausgangsdaten liegen hier typischerweise Protokolle über Anmeldungen an Systemen und Applikationen, Logs der Web-Proxies oder Firewalls oder Mailserver-Logs vor. Damit sieht das System beispielsweise, auf welche Websites Anwender zugreifen, welche Mails sie an wen versenden und wann sie sich wo anmelden. Diesen Ansatz nennt man „User Behavior Analytics“ (UBA) oder „User and Entity Behavior Analytics“ (UEBA).

Unter dem Aspekt „Erkennung von Vorfällen oder Innentätern“ sind diese Lösungen durchaus überzeugend, aber Leistungs- und Verhaltenskontrolle von Mitarbeitern ist in Deutschland ein heikles Thema. Die hier zwangsläufig entstehende Diskussion mit Betriebsräten ist einer der Gründe, warum solche Lösungen in Deutschland keine besonders große Verbreitung gefunden haben. Die Hersteller geben sich zwar viel Mühe, über Pseudonymisierung der Namen oder Kennungen von Benutzern oder über Rollen und Rechtekonzepte für den Zugriff auf diese Systeme einen Missbrauch zu verhindern, aber viele Sicherheitsverantwortliche bevorzugen dann doch andere Ansätze, die weniger interne Konflikte mit sich bringen.

Ein weiterer Baustein

Scharfe, oftmals regelbasierte Erkennung durch eine unscharfe, irgendwie intelligente Erkennung zu ergänzen: Das schreit geradezu danach, die Methoden und Techniken aus aktueller KI-Forschung einzusetzen. Jedoch findet diese Forschung meist in einem Umfeld statt, in dem es keine mutwillig bösen Akteure gibt. In der IT-Security hingegen gilt es, gerade solche Hacker aufzuspüren.

Das Ganze befindet sich aber auch noch in den Kinderschuhen, schließlich ist KI in der IT-Sicherheit noch ein relativ junges Segment, das sich aber stark weiterentwickelt. Der allgemeine Fortschritt im KI-Bereich und die Verfügbarkeit der dafür nötigen Rechenleistung bei Cloud-Anbietern gibt dem Thema einen starken Schub. Es ist naheliegend, dass KI vor allem viele Sicherheitstechniken mit statischen Regeln zur Erkennung oder Klassifikation verbessern kann. Die von einigen AV-Anbietern versprochene Wunderwaffe ist KI zum jetzigen Zeitpunkt aber nicht. *(des@ct.de)* c't