Cybersicherheit nutzt Machine Learning.
Die Power aus der KI ersetzt das, was Menschen nicht leisten können!

Die KI-Forschung entwickelt sich rasant weiter. Ziel ist es, eine permanente, proaktive Wachsamkeit bereitzustellen, um somit den komplexen Bedrohungen von heute besser zu begegnen.

Michael Keller, 13. März 2018

Für Allen Kent, Berater für Digital-Security, kann es mit der Entwicklung der Künstlichen Intelligenz (KI) gar nicht schnell genug gehen.

In Zusammenarbeit mit dem Industriedienstleister NAES Corporation unterstützt er Stromerzeuger dabei, ihre Netzwerke besser gegen Cyberangriffe zu schützen, damit sie die strengen behördlichen Auflagen erfüllen können. Und da Cyberkriminelle und staatlich sanktionierte Hacker immer aufwendigere und zerstörerischere Kampagnen starten, erfordert der Schutz von Unternehmensnetzwerken eine immer anspruchsvollere Planung und Gefahrenabwehr.

Die Manager für Informations-Sicherheit müssen heute eine Kombinationen aus verschiedenen Cyber-Tools einsetzen, um sicherzustellen, dass diese richtig konfiguriert sind. Die Experten müssen auch über die neuesten Bedrohungen aus dem Internet auf dem Laufenden sein und ihre Netzwerke fortlaufend auf Anzeichen von Angriffen überwachen.

Deshalb wünscht sich Kent, es gäbe eine einzelne Lösung, die er empfehlen könnte – eine Lösung, die Kunden einfach nur installieren müssten, um dann darauf zu vertrauen, dass alle Cybersicherheitsprobleme damit erledigt werden. Diese Lösung würde das Netzwerk überwachen, wäre ständig über neue Bedrohungen informiert und könnte Angriffe schon im Vorfeld unterbinden.

„Eine KI-Box, die alles überwacht und Bedrohungen automatisch abwehrt, sobald sie sich abzeichnen – das wäre die optimale Lösung", so Kent. „Aber im Moment haben wir kein geeignetes Tool, das nach der einmaligen Konfiguration völlig autonom arbeitet. Unsere vorhandenen Technologien müssen permanent manuell überwacht werden."

Diese Lücke könnte jedoch bald geschlossen werden. Informatiker und IT-Experten auf der ganzen Welt machen rasante Fortschritte bei der Entwicklung von Machine Learning (ML). Das bedeutet, dass der Code, der in einen Computer eingespeist wird Daten analysiert, um darin Zusammenhänge aufzudecken und Entscheidungen zu treffen, ohne dass er dafür speziell programmiert wurde. Die Forschung liefert eine Fülle von neuen Erkenntnissen, die Anstöße für die Entwicklung von zuverlässigeren KI-Technologien in ganz unterschiedlichen Bereichen geben.

Zu viele Daten für eine manuelle Sichtung

Im Bereich der Cybersicherheit verändert ML sehr schnell die Technologielandschaft. So kann ML die Arbeit automatisieren, Schwachstellen in Netzwerken aufspüren und sich abzeichnende Trends im Netzwerkverkehr aufspüren. Dafür werden enorme Datenmengen durchgekämmt, die von Analysten nicht verarbeitet werden könnten.

Jason O'Keeffe, Berater für Drucksicherheit bei HP, sagt, dass die Datenmengen, die heute zur Überwachung von komplexen Unternehmensnetzwerke generiert werden, mehr Analysen erfordern, als sie jemals von Mitarbeitern geleistet werden könnten. Das ist einer der Gründe für die ML-Begeisterung bei den Cybersicherheitsexperten.

„Das Problem ist, dass es in der Branche zu viele Daten gibt, von denen man nicht, was man damit anfangen soll", so O'Keeffe. „Sie wissen nicht, worauf sie achten müssen, um eine Untersuchung einzuleiten. Niemand sieht sich die Daten genau genug an, um festzustellen, ob etwas Ungewöhnliches vor sich geht. Ich denke, dass man dies der KI überlassen könnte. In den nächsten fünf Jahren wird mehr Technologie für Sicherheitsintelligenz in die Geräte integriert. Bei der Erkennung von Sicherheitslücken werden die Verfahren immer ausgefeilter."

Abgesehen von dieser permanenten Wachsamkeit erlernen ML-basierte Systeme auch die Fähigkeit, infizierte Computer und Geräte unter Quarantäne zu stellen. So werden Angriffe eingedämmt, bevor sie Schaden im gesamten Netzwerk anrichten können.

Es fehlt an geübten Augen und Ohren

Ein weiterer treibender Faktor für eine rasche großflächige ML-Einführung und anderen Automatisierungs-Tools in der Cybersicherheit ist der Mangel an qualifizierten Fachkräften. Dadurch sind viele „Wachposten-Positionen" im Netzwerk unbesetzt, während sich gleichzeitig die Bedrohungslage weiter verschärft. Einem Bericht zufolge werden bis 2021 weltweit mehr als 3,5 Millionen Arbeitsplätze im Bereich der

Cybersicherheit unbesetzt bleiben – ein Defizit, das erhebliche Auswirkungen auf die Unternehmen haben wird, die mit der Sicherung sensibler Daten oder kritischer Infrastrukturen betraut sind.

Mike Ahern, Director of Corporate and Professional Education am Worcester Polytechnic Institute, entwickelt Schulungsprogramme für die Cybersicherheit in kritischen Branchen wie der Energieversorgung. Er sagt, dass diese Unternehmen mehrmals am Tag erleben, dass ihre Sicherheitsmaßnahmen von Angreifern getestet werden und entsprechende Attacken erfolgen. „Sie brauchen Mitarbeiter, die nach Zusammenhängen und Alarm-Hinweisen Ausschau halten", führt er aus. „Es gibt nicht genügend qualifizierte Arbeitskräfte, und diese Kluft wird immer größer, sodass es dann nicht verwundert, wenn den Unternehmen einige Zusammenhänge und Warnungen entgehen."

Ahern sieht ein großes Potenzial für ML, denn damit können Programme, die Liegenschaften, Zugangskontrollen oder den Datenverkehr in Netzen überwachen Anomalien in Daten automatisch erkennen.

Die Notwendigkeit, immer einen Schritt voraus zu sein

Leider nutzen auch die Angreifer diese fortschrittlichen Tools. Laut Threats Predictions Report 2018 der Cybersicherheitsfirma McAfee ist davon auszugehen, dass auch Cyberkriminelle ML nutzen werden, um neue und bessere Wege zu finden, in Netzwerke einzudringen und die ML-basierten Schutz-Programme zu identifizieren und auszuhebeln.

McAfee geht davon aus, dass die Forscher, die in diesem Jahr Cyberangriffe untersuchen, feststellen werden, dass diese von ML-Algorithmen unterstützt wurden. Doch trotz der bedrohlichen Lage sieht McAfee Anlass zum Optimismus. „Unsere Aufgabe ist es, die Fähigkeiten von Computern schneller zu verbessern, als es die Angreifer tun sowie unsere Modelle vor Entdeckung und Zerstörung zu schützen", lautet das Fazit der Berichts-Autoren. „Bei der Zusammenarbeit zwischen Mensch und Maschine schwingt das Pendel wieder auf die Seite der Verteidiger."

Jonathan Griffin, leitender Sicherheitsanalyst bei HP, weist auch daraufhin, dass ML und KI von Angreifern genutzt werden könnten. Aus diesem Grund müssen Technologiehersteller und Experten für Cybersicherheit ständig auf der Hut sein, um nicht zu unterschätzen, wie kreativ Cyberkriminelle bei der Nutzung dieser Technologien sein können. Beispielsweise kann KI einem Angreifer ermöglichen, auf kostengünstige Weise ausgefeilte Spearphishing-E-Mails zu entwickeln, die für normale Benutzer nur sehr schwer von einer rechtmäßigen E-Mail zu unterscheiden sind. Derart raffinierte Angriffe richteten sich bislang nur gegen prominente Ziele wie Politiker und Topmanager.

Griffin sagt, HP dränge darauf, den versiertesten Angreifern immer einen Schritt voraus zu sein. „Wir profitieren zunehmend von der ML und KI, in dem wir diese Technologien in unsere Hardware integrieren", führt er aus. „Wir stehen mit diesen sehr spannenden Entwicklung aber erst am Anfang. Doch eines steht fest: In diesem Bereich der Sicherheitsforschung gibt es eine Menge äußerst interessanter Fragen zu beantworten."

Lesen Sie auch unser PDF (Englisch, 45 Seiten, 11,7 MB): „Wie sich Hacker und Sicherheitsexperten Design und ML zunutze machen". Es enthält die wichtigsten Maßnahmen, die Ihr Unternehmen implementieren kann, um die Cybersicherheit zu verbessern.

Ihr Team dtb
Mit freundlicher Unterstützung von HP Deutschland