http://www.zdnet.de/88300257/artificial-intelligence-und-cyber-security-wo-stehen-wir-heute/

Artificial Intelligence und Cyber Security: Wo stehen wir heute?

Artificial Intelligence (AI) ist in aller Munde, wenn es um Cyber Security geht. Die Frage ist nur: Ist in jeder Lösung, die AI verspricht, auch AI enthalten? Was bietet AI in der Security heute schon?

von Oliver Schonschek am 9. Juni 2017 , 07:36 Uhr

Was ist Artificial Intelligence und was nicht?

Mit Hype-Themen ist es bekanntlich so eine Sache: Man hat den Eindruck, vor einigen Jahren war plötzlich alles Cloud, dann war alles Big Data Analytics, und jetzt findet man auf Messen zur Cyber Security wie Infosecurity Europe 2017 kaum noch einen Anbieter, der nicht sagt, dass er Artificial Intelligence (AI) in seinen Lösungen einsetzt. Es ist deshalb sinnvoll und wichtig, den tatsächlichen Einsatz von AI in der Cyber Security zu hinterfragen. Genau dies wurde bei „European Media Spotlight – Innovators in Cloud, IoT, AI & Security“ von NetEvents in London getan, einen Tag vor Beginn der Infosecurity Europe. Die Themen bei NetEvents reichten von „The Mind of the Hacker: Insights from GCHQ, MI6 and Israeli Intelligence“ und „Track and Attack the Hackers: Don’t be Passive, Fight Back!“ über „Tools, Techniques and Technologies for Protecting the Endpoint“ bis hin zu „Practical Applications of Artificial Intelligence from Cybersecurity to Cloud to Internet of Things”.

Artificial Intelligence oder doch nur Machine Learning?

In den Vorträgen und Diskussionen bei NetEvents wurde deutlich, dass viele Lösungen heute erst auf dem Stand sind, Machine Learning (ML) einzusetzen. Von Artificial Intelligence (AI) erwarteten die anwesenden Experten mehr als die Erkennung von Mustern und die Unterscheidung von normaler Aktivität und verdächtigen Vorgängen in der IT. Erst wenn eine Security-Lösung auch neuartige Bedrohungen erkennen kann, zu denen es noch keine

Muster gibt, die man lernen und wiedererkennen kann, wird die Schwelle hin zur Künstlichen Intelligenz in der Cyber Security überschritten.

Ob es sich wirklich um AI handelt, ob ML hinter einer Lösung steckt und was die intelligente Security-Lösung kann, ist wichtig zu wissen, wenn Unternehmen die Lösungen einsetzen wollen und in ihrem IT-Sicherheitskonzept einplanen. Andernfalls verspricht man sich sonst zu viel oder zumindest das falsche von einer Lösung.

Die Realität heute ist: Ohne Security-Kompetenz im eigenen Unternehmen oder bei den beauftragten Managed Security Service Provider geht es nicht. So können die Lösungen, die Musteranalysen und Machine Learning einsetzen, wichtige Hinweise auf mögliche Gefahren geben. Die Entscheidung, was jeweils zu tun ist, kann vorbereitet werden, doch von einer vollständigen Automatisierung der Security ist man noch weit entfernt. Die internen oder externen Security-Spezialisten können nicht ersetzt werden, viele Anbieter betonen auch, dass sie dies weder wollen noch in Zukunft vorhaben.

Intelligente Security-Lösungen sind ein Muss

Wenn man als Unternehmen weiß, wie weit die intelligente Unterstützung einer Security-Lösung reicht, kann die Lösung ihren Funktionen entsprechend eingeplant und eingesetzt werden. Es ist empfehlenswert, nicht einfach nur auf einen Begriff wie AI zu achten, um eine neuartige, intelligente Lösung zu bekommen. Vielmehr gilt es, den jeweiligen Anbieter genau zu fragen, welche Art von Intelligenz in den Security-Funktionen steckt, was die Lösung genau kann und was nicht.

Wie breit gefächert intelligente Security-Funktionen sind, zeigen viele der vorgestellten Lösungen von den NetEvents und von Infosecurity Europe, darunter diese Beispiele:

- Javelin Networks bietet eine Lösung, die das Netzwerk des Anwenderunternehmens untersucht und visualisiert (Active Directory Assessment). Die analysierte Struktur wird dann künstlich ausgebaut, indem simulierte Geräte in das Netzwerk eingebracht werden, die zu dem jeweiligen Unternehmen passend erscheinen und dann auf mögliche Angreifer warten. Die simulierten Geräte sind für legitime Nutzer nicht sichtbar. Kommt es zu einem Zugriffsversuch auf eine simulierte Maschine, dann wird der Angreifer im „künstlich“ erweiterten Bereich des Netzwerkes gehalten, um die weiteren Schritte der Attacke ermitteln zu können.
- Menlo Security nutzt spezielle Intelligenz, um mögliche Attacken innerhalb von Webseiten und E-Mails zu erkennen. Die Links werden dazu nicht im Browser des Nutzers geöffnet, sondern isoliert in der Cloud. Dort findet dann die Analyse statt, ob und welche Bedrohungen von den Links und möglichen Phishing-Mails ausgehen.
- Bitglass hat die Anti-Malware-Lösung von Cylance integriert und verknüpft so die Funktionen eines CASB (Cloud Access Security Broker) mit der Erkennung und Abwehr von Schadsoftware (Bitglass ATP, powered by Cylance).
- Ixia nutzt in der Lösung BreakingPoint eine Security-Intelligenz zur Simulation von Attacken, um Security-Tests durchzuführen. Genannt werden über 37.000 verschiedene Angriffe und Malware-Typen, die simuliert werden können.
- CA setzt die bei der Aufdeckung von Kreditkartenbetrug erprobte Technologie nun auch zur Bestimmung von Risiken im Bereich digitaler Identitäten ein (CA Threat Analysis for Privileged Access Management).

- Ziften betreibt eine Intelligence Cloud, in der die gespeicherten IT-Aktivitäten der Anwenderunternehmen ausgewertet und nach Anzeichen für Attacken untersucht werden. Bei Ziften wird die Intelligenz also unter anderem in der Forensik genutzt (Lookback Forensics). Die Beispiele zeigen, wie unterschiedlich Funktionen mit Machine Learning (oder AI) heute bereits in der Security eingesetzt werden können. Zweifellos werden diese Funktionen weiter zunehmen und noch wichtiger werden. Nicht nur der Fachkräftemangel in der IT-Security wird dies weiter verstärken, auch die zunehmend intelligenten Attacken machen eine intelligente „Aufrüstung“ in der IT-Sicherheit erforderlich, in der Erkennung, Abwehr, Belastbarkeit und Forensik.