Was kann Künstliche Intelligenz schon heute?

Jeden Tag klassifizieren Lernalgorithmen über eine Milliarde E-Mails als Spam und ersparen so den Empfängern das zeitaufwändige und mühsame Aussortieren unerwünschter Nachrichten. Wenn Algorithmen nicht vorher eingreifen würden, würden diese Mails bei vielen Benutzern 80 bis 90 Prozent des Posteingangs ausmachen. Da die Spam-Versender ständig ihre Taktik anpassen, ist es für ein statisch programmiertes Verfahren äußerst schwierig, Schritt zu halten. Lernende Algorithmen funktionieren hier am besten[i] [ii].

Erfolge in der künstlichen Intelligenz haben bereits Änderungen dahingehend bewirkt, wie Informatik gelehrt[iii] und Softwareentwicklung praktiziert wird. Die künstliche Intelligenz (KI; englisch: Artifical Intelligence beziehungsweise AI) hat in ihrer kurzen Geschichte große Fortschritte gemacht, aber der letzte Satz im Aufsatz *Computing Machinery and Intelligence* von Alan Turing (1950) gilt auch heute noch: *Wir können nicht weit in die Zukunft sehen, aber wir können sehen, dass noch viel zu tun ist.*

Laut einer Studie des Ponemon-Instituts[iv] von 2015 jagt ein durchschnittliches Security Operations-Center (SOC) – das sich als Zentrale für alle sicherheitsrelevanten Services im IT-Umfeld von Organisationen oder Unternehmen versteht – jährlich allein 20.000 Stunden lang Warnungen hinterher, die sich zum Schluss als Fehlalarme entpuppen.

Aber wo wird bereits KI eingesetzt? Ein Gedanke wird IBM Watson[v] gelten. Mit Watson lassen sich Chatbots und virtuelle Agenten entwickeln, die schnell und effizient Fragen von Kunden beantworten und auf deren Bedürfnisse eingehen. Ein Agent ist dabei einfach etwas, das agiert – abgeleitet vom Lateinischen agere: tun, handeln, machen. Dabei operiert er autonom, nimmt seine Umgebung wahr, ist über einen längeren Zeitraum beständig, passt sich an Änderungen an und erzeugt und verfolgt Ziele[vi]. Durch Integration solch einer Technologie in die SOC können diese auf immer raffiniertere Cybergefahren reagieren. Die Bedrohungen durch Hacker und Cyberkriminelle bleibt dadurch allerdings nicht aus: Dafür sind die Angriffsmethoden noch raffiniert genug. Denn nicht zuletzt setzen Hacker selbst auf Künstliche Intelligenz und machen sich maschinelles Lernen oder Technologien zu Eigen wie „Intelligent Phishing“[vii] oder „Smart Malware“[viii]. Letztere erkennt zum Beispiel, wenn sie beobachtet wird.

Es ist das alte Katz-und Maus-Spiel, denn der technische Fortschritt bleibt auch der Gegenseite nicht verwehrt. Daher ist davon auszugehen, dass Cyber-Kriminelle versuchen werden, die Möglichkeiten der Künstlichen Intelligenz auch für sich zu nutzen. Cyberattacken, die durch KI modifiziert werden, sind beispielsweise in der Lage, während ihrer Verbreitung zu lernen und sich damit automatisch zu optimieren, indem sie gezielt auf Abwehrmaßnahmen reagieren. Es besteht dabei die Gefahr, dass sich solch KI-basierte Attacken vorhandenen Schutzmaßnahmen entziehen und im Laufe ihrer Verbreitung resistent werden. Die Schadsoftware kann im „Idealfall“ auf ihre Abwehr reagieren und dadurch den Sicherheitsmaßnahmen stets einen Schritt voraus sein. In einer 100-seitigen Studie[ix] stellt eine Forschungsgemeinschaft mit namhaften Institutionen wie der Universitiy of Oxford und der University of Cambridge mehrere denkbare Szenarien vor, die eintreten könnten, wenn KI ohne zusätzliche regulatorische, organisatorische und technische Sicherheitsmaßnahmen weiterentwickelt wird.

Fazit

Hier gilt es, frühzeitig Strategien und ein klares Regelwerk zu entwickeln, wie sich dies verhindern lässt. Ein Ansatzpunkt ist die VDI-Richtlinie VDI/VDE 3550 Blatt 1 Künstliche Neuronale Netze in der Automatisierungstechnik[x]. Das Dokument legt für den industriellen Einsatz eine einheitliche Basis zur Verwendung der wichtigsten Begriffe mit Definitionen fest. Des Weiteren wird in der DIN EN 61209 der Begriff künstliche Intelligenz definiert als „Fähigkeit einer Einrichtung Funktionen auszuführen, die üblicherweise mit menschlicher Intelligenz verbunden sind, wie Schlussfolgerungen ziehen, Lernen und sich selbst zu verbessern. Zuständig für diese Norm ist das Technische Komitee 80 (TC80) der Internationalen Elektrotechnischen Kommission (IEC) in Abstimmung mit der Internationalen Schifffahrtsorganisation (IMO). Darüber hinaus fand am 23. Januar 2018 die Gründungssitzung des Arbeitsausschusses Künstliche Intelligenz unter der Leitung der Geschäftsstelle des (Normenausschuss Informationstechnik und Anwendungen (NIA) in Berlin statt. Der Arbeitskreis wird ein erstes Arbeitspapier zum Thema Terminologie für die Gründungssitzung des JTC 1/SC42 in Peking am 18. April 2018 erarbeiten[xi]. Das Joint Technical Committee 001- Information Technology ist ein Gemeinschaftskomitee der International Organisation for Standardization (ISO) und der International Electrotechninal Commission (IEC).

Autor:

Dipl.-Ing. (FH)Sven Müller M. A., M. Sc., Projektmanager, DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Frankfurt am Main, sven.mueller@vde.com

---

[i] A Bayesian approach to filtering junk E-Mail. In Learning for Text Categorization: Papers from the 1998 Workshop, M. Sahami, S.T. Dumais, D. Heckerman, E.J. Horvitz (1998)

[ii] Fighting spam with statics. Significance, the Magazine of the Royal Statistical Society, 1,69-72, J. Goodman und D. Heckerman

[iii] Interactive Programming in Java, Lynn Andrea Stein, Morgan Kaufmann Publishers In, ISBN 978-1558605923, 2003

[iv] https://www.ponemon.org/

[v] https://www.ibm.com/watson/

[vi] Künstliche Intelligenz – Ein moderner Ansatz, S. Russel und P. Norvig, Pearson Deutschland GmbH, 2012

[vii] Künstliche Intelligenz macht Phishing-Versuche zielgenauer und effektiver, heise online, 15.08.2016

[viii] Künstliche Intelligenz – mehr IT-Sicherheit, weniger Hacker-Angriffe?, trojaner-info, 07.03.2017

[ix] The Malicoius Use of Artificial Intelligence: Forcecasting, Prevation, and Mitigation, Feb. 2018

[x] VDI/VDE 3550 Blatt 1 Computational Intelligence - Künstliche Neuronale Netze in der Automatisierungstechnik - Begriffe und Definitionen

[xi] DIN Presse Mitteilungen „Arbeitsausschuss Künstliche Intelligenz gegründet“, 31.01.2018