KÜNSTLICHE INTELLIGENZEN

OPTIMALES ERGEBNIS FÜR DIE IT-SECURITY

In der IT-Welt wird noch ein Großteil der Tätigkeiten vom Menschen vollzogen. Computer werden meist nur als unterstützende Komponenten oder als Hilfsmittel eingesetzt, beispielsweise Taschenrechner, doch dies liegt deutlich unter dem Potenzial moderner Computer.

Als konkretes Beispiel im Bereich des Penetrationstests, kurz Pentest, ist der Computer zwar das Hauptarbeitsmittel, jedoch werden diese von Menschen bisher ausschließlich orchestriert, um aktiv nach Sicherheitslücken zu suchen.

Künstliche Intelligenzen (KIs) sollten menschliches Handeln und die dazugehörige Wahrnehmung automatisieren. Dies funktioniert – wie beim Menschen – anhand von Erfahrungen, durch die sich Menschen und Computer grundlegend unterscheiden. Menschen können vergleichsweise schnell lernen, Computer dagegen brauchen dafür Unmengen an Daten.

DIE ZUSAMMENARBEIT ZWISCHEN MENSCH UND MASCHINE WIRD IN DER ZUKUNFT ENTSCHEIDENDER ALS JE ZUVOR SEIN, UM OPTIMALE ERGEBNISSE LIEFERN ZU KÖNNEN.

Emile Hansmaennel, Cybersecurity, Sogeti Deutschland GmbH, www.sogeti.de

Bereits existierende Anwendungsbereiche

Einige Wirtschaftszweige haben die KI für sich entdeckt und in ihren alltäglichen Ablauf eingepflegt, um Aufgaben zu optimieren. Amazon setzt KIs zur Prognose der Nachfrage ein, in der Landwirtschaft werden KIs zur Schädlingserkennung genutzt und der Bereich des Autonomen Fahrens wird fast ausschließlich von KIs bestimmt.

Herausforderungen: Lernen ohne Wissen

Um zu verstehen, warum die Verwendung von KIs in der IT-Security noch nicht weit fortgeschritten ist, muss verstanden werden, wie diese Mechanismen lernen. Dies geschieht anhand von riesigen, bereits existierenden Datenmengen, die am Ende des Pentests aus Datenschutzgründen vernichtet werden und somit nicht als Trainingsdaten verwendet werden können. Es ist somit mithilfe der im Pentest generierten Daten nicht möglich, KIs zu trainieren, da das Wissen welches benötigt wird, nicht mitgeteilt werden darf.

Um KIs verwenden zu können, müssten alle in einem Pentest gesammelten Daten anonymisiert werden, um keine Rückschlüsse auf einen Kunden zu hinterlassen. Dies ist quasi unmöglich, da in einem Web-Pentest, bei dem unter anderem Anfragen an den Server untersucht werden, die meisten Anfragen an einen Webserver den Namen des Kunden beinhalten. Würde man diese rausfiltern, würden grundlegende Funktionalitäten kaputt gehen.

Um trotzdem eine KI zu trainieren, müssen Daten aus einer anderen Quelle bezogen werden. Dies kann jedoch erst mal nur sehr allgemein passieren, da die Daten, wie bereits beschrieben, datenschutzkonform behandelt werden müssen. Eine weitere Möglichkeit wäre es, frei verfügbare Daten aus dem Internet zu nutzen. Das Problem hierbei ist, das kein Standard für Sicherheitslücken existiert, da diese zu unterschiedlich sein können. Dadurch ist es nicht ohne weiteres möglich, einer KI allgemein alle Arten von bekannten Sicherheitslücken beizubringen.

Fazit

KIs werden nicht die Lösung für alles sein, denn eines fehlt ihnen: Intuition. Tipps aus internen Quellen sowie sehr neue Fehler, zu denen noch nicht viele Daten existieren, können der KI nicht einfach mitgeteilt werden. Das Zusammenspiel wird wichtiger denn je, denn so können die Schwachstellen des jeweils anderen ausgeglichen und ein optimales Ergebnis geliefert werden.

Emile Hansmaennel