Sicherheit

Auf Nummer sicher durch KI

Autonomes Fahren mittels Künstlicher Intelligenz

von Bernd Fuhlert

Künstliche Intelligenz ist mittlerweile zu einem der beherrschenden Themen in der Gesellschaft avanciert. Durch die Technologie soll sich einiges zum Besseren wenden (lassen), so lautet allgemein das implizite Versprechen. Insbesondere Industrieunternehmen sind hier sehr zuversichtlich – nicht nur in Bezug auf das Generieren von Wettbewerbsvorteilen, sondern auch bezüglich ihrer Innovationsfähigkeit. Doch beim richtigen Umgang mit Künstlicher Intelligenz müssen manche Sachverhalte vollständig geklärt und andere noch grundsätzlich überdacht werden. Zum Beispiel die IT-Security.

Nicht nur bei der Produktion von Fahrzeugen, auch im Auto selbst soll Künstliche Intelligenz (KI) dafür sorgen, dass für den Anwender alles möglichst komfortabel gestaltet ist – letztendlich mit der Vision, dass eine Person zukünftig lediglich einsteigen muss, um sich dann zum Zielort chauffieren zu lassen. Allerdings ist es bis dahin noch ein weiter Weg, da hierzu bislang die nötige Intelligenz fehlt und die Technologie momentan keineswegs in sicherheitsrelevante Aufgabenstellungen involviert werden kann.

Dafür mangelt es nicht nur an den rechtlichen Voraussetzungen, sondern es tritt in diesem Kontext noch ein ganz anderes

Problem auf. Bei konkreten Entscheidungssituationen basieren die Auswertungsprozesse der KI auf Daten und Wahrscheinlichkeiten, die für den Menschen im Augenblick der Ausführung weder transparent sind noch seiner aktuellen Wahrnehmung entsprechen – von daher wird es für eine Person nahezu unmöglich sein, das ermittelte Ergebnis in der Realität nachzuvollziehen. Dies könnte zu Zweifeln an der Richtigkeit der ausgeführten Handlung und somit zum Vertrauensverlust bezüglich der KI insgesamt führen.

Andererseits belegen verschiedene Umfragen, dass in bestimmten Bereichen mit dem Einsatz von KI schon hohe Erwartungen verbunden sind. Unter anderem werden große Vorteile im Bereich Verkehrsführung gesehen: Acht von zehn Bundesbürgern (83 Prozent, Bitcom Research [BR]) sind davon überzeugt, dass sich mittels KI die Steuerung des Straßenverkehrs verbessern lässt und so Staus reduziert werden können.

Was heute schon geboten wird

KI ist bereits heute im Auto vorhanden: Darüber werden Aufgaben ausgeführt, die nicht unmittelbar mit der Steuerung – ohne vorgesehene Eingriffsmöglichkeiten des Fahrers – des Fahrzeugs zu tun haben, wie beispielsweise die Navigation, das selbstständige Reagieren bei Staus durch Abstandsmessung, um Auffahrunfälle zu vermeiden, oder verschiedene Multimedia-Anwendungen.

Grundsätzlich ermöglichen intelligente Apps den Autoherstellern, ihren Kunden mehr Komfort zu bieten. So stellt beispielsweise Volvo mit „Volvo on Call“ verschiedene Dienste wie „Ziel an Fahrzeug senden“ zur Verfügung – hierüber kann eine Route im Voraus sowie ortsunabhängig am Smartphone oder Tablet geplant und direkt an das Navigationsgerät übermittelt werden. Mittels einer weiteren Funktion ist es möglich, aus der Ferne zu überprüfen, ob das Auto tatsächlich verriegelt ist – ist dies nicht der Fall, dann lässt sich dies mit einem Klick in der Hersteller-App nachholen. Auch für die Ortung, inklusive Wegbeschreibung zum Standort, ist die App einsetzbar.

Daneben gibt es Anwendungen – wie beispielsweise „Android Auto“ –, die speziell unter Einsatz eines Android-Smartphones alternativ bei verschiedenen Automarken, wie etwa Audi, Alfa Romeo oder Fiat, aber auch in Kombination mit Endgerätemarken wie Blaupunkt nutzbar sind. Über das Smartphone ist neben Google Maps auch via Streaming der Zugriff auf Musik verfügbar sowie auf diverse Apps.

(Java-)Apps im Visier der Hacker

Jede App stellt einen potenziellen Angriffsvektor für Hacker dar. Die Gefahr besteht vor allem aufgrund des Ausnutzens von Sicherheitslücken. Diese Erkenntnis ist insbesondere im Rahmen der Programmierung von im Automobil verbauten Systemen relevant und hier speziell für Java-Anwendungen. Denn diese enthalten oftmals mindestens eine Komponente, die als Einfallstor für Cyber-Kriminelle fungiert. Dennoch werden Entwicklungen auf Basis von Java in modernen Autos eingesetzt. Insbesondere im Multimediabereich sind häufig Android-Anwendungen zu finden, die auf dieser Programmiersprache beruhen.

Dies geschieht aus gutem Grund: Java-Programme nutzen eine Laufzeitumgebung, die eine Art virtuelle Maschine darstellt, welche ermöglicht, dass diese Programme (relativ) unabhängig vom darunterliegenden Betriebssystem ausgeführt werden können. Das bietet den Vorteil der Plattformunabhängigkeit.

Die Vorteile von Java bieten jedoch nur dann einen Mehrwert, wenn die Anwendung auch sicher programmiert wird – was definitiv möglich ist. Da jedoch das vernetzte Auto ein relativ neues Thema darstellt und viele Programme in den Autos aus einer Zeit stammen, in der die IT-Security vernachlässigt wurde, stehen Autohersteller derzeit vor dem gleichen Problem wie die Banken beim Aufkommen der ersten Banking-Apps.

Eingebaute Sicherheit ist essenziell

Das Ziel der Hersteller in diesem Kontext ist offensichtlich: Sie wollen möglichst schnell Apps in ihren Fahrzeugen anbieten, um einen potenziellen Käufer mit neuen Funktionalitäten zu überzeugen. Diese Entwicklung ist jedoch unter dem Aspekt kritisch zu überprüfen, dass die geforderte Geschwindigkeit nicht zulasten einer sorgfältigen Programmierung gehen darf. Denn es gibt

nachweislich Fälle, dass Apps missbräuchlich, also zuungunsten des Fahrzeughalters, verwendbar sind. Anhand von umfangreichen Tests ließ sich unter anderem nachweisen, dass einige Apps, die dem Öffnen von Autotüren dienen, angegriffen werden können – durch Fehler in der Programmierung, beispielsweise aufgrund mangelnder Verschlüsselung von Authentifizierungsdaten.

Aber dies ist erst der Anfang. Wenn zunehmend mehr Apps zur Kontrolle der Fahrzeugfunktionen im Einsatz sind, ist es wahrscheinlich, dass die Angriffsmethoden ausgefeilter werden. Denkbar wäre dann, dass Cyber-Kriminelle versuchen, Trojaner einzuschleusen, um beispielsweise das Configuration File zu löschen und mit eigenen Befehlen zu überschreiben. Das Kino hat dieses Szenario schon eindrucksvoll umgesetzt: Im neuesten Teil der „Fast and the Furios“-Filmreihe demonstrieren die Drehbuchautoren, was theoretisch möglich ist, wenn Fahrzeuge ferngesteuert werden.

Wie verlässlich ist die physische Welt?

Aufgrund der hohen Verfügbarkeitsanforderungen werden Anwendungen in die Cloud ausgelagert und auch die Intelligenz zu deren Auswertung. Dies schafft eine zusätzliche Angriffsfläche. Falls hier keine geeigneten Sicherheitskonzepte seitens der Unternehmen bestehen, könnte ein Angriff auf einen zentralen Anbieter wie Amazon Web Services (AWS) einen enormen wirtschaftlichen Schaden anrichten.

Das sollte Anlass genug sein, sich auch mit der Frage zu beschäftigen, wie systemrelevant die großen Cloud-Anbieter mittlerweile sind. Denn ein Angriff auf einen der bekannten Provider hätte unmittelbar zur Folge, dass gleich Tausende von Unternehmen davon betroffen wären. Eine gewisse Zurückhaltung gegenüber diesen Dienstleistern ist somit angebracht, aber da große Datenmengen eine Nutzung der Dienste oftmals notwendig machen, sollten allgemein vor jeder Auftragsvergabe das jeweilige Unternehmen und dessen Schutzmaßnahmen genauestens überprüft werden.

Erhöhung der Sicherheit

Die Sicherheit muss bereits bei der Programmierung von Software ein integraler Bestandteil sein. Das bedeutet unter anderem, dass bei der Auswahl der Module nicht nur auf die Logik des Codes im Sinne der Anwendung fokussiert werden darf, sondern auch die entsprechenden Schutzvorkehrungen zu bedenken sind. Die Basis für eine angemessene Vorgehensweise bietet der Ansatz „Secure Coding“.

Zur entsprechenden Methodik gehört beispielsweise, bei der Auswahl von Bibliotheken diese vorab sorgfältig zu überprüfen. Denn nahezu alle vorhandenen Sicherheitslücken von veralteten oder verwundbaren Bibliotheken sind größtenteils öffentlich dokumentiert – oftmals zusätzlich illustriert anhand von einem Codebeispiel zur besseren Nachvollziehbarkeit – und bieten somit per se ein gutes Angriffsziel für die jeweilige Java-Anwendung.

Dies lässt sich vermeiden, indem stets die aktuellste Version verwendet wird. Als Hilfestellung bei der Suche nach dieser, inklusive der beseitigten Schwachstellen, dient der OWASP Dependency Check [OWASP]. Ebenso essenziell ist die Durchführung einer Quellcodeanalyse zum Auffinden von Programmierfehlern. Verschiedene Studien zeigen auf, dass ein Großteil an ungetesteter Software Mängel aufweist, teilweise wurde in diesem Rahmen bereits unmittelbar bei dem ersten Scan eine Schwachstelle aufgedeckt.

Zur Erhöhung der Sicherheit sind daneben auch Kenntnisse über die weitere Integration in die Infrastruktur notwendig. Dies bedeutet, dass bei der Programmierung nicht nur die Schnittstelle betrachtet werden muss, sondern ebenfalls zu bedenken ist, wie die App mit weiteren Anwendungen in Verbindung steht. Auch der zunehmenden Komplexität von Infrastrukturen muss Rechnung getragen werden. Um die Folgen, die aus kriminellen Angriffen resultieren können, zu minimieren, gilt es, hier die richtigen Schutzmaßnahmen zu etablieren: Dazu gehört selbstverständlich, dass bei der Entwicklung auch die Sicherheit der Kommunikationswege mitberücksichtigt wird.

Fazit

Die Diskussion bezüglich der Notwendigkeit von IT-Security soll keinesfalls als Hemmschuh beim Einsatz von Technologie

verstanden werden, sondern als Plädoyer für ein Umdenken in Bezug auf einen vernünftigen Umgang damit. Insbesondere wenn es um kritische Anwendungen, beispielsweise im Bereich Mobilität, geht, muss der Schutz von Individuen oberste Priorität haben. In Anlehnung daran gilt es unter anderem, zu erörtern, wie der Spagat zwischen dem Nutzen einer modernen Lebensweise einerseits und einer am Ende fehlinterpretierten Experimentierfreudigkeit sowie zu hohen Risikobereitschaft andererseits gelingen kann. Denn der Wettlauf mit den Cyber-Kriminellen wird sich nicht aufhalten lassen.

Hier ist nicht nur der Staat verantwortlich, die richtigen Rahmenbedingungen zu setzen, sondern im Prinzip jeder, der in den Entwicklungsprozess involviert ist. Denn auch dabei ist es möglich, ein Stück zur Erhöhung der Sicherheit beizutragen.

Sicherheit muss in der Entwicklungsumgebung eine hohe Priorität haben

Die Tatsache, dass die Analyse von Java-Programmen leicht durchführbar ist, macht eine entsprechende Absicherung der Entwicklungsumgebung unerlässlich. Folgende Kriterien sind dabei relevant:

1. Grundsätzlich:

   immer die aktuelle Java-Version verwenden

2. Bei der Auswahl und dem Einsatz der Frameworks ist es wichtig, darauf zu achten, dass

   eine adäquate Verschlüsselung,
   sichere Datenbank-Zugriffe,
   eine sichere Authentifizierung realisierbar sind.

3. Der Schutz der eingesetzten Applikationsserver ist durch

   das Absichern der Schnittstellen-Kommunikation (z. B. SOAP, Corba, RPC-XML, REST, RMI),
   das Absichern der Namespaces und Verhindern von Remote-Objekten,
   sichere Kommunikationskanäle in mehrschichtigen Umgebungen zu gewährleisten.

4. Organisatorisch:

   Definition des Rechte-Managements, zum Beispiel in Policies, um hohe Rechte-Anforderungen zu vermeiden.

Literatur & Links

[BR] Bitcom, 15.11.2017, siehe:
https://www.bitkom.org/Presse/Presseinformation/Bundesbuerger-geben-Kuenstlicher-Intelligenz-grosse-Chancen.html

[OWASP]https://www.owasp.org/index.php/OWASP_Dependency_Check

---

Bernd Fuhlert

ist seit 2016 Geschäftsführer der @yet GmbH. Seine zentralen Handlungsfelder sind Online Reputation Management und Datenschutz. Als freier Dozent ist er an der Quadriga Hochschule Berlin sowie für den Management Circle tätig und gilt als gefragter Experte zu den Themen Reputation Management/Datenschutz/Social Media. Für den BvD e. V. doziert er zum Thema Neue Medien bundesweit an Schulen der Sekundarstufe I & II. Zudem ist er Autor/Urheber zahlreicher Veröffentlichungen zum Thema Datenschutz und Reputation Management und veröffentlicht monatlich eine Kolumne in der Zeitung „Datenschutz Digital“ des VNR Verlages.

E-Mail: bernd.fuhlert(at)add-yet.de

Bildnachweise:

Fotolia