Mittelstand 4.0
Kompetenzzentren
Deutschlandweit

ARBEITSPAPIER

Schnittstelle KI und IT-Sicherheit: Potenziale und Herausforderungen

AG IT-Sicherheit und AG Künstliche Intelligenz

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Inhalt

1. Einführung

Durch den Einsatz von Künstlicher Intelligenz (KI) verändern sich die Handlungs- und Interaktionsfelder von Individuum und Gesellschaft. Große Datenmengen, die heutzutage fast in jedem Bereich des Lebens und der Wirtschaft erhoben werden, können durch KI weiterverarbeitet und nutzbar gemacht werden. Deshalb schreibt die Bundesregierung in ihrer nationalen KI-Strategie aus dem Jahr 2018, dass sich KI „als Basisinnovation zum Treiber der Digitalisierung und autonomer Systeme in allen Lebensbereichen [entwickelt].“[1] Für die Zukunft ist KI daher als Schlüsseltechnologie für Wissenschaft, Gesellschaft und Wirtschaft anzusehen.

Die Digitalökonomie hat den Nutzen von KI-basierten Systemen bei der Auswertung von Daten längst erkannt und investiert stetig in neue Anwendungsfelder. Es ist zu erwarten, dass sich dieser Trend fortsetzt. So wurden für das Jahr 2019 weltweit ca. 35,8 Mrd. USD an jährlichen Ausgaben der Industrie im Bereich KI prognostiziert.[2] Bei einer jährlichen Wachstumsrate von ca. 38 % sind für das Jahr 2022 bereits Ausgaben in Höhe von 79,2 Mrd. USD zu erwarten.[3]

1.1 Schnittstelle von IT-Sicherheit und Künstlicher Intelligenz

Damit die Vorteile der Digitalisierung genutzt werden können, ist laut dem Bundesministerium für Wirtschaft und Energie (BMWi) IT-Sicherheit ein „zentraler Wirtschaftsfaktor“.[4] So gab es gemäß dem Bundeskriminalamt im Jahr 2018 mehr als 87.000 Fälle von Cybercrime.[5]

Vor diesem Hintergrund gewinnt auch die Schnittstelle zwischen IT-Sicherheit und KI an Bedeutung, denn KI birgt im Bereich der IT-Sicherheit auch Potenzial für die Abwehr von Cyberangriffen. KI-basierte Systeme können angewandt werden, um sowohl Angriffs- als auch Schutzszenarien zu automatisieren. KI kann bei der proaktiven Suche nach Sicherheitslücken helfen, die Beschaffenheit von Angriffsvek-

1 Bundesregierung: Strategie Künstliche Intelligenz der Bundesregierung, 2018, S. 10, https://www.bundesregierung.de/resource/blob/975226/1550276/3f7d3c41c6e05695741273e78b8039f2/2018-11-15-ki-strategie-data.pdf (zuletzt aufgerufen am 28.10.2020)

2 IDC: Worldwide Spending on Artificial Intelligence Systems Will Grow to Nearly $35.8 Billion, (11.03.2019), https://www.marketingdive.com/news/idc-retail-to-lead-global-ai-spending-in-2019-as-total-market-reaches-35/550240 (zuletzt aufgerufen am 28.10.2020)

3 Ebd.

4 Bundesministerium für Wirtschaft und Energie: IT-Sicherheit, (24.03.2020), https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/it-sicherheit.html (zuletzt aufgerufen am 28.10.2020)

5 Bundeskriminalamt: Cybercrime Bundeslagebild 2018, S. 6

toren erlernen und durch prädiktive Analyse Sicherheitsvorfälle prognostizieren und abwehren. Umgekehrt werden auch Angreifer in der Lage sein, diese Vorteile für kriminelle Ziele zu nutzen.

Darüber hinaus wird KI auch zunehmend in sicherheitsrelevanten Bereichen wie den Kritischen Infrastrukturen eingesetzt. Aus diesem Grund ist es essenziell, dass KI-Systeme auch selbst vor Angriffen geschützt werden. Die Angriffsfläche, die ein KI-System bietet, ist mannigfaltig und erstreckt sich von der Trainings- und Einsatzumgebung bis hin zur Außenwelt. Angesichts dieser Wechselwirkung von IT-Sicherheit und KI ist das Gewährleisten von Sicherheit auch Voraussetzung für die erfolgreiche Nutzung von KI.

1.2 Struktur des Arbeitspapiers

Das vorliegende Papier dient dazu, für den deutschen Mittelstand Potenziale und Herausforderungen an der thematischen Schnittstelle von IT-Sicherheit und Künstlicher Intelligenz zu identifizieren. Hierzu werden zunächst die wichtigsten Begrifflichkeiten vorgestellt und erläutert. Im Anschluss daran werden die Potenziale und Risiken KI-basierter Systeme anhand verschiedener Anwendungsfälle präsentiert und ausgewertet.

2. Definition der Begrifflichkeiten

2.1 IT-Sicherheit

Der Begriff „IT-Sicherheit“ definiert einen Teilbereich der „Informationssicherheit“, der sich insbesondere mit der technischen Absicherung von digitalen Informationen und Systemen befasst. Das heißt, dass die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen gewährleistet werden.[6]

Der Begriff „Informationssicherheit“ wiederum fungiert als Oberbegriff und umfasst sowohl die technischen als auch die nichttechnischen Absicherungsmaßnahmen für alle Informationen, die in einer Organisation existieren. Die Schutzziele oder

6 BSI: Glossar der Cyber-Sicherheit, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 (zuletzt aufgerufen am 28.10.2020)

auch Grundwerte der Informationssicherheit entsprechen denen der IT-Sicherheit.[7]

2.2 Künstliche Intelligenz

Trotz der interdisziplinären Forschung auf dem Gebiet der KI seit den 1950er Jahren hat sich bis heute keine einheitliche Begriffsdefinition durchgesetzt. Die Interpretation des Begriffs hat sich im Laufe der Zeit an die technische Entwicklung angepasst.

In Anlehnung an das Positionspapier des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) und des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) lässt sich Künstliche Intelligenz abstrakt definieren als Beschreibung von Anwendungen aus dem Bereich der Informatik, die das Ziel verfolgen intelligentes Verhalten zu zeigen. Um dies realisieren zu können, ist der Einsatz von vier Kernfähigkeiten – Wahrnehmen, Verstehen, Handeln und Lernen – nötig. Grundsätzlich kann das so erhaltene Modell als Erweiterung des Grundprinzips von EDV-Systemen, Eingabe – Verarbeitung – Ausgabe, um die Aspekte des Lernens und Verstehens angesehen werden. Im Unterschied zu konventionellen Systemen, die in der Regel auf klar definierten und fest programmierten Regeln basieren, kann der Verarbeitungsanteil in echten KI-Systemen trainiert werden: Das KI-System lernt fortwährend dazu.

Die Künstliche Intelligenz wird in zwei Bereiche unterteilt: schwache und starke KI. Anwendungen der schwachen KI fokussieren sich dabei auf die Unterstützung des Menschen bei der Lösung eines konkreten Problems. In spezifischen Problemlösungen kann die Leistung der KI-Anwendungen die menschliche Leistungsfähigkeit übersteigen. Die starke KI wird so definiert, dass KI intellektuelle Fertigkeiten von Menschen erreicht bzw. übertrifft. Wann bzw. ob dieser Stand jemals erreicht wird, ist bisher noch unklar.

Im Rahmen der Mittelstand-Digital Initiative haben die Mitglieder der AG Künstliche Intelligenz aufgrund des fehlenden Praxisbezugs existierender Definitionen ein eigenes Verständnis für den Begriff der Künstlichen Intelligenz erarbeitet:

7 BSI: Glossar der Cyber-Sicherheit, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 (zuletzt aufgerufen am 28.10.2020)

„Angelehnt an menschliche Intelligenzleistung fokussiert sich Künstliche Intelligenz auf die Lösung konkreter (Anwendungs-)Probleme und unterstützt Menschen bei Arbeits- und Entscheidungsprozessen. Mit Künstlicher Intelligenz wird die Lernfähigkeit eines Systems auf Basis von Daten beschrieben."

2.3 Thematische Schnittstelle zwischen IT-Sicherheit und Künstlicher Intelligenz mit Blick auf Cybercrime

Als Cybercrime werden all jene kriminellen und illegalen Handlungen bezeichnet, die durch moderne, digitale Informations- und Kommunikationstechnologien wie Computer, Netzwerke bzw. Netzwerkgeräte realisiert werden oder auf diese abzielen.[8] Solche Angriffe stellen auch für kleine und mittlere Unternehmen (KMU), die oft nur über begrenzte Ressourcen verfügen, gerade im Zeitalter des Internets der Dinge (IoT) und von Industrie 4.0 eine erhebliche Bedrohung dar.[9]

Um diesen Problemen zu begegnen, existieren neben klassischen Softwareapplikationen zur Identifizierung von Bedrohungen wie Antiviren-Programmen bereits einige intelligente Lösungen, die zur Verteidigung auf moderne Algorithmen aus dem Bereich der Künstlichen Intelligenz zurückgreifen.

Der Einsatz von KI kann bei der Abwehr von Gefahren mittelfristig auch einen geringeren Ressourceneinsatz bedeuten. Große Fortschritte wurden in den letzten Jahren im Bereich der Intrusion-Prevention-Systems (IPS) erarbeitet. Diese Systeme lernen Angriffsvektoren und -muster zu erkennen und aktiv abzuwehren. Sowohl im Automobilbereich als auch bei der automatisierten Absicherung von Informationsverbünden werden diese Systeme bereits breitflächig eingesetzt. Weitere Formen der automatisierten Angriffserkennung werden aktuell erforscht und in naher Zukunft als kommerzielle Lösungen für den deutschen Mittelstand zur Verfügung stehen.

Die fortschreitende Entwicklung im Bereich der Künstlichen Intelligenz führt jedoch nicht nur zu neuen KI-basierten Verteidigungsmechanismen, sondern bietet unweigerlich auch die Möglichkeit, diese für Angriffe zu nutzen. Eine Bitkom-Studie von 2018 zeigt, dass der Diebstahl unternehmenbezogener Daten bereits

8 Bundeskriminalamt. Internetkriminalität/Cybercrime. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (zuletzt aufgerufen am 28.10.2020)

9 Bauer, G.: 10 Thesen von Vectra zu Künstlicher Intelligenz und Cybersicherheit im Jahr 2019, (20.12.2018), https://www.infopoint-security.de/10-thesen-von-vectra-zu-kuenstlicher-intelligenz-und-cybersicherheit-im-jahr-2019/a18250 (zuletzt aufgerufen am 28.10.2020)

weit verbreitet ist und über alle Branchen hinweg ein rasant wachsendes Problem darstellt.[10] Auf der Seite der Angreifer ist dies nicht zuletzt auf den Einsatz von Künstlicher Intelligenz und deren einfache Skalierbarkeit sowie die damit einhergehende Verbesserung von Angriffen zurückzuführen.

Um der Begrifflichkeit die Abstraktheit zu nehmen und Schnittstellen von KI im Kontext von Cybercrime aufzuzeigen, werden im Folgenden verschiedene Beispiele angeführt und kurz erläutert. Diese reichen vom klassischen Datendiebstahl über Hacking/Spionage bis hin zu Betrug und Datenmanipulation.

Ein klassischer Cybercrime-Angriff aus dem Bereich des Datendiebstahls ist das sogenannte „Phishing", bei dem gefälschte Websites oder manipulierte WLAN-Netzwerke als Werkzeug für den Datendiebstahl eingesetzt werden.[11] Sind die Phishing-Werkzeuge auf spezielle Nutzergruppen oder Unternehmen zugeschnitten, spricht man von Spear-Phishing-Attacken. Dabei werden Schwachstellen und Interessen von Menschen gezielt ausgenutzt.

KI-Systeme bieten einerseits die Möglichkeit, als Verteidigungsmechanismus eingesetzt zu werden und vermeintliche Phishing-Versuche zu identifizieren. Andererseits können sie im Angriff aber auch dafür genutzt werden, um sensible Informationen über die Zielgruppe zu extrahieren sowie Phishing-Websites und -Mails zu generieren. Solche personalisierten Angriffe sind oft erfolgreich. Mögliche Folgen sind unter anderem Datendiebstähle und -manipulationen, bei denen Datensätze so verändert werden können, dass sie unbrauchbar sind oder eine fehlerhafte Ausführung von Geschäftsprozessen verursachen. Häufig führt dies zu einem immensen wirtschaftlichen Schaden in Unternehmen.

Moderne KI-basierte Authentifizierungsverfahren wie Gesichts- oder Stimmerkennung erfreuen sich in den letzten Jahren immer größerer Beliebtheit. Häufig sind diese Verfahren Teil einer Zwei-Faktoren-Authentifizierung und erhöhen so maßgeblich die Sicherheit. Zukünftig besteht jedoch auch hier die Gefahr, dass solche Verfahren durch KI manipuliert werden.

10 Bartsch, M. et al.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, S. 1–58 (2018)

11 Bundeskriminalamt. Internetkriminalität/Cybercrime. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (zuletzt aufgerufen am 28.10.2020)

Ein weiteres Einsatzgebiet findet sich in der als „Fuzzing“ bezeichneten Identifizierung von Schwachstellen in IT-Systemen oder Softwareapplikationen.[12] Spezielle Algorithmen aus dem Bereich des maschinellen Lernens zur Anomalie-Detektion können darüber hinaus genutzt werden, um auf verdächtige Verhaltensmuster und mögliche Bedrohungen hinzuweisen.[13]

Obwohl die aufgeführten Beispiele nur einen Bruchteil der Schnittstelle zwischen Künstlicher Intelligenz und IT-Sicherheit abbilden, wird schnell deutlich, dass eine thematische Auseinandersetzung damit für die IT-Sicherheit eines jeden Unternehmens unabdingbar ist. Zusammenfassend lässt sich festhalten, dass KI-basierte Angriffe in aller Regel eine KI-basierte Verteidigung erfordern.

3. Risiken KI-basierter Systeme für die IT-Sicherheit kleiner und mittlerer Unternehmen

3.1 Schaden – Bedrohungsrisiken für KMU durch den vermehrten Einsatz KI-basierter Angriffswerkzeuge

Der Einsatz KI-basierter Technologien bei Cyber-Angriffen ist zu einer ernstzunehmenden Bedrohung geworden, die besonders KMU betreffen kann. In KMU kommen oftmals ältere Technologien zum Einsatz, die vor Viren und anderen Bedrohungen schützen sollen. Werden die eingesetzten Viren-Scanner, Firewalls etc. nicht auf dem aktuellen Stand gehalten, dann können über veraltete Bedrohungsdatenbanken bestimmte Angriffe nicht verhindert werden und das Risiko steigt, im Falle eines Angriffs technologisch unterlegen zu sein. Vor allem da die Tools zur Angriffsausführung immer einfacher zu beschaffen und leichter zu benutzen sind.

Ein mittlerweile etabliertes Geschäftsmodell im Darknet und Deep/Hidden Web (Verstecktes Web) ist die sogenannte „Malware-as-a-Service“. Dabei muss ein Angreifer nicht mehr die Kenntnisse aufbringen, Software zu entwerfen, Informationen über ein Angriffsziel zu sammeln und letztendlich die erfassten Daten auszuwerten und weiter zu nutzen. Der Angreifer bedient sich vielmehr einer der

12 Plattform Lernende Systeme (Hrsg.): Neue Geschäftsmodelle mit Künstlicher Intelligenz – Bericht der Arbeitsgruppe Geschäftsmodellinnovationen, München 2019, S.16

13 Pohlmann, N.: Künstliche Intelligenz und Cybersicherheit – Eine Diskussionsgrundlage. 17 (2018)

diversen Online-Plattformen, um Botnetze[14] zu steuern und Schwachstellen in Unternehmensinfrastrukturen einzukaufen.

Nach der Digitalisierungswelle der letzten Jahre, in denen Unternehmen bspw. Sensoren zur Energieüberwachung massenhaft in ihre Netze eingebaut haben, besteht das Risiko einer Kultur des „Einstellens und Vergessens“: IoT-Geräte, die installiert wurden, sind schnell in Vergessenheit geraten, weil sie ihren Dienst verrichten und relativ zuverlässig arbeiten, ohne Instandhaltungsarbeiten zu benötigen und damit sicherheitstechnisch zu „veralten“.

Ein Beispiel für das oben genannte Szenario ist das Mirai-Botnetz. Es verbreitete sich 2016 enorm schnell auf solchen IoT-Geräten und verursachte nicht nur bei KMU, sondern auch bei Großunternehmen enormen Schaden. Nach Veröffentlichung des Source Codes entwickelten sich schnell Varianten der Software, die bis heute existieren. Ob diese auch KI-Techniken einsetzen, ist ungewiss, aber wahrscheinlich.[15]

Eine weitere, nicht offensichtliche Gefahr liegt in der Art und Weise, wie KI arbeitet. Der Prozess ist weitestgehend unbekannt (Black Box) und die Anwender/innen können meist nicht nachvollziehen, warum ein Ergebnis entstanden ist, also welche Vorgänge zu diesem geführt haben. Ein Zusammenhang ist in der Regel nicht zu erkennen. Ebenso können die Anwender/innen oder Administrator/innen dann nur schwer entdecken, ob die Software kompromittiert ist oder fehlerhafte Daten zum Lernen verwendet hat. Wurde nun gelernt, dem erzeugten Ergebnis erstmal zu vertrauen, kann es möglicherweise lange dauern, bis ein tatsächlicher Fehler identifiziert wird. Um dieser Herausforderung zu begegnen, kann es in Einzelfällen sinnvoll sein, die Transparenz mit Blick auf die Funktionsweise von KI bereits in der Entwicklulngsphase zu erhöhen.

Im Folgenden werden einige Anwendungsfälle und Beispiele zu KI und IT-Sicherheit präsentiert bzw. die Thematik noch stärker beleuchtet.

14 Botnetze sind ein Zusammenschluss von mehreren Computern, die über eine Fernsteuerung für bestimme Aktionen missbraucht werden (vgl. BSI. Botnetze. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/botnetze_node.html (zuletzt aufgerufen am 28.10.2020)

15 Gil, Laurent, und Allan Liska: Security with AI and Machine Learning, 2019

3.2 Anwendungsfälle

Neben den Potenzialen und Lösungen für KMU (vgl. Kapitel 4) im Bereich KI und IT-Sicherheit bietet KI auch neue Wege, um bestehende Angriffe auf Netzwerke und Infrastrukturen zu professionalisieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zählt in seinem Lagebericht zur IT-Sicherheit in Deutschland 2019 Identitätsdiebstahl, Schadprogramme, Ransomware, Distributed Denial of Service (DDoS), Botnetze und Spam zu den akuten Angriffsmethoden in den letzten Jahren.[16]

Generell ist es aber schwierig herauszufinden, welche neuen Angriffe durch KI ausgeführt oder unterstützt werden. Das Potenzial, auch Angriffe durch KI aufzuwerten, bietet sich dennoch an und wird für viele Unternehmen durch das Beispiel Emotet (oder allgemein Spam-Malware) in seiner aktuellen Version 3 deutlich. Emotet nistet sich auf einem Computer ein und kann auf das E-Mail-Postfach der Nutzer/innen zugreifen. Die Software versucht sich anschließend per E-Mail weiterzuverbreiten. Sie verfasst im Namen der Nutzer/innen E-Mails und sendet diese an die Kontakte, die die Malware in Postfächern oder Kontaktlisten findet. Die Mail enthält dann bspw. einen Link zu einer Webseite, um auf diese Weise Daten zu erlangen, oder schadhafte Anhänge, die die Malware auf dem Zielrechner installieren. Die Beobachtungen der letzten Monate zeigen eine steigende Authentizität der durch die Malware versendeten E-Mails. So ist Spam in einigen Fällen nicht mehr von authentischen E-Mails zu unterscheiden und Identitätsdiebstahl, CEO-Fraud oder dergleichen werden voraussichtlich häufiger eintreten. Dass Emotet KI einsetzt, um diese E-Mails zu verfassen, ist wahrscheinlich. Um KI-gestützen Angriffen entgegenzuwirken, bedarf es einer spezifischen Schulung der Mitarbeiter/innen.

Auch Ransomware kann durch KI unterstützt werden. Die Ransomware kann dieselben Verfahren einsetzen wie Malware, um sich auszubreiten. E-Mail ist dafür das beste Medium. Durch Machine-Learning-Algorithmen kann ein Angreifer bei der erfolgreichen Infektion eines Computers untersuchen, welcher Angriffsvektor sich am besten eignet bzw. kann er noch nicht geschlossene Lücken (Zero-Day-Exploits) identifizieren[17] und für weitere Angriffe nutzen.

16 Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2019, Bonn, Oktober 2019

17 FileCloud blog. „Machine Vs Machine: A Look at AI-Powered Ransomware“, (27.08.2018) https://www.getfilecloud.com/blog/2018/08/machine-vs-machine-a-look-at-ai-powered-ransomware (zuletzt aufgerufen am 28.10.2020)

KI kann nicht nur aktuelle Angriffsvektoren unterstützen, sondern auch selbst zum Ziel werden, da Prozesse innerhalb eines Machine-Learning-Systems für Nutzer/innen häufig nicht verständlich sind bzw. nicht ersichtlich ist, auf Basis welcher Annahmen das System ein Ergebnis liefert. Die Überprüfbarkeit und Nachvollziehbarkeit ist damit nicht mehr in Gänze gegeben. Künftige Schadsoftware könnte also darauf abzielen, die Eingaben zu manipulieren,die ein Machine-Learning-System nutzt.[18] Charakteristisch für ein Lernendes System ist, dass sich seine Systemantwort im Laufe der Zeit durch die eingefütterten Eingabedaten verändert – gemeint ist: verbessert. Diesen Umstand können sich Angreifer zu Nutze machen, um durch das Füttern eines Systems mit böswilligen Eingabedaten selbiges in ihrem Sinne zu manipulieren und die Systemantwort vom ursprünglich intendierten Rahmen zu entfernen. Das bekannteste Beispiel dieser Art ist sicher der experimentelle Chatbot „Tay“ von Microsoft, der Tonalität und Ausdrucksweisen Heranwachsender erlernen sollte, jedoch durch Rechtsextreme manipuliert wurde.[19] Auch in diesem Zusammenhang kann ein Teil der Lösung die Erhöhung des Transparenzniveaus bei der Datenerhebung sein.

KI und die dahinterliegenden Algorithmen zu verfälschen, nennt sich „Poisoning the well“ bzw. „Membership Inference Attack“. Angreifer verfälschen damit die Trainingsdaten, die ein Algorithmus nutzt, um ihn „blind“ für die eigentlichen Angriffe zu machen. Die Software (bspw. ein Antivirenprogramm) ist anschließend nicht in der Lage, den Angriff als solchen zu identifizieren. Dies ist nur ein Beispiel von vielen möglichen Angriffen auf und durch KI.[20] [21]

Insgesamt wird es wahrscheinlicher, dass KI nicht nur für die Erkennung von Angriffen eingesetzt wird, sondern dass durch die zunehmende Nutzerfreundlichkeit und einfache Handhabung von verfügbaren professionellen Tools zur Angriffsausführung auch Cyberangriffe künftig KI-Methoden enthalten werden.[22]

---

18 Johnson, Anne, und Emily Grumbling, Hrsg.: Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. Washington, D.C.: National Academies Press, 2019, https://doi.org/10.17226/25488 (zuletzt aufgerufen am 28.10.2020)

19 Beuth, Patrick: „Twitter-Nutzer machen Chatbot zur Rassistin“. Zeit Online. (24.03.2016), https://www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch (zuletzt aufgerufen am 28.10.2020)

20 Johnson, Anne, und Emily Grumbling, Hrsg.: Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. Washington, D.C.: National Academies Press, 2019, https://doi.org/10.17226/25488 (zuletzt aufgerufen am 28.10.2020)

21 Kilpatrick, Harold: „The Malicious Use of Artificial Intelligence in Cybersecurity“. SecureAge Technology (blog). (24.08.2018) https://www.secureage.com/malicious-use-artificial-intelligence-cybersecurity (zuletzt aufgerufen am 28.10.2020)

22 Gil, Laurent, und Allan Liska: Security with AI and Machine Learning, 2019

4. Potenziale KI-basierter Systeme für die IT-Sicherheit kleiner und mittlerer Unternehmen

4.1 Schutz – Professionalisierung von Verteidigungsmechanismen durch den Einsatz von KI-basierten Systemen

KI-basierte IT-Infrastruktur-Sicherungslösungen (Intrusion Detection) können auch unbekannte Formen des unbefugten Eindringens in Unternehmenssysteme erkennen. KI „beobachtet" dabei die Systeme und den darauf ablaufenden dynamischen Datenverkehr und erkennt Abweichungen von üblichen Abläufen. Die KI „lernt", anfangs unterstützt durch Menschen (Trainieren der Systeme), welche Änderungen im Bereich des normalen, dynamischen Rahmens akzeptabel sind und welche Abweichungen als Versuch eines unerlaubten Eindringens bzw. als unberechtigter Abruf von Daten zu bewerten sind. Darüber hinaus kann z. B. auch erkannt werden, wenn versucht wird, das IT-System in seiner Leistungsfähigkeit zu stören. Dies sind Anwendungsbeispiele, wie speziell große Unternehmensnetzwerke und IT-Systeme geschützt werden können.

4.2 Anwendungsfall: verhaltensbasierte Authentifizierung

Eine im Unternehmensumfeld, aber auch im Alltag einer Privatperson nutzbare KI-Lösung ist die verhaltensbasierte Authentifizierung. Dieser Methode liegt eine Denkweise zugrunde, die mit der Intrusion Detection vergleichbar ist: das Beobachten und Bewerten von Abläufen und deren Abweichungen von der bekannten Norm unter Berücksichtigung tolerabler Abweichungen. Ziel der verhaltensbasierten Authentifizierung ist es, die Nutzer/innen weitgehend von der lästigen Passworteingabe zu befreien und ihre sehr individuellen Lebensumstände als sicheren Passwortersatz zu nutzen.

Bis heute sind Passwörter das wichtigste Mittel zur Sicherung digitaler Identitäten. Die Forschung zeigt jedoch umfassend, dass diese Sicherheitstechnologie aus verschiedenen Gründen nicht zuverlässig ist, wenn es um den Schutz sicherheitsempfindlicher Bereiche und digitaler Identitäten geht. Die Gründe dafür liegen darin, dass nur sehr wenige Menschen starke Passwörter bzw. viele Internetnutzer/innen die gleiche E-Mail-Adresse-Passwort-Kombination bei verschiedenen Gelegenheiten (Web-Shops etc.) verwenden. Das mit Abstand

am häufigsten verwendete Passwort weltweit ist 123456, gefolgt von 123456789 (zusammen mehr als 50 % aller verwendeten Klarkennwörter).[23]

Zudem kommt es vor, dass viele IT-Dienstanbieter Nutzer-Passwörter nicht verschlüsselt oder mit nur schwacher Verschlüsselung speichern. Das bedeutet, dass digitale Identitäten von Millionen von Benutzer/innen nach einem Datendiebstahl für jeden zugänglich sind, unabhängig von der Komplexität des individuellen Nutzer-Passworts. Diese Bedrohung ist real, denn jeden Tag werden mehr als zehn Millionen digitale Identitäten gestohlen und auf speziellen Internetseiten angeboten. Diese können so für kriminelle Aktivitäten genutzt werden.[24]

Die immer noch verwendete klassische Passwort-Technologie wurde zu einer Zeit eingeführt, als Computer noch nicht flächendeckend mit dem Internet verbunden waren. Doch mit der zunehmenden Vernetzung von Menschen und Maschinen weltweit stößt die bisherige Passwort-Technologie an ihre Grenzen. Die klassische Nutzung von Passwörtern ist nicht bequem. Die Benutzer/innen müssen das Passwort regelmäßig eingeben, damit die Geräte ihre Identität überprüfenkönnen. Dies ist lästig und oft versuchen die Benutzer/innen die Sicherheitseinstellungen zu umgehen, um das Leben wieder komfortabler zu machen.

Deshalb wurden neue Wege zum Schutz digitaler Identitäten entwickelt. Gegenwärtig gelten biometrische Authentifizierungssysteme als State of the Art, bei denen Personen vor allem über Fingerabdrücke, Gesichtserkennung und Sprach- bzw. Stimmenerkennung identifiziert werden. Dies ist ein guter Anfang, aber auch solche eindimensionalen, biometrischen Lösungen bergen ein nicht unerhebliches Risiko. Denn auch biometrische Daten können ohne Wissen des Betroffenen erfasst, gespeichert und weiterverbreitet werden. Daher ist der Schutz solcher biometrischen Lösungen nicht bedeutend besser als die bisherige Passwortlösung. Außerdem hat der Mensch nur maximal zehn Fingerabdruckpasswörter, eine Stimme und ein Gesicht. Damit hat er zwölf individuelle, biometrische Passwörter, die von erfahrenen Dritten replizierbar sind.

Auch andere aktuelle Verfahren, die es ermöglichen z. B. ein Smartphone zu entsperren oder Türen zu öffnen, sind nicht sicher. Verwendet wird dafür die

23 HPI Identity Leak Checker Projekt, https://sec.hpi.de/ilc/statistics (zuletzt aufgerufen am 28.10.2020)
24 Ebd.

Kommunikation des Systems mit einem anderen smarten Gerät, das einer Person eindeutig zuzordnen ist, wie eine Smartwatch.

Es werden also neue Ansätze und weiterführende Lösungen benötigt, die aus Sicherheitsgründen auch laufend angepasst werden müssen. Sie sorgen dafür, dass die Nutzer/innen kaum merkbar starke und quasi nicht angreifbare Passwörter verwenden. Ein vielversprechender, komfortabler und dennoch sehr sicherer Ansatz zum Schutz digitaler Identitäten beruht auf einer neuartigen Technologie[25], die am Hasso-Plattner-Institut erforscht und in Berlin und Potsdam entwickelt wird. Bei der verhaltensbasierten Authentifizierung wird die Identität einer Person überprüft, indem das einzigartige Bewegungsverhalten einer Person (Körperbewegungsmuster wie Gangart etc.) sowie das räumliche Bewegungsmuster (wo ist die Person in ihrem Alltag, zu welchem Zeitpunkt, wie lange) mit Hilfe von Sensoren beobachtet wird. Aus den Sensordaten werden durch KI „Vertrauensebenen“ (level of trust) berechnet, die eine Bewertung ermöglichen, ob eine Person wirklich das zur Nutzung eines digitalen Dienstes berechtigte Individuum ist.

Jedes halbwegs aktuelle Smartphone enthält mindestens 16 High-End-Sensoren. Diese Sensoren können dazu verwendet werden, ein zur Absicherung von Services eindeutig zuordenbares Verhaltensprofil zu erstellen. Die Forschung zeigt, dass es auf Grundlage der Sensordaten möglich ist, Bewegungsprofile der Benutzer/innen zu berechnen, über KI das individuelle Profil der Nutzer/innen zu erlernen und damit die jeweilige Identität abzusichern.

Schon allein die Art, wie eine Person ihr Telefon aus der Tasche zieht, ist sehr individuell. Damit ist es möglich, die Sensordaten des Smartphones dazu zu nutzen, die verschiedenen Arten von aufeinanderfolgenden personenspezifischen Aktionen (Herausholen, aus welcher Tasche, in welcher Geschwindigkeit, mit welchem dreidimensionalen Weg) zu nutzen, um z. B. das Smartphone zu entsperren. Auch andere Aktionen, z. B. welche Funktionen des Smartphones werden auf welche Art und Weise aufgerufen, identifiziert die Nutzer/innen bereits eindeutig.

Wenn für eine autorisierte Person für den Zugang zu verschiedenen digitalen Diensten eine verhaltensbasierte Authentifizierung verwendet wird, kann keine andere Person diese Art der Authentifizierung nachahmen. Wenn das Telefon also gestohlen oder von unbefugten Personen benutzt wird, erkennt das Smartphone

25 Prof. Dr. Christoph Meinel, Christian Tietz, Eric Klieme: Verhaltensbasierte Authentifizierung. https://hpi.de/meinel/security-tech/secure-identity-lab/behavior-based-authentication.html (zuletzt aufgerufen am 28.10.2020)

aufgrund der dann anderen Sensordaten die Verhaltensänderungen und die Vertrauensebene wird abgesenkt, sodass der bequeme direkte Zugriff ohne weitere Passworteingabe auf sicherheitsrelevante Services verwehrt wird.

Der Hauptgedanke hinter der verhaltensbasierten Authentifizierung ist, dass die Geräte ihre Besitzer/innen sicher erkennen und dabei verhindern, dass Unbefugte sie benutzen können. Dabei werden die Sensordaten dazu verwendet, um Bewegungen im Raum zu erfassen, das Verhalten der Nutzer/innen automatisch zu erkennen sowie typische Abläufe zu lernen (Machine Learning). Im Laufe der Zeit können diese korrekt vorhergesagt werden. Dann können die Geräte die Identität ihres Besitzers passiv erkennen und störende Sicherheitsabfragen sind nur noch nötig, wenn ungewohnte, neue Nutzungsszenarien vorliegen. Das aus dem individuellen Bewegungsmuster entstandene „Passwort" kann nicht verloren gehen, muss nicht aufgeschrieben werden und kann auch nicht an unberechtigte Personen weitergegeben werden.

Je mehr Sensoren an der Erfassung von Verhaltensinformationen beteiligt sind, je länger die KI beobachten und lernen kann, desto höher sind die Vertrauenswerte. Allein die Art und Weise, wie Menschen ihr Smartphone benutzten, wie sie es aus der Tasche ziehen, halten und verwenden, berechnet bereits Vertrauenswerte von etwa 70 %. Fügt man z. B. eine Smartwatch dem Smartphone hinzu, erhöht sich die Anzahl der messbaren, individuellen Bewegungsabläufe und der Vertrauenswert steigt bereits auf 90 %.

Für einige Dienste oder Berechtigungen werden Vertrauenswerte von nahezu 100 % benötigt, z. B. für militärische oder ähnlich sicherheitsrelevante industrielle Umgebungen. Dann können weitere einfache Techniken für Arbeitsplätze mit Arbeitskleidung zur Anwendung kommen. Smarte Kleidung enthält bereits heute unsichtbare Sensoren und Elektronik, die messen können, ob das Bewegungsverhalten der Person, die sie trägt, konsistent ist. Die Sensoren in der Kleidung können die Sicherheitsebene erweitern, ggf. auch ergänzt um weitere Sensorik, wie der Messung der Herzschlagfrequenz, der Bewegung des Brustkorbs beim Atmen und Ähnlichem mehr. Je mehr nutzerspezifische Daten lokal erfasst und verarbeitet werden, desto einfacher ist es Vertrauenswerte von nahezu 100 % zu erreichen.

Ein zugangsberechtigter Mitarbeiter mit einer solchen smarten Arbeitskleidung könnte allein durch sein individuelles Bewegungsprofil in einen sensiblen Unternehmensbereich scheinbar unkontrolliert eintreten und im Hintergrund autori-

siert sicherheitsrelevante Dienste nutzen, ohne jemals ein Passwort einzugeben oder Autorisierungspads für Fingerabdrücke und/oder Gesichtsscans etc. nutzen zu müssen. Die Sensordaten der Kleidung und ggf. weiterer smarter Geräte, die unabhängig voneinander das jeweils spezifische Verhaltensprofil ermitteln, werden zum Identifizierungsgerät, z. B. am Arbeitsplatz, übermittelt. Das Gerät berechnet den Vertrauenswert und schaltet alle Geräte und Dienste frei, die eine Identifizierung oder Autorisierung benötigen. Auf diese Weise kann der Zugang zu einem Hochsicherheitstrakt oder jedem anderem Sicherheitsbereich durch einfaches Hingehen entriegelt werden. Passt das Bewegungsprofil nicht, wird der Zugang verweigert. Auf lange Sicht könnten solche hochsicheren Authentifizierungssysteme auch für normale Menschen mit individueller Kleidung verwendet werden, da sie in Standardkleidung eingenäht oder eingewebt werden können.

KI wird bei dieser Lösung genutzt, um das individuelle Bewegungsprofil zu erlernen. Die Sicherheit von Infrastruktur, IT-Systemen u. a. m. wird deutlich erhöht und den Nutzer/innen wird das Leben durch den nun möglichen Verzicht auf Passwörter erleichtert.

Die oben beschriebenen Verfahren werden derzeit entwickelt und in absehbarer Zeit für die unterschiedlichsten Einsatzgebiete in Unternehmen, auch in KMU, zur Verfügung stehen.

5. Zusammenfassung

Dieses Arbeitspapier zeigt, dass KI für KMU nicht nur an Bedeutung gewinnen, sondern auch stärkeren Einfluss auf den Bereich der IT-Sicherheit nehmen wird. KI gestaltet die Angriffsausführung für Cyberkriminelle zunehmend einfacher, indem es die gängigen Angriffsvektoren wie bspw. Phishing oder Malware durch Automatisierung unterstützt. Die Bedrohungslage für KMU wird somit auch zukünftig hoch sein, wenn nicht sogar weiter ansteigen.

Auch kann KI, wie gezeigt wurde, selbst Ziel von Cyberangriffen werden. Vor diesem Hintergrund ist es umso wichtiger, dass der Einsatz von KI-Systemen umfangreich überprüft wird und Hard- und Software stets aktuell gehalten werden. Darüber hinaus wäre es wünschenswert, wenn die Nachvollziehbarkeit von KI-getroffenen Entscheidungen stärker gewährleistet werden könnte.[26]

26 Wie erklärbare KI-Systeme im Gegensatz zu Black-Box-Systemen eingesetzt werden können, zeigt zum Beispiel dieser Artikel: https://www.nature.com/articles/s42256-019-0048-x (zuletzt aufgerufen am 28.10.2020)

Neben den Risiken bietet KI aber auch Potenziale und Lösungen, um mehr IT-Sicherheit zu gewährleisten. Durch den Einsatz von KI-basierten IT-Sicherheitslösungen können Angriffe auf Unternehmenssysteme frühzeitig erkannt und abgewehrt werden. Neue sichere Verfahren wie die verhaltensbasierte Authentifizierung, welche das Verwenden von Passwörtern obsolet macht, werden zukünftig auch für KMU zur Verfügung stehen.

6. Die Arbeitsgruppen (AG)

Dieses Arbeitspapier wurde im Rahmen der vom Bundeswirtschaftsministerium geförderten Initiative Mittelstand-Digital erstellt (Informationen zu Mittelstand-Digital, siehe Kasten 7.1).

In den Arbeitsgruppen IT-Sicherheit und KI, die dieses Arbeitspapier gemeinsam erstellt haben, arbeiten Expert/innen aus den verschiedenen Kompetenzzentren zusammen.

6.1 Die AG IT-Sicherheit

Die Arbeitsgruppe IT-Sicherheit vernetzt die Mittelstand 4.0-Kompetenzzentren des Förderschwerpunkts „Mittelstand-Digital“. Geleitet wird die Arbeitsgruppe durch Dr. Frauke Goll und Dr. Thomas Usländer.

Das wichtigste Ziel der Arbeitsgruppe ist die Aufnahme von sicherheitsrelevanten Problem- und Fragestellungen aus den verschiedenen Wertschöpfungssegmenten sowie deren mittelstandsgerechte Aufarbeitung.

Zentrale Themen, die aktuell von der Arbeitsgruppe bearbeitet werden, sind „Sensibilisierung“ sowie „Risikoeinschätzung“. IT-Sicherheit ist jedoch ein „Moving Target“ – deshalb werden die Themen regelmäßig dem Bedarf der Kompetenzzentren und ihrem Anwenderkreis angepasst.

Neben der internen Vernetzung der Kompetenzzentren steht die Arbeitsgruppe in ständigem Austausch mit anderen Arbeitsgruppen der Initiative „Mittelstand-Digital“, diversen Projekten der Initiative „IT-Sicherheit in der Wirtschaft“ wie auch weiteren relevanten Akteuren aus dem IT-Sicherheitsbereich auf Bundes- wie auch auf Landesebene.

Bei Fragen zur AG IT-Sicherheit
wenden Sie sich bitte an David Ruge,
der die der die Arbeitsgruppe koordiniert.
E-Mail: ruge@fzi.de

6.2 Die AG Künstliche Intelligenz

Die Arbeitsgruppe Künstliche Intelligenz bringt die Mittelstand 4.0-Kompetenzzentren des Förderschwerpunkts „Mittelstand-Digital“ zusammen. Geleitet wird die Arbeitsgruppe durch Keran Sivalingam.

Das Ziel der Arbeitsgruppe ist es, die verschiedenen Themen rund um Künstliche Intelligenz mittelstandsgerecht aufzuarbeiten, relevante Frage- und Problemstellungen zu identifizieren und den Erfahrungsaustausch zwischen den Kompetenzzentren zu fördern.

Aktuell beschäftigt sich die Arbeitsgruppe KI, wie auch die AG IT-Sicherheit, vor allem mit der „Informierung und Sensibilisierung“ des Mittelstands. Das geschieht durch Aufzeigen von Potenzialen und Einsatzmöglichkeiten der KI. Weiterhin dient die AG KI auch zum Informations- und Erfahrungsaustausch zwischen den KI-Trainern und den Kompetenzzentren.

Neben der internen Vernetzung steht die Arbeitsgruppe in ständigem Austausch mit anderen Arbeitsgruppen der Initiative „Mittelstand Digital“ sowie verschiedenen Projekten mit Schwerpunkt Künstlicher Intelligenz.

Bei Fragen zur Arbeitsgruppe wenden Sie sich bitte an Keran Sivalingam,
E-Mail: keran.sivalingam@dfki.de

7. Mittelstand-Digital

7.1 Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung.

Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

7.2 Das KI-Trainer-Programm

Auch im Rahmen des KI-Trainer-Programms „KI für KMU“ begleiten die Kompetenzzentren KMU dabei, den Einsatz und die Etablierung von Künstlicher Intelligenz im Unternehmen in die Wege zu leiten. Die deutschlandweit über 70 KI-Trainer/innen können Ihr Unternehmen an der Schnittstelle von KI und IT-Sicherheit unterstützen.

Weiter Informationen finden Sie unter: https://www.mittelstand-digital.de/MD/Navigation/DE/Praxis/KI-Trainer/ki-trainer.html

8. Impressum

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum
Stuttgart c/o
FZI Forschungszentrum
Informatik
Haid-und-Neu-Straße 10-14
76131 Karlsruhe

Rechtsform:
Das FZI Forschungszentrum
Informatik ist eine Stiftung des
bürgerlichen Rechts.

Redaktion:
Arbeitsgruppe IT-Sicher-
heit und Arbeitsgruppe Künstliche
Intelligenz

Stand: März 2021

9. Mitwirkende

Gemeinschaftsprojekt der Mitglieder der AG IT-Sicherheit und der AG Künstliche Intelligenz aus den deutschlandweiten Mittelstand 4.0-Kompetenzzentren