4. Maschinelles Lernen für die IT-Sicherheit

Katrin Gaßner

Maschinelles Lernen (ML) kann die Werkzeuge und Verfahren verbessern, die in vernetzten IT-Systemen oder generell im Internet für die IT-Sicherheit genutzt werden. Die IT-Sicherheit birgt jedoch ganz besondere Herausforderungen für den Einsatz von ML. In diesem Beitrag geht es darum, wie Unternehmen bereits jetzt maschinelles Lernen zur Verbesserung von IT-Sicherheit nutzen und welchen Beitrag heute die Forschung liefert. Dort ist die Verknüpfung von ML und IT-Sicherheit noch verhältnismäßig rar. Das ist ein Defizit, da Lösungspotenziale, die aus der Kombination der Disziplinen entstehen, zu erwarten sind.

Mit dem zurzeit ganz allgemein zunehmenden Einsatz von KI-Methoden wächst auch für die IT-Sicherheit die Hoffnung, dass ML-Verfahren sichere IT-Systeme ermöglichen, die sich lernend auf Bedrohungen einstellen. Doch ML ist kein Allheilmittel, es kann das Erkennen und Bekämpfen von Angriffen auf Systeme mit IT-Komponenten voraussichtlich nur ergänzen. So eignet sich ML beispielsweise dazu, große Datenmengen auszuwerten oder Anomalien zu erkennen. Aber es ist auch zu bedenken, dass ML-Verfahren selbst angreifbar und kompromittierbar sind, es können also sogar zusätzliche Angriffsvektoren durch die Nutzung von ML entstehen. Außerdem ist der Aufwand für das Trainieren der ML-Systeme hoch und ML-Verfahren sind im Allgemeinen sehr spezialisiert.

ML – Lösungsansatz für die IT-Sicherheit?

Mit der Digitalisierung bieten heute beinahe alle technischen Systeme auch Angriffsflächen für Hacker, Spionage und generell für kriminelle Handlungen. Nicht zu vernachlässigen ist, dass technische Systeme immer in einem sozio-technischen Kontext genutzt werden und die nutzenden Menschen zu potenziellen Angreifern werden können, mit oder ohne Absicht. Die Angriffe erfolgen über die informationstechnischen Systeme, Teilsysteme, Komponenten und Schnittstellen, die heute vielfältig untereinander vernetzt sind. Neben Produktions- und Industrieanlagen sind das Infrastruktureinrichtungen und Bürosysteme ebenso wie Systeme des automatisierten Fahrens oder Fliegens. Und im Internet of Things (IoT) werden inzwischen sogar vernetzte Waschmaschinen, Kameras oder Kaffeeautomaten zu möglichen Angriffspunkten.

V. Wittpahl (Hrsg.), *Künstliche Intelligenz*,
DOI 10.1007/978-3-662-58042-4_5, © Der/die Autor(en) 2019

Die Vielfalt der digitalen Systeme lässt die potenzielle Anzahl der Sicherheitslücken explodieren. Damit einher gehen die endlosen Möglichkeiten, wie und anhand welcher Indizien Bedrohungen erkannt werden können. Mit den seit Jahren zunehmenden Angriffen auf IT-Systeme wuchs die Erkenntnis, dass es eine abschließende Sicherheit nicht geben kann. Auch ein Security by Design (Waidner et al. 2013) kann die Probleme nicht völlig lösen, wohl allerdings die allgemeine Gefährdungslage erheblich verbessern. Diese Erkenntnis ist ein wesentlicher Ausgangspunkt für den Bedarf am Bedarf an ML für die IT-Sicherheit.

Angriffe ändern sich ständig. Beispielsweise modifizieren Angreifer Computerviren automatisch, sodass Virenscanner sie nicht mehr erkennen. Alle drei Monate werden schätzungsweise rund 18 Millionen neue Beispiele für Schadprogramme gefunden (Atos 2017, S. 32). Ziel muss es sein, Programme zu entwickeln, um Angriffe auszumachen, die gerade erst vorbereitet werden, also bevor sie überhaupt Schaden anrichten können. Hinter welchen Daten könnte sich ein Angriff verbergen? Allerdings entsteht aus einzelnen Daten im Allgemeinen kein vollständiges Bild. Es besteht die Hoffnung, dass mit ML entsprechende Muster zu identifizieren sind. Für die riesigen Mengen an Kommunikationsdaten werden außerdem Programme benötigt, die Angriffe und Risiken über Systemgrenzen hinweg erkennen können (vgl. auch Juniper 2016). Generell gilt, dass der Aufwand hoch ist.

Es ist spannend, dass die Forschung und Entwicklung für ML-Sicherheitsprodukte weitgehend innerhalb von Unternehmen stattzufinden scheint. Dies erschwert die strategische Entwicklung des Themas, da die Ergebnisse der Unternehmensforschung sowie die Daten und Algorithmen nicht öffentlich zur Verfügung stehen. Augenfällig ist, dass im Vergleich zur ML-Forschung im Allgemeinen heute nur wenige Fachkonferenzen existieren, auf denen die Verbindung von ML und IT-Sicherheit diskutiert wird. Eine der wenigen Ausnahmen bildet der ACM Workshop on Artificial Intelligence and Security, der seit 2008 jährlich im Rahmen der ACM Conference on Computer and Communications (CCS) ausgerichtet wird. ML ist ansonsten eher Thema auf sogenannten Hacker-Konferenzen wie der DEF CON[8]. Hinzu kommen Konferenzen zur KI und ML, auf denen vereinzelt IT-Sicherheit adressiert wird. Auch auf Konferenzen zur IT-Sicherheit taucht ML bisher eher am Rande auf. Mit dem zunehmenden Bedarf an IT-Sicherheit scheint sich dies jedoch zu ändern. 2017 wurde das „International Symposium on Cyber Security Cryptography and Machine Learning (CSCML 2017)“ ins Leben gerufen, das die Ben-Gurion University in Israel ausrichtete, mit einer Nachfolge in 2018. Der erste DL and Security Workshop im Jahr 2018 hat zusammen mit dem 39th IEEE Symposium on Security and Privacy stattgefunden.

[8] *https://www.youtube.com/watch?v=wbRx18VZlYA , zuletzt geprüft am 22.06.2018*

ML gegen Schadprogramme

Beim Schutz von IT-Systemen besteht eine der wesentlichen Herausforderungen darin, neue Schadprogramme möglichst schnell abzuwehren oder sogar vorausschauend zu handeln. Antivirenprogramme kombinieren dafür im Allgemeinen mehrere Verfahren. Eines davon umfasst die Identifizierung und Verwaltung von Schadprogramm-Signaturen. Signaturen sind kurze Byte-Folgen, die aus den Schadprogrammen extrahiert werden[9]. Die Signatur-Datenbanken müssen ununterbrochen aktualisiert werden. „Es kommen mehr als 100.000 Signaturen von Schadsoftware täglich hinzu."[10] Solche Zahlen sind Schätzungen und sollen teilweise noch deutlich höher liegen. Basierend auf einer Analyse der AV-Test GmbH schätzt Heise.de, dass „täglich über 390.000 neue Schadprogramme, also über 16.000 pro Stunde beziehungsweise 4 bis 5 neue pro Sekunde"[11] auftreten (vgl. auch BSI 2017, S. 22).

Diese enorm hohen Zahlen ergeben sich allerdings vor allem daraus, dass Malware ständig „mutiert" (polymorphe Malware). Signatur-Datenbanken verwalten aus Effizienzgründen Signaturen in Form sogenannter Hashwerte, oft in hexadezimaler Darstellung, die mit Hilfe von Hashfunktionen berechnet werden[12]. Geringste Änderungen eines Schadprogramms führen zu neuen Hashwerten. So entstehen immer wieder ähnliche, aber nicht identische „Schädlinge"[13], die in den Datenbanken als quasi neue Schädlinge trotzdem mit verwaltet werden.

An dieser Stelle kommt ML ins Spiel: Auf Signaturen aufbauende Virenprogramme arbeiten oft regelbasiert. „Aufgrund ihrer Komplexität und der Anfälligkeit für eine verschobene Gewichtung sind regelbasierte Anti-Malware-Systeme sehr anfällig dafür, eine Bedrohung zu übersehen." (Juniper 2016, S. 3). Heute versucht man, diese regelbasierten Ansätze mit Methoden des ML zu überlagern, um Regeln zu gewichten und zu optimieren (Juniper 2016, S. 4).

Strobel (2017) erläutert einen Ansatz, den der Anbieter Cylance verfolgt. Danach nutzt Cylance zwar die vorgesehene Windows-Schnittstelle für Virenschutz, aber die

---

[9] *https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/V/Virensignatur.html, zuletzt geprüft am 22.06.2018*

[10] *http://www.deutschlandfunk.de/antiviren-software-neue-methoden-der-malware-erkennung.684.de.html?dram:article_id=379868, zuletzt geprüft am 22.06.2018*

[11] *https://www.heise.de/newsticker/meldung/Zahlen-bitte-Taeglich-390-000-neue-Schadprogramme-3177141.html, zuletzt geprüft am 22.06.2018*

[12] *https://www.datenschutzbeauftragter-info.de/hashwerte-und-hashfunktionen-einfach-erklaert/, zuletzt geprüft am 22.06.2018*

[13] *https://www.heise.de/newsticker/meldung/Zahlen-bitte-Taeglich-390-000-neue-Schadprogramme-3177141.html, zuletzt geprüft am 22.06.2018*

Malware wird nicht anhand von Signaturen erkannt. Eingesetzt wird ein mathematisches Modell, das mit Malware-Objekten und gutartigen Dateien beim Hersteller trainiert wurde. Der Umweg über die Signaturerkennung ist nicht mehr notwendig, nur das Modell muss an die Kunden ausgeliefert werden. So verlängern sich die Auslieferungszeiten. Strobel (2017) geht davon aus, dass andere Hersteller von Virenschutzprogrammen Methoden der KI einsetzen, um Signaturen beim Hersteller schneller erzeugen zu können. Bei diesem Ansatz muss jedoch weiterhin die Signaturdatenbank an die Kunden geliefert werden.

Cohen, Hendler und Potashnik (2017) erforschen einen Ansatz, um signaturbasierte Schadcodeerkennung zu ergänzen. Sie nutzen Anti-Virus-Reports eines SIEM-Systems (Security Information and Event Management), um Trainingsdaten zu generieren. Systeme, die damit trainiert werden, können automatisch komplexe und dynamische Muster im Systemverhalten besser erkennen.

ML gegen Sicherheitslücken

Größere Software- und Hardwaresysteme besitzen fast immer Schwachstellen (Vulnerabilities). Sie entstehen z. B. durch Fehler bei der Programmierung[14] oder auch durch unbekannte Sicherheitslücken. Bekannt ist etwa die Injektion von Schadcode in Datenbankanfragen, um Daten auszuspähen. „Grobe Schätzungen zeigen, dass ein Programmierer pro 1000 Programmzeilen einen Fehler erzeugt".[15] Sicherheitslücken erlauben beispielsweise „Zero Day Exploits", das sind Angriffe, die am gleichen Tag erfolgen, an dem die Schwachstelle entdeckt wird.[16,17] Seitenkanalangriffe zielen z. B. auf kryptographische Systeme, indem sie durch physikalische Messungen (z. B. elektromagnetische Felder, Energieverbrauch) Zugriff auf sensible Daten bekommen.[18] Zwei der jüngsten und sehr bekannten Seitenkanalangriffe auf Computerchips waren Meltdown und Spectre Anfang 2018.[19] Prozessoren legen aus Performance-

[14] *https://www.security-insider.de/was-ist-eine-sicherheitsluecke-a-648842/, zuletzt geprüft am 22.06.2018*

[15] *https://de.wikipedia.org/wiki/Sicherheitslücke , zuletzt geprüft am 22.06.2018*

[16] *https://www.kaspersky.de/resource-center/definitions/zero-day-exploit; zuletzt geprüft am 22.06.2018*

[17] *https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817322, zuletzt geprüft am 22.06.2018*

[18] *https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html;jsessionid=AB23BDE13869A528AA3EE8D76137BF9E.2_cid341?cms_lv2=9817308, zuletzt geprüft am 22.06.2018*

[19] *http://www.secupedia.info/wiki/Seitenkanalangriff, zuletzt geprüft am 22.06.2018*

gründen vorausschauend Daten im Speicher ab. Mit Meltdown wurde gezeigt, dass bei Intel-Prozessoren auf diese Speicherbereiche zugegriffen werden kann und die Daten auslesbar sind. Von Spectre sind „prinzipiell alle modernen Prozessoren betroffen".[20] Hier bekommen Prozesse Zugriff auf einen virtuellen Speicher in einem Adressraum, der nicht zugänglich sein sollte.[21]

Um Sicherheitslücken zu finden oder auch auszunutzen, müssen Systeme, Programmiersprachen und Hardware bis ins Detail verstanden werden. Im Fall von Spectre und Meltdown haben Forscherteams eine entsprechende Lücke vorhergesagt – und lange geforscht, um sie zu belegen. Sicherheitslücken sind vielfältig. Solche Lücken sind besonders schwierig und vielleicht gar nicht durch ML-Ansätze zu finden, die ganz wesentlich auf der Mustererkennung und Generalsierung beruhen, wofür Trainingsdaten existieren müssen.

Trotzdem bestehen ML-Ansätze für das Aufdecken von Sicherheitslücken, die jedoch wiederum spezialisiert sind. Godefroid, Peleg und Singh (2017) erforschen beispielsweise ML-Ansätze für Input-Fuzzing. Fuzzing bezeichnet das Finden von Sicherheitslücken in Parsern, die Programm-Input überprüfen. Grammatik-basierte Parser-Ansätze werden dort als besonders effektiv eingestuft, um mit komplexem Input umzugehen, wie er beispielsweise für Web-Browser besteht. Diese erhalten als Input u. a. HTML-Dokumente und JavaScript-Code. Die Parser-Grammatiken werden heute noch von Menschen definiert. Der Forschungsansatz untersucht das automatische Generieren der Grammatiken auf Basis von ML-Techniken.

Ein ganz anderer Ansatz wird von Benadjila, Prouff, Strullu, Cagli und Dumas (2018) verfolgt. Sie untersuchen Technologien des tiefen Lernen (Deep Learning, DL) zur Seitenkanalanalyse und setzen auf Ansätze, die zeigen, dass DL-Algorithmen effizient sind, um das Verhalten eingebetteter Systeme und deren Abhängigkeiten untereinander zu evaluieren. Kritisiert wird, dass bei den bestehenden Verfahren die Parametrisierung der neuronalen Netze nicht veröffentlicht wird und entsprechend Ergebnisse nicht reproduziert werden können. Als Ergebnis führen sie eine offene Plattform ein, ASCAD, die alle Quellen der Implementierung offenlegt.

Chen, Sultana und Sahita (2018) stellen einen DL-Ansatz vor, um Kontrollflüsse während der Hardwareprogrammausführung bezüglich Schadcode zu klassifizieren.

[20] *ebd.*

[21] *ebd.*

ML zur sichereren Kommunikation vernetzter IT-Systeme in Unternehmen

Eine weitere Herausforderung bei der Absicherung vernetzter IT-Systeme in Unternehmen besteht darin, dass eine enorm große Menge an Daten beim Monitoring der Netzwerke entsteht. Industrieunternehmen arbeiten häufig mit sehr heterogenen Teilsystemen und Komponenten, womit eine Vielfalt an Schnittstellen und Netzwerkprotokollen einhergeht. Es handelt sich um Systemlandschaften aus EDV, SCADA-Systemen (Supervisory Control and Data Acquisition), eingebetteten Systemen und Produktionsmaschinen sowie Bussystemen, Internettechnologien, Firewalls und Netzwerktechnologie, um nur einen kleinen Ausschnitt zu nennen. Mit der Automatisierung von Prozessen aller Art steigt der Vernetzungsgrad ständig an. Der Schutz durch Firewalls und Antiviren-Programme reicht heute nicht mehr aus, und es wurden deshalb zusätzliche Alarmtechnologien entwickelt, darunter Intrusion Detection Systems (IDS) oder Honeypot.s.[22]

Die Erkennung von Einbrüchen (Intrusion Detection) in solche vernetzten Systemlandschaften basiert im Wesentlichen auf der Analyse der Netzwerkkommunikation, um Angriffsmuster zu identifizieren.[23] Dafür zeichnen Sensoren möglichst umfassend Datenpakete auf (Logging). Das anfallende Datenvolumen stellt allerdings eine Herausforderung für die Auswertung dar, einerseits hinsichtlich der Schnelligkeit, anderseits hinsichtlich der potenziellen Zusammenhänge zwischen den an den verschiedenen Sensoren erfassten Daten.

Die in den Logdaten identifizierten potenziellen Angriffe erzeugen eine sehr hohe Anzahl an Angriffsalarmen. Dies ergibt sich einerseits daraus, dass diverse Alarme ausgelöst werden, obwohl es sich gar nicht um einen Angriff handelt (false positive), andererseits aber auch aus der puren Menge der meist automatisch generierten Angriffe durch Hacker. Ein Sicherheitsanalytiker kann jedoch mit etwa 30 Warnungen pro Tag nur einen Bruchteil dieser Alarme bearbeiten (Patel 2017).

KI und ML sind also dringend notwendig, um diese Analysen zu unterstützen oder zu automatisieren. Die Nutzung von ML-Verfahren ist jedoch aufwendig, da sie im Regelfall umfangreich parametrisiert oder trainiert werden müssen. Der IT-Sicherheitsanbieter Symantec sammelt dafür Bedrohungs- und Angriffsdaten aus 175 Millionen Endgeräten und 57 Millionen Angriffssensoren. Nach deren Angaben resultieren daraus knapp vier Billionen Beziehungen, die ununterbrochen überwacht wer-

[22] *https://de.wikipedia.org/wiki/Honeypot, zuletzt geprüft am 22.06.2018*

[23] *https://de.wikipedia.org/wiki/Intrusion_Detection_System , zuletzt geprüft am 22.06.2018*

den.[24] Außerdem werden mit Hilfe von ML Modelle erlernt, um Voraussagen über Ereignisse und Verwundbarkeiten in der Zukunft zu treffen.[25]

Haq et al. (2015) stellen eine umfangreiche Studie zu Verfahren des ML für IDS vor. Darin untersuchen sie 49 Forschungsbeiträge zu Klassifikationsalgorithmen für Intrusion Detection, sowohl zum überwachten als auch zum unüberwachten Lernen. Beim überwachten Lernen werden meistens die Trainingsdaten vorkategorisiert, vereinfacht in „Angriff" oder „kein Angriff". Durch Vergleiche werden neue Fälle entsprechend einsortiert und die Sortierung wird fortlaufend überwacht.

Methoden zum unüberwachten Lernen lassen sich im Wesentlichen als Clusterverfahren charakterisieren. In Haq et. al. werden dazu eine ganze Reihe von Verfahren genannt, für deren Erläuterung hier auf das Originalpapier verwiesen wird. Beispiele für überwachtes Lernen sind Artificial Neural Network, Bayesian Statistics, Gaussian Process Regression, Lazy learning, Nearest Neighbor algorithm, Support Vector Machine, Hidden Markov Model, Bayesian Networks, Decision Trees (C4.5, ID3, CART, Random Forrest), K-nearest neighbor, Boosting, Ensembles classifiers, Linear Classifiers und Quadratic classifiers. Beispiele für unüberwachtes Lernen sind dort Cluster analysis, Hierarchical clustering, Self-organizing map, Apriori algorithm, Eclat algorithm und Outlier detection.

Besonders schwierig ist die Erkennung von Advanced Persistent Threats (APTs).[26] Sie sind meistens auf ein ganz bestimmtes Ziel im Unternehmen ausgerichtet, nutzen unter Umständen unbekannte Sicherheitslücken und verwenden sehr komplexe Angriffsstrategien, die zudem nicht nur auf IT beruhen. Die Angriffe sind beharrlich und verlaufen über Wochen, Monate oder Jahre. Durch den speziellen Zuschnitt sind sie kaum anhand allgemeiner Muster zu erkennen. Für die Identifizierung sind oft detaillierte Analysen notwendig.

Arnaldo, Cuesta-Infante, Arun, Lam, Bassias und Veeramachaneni (2017) stellen in ihrem Forschungsbeitrag einen Rahmen vor, um Repräsentationen von Logdaten zu lernen, mit dem Ziel, APTs zu erkennen, die sich über mehrere Wochen hinziehen. Der Ansatz nutzt eine divide-and-conquer- Strategie (rekursive Problemzerlegung mit anschließender Synthese) und kombiniert diese mit Verhaltensanalysen und Zeitreihenmodellen. Es wird gezeigt, dass auf einer Basis von drei Milliarden Zeilen Log-

---

[24] *https://www.websecurity.symantec.com/de/de/security-topics/machine-learning-new-frontiers-advanced-threat-detection , zuletzt geprüft am 22.06.2018*

[25] *https://www.recordedfuture.com/machine-learning-application/ , zuletzt geprüft am 22.06.2018*

[26] *https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT, zuletzt geprüft am 22.06.2018*

daten gute Resultate erzielt werden mit 95 von 100 richtig erkannten Beispielen im Vergleich zu Testdaten.

Laurenza et al. (2017) verfolgen hinsichtlich APTs einen anderen Ansatz. Sie gehen davon aus, dass vor allem eine Priorisierung in der großen Anzahl von Informationen zu potenziellen Angriffen erfolgen muss. Vorgeschlagen wird ein Vorgehen für die Sichtung der Alarme mit Fokus auf APTs. Betrachtet werden dafür nur statische Schadcode-Eigenschaften, die schnell ausgewertet werden können. Damit wird ein Random Forest classifier trainiert. Das Verfahren scheint eine hohe Präzision zu erreichen. Es nutzt Entscheidungsbäume, die „zufällig" wachsen, sowie nach der Lernphase Klassifizierungen für Entscheidungen.

ML im Einsatz bei der Kommunikation im Internet

Private Rechner und Unternehmenssysteme inklusive IT-Komponenten von Produktionsanlagen sind heute komplex vernetzt. Hinzu kommt eine stetig steigende Anzahl netzfähiger Geräte, Sensoren und Gegenstände, die das Internet zu einem Internet der Dinge (IoT) erweitern. Alle eingebundenen Elemente kommunizieren miteinander. Über diese Kommunikation können sie kompromittiert bzw. zu einem Verhalten veranlasst werden, das von den Eigentümern nicht zugelassen und erwünscht ist. Botnetze sind ein prominentes Beispiel, und sie erleben geradezu eine Blüte durch die Optionen, die das IoT bietet. Das Risiko und der Aufwand zum „Mieten" von Botnetzen ist für Angreifer verhältnismäßig gering – bei gleichzeitig lukrativen Zielen.[27] Das BSI (BSI 2017, S. 29) geht von 27.000 Bot-Infektionen deutscher Systeme täglich aus.

Ein Botnetz umfasst vernetzte Schadprogramme, die Bots, die ohne Einverständnis der Eigentümer auf deren Rechnern installiert wurden. Häufig sind gerade private Rechner betroffen[28], was insbesondere den Takedown der Botnetze, also deren flächendeckende Abschaltung, sehr aufwendig und kaum organisierbar macht. Nach Schätzungen sind weltweit rund ein Viertel aller Rechner betroffen.[29] Die Infektion durch Bots verläuft auf dem gleichen Weg wie bei anderen Schadprogrammen. Häufig befindet sich der Schadcode in einem E-Mail-Anhang, der durch Anklicken aktiviert wird. Ebenfalls weit verbreitet ist die Infektion durch den Besuch von Webseiten. Durch die Anwahl von Internet-Links oder sogar schon allein durch den Besuch kom-

---

[27] *https://www.heise.de/ix/meldung/IoT-Sicherheitskonferenz-Unsichere-Smart-Meter-Mirai-und-seine-Klone-und-die-Genfer-Konvention-3872793.html , zuletzt geprüft am 22.06.2018*

[28] *http://www.searchsecurity.de/definition/Botnet , zuletzt geprüft am 22.06.2018*

[29] *https://wiki.botfrei.de/Botnetze , zuletzt geprüft am 22.06.2018*

promittierter Webseiten kommt es zum Download von Schadcode: Drive-by-Download. Schadcode kann aber beispielsweise auch in Dokumenten eingebettet sein, etwa in Office-Dokumenten. Häufig verläuft die Infektion zweistufig. Der erste Schritt dient dem Download des Bots oder einer Vorstufe, worüber danach die unerlaubte Kontrolle über den privaten Rechner gewonnen wird (BSI 2017, S. 22). „Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert." (BSI 2017, S. 78).

Es ist üblich, dass kriminelle Betreiber Botnetze aufbauen, diese aber nicht sofort und eventuell nicht selbst einsetzen. Sie werden an Dritte vermietet, die sie für konkrete Angriffe verwenden. Die Botnetze sind beispielsweise in der Lage, private Rechner zum Versenden von Spam-Mails zu nutzen, sodass der wirkliche Versender anonym bleibt. Sehr bekannte Angriffe über Botnetze waren sogenannte DDos-Angriffe. DDos steht für Distributed Denial of Service. Diese „…Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen." (BSI 2017, S.79) Durch den gemeinsamen Angriff einer hohen Anzahl von Bots auf bestimmte Server wird z. B. eine Überlastung der betroffenen Systeme provoziert, um diese lahmzulegen.

Durch Botnetze sind bereits sehr bekannte Angriffe erfolgt. Botfrei.de stellt dazu umfangreiche Informationen zur Verfügung[30]: Avalanche, eines der weltweit größten Botnetze, wurde schon im Jahr 2008 entdeckt. Mit ihm wurden Massen-Spams verteilt und Phishing-Attacken umgesetzt. Avalanche unterhielt weitere 20 Botnetze zur Verbreitung von Schadprogrammen. Erst Ende 2016 konnten die Strafverfolgungsbehörden Avalanche abschalten.[31]

2017 erzielte das Mirai-Botnetz höchstes Aufsehen. Es veranlasste Ausfälle und Störungen bekannter Dienste wie Amazon, Netflix, Twitter und Github.[32] Der DDoS-Angriff nutzte vor allem ungeschützte Geräte im IoT, wie Kameras, Heizungssteuerungen und Babyfons.[33] Mit Bekanntwerden von Mirai wurden Ableger unmittelbar für neue Angriffe genutzt.[34]

Das Detektieren von Botnetzen ist eine Herausforderung.[35] ML ist eine Möglichkeit, bestehende Detektionsmethoden zu ergänzen. So ist es Wissenschaftlern der Ben-

[30] *https://wiki.botfrei.de/Botnetze , zuletzt geprüft am 22.06.2018*

[31] *https://wiki.botfrei.de/Avalanche , zuletzt geprüft am 22.06.2018*

[32] *https://wiki.botfrei.de/Mirai , zuletzt geprüft am 22.06.2018*

[33] *ebd.*

[34] *https://www.heise.de/security/meldung/Mirai-Botnetz-lernt-neue-Tricks-3670226.html , zuletzt geprüft am 22.06.2018*

[35] *https://www.internet-sicherheit.de/forschung/botnetze/botnetz-analyse.html , zuletzt geprüft am 22.06.2018*

Gurion-Universität zusammen mit den Deutsche Telekom Innovation Laboratories 2016 gelungen, mit einem ML-Verfahren Angriffe von realen Personen von denen durch Botnets auf Honeypots zu unterscheiden. So konnten wertvolle Informationen zum Aufspüren der Netze geliefert werden (vgl. Thiede 2016). Stevanovic und Pedersen (2016) stellen einen Überblick über ML-Methoden zum Erkennen von Botnetzen vor, die die Botnetz-Netzwerkkommunikation analysieren. Als bisher ungelöste Probleme werden darin die fehlende Übertragbarkeit bei der Erkennung von Botnetzen bemängelt, die Zeit, die für die Analysen notwendig ist, und die Schwierigkeit, die Methoden verständlich im operationalen Betrieb einzusetzen. Miller und Busby-Earle (2016) analysieren detailliert die Rolle von konkreten ML-Verfahren für die Erkennung von Botnetzen.

Cyber Threat Intelligence (CTI) ist ein Abwehrkonzept, das den gesamten Prozess rund um das Auffinden von Bedrohungen umfasst, deren Auswertung und Aufbereitung sowie Weitergabe. CTI untersucht „Details über die Motivation, die Intention und die Fähigkeiten von Angreifern, ihre Taktik, Techniken und Vorgehensweisen" sowie „technischere Details, wie typische Spuren von Angriffen (IoCs für „Indicators of Compromise"), Listen mit Prüfsummen von Malware-Objekten oder Reputationslisten für Hostnamen / Domains."[36] Um Sicherheitslücken schließen zu können, müssen Software- und Hardware-Anbieter, teilweise auch die Nutzerinnen und Nutzer, möglichst flächendeckend über Schwachstellen und Angriffe informiert werden. Werkzeuge zur „Threat Intelligence" leisten diese Aufgabe. Sie sammeln und aggregieren Daten aus unterschiedlichen Quellen und stellen die Ergebnisse in Form von „Data Feeds" zur Verfügung. Manche Systeme agieren teilweise automatisiert. Die Data Feeds umfassen z. B. Informationen zu IP-Adressen, die eine Bedrohung darstellen, über Phishing-URLs bis hin zu schadhafter Software. Die Nutzung solcher Dienste ermöglicht es, Lücken proaktiv zu schließen. Auch für CTI wird ein Potenzial beim Einsatz von ML gesehen.[37]

Die Nutzung von ML durch Angreifer

Es sind bisher keine Beispiele bekannt, dass Angreifer Lernmodelle kompromittiert haben, aber es ist zu erwarten, dass sie in Zukunft auch ML nutzen.[38] Es ist deshalb

---

[36] *http://www.secupedia.info/wiki/Cyber_Threat_Intelligence#ixzz5C0nLUozU , zuletzt geprüft am 22.06.2018*

[37] *http://www.wipro.com/documents/Demystifying-machine-learning-for-threat-detection.pdf, zuletzt geprüft am 17.07.2018*

[38] *https://www.computerwoche.de/a/wie-maschinelles-lernen-zum-verhaengnis-wird,3544253 , zuletzt geprüft am 22.06.2018*

dringend notwendig, entsprechende Kompetenzen auch bei den Entwicklern von Sicherheitssystemen aufzubauen. ML-Verfahren sind angreifbar, indem die trainierten Klassifizierer, die Modelle, die neuronalen Netze, Bäume etc. mit feindlichen Beispielen unterlaufen werden. Wird der Lernprozess gestört, so entscheiden die Algorithmen am Ende u. U. fehlerhaft zugunsten der Angreifer. Durch den Einsatz von ML-Methoden erhöhen sich also letztlich die möglichen Angriffsvektoren. Allerdings wären solche Angriffe hochkomplex – und es ist unklar, wie hoch das Risiko dafür tatsächlich ist. Hayes und Danezis (2018) diskutieren das Problem, dass Klassifizierer durch feindliches Einschleusen von Falschbeispielen zu schlechten oder falschen Entscheidungen provoziert werden können. Sie stellen das Szenario eines feindlichen Netzwerkes vor, das täuschenden Output für Klassifizierer erzeugt. Auch Kos, Fischer und Song (2017) untersuchen Methoden, wie feindliche Lernbeispiele die Generierung von Modellen beeinflussen. Normalerweise sollten Angreifer keinen Zugang zu den Strukturen und Parametern der ML-Modelle der Sicherheitssysteme besitzen, denn das Zielsystem ist eine Blackbox. Hu und Tan (2017) stellen allerdings einen Algorithmus vor, der diese Blackbox-Modelle umgehen kann. Die Erkennungsrate wird deutlich verringert.

ML gegen Angriffe über verschlüsselte Kommunikation

Verschlüsselung dient dem Schutz von Daten, die während einer Netzkommunikation übertragen werden. Sehr bekannt ist beispielsweise das SSL-Protokoll. Es wird sichtbar, wenn im Web-Browser einer URL „https“ vorangestellt ist. Leider können auch Angreifer verschlüsselte Kommunikation ausnutzen. Sie können mit verschlüsselten Daten verhindern, dass Angriffserkennungssysteme Signaturen (s. o.) sinnvoll einsetzen können. Es besteht dann noch die Option, die Angriffe mit Hilfe der Kommunikationsmetadaten zu entlarven. Für solche Anomalieerkennung eignen sich ML oder auch Methoden der KI.[39]

Im CISCO Security-Report von Februar 2018, wird festgestellt, dass immer mehr Web-Kommunikation verschlüsselt ist und sich innerhalb von 12 Monaten verdreifacht hat.[40] Er geht von einem Anteil von rund 50 Prozent verschlüsselter Kommunikation aus. Nach Angaben von CISCO nutzen heute bereit 34 Prozent der Unterneh-

[39] *https://www.searchsecurity.de/antwort/Wie-lassen-sich-verborgene-SSL-Angriffe-erkennen-und-abwehren, zuletzt geprüft am 22.06.2018*

[40] *http://www.netzwerker.news/content/Malware-versteckt-sich-in-verschluesseltem-Traffic.html?_pr=1, zuletzt geprüft am 22.06.2018*

men ML- und 32 Prozent KI-Systeme, die auch Angriffe mit verschlüsselten Anteilen erkennen können. Das wird zunehmend relevant in Cloud- und IoT-Umgebungen.[41]

ML für datenschutzkonforme IT-Sicherheit

Datenschutz und IT-Sicherheit stehen in einem höchst spannungsgeladenen Zusammenhang. Die Diskussionen dazu sind zu umfangreich, um hier angemessen wiedergegeben zu werden. Verkürzt steht die Behauptung im Raum, es wäre sehr viel einfacher, Angriffe zu erkennen, wenn Kommunikation bis ins Detail überprüft und festgehalten würde und keine Verschlüsselung stattfände. Dies widerspricht jedoch unseren demokratischen Grundwerten mit den über Jahrzehnten entwickelten juristischen Rahmenbedingungen und darf deshalb so nicht umgesetzt werden (vgl. z. B. Friedrich-Ebert-Stiftung 2007).

Eine besondere Herausforderung stellt das für die Erkennung von APTs dar (s. o.). Oft müssen dafür auch Verhaltensweisen von Personen eingeschätzt werden. Das gelingt nur, wenn Daten personenbezogen gespeichert werden. Solche Ansätze werden als User Behavior Analytics (UBA) bezeichnet und nutzen auch ML. Es ist eine Herausforderung, diese datenschutzkonform zu gestalten. Neben den Datenschutzproblemen gibt es für UBA auch schwerwiegende technische Probleme. Wie erkennt man etwa normales Verhalten von Personen? Auf Basis welcher Beispiele wird gelernt und worin bestehen die relevanten Eigenschaften komplexer Situationen? Außerdem fehlt für manche ML-Verfahren die notwendige Menge an Trainingsdaten (Strobel 2017).

ML in der Praxis

In der Praxis werden Methoden des ML heute schon eingesetzt und es existieren diverse Anbieter, die damit werben. Tabelle 4.1 stellt das Ergebnis einer Internetrecherche dazu dar. Die Liste erhebt keinen Anspruch auf Vollständigkeit, sondern bietet nur einen Einblick. Anhand der Informationen, die von den Anbietern öffentlich zur Verfügung gestellt werden, ist nicht im Detail abzulesen, wie fortgeschritten die Nutzung der ML-Methoden ist. Im Rahmen der Recherche wurden die Orte der Hauptsitze der Unternehmen festgehalten und aufgenommen, ob Niederlassungen in Deutschland existieren. Es zeigt sich, dass viele der Unternehmen einen Sitz in Deutschland haben, sodass davon ausgegangen werden kann, dass auch in Deutschland Forscher und Praktiker Kompetenzen zur ML und IT-Sicherheitspraxis besitzen.

[41] *https://gblogs.cisco.com/de/cisco-security-report-gefahrenabwehr-mit-kuenstlicher-intelligenz-machine-learning-und-automation/, zuletzt geprüft am 22.06.2018*

Ein großer regionaler Schwerpunkt der Unternehmen ist das Silicon Valley in den USA.

Tabelle 4.1: Unternehmen, die ML- Methoden in ihren IT-Sicherheitsprodukten einsetzen

ANBIETER	ML-NUTZUNG	FIRMENSITZ
Atos	Atos nutzt Automatisierung und maschinelles Lernen um Angriffe zu verstehen und vorherzusagen.[1] (vgl. auch Atos 2017)	Atos Bezons, Frankreich Atos IT Solutions and Services: München, Deutschland
G DATA	G DATA stellen in ihrem Blog ausführlich dar, welche ML-Ansätze sie gegen Phishing-Angriffe nutzen.[2]	Bochum, Deutschland
Bitdefender	Sandbox-Analyzer nutzt maschinelles Lernen zur Verhaltensanalyse. „Vorausschauende Erkennung unbekannter Malware. Dynamische Dateianalyse trainiert anhand von Milliarden von Beispielen. Bedrohungsdatenbank auf der Basis von über 500 Millionen Endpunkten."[3]	Bukarest, Rumänien Tettnang, Deutschland
Centrify	Centrify ist ein Lösungsanbieter zum Schutz digitaler Identitäten. „Der neue Service nutzt maschinelles Lernen zur Risikoeinschätzung, basierend auf dem sich ständig verändernden Anwenderverhalten. Anhand dieser Risikoeinschätzungen werden Anwenderaktivitäten Risc Scores zugeteilt und die passenden Reaktionen auf diese Aktivitäten durchgeführt. Dabei entscheidet der Service in Echtzeit, ob der Zugriff gewährt wird, ob zu einer besseren Authentifizierung aufgefordert werden soll oder ob der Zugriff komplett geblockt wird."[4, 5]	Santa Clara, USA
CheckPoint	CheckPoint nutzt maschinelles Lernen zur Identifikation von Angriffen.[6] Es werden „Muster von aktuellen Bedrohungsdaten" eingebunden, die beim Kunden anfallen.[7]	Tel Aviv, Israel San Carlos, USA
Cylance	Nutzt Künstliche Intelligenz für Endpunkt-Sicherheit. u.a.: Schadcode Prävention, Applikations- und Skript-Kontrolle, Angriffsverfolgung, Ursachenanalyse[8], weiterhin Erkennung von Schadcode ohne Signaturen mit Hilfe von ML (Strobel, 2017)	Irvine, USA Cylance Germany: München, Deutschland

1 *https://atos.net/en-gb/united-kingdom/digital-vision-programme/digital-vision-cyber-security, zuletzt geprüft am 13.06.2018*

2 *https://www.gdata.de/blog/2018/05/smarterphishing-schutz, zuletzt geprüft am 15.06.2018*

3 *https://www.bitdefender.de/business/elite-security.html, zuletzt geprüft am 13.06.2018*

4 *https://www.it-cloud.today/centrify-analytics-service-stoppt-in-echtzeit-sicherheitsverletzungen-basierend-auf-dem-anwenderverhalten/#more-21199, zuletzt geprüft am 14.06.2018*

5 *https://www.silicon.de/41661245/ki-und-maschinelles-lernen-in-der-it-security/?inf_by=5a1d32c5671db8a0218b4b82, zuletzt geprüft am 14.06.2018*

6 *https://www.checkpoint.com/press/2018/check-point-announces-infinity-total-protection-unique-new-security-model-prevent-gen-v-threats-attacks/, zuletzt geprüft am 14.06.2018*

7 *https://www.silicon.de/41661245/ki-und-maschinelles-lernen-in-der-it-security/, zuletzt geprüft am 14.06.2018*

8 *https://www.cylance.com/content/dam/cylance/pdfs/data_sheets/CylancePROTECT.pdf, zuletzt geprüft am 13.06.2018*

ANBIETER	ML-NUTZUNG	FIRMENSITZ
Darktrace	„Erkennung und Klassifizierung von Bedrohungen auf Basis von Anomalieerkennung mittels Machine Learning“[9]. Eingesetzt wird unbeaufsichtigtes maschinelles Lernen ohne Trainingsdaten. Selbstverteidigung durch Verlangsamen von Angriffen, Unterbrechung der Echtzeit, Stoppen der Angriffe.[10]	Cambridge, Großbritannien
Escrypt (100%iges Tochterunternehmen der ETAS GmbH)	Das Unternehmen fokussiert mit seinen Lösungen auf konkrete Branchen: Automotive, Smart City, Internet der Dinge. Daten aus der Intrusion Detection werden „mithilfe leistungsstarker Algorithmen für maschinelles Lernen“ ausgewertet und „Angriffsmuster für die gesamte Flotte“ visualisiert. Neue Angriffsarten werden identifiziert.[11]	Bochum, Deutschland
Eset Deutschland	Sortierung und Klassifizierung von großen Mengen an Malware-Samples. Platzieren der analysierten Malware-Samples auf einer „Cyber Security Map“, um Relevanz der Malware einzuschätzen. „Neuronale Netzwerke für spezielles tiefgehendes Lernen und ein langes Kurzzeitgedächtnis. Konsolidierter Output von sechs genau gewählten Klassifikationsalgorithmen“[12].	Bratislava, Slowakei Eset Deutschland: Jena, Deutschland
Exabeam	ML für „User Behavior Analytics“ Lösung, Aufzeigen unauthorisierter Systemzugriffe[13]	San Mateo, USA
Finally Safe (Beteiligung duch secunet Security Networks)	Anomalie-Erkennung basiert auf über vier Millionen möglicher Paketinformationen. Mit Verfahren des maschinellen Lernens wird ein Modell der Netzwerk-Kommunikation erstellt, also das Netzwerkverhalten erlernt, um dann Anomalien aufzudecken.[14]	Essen, Deutschland
G+D	Giesecke + Devrient setzen ML zur Aufdeckung von ungewöhnlichen Systemreaktionen ein. Bestandteil der Lösung ist ein lernendes Anomalieerkennungssystem (Anomaly Detection System, ADS).[15]	München, Deutschland
McAffee / McAffee Laps (McAffee Forschung)	„McAfee nutzt maschinelles Lernen und andere unbeaufsichtigte Lernalgorithmen in seinem gesamten Portfolio, von Advanced Threat Defense (ATD) und Security Information and Event Management (SIEM) bis hin zu URL Classification Systems und im Gateway.“ (Patel, 2017)	Santa Clara, USA McAffee Labs: Hamburg, Deutschland

9 *https://www.pallas.com/nachrichten/nachrichten-details/news/pallas-ist-zertifizierter-partner-von-darktrace/, zuletzt geprüft am 13.06.2018*

10 *https://www.wallstreet-online.de/nachricht/8387235-darktrace-cyber-immunsystem-schlaegt, zuletzt geprüft am 13.06.2018*

11 *https://www.escrypt.com/de/news-events/angriff-erkannt-gefahr-gebannt, zuletzt geprüft am 14.06.2018*

12 *https://www.welivesecurity.com/deutsch/2017/06/22/machine-learning-eset-augur-engine/, zuletzt geprüft am 13.06.2018*

13 *https://www.exabeam.com/data-science/machine-learning-sdk-for-security-analytics/, zuletzt geprüft am 13.06.2018*

14 *https://www.finally-safe.com/produkt/, zuletzt geprüft am 13.06.2018*

15 *https://www.gi-de.com/de/de/mobile-security/trends/umgang-mit-cyberrisiken/, zuletzt geprüft am 15.06.2018*

ANBIETER	ML-NUTZUNG	FIRMENSITZ
One Identity	One Identity, heute Teil von Quest Software, erwarb Anfang 2018 das Unternehmen Balabit. Die dort entwickelte Technologie realisiert Privileged-Account-Analytics (PAA), die Analyse privilegierter Nutzerinnen und Nutzer, um insbesondere Insider-Attacken zu erkennen. Dafür werden Verfahren des maschinellen Lernens und der künstlichen Intelligenz eingesetzt.[16, 17]	Aliso Viejo, California
Palo Alto Networks	Bietet Plattform für hoch automatisierte Systemanalysen. Das Unternehmen übernahm 2017 die LightCyber, einen Technologieexperten zur Analyse von Systemverhalten.[18] Gelernt wird „normales" Kommunikationsverhalten (Strobel, 2017).	Santa Clara, USA
Recorded Future	Recorded Future hat eine eingetragene Marke Threat Intelligence Machine™. Genutzt werden ML und Verfahren zum Verstehen natürlicher Sprache.[19]	Somerville, USA
Rhode & Schwarz	Auf Grundlage recherchierten Informationen wird angenommen, dass Rhode & Schwarz „Deep Learning"-Ansätze nutzt oder vorbereitet. Rhode & Schwarz entwickelt auf Basis einer CUDA-Architektur „Deep Learning"-Unterstützung[20]. CUDA wurde von NVIDIA entwickelt und nutzt Grafikprozessoren (GPU), um Lernverfahren in „Deep Learning"-Netzen durch starke Parallelisierung von Rechenprozessen zu beschleunigen.	München, Deutschland
Securonix	ML (sowohl überwachte als auch unüberwachte Verfahren), Angriffsmodellierung und statistisch Ansätze für die Analyse von Systemverhalten zur Umsetzung Signturloser Technologien.[21]	Addison, USA
Sonic Wall	Sonic Wall führt in Echtzeit tiefgreifende Speicheranalysen mit ML-Ansätzen mit einer dafür entwickelten Technologie durch, die in einer Cloud Plattform integriert sind.[22] Sonic Wall liefert performante Lösungen, „um den verschlüsselten Datenverkehr zu entschlüsseln, zu untersuchen und wieder zu verschlüsseln" und „dabei unterschiedlichste Schadsoftware zu erkennen"[23].	San Jose, USA

16 *https://www.silicon.de/41661245/ki-und-maschinelles-lernen-in-der-it-security/, zuletzt geprüft am 13.06.2018*

17 *https://www.quest.com/community/products/one-identity/news/b/press-releases/posts/one-identity-acquires-balabit-to-bolster-privileged-access-management-solutions#, zuletzt geprüft am 13.06.2018*

18 *https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-completes-acquisition-of-lightcyber, zuletzt geprüft am 13.06.2018*

19 *https://www.recordedfuture.com/technology/, zuletzt geprüft am 14.06.2018*

20 *https://www.careers.rohde-schwarz.com/de/spezialseiten/karriere-news/?nid=41, zuletzt geprüft am 13.06.2018*

21 *https://www.securonix.com/leverage-machine-learning-cybersecurity/, zuletzt geprüft am 13.06.2018*

22 *https://www.sonicwall.com/en-us/about-sonicwall/news/press-releases/pr-articles/sonicwall-invents-real-time-deep-memory-inspection zuletzt geprüft am 15.06.2018*

23 *https://www.silicon.de/41661245/ki-und-maschinelles-lernen-in-der-it-security/?inf_by=5a1d32c5671db8a0218b4b82, zuletzt geprüft am 15.06.2018*

ANBIETER	ML-NUTZUNG	FIRMENSITZ
Sophos	Endpunkt-Schutz. Übernahme von Invincea in 2017 mit Kompetenz zum Ausschalten bislang unbekannter Schadsoftware und hochentwickelter Cyberattacken mit Hilfe patentierter neuronaler Netz-Algorithmen (Deep Learning)[24]; dadurch steht Hilfsmittel gegen Zero-Day-Attacken zur Verfügung[25].	Abingdon, Großbritannien
Symantec	Symantec entwickelt in großem Maße ML-Verfahren. „Dazu gehören innovative Forschung zu Deep Learning, probabilistische Programmierung, verstärkendes Lernen ("Reinforcement Learning") und bayessche nichtparametrische Verfahren."[26]	Mountain View, USA München, Deutschland
Trend Micro Deutschland	Maschinelles Lernen wird seit über 10 Jahren eingesetzt „von Antispam-Engines bis zu Erkennungstechniken für bösartige Social-Media-Elemente."[27]	Tokyo, Japan Trend Micro Deutschland: Hallbergmoos, Deutschland
Vectra Networks	Aufdeckung von Angriffen in Echtzeit. Verhaltensanalyse und permanentes maschinelles Lernen. Nutzung unterschiedlicher Verfahren wie überwachtes und unüberwachtes Lernen sowie „Deep-Learning"-Techniken.[28]	San Jose, USA Vectra Networks Germany: München, Deutschland

[24] *https://www.security-insider.de/sophos-investiert-in-maschinelles-lernen-a-583300/, zuletzt geprüft am 13.06.2018*

[25] *https://www.silicon.de/41661245/ki-und-maschinelles-lernen-in-der-it-security/, zuletzt geprüft am 13.06.2018*

[26] *https://www.websecurity.symantec.com/de/de/security-topics/machine-learning-new-frontiers-advanced-threat-detection, zuletzt geprüft am 13.06.2018*

[27] *https://www.silicon.de/41661245/ki-und-maschinelles-lernen-in-der-it-security/, zuletzt geprüft am 14.06.2018*

[28] *https://vectra.ai/dach-press/neun-fragen-zu-k-nstlicher-intelligenz-und-cybersicherheit, zuletzt geprüft am 13.06.2018*

Fazit und Ausblick

Zum Einsatz von ML in der Praxis ist festzuhalten, dass ML bereits von diversen Unternehmen eingesetzt wird, die Werkzeuge zur Verbesserung der IT-Sicherheit anbieten. Anhand der öffentlichen Darstellung ist allerdings nicht immer deutlich, in welchem Umfang und welcher Qualität ML-Verfahren genutzt werden. Das wirtschaftliche Potenzial wurde aber erkannt. Forschung zur ML im Rahmen von IT-Sicherheit existiert aktuell hingegen nur in vergleichsweise geringem Umfang. Die Anzahl von wissenschaftlichen Foren, die die Thematik explizit in den Vordergrund stellen, ist klein.

Dass eine so komplexe Thematik durch die Wirtschaft vorangetrieben wird, ist überraschend. Der Hintergrund kann in der schlechten Verfügbarkeit realistischer Daten für die Forschung sowie im starken Wettbewerb zwischen den Unternehmen liegen. Heute sind jedoch noch viele Fragen zum Einsatz von ML-Verfahren im Rahmen von IT-Sicherheit ungelöst. Es ergibt sich die Hypothese, dass eine bessere Kooperation

von Forschung und Wirtschaft die Potenziale der ML effektiver ausloten würde. Die Recherchen zu diesem Artikel legen nahe, dass eine Analyse zu den Barrieren, die in Bezug auf diese Kooperation bestehen, nützlich wäre.

Wichtige Forschungs- und Entwicklungsfragen, die es zu lösen gilt sind u. a.:

- Die Ergebnisqualität der ML-Methoden hängt maßgeblich vom Training und der Qualität der Trainingsdaten ab. Leider sind reale Kommunikationsdaten für Forscherinnen und Forscher meist schlecht oder gar nicht zugänglich. Wie im Artikel geschildert, bilden aber meist erst Millionen von Datensätzen die Grundlage für ein qualitativ hochwertiges Training der ML-Methoden. Unternehmen sind häufig nicht gewillt, ihre Daten zur Verfügung zu stellen. Hier müssen Lösungen gefunden werden.
- Der Aufwand zum Training der ML-Methoden ist sehr hoch. Es werden jeweils umfangreiche Trainingsdaten benötigt, die mit hohem Auffand aufbereitet werden müssen. Das Verhältnis von Aufwand und Nutzen beim Einsatz von ML muss klarer werden bzw. durch Kooperation verringert werden.
- Die Einsatzfelder konkreter ML-Verfahren sind im Allgemeinen sehr spezialisiert. Ob es möglich ist, der Hoffnung auf umfangreich selbstlernende Systeme nachzukommen, kann in naher Zukunft vermutlich noch nicht beantwortet werden. Es stellen sich Fragen nach der Fokussierung versus Generalisierung sowie der Wiederverwendbarkeit.
- Der Einsatz vom ML erhöht die Anzahl der Angriffsvektoren. In vielen ML-Verfahren kann außerdem nicht expliziert werden, „was" gelernt wurde. Ein nicht unerheblicher Teil der Forschung beschäftigt sich deshalb genau mit der Frage, wie ML-Modelle kompromittiert werden können, aber noch nicht mit dem Schutz der Modelle.
- ML wird auch für das Erlernen von Verhaltensmustern von potenziellen Angreifern genutzt. Die Einhaltung des Datenschutzes ist dabei eine wichtige und schwierige Herausforderung.
- ML-Verfahren haben bei ihren Entscheidungen im Einsatz im Allgemeinen Grauzonen. Wie gut die Ergebnisqualität der Methoden ist oder werden kann, ist in vielen Fällen Forschungsgegenstand.

Literatur

Arnaldo, Ignacio; Cuesta-Infante, Alfredo; Arun, Ankit; Lam, Mei; Bassias, Costas; Veeramachaneni, Kalyan (2017): Learning Representations for Log Data in Cybersecurity. In Proceedings of First int. Conference Cyber Security Cryptography and Machine Learning (CSCML 2017). Dolev, Shlomi; Lodha, Sachin (Hrsg.). Springer International Publishing AG 2017. ISBN 978-3-319-60079-6.

Atos (2018): Digital Vision for Cyber Security. Opinion Paper. Online verfügbar unter https://atos.net/content/dam/uk/white-paper/digital-vision-cyber-security-opinion-paper-new.pdf, zuletzt geprüft am 22.06.2018.

Bauer, Gérard; Schmitz, Peter (2017a): Künstliche Intelligenz, Machine Learning und IT-Sicherheit. Online auf Security Insider. Online verfügbar unter https://www.security-insider.de/machine-learning-und-it-sicherheit-a-591288/, zuletzt geprüft am 22.06.2018.

Bauer, Gérard; Schmitz, Peter (2017b): IT-Security und maschinelles Lernen. Deep Learning in der Cybersicherheit. Online auf Security Insider. Online verfügbar unter https://www.security-insider.de/deep-learning-in-der-cybersicherheit-a-634857/, zuletzt geprüft am 22.06.2018.

Benadjila, Ryad; Prouff, Emmanuel; Strullu, Rémi; Cagli, Eleonora; Dumas, Cécile (2018): Study of Deep Learning Techniques for Side-Channel Analysis and Introduction to ASCAD Database. ANSSI, France & CEA, LETI, MINATEC Campus, France. Online verfügbar unter https://eprint.iacr.org/2018/053.pdf, zuletzt geprüft am 22.06.2018.

BSI (2017): Die Lage der IT-Sicherheit in Deutschland 2017. Hrsg.: Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 22.06.2018.

Chen. Li; Sultana, Salmin; Sahita, Ravi (2018): HeNet: A Deep Learning Approach on Intel® Processor Trace for Effective Exploit Detection. (submitted). arXiv:1801.02318 [cs.CR] Online verfügbar unter https://arxiv.org/pdf/1801.02318.pdf, zuletzt geprüft am 22.06.2018.

Friedrich-Ebert-Stiftung (2007): Datenschutz im Spannungsfeld von Freiheit und Sicherheit. In Dokumentation der Fachkonferenz Datenschutz 2007 am 14. Juni 2007, Berlin. ISBN 978-3-89892-728-4. Online verfügbar unter http://library.fes.de/pdf-files/stabsabteilung/04764.pdf, zuletzt geprüft am 22.06.2018.

Godefroid, Patrice; Pele, Hila; Singh, Rishabh (2017): Learn&Fuzz: machine learning for input fuzzing. In Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering, 2017 Urbana-Champaign, pp. 50-59. IEEE Press Piscataway, NJ, USA ©2017. ISBN: 978-1-5386-2684-9.

Haq, Nutan Farah; Onik, Abdur Rahman; Hridoy, Md. Avishek Khan; Rafni, Musharrat; Shah, Faisal Muhammad; Farid, Dewan Md (2015): Application of Machine Learning Approaches in Intrusion Detection System: A Survey. In International Journal of Advanced Research in Artificial Intelligence, Vol. 4, No.3, 2015, pp. 9-18.

Hayes, Jamie; Danezis, George (2018): Learning Universal Adversarial Perturbations with Generative Models. Submitted. arXiv:1708.05207 [cs.CR].

Hu, Weiwei & Tan, Ying (2017): Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN. arXiv:1702.05983 [cs.LG].

Juniper (2016): Malware überlisten. Warum maschinelles Lernen entscheidend zur Cybersicherheit beiträgt. Hrsg. Juniper Networks, Inc. Online verfügbar unter https://www.krick.net/fileadmin/Dateien/Downloads/outsmarting-malware.PDF, zuletzt geprüft am 22.06.2018.

Kos, Jernej; Fischer, Ian; Song, Dawn (2017): Adversarial Examples for Generative Models. arXiv:1702.06832 [stat.ML].

Laurenza, Giuseppe; Aniello, Leonardo; Lazzeretti, Riccardo; Baldoni, Roberto (2017): Malware Triage Based on Static Features and Public APT Reports. In Proceedings of First int. Conference Cyber Security Cryptography and Machine Learning (CSCML 2017). Dolev, Shlomi & Lodha, Sachin (Hrsg.). Springer International Publishing AG 2017. ISBN 978-3-319-60079-6.

Miller, Sean und Busby-Earle, Curts C. R (2016): The Role of Machine Learning in Botnet Detection. In Proceedings of 11th International Conference for Internet Technology and Secured Transactions (ICITST 2016). DOI: 10.1109/ICITST.2016.7856730.

Patel, Raja (2017): McAffee: Maschinelles Lernen ergänzt die Arbeit von IT-Sicherheitsspezialisten. In: Midrange Magazin. Online verfügbar unter http://www.midrange.de/maschinelles-lernen-ergaenzt-die-arbeit-von-it-sicherheitsspezialisten/, zuletzt geprüft am 22.06.2018.

Plattform Industrie 4.0 (2106): IT-Security in der Industrie 4.0, Erste Schritte zu einer sicheren Produktion. Online verfügbar unter https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/wegweiser-it-security.pdf?__blob=publicationFile&v=16, zuletzt geprüft am 22.06.2018.

Pohl, Helmut (2004): Taxonomie und Modellbildung in der Informationssicherheit. In: Datenschutz und Datensicherheit (DuD); Ausgabe 28.

Stevanovic, Matija; Pedersen, Jens Myrup (2016): On the Use of Machine Learning for Identifying Botnet Network Traffic. Journal of Cyber Security, Vol. 4, pp.1–32. River Publishers. DOI: 10.13052/jcsm2245-1439.421.

Strobel, Stefan (2017): Schlau wie nie. In iX, Magazin für professionelle Informationstechnik, Neue Verfahren in der Schadcode-Erkennung. Ausgabe 7. Online verfügbar unter https://www.heise.de/ix/heft/Schlau-wie-nie-3754380.html, zuletzt geprüft am 22.06.2018.

Thiede, Ulla (2016): Jeder zehnte PC ist ein „Zombie". Israelische Wissenschaftler spüren in Zusammenarbeit mit der Deutschen Telekom infizierte Netze auf. Jeder zehnte PC sei betroffen. Online In General Anzeiger, 5.2.2016. Online verfügbar unter http://www.general-anzeiger-bonn.de/news/wirtschaft/region/Jeder-zehnte-PC-ist-ein-%E2%80%9EZombie%E2%80%9C-article3171482.html, zuletzt geprüft am 22.06.2018.

Cohen, Tomer (2017): Hendler, Danny & Potashnik, Dennis. Supervised Detection of Infected Machines Using Anti-virus Induced Labels. In Proceedings of First int. Conference Cyber Security Cryptography and Machine Learning (CSCML 2017). Dolev, Shlomi & Lodha, Sachin (Hrsg.). Springer International Publishing AG 2017. ISBN 978-3-319-60079-6.

Waidner, Michael; Backes, Michael; Müller-Quade, Jörn; Bodden, Eric; Schneider, Markus; Kreutzer, Michael; Mezini, Mira; Hammer, Christian; Zeller, Andreas; Achenbach, Dirk; Huber, Matthias; Kraschewski, Daniel (2013): Entwicklung sicherer Software durch Security by Design. In SIT Technical Reports, SIT-TR-2013-01. Hrsg: Waidner, Michael; Backes, Michael; Müller-Quade, Jörn. Fraunhofer-Institut für Sichere Informationstechnologie SIT.

Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz http://creativecommons.org/licenses/by/4.0/deed.de) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.