Künstliche Intelligenz und Cybersicherheit
- Eine Diskussionsgrundlage -

Prof. Norbert Pohlmann, Vorstand IT-Sicherheit und Vertrauen
Stand 19.09.2018

Der Bereich Künstliche Intelligenz (KI) hat sich in den vergangenen Jahren kontinuierlich weiterentwickelt und das Technologiefeld gerade in jüngster Zeit enorme Entwicklungen vollzogen. KI-Systeme und -Anwendungen kommen immer häufiger zum Einsatz. Der verstärkte Einsatz solcher Systeme hat die Debatte um den Umgang mit Künstlicher Intelligenz und den Wechselwirkungen für Staat, Wirtschaft und Gesellschaft belebt. Eine der zentralen Herausforderungen sind dabei Fragestellungen nach dem rechtlichen und gesellschaftlichen Ordnungsrahmen für Künstliche Intelligenz.

Die Bundesregierung hat am 18. Juli 2018 Eckpunkte für eine Strategie Künstliche Intelligenz beschlossen. Die Eckpunkte sollen als Grundlage für die Erarbeitung der Strategie dienen und Orientierung für deren Ziele und Handlungsfelder bis zur Verabschiedung der Strategie im Kabinett geben. Im Deutschen Bundestag wurde die Einsetzung Enquetekommission beschlossen, die sich mit dem Thema Künstliche Intelligenz befassen wird.

In diesem Papier des eco – Verband der Internetwirtschaft e.V. soll dargestellt werden, welche Bedeutung die Künstliche Intelligenz (KI) für die Cybersicherheit in Deutschland hat. Es soll als Diskussionsgrundlage für die Einordung, die Anwendungsszenarien und Herausforderungen sowie die Bedeutung vom Künstlicher Intelligenz im Bereich der Cybersicherheit dienen.

Zukunftsfeld Cybersicherheit

Informationstechnik (IT) und das Internet sind Motor und Basis für das Wohlergehen unserer modernen und globalen Informations- und Wissensgesellschaft. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer IT-Systeme, wie Endgeräte, Server, IoT-Geräte und Netzkomponenten zunehmend und sich stetig wandelnden Angriffs- und Bedrohungsszenarien ausgesetzt sind. Auch die Fähigkeiten von Cyberkriminellen und Hackern entwickeln sich kontinuierlich fort und stellen eine Herausforderung für die Cybersicherheit dar. Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker Schwachstellen für erfolgreiche Angriffe zu Nutze machen, Malware installieren, Passwörter sowie Identitäten stehlen, mit Fake News Wahlen beeinflussen, unsere Endgeräte ausspionieren, usw.

Der Schaden im Bereich IT-/Cybersicherheit ist mit 55 Milliarden Euro im Jahr in Deutschland jetzt schon zu groß, wächst aber kontinuierlich weiter. Die Gefahren durch Cyberwar, der Angriff von anderen Staaten und Terroristen

auf unsere Kritischen Infrastrukturen, wird immer wahrscheinlicher. Wir müssen uns auf die hohen Schäden und die neue Wirklichkeit von Cyberwar professionell einstellen und deutlich mehr und wirkungsvollere Cybersicherheitslösungen einsetzen. Cybersicherheit ist seit jeher ein Feld, in dem Innovationen sowohl von Angreifern als auch von Verteidigern genutzt werden. Bislang wurden Cyberangriffe und Cyberabwehr hauptsächlich durch Menschen durchgeführt. Bei zukünftigen Szenarien im Bereich der Cybersicherheit ist von einer intelligenten Kombination von Menschen und KI sowohl auf der Angreifer- als auch auf der Verteidigerseite auszugehen.

Cybersicherheitssysteme, die Künstliche Intelligenz (KI) berücksichtigen, werden in der Zukunft helfen, deutlich besser die intelligenten Hacker und deren Angriffe zu entdecken, Schäden zu vermeiden und Risiken im gewünschten Digitalisierungsprozess zu minimieren. Mit Hilfe von Künstlicher Intelligenz kann die Erkennungsrate von Angriffen im Netzwerk und in ubiquitären IT-Endgeräten (Smartphone, Notebook, Server, IoT, etc.) deutlich erhöht werden. Anders gesagt, können die Erkennungsraten von IT-Systemen, die keine Form der Künstlichen Intelligenz verwenden, nicht dauerhaft auf dem gleichen Sicherheits- und Schutzniveau gehalten werden, wenn auch Angreifer Methoden der KI einsetzen, um IT-Systeme anzugreifen. Somit hat Künstliche Intelligenz vermehrt Auswirkungen auf die Cybersicherheitslage, die durch aktuelle Lagebilder aufzeigbar gemacht werden muss.

Eine große Herausforderung auf Verteidigerseite ist, für welche der sehr vielen erkannten sicherheitsrelevanten Ereignisse zusätzliche noch menschliche Analysten notwendig sind. Nicht alle Ereignisse können durch Spezialisten verarbeitet werden, da die Anzahl der Ereignisse die Verarbeitungsfähigkeit und Verarbeitungskapazitäten menschlicher Analysten an ihre Grenzen bringen. Diesen Umstand können Angreifer ausnutzen und die Verteidiger gezielt ablenken, um unbemerkt in das IT-System einzudringen. Künstliche Intelligenz kann dabei helfen, die Ereignisse in Echtzeit zu analysieren und situationsgerecht zu entscheiden, ob ein menschliches Eingreifen überhaupt noch notwendig ist. In anderen Einsatzszenarien bei denen eine Teilautonomie technisch nicht möglich ist und der Mensch zwingend eingebunden werden muss, kann der Einsatz von KI die Aufgaben und Tätigkeiten des Menschen wesentlich unterstützen. Damit werden die vorhandenen Ressourcen gezielter eingesetzt und das IT-Sicherheitsniveau insgesamt erhöht.

Situationsgerecht bedeutet dabei, dass klassische Verfahren auf Basis von Signaturen nur noch unterstützend eingesetzt werden und neuartige, verhaltensbasierte Verfahren, wie fortgeschrittene Anomalie-Erkennung oder Predictive Analysis Einzug halten. Durch den Einsatz von KI können solche Verfahren möglich werden und einen deutlichen Fortschritt für die Cybersicherheit bringen.

Weiterhin profitieren Identitäts- und Zugangsmanagementsysteme von der automatischen Auswertung der Bewegungsdaten von Nutzern, um nur

berechtigten Nutzern den Zugriff zu IT-Systemen und Anwendungen zu geben. Die Sammlung, Verarbeitung und Speicherung von personenbezogenen Daten müssen jedoch im Einklang mit den datenschutzrechtlichen Bestimmungen (z.B. DSGVO) stehen. Hierbei ist zu beachten, dass die Datenschutzkonformität eine Asymmetrie bei Angriffsszenarien zwischen Verteidiger und Angreifer darstellen kann. Neuartige, passive Identifikations- und Authentifizierungsverfahren können einen Beitrag leisten und zu einer erhöhten Resilienz und Robustheit von IT-Systemen führen. Durch die fehlende Nutzerinteraktion bei dieser Form der Identifizierung und Authentifizierung, beispielsweise durch die Auswertung von Sensordaten im Smartphone, können IT-Systeme sehr einfach sicherer gemacht werden. Aber auch im Bereich der risikobasierten und adaptiven Authentifizierung wird die KI helfen, angemessene IT-Sicherheit situationsbedingt umzusetzen und so die Schäden deutlich zu minimieren.

Einordnung der Künstlichen Intelligenz

Die Wissenschaft „Data Science“ beschäftigt sich mit der Extraktion von Wissen aus den Informationen in Daten. Da es immer mehr Daten mit Informationen gibt, kann auch immer mehr Wissen aus den Informationen der Daten abgeleitet werden, insbesondere auch im Bereich der Cybersicherheit.

Dabei setzt „Künstliche Intelligenz“ intelligentes Verhalten in Algorithmen um, mit der Zielsetzung automatisiert eine „menschenähnliche Intelligenz“ so gut wie möglich nachzubilden.
Maschinelles Lernen (Machine Learning/ML) ist ein Begriff für die „künstliche“ Generierung von Wissen aus den Informationen in Daten mit der Hilfe von IT-Systemen. In Lernphasen lernen entsprechende ML-Algorithmen aus vielen, diversen Beispielen simple Muster, Strukturen, komplexe Merkmale und Gesetzmäßigkeiten zu erkennen. Daraus entstehende Regeln können auf neue Daten und ähnliche Situationen angewendet werden, in denen die KI beispielsweise entscheiden muss, ob es sich um einen Angriff oder eine legitime Nutzeraktion handelt.

KI im Bereich der Cybersicherheit

Enorme Fortschritte der Leistungsfähigkeit von IT-Systemen machen die (zentrale) Speicherung und Verarbeitung von immer größeren Massen von Daten möglich. Dadurch werden immer umfangreichere Prozesse des maschinellen Lernens in akzeptabler Zeit durchführbar. Die Möglichkeit, die Daten schnell zu transportieren und viele IT-Systeme parallel zu verwenden, steigern diese Leistung enorm durch bspw. viele Prozessoren und moderne Grafikkarten oder auch ganze Cluster von IT-Systemen in der Cloud.

Neben der Entwicklung der technischen Leistungsfähigkeit sind die mit der fortschreitenden Digitalisierung stetig zunehmenden Daten ein relevanter Faktor für den Erfolg von KI. Sowohl die Quantität als auch die Qualität der

Daten steigt durch die verbreitete Nutzung von Sensoren in allen Bereichen. Von der Datenerfassung der genutzten IT-Dienste, die verwendeten IT-Geräte (Smartphone, Notebook, PC, Server, Automobilen, etc.) und deren Kommunikation untereinander, fallen immer mehr sicherheitsrelevante Informationen in Daten an.

Hinzu kommt die Verfügbarkeit effizienterer Algorithmen, die optimiertes Maschine-Learning ermöglichen. Der Gesamtablauf wird optimiert, wie zum Beispiel eine Reduktion der Komplexität durch intelligent gewählte Input-Daten. Es findet ein iterativer Lernprozess der Algorithmen statt. Algorithmen des maschinellen Lernens werden durch diese stetigen Verbesserungen praktisch umsetzbar gemacht und auch für komplexere Daten effizient.

In der weiteren Entwicklung wird Maschinelles Lernen durch Deep Learning noch effektiver. Deep Learning ist eine Spezialisierung des maschinellen Lernens und nutzt vorwiegend komplexere neuronale Netze. Dabei werden zusammenhängende Schichten aus künstlichen Neuronen zur Datenverarbeitung genutzt. Das Potenzial von Deep Learning besteht darin, dass im Vergleich zu traditioneller KI nicht nur effektiver analysiert werden kann, sondern durch den effektiveren Lernprozess der KI auch mit unvollständigen Daten eine Analyse erfolgreich umgesetzt werden kann. So kann durch den ständigen Lernprozess des Deep Learnings eine KI in bis dahin unbekannten Situationen angewandt werden. Ein Nachteil des Deep Learnings ist die fehlende Transparenz des Lernprozesses. Oft sind es sogenannte Black-Box Modelle, in die Daten hineinlaufen, wodurch Entscheidungen/Klassifizierzungen am Ende nicht nachvollziehbar werden. Im Sinne der Transparenz und des Verständnisses müssen White- und Grey-Box Modelle erforscht werden, um in die Entscheidungsprozesse blicken zu können. Um diese Modelle besser zu verstehen, sollten entsprechende Forschungsvorhaben unterstützt werden.

Anwendungsszenarien von KI und Cybersicherheit

Im Folgenden werden einige ausgewählte Anwendungsszenarien von KI und Cybersicherheit aufgezeigt, um die Anwendungsvielfalt zu demonstrieren.

- ***Betrugsschutz im Online-Banking***

Im Bereich des Online-Bankings kann zum Beispiel mit Hilfe von KI ermittelt werden, ob eine erhöhte Bedrohungslage herrscht. Dazu werden verschiedene Datenquellen herangezogen und beispielsweise ermittelt, wie viele Banking-Trojaner aktuell aktiv sind, ob es aktuell bekannte Software-Schwachstellen im Umfeld von Online-Banking gibt, die für einen Angriff auf Bankkunden verwendet werden könnten oder ob derzeit vermehrt versucht wird, mit Phishing-Mails Zugangsdaten zu Online-Konten abzugreifen. Diese und andere Indikatoren, wie identifizierte Betrugs- oder Betrugsversuchsfälle der Bank, können dann verwendet werden, um mit verschiedensten Algorithmen aus dem Bereich des Maschinellen Lernens ein

Bedrohungslagebild zu erstellen und den Bankkunden bei hoher Bedrohung zu warnen und entsprechend aufzuklären, um die Schäden zu verhindern.

- ***Erkennen von Angriffen über das Internet und Kommunikationslagebild***

Durch die Analyse der Kommunikationsdaten können mit Hilfe von KI, Angriffe über das Internet erkannt werden. Dadurch können die Kommunikationsmöglichkeiten entsprechend reduziert werden, um den Angriff abzuwehren. Die Reduzierung kann sich zum Beispiel auf einen bestimmten Port oder die ganze Internet-Kommunikation beziehen. Ob ein IT-Sicherheitsexperte bei der Entscheidung eingebunden wird oder das Cybersicherheitssystem dies automatisiert durchführt, ist ein wichtiger Aspekt für die Effektivität und Kosten des Systems. Die Ergebnisse können dann in ein Security Information and Event Management (SIEM)-System einfließen und zum besseren Management von Vorfällen führen. Zusätzlich kann auch ein Kommunikationslagebild erstellt werden, um Angriffe, Bedrohungen und Schwachstellen eines Netzwerks auszuwerten und Handlungsempfehlungen zu geben.

- ***Malware-Erkennung***

Die konventionelle Malware-Erkennung basiert zumeist auf signaturorientierten Detektoren, die bei einer Überprüfung die Signaturen von Dateien und Programmen mit bekannten Signaturen von Malware vergleicht. Wird Malware jedoch nur minimal verändert, kann die Signatur nicht mehr zur Erkennung genutzt werden. Heutige Malware verändert sich daher dynamisch. Dies hat zur Folge, dass immer neuere Varianten erscheinen und die Analyse und Aktualisierungen der Signatur-Datenbanken kaum noch effizient zu bewältigen ist. KI-basierte Detektoren können genutzt werden, um in Echtzeit verdächtige Aktivitäten zu erkennen. Anomalie-Erkennung oder Predictive Malware Analysis sind Verfahren, die durch den Einsatz von KI deutlich verbessert werden können.

- ***Threat Intelligence***

Threat Intelligence ist aktuell meist auch signaturbasiert, mit denselben Nachteilen wie bei der signaturbasierten Malware-Erkennung. Threat Intelligence hat mit der starken Heterogenität von Unternehmensnetzwerken bei der Auswertung und Erkennung von Bedrohungen zu kämpfen. Hier könnten Deep Learning Ansätze, die auch mit heterogenen Datensätzen arbeiten können, u.a. bei der Analyse von Verhaltensmustern und Verhaltensprofilen den gewünschten Erfolg bringen und normale Prozesse von bösartigen unterscheiden (bspw. Lateral Movement oder Exfiltration von Daten).

- ***Authentifikationsverfahren***

Passive, kontinuierliche Authentifizierung ist besonders bei der zunehmenden Verbreitung mobiler Endgeräte ein Zukunftsfeld für KI-Algorithmen. Sensordaten aus Beschleunigungsmessgeräten oder Gyroskopen können während der Nutzung des Gerätes erhoben und ausgewertet werden. Die KI kann folglich unberechtigte Nutzer von der Gerätenutzung ausschließen.

Solche Authentifizierungsverfahren sind ein weiterer Schritt zur Usability von robusten und sicheren Cybersicherheitsmechanismen. Solche Authentifizierungsverfahren sind außerdem inklusiv, da sie keine Nutzerinteraktion erfordern und auch von Nutzern mit (bspw. kognitive) Einschränkungen genutzt werden können. Neben der Analyse von Sensordaten ist auch eine verbesserte Authentifizierung anhand von Bild- oder Spracherkennung möglich, da die Hardware zum Aufnehmen in den Endgeräten vorhanden und die Algorithmen zur Auswertung besser geworden sind.

- ***Identifizierung von Spam-Mails***

Die klassischen Filtermethoden zur Identifizierung und Klassifizierung von Spam-Mails anhand statistischer Modelle, Blacklists oder Datenbank-Lösungen stoßen schon heute an ihre Grenzen. Diese können zum Teil einen hohen Pflegeaufwand erzeugen, da diese regelmäßigen und manuellen Überprüfungen oder Aktualisierungen erfordern. Absender von Spam-Mails sind zunehmend in der Lage, ihre Mails als legitime Mails zu obfuskieren und somit Filter zu überwinden. KI-Lösungen können dazu beitragen, komplexe Muster und Strukturen von Spam-Mails zu identifizieren und zu erlernen, damit Spam-Mails effektiv klassifiziert werden können. Durch jede neue richtig erkannte Spam-Mail lernt die KI weitere Merkmale für die Erkennung. Das Automatisierungspotenzial ist bei einem Einsatz von KI hoch und hilft, IT-Spezialisten zu entlasten.

- ***IT-Forensik***

Im Bereich der IT-Forensik werden KI-Systeme ebenfalls ein relevanter Faktor. Durch die vermehrte Verlagerung von Lebensbereichen in die digitale Welt werden auch zunehmend Straftaten im digitalen Raum begangen, deren Spuren in den gewaltigen Datenmengen der alltäglichen Nutzung gefunden werden müssen. Dabei stoßen klassische Analysewerkzeuge immer schneller an ihre Grenzen, da IT-Systeme prinzipiell heterogener Natur sind. Verschiedenste IT-Geräte mit unterschiedlichen Betriebssystemen, Installationen und Konfigurationen können unzählige Fragmente aufweisen, die im Kontext von Ermittlungen vielfältige Relevanz besitzen. KI-Anwendungen können hier beispielsweise dabei helfen zu entscheiden, ob bestimmte „Adressen“ von einer verdächtigten Person kontaktiert wurden, oder ob es sich um Fragmente handelt, die von Software-Entwicklern standardmäßig in ihr Programm eingebunden wurden – wie es unter anderem bei Support-Adressen häufig der Fall ist.

- ***Advanced Persistent Threats & Cybercrime***

Analog zur Sammlung von Informationen zu Akteuren in klassischen Sicherheitsbereichen, um beispielsweise terroristische Aktivitäten bestimmten Gruppierungen zuordnen zu können, wird auch im digitalen Raum für Verteidiger immer wichtiger, Informationen über verschiedene Akteure zu sammeln und verarbeiten. So konnten in der Vergangenheit wiederholt Schadprogramme und Angriffe auf IT-Systeme, Einzelpersonen oder auch Gruppierungen zugeordnet und laufende Kampagnen identifiziert werden. Diese Informationen sind zum einen unerlässlich, wenn es um die

Strafverfolgung, die Gewinnung weiterer Ermittlungsansätze und letztendlich gerichtsverwertbarer Beweise geht. Zum anderen können sie aber auch in Bedrohungslagebilder eingebettet werden und die Effektivität von Warnmeldungen erhöhen oder auch ganze Strategieentwicklungen im geschäftlichen wie (sicherheits-)politischen Sinne beeinflussen. Die korrekte Identifizierung von Akteuren und den von ihnen ausgehenden Bedrohungen hat demnach eine steigende Bedeutung, unterliegt dabei aber den gleichen Problemen wie in der analogen Welt. Indikatoren können manipuliert, Spuren verschleiert und sogar falsche Spuren gelegt werden. Zugehörigkeiten, Organisationsstrukturen und Geldflüsse werden verschleiert und Handlungsweisen verändern sich mit der Zeit. Des Weiteren steigt die Anzahl der potentiellen Opfer von Cyberkriminalität durch den digitalen Wandel kontinuierlich und erfolgreich angegriffene Systeme versprechen steigende Profite. Hier kann Künstliche Intelligenz unterstützen, indem bisher unerkannte Muster in Datenströmen und -mengen aufgedeckt und Manipulationsversuche enttarnt werden.
Zur Identifizierung von Akteuren auf der Angreifer Seite kann eine Klassifizierung der Akteure vorgenommen werden, um Angriffsziele, Motivation, Risiken bzw. Kritikalität und mögliche Gegenmaßnahmen einzustufen und zu bewerten. Eine Klassifizierung von Akteuren kann dabei anhand von Kategorien und Klassifizierungen erfolgen, beispielsweise interne versus externe Angreifer, Einzeltäter versus organisierte Gruppen, White Hats versus Black Hats, kriminell motivierte Angreifer versus Scriptkiddies, terroristisch motivierte Angreifer sowie staatliche Angreifer.

- ***Weitere Anwendungsszenarien***

Weitere Anwendungsszenarien sind, sichere Softwareentwicklung, erkennen von FakeNews, Bilderkennung von Ausweisen, VideoIdent, Biometrische Verfahren, wie Tippverhalten, Gestik-Erkennung, Seitenkanalanalyse, Kryptoanalyse, usw.

Herausforderung im Bereich der KI und Cybersicherheit

Die Zahl der möglichen Anwendungen von KI im Bereich der Cybersicherheit ist enorm hoch. Allerdings gilt es auch einige Herausforderungen zu überwinden, da diese datengetriebenen Anwendungen sehr schnell in sensible Lebensbereiche eingreifen können. KI-Anwendungen entscheiden in der Regel nicht selbst über eine datenschutzkonforme Nutzung der analysierten Daten. Dadurch können Bürger eventuell in ihrer informationellen Selbstbestimmung eingeschränkt werden. Dies gilt es zu verhindern. Daher müssen bei der Entwicklung von KI-Anwendungen und Algorithmen hohe ethische und datenschutzkonforme Standards berücksichtigt und einbezogen werden. Hierbei müssen auch die einer KI-Anwendung oder einem Algorithmus zu Grunde liegenden Daten und Datensätze einbezogen und berücksichtigt werden ebenso wie die weiteren Schritte einer damit einhergehenden Datenverarbeitung. Weiterhin ist zu berücksichtigen, dass bereits die zu Grunde liegenden Daten und Datensätze per se oder deren Unvollständigkeit sowie schlecht parametrisierte Algorithmen zu einer

wachsenden Diskriminierung führen können. Dadurch werden Drifting-Effekte gefördert. Im Kontext von Drift ergeben sich ebenfalls spannende Herausforderungen für lebenslanges maschinelles Lernen, beispielsweise die vertrauenswürdige Integration von Realwelt-Daten in bestehende Modelle. Die Daten können täglich, wöchentlich, monatlich oder jährlich zum Training des Modells genutzt werden, jedoch ist die Änderung der Klassifikation unter Umständen nicht schnell genug adaptierbar für die einströmenden Echtzeitdaten. Dadurch ist es einem Angreifer über die Zeit möglich, gewisse Entscheidungen unter Umständen zu manipulieren und seinen Angriff durchzuführen. Besonders bei Deep Learning Technologien muss eine erhöhte Transparenz in den Entscheidungsfindungsprozess einfließen, um Ergebnisse vertrauenswürdig zu machen Eine erhöhte Transparenz sorgt dafür, dass der Diskriminierung und dem Drifting entgegengewirkt wird und nicht gezielt ein Entscheidungsprozess attackiert werden kann. Auch müssen Grenzbereiche betrachtet werden, wie reagiert ein System beispielsweise, falls über einen längeren Zeitraum Daten ausfallen oder plötzlich ein deutlicher Anstieg an Inputdaten zu verzeichnen ist. Eine weitere große Herausforderung wird die Entscheidung sein, ob und zu welchem Zeitpunkt des Entscheidungsfindungsprozesses menschliche Expertise erforderlich ist und ein menschlicher Analyst eingeschaltet wird, um auf einen Angriff zu reagieren. Ideal wäre eine automatisierte Reaktion, die Angriffe erfolgreich abwehrt und Schäden verhindert.

Stellenwert und Bedeutung von KI und Cybersicherheit

KI hat im Zusammenspiel mit Cybersicherheit eine wichtige Bedeutung für den Wirtschaftsstandort Deutschland. Die Anwendung und Integration von Methoden der KI im Bereich der Cybersicherheit gewinnt zunehmend an Bedeutung, um Angriffe frühzeitig zu erkennen, zu analysieren, abzuwehren sowie Risiken zu minimieren. Durch die neuen Angriffs- und Bedrohungsszenarien muss Deutschland eigene Kernkompetenz im Bereich der KI und Cybersicherheit aufbauen. Die Entwicklung neuer auf KI basierender Abwehr- und Verteidigungsmechanismen ist auch ein Standort- und Wettbewerbsvorteil für Deutschland. Insbesondere in KMU’s, die ungefähr 95% der Deutschen Unternehmenslandschaft ausmachen, muss die Adaption von resilienten Verteidigungen gegen den Diebstahl von Innovationen und Schutz vor Sabotage vorangetrieben werden. KMUs benötigen einsatzbereite und standardisierte Lösungen, um Office-IT und Production-OT kontinuierlich gegen mögliche Cyberangriffe abzusichern und zu überwachen. Diese Cybersicherheitslösungen werden zunehmend auch KI-Technologie einsetzen und sollten kontinuierlich an den aktuellen Stand der Technik angepasst werden. Auf staatlicher Ebene muss sich Deutschland gegen eine noch schneller ändernde Bedrohungslandschaft durch die KI im Bereich Cybercrime aufstellen. Die hohe Geschwindigkeit und Dynamik, mit der sich die Bedrohungslandschaft stetig ändert, kann von konventionell eingesetzten Technologien nur noch schwer oder mit hohem Aufwand bewältigt werden. Der Einsatz von KI-Cybersicherheitslösungen kann dazu beitragen neue Kapazitäten zu schaffen und vorhandene zu entlasten. Auch

im internationalen Bereich muss sich Deutschland positionieren, um konkurrenzfähig zu bleiben. Daneben ermöglicht der Einsatz von KI auch in anderen Bereichen Entwicklungen durch moderne und sichere Authentifikationsverfahren und kann im Online-Banking zur Prävention gegen Betrug eingesetzt werden. Generell kann KI zur Detektion unterschiedlicher Sachverhalte genutzt werden.

Die Anwendung und Einbeziehung von KI kann die Cybersicherheit in Deutschland insgesamt nachhaltig verbessern. KI-Technologien für Cybersicherheit sind der Lage, auf die sich stetig wandelnde Angriffs- und Bedrohungslage optimal zu erkennen und frühzeitig einzustellen und reagieren zu können. Darüber hinaus ergeben sich für KI insbesondere auch im Bereich der Kritischen Infrastrukturen Einsatz- und Anwendungsfelder, die zur Erkennung, Absicherung und Gewährleistung der Aufrechterhaltung sowie Funktionsfähigkeit kritischer Infrastrukturen einen wesentlichen Beitrag leisten können.

Die Entwicklung robuster Algorithmen nach hohen ethischen und datenschutzkonformen Standards kann für Deutschland einen Wettbewerbsvorteil darstellen. Insbesondere da die technologische Souveränität immer wichtiger wird.

Forschungsschwerpunkt KI und Cybersicherheit

Die Erforschung neuer Angreifer- und Verteidiger-Modelle, die Künstliche Intelligenz berücksichtigen, muss ein zentraler Bestandteil in der zukünftigen Cybersicherheitsstrategie Deutschlands sein. Nur wenn Angriffsmethoden erkannt und methodisiert werden, können wirksame und effiziente Verteidigungsstrategien entwickelt werden. Dabei ist der Einsatz von KI-Technologien nicht nur auf die Verteidigung beschränkt, sondern kann auch von Cyberkriminellen als Mittel eingesetzt werden. Aber auch die Nutzung Künstlicher Intelligenz im Bereich der Identifizierung von Nutzern wird helfen, Schäden und Risiken für Unternehmen und Bürger zu reduzieren. In diesem Bereich sollten auf den Ebenen der richtigen Daten und KI-Algorithmen, der optimalen Verarbeitung sowie Reaktion der Ergebnisse, der Einbindung in die IT-Landschaften und der Zusammenarbeitsformen Forschungsinitiativen gestartet werden.

Ein weiterer Forschungsschwerpunkt sollte die Autonomie von KI-Anwendungen betreffen. Nur wenn es gelingt, selbständig auf Bedrohungs- und Angriffssituationen zu reagieren, kann eine hohe Robustheit langfristig erreicht werden.

Aber auch weitere Cybersicherheitsthemen sollten mit der KI-Unterstützung erforscht werden.

Die zügige Weiterentwicklung von „schwachen“ zu „starken“ KI-Lösungen in Deutschland ist dringend geboten, um hier nicht den Anschluss an dem technischen Fortschritt zu verlieren.

Cybersicherheit für KI

Künstliche Intelligenz wird in den nächsten Jahren in sehr vielen weiteren IT-Feldern zur Anwendung kommen. Daher besteht ein sehr großer Handlungsbedarf passende Cybersicherheits-, Datenschutz- und Vertrauenswürdigkeitsmaßnahmen für KI-Systeme umzusetzen.

Herausforderungen im Bereich Cybersicherheit für KI sind:

- Wie kann verhindert werden, dass die Inputdaten manipuliert werden?
- Wie können Manipulationen der KI-Algorithmen entdeckt werden?
- Wie kann erkannt werden, dass die Verwendung der Ergebnisse nicht richtig ist?
- Wie kann die Berücksichtigung der datenschutzrechtlichen Anforderungen und die Datenschutzkonformität gewährleistet und überprüft werden?
- Wie kann das Vertrauen in KI-Systeme ausgebaut werden?

Konkret liegen die notwendigen Maßnahmen der Anbieter von KI-Systemen in den Bereichen Transparenz und Überprüfbarkeit. Nur wenn Transparenz und Vertrauenswürdigkeit erlangt werden können, können die Potenziale von Künstlicher Intelligenz für das Leben der Menschen, für die Entwicklung des Wohlstandes und die Gesellschaft als Ganzes gefördert und die Risiken von KI-Systemen begrenzt werden.

Erstellung eines gemeinsamen nationalen und globalen Lagebildes

Vor dem Hintergrund der zu erwartenden Entwicklung im Bereich der Bedrohungs- und Angriffsszenarien wird es für die Cybersicherheit zukünftig immer wichtig sein, frühzeitig ein genaues Lagebild über die aktuelle Bedrohungs- und Angriffslage zu haben.

Staatliche und private Stellen, Organisationen und Unternehmen müssen Informationen über ihre sicherheitsrelevanten Ereignisse teilen und aggregiert zentral zur Verfügung stellen. Dadurch werden sicherheitsrelevanten Ereignisse vergleichbar und ein genaueres Lagebild entsteht. Die Entwicklung von sicherheitsrelevanten Vorfällen kann besser nachvollzogen werden. Werden diese Aggregate von vielen Unternehmen und staatlichen Stellen intelligent ausgetauscht, kann ein aussagekräftiges und umfangreiches Lagebild über den jeweiligen aktuellen und vergangenen IT-Zustand generiert werden. Somit können neben branchenorientierten Vergleichsbildern auch globale, kontinentale oder nationale Sichtweisen über Staaten oder Staatenverbünde erstellt werden. Mit diesem Wissen ist es Wirtschaft, Unternehmen und staatlichen Stellen möglich, ihre aktuelle Gefährdungslage

anhand von IT-Sicherheitslagebildern besser einzuschätzen und präventive IT-Sicherheitsmaßnahmen zur deutlichen Erhöhung des Schutzniveaus einzuleiten.

Für Politik und Behörden, Wirtschaft und Unternehmen bietet sich darüber hinaus damit erstmals die Möglichkeit, anhand eines globalen Lagebildes den Zustand der Cybersicherheit in Deutschland einzuschätzen und daraus geeignete und wirkungsvolle IT-Sicherheitsmaßnahmen abzuleiten und zu ergreifen.

Erkennung von netzwerkbasierten Angriffen mittels Künstlicher Intelligenz

Das Institut für Internet-Sicherheit - if(is) hat das Ziel, die Vertrauenswürdigkeit und Sicherheit im Internet zu erhöhen. Um dieses Ziel zu erreichen, hat das Institut für Internet-Sicherheit über viele Jahre das Thema Internet-Frühwarnsysteme als großen Forschungsschwerpunkt betrieben.

Dazu hat das if(is) ein Internet-Analyse-System entwickelt, das die Aufgabe hat, zum einen die Analyse von lokalen Kommunikationsdaten in definierten Teilnetzen des Internet und zum anderen die Erstellung einer globalen Sichtweise auf das Internet durch die Zusammenführung der vielen lokalen Sichten zu erreichen. Die Funktionen des Internet-Analyse-Systems lassen sich in die vier Teilbereiche Aufbau einer Wissensbasis (Musterbildung, Profile, etc.), Beschreibung des Ist-Zustandes, Alarmierung bei erkannten Angriffen und Prognostizierung der Bedrohungslage unterteilen. Im Bereich der Alarmierung bei erkannten Angriffen wurde insbesondere Forschung zu Maschinellem Lernen und KI - Künstlich Neuronale Netz - durchgeführt.[1]

Diese langjährige Forschung ist durch das Bundesamt für Sicherheit in der Informationssicherheit (BSI) und durch das Bundesministerium für Bildung und Forschung über mehrere Forschungsprojekte finanziert worden.

Um das Internet-Analyse-System einem schnellen Technologietransfer zu unterziehen und die Technologie weiter zu entwickeln, wurde als Spin-off des Instituts für Internet-Sicherheit ein Startup gegründet, in dem 7 wissenschaftliche Mitarbeiter aus dem Forschungsbereich Internet-Frühwarnsysteme aktiv sind.

Als praktisches Anwendungsbeispiel aus der universitären Forschung für den Einsatz von KI-Technologien im Bereich der Cybersicherheit wurde dort ein System zur Erkennung von netzwerkbasierten Angriffen in Unternehmensnetzwerken weiterentwickelt. Dieses ermöglicht auch die

[1] nationale und internationale Publikationen unter https://norbert-pohlmann.com/artikel/

Erstellung eines Kommunikationslagebildes für ein einzelnes oder mehrere Unternehmen sowie globaler Lagebilder.

Ausgangslage und Problemstellung

In den vergangenen Jahren wurde in erster Linie mit signaturbasierten Systemen versucht, unerwünschten und bösartigen Netzwerkverkehr zu erkennen. Dies hat in der Vergangenheit für bekannte Angriffe dann funktioniert, wenn die dafür benötigten Signaturen, die mit erheblichem Aufwand kontinuierlich gepflegt werden müssen, verfügbar waren.

Um auch unbekannte Angriffe ohne Signaturen zu detektieren wurden in den letzten Jahren vor allem mittels Machine Learning (ML) große Erfolge erzielt. Hierbei werden typischerweise anhand des bekannten Netzwerkverkehrs Modelle (das Gedächtnis) trainiert, die den gewünschten Normalzustand des Netzwerks beinhalten und den Live-Verkehr damit abgleichen. Die Qualität der Ergebnisse von Machine Learning hängt vor allem von zwei Hauptfaktoren ab: den zur Verfügung stehenden Daten und den eingesetzten Algorithmen.

Für alle modernen Machine Learning Algorithmen werden in der Regel sehr viele Trainingsdaten benötigt. Diese müssen einen sehr hohen Detailgrad von sicherheitsrelevanten Informationen aufweisen und sich gleichzeitig für eine Bearbeitung eignen. Den kompletten Netzwerkverkehr als „Big Data“ permanent speichern und diesen mittels ML trainieren zu wollen, ist technisch nicht machbar. Daher ist eine wichtige Strategie bei der Analyse von Netzwerkverkehr, alle wichtigen und sicherheitsrelevanten Informationen aus dem Netzwerkverkehr zu extrahieren und reduziert abzuspeichern, damit sie für das trainieren von Algorithmen verwendet werden können.

Im Netzwerkbereich ist Netflow/IPFIX ein gängiges Format, das für eine Netzwerkverbindung (Flow) einige Merkmale (IP-Adressen, Ports, übertragene Bytes, etc.) extrahiert. Durch diesen Ansatz kann eine grobe Netzwerkverkehrsvisualisierung dargestellt sowie einfache Angriffserkennungen realisiert werden. Für komplexe Detektionen werden allerdings noch mehr Details über die Netzwerkverbindung sowie deren Inhaltsdaten benötigt.

Technologischer Lösungsansatz

Dieser Herausforderung kann mit einem innovativen Flow-Format für Netzwerksensoren ungesetzt werden, das den Datenverkehr viel detaillierter auf sicherheitsrelevanten Informationen analysiert und für die jeweiligen Flows bis zu vier Millionen Merkmale aus unterschiedlichen Netzwerkprotokollen unterscheiden und speichern kann (Smart Data). Diese beinhalten unter anderen Informationen über verwendete Browser und Betriebssysteme, Daten zur verwendeten Verschlüsselung, Inhaltsdaten von Web-Verkehr, aufgelöste Domains, usw. Durch die Extraktion der Merkmale werden die ursprünglich

enthaltenen wichtigsten sicherheitsrelevanten Informationen beibehalten und es darüber hinaus ermöglicht, diese sehr leicht mittels ML-Verfahren und Deep Learning zu trainieren (was auf Basis von reinem und rohen Netzwerkverkehr so nicht funktioniert). Dabei wird darauf geachtet, dass auch versteckte, aber gleichwohl sicherheitsrelevante Informationen weiterhin enthalten sind. Durch jahrelange Erfahrung auf dem Gebiet und den Eigenentwicklungen können sehr schnell anhand gesammelter neuer Erkenntnisse das Flow-Format und die Sensoren angepasst und optimiert werden, kontinuierlich noch bessere Ergebnisse zu erzielen.

Der komplette Netzwerkverkehr wird somit sehr detailliert auf die wichtigsten Merkmale reduziert sowie um sicherheitsrelevante Informationen angereichert, um diese Daten zum einen als Smart Data sehr lange vorhalten und zum anderen für die Machine Learning Algorithmen die Basis bieten zu können. Die anfallenden Daten können direkt in den Unternehmen unter Berücksichtigung der jeweiligen datenschutzrechtlichen Anforderungen analysiert werden, allerdings auch datenschutzkonform an eine zentralisierte Stelle übermittelt werden, um aus sehr vielen verschiedenen Unternehmen und Bereichen Daten für die Algorithmen zu erhalten, um diese damit stetig zu verbessern und kontinuierlich zu optimieren. Diese Smart Data Ansammlungen sind zudem der Kern, um aus unstrukturierten Daten verwendbare Informationen zu generieren (Data Science). Das entwickelte Flow-Format ist damit ideal für moderne und innovative Erkennungen sowie Vorhersagen und Prognosen geeignet.

Machine Learning auf Basis Künstlicher Intelligenz

Bei der Entwicklung des innovativen Flow-Formats wurden die Expertise und die Erfahrungen im Umgang mit Algorithmen von Machine Learning und Data Science auf extrahiertem Smart Data Netzwerkdaten der letzten 13 Jahre genutzt. Hierbei kommen sehr viele Algorithmen für unterschiedliche Problemlösungen zum Einsatz. Diese umfassen unter anderem sowohl Supervised Learning wie Naive Bayes und Nearest Neighbor sowie Seasonal Average, Verhaltensanalysen und Decision Trees als auch Unsupervised Learning wie Apriori und Hidden Markov Modell.

Schon vor über zehn Jahren wurden in diesem Kontext auch Neuronale Netze (NN) aus probabilistischen Ansätzen heraus verwendet. Diese waren damals allerdings aufgrund mehrerer Faktoren (Hardwareunterstützung, eingeschränkte Varianten von Neuronalen Netzen) nicht so geeignet. Dies hat sich in den jüngsten Jahren radikal geändert, sodass Neuronale Netze mittels Deep Learning nun mit den Smart Data Ansammlungen mittels des entwickelten Flow-Formats angewendet werden können. Dabei kann sowohl der Normalverkehr im Unternehmen als auch der von bekanntem Schadverkehr trainiert werden, um diesen noch zielgerichteter im Live-Betrieb detektieren zu können.

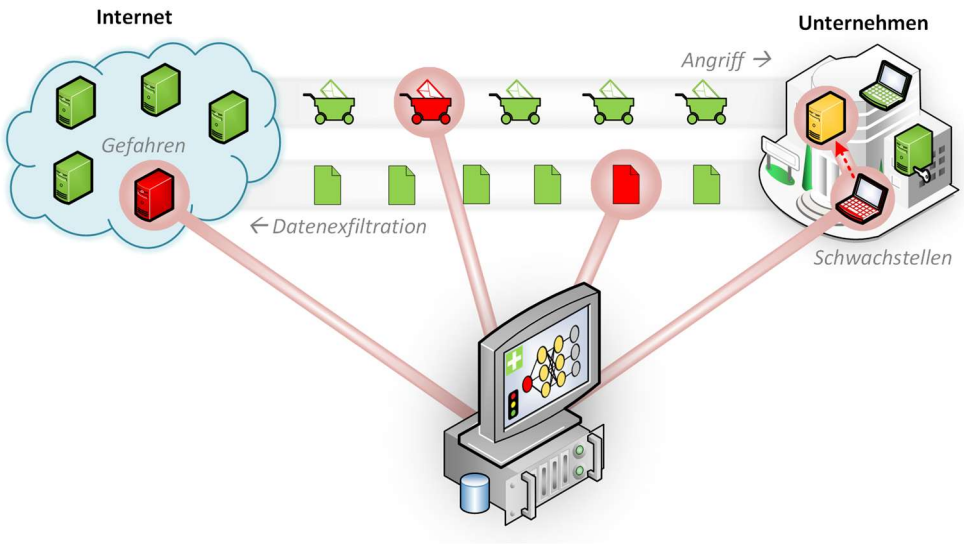

Abbildung 1: Innovative Erkennung von schadhaftem Netzwerkverkehr

Innovative Erkennungen

In vielen anderen Bereichen konnten durch den Einsatz von KI-Technologien bereits deutliche Verbesserungen erreicht werden. Daher bietet der Einsatz von KI auch im Kontext der Netzwerkerkennung sehr viele Chancen und Potential. Die Flow-Daten eignen sich ideal, um innovative Erkennungen mittels KI und Verhaltensanalysen von Systemen durchzuführen. Es werden Verbindungen identifiziert, für die im Vorfeld sowohl „gutartige“ (normale Anwendungen wie E-Mail-Versand, TeamViewer, Cloud-Nutzung oder unternehmenseigene Protokolle) als auch „bösartige“ Netzwerkverbindungen (schadhafter Verkehr wie Trojaner, Ransomware, etc.) trainiert wurden. Auf der Basis sowie aus detaillierten Flow-Merkmalen wird ein Verhaltensmodell über die Kommunikationsbeziehungen für die jeweiligen Systeme erstellt, die im Live-Betrieb kontinuierlich abgeglichen wird. Darüber hinaus werden die Systeme automatisch zu einer Gruppe klassifiziert, und Klassenänderungen beispielsweise durch eine Malware-Infektion gemeldet. So lassen sich neben klassischen Angriffen wie Distributed Denial of Service (DDoS), Brute-Force, etc. auch moderne Schadsoftware mit Nutzung von Zero-Day-Exploits, Trojaner, Remote Administration Tools (RAT), Ransomware, etc. sowie versteckte Kanäle für Command & Control (C&C), Lateral Movement und Exfiltration erkennen, die mit bisher gebräuchlichen Datenformaten nicht detektiert werden konnten. Weitere Beispiele sind ein infizierter Client-PC, der plötzlich nachts ungewöhnlich viel kommuniziert, eine unbekannte Malware-Kommunikation, die ähnlich bekannter/erlernter schadhafter Netzwerkverbindung ist oder eine Malware, die mittels Steganographie in Bildern periodisch auf sog. Image-Server zugreift. So konnten mit den neuen Ansätzen laterale Ausbreitungen in Unternehmen, Schadsoftware auf Steuerungssystemen (Industrial Control System – ICS) im Produktionsumfeld

(Operational Technology – OT) sowie versteckte Kanäle, wie sie bei der Malware UDPoS und bekannten Advanced Persistent Threat-Gruppen (APT) zum Einsatz kamen, erkannt werden.

Das entwickelte innovative Flow-Format kann mit seinem universellen Ansatz alle netzwerkbasierten Bereiche eines Unternehmens wie Office, IT, ICS/OT und dem (Industrial) Internet of Things ((I)IoT) abdecken und deren spezifische Protokolle analysieren. In Verbindung mit dem verwendeten Machine Learning auf Smart Data und angepassten Modellen kommt der technologische Lösungsansatz so auch in der klassischen IT, als auch im ICS-Bereich sowie IoT-Diensten zum Einsatz. Beispiele sind hier ein bisher passiver ICS-Monitor, der plötzlich einigen ICS-Geräten fragwürdige Befehle gibt oder ein IoT-Gerät (wie Kühlschrank oder Webcam), das plötzlich mit einer Bürofernwartung gesteuert wird. Darüber hinaus kann kontinuierlich ein Lagebild über die IT-Sicherheit eines Unternehmens generiert und eine vollständige Netzwerktransparenz geschaffen werden.

Erkennen von Angriffen über das Internet

Durch die Analyse der Kommunikationsdaten in einem Unternehmensnetzwerk können mit Hilfe von KI Angriffe über das Internet auf das Netzwerk erkannt werden. Dadurch können die Kommunikationsmöglichkeiten des Netzwerkes sowohl intern als auch extern sowie zwischen Intranet, Extranet als auch Internet entsprechend kontrolliert und eingeschränkt werden, um den Angriff abzuwehren. Die Reduzierung kann sich zum Beispiel auf einen bestimmten Port oder die ganze Internet-Kommunikation beziehen. Ob in diesen Prozess auch ein IT-Sicherheitsexperte bei der Entscheidung eingebunden wird oder das Cybersicherheitssystem dies automatisiert durchführt, ist ein wichtiger Aspekt für die Effektivität und Kosten des Systems. Die Ergebnisse der Netzwerkanalyse können dann in ein Security Information and Event Management (SIEM)-System einfließen und zum besseren Management von Vorfällen beitragen. Darüber hinaus kann auch ein Kommunikationslagebild des Firmennetzwerkes bzw. Unternehmens erstellt werden, um Angriffe, Bedrohungen und Schwachstellen eines Netzwerks auszuwerten und konkrete Handlungsempfehlungen daraus abzuleiten.

Gemeinsamer Austausch und Erstellung eines globalen Lagebildes

Ein wichtiger Aspekt für die Unternehmen ist, dass sie in Zukunft mehr Informationen über die allgemeine Angriffs- und Bedrohungslage in Netzwerken als Grundlage zur Einschätzung der Sicherheitslage haben, als die aktuellen Monitoring-Systeme in den eigenen Netzen zur Verfügung stellen. Derzeit beziehen Unternehmen relevante Sicherheitsinformationen üblicherweise über extern verfügbare Sharing-Plattformen und Feeds anderer Institutionen sowie aktuelle Threat Intelligence (TI) Informationen die Wissen über die Vorgehensweisen von Angreifern, deren verwendeten Tools sowie

Kontextinformationen beinhalten (operativ, taktisch und strategisch). Auf der operativen Ebene kommen vor allem bekannte Indicator of Compromise (IoC) wie IP-Adressen, Domains und URLs von bösartigen Systemen, Hashes von Malware-Samples, etc. zum Einsatz. Dieser Austausch ist wichtig, um die bekannte Infrastruktur von Angreifern im eigenen Netzwerk leichter erkennen und aufspüren zu können.

Darüber hinaus werden allerdings noch Einblicke in die allgemeine Angriffs- und Bedrohungslage zur Vergleichbarkeit mit anderen Unternehmen benötigt, damit die noch nicht bekannten TI Informationen zugeordnet werden können. Die Flow-Daten bilden die Grundlage, um eine detaillierte und übergreifende Sichtbarkeit zu gewährleisten. Diese können unter Einbehaltung vieler qualifizierter Merkmale aggregiert und datenschutzkonform mit anderen Unternehmen ausgetauscht werden, um eine Vergleichbarkeit herzustellen.

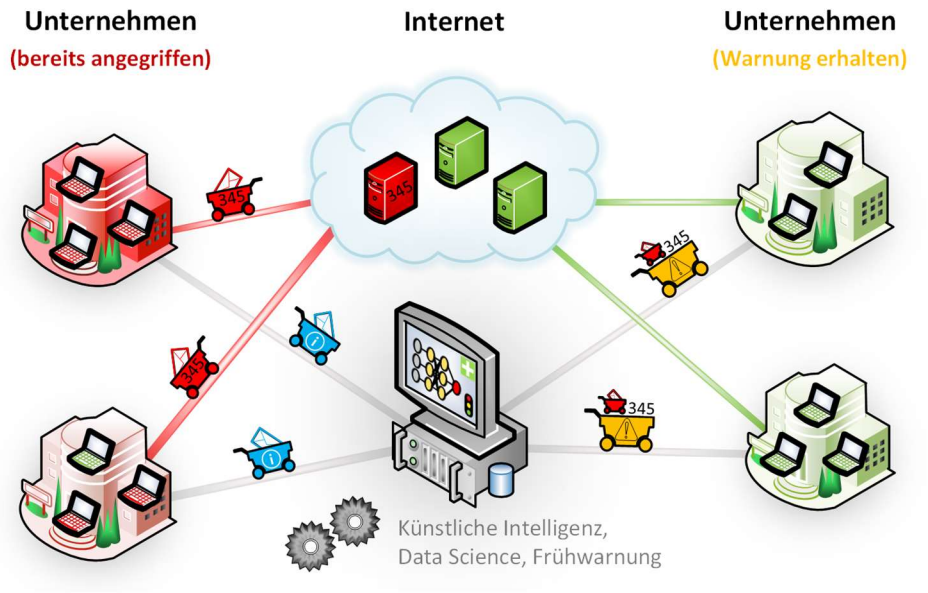

Abbildung 2: Kooperative Erkennung von Bedrohungen und Angriffen

Werden diese Merkmalsaggregate von vielen unterschiedlichen Unternehmen intelligent ausgetauscht, kann ein aussagekräftiges und umfangreiches Lagebild über den jeweiligen aktuellen und vergangenen Netzwerkzustand generiert werden. Somit können neben branchenorientierten Vergleichsbildern auch globale Sichtweisen über die Bundesrepublik, einzelne Bundesländer und eines oder mehrerer Staaten erstellt werden. Mit diesem Wissen ist es Unternehmen möglich, ihre aktuelle Gefährdungslage besser einzuschätzen und präventive Maßnahmen zur deutlichen Erhöhung des Schutzes einzuleiten. Werden von den Sensoren und den intelligent ausgetauschten Daten Angriffe auf mehrere unterschiedliche Unternehmen festgestellt, können andere Unternehmen bereits frühzeitig vorab vor einer

konkreten Gefahr gewarnt werden und sich dementsprechend mit diesem Frühindikator gezielt davor schützen.

Für Politik, Ministerien und Behörden könnte sich dadurch erstmals die Möglichkeit ergeben, anhand eines globalen Lagebildes den Zustand der Netzwerksicherheit in Deutschland einzuschätzen, geeignete Maßnahmen einzuleiten und auch deren Erfolg zu messen.

Public-private-Partnership im Bereich des Austausches von sicherheitsrelevanten Informationen

Mit der weiteren Digitalisierung zentraler Bereiche der Industrie und Wirtschaft erlangt die IT- und Cybersicherheit zunehmend eine zentrale Bedeutung und für den Innovations- und Wirtschaftsstandort Deutschland wird sie unverzichtbar.

In Deutschland besteht ein hoher Schutzbedarf, um das Risiko von Schäden für Wirtschaft und Gesellschaft abzuwenden und zu minimieren. Vor diesem Hintergrund muss IT-Sicherheit einen zentralen Stellenwert einnehmen. Dies erfordert nicht nur ein entsprechendes Bewusstsein in Wirtschaft und Gesellschaft für die Anwendung und Nutzung von IT-Sicherheitstechnologien, sondern insbesondere wird es zukünftig immer wichtiger sein, frühzeitig sicherheitsrelevante Informationen über Ereignisse und die aktuelle Angriffs- und Bedrohungslage zu haben.

Der Anwendung und Integration von Künstlicher Intelligenz kommt hierbei eine wichtige Bedeutung zu auf die neuen Angriffs- und Bedrohungsszenarien zu reagieren. Denn die Methoden der KI im Bereich der Cybersicherheit ermöglicht es Angriffe frühzeitig zu erkennen, zu analysieren, abzuwehren sowie Risiken zu minimieren. Die Anwendung von KI ist besonders erfolgsversprechend, wenn dazu viele Daten und unterschiedliche Datenquellen mit den richtigen Informationen genutzt werden können. Aus diesem Grund ist es bei der Künstlichen Intelligenz und Cybersicherheit sinnvoll, wenn staatliche und private Stellen, Organisationen und Unternehmen sicherheitsrelevante Informationen kontinuierlich austauschen. Mit diesen Informationen wäre es Wirtschaft, Unternehmen und staatlichen Stellen möglich, ihre aktuelle Gefährdungslage besser einzuschätzen und IT-Sicherheitsmaßnahmen zur Prävention oder Abwehr einzuleiten. Dies würde zu einer deutlichen Erhöhung des Schutzniveaus beitragen.

Als ein pragmatischer Ansatz hierfür könnte eine öffentlich-private Partnerschaft sinnvoll sein. Daran teilnehmen sollten die Industrie und Wirtschaft mit den großen Unternehmen, die IHKs und die Handwerkskammern, als Multiplikatoren für die kleineren KMUs, der Staat auf allen Ebenen und die Wissenschaft und Forschung, um die kontinuierliche Optimierung der Ergebnisse zu gewährleisten. Daher sollte angestrebt werden, eine Public-private-Partnership im Bereich des Austausches von sicherheitsrelevanten Informationen zu etablieren.