LINK11

KI und Cyber-Resilienz

Ein Wettlauf zwischen Angreifern und Verteidigern

www.link11.com

KI und Cyber-Resilienz: Ein Wettlauf zwischen Angreifern und Verteidigern

Eine Technologie elektrisiert Wirtschaft, Gesellschaft und Politik gleichermaßen: die Entwicklung von „Künstlicher Intelligenz" (KI). In philosophischen Diskussionen wird aktuell noch um Antworten auf die Frage gerungen, ob der Nutzen von KI für den Menschen überwiegt, oder ob sie nicht auch Gefahren heraufbeschwört. Davon unbeeindruckt halten die verschiedenen KI-Konzepte, wie maschinelles Lernen, Mustererkennung oder Vorhersagen immer stärker Einzug in den Alltag.

Versicherungen setzen KI-Systeme inzwischen zur Betrugserkennung und Fallbearbeitung ein. Banken und Kreditkartengesellschaften nutzen solche Systeme ebenfalls zur Erkennung von betrügerischen Verhalten oder Anomalien in der Nutzung zur Risikoprävention. KI hilft Händlern bei der Warendisposition oder der Analyse von Kundenströmen und Verkaufszahlen. Und in der Medizin unterstützt KI in der bildgebenden Diagnostik oder der Analyse von großen Datenmengen, wie sie etwa während der Bekämpfung der Pandemie mit Covid-19 entstehen.

Unternehmen sollten sich mit KI nicht nur deshalb auseinandersetzen, weil es ihre Wettbewerber tun und hier mit großer Dynamik eine technologische Umwälzung durchstartet. Eine aktive Beschäftigung und Nutzung von KI ist inzwischen besonders in der der Cyber-Resilienz und der dazugehörigen IT-Sicherheit geboten. KI gilt als Schlüsseltechnologie, wenn es darum geht, die Sicherheit vor Cyber-Attacken und die Widerstandskraft der IT-Infrastruktur eines Unternehmens zu organisieren. Aber auch Kriminelle haben die Vorzüge von KI für sich entdeckt.

Künstliche Intelligenz: Künstliche Intelligenz (KI) beziehungsweise Artificial Intelligence (AI) simuliert menschliche Intelligenz mit Maschinen, insbesondere Computersystemen. Dies umfasst das Lernen (die Erfassung von Informationen und Regeln für die Verwendung der Informationen), die Schlussfolgerung (die Verwendung der Regeln, um ungefähre oder endgültige Schlussfolgerungen zu ziehen) und die Selbstkorrektur. Besondere Anwendungen der KI sind Expertensysteme, Spracherkennung und Machine Vision.

Maschinelles Lernen: Machine Learning, im Deutschen maschinelles Lernen, ist ein Teilgebiet der künstlichen Intelligenz. Durch das Erkennen von Mustern in vorliegenden Datenbeständen sind IT-Systeme in der Lage, eigenständig Lösungen für Probleme zu finden.

Deep Learning: Deep Learning ist ein Teilbereich des Machine Learnings und nutzt neuronale Netze sowie große Datenmengen. Die Lernmethoden richten sich nach der Funktionsweise des menschlichen Gehirns und resultieren in der Fähigkeit eigener Prognosen oder Entscheidungen.

So setzen Kriminelle KI heute schon ein

Wenn die IT Ihres Unternehmens bisher noch nicht Ziel einer groß angelegten Attacke durch Kriminelle geworden ist, haben Sie schlichtweg Glück gehabt. Ein geflügeltes Wort unter Experten besagt, dass es nur zwei Arten von Unternehmen gibt: Es gibt solche, die einen großen Hackerangriff bereits hinter sich haben, und diejenigen, die nicht wissen, dass sie bereits angegriffen wurden.

Kriminelle und Hacker verfolgen die Entwicklung von KI genauso aufmerksam wie Unternehmen. Und genau wie diese machen sie sich diese Technologie zunutze. Firmen dürfen sich hier nicht von der trügerischen Idee leiten lassen, dass KI zu komplex oder zu teuer für Kriminelle ist. Denn inzwischen bieten Cloud-Anbieter wie Google, Amazon oder Microsoft bereits Schnittstellen zu Rechensystemen für das maschinelle Lernen. Außerdem darf nicht vergessen werden, dass hinter Angriffen aus dem Internet auch Konkurrenten, Nachrichtendienste und Staaten stehen können. In einem solchen Fall spielt Geld eine untergeordnete Rolle.

Es gibt eine ganze Reihe von Szenarien für den Einsatz von KI durch Kriminelle, z. B.:

- **Biometrie:** Eine Vielzahl beeindruckender Beispiele zeigt, dass mittels KI täuschend echt wirkende Personen und Gesichter virtuell erzeugt werden können. Als Grundlage für solche „Deep Fakes" können die Systeme auch Alltagsaufnahmen der Betroffenen nutzen. Auf diese Weise lassen sich biometrische Sicherheitssysteme, die auf Gesichtserkennung basieren, überwinden.
- **Spracherkennung und Sprachsynthese:** Ähnlich ausgeklügelt sind Anwendungen, die die Fähigkeit besitzen, Sprache künstlich zu generieren. Google beispielsweise hat einen Sprachcomputer entwickelt, der auf Wunsch telefonisch Termine abwickelt. Die Anrufer bemerken dabei nicht, dass sie mit einem Computersystem telefonieren. Mittels„ Natural Language Generation" sind Angreifer in der Lage, Stimme und Tonfall einer vertrauenswürdigen Person zu imitieren und so an womöglich heikle Informationen zu gelangen. Umgekehrt können mittels Spracherkennung und Sprachanalyse Daten aus Telefonmitschnitten oder anderen Informationsquellen gewonnen werden, die Details über Sicherheitssysteme verraten oder Hinweise auf anstehende Transaktionen liefern, die dann abgefangen werden.
- **Maschinelles Lernen:** Maschinelles Lernen wird von Angreifern dazu genutzt, aus großen Datenmengen eines Unternehmens das Verhalten der Opfer besser zu analysieren. Das Ziel ist es, erfolgversprechende Phishing-Attacken zu entwickeln. „Machine Learning" lässt sich aber auch zur Analyse von Schwachstellen der eingesetzten Sicherheitssysteme nutzen. Maschinelles Lernen erlaubt die Programmierung von Malware, die kaum oder nur sehr bedingt zurückverfolgt werden kann. Ein Angriffsszenario wären etwa „selbstlernende" Trojaner.
- **(Predictive) analytics:** KI-Systeme werden vielfach dazu genutzt, Vorhersagen zu treffen. Auf Basis bereits gewonnener Daten aus erfolgreichen und abgewehrten Attacken können intelligente Systeme den Angreifer dabei unterstützen, eine Strategie für eine erfolgversprechende Attacke zu entwickeln. Auch kann ein KI-System automatisiert Schwachstellen in IT-Systemen identifizieren.

Vor diesen überwältigenden technischen Möglichkeiten und der daraus entstehenden konkreten Bedrohung durch Cyberkrimielle für die digitale Geschäftsprozesse sollten Unternehmen nicht zögern, ebenfalls auf KI zur Abwehr von Gefahren zu setzen.

Cyber-Resilienz gewinnt an Bedeutung

In einer zunehmend digitalisierten Geschäftswelt führen Cyber-Attacken häufig unmittelbar zu Betriebsunterbrechungen. Der deutschen Wirtschaft entsteht dadurch ein Schaden von 100 Millionen Euro pro Jahr, stellt der Branchenverband Bitkom fest.[1] Der Stärkung der Widerstandskraft der IT-Infrastrukturen kommt daher eine immer größere Priorität zu. Zu diesem Zweck werden Konzepte erstellt und Maßnahmen definiert, die die Weiterführung und Wiederaufnahme der Geschäftstätigkeiten während bzw. nach einer Cyber-Attacke gewährleisten. Ziel der Cyber-Resilienz ist es, gut vorbereitet und schnell auf Sicherheitsverletzungen zu reagieren sowie Sicherheitsvorfällen entgegenzuwirken und gleichzeitig die Steuerbarkeit des Geschäftes zu erhalten.

Die Widerstandsfähigkeit gegen Angriffe von außen steht und fällt dabei mit der gelebten Sicherheitskultur im Unternehmen sowie mit den eingesetzten Schutzlösungen. Beides erfordert permanente Anpassungen der Sicherheitskonzepte und der Steuerungslösungen. Ein statischer Ansatz, bei dem Prozesse und Schutzlösungen einmalig definiert werden, reicht angesichts der hochdynamischen Sicherheitsrisiken nicht mehr aus. Wer clever in neue Technologien investiert, kann den Grad der Widerstandskraft überproportional steigern. Nach Ergebnissen des State of Cyber Resilience Reports 2019 von Accenture konnten diejenigen Unternehmen, die ihre Investitionen am besten skalierten, ihre Cyber Resilience viermal so stark verbessern wie andere.[2] Als Zukunftstechnologie gilt dabei KI und Maschinelles Lernen.

[1]Born2Invest: Why cybercrime is causing record losses for German companies, November 2019

[2]Accenture: Third Annual State of Cyber Resilience, January 2020

CYBER-RESILIENZ BENCHMARKS 2020

Investitionen in neue Innovationen in der Cyber-Resilienz nehmen zu.

86%

Prozentsatz der Unternehmen, die mehr als 20% ihres Cybersicherheitsbudgets für fortschrittliche Technologien ausgeben.

US$ 380,000

durchschnittliche Kosten pro Angriff für nicht-führende Unternehmen

US$ 107,000

durchschnittliche Kosten pro Angriff für Führer in der Cybersicherheit

72%

Hochleistungsfähige Cybersicherheit kann dazu beitragen, **die Kosten pro Angriff um 72% zu senken**. Diese belaufen sich auf 273.000 US-Dollar.

Fortschrittliche und schubverleihende Technologien die Vorteile für die Cybersicherheit und die Cyber-Resilienz mit sich bringen:

- Künstliche Intelligenz und Maschinelles Lernen
- SOAR (Security, Orchestration, Automation, Response/ Sicherheit, Orchestrierung, Automatisierung, Reaktion)
- NGFW (Next Generation Firewall)

So zahlt sich der Einsatz fortschrittlicher Technologien bei Unternehmen aus, die in der Anwendung von Cybersicherheit führend sind:

- **4x** besser in der Abwehr von Angriffen
- **4x** besser darin, Verstöße schnell zu finden
- **3x** besser darin, Vorfälle schnell zu beheben
- **2x** besser bei der Reduzierung der Auswirkungen von Angriffen

Empfehlungen zur Stärkung der Cyber-Sicherheit

- In die operative Geschwindigkeit investieren
- Wert durch neue Investitionen steigern
- Bereits vorhandenen Ressourcen erhalten

Quelle: Accenture:
Dritter jährlicher„ State of Cyber Resilience", Januar 2020

http://www.accenture.com

KI ist bei der Angriffsabwehr überlegen

KI ist eine neutrale Technologie, die in ihrem Kern weder gut noch böse ist. In den Händen von Kriminellen stellt sie eine ernstzunehmende Bedrohung dar, doch im Umkehrschluss kann sie auch zur Abwehr von Gefahren eingesetzt werden. Der Versuch, bedrohliche KI mit menschlichem Einsatz zu bekämpfen ist aufgrund der technischen Größenunterschiede zum Scheitern verurteilt. In der IT-Sicherheit profitieren Security-Lösungen von KI-Komponenten deutlich, da zahlreiche Schwachstellen traditioneller Lösungen überwunden werden.

1. KI ist schneller

Durch die voranschreitende Digitalisierung stehen Unternehmen heute vor der Herausforderung, eine wachsende Anzahl von Anwendungen, externen Cloud-Anbietern und Geräten zu überwachen und abzusichern. In den kommenden Jahren wird die Zahl der zu überwachenden Systeme durch das Internet der Dinge (IoT) stetig steigen. Intelligente Sensoren übernehmen die Steuerung in der Haustechnik, dienen der Übermittlung von Informationen in der Supply Chain oder erlauben neue Geschäftsmodelle. Ein Abrechnungsmodell, das sich beispielsweise an der konkreten Nutzung von Geräten (Pay per Use) orientiert, ist ohne Sensoren nicht denkbar.

Im Umkehrschluss bedeutet dies, dass die von einer Organisation verarbeiteten Datenmengen weiter anwachsen. Gleichzeitig wird die Zahl der Schnittstellen und Kommunikationskanäle innerhalb des Unternehmens steigen. Bekanntlich ist aber jeder zusätzlich in die IT-Landschaft eingebettete Kanal potenziell auch ein Einfallstor für Angreifer und Kriminelle. Automatisierte KI-Systeme, die etwa den Datenverkehr von IoT-Sensoren überwachen, sind sehr viel schneller in der Lage, Anomalien in deren Verhalten zu entdecken. Sie schlagen schneller Alarm oder leiten Gegenmaßnahmen ein, als es der Mensch je könnte. Die Schlagzeilen der vergangen 18 Monate haben zunehmend verdeutlicht, dass Verschlüsselungstrojaner eine große Gefahr für Rechenzentren darstellen. An dieser Stelle sei an den Ausfall ganzer Rechenverbundsysteme von Krankenhäusern erinnert. Wie eine Umfrage von Bitkom ergeben hat, sind im Jahr 2019 der deutschen Wirtschaft Schäden von 10,5 Mrd. Euro durch Erpressung mit gestohlenen oder verschlüsselten Daten entstanden.[3] Der Einfall eines solchen Computerschädlings erfolgt oft über ein legitimiertes Benutzerkonto.

In großen und möglicherweise weltweit tätigen Unternehmen loggen sich rund um die Uhr Mitarbeiter auf interne Systeme ein. Augenscheinlich zu viele, um diese manuell zu überprüfen. KI kann in diesem Zusammenhang etwa Besonderheiten erkennen, um auf Basis von „Predictive Analytics" und „Mustererkennung" angemessen zu reagieren. Loggt sich ein Mitarbeiter üblicherweise zu festen Arbeitszeiten aus einer definierten Region auf einem System der Firma ein, so ist eine erfolgreiche Anmeldung mitten in der Nacht, aus einer anderen Zeitzone oder einer völlig anderen Region zumindest verdächtig. Ein solches Vorkommnis manuell zu entdecken, gleicht der sprichwörtlichen Suche nach der Stecknadel in einem Heuhaufen.

2. KI übersieht nichts

Groß angelegte Attacken erfordern einige Vorbereitung und zeitlichen Vorlauf. Während dieser Zeit versuchen die Angreifer, möglichst viele Systeme bzw. Angriffsvektoren in Stellung zu bringen. Dabei hinterlassen sie durchaus Spuren auf gekaperten Systemen. Durch Mustererkennung und Analysen können KI-basierte Verteidigungssysteme bereits kleinere Abweichungen erkennen. Administratoren und Sicherheitsverantwortliche erhalten rechtzeitig einen Alarm, wenn das System ein Vorkommnis als potenzielle Vorbereitung eines Angriffs einstuft.

Bei einer drohenden DDoS-Attacke ist schnelles Handeln notwendig. Aber wann handelt es sich noch um ein organisches Wachstum des Netzwerkverkehrs? Wann zeichnet sich eine Attacke ab? Auch in diesem Zusammenhang spielt KI ihre Geschwindigkeit aus. Binnen Sekunden werden regelmäßige Analysen über Wachstum, Datenquellen und Charakteristika einer DDoS-Attacke angestellt. Die Software ist hier selbst erfahrenen Mitarbeitern überlegen, da sie schneller in der Verarbeitung mehrerer Datenquellen, der Analyse und der Ergreifung von Gegenmaßnahmen ist.

[3]Manager Magazin: Chancen und Risiken von KI. Mit künstlicher Intelligenz gegen Cyber-Kriminelle, März 2020

Konventionelle Erkennungssysteme[1]	Erkennungssysteme mit lernender / KI-Komponente
Software (SW) arbeitet mit starren Modellen	SW arbeitet mit adaptiven Modellen
SW erzeugt Entscheidungen basierend auf einem transparenten Regelsystem	SW erzeugt Entscheidungen auf Basis einer graduellen Bewertung
SW ist nicht lernfähig	SW lernt laufend hinzu
SW setzt Signaturen und Korrelationen gegen verschiedene Arten von Daten ein	SW lernt komplexe Muster aus einer großen Menge von Daten

[1] J. Müller-Quade: Künstliche Intelligenz und IT-Sicherheit. Bestandsaufnahme und Lösungsansätze, April 2019

3. KI ist besser als jeder Patch

Die Abwehr krimineller Attacken erinnert häufig an ein Katz-und-Maus-Spiel. Typischerweise unterscheiden Sicherheitslösungen zwischen „guten" und „bösen" Anfragen oder Programmcode. Werden neue Sicherheitslücken entdeckt, besteht die Reaktion in der Regel in manuellen Anpassungen. Es wird ein Patch eingespielt, die Regeln in einer Firewall geändert und Signaturen von Schadprogrammen aktualisiert.

Die Sicherheitssysteme werden so auf den aktuellsten Stand gebracht. Die Entwicklung von Patches, Updates und Regeln benötigt aber Zeit und bezieht sich dabei auf bereits aufgetretene Vorfälle oder entdeckte Sicherheitslücken. In der Zwischenzeit haben die Kriminellen bereits weitergearbeitet. Sie verwenden andere Netzwerke für Attacken, die noch nicht in der Firewall erfasst sind, nutzen neue Sicherheitslücken aus oder setzen sogenannte „polymorphe" Schädlinge ein. Deren Code verändert sich ständig, um Erkennungsprogrammen die Aufgabe zu erschweren und die Tarnung des Schadprogramms zu verbessern.

Analysesysteme auf Basis von KI sorgen hier für Chancengleichheit gegenüber den Angreifern. Selbstlernende KI-Systeme, die sich während des Einsatzes immer weiter verbessern und somit automatisiert eigene Entscheidungen treffen, stellen ein mächtiges Werkzeug dar. Bei einer Strategie des „Whitelistings" wird jeder Netzwerkverkehr zunächst als schädlich klassifiziert bis das Gegenteil bewiesen ist, also beispielsweise Paketinhalte analysiert wurden. KI beschleunigt die Analysen und trifft in einem lernenden System die Entscheidung, welche Datenströme passieren dürfen.

4. KI überwindet Personalmangel

Durch alle Branchen hinweg zeigen sich in den vergangenen Jahren drei parallele Entwicklungen in der IT-Sicherheit, deren Kombination Anlass zur Besorgnis bietet.

Die Zahl der Attacken gegen Unternehmen ist gewachsen. Phishing, erfolgreiche Angriffe mit Ransomware, DDoSAngriffe: Die Bedrohungslage hat sich verschärft. Wie bereits dargestellt hat dies auch damit zu tun, dass die Zahl potenzieller Einfallstore und Plattformen wächst.

Gleichzeitig wurden von der Politik neue Regularien verabschiedet, die unmittelbaren Einfluss auf die IT-Sicherheit haben. Die DSGVO beschreibt im Kern sehr genau, was Unternehmen und Behörden im Rahmen „technisch-organisatorischer" Maßnahmen tun müssen, um Daten vor unbefugten Zugriffen, Manipulation und Diebstahl zu schützen. Somit wachsen die Anforderungen an die IT-Sicherheit auch hier.

Umsetzung der Compliance und Reaktion auf gestiegene Bedrohung erfordern somit mehr Fachpersonal. Der Bedarf an IT-Sicherheitsexperten ist sehr groß. Jedoch gelingt es vielen Unternehmen, insbesondere kleineren und mittelgroßen, gar nicht, diese Fachkräfte zu gewinnen.[4] Es herrscht ein ausgesprochener Mangel an Fachkräften in diesem Segment.

Das hat erwartungsgemäß Konsequenzen: Das vorhandene Personal ist überlastet und kann sich somit wichtigen Themen nur begrenzt widmen. So verwundert es kaum, dass es nach wie vor Organisationen gibt, in denen veraltete Software und Betriebssysteme im Einsatz sind. Doch genau damit machen sich die Firmen wiederum leichter angreifbar.

Eine volkswirtschaftlich bedeutende Konsequenz besteht in einem Innovationsstau. So zeigen sich Unternehmen aus Deutschland IoT-Lösungen gegenüber sehr aufgeschlossen, bringen aber Projekte nicht auf den Weg, weil sie Sicherheitslücken befürchten und sich um den Datenschutz sorgen.[5] Fachkräftemangel und Angst vor Bedrohungen sind also Bremsen für technische Innovationen.

Der Einsatz von KI in IT-Sicherheitslösungen spart personelle Ressourcen, weil die Maschinen viele Entscheidungen selbstständig (auf Basis von Regeln) treffen können, bei der Analyse schneller als der Mensch agieren und deutlich mehr Daten verarbeiten können. Im Gegensatz zum Menschen ermüden KI-Systeme nicht. In der Analyse von Protokolldateien übersehen Algorithmen keine Anomalien, während der Menschen möglicherweise schon müde geworden ist oder nicht mehr so genau hinsieht, weil er beispielsweise in den Feierabend möchte. KI eliminiert also die Fehlerquelle Mensch.

Unternehmen werden in der Zukunft nicht umhinkommen, in der IT-Sicherheit auf KI zu setzen, wenn sie den Fachkräftemangel überwinden und sich gegen hochgradig spezialisierte Kriminelle wehren wollen. So planen 40 % der Entscheidungsträger in der IT-Sicherheit von Unternehmen die Implementierung von KI; das ergab eine weltweite Umfrage von Forrester Research.[6] Mit Blick auf Deutschland gibt es ein wachsendes Bewusstsein für das Sicherheitspotenzial KIbasierter Lösungen. Das bestätigt auch eine Untersuchung von Capgemini.[7] Fast zwei Drittel (62 %) der Unternehmen sind der Meinung, dass sie ohne den Einsatz von KI-Technologien nicht auf Cyber-Angriffe reagieren können.

Die Nutzung von KI unterstützt die Sicherheitsexperten in ihrem Alltag und hilft ihnen dabei, sich auf besonders dringende und zeitkritische Aufgaben zu fokussieren, ohne Abstriche bei der Sicherheit insgesamt machen zu müssen. Konkrete Zahlen dazu, wie der Einsatz von AI das Schutzniveau der Unternehmen verbessert, liefert die Umfrage von Capgemini.

Drei von vier Befragten (74 %) berichten von schnelleren Reaktionen auf Attacken, 69 % stellten eine bessere Angriffserkennung fest. Eine gesteigerte Effizienz in Cybersicherheits-Analysen nannten 60 % der Befragten als Vorteil beim Einsatz von KI.

Der Geschäftsnutzen für den Einsatz von KI in der Cybersicherheit ist stark und offensichtlich.

[4]Welt: Angst vor Cyberattacken lähmt Deutschland, Februar 2020

[5]Digital Business Cloud: Internet der Dinge: Trotz Sicherheitsbedenken immer wichtiger für deutsche Unternehmen, Januar 2020

[6]Forrester Research: Forrester Analytics Global Business Technographics Security Survey 2019

[7]Capgemini: Reinventing Cybersecurity with Artifificial Intelligence, Juli 2019

CYBERSICHERHEIT MIT HILFE KÜNSTLICHER INTELLIGENZ MEISTERN

69%

% der Unternehmen gaben an, **dass sie ohne KI nicht in der Lage sein werden, kritische Bedrohungen zu erkennen.**

Vor 2019

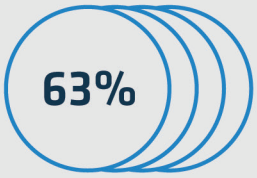
verwendete fast jedes fünfte

Unternehmen

KI in der Cybersicherheit.

Etwa

zwei Drittel der



Unternehmen

PLANEN, **KI** BIS 2020 **ZU NUTZEN.**

28% der

Unternehmen verwenden Sicherheitsprodukte mit **EINGEBETTETER KI.**

73% DER **UNTERNEHMEN**

gaben an, dass sie in irgendeiner Weise Anwendungsfälle für KI in der Cybersicherheit testen.

Quelle: Capgemini Forschungsinstitut: Mit künstlicher Intelligenz die Cybersicherheit neu erfinden, Juli 2019

Wie Link11 Sie dank KI besser schützt

Link11 hat sich bereits früh mit der Frage auseinandergesetzt, wie KI Security-Lösungen noch besser und Unternehmen damit noch resilienter gegen Cyber-Attacken machen kann. So werden maschinelles Lernen, Mustererkennung und Predictive Analytics in immer mehr Services zu einem integralen Bestandteil.

BOT-Management: Wie KI sind Bots an sich nicht gut oder böse. Die von diesen automatisierten Programmen verursachten Anfragen machen in vielen Unternehmen inzwischen einen Großteil des Traffics aus. Suchmaschinen indizieren mit Bots die Inhalte der Seiten. Vergleichsportale verwenden Bots dazu, aktuelle Preisinformationen zu gewinnen. Bots können aber auch betrügerisch und kriminell eingesetzt werden. Beispielsweise wenn sie Werbeformate in betrügerischer Absicht abrufen, oder in krimineller Absatz die Bedienbarkeit von Systemen einschränken.

Mit unserem Bot-Management-Service bieten wir die Möglichkeit, den von Bots verursachten Traffic auf Ihren Systemen zu klassifizieren und zu steuern. KI hilft dem System dabei, bisher unbekannte Bots zu erkennen und zu beurteilen. So hilft die künstliche Intelligenz Ihnen beim Einsatz des Service dabei, echten Nutzern ein besseres Erlebnis beim Besuch ihrer Seiten zu verschaffen, weil auf den Traffic durch unerwünschte Bots reagiert wird.

DDoS-Schutz: Nicht nur die Link11 Cyber-Resilienz-Netzwerkanalysen zeigen, dass DDoS-Attacken immer mehr zunehmen und komplexer werden. Die Schutzlösung von Link11 kombiniert den Einsatz der Cloud mit der Nutzung von künstlicher Intelligenz. Dank der Cloud ist der Schutz gut skalierbar und schnell einsatzbereit. Und mit „Always On" handelt das System rund um die Uhr bei einem Angriff. Im Falle eines Angriffs spielt Zeit eine wichtige Rolle. Die KI-Lösung lernt in Echtzeit aus allen von Link11 abgewehrten Attacken. Das System analysiert jeden Angriff und überträgt die Ergebnisse auf andere Gefährdungsmuster. Anders als bei jedem manuellen Ansatz ist das System somit auf neue Angriffsvektoren vorbereitet. Davon profitieren alle Kunden und Unternehmen, da das Abwehrschild permanent besser wird. Es sieht ähnliche Vorfälle voraus und kann somit immer schneller im Gefährdungsfall reagieren.

KI-Systeme entbinden nicht von Verantwortung

Bei allem Potenzial: Ein Allheilmittel in Sachen IT-Sicherheit und Cyber-Resilienz stellt künstliche Intelligenz – zumindest bis auf Weiteres – nicht dar. Zwar ist KI nach einem intensiven Training stark in der Erkennung von Gefahren wie Malware oder DDoS-Attacken und zudem in einem direkten Vergleich genauer als die menschliche Angriffserkennung. Da die Bedrohungslage in der digitalen Welt aber hochdynamisch ist, wird es weiterhin dem Menschen obliegen, die Angriffe einzuordnen und Maßnahmen daraus abzuleiten. Das wichtigste Assistenzmittel dafür wird künstliche Intelligenz sein. Sie wird den Menschen immer stärker in der Entscheidungsfindung entlasten, aber ihn nicht gänzlich ersetzen.

Wollen Sie mehr darüber erfahren, wie der Einsatz von künstlicher Intelligenz Ihre IT besser schützt und Ihnen dabei hilft, Ihre Cyber-Resilienz-Strategie umzusetzen? Dann kontaktieren Sie noch heute einen unserer Spezialisten.

Über Link11

Link11 ist der im Bereich Cyber-Resilienz führende europäische IT-Sicherheitsanbieter. Die globalen Schutzlösungen der Cloud Security Plattform sind vollständig automatisiert, reagieren in Echtzeit und wehren alle Angriffe, so auch unbekannte und neue Muster, in unter 10 Sekunden ab. Link11 bietet laut einhelliger Analysten-Meinung (Gartner, Frost & Sullivan) die schnellste Mitigation (TTM), die auf dem Markt verfügbar ist. Um Cyber-Resilienz zu gewährleisten, sorgen u.a. Web- und Infrastruktur-DDoS-Schutz, BOT-Management, API-Schutz, Secure-DNS, Zero-Touch-WAF, Secure-CDN bis hin zu Threat-Intelligence-Services für eine ganzheitliche und Plattform-übergreifende Härtung der Netzwerke und kritischer Anwendungen von Unternehmen. Die internationalen Kunden können sich so auf ihr Geschäft und digitales Wachstum konzentrieren. Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovativen Lösungen ausgezeichnet.

Link11 GmbH
Lindleystraße 12
60314 Frankfurt
Germany
✉ info@link11.com

Frankfurt Office
✆ +49 (0)69 – 264929777

UK & Ireland Office
✆ +44 (0)203 - 8688711
✉ info.uk@link11.com

Nordics & Baltics Office
✆ +46 (0)85 - 250 05 71
✉ info.nordics@link11.com

BeNeLux Office
✆ +31 (0)68 - 992 3607
✉ info.benelux@link11.com