Foto: Shutterstock / BeeBright

Threat Intelligence & Security Intelligence

Mit Künstlicher Intelligenz gegen Hacker kämpfen

Big Data, Cloud und Machine Learning helfen, IT-Systeme besser vor Angriffen zu schützen.

Die Zahl der Angriffe auf IT-Systeme steigt weiter stark an. Täglich entdecken die Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI) rund 380.000 neue Varianten von Schadprogrammen, und die Zahl von Spam-Nachrichten mit Schadsoftware im Anhang ist ihren Angaben nach im Vorjahr um 1270 Prozent gestiegen. Kurz: „Die Gefährdungslage ist weiterhin angespannt“, bilanziert das BSI im Jahresbericht zur Lage der IT-Sicherheit in Deutschland 2016.

Auffällig sind dem BSI zufolge drei Entwicklungen: Zum einen ist eine zunehmende Professionalisierung der Angriffe zu erkennen, sodass heutzutage international agierende und hervorragend ausgebildete und ausgerüstete Kriminelle die größte Gefahr für Unternehmen darstellen. Zum anderen eröffnen die Digitalisierung und die zunehmende Vernetzung im Internet der Dinge (IoT) immer neue Angriffsflächen. Und drittens werden Schädlinge immer schneller entwickelt, sodass viele klassische Abwehrmaßnahmen, etwa Antivirenprogramme, damit nicht Schritt halten.

106 Tage
bleiben ins Firmennetz eingedrungene Angreifer in der EMEA-Region im Durchschnitt unentdeckt (weltweit: 99 Tage)

Quelle: FireEye

Die größten Bedrohungen

Zwei Gefahren haben den BSI-Experten zufolge 2016 die IT-Sicherheit besonders strapaziert: Ransomware und IoT-Bot-Netze.

Malware, die Daten verschlüsselt und erst gegen Lösegeld wieder freischaltet, hat sich 2016 noch einmal stärker verbreitet als im Vorjahr, insbesondere in Deutschland. Nach einer Umfrage des BSI waren ein Drittel der befragten Unternehmen in den letzten sechs Monaten

von Ransomware betroffen. Und in jedem fünften dieser Unternehmen waren nicht etwa nur Einzelplatzrechner betroffen, sondern es kam zu einem erheblichen Ausfall der IT-Infrastruktur insgesamt. Kaspersky Lab bezeichnet deshalb 2016 auch als „Jahr der Ransomware".

Erstmals ins Bewusstsein einer breiteren Öffentlichkeit schaffte es 2016 die Erkenntnis, dass mit dem Internet der Dinge auch ein großes Sicherheitsrisiko entsteht. Ende Oktober 2016 kaperten Hacker zunächst schlecht abgesicherte Geräte wie Überwachungskameras, digitale Videorekorder oder private Router und bauten damit ein riesiges Bot-Netz auf. Mit der Kraft der vernetzten IoT-Geräte setzten sie anschließend mit einer massiven Distributed-Denial-of-Service(DDoS)-Attacke eine Reihe prominenter US-Online-Dienste außer Gefecht. Die Folge: Die Seiten und Services von Firmen wie Amazon, Paypal, Netflix, Spotify oder Twitter waren in Teilen der USA und Europas zeitweise nicht verfügbar.

Security braucht Intelligence

Schlagwörter wie Ransomware, Bot-Netze oder Advanced Persistent Threats sind der eindeutige Beweis dafür, dass Cyberkriminelle im Katz-und-Maus-Spiel IT-Sicherheit immer raffiniertere Angriffsmöglichkeiten entwickeln, um Geld zu erpressen, Dienste lahmzulegen oder sensible Informationen wie Kundendaten oder Entwicklungspläne abzugreifen. Entgegen kommt ihnen dabei, dass die IT-Systeme von Unternehmen heute erheblich verwundbarer sind als früher, da mittlerweile nahezu alle Prozesse digitalisiert und viele Systeme über das Internet verbunden sind.

Das zwingt die Firmen dazu, ihr IT-Sicherheitskonzept stetig an neue Bedrohungen anzupassen und ihre Abwehrmaßnahmen fortlaufend zu aktualisieren. Erschwert wird ihnen das durch die schwindende Abwehrkraft klassischer Techniken wie Firewalls, Intrusion-Detection-Systeme, Antiviren-Lösungen oder Berechtigungskonzepte. Unternehmen müssen heute unbedingt zeitnah wissen, welche Bedrohungen gerade akut und für genau ihre IT relevant sind – vor allem aber müssen sie Sicherheitsvorfälle zügig erkennen, um schnell reagieren zu können.

Foto: Check Point

„Bei Threat Intelligence handelt es sich darum, die Gefahren zu verstehen, Security Intelligence zielt darauf ab, die Bedrohungen abzuwehren."

Mirco Kloss
Security Evangelist bei Check Point
www.checkpoint.com

Doch hier haben viele Firmen Nachholbedarf, wie der aktuelle „Corporate IT Security Risks Report" von Kaspersky Lab zeigt. Demnach benötigten 28,7 Prozent von weltweit befragten 4000 Unternehmen im Schnitt mehrere Tage, um eine Sicherheitsverletzung zu entdecken, bei 19,1 Prozent der Firmen dauerte es sogar mehrere Wochen. Dieser lange Zeitraum zwischen Infiltration und Erkennung ist höchst kritisch, da die Angreifer sich in dieser Zeit relativ frei im Unternehmensnetzwerk bewegen und tief in den Systemen einnisten können. Lediglich 8,2 Prozent waren in der Lage, Vorfälle nahezu umgehend zu erkennen.

Noch weniger erbaulich sind die Zahlen des jährlichen Reports „M-Trends", den FireEye Ende März veröffentlicht hat. Demnach schafft es ein Angreifer in der EMEA-Region, wenn er einmal in ein Firmennetz eingedrungen ist, dort durchschnittlich 106 Tage sein Unwesen zu treiben, bevor er entdeckt wird. Der weltweite Durchschnitt liegt bei 99 Tagen. FireEye bemerkt dazu lakonisch: „Positiv zu bewerten ist allerdings die Tatsache, dass sich die Verweildauer gegenüber den M-Trends-Zahlen aus 2015 mit 469 Tagen deutlich verringert hat."

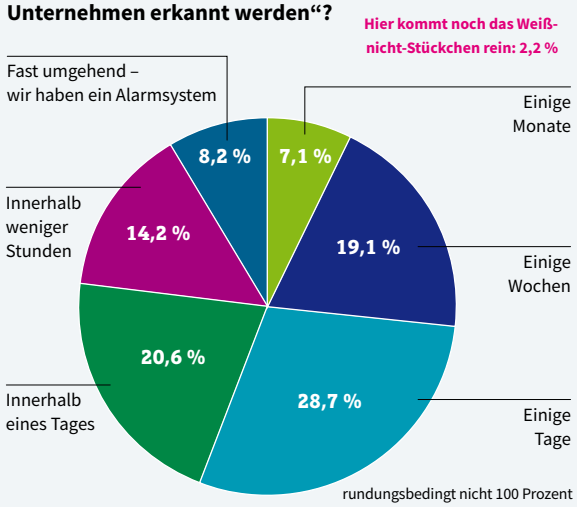
Diese Zahlen machen eines unübersehbar deutlich: Unternehmen benötigen eine bessere Strategie für die Erkennung von Angriffen und die angemessene Reaktion darauf. Als besonders vielversprechende Konzepte kommen hier Threat Intelligence (TI) und Security Intelligence (SI) ins Spiel. Allerdings verstehen die Sicherheitsfirmen längst nicht immer das Gleiche darunter.

Threat und Security Intelligence

Mirco Kloss, Security Evangelist bei Check Point, legt großen Wert auf die Unterscheidung der Begriffe: „Bei Threat Intelligence geht es darum, die Gefahren zu verstehen. Security Intelligence zielt darauf ab, die Bedrohungen abzuwehren. Allerdings hängen beide Begriffe eng zusammen: Wenn ich die Mittel und die Motive eines Angreifers nicht verstehe, wird es sehr schwer, seine Attacken abzuwehren. Daher braucht es Know-how über Schwachstellen und Schädlinge." Threat ▶

Angriffe oft lange unentdeckt

„Wie lange dauert es, bis Sicherheitsvorfälle in Ihrem Unternehmen erkannt werden"?



Kritische Lücke: In etwa 20 Prozent aller Firmen dauert es mehrere Wochen, bis eine Sicherheitsverletzung entdeckt wird.

com! professional 6/17 Quelle: Kaspersky Lab „Corporate IT Security Risks Report"

Intelligence beschreibt in diesem Kontext also das Sammeln und die Analyse von Informationen, die auf geplante Angriffe, Schwachstellen und andere unerwünschte Aktivitäten in der IT-Infrastruktur hindeuten.

Deshalb reicht eine Threat-Intelligence-Lösung allein Kloss zufolge auch keinesfalls aus: Unternehmen müssten Threat Intelligence in eine umfassende Sicherheitsarchitektur umsetzen, die sowohl die Gefahrenlage als auch die individuelle Situation der Firma berücksichtige. „Die Kombination der einzelnen Faktoren wäre dann die Security Intelligence: Die Aufstellung und Implementierung einer passenden Sicherheitsarchitektur."

Martin Zeitler, Senior Systems Engineering Manager bei Palo Alto Networks, weist auf den militärischen Ursprung des Begriffs Intelligence hin: „So werden dort Informationen bezeichnet, die einer Organisation die Grundlagen für Entscheidungen oder auch strategische Vorteile im Konfrontationsfall liefern können." Threat Intelligence (TI) unterteilt er weiter in die Unterkategorien taktische TI und strategische TI. „Bei der taktischen TI ist die Information direkt technisch anwendbar und wird häufig in der Form von IOCs (Indicators of Compromise) bereitgestellt. Die strategische TI verstehe ich hingegen als High-Level-Information über den Angreifer, seine Motivation, Taktik, Technik und Vorgehensweise."

Foto: Akamai

„Security Intelligence wird nur erfolgreich sein, wenn die Lösung in eine umfassende Security-Strategie und entsprechende Sicherheitsrichtlinien eingebettet ist."

Ralf Gehrke
Director Presales für Europa bei Akamai
www.akamai.de

Zur Erklärung: IOCs sind strukturierte Informationen über Merkmale schädlicher Aktivitäten. Damit lassen sich automatisiert Systeme aufspüren, die manipuliert wurden oder gegen die gerade eine Attacke läuft.

Security Intelligence wiederum fasst Martin Zeitler wesentlich weiter. „Bei SI geht es um den grundsätzlichen Schutz einer Organisation gegen externe und interne Bedrohungen praktisch jeder Art."

Akamai schließlich, über dessen Content-Delivery-Network (CDN)-Services rund 30 Prozent des gesamten Internetverkehrs laufen, spricht schon gar nicht mehr von Threat Intelligence, sondern nur noch von Security Intelligence. „SI hat für uns eher einen proaktiven Charakter und ermöglicht es, einen Angreifer bereits im Vorfeld auf Basis von Big Data, heuristischen Methoden und selbstlernenden Algorithmen zu blocken", erläutert Ralf Gehrke, Director Presales für die Region Europa bei Akamai.

Detect, Prevent, Response

Laut Gehrke überwacht und schützt eine SI-Lösung alle neuralgischen Schnittpunkte und Bereiche der IT-Infrastruktur: Endpunkte, IoT-Systeme, Netzwerke mit Routern, Switches und Gateways, Webserver sowie Mitarbeiter, die im Web browsen und eventuell auf einen Link mit Malware klicken. Sie bietet dazu drei grundlegende Funktionen: Detect, Prevent/Protect und Response.

Detect steht für die Entdeckung von Schädlingen und Angriffsversuchen, Prevent/Protect für den Schutz vor und die Blockade von Angriffen und Response für Handlungsempfehlungen und konkrete Maßnahmen, mit denen Firmen auf einen entdeckten Angriff reagieren, der bereits das Netzwerk infiltriert hat.

„Wichtig sind beispielsweise das kontinuierliche Sammeln und sofortige Bereitstellen von Rohdaten – und zwar rund um die Uhr – sowie die zentrale Analyse der Daten über die komplette Infrastruktur hinweg", sagt Achim Kraus, Director of Sales Engineering bei Cybereason, einem Experten für Endpunkt-Schutz.

Als weitere Funktionen einer SI-Lösung nennt Gehrke das automatische Erkennen verdächtiger Vorgänge bis zum Erkennen von Malware-Betriebsschritten und die Einordnung in den Ablauf einer Angriffskette inklusive Visualisierung. „Sobald ein Angriff erkannt und validiert wurde, sollte eine SI-Lösung unverzüglich reagieren und innerhalb von 60 Sekunden Schutzmaßnahmen einleiten, die ein derartiges Ereignis auch künftig verhindern. Dazu gehört, dass alle Endgeräte im Unternehmen damit ausgestattet werden." ▶

Tipps zur SI-Implementierung

Wenn Unternehmen Security-Intelligence-Lösungen implementieren wollen, sollten sie folgende Experten-Tipps beachten.

- Oberstes Ziel ist eine möglichst frühzeitig ansetzende Prävention mit maximaler Automatisierung und dem Einsatz von Threat-Informationen.
- Hilfreich ist ein grundsätzlich neues Verständnis von Security. Es reicht nicht mehr, mit Hilfe von Firewalls Mauern hochzuziehen. Mehr Schutz bringen intelligente Systeme.
- Ohne vorausgehende Risikoanalyse und ohne Security-Strategie wird SI nicht erfolgreich sein.
- Ein ausgewogenes Security-Niveau über sämtliche Unternehmensbereiche ist besser als eine Mischung aus besonders gut und weniger gut geschützten Bereichen.
- Unternehmen sollten ihre Security-Lösungen über Schnittstellen auf einer Plattform harmonisieren und aufeinander abstimmen statt Insellösungen nebeneinander zu betreiben.
- Mehr Schutz bringt es auch, Datenquellen zu konsolidieren und zu verknüpfen. Zudem sollten architekturelle Sicherheitsmaßnahmen wie Zweifaktor-Authentifizierung oder Netzwerk-Segmentierung umgesetzt werden.
- Wichtig ist es, Mitarbeiter, Betriebsrat und Datenschutzbeauftragte mit ins Boot zu holen.

Interview

„KI erhöht die Erkennungsrate um den Faktor 100“

Christian Nern ist Head of Security Software DACH bei IBM. Im Interview erklärt er, was IBM unter Security Intelligence versteht, wie Watson for Cybersecurity mit Künstlicher Intelligenz die Sicherheit erhöht und warum der Mensch wichtig bleibt.

com! professional: *Threat Intelligence und Security Intelligence sind in aller Munde. Was verstehen Sie darunter?*

Christian Nern: Threat Intelligence (TI) meint das Sammeln und die Analyse von Daten über Schwachstellen oder Angriffe in der IT-Umgebung, das Erkennen von Mustern in Angriffen oder dem Nutzerverhalten. TI ist damit eine wichtige oder sogar die Kernkomponente von Security Intelligence (SI), bei der es um das Erkennen und Vermeiden von Angriffen geht.

SI-Lösungen bilden eine neue Generation intelligenter Systeme, die nahezu alles über die IT-Landschaft und deren Bedrohungen, Angriffe und Sicherheits-Events wissen. Und je mehr ich weiß, desto präziser kann ich regelbasierte und (teil-)automatisierte Gegenmaßnahmen ergreifen.

com! professional: *Welche Funktionen sollte eine SI-Lösung denn auf jeden Fall mitbringen?*

Nern: Sie sollte aus der großen Menge an Daten Muster auch von komplexen Angriffen erkennen, flexibel auf Hackerangriffe reagieren, Handlungsempfehlungen geben und Warnungen proaktiv aussprechen. Idealerweise sind SI-Lösungen modular aufgebaut, damit man sie schrittweise erweitern kann. Und sehr wichtig ist der Plattformgedanke, das heißt, Security Intelligence darf keine Insellösung sein, sondern muss über Schnittstellen auch mit den Lösungen anderer Hersteller zusammenarbeiten.

Foto: IBM

Christian Nern
Head of Security Software DACH bei IBM Deutschland
www.ibm.com/de-de

com! professional: *Sie haben die großen Datenmengen angesprochen, die SI-Lösungen verarbeiten. Aus welchen Datenquellen stammen die Inhalte?*

Nern: IBM hat selbst 300 Security Operations Center (SOCs) für Großkunden, in denen wir Informationen wie Sicherheits-Events und Warnungen, Logs und Konfig-Daten, Benutzer- und Netzwerkstatistiken, Bedrohungs- und Schwachstellen-Feeds sammeln. Diese Daten werden alle fünf Minuten aktualisiert.

> **„Security Intelligence darf keine Insellösung sein.“**

Dank Watson for Cybersecurity können wir in unseren SOCs jetzt auch neue Quellen wie forensische Analysen, Angriffsberichte, Forschungsuntersuchungen, Whitepaper, Tweets, Blogs, Wikis und Webseiten mit Security-Inhalten auswerten. Insgesamt speisen wir Watson mit Informationen aus rund zehn Milliarden Knoten beziehungsweise Referenzquellen. So erhalten wir ein umfassendes Bild der Security-Lage in Unternehmen. Denn viele Firmen nutzen im Schnitt nur 8 Prozent des Sicherheitswissens.

com! professional: *Sie sprechen im Zusammenhang mit Watson for Cybersecurity immer von kognitiver IT-Sicherheit. Was meinen Sie damit?*

Nern: Mit Watson setzen wir auch maschinelles Lernen und Künstliche Intelligenz ein, um die Sicherheit von Unternehmen zu erhöhen. Dazu trainierten und fütterten IBM-Experten das System seit Anfang 2016 mit über einer Million sicherheitsbezogener Dokumente. Dank der kognitiven Technologie können wir Cyberbedrohungen schneller und effizienter abwehren. Unternehmen erleben im Schnitt 200.000 sicherheitsrelevante Ereignisse pro Tag. Das zeigt, dass die IT-Fachkräfte Unterstützung von intelligenten Maschinen brauchen.

com! professional: *Welche Vorteile bringen KI und Machine Learning für den Schutz von Unternehmen?*

Nern: Sie erhöhen deren IT-Sicherheit enorm. Das zeigen 40 Beta-Tests von Watson for Cybersecurity in Unternehmen. Zum einen analysiert und wertet Watson umfangreiche Datenmengen fast in Echtzeit aus, in Sekunden statt Minuten. Die Maschine findet Angriffe, Threats oder sicherheitsrelevante Ereignisse um das Fünf- bis Zehnfache schneller als andere Systeme.

Da Watson for Cybersecurity die Relationen von Threats und Events visualisiert und neu erkannte Bedrohungen andersfarbig markiert, vereinfacht sich die Arbeit der Security-Experten. Auch die Erkennungsrate von verdächtigen Ereignissen und damit der

Foto: Feature Photo Service

IBM X-Force Command Center: Security-Analysten bei der Arbeit.

Ausschluss von False Positives ist um den Faktor 100 gestiegen. Watson erkennt auch komplexe Angriffe, zeigt deren Konsequenz für den betroffenen Endpunkt und gibt auf Basis von Logik Handlungsempfehlungen für Sicherheitsmaßnahmen.

com! professional: *Wie sehen diese Handlungsempfehlungen aus?*

Nern: Hier muss ich vorausschicken, dass Watson for Cybersecurity Teilmodul einer integrierten, vernetzten Sicherheitslösung mit IBM QRadar als Kernstück ist. Watson erstellt die Handlungsempfehlung auf Basis von Best Practices, sprich den wahrscheinlichsten und bisher besten Reaktionen auf entsprechende Angriffe. So rät Watson etwa, den betroffenen Client zu isolieren oder einen Patch aufzuspielen. Die verknüpfte Lösung IBM BigFix Detect setzt die empfohlene Reaktion dann regelbasiert und teilweise automatisiert um. Bei vielen Lösungen läuft dieser Prozess zum Teil noch manuell ab.

„IT-Fachkräfte brauchen die Unterstützung von intelligenten Maschinen."

com! professional: *Können kognitive Technologien Security-Experten ersetzen?*

Nern: Nein, natürlich nicht. Selbst wenn Security Intelligence installiert ist, sind Unternehmen noch nicht sicher. SI funktioniert nur, wenn in den Firmen Security-Prozesse vorhanden sind auf Basis von Risikoanalyse, Sicherheits-Policies, Notfallplan oder Schulung der Mitarbeiter. SI-Lösungen unterstützen die Security-Mitarbeiter mit Auswertungen und Handlungsempfehlungen bei Angriffen. Dies wird zukünftig noch relevanter, da die Menge der Security-Daten weiter steigt.

Unternehmen müssen wissen, was bei ihnen passiert. Sie sollten auch ihre Sichtweise von Security ändern: Es reicht nicht mehr, sich mit Firewalls, Proxies oder Gateways abzuschotten und Mauern hochzuziehen. Stattdessen benötigen sie intelligente Systeme mit KI, die vernetzte Plattformen bilden anstelle von Insellösungen, die nicht zusammenarbeiten.

Schlüsse ziehen aus Big Data

Eine Threat-Intelligence-Lösung kann ihre Wirkung erst mit Hilfe von Big Data entfalten, da es hier um die Analyse riesiger Datenmengen geht. Quellen sind etwa Weblogs, Bedrohungs- und Schwachstellen-Feeds, Konfigurationsdateien, Spam-Bots, URLs von Angriffen, Benutzer- und Netzwerkstatistiken, Angriffsberichte und forensische Daten.

Die Dimensionen veranschaulicht ein Blick auf das Security Operations Center (SOC) von Telekom Security und Akamai. Telekom Security erfasst täglich rund eine Milliarde sicherheitsrelevante Events aus 3000 Datenquellen, etwa Firewalls, und verzeichnet vier Millionen Angriffe auf seine 200 physischen Honeypot-Sensoren, sprich vorgetäuschten Zielen, die Angriffsversuche von Cyberkriminellen provozieren. Pro Tag wertet Telekom Security sechs Milliarden Datensätze der DNS-Server auf Attacken hin aus, checkt sieben Millionen Websessions mit mehr als 100 GByte Datenvolumen und untersucht zehn Millionen E-Mails auf Spam.

Foto: Palo Alto Networks

„Taktische Threat Intelligence (TI) liefert direkt technisch anwendbare Informationen (…). Strategische TI verstehe ich als High-Level-Informationen über den Angreifer, seine Motivation, Taktik, Technik und Vorgehensweise."

Martin Zeitler
Senior Manager Systems Engineering Germany bei Palo Alto Networks
www.paloaltonetworks.de

Durch kontinuierliches Monitoring und Analysieren des Verhaltens der Netzinfrastruktur versucht Telekom Security, den störungsfreien Betrieb der IT-Infrastruktur seiner Kunden sicherzustellen. Aus den Erkenntnissen über Angriffe entwickelt das Unternehmen sogenannte Use Cases für wirklich wichtige Auffälligkeiten. „Ohne sinnvolle und effiziente Suchregeln nützt die beste Monitoring-Technik nichts. Durch die intelligente Korrelation von Security-Events und die kontinuierliche Abbildung neuer Angriffsmethoden entsteht ein immer besser werdender Filter für tatsächlich relevante Alarme. Hier kommt auch maschinelles Lernen zum Einsatz. Dadurch erreichen wir sehr hohe Detektionsraten und minimieren die Zahl der False Positives", sagt Dirk Backofen, Leiter Telekom Security.

Big Data, Cloud und KI

Oliver Tavakoli, Chief Technology Officer bei Vectra Networks, einem Spezialisten für die Echtzeit-Erkennung aktiver Cyberangriffe, sieht im Dreigestirn von Big Data, Cloud und maschinellem Lernen (ML) wichtige Vorteile von Security-Intelligence-Systemen: „Big Data macht es auch möglich, rückblickend die Spuren vergangener Attacken zu verfolgen, mit forensischen Mitteln Angriffsschritte zu rekonstruieren und so herauszufinden, wie ein Angriff gelingen konnte. Mit maschinellem Lernen oder Künstlicher Intelligenz schaffen es SI-Lösungen, auch extrem große Mengen ▶

an Daten erfolgreich auf jene Anomalien hin zu durchsuchen, die tatsächlich auf Angriffe hindeuten. Cloud-Umgebungen schließlich sind die Basis für skalierbare Update-Mechanismen, die die SI-Systeme aktuell halten."

Cloudbasierte Services, die die internen Sicherheitsmaßnahmen ergänzen, helfen also Unternehmen dabei, die Herausforderungen der IT-Sicherheit besser zu meistern – vor allem die gestiegene Komplexität, die erhöhte Frequenz und das zunehmende Ausmaß der Cyberattacken, insbesondere, weil sowieso nur wenige Firmen IT-Spezialisten beschäftigen, die sich dezidiert mit IT-Security befassen.


Foto: Cybereason

„Erfolgreiches maschinelles Lernen erfordert eine gute Qualität und kontinuierliche Überwachung der zugrundeliegenden Daten sowie eine stetige Weiterentwicklung der Algorithmen."

Achim Kraus
Director Sales Engineering bei Cybereason
www.cybereason.com

Die Cloud-Dienste verfügen über genügend skalierbare Rechenkapazitäten, um die für Threat Intelligence anfallenden Datenmassen schnell zu analysieren – auch mit Hilfe von maschinellem Lernen und KI. Sie können selbst schwerste DDoS-Angriffe mit einer Bandbreite von mehr als 100 GBit/s abwehren. Und sie sparen Investitions- und Betriebskosten im Vergleich zu einer Lösung im eigenen Rechenzentrum.

Treffer mit Machine Learning

Die von com! professional befragten Experten sind sich einig: Den Unternehmen stehen mit Cloud, Big Data und maschinellem Lernen Technologien zur Verfügung, um größte Datenmengen schnell zu analysieren und Zusammenhänge selbst in umfangreichsten IT-Umgebungen zu erkennen – und so zeitnah auf neuartige Attacken zu reagieren. „So wird es etwa möglich, das Verhalten von fünf Benutzern in einem 10, 50 oder gar 250.000 Mitarbeiter großen Unternehmen nicht nur als verdächtig, sondern als Bestandteil eines gezielten Angriffs zu erkennen. Dies erfordert allerdings eine gute Qualität und kontinuierliche Überwachung der zugrundeliegenden Daten sowie eine stetige Weiterentwicklung der Algorithmen", erklärt Achim Kraus, Director of Sales Engineering bei Cybereason.


Foto: Vectra Networks

„Big Data macht es möglich, rückblickend Spuren vergangener Attacken zu verfolgen, mit forensischen Mitteln Angriffsschritte zu rekonstruieren und so herauszufinden, warum ein Angriff gelingen konnte."

Oliver Tavakoli
CTO bei Vectra Networks
www.vectranetworks.com

Beim maschinellen Lernen wird das System – vereinfacht gesagt – zunächst trainiert und mit Netzwerkinformationen sowie den beschriebenen sicherheitsbezogenen Daten gefüttert. Dabei wird mittels Mustererkennung auch eine Art „Normalverhalten" definiert, anhand dessen später frühzeitig Anomalien erkannt und Bedrohungen entdeckt werden.

Die Anbieter von SI-Lösungen entwickeln ihre Algorithmen stetig weiter und verfeinern sie mit dem Ziel, die Trefferquote zu erhöhen, die Anzahl von Fehlalarmen (False Positives) zu reduzieren und bislang unbekannte Angriffsmuster zu entdecken. Dazu kombinieren sie auch verschiedene Algorithmen miteinander oder verwenden Algorithmen, die auf neuronalen Netzen beruhen.

Letztendlich entstehen so statistische Machine-Learning-Modelle, auf deren Basis eine SI-Lösung in Echtzeit entscheiden kann, ob ein Netzwerkverkehr gut- oder bösartig ist. Zudem erkennen sie das Verhalten moderner Malware besser, die für traditionelle Standardlösungen nicht sichtbar ist. Sie identifizieren und blockieren selbst unbekannte Malware-Familien, die Domänennamen für infizierte Hosts generieren und versuchen, Befehls- und Kontroll-Server zu kontaktieren.

SI hat Grenzen

SI-Lösungen verknüpfen zwar Daten miteinander, die vorher nicht in Beziehung standen, liefern eine Gesamtsicht der Bedrohungen und ermöglichen, in Echtzeit Abwehrmaßnahmen zu treffen und laufend zu verfeinern, ein Allheilmittel sind sie aber nicht. Security Intelligence allein reicht nicht aus, um Unternehmen sicher zu machen.


Foto: T-Systems

„Ohne sinnvolle und effiziente Suchregeln für wirklich wichtige Auffälligkeiten nützt die beste Monitoring-Technik nichts. Hier kommt auch maschinelles Lernen zum Einsatz."

Dirk Backofen
Leiter Telekom Security
www.t-systems.com

„Security Intelligence wird nur erfolgreich sein, wenn die Lösung in eine umfassende Security-Strategie und entsprechende Sicherheitsrichtlinien eingebettet ist. Firmen müssen zuvor ihre Daten klassifizieren und dann die Risiken analysieren. Aus der Risikobewertung heraus erfolgt meist die Security-Strategie mit unterschiedlichen Maßnahmen und Abwehrlinien inklusive einer Schulung der Mitarbeiter. Hier sehen wir unterschiedliche Reifegrade in den Unternehmen", sagt Ralf Gehrke von Akamai.

Oliver Tavakoli, Chief Technology Officer bei Vectra Networks, weist auf weitere Fallstricke wie die niedrige Datenqualität und die hohe Komplexität der multidimensionalen SI-Lösungen hin: „Deshalb fällt es oft schwer, dem Endanwender wirklich verständlich zu machen, warum die Systeme beispielsweise ein bestimmtes Event als verdächtig einstufen und ein anderes nicht." Ein denkbares Risiko beim Einsatz sieht er zudem darin, dass „besonders ausgefuchste Angreifer möglicherweise versuchen werden, ihr Vorgehen auf die Erkennungsstrategien der Lösungen abzustimmen

und die Daten zu kontaminieren, aus denen die Systeme ihre Schlüsse ziehen."

Der Mensch bleibt wichtig

Eine spannende Frage ist auch, inwieweit SI-Lösungen fehlendes Wissen der Mitarbeiter kompensieren können. Für Jochen Rummel, Regional Director DACH bei FireEye, ist die Antwort eindeutig: „Mit Security Intelligence alleine lässt sich kein fehlendes Know-how der Mitarbeiter ausgleichen. Technologie sollte CISOs oder IT-Sicherheitsteams die Arbeit erleichtern, ihnen Sichtbarkeit in ihrem Netzwerk geben, Alerts priorisieren, um sie zu befähigen, eine schnelle Response durchzuführen. Es geht darum, Prozesse zu vereinfachen und zu automatisieren – aber auch darum, erfahrene Security-Analysten zu haben. Die Expertise eines erfahrenen Analysten ist kaum zu ersetzen: Am Ende verstehen Menschen andere Menschen immer noch am besten."

Foto: FireEye

„Die Expertise eines erfahrenen Analysten ist kaum zu ersetzen. Am Ende verstehen Menschen andere Menschen immer noch am besten."

Jochen Rummel
Regional Director DACH
bei FireEye
www.fireeye.de

Ein Urteil, dem im Kern alle befragten Experten zustimmen. Für Marc Fliehe, Bereichsleiter Information Security beim Branchenverband Bitkom, senken Security-Intelligence-Lösungen zwar das Risiko durch „normale" Mitarbeiter aus den Fachbereichen oder bieten einen Mehrwert, wenn im Unternehmen selbst nur geringe Security-Expertise vorhanden ist. „In der Firma selbst muss aber die Kompetenz und Erfahrung vorhanden sein, ob ich mich auf diese Daten und Treffer der Maschine verlassen kann. Es geht darum, die Güte und Qualität der Lösung bewerten zu können. Ist das ein falscher Alarm? Reicht die vorgeschlagene Maßnahme aus?"

Marc Fliehe sieht in Security-Intelligence-Lösungen letztlich ein gutes Mittel zur Unterstützung der Security-Verantwortlichen, das allerdings das Risikomanagement und menschliches Know-how nicht ersetzen kann. Er hält die Cyberkriminellen für kreativ genug, Bedrohungen zu entwickeln, die auch die Maschinen nicht erkennen können – zumal ja auch aus neuen Anwendungen neue Muster entstünden. „Es kann sein, dass ein bestimmtes Kommunikationsverhalten im Netz aus einer neuen Business-Aktivität resultiert und nicht durch einen Angriff erklärt werden kann. Dieses Wissen haben ausschließlich die Mitarbeiter, eine Security-Intelligence-Lösung kann sich das wohl auch mit Künstlicher Intelligenz nicht selbstständig erschließen." ■

Jürgen Mauerer/js
js@com-professional.de