April 2016

Kognitive Sicherheit

Bessere Abwehr von Hackerangriffen mit Sicherheitsfunktionen, die verstehen, Schlüsse ziehen und lernen

Inhalt

Die neue Notwendigkeit

Fast 100 Jahre lang wurden Computer so programmiert, dass sie bei der Lösung komplexer Probleme helfen. Wir können jetzt Wetterbedingungen simulieren, Genomsequenzen darstellen und Daten umgehend weltweit gemeinsam nutzen. Aber Computer sind immer noch nicht in der Lage, für den Menschen alltägliche Dinge zu bewältigen – ein Bild erkennen, ein Buch lesen oder ein Gedicht interpretieren. Herkömmliche Systeme können das nicht leisten.

Dasselbe gilt für die Sicherheit. Jahrzehntelang wurden Computer so programmiert, dass sie Viren, Malware und das Ausnutzen von Sicherheitslücken erkennen. Sie werden kontinuierlich optimiert, damit sie präziser arbeiten. Das reicht aber nicht aus. Hacker verändern ständig ihre Vorgehensweise bei Angriffen und finden kreative Möglichkeiten, um Schutzmaßnahmen zu überwinden. Unternehmen müssen in der Lage sein, selbst kleinste Veränderungen bei Aktivitäten zu erkennen und mit so viel Kontextinformationen wie möglich zu analysieren, um neue Sicherheitsbedrohungen unterscheiden und beseitigen zu können.

80 %
der weltweiten Daten waren bisher unsichtbar.

Bis jetzt.

Die Voraussetzung für das Erkennen von Angriffen und ungewöhnlichen Verhaltensweisen, bevor diese Schäden anrichten können, sind eine dauerhafte Überwachung und die optimale Nutzung von Daten. Weltweit werden allerdings täglich über 2,5 Quintillionen Bytes an Daten generiert. Bei 80 Prozent davon handelt es sich um unstrukturierte Daten. Das heißt, sie werden in natürlicher Sprache ausgedrückt (gesprochen, geschrieben oder visuell), die ein Mensch im Gegensatz zu herkömmlichen Sicherheitssystemen problemlos verstehen kann. Täglich werden Tausende von Beiträgen in Sicherheitsblogs mit detaillierten Informationen über Sicherheitsbedrohungen veröffentlicht. Sicherheitsanalysten können aber unmöglich mit allen darin enthaltenen Zusammenhängen vertraut sein und herkömmliche Sicherheitsfunktionen können diese Erkenntnisse nicht wie ein Analyst analysieren und anwenden.

Aus diesem Grund werden zur Lösung der dringendsten Sicherheitsprobleme weiterhin Personen benötigt, die fundierte Entscheidungen darüber treffen, welche Punkte bearbeitet werden sollen und wobei es sich um einen falschen Alarm handelt. Die besten Sicherheitsexperten erweitern ihr Wissen täglich durch Erfahrungswerte, Gespräche mit Kollegen, die Teilnahme an Konferenzen und indem sie sich über Forschungsergebnisse auf dem Laufenden halten.

Bei IBM® Security entwickeln wir eine neue Generation von Systemen, die in der Lage sein sollen, sich ständig weiterentwickelnde Sicherheitsbedrohungen zu verstehen, Schlüsse daraus zu ziehen und dazu zu lernen. Wir integrieren inzwischen Sicherheitsinstinkte und Fachwissen in neue Sicherheitsmaßnahmen, bei denen Forschungsberichte, Web-Text, Daten über Sicherheitsbedrohungen und andere sicherheitsrelevante strukturierte und unstrukturierte Daten analysiert werden, d. h. die alltäglichen Aufgaben von Sicherheitsexperten – allerdings in einem bisher nicht erreichten Umfang. Das ist der zentrale Aspekt der kognitiven Sicherheit.

Dies führt dazu, dass Analysten auf kognitive Systeme zurückgreifen, um ihr Wissen über eine Sicherheitsbedrohung auszuweiten und sogar zu automatisieren. Analysten erhalten dadurch mehr Informationen über die neuesten Angriffe und werden spürbar entlastet, sodass sie sich auf andere drängende Probleme konzentrieren können.

Was ist kognitive Sicherheit?

Bei kognitiven Systemen handelt es sich um selbstlernende Systeme, die Funktionen für Data-Mining, maschinelles Lernen, die Verarbeitung natürlicher Sprache und Interaktionen zwischen Mensch und Computer nutzen, um das menschliche Gehirn nachzuahmen.

Kognitive Sicherheit ist die Implementierung von zwei umfassenden und zusammenhängenden Funktionen:

- Die Verwendung von kognitiven Systemen zur Analyse von Sicherheitstrends und zur Umwandlung riesiger Mengen an strukturierten und unstrukturierten Daten in Informationen und schließlich in verlässliches Wissen, um die Grundlagen für kontinuierliche sicherheitsspezifische und geschäftliche Verbesserungen zu schaffen
- Die Verwendung automatisierter, datengesteuerter Sicherheitstechnologien, -verfahren und -prozesse, die kognitive Systeme unterstützen, die den höchsten Grad an Kontext und Genauigkeit aufweisen

Von der Compliance zu kognitiven Funktionen

Die Sicherheitstechnologie wurde seit den ersten Netzwerken und Hackern, die bald darauf folgten, weiterentwickelt, um Angriffe abzuwehren. Bislang gab es im Zusammenhang mit der Cybersicherheit zwei verschiedene Zeitalter: Perimeterkontrollen und Security Intelligence. Sie dienen als Grundlage auf dem Weg in das dritte Zeitalter, die kognitive Sicherheit.

Perimeterkontrollen: Sicherheit, die einschränkt (bis 2005)

Zu Beginn wurden statische Sicherheitsmaßnahmen angewendet, um den Datenfluss zu schützen oder zu begrenzen, z. B. durch Firewalls, Antivirus-Software und Web-Gateways. Nach der Weiterentwicklung der Informationssicherheit im Unternehmen galt es zunächst, gesetzliche Bestimmungen einzuhalten. Das Ziel war es, den Zugriff auf vertrauliche Informationen mithilfe von Kennwörtern und einer Reihe von Strategien zur Zugriffssteuerung zu verhindern und einzuschränken. Das Bestehen eines Audits galt bereits als Erfolg. Die Perimetermaßnahmen werden zwar weiterhin verwendet, reichen aber für die Systemumgebungen von heute nicht mehr aus.

Security Intelligence: Sicherheit, die bei Überlegungen hilft (ab 2005)

Im Lauf der Zeit wurden fortschrittliche Überwachungssysteme entwickelt, die riesige Datenmengen sammeln und durchsuchen können, um Sicherheitslücken zu entdecken und potenzielle Angriffe zu priorisieren. Aufgrund dieses Wandels hat sich das Hauptaugenmerk auf Echtzeitinformationen zur Erkennung verdächtiger Aktivitäten gerichtet. Security Intelligence ist heutzutage die Sammlung, Normalisierung und Analyse von strukturierten Daten in Echtzeit, die von Benutzern, Anwendungen und Infrastrukturen generiert werden.

Security Intelligence-Lösungen verwenden Analysen, um Abweichungen von regelmäßigen Mustern zu erkennen, Veränderungen bei Netzwerkübertragungen zu entdecken und Aktivitäten zu ermitteln, die die definierten Grenzwerte überschreiten. Analysen werden in einer Security Intelligence-Infrastruktur für riesige Datenmengen angewendet, um Erkenntnisse über Unternehmensdaten im Kontext zu gewinnen und alltägliche Aktivitäten zu priorisieren. Durch die Bestimmung, welche Abweichungen bedeutsam sind, können Security Intelligence-Lösungen nicht nur dazu beitragen, Beeinträchtigungen schneller zu erkennen, sondern auch die Zahl falsch-positiver Ergebnisse zu verringern, um Zeit und Ressourcen einzusparen.

Kognitive Sicherheit: Sicherheit, die große Datenmengen versteht, Schlüsse zieht und lernt (ab 2015)

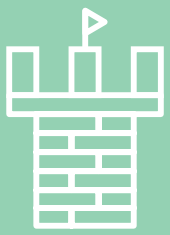
Kognitive Sicherheit basiert auf Security Intelligence-Funktionen, die Big Data-Analysen nutzen. Sie ist durch eine Technologie gekennzeichnet, die in der Lage ist, zu verstehen, Schlüsse zu ziehen und zu lernen. Mithilfe kognitiver Systeme kann jetzt in weitaus größerem Umfang auf relevante Sicherheitsdaten zugegriffen werden. Diese Systeme können 80 Prozent der heutzutage unstrukturierten Daten (z. B. geschriebene und gesprochene Sprache) verarbeiten und interpretieren.

Nach der Verarbeitung von grundlegendem Wissen, das von Experten für ein bestimmtes Thema strukturiert wird, werden kognitive Sicherheitssysteme mithilfe einer Reihe von Frage-Antwort-Paaren „geschult“. Das „Wissen“ des Systems wird anschließend durch Interaktionen von Sicherheitsexperten mit dem System ausgeweitet. Sie liefern Feedback zur Genauigkeit der Antworten des Systems. Ein wesentlicher Unterschied besteht darin, dass ein kognitives System neue Informationen in der Geschwindigkeit versteht und verarbeitet, die die menschlichen Fähigkeiten bei Weitem überschreitet. Technische Sicherheitsmaßnahmen können jetzt geschult werden, um täglich Tausende von Forschungsberichten, Konferenzmaterialien, wissenschaftliche Arbeiten, Presseartikel, Blogbeiträge und Branchenmitteilungen zu analysieren.

Da kognitive Systeme Ereignisse und Verhaltensweisen dauerhaft beobachten, um das Gute vom Schlechten unterscheiden zu können, verbessert sich die Fähigkeit, integrierte Sicherheitsmaßnahmen zur Abwehr neuer Sicherheitsbedrohungen immer weiter. Kognitive Sicherheit trägt dazu bei, dass Sicherheitsanalysten effektiver arbeiten und neue Sicherheitsbedrohungen schneller bekämpft werden können. Dadurch wird der derzeitige Mangel an Fachleuten im Sicherheitsbereich behoben und es wird ein höheres Maß an Vertrauen und Risikokontrolle erreicht (siehe Abbildung 1).

Entwicklungen im Sicherheitsbereich

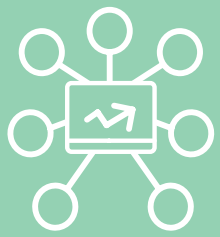
Perimeterkontrollen



Bis 2005

- Statische Sicherheits-maßnahmen
- Kennwortschutz
- Fokus auf Compliance
- Erfolg = Bestehen eines Audits

Security Intelligence



Ab 2005

- Überwachung von Echtzeitaktivitäten
- Fokus auf Abweichungen von bekannten Mustern
- Fähigkeit zur Priorisierung potenzieller Sicherheits-bedrohungen
- Reaktiv und regelbasiert

Kognitive Sicherheit

Ab 2015

- Rückschlüsse, die die menschliche Denkweise simulieren
- Fähigkeit zur Analyse strukturierter und unstrukturierter Daten, um Verhaltensweisen und Bedeutungen zu verstehen
- Automatisiertes Lernen basierend auf kontinuierlichen Informationen über Sicherheitsbedrohungen
- Proaktiver Fokus mithilfe von Beziehungen und Empfehlungen

Abbildung 1

Kognitive Lösungen beeinflussen letztendlich ein Framework, das auf den Grundlagen herkömmlicher Sicherheitsfunktionen basiert. Security Intelligence verschwindet nicht, denn es ist ein wesentliches Element von kognitiven Sicherheitslösungen. Kognitive Funktionen bieten uns die Möglichkeit, Informationen und die Erkennung von Sicherheitsbedrohungen auszuwählen und verlässliche Informationen so schnell und umfangreich wie nie zuvor zu liefern.

Abbildung 2

Da Security Intelligence-Lösungen und Big Data-Analysen traditionell unstrukturiert sind, sorgen kognitive Funktionen für ein wichtiges zusätzliches Maß an Wissen über Vorgänge und mögliche Gegenmaßnahmen. Mit diesem Spektrum an Möglichkeiten können Sie Ihre Sicherheitsumgebung optimal schützen (siehe Abbildung 2).

Das kognitive Sicherheitsniveau

Herkömmliche, programmierbare Sicherheitssysteme reagieren auf Anforderungen, machen Festlegungen und analysieren Daten entsprechend vordefinierter Parameter. Kognitive Systeme interpretieren Daten, erweitern ihre Wissensbasis mit nahezu jeder Interaktion, wägen Wahrscheinlichkeiten basierend auf einem Grad von Erkenntnissen ab und helfen Ihnen, Maßnahmen auf der Grundlage von Überlegungen zu relevanten Variablen durchzuführen.

Während die derzeitige Generation der Systeme reaktiv funktioniert, sind kognitive Sicherheitsfunktionen bei der Erkennung und Reaktion auf Unregelmäßigkeiten oder Hackerangriffen proaktiv. Kognitive Systeme sind zukunftsorientiert und dauerhaft Multitasking-fähig, suchen nach Sicherheitslücken, stellen Verbindungen her, erkennen Abweichungen und durchsuchen Milliarden von Ereignissen, um eine verlässliche Wissensbasis aufzubauen.

Kognitive Lösungen generieren nicht nur Antworten, sondern Hypothesen, evidenzbasierte Rückschlüsse und Empfehlungen. Heute können 80 Prozent der unstrukturierten Daten interpretiert werden, auf die die vorhandenen Systeme bisher nicht zugreifen konnten – und mit strukturierten Daten aus unzähligen Quellen und Standorten integriert werden. In einer globalen Wirtschaft, in der ein geschäftlicher Nutzen immer häufiger aus Informationen entsteht, stellen Daten einen der weltweit am häufigsten vorhandenen, wertvollsten und komplexesten Rohstoff dar. Wir haben jetzt die Möglichkeit, sowohl strukturierte als auch unstrukturierte Daten zu durchsuchen und kontinuierlich Features und Muster zu extrahieren, um in Echtzeit Zusammenhänge für fundierte Entscheidungen zu liefern.

Die folgenden drei Grundsätze der kognitiven Sicherheit haben sich angesichts der unglaublich schnellen Dynamik menschlicher Denkstrukturen bewährt:

1. **Verstehen** und sinnvolles Darstellen unstrukturierter Daten und Texte in natürlicher Sprache. Das schließt die Fähigkeit zur Verarbeitung von Informationen durch das „Lesen“ von Büchern, Berichten, Blogs und relevanten Branchendaten, das „Erkennen“ von Bildern und das „Hören“ natürlicher Sprache im zugehörigen Kontext mit ein.
2. **Schlüsse ziehen** basierend auf der Fähigkeit zur Interpretation und Organisation von Informationen, Erläuterungen zur Bedeutung und Begründungen für Schlussfolgerungen.
3. Kontinuierliches **Lernen** bei der Sammlung von Daten und der Ableitung von Erkenntnissen aus Interaktionen.

Tiefere Einblicke, mehr Erkenntnisse

Ein zielgerichteter Fokus auf die Erkennung von Malware, böswilligen Sicherheitsbedrohungen, Sonderfällen und Unregelmäßigkeiten kann zu übermäßig vielen falsch-positiven Ergebnissen führen. Das ist der Vorteil eines multidimensionalen Umfelds, in dem kognitive Systeme arbeiten.

Im heutigen Geschäftsumfeld ist die Fähigkeit zur Unterscheidung zwischen Schwarz und Weiß nur ein Aspekt des erforderlichen Know-hows für eine integrierte Sicherheitsinfrastruktur. Die Grauzonen werden immer größer, und an dieser Stelle bieten sich kognitive Funktionen als Lösung an.

Kognitive Systeme weisen ein höheres Maß an Intuition, Intelligenz und Verständnis auf. Sie sind so konzipiert, dass sie ständig mithilfe von Daten erweitert werden, um akzeptable Verhaltensweisen von geringfügigen Veränderungen unterscheiden zu können, die möglicherweise auf neue Sicherheitsbedrohungen hinweisen. Dadurch ergeben sich eine umfassendere Perspektive und ein proaktiver Fokus auf das Gesamtbild.

Den Mangel an qualifizierten Fachleuten beseitigen

Nicht nur unsere Systeme müssen bei den heutigen Sicherheitsumgebungen auf dem neuesten Stand bleiben, auch die Mitarbeiter müssen einige Herausforderungen bewältigen. Die Zahl der unbesetzten Stellen im Bereich Informationssicherheit weltweit wird auf 208.000 geschätzt. Es wird erwartet, dass diese Zahl bis zum Jahr 2020 auf 1,5 Mio. steigt. Kognitive Sicherheit bietet sich als Lösung an.

Kognitive Systeme dienen als skalierbares Hilfsmittel zur Unterstützung menschlicher Fähigkeiten. Sie eignen sich hervorragend als Erweiterung in häufig unterbesetzten Sicherheitsabteilungen. Diese neue Dimension ist besonders wichtig, denn heutzutage reicht es nicht mehr aus, die Vorgänge auf den eigenen Systemen genau zu überwachen. Sicherheitsbedrohungen müssen global überwacht werden, um auf potenzielle Hackerangriffe vorbereitet zu sein. Kognitive Systeme können auf Netzwerke für den globalen Austausch zurückgreifen, die pro Sekunde Hunderttausende von Sicherheitsereignissen für Tausende von Kunden auf der ganzen Welt analysieren.

Kognitive Funktionen können die Arbeit von Sicherheitsanalysten vereinfachen, denn sie ermöglichen eine am Menschen orientierte Kommunikation, z. B. erweiterte Darstellungen, interaktive Analysen von Sicherheitslücken, Risikobewertung, Fehlerbehebung und mögliche Zuordnungen. Kognitive Systeme sind in der Lage, Unregelmäßigkeiten und Fehler in der Logik zu erkennen und liefern evidenzbasierte Rückschlüsse. Analysten können dadurch alternative Ergebnisse abwägen und die Entscheidungsfindung verbessern.

Anwendungsfälle:

Das Potenzial kognitiver Lösungen

Mehr Möglichkeiten für Analysten im SOC

Kognitive Systeme können große Mengen an strukturierten und unstrukturierten Daten verarbeiten, sodass junge Analysten schnell einen größeren Nutzen bieten können. Kognitive Systeme können die Verarbeitung von Informationen automatisieren, z. B. Forschungsberichte und bewährte Verfahren, um Echtzeiteingaben zu ermöglichen. Bisher ließen sich dieses Wissen und diese Erkenntnisse nur durch jahrelange Erfahrungswerte erwerben.

Schnellere Reaktion mithilfe externer Informationen

Beim nächsten Heartbleed-Bug werden in Blogs Informationen darüber veröffentlicht, wie man sich davor schützen kann. Obwohl derzeit noch keine Signatur verfügbar ist, gibt es online eine natürliche Sprache, mit der sich die Frage beantworten lässt. Kognitive Systeme können schnell ermitteln, wie man sich vor der nächsten Zero-Day-Attacke schützen kann.

Identifizierung von Sicherheitsbedrohungen mit erweiterten Analysen

Kognitive Systeme können Analysemethoden wie maschinellem Lernen, Clusterin, Graph Mining und Entity Relationship-Modellen zur Identifizierung potenzieller Sicherheitsbedrohungen verwenden. Sie können dazu beitragen, die Erkennung riskanter Verhaltensweisen von Benutzern, die Daten-Exfiltration und die Erkennung von Malware zu beschleunigen, bevor Schäden auftreten.

Höhere Anwendungssicherheit

Kognitive Systeme können den semantischen Zusammenhang Ihrer Analysen und Daten verstehen und dabei Code und Codestrukturen untersuchen. Sie können Tausende von Ergebnissen zu Sicherheitslücken zu einigen wenigen verlässlichen Aussagen zusammenfassen. Außerdem werden die Stellen im Code aufgezeigt, an denen die Fehler behoben werden können.

Weniger Risiken im Unternehmen

Künftig können kognitive Systeme Interaktionen, die Merkmale dieser Interaktionen und deren Anfälligkeit analysieren, um Risikoprofile für Unternehmen, unternehmensweite Maßnahmen, Schulungen und Umschulungen zu entwickeln. Kognitive Systeme können die Verarbeitung natürlicher Sprache verwenden, um vertrauliche Daten im Unternehmen zu ermitteln und zu bearbeiten.

Die Zukunft: Wirtschaftliche Aspekte durch Cyberkriminalität umkehren

Kognitive Systeme können Features oder Merkmale aus enorm vielen böswilligen Softwareprodukten (Malware) analysieren, um selbst kleinste Gemeinsamkeiten zu erkennen. Der Grund, warum dies besonders wichtig ist, ist folgender: die Vielfalt böswilliger Softwareprodukte ist riesig und kriminelle Gruppen entwickeln den zugehörigen Code ständig weiter. Viele Malware-Produkte, die heute in Umlauf sind, hängen eigentlich mit anderer Malware zusammen. Mit kognitiven Systemen können Tausende von Features einer verdächtigen ausführbaren Datei analysiert und zusammengefasst werden, um Muster zu ermitteln. Das System kann Muster identifizieren, mit dem Sie neue Malware-Varianten erkennen und klassifizieren können, ohne zu wissen, um welche Features es sich handelte bzw. wie oder warum sie zugeordnet wurden.

Da die Cognitive Security Community wächst und die Funktionsfähigkeit neuer Angriffe abnimmt, konzentrieren sich Cyberkriminelle künftig auf neue wirtschaftliche Rahmenbedingungen. Maßnahmen zur Entwicklung von Malware, die nicht erkannt werden kann, wird zunehmend komplexer und kostspieliger. Nach den Ergebnissen der Cost of Data Breach Study 2015 des Ponemon Institute dauert es in Unternehmen durchschnittlich 256 Tage, bis hochentwickelte dauerhafte Sicherheitsbedrohungen erkannt werden. Die durchschnittlichen Kosten aufgrund von Datenschutzverletzungen liegen in den USA bei 6,5 Mio. USD. Kognitive Sicherheit bietet Sicherheitsanalysten das nötige Funktionsspektrum, um frühzeitige Warnhinweise auf potenzielle Hackerangriffe suchen zu können und die Erkennung spürbar zu beschleunigen. Für Cyberkriminelle zahlen sich Angriffe immer schwieriger aus.

Cognitive Computing trägt zu einem umfassenden Wandel bei, da nicht nur Daten, sondern auch Bedeutungen, Kenntnisse, Prozessabläufe und der Fortschritt von Aktivitäten genutzt werden – mit unglaublich großer Geschwindigkeit und Reichweite. Unternehmen, die mit kognitiven Funktionen arbeiten, können sich dadurch erhebliche und weit reichende Wettbewerbsvorteile verschaffen.

Integration und Fachwissen für ein kognitives Netzwerk

Integration und Fachwissen sind für das Erreichen eines hohen Sicherheitsniveaus von entscheidender Bedeutung. Zu viele Sicherheitsprodukte basieren auf einer Sammlung von Einzelprodukten, die nicht integriert sind und nicht die Transparenz und verlässlichen Informationen liefern, die Ihr Unternehmen benötigt, um schnell reagieren zu können.

Die Integration ist erst dann umfassend, wenn die Funktionen untereinander in der hybriden IT-Umgebung, über die Unternehmensgrenzen hinaus und im gesamten Kontaktnetzwerk interagieren und kommunizieren können. Durch die richtige Integration erreicht Ihr Unternehmen die nötige Transparenz, um schnell auf Sicherheitsereignisse bei deren Auftreten reagieren zu können. Die Integration ermöglicht Ihnen, mehr Aufgaben mit weniger Mitteln zu bewältigen. Dies ist ein grundlegender Weg, um den Mangel an Fachleuten im Sicherheitsbereich zu beseitigen.

Täglich werden neue Sicherheitsbedrohungen entdeckt. Das bedeutet, Fachwissen im Sicherheitsbereich und der Austausch von Informationen über Sicherheitsbedrohungen sind besonders wichtig. Wenn in Ihrem Unternehmen kein erstklassiges Fachwissen vorhanden ist, das in Lösungen und kognitive Funktionen einfließt, kann es schnell ins Hintertreffen geraten. IBM X-Force Exchange katalogisiert derzeit Informationen über mehr als 88.000 Sicherheitslücken, über 25 Mrd. Webseiten und Daten von 100 Mio. Endpunkten. Damit werden die Grundlagen für Echtzeitkenntnisse und die globale Abdeckung von Fachwissen geschaffen, auf das unmittelbar zugegriffen werden kann.

Unterstützung durch IBM

Der Wandel hin zu kognitiven Lösungen hat gerade erst begonnen, IBM hat aber das nötige Potenzial an geistigem Eigentum und Finanzkraft, um bei dieser Entwicklung im Sicherheitsbereich eine führende Rolle einzunehmen. Über 7.500 IBM Sicherheitsexperten in 36 Security Centern auf der ganzen Welt überwachen täglich 133 Länder und 35 Mrd. Ereignisse. IBM investiert bereits seit Jahrzehnten in kognitive Technologien und kann auf erhebliche Fortschritte in den letzten fünf Jahren verweisen: die Möglichkeit zur Verarbeitung natürlicher Sprache, zur Verarbeitung von Sprach- und Bilddaten und zur Umwandlung unstrukturierter Daten in Tools wie Knowledge Graphs, die auf einfache Weise abgefragt werden können. IBM setzt auf kognitive Lösungen zur kontinuierlichen Erweiterung von Anwendungsfällen im Sicherheitsbereich und zur Weiterleitung dieser Informationen zurück zu den Sicherheitsanalysten.

IBM Security hat bereits heute kognitive Funktionen in Lösungen zur Verfügung. Funktionen für maschinelles Lernen werden verwendet, um die Genauigkeit bei der Ermittlung von Sicherheitslücken zu erhöhen und diese zu priorisieren, damit Ihr Unternehmen deutlich schneller reagieren kann. Funktionen für verhaltensbezogenes Lernen werden verwendet, um Unregelmäßigkeit im Zusammenhang mit Sicherheitsbedrohungen, die im Netzwerk auftreten, proaktiv vorherzusehen und festzustellen.

IBM Security bietet durchgängigen Schutz und ein Immunsystem, das detaillierte Analysen, Identität und Zugriff, komplexe Betrugsfälle, Daten, Anwendungen, Netzwerk, Endpunkte, Cloud, mobile Lösungen und Forschungen umfasst. Auf jeder dieser Plattformen ergeben sich Vorteile durch die kognitiven Funktionen von IBM. Wenn Sie an den Vorteilen kognitiver Sicherheitslösungen interessiert sind, ziehen Sie die Einführung von IBM Plattformen in Betracht, die mithilfe kognitiver Technologien erneuert und erweitert werden.

3 unmittelbare Schritte

1. Weitere Informationen über die Verwendung kognitiver Funktionen zur Beseitigung von Sicherheitsbedrohungen.

2. Entwicklung einer Roadmap für ein höheres Sicherheitsniveau als Vorbereitung für die Umstellung auf kognitive Lösungen.

3. Förderung der Integration in die vorhandene Sicherheitsinfrastruktur.

Weitere Informationen

Bitte wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter: ibm.biz/cognitivesec

Über IBM Security

IBM Security bietet eines der innovativsten und am besten aufeinander abgestimmten Portfolios mit Sicherheitsprodukten und -services für Unternehmen. Das Portfolio, das durch die weithin bekannte Forschungs- und Entwicklungsgruppe IBM X-Force unterstützt wird, bietet die notwendige Security-Intelligence, um Unternehmen beim umfassenden Schutz von Personen, Infrastrukturen, Daten und Anwendungen zu unterstützen. Erreicht wird dies durch die Bereitstellung von Lösungen für Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Diese Lösungen unterstützen Unternehmen beim erfolgreichen Risikomanagement und bei der Implementierung integrierter Sicherheit für mobile, Cloud-, Social Media- und andere Geschäftsarchitekturen. IBM betreibt eine der weltweit größten Einrichtungen für die Erforschung, Entwicklung und Bereitstellung von Sicherheitstechnologien, überwacht täglich ca. 15 Milliarden Sicherheitsereignisse in 133 Ländern und besitzt mehr als 3.700 Patente im Bereich Sicherheitstechnologie.

Finanzierungslösungen von IBM Global Financing können Ihnen bei der kosteneffizienten und strategisch richtigen Anschaffung von Softwarefunktionalität für Ihr Unternehmen helfen. Wir arbeiten bei der Ausarbeitung einer auf Ihre Geschäfts- und Entwicklungsziele abgestimmten Finanzierungslösung mit bonitätsgeprüften Kunden zusammen, um für Sie eine effektive Finanzdisposition und eine Reduzierung der Gesamtbetriebskosten zu erreichen. Finanzieren Sie Ihre kritischen IT-Investitionen und bringen Sie Ihr Unternehmen nach vorne mit IBM Global Financing. Weitere Informationen finden Sie unter: ibm.com/financing

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
Germany
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

SEW03134-DEDE-00