Case Study

DZ BANK ermöglicht Schutz ohne die Privatsphäre zu verletzten – durch KI-gestützte Früherkennung von Cyberangriffen

„Klassische Präventionssysteme wie Firewalls und Intrusion-Detection-/Prevention-Systeme decken keine fortschrittlichen persistenten Bedrohungen oder anomales Verhalten im Netzwerk ab“, erklärt Matthias Tauber, Senior Services Manager für IT-Sicherheit bei der DZ BANK, die als Zentralinstitut für mehr als 900 Genossenschaftsbanken in Deutschland fungiert.

„Signaturbasierte Systeme erkennen nur das, was sie wissen, und das, was sie verpasst haben, bleibt unsichtbar“, erläutert er. „Wir wollten von einer herkömmlichen zu einer neuen Technologie wechseln.“ Tauber und sein Team suchten nach einer Lösung der neuen Klasse KI-gestützter Netzwerkverkehrsanalyse, um versteckte Cyberangriffe zu erkennen und Bedrohungen schneller zu stoppen.

Erreichen von Sicherheit und Datenschutz

Die DZ BANK ist mit 506 Milliarden Euro Bilanzsumme im Jahr 2017 die zweitgrößte Bank deutschlandweit. Genossenschaftsbanken betreuen die vielen kleinen und mittleren Unternehmen (KMU) in Deutschland. Als ihr zentrales Kreditinstitut stärkt die DZ BANK deren Geschäft und bietet Zugang zu den Kapitalmärkten. Sie bietet Privatkunden, Firmenkunden und institutionellen Kunden Bankdienstleistungen an. Die Bank beschäftigt 30.000 Mitarbeiter in Europa, Asien und den USA. Die Mission von Tauber, die Vermögenswerte, den Geschäftsbetrieb und sensible Informationen der Bank zu schützen, wird durch ein breites Spektrum an Datenschutz- und Finanzbestimmungen erschwert. So ist in Deutschland der Einsatz vieler Monitoring-Techniken ebenso verboten wie die elektronische Überwachung von Mitarbeitern und deren Kommunikation.

Betriebsräte vertreten die Arbeitnehmer vor Ort oder von einer höheren Ebene aus, was sich auch auf die Cybersicherheit und den Datenschutz der DZ BANK auswirkt. Darüber hinaus sind 2018 sowohl die Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO) als auch die zweite Richtlinie über Märkte für Finanzinstrumente (MiFID II) in Kraft getreten.

VECTRA®
Security that thinks®

Unternehmen

DZ BANK

Branche

Finanzdienstleistungen

Herausforderung

- Erkennung von fortschrittlichen Bedrohungen, die von herkömmlichen signaturbasierten Firewalls, IDS und IPS übersehen werden.
- Unterscheidung zwischen gutartigem anomalem Verhalten und risikoreichem Angriffsverhalten.

Auswahlkriterien

Eine benutzerfreundliche Plattform zur Analyse des Netzwerkverkehrs, die die Zeit zur Erkennung von Bedrohungen verkürzt, automatisch Warnmeldungen auslöst und die Reaktion auf Vorfälle beschleunigt.

Ergebnisse

- Erkennung von versteckten Angreifern in Rechenzentren sowie Benutzer- und IoT-Geräten unter Einhaltung strenger Datenschutzgesetze.
- Reduzierung des Risikos durch Insider-Bedrohungen und Verstöße gegen IT-Administrationsrichtlinien.
- Reduzierung des Arbeitsaufwands für Sicherheitsoperationen durch KI-gesteuerte Bedrohungserkennung und schnellere Reaktion auf Vorfälle.

Sicherheitslücken identifizieren

Im Rahmen der Bemühungen der Bank, ihre Cybersicherheit kontinuierlich zu verbessern, haben Tauber und sein Team die Sicherheitslage der Finanzinstitution mit dem NIST Cybersecurity Framework verglichen.

„Wir haben festgestellt, dass wir eine Lücke bei der Erkennung fortschrittlicher persistenter Bedrohungen und Anomalien im Netzwerk haben“, so Tauber. Um diese Lücke zu schließen, entschied sich die DZ BANK für die KI-gestützte Cyberangriffserkennungs- und Bedrohungssuchplattform Cognito® von Vectra®. Cognito ermöglicht es der DZ BANK, Bedrohungen in Echtzeit zu erkennen, automatisch Warnmeldungen auszulösen und schnell auf versteckte Angreifer in Rechenzentren sowie Benutzer- und IoT-Geräten zu reagieren. Cognito kombiniert menschliches Fachwissen mit einem breiten Spektrum an Data Science, maschinellen Lerntechniken und Verhaltensanalysen. Die bislang manuelle, zeitaufwändige Suche und Reaktion auf Bedrohungen erfolgt automatisiert. Cognito verkürzt die Bedrohungssuche von Tagen und Wochen auf Minuten, was den Arbeitsaufwand für Sicherheitsmaßnahmen um das 36-Fache reduziert.

Bedrohungen schneller finden

Die ständig lernenden Verhaltensmodelle von Cognito erkennen Angreifer in Echtzeit, um eine schnelle, entscheidende Reaktion und einen logischen Ausgangspunkt für Untersuchungen zur Verfügung zu stellen.

„Cognito macht es möglich, dass wir uns auf die risikoreichsten Bedrohungen konzentrieren“, erklärt Matthias Tauber, Senior Services Manager für IT-Sicherheit bei der DZ BANK. „Bei anderen Lösungen muss ich erst filtern, um Hunderte oder Tausende von Fehlalarmen auszusortieren.“

Cognito testet automatisch Warnmeldungen mit Bedrohungs- und Sicherheitswerten, die im intuitiven Vectra Threat Certainty Index™ angezeigt werden. Dadurch weiß die DZ BANK sofort zuverlässig, welche Host-Geräte mit Angriffsindikatoren das größte Risiko darstellen.

Da Cognito angereicherte Netzwerk-Metadaten, relevante Protokolle und Cloud-Ereignisse analysiert, und nicht Nutzlasten oder Kommunikationsinhalte, erkennt die DZ BANK automatisch fortschrittliche Bedrohungen in Echtzeit und hält dabei strenge Datenschutzgesetze ein.

Eine koordinierte Anstrengung

„Cognito hilft uns, den Mangel an fachlich versierten personellen Ressourcen auszugleichen“, sagt Tauber. „Cognito ist einfach zu bedienen und zu verstehen, und das macht es für uns einfacher, Runbooks für das Security Operations Team zu schreiben.“ Der Frontline-Betrieb wird von einem Managed Security Service Provider durchgeführt. Tier-1- und Tier-2-Agenten nutzen Cognito, um Cyberangriffe zu erkennen und die am höchsten gefährdeten Bedrohungen für das Sicherheitsteam der DZ BANK zu eskalieren, das Cognito auch für weitere Untersuchungen einsetzt. Mit Cognito können wir Verhaltensweisen in den Grauzonen erkennen“, erklärt Tauber. „Wenn wir verdächtige Aktivitäten beobachten, können wir herausfinden, was in der Nähe des Clients passiert.“

Reduzierung des Risikos von Insiderangriffen

Die DZ BANK hat sich für Cognito entschieden, um in ihrem globalen Netzwerk fortschrittliche Bedrohungen zu erkennen und gutartige Anomalien von bösartigen Aktivitäten, also für Angreifer typischem Verhalten, zu unterscheiden. Die Lösung wurde jedoch innerhalb kurzer Zeit zu einem unverzichtbaren Instrument, um auch das Risiko von Insider-Bedrohungen zu reduzieren. Die Konten von IT-Administratoren sind für Angreifer besonders wertvoll. Im Rahmen der Sicherheitspraktiken der DZ BANK können IT-Administratoren ihre Arbeit nur von bestimmten, besonders geschützten Clients ausführen. In Eile oder Vergesslichkeit überspringen die Mitarbeiter manchmal diese Vorsichtsmaßnahmen. „Wir haben Richtlinien, dass alle Administratoren nur ihre spezifischen administrativen Clients verwenden dürfen“, sagt Tauber. „Wir benutzen Cognito, um sicherzustellen, dass sie sich an diese Vorgabe halten.“

Wenn Cognito beispielsweise Remote-Command-and-Control-Verhalten erkennt, kann dies ein Hinweis darauf sein, dass jemand vom Client eines nicht genehmigten IT-Administrators aus aktiv ist oder ein kompromittiertes Konto eingesetzt wird. Mit Cognito kann das Sicherheitsteam schnell feststellen, ob es sich um eine hochriskante Bedrohung handelt. Wenn es sich um ein internes System handelt, kann das Team herausfinden, warum der IT-Administrator die Richtlinien nicht befolgt hat.

Eine Automatisierungsreise

Tauber und sein Team treiben den Einsatz der KI-gesteuerten Lösung voran, um die Erkennung von Bedrohungen in Echtzeit zu automatisieren und die Reaktion auf Vorfälle zu beschleunigen sowie den Arbeitsaufwand für interne und externe Teams zu reduzieren. Cognito ist nun auch Teil des gut koordinierten Sicherheitsökosystems der DZ BANK. Von Cognito erfasste Ereignisse werden auch an das Security Information and Event Management (SIEM)-System Splunk veröffentlicht. Tauber erwägt nun, die Fähigkeiten der Cognito-Plattform zu erweitern, um schnellere, schlüssigere Untersuchungen von Sicherheitsvorfällen durchzuführen und rückwirkend nach verdeckten Cyberangriffen zu suchen.

VECTRA
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai