Zu Denken wie ein Angreifer

Warum Security Graphen den nächsten Schritt in der Bedrohungserkennung und -abwehr darstellen

VON DR. CHASE CUNNINGHAM (DRZEROTRUST)

Think Like An Attacker: Why Security Graphs are the Next Frontier of Threat Detection and Response

Chase Cunningham
Nokesville, VA
Chase@drzerotrust.com

Ordering Information:
Special discounts are available on quantity purchases by corporations, associations, educational institutions, and others. For details, contact Chase Cunningham above.

Printed in the United States of America

First Edition
Softcover ISBN 979-8-89940-480-1
Publisher
Winsome Entertainment Group LLC
Murray, UT

Einleitung

Cyberbedrohungen nehmen in ihrem Ausmaß und ihrer Raffinesse stetig zu und stellen Organisationen im digitalen Zeitalter vor enorme Herausforderungen. Es wird erwartet, dass die weltweite Cyberkriminalität im Jahr 2025 Schäden in Höhe von 10,5 Billionen US-Dollar verursachen wird / verursacht haben wird – ein drastischer Anstieg gegenüber 3 Billionen im Jahr 2015. Diese explosionsartige Zunahme von Cyberbedrohungen wird durch die Komplexität moderner IT-Landschaften zusätzlich noch verschärft: von lokalen Netzwerken über Cloud-Dienste bis hin zu IoT-Geräten, die täglich Milliarden von Ereignissen und Warnmeldungen generieren. Sicherheitsteams stehen vor der Aufgabe, sich durch diese dynamischen und komplexen Datenmengen zu arbeiten, um die wirklich relevanten Informationen herauszufiltern. In einem solchen Szenario wird es immer wichtiger, die Beziehungen zwischen Nutzern, Geräten, Anwendungen und Bedrohungen zu verstehen und sichtbar zu machen. Denn Angriffsmuster verbergen sich häufig genau hinter diesen Beziehungen, etwa wenn sich Malware über verbundene Maschinen ausbreitet oder ein Insider auf Systeme zugreift, für die er keine Berechtigung hat. Eine wirksame Verteidigung setzt daher voraus, diese Verbindungen zu sehen und klar zu erkennen. Graphentheorie und Linkanalyse bieten hier einen wirkungsvollen Ansatz. Die Graphentheorie – die Mathematik hinter Netzwerken – ermöglicht es, komplexe Zusammenhänge als Knoten (Nodes) und Kanten (Edges) abzubilden. Die Linkanalyse überträgt dieses Konzept auf reale Daten und visualisiert diese Beziehungen, um bislang verborgene Muster aufzudecken. Die visuelle Darstellung von Daten als ein Netzwerkdiagramm gilt heute als „die schnellste und zuverlässigste Methode, komplexe Verbindungen zu verstehen sowie versteckte Muster und Anomalien zu identifizieren“. In der Cybersicherheit bedeutet das konkret: Abstrakte Logdaten und Warnmeldungen in intuitive visuelle Netzwerkkarten überführen – also in Graphen, die Analysten dabei helfen, Angriffswege, Abhängigkeiten und Schwachstellen im Unternehmen zu erkennen. Die Fähigkeit, die „Punkte zu verbinden“ – also Zusammenhänge zwischen scheinbar getrennten Datenpunkten zu erkennen – ist für Verteidiger von unschätzbarem Wert.

Dieses Paper beleuchtet die Anwendung von Graphanalyse und graphbasierten Technologien in der Cybersicherheit aus historischer, gegenwärtiger und zukünftiger Perspektive. Es beginnt mit den Ursprüngen der Graphentheorie und ihrer frühen Nutzung durch Nachrichtendienste und in der Strafverfolgung. Anschließend wird gezeigt, wie moderne Sicherheitsteams graphbasierte Methoden einsetzen, um Netzwerke zu analysieren, Bedrohungen sowie Schwachstellen zu erkennen und Insider-Risiken aufzudecken. Ein besonderer Fokus liegt auf dem Einsatz von Graphanalyse bei der Umsetzung des Zero-Trust-Modells (einem Sicherheitsansatz, der auf den Prinzipien „Assume Breach“, „Least Privilege“ und „Continuous Verification“ basiert). Anhand realer Beispiele wird erläutert, wie Security Graphen Sicherheitskontrollen gezielt stärken können.
Darüber hinaus wird aufgezeigt, welchen strategischen Wert diese Ansätze für große Unternehmen wie auch kleine und mittlere Betriebe (KMU) haben – sei es zur besseren Skalierbarkeit, zur Einhaltung regulatorischer Anforderungen oder zur effizienten Nutzung begrenzter Ressourcen. Zum Schluss wirft das Paper einen strategischen Blick in die Zukunft: Es beleuchtet, wie graphbasierte Cybersicherheit durch KI und Machine Learning weiterentwickelt wird, welchen Stellenwert sie in Cloud- und Hybrid-Umgebungen einnimmt – und welche technischen sowie ethischen Fragen künftig an Bedeutung gewinnen. Ziel ist es, IT- und Sicherheitsexperten ebenso wie Unternehmensentscheider mit einem umfassenden Verständnis dafür auszustatten, warum Graphanalyse heute ein entscheidender Faktor für Cybersicherheit ist, wie sie aktuell eingesetzt wird und wie sie dabei helfen kann, Sicherheitsstrategien nachhaltig zu stärken.

Historischer Hintergrund der Graphanalyse

Die Wurzeln der Graphanalyse reichen über zwei Jahrhunderte zurück. Im Jahr 1736 legte der Schweizer Mathematiker Leonhard Euler mit der Lösung des berühmten Königsberger-Brückenproblems den Grundstein für

die moderne Graphentheorie. Die Frage, die ihn damals beschäftigte: Lässt sich ein Rundgang durch die Stadt Königsberg so gestalten, dass jede ihrer sieben Brücken genau einmal überquert wird? Euler bewies, dass dies unmöglich ist. Dabei führte er das Prinzip ein, Landmassen als Knoten und Brücken als Kanten zu modellieren – und erschuf damit den ersten mathematischen Graphen. Diese sogenannte „Geometrie der Lage" gilt als das erste Theorem der Graphentheorie und demonstriert, wie sich reale Probleme durch Knoten-Kanten-Beziehungen abbilden und lösen lassen.

Im 19. und 20. Jahrhundert entwickelte sich die Graphentheorie innerhalb der Mathematik weiter und fand bald Anwendung in den Sozialwissenschaften, insbesondere in der Analyse sozialer Netzwerke. Bereits Mitte des 20. Jahrhunderts kartierten Soziologen Beziehungen in kleinen Gruppen und etablierten damit den Ansatz, Graphen zur Analyse und zum Verständnis menschlicher Netzwerke einzusetzen. Diese Konzepte weckten schon bald das Interesse von Geheimdiensten und Strafverfolgungsbehörden, die darin ein leistungsfähiges Werkzeug erkannten, um kriminelle und terroristische Netzwerke sichtbar zu machen. Schon in den 1970er-Jahren begannen Polizeiermittler damit, Techniken der Linkanalyse systematisch zu nutzen. Ein Meilenstein war 1975 die Entwicklung der Anacapa-Charts durch das FBI. Dieser methodische Ansatz ermöglichte es, Personen, Organisationen und Besitzverhältnisse als Graphen auf Papier darzustellen. Ermittler erstellten auf manuelle Weise sogenannte Assoziationsmatrizen und zeichneten Verbindungsdiagramme – ein aufwändiger, aber hochwirksamer Prozess, der verborgene Zusammenhänge sichtbar machte, etwa in Drogenkartellen oder mafiösen Strukturen, die in reinen Textberichten kaum erkennbar gewesen wären.

Mit dem Fortschritt in der Computertechnik wurden diese Werkzeuge zunehmend digitalisiert. In den 1990er Jahren kamen erste Softwarelösungen wie IBM's Analyst's Notebook auf, die die Erstellung solcher Linkdiagramme teilweise automatisierten. Analysten konnten Daten eingeben und daraus automatisch Netzwerkdiagramme generieren lassen, auch wenn zur Interpretation weiterhin Fachwissen erforderlich war. Nach den Terroranschlägen vom 11. September 2001 erkannten Nachrichtendienste, dass sie entscheidende Hinweise nicht rechtzeitig miteinander verknüpft hatten. Die Fähigkeit, „die Punkte zu verbinden", rückte in den Mittelpunkt moderner Aufklärungsarbeit. In der Folge investierten Behörden massiv in graphbasierte Analysetools. Die Linkanalyse wurde zu einem zentralen Instrument der Terrorismusbekämpfung und kam bei der Kartierung von Terrorzellen, der Aufdeckung extremistischer Netzwerke und der Koordination von länderübergreifenden Ermittlungen zum Einsatz. Eine nachrichtendienstliche Überprüfung bestätigte dieses Versäumnis: Die Dienste hatten es versäumt, verstreute Hinweise zu einem zusammenhängenden Lagebild zu verknüpfen. Als Konsequenz setzten sie verstärkt auf groß angelegte, graphbasierte Systeme zur Auswertung von Kommunikationsdaten und offenen Quellen. Diese halfen, Beziehungen zwischen Zielpersonen, Kommunikationswegen und Finanzströmen zu erkennen – und Bedrohungen frühzeitig zu identifizieren.

Parallel dazu fand die Graphanalyse auch im kommerziellen Bereich immer mehr Anwendung. Das wohl bekannteste Beispiel dafür ist der von Google in den späten 1990er-Jahren eingeführte PageRank-Algorithmus, der das gesamte World Wide Web als Graph aus miteinander verbundenen Seiten modellierte. PageRank bewertete die Bedeutung einer Webseite anhand der Links (Kanten) zwischen Seiten (Knoten) und führte damit im Grunde eine Linkanalyse im Größenmaßstab des Internets durch. Dieses graphbasierte Ranking revolutionierte Suchmaschinen und demonstrierte eindrucksvoll die Leistungsfähigkeit netzwerkbasierter Analysen für Big Data.

Wenig später machten soziale Netzwerke das Konzept des Graphen allgegenwärtig. Der Erfolg von Facebook wurde maßgeblich auf die Nutzung des sogenannten „Social Graph" zurückgeführt, die visuelle Darstellung des Netzwerks menschlicher Beziehungen. Schon 2007 kommentierte ein Beobachter: „PageRank beruhte auf einem großen Graphen – den Links, die das Web ausmachen. Der nächste Durchbruch […] wird auf dem Social Graph basieren, den Verbindungen zwischen uns allen." Plattformen wie Facebook und LinkedIn bauten ganze Geschäftsmodelle darauf auf, solche Relationship Graphs zu analysieren und etwa für Freundschaftsvorschläge, Community Detection oder zielgerichtete Werbung zu nutzen. Diese breite Anwendung in der Webtechnologie machte eine ganze Generation von Ingenieuren und Analysten mit graphbasiertem Denken vertraut.

Auch der Finanzsektor erkannte früh den Mehrwert der Graphanalyse. Besonders im Bankwesen sowie bei der Betrugsbekämpfung bot sich der Graph sehr gut dazu an, das klassische „Follow-the-Money“-Prinzip effizienter umsetzen. Geldwäsche erfolgt häufig über komplexe Geflechte von Transaktionen über verschiedene Konten und Scheinfirmen. Werden verdächtige Überweisungen als Netzwerkdiagramme dargestellt, lassen sich zentrale Umschlagpunkte illegaler Aktivitäten identifizieren und die Kontrollstrukturen dahinter sichtbar machen. Graphalgorithmen helfen dabei, Schlüsselakteure in Betrugsnetzwerken zu erkennen (z.B. über Maße wie Knoten-Zentralität oder Konnektivität) und Geldflüsse durch sonst undurchsichtige Systeme nachzuverfolgen. Die Linkanalyse wurde so zu einer entscheidenden Methode für Anti-Money-Laundering-Compliance (AML) und für Betrugsabteilungen in Finanzinstituten. Sie ermöglicht es, innerhalb riesiger Transaktionsdatensätze „verborgene Beziehungen, Muster und Anomalien zu identifizieren, die auf kriminelle Aktivitäten hindeuten könnten“.

Nicht nur Banken, sondern auch andere Bereiche wie die Unternehmenssicherheit, Forensik und Ermittlungsberatung begannen, die Methoden der Geheimdienste und Strafverfolgung zu übernehmen. Tools wie i2 Analyst’s Notebook, Palantir oder Open-Source-Plattformen zur Linkanalyse wurden zum Standard für Analysten, die alles, von Insiderhandelsnetzwerken über Korruption bis hin zu Betrug in Lieferketten, untersuchten. Anfang der 2010er-Jahre hatte sich die Graphanalyse in zahlreichen Branchen etabliert – als anerkanntes Werkzeug zur Analyse komplexer, vernetzter Systeme. Damit war der Weg geebnet für den nächsten logischen Schritt: die Anwendung in der Cybersicherheit. Sicherheitsexperten erkannten zunehmend, dass moderne IT-Landschaften mit ihren komplexen Abhängigkeiten und Kommunikationspfaden – ähnlich wie soziale Netzwerke oder Finanzsysteme – durch graphbasierte Modelle wesentlich besser verstanden, analysiert und geschützt werden konnten.

Graphanalyse in der modernen Cybersicherheit

Heute zählt die Graphanalyse zu den fortschrittlichsten Methoden der Cybersicherheit. Sie hilft Verteidigern, komplexe, miteinander verknüpfte Daten zu verstehen und Bedrohungen zu erkennen, die sonst unentdeckt bleiben würden. Typischerweise wird dabei ein sogenannter „Security Graph“ aufgebaut, der die gesamte IT-Umgebung modelliert. Dabei werden alle relevanten Entitäten (z.B. Benutzer, Geräte, Anwendungen, IP-Adressen, Schwachstellen und Ereignisse) als Knoten darstellt, während die Beziehungen zwischen ihnen (z.B. Netzwerkverbindungen, Benutzerrechte, Datenflüsse) als Kanten modelliert werden. Durch gezielte Abfragen und Visualisierungen dieses Graphen erhalten Analysten einen ganzheitlichen Überblick über die Sicherheitslage und können tiefgehende Analysen durchführen.

Im Folgenden werden zentrale Anwendungsfälle vorgestellt, in denen Graphanalyse heute in der Cybersicherheit eingesetzt wird, und wie solche graphischen Visualisierungen die Sicherheitsoperationen verbessern.

Netzwerkvisibilität und Assetmanagement

Eine der grundlegendsten Anwendungen der Graphanalyse in der Cybersicherheit besteht darin, vollständige Sichtbarkeit innerhalb des Netzwerks zu schaffen. Viele Unternehmen tun sich schwer damit, ein aktuelles und vollständiges Inventar aller Geräte, Applikationen und Datenflüsse zu pflegen, insbesondere seit dem Aufkommen von Cloud-Diensten und hybriden IT-Umgebungen. Graphbasierte Mapping-Tools lösen dieses Problem, indem sie Daten aus unterschiedlichsten Quellen (z.B. Asset-Datenbanken, Cloud-APIs, Netzwerkscans) zusammenführen und daraus ein dynamisches Infrastrukturmodell erzeugen.

Der resultierende Security Graph zeigt, wie Assets miteinander verbunden und konfiguriert sind und bildet damit eine entscheidende Grundlage für ein wirksames Management der Angriffsfläche. Denn: „Es ist unmöglich, ein Cloud-Netzwerk zu schützen, wenn man nicht weiß, welche Assets existieren und wie sie miteinander verbunden sind.“ Ein Security Graph bietet eine visuelle Karte des digitalen Ökosystems eines Unternehmens – von lokalen Servern, die mit Datenbanken verbunden sind, über Cloud-Instanzen, die Storage-Buckets mit Benutzerkonten verknüpfen, bis hin zu Geräten, die diesen Nutzern zugeordnet sind. Sicherheitsteams können gezielt in bestimmte Netzwerksegmente oder Cloud-Bereiche hineinzoomen und sofort alle Knoten (Assets) und Kanten (Verbindungen) in diesem Bereich sehen. Lücken oder unbekannte Systeme werden so unmittelbar erkennbar.

Diese Sichtbarkeit ist keine starre Momentaufnahme: Graphen lassen sich nahezu in Echtzeit aktualisieren, etwa wenn neue virtuelle Maschinen erstellt oder Geräte dem Netzwerk hinzugefügt werden. Im Vergleich zu statischen CMDB-Tabellen oder Excel-Listen ist ein graphbasiertes Modell deutlich intuitiver und aussagekräftiger. Beziehungen, die sonst in verschiedenen Datensilos verborgen bleiben, werden durch den Graphen sofort erkennbar. Ein Beispiel: Eine graphische Visualisierung könnte aufzeigen, dass ein kritischer Datenbankserver durch eine übersehene Firewall-Regel nur einen Sprung vom Internet entfernt ist. Solche Erkenntnisse ermöglichen sofortiges Gegensteuern – etwa durch das Schließen dieses Pfads.

Darüber hinaus unterstützt graphbasiertes Assetmanagement auch die Erfüllung regulatorischer Vorgaben, indem es Systembeziehungen nachvollziehbar dokumentiert. So lassen sich aus dem Security Graph automatisch Karten generieren, die Datenflüsse gemäß DSGVO oder Netzwerksegmentierungen nach PCI-DSS visualisieren. Diese lassen sich als Nachweis gegenüber Auditoren verwenden und zeigen, dass die Organisation versteht und kontrolliert, wohin sensible Daten fließen. Immer mehr Sicherheitsteams sehen einen einheitlichen Asset Service Graph inzwischen als zentrale Grundlage für ihr Situationsbewusstsein.

Bedrohungserkennung und Incident Response

Über die reine Bestandsaufnahme hinaus entfaltet die Graphanalyse ihr volles Potenzial insbesondere bei der Erkennung von Bedrohungen und der Reaktion auf Sicherheitsvorfälle. Moderne Cyberangriffe verlaufen mehrstufig und möglichst unauffällig: Ein Angreifer verschafft sich per Phishing Zugang zu einem Benutzerkonto, bewegt sich durch interne Systeme, eskaliert Rechte und exfiltriert schließlich sensible Daten. Ein solches Angriffsszenario allein anhand von Logdaten nachzuvollziehen, gleicht der Suche nach mehreren Nadeln in verschiedenen Heuhaufen gleichzeitig.

Hier kommt die Graphanalyse ins Spiel: Sie kann die einzelnen Punkte einer Angriffskampagne automatisch

miteinander verknüpfen. Durch die Korrelation unterschiedlicher Warnmeldungen und Ereignisse in einem einheitlichen Graphen lassen sich so Muster koordinierter Angriffe erkennen – etwa eine Reihe fehlgeschlagener Anmeldeversuche auf einem System, ein erfolgreicher Admin-Login auf einem anderen und anschließend ein ungewöhnlicher Datenabfluss von einer Datenbank. All das kann in einem Graphen als zusammenhängende Kette dargestellt werden, die in diesem Fall eine laterale Bewegung mit anschließender Datenexfiltrierung erkennbar macht. Analysten sprechen in solchen Fällen von der Abbildung des Angriffspfads, auch bekannt als die „Kill Chain". Graphbasierte Tools können bekannte Angriffstaktiken – etwa aus dem MITRE ATT&CK-Framework – als Teilgraphen hinterlegen. Tritt ein solches Beziehungsmuster in den Echtzeitdaten auf (z.B. ein Knoten für gestohlene Zugangsdaten, verbunden mit einem Knoten für laterale Bewegung und einem weiteren für Data Staging), schlägt das System automatisch Alarm.

Ein besonders anschauliches Beispiel für diesen Ansatz ist das Konzept des Attack Graphs. Ein Attack Graph ist eine visuelle Darstellung möglicher Angriffspfade innerhalb einer Umgebung – basierend auf bekannten Schwachstellen und Konfigurationen. Knoten in einem solchen Graph repräsentieren Systeme oder Schwachstellen, Kanten die Schritte, mit denen sich ein Angreifer durch das Netzwerk bewegen könnte. Sicherheitsteams nutzen Attack Graphen proaktiv, um zu erkennen, wie sich Schwachstellen kombinieren lassen, um kritische Assets zu erreichen. Studien zeigen, dass 75 Prozent der Exploits nach Bekanntwerden einer Schwachstelle innerhalb von nur 19 Tagen erfolgen – ein äußerst knappes Zeitfenster für Abwehrmaßnahmen. Attack Graphen helfen dabei, Prioritäten bei der Behebung von Schwachstellen zu setzen, indem sie die gefährlichsten Angriffspfade hervorheben: Wenn etwa eine bestimmte Serverschwachstelle gemeinsam mit einer Fehlkonfiguration einen Pfad zur Kundendatenbank ermöglicht, zeigt der Graph diesen Pfad auf, indem er seine Elemente in Verbindung setzt. Verteidiger erkennen so unmittelbar, welche Schwachstellen zuerst behoben werden müssen, um den Angriffspfad zu unterbrechen. Der Attack Graph beschreibt „die Beziehungen zwischen Systemen, Schwachstellen und Angriffsvektoren und ermöglicht es Sicherheitsteams, Schwachstellen proaktiv zu identifizieren und vorherzusehen, wie ein Angreifer sie ausnutzen könnte". Auch während aktiver Sicherheitsvorfälle helfen Graphen Incident-Response-Teams dabei, das Ausmaß eines Angriffs zu bestimmen und mittels der Rückverfolgung des Angriffspfades betroffene Systeme gezielt zu isolieren.

Ein weiterer Anwendungsbereich ist die Threat Intelligence Analysis. Informationen über Cyberbedrohungen (wie Feeds zu bösartigen IP-Adressen, Domains, Malware-Signaturen oder Angreifergruppen) sind stark miteinander vernetzt. Graphdatenbanken ermöglichen den Aufbau sogenannter Knowledge Graphen: Knoten stehen für Bedrohungsindikatoren (z.B. IP-Adressen oder Malware-Hashes), Kanten verbinden sie mit bekannten Angreifern oder Kampagnen. Analysten nutzen diese Graphen, um Alarme zu kontextualisieren, etwa wenn ein Endpunkt auf eine Domain anspringt, die mit einer bekannten Phishing-Kampagne gegen die Finanzabteilung in Verbindung steht. Die Visualisierung von Informationen über Bedrohungen als Graph offenbart „Muster, Ausreißer und Anomalien – und damit das Bedrohungsumfeld und die Angriffsarten, mit denen eine Organisation konfrontiert ist." So können scheinbar unabhängige Alarme als Teil einer einzigen Kampagne erkannt werden, beispielsweise weil sie alle auf denselben Command-and-Control-Server im Threat Intelligence Graph zurückführen. Graphbasiertes Threat Hunting beschleunigt die Erkennung komplexer Angriffe, da Analysten mühelos zwischen verschiedenen Datenquellen wechseln können – von Netzwerkprotokollen über Endpoint-Telemetrie bis hin zu Threat-Intel-Feeds – und dabei jederzeit die übergreifenden Zusammenhänge erkennen.

In Security Operations Centers (SOCs) gehört die interaktive graphbasierte Visualisierung heute zur Grundausstattung. SOC-Teams müssen täglich eine enorme Menge an Warnmeldungen und Ereignissen auswerten. Graphbasierte Dashboards zeigen alle Beziehungen auf einen Blick: Statt Listen mit tausenden Einträgen zu sichten, erhält der Analyst eine visuelle Übersicht in Form eines Graphen, in dem Knoten für Alarme oder Assets stehen und Kanten gemeinsame Elemente anzeigen – etwa denselben Host in mehreren Warnmeldungen. Eine solche Darstellung liefert sofort Kontext: Wenn ein einzelner Rechner beispielsweise mit 50 Warnmeldungen in Verbindung steht und diese wiederum zu einem bekannten Malware-Hash führen, weiß der Analyst sofort, wo er mit seiner Untersuchung beginnen muss. „Interaktive Graphvisualisierung […] bietet eine schnelle, intuitive

und aufschlussreiche Sicht auf die Daten“ und ermöglicht es Analysten, laufende Sicherheitsvorfälle in Echtzeit zu beobachten. Graphische Zeitachsen können die Ausbreitung einer Infektion im Netzwerk sogar animiert darstellen. Das beschleunigt Erkennung und Reaktion erheblich.

Zusammenfassend lässt sich sagen: Die Graphanalyse verbessert die Bedrohungserkennung durch die Verbindung einzelner Signale zu kohärenten Mustern und stärkt die Incident Response, indem sie Ausmaß und Verlauf eines Angriffs präzise abbildet.

Schwachstellenmanagement und Risikopriorisierung

In Unternehmensnetzwerken bestehen zu jedem Zeitpunkt Tausende von Schwachstellen und Fehlkonfigurationen. Eine der größten Herausforderungen im Sicherheitsmanagement besteht darin, zu entscheiden, welche Risiken zuerst adressiert werden müssen. Die Graphanalyse bietet hierfür einen wirkungsvollen Ansatz: Sie ermöglicht die Erstellung von Attack Graphen oder sogenannten Vulnerability Graphen – also Visualisierungen, die zeigen, wie einzelne Schwachstellen in Kombination kritische Assets gefährden können. Anstatt jede Schwachstelle isoliert zu betrachten, nutzen Sicherheitsteams graphbasierte Algorithmen, um zu analysieren, welche Pfade ein Angreifer durch das Netzwerk nehmen könnte. Ein einfaches Beispiel: Server A weist eine ungepatchte Schwachstelle (Vulnerability X) auf, die Remote Code Execution ermöglicht; Server B hingegen verfügt über schwach gesicherte Zugangsdaten. Für sich genommen sind beide Schwachstelle relevant, doch wenn Server A über das Netzwerk auf Server B zugreifen kann, entsteht ein Angriffspfad: Ein Angreifer könnte A kompromittieren und sich dann anschließend zu B weiterbewegen, wodurch sich das Gesamtrisiko deutlich erhöhen würde. Solche Zusammenhänge lassen sich mithilfe einer Graphanalyse leicht erkennen. In klassischen Schwachstellenlisten bleiben sie hingegen oft unentdeckt.

Forschung und Industrie setzen die Graphentheorie gezielt für diesen Zweck ein. Die sogenannte Topological Vulnerability Analysis, ursprünglich von Organisationen wie MITRE entwickelt, kombiniert die Netzwerktopologie mit dem Vulnerability Graph, um mögliche mehrstufige Angriffsszenarien zu identifizieren. Ein bekanntes Beispiel dafür ist MITREs CyGraph: Die Plattform aggregiert Daten aus Schwachstellenscannern, Netzwerkkonfigurationen und der geschäftlichen Relevanz der Assets zu einem einheitlichen Property Graph. Daraus entsteht eine Wissensbasis über die Resilienz des Unternehmens, die gezielt nach gefährlichen Mustern durchsucht werden kann. CyGraph kann „risikoreiche, mehrstufige Muster zwischen Datenflüssen, Alarmen und Schwachstellen“ identifizieren und priorisieren. Auf diese Weise lassen sich gezielt Angriffspfade erkennen, die besonders geschäftskritische Assets gefährden. Im Zentrum steht dabei die Analyse von Beziehungen: Welche Hosts können miteinander kommunizieren? Welche Schwachstelle ermöglicht den Zugriff auf welche Ressource? Basierend auf diesen Informationen wird so eine priorisierte Liste von Maßnahmen zur Schwachstellenbehebung erstellt, mit der sich die gefährlichsten Angriffspfade gezielt unterbrechen lassen. Dieser Ansatz bietet einen entscheidenden Vorteil gegenüber traditionellen Risikomodellen, die solch komplexe, miteinander verknüpfte Risiken oft nicht erfassen. In der Praxis konnten Organisationen durch den Einsatz von Attack Graphen zahlreiche schwerwiegende Vorfälle verhindern, indem sie feststellten, dass ein ungepatchter Webserver, der isoliert betrachtet als geringes Risiko eingestuft wurde, nur einen Schritt von einer sensiblen Datenbank entfernt war. Das Problem wurde sofort neu bewertet und priorisiert behoben.

Graphische Visualisierungen erleichtern zudem die Kommunikation mit nicht-technischen Stakeholdern, wie etwa Führungskräften oder anderen Fachabteilungen. Anstatt mit langen Listen von CVEs (Common Vulnerabilities and Exposures) und abstrakten Risikoscores zu arbeiten, können Sicherheitsteams mit vereinfachten Graphen die sogenannten „Crown Jewels“ – also besonders schützenswerte Systeme – und die Schwachstellen-

ketten zu ihnen hin, anschaulich darstellen. Diese Form der visuellen Kommunikation vermittelt Risiken auf anschauliche Weise – vergleichbar mit der Vorgehensweise von Penetrationstestern, wenn sie nach einem erfolgreichen Test demonstrieren, wie sie sich durch ein Netzwerk bewegt haben. Der entscheidende Unterschied: Verteidiger können diese Angriffspfade nun frühzeitig erkennen und proaktiv schließen.

Für viele Organisationen ist die fortlaufende Pflege des Attack Graphs heute ein integraler Bestandteil ihres kontinuierlichen Risikomanagements. Bei jedem neuen Scan wird der Graph automatisch aktualisiert, und die wahrscheinlichsten Angriffspfade werden neu berechnet. Das ermöglicht eine stets aktuelle Einschätzung der Sicherheitslage – und steht damit auch im Einklang mit dem Ansatz von Continuous Diagnostics and Mitigation (CDM) in aktuellen Cybersecurity-Frameworks.

Insider-Bedrohungen erkennen

Insider-Bedrohungen – also böswillige oder fahrlässige Handlungen von Mitarbeitenden oder anderen internen Nutzern – sind besonders schwer zu erkennen. Herkömmliche Sicherheitstools konzentrieren sich meist auf externe Angriffe, während Insider bereits über gültige Anmeldeinformationen und legitimen Zugriff verfügen. Ihre Aktivitäten lösen daher oft keine Alarme aus. Graphanalyse eröffnet neue Möglichkeiten, um Insider-Risiken aufzudecken, indem sie das Verhalten von Nutzern und deren Beziehungen modelliert. Ein gängiger Ansatz besteht darin, einen Graphen zu erstellen, der die Interaktionen der Nutzer mit Assets und Ressourcen (z.B. Dateien, Datenbanken, Anwendungen) sowie gegebenenfalls mit Kollegen oder anderen Abteilungen abbildet. Dieser Graph wird anschließend auf Anomalien untersucht, die auf möglichen Missbrauch hindeuten könnten.

In einer gesunden Organisationsstruktur entstehen typische Zugriffsmuster: Führungskräfte greifen auf HR-Systeme zu, Entwickler auf Quellcode-Repositories usw. Wenn ein Benutzerknoten plötzlich eine Verbindung zu einer Ressource aufweist, die weit außerhalb seines üblichen Aufgabenbereichs liegt (etwa ein Buchhalter, der auf Build-Server der Entwicklungsabteilung zugreift), kann dies als Anomalie markiert werden. Graphbasierte Algorithmen zur Erkennung von Anomalien sind darauf ausgelegt, Teilgraphen zu identifizieren, die vom normalen Muster des Gesamtgraphen abweichen. Ein Insider, der Daten exfiltriert, hinterlässt im Graphen ein einzigartiges „strukturelles Signaturmuster“, beispielsweise durch eine Kombination aus ungewöhnlichen Verbindungen mit externen Websites und dem gleichzeitigen Zugriff auf interne Daten, die er zuvor nie verwendet hat. Ein Graphmodell kann solche kontextuellen Abweichungen sichtbar machen, indem es Kommunikationsprotokolle, Datei-Zugriffe und soziale Strukturen miteinander verknüpft.

Wissenschaftliche Studien belegen diesen Ansatz. Sie zeigen, dass graphbasierte Verfahren zur Anomalieerkennung besonders gut geeignet sind, um verdächtige Insider-Aktivitäten aufzudecken, die auf den ersten Blick unauffällig erscheinen, sich aber bei genauerer Analyse der Verbindungen als ungewöhnlich herausstellen. Ein typisches Beispiel: Ein Insider versucht, sensible Informationen in je kleinen Mengen über verschiedene Kanäle hinweg abzuschöpfen, um unentdeckt zu bleiben. Graphanalyse kann diese scheinbar harmlosen Aktionen miteinander in Verbindung setzen – etwa viele kleine Datei-Zugriffe auf unterschiedlichen Servern – und daraus ein konsistentes, verdächtiges Muster ableiten. Ein in der Forschung vorgestellter Prototyp zeigte, wie sich ein sogenannter Organizational Graph aus Nutzern, Rollen und Geräten aufbauen lässt, der kontinuierlich auf ungewöhnliche Pfade oder neu gebildete Teilgraphen überwacht wird. Unternehmen setzen graphbasierte Tools – häufig im Rahmen von User and Entity Behavior Analytics (UEBA) – bereits gezielt zur Erkennung von Insider-Bedrohungen ein.

Ein besonderer Vorteil graphischer Visualisierung liegt darin, dass sie nicht nur potenziellen Missbrauch sichtbar macht, sondern auch die nachgelagerte Analyse erleichtert. Wird ein Benutzer als verdächtig eingestuft, kann ein Analyst seine Verbindungen visuell nachverfolgen: Welche Systeme wurden genutzt? Mit wem be-

stand Kommunikation? In welche Datenflüsse war die Person eingebunden? Diese konsolidierte Darstellung ermöglicht es, schnell zu unterscheiden, ob es sich tatsächlich um einen böswilligen Insider handelt – erkennbar etwa an Verbindungen zu sensiblen Assets oder zu externen Empfängern – oder lediglich um ein ungewöhnliches, aber letztlich harmloses Verhalten.

Graphanalyse ergänzt klassische, signaturbasierte Verfahren in der Cybersicherheit um eine verhaltensbasierte Dimension. Durch das Verständnis der normalen Beziehungsnetzwerke – zwischen Nutzern und Daten, zwischen Prozessen auf einem Host oder Diensten innerhalb einer Architektur – ermöglichen Graphen es, abweichende Muster zu erkennen, die häufig auf interne wie externe Angriffe hindeuten.

Für Sicherheitsoperationen ergeben sich daraus erhebliche Vorteile: verbesserte Visibilität, schnellere Erkennung und Reaktion sowie bessere Zusammenarbeit. Wie ein Branchenexperte festhielt, ist die graphische Visualisierung besonders intuitiv – das menschliche Gehirn kann visuelle Knoten und Verbindungen deutlich leichter interpretieren und Muster oder Ausreißer viel schneller erkennen, als wenn sie in Form von Rohdaten oder Tabellen präsentiert werden. Das erleichtert nicht nur Analysten die Arbeit, sondern auch die Kommunikation mit nicht-technischen Entscheidungsträgern.

Graphbasierte Visualisierungen helfen dabei, Führungskräfte oder bereichsübergreifende Teams schnell und verständlich über Bedrohungssituationen zu informieren. Was in einer Tabellenansicht unübersichtlich oder missverständlich wirkt, erzählt als Netzwerkdiagramm eine klare Geschichte. In der Sicherheit ist Zeit ein entscheidender Faktor – die Graphanalyse wird damit zu einem echten Gamechanger in der modernen Cyberabwehr.

Graphbasierte Technologien im Kontext von Zero Trust

Zero Trust hat sich in den vergangenen Jahren als zentrales Modell moderner Cybersicherheitsarchitekturen etabliert – und graphbasierte Technologien fügen sich auf natürliche Weise in dieses ein. Der Zero-Trust-Ansatz löst sich vom traditionellen, perimeterbasierten Sicherheitsdenken („alles innerhalb des Netzwerks ist vertrauenswürdig“) und ersetzt es durch das Prinzip, dass grundsätzlich keinem Nutzer oder Gerät vertraut wird – selbst innerhalb des Netzwerks. Das zugrunde liegende Motto lautet: „Never trust, always verify.“

Kernelemente von Zero Trust sind zudem die Annahme, dass ein Angreifer möglicherweise bereits im System ist („Assume Breach“), die konsequente Durchsetzung des „Least Privilege“-Prinzips (jedem Benutzer und jedem System werden nur die minimal notwendigen Zugriffsrechte gewährt) sowie die kontinuierliche Überprüfung von Identität, Kontext und Sicherheitsstatus bei jeder Interaktion.

Die Umsetzung des Zero-Trust-Modells basiert somit auf dynamischen, kontextabhängigen Zugriffsentscheidungen und einer lückenlosen Überwachung sämtlicher Aktivitäten in Echtzeit – Aufgaben, für die sich graphbasierte Ansätze besonders gut eignen.

Echtzeitüberwachung und Mikrosegmentierung

In einem Zero-Trust-Netzwerk ist es das Ziel, die Umgebung möglichst fein zu segmentieren (ein Prinzip, das häufig als Mikrosegmentierung bezeichnet wird). So wird sichergestellt, dass jede Anwendung oder jeder Dienst nur die Kommunikation ausführt, die tatsächlich notwendig ist, und jeder Nutzer ausschließlich auf die Ressourcen zugreift, die er wirklich benötigt.

Graphanalyse kann dabei eine zentrale Rolle spielen, diese Segmentierungsgrenzen zu definieren und durchzusetzen. Durch die Analyse von Kommunikationsmustern in Form eines Graphen können Sicherheitsteams Systemgruppen identifizieren, die regelmäßig miteinander interagieren und logisch ein Segment bilden sollten. Gleichzeitig lassen sich so auch Übergangspunkte zwischen Segmenten erkennen, an denen Sicherheitskontrollen wie etwa Firewalls oder softwaredefinierte Richtlinien implementiert werden können.

Ein Graph der Netzwerkflüsse könnte beispielsweise zeigen, dass ein Anwendungsserver regelmäßig mit einer Datenbank und einem Cache kommuniziert. Diese drei Systeme könnten dementsprechend ein sinnvolles Segment bilden. Wenn der gleiche Server jedoch plötzlich eine Verbindung zu einem HR-System in einem völlig anderen Segment aufbaut, kann dies entweder auf eine Fehlkonfiguration oder auf potenziell böswillige Aktivität hindeuten.

In modernen Netzwerken lassen sich Daten der Netzwerküberwachung in Echtzeit in den Graphen einspeisen, sodass jede neu auftretende Verbindung (Kante) sofort überprüft wird. Entspricht sie keinem zugelassenen Kommunikationsmuster, kann das System sie markieren oder automatisch blockieren. So funktionieren moderne, softwaredefinierte Mikrosegmentierungslösungen: Sie erstellen einen sogenannten Workload Connectivity Graph und setzen Richtlinien für erlaubte und unerlaubte Verbindungen durch. Das Graphmodell ist hierfür besonders gut geeignet, weil es komplexe, „many-to-many“-Beziehungen effizient abbilden kann. Kommen neue Systeme hinzu oder entstehen neue Verbindungen, lassen sich diese als zusätzliche Knoten und Kanten dem Graphen hinzufügen und sofort im Gesamtzusammenhang bewerten.

Anomale Muster erkennen

Da Zero Trust grundsätzlich davon ausgeht, dass sich ein Angreifer bereits im Netzwerk befinden könnte, legt das Modell besonderen Wert auf die kontinuierliche Erkennung von Anomalien. Graphanalyse unterstützt diesen Ansatz, indem sie Kontext schafft, um Abweichungen zu erkennen, die sich über mehrere Datenquellen hinweg erstrecken. Besonders deutlich wird das am Beispiel des Benutzerverhaltens: Zero Trust fordert, dass jede Aktivität eines Nutzers fortlaufend auf Legitimität geprüft wird. Wird ein Graph erstellt, der Benutzer mit ihren Geräten, geografischen Standorten, Zugriffshistorien und Ressourcennutzungen verknüpft, lassen sich so Richtlinien definieren wie: „Löse einen Alarm aus, wenn das Gerät eines Nutzers nicht vertrauenswürdig ist, und der Nutzer versucht, von einem ungewöhnlichen Standort aus auf einen sensiblen Server zuzugreifen, auf den er zuvor noch nie zugegriffen hatte.“ Solche komplexen Anomalien – also Ereignisse, die mehrere Bedingungen gleichzeitig erfüllen – lassen sich mit isolierten Überwachungssystemen nur schwer erkennen. Graphabfragen hingegen können diese Zusammenhänge in Echtzeit auswerten, da alle relevanten Beziehungen (Benutzer – Gerätezustand, Benutzer – Ressource, Benutzer – Standort) im Modell bereits miteinander verknüpft sind.

In einer Zero-Trust-Umgebung muss Zugriffskontrolle also stets kontextabhängige Faktoren berücksichtigen

– nicht nur, wer der Benutzer ist, sondern auch, wo er sich befindet, welches Gerät er verwendet und welche Ressourcen er ansteuert. Der Vertrauensgrad wird dabei fortlaufend anhand des Kontexts neu bewertet und angepasst. Graphdatenbanken sind dafür besonders geeignet, da sie Kontextinformationen als Beziehungen speichern und in Echtzeit auswerten können. Ein Sicherheitsexperte bringt es auf den Punkt: „Graphdatenbanken ermöglichen Graphabfragen in Echtzeit, um Faktoren wie Gerätezustand, Nutzerverhalten und Netzwerksicherheit zu prüfen, bevor der Zugriff gewährt wird." Entspricht eine dieser Bedingungen nicht den Richtlinien, wird der Zugriff verweigert oder eine zusätzliche Authentifizierung (z.B. Step-up-Authentifizierung) verlangt.

Ein weiteres Beispiel für ein anomales Muster ist die Erkennung lateraler Bewegung. In einem gut segmentierten Zero-Trust-Netzwerk erzeugen Angreifer bei dem Versuch, über ein kompromittiertes Gerät auf andere Systeme zuzugreifen, häufig neue Kanten im Graphen – Verbindungen, die unter normalen Umständen nicht existieren. Solche plötzlichen Kommunikationspfade können durch kontinuierliche Graphanalyse als potenzielle Sicherheitsverletzungen erkannt werden, noch während ein Angriff im Gange ist.

Durchsetzung granularer Zugriffskontrollen

Eine der größten Herausforderungen bei der Umsetzung von Zero Trust ist die Einführung granularer Zugriffskontrollen – also der Übergang von groben, netzwerkbasierten Regeln hin zu identitäts- und beziehungsbasierten Richtlinien. Graphbasierte Technologien unterstützen diesen Ansatz direkt, insbesondere im Rahmen von Relationship-based Access Control (ReBAC).

Statt einfache Rollenmodelle zu definieren, können Richtlinien deutlich komplexere Bedingungen formulieren, etwa: „Gewähre Zugriff, wenn der Benutzer einem Manager unterstellt ist, der das Projekt verantwortet, zu dem die Ressource gehört, und die Anfrage während der Geschäftszeiten erfolgt." Solche Richtlinien, die Organisationsstrukturen, Projektverantwortung und zeitliche Kontexte berücksichtigen, lassen sich in relationalen Datenbanken nur schwer abbilden. In einem Graphen hingegen werden Benutzer, Manager, Projekte usw. als Knoten modelliert, deren Beziehungen – etwa „reports_to" oder „owns" – durch Kanten definiert sind. Die Umsetzung einer Richtlinie reduziert sich somit auf das Durchlaufen des Graphen, um zu prüfen, ob alle relevanten Beziehungen erfüllt sind.

Diese Form der dynamischen, kontextabhängigen Entscheidungsfindung entspricht genau dem Anspruch von Zero Trust. Wie es eine Analyse treffend festhält: „Graphdatenbanken ermöglichen die Modellierung kontextbewusster Zugriffskontrollen, bei denen Entscheidungen nicht allein auf Basis von Rollen oder Attributen des Benutzers, sondern im Zusammenspiel mit relevanten Kontextbeziehungen getroffen werden – etwa dem Standort eines Nutzers, dem Zustand seines Geräts oder dem Zeitpunkt des Zugriffs."

Einige moderne Systeme für Identity and Access Management (IAM) setzen bereits auf graphbasierte Backends. Sie ermöglichen es, in Echtzeit zu prüfen, ob eine Zugriffsanfrage alle erforderlichen Beziehungen besitzt – etwa zwischen Identität und Gerätezustand, zwischen Identität und Gruppenmitgliedschaft oder zwischen Ressource und Klassifizierungsstufe. Dieser Ansatz ist oft schneller und flexibler als die Durchführung vieler einzelner Prüfungen, da der Graph den vollständigen Kontext einer Entität mit einer einzigen Abfrage erfassen kann. Zugleich erlaubt dieser Ansatz eine kontinuierliche Neubewertung der Vertrauenslage: Ändert sich zum Beispiel der Sicherheitsstatus eines Geräts (etwa durch einen Compliance-Verstoß), wird die entsprechende Kante („trusted device") im Graphen entfernt. Alle bestehenden Sitzungen, die auf dieser Beziehung beruhen, können daraufhin sofort überprüft und bei Bedarf beendet werden. Graphbasierte Policy-Engines setzen das „Never Trust"-Prinzip damit konsequent um: Vertrauen wird nicht als statischer Zustand behandelt, sondern kontinuierlich und kontextabhängig anhand aktueller Beziehungsdaten neu bewertet.

Wie sich dieser Ansatz in der Praxis bewährt, kann man am Beispiel eines großen Finanzinstituts zeigen, das im Rahmen seiner Zero-Trust-Strategie eine graphbasierte Plattform für Sicherheitsanalysen einführte: Dazu wurde ein Graph aufgebaut, der Daten aus verschiedenen Quellen zusammenführte, darunter Active Directory (Benutzer und Gruppen), Endpoint-Management-Systeme (Gerätezustand), Netzwerkprotokolle (Verbindungen) und HR-Datenbanken (Organisationsstruktur). Eines Tages schlug das System Alarm: Ein Benutzerkonto aus der Finanzabteilung versuchte, auf einen Software-Repository-Server im Forschungs- und Entwicklungsbereich zuzugreifen – ein untypisches Verhalten. Der Graph zeigte, dass es zuvor keine Beziehung zwischen dem Nutzer und diesem Server gab (keine Kanten im Graphen), und dass das verwendete Gerät ein privater, bisher nicht registrierter Laptop war (der Geräteknoten war als „untrusted“ markiert). Gemäß dem Zero-Trust-Prinzip des Least Privilege, blockierte das System den Zugriff automatisch und generierte eine Warnung. Die anschließende Untersuchung ergab, dass die Zugangsdaten des Mitarbeiters kompromittiert worden waren. Ein Angreifer hatte versucht, sich von den Finanzsystemen in die Produkt- und Entwicklungsumgebung vorzubewegen – vermutlich mit dem Ziel der Industriespionage. Der Angriff konnte im Keim erstickt werden, da die graphbasierte Richtlinien-Engine die Situation korrekt bewertete: „Finanznutzer + unbekanntes Gerät + Zugriff auf R&D-Server = verdächtig“. In einer herkömmlichen, Architektur mit flachen Netzwerkstrukturen und rein rollenbasierten Zugriffsregeln wäre dieser Vorfall möglicherweise unbemerkt geblieben.

Ein weiteres Beispiel zeigt den Einsatz graphbasierter Visualisierung bei der Planung einer Zero-Trust-Netzwerkarchitektur in einem Technologieunternehmen: Das Unternehmen erstellte einen Graphen aller Kommunikationsbeziehungen zwischen seinen Microservices in der Cloud. Dabei traten mehrere unerwartete Verbindungen zutage, darunter auch ein Backend-Dienst, der direkt mit einer externen API kommunizierte, obwohl diese nirgends dokumentiert war, sowie einige veraltete Services, die noch immer Zugriff auf Datenbanken in der Produktion hatten. Diese Verbindungen stellten ein Sicherheitsrisiko dar, da sie gegen das Least-Privilege-Prinzip verstießen. In der Folge wurden die Netzwerksegmente überarbeitet und überflüssige Kommunikationspfade entfernt. Das Ergebnis war ein schlankeres Netzwerk, in dem jeder Service nur mit den Systemen kommuniziert, die für seine Funktion zwingend erforderlich sind. Die laufende Überwachung erfolgt seitdem durch das kontinuierliche Einspeisen von Netzwerk-Telemetriedaten in den Graphen. Versucht ein Dienst, eine Verbindung außerhalb seiner zugelassenen Kommunikationswege (Kanten) herzustellen, wird automatisch eine Gegenmaßnahme ausgelöst, die die Verbindung blockiert und das Ereignis protokolliert. Diese Implementierung in Echtzeit knüpft direkt an das Zero-Trust-Prinzip des „Assume Breach“ an: Das System operiert stets unter der Annahme, dass jeder unerwartete Verbindungsversuch auf einen Angreifer hindeuten könnte – und behandelt ihn entsprechend vorsorglich als Bedrohung, bis das Gegenteil bewiesen ist.

Graphbasierte Technologien ergänzen Zero Trust, indem sie die notwendige Datenstruktur und Analytik bereitstellen, die für ganzheitliche, kontextabhängige Sicherheitsentscheidungen in Echtzeit notwendig sind. Sie unterstützen die Umsetzung der zentralen Prinzipien des Zero-Trust-Modells: die kontinuierliche Verifizierung aller Entitäten (durch dynamische Abfragen im Security Graph), die konsequente Durchsetzung von „Least Privilege“ (mithilfe präziser, beziehungsbasierter Richtlinien und Mikrosegmentierung) sowie das „Assume Breach“-Prinzip (durch die schnelle Identifikation von Anomalien und unautorisierten Verbindungen). Die Synergie zwischen Graphanalyse und Zero Trust liegt auf der Hand: Beide Konzepte beruhen darauf, Beziehungen innerhalb eines Systems zu verstehen und kontrollierbar zu machen. Im Zuge der zunehmenden Umsetzung von Zero-Trust-Architekturen wird der Einsatz graphbasierter Ansätze für Sicherheitsüberwachung und Zugriffskontrolle voraussichtlich weiter zunehmen – insbesondere weil sie die Komplexität granularer Vertrauensentscheidungen wirksam adressieren.

Strategischer Wert für Großunternehmen und KMU

Graphbasierte Ansätze in der Cybersicherheit bieten Organisationen jeder Größe strategische Vorteile. Ganz gleich, ob es sich um ein globales Unternehmen mit einer enormen IT-Umgebung oder um ein mittelständisches Unternehmen mit begrenzten Ressourcen handelt – durch den Einsatz von Graphanalyse kann ein jedes Unternehmen seine Sicherheitslage gezielt verbessern und effizienter verwalten. Im Folgenden werden die wichtigsten Vorteile für Großunternehmen und kleine bis mittlere Betriebe (KMU) aufgezeigt.

Vorteile für Großunternehmen

Skalierbares Monitoring komplexer Systeme: Großunternehmen verfügen häufig über äußerst komplexe IT-Umgebungen – mit Tausenden von Mitarbeitern, Geräten, Anwendungen und wechselseitigen Abhängigkeiten, die sich über lokale Rechenzentren und Multi-Cloud-Plattformen hinweg erstrecken. Traditionelle Monitoring-Tools geraten hier oft an ihre Grenzen, wenn es darum geht, ein einheitliches Gesamtbild zu liefern. Graphbasierte Lösungen hingegen sind von Grund auf darauf ausgelegt, große Mengen vernetzter Daten zu verarbeiten.

Ein solcher Graph kann Daten aus den unterschiedlichsten Quellen wie Cloud-Asset-Inventaren, On-Premises-Network Maps, Identitätsverzeichnissen und mehr zu einem einheitlichen Modell zusammenführen. Diese ganzheitliche Visibilität ermöglicht es Sicherheitsteams, domänenübergreifende Fragen zu stellen, wie etwa: „Welche externen Verbindungen bestehen zu unseren Finanzsystemen und welche Authentifizierungsmethoden wurden dabei verwendet?“ Die Antwort liefert einen vollständigen Überblick, der alle relevanten Datenquellen umfasst.

Diese Fähigkeit, das „große Ganze“ sichtbar zu machen, ist weit mehr als nur ein Komfort – sie ist entscheidend, um zu erkennen, wie sich ein lokales Problem auf kritische Systeme an anderer Stelle auswirken könnte. So kann ein Unternehmen etwa Schwachstellenscans und etablierte Vertrauensbeziehungen aus dem Active Directory in einen Graphen integrieren, um auf einen Blick zu erkennen, ob eine schwerwiegende Schwachstelle auf einem System besteht, das administrativen Zugriff auf Dutzende andere Maschinen hat – potenzielle Risiken für ganze Domänen werden sofort sichtbar. Solche domänenübergreifenden Erkenntnisse sind ein zentraler Mehrwert von graphbasierten Sicherheitsmodellen.

Die Graphen helfen großen Unternehmen auch im Bereich von Advanced Analytics. Sie können Algorithmen – etwa zur Ermittlung von Zentralität, Community Detection oder kürzeste Pfade – einsetzen, um besonders relevante Knotenpunkte zu identifizieren; beispielsweise ein Server, dessen Kompromittierung den Zugriff auf zahlreiche weitere Systeme ermöglicht. Ebenso lassen sich Subnetzwerke isolieren, die zu einem bestimmten Geschäftsbereich gehören oder ein spezielles Risiko darstellen. Diese Einblicke liefern wertvolle Erkenntnisse für das Risikomanagement sowie für strategische Entscheidungen zum Aufbau der Architektur. Sie ermöglichen es, potenzielle Angriffs- oder Ausfallsszenarien in einem Modell des Netzwerks zu simulieren, bevor sie tatsächlich eintreten – und dienen so als Grundlage für proaktive Maßnahmen.

Verbesserte Incident Response und Collaboration: In großen Organisationen sind bei Sicherheitsvorfällen in der Regel mehrere Teams beteiligt – von den Sicherheitsteams über IT und Engineering bis hin zu Compliance und Management. Graphbasierte Visualisierungen dienen dabei als gemeinsame, leicht verständliche Referenz

für alle Beteiligten. Bei schwerwiegenden Vorfällen kann eine graphbasierte Incident Map – also eine visuelle Darstellung des Angriffsverlaufs – in einem sogenannten „War Room“ eingesetzt werden, um den Verlauf des Angriffs sowie die betroffenen Systeme visuell darzustellen. Das verbessert die Kommunikation und Koordination zwischen den Teams und stellt sicher, dass alle – von den technischen Incident-Respondern bis hin zur Geschäftsführung – denselben Informationsstand und dieselbe Einschätzung der Lage teilen.

Zugleich schaffen Graphen einen nachvollziehbaren Audit Trail für Untersuchungen. Indem Analysten während eines Angriffs kompromittierte Systeme markieren und eingeleitete Eindämmungsmaßnahmen wie das Trennen von Verbindungen in den Graphen einpflegen, entsteht damit eine lückenlose Dokumentation des Vorfalls in Echtzeit. Nach dessen Bewältigung kann der Graph dann ausgewertet werden, um daraus Erkenntnisse für die Nachbereitung, interne Berichterstattung und zur Verbesserung künftiger Präventionsmaßnahmen abzuleiten.

Dokumentation für regulatorische Compliance: Unternehmen in stark regulierten Branchen (z.B. in der Finanzbranche, im Gesundheitssektor oder im Versorgungswesen) unterliegen strengen Anforderungen, wenn es um die Dokumentation von Sicherheitsmaßnahmen und -vorfällen geht. Graphbasierte Ansätze können diese Aufgabe erheblich erleichtern, da sie anschauliche Nachweise zu Netzwerksegmentierung, Datenflusskontrollen und Vorfallauswirkungen liefern. Ein Beispiel: Eine Bank muss nachweisen, dass Kundendaten durch mehrere Sicherheitskontrollen vom Internet isoliert sind. Ein Graphmodell erfüllt diese Anforderung unmittelbar, indem es anhand einer einzigen Visualisierung alle Netzwerkebenen zwischen den Kundendatenbanken und externen Netzen darstellt.

Compliance-Standards wie PCI-DSS verlangen häufig aktuelle Netzwerkdiagramme und Inventarlisten. Diese manuell zu pflegen ist aufwendig; hingegen kann ein dynamischer Graph solche Darstellungen jederzeit automatisch erzeugen. Auch für die kontinuierliche Einhaltung von Vorgaben (Continuous Compliance) bieten Graphsysteme Unterstützung: Sobald eine neue Verbindung oder ein Asset auftaucht, welches gegen bestehende Regeln verstößt (etwa eine nicht zulässige Verbindung zwischen einem PCI- und einem Nicht-PCI-System), wird dies automatisch erkannt und markiert.

Graphanalyse trägt damit nicht nur zur Erfüllung von Compliance-Vorgaben bei, sondern reduziert auch den personellen Aufwand für Audits. Immer mehr Unternehmen setzen daher gezielt „Graphtechnologien für regulatorische Compliance“ ein, um komplexen gesetzlichen Anforderungen gerecht zu werden – laut Branchenstimmen ist Graphanalyse „das ideale Werkzeug“, um die Einhaltung von Vorschriften auch über vernetzte Datensätze hinweg zu verstehen, zu überwachen und nachzuweisen. Gerade im Finanzwesen zeigen sich die Vorteile besonders deutlich: Graphische Visualisierungen unterstützen KYC- (Know Your Customer) und AML-Prozesse (Anti-Money Laundering), indem sie komplexe Beziehungen zwischen Kunden sowie Transaktionen sichtbar machen – ein zentraler Aspekt, der von Aufsichtsbehörden besonders genau geprüft wird. So können Unternehmen Prüfungen sicherer bestehen und das Risiko von Verstößen deutlich verringern.

Strategischer Mehrwert durch proaktive Verteidigung: Darüber hinaus bietet der Einsatz graphbasierter Cybersicherheitsansätze Unternehmen insbesondere im Hinblick auf eine proaktive und vorausschauende Verteidigung einen klaren strategischen Vorteil. Mithilfe graphgestützter Analysen können Sicherheitsteams von einer rein reaktiven hin zu einer präventiven und prognostischen Sicherheitsstrategie übergehen (wie zuvor bereits im Zusammenhang mit Attack Graphen und der Analyse von Angriffsmustern beschrieben). Dies steht im Einklang mit den übergeordneten Zielen vieler Unternehmen, Sicherheitsvorfälle zu vermeiden und teure Ausfallzeiten zu reduzieren.

Vorstände und Geschäftsleitungen fordern zunehmend quantifizierbare Einblicke von Sicherheitsverantwortlichen in das aktuelle Risikoprofil – etwa durch konkrete Fragen wie:
„Was sind derzeit unsere fünf größten Cyberrisiken?“. Graphanalysen liefern hierfür die notwendige Grundlage, indem sie Risikokonzentrationen und potenzielle Angriffspfade identifizieren, die sich anschließend in

geschäftsrelevante Aussagen übersetzen lassen. Ein CISO könnte so beispielsweise erklären: „Unsere Analyse zeigt, dass das HR-System und das F&E-Netzwerk derzeit auf riskante Weise miteinander verbunden sind. Durch gezielte Segmentierung dieser Bereiche – wie in diesem Graph dargestellt – lässt sich das potenzielle Schadensausmaß eines Angriffs um x % reduzieren.“ Solche datenbasierten Argumente für Investitionen in Sicherheitsmaßnahmen – etwa in Mikrosegmentierung oder neue Detection Tools – überzeugen auch auf Vorstandsebene.

Zusammenfassend lässt sich sagen: Graphbasierte Cybersicherheit verschafft Großunternehmen entscheidende strategische Vorteile – darunter Skalierbarkeit, tiefere Einblicke und eine deutlich verbesserte Fähigkeit, Risiken in komplexen Umgebungen zu erkennen, gezielt zu steuern und wirksam zu kommunizieren.

Vorteile für kleine und mittlere Unternehmen (KMU)

Kleine und mittlere Unternehmen stehen in der Cybersicherheit vor anderen Herausforderungen als Großunternehmen. Sie verfügen oft nur über begrenzte Budgets und selten über spezialisierte Sicherheitsteams – gleichzeitig nehmen gezielte Angriffe auf genau solche Unternehmen stetig zu. Mittlerweile richten sich über die Hälfte aller Cyberangriffe gegen KMU, und viele Betroffene verfügen nicht über die Ressourcen, um sich ausreichend zu schützen. Die Folge: Ein erheblicher Teil der betroffenen Unternehmen muss nach einem schweren Vorfall den Betrieb dauerhaft einstellen.

Graphbasierte Ansätze können hier als effektiver Gegenhebel wirken: Sie bieten kosteneffiziente Funktionen zur Visualisierung und Bedrohungserkennung, mit denen auch kleine Sicherheitsteams ihre Schutzwirkung steigern können.

Kosteneffiziente Visualisierung und Bedrohungserkennung: Auch IT-Umgebungen kleinerer und mittlerer Unternehmen sind häufig komplexer, als es zunächst erscheint. Eine Handvoll Cloud-Dienste, lokale Server, Remote-Mitarbeiter – all das bildet ein vernetztes System mit vielen Abhängigkeiten. Oft ist es aber nur eine einzelne Person, die für dieses gesamte Setup – vom Netzwerkmanagement über den IT-Betrieb bis hin zur Sicherheit – zuständig ist, ohne die Unterstützung mehrerer spezialisierter Teams. Gerade in solchen Szenarien ist eine einheitliche, leicht verständliche visuelle Übersicht über das gesamte Netzwerk und dessen Sicherheitszustand von großem Wert. Graphbasierte Tools – viele davon Open-Source-Lösungen oder Bestandteil kostengünstiger Sicherheitsprodukte – ermöglichen genau das: Sie stellen alle Systeme und deren Beziehungen in einer zentralen Ansicht dar. So lassen sich Schwachstellen oder Auffälligkeiten wesentlich schneller erkennen und analysieren. Kommt es dann beispielsweise zu einem Ransomware-Angriff auf ein kleineres Unternehmen, kann ein IT-Verantwortlicher einen Graphen aufrufen (oder mithilfe automatisierter Discovery Tools schnell einen erstellen), um nachvollziehen zu können, welche Geräte mit dem infizierten Knoten kommunizieren und welche Benutzerkonten betroffen sein könnten. Dieser unmittelbare, beziehungsbezogene Kontext kann den entscheidenden Unterschied ausmachen, ob eine Bedrohung frühzeitig isoliert wird, oder ob sie sich über mehrere Stunden unbemerkt weiter im Netzwerk ausbreitet.

Effizienter Einsatz begrenzter Ressourcen: Kleine und mittlere Unternehmen müssen ihre begrenzten personellen und finanziellen Ressourcen besonders gezielt einsetzen. Graphanalyse kann dabei helfen, Prioritäten sinnvoll zu setzen und den Einsatz vorhandener Ressourcen zu optimieren. Anstatt gleichmäßig Zeit und Budget auf das Patchen aller Systeme zu verteilen, können KMU mithilfe einer vereinfachten Attack-Graph-Analyse den kritischen Pfad ermitteln – und dabei bereits mit der Behebung fünf besonders kritischer Schwachstellen das Risiko eines Breaches deutlich reduzieren. Gerade bei knappen Ressourcen ist solch ein fokussierter Ansatz

besonders wirkungsvoll.

Auch wiederkehrende Prüfungen lassen sich durch Graphabfragen effizient automatisieren – etwa mit Fragen wie: „Wer hat Zugriff auf was?“ „Sind ehemalige Mitarbeitende noch mit irgendeinem System verbunden?“ „Gibt es Geräte im Netzwerk, die nicht im Asset-Inventar erfasst sind?“ Ein Graphmodell beantwortet solche Fragen in Sekundenschnelle – und ersetzt damit aufwändige manuelle Audits. Das Ergebnis ist eine gestärkte Sicherheitslage bei minimalem Personalaufwand.

Ein weiterer Vorteil: Graphbasierte Visualisierungen machen Sicherheitsrisiken auch für Führungskräfte ohne technischen Hintergrund greifbar. Viele Inhaber oder Führungskräfte von KMU haben keinen Bezug zu IT-Sicherheit – Berichte voll mit technischen Fachbegriffen oder Rohdaten sind für sie oft schwer nachvollziehbar und liefern ihnen keine konkreten Handlungsansätze. Ein Network Graph hingegen, der beispielsweise zeigt, dass die zentrale Unternehmensdatenbank direkt vom PC-Netzwerk der Mitarbeiter erreichbar ist, ohne dazwischenliegende Sicherheitskontrollen, vermittelt das Risiko überzeugend und zeigt, warum entsprechende Investitionen in die Sicherheit hier notwendig sind. Graphen schlagen damit eine wichtige Brücke in der Kommunikation zwischen Technik- und Managementebene. Dies ist besonders relevant, da Studien zeigen, dass rund 42 % der KMU-Führungskräfte Schwierigkeiten haben, das tatsächliche Ausmaß eines Cyberangriffs zu erfassen – ein klarer Hinweis auf bestehende Lücken in der Krisenvorbereitung. Durch die Visualisierung potenzieller Angriffspfade oder möglicher Auswirkungen eines Vorfalls machen Graphen Cyberrisiken für Entscheidungsträger greifbar und liefern damit eine starke Grundlage, um Investitionen in Sicherheitsmaßnahmen auch in kostenbewussten Organisationen zu rechtfertigen.

Nutzung moderner Plattformen: Ein weiterer Vorteil für kleine und mittlere Unternehmen besteht darin, dass sie auf cloudbasierte Graph-Security-Services zurückgreifen können, ganz ohne eigene Infrastruktur vor Ort. Einige „Security-as-a-Service“-Anbieter setzen graphbasierte Verfahren bereits im Hintergrund ein, um Warnmeldungen zu korrelieren, Zusammenhänge zu erkennen und Handlungsempfehlungen abzuleiten. Damit erhalten auch kleinere Unternehmen Zugang zu Analysefunktionen, die sonst nur Großunternehmen zur Verfügung stehen – flexibel über ein Abonnementmodell, ohne dabei selbst komplexe Systeme aufbauen und betreiben zu müssen. Graphanalyse wird so zu einem kosteneffizienten Hebel, um das eigene Sicherheitsniveau deutlich zu steigern und Angreifern wirksam entgegenzutreten. Im Kern hilft graphbasierte Cybersicherheit kleinen Unternehmen, über sich hinauszuwachsen: Sie automatisiert jene Analyse- und Korrelationstätigkeiten, die in Großunternehmen normalerweise ein ganzes Security Operations Center übernimmt – und kompensiert so den Mangel an personellen Ressourcen. Dabei funktioniert das System intuitiv: Es folgt den Verbindungen und Abhängigkeiten zwischen Systemen, um Probleme nachvollziehen und Ursachen eingrenzen zu können, so wie ein ganzes IT-Team es tun würde.

Sowohl für Konzerne als auch für KMU liegt ein zentraler strategischer Vorteil graphbasierter Ansätze in der besseren Entscheidungsfindung. Anstatt sich auf Schätzungen oder allgemeine Best Practices zu verlassen, können Verantwortliche ihre Sicherheitsstrategie auf fundierte Erkenntnisse über die Beziehungen zwischen ihren Systemen und Risiken stützen. Für Großunternehmen bedeutet das, Sicherheitsinvestitionen gezielt dort zu platzieren, wo sie den größten Effekt auf die Sicherheit ihrer gesamten Umgebung haben. Für KMU wiederum heißt es, mit begrenzten Mitteln maximale Wirkung zu erzielen. In beiden Fällen tragen graphbasierte Technologien dazu bei, Sicherheit proaktiver und resilienter zu gestalten – und schaffen so einen geschäftlichen Mehrwert: geringere Ausfallzeiten, besserer Schutz vor finanziellen Verlusten, stärkere Kundenbindung und ein ungefährdeter fortlaufender Geschäftsbetrieb.

Die Zukunft graphbasierter Technologien in der Cybersicherheit

Angesichts sich zunehmend entwickelnder Cyberbedrohungen werden graphbasierte Technologien künftig eine noch wichtigere Rolle in der digitalen Verteidigung spielen. In den kommenden Jahren ist zu erwarten, dass sie noch stärker mit Künstlicher Intelligenz (KI) und Machine Learning (ML) integriert werden, ebenso wie mit ihrem breiteren Einsatz in Cloud- und Hybridumgebungen. Gleichzeitig werden neue technische und ethische Herausforderungen in den Fokus rücken – etwa im Hinblick auf Datenschutz, Skalierbarkeit sowie die Nachvollziehbarkeit automatisierter Entscheidungen.

Die Kombination von Graphen mit anderen innovativen Technologien eröffnet dabei neue Möglichkeiten – vom Predictive Threat Modeling bis hin zu vollautomatisierten Reaktionen auf Angriffe. Dies verändert grundlegend, wie digitale Assets künftig geschützt werden.

Integration von KI und ML für Predictive Analytics und automatisierte Erkennung: Ein besonders dynamisches Anwendungsfeld liegt in der Kombination von Graphanalyse mit KI und ML. Graphen liefern umfangreiche kontextuelle und strukturelle Informationen, die KI-Modelle für präzisere Vorhersagen nutzen können. Maschinelle Lernverfahren können beispielsweise graphbasierte Metriken – etwa Zentralitätsmaße oder Clusterzugehörigkeiten – als zusätzliche Parameter verwenden, um besser zwischen legitimen und potenziell schädlichen Aktivitäten zu unterscheiden. So kann ein solches Modell lernen, Warnmeldungen von bestimmten Endpunkten höher zu priorisieren, wenn diese stark mit anderen geschäftskritischen Systemen vernetzt sind (dies würde einen zentralen Knoten auf dem Graph darstellen).

Neben der Nutzung von Graphen für die Verbesserung von „klassischen“ ML-Funktionen, rückt zunehmend auch ein spezialisiertes Teilgebiet in den Fokus: Graph Machine Learning und Graph Neural Networks (GNNs) – KI-Modelle, die speziell auf die Verarbeitung von Graphdaten ausgelegt sind und komplexe Beziehungsmuster lernen. In der Cybersicherheitsforschung werden GNNs zunehmend eingesetzt, um Angriffsmuster anhand von Graphen zu erkennen, in denen Knoten Prozesse oder Netzwerkentitäten darstellen und Kanten deren Kommunikationsbeziehungen abbilden. Dabei lernt ein GNN, bestimmte Knoten oder Teilgraphen als unauffällig oder verdächtig zu klassifizieren – basierend auf typischen Mustern aus Trainingsdaten. In einer Studie wurden beispielsweise GNN-Modelle angewendet, um Knoten in einem Network Traffic Graph zu klassifizieren. Sie identifizierten dabei erfolgreich, welche IP-Ports Quellen bzw. Ziele von Angriffstaktiken aus dem MITRE-ATT&CK-Framework waren. Solche Ansätze gelten als besonders vielversprechend, da sie auch subtilere Angriffsmuster erkennen können, die sich nur im Zusammenspiel vieler Systeme und Ereignisse offenbaren.

Predictive Threat Analytics und automatisierte Erkennung: Ein weiteres zukunftsweisendes Einsatzfeld ist Predictive Threat Analytics. Durch die Auswertung historischer Incident Graphen können ML-Modelle Vorhersagen darüber treffen, wie sich ein zukünftiger Angriff im Netzwerk ausbreiten könnte oder welche Schwachstellen als Nächstes ins Visier geraten könnten. Erste Erkenntnisse deuten darauf hin, dass graphbasiertes Machine Learning potenzielle Bedrohungen identifizieren kann, die regelbasierte Systeme übersehen würden. So könnte beispielsweise unüberwachtes Lernen auf dem Graphen (etwa durch Algorithmen zur Erkennung von Anomalien oder Clustern) ungewöhnliche Muster oder Gruppierungen von Aktivitäten sichtbar machen, die keine bekannten Angriffssignaturen aufweisen, aber dennoch verdächtig sind und einer genaueren Untersuchung bedürfen.

Mit zunehmender Reife könnten KI-Modelle lernen, den Sicherheitsgraphen kontinuierlich zu beobachten und selbstständig frühe Anzeichen eines Angriffs zu erkennen – also eine automatisierte Threat-Hunting-Funktion

übernehmen, ganz ohne menschliches Zutun. Ebenso denkbar sind graphbasierte Funktionen zur Erkennung und Reaktion, die direkt ineinandergreifen: So könnte ein KI-System beispielsweise feststellen, dass ein bestimmter Angriffspfad im Graphen aktiv durchlaufen wird (z.B. die Kompromittierung eines Benutzerkontos, die zu einer Rechteausweitung führt) und daraufhin automatisch Gegenmaßnahmen einleiten (etwa die Isolation betroffener Knoten oder das Patchen einer Schwachstelle). Erste Ansätze finden sich bereits in heutigen SOAR-Plattformen (Security Orchestration, Automation and Response). Mit der zunehmenden Integration von Graph Intelligence werden sie künftig jedoch noch deutlich kontextbewusster und präziser agieren. Langfristig könnten daraus selbstheilende Netzwerke entstehen, in denen graphbasierte KI laufend dazulernt und gefährliche Verbindungen proaktiv unterbindet – noch bevor ein Angriff überhaupt Schaden anrichtet.

Einsatz in Cloud- und Hybridumgebungen: Der fortschreitende Übergang zu Cloud-basierten und hybriden IT-Infrastrukturen (also Umgebungen, die On-Premises-Systeme mit Cloud-Diensten kombinieren) bringt neue Sicherheitsherausforderungen mit sich, die sich besonders gut mit graphbasierten Technologien bewältigen lassen. Cloud-Umgebungen sind hochdynamisch: Server werden bei Bedarf automatisch gestartet oder beendet, Datenflüsse ändern sich ständig, klassische Netzwerkgrenzen verschwinden zunehmend. Graphbasierte Darstellungen sind in diesem Kontext besonders geeignet, da sie den sich ständig verändernden Zustand von Cloud-Konfigurationen sowie der Beziehungen zwischen ihren Komponenten präzise abbilden kann. Tatsächlich setzen immer mehr Lösungen im Bereich Cloud Security Posture Management (CSPM) auf Graphdatenbanken, um die Beziehungen zwischen Cloud-Ressourcen abzubilden – etwa, welche Benutzer oder Rollen auf welche Ressourcen zugreifen dürfen oder welche Netzwerksicherheitsgruppen welche virtuellen Maschinen betreffen. Eine einzige Fehlkonfiguration in der Cloud (beispielsweise ein öffentlich zugänglicher Speicher-Bucket oder eine zu weit gefasste IAM-Rolle) kann bereits zu einem Sicherheitsvorfall führen Diese Schwächen sind im Kern auf fehlerhafte Beziehungen zwischen Ressourcen zurückzuführen, etwa wenn ein Bucket für „Everyone“ freigegeben ist oder eine Rolle externen Konten vertraut. Mit Graphabfragen lassen sich solche Beziehungsmuster schnell und skalierbar über Tausende von Ressourcen hinweg aufspüren. Es ist absehbar, dass Security Graphen künftig in Echtzeit mit jeder API-Aktion in der Cloud-Umgebung aktualisiert werden, sodass sich potenziell riskante Änderungen sofort erkennen lassen. Es gibt bereits einige Cloud-Anbieter die graphbasierte Sicherheits-Tools zur Verfügung stellen: Microsoft Azure bietet beispielsweise eine Security Graph API an, während AWS Neptune zur Analyse von IAM-Beziehungen nutzt. Drittanbieterplattformen gehen noch einen Schritt weiter und aggregieren Daten aus Multi-Cloud-Umgebungen in einem zentralen Graphen.

Das langfristige Ziel ist ein globaler Knowledge Graph, der die gesamte digitale Infrastruktur eines Unternehmens abbildet, inklusive On-Prem-Systemen, Cloud-Diensten, SaaS-Anwendungen, mobilen Geräten usw. Verknüpft über die zugehörigen Benutzer, Daten und Workflows, soll so eine ganzheitliche Form der Sicherheitsüberwachung entstehen, die nicht mehr an einzelne Plattformen gebunden ist, und damit die zentrale Frage moderner Sicherheitsstrategien beantworten soll: „Wie ist unsere aktuelle Sicherheitslage über alle Systeme hinweg?“

Auch in hybriden IT-Umgebungen eröffnet der Einsatz von Graphen neue Möglichkeiten zur Optimierung von Verteidigungsmaßnahmen über unterschiedliche Bereiche hinweg. So könnte ein Angriffsszenario einen Übergang zwischen Cloud und On-Premise beinhalten – etwa wenn ein Angreifer eine Cloud-VM kompromittiert und dort hinterlegte Zugangsdaten nutzt, um auf eine lokale Datenbank zuzugreifen. Ein Security Graph, der beide Umgebungen abbildet, würde solche übergreifenden Bewegungen sofort erkennen – anders als herkömmliche, voneinander getrennte Überwachungssysteme von Cloud- und On-Prem-Systemen, welche sie möglicherweise übersehen würden.

Mit der zunehmenden Nutzung containerisierter Microservices, serverloser Funktionen sowie von Edge-Computing wird auch deren Einbindung in den Security Graph immer wichtiger. Der Graph fungiert dabei als verbindendes Element, das es Sicherheitsteams ermöglicht, eine komplexe IT-Architektur ohne klare physische Grenzen zu verstehen und zu überwachen. Gerade für DevSecOps-Teams ergeben sich daraus große Vorteile:

Entwickler und Sicherheitsexperten können auf Basis des Graphen gemeinsam prüfen, ob neue Deployments unerwünschte Verbindungen schaffen oder bestehende Sicherheitsrichtlinien verletzen. Künftige Ansätze könnten sogar Graphtechnologien verwenden, um Änderungen noch vor der eigentlichen Umsetzung zu simulieren, etwa nach dem Prinzip: „Zeig mir, wie sich der Einsatz dieses neuen Microservices auf unsere Umgebung auswirkt und welche potenziellen Risiken dadurch entstehen könnten." Die Graphmodellierung wird so zu einem Werkzeug für vorausschauende, präventive Sicherheitsplanung – lange bevor ein System tatsächlich in Betrieb geht.

Technische und ethische Herausforderungen: Aus großer Macht folgt große Verantwortung

Trotz ihres Potenzials, bringt die breite Einführung graphbasierter Cybersicherheit technische wie ethische Herausforderungen mit sich, die ernsthaft adressiert werden müssen:

- **Datenschutz und Governance:** Security Graphen erfassen naturgemäß sehr detaillierte Informationen über Systeme, Nutzer und deren Interaktionen. Werden diese Daten nicht sorgfältig verwaltet, kann das zu erheblichen Datenschutzbedenken führen, oder dazu, dass der Security Graph selbst zum Angriffsziel wird. Ein Beispiel: Ein Insider-Threat-Graph, der sämtliche Zugriffe und Kommunikationsmuster aller Mitarbeiter abbildet, gleicht im Grunde einem sehr sensiblen Dossier über die jeweils einzelnen Personen. Umso wichtiger ist es, dass Unternehmen strikte Zugriffskontrollen und klare ethische Richtlinien dafür definieren, wer Sicherheitsgraphen einsehen oder abfragen darf. Auch gesetzliche Vorgaben wie die DSGVO spielen eine zentrale Rolle, sobald persönliche Informationen in die Analyse einfließen. Eine besondere Herausforderung besteht darin, sicherzustellen, dass Graphdaten ausschließlich zur Verbesserung der Sicherheit verwendet werden und nicht zur unverhältnismäßigen Überwachung von Mitarbeitenden. Das Spannungsfeld zwischen Sicherheit und Privatsphäre wird auch künftig ein zentrales Thema sein. Gleichzeitig können Graphen aber auch zum Schutz der Privatsphäre beitragen, etwa durch das Erkennen ungesicherter personenbezogener Daten oder die konsequente Durchsetzung von Least Privilege. Entscheidend ist: Der Einsatz dieser Technologien muss stets transparent, zweckgebunden und verhältnismäßig erfolgen.

- **Skalierung und Performance:** Die Graphanalyse großer Datenmengen ist technisch anspruchsvoll. Security Graphen in Unternehmen können Millionen von Knoten – etwa Nutzer, Geräte oder Dateien – und zig Millionen von Kanten (z.B. Logins, Netzwerkflüsse oder Zugriffsberechtigungen) umfassen. Diese Datenmengen in nahezu Echtzeit auszuwerten, stellt hohe Anforderungen an graphbasierte Datenbanken und Analyseverfahren. Fortschritte in verteilten Graphdatenbanken und Big-Data-Verarbeitung – etwa durch Partitionierung oder parallele Rechenverfahren – ermöglichen es inzwischen, sehr große Graphen wirksam zu analysieren. Die Verarbeitung sogenannter „Big Graph Data" ist bereits heute ein aktives Forschungsfeld in der Informatik. Eine Studie etwa nutzte einen Security Graph mit rund 263.000 Knoten und 18,5 Millionen Kanten, um erfolgreich Netzwerkverkehr und Angriffstaktiken zu analysieren. Bei globalen Infrastrukturen mit Milliarden von Knoten und Kanten kommen aktuelle Systeme allerdings noch immer an ihre Grenzen. Gleichzeitig ist die Entwicklung vielversprechend: Moderne Graphdatenbanken werden stetig skalierbarer, und spezialisierte Graph-Analytics-Engines (die oft In-Memory-Computing oder GPUs einsetzen), machen es zunehmend möglich, selbst größte Datenmengen effizient zu verarbeiten.

- **Komplexität und Fachwissen:** Der produktive Einsatz graphbasierter Methoden erfordert spezifisches Know-how – und genau daran mangelt es vielen Organisationen noch. Sicherheitsanalysten und -ingenieure müssen sich mit Graph-Abfragesprachen wie Cypher, Gremlin oder GraphQL vertraut machen, um die Ergebnisse solcher Analysen richtig interpretieren zu können. Für viele Sicherheitsteams, die bisher vorwiegend mit linearen oder tabellarischen Datenmodellen gearbeitet haben, bedeutet das eine erhebliche Umstellung. Um diese Einstiegshürden zu senken, entstehen zunehmend benutzerfreundliche Oberflächen und Schulungsprogramme, die die Nutzung von Graphanalyse breiter zugänglich machen. Auch Visualisierungstools werden stetig weiterentwickelt, mit dem Ziel, dass sich Graphausgaben so intuitiv lesen lassen wie ein Diagramm,

ohne dass dafür tiefgehende mathematische Kenntnisse erforderlich sind. Langfristig wird sich das analytische Sicherheitsdenken stärker auf das Verständnis von Beziehungen ausrichten. Für kommende Generationen von Fachkräften wird der kompetente Umgang mit Graphen („Graph Literacy“) somit zum festen Bestandteil der Ausbildung in der Cybersicherheit werden.

- **Interoperabilität:** Mit dem wachsenden Angebot spezialisierter graphbasierter Sicherheitstools – etwa für Cloud-Umgebungen, Identitätsmanagement oder Schwachstellenanalyse – stellt sich eine weitere Herausforderung: die Integration dieser Systeme in eine nahtlos und einheitliche Sicherheitsarchitektur. Damit Unternehmen nicht in isolierten „Graph-Silos“ arbeiten, braucht es gemeinsame Austauschformate und Datenmodelle. Standards wie STIX, das bereits graphähnliche Strukturen für Threat Intelligence aufweist, könnten hier eine Basis bilden. Denkbar ist auch die zunehmende Verbreitung föderierter Graphabfragen – also die Möglichkeit, mehrere Graphen mit einer einzigen Abfrage gleichzeitig zu durchsuchen, beispielsweise den internen Asset Graph und den Threat Intelligence Knowledge Graph.

Trotz dieser Herausforderungen bewegt sich die Cybersicherheit eindeutig in Richtung einer stärkeren Integration graphbasierter Technologien, zumal ihre Vorteile viele der zentralen Schwachpunkte moderner Sicherheitsoperationen adressieren. Graphbasierte KI-Systeme werden voraussichtlich als intelligente Assistenten für menschliche Analysten fungieren und Zusammenhänge wesentlich schneller erkennen, als dies mit manuellen Methoden möglich wäre. Cloud Security Graphen könnten als Echtzeit-Karten in einem War Room genutzt werden, um auf einen Blick zu zeigen, wo sich in der zunehmend komplexeren Cloud-Umgebung kritische Vorfälle anbahnen. Ebenso denkbar sind graphgestützte Sicherheitssimulationen – vergleichbar mit digitalen Kriegsspielen – bei denen hypothetische Bedrohungen in einen Security Graph eingespeist werden, um zu beobachten, wie das System darauf reagiert. Schwachstellen könnten auf diese Weise erkannt und gezielt behoben werden, noch bevor ein echter Angriff erfolgt.

Im Sinne einer verantwortungsvollen technologischen Entwicklung muss die Cybersicherheitsbranche jedoch sicherstellen, dass diese Werkzeuge ethisch eingesetzt und nicht unbeabsichtigt zum Mittel der Überwachung oder Diskriminierung werden. Das bedeutet: Datenschutz muss von Anfang an mitgedacht werden („Privacy by Design“). Automatisierte Entscheidungen müssen nachvollziehbar und überprüfbar bleiben – etwa um zu verhindern, dass eine KI einen legitimen Benutzer fälschlicherweise aussperrt. Und nicht zuletzt gilt: Bei sicherheitskritischen Vorgängen darf der Mensch als letzte Entscheidungsinstanz nicht fehlen – „Human in the Loop“ bleibt unverzichtbar.

Fazit und Call to Action

In einer Zeit zunehmender Cyberbedrohungen und immer komplexerer IT-Umgebungen, hat sich die Graphanalyse zu einem strategischen Eckpfeiler moderner Cybersicherheit entwickelt.

Dieses Paper hat aufgezeigt, wie sich die ursprünglich mathematische Disziplin der Graphentheorie seit Eulers berühmtem Brückenrätsel aus dem 18. Jahrhundert zu einem unverzichtbaren Werkzeug in der digitalen Verteidigung weiterentwickelt hat. Heute bildet sie die Grundlage für zentrale Sicherheitsanwendungen wie Netzwerkvisualisierung, Bedrohungserkennung und die Umsetzung von Zero-Trust-Richtlinien. Die Vorteile graphbasierter Ansätze sind klar: Sie liefern Kontext und Übersicht dort, wo klassische Tools häufig an ihre Grenzen stoßen. Sie ermöglichen es Sicherheitsteams, auch in riesigen Datenmengen Zusammenhänge zu erkennen, verborgene Angriffspfade aufzudecken, Abhängigkeiten zwischen Systemen und Assets zu visualisieren und Ereignisse in Echtzeit miteinander zu verknüpfen.

Für Entscheidungsträger in Unternehmen bedeutet das konkret: besserer Schutz geschäftskritischer Assets,

effizientere Nutzung von Sicherheitsressourcen und fundierte datengestützte Entscheidungen im Risikomanagement. Für Sicherheitsverantwortliche wiederum bedeutet es ein neues Werkzeug, um verstreute Hinweise zu einem klaren Bedrohungsbild zusammenzuführen – häufig in Sekundenbruchteilen.

Im Zusammenhang mit Zero Trust zeigt sich der Mehrwert graphbasierter Technologien besonders deutlich. Zero Trust verlangt eine kontinuierliche Überprüfung und granulare Kontrolle aller Verbindungen. Im Grunde behandelt es jedes Unternehmen als einen dynamischen Graphen von Interaktionen, bei dem jede Verbindung kontinuierlich verifiziert werden muss. Graphtechnologien machen in diesem Kontext das Unsichtbare sichtbar: Sie kartieren Mikroperimeter, validieren jede Verbindung und ermöglichen eine konsistente Durchsetzung von Zero-Trust-Prinzipien. Organisationen, die Graphanalyse in ihre Zero-Trust-Strategie integrieren, gewinnen so einen entscheidenden Vorteil bei der Erkennung von Anomalien und der Eindämmung lateraler Bewegungen. Angesichts all dieser Vorteile liegt der nächste Schritt auf der Hand: Unternehmen sollten beginnen, graphbasierte Sicherheitsansätze schrittweise und praxisorientiert einzuführen. Dazu bieten sich folgende Maßnahmen an:

- **Identifizieren Sie Potenzial in Ihrer Umgebung:** Analysieren Sie, wo Beziehungen in Ihrer Umgebung eine zentrale Rolle spielen – etwa bei mangelnder Netzwerkvisibilität, unvollständigem Kontext in Incident-Untersuchungen oder unklaren Cloud-Zugriffsrechten. Solche Problemfelder eignen sich hervorragend für erste graphbasierte Anwendungsfälle. Wählen Sie ein konkretes Einsatzszenario (z.B. die Visualisierung von Berechtigungsstrukturen oder die Nachverfolgung eines früheren Sicherheitsvorfalls) und erproben Sie dort einen graphbasierten Ansatz.

- **Nutzen Sie bestehende Tools und Plattformen:** Es ist nicht nötig, eine eigene Graphlösung von Grund auf zu entwickeln. Viele moderne Sicherheitsplattformen bieten bereits graphbasierte Visualisierungen und Analysefunktionen an. Einige SIEM- und XDR-Lösungen stellen beispielsweise Attack Graphen oder Ansichten der Beziehungen zwischen Entitäten bereit. Auch Cloud-Anbieter bieten Werkzeuge, mit denen sich die Beziehungen zwischen Ressourcen abbilden lassen.

Diese Funktionen lassen sich oft direkt in bestehende Sicherheitsprozesse einbinden. Darüber hinaus können Open-Source-Graphdatenbanken wie Neo4j oder TigerGraph genutzt werden, um mit exportierten Sicherheitsdaten zu experimentieren – etwa durch eigene Abfragen oder maßgeschneiderte Visualisierungen. Selbst ein „Proof-of-Concept"-Graph, der nur einen Ausschnitt der eigenen Umgebung abbildet, kann bereits erste wertvolle Erkenntnisse liefern.

- **Investieren Sie in Know-how und Kultur:** Motivieren Sie Ihre Sicherheitsanalysten und IT-Mitarbeiter, sich mit den Grundlagen der Graphanalyse vertraut zu machen. Dazu können Schulungen zu Graph-Abfrage-Sprachen oder Workshops zu visueller Analytik gehören. Fördern Sie eine Denkweise, in der Teams bei komplexen Problemen sich die Frage stellen: „Kann man das als Graph modellieren?". Mit wachsender Erfahrung wird die Nutzung von Graphen so zu einem natürlichen Bestandteil des Sicherheits-Toolkits. Es kann außerdem hilfreich sein, eine Person zum sogenannten „Graph Champion" zu ernennen, der erste Projekte vorantreibt und erfolgreiche Anwendungsbeispiele intern weitergibt.

- **Integration und Weiterentwicklung:** Sobald erste graphbasierte Erkenntnisse vorliegen, sollten diese in die täglichen Abläufe integriert werden. Beispielsweise kann eine graphbasierte Visualisierung in das Dashboard des Security Operations Centers (SOC) aufgenommen werden, um besonders kritische Vorfälle zu überwachen. Ebenso können die Ergebnisse von Graphanalysen in Risikoberichten für das Management berücksichtigt werden. Sammeln Sie regelmäßig Feedback und verbessern Sie fortlaufend die Datenquellen und Abfragen, die Ihren Security Graph speisen. Sicherheit ist ein fortlaufender Prozess – und ebenso werden sich auch Ihre Graphen weiterentwickeln: durch neue Datenquellen (etwa Threat-Intelligence-Feeds oder Benutzerdaten), neue Analyseverfahren (z.B. den Einsatz von Machine-Learning-Modellen im Graphen) und mit jeder schritt-

weisen Erweiterung – vom ersten Anwendungsfall bis hin zum unternehmensweiten Einsatz.

- **Führungsebene mit visuellen Erkenntnissen einbinden:** Unterschätzen Sie nicht die Wirkung von graphbasierten Visualisierungen in Präsentationen für Führungskräfte oder Aufsichtsgremien. Eine prägnante Darstellung der Bedrohungslandschaft oder der größten Risiken – mit Knoten und Kanten – kann einen bleibenden Eindruck hinterlassen und das Bewusstsein für vernetzte Risiken deutlich schärfen. Solche Visualisierungen fördern das Verständnis für komplexe Zusammenhänge und unterstützen Sicherheitsinitiativen durch anschauliche, datenbasierte Einblicke. Sie vermitteln einen modernen, erkenntnisgetriebenen Ansatz für Cybersicherheit, der bei Entscheidungsträgern auf Akzeptanz stößt.

Der Einsatz graphbasierter Cybersicherheit bringt Organisationen auf das nächste Reifegradniveau. Er verschafft Organisationen die notwendige Übersicht, um Bedrohungen nicht nur zu erkennen, sondern auch zu antizipieren und letztlich zu verhindern. Da Cyberangriffe immer komplexer werden – etwa durch KI-gestützte Attacken, Angriffe auf Lieferketten oder die zunehmende Anwendung von Cloud-Diensten – wird die Fähigkeit, die gesamte Sicherheitsumgebung als zusammenhängendes System zu verstehen, immer wichtiger. Nur wer diese Zusammenhänge erkennt, kann effektiv handeln. Graphtechnologien bieten genau diese ganzheitliche Perspektive. Unternehmen, die bereits heute beginnen, ihren eigenen Security Graph aufzubauen, verschaffen sich damit einen entscheidenden Vorsprung – durch mehr Visibilität, schnellere Reaktionsfähigkeit und ein tieferes Verständnis ihrer gesamten digitalen Infrastruktur.