GLOBAL PERSPECTIVES & INSIGHTS

Cybersicherheit

TEIL 1: Cyberbedrohungen in einer von KI geprägten Welt

TEIL 2: Sicherstellung der Cyberresilienz

TEIL 3: Festlegung einer neuen Zero-Trust-Grenze

The Institute of Internal Auditors

TEIL 1

Cyberbedrohungen in einer von KI geprägten Welt

Über die Experten

Antonio Cacciapuoti, CIA

Antonio Cacciapuoti ist Leiter der Internen Revision bei Eurizon Capital S.A. Luxemburg, der Vermögensverwaltungsgesellschaft der Intesa Sanpaolo Gruppe.

Bradley Niedzielski, CPA

Bradley Niedzielski ist Partner im Bereich Audit and Assurance und Leiter des Bereichs Finance Transformation and GenAI bei Deloitte & Touche LLP, wo er öffentliche und private Unternehmen aus der Finanzdienstleistungsbranche betreut.

Die Fortschritte im Bereich der künstlichen Intelligenz (KI) haben im letzten Jahr dazu geführt, dass sich Unternehmen bemühen, mit der Entwicklung Schritt zu halten und die Chancen und Gefahren zu verstehen, die diese Technologien darstellen. Als Teil dieser Bemühungen müssen Unternehmen die wachsende Gefahr berücksichtigen, die KI für ihre Sicherheitsbemühungen darstellen kann, insbesondere angesichts der nahezu vollständigen Abhängigkeit der Unternehmen von Online-Informationen und -Transaktionen. Böswillige Akteure haben sich schnell KI-gestützten Tools zugewandt, um ihre Fähigkeit zu verbessern, die Cyberabwehr von Unternehmen zu durchbrechen. In diesem Kurzbericht wird untersucht, wie sich Cyberbedrohungen in einer KI-gesteuerten Welt verändert haben und wie die Interne Revision Unternehmen dabei helfen kann, neue Ansätze für Cybersicherheit zu entwickeln

Eine Evolution der Cyberkriminalität

Während eine starke Cyberabwehr schon immer von entscheidender Bedeutung war, nutzen bösartige Akteure nun KI, um ihre Fähigkeit, die Abwehrmechanismen von Unternehmen zu überwinden, zu verbessern und zu erweitern. „KI ist keine neue Art von Cyberangriff, sondern eine Weiterentwicklung", sagt Antonio Cacciapuoti, Leiter der Internen Revision bei Eurizon Capital S.A. Luxemburg. KI wird in einer Weise eingesetzt, die in Bezug auf Geschwindigkeit, Umfang, Komplexität und Anpassungsfähigkeit fortschrittlicher ist als herkömmliche Cyberangriffe. Außerdem „baut sie wie ein Virus mit der Zeit eine Resistenz auf, was sie noch gefährlicher macht", sagt er.

KI wird für Angriffe eingesetzt, die von eng gefassten bis hin zu breit angelegten zerstörerischen Angriffen reichen. Während viele in der Geschäftswelt inzwischen regelmäßig KI-generierte Dokumente für E-Mails oder Berichte verwenden, nutzen böse Akteure KI-generierte Dokumente auch für kriminelle Zwecke, sagt Bradley Niedzielski, Partner für Audit and Assurance bei Deloitte in New York.

An einer anderen Front zielen Phishing-Angriffen darauf, Sicherheitsbarrieren zu durchbrechen und an wertvolle Daten zu gelangen. Phishing ist zwar nicht neu, aber das FBI warnt vor KI-gesteuerten Phishing-Angriffen, „die sich dadurch auszeichnen, dass sie überzeugende Nachrichten erstellen, die auf bestimmte Empfänger zugeschnitten sind und eine korrekte Grammatik und Rechtschreibung enthalten, wodurch die Wahrscheinlichkeit einer erfolgreichen Täuschung und eines Datendiebstahls erhöht wird".

Automatisiertes Spear-Phishing ist beispielsweise auf eine Person oder eine Gruppe zugeschnitten und zielt darauf ab, sensible Informationen zu stehlen oder sich Zugang zu einem System zu verschaffen. „KI kann soziale Medien, Kommunikationsmuster und verfügbare Daten über ein Ziel analysieren und dann Nachrichten erstellen, die den Empfänger eher dazu verleiten, sensible Informationen preiszugeben oder auf bösartige Links zu klicken", erklärt Cacciapuoti. Während es in der Vergangenheit möglich war, einem Video oder Anruf aufgrund der Kenntnis der Stimme oder der Merkmale einer Person zu vertrauen, ist es mit Deepfakes (simulierten Videos einer Person) und Voice Hacking, bei dem die Stimme einer Person nachgeahmt wird, möglich, bestimmte Ziele zu täuschen und zu manipulieren.

Dies sind nicht die einzigen KI-bezogenen Bedrohungen, mit denen Unternehmen konfrontiert sind. KI-gesteuerte Malware kann sich an die Zielumgebung anpassen und ihr Verhalten ändern, sodass sie für herkömmliche Sicherheitssysteme schwerer zu erkennen ist, so Cacciapuoti. „Sie kann der grundlegenden Erkennung leicht entgehen und polymorphe Techniken verwenden, um ihren Code zu ändern und sogar Abwehrmaßnahmen zu analysieren, um sie zu umgehen", sagt er. Noch wichtiger ist, dass sie vergiftete Daten in ein KI-Modell für maschinelles Lernen einbringen kann, das in Betrugserkennungssystemen verwendet wird, was dazu führt, dass die KI ungenaue Vorhersagen macht und gewisse Betrugsindikatoren übersieht.

Bei der intelligenten Datenexfiltration kann die KI gestohlene Daten und geistiges Eigentum in Echtzeit analysieren und Prioritäten setzen, welche Informationen am wertvollsten für die Exfiltration sind. Sie kann diese Informationen dann verschlüsseln und ein Lösegeld für ihre Freigabe verlangen, sagt er. KI-gesteuerte Angriffe können auch die Anmeldeinformationen gültiger Benutzer kompromittieren, sodass sie sich im System bewegen können.

Die Risiken von KI-gesteuerten Cyberangriffen sind wichtig, weil so viel auf dem Spiel steht. Das Durchsickern oder der Missbrauch sensibler Daten könnte die Wettbewerbsposition eines Unternehmens beeinträchtigen oder Strafen für die Nichteinhaltung von Datenschutzbestimmungen nach sich ziehen. Jeder Verstoß könnte dazu führen, dass Kunden und Geschäftspartner das Vertrauen in das Unternehmen verlieren. Ransomware- und Malware-Angriffe können den Betrieb stören und wichtige Systeme lahmlegen.

Viele Anwendungen wären vor nicht allzu langer Zeit noch nicht vorstellbar gewesen, aber sie finden heute in Echtzeit statt. So

zahlte beispielsweise ein Angestellter eines multinationalen Unternehmens in Hongkong unwissentlich 25 Millionen Dollar an Betrüger, nachdem er in einem Videoanruf durch eine Deepfake-Simulation des Finanzchefs des Unternehmens dazu überredet worden war, wie CNN berichtet.

An anderer Stelle berichtet The Drive, dass ein leitender Angestellter von Ferrari einen Anruf von einem Deepfake erhielt, der sich als CEO des Unternehmens ausgab. Der Versuch wurde vereitelt, als die Zielperson eine Frage stellte, die nur der CEO beantworten konnte. In einem von Greylock Partners zitierten Fall nutzte ein nordkoreanischer Spion eine gefälschte Identität, um von einer Cybersicherheitsfirma eingestellt zu werden, und installierte dann sofort Malware auf den Geräten des Unternehmens.

Die beste Verteidigung

Glücklicherweise kann KI den Unternehmen auch dabei helfen, bösartige Akteure auszuschalten. „Um KI zu stoppen, muss man KI nutzen", sagt Cacciapuoti. Unternehmen müssen ausgefeiltere KI-gestützte Cybersicherheitsmaßnahmen einführen, um mit den sich entwickelnden Bedrohungen Schritt zu halten. „Wenn man die Technologie, die Kriminelle einsetzen, nicht genau kennt, wie kann man sie dann aufhalten?", fragt er. Unternehmen sollten sich mit den Tools und Strategien vertraut machen, die Cyberkriminelle einsetzen, und die vielen Möglichkeiten kennen, die sie zur Verbesserung der Cybersicherheit nutzen können.

Die Studie „The Need for AI-powered Cybersecurity to Tackle AI-driven Attacks“ der ISACA zeigt zahlreiche Möglichkeiten auf, wie fortschrittliche Technologien Angriffe verhindern können:

Wege zur Verhinderung von Angriffen

- Analyse umfangreicher Datensätze, um die Nutzung von Unternehmensressourcen und gefährdete Bereiche zu ermitteln, Bestandsaufnahme der Werte zu erstellen und Trends im Netzwerkverkehr und bei den Verhaltensweisen der Benutzer zu erkennen.
- Erkennung von Anomalien, einschließlich „ungewöhnlicher Anmeldungen, Zugriffsanfragen von einem neuen geografischen Standort oder einer neuen IP-Adresse, Zugriff neuer Nutzer, Berechtigungsänderungen für Dateien und andere Ressourcen, Abzug oder Löschen großer Datenmengen und ein exponentieller Anstieg des Datenverkehrs“.
- Einsatz von KI zum proaktiven Sperren, Abmelden oder Blockieren mutmaßlich bösartiger Akteure und Warnung der Systemadministratoren vor deren Aktivitäten.
- Kontinuierliche Überwachung der Systeme, um rasche Reaktionen zu ermöglichen.
- Nutzung prädiktiver Analyse, um potenzielle Sicherheitsbedrohungen zu antizipieren und Maßnahmen zu deren Vermeidung zu ergreifen.
- Aufspüren und Verhindern von Zero-Day-Bedrohungen, d. h. von neuen und unentdeckten Sicherheitslücken.
- Verringerung der Anzahl falsch positiver potenzieller Bedrohungen.
- Automatisierung von Sicherheitsbeurteilungen, um Reaktionen zu beschleunigen und menschliche Fehler zu minimieren.
- Skalierung zur Anpassung an neue Entwicklungen und Umgebungen, um kontinuierlichen Schutz zu bieten.

Unternehmen können KI nutzen, um Daten aus verschiedenen Quellen zu aggregieren, zu analysieren und zu korrelieren, um tiefere Einblicke zu gewinnen, sagt Cacciapuoti. Sie können auch die Verarbeitung natürlicher Sprache (NLP) nutzen, um große Textdaten zu analysieren. Wenn Interne Revisoren beispielsweise Verträge analysieren sollen, kann NLP wichtige Textdaten extrahieren, die das System dann auswerten kann.

Berücksichtigung von KI-Überlegungen

Da ein Unternehmen nie 100 % des Risikos abdecken kann, empfiehlt Niedzielski, zunächst die Bedrohungen in den verschiedenen Geschäftsbereichen strategisch zu beurteilen. Dazu gehört die Identifizierung potenzieller KI-Betrugsvektoren und die Bewertung der Wahrscheinlichkeit, dass sie angegriffen werden, sowie des potenziellen Ausmaßes und der Auswirkungen. Der nächste Schritt besteht seiner Meinung nach darin, die Wirksamkeit der bestehenden Kontrollen zu ermitteln.

Als Teil dieser Bemühungen empfiehlt Niedzielski, die entstehenden Fähigkeiten von GenAI zu nutzen, wie z. B. Advanced Reasoning und Mustererkennung, um gängige Taktiken wie KI-generierte Phishing-Versuche und Deepfakes zu erkennen. Einige Unternehmen verwenden Protokolle und Technologien, um zu überprüfen, ob ein Anruf von intern oder extern getätigt wurde.

„Fortschrittliche Technologien können helfen, damit verbundene Risiko zu minimieren“, sagt er. In einigen Fällen jedoch, z. B. wenn es darum geht, sofort festzustellen, ob ein Anrufer oder ein Sitzungsteilnehmer ein Betrüger ist, müssen sich die Mitarbeiter auf ihr Bauchgefühl verlassen oder bereit sein zu hinterfragen, warum z. B. ein CEO anruft und um eine Überweisung bittet. In solchen Situationen sollten die Mitarbeiter ermutigt werden, ihrem Instinkt zu vertrauen und die Person unter ihrer Firmennummer zurückzurufen oder, wenn sich der vermeintliche Anrufer im selben Gebäude befindet, einfach zu überprüfen, wer es ist.

Ein multidisziplinäres Team aus Fachleuten von Interner Revision, Risikomanagement, IT, Cybersicherheit und anderen relevanten Funktionen kann die Fortschritte bei der KI überwachen und kontinuierlich Updates für das Risikomanagement, Sicherheitsprotokolle und Betrugserkennungssysteme bereitstellen. Das Team kann zusammenarbeiten, Versuche identifizieren und darauf reagieren, indem es beispielsweise überlegt, welche Kontrollen Schäden am besten verhindern oder begrenzen, sagt Niedzielski.

Er empfiehlt den Unternehmen auch, regelmäßig ihre Erfahrungen auszutauschen und KI-Schwachstellen zu diskutieren, mit denen andere konfrontiert wurden. „Nicht nur erfolgreiche Bemühungen, sondern auch Zeiten, in denen etwas schiefgelaufen ist und wie das Unternehmen daraus gelernt hat“, rät er. „Durch Wissensaustausch, Schulungen und angemessene Risikobeurteilungen lässt sich das Risiko von KI-bedingtem Betrug minimieren.“

In diesem Umfeld sollten Schulungen oberste Priorität haben, um das Bewusstsein der Mitarbeiter für potenziell verdächtige Aktivitäten zu schärfen und gleichzeitig geeignete Maßnahmen zur Behebung von Vorfällen zu ergreifen, so Niedzielski. Cacciapuoti merkt an, dass es auch möglich ist, KI-Simulationen zu verwenden, um Cybersicherheitsschulungen in Echtzeit in realen Situationen durchzuführen. KI kann das Verhalten einzelner Mitarbeiter bei Schulungen analysieren und Erkenntnisse für Verbesserungen liefern.

Der Beitrag der Internen Revision

Die Interne Revision kann laut Cacciapuoti dazu beitragen, dass die Bemühungen des Unternehmens den Herausforderungen der KI gerecht werden, einschließlich der Nutzung des Potenzials bei gleichzeitiger Risikominderung. „Die Interne Revision sollte eine umfassende Beurteilung der Risiken vornehmen, KI-Systeme auf Sicherheit, Ethik und Complia nce prüfen und sichere Innovationen unterstützen“, sagt er. „Sie kann sich an der Ausarbeitung einer Cyberstrategie beteiligen, die robust genug ist, um mit KI-Bedrohungen fertig zu werden.“

> „KI wird Interne Revisoren niemals ersetzen, aber sie kann ein leistungsstarker Helfer sein.“
>
> **Antonio Cacciapuoti, CIA**

Während die Interne Revision in der Regel eine wichtige Verteidigungslinie darstellt, sollte sie laut Cacciapuoti in Bezug auf KI auch als Offensivlinie fungieren und einen dynamischen Ansatz beim Risikomanagement verfolgen. „Warum warten, bis das Risiko eintritt, wenn man es direkt attackieren kann?“, fragt er.

Das bedeutet, bei der Nutzung neuer Technologien eine Vorreiterrolle einzunehmen, damit das Unternehmen seine Chancen maximieren und gleichzeitig angemessene Governance-Kontrollen und kontinuierliche Verbesserungen gewährleisten kann.

In der Internen Revision „wird KI die Internen Revisoren niemals ersetzen, aber sie kann ein leistungsstarker Helfer sein“, so Cacciapuoti. Er sagt, dass die Interne Revision vom Einsatz von KI profitieren kann, um:

- Große Datenmengen zu analysieren und Stichproben in den Tests so zu erweitern, dass sie der Grundgesamtheit sehr nahekommen.
- Testverfahren zu automatisieren und Schlüsselkontrollen zu überwachen, indem Sie sich wiederholende Aufgaben übernehmen, damit sich die Internen Revisoren auf höherwertige Aufgaben konzentrieren können.
- KI-Algorithmen zur kontinuierlichen Überwachung von Daten zu nutzen, anstatt sich auf periodische Prüfungen zu verlassen. So können ungewöhnliche Aktivitäten viel früher erkannt und angegangen werden.
- Prädiktive Analysen für die Prognose zukünftige Ergebnisse zu nutzen und fundiertere Entscheidungen und Empfehlungen zu treffen.
- Arbeitspapiere schnell zusammenzufassen, damit Interne Revisoren sie für die Erstellung von Abschlussberichten verwenden können.

KI ermöglicht eine einheitlichere und effizientere Verwaltung von Feststellungen über alle Kontrollfunktionen hinweg. „In einem großen Unternehmen gibt es viele Aufträge aus verschiedenen Funktionen zu berücksichtigen“, sagt Cacciapuoti. KI ermöglicht es den Internen Revisoren, die Daten auf einheitliche Weise zusammenzuführen, um Doppelarbeiten zu vermeiden.

Um die Risiken zu mindern und die Vorteile zu nutzen, empfiehlt Niedzielski, dass Interne Revisoren ihr Wissen über technologische Fortschritte ständig aktualisieren. „Es gibt jeden Tag etwas Neues“, sagt er.

KI-gestützte Cyberbedrohungen: Die Fakten

- 97 % der Sicherheitsexperten sind besorgt, dass es in ihrem Unternehmen zu einem durch KI ausgelösten fatalen Cybersicherheitsvorfall kommen wird.
- 75 % der Sicherheitsexperten mussten ihre Cybersicherheitsstrategie im letzten Jahr aufgrund der Zunahme von KI-gestützten Cyberbedrohungen ändern.
- 73 % der Sicherheitsteams wollen sich stärker auf präventive Fähigkeiten konzentrieren.
- 61 % der Unternehmen verzeichneten im vergangenen Jahr einen Anstieg der Deepfake-Vorfälle.
- 75 % dieser Angriffe gaben sich als CEO oder als ein anderes Mitglied der Führungsebene aus.

Quelle: GenAI in Cybersecurity: Friend or Foe? Voice of SECOPS, Fifth Edition 2024.

Sie sollten sich darauf konzentrieren, proaktive, nicht reaktive, Antworten auf potenzielle Risiken zu finden. Während die Welt versucht, sich neue Technologien zunutze zu machen, sollten sich Interne Revisoren auch auf Governance und die Einhaltung neuer Vorschriften und ethischer Standards konzentrieren, um die Integrität des Unternehmens zu schützen, sagt er.

„Interne Revisoren sollten sich in die Lage eines Angreifers versetzen“, sagt Niedzielski. „Fragen Sie nicht, wie ein böser Akteur die Organisation infiltrieren würde, sondern was Sie tun würden, wenn Sie ein böser Akteur wären, basierend auf dem, was Sie über die Organisation wissen. Berücksichtigen Sie nicht nur eine quantitative, sondern auch eine qualitative Sicht auf die Organisation.“

Interne Revisoren sollten nicht versuchen, im Alleingang vorzugehen, sagt Cacciapuoti. Er empfiehlt die Koordination mit allen Anbietern von Prüfungssicherheit und Stakeholdern, einschließlich der Kontrollfunktionen, der Compliance, dem Risikomanagement, den externen Prüfern und den Regulatoren, um Risiken zu verhindern und zu mindern. „Die Zusammenarbeit zwischen KI-Tools und Cybersicherheitsexperten sowie ein starker Governance-Rahmen sind unerlässlich, um in dieser Landschaft zu navigieren und auf neue und aufkommende Risiken zu reagieren“, sagt er.

TEIL 2

Sicherstellung der Cyberresilienz

Über die Experten

DC Chang, CPA, CDPSE, CISSP, CRISC, CISA

DC Chang ist Audit Director, Digital Technology and Cybersecurity, bei United Airlines in Dallas, Texas.

Michael Echols, CISSP

Michael Echols ist CEO von Max Cybersecurity LLC in Washington, DC.

Justin Headley, CPA, CISSP, CISA, CRISC

Justin Headley ist Senior Manager in der Risk Advisory & Assurance Services Group von Warren Averett in Birmingham, Alabama.

Auch wenn Unternehmen sich bemühen, geeignete Instrumente zur Verhinderung von Cyberangriffen einzusetzen, ist es fast sicher, dass sie in irgendeiner Form von Sicherheitsverletzungen oder Angriffen betroffen sein werden. Vor diesem Hintergrund müssen sich Unternehmen auch auf ihre Fähigkeit konzentrieren, auf einen Cyberangriff zu reagieren und sich schnell davon zu erholen. In diesem Teil wird erörtert, wie man Angriffe am besten verstehen und abwehren kann, und es wird die Rolle des Internen Revisors bei der Stärkung der Reaktionsfähigkeit einer Organisation beschrieben.

Die Weichen für die Erholung stellen

Im besten Fall ist Cyberresilienz nicht nur eine Reaktion auf eine schwierige Situation. Laut Michael Echols, CEO von Max Cybersecurity LLC, handelt es sich um ein Kontinuum von Praktiken (Planung, Prozesse, Analyse, Schulung, kritische Dienste und Management), die sicherstellen, dass ein Unternehmen seinen Betrieb aufrechterhalten kann. Diese Praktiken ermöglichen die Wiederherstellung oder Aufrechterhaltung der Unternehmensfunktionen nach einem Angriff, müssen aber lange vor dem Auftreten eines Problems eingerichtet werden.

Echols arbeitete beispielsweise mit einer Anwaltskanzlei zusammen, die alle ihre Kontakte über ihre Website erhielt. In der Regel erhielt die Kanzlei täglich viele Anfragen, aber irgendwann vergingen zwei bis drei Tage, bis die Kanzlei bemerkte, dass sie keine Anfragen mehr erhielt und schließlich feststellte, dass sie gehackt worden war. „Die Kanzlei hätte bereits einen Prozess für die kontinuierliche Überwachung und Benachrichtigung über einen ungewöhnlichen Rückgang der Anfragen über das Internet einrichten müssen, da diese die Hauptgeschäftsquelle (eine kritische Funktion) darstellten", sagt er.

Zu identifizierende Probleme, wie z. B. ein Rückgang des Internetverkehrs, werden für jedes Unternehmen unterschiedlich sein, und es wird wahrscheinlich mehr als ein Problem geben. In vielen Fällen werden Unternehmen auf einen Vorfall vorbereitet sein wollen, der ihre Stromversorgung beeinträchtigt, indem sie Maßnahmen zum Einsatz von Generatoren ergreifen, die vom Hauptgeschäft unabhängig sind, sodass sie nicht von dem Angriff betroffen sind, sagt Echols.

> Cyberresilienz ist „die Fähigkeit, ungünstige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen, die Cyberressourcen nutzen oder durch sie ermöglicht werden, zu antizipieren, ihnen standzuhalten, sich von ihnen zu erholen und sich an sie anzupassen. Cyberresilienz soll es ermöglichen, Missionen oder Geschäftsziele, die von Cyberressourcen abhängen, in einer umkämpften Cyberumgebung zu erreichen."
>
> **U.S. National Institute of Standards and Technology**

Um sich auf die Zukunft vorzubereiten, muss man die aktuelle Cybersicherheitsumgebung im Kontext sehen, so DC Chang, Audit Director, Digital Technology and Cybersecurity, bei United Airlines. Vor zwanzig Jahren hatten die Unternehmen ihre eigenen Rechenzentren, und die Cybersicherheit bestand bis zu einem gewissen Grad darin, die Server hinter physischen Türen und Fenstern zu verschließen. Heute werden die Daten in einer virtuellen Umgebung gespeichert, die für böswillige Akteure auf der ganzen Welt angreifbar sein kann.

„Es gibt Abertausende von Fenstern und Türen, die wir jetzt, wo wir digital sind, im Auge behalten müssen, und täglich werden welche hinzugefügt oder entfernt", sagt Chang. Unternehmen müssen sich des Tempos und des Umfangs der digitalen Beschleunigung bewusst sein, um die Widerstandsfähigkeit zu entwickeln, die sie in einer Krise benötigen.

Governance und Kultur

Laut Justin Headley, Senior Manager in der Risk Advisory & Assurance Services Group von Warren Averett, spielt die Governance eine Schlüsselrolle beim Aufbau von Cyberresilienz. „Wir hören immer wieder, dass die Mitarbeiter die Schwachstelle sind, weil sie ein schwaches Passwort verwenden oder auf verdächtige Links klicken", sagt er. „Aber wenn die Führungskräfte nicht mitziehen, kann man nicht erwarten, dass die Mitarbeiter ihren Teil beitragen."

In vielerlei Hinsicht ist Cybersicherheit nicht nur ein technologisches, sondern auch ein kulturelles Problem. „Wenn Sie zwar die Einstellung von 90 % der Mitarbeiter im Unternehmen ändern , aber nur eine Person einen Link in einer E-Mail öffnet, kann dies

den Untergang des Unternehmens bedeuten“, sagt Echols. Eine Kultur, die sich der Cybersicherheit bewusst ist, klärt die Erwartungen des Unternehmens und stärkt das Vertrauen der Kunden und Geschäftspartner. „Banken waren unter den ersten, die sich für den Schutz vor Cyberangriffen entschieden haben“, sagt er, weil sie auf das Vertrauen der Kunden angewiesen sind.

Headley empfiehlt Führungskräften, eine Kultur der Cybersicherheit zu fördern, die über Standardmaßnahmen wie vierteljährliche E-Mails mit Tipps zur Cybersicherheit oder rudimentäre jährliche Sicherheitsschulungen hinausgeht. Zu den Maßnahmen, die sein Unternehmen ergreift, gehört der Versand eigener gefälschter Phishing-E-Mails an die Mitarbeiter und die anschließende Schulung derjenigen, die auf die eingebetteten verdächtigen Links klicken. „Man muss zeigen, wie Cybergovernance in der Praxis funktioniert, nicht nur in der Theorie", sagt er.

Führungskräfte können auch konkrete Schritte für den Fall eines Angriffs vorgeben. „Eine Organisation kann einen Angriff stoppen und sich erholen, wenn es praktische, wiederholbare Richtlinien und Verfahren gibt, die im Falle eines Vorfalls zu befolgen sind“, so Headley. Wenn die Führungskräfte an der Erprobung dieser Schritte beteiligt sind und an der Aufarbeitung der Probleme mitwirken, zeigen sie ihr Engagement für die Bemühungen, was für den Erfolg der Cybersicherheitsstrategie von großer Bedeutung sein kann.

- Bei 68 % der Sicherheitsverletzungen war ein nicht bösartiges menschliches Element beteiligt, z. B. wenn jemand auf einen Social-Engineering-Angriff hereinfällt oder einen Fehler macht.
- Die durchschnittliche Zeit, bis Nutzer auf Phishing-E-Mails hereinfallen, betrug weniger als 60 Sekunden.
- 15 % der Verstöße betrafen Dritte oder Lieferanten, einschließlich Software-Lieferketten, Hosting-Partner Infrastrukturen oder Datenverwahrer.

Quelle: Verizon Business 2024 Data Breach Investigations Report

Die Auswirkungen der Regulierung

Mit der endgültigen Regelung Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure hat die US-Börsenaufsicht die Erwartungen erhöht, indem sie von börsennotierten Unternehmen verlangt, wesentliche Vorfälle im Bereich der Cybersicherheit offenzulegen und regelmäßig offenzulegen, wie sie Cyberrisiken beurteilen, identifizieren und managen. „Die Vorschrift macht deutlich, dass es sich um ein wichtiges Thema handelt, mit dem sich jedes Unternehmen auf der Welt auseinandersetzen muss“, so Chang.

Neben anderen Anforderungen zwingt die Vorschrift Unternehmen dazu, sicherzustellen, dass ihre Cyberpraktiken einsatzfähig sind, so Headley. Er merkt an, dass die IT-Abteilung oft in einem Silo arbeitet und das Vertrauen von Führungskräften genießt, die ihre Arbeitsweise möglicherweise nicht vollständig verstehen. „Das wird sich ändern müssen", sagt er.

Es wird ein unternehmensweites Verständnis für den Umgang mit internen und Kundendaten sowie für den Umgang mit Cyberproblemen geben müssen. Wie bei vielen anderen Vorschriften, „wird es auf Transparenz ankommen“, sagt Echols. „Wenn es zu einem wesentlichen Vorfall gekommen ist, muss das Unternehmen einen klaren Prozess haben, wie es darauf reagiert.

KI in den Mix einbringen

Künstliche Intelligenz (KI) kann ein unschätzbares Werkzeug sein, um die Prävention von Cyberproblemen und die Widerstandsfähigkeit nach einem Angriff zu verbessern. Technologien wie Firewalls der nächsten Generation und Point-Protection-Systeme machen es einfacher, den Datenverkehr zu durchforsten und Anomalien zu finden, die untersucht werden sollten, sagt Headley. „Der Einsatz von KI hat sich in den letzten Jahren stark verändert und wird Unternehmen weiterhin dabei helfen, Angriffe besser zu erkennen und darauf zu reagieren.“

KI kann auch als Waffe gegen Unternehmen eingesetzt werden. „Wenn Sie Schwachstellen haben, die ignoriert wurden, wird KI den Hackern helfen, diese zu finden“, sagt Echols.

Neben anderen Erwägungen müssen die Unternehmen ein Gleichgewicht zwischen dem Streben nach größerer Effizienz durch neue Tools und der Notwendigkeit des Schutzes von Sicherheit und Privatsphäre finden, so Headley. Neue Technologien helfen Unternehmen, sich wiederholende Aufgaben zu eliminieren, die oft mit der Erfassung sensibler Informationen in Programme verbunden sind. Gleichzeitig „sehen wir weiterhin gezielte Angriffe auf diese Technologien, weil die Angreifer wissen, dass die Menschen die Technologie nicht vollständig verstehen“, was die sensiblen Daten in den Programmen besonders angreifbar machen kann.

Beim Aufbau der Resilienz müssen Unternehmen ihre Mitarbeiter in den sich entwickelnden Technologien schulen und sicherstellen, dass die Nutzung mit der Risikobereitschaft des Unternehmens übereinstimmt. „Ein Unternehmen kann über die besten Technologien und Fähigkeiten verfügen, aber ein Benutzer kann trotzdem unwissentlich oder manchmal auch wissentlich Daten über ein GenAI-Tool durch die Vordertür entweichen lassen“, sagt Headley.

Unternehmen sollten auch darauf achten, dass sie traditionelle Ansätze für Cyberangriffe nicht vernachlässigen. Viele Cyberprobleme werden durch Probleme verursacht, die nicht neu sind, wie z. B. Fehlkonfigurationen oder die Nichteinhaltung etablierter Praktiken, sagt Echols. Viele Vorfälle gehen auf bekannte Schwachstellen zurück, die nie behoben wurden, oder auf Patches, die nicht installiert wurden, sagt er. Daher ist es besonders wichtig, die Endbenutzer über neue und bestehende Bedrohungen aufzuklären. „Revisoren müssen unter die Haube schauen und ihren Kunden die richtigen Fragen stellen, um versteckte Schwachstellen zu entdecken, die durch Gleichgültigkeit entstanden sind“, sagt er.

„Stakeholder, insbesondere Geschäftsleitung und Überwachungsorgan einer Organisation, verlassen sich auf unabhängige, objektive und kompetente Prüfungssicherheit, um zu überprüfen, ob die Kontrollen für die Reaktion auf Cybervorfälle und die Wiederherstellung gut konzipiert und effektiv und effizient umgesetzt sind. Die Interne Revision schafft einen Mehrwert für die Organisation, wenn sie solche Dienstleistungen unter Einhaltung der Standards und unter Bezugnahme auf weithin anerkannte Kontrollrahmenwerke erbringt, insbesondere auf solche, die ausdrücklich von den IT- und IT-Sicherheitsfunktionen der Organisation verwendet werden.“

Quelle: Global Technology Audit Guide: Auditing Cyber Incident Response and Recovery, 2nd Edition, Global Practice Guide, The Institute of Internal Auditors, 2024

Wie die Interne Revision zur Verbesserung der Widerstandsfähigkeit beitragen kann

In diesem Umfeld sollte die Interne Revision darauf vorbereitet sein, die Ergebnisse ihrer Prüfungen so zu formulieren, dass sie die Widerstandsfähigkeit verbessern und Schwachstellen aufzeigen, damit die Kunden die potenziellen Folgen einer laxen Cybersicherheit verstehen, sagt Echols. Während die Kunden vielleicht davon ausgehen, dass ihnen das Schlimmste nie passieren kann, müssen die Internen Revisoren ihre Ungläubigkeit überwinden, damit sie sich das Unvorstellbare besser vorstellen können. Echols hatte zum Beispiel einen Kunden, dessen bewährte Praxis die Verwendung von Firmen-E-Mail-Adressen in Social-Media-Konten verbot, aber es gab keine offizielle Richtlinie. Der Fehler dieses Ansatzes wurde deutlich, als Ende letzten Jahres MGM einen erheblichen Datenverlust erlitt. Bei der Untersuchung des Vorfalls stellte sich heraus, dass ein Mitarbeiter seine berufliche E-Mail-Adresse auf einer Social-Media-Plattform verwendete. Die Hacker fanden die Informationen des Mitarbeiters auf LinkedIn und gaben sich bei einem Anruf beim IT-Helpdesk von MGM als jener Mitarbeiter aus, wodurch sie die Zugangsdaten für den Zugriff auf die Systeme von MGM erhielten und diese infizierten. „Bewährte Praktiken leiten sich aus Erfahrungen vieler ab und sollten, wenn möglich, zur Richtlinie gemacht werden“, sagt Echols.

Interne Revisoren müssen auch verstehen, dass der Complianceaspekt der Prüfung nur der erste Schritt zum Aufbau von Cyberresilienz ist. „Compliance ist nicht Sicherheit“, sagt Echols. Interne Revisoren sollten sich bemühen, ihre Feststellungen in größere Einsichten zu übersetzen, die das Team ihrer Kunden zur Verbesserung der Sicherheit nutzen kann, und Fragen zu stellen, die das Team möglicherweise noch nicht beantworten kann.

„Sie sollten in der Lage sein, den Kunden darauf hinzuweisen, dass das Versäumnis, eine Antwort auf diese Frage zu suchen und zu finden, eine Schwachstelle darstellt", so Echols.

Zwischen den Prüfungen sollte die Interne Revision die Kommunikation aufrechterhalten, indem sie Zeiten für Rückfragen einplant und sich über die Herausforderungen der Teams informiert. „Wenn die Revisoren in der Lage sind, sich als vertrauenswürdige Berater zu positionieren, ist das ein absoluter Wendepunkt", sagt Headley.

Transparenz ist entscheidend. Interne Revisoren sollten sich über den Umfang und die geplanten Prüfverfahren klar äußern und über aufgetretene Probleme. „Stellen Sie sicher, dass Sie früh und oft kommunizieren“, sagt er, „besonders wenn es um IT-Risiken geht.“ Er rät den Revisoren, keine vorzeitigen Urteile zu fällen, sondern stattdessen ein offenes Gespräch über die Gedankengänge des Kundenteams zu führen und die Zusammenarbeit zu fördern.

Headley merkt an, dass IT-Teams oft damit beschäftigt sind, die Anforderungen der verschiedenen Geschäftsbereiche zu erfüllen und die Verantwortung für alles zu übernehmen, von der Aufrechterhaltung des Betriebs von Anwendungen bis hin zur Bewältigung alltäglicher Hardware-Probleme. Infolgedessen habe die Cybersicherheit nicht immer höchste Priorität. Interne Revisoren können das Bewusstsein für diese Herausforderungen schärfen und die Teams über Möglichkeiten zu ihrer Bewältigung aufklären, sodass Prüfungen einen echten Mehrwert darstellen.

„Interne Revisoren können Partner sein, wenn es darum geht, die Widerstandsfähigkeit von Unternehmen zu stärken“, so Headley. Sie können unter anderem dazu beitragen, die Differenzen zwischen der Unternehmensführung und den IT-Teams auszugleichen, die oft nicht die gleiche Sprache sprechen. Da Interne Revisoren sowohl Geschäfts- als auch IT-Risiken verstehen, können sie helfen, diese Kluft zu überbrücken.

Interne Revisoren können auch das Verständnis von Cyberrisiken und die damit verbundene Problemlösung in einer Weise beeinflussen, die von der bisherigen Praxis abweicht, so Chang. Wenn sich Organisationen von der traditionellen Business-Continuity-Planung oder Business-Disaster-Recovery abwenden, können Interne Revisoren ihnen helfen, facettenreichere und differenziertere Ansätze zu verfolgen. Sie können diese Bemühungen verstärken, indem sie eine Rolle als Storyteller übernehmen, unzusammenhängende Informationen und Datenpunkte verarbeiten und sie zu einer überzeugenden Erzählung zusammenfügen, die eine bessere Entscheidungsfindung ermöglicht.

Ausgleich der Chancen

Letztendlich bedeutet Resilienz, die Unvermeidbarkeit von Angriffen zu akzeptieren und davon auszugehen, dass die äußeren Mauern der Organisation nicht undurchdringlich sind, stellt Echols fest. Im Rahmen dieser Bemühungen müssen Unternehmen erkennen, dass sie sich in einem unfairen Kampf befinden. Während Unternehmen sich bemühen, 100 % der Angriffe, denen sie ausgesetzt sind, abzuwehren, brauchen Hacker nur eine einzige Tür zu öffnen, um Schaden anzurichten, stellt Chang fest. „Es ist viel schwieriger, der Verteidiger zu sein als der Täter“, sagt er. Die Interne Revision kann die Erkenntnisse und Informationen liefern, die die Unternehmen benötigen, um ihre Aussichten auf Erfolg im Bereich der Cybersicherheit zu verbessern.

Laut einer Umfrage unter Entscheidungsträgern im Bereich IT und Sicherheit:

- Geben nur 2 % der Befragten an, dass sie innerhalb von 24 Stunden nach einem Cyberangriff ihre Daten wiederherstellen und ihre Geschäftsabläufe wiederherstellen könnten.
- Geben 69 % der Befragten an, dass ihr Unternehmen im letzten Jahr Lösegeld gezahlt hat, obwohl 77 % der Befragten eine definierte Richtlinie gegen die Zahlung von Lösegeld haben.
- Geben 42 % an, dass ihre Unternehmen sensible Daten identifizieren und die geltenden Datenschutzgesetze und -vorschriften einhalten könnten. Andere haben keine ausreichenden IT- und Sicherheitskapazitäten dafür.

Quelle: Cohesity Global Cyber Resilience Report 2024

TEIL 3

Festlegung einer neuen Zero-Trust-Grenze

Über die Experten

Adam Kohnke

Adam Kohnke, mit Sitz in Madison, Wisconsin, ist der Informationssicherheitsmanager des Chemieunternehmens Charter Next Generation.

Julio Tirado

Julio Tirado ist Executive Vice President und Direktor für Interne Revision und Compliance bei der SpiritBank mit Sitz in Tulsa, Oklahoma.

Für jedes Unternehmen sollte es eine Grundvoraussetzung sein, über Verfahren und Kontrollen zu verfügen, die die Sicherheit seiner Netzwerke gewährleisten. Mit dem technologischen Fortschritt und der zunehmenden Größe und Komplexität von Netzwerken hat sich jedoch der Standard für ein sicheres Netzwerk geändert. Eine der wichtigsten Änderungen ist der Übergang von einem standortbezogenen Sicherheitsmodell zu einem eher datenbezogenen Modell. Wir nennen dieses Modell „Zero Trust“.

Was ist Zero Trust?

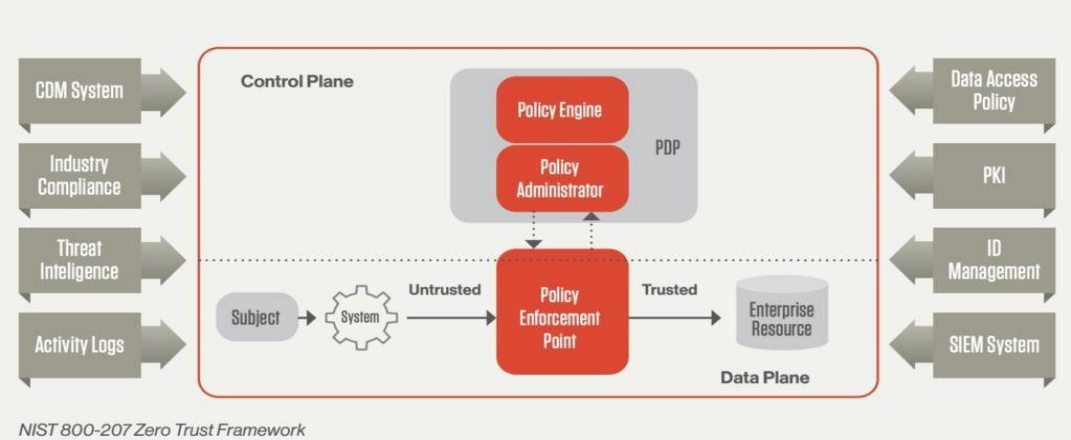
Im Allgemeinen erfordert ein Zero-Trust-Sicherheitsrahmenwerk, dass alle Benutzer, die innerhalb eines Netzwerks – sowohl innerhalb als auch außerhalb des Unternehmens selbst – arbeiten, vor dem Zugriff auf Anwendungen und Daten authentifiziert und dann regelmäßig validiert werden. Wie der Name sagt, spielt „Vertrauen“ oder genauer gesagt „vertraue, aber überprüfe" in diesem System keine Rolle, und der Zugriff auf alles, was mit dem Unternehmen zu tun hat, muss ständig auf der Grundlage der Unternehmensrichtlinien begründet und beurteilt werden.

Traditionell wurden Cybermodelle auf der Grundlage des Standorts des Netzwerks erstellt, aber in einem Zero-Trust-System ist das, was ein „Netzwerk“ ausmacht, weniger streng definiert, da ein Unternehmensnetzwerk lokal, in einer Cloud oder eine Mischung aus beidem sein kann. Insbesondere nach der COVID-19-Pandemie, die eine neue Ära von Remote Work eingeläutet hat, sind hybride oder vollständig Cloud-basierte Systeme zur Norm geworden, und die Rahmenwerke für Cybersicherheit mussten weiterentwickelt werden, um dies zu berücksichtigen.

Es gibt mehrere formale Zero-Trust-Rahmenwerke, unter anderem:

- Standard 800-207 des National Institute of Standards and Technology (NIST). Dies ist das Rahmenwerk, das von den US-Bundesbehörden ab 2021 verwendet werden muss (siehe Abbildung 1).
- Google BeyondCorp.
- Microsoft Zero Trust Strategy.
- Zero Trust Maturity Model von der Cybersecurity and Infrastructure Security Agency (CISA).

Abbildung 1



Quelle: Zero Trust Networks | NIST

Sie haben zwar alle ihre eigenen Merkmale, aber sie teilen die gleichen Grundprinzipien, nämlich:

- Kontinuierliche Überprüfung des Zugriffs auf alle Ressourcen.
- Minimierung des Bereichs der Auswirkungen im Falle eines externen oder internen Vorfalls.
- Nutzung von Verhaltensdaten, um den Kontext aus der IT-Infrastruktur zu erfassen.

Auch wenn der Übergang zu einem solchen System beträchtlich erscheinen mag, ist es wichtig zu wissen, dass es nicht als Ersatz für die derzeitigen Systeme gedacht ist. „Zero Trust soll die derzeitigen Netzwerkschutzmodelle oder sogar Änderungen an der Infrastruktur nicht vollständig ersetzen“, sagt Adam Kohnke, Informationssicherheitsmanager beim Chemieunternehmen Charter Next Generation, „sondern sie vielmehr ergänzen, um den Netzwerkschutz zu verbessern. Es soll eine Erweiterung sein, weil traditionelle Systeme wie Firewalls, Web-Proxies und Boundary Isolation Mechanismen nicht funktioniert haben."

Nach Angaben von IBM betrugen die durchschnittlichen Kosten einer einzelnen Datenlecks im Jahr 2024 4,88 Millionen US-Dollar. Darüber hinaus betrug der durchschnittliche Lebenszyklus eines Vorfalls volle 292 Tage von der Identifizierung bis zur Eindämmung. Es ist klar, dass der herkömmliche Netzwerkschutz nicht ausreicht und erhebliche Aufmerksamkeit erfordert.

Die Rolle der Internen Revision

Auch wenn die Details variieren können, können Interne Revisoren eine Vielzahl von Aufgaben im Zusammenhang mit der Einführung und Aufrechterhaltung eines Zero-Trust-Systems wahrnehmen. Zur Veranschaulichung seien hier einige Bereiche genannt, in denen eine Beurteilung durch die Interne Revision den größten Nutzen haben kann.

Definition von Schutzflächen

Traditionell konzentrierte sich ein Cybersicherheitssystem darauf, die Sicherheitsparameter für ein Unternehmensnetz zu definieren. Firewalls und VPN-Systeme sind nach diesem Konzept konzipiert, um sensible Daten und anfällige Informationen so weit wie möglich von der Netzgrenze entfernt zu halten. Bei einem Zero-Trust-System liegt der Schwerpunkt jedoch nicht auf Parametern, sondern auf Gruppierungen von Daten, Anwendungen, Anlagen und Diensten (DAAS), die zusammen als „Schutzflächen“ bezeichnet werden.

Sicherzustellen, dass diese Flächen angemessen identifiziert werden, muss Mittelpunkt einer umfassenden Beurteilung der Internen Revision sein.

Laut Julio Tirado, Executive Vice President, Director of Internal Audit and Compliance bei der SpiritBank, „sollte sich die Beurteilung auf die Überprüfung der Datenklassifizierungsrichtlinien des Unternehmens konzentrieren, um festzustellen, ob Systeme und Daten angemessen klassifiziert sind und ob die für sie geltenden Schutzrichtlinien angemessen sind“.

Geschützte Dienste sind nur auf Daten beschränkt, sagt Tirado. Auch für physische Anlagen, die beim Zugriff auf sensible Daten eine Rolle spielen, müssen Prozesse und Verfahren vorhanden sein, die sicherstellen, dass sie inventarisiert und regelmäßig beurteilt werden.

> Die Beurteilung sollte sich auf die Überprüfung der Datenklassifizierungsrichtlinien des Unternehmens konzentrieren, um festzustellen, ob die Systeme und Daten angemessen klassifiziert sind und ob die für sie geltenden Schutzrichtlinien angemessen sind.
>
> **Julio Tirado, SpiritBank**

Überprüfen von Map Transaction Flows

Sobald die Prüfungssicherheit gegeben ist, besteht der nächste Schritt der Beurteilung darin, sicherzustellen, dass die Beteiligten verstehen, wie all diese DAAS-Systeme interagieren. Die IT-Teams sollten über detaillierte Dokumentationsdiagramme verfügen, die das komplexe Netz von Ports, Netzwerk Traffic Baselines und Protokollen abbilden, die insgesamt beschreiben, wie diese Systeme aufeinander zugreifen und wohin ihre Nutzung führen kann.

Obwohl die Interne Revision in den meisten Unternehmen nicht über ausreichende Kenntnisse oder Erfahrungen verfügt, um die Korrektheit dieser Diagramme selbst zu überprüfen, kann die sie laut Kohnke mit den Beteiligten oder einer vertrauenswürdigen Drittpartei zusammenarbeiten, um sicherzustellen, dass die Darstellungen ausreichend sind. „Wichtig ist“, so Kohnke, „dass die relevanten DAAS in jedem Diagramm berücksichtigt werden und genügend Details vorhanden sind ... und ob die in den vorherigen Schritten definierten, ursprünglichen Sicherheitsrichtlinien geändert wurden oder zusätzliche Kontrollen erforderlich sind.“

Überprüfung der Erstellung und kontinuierliche Verbesserung von Zero-Trust-Richtlinien

Zero-Trust-Strategien sollten für jede Schutzfläche detailliert ausgearbeitet werden und solche kritischen Fragen beantworten:

- Wer sollte Zugang zu den DAAS-Systemen des Unternehmens haben?
- Welche Anwendungen dürfen auf die DAAS-Systeme des Unternehmens zugreifen?
- Wann sollte der Zugang zu den DAAS-Systemen des Unternehmens erfolgen bzw. erfolgen können?
- Wo befinden sich die DAAS-Systeme des Unternehmens?
- Warum ist der Zugriff auf die DAAS-Systeme des Unternehmens erforderlich?
- Wie sollte der Zugang zu DAAS-Systemen im Unternehmen gewährt werden?

Um die Relevanz und Gültigkeit der erstellten Zero-Trust-Richtlinien beurteilen zu können, ist eine kontinuierliche Interaktion mit den IT-Stakeholdern von entscheidender Bedeutung, da das Unternehmensnetzwerk ständig erweitert und weiterentwickelt wird. „Zero Trust ist fester Zielort", sagt Tirado, „daher sollten sich die Sicherheitsrichtlinien und die DAAS-Schutzanforderungen im Laufe des Prozesses weiterentwickeln."

Das Ziel, so Tirado, sollte eine immer besser werdende Richtlinie sein, die sich mit jeder Art von Datenverkehr befasst, der in ein Netzwerk eindringen, es verlassen oder es durchqueren könnte. „Es sollte nichts imNetzwerk geben, dessen Quelle oder Zweck nicht identifiziert werden kann", sagt er. „Der Interne Revisor muss bei seiner Beurteilung feststellen, ob Überprüfungen durchgeführt werden, ob sie in ausreichendem Maße durchgeführt werden und ob die vorhandenen Richtlinien genau auf das eingehen, was er findet."

Zero-Trust-Architektur-Überwachung

Wie die vorangegangenen Beispiele zeigen, ist die laufende Überwachung entscheidend für den Erfolg eines Zero-Trust-Systems. Im Gegens atz zu einem traditionellen System, bei dem sich die Überwachung auf Sicherheitsparameter konzentriert, konzentrieren sich die Überwachungssysteme eines Zero-Trust-Systems auf Benutzer, Geräte und Dienste. „Die Überwachung sollte in Ihren Netzwerken durchgeführt werden, um die Leistung zu messen, alle an angeschlossenen Geräte zu identifizieren und abtrünnige Geräte und böswillige Aktivitäten zu erkennen", so das National Cyber Security Center in seiner Zero-Trust-Anleitung. Dies gilt vor allem, wenn Sie Dienste vor Ort hosten, aber da dies immer häufiger vorkommt, sollte auch die Verwaltung mobiler Geräte berücksichtigt werden.

> Ihre Netze sollten überwacht werden, um die Leistung zu messen, alle angeschlossenen Geräte zu identifizieren und abtrünnige Geräte und bösartige Aktivitäten zu erkennen.
>
> **National Cyber Security Center**

„Unternehmen wie das meine setzen für die Verwaltung mobiler Geräte eine Software ein, die ein gewisses Maß an Kontrolle über das jeweilige Gerät bietet, sofern der Benutzer dies akzeptiert", sagt Tirado. „Sie wird Aktivitäten überwachen, dabei helfen, gefährliche Websites einzuschränken, bestimmte Software zu beschränken, die auf dem Gerät installiert werden kann, und bietet eine Kontrolle für die Bereitstellung von Updates für dieses bestimmte System."

Darüber hinaus sollte nicht nur die tatsächliche Nutzung der Systeme überwacht werden, sondern auch, wie lange sie genutzt werden. Wie das National Cyber Security Center feststellt, ist „das Nutzerverhalten, wie die normalen Arbeitszeiten oder der normale Arbeitsort, eine wichtige Messgröße, die überwacht werden muss".

Es gibt verschiedene Überwachungssysteme, die auf die spezifischen Bedürfnisse des jeweiligen Netzes zugeschnitten sind, aber im Allgemeinen übertragen diese Systeme die gesammelten Daten an eine zentrale Stelle, wo sie dann analysiert werden können. Diese Informationen wird im Laufe der Zeit eine „Basislinie" für normales Verhalten in Bezug auf Variablen wie Transaktionsvolumen, Anlagenkommunikation und Benutzeraktivität.

Durch ihre Beurteilungen können Interne Revisoren sicherstellen, dass regelmäßige Überprüfungen dieser Daten durchgeführt werden – und dass das Management diese Aufgabe in angemessener Weise übernimmt - und dass ihre Feststellungen eine Ausgangsbasis schaffen, die die Realität des Netzes genau widerspiegelt.

„Für die Internen Revisoren kommt es vor allem auf die Governance an", sagt Tirado. „Das Management muss über die Rolle informiert werden, die es bei der Sicherung des Systems spielt, denn das System wird nicht lange von alleine bestehen.

Änderungen an den Sicherheitsrichtlinien hängen davon ab, was die Baseline als „normal“ und „abnormal“ festlegt. Management-Reviews legen diese Baseline fest.“

Festlegung einer Baseline

Wie bei vielen Elementen der Cybersicherheit oder des Risikomanagements gibt es kein „Einheitsmodell“, und der Beitrag der Internen Revision zu diesem Thema ist daher sehr unterschiedlich. „Es hängt von den Ressourcen ab“, sagt Tirado. „Es hängt von der Größe der Organisation ab. Es hängt vom Mandat der Internen Revision ab.“

Ein guter Ausgangspunkt ist die Entwicklung eines Prozesses zur Erlangung von Prüfungssicherheit, ähnlich wie bei jedem anderen Prüfungssystem. „Denken Sie zum Beispiel an Sarbanes-Oxley“, sagt er. „Jedes börsennotierte Unternehmen muss die internen Kontrollen im Zusammenhang mit den Jahresabschlüssen darstellen und diese Matrix entwickeln. Und als Teil dieser Abbildung werden Sie Testverfahren für einen bestimmten Zeitraum – etwa ein bestimmtes Jahr – erstellen. Den gleichen Ansatz würde man auch bei Zero Trust verfolgen, indem man die Prüfungssicherheit über das ganze Jahr hinweg aufteilt und dabei die Größe des Unternehmens, die Ressourcen usw. berücksichtigt.

Allen Fällen gemeinsam ist jedoch die Verpflichtung der Internen Revision, sich kontinuierlich für die Umsetzung und laufende Verbesserung eines Zero-Trust-Systems einzusetzen. Es gibt eine Vielzahl von Ressourcen auf dem Markt, die bei der Aufgabe helfen, je nach dem Element, auf das sich das Zero-Trust-Modell konzentriert. Im Hinblick auf Ransomware-Risiken verwendet Tirado beispielsweise InfraGard, ein kostenloses Tool zum Informationsaustausch, das in Zusammenarbeit von FBI und Privatwirtschaft entwickelt wurde. In nur wenigen Minuten kann sich Tirado zu Beginn eines jeden Tages über neuesten Ransomware-Angriffe und Datenlecks innerhalb und außerhalb seiner Branche informieren. „Das Ausmaß dieser Angriffe verlangt nach einem Ansatz, der über ein perimeterbasiertes Sicherheitsmodell hinausgeht“, erklärt er. „Die Stakeholder darüber zu informieren, wie das Risikoumfeld aussieht und was auf dem Spiel steht, ist die oberste Priorität der Internen Revision.“

Außerdem ist es wichtig zu wissen, dass dieser Übergang nicht auf einmal erfolgen muss. „Selbst in partieller Form hat ein Zero-Trust-Modell einen immensen Wert“, sagt Tirado. „Letztendlich besteht ein Zero-Trust-Modell aus einer Spalte mit Kontrollen in einer Tabellenkalkulation. Vielleicht sind es 20, vielleicht sind es auch nur 10 oder 12. Das ist auf jeden Fall besser als fünf.“

Beispiele für einfache Kontrollen, die in der Anfangsphase eines Zero-Trust-Modells in Betracht gezogen werden können:

- Datenverschlüsselung.
- Schulung zum Sicherheitsbewusstsein.
- Pläne für die Reaktion auf Vorfälle.
- Endpunkt-Erkennungs- und Reaktionssysteme.
- Mikro-Segmentierung.
- Compliance-Überwachung.
- Verhaltensanalyse und userbezogene Verhaltensanalyse.

Das Fundament ist bereits vorhanden

Trotz der grundlegenden Änderung in der Netzwerkphilosophie sollten Interne Revisoren, sobald Zero-Trust verstanden wurde, erkennen, dass sich die Aufgaben der Funktion selbst nicht völlig von dem unterscheiden, was von ihnen zuvor erwartet wurde. Die Umsetzung von Zero-Trust selbst erfordert keine Änderungen an der Architektur oder Infrastruktur, abgesehen von der möglichen Einführung bestimmter kommerzieller Tools, und somit auch nicht an den Systemen, die die Prüfungssicherheit gewährleisten.

Zu den Grundpfeilern jeder Prüfungstätigkeit gehören Identifizierung, Kommunikation und Prüfungssicherheit, und jede dieser Aufgaben bleibt erhalten. Mit einer ruhigen Hand, der Einhaltung der Global Internal Audit Standards™ und der Bereitschaft zu lernen ist der Übergang zu einer Zero-Trust-Netzwerkarchitektur nichts, was eine Organisation fürchten müsste.

Frühere Ausgaben

Frühere Ausgaben von Global Perspectives and Insights finden Sie unter theiia.org/GPI.

Leser-Feedback

Senden Sie Fragen oder Kommentare an globalperspectives@theiia.org.

Über das IIA

Das Institute of Internal Auditors (IIA) ist ein internationaler Berufsverband, der mehr als 255.000 Mitglieder betreut und 200.000 Zertifizierungen zum Certified Internal Auditor® (CIA®) vergeben hat. Das IIA wurde 1941 gegründet und ist weltweit als führend in den Bereichen Standards, Zertifizierung, Ausbildung, Forschung und fachliche Leitlinien für den Berufsstand der Internen Revision anerkannt. Weitere Informationen finden Sie unter theiia.org.

Haftungsausschluss

Urheberrecht

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101