Einkaufsleitfaden für Lösungen zur Abwehr von Insider-Bedrohungen

Dieser Einkaufsleitfaden beschreibt die wichtigsten Funktionen einer Lösung zur Abwehr von Insider-Bedrohungen und die Erfahrungen, die Proofpoint bei seinen erfolgreichen Projekten zur Insider-Risiko-Abwehr bei Unternehmen verschiedenster Größe in aller Welt und allen Branchen sammeln konnte. Darüber hinaus soll er als praktische Referenz für Leser dienen, die sich erstmals mit der Abwehr von Insider-Bedrohungen (Insider Threat Management, ITM) beschäftigen oder ihre vorhandene ITM-Lösung aktualisieren möchten.

Personenzentrierte Sicherheit als Ausgangspunkt

Um Daten vor Insider-Bedrohungen schützen zu können, benötigen Sie eine Lösung, die ein personenzentriertes Sicherheitsmodell unterstützt. Ein solches Modell bietet einen umfassenden Überblick über das riskante Verhalten von Anwendern und zeigt, wie diese mit vertraulichen Daten interagieren. Dadurch erhalten Sie wichtigen Kontext über die Absichten von Aktionen, mit denen dem Unternehmen vorsätzlich oder unabsichtlich Schaden zugefügt wird.

Mit einer Lösung, die einem personenzentrierten Ansatz folgt, können Sie Ihre Insider-Risiken anhand von Verhaltensindikatoren schnell verstehen. Durch einen ganzheitlichen Blick auf diese Indikatoren, der den Zeitverlauf und den Kontext anderer Aktivitäten berücksichtigt, lässt sich erkennen, ob ein Anwender das Unternehmen schädigen will. Dies könnte weitere Untersuchungen nach sich ziehen, um die richtigen Reaktionsmaßnahmen zu wählen.

Wichtige Elemente einer ITM-Lösung

Wenn Sie Insider-Bedrohungen stoppen möchten, müssen Sie damit zusammenhängende Zwischenfälle erkennen, abwehren, verhindern sowie darauf reagieren können. Zur effektiven Reduzierung der Insider-Risiken müssen Sie proaktiv und koordiniert vorgehen.

Identifizierung

Sie benötigen eine Lösung, die riskantes Verhalten noch vor dem Eintreten eines Zwischenfalls aufdeckt und ungewöhnliche Verhaltensmuster erkennt, die von einer festgelegten Baseline abweichen. Eine solche Lösung sollte riskante Anwender überwachen, die zum Beispiel privilegierte Zugriffsrechte besitzen, demnächst das Unternehmen verlassen könnten oder bereits gekündigt haben, sowie Auftragnehmer, Führungskräfte und verdächtige Anwender. Stressfaktoren wie Änderungen beim beruflichen Status (z. B. Kündigung durch den Arbeitnehmer oder Arbeitgeber), Veränderungen im Unternehmen (z. B. Fusionen und Übernahmen oder Umstrukturierungen) sowie problematisches Verhalten (z. B. verärgerte Aktionen oder finanzielle Konflikte) können beim Identifizieren riskanter Anwender ebenfalls berücksichtigt werden.

Jedes Unternehmen sollte festlegen, welche präventiven Maßnahmen am besten zu den individuellen Geschäftszielen, der Unternehmenskultur und der Innovationsgeschwindigkeit passen.

Schutz

Ihre Lösung sollte vertrauliche Daten und Systeme mit personenzentrierten Sicherheitskontrollen schützen, die Verhaltensindikatoren in ihren Richtlinien und Regeln berücksichtigen.

Wichtig ist, mithilfe von Anwenderschulungen, in Echtzeit versendeten Erinnerungen und Blockierungen zu verhindern, dass Anwender versehentlich oder absichtlich Sicherheitsrichtlinien verletzen. Dabei dürfen und sollten nicht alle Aktivitäten unterbunden werden, da ansonsten die Anwenderproduktivität leidet. Jedes Unternehmen sollte festlegen, welche präventiven Maßnahmen am besten zu den eigenen Geschäftszielen, der Unternehmenskultur und der Innovationsgeschwindigkeit passen.

Eine ITM-Lösung sollte auch eine flexible und einfache Möglichkeit bieten, den Zugriff auf Anwenderdaten zu kontrollieren und zu gewährleisten, dass Sicherheitsanalysten nur bei Bedarf auf diese Daten zugreifen können.

Erkennung

Eine ITM-Lösung sollte in Echtzeit Warnungen zu Anwenderverhalten liefern und Maßnahmen ermöglichen, wobei bei riskanten Anwenderaktivitäten in folgenden Situationen Warnungen erfolgen können:

- Verbergen von Informationen
- Erweiterung von Berechtigungen
- Umgehung der Sicherheitskontrollen
- Datenexfiltration
- Download nicht genehmigter Software
- IT-Sabotage
- Erstellen einer Backdoor
- Nicht autorisierter Zugriff
- Nicht akzeptable Nutzung

Wenn es zu einem Regelverstoß kommt, sollte die Lösung Informationen zum Wer, Was, Wann und Wo im Zusammenhang mit den relevanten Anwenderaktivitäten liefern, um detaillierten Kontext und Einblicke in Verhaltensweisen und Absichten bereitzustellen. Die Lösung sollte auch Screenshots speichern, um im Rahmen von Untersuchungen unwiderlegbare Beweise zu sammeln. Gleichzeitig muss die ITM-Lösung flexibel genug sein, um dynamisch auf riskantes Verhalten zu reagieren und Screenshots nur bei einem Alarm zu speichern. Dadurch ist gewährleistet, dass dem Datenschutz Rechnung getragen wird und Sicherheitsanalysten effizienter arbeiten können.

Fahrlässige Anwender sind die häufigste Ursache für Datenverlust und Insider-Bedrohungen. Sie zeichnen sich dadurch aus, dass sie trotz guter Absichten schlechte Entscheidungen treffen, die schwerwiegende Folgen nach sich ziehen können.

Reaktion

Es ist wichtig, Zwischenfälle schnell und effizient untersuchen und darauf reagieren zu können. Je länger eine Bedrohung fortbesteht, desto mehr Schaden kann sie anrichten – sowohl für die Reputation Ihres Unternehmens als auch in finanzieller Hinsicht. Für die Nachverfolgung des Status eines Zwischenfalls sind festgelegte Untersuchungsabläufe unverzichtbar. Das gilt besonders dann, wenn bei der Eskalation andere Abteilungen einbezogen werden müssen, z. B. die Personalabteilung, Rechtsabteilung, Compliance und Datenschutz. Eine robuste ITM-Lösung sollte sich in eine zentrale Ereignisverwaltung wie ein SIEM-System integrieren, mit dem die Sicherheitsanalysten bereits vertraut sind.

Drei primäre Anwendungsfälle

Grundsätzlich gibt es drei Arten von Insider-Bedrohungen – und alle drei Schwachstellen beziehen sich auf den Faktor Mensch. Eine personenzentrierte ITM-Lösung muss Reaktionsmöglichkeiten für folgende Fälle parat haben:

- **Fahrlässige Anwender:** Personen, die unaufmerksam sind und Fehler machen
- **Böswillige Anwender:** Personen, die vorsätzlich Schaden anrichten wollen
- **Kompromittierte Anwender:** Personen, deren Anmeldedaten von einem externen Bedrohungsakteur gestohlen wurden

1. Fahrlässige Anwender und häufige Fehler

Als häufigste Ursache für Datenverlust und Insider-Bedrohungen wurden im Proofpoint Data Loss Landscape-Bericht 2024 fahrlässige Anwender genannt. Diese Anwender zeichnen sich dadurch aus, dass sie trotz guter Absichten schlechte Entscheidungen treffen, weil sie häufig einfach ihre Arbeit so effizient wie möglich erledigen wollen. Ihre Fehler können jedoch ernste Konsequenzen haben, wenn sie zum Beispiel zu Betriebsunterbrechungen führen, die Marke schädigen, die Wettbewerbsposition schwächen, gegen Gesetze verstoßen oder Bußgelder und Gerichtsverfahren nach sich ziehen.

Diese Anwender verursachen unter anderem durch folgende Fehler Risiken:

- Senden von E-Mails (mit oder ohne Anhang) an die falschen Empfänger
- Weitergabe vertraulicher Daten an GenAI-Websites
- Aufrufen von Phishing-Websites
- Installieren nicht autorisierter Software
- Weitergabe, Freigabe oder Veröffentlichung vertraulicher Dateien und Daten
- Senden personenbezogener Daten an ein privates E-Mail-Konto
- Speichern vertraulicher Unternehmensdaten auf privaten Geräten

Böswillige Anwender sind gefährlich, weil sie sich in einer idealen Position befinden, um vertrauliche Daten zu stehlen und dem Unternehmen zu schaden. Sie sind vom persönlichen Vorteil motiviert.

Schutz vor fahrlässigem Verhalten

Eine effektive ITM-Lösung kann riskante Aktivitäten erkennen und verhindern. Darüber hinaus bietet sie fahrlässig handelnden Anwendern Hilfe an, damit sie verstehen, was sie falsch gemacht haben, und ihr Verhalten ändern können.

Darauf sollten Sie achten:

- **Klassifizierung:** Stellen Sie sicher, dass E-Mails, Daten und Inhalte kontinuierlich manuell und mit künstlicher Intelligenz (KI) überwacht werden, um riskant handelnde Anwender zu identifizieren und zu klassifizieren. Als hochriskant eingestuften Anwendern wird vom System ein Risikowert zugewiesen, damit Daten zusätzlich geschützt werden.
- **Überwachung:** Die Lösung sollte nach riskantem Verhalten und Aktivitäten wie unbefugter Anwendungs- und Webnutzung, Ändern von Dateinamen und -typen bei vertraulichen Dokumenten, Abruf von Daten außerhalb des Aufgabenbereichs sowie Exfiltration einer großen Zahl vertraulicher Dokumente suchen. Durch die Überwachung von Hochrisikogruppen lassen sich Anwender identifizieren, bei denen gründlichere Kontrollen notwendig sind.
- **Prävention:** Es muss verhindert werden, dass Anwender vertrauliche Daten vom Endpunkt exfiltrieren. Dazu gehören auch fehlgeleitete E-Mails (mit und ohne Anhang), USB-Sticks, Web-Uploads, Cloud-Synchronisierungen, Netzwerkfreigaben und Ausdrucke. Wenn Anwender einen Fehler machen, sollten sie noch im selben Moment eine Warnmeldung mit Kontext sowie die Möglichkeit erhalten, den Fehler in Echtzeit und ohne Eingreifen eines Administrators zu korrigieren, sodass der Datenverlust verhindert werden kann. In Ausnahmefällen können Anwender begründen, warum sie auf entsprechende Daten zugreifen müssen, und das Sicherheitsteam kann die Anfrage erlauben oder ablehnen.
- **Laufende Schulungen:** Fahrlässige Anwender sind sich häufig nicht bewusst, dass ihr Verhalten mit Risiken verbunden ist. Daher sollte eine ITM-Lösung die Endnutzer bei riskantem Verhalten mithilfe von Benachrichtigungen informieren und auf die entsprechenden Unternehmensrichtlinien verweisen.

2. Böswillige Anwender

Böswillige Anwender sind gefährlich, weil sie sich in einer idealen Position befinden, um vertrauliche Daten zu stehlen und dem Unternehmen zu schaden. Zudem sind sie vom persönlichen Vorteil motiviert. Mitarbeiter, die das Unternehmen verlassen, gehören zu den gefährlichsten Insidern – sind jedoch bei weitem nicht die einzigen, die eine Gefahr darstellen.

Bedrohungen durch böswillige Insider lassen sich in diese grundsätzlichen Kategorien einteilen:

- **Betrug:** Dazu gehören Täuschungsmaßnahmen, die den Geschäftsbetrieb stören können.
- **Sabotage:** Betrifft auch Schäden an Systemen oder die Beschädigung bzw. Vernichtung von Daten.
- **Diebstahl:** Bezeichnet die Exfiltration proprietärer Informationen, die für das Unternehmen wertvoll sind.
- **Spionage:** Der Verkauf wertvoller Daten, Geschäftsgeheimnisse und weiterer Informationen an Mitbewerber oder Gegenspieler.

Ein personenzentriertes System überwacht bestimmte Anwender genauer als andere und unterzieht die riskantesten Anwender strikteren Sicherheitskontrollen.

Böswillige Insider sind vor allem deshalb eine echte Gefahr, weil sie eine Vertrauensstellung genießen. Sie können den richtigen Augenblick abwarten, um ihren privilegierten Zugriff für die Suche nach wertvollen Daten und Sicherheitsschwachstellen auszunutzen. Hinzu kommt, dass Unternehmen oft selbst Schwachstellen schaffen, weil sie Mitarbeitern erlauben, Daten auf privaten Geräten zu nutzen und zu speichern, und so den Diebstahl vertraulicher Daten sowie das Verursachen von Schaden erleichtern.

Schutz vor böswilligen Anwendern

Ein personenzentriertes System kann bestimmte Anwender genauer überwachen als andere und unterzieht die riskantesten Anwender strikteren Sicherheitskontrollen. Darüber hinaus blockiert es schädliche Aktionen basierend auf Risikofaktoren, z. B. wenn ein Mitarbeiter kündigt oder gekündigt wird.

Darauf sollten Sie achten:

- **Transparenz:** Kanalübergreifende Transparenz (Datenaktivitäten und Verhalten) bietet einen umfassenden Überblick und kontextbezogene Einblicke in die Aktivitäten und Absichten von Anwendern. Telemetriedaten ihrer Interaktionen mit Daten und Systemen sollten erfasst werden, z. B. wenn sie eine vertrauliche Datei umbenennen oder sie auf eine nicht autorisierte Website oder einen Cloud-Synchronisierungsordner hochladen. Auch riskante Aktivitäten wie das Herunterladen nicht genehmigter Anwendungen, das Manipulieren von Sicherheitskontrollen oder das Installieren eines Tor-Browsers rechtfertigen eine Warnmeldung. Eine kontextbezogene Zeitleiste der Ereignisse hilft, das Wer, Was, Wann und Wo von Anwenderaktivitäten zu verstehen, und liefert Informationen dazu, was ein Anwender vor und nach einer Warnmeldung getan hat.
- **Bedrohungsbibliothek:** Das System sollte eine Bibliothek mit Warnmeldungen für die gängigsten Insider-Bedrohungen (Arbeitszeitbetrug, Datenexfiltration, Umgehung von Sicherheitskontrollen) enthalten, da dies die Einrichtung von Regeln für die gängigsten Verhaltensindikatoren deutlich beschleunigt.
- **Untersuchungen:** Ihre Lösung sollte detaillierte Metadaten und Screenshots von Anwenderaktivitäten sichern, um forensische Nachweise für Untersuchungen bereitzustellen. Kooperative Workflows sind für die Behebung von Insider-Vorfällen wichtig. Da bei solchen Untersuchungen Vertreter anderer Abteilungen wie der Personalabteilung, Rechtsabteilung, Datenschutz und Compliance beteiligt sind, müssen Sie Berichte zu Anwenderrisiken in leicht lesbaren Formaten wie PDF-Dokumenten weitergeben.
- **Datenschutzkontrollen:** Eine leistungsstarke ITM-Lösung bietet Funktionen wie attributbasierte Zugriffssteuerung, Datenmaskierung und -anonymisierung sowie Unterstützung für standortübergreifende Rechenzentren, damit Sie die Anforderungen in Bezug auf Datenschutz und Datenaufbewahrung erfüllen und unvoreingenommene Untersuchungen durchführen können. Sie müssen die Überwachungsrichtlinie für einen Anwender dynamisch und flexibel in Echtzeit ändern können, sobald er eine Warnmeldung auslöst. Da Screenshots nur bei Bedarf erfasst werden, bleibt die Privatsphäre des Anwenders geschützt.

3. Kompromittierte Anwender

Kompromittierte Anwender sind Opfer eines externen Bedrohungsakteurs, der die Kontrolle über ihre Konten übernimmt und diese missbräuchlich verwendet. Sobald die Konten kompromittiert sind, haben die Angreifer umfassende Zugriffsberechtigungen auf Daten und Systeme. Die Gefahr durch kompromittierte Anwender ist deshalb so groß, weil Bedrohungsakteure monatelang unentdeckt in den internen Systemen verweilen können.

Externe Cyberangreifer nutzen in erster Linie menschliche Schwachstellen aus, wobei sie am häufigsten auf Social-Engineering-Taktiken und insbesondere Phishing setzen. Angesichts der Tatsache, dass 71 % aller Unternehmen schon einmal einen erfolgreichen Phishing-Angriff verzeichnet haben, ist das keine Überraschung.

Zu den typischen Phishing-Techniken gehören:

- Versand schädlicher Links und Anhänge sowie böswilliger Datenanfragen
- Smishing (SMS-Phishing)
- Social-Media-Phishing
- Angriffe per Telefon (TOAD)
- Business Email Compromise (BEC)
- Multifaktor-Authentifizierung (MFA)

Das Ziel externer Bedrohungsakteure ist letztendlich immer der Zugriff auf wertvolle Daten und Systeme, die sie zu ihrem Vorteil und finanziellen Gewinn missbrauchen wollen.

Schutz vor kompromittierten Anwendern

Eine effektive ITM-Lösung bietet Einblick sowie Kontext und zeigt, ob das Verhalten eines Anwenders ungewöhnlich ist. Wenn der Anwender häufiger auf Phishing-Links klickt, können Sie ihn auf jegliches ungewöhnliches Verhalten überwachen. Zum Schutz Ihrer Daten können Sie außerdem gewährleisten, dass nur dazu befugte Personen sie überhaupt sehen können.

Darauf sollten Sie achten:

- **Proaktive Überwachung:** Wenn Ihre Teams individuelle Prüfungen erstellen und speichern, können sie regelmäßig nach Datenexfiltrationen und riskanten Aktivitäten suchen. Very Attacked People (VAPs), die häufiger auf schädliche Links oder Anhänge klicken bzw. mit riskanten Anwendungen interagieren, können auf ungewöhnliches Verhalten überwacht werden, das auf eine Kompromittierung hinweist. Der gleiche Ansatz kann für andere hochriskante Gruppen wie Angestellte, die das Unternehmen verlassen, oder Anwender mit privilegierten Zugriffsrechten verwendet werden. Da es nahezu unmöglich ist, alle riskanten Insider rechtzeitig zu identifizieren, sollte die ITM-Lösung die Überwachungsrichtlinie für einen Anwender dynamisch und flexibel in Echtzeit ändern können, sobald dieser eine Warnmeldung auslöst.
- **Adaptive Zugriffskontrollen:** Sie können bedingte Zugriffsregeln auf Daten anwenden, z. B. Safe- oder Blocklists für bestimmte Länder, Netzwerke oder riskante IP-Adressen. Zudem können Sie den Zugriff auf vertrauliche Daten auf bestimmte privilegierte Anwender und Gruppen beschränken sowie Uploads und Downloads nur für verwaltete Geräte erlauben. Mit attributbasierten Zugriffskontrollen ist es möglich, Datenschutzanforderungen einzuhalten.
- **Integrationen:** Eine effektive ITM-Lösung ergänzt Ihr Sicherheitssystem und liefert wichtigen Kontext, weil sie sich problemlos mit verschiedenen Tools integrieren lässt, einschließlich:
  - Security Orchestration, Automation and Response (SOAR, Koordinierung und Automatisierung von Sicherheitsmaßnahmen)
  - SIEM-Systeme (Sicherheitsinformations- und Ereignis-Management)
  - Reaktion auf Zwischenfälle
  - Ticket-Management-Systeme
- **Moderne Architektur:** Eine Cloud-native Plattform bietet den Vorteil, dass sie sich auf hunderttausende Anwender skalieren lässt. Eine ITM-Lösung erfasst Telemetriedaten mithilfe eines ressourcenschonenden Endpunkt-Agenten, der die Anwenderproduktivität nicht beeinträchtigt und keine Konflikte mit anderen Lösungen auslöst.

Fazit

Für den Schutz Ihres Unternehmens vor bewussten oder fahrlässigen Insider-Risiken benötigen Sie eine ITM-Lösung, die einen proaktiven Ansatz erlaubt. Diese Lösung sollte einen Überblick über riskantes Verhalten liefern und dynamische sowie automatische Reaktionsmaßnahmen ermöglichen. Eine gute ITM-Lösung bietet festgelegte Untersuchungsabläufe und erfasst unwiderlegbare Beweise wie Screenshots, um Untersuchungen zu beschleunigen, die abteilungsübergreifende Zusammenarbeit zu verbessern und Initiativen zur Abwehr von Insider-Risiken zu unterstützen. Und schließlich sollte eine ITM-Lösung mit Ihren geschäftlichen Anforderungen mitwachsen, Ihre vorhandenen Investitionen nutzen und die Compliance mit flexiblen Zugriffs- und Datenschutzkontrollen gewährleisten. Eine ITM-Lösung mit diesen notwendigen Funktionen unterstützt Ihr Sicherheitsteam dabei, zuverlässigen Schutz vor Insider-Risiken sicherzustellen.

MEHR ERFAHREN

Weitere Informationen finden Sie unter **proofpoint.com/de**.