proofpoint.

EINKAUFSLEITFADEN

Leitfaden für CISOs zum Stoppen von personenzentrierten und KI-zentrierten Bedrohungen

Wichtige Funktionen

Dies sind die fünf Fähigkeiten , die Sie benötigen, um Ihr Unternehmen vor personenzentrierten und KI-zentrierten Bedrohungen zu schützen:

1. Umfassender Überblick über Bedrohungen und Risiken
2. Automatischer Bedrohungsschutz für E-Mails und darüber hinaus
3. Schutz für vertrauenswürdige Geschäftskommunikation
4. Anleitung für Mitarbeiter
5. Schutz vor Kontoübernahme

Überblick

Bedrohungsakteure verstärken weiter ihre Bemühungen, durch Exfiltration von Daten und Ausnutzung von geschäftlicher Kommunikation finanzielle Vorteile zu erlangen. Und während die Anzahl dieser Bedrohungen ständig zunimmt, bleiben die Bedrohungstaktiken selbst weitgehend gleich. Angriffe per Phishing, Malware, Ransomware, Business Email Compromise (BEC) und Social Engineering sind nach wie vor beliebte personenzentrierte Methoden.

Neu ist, dass KI diese bekannten Taktiken enorm verstärkt. Bedrohungsakteure nutzen große Sprachmodelle, um hochgradig personalisierte Phishing-Köder zu erstellen, 80–90 % der Angriffskette zu automatisieren und mehrstufige, kanalübergreifende Kampagnen in noch nie dagewesenem Umfang zu starten. Proofpoint beobachtete allein im Jahr 2025 einen Anstieg der E-Mail-Bedrohungen gegen Kunden um 94 %. Durch KI entstehen auch völlig neue Angriffsvektoren, z. B. Prompt-Injection-Angriffe, bei denen KI-Assistenten in Unternehmen durch versteckte Anweisungen in E-Mails manipuliert werden.

In diesem Leitfaden erläutern wir die wichtigen Funktionen, die Sie für zuverlässigen Schutz vor allen personen- und KI-zentrierten Bedrohungen benötigen – ganz gleich, ob die Angriffe über E-Mails oder andere Vektoren erfolgen. Wir zeigen Ihnen außerdem, worauf Sie bei der Wahl der Sicherheitsplattform für Ihr Unternehmen achten sollten.

Abb. 1: Bedrohungen und Risiken digitaler Arbeitsplätze.

1. Umfassender Überblick über Bedrohungen und Risiken

Um personenzentrierte und KI-zentrierte Bedrohungen stoppen zu können, müssen Sie wissen, welche Ihrer Anwender angegriffen werden – und auf welche Weise. Nur dann können Sie Ihre Maßnahmen mit anpassbaren Sicherheitskontrollen optimieren und die am stärksten gefährdeten Personen schützen.

Mit einem umfassenden Überblick über Bedrohungen in E-Mails und digitalen Kanälen erhalten Sie ein vollständiges Bild Ihrer Schwachstellen.

Eine Lösung sollte Ihnen folgende Informationen liefern:

- **Anwender, die ins Visier genommen werden**, einschließlich der Bedrohungen, denen sie ausgesetzt sind, und ob sie mit Angreifern interagiert haben.
- **Forensische Details**, z. B. Bedrohungsakteur, Bedrohungsfamilie, betroffene Anwender, Angriffstechniken sowie Themen und Ziele von Angriffskampagnen
- **Gefährdete Anwender**, um die Personen zu identifizieren, die das größte Risiko für Ihr Unternehmen darstellen und warum
- **Bedrohungen in vertrauenswürdiger Geschäftskommunikation**, einschließlich gefälschte und Doppelgänger-Domains bzw. Websites, die die Reputation Ihrer Marke schädigen könnten
- **Verhaltensänderungen und Bedrohungsdaten**, die Anzeichen dafür sein können, dass einer Ihrer Lieferanten oder vertrauenswürdigen Drittanbieter kompromittiert wurde
- **Verdächtige Aktivitäten**, die auf mögliche aktive Kontoübernahmen hindeuten

4,88 Mio. $

Dies ist der durchschnittliche Kostenaufwand für eine Datenschutzverletzung im Rahmen eines Phishing- oder BEC-Angriffs. [1]

1. IBM: Cost of a Data Breach Report (Kosten eines Datenschutzverstoßes), 2024 2024.

Eine KI-gestützte Plattform kann Indikatoren bereichsübergreifend mithilfe von Beziehungsdiagrammen korrelieren, um normale Kommunikationsmuster zu ermitteln, mit Sprachmodellen die Absicht der Nachricht interpretieren sowie anhand von Bedrohungsdaten das Verhalten von Angreifern in einen Kontext setzen. Das Ergebnis sind tiefergehende und entscheidungsrelevante Erkenntnisse über Risiken, die über manuelle Analysen allein hinausgehen.

Dieser Überblick muss jedoch nicht nur bei der Erstbereitstellung, sondern jederzeit gegeben sein. Denn nur mit vollständiger Transparenz können Sie Ihre Schutzmaßnahmen an neue Angriffsmethoden anpassen.

2. Automatischer Bedrohungsschutz für E-Mails und darüber hinaus

Die Bedrohungslandschaft entwickelt sich ständig weiter. Leider verfügen Unternehmen häufig nicht über das notwendige Sicherheitspersonal und die Ressourcen, um mit dieser Entwicklung Schritt zu halten. Folglich haben Teams häufig schlichtweg nicht die Zeit, jedes Sicherheitsereignis zu untersuchen. Gleichzeitig verursachen diese Ereignisse immer höhere Kosten.

Deshalb benötigen Sie eine Lösung, mit der Sie Bedrohungen genau und effizient erkennen und stoppen können, ohne dabei die Produktivität Ihrer Mitarbeiter zu beeinträchtigen. Da Bedrohungen zunehmend von KI generiert und verbreitet werden, müssen auch Ihre Sicherheitsfunktionen zur Erkennung dieser Angriffe KI-gestützt sein.

Eine Lösung sollte folgende Schritte automatisch durchführen:

- **Abwehr von Bedrohungen vor der Zustellung** mit einer Genauigkeit von mindestens 99,999 %, damit sie nicht die Posteingänge Ihrer Anwender erreichen
- **Erkennung und Blockierung KI-generierter Bedrohungen,** darunter KI-erstellte BEC-Nachrichten, KI-personalisiertes Phishing und versteckte Prompt-Injection-Angriffe, die KI-Assistenten wie Microsoft Copilot ins Visier nehmen
- **Analyse von Verhaltensmustern bei internen E-Mails** mithilfe von Bedrohungsdaten-gestützter Technologie, die KI und Machine Learning nutzt, um laterale Phishing-Aktivitäten zu erkennen
- **Untersuchung und Blockierung schädlicher URLs in Echtzeit**, damit sie nicht über E-Mail oder Messaging- und Collaboration-Plattformen zu den Anwendern gelangen können
- **Erkennung von und Reaktion auf kompromittierte Konten von Identitätsanbietern,** die in der Cloud gehostet werden
- **Analyse verdächtiger QR-Codes vor der Zustellung** mithilfe von KI-gestützter Computer-Vision, semantischer Analyse und der Bereitstellung von Sandbox-Analysen
- **Anzeige von Warnhinweisen**, die Anwender auf verdächtige Nachrichten aufmerksam machen

Wenn ein Angreifer erfolgreich Erstzugriff erlangt, ist es unerlässlich, diese Bedrohung rasch zu erkennen und zu bekämpfen. Denn dies kann den Unterschied ausmachen zwischen einem kleinen Zwischenfall und einem groß angelegten Sicherheitsvorfall.

3. Schutz für vertrauenswürdige Geschäftskommunikation

Digitale Kommunikation ist das Lebenselixier jedes Unternehmens. Es ist daher nachvollziehbar, warum Bedrohungsakteure so intensiv daran arbeiten, vertrauenswürdige Kommunikationswege zu infiltrieren. Wenn Empfänger zu der Annahme verleitet werden können, dass sie mit vertrauenswürdigen Quellen kommunizieren, sind Angriffe wie BEC, Phishing und Ransomware wesentlich erfolgreicher.

Um ihre Erfolgschancen weiter zu erhöhen, nutzen Bedrohungsakteure eine breite Palette an Nachahmungstaktiken. KI hat Nachahmung dramatisch effektiver gemacht. Angreifer können nun innerhalb von Sekunden ausgefeilte, kontextbezogene Nachrichten generieren, die den Tonfall und Schreibstil einer Führungskraft nachahmen. Deshalb ist es unerlässlich, mehrere Schutzebenen zu implementieren, um sie aufzuhalten.

Suchen Sie nach einer Lösung, die folgende Funktionen umfasst:

- **Ermöglicht die E-Mail-Authentifizierung** sowohl für von Anwendern erstellte als auch für von Anwendungen generierte E-Mails
- **Bereitstellung einer sicheren, dedizierten Umgebung** für die Weiterleitung von anwendungsgenerierten Transaktions-E-Mails
- **Unterstützt bei der Implementierung von DMARC,** um die Effektivität der E-Mail-Authentifizierung zu maximieren und vollständige DMARC-Compliance sicherzustellen
- **Bietet Schutz vor Doppelgänger-Domains,** einschließlich Erkennung und Unterstützung bei der Blockierung oder physischen Abschaltung solcher Domains
- **Überwacht kompromittierte Lieferantenkonten mithilfe** von verhaltensbasierter KI und Bedrohungsdaten und ergreift automatisierte Maßnahmen, um sich dagegen zu schützen

Wenn Sie Ihre vertrauenswürdige Geschäftskommunikation schützen, schützen Sie nicht nur Ihre Mitarbeiter, sondern auch Ihre Geschäftspartner und Kunden.

71 %

der Mitarbeiter gaben zu, dass sie sich mitunter riskant verhalten, z. B. Kennwörter wiederverwenden oder auf unbekannte Links klicken.

2. Proofpoint. *2024 State of the Phish Report.* 2024.

4. Anleitung für Mitarbeiter

Selbst wenn Technologien 99 % der Bedrohungen blockieren, kann das restliche 1 % immer noch einen schwerwiegenden Zwischenfall verursachen. Hier wird das menschliche Verhalten zum entscheidenden Faktor. denn Bedrohungsakteure benötigen bei ihren schädlichen Kampagnen in der Regel die Unterstützung Ihrer Mitarbeiter.

Doch Angriffe sind nicht das einzige Problem. Anwender gefährden oft aus Bequemlichkeit die Sicherheit ihrer Unternehmen. Laut dem Proofpoint *2024 State of the Phish*-Bericht:

- 71 % der Mitarbeiter gaben zu, dass sie sich mitunter riskant verhalten, z. B. Kennwörter wiederverwenden oder auf unbekannte Links klicken.
- 96 % dieser Mitarbeiter wussten, dass ihr Verhalten riskant war, handelten aber trotzdem so.

Da KI-Tools zunehmend in den Arbeitsalltag integriert werden, sind Mitarbeiter auch neuen Risiken ausgesetzt, wie etwa der Weitergabe vertraulicher Daten an unbefugte KI-Anwendungen oder dem unbeabsichtigten Auslösen versteckter Prompt-Injections durch die Interaktion mit KI-Assistenten.

Wenn Angriffe und fahrlässige Handlungen von Anwendern zusammenkommen, erhöht sich die Erfolgschance einer Kompromittierung. Genau aus diesem Grund müssen Sie Ihre Anwender schulen.

Suchen Sie nach einer Lösung, die folgende Funktionen umfasst:

- **Nutzung Ihrer Bedrohungsdaten,** um Ihre am häufigsten angegriffenen und besonders gefährdeten Anwender zu identifizieren
- **Bereitstellung risikobezogener Anwenderschulungen mit realen Bedrohungsbeispielen,** die Ihr Unternehmen tatsächlich ins Visier nehmen
- **Ausrichtung auf echte Verhaltensänderung** und nicht nur auf das reine Absolvieren der jährlichen Sicherheitsschulung
- **Motiviert die Mitarbeiter dadurch,** dass ihnen ihre individuellen Risikowerte sowie deren Einfluss auf die Sicherheitslage des Unternehmens aufgezeigt werden
- **Bewertung der Effektivität** und Bereitstellung nützlicher Berichte, die Ihnen helfen, Ihre Strategie zu verfeinern
- **Thematisierung von KI-Risiken in Schulungen,** einschließlich der sicheren Verwendung von generativer KI und der Erkennung von KI-generierten Social-Engineering-Angriffen

Starke Technologie und wachsame Mitarbeiter sind entscheidend, um personenzentrierte Bedrohungen zu stoppen. Beim Schutz Ihrer Geschäftsabläufe ist jeder Anwender gefragt.

5. Schutz vor Kontoübernahmen

Proofpoint-Daten zeigen, dass 99 % der Unternehmen regelmäßig von Kontoübernahmeversuchen betroffen sind. Diese Angriffe sind eine Form des Identitätsdiebstahls, bei denen sich Cyberkriminelle Zugriff auf ein Online-Konto verschaffen oder es „übernehmen". Es überrascht daher nicht, dass Cloud-basierte Identitätsanbieter wie Microsoft Entra ID, Google und Okta am häufigsten angegriffen werden. Diese Konten dienen als Single-Sign-On-Gateways zu den Unternehmensanwendungen eines Anwenders.

Sie müssen sich jedoch nicht nur um Ihre eigenen Konten Sorgen machen. Cyberkriminelle kompromittieren auch die Konten vertrauenswürdiger Geschäftspartner, um Aufklärung durchzuführen und weitere Angriffe zu starten. Diese kompromittierten Konten dienen als Einstiegspunkt für mehrstufige Angriffe, die sich über das gesamte Ökosystem eines Unternehmens ausbreiten, während sie sensible Daten stehlen, betrügerische Transaktionen tätigen und Chaos anrichten.

Künstliche Intelligenz und Machine Learning sind unerlässlich für die Überwachung der Geschäftskommunikation im großen Umfang sowie für die Automatisierung der Reaktionsmaßnahmen. Verhaltensbasierte KI-Modelle können subtile Anzeichen für eine Kontenkompromittierung erkennen, z. B. ungewöhnliches Anmelde- und E-Mail-Versandverhalten oder Veränderungen in den Kommunikationsbeziehungen, was regelbasierte Systeme übersehen würden.

Suchen Sie nach einer Lösung, die folgende Funktionen umfasst:

- **Kontinuierliche Überwachung aller Konten** von Cloud-basierten Identitätsanbieter-Diensten wie Microsoft Entra ID, Google und Okta
- **Nutzung von Bedrohungsdaten** in Kombination mit Verhaltensdaten und Machine Learning, um kompromittierte Konten zu erkennen
- **Schützt vor Kontoübernahmeangriffen,** die die Multifaktor-Authentifizierung (MFA) umgehen; bei 65 % der übernommenen Konten war MFA aktiviert
- **Beschleunigt Ihre Untersuchungen** durch Bereitstellung einer zentralen Übersicht aller Aktivitäten nach einer Kontoübernahme
- **Automatisiert Reaktionsmaßnahmen** wie die Sperrung von Konten, das Erzwingen von Kennwortzurücksetzungen und das Rückgängigmachen böswilliger Änderungen an Postfachregeln und MFA-Einstellungen
- **Entfernt verdächtige Drittanbieter-Anwendungen** als Teil der Bereinigung nach einer Kontoübernahme

Kontoübernahmen können hohe Kosten verursachen und Ihre Marke schädigen. Deshalb benötigen Sie starke Schutzmaßnahmen, mit denen Sie Ihr Risiko minimieren können.

Vermeiden Sie einen fragmentierten Ansatz

Beim Aufbau einer Verteidigungslinie gegen Angriffe über E-Mail oder andere Vektoren scheinen Einzellösungen von mehreren spezialisierten Anbietern naheliegend. Schließlich können spezialisierte Anbieter den Eindruck erwecken, dass sie für die Abwehr bestimmter Arten von Angriffen gut ausgerüstet sind. Dieser isolierte Ansatz weist jedoch mehrere Nachteile auf.

Zunächst einmal verursacht er blinde Flecken in den Sicherheitsmaßnahmen. Bei nicht nahtlos integrierten Tools ist es für Sicherheitsteams schwierig, sich einen Überblick über die gesamte Sicherheitsumgebung zu verschaffen. Das erhöht die Gefahr, dass Bedrohungen nicht erkannt werden, und verzögert die Reaktion auf Zwischenfälle.

Fragmentierte Tools können auch nicht den umfassenden KI-Ansatz bieten, der zur Abwehr heutiger Bedrohungen erforderlich ist. Ausgeklügelte, KI-generierte Angriffe lassen sich nur aufdecken, wenn Sprachmodelle, Computer Vision, Analysen des Benutzerverhaltens und Bedrohungsdaten zusammenarbeiten und Kontextinformationen austauschen.

Zudem ist es für Teams zeitaufwändig und ineffektiv, mehrere Sicherheitstools zu verwalten, da sie zudem Daten aus isolierten Kontrollpunkten zusammenführen müssen. Hinzu kommt die überwältigende Anzahl der von diesen Plattformen generierten Warnmeldungen, die Ihre Mitarbeiter überlasten und dazu führen, dass Bedrohungen übersehen werden. All das treibt die Betriebskosten in die Höhe.

Warum also nicht einen effektiveren Ansatz verfolgen? Setzen Sie eine ganzheitliche, vorab integrierte Sicherheitsplattform ein, die alle personenzentrierten Bedrohungen abdeckt. Die Entscheidung für einen einzigen vertrauenswürdigen Partner ermöglicht nicht nur vereinfachte Verwaltungsabläufe, sondern bietet auch finanzielle Vorteile.

99 %

der Unternehmen sind regelmäßig von Kontoübernahmeversuchen betroffen.

3. Proofpoint-Forschung.
4. Ebd.

Fazit

Eine umfassende personenzentrierte Sicherheitsstrategie kann Ihr Unternehmen vor einem breiten Spektrum an Bedrohungen schützen. Als ersten Schritt zu diesem Ziel sollten Sie sich für die richtige Lösung entscheiden. Suchen Sie nach einer Lösung, die Bedrohungsdaten für E-Mails, Collaboration-Tools, Messaging-Plattformen und Cloud-Anwendungen aggregiert. Es sollte auch wichtige Einblicke in riskantes Anwenderverhalten bieten und Ihre Sicherheitskultur fördern.

Ist Ihre aktuelle Lösung ausschließlich auf E-Mails beschränkt? Oder verlassen Sie sich auf fragmentierte Einzellösungen? Dann besteht Verbesserungspotenzial. Bewerten Sie jetzt, wie gut Ihre Sicherheitsmaßnahmen Sie vor allen personenzentrierten Bedrohungen schützen – in E-Mails und darüber hinaus.

Konsolidierung mit Proofpoint

Mit Proofpoint Prime Threat Protection erhalten Sie eine vorab integrierte Sicherheitsplattform, die umfassenden Schutz bietet Prime blockiert Bedrohungen in modernen Arbeitswelten, einschließlich E-Mails und digitaler Kanäle. Die Lösung schützt jedoch nicht nur vor dem breitesten Spektrum an Bedrohungen, sondern erreicht dabei auch erstklassige Erkennungsgenauigkeit. Proofpoint Prime wird von der Proofpoint Nexus AI-Plattform unterstützt, einer Kombination aus KI-Modulen, darunter Sprachmodelle, Machine Learning, Computer Vision, Beziehungsdiagrammen und Bedrohungsdaten. Damit erzielt die Plattform eine Erkennungseffizienz von 99,999 % sowohl bei herkömmlichen als auch bei KI-generierten Bedrohungen.

Als weiteres Plus liefert Proofpoint Prime detaillierte Einblicke in das personenbezogene Risiko und stärkt die Anwenderresilienz. Außerdem schützt die Lösung sowohl vor kompromittierten Anwender- als auch vor kompromittierten Lieferantenkonten, um Ihre vertrauenswürdige Geschäftskommunikation sicher zu halten.

Proofpoint bietet die einzige moderne Cybersicherheitsarchitektur, die einen adaptiven Ansatz verfolgt, um die wertvollste Ressource und den größten Risikofaktor Ihres Unternehmens zu schützen: Ihre Mitarbeiter. Deshalb vertrauen mehr als 2,7 Millionen Kunden aller Größen, darunter mehr als 80 der Fortune 100, auf Proofpoint.

proofpoint.

LERNENSIE DIE PROOFPOINT-PLATTFORM KENNEN →