proofpoint.

Einkaufsleitfaden für Lösungen zur Datenverlustprävention

Dieser Einkaufsleitfaden beschreibt die wichtigsten Funktionen einer modernen Datenschutzlösung und die Erfahrungen, die Proofpoint bei seinen erfolgreichen Projekten zur Datenverlustprävention für 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 Datenverlustprävention (Data Loss Prevention, DLP) beschäftigen oder ihre vorhandenen DLP-Systeme aktualisieren möchten.

Personenzentrierte Sicherheit als Ausgangspunkt

Um Daten vor speziellen und gängigen Bedrohungen schützen zu können, benötigen Sie eine Plattform, die ein personenzentriertes Sicherheitsmodell unterstützt. Grundsätzlich bietet ein solches Sicherheitsmodell einen vollständigen Überblick darüber, wie Anwender mit vertraulichen Daten interagieren, wobei alle riskanten Verhaltensweisen erfasst werden. Dadurch steht Ihnen wichtiger Kontext zu den Absichten der Anwender zur Verfügung, falls Daten verloren gehen oder gestohlen werden oder deren Handlungen verdächtig erscheinen.

Mit einer Lösung, die einen personenzentrierten Ansatz verfolgt, können Sie drohende Datenverluste in E-Mails, auf Endpunkten und in Cloud-Anwendungen wie Microsoft 365, Google Workspace und Salesforce usw. frühzeitig erkennen. Einblicke dieser Art erlauben eine schnelle Reaktion und gewährleisten, dass Sie die richtigen Maßnahmen zur Vermeidung von Datenverlustereignissen ergreifen können.

Wichtige Elemente einer modernen DLP-Lösung

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

Überwachung

Informationsschutz darf sich nicht nur auf Inhalte konzentrieren, sondern muss auch berücksichtigen, was Insider damit machen. Wenn Sie die Datenaktivitäten aller Anwender auf Endpunkten, in E-Mails, in der Cloud und im Web überwachen, erhalten Sie einen umfassenden Überblick und kontextbezogene Einblicke.

85 %

der Unternehmen waren 2023 von mindestens einer Datenschutzverletzung betroffen

50 %

der berufstätigen Erwachsenen haben in den letzten zwei Jahren den Arbeitsplatz gewechselt und bei ihrem Weggang Daten mitgenommen

Erkennung

Sie benötigen eine Lösung, die Bedrohungen möglichst in Echtzeit erkennt, wenn ein Anwender riskante Aktivitäten ausführt oder Daten potenziell offengelegt werden, selbst wenn diese Vorfälle nicht das Ausmaß eines veritablen „Zwischenfalls“ erreichen. Bei den Erkennungsfunktionen müssen Sie auf ein gutes Gleichgewicht achten, um im Idealfall ausschließlich aktuelle und entscheidungsrelevante Warnmeldungen zu erhalten. Dabei darf die Zahl der eingehenden Warnmeldungen die Anwender nicht überfordern.

Analyse

Mit guten Analysefunktionen können Sie Trends im Anwenderverhalten analysieren und nach Bedrohungen suchen. Dies ist jedoch nur möglich, wenn die DLP-Lösung die Anwenderaktivitäten der verschiedenen Kanäle kombiniert, da sie nur dann alle riskanten Verhaltensweisen der Anwender erkennen kann. Dies lässt sich zwar automatisieren, doch für den Erfolg ist es entscheidend, dass die Analysten sich mit den Daten selbst intensiv auseinandersetzen können.

Reaktion

Es ist wichtig, Zwischenfälle schnell und effizient zu untersuchen und darauf zu reagieren. Je länger eine Bedrohung fortbesteht, desto mehr Schaden kann sie anrichten – sowohl für die Reputation Ihres Unternehmens als auch in finanzieller Hinsicht. Eine moderne DLP-Lösung kann Richtlinien automatisch durchsetzen und Bedrohungen beheben. Die Automatisierung schützt Ihre wertvollsten Daten und erhöht die Effizienz Ihres Sicherheitsteams.

Prävention

Prävention umfasst die Maßnahmen, die Anwender davon abhalten, absichtlich oder unabsichtlich gegen Sicherheitsrichtlinien zu verstoßen. Dazu müssen die Anwender geschult, Echtzeit-Erinnerungen ausgegeben und Anwenderaktivitäten bei Bedarf blockiert werden.

Drei primäre Anwendungsfälle

Unternehmen verlieren vor allem durch drei große Schwachstellen Daten – und alle drei Schwachstellen beziehen sich auf den Faktor Mensch.
Eine personenzentrierte Datenschutzplattform muss Reaktionsmöglichkeiten für folgende Schwachstellen parat haben:

- Fahrlässige Anwender, die nicht sorgfältig mit vertraulichen Daten umgehen
- Fahrlässige Anwender, die vertrauliche Daten bei der Nutzung von Apps für generative KI (GenAI) gefährden
- Böswillige Insider, die vorsätzlich Schaden anrichten wollen

1. Fahrlässige Anwender und häufige Fehler

Proofpoint hat in seinem Data Loss Landscape-Bericht 2024 fahrlässige Anwender als häufigste Ursache für Datenverlust genannt. Diese Anwender haben nicht die Absicht, Daten zu verlieren, sondern wollen einfach ihre Arbeit so effizient wie möglich erledigen. 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.

3,5 Mrd. USD werden laut Schätzungen im Jahr 2025 insgesamt für DLP ausgegeben[1]

77 TAGE dauert die Behebung der Folgen von Insider-Bedrohungen[2]

85 % aller Unternehmen sind Ziele von Cloud-Angriffen[3]

56 % der Zwischenfälle werden durch fahrlässige Anwender verursacht[4]

Diese Anwender verursachen unter anderem durch folgende Fehler Risiken:

- Senden von E-Mails (mit oder ohne Anhang) an die falschen Empfänger
- 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

Schutz vor fahrlässigem Verhalten

Ein effektives personenzentriertes System für Informationsschutz blockiert riskante Aktivitäten. Darüber hinaus bietet es 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.
- **Erkennung:** Das System sollte E-Mails, Dokumente und Daten überwachen und dabei kontinuierlich die Compliance-Risiken bewerten. Da Inhalte verschiedene Kanäle durchlaufen (z. B. Endpunkte, E-Mails, die Cloud oder das Web), sollten sie gescannt werden, um sicherzustellen, dass ihre Übertragung, Weitergabe oder Freigabe nicht gegen die Richtlinien Ihres Unternehmens verstößt. Wenn in einer E-Mail ein Verstoß erkannt wird, sollten Sicherheitsteams die Möglichkeit erhalten, die E-Mail zu blockieren oder zur weiteren Beobachtung zu verfolgen.
- **Prävention:** Es muss verhindert werden, dass Anwender vertrauliche Daten über die verschiedenen Kanäle und Geräte exfiltrieren. Dazu gehören auch fehlgeleitete E-Mails (mit und ohne Anhang), USB-Sticks, Web-Uploads, Cloud-Synchronisierungen 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.

1 The Radicati Group: „Data loss prevention (DLP) market value revenue forecast worldwide from 2019 to 2025“ (Prognosen zum weltweiten DLP-Markt 2019–2025), Mai 2022.
2 Ponemon Institute: „2022 Cost of Insider Threats: Global Report“ (Kosten von Insider-Bedrohungen 2022: Weltweit), Februar 2022.
3 Assaf Friedman und Itir Clarke (Proofpoint): „How Attackers Use Compromised Accounts to Create and Distribute OAuth Apps“ (Wie Angreifer mit kompromittierten Konten OAuth-Apps erstellen und verteilen), Mai 2021.
4 Ponemon Institute: „2022 Cost of Insider Threats: Global Report“ (Kosten von Insider-Bedrohungen 2022: Weltweit), Februar 2022.

2. Fahrlässige Anwender und GenAI-Apps

Mit GenAI-Tools wie ChatGPT können Anwender ihre Produktivität deutlich steigern. Allerdings werden dabei häufig vertrauliche Daten geleakt.
Um Datenverlust zu verhindern, ohne die Produktivität zu beeinträchtigen, müssen Sie robuste Datenschutzmaßnahmen ergreifen. Unternehmen können jedoch keine Nutzungsrichtlinien für generative KI durchsetzen, wenn sie ihre eigenen Inhalte nicht kennen und nicht wissen, wie ihre Anwender damit umgehen.

Schutz vor fahrlässigem Verhalten bei GenAI-Tools

Sie müssen durch zuverlässige Datenschutzmaßnahmen sicherstellen, dass durch diese Tools keine vertraulichen Daten offengelegt werden. Die komplette Blockierung des Zugriffs auf GenAI-Tools ist keine Option. Vielmehr müssen Sie Wege finden, um Anwendern Zugriff auf diese Tools zu gewähren, mit denen sich die Produktivität steigern und Innovationen vorantreiben lassen.

Wenn Ihre Mitarbeiter GenAI-Tools nutzen sollen, ohne dabei Ihre Daten zu gefährden, müssen Sie einen personenzentrierten DLP-Ansatz verfolgen.
Eine entsprechende Lösung erlaubt bzw. verbietet Mitarbeitern sehr zielgenau die Nutzung von GenAI-Tools auf der Basis ihrer Verhaltensweisen und der eingegebenen Inhalte, selbst wenn die Daten manipuliert oder über mehrere Kanäle übertragen wurden.

Darauf sollten Sie achten:

- **Identifizierung vertraulicher Inhalte:** Wenn ein System identifizieren kann, welche Inhalte geschützt werden müssen, kann es Datenverlust viel effektiver stoppen. Achten Sie auf fortgeschrittene Methoden zur Identifizierung und Klassifizierung von Inhalten, z. B. Texterkennung mit OCR (Optical Character Recognition), exakter Datenabgleich und Abgleich indexierter Dokumente (IDM).
- **Anwenderüberwachung:** Sie müssen sehen können, wer GenAI-Tools wie in Ihrer Umgebung nutzt. Das System muss viele Arten von Anwenderaktionen erkennen, blockieren und melden können. Dazu gehören auch das Hochladen von Quellcode-Dateien und das Einfügen von geistigem Unternehmenseigentum.
- **Proaktive Abwehr von Risiken:** Wenn Ihre Teams individuelle Prüfungen erstellen und speichern, können sie regelmäßig nach Datenexfiltrationen und anderen riskanten Aktivitäten im Zusammenhang mit GenAI-Tools suchen.

3. Böswillige Anwender

Böswillige Anwender sind gefährlich, weil sie sich in einer idealen Position befinden, um vertrauliche Daten zu stehlen. Zu den riskantesten Insidern gehören Mitarbeiter, die das Unternehmen verlassen. 2023 waren sie in einem neunmonatigen Erfassungszeitraum für 87 % aller anormalen Dateiexfiltrationen bei Cloud-Mandanten verantwortlich, die die Proofpoint Information Protection-Plattform nutzen. Oft glauben diese Anwender, dass sie aufgrund der vielen Zeit, die sie in ihre Projekte investiert haben, das Recht haben, Daten mitzunehmen.

Böswillige Insider bergen ein besonders großes Risiko, weil sie den richtigen Augenblick abwarten können, um ihren privilegierten Zugriff für die Suche nach wertvollen Daten und Sicherheitsschwachstellen auszunutzen. Hinzu kommt, dass sich Firmen oft selbst das Leben schwer machen, weil sie Mitarbeitern erlauben, Daten auf privaten Geräten zu nutzen und zu speichern, und so den Diebstahl vertraulicher Daten erleichtern.

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

Schutz vor böswilligen Anwendern

Ein personenzentriertes System überwacht bestimmte Anwender genauer 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 (Endpunkte, E-Mails, Cloud und Web) bietet einen umfassenden Überblick und kontextbezogene Einblicke in Anwenderaktivitäten. 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. Wenn Anwender nicht autorisierte Anwendungen installieren oder ausführen, sollten diese Aktivitäten ebenfalls überwacht werden. Zudem sollte das Sicherheitsteam alle Anwender, die eine Warnmeldung auslösen, in Echtzeit überwachen können.
- **Untersuchungen:** Das System sollte eine Bibliothek an Warnmeldungen für die gängigsten Anwendungsszenarien (Arbeitszeitbetrug, Datenexfiltration, Umgehung von Sicherheitskontrollen) enthalten, da dies die Einrichtung deutlich beschleunigt. Das Sicherheitsteam sollte Warnmeldungen mit detaillierten Metadaten und Screenshots von Anwenderaktivitäten erhalten. Eine kontextbezogene Zeitleiste der Ereignisse hilft den Analysten, die Fragen nach dem Wer, Was, Wo und Wann in Bezug auf Anwenderaktivitäten zu verstehen.
- **Moderne Architektur:** Eine Cloud-native Plattform bietet den Vorteil, dass sie sich auf hunderttausende Anwender skalieren lässt. Wenn sie Funktionen wie attributbasierte Zugriffssteuerung, Datenmaskierung und -anonymisierung sowie Unterstützung für standortübergreifende Rechenzentren beinhaltet, können Sie die Anforderungen in Bezug auf Datenschutz und Datenaufbewahrung erfüllen. Zudem erweitert ein modernes System Ihr Sicherheitssystem, weil es 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

Erforderliche Funktionen

Nachdem Sie die Funktionsweise moderner personenzentrierter DLP-Systeme kennengelernt haben, sehen wir uns an, welche Funktionen Sie genau benötigen. Diese werden in drei Kategorien unterteilt:

- Erkennung und Verhinderung von Datenverlustrisiken
- Analyse und Reaktion
- Bereitstellung und Implementierung

Erkennung und Verhinderung von Datenverlustrisiken

Mit Einblicken in das Anwenderverhalten und vertrauliche Inhalte können Sicherheitsteams angemessen und zielgerichtet auf Datenrisiken reagieren.

KUNDENANFORDERUNG	ERFORDERLICHE FUNKTIONEN
Erkennung vertraulicher Inhalte	Erkennung und Analyse vertraulicher Daten in E-Mails, auf Endpunkten, in der Cloud und im Web
	Integrierte Funktion zur Klassifizierung vertraulicher Daten innerhalb des Unternehmenskontexts
	KI-gestützte Datenklassifizierung mit Large Language Models (LLM)
	Fortgeschrittene Identifizierungsmethoden, einschließlich: • OCR (Optical Character Recognition) • Exakter Datenabgleich (EDM) • Abgleich indexierter Dokumente (IDM)
	Vorkonfigurierte Richtlinien zur Erkennung vertraulicher Daten, z. B.: • Personenbezogene Daten • PCI DSS, SOX, GLBA, SEC-Insiderhandel-Bestimmungen • Geschützte Gesundheitsdaten, HIPAA, ICD-9, ICD-11, National Drug Code • DSGVO, DPA (Großbritannien), DPD (EU), PIPEDA (Kanada)
	Möglichkeit zum Festlegen von Richtlinien für das Lesen und Anwenden von Microsoft Information Protection-Vertraulichkeitsbezeichnungen, um geschäftskritische Daten zu identifizieren

KUNDENANFORDERUNG	ERFORDERLICHE FUNKTIONEN
Überwachung des Anwenderverhaltens	Personenzentrierter Ansatz, mit dem Analysten schnell reagieren können, weil er Einblicke in folgende Punkte liefert: • Anwenderabsicht • Datenzugriffsmuster • Anwendungszugriffsmuster
	Möglichkeit zum Überwachen von Anwenderinteraktionen mit Daten auf verwalteten und nicht verwalteten Endpunkten sowie in der Cloud, z. B.: • Umbenennung von Dateien • Änderung von Dateierweiterungen • Web-Upload und -Download • Kopie auf USB-Gerät • Synchronisierung mit Cloud-Freigaben • Dokumentöffnung • Ungewöhnliche Dateiaktivitäten
	Überwachung der Nutzung von Websites und Anwendungen, z. B.: • Hochladen, Einfügen oder Eingeben von Inhalten auf GenAI-Seiten • Herunterladen und Installieren von Datensicherungs- und Hacking-Tools
	Überwachung der Verhaltensweisen besonders riskanter Insider, um deren Absichten zu verstehen und Risiken zu minimieren, z. B. Manipulierung der Windows-Registrierung zur Deaktivierung von Kontrollen
	Proaktive Überwachung riskanter Anwender ausschließlich mithilfe von Screenshots bei Warnmeldungen, um Datenschutz zu gewährleisten
	Möglichkeit zur Schulung von Anwendern und zur Abfrage des Grunds für den Zugriff auf vertrauliche Daten, statt sie zu blockieren und die Produktivität zu beeinträchtigen (E-Mail, Endpunkt, Cloud, Web)
Verhinderung von Datenverlust	Security-Awareness-Schulungen, die Anwendern helfen, ihr Verhalten zu ändern, indem sie lernen, wie sie Cybersicherheitsrisiken vermeiden und vertrauliche Daten schützen
	Verhinderung der Exfiltration vertraulicher Daten über verwaltete Endpunkte, z. B.: • Kopieren von Dateien auf nicht autorisierte USB-Geräte • Hochladen von Dateien in einen privaten Cloud-Ordner • Ausdruck vertraulicher Dokumente • Einfügen vertraulicher Inhalte aus der Zwischenablage • Netzwerkfreigaben
	Automatische Korrektur von zu weit gefassten Dateifreigaben in Cloud-Anwendungen und Reduzierung von Dateifreigabe-Berechtigungen
	Ermöglichung des sicheren Zugriffs auf vertrauliche Dateien in von der IT freigegebenen Cloud-Anwendungen über nicht verwaltete Geräte
	Automatische Erkennung von E-Mails mit oder ohne Anhang, die an die falsche Person gesendet werden, und Verhinderung ihrer Zustellung
	Automatische Erkennung von E-Mails, die zwar an die richtige Person, aber mit dem falschen Dateianhang gesendet werden, und Verhinderung ihrer Zustellung
	Verhinderung der Weitergabe oder Freigabe vertraulicher Daten, die noch nicht vordefiniert wurden, für private E-Mail-Konten und andere nicht autorisierte Konten

Analyse und Reaktion

Sicherheitsteams müssen Zwischenfälle in allen Kanälen schnell beheben können. Zudem gilt: Je weniger Daten Sie offenlegen, desto unwahrscheinlicher ist ein möglicher Missbrauch.

KUNDENANFORDERUNG	ERFORDERLICHE FUNKTIONEN
Kanalübergreifende Behebung von Zwischenfällen	Einheitliche kanalübergreifende Konsole für E-Mails, Endpunkte und Cloud, die für folgende Zwecke genutzt werden kann: • Triage-Prüfung von Warnmeldungen • Untersuchungen • Individuelle Untersuchungen • Reaktion
	Kanalübergreifende Analysen, die folgende Informationen liefern: • Anwenderaktivitäten im Zeitverlauf • Dateiaktivitäten im Zeitverlauf, d. h. Erstellung, Änderung und Weitergabe/Freigabe
	Proaktive Analysefunktionen, die Echtzeiteinblicke in riskantes Anwenderverhalten liefern
	Integration mit dem SIEM Ihres Unternehmens, um Triage-Workflows mit Ihren vorhandenen Tools zu ermöglichen
	Möglichkeit zur Erkennung und automatischen Behebung von Datenverlustrisiken durch kompromittierte Anwender, z. B.: • Beenden von Sitzungen • Zurücksetzen von Kennwörtern • Minimieren von Risiken • Ermitteln der Auswirkungen
Datenschutz	Flexible Zugriffssteuerung, damit Analysten nur die Daten sehen, die sie für Untersuchungen benötigen
	Anonymisierung von Informationen zur Anwenderidentifizierung und Maskierung vertraulicher Inhalte, um Daten zu schützen und Voreingenommenheit von Analysten zu vermeiden

Bereitstellung und Implementierung

Nachdem Sie die beste DLP-Lösung für Ihr Unternehmen ausgewählt haben, müssen Sie sie bereitstellen. Der Schlüssel zu einem reibungslosen Implementierungsprozess liegt in der Wahl des richtigen Partners für Ihr DLP-Projekt.

KUNDENANFORDERUNG	ERFORDERLICHE FUNKTIONEN
Implementierung	Cloud-native Lösung, die schnell bereitgestellt werden kann
	Hochskalierbare Lösung, die einfach auf hunderttausende Anwender pro Mandant erweitert werden kann
	Wartungsfreundliche Lösung mit minimalem Pflege- und Eingabeaufwand, bei der Updates eindeutig kommuniziert werden und Herstellerunterstützung bei Bedarf verfügbar ist
	Zentralisierte Richtlinie und Administration, die Datenaufbewahrungsanforderungen für verschiedene Regionen erfüllt
	Flexible Plattform, die mit Ihrem Sicherheitsökosystem integriert werden kann, einschließlich Lösungen von: • Microsoft • Okta und Sailpoint • CrowdStrike • Splunk und Service Now • Zscaler und Citrix ShareFile
	Ressourcenschonender Endpunkt-Agent (der im Benutzermodus arbeitet) mit folgenden Eigenschaften: • Liefert mehr Einblicke in potenzielle Insider-Bedrohungen • Verbessert die Anwenderproduktivität • Beseitigt Stabilitätsprobleme • Verursacht keine Konflikte mit anderen Lösungen
Implementierung	Professional Services, die Sie mit einem Team erfahrener Experten bei der schnellen Bereitstellung unterstützen, Ihr System an Ihren Anforderungen ausrichten und bei der Implementierung einer DLP-Lösung helfen, einschließlich: • Ermittlung der Anforderungen • Konzeption • Anpassung der Lösung • Tests und Optimierung • Schulung von Administratoren und Anwendern • Dokumentation
Managed DLP	Unternehmen jeder Größe sollten die Nutzung eines Managed DLP-Angebots in Erwägung ziehen, bei dem ein festes Team aus erfahrenen Experten Sie bei der Entwicklung, Bereitstellung und gemeinsamen Verwaltung unterstützt sowie gewährleistet, dass kontinuierlich Personal zur Verfügung steht.

MEHR ERFAHREN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

1207-013-04-01 7/24