proofpoint.

Zugriffs- und Datenschutzkontrollen für Proofpoint Information Protection

Einhaltung von Compliance-Vorgaben bei gleichzeitigem Schutz der Mitarbeiterrechte und Vermeidung von Voreingenommenheit

Wichtige Vorteile

- Gewinnung des Mitarbeitervertrauens
- Schutz kritischer Unternehmensdaten
- Einhaltung von Datenschutzgesetzen
- Vermeidung von Voreingenommenheit bei Untersuchungen

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

Datenschutz spielt heute eine immer größere Rolle – und seine Umsetzung wird immer schwieriger. Zusätzlich machen das hohe Tempo der digitalen Transformation, die Hybrid-Arbeit und die Zunahme von Cloud-Anwendungen den Schutz vertraulicher Daten immer komplexer. Und während Unternehmen immer größere Datenmengen sammeln, steigt auch der Wert dieser Daten – und das Risiko, dass diese wertvollen Daten verloren gehen oder (auch durch Insider) gestohlen werden.

Trotz der wachsenden Herausforderungen können sich Unternehmen auf der ganzen Welt keine Fehler erlauben. Auf ihnen lastet ein immer größerer Druck, strenge Datenschutzgesetze einzuhalten, die strikte Schutzmaßnahmen vorschreiben. Verstöße können teuer werden und auch zu hohen Geldstrafen und Marktverlusten führen. Tatsächlich nennt ein Drittel der Sicherheitsexperten Rechtsverstöße und Geldstrafen als Konsequenzen von Datenverlust.[1]

Proofpoint bietet eine umfassende Palette an Produkten, die speziell für die Verbesserung der Datensicherheit und die Verwaltung von Insider-Bedrohungen konzipiert wurde, ohne die Einhaltung der Datenschutzbestimmungen zu vernachlässigen. Die Proofpoint Information Protection-Produktfamilie implementiert robuste Zugriffs- und Datenschutzkontrollen. Sie beschränkt die Sichtbarkeit von Daten auf die Anwender, die sie wirklich sehen müssen, und gewährleistet die Anonymität der Mitarbeiter, indem identifizierende Daten vertraulich behandelt werden. Dadurch stärkt Proofpoint den Datenschutz und ermöglicht zudem unvoreingenommene Untersuchungen für einen ausgewogenen Informationssicherheitsansatz.

Datenschutz-orientierter Sicherheitsansatz

Proofpoint Information Protection basiert auf den Grundsätzen des standardmäßig integrierten Datenschutzes. Das bedeutet, dass Datenschutz proaktiv gewährleistet wird und bei der Systementwicklung eine zentrale Rolle spielt. Dadurch wird sichergestellt, dass IT-Systeme, Infrastrukturen und Geschäftsprozesse den Datenschutz bereits von Anfang an als Kernelement implementieren. Dieser Ansatz integriert Übersicht, Transparenz und Benutzerfreundlichkeit in das Design.

1 Proofpoint: Data Loss Landscape-Bericht, 2024.

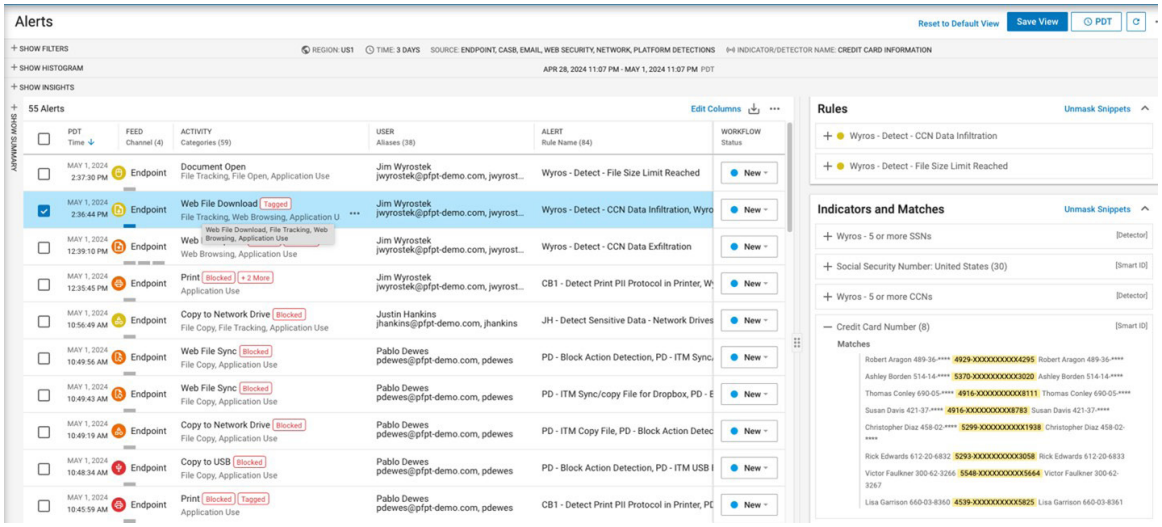

Abb. 1: Die Maskierung von Kreditkartennummern in Proofpoint Information Protection.

Verwaltung der Datenspeicherung

Proofpoint betreibt regionale Rechenzentren in den USA, Kanada, Europa, Australien und Japan, um die Vorschriften zu Datenschutz und Datenspeicherort einzuhalten. Sie haben vollständige Kontrolle darüber, in welchem dieser Rechenzentren Ihre Daten gespeichert sind.

Zur Verwaltung des Speicherorts auf den jeweiligen Geräten ermöglicht Proofpoint die Gruppierung von Endpunkten, wobei jede Gruppe einem bestimmten Rechenzentrum zugeordnet werden kann. Dadurch können Sie die Daten auf einfache Weise geografisch trennen, z. B. indem Sie eine US-Gruppe erstellen, die Daten zu Endpunkten in den USA verwaltet und in einem Rechenzentrum in USA speichert.

Gewährleistung von Datenschutz mit attributbasierter Zugriffssteuerung

Die attributbasierte Zugriffssteuerung von Proofpoint Information Protection ermöglicht die flexible und effiziente Verwaltung von Datenzugriffen. Sie gewährleistet, dass Sicherheitsanalysten nur die Daten sehen können, die sie für Untersuchungen sehen müssen.

Sie können zum Beispiel granulare Richtlinien erstellen und den Zugriff so zuweisen, dass Sicherheitsanalysten in den USA nur Daten zu US-amerikanischen Anwendern sehen können, aber keine Daten, die Anwender in Europa oder im Asien-Pazifik-Raum betreffen. Dank dieser spezifischen Zugriffssteuerung wird das Risiko unnötiger Datenexposition enorm reduziert. Wenn Analysten für eine Untersuchung auf die Daten eines bestimmten Anwenders zugreifen müssen, können Systemadministratoren den Zugriff auch zeitlich begrenzen, d. h. sie können festlegen, dass der Zugriff nur für einen bestimmten Zeitraum möglich ist.

Maskierung bei vertraulichen Daten

Proofpoint Information Protection umfasst eine Maskierungsfunktion, damit Daten vertraulich bleiben. Mit der Datenmaskierung werden vertrauliche Forensik-Daten wie geschützte Gesundheitsdaten und personenbezogene Daten in der Konsole verschleiert, wodurch sie nicht identifizierbar sind. Durch diesen Ansatz erhalten nur die Personen Zugriff auf die Daten, die diese vollständig und unmaskiert sehen können müssen.

Systemadministratoren können festlegen, welche Datenidentifikatoren wie maskiert werden sollen, z. B. dass von einer Kreditkartennummer alle Stellen bis auf die letzten vier Ziffern maskiert werden. Administratoren können auch basierend auf der Rolle der Anwender auswählen, welche und wie viele Daten angezeigt werden, z. B. dass nur autorisierte Analysten Ausschnitte von vertraulichen Daten sehen dürfen.

Schutz der Anwenderdaten mit Anonymisierung

Proofpoint Information Protection schützt Anwenderdaten mithilfe von Anonymisierung, wodurch Sie die Identität des Anwenders verbergen können. Sie können den Namen des Anwenders, den Hostnamen, die IP-Adresse, die Standortdaten und die Dateinamen anonymisieren.

Durch die Anonymisierung wird sichergestellt, dass nur autorisierte Sicherheitsanalysten die Daten anzeigen können, mit denen überwachte Anwender identifiziert werden können. Dies ermöglicht zudem unvoreingenommene Untersuchungen. Wenn es sich bei einem Anwender, der gerade gegen eine Unternehmensrichtlinie verstoßen hat, zum Beispiel um eine hochrangige Führungskraft handelt und die Identität des Anwenders bekannt wäre, würde der Zwischenfall möglicherweise anders behandelt werden oder der Sicherheitsanalyst würde vielleicht darüber hinwegsehen.

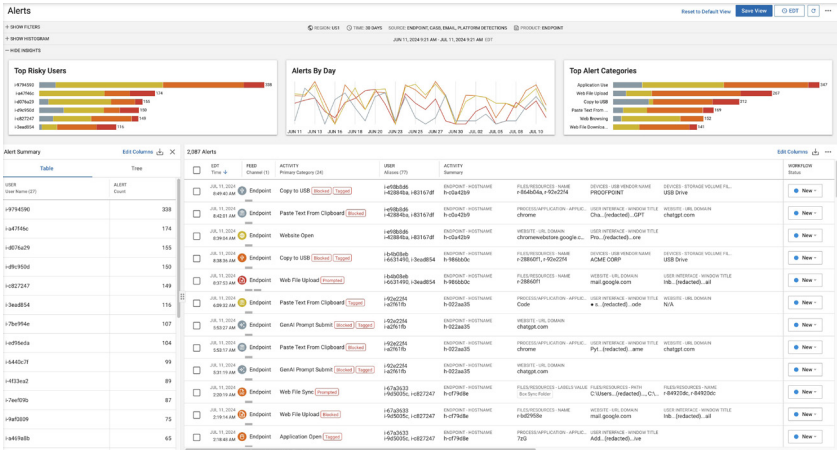

Abb. 2: Anonymisierte Anwenderdaten in Proofpoint Information Protection.

Falls die Identität des Anwenders im Laufe einer Untersuchung benötigt wird, kann der Sicherheitsanalyst die Deanonymisierung beantragen und ein Administrator kann diese gewähren.

Gleichgewicht zwischen Datenschutz und Datensicherheit

Ein gutes Gleichgewicht zwischen Datenschutz und Datensicherheit ist für alle Unternehmen wichtig. Daher sollten Sie folgende Prinzipien beachten:

- **Überwachung der Datenverlustkanäle:** Konzentrieren Sie Ihre Datensicherheitsmaßnahmen auf die Arbeitsweise der Mitarbeiter. Die meisten Datenlecks und -kompromittierungen erfolgen über E-Mails, Cloud-Anwendungen und USB-Laufwerke.
- **Klarheit und Transparenz:** Stellen Sie sicher, dass Ihre Mitarbeiter die Unternehmensrichtlinien zu Datenschutz und Datensicherheit kennen. Teilen Sie ihnen auch ganz genau mit, was Sie überwachen. Nur so können Sie Vertrauen aufbauen.
- **Schulung der Anwender mit automatisierten Benachrichtigungen:** Wenn ein Anwender gegen eine Unternehmensrichtlinie verstößt, kann der Anwender mithilfe einer automatisch generierten Nachricht darüber informiert werden. Mithilfe solcher automatisierten Benachrichtigungen können Sie Anwender auf ihr riskantes Verhalten hinweisen, ohne das peinliche Gefühl und die Emotionen, die mit einem Gespräch mit der Personalabteilung oder ihren Managern verbunden sind.
- **Selektivität:** Sie müssen nicht mehr Daten über alles und jeden sammeln, sondern können entscheiden, welche Daten wichtig sind und wie viel Sie wirklich über die Aktivitäten der Mitarbeiter wissen müssen.
- **Kontrolle des Datenzugriffs:** Sicherheitsadministratoren, Analysten sowie Mitarbeiter der Rechts- und Personalabteilungen haben häufig vollen Zugriff auf die Mitarbeiterdaten. Das ist jedoch nicht immer gut für den Datenschutz. Nutzen Sie daher unbedingt die in DLP- und ITM-Tools integrierten Zugriffssteuerungen.

Gewährleistung von Datenschutz mit Proofpoint

Mit Proofpoint Information Protection-Lösungen wie Proofpoint Data Loss Prevention und Proofpoint Insider Threat Management können Sie äußerst starken Datenschutz verwalten und gleichzeitig die Datenschutzbestimmungen einhalten. Außerdem ermöglicht die Lösung unvoreingenommene Untersuchungen. Proofpoint Information Protection berücksichtigt Inhalte und Verhaltensweisen, sodass Sie vertrauliche oder regulierte Daten identifizieren sowie auf riskante Anwenderaktivitäten und schädliche Inhalte hinweisen können – alles über eine zentrale Konsole, die Überblick über alle Kanäle bietet, einschließlich Endpunkte, E-Mail, Cloud und Web.

Proofpoint Managed Information Protection kombiniert die richtigen Menschen, Prozesse und Technologien, damit Sie Ihr Programm konzipieren, implementieren und weiterentwickeln können und optimierten Datenschutz sowie Datensicherheit erreichen.

MEHR ERFAHREN

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