Proofpoint Threat Response und die DSGVO

So erzielen Sie Compliance mit Sicherheitsautomatisierung und bewährten Datenschutzmethoden

WICHTIGE VORTEILE

Befolgung bewährter Sicherheitsmethoden

- Schnellere und effizientere Behebung gezielter Bedrohungen
- Entlastung Ihres IT-Teams dank automatisierter Reaktionen auf Zwischenfälle
- Keine Überlastung durch zu viele Warnmeldungen
- Erfassung und Priorisierung von Daten aus nicht vernetzten Sicherheitsgeräten
- Einblick in alle Bedrohungen mit umfangreichem Kontext

Einhaltung der DSGVO

- Verhinderung der Weitergabe personenbezogener Daten an externe Parteien
- Integration mit internen Kontrollsystemen
- Ergänzung interner Datenverarbeitungsressourcen
- Von Proofpoint unterstützter Compliance-Nachweis

Die meisten erfolgreichen Unternehmen setzen bei der Handhabung von Sicherheitszwischenfällen heute auf Automatisierungstechnologie. Was sind die Gründe für diesen Trend? Und was sollten Sie bedenken, wenn Sie Sicherheitsautomatisierung einführen, um die Einhaltung von Vorschriften, die Nutzung bewährter Vorgehensweisen und die Erzielung langfristiger geschäftlicher Ziele zu vereinfachen?

AUTOMATISIERUNG DER REAKTION AUF ZWISCHENFÄLLE TUT NOT

Die heute Cybersicherheitslandschaft verlangt nach schnellen Reaktionen. Die Sicherheitsteams stehen jedoch vor Herausforderungen, die die rasche und effiziente Reaktion auf gezielte Bedrohungen verhindern. Dazu gehören:

- **Mitarbeiter knappheit:** Die Reaktion auf Zwischenfälle kann sehr langwierig und aufwändig sein. Einige Aufgaben sind mit sehr viel Zeitaufwand verbunden und führen zu Engpässen. Wenn dieselben Aufgaben zudem für jeden Zwischenfall wiederholt werden müssen, können ohnehin schon stark ausgelastete Sicherheitsteams an ihre Grenzen stoßen.
- **Überlastung durch zu viele Warnmeldungen:** Je mehr Sicherheitsgeräte Sie einsetzen, desto mehr Warnmeldungen werden generiert, die von Ihrem Sicherheitsteam manuell einer Triage-Prüfung unterzogen werden müssen. Leider ist dieser Prozess für menschliche Fehler anfällig – und tatsächliche Zwischenfälle werden häufig nicht als solche erkannt und daher vernachlässigt.
- **Getrennt verwaltete Sicherheitsgeräte und Daten:** Zur Untersuchung von Zwischenfällen werden Informationen aus mehreren isolierten Quellen herangezogen, wobei jeder weitere Datenpunkt einem Puzzleteil ähnelt. Wie viele andere Unternehmen verzeichnen auch Sie zunehmend gezielte Bedrohungen, auf die Sie innerhalb von Minuten reagieren müssen. Wenn die Informationen jedoch zu sehr isoliert sind, werden Ihre möglichen Reaktionen ausgebremst.

SOAR-Lösungen (Security Orchestration, Automation and Response) zur Koordinierung, Automatisierung und Reaktion auf Sicherheitsmaßnahmen können dazu beitragen, diese Probleme zu beheben. Sie sammeln Warnmeldungen aus verschiedenen Quellen und bieten Workflows, mit denen die Reaktionen auf Zwischenfälle automatisiert werden. Mit einer SOAR-Lösung sparen Sie also Zeit. Zudem verringern Sie durch die Automatisierung der Reaktionsschritte die Zahl der Vollzeitmitarbeiter, die Sie für die Problembehebung benötigen, sowie die durchschnittlich erforderliche Zeit für die Erkennung, Eindämmung und Behebung von Bedrohungen.

Proofpoint Threat Response ist eine solche SOAR-Lösung, dank der der manuelle Aufwand und das Rätselraten rings um die Reaktion auf Zwischenfälle entfallen, sodass Ihr Sicherheitsteam Bedrohungen schneller und effizienter beseitigen kann. Threat Response erfasst Warnmeldungen aus verschiedenen Quellen, gruppiert die Meldungen und reichert sie automatisch mit wertvollem Kontext aus unseren Proofpoint-Bedrohungsdaten an. Das dauert nur wenige Sekunden. Dadurch erhalten Sie die wichtigsten Fakten zu Angriffen (wer, was und wo?), eine Zuordnungen zu IP-Adressen sowie Informationen aus externen Bedrohungsdatenquellen wie den Branchenstandard-Feeds STIX und TAXII. Ihre Analysten können die Sicherheitszwischenfälle schnell einer Triage-Prüfung unterziehen. Basierend auf den vom System erfassten sowie analysierten Kontext- und Forensikdaten liefert Threat Response eine umfassende Übersicht über die Bedrohung. Ihre Analysten können verschiedene automatisierte Reaktionen auslösen:

- Zugestellte E-Mails aus den Postfächern der Anwender entfernen
- Anwender zu Gruppen hinzufügen, die nur über eingeschränkte Berechtigungen verfügen
- Blockierungslisten für Firewalls und Webfilter aktualisieren
- Bedrohung durch Blockieren/Isolieren von Angriffen eindämmen – für Microsoft Exchange, Firewalls, Endpoint Detection and Response (EDR), Web-Gateway, Microsoft Active Directory, Netzwerkzugriffssteuerung (NAC) und andere Lösungen

DATENSCHUTZ UND SICHERHEITSABLÄUFE

DSGVO und die „Rechtmäßigkeit der Verarbeitung“

Entsprechend der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie von relevanten Datenverantwortlichen durchgeführt wird. Das ist zum Beispiel der Fall, wenn die personenbezogenen Daten erforderlich sind, um die Netzwerk- und Informationssicherheit zu gewährleisten. Die Verarbeitung personenbezogener Daten ist auch dann rechtmäßig, wenn sie unrechtmäßige oder schädliche Aktionen verhindert, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der gespeicherten oder übertragenen Daten gefährden. Diese „rechtmäßigen Interessen“ sind in der DSGVO in Artikel 6 „Rechtmäßigkeit der Verarbeitung“ definiert. Das rechtmäßige Interesse kann rechtskräftig festgestellt werden. Das ist jedoch nur möglich, wenn Sie die Datenverarbeitung begründen können und diese mit den Grundsätzen der Verhältnismäßigkeit und des Subsidiaritätsprinzips vereinbar ist. Diese Ausnahmen, die die Nutzung personenbezogener Daten für die IT-Sicherheit erlauben, sind in der DSGVO in Artikel 6(1)f und in Erwägungsgrund 49 definiert.

Für die Einhaltung der DSGVO-Vorgaben bietet die Erweiterung und Absicherung Ihrer Infrastruktur mit Sicherheitsservices wie Threat Response einen großen Vorteil. Diese Lösung ist ein wesentlicher Bestandteil einer modernen IT-Architektur. Threat Response kann so konfiguriert werden, dass die Verarbeitung von Daten in externen Sicherheitsarchitekturen (z. B. durch einen Anbieter für Bedrohungsdaten oder Sicherheitsservices) erfolgt. Threat Response stellt externen Parteien keinerlei Daten zur Verfügung, sondern verwendet diese Daten ausschließlich zu den Zwecken, die in der zwischen Ihnen und Proofpoint abgeschlossenen schriftlichen Servicevereinbarung beschrieben sind. Threat Response ist ausschließlich als lokale Lösung verfügbar und überträgt standardmäßig keine Daten aus dem Unternehmen.

Threat Response zu Verzeichnis von Verarbeitungstätigkeiten hinzufügen

Laut DSGVO sind die richtigen Einstellungen und die Integration in andere Systeme für die Compliance wichtig. Sie können Threat Response zu internen Aufzeichnungen von Datenverarbeitungsvorgängen hinzufügen, so wie es in der DSGVO in Artikel 30 „Verzeichnis von Verarbeitungstätigkeiten“ verlangt wird.

Interner Austausch personenbezogener Daten

Laut DSGVO Artikel 47, „Verbindliche interne Datenschutzvorschriften“, ist der interne grenzüberschreitende Informationsaustausch zulässig. Diese Unternehmensregeln sollten sämtliche Grundprinzipien und durchsetzbaren Rechte enthalten, die geeignete Garantien für die Übermittlungen beziehungsweise Kategorien von Übermittlungen personenbezogener Daten bieten.

Zur Gewährleistung der Einhaltung der DSGVO-Vorgaben muss die Implementierung über ein internes Kontrollsystem erfolgen. Dazu müssen Sie ein solches internes Kontrollsystem einrichten, wobei ein konformes System aus Elementen eines internen Kontrollsystems und einem Überwachungssystem besteht und Möglichkeiten bietet, die Aktivitäten in Ihrem Unternehmen zu kontrollieren. So wird gewährleistet, dass Geschäftstransaktionen ordnungsgemäß erfasst und dokumentiert sowie die DSGVO-Grundprinzipien eingehalten werden.

DATENAUSTAUSCH MIT DRITTEN[1]

Um angemessenen Schutz zu erreichen, erlaubt die DSGVO Unternehmen die Einbeziehung externer Experten, Tools und Services, die interne Sicherheitsmaßnahmen unterstützen. Die DSGVO-Vorgaben schreiben strikt vor, dass gewährleistet werden muss, dass Drittanbieter (Datenverarbeiter) Ihre Datenschutzstufe unterstützen. Dies wird in Artikel 28, „Auftragsverarbeiter", definiert. Der Datenverantwortliche darf nur Datenverarbeiter einsetzen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Um Sie bei der Einhaltung dieser strikten Vorgaben zu unterstützen, stellt Proofpoint Ihnen verschiedene Dokumente für alle ergänzenden Produkte zur Verfügung. Dazu gehören die Vereinbarungen über die Datenverarbeitung, die Sie für Ihr Prozessverzeichnis benötigen.

Threat Response basiert auf bewährten branchenspezifischen und Compliance-Methoden. Mit dieser Lösung wird die Reaktion auf Zwischenfälle automatisiert und beschleunigt sowie gewährleistet, dass Sie personenbezogene Daten im Sicherheitskontext strikt nach den Vorgaben der DSGVO verwenden. Als zusätzlichen Vorteil bietet Proofpoint rechtssichere Dokumentation, damit Sie Ihre Compliance nachweisen können.

1 Dies gilt, wenn externer Datenaustausch oder externe Services konfiguriert werden (z. B. Proofpoint Targeted Attack Protection).

WEITERE INFORMATIONEN

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

proofpoint.

0203-001-01-01 1/20