Checkliste:
Fünf Gründe, warum DLP in Ihrem MSP-Portfolio nicht fehlen darf

Warum ist Schutz vor Datenverlust für Service Provider wichtig?

Seit Jahren gelingt es Unternehmen kaum, sensible Daten vor nicht autorisierten Zugriffen und Exfiltration zu schützen – Gefahren, die durch externe Angriffe oder Insider-Bedrohungen (z. B. IT-Konfigurationsfehler und menschliche Fehler) entstehen. Die Folge sind häufig peinliche Schlagzeilen, verlorenes Vertrauen bei Kunden und Partnern, finanzielle Verluste und behördliche Sanktionen.

Mit den neuen verhaltensbasierten DLP-Technologien (Data Loss Prevention, Schutz vor Datenverlust) können MSPs nun DLP-Services anbieten und verwalten, mit denen sich die Datenverlustrisiken ihrer Kunden mit minimalem Aufwand verringern lassen.

Nutzen Sie diesen aktuellen Trend und geben Sie Ihren Kunden die Gewissheit, dass ihre Daten sicher geschützt sind und alle gesetzlichen Vorschriften eingehalten werden.

„80 % der weltweit tätigen Unternehmen gehen davon aus, dass es in den nächsten 12 Monaten wahrscheinlich zu einer Kompromittierung ihrer Kundendaten kommen wird.“

Quelle: Cyber Risk Index Report, 2021, Ponemon Institute

Fünf Gründe, warum DLP in Ihrem Angebot nicht fehlen darf

1 Die Mitarbeiter der Kunden greifen über Endpunkte auf sensible (z. B. regulierte) Daten zu

Ihre Kunden möchten sensible Daten in der Cloud speichern. Wenn die Mitarbeiter über ihre Workstations darauf zugreifen können, können die Daten jedoch leicht über Peripheriegeräte oder Kommunikationskanäle wie E-Mail oder Instant Messenger exfiltriert werden.

Laut dem Verizon Data Breach Investigation Report 2022 stecken hinter mehr als 80 % der Datenschutzverletzungen finanzielle Motive. Deshalb sind primäre Daten – zum Beispiel regulierte Informationen, Geschäftsgeheimnisse sowie geistiges Eigentum – ein äußerst lukratives Angriffsziel.

Wenn die Mitarbeiter Ihrer Kunden auf ihren Endpunkten mit diesen Daten arbeiten, müssen Sie nicht autorisierte Zugriffe zuverlässig verhindern, damit Ihre Kunden keinen erheblichen finanziellen, regulatorischen oder Reputationsrisiken ausgesetzt sind.

2 Sie suchen nach neuen Einnahmequellen für Ihr Geschäft

Im Acronis Pulse of the MSP-Bericht für das Jahr 2021 können wir sehen, dass MSPs davon ausgehen, ihre Haupteinnahmen in den nächsten Jahren hauptsächlich im Bereich Cyber Security zu erzielen. Da jedoch die Mehrzahl der Service Provider eine Form verwalteter Sicherheits-Services anbietet, verschärft sich der Wettbewerb in der Branche deutlich.

Die neuen verhaltensbasierten DLP-Technologien ermöglichen Ihnen, Ihr Portfolio mit DLP-Services zu diversifizieren, die MSPs und kleineren Unternehmen bisher verwehrt waren. Der Grund dafür lag in der hohen Komplexität, den erheblichen Kosten für die Service-Bereitstellung und einer langwierigen Amortisierung, da die Richtlinien an die sich ständig verändernden Geschäftsprozesse des jeweiligen Kunden angepasst werden mussten.

Verhaltensbasierte DLP-Technologien bieten Ihnen eine neue Einnahmequelle und ein attraktives DLP-Service-Angebot für Unternehmen aller Größen, mit dem Sie die Daten Ihrer Kunden besser vor nicht autorisierten Zugriffen schützen können.

3 Sie haben Kunden in streng regulierten Branchen (z. B. Gesundheitsdienstleister, Banken und Versicherungen, Behörden)

Falls Ihre Kunden mit personenbezogenen Informationen, Patientendaten, Karteninhaberdaten oder anderen sensiblen Daten streng regulierter Branchen arbeiten oder diese speichern, müssen diese mit mehr als nur mit Backups geschützt sein.

In den meisten gesetzlichen Bestimmungen (z. B. GDPR, HIPAA und PCI-DSS) ist festgelegt, dass die Meldung von Datenschutzverletzungen und Datenlecks innerhalb eines knappen Zeitraums erfolgen muss und die Kunden schwere Geldstrafen riskieren, wenn es zum Verlust sensibler Daten kommt.

DLP-Lösungen können als einzige Technologie Datenflüsse im Unternehmen überwachen und Datenlecks verhindern. Gleichzeitig bieten sie einen besseren Überblick über DLP-Ereignisse und ermöglichen ihre Untersuchung.

4 Einige Ihrer Kunden verzeichnen häufiger Angriffe und Datenlecks

Schon länger gibt es Branchen mit gravierenden Sicherheitslücken, die wertvolle sensible Daten verwalten und daher ein lukratives Ziel für Cyber-angreifer darstellen. Typische Beispiele sind das Bildungs- und Gesundheitswesen sowie andere öffentliche Sektoren. Dort muss der Zugriff auf Daten gewährleistet sein, gleichzeitig aber sollen die Daten ordnungsgemäß vor Datenlecks geschützt werden.

Dank verhaltensbasierter DLP-Technologien können Sie einen leistungsstarken DLP-Service zu einem äußerst günstigen Preis anbieten, der diese Unternehmen vor Compliance-Verstößen und Risiken durch Datenlecks schützt.

5 Sie haben Kunden, die Haftungsrisiken mit einer Cyberversicherung reduzieren (möchten)

Fakt ist: In den letzten Jahren waren Cyberversicherungen eines der heißesten Themen im Cyber Security-Bereich. Viele Kunden möchten ihre geschäftlichen Haftungsrisiken für den Fall einer Datenschutzverletzung mit einer Cyberversicherung minimieren.

Die Kosten dafür hängen unter anderem vom Jahres-umsatz, der Branche, den Datentypen und der Daten-menge sowie den vorhandenen Sicherheitsmaßnahmen ab. Sie haben nun die Möglichkeit, die DLP-Technologie in Ihr Service-Paket aufzunehmen, um Datenschutz-anforderungen für Cyberversicherungen zu erfüllen und die Versicherungskosten für Ihre Kunden zu minimieren.

Advanced DLP

Mit Advanced DLP für Acronis Cyber Protect Cloud schützen Sie vertrauliche Daten vor nicht autorisierten Zugriffen – damit Ihre Kunden nachts ruhig schlafen können. Die einzigartige verhaltensbasierte Technologie ermöglicht die individuelle Erstellung und kontinuierliche Erweiterung von DLP-Richtlinien für jeden einzelnen Kunden. Starten Sie Ihren Service mit minimalem Aufwand so einfach wie nie zuvor.

Acronis

Weitere Informationen auf www.acronis.com