チェックリスト
MSPでDLPサービスを提供する5つの理由

なぜMSPにとって情報漏えい防止（DLP）が重要なのか？

残念ながら現在も、組織は機密データを外部からの不正アクセスや流出、そして、ITの設定ミスやヒューマンエラーなどの内部リスクから保護することに成功していません。情報漏えい事故は、企業イメージや取引先からの信頼失墜、金銭被害、法的制裁などの結果をもたらします。

振る舞い検知ベースの情報漏えい防止（DLP）技術の進化に伴い、MSPは顧客のデータ損失のリスクを低減するために、簡単にDLPサービスの提供を開始し、管理できるようになりました。

今こうしたトレンドに投資し、データ保護規制コンプライアンスの取り組みを提供することでユーザーに安心・安全を提供するには良い機会です。

世界中80%の組織が、「今後12か月以内に顧客情報に影響を与える情報漏えい事故の可能性がある」と報告しています。

出典：Cyber Risk Index Report, 2021年、Ponemon Institute

MSPでDLPサービスを提供する5つの理由

1 顧客の従業員が、PC端末から機密データにアクセスできる（例えば、規制対象のデータ）

もし従業員がPC端末から機密データにアクセスできるなら、それらをクラウドに保存しようが何の意味もありません。データは周辺機器やEメールやインスタントメッセンジャーなどのネットワークチャネルを通じて容易に漏えいする可能性があります。

Verizon Data Breach Investigation Report（2022年版）によると、80%以上のデータ漏えいは金銭的な動機に基づくものです。このため、攻撃の標的になる主要なデータは、金銭上の利益を獲得するために活用される規制対象のデータや企業秘密、知的財産データのように価値の高いものです。

顧客の従業員がPC端末でこのようなデータの作成、保管、作業を行う場合、不正なユーザーや組織への情報漏えいを防止し、顧客の金銭被害、風評被害、コンプライアンス違反のリスクから救う必要があります。

2 ビジネスを成長させるために新しい収益源を探している

「Acronis Pulse of the MSP 2021 Report」 で は、MSP は2022年の主要な収益がサイバーセキュリティからくると予想しています。一方、マネージドセキュリティサービスを提供している大半のサービスプロバイダーにとっては、業界での競合が第一の課題になっています。

アクロニスの振る舞い検知ベースのDLP技術の進化によって、DLPサービスでポートフォリオを差別化できるようになっています。DLPサービスはかつて、顧客ごとに固有で変化を続けるビジネスプロセスに対して、ポリシーをマッピングする必要があったため、複雑すぎたり、サービスデリバリーコストが高すぎたり、価値を生み出すまでの時間が遅すぎたりするためにMSPや小規模組織では利用できなかったサービスでした。

アクロニスの振る舞いベースのDLP技術を使えば、新しい収益源を探し、あらゆる規模の組織に対して魅力的なDLPサービスを提供し、これによって顧客の機密データへのアクセスを許可されていない人物や組織による不正アクセスのリスクを低減します。

3 高度に規制された業界（例えば、ヘルスケア、SFSI、政府など）の顧客がいる

顧客が個人を特定できる情報（PII）、患者健康情報（PHI）、カード所有者データまたは高度に規制された業界で使用されるその他の機密データを操作したり保存したりする場合、単なるバックアップを超えたより高度なレベルの保護が必要になります。

GDPR、HIPAAおよびPCI-DSSのような規制の大半ではデータ侵害や漏えいを速やかに報告する必要があり、機密データ漏えいが発生した場合、深刻な反則金が顧客に課される可能性もあります。

データ漏えい防止ソリューションは、組織内のデータフローを監視し、可視化を進める一方でデータ漏えいを防止し、DLPイベントの調査を可能にする機能を提供します。

4 攻撃やデータ漏えいリスクに脆弱な顧客がいる

以前から、重要な機密データを保存しており、サイバー攻撃の標的になりやすいセキュリティ脆弱性を抱えた業界があります。データアクセシビリティが必要であると同時に不正なユーザーにデータを漏えいしないように効率的な保護が必要な教育、ヘルスケア、その他の公共セクターなどがこうした業界の一例です。

振る舞いベースのDLP技術によって、高度に競争力のあるDLPサービスを導入しやすい価格で提供し、コンプライアンス違反やデータ漏えいのリスクから組織を保護できるようになります。

5 責任を軽減するためにサイバー保険を検討中 / すでに契約した顧客がいる

現実に目を向けると、サイバー保険はこの数年にわたってサイバーセキュリティ業界の最も話題になっているトピックです。顧客はサイバー保険業者に注目し、データ漏えいが発生した場合にビジネス上の責任を制限しようとしています。

サイバー保険のコストは、企業の売り上げ規模や業界、保存するデータの種類や量、セキュリティのレベルなどを含むいくつかの要因に依存します。DLPをサービススタックに追加し、サイバー保険のデータ保護要件をカバーしたり顧客のコストを最小化することが可能です。

Acronis

詳細情報:
www.acronis.com