Acronis

WHITEPAPER

Bereitstellung und Skalierung von DLP-Services: Ein Leitfaden für MSPs

Trotz aller Aufmerksamkeit, Sicherheitsprotokolle und Gesetze versuchen kleine wie große Unternehmen seit Jahren mehr oder weniger erfolglos, die Gefahren von Datenlecks zu bannen. Die Zahl der Vorfälle steigt sogar: Risk Based Security meldet im „2021 Year End Report: Data Breach QuickView“ mehr als 22 Milliarden kompromittierte vertrauliche Datensätze. Dies ist der zweithöchste Wert seit 2005. Die überwältigende Mehrheit dieser Datensätze stammt aus Datenlecks. Ein Datenleck wird definiert als eine Sicherheitsverletzung, bei der vertrauliche, sensible oder geschützte Daten versehentlich oder absichtlich an eine nicht vertrauenswürdige Umgebung oder nicht autorisierte Benutzer inner- oder außerhalb des Unternehmens weitergegeben werden.

Was sind die zwei Hauptgründe für Datenlecks?

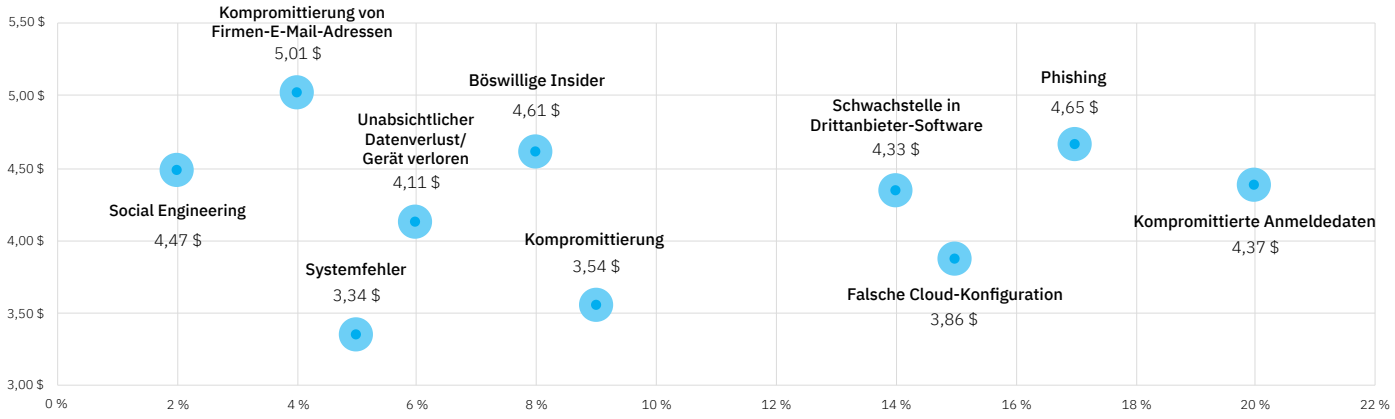
1. Externe Cyberbedrohungen

Laut der Definition im MITRE ATT&CK-Framework gehört die Datenexfiltration zu den letzten Taktiken, die böswillige Akteure im Rahmen eines Angriffs anwenden. Bei mehr als 80 % der Datenschutzverletzungen handeln die Angreifer laut Verizon Data Breach Investigation Report 2022 aus finanziellen Motiven.

Deshalb sind in der Mehrheit der Fälle sensible Daten das primäre Ziel. Sobald sich Angreifer Zugang zur Unternehmensumgebung verschafft haben, können sie versuchen, Daten über verschiedene Kanäle zu exfiltrieren. Da die Angriffe immer komplexer und Sicherheitsmaßnahmen immer erfolgreicher umgangen werden, steigt die Gefahr für die Daten der Unternehmen exponentiell.

2. Interne Risiken

Da externe Angriffe vom Malware-Schutz und anderen Endpunktschutztechnologien erkannt und gestoppt werden können, rücken andere – Insider-bezogene – Risiken für Unternehmensdaten in den Fokus. Ein gängiges Beispiel sind Endbenutzer, die Daten unabsichtlich an nicht autorisierte Parteien weitergeben (z. B. indem sie eine E-Mail weiterleiten). Ursache können versehentliche Fehler von Mitarbeitern, falsche IT-Konfigurationen oder böswillige Insider sein. Alle diese Fälle sind eine ernste Bedrohung für das Unternehmen und können zu äußerst kostspieligen Datenschutzverletzungen führen.



Dennoch werden die internen Risiken von einigen Unternehmen weiterhin unterschätzt. Deshalb möchten wir an dieser Stelle auf den „Cost of Data Breach Report 2021“ des Ponemon Institute verweisen, laut dem Insider an rund einem Drittel aller Datenschutzverletzungen beteiligt sind.

Welche Folgen haben Datenlecks für Unternehmen?

Datenlecks stellen für Unternehmen eine erhebliche Gefahr dar. Die Exfiltration sensibler Daten durch nicht autorisierte Personen hat diese Folgen:

- **Verstoß gegen Compliance-Vorgaben:** Die Speicherung, der Schutz und der Zugriff auf sensible Daten wie personenbezogene Daten von Mitarbeitern und Kunden, geschützte Gesundheitsinformationen und Karteninhaberdaten sind durch lokale und internationale Gesetze und Vorschriften (wie GDPR, CCPA, HIPAA, PCI-DSS) streng reguliert. Einige Standards wie GDPR schreiben sogar vor, dass Kompromittierungen innerhalb kürzester Zeit gemeldet werden müssen. Wenn Unternehmen die vorgeschriebene Frist für die Meldung einer Datenschutzverletzung versäumen, können hohe Strafen und sogar der Verlust der Compliance-Zertifizierungen drohen.
- **Finanzielle Schäden:** Bei Datenverlusten drohen Service Providern – neben möglichen behördlichen Geldstrafen für ihre MSP-Kunden – auch finanzielle Schäden aus der Haftung für die Sicherheit der Kunden, die unter Umständen vor Gericht geklärt wird. Darüber hinaus kann die Exfiltration von Geschäftsgeheimnissen oder geistigem Eigentum weitere finanzielle Verluste für Firmen bedeuten und sogar ihre Marktposition schädigen.
- **Reputationsrisiken:** Die Bloßstellung in peinlichen Schlagzeilen nach Datenschutzverletzungen kann für Unternehmen verheerend sein. In der Folge können nicht nur deren Kunden abwandern, sondern auch bestehende Partnerschaften und Neukundengeschäfte Schaden nehmen. Datenverluste bei Ihren Kunden können auch Ihren Ruf und Ihr Geschäft beeinträchtigen.

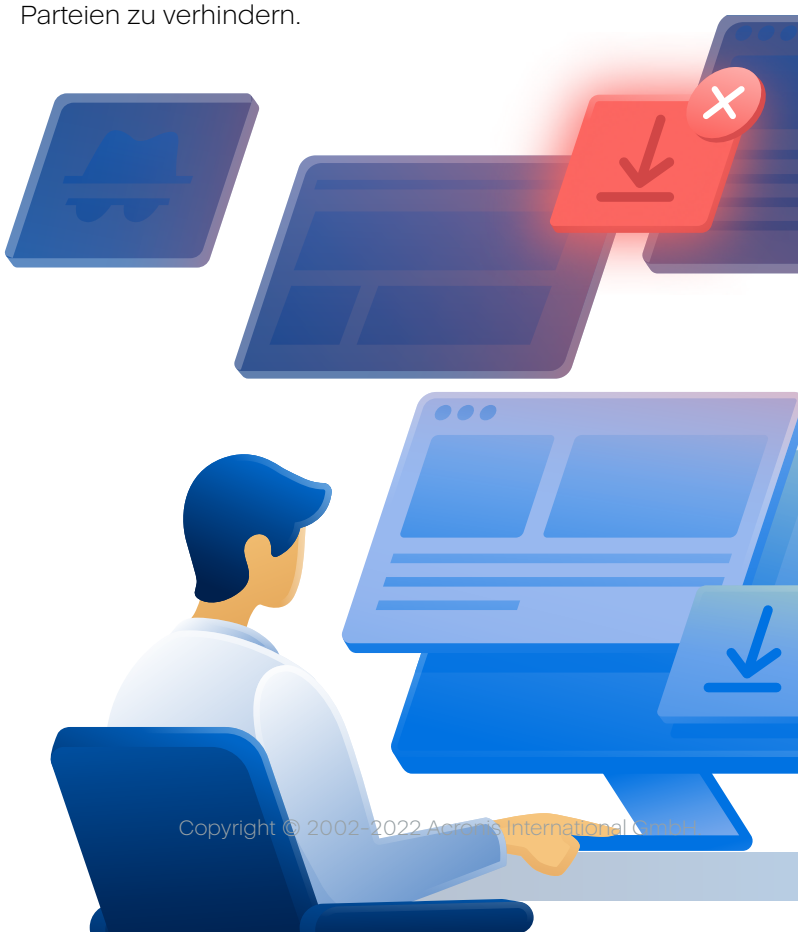
Was ist Data Loss Prevention (DLP)?

Data Loss Prevention ist eine bewährte Kategorie von Sicherheitslösungen, die mit integrierten Informationssicherheitstechnologien die nicht autorisierte Nutzung, Übertragung und Speicherung vertraulicher, sensibler Daten erkennen und verhindern.

DLP-Lösungen nutzen dafür eine Kombination aus Datenflusskontrollen sowie Inhaltsanalysen und implementieren unternehmensweite Richtlinien für die zulässige Datennutzung und -verarbeitung, die die Exfiltration sensibler Daten durch nicht autorisierte (interne und externe) Akteure verhindern.

Bei Data Protection geht es zwar hauptsächlich um Backup und Disaster Recovery, es gibt jedoch weitere wichtige Technologien wie DLP, Beglaubigung und Verschlüsselung, die sensible Informationen vor einer breiteren Palette von Bedrohungen – einschließlich Datenlecks – schützen.

DLP ist die einzige Technologie, die Transparenz und Kontrolle für sensible Daten bietet, die in einem Unternehmen übertragen und dort gespeichert werden, um ihre Weitergabe an nicht autorisierte Parteien zu verhindern.



Datenzustände und Schutzwirkung verschiedener funktionaler DLPs

Daten kommen in einem Unternehmen in einem der folgenden **drei Hauptzustände** vor:

- **Genutzte Daten:** Daten werden in lokalen Kanälen (z. B. Peripheriegeräte oder Wechselmedien) und Applikationen auf Endpunkt-Computern genutzt bzw. übertragen. Ein Beispiel für solche Daten sind Dateien, die von einem Endpunkt-Computer an ein USB-Laufwerk übertragen werden.
- **Übertragene Daten:** Hierbei handelt es sich um Daten, die zwischen Computer-Systemen verschoben oder übertragen werden. Dazu gehören Daten, die aus einem lokalen Datei-Storage in einen Cloud-Speicher übertragen werden, oder Daten, die von einem Endpunkt-Computer per Instant Messenger oder E-Mail an einen anderen Endpunkt übertragen werden.
- **Gespeicherte Daten:** Hierbei handelt es sich um Daten, die lokal oder in einem Netzwerk gespeichert sind und auf die gerade nicht zugegriffen wird bzw. die gerade nicht übertragen werden. Dazu gehören Daten, die in Netzwerkfreigaben oder lokalen Servern gespeichert sind.

Die meisten Daten ändern ihren Zustand häufig und regelmäßig. Einige Daten behalten ihren Zustand jedoch über den gesamten Lebenszyklus eines Endpunkts bei. Wenn Kunden die verschiedenen Zustände der Daten, ihre Besonderheiten und Unterschiede kennen, können sie sicherer mit ihren Unternehmensdaten umgehen und sie vor Kompromittierung schützen.

Es gibt drei grundlegende funktionsbezogene DLP-Typen, die jeweils für den Schutz eines Datenzustands zuständig sind:

- **DLP für genutzte Daten**
- **DLP für übertragene Daten**
- **DLP für gespeicherte Daten**

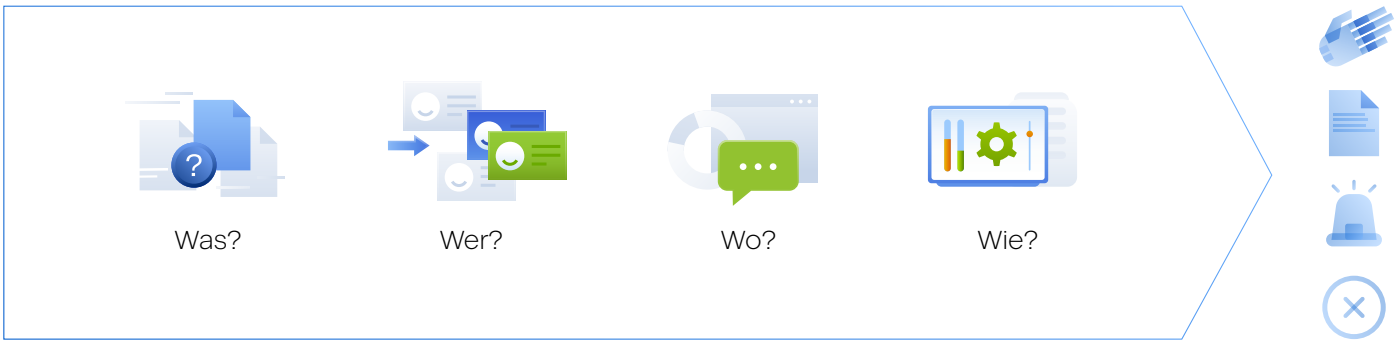
Es gibt zwar andere Technologien wie die Identitätsverwaltung oder die Verschlüsselung, die verschiedene Datenrisiken (z. B. Zugriff oder Datenschutz) mindern können. DLP kann die Daten als einzige Technologie jedoch über mehrere Zustände hinweg schützen, um Datenlecks zu verhindern und gleichzeitig transparente Einblicke in die Datenflüsse zu geben.

DLP-Kontrollen: Vergleich Inhalt – Kontext

Jeder Datenfluss in Unternehmen hat seinen eigenen Kontext und Inhalt. Der Kontext bezieht sich auf Umgebungsfaktoren wie die an einem Datenfluss beteiligten Benutzer, die verwendeten Kanäle, die Flussrichtung der Daten usw. Der Inhalt beschreibt den eigentlichen Typ bzw. die Kategorie der übertragenen Informationen, z. B. Patientendatensätze oder personenbezogene Daten von Mitarbeitern.

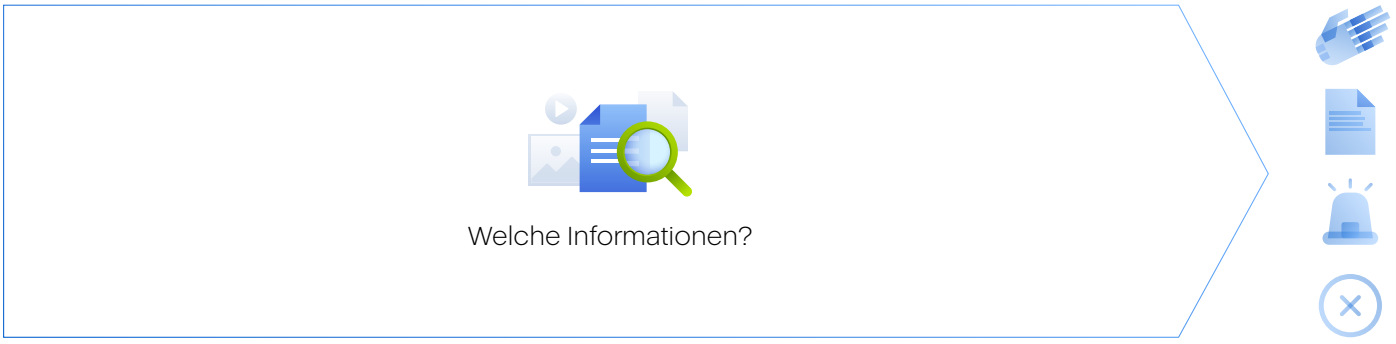
Effiziente DLP-Lösungen müssen Datenflusskontrollen basierend Kontext UND Inhalt implementieren:

- **Kontextbezogene DLP-Kontrollen:** Datenübertragungen werden anhand ihres Kontexts mithilfe von Attributen wie beteiligte Benutzer, verwendete Kanäle, Flussrichtung der übertragenen Daten, Ziel, Zeit usw. kontrolliert.



Beispiel: Richtlinien, die Kopiervorgänge von Daten (Was) durch Benutzer (Wer) auf verschlüsselte USB-Geräte (Wo) zulassen und Kopiervorgänge von Daten auf unverschlüsselte USB-Geräte blockieren.

- **Inhaltsbezogene DLP-Kontrollen:** Die tiefgehendere Kontrolle über die Datenflüsse basiert auf dem Typ und der Sensibilität der tatsächlich übertragenen Informationen (Inhalt).

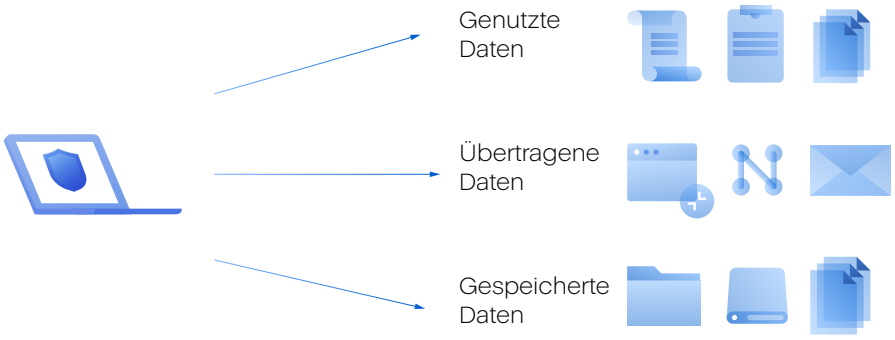


Beispiel: Dokumente mit HIPAA-bezogenen Informationen (welche Informationen) dürfen in keinem Fall auf USB-Geräte kopiert werden.

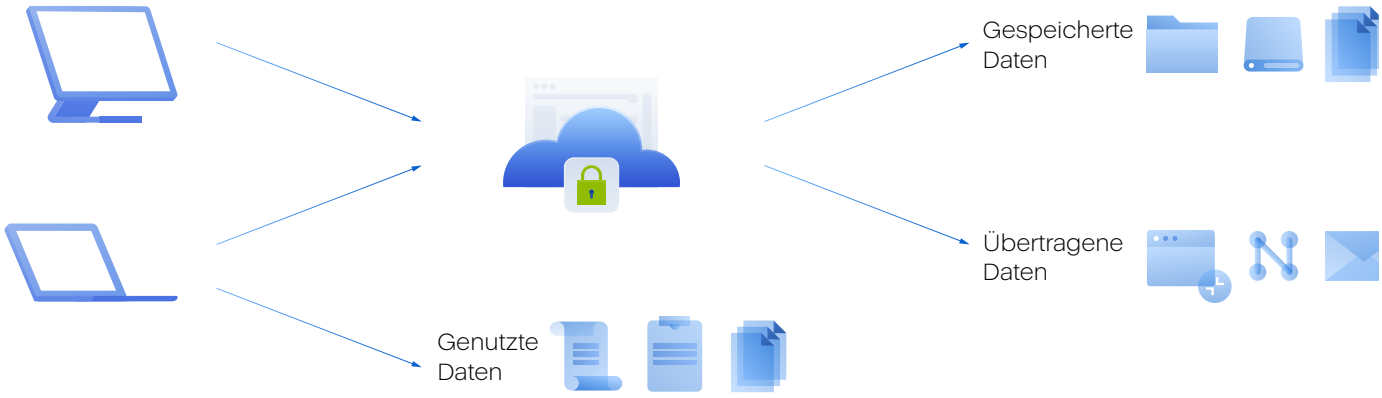
Typen von DLP-Architekturen

Je nach Bereitstellung und Umsetzung gibt es drei Haupttypen von DLPs:

- **Endpunkt-DLPs:** Lösungen, die DLP-Agenten auf Endpunkt-Computern einsetzen und den Verlust genutzter, übertragener und gespeicherter Daten von diesen Computern verhindern. Dabei spielt es keine Rolle, ob sie innerhalb des Firmennetzwerks oder im Internet verwendet werden.



- **Netzwerk-/Cloud-DLPs:** Lösungen, die nur netzwerkresidente Komponenten beinhalten (einschließlich Hardware, virtuelle DLP-Gateways, Server), übertragene oder gespeicherte Daten auf Computern im Firmennetzwerk schützen und Datenverluste an nicht autorisierte Empfänger und Ziele außerhalb des Firmennetzwerk verhindern.



- **Hybride DLPs:** Lösungen, die DLP-Komponenten im Netzwerk und auf Endpunkten nutzen, um alle Funktionen der DLP-Architekturen auf den Endpunkten und in den Netzwerken auszuführen.

Wichtig: Aufgrund ihrer Architektur können Netzwerk-DLPs keine genutzten Daten schützen und nur Datenverluste an nicht autorisierte Parteien außerhalb des Firmennetzwerks verhindern, während Endpunkt- und hybride DLPs Daten aller Zustände schützen und Datenverluste an interne sowie externe nicht autorisierte Parteien verhindern können.

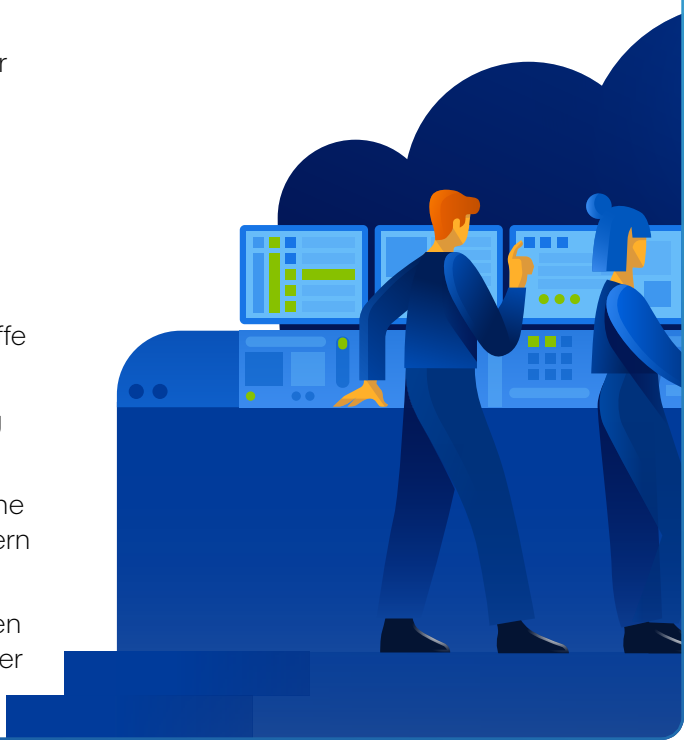
Für diesen Leitfaden konzentrieren wir uns auf das Starten, Ausführen und Skalieren eines DLP-Services auf der Basis der Endpunkt-DLP-Architektur.

Warum brauchen Kunden DLP?

Laut dem „Cost of Data Breach Report 2021“ des Ponemon Institute liegen die durchschnittlichen Gesamtkosten einer Datenschutzverletzung weltweit bei 4,24 Millionen US-Dollar. Das entspricht einer Steigerung von 10 % im Vergleich zu 2020. Doch nicht nur die Kosten durch Datenschutzverletzungen steigen: Die durchschnittliche Zeit für die Erkennung und Eindämmung einer Kompromittierung liegt inzwischen bei 287 Tagen. Das bedeutet, dass Ihre Kunden in der Zeit bis zur Eindämmung einer Kompromittierung einem erheblichen Risiko ausgesetzt sind – was schwerwiegende finanzielle Folgen und Auswirkungen auf die Reputation und die Compliance haben kann.

DLP-Services bieten Ihnen hauptsächlich folgende Möglichkeiten, um die Risiken für Ihre Kunden zu reduzieren:

- **Hilfe beim Erreichen der Compliance** in Bezug auf gesetzliche Bestimmungen und den Schutz regulierter Informationen, einschließlich personenbezogene Daten (GDPR, CCPA), Gesundheitsdaten (HIPAA), Zahlungskarteninformation (PCI-DSS) usw.
- **Schutz der Kundendaten**, insbesondere geistiges Eigentum und Geschäftsgeheimnisse
- **Risikominimierung** durch Verhinderung von Daten-exfiltration per Malware und Social-Engineering-Angriffe
- **Verbesserung der Sicherheit von Remote-Arbeit** und BYOD-Initiativen sowie Verhinderung der Übertragung sensibler Daten in privaten Cloud-basierten Storage
- **Verhinderung von Datenlecks**, die durch unabsichtliche Fehler, Fahrlässigkeit oder Fehlverhalten von Mitarbeitern verursacht werden
- **Schnelle Reaktion** auf Datenlecks und Untersuchungen nach erfolgreichen Kompromittierungen mit lückenloser Transparenz bei den DLP-Ereignissen



Ablauf der DLP-Servicebereitstellung

Bevor wir uns eingehender mit den Details zum Starten, Ausführen und Skalieren eines DLP-Services befassen, möchten wir darauf hinweisen, dass die Bereitstellung der DLP-Services aufgrund ihrer Besonderheiten einer speziellen Sequenz folgt. Sie beinhaltet die folgenden Schritte:

- **Bereitstellung des DLP-Agenten:** Die Entscheidung über die Endpunkte, auf denen mit DLP-Services zuverlässiger Schutz der Firmendaten gewährleistet werden soll, und die Bereitstellung der DLP-Agenten auf diesen Endpunkten gehören zu den ersten Schritten in Ihrem Service-Bereitstellungsprozess. Dabei wird empfohlen, für alle Workloads, auf denen sensible Daten erstellt, gespeichert oder genutzt werden, einen DLP-Agenten zu installieren. Wenn solche Workloads ungeschützt bleiben, können Lücken für Datenlecks im IT-Sicherheitssystem des Unternehmens entstehen.

- **Erstellung von DLP-Richtlinien:** Ein weiterer Schritt in der Anfangsphase ist die Erstellung von DLP-Richtlinien, die die korrekte Datennutzung sicherstellen, und von Richtlinien zur Datenverarbeitung, die Datenlecks verhindern. Dieser Schritt kann je nach verwendeter DLP-Technologie auch vor der Bereitstellung stehen. **Wichtiger Hinweis:** DLP-Richtlinien sind nicht allgemeingültig, sondern immer kundenspezifisch, weil jedes Unternehmen eigene interne Prozesse hat, andere gesetzliche Bestimmungen befolgen muss sowie individuelle Anforderungen an Datenzugriffe und an die Datenweitergabe hat. Aufgrund dieser Besonderheiten ist die Erstellung von DLP-Richtlinien bei herkömmlichen DLP-Lösungen, bei denen die Richtlinien manuell verwaltet werden müssen, äußerst komplex. Außerdem entsteht hoher Kostenaufwand für Service Provider, die damit DLP-Services erstellen möchten.
- **Validierung der DLP-Richtlinien:** Ein wichtiger Schritt nach der Erstellung der initialen DLP-Richtlinien ist ihre gemeinsame Validierung mit dem Kunden, um sicherzustellen, dass sie den geschäftlichen Anforderungen entsprechen. Schließlich kennen MSPs die geschäftlichen Besonderheiten nie so gut wie der Kunde selbst. Je komplexer und „technischer" die visuelle Darstellung der Richtlinie, desto mehr Zeit und Expertise erfordert ihre Validierung durch die Kunden.
- **Implementierung und Verwaltung von DLP-Richtlinien:** Nach ihrer Validierung mit dem Kunden können die DLP-Richtlinien implementiert werden, um sensible Unternehmensdaten vor Kompromittierung zu schützen. DLP-Technologien kontrollieren den Fluss der sensiblen Unternehmensdaten und blockieren nicht autorisierte Datenübertragungen. Unternehmen entwickeln sich jedoch ständig weiter, führen neue Prozesse ein und müssen auf neue Vorschriften und Änderungen bei den alten Bestimmungen achten. Deshalb müssen die initialen DLP-Richtlinien fortlaufend an sich ändernde Geschäftsanforderungen angepasst werden, damit keine neuen wichtigen Datenflüsse blockiert und alle Datenlecks verhindert werden. Dies kann durch manuelle Richtlinienoptimierung oder mit automatischen Methoden für adaptive Richtlinienanpassungen erfolgen.
- **Berichte zur Effektivität der DLP-Services:** Mit regelmäßigen Berichten zu blockierten Datenübertragungen und DLP-Maßnahmen bei Endbenutzeraktionen können Sie die Effektivität der DLP-Services demonstrieren. Damit verbessern Sie die Kundenbindung und zeigen Kunden, die sich ihrer Datenleckprobleme nicht bewusst sind, wie gut die Risikominderung funktioniert.

Herausforderungen für MSPs bei aktuellen DLP-Lösungen

DLP ist ein ausgereifter, auf Großfirmenkunden orientierter Markt mit etablierten Playern. Der breitere Markt (z. B. Service Provider und ihre KMU-Kunden) konnte ihn bisher nicht erschließen. Der Grund: DLP-Anbieter müssen sich kontinuierlich und eingehend mit den Spezifika des jeweiligen Unternehmens vertraut machen und diese den entsprechenden DLP-Kontrollen zuordnen. Außerdem müssen sie die relevanten gesetzlichen Vorschriften und die Anforderungen an die Daten-Compliance kennen. Das hat dazu geführt, dass sich die DLP-Branche bisher hauptsächlich auf große Unternehmen konzentriert, die sich das teure interne Know-how für die DLP-Verwaltung leisten können.

Die größten Herausforderungen für MSPs bei der Implementierung und beim Betrieb eines DLP-Services:

- **Der Betrieb eines DLP-Services ist kostenintensiv und komplex:** Da herkömmliche DLP-Lösungen für die Erstellung der initialen Richtlinien und ihre nachfolgende Anpassung komplexe manuelle Prozesse erfordern, ist der Service aufgrund des Zeit- und Arbeitsaufwands für die Implementierung einer effektiven DLP-Lösung für mehrere Kunden zu kostspielig. Zudem müssen für diese komplexe Aufgabe DLP-Experten eingestellt werden – und diese sind noch viel schwerer zu finden und teurer als allgemeine IT-Sicherheitsspezialisten.

- **Eine effiziente DLP-Lösung erfordert kundenspezifische Richtlinien:** Wie bereits erwähnt, sind die Geschäftsprozesse und sensiblen Daten jedes Unternehmens einzigartig und veränderlich, sodass die DLP-Richtlinien ständig an die geschäftlichen Besonderheiten angepasst werden müssen. MSPs fehlt jedoch das detaillierte Verständnis für die Geschäftsprozesse der einzelnen Kunden und sie können es sich auch nicht aneignen und auf dem neuesten Stand halten. Dies stellt ein erhebliches Skalierungsproblem für MSPs dar, die herkömmliche DLP-Technologien einsetzen.
- **Falsch konfigurierte DLP-Richtlinien können geschäftliche Abläufe stören:** Einerseits ist die manuelle Erstellung und Konfiguration von DLP-Richtlinien aufgrund ihrer Komplexität und Granularität sehr fehleranfällig. Gleichzeitig blockieren DLP-Technologien alle nicht autorisierten Datenflüsse. Die Kombination beider Faktoren kann dazu führen, dass wichtige Geschäftsprozesse gestört werden, wenn versehentlich für das Unternehmen notwendige Datenflüsse blockiert, DLP-Richtlinien falsch konfiguriert oder neue Geschäftsprozesse nicht umgehend von diesen Richtlinien abgedeckt werden.
- **Mitarbeiter sind die schwächsten Glieder beim Kunden:** Auch wenn MSPs und ihre Kunden kaum Zugriff auf DLP-Technologien haben, sind menschliche Fehler und externe Angriffe auf Mitarbeiter die häufigsten Ursachen für Datenlecks. Selbst wenn Service Provider in der Lage sind, das Risiko externer Bedrohungen durch andere Endpunktschutz-Technologien zu minimieren, werden am Ende sie verantwortlich gemacht, wenn Benutzer unabsichtlich sensible Daten weitergeben und damit eine Datenschutzverletzung verursachen.
- **Kunden sind sich des Datenleckproblems unter Umständen gar nicht bewusst:** Aufgrund des bisher schwierigen Zugangs zu DLP-Lösungen sind Kunden sich möglicherweise nicht bewusst, das Datenlecks für Unternehmen jeder Größe ein erhebliches Problem darstellen. Wenn MSPs einen DLP-Service anbieten, müssen sie ihre Kunden auf bestehende Datenleckrisiken sowie darauf hinweisen, dass sich diese Gefahren nur mithilfe von DLP eindämmen lassen.

Mit neuen Trends und Technologien wie der automatischen, verhaltensbasierten Erstellung, Erweiterung und Überwachung von Richtlinien können die sich schnell ändernden DLP-Regeln berücksichtigt werden, um neben den gesetzlichen Vorschriften auch den dynamischen Geschäftsabläufen Rechnung zu tragen. Diese neuen Möglichkeiten demokratisieren den DLP-Markt effektiv und öffnen ihn für die Service Provider und ihre Kunden. Jetzt ist ein hervorragender Zeitpunkt, über die Erweiterung Ihres Portfolios mit DLP-Services nachzudenken.

Planung und Einführung eines DLP-Services

Bei der Planung und Einführung eines DLP-Services müssen Sie zunächst prüfen, ob Ihre Kunden überhaupt eine DLP-Lösung benötigen.

Kunden benötigen einen DLP-Service, um ihr Datenverlustrisiko zu minimieren, wenn einige oder alle der folgenden Bedingungen erfüllt sind:

- Sie erstellen, speichern oder verarbeiten auf ihren Workloads sensible Daten, die gesetzlichen Vorschriften unterliegen.
- Sie haben Geschäftsgeheimnisse oder geistiges Eigentum, die vor Verlusten geschützt werden müssen.
- Sie agieren in stark regulierten Branchen.
- Sie haben bereits eine Datenschutzverletzung erlitten und möchten ihre Umgebung sichern sowie Risiken mindern.
- Sie haben bzw. benötigen Compliance-Zertifizierungen.
- Sie haben oder möchten eventuell eine Cyberversicherung abschließen, um ihre Haftung zu begrenzen.
- Sie haben zu wenig Sicherheitspersonal und -expertise.

Außerdem haben Kunden in den folgenden Branchen in der Vergangenheit ein größeres Interesse an DLP gezeigt:

- Banken und Finanzdienstleister
- Gesundheitswesen
- Rechtsbranche
- IT- und Telekommunikation
- Behörden und öffentlicher Sektor
- Fertigungsindustrie
- Einzelhandel und Logistik
- Bildungseinrichtungen
- Energieversorgung

Wenn Sie Kunden haben, die diese Bedingungen erfüllen oder in den genannten Branchen arbeiten, sollten Sie jetzt überlegen, ob Sie DLP-Lösungen in Ihr Service-Portfolio aufnehmen, um die schnell wachsende Nachfrage nach minimierten Datenverlustrisiken und einfacherer Einhaltung von Vorschriften zu erfüllen.

Planung der Services und Kostenschätzung

Der Preis Ihres Services setzt sich aus drei Hauptfaktoren zusammen: Arbeitskosten, Produktkosten und gewünschte Marge. Sie wirken sich jeweils wie folgt auf Ihr Preisangebot aus:

- **Arbeitskosten:** Die Komplexität der gewählten Lösung entscheidet über den Zeitaufwand Ihrer Service-Techniker für die Bereitstellung und Verwaltung des Services sowie über die erforderliche IT-Sicherheitsexpertise.
- **Produktkosten:** DLP-Lösungen, die bisher nur von größeren Unternehmen genutzt wurden, verursachen hohe Kosten und sind daher für kleine und mittlere Unternehmen unerschwinglich. Wenn es sich bei Ihren Kunden hauptsächlich um KMUs handelt, benötigen Sie eine kostengünstige Lösung.
- **Gewünschte Marge:** MSPs erwirtschaften Brutto-Margen von 50 % bei remote bereitgestellten Services, die im Rahmen eines Modells mit wiederholten Umsätzen verkauft werden.

Umsetzung eines DLP-Services mit dem Acronis Advanced DLP Paket

Acronis bietet eine verhaltensbasierte DLP-Lösung an, die kundenspezifische Richtlinien automatisch erstellt und sie kontinuierlich pflegt, ohne dass Monate für die Bereitstellung vergehen, ganze Teams für die Pflege benötigt werden oder ein Doktortitel in Datenschutzrecht benötigt wird, um die Problematik zu verstehen.

Mit dem Acronis Advanced DLP Paket können Sie Ihren Kunden eine umfassende DLP-Lösung für übertragene und genutzte Daten mit einer bisher nicht gekannten Einfachheit und folgenden Vorteilen bieten:

- **Neue Chancen für höhere Rentabilität:** Erweitern Sie Ihr Portfolio, um mehr Kunden zu gewinnen, und steigern Sie Ihren Umsatz pro Kunde mit DLP-Services, die bisher nur großen Unternehmen vorbehalten waren.
- **Minimierter Arbeitsaufwand:** Erweitern Sie Ihr Angebot mit DLP, ohne dass die Komplexität, Kosten und Mitarbeiterzahl für Ihre Verwaltung steigen.
- **Weniger Sicherheitsrisiken für Kunden:** Verhindern Sie den Verlust sensibler Daten.
- **Zuverlässige Einhaltung von Vorschriften beim Kunden:** Sofort einsatzbereite Daten-klassifizierungsvorlagen für Vorschriften wie GDPR, HIPAA und PCI-DSS.
- **Einfachere Bereitstellung und Verwaltung der Services:** Automatisieren Sie die Bereitstellung der DLP-Services, die Konfiguration der initialen Richtlinien und ihre Anpassung im laufenden Betrieb.
- **Kundenspezifische DLP-Richtlinien für jede Größe:** Passen Sie DLP-Richtlinien mit einer verhaltensbasierten Technologie automatisch an sich ändernde Spezifika des Unternehmens an. Dadurch wird auch die Validierung der Richtlinien mit dem Kunden vor ihrer Implementierung vereinfacht.
- **Schnellere Reaktion auf DLP-Ereignisse:** Vereinfachen Sie den Betrieb der DLP-Services, die Pflege der Richtlinien, IT-Sicherheitsaudits und die Untersuchung von Vorfällen durch zentralisierte, richtlinienbasierte Auditprotokolle und Sicherheitswarnungen.

Acronis Advanced DLP Paket

Mit dem Advanced DLP-Paket 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 erhalten Sie unter www.acronis.com