Der praktische Leitfaden für Geschäftsführer zum Verhindern von Datenverlust

Implementieren eines Datensicherheits-programms in 5 Phasen

Forcepoint

Whitepaper

Inhaltsverzeichnis

Das Problem

Auf dem Markt herrscht große Verwirrung hinsichtlich der Kontrolle zur Verhinderung von Datenverlust (Data Loss Prevention, DLP). Es gibt zahlreiche Faktoren, die hierzu beitragen. Unter Anbietern scheint ein allgemeines Verständnis darüber zu fehlen, wie Datensicherheit funktioniert und woran sich Risiken für ein Unternehmen erkennen lassen. In der Vergangenheit wurden vollkommen unpraktische Prozesse entworfen, die zu operativen Engpässen führten. Gleichzeitig wurde das Risiko eines Datenverlusts oder Datenraubs kein Stück reduziert. Schlechte Erfahrungen eines Unternehmens können unmittelbar mit unklaren Programmzielen, unzureichender Planung und mangelhafter Umsetzung zusammenhängen.

Daher sind Unternehmen, die unter Einhaltung der Gesetze und Vorschriften ihre vertraulichen Daten schützen, den sicheren Zugriff gewährleisten und ihre Mitarbeiter in einer zunehmend hybriden Arbeitsumgebung schützen möchten, häufig skeptisch und unsicher und wissen nicht, an wen sie sich wenden sollen. Einige haben sich an erfolglosen Implementierungen bereits die Finger verbrannt.

Die wichtigste Erkenntnis ist: Nicht die Technologie hinter DLP-Kontrollen ist der kritischste Faktor, der letztlich über Erfolg oder Misserfolg bestimmt – für Ihren Erfolg ist vielmehr die von Ihrem Anbieter gewählte Methodik und die entsprechende Umsetzungsstrategie entscheidend.

Dieses Whitepaper soll Leitlinien und Klarheit bieten.

- → Es erläutert die Herausforderungen beim Schutz der Mitarbeiter in einer hybriden Arbeitsumgebung und den Kontext, warum die Datensicherheit in Programmen für den Zugriffsschutz eine zentrale Rolle spielen sollte.
- → Es erklärt wichtige Unterscheidungsmerkmale und bietet Anhaltspunkte zur Beurteilung eines potenziellen Anbieters.
- → Es liefert nützliche Einblicke in Trends bei Datenschutzverletzungen.
- → Es erläutert einen einfachen fünfstufigen Prozess zur Implementierung und Umsetzung einer Datenschutzstrategie auf praktische, messbare und risikogerechte Weise.
- → Schließlich stellt es zahlreiche praxistaugliche Best Practices vor, mit denen häufige Stolperfallen vermieden und ein Großteil der operativen Herausforderungen bei der DLP-Implementierung gemeistert werden können.

„Nicht die Technologie hinter DLP-Kontrollen ist der kritischste Faktor, der letztlich über Erfolg oder Misserfolg bestimmt – für Ihren Erfolg ist vielmehr die von Ihrem Anbieter gewählte Methodik und die entsprechende Umsetzungsstrategie entscheidend.“

Ausgangspunkt

Alle DLP-Kontrollen sollten die ersten beiden Ziele der folgenden Liste erfüllen.

1. Sie bieten die Möglichkeit zur Identifizierung von Daten.

- → **Daten während der Übertragung** (die durch das Netzwerk gesendet werden)
- → **Genutzte Daten** (die gerade am Endpunkt verwendet werden)
- → **Ruhende Daten** (die ungenutzt an einem Speicherort vorgehalten werden)
- → **Daten in der Cloud** (während der Nutzung, Übertragung oder im Speicher)

2. Sie identifizieren Daten als beschrieben oder registriert.

- → **Beschrieben:** Standardmäßig bereitgestellte Kennungen und Richtlinienvorlagen helfen, Arten von Daten zu identifizieren. Dies ist hilfreich, wenn Sie nach Inhalten, z. B. nach personenbezogenen Daten suchen.
- → **Registriert:** Daten werden vom System registriert, um einen „Fingerabdruck" zu erstellen, der einen vollständigen oder partiellen Abgleich bestimmter Informationen ermöglicht, beispielsweise für geistiges Eigentum.

Eine fortschrittlichere DLP-Lösung zeichnet sich zudem durch eine dritte Funktion aus.

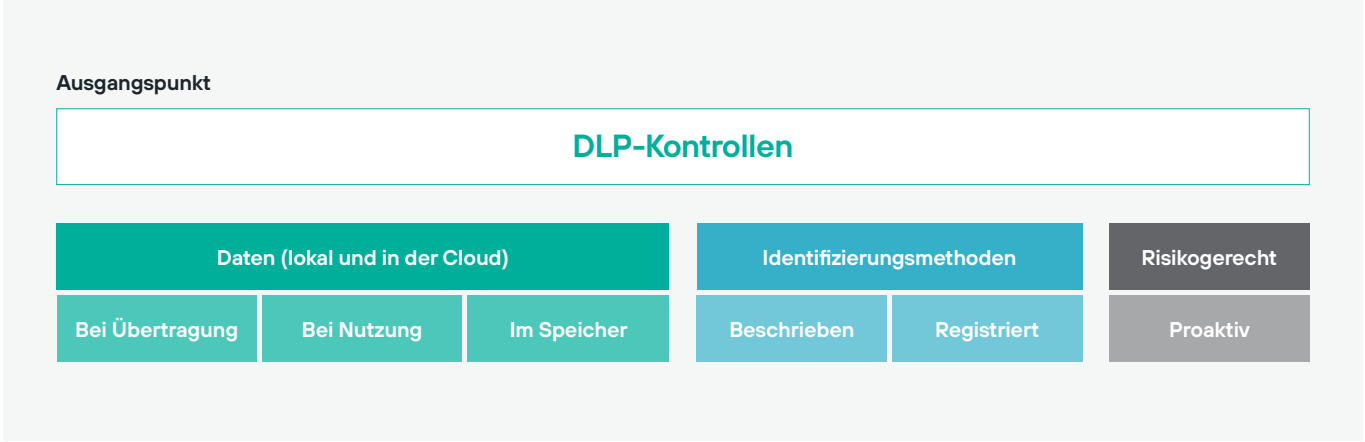
3. Sie verfolgen einen risikogerechten Ansatz für DLP.

- → Ein risikogerechter Ansatz macht bei fortschrittlichen Lösungen zur Verhinderung von Datenverlust den Unterschied gegenüber herkömmlichen DLP-Tools aus. Risikogerechte DLP, die vom CARTA-Ansatz (Continuous Adaptive Risk and Trust Assessments) von Gartner abgeleitet ist, erhöht die Flexibilität und die Wirksamkeit von DLP. Dabei wird die DLP-Richtlinie autonom angepasst und durchgesetzt, basierend auf dem Risiko, das eine Person für ein Unternehmen zu einem beliebigen Zeitpunkt darstellt. Mittels Echtzeit-Durchsetzung können Sicherheitsverstöße vorhergesehen und verhindert werden, bevor sie auftreten. Die Produktivität steigt, weil Benutzer weniger durch lästige Sicherheitsmaßnahmen ausgebremst werden. Gleichzeitig werden IT-Untersuchungen durch Reduzierung von Fehlalarmen und Vorfalls-Risikoranking erleichtert.

Zur Veranschaulichung, wie die ersten beiden allgemeinen Funktionen arbeiten, wird ein DLP-System angewiesen:

- → Was gesucht werden soll (z. B. Kreditkartennummern)
- → Welche Methode für die Identifizierung der Informationen verwendet werden soll (beschrieben/registriert)
- → Wo gesucht werden soll (z. B. Netzwerk, Endpoint, Speicher, Cloud)

Was passiert, nachdem das DLP-System die Informationen identifiziert hat, ist abhängig a) von der Risikotoleranz des Dateneigentümers, b) von den verfügbaren Reaktionsoptionen im Falle eines Datenverlusts und c) davon, ob die Lösung risikogerecht arbeitet.



Von der Vision zur Implementierung

Alle DLP-Systeme bieten einen ähnlichen Funktionsumfang, es ist jedoch wichtig zu verstehen, dass nicht alle Anbieter dieselbe Vision haben, wie DLP Ihnen helfen soll, das Problem eines Datenverlusts in den Griff zu bekommen. Daher sollte Ihr erster Schritt darin liegen, die Methodik und die Umsetzungsstrategie jedes Anbieters, den Sie in Erwägung ziehen, zu verstehen.

Wenn Sie einen Anbieter fragen: „Welche Methodik wenden Sie an?", fragen Sie in Wirklichkeit: „Welche Vision haben Sie, wie dieses Tool einen drohenden Datenverlusts verhindern wird?".

Dies ist eine wichtige, aber nur selten gestellte Frage. Die Antwort erlaubt Ihnen, die Vision eines Anbieters zu verstehen, was Sie wiederum in die Lage versetzt, dessen individuelle Fähigkeiten einzuschätzen und künftige Entwicklungen abzusehen. Für Entscheidungsträger gilt: Das Wissen, warum Anbieter das tun was sie tun, hat einen sehr viel stärkeren Einfluss auf Ihren Erfolg und ihre langfristige Zufriedenheit als das Wissen, was genau getan wird.

Die verwendete Methodik eines Anbieters hat einen starken Einfluss auf dessen Umsetzungs- bzw. Implementierungsstrategie. Wenn die Methodik eines Anbieters beispielsweise mit der Beurteilung ruhender Daten beginnt, während ein anderer Anbieter mithilfe risikogerechter Kontrollen zunächst auf Daten während der Übertragung eingeht, so verfolgen die beiden eine sehr unterschiedliche Umsetzungsstrategie. Wie ein Anbieter DLP-Kontrollen umsetzt, ist wichtig, weil es auf Ihre Gesamtbetriebskosten (TCO) und auch Ihre erwartete Amortisierungsdauer Auswirkungen hat. Beides sind Faktoren, die für eine korrekte Kaufentscheidung und die Etablierung angemessener Erwartungen unter allen Beteiligten von zentraler Bedeutung sind.

Wichtig zu beachten ist: Sie sollten vermeiden, die Methodik eines Anbieters auf die Technologie eines anderen anzuwenden. Die Methodik definiert und steuert die Technologieentwicklung eines Anbieters. Wenn Sie die beiden Aspekte vermischen, laufen Sie Gefahr, in eine Technologie zu investieren, die Ihre langfristigen Anforderungen nicht erfüllen wird.

Messbare und praktische DLP

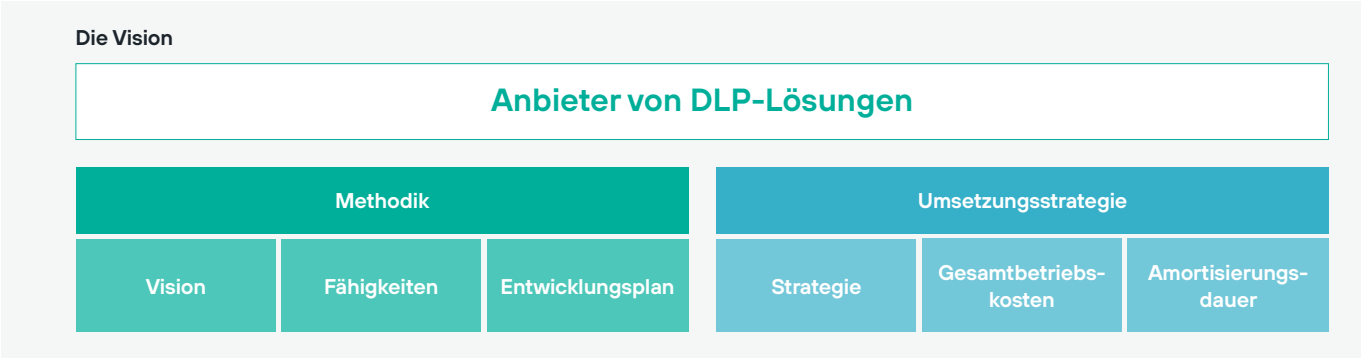
Wenn Sie an einer Konferenz teilgenommen oder eine Studie über Best Practices im Bereich DLP gelesen haben, sind Sie wahrscheinlich mit der Metapher „versuchen Sie nicht, den Ozean zum Kochen zu bringen" vertraut. Diese Redewendung bedeutet, dass es nicht möglich ist, ein vollständiges DLP-Programm auf einen Streich umzusetzen. Der Hinweis ist nicht besonders zweckdienlich, da er Ihnen nicht dabei hilft herauszufinden, was genau Sie tun sollten – und wann. In mancherlei Hinsicht klingt „versuchen Sie nicht, den Ozean zum Kochen zu bringen" eher nach einer Warnung als nach einer Handlungsanweisung.

Leider sind viele der veröffentlichten „Best Practices" nicht immer besonders pragmatisch ausgerichtet. Fehlende (finanzielle oder sonstige) Ressourcen und andere unternehmensinterne Schwierigkeiten führen häufig dazu, dass Best Practices nicht befolgt werden – und somit nutzlos bleiben. Ebenso sind viele Richtlinien zu extrem: Daten sollten zwar sicher, aber gleichzeitig auch zugänglich sein. Zu stark eingreifende, unflexible Richtlinien können die Produktivität behindern und für das Unternehmen nachteilig sein. Wesentlich mehr Nutzen bieten praxisorientierte Best Practices. Diese berücksichtigen Kosten, Nutzen und Aufwand für ihre Befolgung und lassen sich messen, um zu ermitteln, ob Sie und Ihre Organisation diese umsetzen können bzw. sollten.

Damit Ihr DLP-System das Risiko eines Datenverlusts messbar und praktisch verwalten und vermindern kann, müssen Sie zwei grundlegende Tatsachen kennen und verstehen:

1. Um eine Messung zu ermöglichen, müssen Sie die Risikoformel für Datenverlust kennen und anwenden. Die Risikoformel für Datenverlust ist zwar anderen Risikomodellen ähnlich, zeichnet sich jedoch durch einen wesentlichen Unterschied aus, den wir weiter unten erläutern werden.

2. Um pragmatisch vorgehen zu können, müssen Sie verstehen, wo bei Ihnen mit höchster Wahrscheinlichkeit eine Datenschutzverletzung mit erheblichen Auswirkungen eintreten könnte. Wenden Sie dann die 80-20-Regel an, um Ihre Aufmerksamkeit und ihre Ressourcen genau hierauf zu konzentrieren.



Die Risikoformel für Datenverlust

Die grundlegende Risikoformel, mit der die meisten von uns vertraut sind, lautet:

Risiko = Auswirkungen × Wahrscheinlichkeit

Die Herausforderung bei den meisten Risikomodellen liegt darin, die Wahrscheinlichkeit, mit der eine bestimmte Bedrohung eintreten wird, zu ermitteln. Diese Wahrscheinlichkeit ist von zentraler Bedeutung, wenn Sie bestimmen wollen, ob Sie Geld für eine Lösung zur Abwehr der Bedrohung ausgeben oder sich die Investition lieber ersparen und das Risiko auf sich nehmen möchten.

Der Unterschied bei der Risikoformel für Datenverlust liegt darin, dass eben diese Wahrscheinlichkeit keine Unbekannte darstellt. Sie erkennt an, dass Datenverlust unvermeidlich und meist unbeabsichtigt ist. Vor allem aber können Sie mithilfe der Risikoformel Risiken messen und auf ein Niveau eindämmen, mit dem sich Ihr Unternehmen wohl fühlt.

Daher wird als Kennzahl für die Verfolgung der Reduzierung des Datenrisikos und die Messung der Investitionsrendite auf DLP-Systeme die Eintrittshäufigkeit verwendet.

Risiko = Auswirkungen × Eintrittshäufigkeit

Die Eintrittshäufigkeit gibt an, wie oft innerhalb eines bestimmten Zeitraums Daten auf eine Weise verwendet oder übertragen werden, die sie dem Risiko eines Verlusts, eines Diebstahls oder einer Gefährdung aussetzen. Die Eintrittshäufigkeit wird vor und nach Umsetzung der DLP-Kontrollen gemessen, um aufzeigen zu können, wie stark das Risiko durch die jeweiligen Maßnahmen reduziert wurde.

Wenn Sie beispielsweise mit einer Eintrittshäufigkeit von 100 Vorfällen über einen Zeitraum von zwei Wochen beginnen und in der Lage sind, diesen Wert durch die Implementierung von DLP-Kontrollen auf 50 Vorfälle innerhalb von zwei Wochen zu reduzieren, haben Sie die Wahrscheinlichkeit eines Datenverlustereignisses (einer Datenschutzverletzung) um 50 % reduziert.

Risikogerechte Lösungen sind besonders wirksam, wenn es darum geht, die Eintrittshäufigkeit zu minimieren, denn sie können echte Datenrisiken im Kontext der allgemeinen Interaktionen eines Benutzers weitaus genauer erkennen. Dadurch können Fehlalarme erheblich reduziert werden. Diese Lösungen bieten somit einen Vorteil gegenüber herkömmlichen DLP-Lösungen, weil sie das Risiko nicht nur minimieren, sondern auch genauer abbilden.

Die 80-20-Regel für DLP

Neben der Ermittlung der Eintrittshäufigkeit ist es wichtig, zu bestimmen, wo innerhalb Ihrer Organisation eine Datenschutzverletzung mit starken Auswirkungen mit der höchsten Wahrscheinlichkeit eintreten könnte. Hierfür müssen Sie die jüngsten Trends bei Datenschutzverletzungen untersuchen und dann die 80-20-Regel anwenden, um zu bestimmen, wo Sie mit Ihren DLP-Aktivitäten beginnen sollten. Dank einer aktuellen Studie sind diese Informationen problemlos verfügbar.

Laut einer Studie des Ponemon Institute aus dem Jahr 2021 sind unrechtmäßig verwendete Anmeldedaten der häufigste erste Angriffsvektor und für 20 % der Datenschutzverletzungen verantwortlich, gefolgt von Phishing mit 17 %.[1]

Für ein wirklich effektives Programm zum Schutz vor Datenverlust müssen Sie sich sicher sein, dass Sie erkennen, wenn Daten über das Web, per E-Mail, über die Cloud oder Wechselmedien bewegt werden, und dass Sie darauf reagieren können.

Hier kann eine risikogerechte DLP-Lösung einen Vorteil bieten. Herkömmliche DLP-Lösungen haben oft Schwierigkeiten, Elemente wie unterbrochene Geschäftsprozesse oder regelwidrige Aktivitäten zu identifizieren, die beide zu erheblichem Datenverlust führen können. Eine risikogerechte DLP-Lösung versteht das Verhalten einzelner Benutzer und vergleicht sie mit beobachteten Ausgangswerten, um die DLP-Kontrollen schnell und autonom zu verschärfen, sobald Aktivitäten nicht zum Aufgabenbereich oder normalen Verhalten des Endbenutzers passen. Dieser progressive Ansatz kann das Risiko eines versehentlichen Verlusts von Daten und ihrer Preisgabe verringern.

[1] Report „Cost of a Data Breach", 2021, erstellt vom Ponemon Institute im Auftrag von IBM.

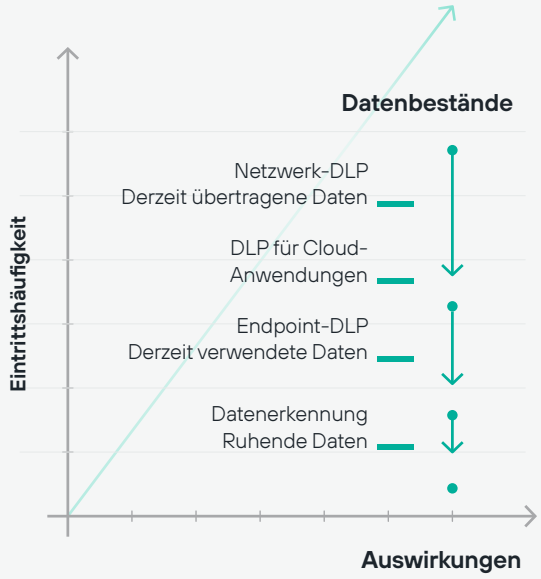
Die DLP-Methodik und Umsetzungsstrategie von Forcepoint

Die Berücksichtigung der neuesten Trends bei Datenschutzverletzungen und die Befolgung der Risikoformel für Datenverlust sind die ersten Schritte zur Entwicklung einer Strategie zur Vermeidung von Datenverlust. Die effektivste DLP-Methodik konzentriert sich auf das Verstehen der Benutzerabsicht, um so Datenverlust zu vermeiden, bevor er auftritt. Die Umsetzung sollte sich darauf konzentrieren, die kürzeste Amortisierungsdauer für den Nachweis einer messbaren Risikominderung zu liefern.

Amortisierungsdauer

Die Amortisierungsdauer ist der Zeitraum zwischen der Implementierung von DLP-Kontrollen und der Erzielung messbarer Ergebnisse bei der Reduzierung von Risiken. Der Benutzer ist der größte Datenrisiko-Faktor, ob unwissentlich oder mutwillig durch einen internen Insider oder als Ziel externer Angriffsvektoren. Daher erzielen Sie die beste Amortisierungsdauer mit einer DLP-Lösung, die sich mithilfe risikogerechter Technologie im Hintergrund auf Daten während der Übertragung und im Speicher konzentriert.

Möglicherweise wundern Sie sich jetzt, weil Ihnen andere Anbieter oder Experten erklärt haben, Sie sollten Ihre DLP-Kontrollen zunächst einmal auf ruhende Daten fokussieren. So bekommt man häufig zu hören: „Wenn man nicht weiß, was man hat und wo es sich befindet, kann man es auch nicht schützen." Aber das ist nicht wahr, denn in der Tat sind DLP-Systeme genau dafür konzipiert. Entweder verstehen die anderen Anbieter und Experten nicht, wie Risiken korrekt zu beurteilen und in den Griff zu bekommen sind, oder sie wiederholen lediglich das, was sie von anderen zu hören bekommen, weil es für sie selbst gut zu funktionieren scheint.



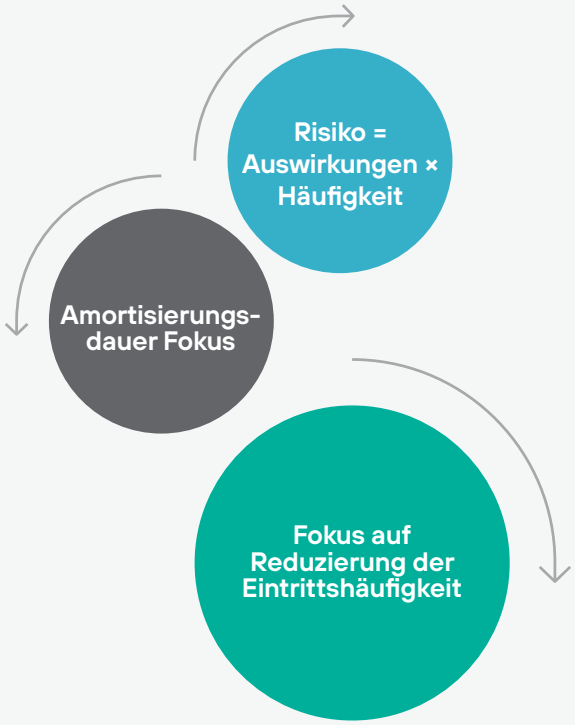


Abbildung 1. Die DLP-Methodik und Umsetzungsstrategie von Forcepoint

Warum sollten Sie die Empfehlung, mit ruhenden Daten zu beginnen, hinterfragen? Denken Sie über folgende Aspekte nach:

1. Kennen Sie irgendeine Organisation, die erfolgreich sämtliche vertraulichen Daten identifiziert und abgesichert hat, insbesondere durch eine beschleunigte Cloud-Einführung?
2. Haben Sie irgendeine Vorstellung, wie lange es dauern wird, sämtliche Dateien mit vertraulichen Informationen zu durchsuchen, zu identifizieren und abzusichern?
3. Wissen Sie, wie stark sich hierdurch Ihr Risiko reduziert?

Das Problem mit einer anfänglichen Fokussierung auf ruhende Daten liegt darin, dass der Schwerpunkt auf implizitem Risiko und nicht auf dem tatsächlichen Risiko liegt. Daher lassen sich Ergebnisse hinsichtlich einer Reduzierung des Risikos nicht messen. Implizites Risiko bedeutet, dass andere Bedingungen erfüllt sein müssen, bevor eine negative Konsequenz eintreten kann. Im Zusammenhang mit Datenverlust handelt es sich bei diesen Bedingungen um folgende Punkte:

- → Jemand oder etwas mit böswilliger Absicht muss sich in Ihrem Netzwerk befinden oder auf Ihre Cloud-Umgebungen zugreifen.
- → Die potenziellen Täter müssen nach Ihren vertraulichen Daten suchen.
- → Sie müssen diese finden.
- → Sie müssen diese verschieben.

Dies trifft auf jede Organisation zu und führt uns zu der sehr viel wichtigeren Frage: „Wie zuversichtlich sind Sie, dass Ihre Organisation erkennt, ob Daten verschoben werden, und angemessen hierauf reagieren kann?"

Es gibt drei Kanäle, auf denen Datenverlust erfolgt, und genau dort finden Sie auch tatsächliche Risiken, auf die Sie reagieren können:

- → Netzwerk (z. B. E-Mail, Web, Remote-Zugriffspunkte, FTP)
- → Endpunkt (z. B. USB-Speicher, Drucker)
- → Cloud (z. B. Office 365, Box)

Was ist mit ruhenden Daten und Compliance-Themen?

Zur Einhaltung zahlreicher Vorschriften müssen Sie Ihre Datenspeicher auf ungeschützte ruhende Daten durchsuchen. Daher fragen Sie sich möglicherweise, warum eine DLP-Methodik und Umsetzungsstrategie nicht dort ansetzt. Tatsache ist: Prüfer achten im Rahmen einer Revision mehr darauf, ob Sie Vorschriften derzeit einhalten, als darauf, ob Sie sämtliche Vorgaben in der Vergangenheit beachtet haben.

Eine Durchsuchung Ihrer ruhenden Daten ist also für Compliance-Zwecke wichtig, jedoch nicht das Hauptziel Ihrer DLP-Policies und somit auch nicht der Bereich, in dem diese den größten Wert liefern. Planen Sie daher ruhig, DLP zur Datenerkennung und für Compliance-Zwecke zu nutzen, jedoch auf eine Art, die für Ihre Organisation praktisch und nachhaltig ist.

Erstellen Sie Richtlinien für die vertretbare Löschung (Löschen von Dateien, die nicht mehr benötigt werden), um Risiken zu reduzieren, und für die langfristige Aufbewahrung, sofern gesetzlich vorgeschrieben. Der beste Ausgangspunkt ist der Einsatz von DLP zur automatischen Quarantäne von Dateien, auf die seit mindestens sechs Monaten nicht mehr zugegriffen wurde. Weisen Sie Ihren Rechts- und Compliance-Teams Berechtigungen zu, mit denen sie Entscheidungen auf Grundlage von Datenaufbewahrungsrichtlinien treffen können.

Die Fünf Phasen zum DLP-Erfolg

Die folgenden fünf Phasen umfassen einen Prozess für die Implementierung von DLP-Kontrollen, den Ihr Unternehmen praktisch umsetzen kann, um messbare Ergebnisse zu erzielen. Unabhängig davon, ob Sie sich noch in der Anfangsphase Ihrer DLP-Entwicklung oder bereits in einer späteren Phase befinden, können Sie diese Schritte zum Erfolg sowohl für herkömmliche DLP-Anwendungen als auch zur Erweiterung Ihres Datenschutzansatzes durch eine risikogerechte DLP-Lösung verwenden.

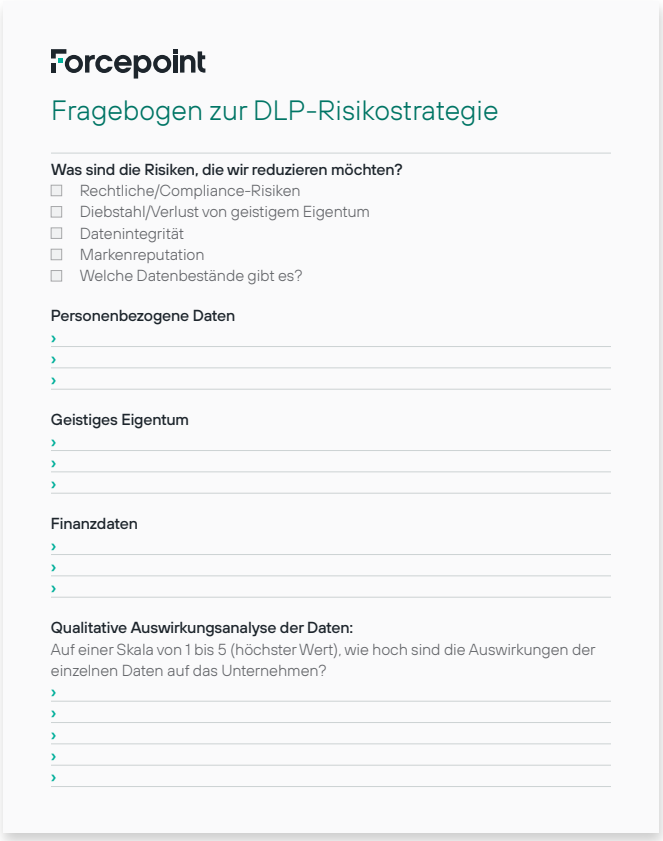
Phase 1:

Erstellen Sie ein Informationsrisikoprofil

Ziel: Erlangen Sie ein Verständnis für den Umfang Ihrer Datenschutzanforderungen.
Übersicht: Erstellen Sie ein anfängliches Informationsrisikoprofil, das folgende Aspekte abdeckt:

- → Eine Aufstellung der potenziellen Konsequenzen, wenn Sie untätig bleiben.
- → Eine Beschreibung der Datentypen im Geltungsbereich (z. B. personenbezogene Daten, geistiges Eigentum, Finanzdaten).
- → Definitionen der Netzwerk-, Endpoint- und Cloud-Kanäle, über die Informationen verloren gehen oder gestohlen werden können.
- → Eine Liste bestehender Sicherheitskontrollen, die derzeit für Datenschutzzwecke eingesetzt werden (z. B. Verschlüsselung).

1. **Definieren Sie das Risiko, das Sie reduzieren möchten.**
2. **Beginnen Sie mit einer Auflistung Ihrer wertvollen Daten und gruppieren Sie diese nach Datentypen.**
3. **Arrangieren Sie Interviews mit Datenbesitzern, um die Auswirkungen einer Datenschutzverletzung zu ermitteln.**
4. **Erstellen Sie eine Liste von Kanälen, über die Informationen übertragen werden können.**



Forcepoint

Fragebogen zur DLP-Risikostrategie

Was sind die Risiken, die wir reduzieren möchten?
- ☐ Rechtliche/Compliance-Risiken
- ☐ Diebstahl/Verlust von geistigem Eigentum
- ☐ Datenintegrität
- ☐ Markenreputation
- ☐ Welche Datenbestände gibt es?

Personenbezogene Daten
›
›
›

Geistiges Eigentum
›
›
›

Finanzdaten
›
›
›

Qualitative Auswirkungsanalyse der Daten:
Auf einer Skala von 1 bis 5 (höchster Wert), wie hoch sind die Auswirkungen der einzelnen Daten auf das Unternehmen?
›
›
›
›
›

Phase 2:

Entwerfen Sie Aktionsszenarien für verschiedene Ernstfälle

Ziel: Die Reaktionszeiten bei Datenverlustereignissen in Abhängigkeit vom Schweregrad zu ermitteln.

Übersicht: Arrangieren Sie Gespräche zwischen Ihrem DLP-Implementierungsteam und den Datenbesitzern, um die Auswirkungen bei Verlust, Diebstahl oder Gefährdung von Daten zu ermitteln. Verwenden Sie zur Beschreibung der Auswirkungen eine qualitative Analyse, beispielsweise eine Skala von 1 bis 5. Dies hilft dabei, die Reaktionsmaßnahmen bei Vorfällen zu priorisieren, und wird zur Ermittlung der angemessenen Reaktionszeit verwendet.

Risikogerechte DLP-Option: Beachten Sie, dass eine DLP-Lösung mit risikogerechtem Ansatz darauf ausgelegt ist, risikobehaftete Aktivitäten zu priorisieren, risikobasierte Kontrollen autonom durchzusetzen und die benötigte Zeit zur Untersuchung eines Vorfalls zu verkürzen. Das Ergebnis ist ein geringeres Risiko von Auswirkungen und eine aktivere Kontrolle kritischer Daten.

Die Anfangsphasen gelten weiterhin, werden aber durch risikogerechte DLP ergänzt.

1. **Beginnen Sie mit einer Diskussion über die Art von Daten, die geschützt werden sollen.**
2. **Stellen Sie anwendbare Vorschriften den identifizierten Datentypen gegenüber.**
3. **Bestimmen Sie, wie Sie die Daten identifizieren werden.**
4. **Bestimmen Sie den Schweregrad der Auswirkungen und die jeweils angemessene Reaktion auf einen Vorfall.**

„DSGVO-Verletzungen in Bezug auf personenbezogene Daten müssen der entsprechenden Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls gemeldet werden."

Verordnungen			**Schritt 1:** Allgemeine Datentypen besprechen **Schritt 2:** Relative Verordnungen (Assistent verfügbar) **Schritt 3:** „ID" – registriert oder beschrieben **Schritt 4:** Menge oder % für hoch/mittel/niedrig		Legende Auswirkungsbewertung		
Benachrichtigung bei Verstößen	HIPAA	PCI/PCI-DSS			5, 4	3, 2	1
			Personenbezogene Daten	ID	Hoch	Mittel	Niedrig
			VIP PII	R	1	-	-
			PII	D	> 100	> 25	> 2
			PHI	D	> 100	> 50	> 2
			Finanzinformationen	ID	Hoch	Mittel	Niedrig
			Kreditkarten	D	> 25	> 5	> 2
			Gehaltsabrechnung	D	> 25	> 5	> 2
			Geistiges Eigentum	ID	Hoch	Mittel	Niedrig
			Projekt X	R	> 25 %	> 10 %	10 % <
			Konstruktionspläne	R	> 25 %	> 10 %	10 % <
			Benutzername und Kennwörter	R	> 25 %	> 10 %	10 % <

Schritt 1: Bestimmen Sie die Reaktion auf Vorfälle auf der Grundlage von Schweregrad und Kanal

Ziel: Definieren Sie, was auf der Grundlage des jeweiligen Schweregrads und des betroffenen Kanals als Reaktion auf Datenverlustvorfälle geschieht.

Übersicht: Ihre Organisation verfügt über eine beschränkte Anzahl von Kanälen, über die Informationen übertragen werden. Diese Kanäle fungieren als Kontrollpunkte, welche die DLP-Kontrollen verwenden, um Datenverlust zu ermitteln und darauf zu reagieren. Listen Sie alle verfügbaren Kommunikationskanäle in Ihrem Netzwerk, am Endpunkt und in der Cloud (d. h. genehmigte Cloud-Anwendungen) in einem Arbeitsblatt auf. Bestimmen Sie dann (auf Grundlage des Schweregrads des Vorfalls) für den jeweiligen Kanal eine der über die DLP-Kontrollen bereitgestellten Reaktionsoptionen.

Sie können zudem etwaige Zusatzanforderungen Ihrer Organisation für die Durchführung der gewünschten Reaktion klären, z. B. Verschlüsselung oder SSL-Inspizierung. So ist beispielsweise ein Wechselmedium einer der drei wichtigsten Kanäle für Datenverlust, aber es ist auch ein hervorragendes Instrument zur Steigerung der Produktivität.

Eine Möglichkeit, das Risiko von Datenverlust für Box oder Google Drive zu minimieren, ist die Freigabe von Dateien mit sensiblen Informationen, die in Cloud-Speicher übertragen und extern freigegeben werden, automatisch aufzuheben.

Risikogerechte DLP-Option: Eine risikogerechte DLP-Lösung kann Unternehmen detaillierte Durchsetzungskontrollen für alle Kanäle zur Verfügung stellen und bietet die Flexibilität, die Reaktion auf der Grundlage des Risikoniveaus des Benutzers anzupassen (z. B. „Nur prüfen" für Benutzer mit geringem Risiko oder „Sperren" für Benutzer mit hohem Risiko). Dies ermöglicht Benutzern, ihre Aufgaben effektiv und ohne Gefährdung ihrer Daten zu erledigen.

1. **Wählen Sie die Daten bzw. den Datentyp aus.**
2. **Bestätigen Sie die Kanäle, die überwacht werden sollen.**
3. **Bestimmen Sie die Reaktion auf Grundlage des Schweregrads.**
4. **Geben Sie Zusatzanforderungen für die gewünschte Reaktion an.**

Kanäle	Ebene 1 Niedrig	Ebene 2* Niedrig-Mittel	Ebene 3 Mittel	Ebene 4 Mittel-Hoch	Ebene 5 Hoch	Hinweise
Web	Prüfen	Prüfen/ Benachrichtigen	Sperren/ Benachrichtigen	Sperren/Warnen	Sperren	Proxy Sperren
Sicheres Web	Prüfen	Prüfen/ Benachrichtigen	Sperren/ Benachrichtigen	Sperren/Warnen	Sperren	SSL-Inspektion
E-Mail	Verschlüsseln	E-Mail-Anlagen löschen	In Quarantäne stellen	In Quarantäne stellen	Sperren	Verschlüsselung
FTP	Prüfen	Prüfen/ Benachrichtigen	Sperren/ Benachrichtigen	Sperren/Warnen	Sperren	Proxy Sperren
Netzwerkdrucker	Prüfen	Prüfen/ Benachrichtigen	Sperren/ Benachrichtigen	Sperren/Warnen	Sperren	DLP-Drucker-Agent installieren
Cloud-Anwendungen	Prüfen	Prüfen/ Benachrichtigen	Mit Hinweis in Quarantäne stellen	In Quarantäne stellen	Sperren	
Benutzerdefiniert	Prüfen	Prüfen/ Benachrichtigen	Sperren/ Benachrichtigen	Sperren/Warnen	Sperren	k.A.

* Zusätzliche Granularität durch risikogerechte DLP möglich

Abbildung 2. Zuordnung DLP-Kanalrichtlinie

Schritt 2: Definieren Sie einen Workflow zur Reaktion auf Vorfälle

Ziel: Stellen Sie sicher, dass Verfahren für die Identifizierung von Vorfällen und die Reaktion darauf tatsächlich befolgt werden.

Übersicht: Das in Abbildung 3 abgebildete Workflow-Diagramm für Vorfälle zeigt den Prozess, nach dem Vorfälle auf Grundlage des jeweiligen Schweregrads verwaltet werden. Es stellt dar, was genau geschieht, nachdem ein Vorfall erkannt wurde. Arbeiten Sie bei Vorfällen mit geringem Schweregrad nach Möglichkeit mit Automatisierung. Dazu gehört meist die Benachrichtigung von Benutzern und Führungskräften bei riskantem Verhalten. Es kann auch ein Coaching der Mitarbeiter einschließen, um die selbstständige Beseitigung von Risiken zu erleichtern.

Vorfälle mit schwerwiegenderen Auswirkungen erfordern das Eingreifen eines entsprechend spezialisierten Analysten, der die Art der Bedrohung (z. B. versehentlich, absichtlich oder böswillig) untersucht und ermittelt. Der Analyst leitet den Vorfall samt Analyse an den Programmmanager (d. h. normalerweise an den Leiter Sicherheit bzw. Compliance) weiter, und dieser bestimmt dann, welche Maßnahmen ergriffen und welche Teams eingebunden werden sollen.

Risikogerechte DLP-Option: Wenn Sie sich für eine risikogerechte Lösung entscheiden, ist eine Untersuchung durch einen auf Sicherheitsvorfälle spezialisierten Analysten nicht erforderlich, bevor Maßnahmen ergriffen werden. Vorfälle, die Benutzern mit geringem Risiko zugeschrieben werden, sind möglicherweise keine Bedrohung für das Unternehmen und sollten so zugelassen werden, dass sie die Produktivität nicht beeinträchtigen. Zu diesen zulässigen Aktionen gehören jedoch auch Sicherheitsvorkehrungen wie das Anfordern einer Verschlüsselung bei Speicherung auf USB-Geräten oder das Ablegen von per E-Mail gesendeten Anlagen.

Für Benutzer mit erhöhtem Risiko und die damit verbundenen Vorfälle können Administratoren einen aktiven Ansatz verfolgen, indem sie bestimmte Aktionen automatisch sperren oder einschränken, bis sie von Vorfallanalysten untersucht werden können.

Arbeitsabläufe beruhen auf Schweregrad und Priorität des Vorfalls

Bei risikogerechten DLP-Lösungen werden Richtlinien auf jeder Risikostufe automatisch durchgesetzt.

Niedrig (Stufe 1)	Prüfen
Niedrig-Mittel (Stufe 2)	Prüfen und Benachrichtigen
Mittel (Stufe 3)	Zugriff beschränken / Benachrichtigen / Automatische Durchsetzung von Richtlinien
Mittel-Hoch (Stufe 4)	Zugriff beschränken / Untersuchen / Automatische Durchsetzung von Richtlinien
Hoch (Stufe 5)	Zugriff sperren / Untersuchen / Automatische Durchsetzung von Richtlinien

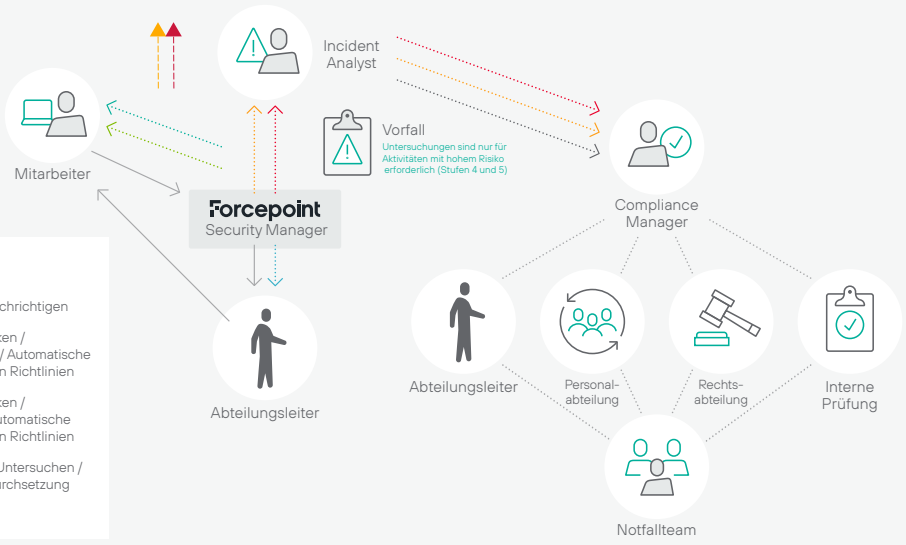


Abbildung 3. Workflow zur Reaktion auf Vorfälle

Phase 3:

Testen Sie das Überwachungsprogramm im Rahmen eines Pilotprojekts

Ziel: Netzwerk-DLP implementieren, um Risiken zu messen und mit der Risikominderung zu beginnen.

Übersicht: Phase 3 hat vier zusätzliche Schritte. In Schritt 1 weisen Sie den wichtigsten Stakeholdern Rollen und Verantwortlichkeiten zu. In Schritt 2 schaffen Sie den technischen Rahmen. In Schritt 3 erweitern Sie die Abdeckung von DLP-Kontrollen. In Schritt 4 integrieren Sie diese Kontrollen dann in die gesamte Organisation.

Vor der aktiven Anwendung sollte DLP zunächst passiv ausgeführt werden, damit Sie die Auswirkungen Ihrer Richtlinien verstehen. Sobald Sie sich einen besseren Überblick über die Bewegung und Nutzung von Daten in Ihrer Organisation verschafft haben, können Sie die Kontrollen anpassen, um die Richtlinien für Benutzer mit höherem Risiko durchzusetzen.

Nach der anfänglichen Überwachungsphase, während der Sie eine Netzwerk-DLP-Kontrolle implementieren, nehmen Sie eine Analyse vor und präsentieren die wesentlichen Erkenntnisse der Geschäftsleitung. Diese Präsentation sollte Empfehlungen für Risikominderungsaktivitäten umfassen, mit denen sich die Eintrittshäufigkeit von Vorfällen, an denen gefährdete Daten beteiligt sind, reduzieren lässt. Ermitteln Sie anschließend die Ergebnisse, und melden Sie diese an die Geschäftsleitung.

Risikogerechte DLP-Option: Wenn Sie sich für die Implementierung einer risikogerechten DLP entscheiden, können Sie eine Analyse von Vorfällen im Modus „Nur prüfen" im Vergleich zum abgestuften Durchsetzungsmodus durchführen.

Diese Gegenüberstellung verdeutlicht die geringere Anzahl von Vorfällen, die eine Untersuchung erfordern, ohne dass Ihre Daten gefährdet werden. Die beobachteten Ergebnisse sind eher ein Indikator für echte Vorfälle. Sie können damit auch die Vorteile der Automatisierung, die Reduzierung des Ressourcenbedarfs zur Überwachung und Bewältigung von Vorfällen und die Steigerung der Produktivität der betroffenen Teams nachweisen.

Schritt 1: Zuweisung von Rollen und Verantwortlichkeiten

Ziel: Höhere Stabilität, Skalierbarkeit und operative Effizienz des DLP-Programms.

Übersicht: Normalerweise werden vier verschiedene Rollen zugeordnet, um die Integrität der DLP-Kontrollen zu wahren und die operative Effizienz eines entsprechenden Programms zu steigern.

- → Technischer Administrator
- → Auf Sicherheitsvorfälle spezialisierter Analyst/Manager
- → Forensischer Ermittler
- → Prüfer

Jede Rolle wird gemäß ihren Verantwortlichkeiten definiert und dem jeweils geeigneten Stakeholder zugewiesen. In dieser Phase agieren für gewöhnlich die Mitglieder des DLP-Implementierungsteams als Vorfallsmanager. Wenn die DLP-Kontrollen jedoch ein ausgereifteres Niveau erreichen und einen hohen Grad an Zuversicht vermitteln, werden diese Rollen an die jeweiligen Dateneigner übertragen.

Abbildung 4. Zuweisung von Rollen und Verantwortlichkeiten

Schritt 2: Schaffung des technischen Rahmens

Ziel: Die Ausgangslage für die Datensicherheitskontrollen zu ermitteln, um Ihrer Organisation dabei zu helfen, normales Nutzerverhalten zu erkennen und Datenschutzverletzungen mit erheblichen Auswirkungen zu verhindern.

Übersicht: In dieser Phase übernimmt das DLP-System vornehmlich eine Überwachungsrolle und blockiert nur Vorfälle von erheblicher Tragweite, (z. B. wenn Daten an bekanntermaßen kriminelle Zieladressen hochgeladen werden oder eine große Menge ungeschützter Datensätze im Rahmen einer einzelnen riskanten Transaktion hochgeladen wird). Der Ansatz „Nur prüfen" kann auch bei Verwendung einer risikogerechten DLP-Lösung befolgt werden, indem jede Risikostufe auf „Nur prüfen" eingestellt wird.

Die Phasen 4 und 5 befassen sich eingehender mit dem Reporting, der Investitionsrendite und dem Verfolgen der Risikoreduzierung.

1. **Installieren und Konfigurieren**
2. **Überwachen des Netzwerks**
3. **Analysieren von Ergebnissen**
4. **Erste Präsentation an Geschäftsleitung**
5. **Maßnahmen zur Risikominderung** (z. B. Sperrrichtlinien aktivieren)
6. **Analysieren von Ergebnissen**
7. **Zweite Präsentation an Geschäftsleitung**

Schaffung des technischen Rahmens	Montag	Dienstag	Mittwoch	Donnerstag	Freitag
Woche 1: Installieren / Optimieren / Schulen					
Woche 2: Überwachen					
Woche 3: Überwachen					
Woche 4: Erste Präsentation an Geschäftsleitung					
Woche 5: Risikominderung					
Woche 6: Zweite Präsentation an Geschäftsleitung					

Abbildung 5. Implementierungszeitplan – Teil 1

Schritt 3: Erweiterung der Abdeckung von DLP-Kontrollen

Ziel: Implementieren von DLP für Endpunkte und genehmigte Cloud-Anwendungen, um Risiken zu messen und zu reduzieren.

Übersicht: Nun sind Sie bereit, um auf derzeit verwendete und ruhende Daten einzugehen. In diesem Schritt implementieren Sie DLP für Endpunkte und genehmigte Cloud-Anwendungen, überwachen und analysieren Ihre Daten, bringen die Geschäftsleitung auf den neuesten Stand und führen ganz ähnlich wie zu Beginn in Phase 3 risikomindernde Aktivitäten durch. Der wesentliche Unterschied ist der, dass Sie nun auf Grundlage der unterschiedlichen Kanäle und der Optionen, die für derzeit auf den Endpunkten und in Cloud-Anwendungen verwendete Daten verfügbar sind, auf Vorfälle reagieren. (Den Schweregrad eines Vorfalls und die jeweils angemessene Reaktion auf Basis des Kanals haben Sie bereits in Phase 2 ermittelt.)

Für ruhende Daten identifiziert und priorisiert der Prozess mögliche Ziele, die durchsucht werden sollen. Veraltete Daten werden in Quarantäne verschoben, wo Ihre Rechts- und Compliance-Teams das weitere Vorgehen auf Grundlage der Datenaufbewahrungsrichtlinien Ihrer Organisation bestimmen können. In Bezug auf Compliance geht es um Kooperation – also kooperieren Sie auch. Allerdings mit einer Geschwindigkeit, die für Ihre Organisation angemessen ist. Denken Sie daran: Niemand erhält einen Preis dafür, der Erste zu sein.

Falls Sie eine Discovery-Task früher als geplant durchführen müssen, sollten Sie im Hinterkopf behalten, dass Sie die Erkennungsaufgaben vorübergehend (oder dauerhaft) beschleunigen können, indem Sie lokale Discovery Agents einsetzen oder mehrere Netzwerk-Discovery-Geräte einrichten.

1. **Bereitstellen und Überwachen von Endpunkten und (genehmigten) Cloud-Anwendungen**
2. **Einleiten von Suchläufen zur Ermittlung**
3. **Analysieren von Ergebnissen**
4. **Dritte Präsentation an Geschäftsleitung**
5. **Maßnahmen zur Risikominderung**
6. **Analysieren von Ergebnissen**
7. **Vierte Präsentation an Geschäftsleitung**

Erweiterung der Abdeckung von DLP-Kontrollen	Montag	Dienstag	Mittwoch	Donnerstag	Freitag
Woche 7: Bereitstellen von Endpunkten und (genehmigten) Cloud-Anwendungen					
Woche 8: Überwachung von Endpunkten und (genehmigten) Cloud-Anwendungen/Ruhende Daten					
Woche 9: Überwachung von Endpunkten und (genehmigten) Cloud-Anwendungen/Ruhende Daten					
Woche 10: Dritte Präsentation an Geschäftsleitung					
Woche 11: Risikominderung					
Woche 12: Vierte Präsentation an Geschäftsleitung					

Abbildung 6. Implementierungszeitplan – Teil 2

Schritt 4: Integration von DLP-Kontrollen in den Rest der Organisation

Ziel: Das Vorfallsmanagement an die wesentlichen Stakeholder der Hauptgeschäftsbereiche zu übertragen.

Übersicht: Wenn Sie die Datenbesitzer und die anderen wesentlichen Stakeholder im Rahmen der DLP-Implementierung noch nicht direkt eingebunden haben, ist nun der Zeitpunkt hierfür gekommen.

Insbesondere die Rolle des Vorfallmanagers eignet sich am besten für Datenbesitzer, da diese im Fall eines Datenverlusts haftbar sind. Indem ihnen die Verantwortung für ihr Vorfallmanagement übertragen wird, wird der Mittelsmann ausgeschaltet, was die operative Effizienz steigert. Darüber hinaus werden sie hierdurch jeweils in die Lage versetzt, ihre Risikotoleranz akkurat einzuschätzen und genau zu verstehen, wie ihre Daten von anderen genutzt werden.

Während dieses Schritts sollten Sie das DLP-Implementierungsteam bitten, ein Kick-Off-Meeting zu veranstalten, um den anderen Beteiligten die DLP-Kontrollen vorzustellen. Hierauf sollte eine entsprechende Schulung folgen, im Rahmen derer die neuen Teammitglieder mit der Anwendung für Vorfallmanagement vertraut gemacht werden. Bevor die Verantwortung für das Vorfallmanagement übergeben wird, sollte ein Zeitraum festgelegt werden, in dem Sie die neuen Teammitglieder bei der Reaktion auf Vorfälle unterstützen, so dass diese korrekt eingearbeitet werden.

1. **Ausschuss einberufen und einbinden**
2. **Information über Programm und Zuordnung von Rollen**
3. **Schulung**
4. **Bei Reaktion auf Vorfälle unterstützen**
5. **Fünfte Präsentation an Geschäftsleitung**
6. **Reaktion auf Vorfälle durch Ausschuss**
7. **Sechste Präsentation an Geschäftsleitung**

Integration von DLP-Kontrollen in den Rest der Organisation	Montag	Dienstag	Mittwoch	Donnerstag	Freitag
Woche 13: Auswahl und Benachrichtigung					
Woche 14: Information über Programm und Zuordnung von Rollen					
Woche 15: Schulung mit Unterstützung bei Reaktionen					
Woche 16: Fünfte Präsentation an Geschäftsleitung					
Woche 17: Reaktion auf Vorfälle durch Ausschuss					
Woche 18: Sechste Präsentation an Geschäftsleitung					

Abbildung 7. Implementierungszeitplan – Teil 3

Phase 4:

Setzen Sie Sicherheit aktiv um

Ziel: Wechsel zu automatischem Schutz und automatischer Reaktion auf Vorfälle mit hohem Risiko.

Übersicht: In Organisationen erfolgen die Umstellung auf aktiven, automatischen Schutz und die Personalisierung normalerweise in zwei Schritten. Im ersten Schritt wird von Prüfung auf Analyse umgestellt. Der zweite Schritt umfasst die Automatisierung der Reaktion. Beachten Sie, dass in den meisten Fällen keine Phasen übersprungen werden können.

Schritt 1: Analyse und Warnungen

Ziel: Beginnen Sie mit der Analyse von Daten und ihrer Bewegung innerhalb der Organisation, um nachzuvollziehen, was bei einer Datenschutzverletzung passiert ist.

Übersicht: Eine Prüfung reicht nicht mehr aus, Sie müssen vielmehr analysieren, wie eine Verletzung stattgefunden hat. Dazu braucht es Transparenz: Sie müssen wissen, wo Daten gespeichert sind, wie sie sich verhalten und wohin sie übertragen werden. Suchwerkzeuge für Big Data und traditionelle DLP-Produkte, die lediglich Funktionen zur Datenerkennung und Kontrolle bieten, haben eine Schwachstelle: Sie warnen Cyber-Sicherheitsadministratoren erst dann vor Datenschutzverletzungen, wenn diese bereits aufgetreten sind. Zudem bieten sie meist keine umfassenden forensischen Tools zur Analyse. Der voreingestellte Modus „Nur prüfen" soll dafür sorgen, dass legitime geschäftliche Transaktionen nicht beeinträchtigt werden. Das hat jedoch zur Folge, dass diese Werkzeuge bei der Vermeidung zukünftiger Vorfälle keine große Hilfe sind. In dieser Phase sind Unternehmen zwar „konform", jedoch keineswegs sicher.

Die Analyse nach dem Sicherheitsvorfall mag zwar sehr umfangreich sein und die besten verfügbaren forensischen Tools nutzen, bietet jedoch letztendlich nur einen reaktiven Schutz. Dennoch können Unternehmen in dieser Phase die gewonnenen Informationen nutzen, um ihre Datensicherheitsrichtlinien manuell anzupassen, um nachfolgende Vorfälle zu unterbinden.

Schritt 2: Aktive Automatisierung und Personalisierung der Datensicherheit

Ziel: Schützen Sie sich aktiv vor einer Datenschutzverletzung durch Infiltration oder Herausschleusen von Daten, indem Sie das Verhalten von Benutzern und System automatisch analysieren, den Zugriff und Aktivitäten, die als Bedrohung betrachtet werden, sperren und Richtlinien automatisch an die jeweiligen Personen anpassen, wenn sie den Kontext des betreffenden Verhaltens kennen. Bei einem vollständig automatisierten Ansatz erhält der Benutzer in einem Unternehmen eine verhaltensbasierte Risikobewertung. Basierend auf dieser Bewertung wird die Sicherheit dann vorausschauend angepasst, ohne dass der Benutzer dadurch beeinträchtigt wird. Risikobewertungen berücksichtigen die Unwägbarkeiten der Interaktion des Benutzers mit Daten, System und Anwendungen und liefern den nötigen Kontext für das Verhalten, wodurch die Anzahl der Fehlalarme verringert werden kann. Aktionen von geringem Risiko sind zulässig, während bei Aktivitäten mit einem höheren Risiko automatisch Reaktionen generiert werden, z. B. Administratorwarnungen, Verschlüsselung, vollständige Sperrung und andere vordefinierte Sicherheitsmaßnahmen.

So sieht moderne Datensicherheit aus: ein anpassbarer, automatischer Prozess, der Geschäftsabläufe so wenig wie möglich beeinträchtigt, da er risikobehaftete Aktivitäten verhindert, normale Benutzer und Systeme aber nicht durch überzogene Maßnahmen einschränkt. Risikobasierte DLP-Lösungen sollen die Erreichung der Unternehmensziele unterstützen und nicht ausbremsen, und sie sollen die Mitarbeiter und Daten eines Unternehmens schützen, ohne den Umgang der Benutzer mit den Daten, die sie für ihre Arbeit benötigen, zu beeinträchtigen.

> **„Risikobasierte DLP-Lösungen sollen die Erreichung der Unternehmensziele unterstützen und nicht ausbremsen, und sie sollen die Mitarbeiter und Daten eines Unternehmens schützen, ohne den Umgang der Benutzer mit den Daten, die sie für ihre Arbeit benötigen, zu beeinträchtigen."**

Durch den Umstieg von einer passiven DLP-Lösung auf eine risikogerechte Datensicherheit können Unternehmen das Risiko von Marken- und finanziellen Schäden infolge von Datenschutzverletzungen verringern und gleichzeitig durch die Nutzung von Verhaltensanalysen ihre Ziele leichter erreichen.

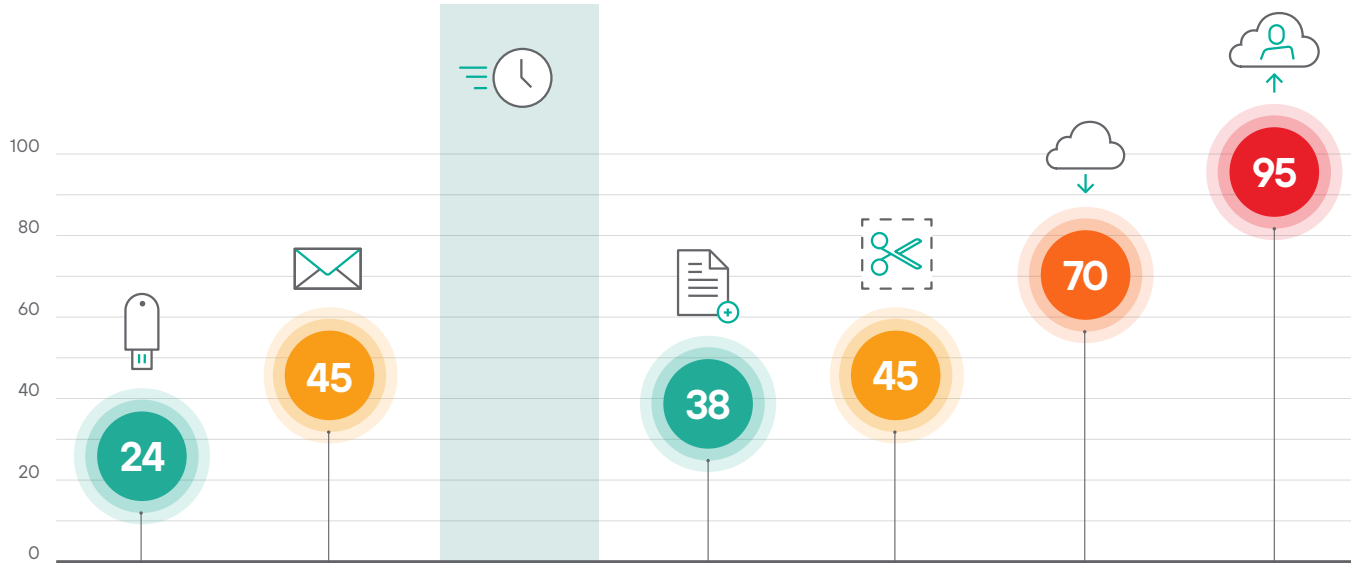


Abbildung 8. Wie das Benutzerverhalten die Risikobewertung des Benutzers negativ beeinflussen kann

Phase 5:

Messen Sie den Erfolg der Risikoreduzierung

Ziel: Die Investitionsrendite durch eine messbare Reduzierung des Risikos aufzuzeigen.

Übersicht: Es gibt zwei wesentliche Punkte, die zum in Phase 3 erwähnten Prozess zur Überwachung der Risikoreduzierung hinzugefügt werden müssen. Hierbei handelt es sich um:

1. Miteinander verbundene Vorfälle sollten zusammengefasst werden.
Zu den häufigsten Gruppen zählen Schweregrad, Kanal, Datentyp und Vorschrift. Für größere Organisationen helfen zusätzliche Untergruppen, das Risiko nach geografischen Standorten oder Tochtergesellschaften weiter zu klären.

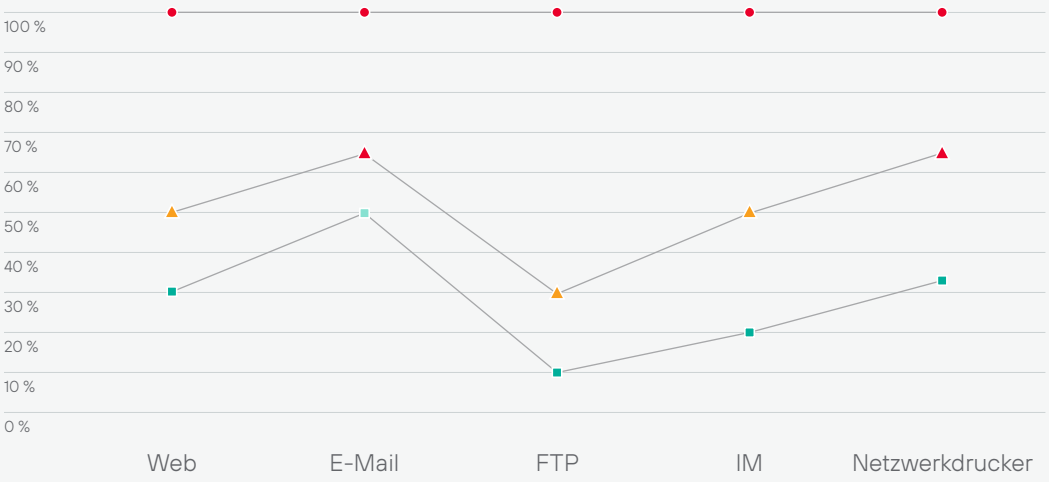
2. Zwischen Risikoreduzierungsphasen sollte die Konsistenz gewahrt werden.
Um die Integrität Ihrer Ergebnisse zu wahren, müssen die Zeiträume für Überwachung und Risikoreduzierung jeweils gleich lang sein. Für den Anfang empfehlen wir zwei Wochen, um die Amortisierungsdauer zu verbessern und die Analyse zu vereinfachen. Sie sind jedoch selbst in der besten Position um zu ermitteln, welcher Zeitraum für Ihre Organisation angemessen ist.

Unten sehen Sie ein Beispiel dafür, wie eine Gruppierung vorgenommen und die Risikoreduzierung überwacht werden kann. Beachten Sie, dass die Zeiträume konstant sind, der Schwerpunkt auf Vorfällen mit hohem Risiko liegt und dass diese Vorfälle nach dem jeweiligen Kanal gruppiert sind.

Risikogerechte DLP-Option: Wenn Sie sich für einen risikogerechten Ansatz entschieden haben, sollten Sie einen Vergleich der im Modus "Nur prüfen" erfassten Vorfälle (alle Vorfälle) mit den Vorfällen mit abgestufter Durchsetzung erstellen. In der Zusammenfassung sollte die Anzahl der Vorfälle für jede Risikostufe 1–5 gegenüber den tatsächlich zu untersuchenden Vorfällen (Risikostufen 4–5) ersichtlich sein.

Wenn Sie Ihrer Geschäftsleitung schließlich aktuelle Informationen zum DLP-Prozess und den erzielten Ergebnissen liefern, denken Sie daran, dass weniger oft mehr ist. Konzentrieren Sie sich auf das Gesamtbild, wenn Sie die Vektoren mit dem höchsten Risiko für Ihre Organisation erläutern, und skizzieren Sie Ihre empfohlenen Maßnahmen zur Risikominderung sowie die jeweils damit verbundenen Kosten, Nutzen und Anstrengungen.

Wahrscheinlichkeit eines Datenverlusts



Markierungslegende

- Hoch
- Mittel
- Niedrig
- Akzeptabel
- 30 Tage (Ausgangswert)
- 60 Tage
- 90 Tage

Anzahl Vorfälle in 90 Tagen

Vorfälle	Web	E-Mail	FTP	IM	Netzwerkdrucker
30 Tage (Ausgangswert)	200	150	50	10	45
60 Tage (Ausgangswert)	100	100	15	15	30
› Risikoreduzierung nach 60 Tagen	50 %	33 %	70 %	50 %	33 %
90 Tage (Ausgangswert)	60	76	5	2	15
› Risikoreduzierung nach 90 Tagen	70 %	49 %	90 %	80 %	67 %

Ziele

- **60 Tage** Reduzierung um 25 % oder mehr
- **90 Tage** Reduzierung um 50 % oder mehr

Abbildung 9. Verfolgung des Risikos von Datenverlusten

Fazit

Eine erfolgreiche DLP-Implementierung wird nicht durch neuen technischen Schnickschnack erreicht, noch lässt sie sich einfach im Rechenzentrum abarbeiten. Der Erfolg hängt vielmehr von Ihrer Fähigkeit ab:

1. die Methodik und Umsetzungsstrategie eines DLP-Anbieters zu verstehen. Ihre Organisation profitiert davon, zu unterscheiden, wie verschiedene Anbieter an das Thema DLP herangehen. Hierdurch können Sie die vielversprechendsten Anbietermethoden für Ihre Umgebung ermitteln und bestimmen, welche DLP-Technologien Sie beurteilen sollten. Die Berücksichtigung eines Anbieters, der eine risikogerechte Lösung bereitstellt, kann einem Unternehmen langfristige Vorteile bringen, z. B. mehr Effizienz und Produktivität. Und vergessen Sie nicht: Die Methodik eines Anbieters auf die Technologie eines anderen anzuwenden, hat negative langfristige Konsequenzen.

2. die Risikoformel für Datenverlust anzuwenden. Nachdem Ihr Sicherheitsteam die Risikoformel für Datenverlust verstanden und angewandt hat, kann es mit Dateneignern zusammenarbeiten, um Ihre wertvollsten Daten zu identifizieren und zu priorisieren. Darüber hinaus sollte jede Aktivität zur Risikominderung einzig und allein auf das Ziel ausgerichtet sein, die Eintrittshäufigkeit von Datenverlusten zu reduzieren. Die Eintrittshäufigkeit ist die korrekte Kennzahl für die Messung der Risikominderung und den Nachweis der Investitionsrendite auf DLP-Kontrollen. Zur Erinnerung: Achten Sie beim Vergleich herkömmlicher DLP-Lösungen mit einer DLP-Lösung mit risikogerechter Technologie besonders darauf, dass Sie Fehlalarme nicht mit echten Vorfällen vergleichen.

3. die 80-20-Regel für eine Ressourcenzuteilung anzuwenden. Wenn Sie verstehen, welche Datenverlustvektoren das größte Risiko für eine Datenschutzverletzung mit erheblichen Auswirkungen bedeuten, können Sie die 80-20-Regel anwenden, um Ressourcen zuzuweisen und effektive Datenschutzstrategien zu entwickeln.

4. die neun Schritte zum DLP-Erfolg zu befolgen. Unabhängig davon, ob Sie einen herkömmlichen oder einen risikogerechten DLP-Ansatz verfolgen, bietet unser neunstufiger Prozess eine bewährte Formel für die praktische Implementierung von DLP-Kontrollen in Ihrem Unternehmen – damit Sie umsetzbare, messbare und risikogerechte Ergebnisse erzielen können.

Forcepoint

forcepoint.com/contact

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datensicherheit und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die auf menschlichem Verhalten basierenden Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.

[Practical-Execs-Guide-to-DLP-Whitepaper-DE] 24Sept2021