proofpoint.

E-BOOK

DLP neu definiert

Warum brauchen Unternehmen einen moderneren Ansatz für Data Loss Prevention

proofpoint.com/de

Überblick: Datenverlustprävention in einer Zeit des Wandels

Ein Mitarbeiter eines bekannten Anbieters für Cybersicherheit verkauft die Daten von 68.000 Kunden an einen Telefonbetrüger.[1] Über ein Datenleck bei einem großen Anbieter aus dem Medizin- und Gesundheitssektor in Singapur gelangen die Datensätze von 1,5 Millionen Patienten in falsche Hände, darunter auch die Daten des Premierministers.[2] Bedingt durch die mangelhafte Sicherheitshygiene eines IT-Anbieters werden bei der ältesten französischen Tageszeitung 7,4 Milliarden Datensätze offengelegt, darunter auch personenbezogene Daten der Leser.[3]

Jeder dieser realen Fälle ist auf seine Weise einzigartig – und sie alle führten zu Datenverlust. Hinzu kamen die damit verbundenen Public Relations-Probleme, die Kosten für die Behebung und der Imageschaden.

Datenverlust ist ein altbekanntes und in jedem Fall ernstes Sicherheitsproblem, ganz gleich ob er auf einen externen Angriff oder Insider-Bedrohungen zurückgeht. In modernen Geschäftsumgebungen ist diese Herausforderung jedoch noch komplizierter und dringender geworden. In heutigen Unternehmen sind Cloud-basierte Infrastrukturen, Remote-Arbeit und hybride Belegschaften – bestehend aus Mitarbeitern, Auftragnehmern und Freiberuflern – längst kein Fremdwort mehr.

Auch wenn jedes Unternehmen anders ist, eines ist sicher: Daten bewegen sich nicht von selbst. Es ist der Mensch, der Daten verschiebt, missbräuchlich verwendet und abzweigt.

Die Bewältigung der Datenverlustproblematik lässt sich jedoch kaum noch mit der Vielzahl von Compliance-Vorschriften vereinbaren. Gleichzeitig sind die Strafen für Vorschriftenverstöße härter denn je.

Die Lösung dieses Dilemmas verlangt einen neuen Ansatz.

In diesem E-Book werden die zunehmenden Herausforderungen analysiert, denen die schnelllebigen Arbeitsplatz- und IT-Umgebungen heute ausgesetzt sind. Anschließend wird erläutert, weshalb herkömmliche Ansätze für Data Loss Prevention (DLP) der Aufgabe nicht gewachsen sind. Schließlich zeigt das E-Book eine Roadmap für DLP auf, das speziell auf die Arbeitsweise moderner Unternehmen zugeschnitten ist.

Die Fakten

85 % der Datenschutzverletzungen gehen mit einer menschlichen Komponente einher[4]

30 % der Datenschutzverletzungen gehen auf böswillig oder fahrlässig handelnde oder kompromittierte Insider zurück[5]

52 % der Unternehmen beklagen kompromittierte Cloud-Konten[6]

32 % der kompromittierten Unternehmen verzeichneten nach dem Angriff Aktivitäten wie Dateimanipulationen, E-Mail-Weiterleitungen und OAuth-Aktionen.[7]

1 Trend Micro: „Trend Micro Discloses Insider Threat“ (Trend Micro gibt Insider-Bedrohung bekannt), November 2019.
2 Jessica Davis *(Xtelligent Healthcare Media)*: „Massive SingHealth Data Breach Caused by Lack of Basic Security“ (Massive Datenschutzverletzung bei SingHealth durch fehlende grundlegende Sicherheit verursacht), Januar 2019.
3 Phil Muncaster *(Infosecurity Magazine)*: „French Newspaper Le Figaro Leaks 7.4 Billion Records“ (Bei der französischen Tageszeitung Le Figaro werden 7,4 Milliarden Datensätze geleakt), Mai 2020.
4 Verizon: „2020 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2020), Juni 2019.
5 ebd.
6 Itir Clarke und Assaf Friedman (Proofpoint): „OAuth abuse: Think SolarWinds/Solorigate campaign with focus on cloud applications“ (OAuth-Missbrauch: SolarWinds/Solorigate-Kampagne mit Fokus auf Cloud-Anwendungen), März 2021.
7 ebd.

Inhaltsverzeichnis

1 **Datenverlust und moderne Unternehmen** 4

2 **Weshalb es an der Zeit ist, Data Loss Prevention neu zu definieren** 6

3 **Wodurch sich modernes DLP auszeichnet**. 11

4 **Schlussfolgerung und Empfehlungen**. 15

Abschnitt 1

Datenverlust und moderne Unternehmen

Für die meisten Unternehmen waren die letzten Jahre von turbulenten Veränderungen geprägt. Die zunehmend dezentrale Belegschaft, neue Geschäftsmodelle und der Umstieg in die Cloud haben unsere Arbeitsweise nachhaltig verändert. Diese Trends haben jedoch die Einhaltung von Vorschriften erschwert. Dies ist insbesondere dann der Fall, wenn lediglich Sicherheitstools und -prozesse zur Verfügung stehen, die ursprünglich für ein anderes Zeitalter der Arbeit entwickelt wurden.

74 %	der führenden Finanzunternehmen gehen davon aus, dass das Arbeiten im Home Office die Pandemie überdauern wird[8]
11,45 Mio. $	kostet eine durch einen Insider bedingte Datenverletzung im Durchschnitt[9]
Etwa **70 %**	der Fälle von Datenmissbrauch infolge von Datenschutzverletzungen gingen 2021 auf die unerlaubte Nutzung von Berechtigungen zurück[10]

Fahrlässige Anwender machen ohne böse Absicht einen Fehler oder suchen bei der Wahrnehmung ihrer Aufgaben nach einem einfacheren Weg.

Kompromittierte Anwender sind Opfer eines externen Cyberangreifers, der die Kontrolle über ihre Konten übernimmt und diese missbräuchlich verwendet.

Böswillige Anwender exfiltrieren vorsätzlich Daten zu ihrem persönlichen Vorteil.

Mehr Home Office- und hybride Beschäftigungsmodelle

Bereits bevor die weltweite COVID-19-Pandemie Schluss mit „Business as usual“ machte, war unsere Arbeitsweise großen Veränderungen unterworfen. Begriffe wie „von zu Hause arbeiten“ oder „Arbeiten von überall“ gehören längst zum Alltagswortschatz. Home Office-Arbeit oder hybride Dienstpläne – einst attraktive Jobvorteile – sind mittlerweile Routine. Wissensmitarbeiter sind nicht mehr an ihr Büro gebunden, das durch perimeterbasierte Sicherheitstools geschützt ist. Auch dem Blickfeld des Vorgesetzten können sie sich jetzt entziehen.

Gleichzeitig vermischen sich Arbeit und Freizeit. Dadurch werden private Geräte beruflich eingesetzt und die vom Arbeitgeber bereitgestellten Geräte werden von der Familie und für private Zwecke genutzt. Dieser Trend erschwert selbst die besten Vorkehrungen für Informations- und Datenschutz.

8 Gartner: „Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently“ (Gartner-Umfrage unter CFO zeigt, dass 74 % der Unternehmen für einige Angestellte permanente Remote-Arbeit planen), April 2020.
9 Ponemon Institute: „2020 Cost of Insider Threats: Global Report“ (Kosten von Insider-Bedrohungen 2020: Weltweit), Februar 2020.
10 Verizon: „2021 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2021), Mai 2019.

ARBEIT UND FREIZEIT HABEN SICH VERMISCHT

Dadurch werden private Geräte beruflich eingesetzt und die vom Arbeitgeber bereitgestellten Geräte werden von der Familie und für private Zwecke genutzt. Dieser Trend erschwert selbst die besten Vorkehrungen für Informations- und Datenschutz.

Neben dem Anbieten von Home Office-Arbeitsplätzen haben sich viele Unternehmen für die Cloud entschieden. So nutzen viele Anwender Software-as-a-Service (SaaS)-Plattformen, Cloud-Speicher, Tools für Zusammenarbeit sowie Chat- und Videokonferenzfunktionen.

Mehr Angriffspunkte für Datenlecks

Neben dem Anbieten von Home Office-Arbeitsplätzen haben sich viele Unternehmen für die Cloud entschieden. So nutzen viele Anwender Software-as-a-Service (SaaS)-Plattformen, Cloud-Speicher, Tools für Zusammenarbeit sowie Chat- und Videokonferenzfunktionen. Auch eher konservative Branchen, wie Behörden oder der Medizin- und Gesundheitssektor, hosten ihre Serviceleistungen für Kunden, Mitarbeiter und Bürger auf Infrastructure-as-a-Service (IaaS)-Plattformen.

Mit dem Sicherheitsmodell der „gemeinsamen Verantwortung“ übertragen Cloud-Anbieter die Verpflichtung zum Schutz der Informationen, Systeme und Apps an die Unternehmen. Hinzukommt, dass vorhandene Legacy-Infrastrukturen und -Anwendungen mitunter historische vertrauliche Informationen enthalten.

In solch diversen Anwendungs- und Cloud-Umgebungen können Sicherheitsteams kaum erkennen, wenn Daten ihre übliche Umgebung verlassen, eventuell verloren gehen oder offengelegt werden. Moderne Unternehmen müssen sich nicht nur mit externen Bedrohungen auseinandersetzen, sondern auch mit böswilligen, fahrlässigen oder kompromittierten Anwendern in den eigenen Rängen.

Mehr „Outsider“ mit Zugriff auf Insider-Ebene

Ergänzend zu ihren festangestellten Mitarbeitern setzen Unternehmen seit Langem auf eine ganze Armee aus externen Hilfskräften, darunter Auftragnehmer, Dienstleister, Zeitarbeiter, Logistikpartner usw. Viele gehen sogar noch weiter: Sie fokussieren sich wieder auf ihr Kerngeschäft und überlassen andere wichtige Funktionen externen Dritten.

Nur wenige Sicherheitsteams verfügen über die Kontrollen, geschweige denn über die personellen Ressourcen, um all diese externen Anbieter zu verwalten und zu überwachen. Auch können sie nicht gewährleisten, dass die externen Mitarbeiter in den Bereichen Sicherheit, Datenverlust und Insider-Risikomanagement ausreichend geschult wurden.

Die meisten Unternehmen haben Prozesse für die Compliance externer Anbieter implementiert. Vielleicht verfügen sie sogar über perimeterbasierte Zugriffskontrollen, die sicherstellen, dass vertrauliche Daten das Netzwerk nicht verlassen.

Was ihnen jedoch fehlt, sind personenbezogene Sichtbarkeit bzw. entsprechende Kontrollen. Dies hat zur Folge, dass Sicherheitsteams keine Zugriffskontrollen für kritische Anwendungen und vertrauliche Dateien festlegen können. Ebenso fehlt die Sichtbarkeit auf Anwenderebene, sodass die Aktivitäten von Auftragnehmern und externe Partnern beim Verschieben wichtiger Dateien, Interagieren mit kritischen Anwendungen oder Nutzen gemeinsamer Konten auf Servern alles andere als transparent sind.

ABSCHNITT 2

Weshalb es an der Zeit ist, Data Loss Prevention neu zu definieren

FAHRLÄSSIGE ANWENDER MÜSSEN GESCHULT, BÖSWILLIGE ANWENDER ÜBERWACHT UND KOMPROMITTIERTE ANWENDER VERMIEDEN WERDEN.

Anders ausgedrückt: Es geht darum, dass Sie Ihre Methoden für Schutz, Erkennung und Reaktion an die Art der Datenschutzverletzung anpassen.

Unsere Vorgehensweise beim Erstellen, Speichern und Verwenden von Daten hat sich geändert. Die Kategorien der Anwender, denen Zugriff auf diese Daten gewährt wird, haben sich geändert. Die Risiken und potenziellen Auswirkungen haben sich geändert.

Höchste Zeit, auch unseren Ansatz für DLP zu ändern. Unternehmen investieren immer stärker in DLP und Datenschutz und bekommen immer weniger Gegenleistung. Herkömmliche DLP-Tools bieten keine echte Möglichkeit, externe oder interne Bedrohungen zu stoppen.

Sie sehen für fahrlässige, kompromittierte und böswillige Anwender lediglich einen universellen Sicherheitsansatz vor. Das Ergebnis: Fahrlässige Anwender sind frustriert, weil sie blockiert werden, während böswillige Anwender und externe Angreifer die Kontrollen schlicht umgehen.

Unternehmen können sich nicht mehr allein auf den Perimeter-Schutz konzentrieren (der Insider-Bedrohungen ohne nie wirksam abwehren konnte). Stattdessen müssen sie einen modernen, personenzentrierten DLP-Ansatz verfolgen, der folgende Fragen beantwortet: Wer greift auf welche Daten zu? Was geschieht mit den Daten? Wie werden die Daten an andere weitergegeben?

Fahrlässige Anwender müssen geschult, böswillige Anwender überwacht und kompromittierte Anwender vermieden werden. Mit anderen Worten: Es geht darum, dass Sie Ihre Methoden für Schutz, Erkennung und Reaktion an die Art der Datenschutzverletzung anpassen.

Schrittweise Verbesserungen sind nicht ausreichend. Um moderne DLP-Herausforderungen in den Griff zu bekommen, bedarf es einer völlig neuen Denkweise.

DLP: das Ziel

Das Hauptziel von DLP-Programmen besteht darin, Schutz vor Mitarbeitern zu bieten, die vertrauliche oder kritische Daten auf riskante oder gegen die Richtlinie verstoßende Art und Weise aus dem Unternehmen nach außen verlagern.

Gewährleisten von Vertraulichkeit

Nachfolgend einige Beispiele für vertrauliche Daten, die mit DLP geschützt werden sollen:

- Personenbezogene Informationen zu Mitarbeitern und Kunden
- Personenbezogene Patientendaten zu Mitarbeitern und Kunden
- Personenbezogene Finanz- und Bankdaten zu Mitarbeitern und Kunden
- Handelsgeheimnisse
- Geistiges Eigentum
- Kundenlisten
- Lieferanteninformationen
- Wichtige, nicht öffentliche Informationen
- Andere vertrauliche Geschäftsdaten

DLP-Programme spielen eine immer wichtigere Rolle bei der Einhaltung branchenspezifischer und regionaler Datenschutzbestimmungen.

DLP-Technologien stehen jedoch vor einer zweifachen Herausforderung. Einerseits müssen sie gewährleisten, dass Mitarbeiter angemessen auf sensible oder kritische Daten zugreifen und diese verwenden können. Andererseits sollten DLP-Lösungen geschäftliche Transaktionen natürlich nicht versehentlich blockieren oder die Anwenderproduktivität beeinträchtigen.

81 %

der Entscheidungsträger wünschten sich bereits vor der Pandemie eine bessere Lösung für den Schutz ihrer vertraulichen Daten, die ihre Innovationsfähigkeit nicht beeinträchtigt.[11]

86 %

Nie zuvor gaben sie mehr Geld für die Bekämpfung von Insider-Bedrohungen aus als heute. Die Kosten für die Untersuchung dieser Art von Bedrohungen sind in nur drei Jahren um 86 % gestiegen.[12]

DLP: die Realität

Die meisten Unternehmen verfügen über herkömmliche DLP-Technologien, mit der sie die Einhaltung von Vorschriften gewährleisten möchten. Diese Tools sind jedoch oft kostspielig und umständlich in der Wartung. Zudem stören sie die Arbeitsabläufe der Anwender. Das Schlimmste dabei: Sie halten nicht, was sie versprechen, und das ist ohnehin nicht viel.

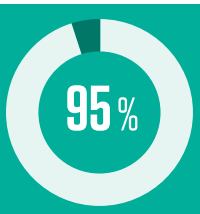
Kein Wunder, dass sich bereits vor der Pandemie 81 % der Entscheidungsträger eine bessere Lösung für den Schutz ihrer vertraulichen Daten wünschten, die ihre Innovationsfähigkeit nicht beeinträchtigt.[11]

Dabei kann man nicht behaupten, dass Unternehmen untätig seien. Nie zuvor gaben sie mehr Geld für die Bekämpfung von Insider-Bedrohungen aus als heute. Die Ausgaben sind um 60 % höher als noch vor drei Jahren und die Kosten für die Untersuchung dieser Art von Bedrohungen sind in nur drei Jahren um 86 % gestiegen.[12]

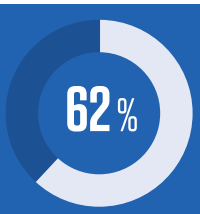
Herkömmliches DLP funktioniert nicht mehr

1,64 $ MILLIARDEN
werden 2021 schätzungsweise weltweit insgesamt für DLP ausgegeben.[13]

77 TAGE
dauert die Behebung der Folgen von Insider-Bedrohungen.[14]



der Unternehmen sind Opfer von Cloud-Angriffen[15]



der Zwischenfälle sind durch fahrlässige Nutzer bedingt.[16]

11 Forrester: „It's Time For Next-Generation Data Loss Prevention" (Es ist Zeit für Datenverlustprävention der nächsten Generation), Mai 2019.
12 Ponemon Institute: „2020 Cost of Insider Threats: Global Report" (Kosten von Insider-Bedrohungen 2020: Weltweit), Februar 2020.
13 The Radicati Group: „Data loss prevention (DLP) market revenue forecast worldwide from 2019 to 2023" (Prognosen zum weltweiten DLP-Markt 2019–2023), April 2021.
14 Ponemon Institute: „2020 Cost of Insider Threats: Global Report" (Kosten von Insider-Bedrohungen 2020: Weltweit), Februar 2020.
15 Assaf Friedman und Itir Clarke (Proofpoint): „How Attackers Use Compromised Accounts to Create and Distribute Malicious OAuth Apps" (Wie Angreifer mit kompromittierten Konten schädliche OAuth-Apps erstellen und verteilen), Mai 2021.
16 Ponemon Institute: „2020 Cost of Insider Threats: Global Report" (Kosten von Insider-Bedrohungen 2020: Weltweit), Februar 2020.

DATEN BEWEGEN SICH NICHT VON SELBST

Der Mensch ist für ihren Verlust oder Missbrauch verantwortlich. Deshalb ist es beim Schutz von Daten wichtig, dass der Kontext bekannt ist. Sie müssen wissen, auf welche Daten Ihre Mitarbeiter zugreifen, was sie damit machen und welche Mitarbeiter bevorzugtes Ziel von Cyberangreifern sein könnten.

Verhalten und Bedrohungskontext kommen zu kurz

Daten bewegen sich nicht von selbst. Der Mensch ist für ihren Verlust oder Missbrauch verantwortlich. Deshalb ist es beim Schutz von Daten wichtig, dass der Kontext bekannt ist. Sie müssen wissen, auf welche Daten Ihre Mitarbeiter zugreifen, was sie damit machen und welche Mitarbeiter bevorzugtes Ziel von Cyberangreifern sein könnten. Es genügt nicht, bei DLP lediglich die Daten im Blick zu haben, auch die Mitarbeiter und die Art der Bedrohung müssen berücksichtigt werden.

Herkömmliches DLP liefert in der Regel keinen Kontext.

- Es besteht nur begrenzter oder gar kein Einblick dazu, wer mit vertraulichen Daten interagiert, diese in der Cloud oder im Internet bereitstellt, wer sie druckt, per E-Mail sendet oder auf USB-Geräten und Endpunkten speichert.
- Die Erkennung von und Reaktion auf Insider-Bedrohungen fehlen vollständig.
- Herkömmliches DLP kann keinen Zusammenhang zwischen Aktivitäten herstellen oder Aktivitäten richtig interpretieren, die zwar zu geringfügig sind, um einen Alarm auszulösen, aber im jeweiligen Kontext dennoch kritisch sind.
- DLP ist nicht in eine Plattform für Bedrohungsschutz oder in Echtzeit-Bedrohungsdaten integriert.

DLP-Richtlinien: schwer zu formulieren, einfach zu umgehen

Herkömmliche DLP-Tools wurden für regulierte Daten entwickelt, die von Tools einfach zu erkennen und für Anwender schwer zu ändern waren. Zur Vermeidung von False Positives waren präzise und granulare Richtlinien erforderlich. Eine typische Richtlinie enthielt bestimmte Merkmale wie Datenkennungen, Anwendungsnamen, Datenexfiltrationskanäle usw.

Dieser Grad an Ausführlichkeit war für Daten geeignet, die in Datenbanken, auf Servern und an einigen statischen Standorten gespeichert wurden.

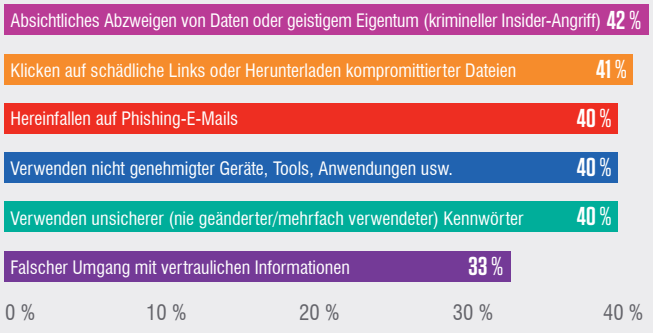
Heute kommen vertrauliche Geschäftsinformationen, regulierte Daten und geistiges Eigentum nahezu überall in allen Arten von Dateien und Dokumenten vor. Dadurch ist das Verfassen von DLP-Richtlinien wesentlich schwieriger geworden, das Umgehen dafür umso einfacher.

Vertrauliche Daten und Dokumente sind viel schwieriger zu erkennen und mit einfachen Datenkennungen zu kennzeichnen. Anwender können diese außerdem einfach ändern. Sei es aus einem berechtigten geschäftlichen Grund, versehentlich oder im Rahmen einer böswilligen Aktion.

Um solche Aktionen zu verhindern, muss eine komplexe Liste mit sich überschneidenden DLP-Richtlinien erstellt und verwaltet werden. Telemetriedaten zu Datenbewegungen außerhalb eines erkannten Alarms werden in Protokolldateien gespeichert, die bestenfalls schwer zugänglich und zu analysieren sind. Telemetrie zu Anwenderverhalten und Bedrohungen wird überhaupt nicht erfasst. Wenn Sicherheitsanalysten all diese Einzelereignisse zu einem Gesamtbild zusammenfügen wollten, müssten sie dies manuell oder unter Verwendung mehrerer getrennter Tools tun.

Es liegt auf der Hand, dass die meisten Sicherheitsteams nur sehr begrenzt Einblick in die Datenbewegungen innerhalb ihres Unternehmens haben.

Wie machen Ihre Mitarbeiter Ihrer Ansicht nach Ihr Unternehmen für Cyberangriffe anfällig? (Bitte drei Antworten wählen)



Quelle: 2021 Voice of the CISO Report

Begrenzte Prävention fahrlässiger Anwenderfehler

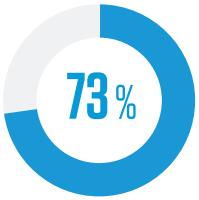
Diese sehr konkreten Richtlinien begrenzen natürlich den Umfang, in dem herkömmliche DLP-Tools Daten schützen können. Sie bieten außerdem keine Lösungsansätze für unbeabsichtigtes oder fahrlässiges Anwenderverhalten, sodass vertrauliche Daten nahezu ungeschützt zugänglich sind. (Das Verwenden ungeschützter Datenbanken oder Speichern von Kennwörtern in ungesicherten Dateien sind nur zwei Beispiele für typische Verhaltensweisen.)

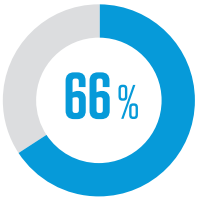
In einigen Fällen sind die Kontrollen so missverständlich, dass Anwender ihre Daten unbeabsichtigt einem Risiko aussetzen, indem sie sie öffentlich freigeben, statt nur innerhalb des Unternehmens. Mitunter sind Daten allein deshalb angreifbar, weil herkömmliche DLP-Tools nicht auf Malware oder riskante Anwenderaktionen ausgelegt sind.

Kontrollen: eine Belastung für Anwender und Systeme

Zusätzlich zu den ressourcenintensiven Endpunkt-Agenten können auch weitere Aspekte herkömmlicher DLP-Tools die Systemressourcen stark belasten und Anwendern beschwerliche Kontrollen aufbürden, die sie an der eigentlichen Arbeit hindern.

Je mehr Anforderungen Unternehmen an ihre DLP-Tools stellen, desto weniger bekommen sie. Versuchen Unternehmen beispielsweise, komplexe und sich überschneidende Erkennungs- und Präventionsrichtlinien einzurichten, die eine gründlichere Untersuchung von Inhalten verlangen, müssen sie dafür nicht selten Leistungseinbußen hinnehmen. (Das ist sicherlich der falsche Anreiz.)





Bei 73 % der Unternehmen, die DLP einsetzen, beschweren sich die Mitarbeiter darüber.[17] Der Grund dafür liegt auf der Hand: Die Produktivität der Mitarbeiter wird ausgebremst.

66 % der Unternehmen gaben an, dass ihre DLP-Lösungen die Mitarbeiter, trotz Einhaltung der Richtlinie, oft am Datenzugriff hindern würden.[18]

Warum Legacy-DLP-Tools bei Anwendern so unbeliebt sind

Herkömmliche DLP-Lösungen sind manchmal etwas übereifrig, wenn es um die Blockierung von Aktionen geht. Das Arbeiten im Home Office und hybride Arbeitsansätze werden immer mehr zur Norm. Sicherheitsteams können kaum noch vorhersagen, wann welche Mitarbeiter auf welche Art arbeiten möchten. Setzt ein Unternehmen auf Blockierungsrichtlinien, verhindert es unter Umständen, dass seine Mitarbeiter das öffentliche Internet nutzen, am Arbeitsplatz auf private E-Mails zugreifen oder mit neuen Cloud-basierten Tools arbeiten können.

Laut einer Umfrage von Forrester ist dies für die Mitarbeiter von 73 % der Unternehmen, die DLP einsetzen, ein Problem.[17] Der Grund dafür liegt auf der Hand: Die Produktivität der Mitarbeiter wird ausgebremst. Oft werden Anwender ungewollt daran gehindert, auf Daten zuzugreifen oder diese weiterzugeben, selbst wenn sie die Richtlinie beachten.

In derselben Studie gaben 66 % der Unternehmen an, dass ihre DLP-Lösungen die Mitarbeiter, trotz Einhaltung der Richtlinie, oft am Datenzugriff hindern würden.[18] Ungewollte Konsequenz: Die Anwender weichen auf Schatten-IT aus (und verwenden nicht genehmigte Anwendungen und Services), um ihre Arbeit zu erledigen.

Wenn Blockierungsrichtlinien zum Hemmschuh werden

Einige DLP-Systeme blockieren sogar legitime Prozesse, weil diese schlicht nicht in den DLP-Richtlinien und genehmigten Listen aufgeführt sind. Für moderne Unternehmen, die auf reibungslose digitale Transaktionen und Kommunikation angewiesen sind, stellt dies ein großes Problem dar. Blockieren DLP-Richtlinien versehentlich eine legitime Transaktion oder Nachricht, müssen sich die Sicherheitsteams hinterher mit den (berechtigten) Beschwerden der Anwender auseinandersetzen.

17 Forrester: „It's Time For Next-Generation Data Loss Prevention“ (Es ist Zeit für Datenverlustprävention der nächsten Generation), Mai 2019.
18 ebd.

Im schlimmsten Fall kollidiert die Endpunkt-DLP-Lösung mit einem anderen Sicherheitstool am Endpunkt oder verursacht einen Systemabsturz. Die Folge davon ist ein höheres Aufkommen an sicherheitsbezogenen Support-Tickets und E-Mails und auch nachhaltige Folgen für Mitarbeiter, Kunden und Geschäftspartner.

Datenerkennung und -klassifizierung sind zu zeitintensiv

Bei herkömmlichen DLP-Lösungen kann das Erkennen und Klassifizieren von Daten mehrere Monate in Anspruch nehmen. Statt sich auf die Frage zu konzentrieren, wie Anwender Daten im Hier und Jetzt verschieben (und das womöglich auf riskante Weise), beschäftigt sich herkömmliches DLP damit, was in der Vergangenheit mit den Daten geschehen ist.

Die Datenerkennung ist ein langwieriger Prozess. Suchläufe werden in der Regel außerhalb der Geschäftszeiten durchgeführt, um die erheblichen Auswirkungen auf Systemleistung und Produktivität auf ein Minimum zu reduzieren.

Ein weiteres Problem ist die Tatsache, dass die meisten DLP-Tools nicht in der Lage sind, frühere Datenklassifizierungen einzulesen, ohne dass der Kunde hochpreisige Professional Services in Anspruch nehmen muss. Das gilt zum Beispiel für Microsoft Information Protection. Für jedes neue Programm müssen Unternehmen ihre Daten innerhalb des neuen Tools neu klassifizieren.

Etwa 75 % der von Forrester befragten IT-Verantwortlichen gaben an, dass die Bereitstellung ihrer DLP-Lösung mindestens einen Monat dauerte. Ganze 24 % gaben eine Dauer von sechs Monaten und mehr an.[19]

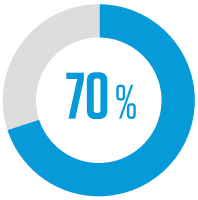
Bereitstellung und Wartung sind komplex und kostspielig

Das Bereitstellen herkömmlicher DLP-Tools ist häufig komplex und teuer – vor allem, wenn sie lokal eingesetzt werden. Die Installation und Integration von Servern, Anwendungen, Datenbanken und anderen Infrastrukturkomponenten kann mehrere Monate in Anspruch nehmen. Die Wertschöpfung kann sich sogar noch länger hinziehen.

Etwa 75 % der von Forrester befragten IT-Verantwortlichen gaben an, dass die Bereitstellung ihrer DLP-Lösung mindestens einen Monat dauerte. Ganze 24 % gaben eine Dauer von sechs Monaten und mehr an.[19]

Endpunkt-DLP-Produkte sind oft nicht minder problematisch. Bei vielen kommen Endpunkt-Agenten im Kernel-Modus zum Einsatz, die jede Transaktion auf Betriebssystemebene abfangen und den Endpunkt daher stark in Mitleidenschaft ziehen können. Dadurch bringen sie mitunter die Arbeit der Anwender zum Erliegen, interferieren mit Anwendungen oder führen sogar zum Absturz des Gerätes. (In vielen Fällen sind diese Probleme schwerwiegend und treten bereits in frühen Testphasen auf.)

Nach der Installation müssen für viele DLP-Lösungen komplexe Regeln und Richtlinien eingerichtet und gepflegt werden, was eine erhebliche Investition von Zeit und Geld bedeutet.



Etwa 70 % der Befragten gaben an, dass bis zu drei Viertel der von ihnen täglich untersuchten Alarme False Positives seien.[20]

False Positives führen zu Alarmmüdigkeit

DLP-Verantwortliche kritisieren außerdem die mangelnde Genauigkeit herkömmlicher DLP-Lösungen. Um eine potenzielle aktive Datenschutzverletzung aufzuhalten, müssen sie schnell reagieren. Allerdings können sie dem enormen Aufkommen an DLP-Alarmen kaum Herr werden, von denen sich viele als False Positives entpuppen.

In einer aktuellen Studie gaben etwa 70 % der Befragten an, dass bis zu drei Viertel der von ihnen täglich untersuchten Alarme False Positives seien.[20]
Es kommt noch schlimmer: Fast die Hälfte der Befragten gab an, Alarmfunktionen mit besonders vielen Meldungen auszuschalten. Dadurch gehen echte Alarme möglicherweise komplett unter.[21]

19 Forrester: „It's Time For Next-Generation Data Loss Prevention" (Es ist Zeit für Datenverlustprävention der nächsten Generation), Mai 2019.
20 Help Net Security: „Alert overload still plagues cybersecurity industry" (Alarmmüdigkeit in Cybersicherheit weiterhin Problem), März 2021.
21 ebd.

ABSCHNITT 3

Wodurch sich modernes DLP auszeichnet

Im Gegensatz zu Legacy-DLP-Tools konzentriert sich ein moderner DLP-Ansatz auf die Mitarbeiter – und nicht nur auf Daten. Der adaptive Ansatz richtet sich danach, ob die Risiken und Bedrohungen von einem fahrlässigen, einem kompromittierten oder einem böswilligen Anwender ausgehen.

Er bietet eine konsolidierte, einfach zu verwaltende Lösung, die für alle von den Mitarbeitern verwendeten Tools funktioniert: E-Mails, Clouds, Endpunkte, das Internet und Dateifreigaben. Er nutzt eine Cloud-basierte Architektur, die einfach bereitgestellt werden kann, Datenschutz und Sicherheit durch Technikgestaltung (Datenschutzfreundlichkeit) bietet, mühelos skalierbar ist und sich in ein umfassenderes Sicherheitsökosystem integrieren lässt.

Moderne DLP-Tools sind effektiver als herkömmliche DLPs und mit einem geringeren administrativen Aufwand verbunden. Sie ermöglichen schnellere Untersuchungen, Reaktionen und Behebungen, wodurch schwerwiegende Datenschutzverletzungen weniger wahrscheinlich sind. Sicherheitsteams können effizienter und produktiver arbeiten.

Dies sind einige der Vorteile moderner DLP-Tools im Vergleich mit herkömmlichen DLP-Lösungen:

- Schnelle und einfache Bereitstellung und dadurch schnellere Wertschöpfung
- Skalierbarkeit und Anpassungsfähigkeit
- Datenschutz durch Technikgestaltung (Datenschutzfreundlichkeit) und dadurch einfachere Compliance mit der wachsenden Anzahl von Datenschutzbestimmungen weltweit
- Kontext ermöglicht Differenzierung zwischen böswilligen, kompromittierten und fahrlässigen Anwendern
- Besserer Schutz für vertrauliche Daten und geistiges Eigentum
- Konsistente Richtlinien für mehrere Kanäle
- Erweiterbarkeit ohne großen technischen Aufwand, für abgestimmtes Zusammenwirken mit breiterem Sicherheitsökosystem

FOKUS AUF MITARBEITER UND DATEN

Der adaptive Ansatz richtet sich danach, ob die Risiken und Bedrohungen von einem fahrlässigen, einem kompromittierten oder einem böswilligen Anwender ausgehen.

Modernes DLP ist personenzentriert

Eine moderne DLP-Lösung stellt den Zusammenhang zwischen böswilligen, kompromittierten und fahrlässigen Anwendern und Datenbewegungen oder riskantem Verhalten hinsichtlich Dateien, Anwendungen und Endpunkten her. Sie gibt Aufschluss über die Abfolge von Ereignissen und ermöglicht dadurch den Teams für Cybersicherheit, IT, Personalwesen und Recht, Kontext schnell und einfach nachzuvollziehen. Dadurch ist für jeden (und nicht nur für das IT-Team) das Wer, Was, Wo, Wann und Warum von Sicherheitsalarmen und Zwischenfällen ersichtlich.

Die wichtigsten Bausteine des personenzentrierten Ansatzes:

- **Kenntnis des Inhalts** zum Identifizieren vertraulicher oder regulierter Daten auf mehreren digitalen Kanälen unter Nutzung von Fähigkeiten wie Datenklassifizierung, Beschriftung/Tagging, genauer Datenabgleich in mehreren Spalten, Wörterbücher, Proximitätsabgleich usw.
- **Kenntnis des Anwenderverhaltens** zum Erkennen der Anwender-aktivitäten und Bestimmen der Absicht: digitale Kanäle, Zugriffs-aktivitäten, Dateiquellen und -ziele, Laufwerke, Netzwerke, Rollen, Überwachungslisten usw.
- **Kenntnis externer Bedrohungen** in Verbindung mit Bedrohungsdaten zum Identifizieren kompromittierter Konten und der Anwender, die Opfer von Phishing-Kampagnen in der Cloud und im E-Mail-System wurden.

Fahrlässige Anwender machen ohne böse Absicht einen Fehler oder suchen bei der Wahrnehmung ihrer Aufgaben nach einem einfacheren Weg.

Zusätzlich zum Blockieren von riskanten Aktivitäten bietet modernes DLP für diese Anwender Coaching an, damit sie ihr Verhalten verstehen und ändern und dennoch produktiv bleiben.

Kompromittierte Anwender sind Opfer eines externen Cyberangreifers, der die Kontrolle über ihre Konten übernimmt und diese missbräuchlich verwendet.

Modernes DLP nutzt risikobezogene Kontrollen, um nach Anzeichen für eine Kompromittierung zu suchen, zusätzliche Sicherheitskontrollen anzuwenden und bei Bedarf riskante Aktivitäten zu blockieren.

Böswillige Anwender exfiltrieren vorsätzlich Daten zu ihrem persönlichen Vorteil.

Basierend auf Risikofaktoren wie Kündigungen oder unüblichen Aktivitäten in Verbindung mit vertraulichen Dateien ist es mit modernem DLP möglich, bestimmte Anwender enger zu überwachen, strengere Zugriffskontrollen anzuwenden und schädliche Aktionen proaktiv zu blockieren.

Dank personenzentriertem DLP sind Sicherheitsteams in der Lage Kontext-basiert zwischen böswilligen, kompromittierten und fahrlässigen Anwendern zu differenzieren. Diese Erkenntnis erleichtert es Teams, ihre Sicherheitskonzepte zu optimieren und effektiver zu automatisieren.

Modernes DLP ist konsolidiert und einheitlich

Das ständige Wechseln zwischen Kontext und Bildschirmen ist in jeder mit Technologie verbundenen Funktion anstrengend und ineffizient. Studien haben ergeben, dass das häufige Wechseln zwischen verschiedenen Aufgaben (so genanntes Multitasking) Stress hervorruft und die Konzentrationsfähigkeit beeinträchtigt. Die Produktivität kann dadurch sogar um 40 % sinken.[22]

Moderne DLP-Lösungen bieten Sicherheits- und IT-Teams eine angenehme Erfahrung. Abgesehen von den Produktivitätsvorteilen, die die Verwendung von nur einer Konsole bietet, liefert ein moderner DLP-Ansatz IT- und Sicherheitsexperten einen vollständigeren Überblick über Datenverlust.

Er fügt die drei wichtigsten digitalen Kanäle – Endpunkt, Netzwerk und Cloud – zu einem zusammenhängenden Gesamtbild zusammen. Sämtliche Alarme werden in einer einzigen Konsole aufgerufen, sodass technische Teams alles im Blick haben. Datenbewegungen von Anwendern lassen sich direkt verfolgen. Die Exfiltration kann selbst dann verhindert werden, wenn die Daten zwischen zwei Kanälen verschoben werden.

Modernes DLP ist Cloud-nativ und skalierbar

Eine moderne DLP-Lösung ist Cloud-basiert – und muss es auch sein.

Die meisten Unternehmen haben sich für eine Cloud-basierte IT entschieden. Die Architektur herkömmlicher DLP-Tools ist jedoch auf lokale Umgebungen ausgerichtet, sodass sie sich nicht skalieren lässt und auch nicht die Sicherheit bietet, die moderne Unternehmen brauchen. Da sie zudem schwierig zu verwalten und nicht erweiterbar sind, können sie sich nicht anpassen, wenn sich Ihre Infrastruktur und Ihre Anforderungen verändern.

Eine moderne Cloud-basierte Architektur ist die einzige Möglichkeit, den Umfang Ihrer DLP-Lösung zu skalieren, ohne die Leistung in Mitleidenschaft zu ziehen – und das zu planbaren Kosten. Sie ist auch die einzige Möglichkeit, umfassende Transparenz für die relevanten digitalen Kanäle herzustellen.

Cloud-basierte DLP-Architekturen werden oberhalb von leichtgewichtigen, aber umfassenden Telemetrie-Kollektoren implementiert. Sie kombinieren Cloud-Anwendungs-API-Verbindungen, Endpunkt-Agenten im Anwendermodus und E-Mail-Gateways und liefern auf diese Weise einen vollständigen Überblick über Datenbewegungen, Anwenderverhalten und externe Bedrohungen.

Mit anderen Worten: Sie erhalten einen aussagekräftigen, anwendungs-agnostischen Einblick in die Aktivitäten Ihrer Anwender in E-Mails, in der Cloud und auf dem Endpunkt, ohne ihre Arbeit zu behindern. Ein Cloud-basierter Ansatz bietet außerdem Sicherheitskontrollen, die die versehentliche Weitergabe von Daten bzw. die böswillige Weitergabe von Daten über kompromittierte Anwenderkonten verhindern.

22 Kendra Cherry *(Verywell Mind)*: „How Multitasking Affects Productivity and Brain Health“ (Wie Multitasking Produktivität und Gesundheit des Gehirns beeinträchtigt), März 2020.

Weshalb sich die Modernisierung Ihres DLP-Ansatzes lohnt

Nachfolgend finden Sie einen Vergleich zwischen modernem DLP und Legacy-DLP sowie eine Übersicht der Fähigkeiten beider Ansätze in typischen Anwendungsfällen.

ÜBERWACHUNG		
LEGACY-DLP	MODERNES DLP	ANWENDUNGSFÄLLE
●	●	Datenerkennung
○	●	Insider-Risiken (böswillige Anwender, Anwender mit umfangreichen Berechtigungen, ausscheidende Mitarbeiter, Server- und Workstation-Nutzung)
○	●	Nutzung von Anwendungen durch Dritte
○	●	Bedrohungssuche und DLP-Analyse (einschließlich Daten- und Dateiverlauf)

ERKENNUNG		
LEGACY-DLP	MODERNES DLP	ANWENDUNGSFÄLLE
●	●	Geistiges Eigentum und regulierte Daten in Clouds, E-Mails und auf Endpunkten (unbeabsichtigte Datenlecks oder schädliche Datenexfiltration)
○	●	Anormales Anwenderverhalten (kompromittierte Anmeldung, schädlicher Inhalt oder böswilliges Anwenderverhalten)

PRÄVENTION		
LEGACY-DLP	MODERNES DLP	ANWENDUNGSFÄLLE
●	●	Datenverlust auf verschiedenen Kanälen (E-Mail, Cloud und Endpunkt)
○	●	Anormales Anwenderverhalten (kompromittierte oder böswillige Anwender)

REAKTION		
LEGACY-DLP	MODERNES DLP	ANWENDUNGSFÄLLE
○	●	Untersuchung von Datenverlust, Insider-Bedrohungen und Kontenkompromittierungen
◐	●	Integration in SIEM, SOAR, Tools für geschäftliche Kommunikation und Ticket-Management

○ Nicht vorhanden ◐ Teilweise vorhanden ● Vollständig enthalten

ABSCHNITT 4

Schlussfolgerung und Empfehlungen

Unternehmen bevorzugen die Cloud, unterstützen eine Kultur des ortsunabhängigen Arbeitens und betrachten Innovation als einen ihrer Kernwerte. All das sollte Ihre DLP-Lösung berücksichtigen.

Modernes DLP nutzt eine Cloud-basierte Architektur und ist daher in der Lage, durch Insider-Risiken oder externe Bedrohungen bedingte Datenverluste zu reduzieren. Sie optimiert die Arbeitsabläufe Ihres Teams und beschleunigt die Erkennung von und Reaktion auf Zwischenfälle.

Halten Sie beim Umstieg auf moderne DLP Ausschau nach einer Lösung, die einen ganzheitlichen DLP-Ansatz verfolgt und die folgenden wesentlichen Merkmale erfüllt:

- **Skalierbarer Schutz von Informationen.** Die Lösung schützt alle Datentypen, E-Mails und Cloud-Anwendungen und differenziert dabei zwischen fahrlässigen, böswilligen und kompromittierten Anwendern.
- **Cloud-native, flexible Architektur.** Die Lösung integriert sich nahtlos mit anderen Sicherheitslösungen.
- **Schnelle Bereitstellung, wenig Aufwand.** Die Lösung überwacht, was sich am Endpunkt, in der Cloud und in E-Mails tut. Sie lässt sich in wenigen Tagen oder Wochen bereitstellen.
- **Sicherheit und Datenschutz durch Technikgestaltung (Datenschutz-freundlichkeit).** Die Lösung gewährleistet durch genau definierte Datenausschlussrichtlinien und starke Zugriffskontrollen, dass die richtigen Mitarbeiter – und nur die – zum richtigen Zeitpunkt Zugriff auf die richtigen Daten haben.

Erfahren Sie, wie Proofpoint Sie bei der Bereitstellung einer modernen DLP-Architektur unterstützen kann. Weitere Informationen finden Sie unter **www.proofpoint.com/de/products/information-protection**.

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.com/de**.

proofpoint.

0507-001-01-01 06/21