LERNEN LEICHT GEMACHT

Sonderausgabe von Netskope

Modern Data Loss Prevention (DLP)

für dummies®
A Wiley Brand

Anwendung moderner DLP-Methoden

Zero-Trust-Prinzipien zum Schutz von Daten an jedem Ort

Bessere Cloud-Sicherheit

Präsentiert von

netskope

Carmine Clementelli

Über Netskope

Netskope ist ein weltweit führender Anbieter von SASE-Lösungen, der die Cloud-, Daten- und Netzwerksicherheit neu definiert hat und Unternehmen bei der Anwendung von Zero-Trust-Prinzipien zum Schutz ihrer Daten unterstützt. Die schnell und einfach zu nutzende Netskope-Plattform bietet optimierten Zugriff und Echtzeit-Sicherheit für Personen, Geräte und Daten, wo immer sie sich befinden. Netskope hilft seinen Kunden dabei, ihre Risiken zu reduzieren, ihre Leistung zu steigern und unübertroffene Einblicke in alle Aktivitäten von Cloud-, Web- und privaten Anwendungen zu erhalten. Tausende von Kunden, darunter mehr als 25 der Fortune-100-Unternehmen, vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk bei der Bewältigung aufkommender Bedrohungen, neuer Risiken, technologischer Entwicklungen, unternehmens- und netzwerkbezogener Veränderungen sowie neuer gesetzlicher Anforderungen. Um zu erfahren, wie Netskope seine Kunden bei der Vorbereitung auf ihrer SASE-Reise unterstützt, besuchen Sie netskope.com.

Wir möchten uns bei einer Reihe von Personen bedanken, die dieses Buch gemeinsam mit dem Autor möglich gemacht haben:

Bei Netskope: Amanda Anderson, Chad Berndtson, Jason Clark, Scott Hogrefe, Kathy Jacobsen, Naveen Palavalli, Stephenie Pang, Lauren Polito, Carolyn Robinson, Neil Thacker

Bei Evolved Media: David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Modern Data Loss Prevention (DLP)

Sonderausgabe von Netskope

Carmine Clementelli

für dummies®

Moderne Data Loss Prevention (DLP) Für Dummies®, Sonderausgabe von Netskope

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-20802-9 (pbk); ISBN 978-1-394-20803-6 (ebk)

Allgemeine Informationen zu unseren sonstigen Produkten und Services oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA telefonisch unter Tel. 877-409-4177 oder per E-Mail unter info@dummies.biz. Alternativ können Sie uns auch auf www.wiley.com/go/custompub besuchen. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Services kontaktieren Sie bitte BrandedRights&Licenses@Wiley.com.

Danksagung des Verlags

Die folgenden Personen haben dabei geholfen, dieses Buch auf den Markt zu bringen:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Account Manager: Jeremith Coward

Production Editor: Mohammed Zafar Ali

Besondere Unterstützung: Nicole Sholly

Einführung

Datenschutz als Konzept ist in der Cybersicherheit keine Neuheit. Die an bestehende Datenschutzsysteme gestellten Anforderungen haben sich jedoch im letzten Jahrzehnt grundlegend geändert. Früher konnten sich Sicherheitsfachkräfte darauf verlassen, dass wertvolle Unternehmensdaten im streng abgesicherten Rechenzentrum gut aufgehoben waren. Im Zuge der digitalen Transformation verlagerten jedoch immer mehr Unternehmen jeder Größe ihre Daten in die Cloud und an verteilte Standorte. Daten sind jetzt überall dort, wo sich ihre Benutzer aufhalten – und das können die unterschiedlichsten Orte sein. Ihr Unternehmen kann digitale Verbindungen zu einer großen Anzahl von Dritt- und sogar Viertanbietern, Partnern und Auftragnehmern unterhalten. Diese Szenarien bieten ungeahnte geschäftliche Möglichkeiten (das ist die gute Nachricht), bringen aber auch zahlreiche Sicherheitsherausforderungen mit sich, besonders im Hinblick auf den Datenschutz (das ist die schlechte Nachricht).

Erfolgreiche Sicherheitsverletzungen können verheerende Folgen für ein Unternehmen haben. Die von Insidern ausgehenden Risiken (ob böswillig oder fahrlässig) sind für Ihr Unternehmen ebenso gefährlich wie schlagzeilenträchtige Angriffe von Außenstehenden. Bei all diesen Szenarien besteht die Gefahr, dass sensible Informationen offengelegt werden. Der Datenschutz ist heute ein wichtiger Eckpfeiler aller Compliance-Richtlinien. In Branchen- und Datenschutzbestimmungen sind die Pflichten Ihres Unternehmens und die bei Nichteinhaltung drohenden hohen Strafen genau festgelegt.

Unternehmen brauchen einen neuen Ansatz und müssen Datenschutzrichtlinien überall dort anwenden, wohin ihre Daten gehen, und zwar konsequent. Im Idealfall unterstützt der Datenschutz die Unternehmensziele und schützt gleichzeitig das Unternehmen. Die Verwaltung von Datenschutzrichtlinien und der zu ihrer Durchsetzung erforderlichen Tools kann jedoch komplex und kostspielig sein. Unternehmen benötigen Datenschutzlösungen, die die Durchsetzung von Richtlinien vereinfachen und gleichzeitig die Wirksamkeit dieser Richtlinien gewährleisten. Es gibt jetzt eine neue Generation von cloudbasierten Data Loss Prevention (DLP)-Lösungen, die Ihnen genau das bieten können. Unternehmen brauchen eine in der Cloud bereitgestellte Lösung, die weniger komplex, hochgradig skalierbar und kosteneffizienter ist und im Idealfall Daten mit höherer Zuverlässigkeit und Genauigkeit schützt und das Risiko eines unbefugten Zugriffs oder Missbrauchs

minimiert. Es kann schwierig sein, dabei das richtige Gleichgewicht zu finden, doch mit der richtigen Beratung können Sie dieses Ziel jetzt erreichen.

Über dieses Buch

Dieses Buch kann Ihnen dabei helfen, fundierte Entscheidungen über die Bewertung des derzeitigen Datenschutzansatzes Ihres Unternehmens zu treffen und neue Datenschutzlösungen zu evaluieren, um die beste Lösung für Ihre Anforderungen zu finden. Zero-Trust-Prinzipien sollten dabei als Leitfaden für die kontextbezogene und einheitliche Anwendung von Sicherheitsmaßnahmen dienen. Dieses Buch erklärt, wie moderne DLP-Systeme in der Cloud funktionieren, und durchdringt das Marketing-Dickicht, um die Merkmale und Fähigkeiten zu finden, die Sie für einen zuverlässigen Schutz Ihrer Daten benötigen – unabhängig davon, wo sie verwendet werden.

Leichtfertige Annahmen

Dieses Buch geht davon aus, dass Sie bereits wissen, wie Unternehmen Cloud-Computing nutzen, um flexibler zu werden und besser für die digitale Transformation gerüstet zu sein. Wir nehmen außerdem an, dass Sie nach der richtigen Kombination von Technologie und Prozessverbesserungen zum Schutz sensibler Daten suchen - unabhängig davon, wo sie sich befinden und wohin sie sich in Ihrer Rechenumgebung bewegen.

In diesem Buch verwendete Symbole

In diesem Buch verwenden wir unterschiedliche Symbole, um auf wichtige Informationen aufmerksam zu machen. Sie werden auf die folgenden Bildzeichen stoßen:

TIPP

Alles, was mit dem Tipp-Symbol gekennzeichnet ist, soll Ihnen eine bestimmte Aufgabe erleichtern.

ERINNERUNG

Das Erinnerungssymbol hebt besonders wichtige Fakten hervor.

TECHNISCHES

Hochtechnische Informationen, die Sie getrost überspringen können, sind mit dem Symbol „Technisches“ versehen.

HINWEIS

Bitte beachten Sie alles, was mit dem Warnsymbol gekennzeichnet ist, um sich unnötige Kopfschmerzen zu ersparen.

Zusätzliche Informationen

Dieses Buch steckt voller nützlicher Informationen, doch es kann durchaus sein, dass Sie sich nach der Lektüre fragen: „Wo kann ich mehr erfahren?“. Gehen Sie in diesem Fall einfach zu `www.netskope.com`.

IN DIESEM KAPITEL

- **wo sensible Daten gespeichert sind und wie sie überwacht werden**
- **worum es beim Datenschutz wirklich geht**
- **Data Loss Prevention (DLP)**
- **warum ältere DLP-Lösungen nicht mehr ausreichen**
- **Umstellung auf eine Cloud-First-Strategie mit einer modernen DLP-Lösung**
- **mit DLP-Mythen aufräumen**

Kapitel 1
Sensible Daten sind überall – und es wird immer schwieriger, sie zu finden

Wer von sensiblen Daten spricht, meint in der Regel vertrauliche oder persönliche Informationen. Welche Daten als sensibel gelten, hängt in hohem Maße davon ab, ob diese Daten aus der Perspektive des Unternehmens oder des Einzelnen betrachtet werden.

Sensible Daten – ein kurzer Überblick

Die meisten als „sensibel" bezeichneten Daten gibt es in irgendeiner Form schon seit vielen Jahren, darunter:

- personenbezogene Daten/Informationen wie Sozialversicherungsnummern, Kreditkartennummern, Führerscheinnummern, Gesundheitsdaten und Wohnadressen

- geistiges Eigentum wie Produktdesigns, Erfindungen, Patente und Quellcode
- vertrauliche Informationen und Geschäftsgeheimnisse wie Finanzpläne, Verträge, Steuerberichte, Informationen über Fusionen und Übernahmen und Dokumente mit Sperrfrist wie Pressemitteilungen

Inzwischen hat sich jedoch eine grundlegende Veränderung vollzogen: In der modernen Unternehmenslandschaft werden Daten auf völlig neue Weise ausgetauscht und (leider manchmal auch) offengelegt. Viele Unternehmen haben sich – nicht zuletzt im Zuge der COVID-19-Pandemie – für eine hybride Arbeitsumgebung entschieden.

Fast alle Arten sensibler Daten werden heute digital erstellt, gespeichert und übertragen. Daten bewegen sich zwischen Cloud-Services, Unternehmensnetzwerken und anderen Orten, an denen Benutzer auf sie zugreifen können. Diese Daten werden von immer mehr Anwendungen plattformübergreifend gespeichert und ausgetauscht und sind von praktisch jedem Gerät von entfernten Standorten aus zugänglich. Da die Menge, Vielfalt und Geschwindigkeit der verfügbaren Daten exponentiell zunimmt, wird es immer schwieriger, sensible Informationen zu identifizieren und zu schützen. Herkömmliche Sicherheitsmechanismen sind aufgrund der schieren Menge verfügbarer Daten kaum noch in der Lage, mit den neuen Bedrohungen Schritt zu halten.

Bewältigung der Datenflut

Die IDC sagt voraus, dass die globale Datensphäre bis zum Jahr 2025 auf 181 Zettabyte anwachsen wird! Ein beträchtlicher Teil davon wird direkt in der Cloud erstellt und gespeichert – und das Datenvolumen nimmt Jahr für Jahr zu. Datenschutzsysteme und ihre Betreiber werden dadurch unter anderem mit folgenden Herausforderungen konfrontiert:

- **Zu viele Kategorien sensibler Daten:** Weltweit werden immer mehr Datenschutzbestimmungen und -gesetze zum Schutz von Personen und Informationen jeder Art umgesetzt. Dementsprechend entstehen ständig neue Kategorien sensibler Daten. Dazu gehören Informationen, mit denen Personen identifiziert werden können, z. B. ihr Aufenthaltsort, finanzielle und gesundheitliche Informationen, persönliche Vorlieben, religiöse Überzeugungen und sexuelle Orientierung. Sensible Daten umfassen Informationen wie nationale Ausweisnummern, Kreditkartenangaben, Quellcode, Entwürfe, Finanzpläne, Bankkonten, Verträge, Steuerformulare, Passwörter, Informationen über Fusionen und Übernahmen, geschützte

Gesundheitsinformationen, vertrauliche E-Mails, Angaben zu Geschlecht und Religion. Die einzelnen Kategorien sensibler Daten unterscheiden sich von Land zu Land, liegen in unterschiedlichen Sprachen vor und sind länderspezifisch.

- **Zu viele Datenformate und -typen:** PDF- und Bilddateien (z. B. JPG, PNG und BMP), komprimierte und gekapselte Dateien (z. B. ZIP, RAR und ISO), Anhänge, Slack-Nachrichten, Chats, Online-Formulare, Screenshots, Tabellenkalkulationen, Computer-Aided Design (CAD), Beiträge in sozialen Netzwerken, Textdateien, Präsentationen und E-Mails.
- **Zu viel Kontext:** Wenn Entscheidungen über die Art des Zugriffs auf sensible Daten, ihre Nutzung, Übertragung und ihren Austausch getroffen werden müssen, sollte der Kontext der ausschlaggebende Faktor sein. Er gibt Aufschluss darüber, welche Handlungen im Zusammenhang mit sensiblen Daten riskant sind und was als Verletzung bzw. als versuchte Verletzung betrachtet werden sollte (wer, wo, was, wie, warum, wann, an wen und andere Faktoren).

Angesichts der zunehmenden Flut unübersichtlicher Daten müssen bestehende Sicherheitssysteme besondere Vorsicht walten lassen. Dadurch hat sich der Verwaltungsaufwand um ein Vielfaches erhöht. Warum? Sicherheitsteams, die auf Vorfälle reagieren, sehen sich mit einer Unmenge an falsch-positiven Meldungen konfrontiert, die meist von den ohnehin schon überlasteten Mitarbeitern manuell ausgewertet werden müssen.

Beim Datenschutz geht es um viel mehr als „nur" um Daten

Unternehmen benötigen neue Automatisierungsstrategien, um ihre wertvollen Daten effektiv identifizieren, überwachen und schützen zu können. Im Bereich des Datenschutzes gibt es immer wieder neue Herausforderungen, die das Sicherheitsdilemma noch verschärfen. Zu diesen neuen Herausforderungen gehören:

- **mehr Cyberrisiken:** Unternehmen haben mehr Schwachstellen als je zuvor und sind anfälliger für Datenschutzverletzungen. Dabei kann es sich sowohl um beabsichtigte als auch um unbeabsichtigte Schwachstellen handeln. Die sensiblen Informationen eines Unternehmens können durch das Verhalten von Insidern gefährdet werden, z. B. wenn Mitarbeiter Daten stehlen oder missbräuchlich verwenden (ja, das soll vorkommen!). Bei zweiundachtzig Prozent

aller Datenschutzverletzungen spielt das „menschliche Element" eine Rolle, darunter:

- *böswillige Insider:* Wenn ein verärgerter Mitarbeiter zum Beispiel Screenshots einer wichtigen Kalkulationstabelle anfertigt und Daten an eine persönliche Instanz einer Software-as-a-Service (SaaS)-Anwendung oder über eine private Instanz eines geschäftlichen E-Mail-Kontos (d. h. persönliches Gmail im Gegensatz zum Unternehmens-Gmail) sendet.
- *unbeabsichtigte Offenlegung:* Diese passiert beispielsweise durch Mitarbeiter, die versehentlich zu viele Informationen an einen Lieferanten senden oder fahrlässig zu viele Dateien in einem OneDrive-Ordner freigeben. Dies sind die wichtigsten Ursachen für Datenschutzverletzungen.

Auch bei externen Angriffen oder Hacking-Versuchen besteht die Gefahr, dass Unternehmensgeheimnisse erpresst oder an die Öffentlichkeit bzw. an konkurrierende Unternehmen weitergegeben werden.

- **die Cloud, einschließlich SaaS und Infrastructure-as-a-Service (IaaS) in der Public Cloud:** Gerade die Nutzung von SaaS-Anwendungen nimmt in rasantem Tempo zu. Aktuellen Studien zufolge nutzt ein durchschnittliches Unternehmen mehr als 2.400 Cloud-Anwendungen. 97 Prozent davon gelten als *Schatten-IT* (nicht von der IT-Abteilung genehmigt, unbekannt oder für sie unsichtbar). Dies stellt eine technische und sicherheitsbezogene Herausforderung dar, da Daten in vielen SaaS-Anwendungen gespeichert und zwischen ihnen ausgetauscht werden. Daten werden über Unternehmensnetzwerke und verwaltete Geräte hinweg übertragen und können einfach von Mitarbeitern und selbst externen Benutzern abgerufen werden, die sich von entfernten Standorten aus mit nicht verwalteten Geräten verbinden. Cloud-Anwendungen können schnell zu einem primären Angriffsvektor werden, wenn sie nicht richtig überwacht und verwaltet werden. Um sich vor derartigen Bedrohungen schützen zu können, kommen Unternehmen nicht umhin, ihre Datenschutzlösungen zu aktualisieren.
- **hybrides Arbeiten:** Die Zunahme hybrider Belegschaften hat die Art und Weise verändert, wie Unternehmen sensible Daten speichern und darauf zugreifen. Früher bewahrten Unternehmen die meisten kritischen Informationen in einem privaten Rechenzentrum auf, über das sie selbst die Kontrolle hatten. Das hat sich inzwischen grundlegend geändert. Hybride Arbeitsmodelle haben eine neue Ära eingeläutet, in der sensible Daten hochgradig verteilt sind und sich an Orten außerhalb der Unternehmensgrenzen befinden, die das Unternehmen weder sehen noch kontrollieren kann. Daten sind heutzutage über unterschiedliche digitale und physische

Umgebungen verstreut – Rechenzentren, die Unternehmenszentrale, Zweigstellen, Homeoffices und die Geräte von Außendienstmitarbeitern (persönliche und Unternehmensgeräte).

- **neue Compliance-Anforderungen:** Compliance war schon immer ein wichtiges Thema – doch heute mehr denn je. Unternehmen werden stärker reguliert und Verstöße gegen Datenschutzgesetze ziehen zunehmend hohe Geldstrafen und rechtliche Schritte nach sich, sodass Unternehmen jeder Größe unter einem erheblichen Druck stehen, ihre Compliance-Vorgaben zu erfüllen und ihre sensiblen Daten angemessen zu schützen. Unternehmen müssen entsprechende Maßnahmen ergreifen, um die Anforderungen branchenweiter Standards und Vorschriften zu erfüllen, darunter der Payment Card Industry Data Security Standard (PCI-DSS), der Health Insurance Portability and Accountability Act (HIPAA) und der Gramm–Leach–Bliley Act (GLBA). Gleichzeitig müssen sie sicherstellen, dass sie die Bestimmungen der geltenden Datenschutzgesetze und -vorschriften einhalten, darunter die Datenschutz-Grundverordnung (DSGVO), der California Consumer Privacy Act (CCPA), der Colorado Privacy Act, der Connecticut Data Privacy Act, der Virginia Consumer Data Protection Act und der Utah Consumer Privacy Act, um nur einige zu nennen. In vielen Ländern ist der Datenschutz gesetzlich geregelt, unter anderem in Brasilien, Singapur, Japan und im Vereinigten Königreich. Unternehmen müssen heute mehr denn je nachweisen können, dass sie die notwendigen Maßnahmen zum Schutz der personenbezogenen Daten ihrer Kunden ergreifen und alle relevanten gesetzlichen Bestimmungen einhalten, da ihnen sonst schwere Strafen drohen.
- **gefragte und teure Mitarbeiter:** Die für die Ausführung komplexer Datenschutzprogramme benötigten Fachkräfte sind rar. Datenschutztechnologien erfordern kompetentes Personal, das die zahlreichen vom System gemeldeten Vorfälle bearbeiten kann. Dieses Problem verschärft sich noch, wenn ältere Datenschutzsysteme Cloud-Services wie SaaS-Anwendungen überwachen (etwas, wofür sie ursprünglich nicht konzipiert wurden). Dies führt zu mehr falsch-positiven Meldungen und einem Zusatzaufwand für das Team. Hoch qualifizierte IT-Fachkräfte verlangen je nach den von ihnen angebotenen Fähigkeiten sehr hohe Gehälter. Dadurch können Unternehmen erhebliche Kosten entstehen. Oft bleiben diese Fachkräfte aufgrund von Überlastung nicht lange in einem Unternehmen und müssen ersetzt werden, was zusätzliche Kosten verursacht.

Was ist DLP und wie kann sie helfen?

DLP-Sicherheitstechnologien sind Systeme, die die Speicherung, den Fluss und die Verwendung sensibler Daten überall in den Netzwerken

und durch die Benutzer und Services eines Unternehmens automatisch erkennen und schützen. Diese Technologie wird eingesetzt, um unterschiedliche Arten sensibler Daten zu erkennen, z. B. personenbezogene Daten/Informationen von Kunden und Mitarbeitern, Finanzdokumente und geistiges Eigentum. DLP überwacht, wie auf diese Daten zugegriffen wird und wie sie verwendet werden, um Datenverluste, eine versehentliche Offenlegung und Datendiebstahl zu verhindern. Mithilfe von DLP sind Unternehmen in der Lage, das Risiko von Datenschutzverletzungen zu verringern und ihre Dateien auf eine versehentliche Veröffentlichung von vertraulichen Informationen hin zu überprüfen. Da die Compliance-Landschaft sowohl strikter als auch weitreichender geworden ist, hat sich DLP zu einer zunehmend wichtigen Sicherheitstechnologie entwickelt, mit deren Hilfe sich Unternehmen vor kostspieligen Datenschutzverletzungen schützen und die Anforderungen der geltenden Compliance-Regelungen erfüllen können.

Warum ältere DLP-Lösungen heute nicht mehr ausreichen

Traditionelle DLP-Lösungen werden seit mehr als zehn Jahren zum Schutz von Daten eingesetzt. Mit der Zeit stellte sich jedoch heraus, dass sich diese Technologie schwer implementieren und verwalten lässt, dass sie kostspielig, ungenau und in ihrem Leistungsumfang begrenzt ist und nicht den umfassenden Schutz bietet, der im heutigen „Work-from-anywhere"-Umfeld benötigt wird. DLP-Lösungen wurden zum Schutz von Daten im Rechenzentrum und On-Premises im Unternehmen entwickelt. Diese Lösungen konnten sich nur schwer an die mit der Cloud-Ära einhergehenden Veränderungen anpassen. Ältere DLP-Lösungen sind geeignet für das, wofür sie ursprünglich entwickelt wurden. Jetzt sollen sie jedoch eine Aufgabe erfüllen, für die sie nie vorgesehen waren: die Sicherung von Daten in der Cloud oder deren Übertragung über viele Clouds hinweg. Das perimeterbasierte Sicherheitsmodell kann zudem nicht mit Daten mithalten, die über mehrere Standorte und Anwendungen verteilt sind.

Die Nachteile älterer DLP-Lösungen

Ältere DLP-Systeme, die aus mehreren Software- und Hardwarekomponenten bestehen, sind oft schwer zu implementieren und zu warten. Die Einrichtung kann komplex und kostspielig sein – nicht ideal für Unternehmen, die mit einem kleinen Budget oder begrenzten IT-Ressourcen arbeiten müssen. Die Sicherung hochgradig verteilter Unternehmen ist ebenfalls eine beträchtliche und kostspielige Aufgabe, da die On-Premises-DLP-Architektur höchstwahrscheinlich in jeder

Zweigstelle repliziert werden muss. Doch selbst dieser Ansatz lässt wichtige moderne Anforderungen unberücksichtigt, z. B. Remote-Mitarbeiter, die Cloud und die Flexibilität des BYOD-Konzepts (Bring Your Own Device).

Ältere DLP-Technologien erfordern außerdem langwierige Software-Upgrades und ständige Anpassungen. Die damit verbundenen Geschäftsunterbrechungen lassen sich nicht einfach als notwendiges Übel abtun. Diese Unterbrechungen sind der Grund, warum manche Unternehmen Upgrades oft gänzlich vermeiden. Sie verwenden DLP-Versionen, die seit Monaten oder sogar Jahren nicht mehr aktuell sind und sie nicht vor den neuesten Risiken schützen können – ganz zu schweigen von den Datenschutz- und Compliance-Anforderungen, die nicht mehr erfüllt werden.

Wird ein DLP-System nicht aktualisiert und gepatcht, können zahlreiche Probleme auftreten, die sich kein Unternehmen wünscht, darunter Sicherheitslücken, Datenschutzverletzungen und unzureichender Datenschutz. Dies gefährdet sensible Daten und kann dazu führen, dass Unternehmen die Datenschutzbestimmungen nicht mehr einhalten. Die Komplexität älterer DLP-Lösungen geht auch oft mit uneinheitlichen und unnötig komplexen Datenschutzpraktiken einher, was wiederum eine ineffiziente Nutzung der verfügbaren Zeit und Ressourcen zur Folge hat.

HINWEIS

Einige Unternehmen halten die durch ihr bestehendes DLP-System verursachten Unterbrechungen des Geschäftsbetriebs für so schwerwiegend, dass sie ihre DLP-Systeme in einen reinen Überwachungsmodus versetzen. Das System beobachtet also nur, was passiert, setzt aber keine Datenschutzrichtlinien durch. Wenn eine DLP-Lösung ohne die Durchsetzung von Richtlinien betrieben wird, ist das so, als würde man einen Safe in der Hoffnung offenlassen, dass niemand mit dem darin befindlichem Bargeld, dem Schmuck und den wichtigen Papieren das Weite sucht.

Das Problem mit falsch-positiven Ergebnissen

Ältere DLP-Systeme sind nicht nur für ihre komplizierten Implementierungen und Prozesse bekannt, sondern benötigen auch viele Ressourcen und Arbeitskräfte zu deren effektiven Überwachung und kontinuierlichen Optimierung. Ich habe bereits erwähnt, dass falsch-positive Meldungen Sicherheitsteams stark unter Druck setzen. Es lohnt sich jedoch, diese Situation etwas genauer zu betrachten.

Aufgrund der zunehmenden Anzahl von Vorfällen, die manuell bearbeitet werden müssen, sind Incident-Response-Teams nicht mehr in der Lage, alle Vorfälle zu berücksichtigen, geschweige denn zu bearbeiten.

Incident-Response-Teams erhalten viele Warnmeldungen, bei denen es sich nicht um tatsächliche Probleme handelt und denen der Kontext fehlt, um ihren Risikograd im Nachhinein bestimmen zu können. (Da die Warnmeldungen zu spät nach Eintreten eines Vorfalls eingehen, ist kein Kontext vorhanden. Teams müssen auch Vorfälle klären, die sich vor längerer Zeit ereignet haben, und selbst die Mitarbeiter, die die Vorfälle verursacht haben, können ihnen nicht helfen, da sie sich selbst nicht mehr an Einzelheiten erinnern.) Jeden Tag können Tausende, wenn nicht Hunderttausende von Warnmeldungen aus vielen unterschiedlichen Quellen eingehen. Da ständig neue Vorfälle auftreten, können Sicherheitsteams nicht auf alle Warnmeldungen eingehen; sie müssen sogar viele ignorieren, um nicht vollkommen den Überblick zu verlieren.

Entscheidend ist auch, dass Daten heute an vielen Orten außerhalb des verwalteten Rechenzentrumsnetzwerks gespeichert und übertragen werden. Ältere DLP-Lösungen sind nicht in der Lage, mit der ständig wachsenden Vielfalt und Menge an Daten Schritt zu halten. Sie verfügen weder über neuere, durch maschinelles Lernen unterstützte Erkennungsfunktionen, noch über moderne Anwendungsmöglichkeiten für die gemeinsame Nutzung von Daten. Außerdem fehlt es ihnen an Kontextsensitivität. Ihre statischen Richtlinien können nicht effektiv an neue Geschäftsrisiken und Kontexte angepasst werden, z. B. wer die Daten wie und in welcher Umgebung/Anwendungsinstanz verwendet, ob sie sich unauffällig verhalten und welches Ziel sie haben.

Automatisierungs- und Orchestrierungstools für die Cybersicherheit wie User and Entity Behavior Analytics (UEBA) wurden eingeführt, um einen Teil dieses Problems durch die Erfassung und schnellere Bearbeitung von Warnmeldungen zu lösen. Wenn ein DLP-System jedoch ungenau ist, wenn es an Geschäftskontext und Risikobewusstsein mangelt und zahlreiche Lücken vorhanden sind, funktionieren UEBA-Modelle nicht ordnungsgemäß.

Für einen wirksamen Schutz sensibler Daten sollte ein DLP-System integriert und automatisiert werden, das die Identität autorisierter Personen und Geräte, ihr Verhalten, ihr Zusammenwirken und den externen Datenaustausch, die von ihnen genutzten Anwendungen und deren Risiken sowie viele andere kontextbezogene Faktoren kontinuierlich überwacht und prüft. Dieser Zero-Trust-Ansatz (siehe Kapitel 3) ermöglicht präzise Richtlinienempfehlungen und die Erstellung von Incident-Response-Regeln, die sich an veränderte Risikobedingungen und den spezifischen geschäftlichen Kontext anpassen, in dem die Daten verwendet werden. Bei diesem Ansatz werden moderne Geschäftsabläufe nicht beeinträchtigt, sondern durch Sicherheitsfunktionen unterstützt.

Ältere DLP-Systeme bieten keine ausreichende Cloud-Abdeckung

Ältere DLP-Systeme wurden auf der Grundlage eines perimeterbasierten Sicherheitsmodells entwickelt, das davon ausgeht, dass alle Daten innerhalb des Unternehmensnetzwerks und der verwalteten Umgebungen gespeichert sind. Dieses Modell reicht im Zeitalter der Cloud nicht mehr aus, da Daten nun an mehreren cloudbasierten Standorten gespeichert sind und Benutzer und Geräte außerhalb des Unternehmensnetzwerks darauf zugreifen. Zudem sind ältere DLP-Systeme möglicherweise nicht auf die Integration mit den zahlreichen heute verfügbaren Cloud-Services und -Infrastrukturen ausgelegt, was einen umfassenden Schutz von Daten in der Cloud erschwert oder sogar unmöglich macht.

Das Hinzufügen zusätzlicher Technologien wie Cloud Access Security Broker (CASB) und cloudbasierte Secure Web Gateways (SWGs) zu einem vor Ort installierten DLP-System kann zwar einen gewissen zusätzlichen Schutz für Cloud-Repositorys bieten, doch die grundlegenden Einschränkungen des bestehenden Systems werden dadurch nicht behoben. Darüber hinaus müssen Teams mit getrennten Verwaltungskonsolen und unkoordinierten Datenschutzrichtlinien arbeiten – zwei häufige Nebeneffekte, wenn CASB und SWG zu einem bestehenden DLP-System hinzukommen.

Mit anderen Worten: Das Hinzufügen zusätzlicher Technologien zu einem veralteten DLP-System macht die Lösung nicht Cloud-fähig, sondern erhöht nur ihre Komplexität. Ein DLP-System muss in der Lage sein, die sich ständig weiterentwickelnden Standards der Cloud-Sicherheit adaptiv mit seinen eigenen dynamischen Richtlinien und Funktionen zur Risikobewertung in Echtzeit zu erfüllen, damit Unternehmen ihre Mitarbeiter, Kunden und Daten effektiv schützen können. Ältere DLP-Lösungen sind On-Premises-Lösungen. Punkt.

ERINNERUNG

Um Daten in der Cloud zu schützen, müssen ältere DLP-Lösungen auf elegante Weise mit Cloud-Sicherheitslösungen integriert werden. Daten in der Cloud brauchen auch eine Cloud-gerechte Sicherheit.

TECHNISCHES

In den meisten Unternehmen werden derzeit meist zwei Cloud-Sicherheitslösungen mit einer älteren DLP-Lösung kombiniert: CASB für den Cloud-Anwendungsdatenverkehr und SWG für den Webdatenverkehr von externen Mitarbeitern und Zweigstellen. Diese Lösungen sind zwar für die Cloud vorgesehen, haben jedoch meist nur begrenzte Datenschutzfunktionen. Durch die Integration dieser Lösungen sollen ältere DLP-Lösungen Einblicke in die Cloud erhalten, um ihre bestehenden On-Premises-Funktionen auf die Cloud auszuweiten und nach sensiblen Daten außerhalb des Rechenzentrums zu suchen. Leider hat sich

diese Integration als sehr schwierig erwiesen, da sie eine Umleitung des Netzwerkverkehrs erfordert, die auf dem sehr komplizierten Internet Content Adaptation Protocol (ICAP) beruht, das glücklicherweise nicht Gegenstand dieses Buches ist.

Selbst wenn eine Integration erreicht wird, ist dieser Ansatz nicht tragfähig. Zum einen verwenden CASBs Programmierschnittstellen (APIs), um sich mit Cloud-Anwendungen des Unternehmens wie Microsoft 365, Salesforce, Slack, Zoom, Teams, Google Workspace, Amazon Web Services (AWS) und Box zu verbinden. Die APIs bieten dem bestehenden DLP-System das gewünschte Fenster, um einen Blick in diese Cloud-Anwendungen zu werfen. Wenn sensible Daten zum Beispiel in Salesforce gespeichert sind, kann das DLP-System sie scannen und schützen. CASBs nutzen auch die Inline-Erkennung, um Daten-Uploads und -Downloads in Tausenden von SaaS-Anwendungen zu überprüfen.

Es ist nicht leicht, Datenschutzrichtlinien zwischen On-Premises- und Cloud-Systemen zu konsolidieren. Oft können CASBs zum Beispiel nicht dieselben Richtlinien duplizieren wie ältere DLP-Systeme. Die unterschiedlichen Fähigkeiten dieser Technologien führen zu fragmentierten Richtlinien und Verwaltungskonsolen, die nicht aufeinander abgestimmt sind.

Das Problem bei dieser Architektur besteht darin, dass die Integration eines On-Premises-DLP-Systems durch CASB mit einer Anwendung in der Cloud auch zu einer Verzögerung führt, die als *Latenz* bezeichnet wird. Latenz bedeutet, dass es bei einer vom DLP-System erkannten Datenverletzung in der Cloud mehrere Minuten, Stunden und sogar noch länger dauern kann, bis eine Reaktion erfolgt. Stellen Sie sich folgendes Szenario vor: Die Datenverletzung ist eingetreten, sie wurde entdeckt, doch Sie konnten sie nicht rechtzeitig stoppen (d. h. Ihre Daten sind gefährdet!).

Letztendlich kann man die Kombination von DLP mit Cloud-Technologien mit dem Versuch vergleichen, zwei völlig unterschiedliche Tiere miteinander zu kreuzen. Das eine ist ein Cloud-Service (CASB) und das andere eine umfassende On-Premises-Bereitstellung von Hardware und Software (bestehende DLP-Lösung). Das Ergebnis ist eine problematische Kreuzung, die fehleranfällig ist, hohe Latenzzeiten verursacht und sehr schwer zu optimieren und zu warten ist. Im Idealfall wollen Sie sich von dieser Komplexität befreien und alles rationalisieren und vereinfachen, damit möglichst wenig Probleme entstehen.

Die Effektivität älterer DLP-Lösungen, die an die On-Premises-Infrastruktur gebunden sind und weder schnell noch kostengünstig skaliert werden können, ist in Cloud-Umgebungen erheblich eingeschränkt. Dieser Ansatz ist einfach nicht mehr tragbar.

ERINNERUNG

Damit DLP effektiv sein kann, muss der Schwerpunkt von der äußeren Absicherung Ihres Datenbestandes auf die Daten selbst verlagert werden – und darauf, wie und wohin sie übertragen werden. Unternehmen können sich nicht mehr auf veraltete DLP-Strategien verlassen, wenn sie ihre Daten in der Cloud wirksam schützen wollen.

DLP für die Cloud-Ära

Die digitale Transformation hat die Art und Weise revolutioniert, wie Unternehmen ihren Kunden Dienstleistungen bereitstellen und Produkte und Services entwickeln. Auch die Sicherung von Daten hat sich erheblich verändert. Unternehmen jeder Größe verlassen sich verstärkt auf Cloud-Technologien, um ihr Wachstum voranzutreiben und ihr Geschäft zu optimieren; ihre Sicherheitsstrategien müssen mit diesen Veränderungen Schritt halten. Die von Unternehmen eingesetzte DLP-Architektur muss sich an die ständig zunehmende hybride Belegschaft anpassen können und zu einer „Cloud-first"-Strategie übergehen, um eine breitere Abdeckung, eine verbesserte Effizienz und Skalierbarkeit, leistungsstarke Rechenkapazitäten und effektivere Maßnahmen zur Risikoprävention bieten zu können. Mit einem optimierten DLP-Modell können moderne Unternehmen in einer hybriden Arbeitsumgebung erfolgreich sein und ihr Geschäftsmodell zukunftssicher gestalten. Die Modernisierung der DLP Ihres Unternehmens ist kein leichtes Unterfangen, Sie sollten sie aber in Betracht ziehen, da nicht nur die Risiken ständig zunehmen, sondern auch Fortschritte im Bereich Cloud-fähiger DLP-Lösungen gemacht werden.

Mit einer Cloud-DLP-Lösung ist die Bereitstellung nicht kompliziert, Sie brauchen nur einen Cloud-Service zu aktivieren. Sie müssen sich nicht mit zahlreichen Komponenten und Software befassen, die aktualisiert und manuell gewartet werden muss. Sie müssen keine DLP-Datenbanken mehr pflegen und keine Datenbankexperten einstellen. Es gibt keine DLP-Server mehr, die mit der Zeit veralten und ersetzt werden müssen. Und es gibt auch keine zu aktualisierenden Hardware-Proxys mehr.

Cloudbasierte Datenschutzplattformen sind so konzipiert, dass sie sich problemlos in Sicherheits-, Netzwerk-, Infrastruktur- und Cloud-Services integrieren lassen und gleichzeitig den Risiko- und Organisationskontext anderer Kontrollmechanismen konsistent erfassen. Datenüberwachungs- und Erkennungsalgorithmen funktionieren besser in der Cloud, wo die Belastung Ihrer Computerinfrastruktur durch den Zugriff auf unbegrenzt skalierbare Ressourcen reduziert wird. Gleichzeitig können sie mit neueren Anwendungsfällen und Ihren unzähligen, ständig zunehmenden Endpunkt-Agenten Schritt halten. Sie sind nicht mehr durch eine On-Premises-Infrastruktur eingeschränkt, und Ihre Benutzer sind überall geschützt.

Da eine in der Cloud bereitgestellte Architektur nicht an Ihre Infrastruktur und Ihren Zeitplan gebunden ist, bleibt Ihre DLP-Lösung zudem immer auf dem neuesten Stand, da Echtzeit-Updates überall verfügbar sind. Dieser Ansatz schafft die Grundlage für ein viel effizienteres Tool zum Schutz Ihrer wertvollen Unternehmensdaten.

Mit Mythen aufräumen

Es ist kein Geheimnis, dass der Markt für Cloud-DLP-Lösungen von Schlagwörtern, hochtrabenden Versprechungen und technischem Fachjargon geprägt ist. Kein Wunder, dass sich viele Anwender von den verfügbaren Optionen überfordert und verunsichert fühlen. Tatsache ist jedoch, dass nicht alle DLP-Lösungen gleich sind. In diesem Buch zeige ich Ihnen, wie Sie bei der Auswahl einer Lösung zwischen Fakten und Marketing-Hype unterscheiden können. Außerdem werde ich Ihnen die wichtigsten Merkmale und Funktionen der einzelnen Lösungen vorstellen.

Zunächst wollen wir einige weit verbreitete Mythen rund um den Datenschutz aus der Cloud widerlegen, damit Sie sich einen Überblick verschaffen und eine fundierte Entscheidung treffen können, die perfekt auf Ihr Unternehmen zugeschnitten ist.

Mythos: Neue DLP-Lösungen sind die besten

Die Realität: Wenn es um Datenschutzprogramme geht, sollten Sie nichts dem Zufall überlassen. Um die nötige Sicherheit zu gewährleisten, brauchen Sie nicht nur ausreichende Funktionen im Programm, sondern auch einen engagierten und sachkundigen Anbieter mit fundierter Erfahrung im DLP-Bereich. Ältere DLP-Lösungen wurden zwar nicht mit Blick auf Cloud-Technologie entwickelt, doch in puncto Reife können die meisten Cloud-DLP-Lösungen einiges von ihnen lernen.

Die zuverlässigsten Datenschutzlösungen haben eine lange Reifezeit hinter sich und sind im Laufe der Zeit mit neuen Funktionen ausgestattet worden. Wenn Sie Investitionen in ein umfassendes Datenschutzprogramm in Erwägung ziehen, sollten Sie sich vergewissern, dass Ihr Anbieter alle Ihre Anforderungen – von Cloud-Support bis zur Funktionsreife – erfüllen kann, um die höchste Datensicherheit zu gewährleisten. Die neueste Anbieterlösung ist also nicht unbedingt die beste Lösung.

Mythos: Bisherige DLP-Lösungen waren ungenau

Die Realität: Die bisherigen DLP-Lösungen wurden von Anbietern entwickelt, die mindestens ein Jahrzehnt in die Entwicklung präziser

Algorithmen und Richtlinien investiert haben, die eine unbefugte Übertragung von sensiblen Daten erkennen und verhindern.

Genauigkeit ist nicht der Kern des Problems. Wie bereits in diesem Kapitel erwähnt, hat das eigentliche Problem viel mehr mit falsch-positiven Ergebnissen zu tun. Falsch-positive Meldungen können zu gefährlichen Situationen führen, in denen echte Bedrohungen unbemerkt bleiben und sensible Daten versehentlich offengelegt werden. Dies führt auch dazu, dass qualifizierte (d. h. teure) Incident-Response-Teams immer größer werden, um die zunehmende Anzahl von Vorfällen bewältigen zu können. In Kapitel 2 erkläre ich, warum DLP-Systeme präzise und genau sein müssen, um Vertrauen herzustellen.

Mythos: Bei DLP ist „gut genug" ausreichend

Die Realität: Wenn es um den Schutz der Daten Ihres Unternehmens geht, sollten Sie nicht an der falschen Stelle sparen. Würden Sie eine Cloud-Lösung in Betracht ziehen, die verspricht, dass die von ihr gebotene Sicherheit gerade einmal „gut genug" ist? Wahrscheinlich nicht! Sonst müssten Sie sich vielleicht mit einem reduzierten Funktionsumfang und einer oberflächlichen Prüfung von Angriffsvektoren und Datentypen abfinden – und mit einem erhöhten Risiko bösartiger Aktivitäten, falsch-positiver Ergebnisse und einer ungenauen Erkennung.

Investieren Sie stattdessen in ein modernes Cloud-DLP-System, das eine hohe Genauigkeit bei der Datenerkennung bietet, zusätzliche Sicherheitsebenen bereitstellt und einen umfassenden Schutz vor möglichen Bedrohungen Ihrer Geschäftsdaten oder anderer vertraulicher Materialien gewährleistet. Es versteht sich von selbst, dass Sie nicht leichtfertig mit den Daten Ihres Unternehmens umgehen wollen. Investieren Sie deshalb in das richtige DLP-System, das Ihnen die höchste Sicherheit und Leistung bieten kann.

Mythos: Cloud-DLP-Lösungen sind weniger leistungsfähig als ältere DLP-Lösungen

Die Realität: Derzeit verwenden viele Cloud-DLP-Systeme weniger als 100 Datenkennungen (siehe Kapitel 2) und scannen nur wenige Dateitypen, d. h. sie können kaum etwas erkennen. Der Grund? Die Technologie hat einfach noch nicht den nötigen Reifegrad. Im Gegensatz zu DLP-Systemen, die bereits seit einem Jahrzehnt genutzt und weiterentwickelt werden, wurden diese Systeme speziell für neue Anwendungsfälle entwickelt, z. B. für bestimmte Cloud-Anwendungen, und schützen daher nur wenige gängige Dateitypen. Aufgrund dieser mangelnden Fokussierung fehlt ihnen die nötige Genauigkeit, um Datenschutz und Geschäftsanforderungen effektiv miteinander in Einklang

zu bringen, was zu anhaltenden Reibungen zwischen beiden Bereichen führt. Cloudbasierte DLP-Technologie ist älteren DLP-Technologien schon deshalb überlegen, weil sie eine enorme Skalierbarkeit bietet. Mit einer derartigen Skalierbarkeit sollte es möglich sein, falsch-positive Meldungen zu beseitigen und die Genauigkeit insgesamt zu verbessern.

HINWEIS

Wenn es um Datenschutz geht, gilt der altbekannte Spruch: „Erfahrung zählt!“ Auch wenn verlockende neue Optionen – auf dem Papier oder auf den ersten Blick – großartig aussehen, bieten ausgereifte DLP-Lösungen ein höheres Maß an Sicherheit und Transparenz, da sie im Laufe der Zeit gewachsen sind und ständig verbessert wurden. Entscheiden Sie sich für einen bewährten Anbieter und testen Sie selbst mehrere Systeme, damit Sie sich beim Schutz Ihrer wichtigen Daten absolut sicher fühlen können.

Mythos: Ein Bündel von Datensicherungssystemen ist genauso gut wie eine vollständige, integrierte Datenschutzlösung

Die Realität: Sicherheitsinitiativen und -programme, die versuchen, eine Vielzahl unterschiedlicher DLP-Produkte und -Services von mehreren Anbietern zu bündeln, können zunächst logisch erscheinen. Schließlich sind DLP-Services oft bereits in SaaS-Anwendungen, Public-Cloud-Services, Firewalls und SWG-Lösungen integriert. Früher oder später werden sich diese Multiservice-Datenschutzprogramme jedoch in puncto Sicherheit als unzureichend erweisen. Durch die Zusammenführung einzelner Systeme, die nicht gemeinsam entwickelt wurden, bieten derartige Lösungen nur eingeschränkte Einblicke in den Geschäftskontext und vorhandene Risiken. Darüber hinaus müssen Datenschutzverantwortliche mit unzusammenhängenden Datenschutzrichtlinien und mehreren Konsolen arbeiten. Der Anwendungsbereich jedes integrierten DLP-Services ist oft auf bestimmte Umgebungen und Kanäle beschränkt und deckt z. B. nur den Webverkehr oder bestimmte Kontrollpunkte wie eine oder mehrere SaaS-Anwendungen ab. So sind Ihre Daten angreifbar, sobald sie in die Öffentlichkeit gelangen.

Um sich und Ihr Unternehmen zu schützen, sollten Sie nach vollständig integrierten Lösungen Ausschau halten, die einen umfassenden Datenschutz bieten, um alle potenziellen Risikobereiche über Cloud-Services, On-Premises-Umgebungen, E-Mail-Services und Endpunkte hinweg abzudecken und eine vollständige Absicherung über unterschiedliche Arten von Daten und Kontrollmechanismen hinweg zu gewährleisten.

IN DIESEM KAPITEL

- Informationen zu Herausforderungen älterer DLP-Lösungen
- Vorbereitung auf zukünftige Veränderungen und Wachstum
- Vorteile und Einschränkungen cloudbasierter DLP-Lösungen
- Wie DLP die Effektivität anderer Sicherheitstools erhöht

Kapitel 2
Schutz für das gesamte Cloud-zentrierte Unternehmen

Warum ist es so wichtig, Datenschutzsysteme einzusetzen, die das gesamte Unternehmen, einschließlich seiner Cloud-Anwendungen, schützen? Weil der unbefugte Zugriff auf Daten oder ihr Verlust schwerwiegende Folgen für Unternehmen und ihre Stakeholder haben kann. Das klingt wie eine Selbstverständlichkeit, doch leider gibt es in der Praxis viele Faktoren, die diesem Ziel entgegenwirken. In diesem Kapitel erkläre ich, warum die Umsetzung eines vollständigen Datenschutzes für Ihr ganzes Unternehmen ein Prozess ist, der schnelle Resultate und langfristige strategische Vorteile bringt.

Unternehmen ohne Grenzen

Noch vor einem Jahrzehnt wurde das Konzept „Unternehmen“ weitgehend durch die physischen Grenzen eines Gebäudes oder Standorts definiert und umfasste in der Regel die Mitarbeiter, Ausrüstung und Ressourcen, die sich innerhalb dieser Grenzen befanden. Im Laufe der Zeit veränderte sich die Art der Geschäftstätigkeit, Technologien entwickelten sich weiter und die Definition des Unternehmens musste an diese neuen Gegebenheiten angepasst werden. Heute sind Unternehmen nicht mehr an einen physischen Standort gebunden.

Remote-Arbeit wird immer mehr zur Norm und wertvolle Unternehmensdaten haben nun die Geräte und Heimnetzwerke Ihrer Mitarbeiter erreicht. Aufgrund der zunehmenden Verbreitung von Cloud-Services

sind Ihre Daten möglicherweise über eine Vielzahl von Cloud-Speicherorten verteilt, einschließlich Software-as-a-Service (SaaS)-Anwendungen wie Microsoft 365 und Salesforce sowie in Online-Gesprächen auf Collaboration-Anwendungen wie Slack und Microsoft Teams (siehe Abbildung 2-1). Zum Unternehmen gehören nun auch die zahlreichen Endpunkte, mit denen Mitarbeiter auf Unternehmensressourcen zugreifen, sowie die Tausenden von genehmigten und (manchmal auch nicht genehmigten) Cloud-Anwendungen, die in Unternehmen genutzt werden können.

HINWEIS

Wenn Sie nicht wissen, welche sensiblen Daten Sie haben und wo sie sich befinden, können Sie diese Daten nicht schützen. Wenn Sie wissen, dass sensible Daten vorhanden sind, aber nicht, wo sie sich befinden und wohin sie übertragen werden, können Sie sie ebenfalls nicht schützen.

ERINNERUNG

Sie brauchen einen ganzheitlichen Ansatz zur Erkennung und zum Schutz von Daten, um zu gewährleisten, dass alle sensiblen Daten unabhängig von ihrem Speicherort und ihrem Übertragungsweg erkannt und geschützt werden. Ihre Sicherheitssysteme dürfen keine „blinden Flecken" aufweisen, die es möglich machen, Daten ohne Ihr Wissen auszuschleusen oder versehentlich offenzulegen.

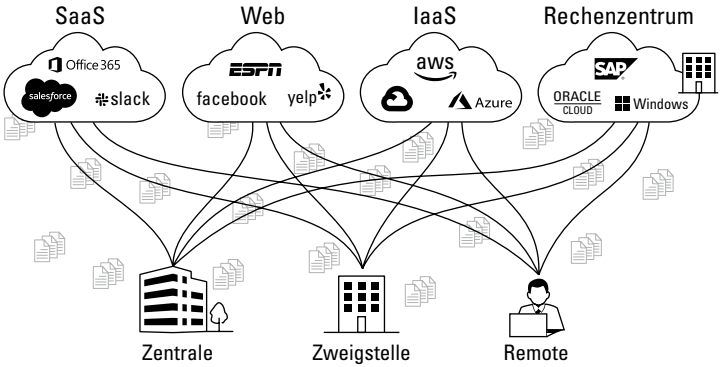

ABBILDUNG 2-1: In einem modernen, hochgradig verteilten Unternehmen werden Daten in vielen neuen Umgebungen gespeichert und übertragen.

DLP – Entwicklung und Herausforderungen

Wie in Kapitel 1 erläutert, waren DLP-Systeme bisher hauptsächlich auf den Schutz von Daten ausgerichtet, die *im* Rechenzentrum des Unternehmens gespeichert wurden. Heute können sich Daten an den unterschiedlichsten Orten befinden und müssen dort geschützt werden – sei es in der Cloud, auf Remote-Geräten, im Unternehmensnetzwerk oder

an externen Standorten. Ältere DLP-Systeme, die für den Schutz von Daten innerhalb der Unternehmensgrenzen entwickelt wurden, reichen daher nicht mehr aus.

ERINNERUNG

Sie müssen nach wie vor alle Orte kennen, an denen Ihre Daten gespeichert sind und an die sie übertragen werden. Wenn Sie jedoch den Schwerpunkt Ihres Datenschutzes auf die Daten selbst verlagern und nicht ihren Ursprungs- und Speicherort in den Mittelpunkt stellen, können Sie enorme Vorteile in Bezug auf Flexibilität und Effektivität erzielen. Man kann sich das wie ein Basketballteam vorstellen, das von der Zonenverteidigung zur Manndeckung übergeht. Wie ich später noch erläutern werde, können Sie Ihre sensiblen Daten mit diesem ganzheitlichen Ansatz zuverlässig schützen und verhindern, dass sie in die falschen Hände geraten.

Eine Lösung, die ein bestehendes DLP-System ersetzen soll, muss einen vollständigen Schutz für das gesamte Unternehmen bieten können – nicht nur für die klassischen lokalen Kanäle, sondern auch für Cloud-Kanäle. Selbst moderne Cloud-DLP-Lösungen sind meist nur für den Schutz bestimmter Kanäle vor Ort vorgesehen. Sie können ein Netzwerk, eine bestimmte Anzahl von Endpunkten oder spezifische Anwendungen schützen, decken jedoch nicht die ganze Vielfalt moderner Anwendungsfälle ab.

Um einen vollständigen Schutz des gesamten Unternehmens zu gewährleisten, muss eine DLP-Lösung alle Daten bei der Übertragung zu und von jedem Standort und Gerät schützen. Dies umfasst verwaltete und nicht verwaltete Geräte an allen Aufenthaltsorten von Benutzern – sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks – sowie in SaaS-Anwendungen, Infrastructure-as-a-Service (IaaS), E-Mail, privaten Anwendungen und Endpunkten. Um dies zu erreichen, ist eine umfassende und flexible DLP-Lösung erforderlich, die den sich ständig ändernden Anforderungen eines stark verteilten Unternehmens gerecht wird.

In den folgenden Abschnitten werde ich auf die wichtigsten Überlegungen eingehen, die bei der Entwicklung einer DLP-Lösung für das moderne Unternehmen ohne Grenzen zum Tragen kommen.

Skalierbarkeit und Zukunftssicherheit

Vor nicht allzu langer Zeit hielt sich die Nutzung von SaaS-Anwendungen im Unternehmen noch in Grenzen, doch mit der Zeit begannen immer mehr Mitarbeiter, SaaS-Anwendungen zu nutzen. Heute verwenden Unternehmen nicht selten Hunderte von genehmigten SaaS-Anwendungen. Hinzu kommen die von Mitarbeitern genutzten Anwendungen, von deren Existenz das Unternehmen nicht einmal

etwas weiß. Diese Zahl geht möglicherweise in die Tausende – ein beängstigender Gedanke!

TIPP

Skalierbarkeit ist nicht nur wichtig, um aktuelle Anforderungen zu erfüllen, sondern auch, um auf zukünftiges Wachstum und potenzielle Veränderungen vorbereitet zu sein. Für die Entwicklung flexibler, agiler Lösungen, die mit einer ständig steigenden Workload oder einer kontinuierlichen Erweiterung umgehen können, ohne Kompromisse in puncto Leistung oder Funktionalität einzugehen, ist ein vorausschauender Ansatz unerlässlich. Skalierbarkeit trägt dazu bei, dass Ihre Systeme auch bei unvorhergesehenen Veränderungen effektiv und effizient bleiben.

Dabei geht es jedoch nicht nur um den Schutz von Daten in neuen Umgebungen und an neuen Orten. Skalierbarkeit bedeutet auch, mit der zunehmenden Geschwindigkeit, Vielfalt und Menge von Daten Schritt halten zu können. Heutzutage wird eine noch nie dagewesene Menge an Daten erzeugt und gesammelt. Wegen der zunehmenden Verbreitung von Collaboration-Anwendungen und Onlinetools können Daten jetzt auch in Form von Gesprächen vorliegen, z. B. in Anwendungen wie Slack, Teams und Zoom, in cloudbasierten E-Mail-Anwendungen wie Gmail oder in Form von Bildern, z. B. als Fotos und Screenshots. Oft ist es einfacher, einen Screenshot von wichtigen Informationen anzufertigen, als sie zu kopieren und in ein Dokument einzufügen. Skalierbarkeit ermöglicht den Schutz unterschiedlichster Datenformate bei allen erwähnten Anwendungsfällen – und sogar bei jenen, die überhaupt noch nicht entwickelt wurden!

ERINNERUNG

Im Abschnitt „Moderne DLP in Aktion“ in diesem Kapitel wird ausführlich auf die Funktionsweise von DLP-Systemen eingegangen. Denken Sie daran, dass die grundlegende Funktion eines DLP-Systems darin besteht, sensible Daten zu erkennen und zu schützen.

Wie DLP vom Helden zum Sorgenkind wurde

Als Unternehmen damit begannen, Cloud-Anwendungen einzuführen und an neue Standorte zu expandieren, wurde es immer schwieriger, ältere DLP-Systeme einzusetzen. Da diese Systeme für die Installation und Wartung vor Ort vorgesehen waren, mussten sie an jedem neuen Standort und in jeder neuen Niederlassung dupliziert und installiert werden. Dies erhöhte die Komplexität und machte zusätzliche Ressourcen wie neue Hardware erforderlich, während der Wartungs- und Personalaufwand zunahm. Der anhaltende Trend zur Remote-Arbeit machte die ganze Sache nicht einfacher, da Arbeitnehmer nun von einer Vielzahl unterschiedlicher Geräte und Standorte aus auf sensible Daten zugreifen konnten. Alle diese Faktoren machten die effektive Verwaltung von DLP-Systemen für Unternehmen immer schwieriger, was wiederum zu höheren Kosten und potenziellen Sicherheitsrisiken führte.

Haben Sie sich jemals davor gescheut, ein Software-Update auf Ihrem Smartphone oder Laptop durchzuführen, weil sie befürchteten, dass eine Ihrer Lieblingsanwendungen danach nicht mehr funktionieren oder dass ein anderes lästiges Problem auftreten könnte? Nun stellen Sie sich vor, Sie müssten Ihre bestehende DLP-Software für zahlreiche Server und Zweigstellen sowie für Tausende von Mitarbeitergeräten aktualisieren. Kein Wunder, dass manche Kunden an älteren Versionen ihrer DLP-Software festhalten – das ist mit viel weniger Arbeit verbunden als der Versuch eines Updates.

HINWEIS

Wenn Sie keine regelmäßigen Upgrades durchführen, bleiben Ihre Daten ungeschützt und das Risiko von Compliance-Verstößen und Datenschutzverletzungen nimmt zu.

DLP muss nicht härter, sondern intelligenter arbeiten

Ältere DLP-Systeme scannen alle Datenformate und erkennen sensible Informationen, die geschützt werden müssen. Diesem Ansatz liegt die Idee zugrunde, dass nur sensible Daten geschützt werden müssen, da der Schutz aller anderen Daten die Produktivität beeinträchtigen kann. Es ist zwar wichtig, zu verhindern, dass bestimmte sensible Daten per E-Mail an Dritte weitergegeben werden, doch das bedeutet nicht, dass die gesamte E-Mail-Kommunikation mit Dritten geschützt werden muss. Dadurch können nämlich Verzögerungen auftreten, die die Kommunikation und Zusammenarbeit behindern, und zu viele Warnmeldungen für das Incident-Response-Team erzeugt werden. Oft erlauben Unternehmen ihren Mitarbeiter sogar, Unternehmensressourcen für nicht arbeitsbezogene Aktivitäten zu nutzen, z. B. zum Hochladen persönlicher Bilder in soziale Medien, solange der Inhalt nicht sensibel ist und keine Unternehmensgeheimnisse enthält. Da ältere DLP-Systeme aus Software- und Hardwarekomponenten bestehen, müssen zusätzliche Erkennungsserver, Module und größere Datenbanken bereitgestellt werden, um den gesamten Webverkehr und alle Datei-Repositorys zu scannen und nach sensiblen Daten jeder Art zu suchen.

Da sie vor Ort eingesetzt werden, sind ältere DLP-Systeme auf Hardware-Rechenressourcen angewiesen, die zwangsläufig begrenzt sind. Die auf den Computern von Mitarbeitern installierte Endpunkt-DLP-Software ist zum Beispiel bewusst mit eingeschränkten Datenerkennungsfunktionen ausgestattet und verlässt sich auf einfache Erkennungsmodule, die weniger ressourcenintensiv sind. Sie kann zwar einige sensible Daten auf Endpunkten aufspüren, ist jedoch nicht in der Lage, fortschrittliche Erkennungsmethoden einzusetzen, sodass beträchtliche Mengen an sensiblen Daten unentdeckt bleiben können. Ältere DLP-Systeme können zum Beispiel keine fortschrittlichen Technologien nutzen, die umfangreiche Verarbeitungsressourcen wie maschinelles Lernen (ML) und Exact Data Matching (siehe nächster Abschnitt). In der Cloud bereitgestellte DLP verlagert

ressourcenintensive Aktivitäten in die Cloud und setzt sie gleichzeitig auf dem Endpunkt durch. Die Skalierbarkeit dieses Ansatzes stellt eine erhebliche Verbesserung dar und ermöglicht es DLP-Systemen, Fingerabdrücke von Daten zu erstellen, z. B. von bestimmten Namen, Sozialversicherungsnummern und anderen sensiblen Details in Verbindung mit bestimmten Personen.

ERINNERUNG

Die Cloud kann die für die Bereitstellung dieser Erkennungsfunktionen erforderliche nahezu unbegrenzte Skalierbarkeit bieten. DLP-Systeme können sich dann auf die wichtigsten Daten konzentrieren und diese vor unbefugtem Zugriff schützen können.

Präzision ist gefragt

Einer der verbreiteten Mythen, die ich in Kapitel 1 erwähnt habe, bezieht sich auf die Ungenauigkeit älterer DLP-Lösungen. Genauigkeit ist hierbei jedoch nicht das eigentliche Problem, oder zumindest nicht das größte. Das Hauptproblem sind falsch-positive Ergebnisse (ebenfalls in Kapitel 1 besprochen), die hauptsächlich auf fehlenden Kontext zurückzuführen sind. Natürlich sind ältere DLPs angesichts der wachsenden Datenmenge überfordert, die sich auf eine zunehmende Anzahl von Geräten und Anwendungen außerhalb der Unternehmensgrenzen ausbreitet. Gleichzeitig wird die Erkennung sensibler Daten aufgrund der Zunahme von Datentypen immer schwieriger, worunter die Genauigkeit litt. Das Hauptproblem besteht jedoch darin, dass ältere DLP-Lösungen in der Regel zu restriktiv sind. Sie melden positive Aktionen als Verstöße und blockieren sie sogar, ohne den geschäftlichen Kontext oder das Risikoniveau zu verstehen. In einer Welt, in der die Zusammenarbeit für die neue Art der Geschäftsabwicklung unerlässlich ist, gibt es zu viele dieser falsch-positiven Ergebnisse.

Eine DLP-Lösung darf keine Reibungen für das Unternehmen verursachen und den für nutzbringende Geschäftsabläufe erforderlichen Datenfluss nicht beeinträchtigen. Wenn ein Mitarbeiter zum Beispiel eine Datei an einen vertrauenswürdigen Auftragnehmer senden möchte, der gerade an einem wichtigen Projekt arbeitet, sollte diese Übertragung nicht durch das DLP-System verhindert werden. Im Idealfall sollten Incident-Response-Teams mithilfe eines DLP-Systems effektiver arbeiten können, da legitime Meldungen über potenzielle Datenverluste hervorgehoben und falsch-positive Meldungen herausgefiltert werden.

Genauigkeit und Präzision gehörten nicht zu den Hauptproblemen älterer DLP-Systeme, doch bei den weniger ausgereiften neuen cloudbasierten DLP-Lösungen sind sie es durchaus. Dabei sind zwei Aspekte zu berücksichtigen:

- Ungenauigkeit bei der Datenerkennung führt dazu, dass zu viele Daten unnötig geschützt werden, d. h. zu viele Daten werden als

sensibel eingestuft, obwohl sie es gar nicht sind. Dadurch kann es passieren, dass eine legitime Geschäftskommunikation verhindert wird.

- Unter Umständen gibt es keine ausreichenden Erkennungsmethoden, um Daten zu identifizieren, die tatsächlich sensibel sind – also fehlende sensible Daten – z. B. bestimmte Dateitypen wie Bilder oder komprimierte Formate, Passnummern, Gesundheitsdaten, internationale Weiterleitungsnummern und länderspezifische nationale IDs, weil das System nicht in der Lage ist, diese Datenformate und Dateitypen zu identifizieren.

ERINNERUNG

DLP-Systeme müssen präzise und genau sein, damit das Unternehmen weiß, dass es sich auf sie verlassen kann. Sie dürfen nur jene Datenübertragungen melden und blockieren, die tatsächlich bösartig sind, und nicht zu viele falsch-positive Meldungen erzeugen.

Hauptbestandteil 1: Datenkennungen

Datenkennungen werden verwendet, um sensible Informationen wie Sozialversicherungs- oder Kreditkartennummern auf der Grundlage von generisch beschriebenen Inhalten wie regulären Ausdrücken (auch als *Regex* bezeichnet) zu finden. Dies ist ein leistungsstarkes Tool, mit dem DLP-Systeme automatisch bestimmte Datentypen anhand von natürlichen, alltäglichen Begriffen, Ausdrücken und Mustern identifizieren können („nach einer neunstelligen Zahl suchen"). Möglicherweise handelt es sich bei der Zahl um eine Sozialversicherungsnummer, aber wie können Sie das mit Sicherheit wissen?

Datenkennungen ermitteln die Antwort mithilfe spezieller Regeln, die auf der Anzahl von Ziffern, Textmustern, Sequenzen, Trennungen und begriffsnahen Schlüsselwörtern (wie Sozialversicherungsnummer [SVNR], Passwort [PW], Kartenprüfnummer [CVV] und so weiter) basieren, um diese Nummern zu erkennen und zu schützen. Hier sind einige wichtige Punkte, die Sie in Bezug auf Datenkennungen beachten sollten:

- Es werden Tausende von vordefinierten Datenkennungen und die Fähigkeit benötigt, diese an Ihr Unternehmen anzupassen, um Ihre Informationen zuverlässig zu schützen und die geltenden Governance-Regeln zu erfüllen. Wichtig ist auch die Fähigkeit, benutzerdefinierte Datenkennungen zu bearbeiten oder zu erstellen – jedes Unternehmen hat andere sensible Informationen, die geschützt werden müssen.
- Datenkennungen müssen Tausende von Dateitypen (Word, XLS, JPG, PNG, PDF, CSV, ZIP, RAR usw.), -formaten und -kategorien unterstützen (Bild, Analyse, archiviert and komprimiert, Tabellenkalkulation, Audio, Video, Datenbank usw.). Siehe hierzu Kapitel 1.

- Sie müssen eine Vielzahl von länderspezifischen Identifikationsnummern (z. B. internationale Bankdaten, Adressen, Postleitzahlen, nationale Ausweisnummern, Passnummern und Telefonvorwahlen) sowie Profile zur Einhaltung von Vorschriften und Datenschutzbestimmungen unterstützen, um sicherzustellen, dass die DLP-Lösung mit den neuesten Governance-Anforderungen Schritt halten kann.

TIPP

Damit Ihr DLP-System funktioniert, benötigt es Tausende von Datenkennungen. Damit können potenziell sensible Daten genau identifiziert und gekennzeichnet werden, unabhängig davon, in welchem Staat, in welcher Region oder in welchem Land sie sich befinden.

Hauptbestandteil 2: Exact Data Matching (EDM)

EDM ist ein Verfahren zum Auffinden bestimmter strukturierter Informationen in Quellen wie Tabellenkalkulationen und Datenbanken. Mit EDM kann eine DLP-Lösung Fingerabdrücke und Indizes von vertraulichen Kunden- und Mitarbeiterdatensätzen erstellen, die zur Identifizierung einer Person anhand ihres vollständigen Namens, ihrer Sozialversicherungsnummer, ihrer Adresse und anderer Identifikationsnummern verwendet werden können. EDM kann auch bei der Suche nach Finanzdaten eingesetzt werden, die Aufschluss über die Vermögensverhältnisse einer Person geben, z. B. Kreditkarten- oder Kontonummern. Die Lösung kann sogar für Gesundheitsdaten und Datenbanken zur Produktidentifizierung und Preisgestaltung verwendet werden. Mit EDM ist eine DLP-Lösung in der Lage, diese Informationen zu indizieren, damit sie später überall auffindbar sind. EDM ist jedoch nur dann effektiv und genau, wenn unterschiedliche indizierte Daten abgeglichen und Datenfelder aus einem bestimmten Datensatz miteinander kombiniert werden. Die Technologie muss auch in der Lage sein, Milliarden von Datensätzen zu indizieren, um expandierende Unternehmen mit ihren wachsenden Datenbanken und die ständig zunehmende Menge an verfügbaren Informationen zu unterstützen. Deshalb ist der Bearbeitungsumfang für EDM so wichtig.

Hauptbestandteil 3: Erweiterte Datenerkennungsfunktionen

Es gibt heute mehr Datentypen und Arten der Datenübertragung als je zuvor. Unternehmen benötigen daher DLP-Systeme, die in der Lage sind, sensible Informationen präzise zu erkennen. *Erweiterte Erkennungsfunktionen* ist eine Art Sammelbegriff, der sich auf Funktionen wie die folgenden bezieht:

- **Optische Zeichenerkennung (Optical Character Recognition, OCR) und auf künstlicher Intelligenz (KI) basierende Bilderkennung:** Beim Schutz von Daten spielen diese Funktionen eine zunehmend

wichtige Rolle. Heute ist es ein Kinderspiel, Dokumente, Formulare, Ausweise, Whiteboards und Bilder von anderen Bildern zu fotografieren. Oft werden Screenshots oder Schnappschüsse angefertigt, um schnell bestimmte Informationen festzuhalten und mit Kollegen zu teilen. Dank OCR können DLP-Lösungen Text aus einem Bild extrahieren und dann eine Datenklassifizierung auf der Grundlage der vorhandenen Erkennungsrichtlinien vornehmen.

- **KI und ML:** Dank hoch entwickelter Erkennungsmethoden können KI- und ML-Bildklassifizierungsverfahren gängige Datei- und Dokumententypen wie Kreditkarten, Steuerformulare, Geheimhaltungsvereinbarungen, Formulare für Fusionen und Übernahmen und Patente erkennen, ohne deren Inhalte extrahieren zu müssen. Mithilfe dieser Methoden lassen sich unscharfe oder beschädigte Inhalte erkennen, auch wenn die Informationen schwer lesbar sind. Das ist möglich, weil die Algorithmen darauf trainiert sind, für jede Art von Dokument spezifische Muster und Merkmale zu erkennen, z. B. die verwendeten Layouts, Schriftarten und Farben. Außerdem können sie den Kontext berücksichtigen, in dem das Dokument verwendet wird. Dadurch kann die KI das Dokument auch unter schwierigen Bedingungen genau klassifizieren, wie z. B. bei schlechter Bildqualität oder wenn Dokumente beschädigt sind.
- **Fingerprinting von Dateien und Dokumenten:** Diese Methode ist ein unerlässliches Hilfsmittel für Unternehmen, um die Sicherheit und Vertraulichkeit ihrer geschäftskritischen Dokumente und hochsensiblen Dateien zu gewährleisten. Durch die Indizierung des gesamten Dokuments und die Erkennung exakter oder teilweiser Kopien des Inhalts können Unternehmen die unbefugte Weitergabe und Vervielfältigung ihrer vertraulichen Informationen (z. B. Dokumente über Fusionen und Übernahmen, Vorabinformationen, technische Entwürfe oder investorenbezogene Daten) verhindern. Diese Methode ist besonders nützlich, um Kopien sensibler Dateien in risikoreichen Umgebungen und Übertragungskanälen zu erkennen, z. B. bei ausgehenden E-Mails und beim Hochladen von E-Mails auf persönliche Anwendungsinstanzen.

Als sich alles noch vor Ort befand, lieferten ältere DLP-Lösungen in dieser Hinsicht tatsächlich einige gute Ergebnisse, doch jetzt stoßen sie eindeutig an ihre Grenzen. Sie bieten einfach keine ausreichende Rechenleistung und Skalierbarkeit.

Hauptbestandteil 4: Viel Kontext und ein Zero-Trust-Datenschutzmodell

So wie sich die Wellen des Meeres unaufhörlich bewegen und verändern, so sind auch die Menschen, Netzwerke, Anwendungen, Daten

und Governance-Regeln im Unternehmen stets im Wandel begriffen. Um potenziellen Risiken einen Schritt voraus zu sein, müssen sich DLP-Systeme und die dazugehörigen Strategien schnell und effektiv an die sich ändernde Datenlandschaft anpassen und auf Entwicklungen reagieren können. Dieses Konzept wird auch als *Kontextverständnis* bezeichnet. Dank dieser Flexibilität ist das DLP-System in der Lage, sensible Daten effektiv zu schützen, das Risiko von Datenschutzverletzungen zu minimieren und die Einhaltung einschlägiger Vorschriften zu gewährleisten, ohne die Benutzerproduktivität zu beeinträchtigen und die Geschäftskontinuität einzuschränken.

Um eine solche Nuancierung und Flexibilität zu erreichen, sollte eine in der Cloud bereitgestellte Datenschutzplattform in die übergreifende Sicherheits- und Netzwerkinfrastruktur des Unternehmens integriert werden. Die DLP-Plattform sollte auch kontinuierlich Informationen aus unterschiedlichen Quellen erfassen, z. B. Identitätsmanagement, Verhaltensanalyse, Netzwerkprotokolle, Cloud-Sicherheitstools, Bedrohungsanalyse, Netzwerksicherheit, SaaS- und Cloud-Sicherheitsstatus, Cloud Access Security Brokers (CASB)-nativen Cloud Confidence Indexes und Endpunktsicherheitsstatus. Diese Informationen können dann verwendet werden, um die konkreten Umstände des Zugriffs auf sensible Daten, den geschäftlichen Kontext und die damit verbundenen potenziellen Risiken genau zu identifizieren und dadurch die angemessene Zugriffsstufe und die richtigen Maßnahmen für den Schutz der jeweiligen Daten festzulegen. Dies geschieht auf der Grundlage von Faktoren wie der Identität, dem Aufenthaltsort und dem Verhalten der Person, der Sicherheit ihres Geräts, der Vertrauenswürdigkeit des Netzwerks, dem Ruf der verwendeten Anwendung, dem endgültigen Ziel der Datenübertragung usw.

TIPP

Eine risiko- und kontextbewusste Datenschutzplattform, kann sich stets an die jeweiligen Gegebenheiten anpassen und effizient und präzise auf Vorfälle reagieren.

Kapitel 3 befasst sich mit dem Zero-Trust-Konzept und der entscheidenden Rolle, die es bei der effektiven DLP spielt. Denken Sie daran, dass Zero Trust eine grundlegende Sicherheitsstrategie ist, die davon ausgeht, dass alle Benutzer, Geräte und Netzwerke in der Umgebung eines Unternehmens potenziell bösartig sind und jederzeit mit Vorsicht behandelt werden sollten.

Das bedeutet, dass jeder Zugriff auf Ressourcen und Systeme streng kontrolliert und überprüft wird, ganz gleich, ob sich der Benutzer oder das Gerät innerhalb oder außerhalb des Netzwerkperimeters befindet. Der Kontext ist die Basis für eine Zero-Trust-Strategie, da das DLP-System mit seiner Hilfe fundierte Entscheidungen darüber treffen kann, wann es datenbezogene Aktivitäten zulassen soll und wann nicht.

ERINNERUNG

Die Nutzung integrierter Sicherheitslösungen und ergänzender Datenschutztechnologien ist der entscheidende Unterschied zwischen einem Datenschutz-Tool und einer echten Datenschutz-Plattform.

Moderne DLP in Aktion

DLP ist das Herzstück des Informationssicherheitssystems eines Unternehmens und erhöht die Effektivität anderer Sicherheitstools. Es erfüllt mehrere wichtige Funktionen, darunter die folgenden:

- **DLP erkennt sensible Daten, ganz gleich, wo sie sich befinden und wohin sie übertragen werden, z. B.:**
  - *Data in Motion:* Das sind Daten, die über das Internet, Netzwerke und zwischen Anwendungen und Geräten übertragen werden (wie Uploads und Downloads).
  - *Data at Rest:* Das sind gespeicherte Daten. Dies können Daten in Ihren privaten Anwendungen oder einer vom Unternehmen genutzten SaaS-Anwendung sein, z. B. wenn Kundendaten in Salesforce eingegeben werden, oder interne Dokumente, die auf Microsoft OneDrive oder Microsoft SharePoint gespeichert und freigegeben werden.
  - *Data in Use:* Das sind Daten, die aktiv genutzt und bearbeitet werden, z. B. beim Kopieren auf USB oder bei Aktivitäten wie Drucken oder Faxen. (Wird heute überhaupt noch gefaxt?!)
- **DLP überwacht die Datenumgebung**, um herauszufinden, wer auf Daten zugreift und was mit diesen Daten geschieht. Durch die Überwachung von Aktivitäten kann DLP Vorfälle aufdecken, z. B. die unbefugte, gegen die Unternehmensrichtlinien verstoßende Weitergabe vertraulicher Informationen, und kann geeignete Gegenmaßnahmen einleiten. Dadurch kann sichergestellt werden, dass sensible Daten nicht ohne die richtigen Berechtigungen (Mitarbeiter und Außenstehende oder Firmen- und Privatgeräte) oder ohne Autorisierung bzw. Kontrolle (z. B. verdächtige Massendownloads zahlreicher Dateien) abgerufen oder verwendet werden. Zudem lassen sich mögliche Sicherheitsverletzungen schnell erkennen und beheben.
- **DLP ergreift automatisch Maßnahmen zur Durchsetzung von Richtlinien**, zum Beispiel indem sie den Datenfluss stoppt, Daten verschlüsselt, vertrauliche Informationen in Quarantäne stellt oder die Freigabe der Daten in einer SaaS-Anwendung aufhebt. Wenn ein Mitarbeiter zum Beispiel OneDrive verwendet und eine Datei mit vertraulichen Informationen absichtlich oder versehentlich an externe Benutzer freigibt, kann DLP die Freigabe der Datei automatisch aufheben, um die unbefugte Weitergabe der Informationen zu verhindern.

- **DLP bietet Benutzer-Coaching**, d. h. Benutzer werden automatisch über Sicherheitsverstöße und die Gründe dafür informiert und gleichzeitig im sicheren Umgang mit Daten geschult. Durch Benachrichtigungen können Benutzer auch sofort über Sicherheitsrichtlinien in Kenntnis gesetzt werden, sodass Incident-Response-Teams bei Zwischenfällen weniger Probleme manuell selektieren müssen. Eine gute DLP-Lösung sollte außerdem in der Lage sein, Benutzer sofort und ohne Verzögerung zu informieren und bei Bedarf Benachrichtigungen an Führungskräfte, das Incident-Response-Team oder die Personalabteilung weiterzuleiten.

Es ist Zeit für eine neue DLP-Lösung

Ältere DLP-Lösungen waren jahrelang eine verlässliche Sicherheitslösung - kein Wunder, dass sie immer noch so viele Fans haben! Wie bereits erwähnt, haben sich diese Systeme in den letzten zehn Jahren erheblich weiterentwickelt, um On-Premises-Netzwerke in der Zeit vor der Cloud vor Bedrohungen zu schützen.

Anbieter älterer DLP-Systeme bemühten sich redlich, die Lücke zwischen ihren Systemen und den Anforderungen moderner, Cloud-First-Unternehmen zu schließen, beispielsweise mithilfe von Technologien wie cloudbasierten Secure Web Gateways (SWGs) und CASB-Lösungen, die das Internet Content Adaptation Protocol (ICAP) integrieren.

HINWEIS

Leider sind die meisten älteren DLP-Systeme nicht für Cloud- und hybride Arbeitsumgebungen ausgelegt, die Integrationen und Funktionen mit Cloud-Services erfordern, die von diesen DLP-Systemen nicht ohne Weiteres unterstützt werden können. Dies kann zu Kompatibilitätsproblemen und Leistungseinbußen führen.

Aufgrund dieser und der vielen anderen in den vorangegangenen Kapiteln besprochenen Einschränkungen haben ältere DLP-Tools stark an Popularität eingebüßt, was viele Unternehmen dazu veranlasst hat, diese Tools einfach ganz abzuschalten. Da Unternehmen ihre Daten zunehmend in die Cloud verlagern, besteht zunehmend Bedarf an cloudbasierten DLP-Systemen, die veränderliche Kontexte und Risiken im Zusammenhang mit der Datenverwaltung erkennen können. Es sollte einfach sein, diese Systeme zu implementieren, zu erweitern und zu skalieren und dabei bestehende und moderne Anwendungsfälle abzudecken. Da sie in der Cloud bereitgestellt werden, sind diese Lösungen auch stets auf dem neuesten Stand und bieten auch dann einen zuverlässigen Schutz, wenn sich der Geschäftskontext und die Risiken ändern.

IN DIESEM KAPITEL

- **Wie veraltete Datensicherheitslösungen Ihrem Unternehmen schaden können**
- **Datenkontexttypen und Gewährleistung reibungsloser Geschäftsabläufe**
- **Anpassung an sich ändernde Risikobedingungen Schutz von Daten**
- **Sichere Realisierung moderner Anwendungsfälle im Unternehmen**
- **Bewertung von Geschäftskontext, Risiko und Benutzerverhalten für einen zukunftssicheren Datenschutz**

Kapitel 3
Die Rolle von Zero Trust bei modernen DLP-Lösungen

Ein sehr wichtiges Sicherheitskonzept – nicht nur im Zusammenhang mit DLP – ist Zero Trust. Eine Zero-Trust-Strategie geht davon aus, dass alle Benutzer und Geräte, auch innerhalb des Unternehmensnetzwerks, potenziell gefährlich und nicht vertrauenswürdig sind. Der Zugriff auf sensible Daten und Systeme wird also nicht automatisch auf der Grundlage der persönlichen Identität und Unternehmenszugehörigkeit gewährt. Stattdessen erfolgt der Zugriff erst nach sorgfältiger Authentifizierung, Überprüfung des Sicherheitsstatus und Berücksichtigung des Risikokontextes, der ständig neu bewertet wird. Zero Trust sollte die Produktivität nicht behindern, sondern einen sicheren Umgang mit sensiblen Daten ermöglichen und moderne Geschäftspraktiken mit Blick auf die Sicherheit unterstützen, wobei eine automatische Anpassung an veränderte Risikobedingungen erfolgen muss.

Zero Trust bewertet die Vertrauenswürdigkeit jeder Person, jedes Geräts und jeder Betriebsumgebung stets neu, bevor ihnen der Zugriff auf sensible Daten oder eine bestimmte Verwendung für diese sensiblen Daten gestattet wird. Selbst ein Mitarbeiter, der schon einmal Zugriff erhalten hat, muss sorgfältig geprüft werden, z. B. durch die Verifizierung seiner Identität, seines Geräts und seiner Netzwerkverbindung, durch

die Einschätzung der mit den betreffenden Anwendungen verbundenen Risiken und die Überwachung seines Verhaltens. So wird sichergestellt, dass er *weiterhin* vertrauenswürdig ist. Wenn der Benutzer sich verdächtig verhält oder Anzeichen von Nachlässigkeit zeigt, z. B., wenn er zu viele Daten weitergibt, reagiert das System auf dieses Verhalten, indem es z. B. seine Berechtigungen einschränkt. Dadurch können sensible Daten vor potenziellen Verlusten geschützt werden, und es wird sichergestellt, dass nur vertrauenswürdige Personen auf diese Daten zugreifen und sie mit anderen vertrauenswürdigen Personen teilen können.

Mit Zero Trust soll eine sichere und kontrollierte Umgebung für den Datenzugriff und -transfer geschaffen werden, um das Risiko von Datenschutzverletzungen zu verringern und sensible Daten vor unbefugtem Zugriff zu schützen. Dies wird durch die Implementierung strenger Zugriffskontrollen und die kontinuierliche Überwachung und Verifizierung von Benutzeraktionen, kontextbezogenen Risiken und Verhaltensweisen erreicht. Bei der Data Loss Prevention (DLP) reduziert ein Zero-Trust-Sicherheitsmodell das Risiko von Datenschutzverletzungen erheblich, liefert zuverlässigere Datenschutzergebnisse und optimiert die Incident-Response-Zyklen durch die Berücksichtigung des geschäftlichen Kontextes und Risikos. Da nur autorisierte Benutzer sicheren Zugriff und das Recht zur Nutzung sensibler Daten erhalten und alle böswilligen, verdächtigen, fahrlässigen oder riskanten Zugriffs- oder Übertragungsversuche verhindert werden, sind Unternehmen besser in der Lage, ihre Vermögenswerte zu schützen.

Die Risiken veralteter Sicherheitslösungen

DLP-Systeme wurden entwickelt, um zu verhindern, dass sensible Informationen das Unternehmen verlassen. Ältere Versionen decken nur eine begrenzte Anzahl gängiger Datenverlust-Szenarien ab. Ihr Hauptzweck besteht darin, sensible Daten zu identifizieren und mithilfe eines perimetergestützten Ansatzes, der sich auf die Kontrolle des Datenflusses zum und vom Unternehmensnetzwerk befasst, im Unternehmen zu behalten.

DLP konzentriert sich darauf, vordefinierte Datenverletzungen zu erkennen und darauf zu reagieren und nutzt dabei einen Ansatz, der als *implizites Vertrauen* bezeichnet wird. Bei diesem Ansatz fehlt jedoch der Kontext in Bezug auf Benutzer und ihre geschäftlichen Absichten sowie die mit einer bestimmten Aktion verbundenen Risiken.

Ein älteres DLP-System sucht möglicherweise nach Sozialversicherungsnummern und verhindert jeden Versuch, eine Sozialversicherungsnummer an einen Ort außerhalb des Unternehmensgeländes zu senden. In einem anderen Fall verhindert es vielleicht, dass sensible Daten einfach in eine SaaS-Anwendung hochgeladen werden, ohne dass zwischen

einer geschäftlichen Instanz einer genehmigten SaaS-Anwendung wie Microsoft Teams und einer privaten Instanz der gleichen Anwendung unterschieden wird. Dieser Ansatz mag zwar sicher erscheinen, doch er ist in Wirklichkeit ziemlich unflexibel und bietet keine Einblicke in Benutzer, Geräte, Netzwerke, Anwendungen und Ziele, die auf zulässige Aktivitäten hindeuten könnten. Implizites Vertrauen ist ein geschäftliches Hindernis, das die für das Wachstum eines modernen Unternehmens notwendige mühelose Kommunikation und den reibungslosen Datenfluss verhindert.

HINWEIS

Da ältere DLP-Systeme den Geschäftskontext und das damit verbundene Risiko nicht kontinuierlich überprüfen, können sie keine fundierten Datenschutzentscheidungen treffen und verursachen unnötige Unterbrechungen des Geschäftsbetriebs.

Bei Anwendung laxer Richtlinien erhalten Benutzer oder Geräte beim Modell des impliziten Vertrauens Zugriff auf sensible Daten, ohne dass ihre Identität und Vertrauenswürdigkeit laufend überprüft wird. Dadurch werden Unternehmen anfälliger für den Missbrauch ihrer sensiblen Daten. Wenn sensible Daten den Perimeter erst einmal verlassen haben, entziehen sie sich der Kontrolle durch die Sicherheitsabteilung des Unternehmens.

Diese Tatsache stellt im Cloud-Zeitalter ein großes Problem dar. Sensible Daten werden selbst für die alltäglichsten Geschäftsfunktionen außerhalb der Grenzen des Unternehmens genutzt und verbreitet. Gängige Cloud-Anwendungen und -Services wie Dropbox und Google Drive erlauben es Mitarbeitern zum Beispiel, innerhalb und außerhalb der Unternehmensumgebung auf sensible Daten zuzugreifen, sie zu teilen und gemeinsam damit zu arbeiten. Ältere DLP-Systeme, die sich auf implizites Vertrauen stützen, unterbrechen jedoch eine legitime Zusammenarbeit oder lassen Daten achtlos nach außen gelangen, was sie anfällig für potenzielle Bedrohungen macht.

Beim Datenschutz nach dem Zero-Trust-Prinzip ist die Nutzung und Weitergabe sensibler Daten gestattet, solange die Sicherheitsbedingungen kontinuierlich überprüft werden. Sensible Daten können zwischen Benutzern und Geräten ausgetauscht und in unterschiedlichen Cloud-Services gespeichert werden, da Sicherheitsbedingungen wie Benutzeridentität, Geräte-, Netzwerk- und Anwendungssicherheit sowie das Benutzerverhalten langfristig kontinuierlich überprüft werden. Zero-Trust-Datenschutz wird speziell auf sensible Daten angewandt und stellt sicher, dass alle Sicherheitsanforderungen jederzeit erfüllt sind, was Anwendungsfälle wie hybrides Arbeiten, Cloud- und moderne Geschäftsanwendungen ermöglicht.

ERINNERUNG

Ein modernes, in der Cloud bereitgestelltes DLP-System, das auf dem Zero-Trust-Prinzip basiert, überwacht und kontrolliert Daten nicht nur überall dort, wo Unternehmensanwender eine Verbindung herstellen und auf Daten zugreifen möchten, sondern auch wo sie gespeichert und

übertragen werden können: in Cloud-Anwendungs-Repositorys und in On-Premises-Umgebungen.

Ein weiteres Problem bei herkömmlichen, auf mehreren Produkten und implizitem Vertrauen basierenden Sicherheitsansätzen besteht darin, dass diese Produkte voneinander isoliert sind und jeweils nur eine Sicherheitskontrolle anwenden. Die einzelnen Sicherheitskontrollen werden nicht miteinander integriert und Risikoinformationen werden nicht mit anderen Tools geteilt. Wenn unterschiedliche Sicherheitskontrollen voneinander isoliert sind und nicht in eine zusammenhängende Sicherheitsplattform integriert werden, entstehen Lücken in der gesamten Sicherheitsstrategie. Um Ihre Daten umfassend schützen zu können, müssen mehrere Sicherheitskontrollen zusammenwirken und Informationen austauschen können.

Das Zero-Trust-Konzept verfolgt einen ganzheitlicheren und dynamischeren Datenschutzansatz. Es berücksichtigt den Kontext des Benutzers, des Geräts, des Netzwerks und andere Faktoren, um fundiertere Datenschutzentscheidungen zu treffen. Dieser Ansatz unterstützt die Integration von DLP mit anderen Sicherheitskontrollen und Produktivitätstools und sorgt so dafür, dass das System Bedrohungen, Risiken und Geschäftsbedingungen kontinuierlich überwacht und sich an Veränderungen anpasst.

Unternehmen, die DLP auf der Grundlage von implizitem Vertrauen einsetzen, müssen von der falschen Annahme ausgehen, dass Benutzer innerhalb des Unternehmens vertrauenswürdig und sicherheitsbewusst sind und niemals sensible Daten gefährden. Aufgrund des fehlenden Sicherheitskontextes führt eine restriktive Durchsetzung von DLP-Richtlinien häufig zur Unterbrechung legitimer Geschäftsprozesse. DLP auf der Basis von Zero Trust hingegen überwacht und kontrolliert die Datennutzung zu jeder Zeit, um Verstöße gegen Datenrichtlinien adaptiv zu verhindern.

Ein DLP-System, das auf implizitem Vertrauen basiert, schützt eine Kreditkartennummer, indem es autorisierten Benutzern den Zugriff auf die sensiblen Daten gestattet, während es unbefugten Benutzern den Zugriff verweigert. Dabei wird davon ausgegangen, dass autorisierte Benutzer vertrauenswürdig genug sind, um sicher mit den Daten umzugehen und sie nicht zu missbrauchen.

Im Gegensatz zu älteren, auf implizitem Vertrauen basierenden DLP-Systemen verlässt sich ein auf Zero-Trust-Prinzipien basierendes DLP-System nicht auf die Annahme, dass Vertrauen bei Benutzern vorausgesetzt werden kann. Stattdessen schützt es sensible Daten wie Kreditkartennummern, indem es von allen Benutzern unabhängig von ihrer Berechtigungsstufe zunächst verlangt, sich zu authentifizieren. Dabei

könnte es sich um eine Multifaktor-Authentifizierung handeln, z. B. ein Passwort und einen Einmalcode, der an ein mobiles Gerät gesendet wird.

Außerdem bewertet das System kontinuierlich die potenziellen Risiken im Zusammenhang mit Geräten, Benutzern, Daten und Anwendungen. Es überprüft, ob die Geräte vertrauenswürdig und sicher sind, ob die verwendeten Anwendungen und ihre Instanzen (d. h. unternehmenseigene oder private) sicher und richtlinienkonform sind, ob das Netzwerk sicher und vertrauenswürdig ist, ob die Daten an vertrauenswürdige Ziele und Empfänger übermittelt werden und ob das Verhalten des Benutzers richtlinienkonform ist. Diese Bedingungen werden ständig überprüft, und das System passt seine Schutzmaßnahmen entsprechend an. Das System überwacht und verfolgt außerdem den Benutzerzugriff auf sensible Daten, alarmiert Administratoren bei verdächtigem Verhalten oder potenziellen Sicherheitsverletzungen und betreut Benutzer beim sicheren Umgang mit Daten, falls es zu Verstößen gegen die Unternehmensrichtlinien kommen sollte. Mit diesem Ansatz wird das Risiko eines unbefugten Zugriffs auf sensible Daten verringert, da das System zunächst alle Benutzer überprüft, bevor ihnen der Zugriff gewährt wird. Außerdem lassen sich die Risiken für sensible Daten im Laufe der Zeit minimieren, da Benutzer in Echtzeit geschult werden.

Kontext zur Erkennung wichtiger Geschäftsaktivitäten

Mithilfe von Zero Trust können Datenschutzsysteme fundierte Entscheidungen über die Zulassung oder Beschränkung bestimmter Aktivitäten treffen. Dabei werden mehrere Faktoren oder Kontexte berücksichtigt, z. B. die Identität des Benutzers, das verwendete Gerät, die Vertrauenswürdigkeit der Anwendung und der Kontext der betroffenen Daten. (Zero Trust erfasst den Kontext mithilfe anderer Lösungen, auf die ich im Abschnitt „DLP sollte nicht isoliert eingesetzt werden“ eingehen werde.) Da alle diese Kontextelemente berücksichtigt werden, lässt sich anhand von Zero-Trust-Prinzipien genauer ermitteln, ob eine bestimmte Aktivität für das Unternehmen nützlich oder notwendig ist und daher zugelassen werden kann. So werden Daten zuverlässig geschützt, das Risiko von Sicherheitsverletzungen oder anderen Bedrohungen sinkt und Geschäftsabläufe können reibungslos fortgesetzt werden.

Die folgende Liste enthält die Kontexttypen, die bei Zero Trust verwendet werden:

- **Benutzerkontext:** Wer eine Handlung ausführt oder wer von einer Handlung betroffen ist. Anhand dieser Informationen lässt sich feststellen, ob das Verhalten eines Benutzers angemessen ist oder ob etwas nicht stimmt. Angenommen, ein Benutzer verschiebt plötzlich

viel mehr Daten als sonst, meldet sich von ungewöhnlichen Orten aus an oder verhält sich einfach anders. Das könnte ein Zeichen für riskantes oder böswilliges Verhalten sein. Dasselbe gilt, wenn ein Benutzer auf sensible Daten zugreift bzw. diese verwendet und/oder sie an private Anwendungen sendet. Auf Grundlage der Identität und des Verhaltens eines Benutzers können die Benutzerrechte zum Schutz sensibler Daten geändert werden. So wird sichergestellt, dass nur autorisierte Benutzer auf diese Daten zugreifen, sie mit autorisierten Empfängern teilen und sie an sichere Ziele übertragen können.

- **Gerätekontext:** Das Gerät, das versucht, auf Ihre Daten zuzugreifen. Sie sollten berücksichtigen, ob es sich um ein privates oder ein firmeneigenes Gerät handelt, wie sicher dieses Gerät ist und ob es gepatcht und auf dem neuesten Stand ist. Auch Faktoren in der Nähe des Geräts können betrachtet werden, z. B. die Vertrauenswürdigkeit des Standorts, von dem aus die Verbindung hergestellt wird. Wenn Sie all diese Dinge prüfen, können Sie je nach Vertrauenswürdigkeit und Risiko die richtige Berechtigungsstufe für das Gerät festlegen. Selbst ein normalerweise zuverlässiger Benutzer kann ein kompromittiertes Gerät haben oder ein Sicherheitsrisiko darstellen. Der Gerätekontext ist daher entscheidend für die Festlegung der zu gewährenden Berechtigungen.
- **Anwendungskontext:** Der Ruf und die Vertrauenswürdigkeit der Anwendung, die für den Zugriff auf oder die Verarbeitung von Daten verwendet wird. Dieser Faktor ist wichtig, weil Anwendungen, die einen schlechten Ruf haben oder die nicht vertrauenswürdig sind, ein Risiko für die Sicherheit der Daten darstellen, auf die zugegriffen wird bzw. die bearbeitet werden sollen. Datenschutzsysteme können auf andere Systeme wie einen Cloud Access Security Broker (CASB) zurückgreifen, um Informationen über die Compliance- und risikobezogenen Attribute der Anwendung zu erfassen. Dadurch kann das System feststellen, ob eine Anwendung ein Risiko darstellt, z. B. einen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO), weil möglicherweise zu viele sensible Daten offengelegt werden.

  Ein Benutzer kann Zugriff auf mehrere Instanzen einer Cloud-Anwendung haben, was eine differenziertere Kontrolle bezüglich sensibler Daten erfordert, um eine versehentliche Freigabe für private Konten zu verhindern. Anwendungen für die kollaborative Kommunikation wie Slack und Microsoft Teams können ebenfalls ein Risiko darstellen, wenn diese Anwendungen Kanäle haben, die sowohl von internen als auch von externen Anwendern genutzt werden. Das System muss daher in der Lage sein, zwischen diesen beiden Gruppen zu unterscheiden, um Datenlecks zu verhindern. Beachten Sie alle diese Punkte, um sicherzustellen, dass die genutzten Anwendungen seriös und vertrauenswürdig sind, damit Ihre Daten keinen unnötigen Risiken ausgesetzt werden.

- **Datenkontext:** Liefert Informationen zur Sensibilität bestimmter Daten, zu ihrem Format, ihrer Größe und zu anderen Faktoren. Er gibt an, wo Ihre Daten verwendet werden und ob diese Verwendung zulässig ist. Es ist hilfreich, zu wissen, auf welche Art von Daten zugegriffen wird, welche Daten verschoben werden und ob sie am richtigen Ort verwendet werden. Wenn sensible Daten abgerufen oder an einen nicht autorisierten Ort übertragen werden, müssen Maßnahmen ergriffen werden, um ein Datenleck oder eine Datenschutzverletzung zu verhindern. Der Datenkontext ist von entscheidender Bedeutung, um sicherzustellen, dass Daten korrekt gehandhabt werden und je nach ihrer Kritikalität nur von autorisierten Benutzern an autorisierten Orten eingesehen werden können. Dies hilft bei der Entscheidung, ob eine Aktivität für das Unternehmen wirklich notwendig ist und ob sie das Risiko überhaupt wert ist.

HINWEIS

Die meisten DLP-Lösungen, nicht nur ältere Versionen, verursachen Probleme beim Geschäftsbetrieb, da sie meist keine ausreichenden Informationen über das Unternehmen und die bestehenden Risiken erfassen. Bei den meisten DLP-Lösungen ist Ihr Unternehmen gezwungen, sich auf Incident-Response-Teams zu verlassen, die anhand manueller Methoden entscheiden, wie vorzugehen ist. Das ist frustrierend, ineffizient und teuer!

Mit Zero Trust werden diese Probleme mit Sicherheit auf ein Minimum reduziert. Ein modernes DLP-System, das auf Zero-Trust-Prinzipien basiert, berücksichtigt alle von Benutzern, Geräten, Daten, Netzwerken und Anwendungen ausgehenden Risiken. Dadurch hat das System ein viel besseres Verständnis für die jeweiligen Risiken und kann auf der Grundlage von dynamischen Datenschutzrichtlinien, die auf Ihre konkreten Geschäftsanforderungen abgestimmt sind, automatisch die richtigen Entscheidungen zum Schutz Ihrer Daten treffen. Zero Trust sorgt dafür, dass Ihre Daten sicher sind und Ihr Geschäft reibungslos läuft.

DLP sollte nicht isoliert eingesetzt werden

Datenschutzmechanismen werden in älteren und neuen DLP-Systemen verwendet. Tatsächlich wurde DLP speziell zur Identifizierung und zum Schutz sensibler Daten entwickelt. Bei den meisten dieser Datenkontrollen gibt es jedoch ein Problem: Ihnen fehlt der Kontext. DLP muss Teil einer größeren Plattform sein, die auf Zero-Trust-Prinzipien basiert und den gesamten verfügbaren Kontext nutzt, um fundierte Entscheidungen zu treffen. DLP braucht Unterstützung und Informationen von anderen Lösungen, um den gesamten notwendigen Kontext zu erfassen, z. B. den Benutzerkontext, den Gerätekontext, den Anwendungskontext und den Datenkontext. Deshalb ist ein System auf der Grundlage von Zero-Trust-Prinzipien ein integriertes System, das sich auf die Kontrolle kontextbezogener Daten konzentriert, anstatt allem blind zu vertrauen.

Dieser Ansatz kann Ihnen dabei helfen, sich an veränderte Risikobedingungen anzupassen und Ihre Daten jedes Mal automatisch mit der am besten geeigneten Maßnahme zu schützen.

TIPP

Achten Sie beim Datenschutz nach Zero-Trust-Prinzipien auf konsolidierte Kontrollen, die Informationen miteinander austauschen und nahtlos zusammenarbeiten, um Ihre Daten zu schützen. Der intelligente Security Service Edge (SSE) von Netskope aktiviert beispielsweise Zero-Trust-Prinzipien direkt und ermöglicht mit DLP als seinem Kernelement den Austausch von Kontext zwischen Kontrollen. Dadurch wird der Schutz Ihrer Daten zu einem sehr einfachen und effizienten Prozess.

Der intelligente SSE von Netskope unterstützt seine umfassende DLP-Plattform noch mit einigen weiteren Sicherheitslösungen. Hier sind einige der wichtigsten:

- **Secure Web Gateway (SWG):** Ein SWG ist eine Sicherheitslösung, die sich zwischen den Benutzern und dem Internet befindet. Sie sorgt für sichere Internetverbindungen und schützt vor Bedrohungen aus dem Web. Netskope DLP stellt mithilfe von SWG sicher, dass sensible Daten nicht über ungesicherte, riskante Internetverbindungen geleakt werden. Dies schließt auch den verschlüsselten Datenverkehr ein. Die Lösung erkennt und überwacht sensible Unternehmensdaten und verhindert, dass sie über Internetverbindungen von Homeoffices, Zweigstellen und öffentlichen WLAN-Standorten geleakt oder offengelegt werden.
- **CASB:** Mithilfe von CASB erkennt, überwacht und schützt Netskope DLP sensible Daten in SaaS-Anwendungen (Software as a Service), die sich in IaaS-Umgebungen (Infrastructure as a Service), Unternehmensnetzwerken und Zweigstellen, bei mobilen Mitarbeitern, E-Mail-Services und in Mitarbeiter-Endpunkten befinden. Dieser zentralisierte in der Cloud bereitgestellte Service setzt einheitliche Datenschutzrichtlinien überall dort durch, wo sensible Daten gespeichert, verwendet oder übertragen werden, und schützt sensible Daten bei der Übertragung und im Ruhezustand. Er deckt Tausende von SaaS-Anwendungen ab und hat einen einzigartigen Überblick über Daten, die an persönliche Anwendungsinstanzen (z. B. das OneDrive-Konto des Unternehmens an ein privates OneDrive-Konto) und riskante Anwendungen übertragen werden. Er scannt Tausende unterschiedlicher Dateitypen sowie Posts und asynchrone Kommunikation über Collaboration-Anwendungen und E-Mail-Services. Datenschutz, Compliance und Datenschutzrichtlinien werden über Public-Cloud-Services hinweg einheitlich durchgesetzt und automatisch mit der gesamten DLP-Plattform synchronisiert.
- **SaaS Security Posture Management (SSPM) und Cloud Security Posture Management (CSPM):** Diese Technologien stellen Posture Management für SaaS- und Public-Cloud-Umgebungen zur

Verfügung und sorgen für Sicherheit und Compliance. Sie überwachen und bewerten den Sicherheitsstatus kontinuierlich, identifizieren potenzielle Risiken und Fehlkonfigurationen und liefern umsetzbare Erkenntnisse und Empfehlungen. Durch automatisierte Fehlerbehebungsfunktionen werden die erkannten Probleme in Echtzeit gelöst.

- **Software für den Endpunktschutz:** Netskope Endpoint DLP ist eine Lösung, die sensible Daten auf den Endpunkten von Mitarbeitern erkennt, überwacht und schützt. Da die Lösung in den Netskope-Client integriert ist, muss kein separater Agent bereitgestellt werden. Netskope Endpoint DLP minimiert die Ressourcennutzung und bietet eine umfangreiche Funktionspalette, darunter ML-basierte Klassifizierer, optische Zeichenerkennung (OCR), Fingerprinting von Dateien und Exact Data Matching. Durch die Nutzung des in der Cloud bereitgestellten DLP-Services und der über die gesamte DLP-Plattform verteilten Intelligence wird das mehrfache Scannen von Daten aus der Cloud vermieden, was zu einer reibungslosen Benutzererfahrung und einem wirksameren Schutz führt.
- **User and Entity Behavior Analytics (UEBA):** Bei dieser Sicherheitskontrolle wird das Benutzerverhalten kontinuierlich bewertet, um ungewöhnliche oder potenziell riskante Aktivitäten zu erkennen. Früher war UEBA oft eine isolierte Sicherheitskontrolle, doch um wirklich effektiv zu sein, muss der Prozess mit DLP integriert werden. Da das Verfahren UEBA Protokolle von DLP-Sicherheitsverstößen erfasst und riskantes Verhalten zur weiteren Prüfung kennzeichnet, kann es spätere Änderungen bei der Durchsetzung von Richtlinien unterstützen und zum Schutz Ihrer Daten beitragen.
- **Identity and Access Management (IAM):** IAM ist eine Methode zur Verwaltung und Kontrolle des Zugriffs auf Ressourcen auf der Grundlage der Benutzeridentität. Sie umfasst Technologien wie Multi-Faktor-Authentifizierung, Single Sign-On und Zugriffskontrolllisten. Netskope lässt sich mit den Produkten vieler IAM-Anbieter integrieren, damit Unternehmen sicherstellen können, dass ihre Ressourcen vor unbefugtem Zugriff geschützt sind und dass nur autorisierte Benutzer Zugriff darauf haben. IAM ist ein wichtiger Bestandteil der Zero-Trust-Sicherheitsstrategie jedes Unternehmens und trägt entscheidend dazu bei, Ressourcen zu schützen und die Einhaltung von Sicherheitsrichtlinien und -vorschriften zu gewährleisten.
- **E-Mail-Schutz**. Netskope bietet eine äußerst umfassende DLP-Lösung für E-Mail wie Microsoft 365 und Gmail, und zwar sowohl für Daten bei der Übertragung als auch im Ruhezustand. Die Lösung schützt ausgehende sensible E-Mails in Echtzeit über SMTP-Proxy und Webmail und kann sensible Daten, die über ein persönliches E-Mail-Konto verschickt werden, von Daten unterscheiden, die über ein geschäftliches E-Mail-Konto oder über private E-Mail-Services gesendet werden.

- **Zero Trust Network Access (ZTNA):** Die Lösung Netskope DLP, die über die Fernzugriffslösung Netskope Private Access (NPA) bereitgestellt wird, verhindert Datenverlust und -exfiltration bei privaten Ressourcen im Rechenzentrum und in Public-Cloud-Umgebungen. Sie bietet außerdem Datenschutz für den browserbasierten Zugriff auf private Anwendungen, ganz gleich, von wo aus sich Benutzer anmelden.

Da Netskope SSE diese Kernkomponenten in einer einzigen, integrierten Plattform vereint, bietet sie eine umfassende Sicherheitslösung, die Ihr Unternehmen vor einer Vielzahl von Bedrohungen schützen kann.

Anwendung von Zero-Trust-Prinzipien mit DLP

ERINNERUNG

Der Datenschutz nach dem Zero-Trust-Prinzip soll nicht nur verhindern, dass sensible Daten das Unternehmen verlassen. Er dient auch dazu, moderne Anwendungsfälle zu realisieren, ohne die Sicherheit und potenzielle Risiken aus den Augen zu verlieren.

Dies beinhaltet die Unterstützung von Benutzern an unterschiedlichen Standorten und die Verbesserung der Zusammenarbeit, während Ihre Daten zuverlässig geschützt werden. Zero-Trust-Datenschutz bedeutet, dass Mitarbeiter von überall aus arbeiten können und trotzdem Zugriff auf alle benötigten Ressourcen haben und mit Teammitgliedern und externen Partnern zusammenarbeiten können, ohne sich Gedanken über Datenlecks machen zu müssen. Mit einer einheitlichen Lösung wie Netskope SSE können Sie Ihre Daten zuverlässig schützen und alle Vorteile moderner Daten-Workflows im Unternehmen nutzen. Die folgenden Beispiele zeigen, wie dies in der Praxis funktioniert:

- Stellen Sie sich vor, Sie arbeiten an Ihrem Laptop und sind über Netskope SSE beim Netzwerk Ihres Unternehmens angemeldet. Sie rufen einige wichtige Verkaufsdokumente ab und beginnen mit ihrer Bearbeitung. Dann versuchen Sie jedoch irrtümlicherweise, eine Kopie der Dokumente auf Ihrem privaten Cloud-Speicher-Konto, anstatt auf der Unternehmensinstanz der gleichen Cloud-Speicher-Anwendung zu speichern.
- Mit DLP, die auf Zero-Trust-Prinzipien basiert, erkennt das System Ihren Versuch, sensible Unternehmensdaten an eine persönliche Anwendungsinstanz zu senden, und verhindert, dass die Daten gespeichert werden. Stattdessen zeigt das System eine Benutzer-Coaching-Benachrichtigung an, ein Pop-up-Fenster, das Sie sofort über den Sicherheitsverstoß informiert und Sie an den richtigen Speicherort für die Dokumente erinnert. Auf diese Weise können Sie von überall aus arbeiten und haben dennoch Zugriff auf alle benötigten Ressourcen, ohne sich Sorgen machen zu müssen, dass sensible Daten versehentlich an einen falschen Ort geraten. Coaching-Benachrichtigungen klären Benutzer über sichere Praktiken und Unternehmensrichtlinien auf,

sodass das Risiko eines Datenverlusts im Laufe der Zeit immer geringer wird und später weniger zeitaufwendige Schulungen erforderlich sind.

» Angenommen, Sie arbeiten mit externen Partnern an einem Projekt zusammen und möchten einige Dokumente mit ihnen teilen. Mit DLP, das auf dem Zero-Trust-Prinzip basiert, prüft das System den Ruf und die Vertrauenswürdigkeit der Anwendung, die Sie zum Teilen von Dokumenten verwenden, Ihre Identität und Ihr Verhalten, das verwendete Gerät und das Übertragungsziel.

  Wenn Sie eine private Cloud-Speicheranwendung nutzen, die eine andere Sicherheitsstufe hat als die Unternehmensanwendung, kann das System verhindern, dass Sie die Daten über diese Anwendung freigeben. Stattdessen kann es Ihnen vorschlagen, eine andere Anwendung zu nutzen oder die Dokumente über einen sicheren Kanal zu senden. Die DLP prüft auch das Ziel der Übertragung, z. B., ob der Empfänger ein externer Benutzer oder ein Mitarbeiter ist und ob das Ziel sicher ist. Die DLP kann eine Benachrichtigung an Sie senden und Sie darin fragen, ob Sie sicher sind, dass Sie sensible Daten an den externen Empfänger weitergeben wollen. Sie kann Sie sogar bitten, Ihre Handlung zu begründen. Auf diese Weise können Sie bei der Zusammenarbeit sicher sein, dass Ihre Daten geschützt sind und dass nur autorisierte Benutzer auf sie zugreifen können.

Adaptives Zero-Trust-Modell

Beim adaptiven Zero-Trust-Modell liegt die Erkenntnis zugrunde, dass sich alles im Laufe der Zeit ändert. Der Zero-Trust-Datenschutz muss also kontinuierlich den Geschäftskontext, das Risiko und das Benutzerverhalten bewerten, um Ihre Daten zuverlässig zu schützen.

Hier ist ein Beispiel, das diesen Punkt sehr gut veranschaulicht: Stellen Sie sich den Türsteher eines Nachtclubs vor. Als er wie jeden Abend vor der Tür steht, nähert sich eine Gruppe junger Leute dem Eingang. Der Türsteher überprüft die Ausweise. Alles scheint in Ordnung zu sein und die Gruppe wird eingelassen. Im Laufe des Abends bemerkt der Türsteher jedoch, dass sich eine der Personen aus der Gruppe seltsam verhält. Sie ist aggressiv oder versucht sich Zugang zu verbotenen Bereichen des Clubs zu verschaffen. Mit dem adaptiven Zero-Trust-Modell würde unser Türsteher diese Verhaltensänderung erkennen und Maßnahmen ergreifen, um die anderen Gäste und den Club zu schützen. Er würde die Person genauer im Auge behalten, um sicherzustellen, dass sie keine Probleme verursacht, oder sie sogar bitten, den Club zu verlassen. Auf diese Weise ist die Sicherheit anderer Personen und des Clubs gewährleistet, auch wenn sich das Verhalten einer Person ändert.

Ihr Unternehmen könnte zum Beispiel mit den folgenden häufig auftretenden Szenarien konfrontiert werden:

- **Das Verhalten einer Person ändert sich**. Sie haben einen vertrauenswürdigen Mitarbeiter, der schon immer Zugriff auf bestimmte sensible Unternehmensdaten hatte. Eines Tages, vielleicht nach einer Leistungsbeurteilung, verhält sich der Mitarbeiter anders als bisher. Er beginnt, auf mehr sensible Daten als sonst zuzugreifen und sie herunterzuladen oder sich von ungewöhnlichen Orten aus anzumelden. Mit dem adaptiven Zero-Trust-Modell erkennt das System diese Verhaltensänderung und passt die Berechtigungen des Mitarbeiters entsprechend an. Das System kann zum Beispiel seinen Zugriff auf bestimmte Daten einschränken oder das Sicherheitsteam benachrichtigen, damit eine weitere Überprüfung durchgeführt wird. So sind Ihre Daten auch dann geschützt, wenn sich das Verhalten eines vertrauenswürdigen Mitarbeiters ändern sollte.
- **Der Ruf und die Vertrauenswürdigkeit von Anwendungen ändern sich**. Anwendungen ändern sich mit der Zeit; nicht nur ihre Funktionalität, sondern auch ihr Ruf, ihr Sicherheitsstatus und ihre Vertrauenswürdigkeit können sich ändern. Zum Beispiel kann eine Cloud-Speicher-Anwendung, die bisher als sicher galt, eine neue Schwachstelle oder Fehlkonfiguration aufweisen, die ihre Vertrauenswürdigkeit beeinträchtigt. Mit dem adaptiven Zero-Trust-Modell überprüft die Lösung kontinuierlich das Risikoniveau der Anwendung und passt die Berechtigungen entsprechend an. So sind Ihre Daten auch dann geschützt, wenn sich die Vertrauenswürdigkeit einer Anwendung ändert.
- **Geräte werden kompromittiert**. Geräte können mit der Zeit anfälliger für Bedrohungen werden. Es kann sogar passieren, dass sie kompromittiert werden, ohne dass der Benutzer dies überhaupt bemerkt. Ein Laptop, der bisher als sicher galt, kann zum Beispiel mit Malware infiziert werden, oder seine Sicherheitseinstellungen werden ohne das Wissen des Benutzers geändert. Mit dem adaptiven Zero-Trust-Modell bewertet das System kontinuierlich den Sicherheitsstatus des Geräts und passt die Berechtigungen nach Bedarf an. So sind Ihre Daten auch dann geschützt, wenn ein Gerät kompromittiert worden ist.
- **Der Datenfluss ändert sich**. Der Datenfluss kann sich aufgrund von Änderungen der Compliance-Vorschriften auf unterschiedlichen Ebenen ändern. Ein Datenfluss kann z. B. als unbedenklich angesehen werden, doch wenn die Zieladresse nicht richtlinienkonform bzw. unsicher ist, können die Vorschriften trotzdem verlangen, dass das Unternehmen den Datenfluss schützt. Dies ist bei der DSGVO der Fall, die vorschreibt, dass bestimmte private Daten die EU nur dann verlassen dürfen, wenn eine Angemessenheitserklärung oder ein gültiges Übermittlungsabkommen vorliegt. Mit dem adaptiven Zero-Trust-Modell bewertet das System die Risiken kontinuierlich und passt die Berechtigungen entsprechend an. So sind Ihre Daten auch dann geschützt, wenn sich die Regeln ändern.

- **Die Rolle oder der Status eines Benutzers ändert sich**. Benutzer, die ihre zweiwöchige Kündigungsfrist einhalten, haben in dieser Zeit eventuell noch Zugriff auf sensible Daten. Mit dem adaptiven Zero-Trust-Modell bewertet das System kontinuierlich die Risiken und passt die Berechtigungen gegebenenfalls an. Das System kann zum Beispiel den Zugriff des Benutzers auf bestimmte Daten einschränken oder das Sicherheitsteam über eine Aktion informieren, die weiter geprüft werden muss.

TIPP

Das adaptive Zero-Trust-Modell beurteilt die Datennutzung aus möglichst vielen Blickwinkeln, um Berechtigungen so anzupassen, dass die sensiblen Daten und der Ruf des Unternehmens geschützt werden und die Geschäftsaktivität nicht beeinträchtigt wird.

Das adaptive Zero-Trust-Modell erhöht den Schutz und macht Daten und Mitarbeiter produktiver. Es bietet dynamische, anpassungsfähige Datenschutzrichtlinien, da die Risiken kontinuierlich bewertet und die Berechtigungen nach Bedarf angepasst werden. Damit unterscheidet es sich deutlich von den typischen älteren wie neuen DLP-Systemen, die sich auf einen punktuellen Ansatz stützen, der auf implizitem Vertrauen basiert und zu vielen Fehlalarmen und einer Ermüdung bei der Triage von Vorfällen führt. Ein umständlicher Ansatz zwingt das Incident-Response-Team dazu, bei jedem Vorfall manuell zu prüfen, ob es sich um einen tatsächlichen Sicherheitsverstoß handelt, und dann den verantwortlichen Benutzer zu benachrichtigen (oft nachdem dieser vergessen hat, was er vorher gemacht hat). Das Team muss dann den gesamten Datenfluss entschlüsseln, was ein langer, ressourcenintensiver Prozess ist. Das adaptive Zero-Trust-Modell bietet ein Modell für kontinuierlichen Schutz, das Ihnen die Sicherung Ihrer Daten und den reibungslosen Geschäftsbetrieb erheblich erleichtert.

Datenschutz mit dem adaptiven Zero-Trust-Modell von Netskope

Bei der Implementierung von Datenschutz mit dem adaptiven Zero-Trust-Modell von Netskope steht der Kontext im Vordergrund. Durch die Überwachung des Datenverkehrs zwischen Benutzern, Geräten, Anwendungen, Netzwerken und Zielen entwickelt Netskope ein umfassendes Verständnis von den Vorgängen in Ihrem Unternehmen. Dadurch kann das System den Datenzugriff granular steuern, sodass Ihre sensiblen Daten geschützt sind und Ihr Geschäftsbetrieb nicht beeinträchtigt wird.

Stellen Sie sich zum Beispiel vor, ein Benutzer versucht, von einem privaten Gerät aus auf sensible Unternehmensdaten zuzugreifen. Mit Netskope beginnt der Prozess mit der genauen Erkennung der sensiblen Daten. Da unterschiedliche kontextbezogene Faktoren berücksichtigt

werden, kann eine präzisere und effektivere Reaktion auf Vorfälle erzielt werden, die eine manuelle Triage überflüssig macht und die Belastung der Sicherheitsteams minimiert. Das System bewertet den Sicherheitsstatus des Geräts, die Identität des Benutzers und sein Verhalten, um zu entscheiden, ob Zugriff gewährt werden sollte.

Faktoren wie die Netzwerkverbindung und der Standort, potenzielle Schwachstellen und verfügbare Bedrohungsdaten werden ebenfalls berücksichtigt. Die mit der Anwendung verbundenen Risiken und ihr Ruf werden im Netskope Cloud Confidence Index (CCI) erfasst, einer Datenbank mit fast 60.000 Cloud-Anwendungen (Tendenz steigend!), die Netskope anhand von etwa 50 risikobasierten Kriterien bewertet hat. Anhand dieser Kriterien wird die Unternehmensfähigkeit einer Anwendung gemessen und ihre Sicherheit, Überprüfbarkeit und die Geschäftskontinuität berücksichtigt werden.

Wenn das Gerät als riskant oder das Verhalten des Benutzers als ungewöhnlich eingestuft wird, kann der Zugriff eingeschränkt oder das Sicherheitsteam benachrichtigt werden, um weitere Untersuchungen durchzuführen. Ist das Gerät sicher und das Verhalten des Benutzers normal, kann der Zugriff gewährt werden.

TIPP

Die Grundlage des Datenschutzes von Netskope ist seine SSE-Lösung, die Teil der umfassenderen Netskope Secure Access Service Edge (SASE)-Plattform ist. Diese konvergente, cloudnative Sicherheitslösung konsolidiert die zuvor beschriebenen wichtigen Sicherheitstechnologien in einer einzigen, integrierten Plattform. Netskope kombiniert diese Technologien in einer einzigen Plattform, um Ihnen die Verwaltung Ihrer Sicherheit von einem zentralen Ort aus zu erleichtern. Netskope SSE ist cloudnativ, d. h. die Lösung kann schnell und effizient skaliert werden, um die Anforderungen Ihres Unternehmens zu erfüllen. Außerdem ist sie sehr flexibel und lässt sich problemlos an Ihre konkreten Sicherheitsanforderungen anpassen.

Netskope SSE wurde unter der Prämisse entwickelt, dass es bei der Sicherheit um mehr als die Durchsetzung von Richtlinien geht. Ein wichtiger Aspekt ist zudem die Schulung des Personals und die Förderung eines sicheren Verhaltens im Umgang mit Daten. Deshalb bietet die Lösung dem Benutzer die Möglichkeit, geschäftliche Entscheidungen in der Gewissheit zu treffen, dass die Unternehmensdaten geschützt sind. Bei einem Verstoß kann Netskope SSE Ihre Mitarbeiter zum Beispiel auf eine Schulung zum Umgang mit sensiblen Daten hinweisen, Fragen stellen, um den Kontext weiter zu bewerten, oder sie über Tipps und bewährte Verfahren für sicheres Arbeiten im Homeoffice informieren. Dank eines ganzheitlichen Datenschutzansatzes hilft Netskope Ihnen bei der Schaffung einer Sicherheitskultur in Ihrem Unternehmen.

IN DIESEM KAPITEL

- **Vergleich moderner und älterer DLP-Lösungen**
- **Sicherheit, wo immer auf Daten zugegriffen wird**
- **Verwendung einheitlicher Richtlinien und Zugriffskontrollen**
- **Vorteile und Differenzierungsmerkmale von Netskope DLP**

Kapitel 4
Warum ist Netskope der beste Partner für moderne DLP?

Chief Information Security Officers (CISOs) und IT-Sicherheitsteams stehen oft vor einer schwierigen Entscheidung: Sollen sie an bewährten, aber komplexen und kostspieligen älteren DLP-Lösungen festhalten oder auf einfach zu implementierende Cloud-Optionen umsteigen, die möglicherweise nicht die erforderliche Tiefe und Reichweite bieten? Nachdem Sie dieses Kapitel gelesen und die wichtigsten Vorteile von cloudbasierten DLP-Lösungen kennengelernt haben, können Sie diese Frage problemlos beantworten:

- **Sie können eine umfassende Abdeckung bieten.** Ganz gleich, wo Ihre Daten gespeichert sind, wohin sie übertragen werden oder wie auf sie zugegriffen wird – eine in der Cloud bereitgestellte DLP kann diese Daten schützen.
- **Sie können Abdeckung für Cloud-Umgebungen bieten.** SaaS-Anwendungen, IaaS-Services in der Public Cloud und Internetzugriff, unabhängig davon, von wo aus sich Ihre Benutzer im modernen, auf Hybridarbeit ausgelegten Unternehmen verbinden.
- **Sie machen die Einrichtung einer zusätzlichen Infrastruktur überflüssig, da sie schnell und einfach als Cloud-Services bereitgestellt werden können.**

- **Sie schützen Ihre sensiblen Daten, ohne die Ressourcen Ihres Netzwerks und Ihrer Endpunkte zu belasten.** Ein Cloud-DLP-System kann alle von Ihnen benötigten Datenüberprüfungs- und Erkennungsalgorithmen mit höchster Leistungsfähigkeit ausführen.
- **Sie lassen sich leichter mit zahlreichen anderen Sicherheitstools integrieren.**
- **Sie sorgen für eine bessere Sichtbarkeit von Daten, die außerhalb Ihrer Unternehmensgrenzen übertragen und gespeichert werden.**
- **Sie können leichter gewartet und in Echtzeit aktualisiert werden und ermöglichen eine schnellere und einfachere Skalierung als ältere On-Premise-Modelle.**

Nach der Lektüre dieses Kapitels werden Sie verstehen, wie Ihr Unternehmen von diesen Vorteilen profitieren kann, und können eine fundierte Entscheidung darüber treffen, welche cloudbasierte DLP-Lösung für Ihr Unternehmen am besten geeignet ist. Außerdem geben wir Ihnen konkrete Informationen über die Differenzierungsmerkmale der Netskope-Plattform.

Unterschiede zwischen cloudbasierten DLP-Angeboten

Moderne DLP muss in der Cloud bereitgestellt werden. Es gibt zwei Arten von DPL-Lösungen. Cloudnative DLP ist in der Regel in IaaS-Plattformen und SaaS-Anwendungen von Cloud-Service-Anbietern eingebettet. Integrierte Cloud-DLP-Lösungen sind meist Teil eines Sicherheitsservices oder -produkts, z. B. eines Secure Web Gateways (SWG), einer Next-Generation Firewall (NGFW) oder eines Cloud-Access Security Brokers (CASB).

Typ 1: Netskope DLP im Vergleich zu cloudnativen Punktlösungen

Netskope DLP bietet eine Reihe von Vorteilen im Vergleich zu cloudnativen Punktlösungen, die mehrere Einschränkungen aufweisen. Ein entscheidender Vorteil ist die breitere Abdeckung durch eine einzige DLP-Richtlinien-Engine der Enterprise-Klasse, die sicherstellt, dass sensible Daten in zahlreichen Formaten, Kommunikationskanälen und Umgebungen geschützt werden. Dazu gehören beispielsweise SaaS-Anwendungen, IaaS-Services, private Anwendungen, E-Mail-Services, Dateifreigabe und Webtransaktionen - überall dort, wo Ihre Benutzer sind. Netskope DLP enthält auch einen wichtigen

Endpunkt-DLP-Schutz, der dazu beiträgt, dass alle Ihre sensiblen Daten geschützt sind - sogar auf Endpunkten an entfernten Standorten, die über ein bestimmtes Netzwerk mit der Cloud verbunden sein können. Da es nur eine einzige DLP-Richtlinien-Engine gibt, wird die Komplexität erheblich reduziert, weil nicht mehrere DLP-Richtlinien für unterschiedliche Kanäle und Cloud-Services verwaltet werden müssen.

Ein weiterer Vorteil von Netskope DLP ist die erstklassige Erkennungsgenauigkeit dieser Lösung. Netskope DLP überprüft das gesamte Spektrum von Dateitypen und Datenformaten und nutzt dabei eine Reihe von Datenerkennungsalgorithmen und ML, um zahlreiche Informationen und Dokumente sowie deren spezifischen Kontext zu verstehen. Dadurch ist es in der Lage, sensible Daten genau zu identifizieren und zu klassifizieren, selbst wenn sie in unterschiedlichen Strukturen, Formaten, Sprachen oder in Bilder eingebettet gespeichert und übertragen werden. Diese wichtige Funktion trägt dazu bei, dass sensible Daten jeglicher Art nicht versehentlich geleakt oder offengelegt werden, was schwerwiegende Folgen für das Unternehmen haben könnte. Außerdem sorgt sie dafür, dass das System tatsächliche Datensicherheitsmeldungen erzeugt und keine falsch-positiven Meldungen.

Außerdem ist Zero-Trust-Kontext in Netskope DLP integriert, d. h. die Lösung ist so konzipiert, dass sie im Rahmen eines umfassenden Zero-Trust-Sicherheitsframeworks arbeitet. Dieser wichtige Aspekt trägt dazu bei, dass der Zugriff auf sensible Daten sorgfältig und im richtigen Risikokontext kontrolliert und überwacht wird, um das Risiko eines unbefugten Zugriffs, einer übermäßigen Exposition oder eines Datenlecks zu verringern.

Heute bieten viele Cloud Service Provider (CSPs) und SaaS-Anbieter direkt in ihre Plattformen integrierte native DLP-Funktionen an. Diese leicht zugänglichen, auf die Cloud ausgerichteten Lösungen werden häufig von Unternehmen gewählt, die eine Cloud-First-Strategie verfolgen oder gerade erst mit einem Datenschutzprogramm beginnen. Auch wenn diese Lösungen die konkreten Schutzanforderungen von Cloud-Daten erfüllen, für die sie ursprünglich entwickelt wurden, decken sie möglicherweise nicht alle Bereiche ab und sind nicht so umfassend wie ältere DLP-Lösungen.

HINWEIS

Einige Unternehmen beginnen mit diesen cloudnativen DLP-Lösungen, weil sie schnell und einfach zu implementieren sind. Allerdings sollten diese Lösungen sorgfältig geprüft werden, da sie möglicherweise nicht alle Ihre Datenschutzanforderungen erfüllen können. In manchen Fällen sehen sich Unternehmen gezwungen, mehrere unzusammenhängende, voneinander isolierte DLP-Lösungen für spätere

Anwendungsfälle einzusetzen, was zu einer fragmentierten und potenziell weniger effektiven Datenschutzstrategie führt.

Typ 2: Nicht alle integrierten cloudbasierten DLP-Lösungen sind gleich

Beachten Sie bei der Auswahl einer cloudbasierten DLP-Lösung, dass viele neuere Lösungen auf dem Markt erhebliche Mängel aufweisen:

- Sie bieten zwar eine weitreichende Abdeckung, verfügen aber nicht über die technologische Tiefe und die erforderlichen Funktionen, um die sensiblen Daten Ihres Unternehmens in allen modernen Anwendungsfällen effektiv und zuverlässig zu schützen.
- Möglicherweise bieten sie einige der neuesten Methoden und Funktionen für einige spezifische Anwendungsfälle und Datenformate, aber es fehlt ihnen an der nötigen Abdeckung, um die sensiblen Daten Ihres Unternehmens umfassend zu schützen.

HINWEIS

Einige neuere cloudbasierte DLP-Lösungen werden zwar gut vermarktet, sind aber bei Weitem nicht so hoch entwickelt und ausgereift wie die älteren DLP-Lösungen, die sie ersetzen sollen.

Es ist wichtig, DLP-Lösungen gründlich zu recherchieren und miteinander zu vergleichen, um eine Lösung auszuwählen, die die Anforderungen Ihres Unternehmens optimal erfüllt. Achten Sie auf Faktoren wie den Umfang und die Ausgereiftheit der Datenerkennungsfunktionen (z. B. wie viele Dateitypen überprüft werden können und wie viele Datenkennungen verwendet werden, einschließlich länderspezifischer Datentypen), die Bandbreite der abgedeckten Kanäle, die Fähigkeit zur Anpassung an sich ändernde Risiken und Umgebungen sowie das Integrations- und Anpassungspotenzial der Lösung.

Wenn Sie den Einsatz einer cloudbasierten DLP-Lösung in Erwägung ziehen, werden Sie sich wahrscheinlich fragen, welcher Typ für Sie am besten geeignet ist. Folgende Aspekte gibt es dabei zu beachten:

- **Umfang der Abdeckung:** Integrierte DLP-Lösungen sind gewöhnlich in einem SWG, CASB oder NGFW enthalten und oft Teil eines Zero Trust Network Access (ZTNA)-Service. Diese Lösungen werden über die Cloud bereitgestellt und sind in der Regel in einen Netzwerksicherheitsservice integriert. Sie sind in ihrem Umfang begrenzt und bieten zum Beispiel keinen Datenschutz für ausgehende E-Mails, Endpunkte, ein größeres Spektrum an SaaS-Anwendungen und deren spezifische Instanzen (d. h. Firmen- vs. Privatkonten).

- **Einschränkungen der Lösungen:** Beachten Sie, dass diese Lösungen möglicherweise nicht alle modernen und klassischen Anwendungsfälle abdecken, z. B. die Zusammenarbeit mit externen Benutzern in der Cloud, Datentransfers über persönliche E-Mails oder E-Mail-Entwürfe, USB-Dateitransfers, Screenshots und Bilder von sensiblen Dokumenten, neue Compliance-Vorlagen, Daten in Fremdsprachen und Formaten usw. Vor allem ist zu beachten, dass sie möglicherweise unzureichende Erkennungsfunktionen haben. Außerdem sind ihre ML- und KI-Fähigkeiten eventuell ungenügend.
- **Genauigkeit bei der Erkennung sensibler Daten:** Viele neuere cloudbasierte DLP-Lösungen sind nicht in der Lage, sensible Daten genau und granular zu erkennen. Sie überprüfen oft nur eine begrenzte Anzahl von Dateitypen und verfügen nicht über die vielfältigen Datenkennungen, die ausgereiftere Lösungen bieten. Viele dieser Lösungen machen mit ein oder zwei besonderen Funktionen von sich reden, sind aber letztendlich nicht in der Lage, einen umfassenden Datenschutz zu bieten.

  Eine ausgereifte Lösung bietet Tausende von vordefinierten Datenkennungen, einschließlich einer Vielzahl von persönlich identifizierbaren Informationen (PII), darunter Pass- und Kontonummern, internationale Bankdaten, Ausweisinformationen, Finanzdaten, medizinische Daten, Biodaten und branchenspezifische Informationen sowie unterschiedliche Sprachen und anpassbare Kennungen. Die Lösung bietet außerdem eine Reihe vordefinierter Richtlinienprofile zur Unterstützung von Anwendungsfällen und Compliance-Anforderungen wie der Datenschutz-Grundverordnung (DSGVO), dem California Consumer Privacy Act (CCPA), dem Payment Card Industry Data Security Standard (PCI-DSS), dem Health Insurance Portability and Accountability Act (HIPAA) und dem Gramm-Leach-Bliley Act (GLBA), um nur einige zu nennen.
- **Integration in eine Plattform:** Eine cloudbasierte DLP muss eng in eine erweiterte Sicherheitsplattform integriert werden, um sensible Daten im gesamten Risikokontext von Benutzern, Geräten, Netzwerken, Anwendungen, Verhaltensweisen und Zielen effektiv schützen zu können. Eine gut integrierte DLP-Lösung nutzt Informationen von anderen Kontrollpunkten, z. B. Analysen des Benutzerverhaltens, Security Web Gateways der nächsten Generation, CASB, ZTNA und Security Posture Management, um den Sicherheitsstatus eines Unternehmens und die Risiken genau zu verstehen, die mit jeder einzelnen Interaktion mit sensiblen Daten verbunden sind. Die Lösung ist sich der spezifischen Instanzen der verwendeten SaaS-Anwendungen und -Geräte bewusst, unterscheidet zwischen privaten und geschäftlichen E-Mail-Konten, Benutzeridentitäten, den Empfängern

freigegebener Daten und vielen anderen Faktoren. Dank dieser umfassenden Integration ist ein genauerer und detaillierterer Ansatz zur Erkennung und zum Schutz sensibler Daten möglich.

TIPP

Nicht alle Datenschutzlösungen sind gleich, und vielen fehlt es an der notwendigen Ausgereiftheit und Differenziertheit, um ältere Lösungen effektiv zu ersetzen. Einige Hersteller bieten DLP als Add-on zu ihren Kernprodukten an, aber ohne die notwendige Breite und Tiefe bieten diese Lösungen oft nicht das von Unternehmen benötigte Schutzniveau. Jede von Ihnen in Betracht gezogene Lösung sollte getestet werden, damit Sie sicher sein können, dass sie alle derzeit benötigten Datentypen und -mengen unterstützt und ohne Kompromisse alle Punkte abdeckt, an denen Daten das Netzwerk verlassen – sowohl in On-Premises- als auch in Cloud-Umgebungen.

Prüfen Sie sorgfältig, welche Funktionen die einzelnen DLP-Lösungen bieten, und wählen Sie dann eine Lösung aus, die den Anforderungen Ihres Unternehmens sowohl jetzt als auch in Zukunft gerecht wird. Ausgereifte Funktionen und ein engagierter Anbieter sind ausschlaggebend für den Erfolg. Wenn Sie sich nur mit dem Wesentlichen begnügen, kann dies zu ungenauen Ergebnissen, einer eingeschränkten Erkennung und Unmengen an falsch-positiven Meldungen führen.

Netskope blickt auf ein Jahrzehnt kontinuierlicher Innovation und intensiver Bemühungen im Bereich des Datenschutzes zurück und gilt im Vergleich zu anderen SASE- und Security Service Edge (SSE)-Anbietern eindeutig als Vorreiter in der Branche. In den folgenden Abschnitten gehen wir auf die Funktionen und Fähigkeiten ein, durch die sich Netskope DLP auszeichnet.

Wie Netskope DLP für Ihre Sicherheit sorgt

Netskope DLP ist eine umfassende, cloudbasierte integrierte Lösung, mit der Sie Ihre Daten über alle wesentlichen Kanäle hinweg schützen können, einschließlich Clouds, Netzwerken, E-Mails, Endpunkten und Benutzern an jedem Standort. Die Lösung ist risiko- und kontextbewusst, sodass Sie sich darauf verlassen können, dass Ihre Daten immer und überall geschützt sind.

Netskope DLP ist *vollständig* in die in Kapitel 3 beschriebene umfassende SSE-Lösung von Netskope integriert und wird als Teil einer vollständigen SASE-Plattform bereitgestellt. Sie erhalten also eine konvergente, cloudnative Sicherheitsplattform, die blinde Flecken beseitigt,

für Einheitlichkeit sorgt, die Systemleistung verbessert und Kosten und Komplexität reduziert.

Netskope DLP deckt alle Kanäle und alle Arten der Datenübertragung ab, wie in Abbildung 4–1 zu sehen ist. So können Sie sich darauf verlassen, dass Ihre sensiblen Informationen stets geschützt sind. Die Abdeckung umfasst Folgendes:

- fast 60.000 SaaS-Anwendungen, wobei neue Anwendungen und jede Instanz dieser Anwendungen dynamisch klassifiziert werden;
- alle großen IaaS-Anbieter, einschließlich Amazon Web Services (AWS), Google Cloud und Microsoft Azure;
- private Anwendungen im Rechenzentrum oder in der Public Cloud gehostet;
- Ihre Unternehmensnetzwerke und Zweigstellen;
- Ihre mobile Belegschaft;
- alle E-Mail-Services, On-Premises und in der Cloud, einschließlich Webmail;
- alle Endpunkte Ihrer Mitarbeiter, On- und Off-Premises.

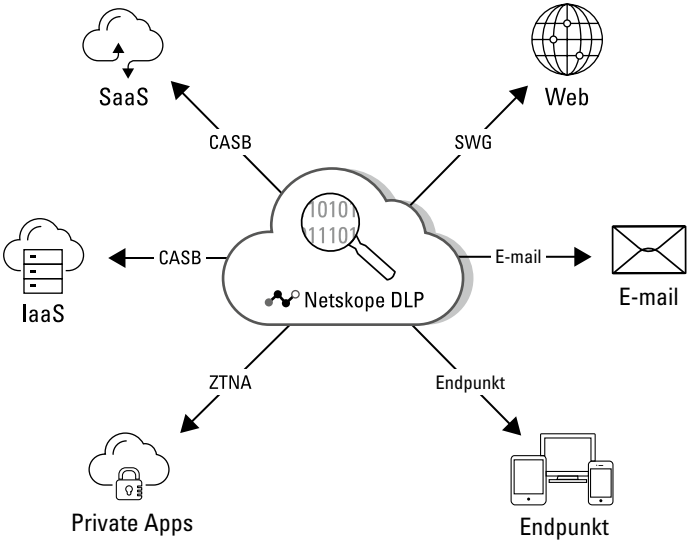

ABBILDUNG 4-1: Netskope DLP schützt Ihre Daten, ganz gleich, wo sie sich befinden.

Wichtige Differenzierungsmerkmale

Einem gängigen Mythos zufolge sind ältere DLP-Lösungen ungenau. Das tatsächliche Problem sind jedoch die falsch-positiven Meldungen, deren Eliminierung mehr Präzision erfordert. Wir haben dies in Kapitel 2 erläutert, wo wir auch über die Hauptbestandteile gesprochen haben, die DLP-Systeme präziser machen können. In diesem Kapitel wird beschrieben, wie Netskope diese Schlüsselfaktoren in wichtige Differenzierungsmerkmale umgewandelt hat, um eine moderne DLP-Lösung bereitzustellen, die an die Bedürfnisse Ihres Unternehmens angepasst und automatisiert werden kann.

Vollständige Abdeckung aller wichtigen Kanäle mit einheitlichen Richtlinien

Sensible Daten, die sich außerhalb der klassischen Unternehmensgrenzen befinden, sind schwerer zu überwachen und zu schützen, und sie sind anfälliger dafür, absichtlich und unabsichtlich offengelegt zu werden. Netskope Cloud DLP erkennt, überwacht und schützt sensible Daten während der Übertragung, im Ruhezustand und bei der Nutzung im gesamten Ökosystem des Unternehmens, beispielsweise in SaaS-Anwendungen, IaaS-Anwendungen in Public Clouds, Unternehmensnetzwerken und Zweigstellen, bei mobilen Mitarbeitern, E-Mail-Services und in Mitarbeiter-Endpunkten.

Die Lösung bietet einheitliche Datenschutzrichtlinien für jeden Ort, an dem Daten gespeichert, verwendet oder übertragen werden, und wird von einem zentralisierten Cloud-Service bereitgestellt.

Eine einzige Konsole mit rollenbasierter Zugriffskontrolle stellt sicher, dass Richtlinienkonfigurationen, Überwachung, Berichterstattung und Incident Response für alle Kanäle über eine einzige Benutzeroberfläche verwaltet werden können.

Erstklassige Erkennung und Schutz sensibler Daten

Datenkennungen sind entscheidend, damit eine DLP-Lösung sensible Daten anhand spezifischer Merkmale identifizieren kann. Dazu gehören Schlüsselwörter, reguläre Ausdrücke, die Anzahl von Ziffern, Sonderzeichen, Muster, Näherungsanalyse usw. Achten Sie beim Kauf einer DLP-Lösung darauf, dass sie über die Identifizierungsfunktionen verfügt, die alle Ihre aktuellen und zukünftigen Anwendungsfälle abdecken. Eine gute DLP-Lösung sollte mehrere Tausend vordefinierte

Kennungen bereitstellen können, um nach den unterschiedlichsten Arten und geringfügigen Variationen von sensiblen Daten suchen und sie genau identifizieren zu können. Dies ist besonders für globale Unternehmen wichtig, die Kennungen für mehrere Länder benötigen. Netskope bietet alle diese Funktionen mit ML sowie die Möglichkeit, Kennungen und Richtlinienvorlagen granular anzupassen, und stellt gleichzeitig sicher, dass alle Ihre Datenschutzanforderungen erfüllt werden.

TIPP

Denken Sie nicht nur an die Datenkennungen, die Sie jetzt benötigen. Sie brauchen eine zukunftssichere Lösung, die auch für Datentypen, Anwendungen und Vorschriften geeignet ist, die es heute noch gar nicht gibt. Halten Sie nach einer Lösung Ausschau, die über Tausende von vordefinierten Datenkennungen und Richtlinienvorlagen für Compliance-Vorschriften wie die DSGVO und CCPA verfügt. Denken Sie auch an die Möglichkeit, benutzerdefinierte Datenkennungen zu erstellen und zu bearbeiten, die an Ihre speziellen Anforderungen angepasst werden können.

Es gibt Tausende von Dateitypen, die sensible Informationen enthalten können, z. B. komprimierte Dateien (ZIP, RAR, ISO usw.), Präsentationen, E-Mails, Bilddateien (BMP, JPG, PNG usw.), Tabellenkalkulationen, CAD-Dateien (Computer-Aided Design), Beiträge in sozialen Medien, Online-Formulare, Chat-Nachrichten, diverse Anhänge und Grafiken. Sie müssen also viele unterschiedliche Arten von Daten im Auge behalten und brauchen eine DLP-Lösung, die mit all diesen Daten umgehen kann.

Die Skalierung von Exact Data Matching (EDM) ist ein wesentlicher Aspekt, den Sie berücksichtigen sollten, besonders wenn Sie ein großes Unternehmen haben oder später expandieren wollen. Ihre DLP-Lösung sollte in der Lage sein, Millionen oder sogar Milliarden von Datensätzen mühelos zu verarbeiten. Moderne cloudbasierte DLP-Lösungen wie Netskope können Cloud-Computing nutzen, um umfangreiche Daten-Fingerprinting-Analysen sogar auf Endpunkten durchzuführen, ohne andere wichtige Prozesse zu beeinträchtigen. Auf diese Weise wird die Gesamtheit der personenbezogenen Daten von Mitarbeitern, Kunden und Partnern usw. umfassend geschützt.

Halten Sie nach einer DLP-Lösung mit fortschrittlichen Erkennungsfunktionen Ausschau – optische Zeichenerkennung (OCR), KI, ML, Fingerprinting von Dateien und Zero-Trust-Strategien –, damit Ihre sensiblen Daten optimal geschützt sind. Alle diese Funktionen sind in Netskope DLP enthalten (und werden in Kapitel 2 beschrieben).

TIPP

REDUZIERUNG DER ANGRIFFSFLÄCHE

Unternehmen, die ihre sensiblen Daten vor Cyberbedrohungen schützen wollen, müssen alle Lücken in Ihrem Schutzsystem eliminieren. Die Angriffsfläche ist die Gesamtheit aller potenziellen Schwachstellen oder Einstiegspunkte, die von Angreifern missbraucht und von Insidern absichtlich oder böswillig genutzt werden könnten. Durch die Begrenzung der Angriffsfläche wird es für Angreifer schwieriger, Schwachstellen zu finden und auszunutzen. Das Schließen bestehender Lücken im Sicherheitssystem kann außerdem das Risiko eines erfolgreichen Angriffs und einer versehentlichen Offenlegung von Daten erheblich verringern. Alle Geräte, Anwendungen und Netzwerke müssen ausreichend gesichert sein, um Sicherheitslücken zu beseitigen, die eine Gefährdung begünstigen könnten.

Netskope DLP kann genau identifizieren, welche Daten sensibel sind, selbst wenn sie in modernen unstrukturierten Formaten wie Bildern (Screenshots und Fotos) oder in unterschiedlichen Sprachen gespeichert sind. Dank hoch entwickelter ML-Klassifizierer ist die Lösung in der Lage, sensible Bilddaten, z. B. in Führerscheinen, Kreditkarten, Ausweisen, Verträgen, Patenten, Dokumenten zu Fusionen und Übernahmen und Schecks zu erkennen, selbst wenn diese Bilder unklar, verschwommen, verzerrt oder beschädigt sind. Die Lösung stellt einen aktiven Schutz für sensible Informationen zur Verfügung, sodass Sie sich darauf verlassen können, dass Ihre Daten auch in der dynamischen Cloud-Welt sicher aufgehoben sind. Auch der Arbeitsaufwand für Ihre Sicherheitsteams wird geringer, da sensible Daten automatisch identifiziert und geschützt werden.

Netskope DLP verfügt über eine Vielzahl von fortschrittlichen ML-basierten Klassifizierungstools, darunter Tausende von Datenkennungen. Die Lösung scannt über 1.600 unterschiedliche Dateitypen mit kontextbezogenen Erkennungsrichtlinien, hochgradig skalierbarem Exact Data Matching, Fingerprinting strukturierter und unstrukturierter Dokumente, präziser ML-basierter Bildklassifizierung, fortschrittlicher OCR und KI/ML-Datenklassifizierer für die Datenerkennung und -identifizierung.

Kontext- und risikobewusster Datenschutz

Bei einem effektiven Datenschutz kommt es vor allem auf den Kontext an. Die Überwachung des Datenverkehrs zwischen Benutzern und

Anwendungen sorgt für eine granulare Kontrolle und bietet Ihnen die Möglichkeit, die Nutzung sensibler Daten auf der Grundlage zahlreicher Faktoren zuzulassen oder zu verhindern. Zum Beispiel basierend darauf, wer der Benutzer ist, was dieser tut und warum er es tut. Dieser datenzentrierte Ansatz ist die beste Methode zur Verwaltung von Risiken in modernen, hybriden Unternehmen.

Mit Netskope DLP gehören Ermüdungserscheinungen bei der Incident Response und Geschäftsunterbrechungen der Vergangenheit an. Die DLP-Lösung von Netskope bietet mehr als einen statischen Ansatz zur Erkennung sensibler Informationen und zur Umsetzung von Richtlinien zur Verhinderung von Sicherheitsverstößen. Sie berücksichtigt den Unternehmenskontext und die damit verbundenen Sicherheitsrisiken, um auf der Grundlage der sich ändernden Bedingungen einen dynamischen Schutz zu gewährleisten.

Netskope DLP ist nativ in die umfassende Netskope Security Service Edge (SSE)-Lösung integriert - eine vollständig konvergierte cloudnative Sicherheitsplattform, die Sicherheitstechnologien wie SWG, CASB und UEBA auf einer einheitlichen, integrierten cloudnativen Plattform konsolidiert. Dieser Ansatz eliminiert blinde Flecken, sorgt für Richtlinienkonsistenz und reduziert die Kosten und Komplexität erheblich. Die Plattform kennt jederzeit das Benutzerverhalten, den geografischen Standort, den Sicherheitsstatus, die Geräterisiken, die mit einer Anwendung verbundenen Risiken und ihren Ruf, die persönlichen Anwendungsinstanzen usw. und ermöglicht es DLP, Incident-Response-Maßnahmen auf echte Datensicherheitsvorfälle zuzuschneiden und dadurch falsch-positive Meldungen, die Triage von Vorfällen und Geschäftsunterbrechungen zu minimieren.

Mit einer einzigen, konvergierten SASE-Datenschutzlösung, die auf Zero-Trust-Prinzipien und fortschrittlichen Datenschutzkontrollen basiert, können Sie die Transparenz und die Risikobegrenzung für alle wichtigen Vektoren verbessern. Doch das ist noch nicht alles: Sie können die Datenklassifizierung, die Definition von Richtlinien und das Vorfallmanagement mit einer konvergenten Plattform vereinfachen, die ML, umfangreiche Berichterstattungsfunktionen und fortschrittliche Analysen nutzt. Und mit flexiblen, kontextgesteuerten Richtlinien und einem schlanken Agenten können Sie die Agilität der Endbenutzer verbessern und Reibungen reduzieren.

ERINNERUNG

Damit Ihr Datenschutzprogramm ein Erfolg wird, müssen Sie Ihre Mitarbeiter schulen und sie zum sicheren Umgang mit Daten anhalten. Netskope DLP bietet Benutzer-Coaching und Sensibilisierungsprogramme in Echtzeit, um genau dies zu erreichen. Außerdem lässt sich die Lösung in führende Lernmanagementsysteme integrieren

und verfügt über ein anpassbares Endbenutzer-Portal für Self-Service-Schulungen zum Thema Datenschutz.

Intelligenter arbeiten mit DLP

Netskope DLP wird aus der Cloud bereitgestellt und ist daher nicht auf On-Premises-Komponenten angewiesen. Außerdem bietet die Lösung einen stets verfügbaren und aktuellen Schutz, sodass manuelle Software-Updates wie bei älteren DLP-Lösungen nicht mehr erforderlich sind.

Mit einheitlichen Datenschutzrichtlinien, einer einzigen Konsole und rollenbasierter Zugriffskontrolle wird die Verwaltung von Richtlinienkonfigurationen ebenso wie die Überwachung, Berichterstattung und die Reaktion auf Vorfälle zum Kinderspiel.

Früher mussten Unternehmen getrennte Richtlinien für alle Kanäle (z. B. Internet, E-Mail und jede einzelne Anwendung) erstellen, was äußerst ressourcenintensiv und zeitaufwendig war. Netskope DLP ist ein einheitlicher, zentralisierter Cloud-Service, mit dem Sie eine einzige Richtlinie für Ihr Unternehmen festlegen und diese automatisch über alle Kanäle hinweg synchronisieren können. Sie müssen Ihre Richtlinie nur einmal erstellen und brauchen sie nicht ständig zu überarbeiten und an mehreren Stellen zu wiederholen.

TIPP

Bei älteren DLP-Lösungen waren viele Systemadministratoren erforderlich, um Richtlinien zu erstellen und zu verwalten. Angesichts des heutigen Fachkräftemangels ist es wichtig, eine Lösung zu haben, die einfach zu verwalten ist.

Eine zentralisierte Benutzeroberfläche und eine einheitliche Verwaltungskonsole sind ebenfalls wichtig, um effektiv und effizient auf Vorfälle reagieren zu können. Vielleicht hatten Sie bisher getrennte Konsolen für On-Premises- und Cloud-Tools, deren Verwaltung oft sehr mühsam und zeitaufwendig ist. Es gibt immer noch einige Anbieter neuerer DLP-Lösungen, die mit mehreren Konsolen arbeiten, was die Sache noch komplizierter macht. Mit Netskope DLP erhalten Sie alle Meldungen über Sicherheitsverstöße an einer Stelle. Die Erkennung sensibler Daten und die Reaktion auf Vorfälle erfolgt einheitlich und in Echtzeit, sodass Sie schnell und effektiv auf potenzielle Bedrohungen reagieren können.

TIPP

Eine zentralisierte Benutzeroberfläche und eine einheitliche Verwaltungskonsole erleichtern den Überblick und optimieren den Incident-Response-Prozess.

Kapitel 5
Zehn Tipps für einen erfolgreichen Übergang zu einer modernen, cloud-basierten DLP-Lösung

Der Austausch eines älteren Sicherheitssystems wie Data Loss Prevention (DLP) durch eine neue Lösung mag uns wie ein gewaltiges Unterfangen vorkommen. Ihre derzeitige Version ist schließlich das Ergebnis jahrelanger Arbeit und komplizierter, aufeinander aufbauender Prozesse. Wie bei einem Kartenhaus berührt jedes Element das andere, und wenn eines davon entfernt wird, droht die gesamte Struktur einzustürzen.

Lassen Sie sich nicht einschüchtern! Eine innovative digitale Transformation ist ein lohnendes Ziel. Und Veränderungen passieren schließlich nicht über Nacht. Beginnen Sie mit kleinen Schritten. Setzen Sie Ihre derzeitigen Investitionen sinnvoll ein, und schon sind Sie auf dem Weg zu einer umfassenden Datenschutzlösung, die sensible Informationen auf allen Plattformen schützt – vor Ort und in der Cloud.

- **Bewerten Sie Ihre Datenschutzanforderungen.** Nehmen Sie sich die Zeit, die aktuelle Technologieumgebung Ihres Unternehmens sorgfältig zu bewerten. Bestimmen Sie, welche Daten geschützt

werden müssen, welche Services und Repositorys zum Speichern und Verarbeiten sensibler Informationen verwendet werden sollen und wie diese Services von Abteilungen und Personen genutzt werden können. Bitten Sie Ihr Sicherheitsteam, speziell alle Unternehmensanwendungen, E-Mail-Services, Collaboration-Tools, Netzwerkstandorte, die hybriden Arbeitspraktiken von Benutzern, externe Geräte und Geschäftsprozesse zu identifizieren und zu bewerten, um Datenflüsse nachzuvollziehen und festzustellen, wie Daten zwischen Mitarbeitern oder mit Dritten ausgetauscht werden.

TIPP

Beschränken Sie sich nicht auf das Sicherheitsteam. Der Chief Data Officer Ihres Unternehmens, die Rechtsabteilung und die Personalabteilung sind weitere Stakeholder, die Ihnen Informationen über die Datennutzung in Ihrem Unternehmen geben können.

Untersuchen Sie alle Kategorien gespeicherter Daten und alle Transaktionen, bei denen Daten über Netzwerke übertragen werden. Bestimmen Sie, welche Priorität unterschiedlichen Datentypen in Ihrem Unternehmen eingeräumt werden sollte. Für Unternehmen, die Unterstützung bei der Einhaltung gesetzlicher Vorschriften benötigen oder aufgrund ineffektiver veralteter Systeme neue DLP-Implementierungen vornehmen müssen, kann diese Phase schnell nützliche Ergebnisse bringen.

- **Identifizieren und mindern Sie Ihre größten Risiken.** Wenn Sie auf eine Datenschutzlösung aus der Cloud umsteigen möchten, sollten Sie zunächst bestimmen, welche Bereiche Ihrer derzeitigen Technologieumgebung die größten Risiken bergen. Denken Sie an die unbeabsichtigte Weitergabe von Daten, die böswillige Exfiltration und andere cloudbasierte Cyberbedrohungen, die mit SaaS-Anwendungen, Cloud-E-Mail und IaaS verbunden sind. Die marktführende Cloud Access Security Broker (CASB)-Lösung von Netskope beinhaltet DLP als Kernkomponente, um die Datensicherheit sowohl für die vom Unternehmen genehmigten Cloud-Anwendungen als auch für nicht genehmigte Anwendungen zu gewährleisten. (Wenn Sie glauben, dass Mitarbeiter keine ungenehmigten Anwendungen nutzen, dann täuschen Sie sich!)
- **Wählen Sie Ihren Datenschutzanbieter sorgfältig aus.** Wählen Sie einen Anbieter, der die Anforderungen Ihres Unternehmens in jeder Umgebung erfüllen kann – heute und in absehbarer Zukunft. Netskope DLP ist der einzige Anbieter, der eine umfassende Abdeckung für alle Cloud-Anforderungen und darüber hinaus bietet. Dies umfasst den Schutz von Daten im Ruhezustand, während der Übertragung und bei der Nutzung in Clouds und vor Ort, Endpunkt-DLP, E-Mail-DLP, Netzwerk-DLP für das Internet und

für E-Mails, DLP für SaaS und IaaS sowie DLP für private Anwendungen. Diese umfassende Abdeckung aller Datenbewegungen in modernen Umgebungen stellt sicher, dass Unternehmen nicht nur beste transparente Einblicke in ihr gesamtes System, sondern auch in nicht vertrauenswürdige Orte haben. Prüfen Sie sorgfältig den Funktionsumfang jeder Lösung, z. B. wie viele und welche Dateitypen die Lösung prüfen kann, die Fähigkeit, Bildformate zu verstehen, und die Abdeckung der unterschiedlichsten sensiblen Daten, einschließlich internationaler und länderspezifischer Kennungen. Beurteilen Sie die Fähigkeit des Systems, so viel Risiko- und Geschäftskontext wie möglich zu nutzen und daher bei jeder Verwendung sensibler Daten adaptiv automatisierte und fundierte Entscheidungen bei der Incident Response zu treffen. Grundsätzlich sollten Sie beim Datenschutz niemals einen oberflächlichen Ansatz wählen, der mehr Probleme schafft als Lösungen bietet.

- **Schützen Sie Ihre E-Mail-Services und Ihre Collaboration-Anwendungen.** Mit Netskope DLP können Sie sich die Leistungsfähigkeit von cloudbasiertem E-Mail- und SaaS-Schutz zunutze machen. Diese umfassende DLP-Lösung schützt alle sensiblen Daten Ihres Unternehmens, einschließlich ausgehender sensibler E-Mails und asynchroner Kommunikation über SaaS-basierte Collaboration-Anwendungen wie Slack und Teams. Mit Programmierschnittstellen (APIs), Inline-Schutz in Echtzeit, Schutz für die Zusammenarbeit mit externen Partnern und sogar Instanzerkennung – also die Unterscheidung zwischen privaten E-Mail- und SaaS-Instanzen und geschäftlichen Instanzen derselben Services – können Sie sicher sein, dass Ihre Unternehmensdaten unter allen Umständen geschützt sind. Mit Netskope können Sie sich darauf verlassen, dass die Zusammenarbeit und Kommunikation in Ihrem Unternehmen reibungslos abläuft.
- **Schützen Sie Ihre cloudbasierte E-Mail.** Entdecken Sie die Leistungsfähigkeit des cloudbasierten E-Mail-Schutzes von Netskope DLP. Diese umfassende DLP-Lösung schützt alle sensiblen Daten Ihres Unternehmens vor böswilligen Angriffen und unbeabsichtigter Datenfreigabe. Mit Programmierschnittstellen (APIs), Inline-Schutz in Echtzeit und sogar Datenschutz in privaten E-Mail-Instanzen können Sie sich darauf verlassen, dass Ihre Unternehmensdaten in jedem Fall sicher sind. Mithilfe von Netskope können Sie Ihren E-Mail-Service beruhigt in die Cloud migrieren.
- **Sichern Sie Ihre Daten während der Übertragung ab.** Es kann schwierig sein, Daten zu verwalten und zu schützen, die über unterschiedliche Standorte, Verbindungen, Services und Geräte hinweg übertragen werden, z. B. über Heimnetzwerke, Firmenbüros,

Zweigstellen, Unternehmensgeräte und persönliche Geräte. Herkömmliche DLP-Lösungen mit Proxy-Verbindung garantieren nicht immer einen ausreichenden Schutz bei der Übertragung von Daten. Netskope bietet einen einheitlichen DLP-Service, der über die gesamte intelligente Security Service Edge (SSE)-Plattform von Netskope bereitgestellt wird. Er schützt sensible Daten an jedem Ort, an dem Ihre Mitarbeiter arbeiten. So erhalten Sie ein Höchstmaß an Sicherheit für Ihre Datentransaktionen, einschließlich aller Vorteile, die Zero-Trust-Prinzipien und der gesamte verfügbare Risikokontext bieten, ohne dass Sie sich mit obskuren Hardwarekonfigurationen abmühen müssen. Mit der innovativen DLP-Lösung von Netskope können Sie sich darauf verlassen, dass Ihre Daten zu jeder Zeit und an jedem Ort geschützt sind.

- **Schützen Sie die Daten auf den Endpunkten Ihrer Mitarbeiter.** Auch wenn immer mehr Daten heute in der Cloud gespeichert werden, müssen Sie dennoch sicherstellen, dass auf Endpunkten befindliche sensible Dateien nicht verloren gehen oder gestohlen werden. Dabei spielt es keine Rolle, ob diese Geräte mit einem Unternehmensnetzwerk verbunden sind oder nicht. Netskope DLP kann Ihnen beim Schutz Ihrer sensiblen Daten helfen, ganz gleich, ob sie auf einem Endpunkt erstellt oder aus der Cloud heruntergeladen wurden. Diese kompakte Endpunktlösung bietet alle fortschrittlichen DLP-Funktionen – wie auf maschinellem Lernen (ML) basierende Klassifizierer, optische Zeichenerkennung (OCR), Fingerprinting von Dateien, Exact Data Matching (EDM) und mehr – bei minimaler Ressourcenbelastung, da sie die Cloud nutzt. Mithilfe der Lösung kann eine Vielzahl von Anwendungsfällen wie die Erkennung von Daten, die über USB übertragen werden, abgedeckt werden. Sie bietet außerdem Schutz von USB-Geräten und andere Richtlinien zur Gerätekontrolle, damit Ihre vertraulichen Daten sicher sind, ganz gleich, von wo aus Ihre Mitarbeiter auf sie zugreifen wollen.
- **Halten Sie an dem fest, was für Sie funktioniert, während Sie für die Zukunft planen.** Wenn Sie vor Kurzem in DLP-Funktionen eines Cloud Service Providers oder SaaS-Anbieters investiert haben, kann es sinnvoll sein, zunächst bei diesem Anbieter zu bleiben. Wenn zum Beispiel ein SaaS-Anbieter Ihre Office-Anwendungen bereits gut schützt, müssen Sie nicht sofort wechseln. Irgendwann wird jedoch der Punkt erreicht sein, an dem Sie zu viele einzelne, unzusammenhängende Richtlinien verwalten müssen. Wenn Sie den Datenschutz auf mehrere Clouds und SaaS-Anwendungen ausweiten möchten, haben Sie es am Ende mit zu vielen Konsolen und unterschiedlichen Richtlinien zu tun. Netskope DLP bietet eine

einfachere Lösung: eine Konsole mit einheitlichen Richtlinien, die Ihre Daten unabhängig von ihrem Speicher- oder Zugriffsort schützen kann.

- **Profitieren Sie von einem umfassenden Datenschutz.** Netskope DLP bietet einen modernen Ansatz zum Schutz von Daten, der effizienter und effektiver ist als jemals zuvor. Fortschrittliche Erkennungstechnologien wie ML, das Fingerprinting von Daten und Bilderkennung werden in vollem Umfang und in noch nie dagewesenem Ausmaß genutzt, sogar auf den Endpunkten, da die Rechenkapazität aus der Cloud bereitgestellt wird. Die zentrale Konsole mit einheitlichen Richtlinien erleichtert die Verwaltung der Datenschutzanforderungen des gesamten Unternehmens. Durch das Erfassen und Analysieren von Risikofaktoren und kontextbezogenen Informationen über Benutzer, Geräte, Daten, Netzwerke, Clouds und Verhaltensweisen ist Netskope DLP in der Lage, jede Interaktion mit sensiblen Daten zu bewerten und Maßnahmen dynamisch an jede spezifische Richtlinienverletzung anzupassen. Dieser neue Ansatz unterstützt sichere Praktiken für die Zusammenarbeit und die gemeinsame Nutzung von Daten, ohne die Produktivität zu beeinträchtigen. Er minimiert Fehlalarme und führt zu genaueren Datenschutzergebnissen. Netskope DLP ist nativ in die übergreifende Netskope SSE-Plattform integriert und daher stets über Geschäftsrisiken, Verhaltensweisen und Sicherheitsschwachstellen informiert. Da Netskope DLP vollständig in Netskope SSE eingebunden ist, sind Unternehmen stets über Geschäftsrisiken, Verhaltensweisen und Schwachstellen informiert.
- **Nutzen Sie institutionelles Wissen.** Die Umstellung auf eine neue cloudbasierte Lösung für DLP kann überwältigend erscheinen. Das muss aber nicht so sein. Nutzen Sie die Erfahrung und das Wissen der Mitarbeiter, die Ihr bestehendes DLP-System verwaltet haben, ebenso wie die Kenntnisse Ihrer Richtlinienadministratoren und Ihres Incident-Response-Teams. Ihr Fachwissen kann dazu beitragen, dass Best Practices bei der Umstellung auf ein cloudbasiertes System übernommen werden. Dieses Know-how kann Ihrem Unternehmen auch dabei helfen, technologische Anforderungen zu erfüllen, da Profile für die Einhaltung von Richtlinien erstellt und neue Workflows zur Behebung von Vorfällen entwickelt werden können. Netskope DLP hilft Ihnen dabei, die an Ihr DLP-Team gestellten Anforderungen zu reduzieren. Ihre Sicherheitsteams werden also immer weniger Zeit mit der Bewältigung frustrierender Vorfälle verbringen und mehr Zeit für proaktive Initiativen haben, die die Sicherheit Ihres Unternehmens erhöhen.

- **Setzen Sie auf Reife, nicht auf Hype.** Für den Erfolg ist mehr als technisches Know-how erforderlich. Sie müssen viel beachten, von der Entwicklung von Kennzahlen für die Geschäftsleitung bis hin zu Anleitungen und Aktionspunkten für Ihre Mitarbeiter. Lassen Sie sich von den Support-Teams Ihres Anbieters bei der Strukturierung des Prozesses unterstützen. Mit seiner Hilfe können Sie das Potenzial Ihrer Unternehmensinnovation voll ausschöpfen und eine erfolgreiche Umstellung erreichen.

Sicherheit, die auf alles vorbereitet ist

Netskope, ein weltweit führender SASE-Anbieter, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen dabei zu helfen, Zero-Trust-Prinzipien zum Schutz von Daten anzuwenden. Die Netskope-Plattform ist schnell und einfach zu bedienen und bietet optimierten Zugriff und Echtzeitsicherheit für Personen, Geräte und Daten, egal wo sie sich befinden. Netskope hilft Kunden, Risiken zu reduzieren, die Leistung zu steigern und einen unübertroffenen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten. Tausende Kunden, darunter mehr als 25 der Fortune 100, vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk bei der Bewältigung sich entwickelnder Bedrohungen, neuer Risiken, technologischer Veränderungen, organisatorischer und netzwerkbezogener Änderungen sowie regulatorischer Anforderungen. Erfahren Sie, wie Netskope Kunden dabei hilft, auf ihrer SASE-Reise auf alles vorbereitet zu sein, besuchen **Sie netskope.com/de**.

netskope

Vorbereitung auf eine Cloud-First-Zukunft mit moderner DLP-Technologie

Der raschen Verbreitung von Cloud-Computing und dem Trend zum dezentralen Arbeiten sind ehemals fortschrittliche Datenschutztechnologien nicht mehr gewachsen. Datensicherheitsbemühungen sind überall dort erforderlich, wo Menschen und Daten unterwegs sind. Die ideale Lösung für eine moderne Data Loss Prevention (DLP) muss speziell für die Cloud entwickelt worden sein. Es reicht nicht, ältere Systeme nachträglich für Cloud-Anwendungsfälle umzurüsten. Die Lösung muss Zero-Trust-Prinzipien anwenden, die Komplexität reduzieren und eine einheitliche Durchsetzung von Richtlinien gewährleisten, und zwar überall.

Im Buch ...

- Bewertung Ihres Datenschutzansatzes
- Schutz Ihrer Daten und Unterstützung der Geschäftsziele
- Die Funktionsweise moderner DLP
- Minimierung von unbefugtem Datenzugriff
- Vereinfachte, effektive Sicherheitsrichtlinien
- Sicheres Verschieben von Daten in die Cloud und zwischen Cloud-Anwendungen

netskope

Carmine Clementelli ist Spezialist für Cybersicherheit und führender Technologieexperte für Datensicherheit, Cloud-Sicherheit, Zero Trust und Security Service Edge (SSE) bei Netskope. Er war zuvor bei Palo Alto Networks, Symantec und anderen globalen Unternehmen tätig und verfügt über jahrzehntelange Erfahrung als Autor, Referent und Berater.

ISBN: 978-1-394-20802-9
Nicht für den Wiederverkauf.

für dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.