

Data Loss Prevention – Anforderungskatalog

MÄRZ 2009

Gijo Mathew

CA SECURITY MANAGEMENT

Inhaltsverzeichnis

Kurzfassung	1
ABSCHNITT 1	2
Warum ist Data Loss Prevention einer der wichtigsten Bereiche der IT-Sicherheit?	2
ABSCHNITT 2	2
Die acht wichtigsten Voraussetzungen zur effektiven Vermeidung von Datenverlusten	2
ABSCHNITT 3	8
Fazit	8
ABSCHNITT 4	9
Der Autor	9

Kurzfassung

Ausgangssituation

Immer mehr digitale Informationen werden in Unternehmen erstellt und gemeinsam genutzt. Diese Daten effektiv und effizient zwischen Standorten oder Personen austauschen zu können, ist für den Erfolg jedes Unternehmens eine wichtige Voraussetzung. Jedoch genau die Technologien (z. B. E-Mail, Web, IM usw.), die dieses hohe Maß an Konnektivität und Zusammenarbeit von Mitarbeitern, Kunden und Partnern ermöglichen, stellen zugleich ein immenses Sicherheitsrisiko für Unternehmen dar. Ein einziger Missbrauch vertraulicher Daten durch „Insider“ – sei es aus Versehen, absichtlich oder gar mutwillig – kann für Unternehmen weitreichende finanzielle und juristische Folgen haben, große Vertrauensverluste bedeuten und das Markenimage schädigen.

Chance

Es gibt die Möglichkeit, das Bewusstsein für den Wert und die korrekte Nutzung vertraulicher Informationen zu schaffen. Wenn Sie wissen, wo sich die wertvollen Informationen im Unternehmen befinden, wie und wohin sie bewegt werden und welches Risiko sie darstellen, können Sie Risiken minimieren. Ihre DLP-Lösung sollte neben der Vorbeugung von Verstößen gegen die Sicherheit persönlicher Daten, geistigen Eigentums und anderer nichtöffentlicher Informationen auch in der Lage sein, Gefahren durch ungeschützte und nicht regelkonforme elektronische Datenübertragungen zu mindern.

Nutzen

Mit einer umfassenden Lösung können Unternehmen die Nutzung vertraulicher Daten im Unternehmen erkennen, klassifizieren und kontrollieren. Das bietet folgende Vorteile.

- Identifizierung und Analyse von Daten an allen Kontrollpunkten, z. B. am Endpunkt, im Nachrichtenserver und im Netzwerk
- Minimierung des Risikos spektakulärer Verluste persönlicher Daten und geschützter Patienteninformationen
- Verhinderung der versehentlichen oder vorsätzlichen Veröffentlichung sensibler Daten
- Einhaltung von behördlichen und branchenspezifischen Datenschutzvorschriften
- Vermeidung von Verstößen gegen allgemeine Sicherheits- und Verhaltensregeln des Unternehmens

ABSCHNITT 1

Warum ist Data Loss Prevention einer der wichtigsten Bereiche der IT-Sicherheit?

Informationen gehören zu den wichtigsten Ressourcen von Unternehmen. Jedes Unternehmen möchte in der Lage sein, überall und von jedem Gerät auf Informationen zuzugreifen und mit praktisch jedermann zusammenzuarbeiten. Der Wunsch nach „freien“ Informationen birgt jedoch viele Herausforderungen beim Sicherheits- und Risikomanagement. Unternehmen sind inzwischen dazu übergegangen, nicht mehr die IT-Infrastruktur, sondern die Informationen selbst zu schützen. Dazu müssen sie wissen, wo kritische Daten verwendet und gespeichert werden. Kompliziert wird diese Herausforderung durch firmeneigene und gesetzliche Compliance-Anforderungen, die Sorge um den Schutz von Kunden- und Mitarbeiterdaten sowie höhere Kosten im Falle eines Datenverlusts.

Um die Risiken unkontrollierter Nachrichtenübermittlung oder Internet- und Dateiaktionen einzudämmen, müssen Unternehmen wissen, wo sich ihre wertvollen Informationen genau befinden, wie und wo sie verwendet werden und welches Risiko sie darstellen. Vor allem müssen sie sicherstellen, dass sie nicht in falsche Hände gelangen – sowohl innerhalb als auch außerhalb des Unternehmens.

Es gibt sehr viele DLP-Lösungen auf dem Markt, die sich alle ähnlicher Fähigkeiten zur Minimierung von Datenverlusten rühmen. Deshalb ist es schwierig zu erkennen, welcher Weg für Ihr Unternehmen der beste ist, um das Gefahrenpotenzial zu verringern und ihre vertraulichen und sensiblen Daten optimal zu schützen. Mit unkomplizierter Sprache, viel gesundem Menschenverstand und unter Anlehnung an vorhandene Standards soll Ihnen dieser Leitfaden die acht wichtigsten Anforderungen an eine DLP-Lösung nahe bringen, die Sie dabei unterstützt, Datenschutzverletzungen abzuwehren, bevor sie überhaupt auftreten. Wir haben in diesem aufschlussreichen Leitfaden die wichtigsten Anforderungen einiger der Unternehmen für Sie zusammengestellt, die sich weltweit am meisten für den Datenschutz einsetzen.

ABSCHNITT 2

Die acht wichtigsten Voraussetzungen zur effektiven Vermeidung von Datenverlusten

1. Anfälligste Schwachstellen erkennen und vorrangig beseitigen

Die ungewollte, interne oder externe, Offenlegung vertraulicher Informationen (Finanz-, Geschäfts-, Personaldaten, juristische oder behördliche Informationen), persönlicher Daten (Sozialversicherungsnummern, Kreditkarteninformationen, Patienteninformationen) und geistigen Eigentums (Patente, Markenzeichen, Entwürfe) kann an vielen verschiedenen Stellen in Ihrem Netzwerk passieren. Deshalb muss eine umfassende DLP-Lösung wirklich alle potenziellen Schwachstellen in Ihrem Unternehmen schützen.

Der lückenlose Schutz aller gefährdeten Stellen ist für eine DLP-Lösung zwar das ultimative Ziel, tatsächlich macht es aus taktischen und finanziellen Gründen jedoch durchaus mehr Sinn, zunächst die Daten (und die Systeme, mit denen diese Daten übertragen werden) zu schützen, die für Ihr Unternehmen das größte Risiko darstellen. Für die meisten Unternehmen ist als meist genutzte elektronische Anwendung sicherlich E-Mail das anfälligste Medium mit einem hohen Datenverlustrisiko. Angesichts der Tatsache, dass in einem normalen Unternehmen nahezu jeder Mitarbeiter mehr als 100 Nachrichten pro Tag versendet und

Riskantes Verhalten

- Schätzungen von Forrester zufolge geschehen 80 % aller Datenschutzverletzungen aus Versehen. Quelle: The Forrester Wave™: Data Leak Prevention, 2. Quartal 2008, Forrester Research, 6. Juni 2008
- Der interne Missbrauch von Netzwerkzugriffen oder E-Mail verwies Virenangriffe auf Platz 2 bei den häufigsten Sicherheitsproblemen. Quelle: Umfrage von CSI/FBI
- Neue staatliche bzw. regionale Vorschriften und neue Branchenregelungen setzen die IT-Abteilungen zusätzlich unter Druck, wenn es darum geht, private und vertrauliche Informationen zu schützen.

empfängt, stellt E-Mail eine wahrlich offensichtliche Gefährdung dar, denn sensible und vertrauliche Informationen können allzu leicht in falsche Hände geraten. Eine zusätzliche Gefahr sind die unterschiedlichen Quellen von E-Mails, von denen nicht wenige Sicherheitslücken aufweisen, z. B. Desktops, mobile Geräte, öffentliche Computer, webbasiertes Firmen-E-Mail und vom Netzwerk getrennte Laptops.

Direkt nach E-Mail folgen bei den Risiken für das Unternehmen Wechselspeichermedien wie USB-Sticks, iPods, CD/DVD-Brenner und vom Netzwerk getrennte Laptops, denn auf diesen Geräten können mehrere Hunderte Megabyte Daten gespeichert werden. Auch nicht kontrollierte Aktivitäten im Internet bergen unzählige Risiken für Datenverluste, insbesondere Tools, bei denen Dateien freigegeben werden, oder die populären sozialen Netzwerke, u. a. Instant Messaging, Webmail, Internetforen, Blogs und Wikis.

Weitere Schwachstellen, die geschützt werden müssen, sind Dateiscansysteme, Repositories, Dokumentmanagementsysteme, Mailarchive für sensible und vertrauliche Daten sowie Kommunikationsprotokolle wie FTP, SMTP und HTTP.

KERNPUNKT 1 Erst wenn die Hauptrisiken wie Firmen-E-Mail, Wechselspeichergeräte und Internetaktivitäten an allen wichtigen Schwachpunkten – Netzwerk, Endgeräte (Desktop-PCs, Laptops usw.) und Infrastrukturserver für Messaginganwendungen – ausreichend geschützt sind, macht es Sinn, andere exponierte Stellen im Unternehmen zu überwachen und zu schützen.

2. Hohe Präzision ist entscheidend

Da bei einfachen inhaltsbasierten Analysen Datenschutzverletzungen mit Hilfe eines lexikalischen Abgleichs aufgedeckt werden, werden für jeden gefundenen echten Verstoß auch Hunderte eigentlich konforme Ereignisse gekennzeichnet. Wenn Ihre Prüfwarteschlange voller „Fehlalarme“ ist, bleibt Ihnen nichts anderes übrig, als Hunderte Vorfälle (davon die meisten legitime Aktionen) manuell zu überprüfen, Verstöße erst nach dem Ereignis zu bewerten, oder Richtlinien zu übergehen. All diese Optionen, die auf einfachen Erkennungsmethoden beruhen, erhöhen die Wahrscheinlichkeit eines Datenverlusts erheblich, da tatsächliche Verstöße unerkannt bleiben und die Kennzeichnung zu vieler Ereignisse zu signifikanter Beeinträchtigung des Betriebs führen kann.

Die einzige Möglichkeit, potenzielle Verstöße wirksam zu bekämpfen, ist der Einsatz einer Analysetechnik, die Identitäten und Geschäftsabläufe erkennt, d. h. wirkliche Verletzungen aufdeckt aber legitime Geschäftsaktivitäten zulässt. Dieses Maß an Präzision ist nur möglich, wenn die Lösung nicht nur einfache Schlüsselwörter und Phrasen abgleicht, sondern den Inhaltzusammenhang und den Kontext untersucht und auch die Unternehmenshierarchie und die Identität der Endbenutzer berücksichtigt. Besonders der Kontext spielt bei der Unterscheidung eines möglichen Datenschutzverstoßes von einer berechtigten Aktion eine große Rolle. Ein Beispiel: Bei einem inhaltsbasierten Ansatz würde zur Erkennung dreistelliger Creditscores eine Datei oder Nachricht, die die Zahl „225“ enthält, wahrscheinlich als potenzieller Verstoß gekennzeichnet werden. Auch wenn dreistellige Creditscores nur zwischen 300 und 850 gültig sind, sollte diese Information nicht sofort als mögliche Datenschutzverletzung ausgelegt werden. Wird z. B. die Zahl „703“ zwischen zwei Klammern erkannt, handelt es sich viel wahrscheinlicher um eine Telefonvorwahl im US-Staat Virginia als um einen Creditscore.

Neben der standardmäßigen Beurteilung positiver Treffer gehört zur exakten Analyse auch die Gewichtung und Einordnung von Regelabweichungen, um zu bestimmen, ob eine Datei oder Nachricht gekennzeichnet werden soll oder nicht. So kann ein spezieller Schwellenwert beispielsweise eine Datenschutzverletzung vorgeben, wenn in einem Dokument oder einer Nachricht 50 neunstellige Zahlen gefunden werden. Aber was ist, wenn nur 48 dieser Zahlen vorhanden sind – sollte das Objekt dann grünes Licht erhalten? Wohl eher nicht.

Die Berücksichtigung von Identitäten, z. B. den Autor eines Dokuments, den Absender/Empfänger einer E-Mail und die jeweilige Rolle im Unternehmen, ist eine weitere wichtige Analyseverfahren, um festzustellen, ob eine Aktion ein wirkliches Datenverlustrisiko darstellt.

KERNPUNKT 2 Wenn die DLP-Lösung, für die sich Ihr Unternehmen entscheidet, keine umfassende und präzise Inhaltsanalyse durchführen kann, werden Sie nicht in der Lage sein, unter unzähligen Fehlalarmen tatsächliche Verstöße zu erkennen und zu beheben. Ein derart wirkungsloses Erkennungssystem wird Sie also sogar daran hindern, potenzielle Datenschutzverletzungen sicher und proaktiv abzuwehren, da viele der gekennzeichneten Aktionen zulässige Geschäftsaktivitäten sind.

3. Auf bewährten, vordefinierten Richtlinien beharren

Jeder DLP-Lösung sollte ein umfassender Katalog mit effektiven Richtlinien zugrunde liegen, der zudem umfassende und präzise Analysen nutzt, um für ein Ereignis die richtige Reaktion bereitzustellen.

Es ist zwar wichtig, schnell und einfach Richtlinien erstellen und anwenden zu können, ebenso wichtig ist es jedoch, dass die angewandten Richtlinien die Best Practices und Geschäftsregeln Ihres Unternehmens effektiv umsetzen.

Ihre DLP-Lösung sollte ein vollständiges Paket von anpassbaren, vordefinierten und getesteten Richtlinien beinhalten, mit denen zahlreiche Sicherheits- und Complianceprobleme angegangen werden können bzw. die mit höchster Genauigkeit ein bestimmtes Risikogebiet abdecken. Die meisten Richtlinien sollten sich sofort und hundertprozentig an allen kritischen Schwachstellen einsetzen lassen, darunter E-Mail, Internet und Instant Messaging. Einige erfordern möglicherweise eine kundenspezifische Konfiguration, um in einer bestimmten Umgebung optimalen Betrieb zu gewährleisten. Mit beiden Ansätzen lassen sich der Zeit- und Arbeitsaufwand für die Konzeption, Priorisierung, Entwicklung und Implementierung Ihrer DLP-Richtlinien erheblich senken.

Ein idealer Richtlinienkatalog sollte vorgefertigte, erprobte Methoden und Konzepte enthalten, die Optionen zur angemessenen Reaktion auf Verstöße bieten, und zwar auf Grundlage dessen, wer beteiligt war, was passiert ist und was gefunden wurde.

KERNPUNKT 3 Auch wenn sich eine Richtlinie einfach konfigurieren lässt, wird eine DLP-Lösung mit zu einfachen oder eingeschränkten Richtlinienfunktionen keinen ausreichenden Schutz vor Datenverlust bieten können. Sie sollten auf einem umfassenden Paket bewährter, vordefinierter Richtlinien beharren, um möglichst viele Risiken abzudecken und schnell einsatzfähig zu sein.

4. Mehr als nur vertrauliche und sensible Daten schützen

Ihre DLP-Lösung sollte neben der Vermeidung von Verstößen gegen die Sicherheit persönlicher Daten, geistigen Eigentums und anderer nichtöffentlicher Informationen auch in der Lage sein, Gefahren durch ungeschützte und nicht regelkonforme elektronische Datenübertragungen zu mindern. Zu diesem Spektrum gehören auch unangemessenes oder anstößiges Verhalten von Mitarbeitern, Kommunikation, die gegen behördliche und gerichtliche Vorgaben verstößt, Verhalten, das Rechtsansprüche und Strategie des Unternehmens gefährdet, unkontrollierte Finanztransaktionen und unangemessene Behandlung von Kundenbeschwerden.

Sie sollten außerdem sicherstellen, dass die Lösung umfassende firmeneigene Regelungen und gesetzliche Anforderungen erfüllt: von HIPAA, SOX, GLBA und PCI bis zu branchenspezifischen Vorgaben von SEC, NASD, NYSE und FSA.

KERNPUNKT 4 Eine effektive DLP-Lösung kann und sollte zahlreiche Probleme im Bereich Informationssicherheit angehen, die über den reinen Schutz sensibler und vertraulicher Informationen hinausgehen. Die meisten Unternehmen beginnen zunächst mit dem reinen Schutz vor Datenverlust und dehnen den Schutz dann auf weitere Gebiete aus, wie den Missbrauch von Informationen.

5. Angemessen auf jeden einzelnen Vorfall reagieren

Sobald ein Ereignis als Verstoß identifiziert wurde, sollte Ihre DLP-Lösung in Echtzeit mit einer geeigneten Aktion darauf reagieren, z. B. Objekte sperren, in Quarantäne stellen, Warnmeldungen ausgeben, Daten verschlüsseln oder einfach nur informieren. Danach sollten entsprechende Schritte für die sofortige Lösung des Problems bereitgestellt werden. Jede Antwort sollte speziell auf die Art und den Schweregrad der Verletzung zugeschnitten sein. Insbesondere muss dabei berücksichtigt werden, wer involviert ist. So muss z. B. eine Verletzung, die durch den Vorstand des Unternehmens verursacht wurde, anders behandelt werden als ein Verstoß durch Vertriebsmitarbeiter oder Forschungsteammitglieder.

Weitere geeignete Reaktionen sind: Umleitung einer Nachricht oder eines Benutzers auf eine Website mit Angaben zu den Sicherheitsrichtlinien des Unternehmens, Unterstützung bei der Durchführung der aktuellen Aufgabe, Klassifizierung der entsprechenden Nachricht oder Datei, Aktualisierung eines Incident-Dashboards oder die unbemerkte Aufzeichnung problematischer Aktivitäten. Außerdem sollten Sie in der Lage sein, alle ruhenden Dateien zu verschieben, zu kopieren, zu löschen oder zu kennzeichnen.

Um sicherzustellen, dass Verstöße immer lokal behandelt werden, müssen die Reaktionsmaßnahmen an allen potenziellen Schwachstellen greifen, darunter Desktops, Nachrichtenserver, Netzwerk, Dateirepositorys sowie bei Import und Analyse vergangener Ereignisse.

KERNPUNKT 5 Anstelle eines allgemeinen Ansatzes, der nur passive Prüfung nach dem Ereignis oder wahlloses Sperren aller vermeintlichen Datenschutzverletzungen erlaubt, sollte Ihre DLP-Lösung ausreichend Flexibilität bieten, damit bei jedem Richtlinienverstoß die richtige Maßnahme erfolgen kann.

6. Reaktionsprozesse optimieren

Bei der Hälfte des Kampfes gegen Datenverluste geht es darum, tatsächliche Informationslecks aufzudecken und gleichzeitig Fehlalarme auf ein Minimum zu reduzieren. Die andere Hälfte ist die effiziente, entschiedene Lösung der Verstöße, und zwar so zeitnah wie möglich. Um dieses Ziel ohne Beeinträchtigung der Geschäftsabläufe zu erreichen, benötigen Sie eine umfassende, automatisierte und rundum anpassbare Anwendung zur Problembekämpfung, mit deren Hilfe Vorgesetzte und Administratoren problematische Aktivitäten überprüfen, eskalieren, kommentieren, melden und lösen können.

Der optimale Prozess zur Problembekämpfung sollte stets systemeigene Sichtbarkeitskontrollen enthalten, mit denen sich eindeutig bestimmen lässt, welcher Vorgesetzte eine bestimmte Datenschutzverletzung überprüfen darf. Um den ordnungsgemäßen Ablauf einer Aktion zu unterstützen, muss eine webbasierte Problembekämpfungsanwendung konfigurierbare und benutzerfreundliche Prüffunktionen bereitstellen, damit Ereignisse vollständig und einfach bewertet werden können. Hierzu gehören auch die Automatisierung der Prüfprotokollerstellung und die Aufzeichnung wie, wann und von wem ein Vorfall im System bearbeitet wurde. Der Prüfer muss in der Lage sein, alle relevanten Informationen anzuzeigen, d. h. die vollständige Nachricht, ganze Dateien und Anhänge im Originalformat. Außerdem muss er automatisch bzw. ad hoc Suchläufe durchführen und ähnliche Vorfälle leicht auffinden können, die ihm bei weiteren Nachforschungen helfen.

Der Einsatz von Fall-Management-Tools von Drittanbietern oder die Verarbeitung schwer verständlicher Systemaktivitätsprotokolle darf nicht erforderlich sein. Der Autor problematischer Inhalte muss bei Bedarf über automatische, geschützte und von der Prüfanwendung versendete Nachrichten über den Status des Vorfalls bzw. die erforderlichen Maßnahmen benachrichtigt werden können.

KERNPUNKT 6 Ihre DLP-Lösung sollte nicht nur alle tatsächlichen Datenschutzverstöße aufdecken, sondern auch eine schnelle und effiziente Lösung ermöglichen.

7. Aufklärung und Selbsthilfe für Endbenutzer

Eine effektive Data Loss Prevention-Lösung muss mit den Mitarbeitern kommunizieren, damit sie verstehen, warum eine bestimmte Aktivität unangemessen ist, und so potenzielle Verstöße in Zukunft selbst korrigieren und vermeiden können.

Die kontinuierliche Sensibilisierung der Benutzer fördert korrektes Verhalten und über die Konsequenzen der Verletzung von Unternehmensrichtlinien auf. Durch geeignete Kommunikation zum richtigen Zeitpunkt lässt sich sicherstellen, dass Richtlinien den Mitarbeitern immer bewusst sind, was die Sensibilisierung für die Problematik von Datenverlusten stärkt. Dieses Element der Lösung kann Ihre laufenden Schulungs- und Sensibilisierungsmaßnahmen in den Bereichen Nutzung elektronischer Kommunikation, Personalwesen, Ethik, Elektronikrichtlinien usw. nahtlos ergänzen.

Wenn Unternehmen ihre Mitarbeiter besser und zeitnah (d. h. schon beim Klicken auf „Senden“) über die Gefahren von Datenverlusten aufklären, lassen sich eventuelle Verstöße langfristig drastisch reduzieren, was das Unternehmensrisiko, die Arbeitslast der IT sowie den Zeit- und Kostenaufwand erheblich verringert.

KERNPUNKT 7 Die meisten Daten kommen zwar unbeabsichtigt abhanden, kontinuierliche Aufklärung hat jedoch auch eine abschreckende Wirkung auf die Personen, die mutwillige Aktionen planen, da sie sich so bewusst werden, dass ihre Aktivitäten unter Beobachtung stehen. Und die Mitarbeiter, die aus Versehen gegen Richtlinien verstoßen, sind froh zu wissen, wie sie ihre Aktionen korrigieren können.

8. Flexible Architektur implementieren

Mit einer auf modularen, verteilten Datenanalysekomponenten basierenden DLP-Lösung können Unternehmen ihren dringendsten Anforderungen unmittelbar und kosteneffektiv nachkommen und neue Kontrollmöglichkeiten einführen, sobald dies nötig ist. Eine derartige Plattformarchitektur ermöglicht es Systemadministratoren zu bestimmen, welche Kombination von Kontrollpunkten den für ihr Unternehmen erforderlichen Schutz bietet. In manchen Fällen sind vielleicht nur Kontrollen für Desktops oder Laptops erwünscht, während in anderen Kontrollpunkte im Netzwerk erforderlich sind. In bestimmten Situationen lassen sich die DLP-Ziele eines Unternehmens durch die Kombination serverbasierter Kontrollen mit Desktop- und Netzwerkkontrollen erreichen.

Ein modularer Ansatz ermöglicht die schnelle Implementierung, eliminiert einzelne Fehlerquellen, lässt sich problemlos skalieren und sorgt so für den Schutz von 500 oder auch 500.000 Mitarbeitern. Die Endpunkt- oder Clientkomponenten sollten auch dann Schutz bieten, wenn sie von einem zentralen Server oder dem Firmennetzwerk getrennt werden. Wenn sich der Benutzer wieder mit dem Netzwerk des Unternehmens verbindet, müssen neue Richtlinien automatisch heruntergeladen und erfasste Vorfälle sofort hochgeladen werden.

Die Plattform sollte die automatische Verteilung der Richtlinien sicherstellen, so dass unmerklich für den Benutzer die richtige Richtlinie schnell, sicher und an der richtigen Stelle angewendet wird. Dies fördert zugleich die Akzeptanz. Alle Funktionen müssen unabhängig von der Anzahl verwendeter Richtlinien oder Kontrollpunkte (50.000 Desktops oder fünf Netzwerkausgangspunkte) unterstützt werden.

Darüber hinaus muss die DLP-Lösung in beliebiger Abfolge an unterschiedlichen Stellen (z. B. Desktops, Netzwerk, Messaging-Server und Repositories) funktionieren, und ergänzende Module müssen mit wenig Aufwand später hinzugefügt werden können. Bei Einführung neuer Datentypen, Kanäle und Protokolle sollte sich die Lösung auch auf diese neuen Anforderungen umstellen lassen.

KERNPUNKT 8 Im Vergleich zu einer starren oder unerprobten Lösung ist eine modulare, verteilte Architektur, die höchste Flexibilität, Skalierbarkeit, Leistungsfähigkeit und Fehlertoleranz bietet, der beste Weg, um sowohl aktuelle als auch künftige Anforderungen im Bereich Datenschutz zu erfüllen.

Fazit

CA Orchestra Data Loss Prevention erfüllt alle acht entscheidenden Anforderungen

CA Orchestra DLP schützt Unternehmen vor den verschiedensten Formen des Datenverlustes und Missbrauchs. Es erkennt tatsächliche Datenschutzverletzungen mit weitreichenden finanziellen und juristischen Folgen, großem Vertrauensverlust und Schädigung des Markenimage, und behandelt sie angemessen. Branchenführende Erkennungs- und Analysemethoden verhindern, dass riesige Warteschlangen mit Fehlalarmen entstehen. So können sich Unternehmen auf die Überwachung von Richtlinienverstößen und Datenverlusten durch tatsächliche Verletzungen konzentrieren und sofort Abhilfemaßnahmen ergreifen.

CA Orchestra DLP überwacht und erkennt Verstöße an vielen Kontrollpunkten, darunter E-Mail, IM, Internet, Mobile Mail, FTP, Dateirepositorys und Aktivitäten am Endgerät. Sobald eine Datenschutzverletzung gefunden wird, werden entsprechende Aktionen eingeleitet wie Sperren, Warnmeldungen, Quarantäne oder die Benachrichtigung von Vorgesetzten.

Wichtig ist auch, dass der intelligente Prüfvorgang zahlreiche Funktionen zur Verfügung stellt, mit denen Administratoren sich ausschließlich auf die Sicherheitsverletzungen konzentrieren können, die in ihren Zuständigkeitsbereich fallen. Ein integrierter Workflow bietet erweiterte Suchfunktionen, Eskalationsmöglichkeiten und weitere Fallmanagementmaßnahmen, die alle automatisch in einem umfassenden Prüfprotokoll aufgezeichnet werden. Nicht zuletzt trägt die laufende Aufklärung dazu bei, dass Mitarbeiter Datenverlustrisiken verstehen, selbst korrigieren und in Zukunft vermeiden.

Mit CA Orchestra Data Loss Prevention können Unternehmen ihre vertraulichen und sensiblen Daten schützen und kontrollieren, wo auch immer sie gespeichert und verwendet werden. Dies senkt die Risiken durch unkontrollierte Informationen erheblich. Die Lösung zielt auf die ganze Bandbreite an Risiken, minimiert jedoch auch Beeinträchtigungen des Betriebs, die durch die Erkennung und Behebung dieser Risiken entstehen können. Die Verhinderung von Datenverlusten ist Teil einer ganzheitlichen IAM (Identity and Access Management)-Strategie. Mit einer Komplettlösung sind Unternehmen in der Lage, Identitäten zu verwalten, Zugriffe zu kontrollieren und die Datennutzung berechtigter Anwender zu schützen. Dieser Ansatz unterstützt Unternehmen bei der Rationalisierung ihrer IT-Sicherheitsumgebungen und der Einhaltung von Vorschriften und Datenschutzregelungen und bietet ihnen mehr Sicherheit und Flexibilität. Durch die Implementierung umfassender, automatisierter und integrierter Lösungen erhalten Unternehmen schlanke und effiziente IT-Systeme und erreichen eine schnellere Amortisierung und die Reduzierung von Kosten, manuelle Prüfungen und Sicherheitsrisiken.

Weitere Informationen, wie CA Orchestra Data Loss Prevention das IT-Management vereinheitlicht und vereinfacht, finden Sie unter www.ca.com/dlp.

Der Autor

Gijo Mathew – Vice President, CA

Gijo Mathew ist dank seiner zehnjährigen Erfahrung in der Software-Entwicklung und bei Sicherheitsthemen in der Lage, die Anforderungen von Kunden zu erkennen, das Sicherheitsbewusstsein zu stärken und geschäftsorientierte Strategien in Unternehmen umzusetzen. Bei CA stellt er sicher, dass Lösungen den Ansprüchen von Kunden, den Anforderungen des Marktes und den Branchenstandards entsprechen. Seine Fachkompetenz erstreckt sich auf viele Sicherheitsbereiche, darunter Data Loss Prevention, Security Information Management und Identity Management. Gijo Mathew ist Certified Information Systems Security Professional und bringt seine Fachkenntnisse ein, um Unternehmen dabei zu unterstützen, Sicherheitsmaßnahmen mit einem ausgewogenem Verhältnis von Geschäftsanforderungen und Risiken umzusetzen.

CA, einer der größten Anbieter von IT-Management-Software, vereinheitlicht und vereinfacht unternehmensweite IT-Umgebungen auf sichere Weise, um bessere Ergebnisse zu erzielen. Unsere Vision eines Enterprise IT Managements und die daraus entwickelten Lösungen unterstützen unsere Kunden dabei, ihrer IT effizient zu steuern, zu verwalten und zu sichern.

Weitere Informationen, wie CA das IT-Management vereinheitlicht und vereinfacht, finden Sie unter:

CA Deutschland GmbH
ca.com/de

CA Software Österreich GmbH
ca.com/at

CA (Schweiz) IT Solutions Management AG
ca.com/ch/de

MP335110309