druva

White Paper

Vorbereitung auf die neue Welt des Datenschutzes: Was globale Unternehmen wissen müssen

Dieses Papier ist für leitende IT-Führungskräfte, welche die Datenschutzbelange in ihren Organisationen adressieren

Zusammenfassung

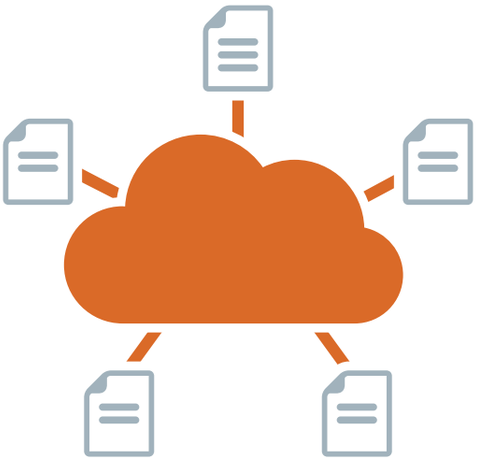
Aufgrund der strenger werdenden Datenschutzbestimmungen auf der ganzen Welt gibt es ein immer größeres globales Bewusstsein für den Datenschutz. Nachrichten über das elektronische Massenüberwachungs-Data-Mining-Programm der NSA (PRISM), großflächige Überwachungspraktiken von EU-Mitgliedstaaten, stark beachtete Datenlecks und Diebstähle, und „Bring-your-own-device (BYOD)“ erhöhen das Bewusstsein für dieses Problem. Globale Unternehmen wissen, dass sie ihre IT-Infrastruktur anpassen müssen, um immer vielfältigere regionale Datenschutzbestimmungen zu unterstützen oder sich potenziellen Sanktionen und/oder rechtlichen Folgen gegenüber sehen. Allerdings weiß aber nicht jeder genau, was notwendig ist, um sich in der neuen Datenschutzlandschaft richtig zu verhalten. Dieses Papier gibt Empfehlungen für Unternehmen, die sich auf diese neue Welt der Datenschutz-Compliance vorbereiten.

Unternehmerische Bedenken bei Speicherung von Daten in der Cloud

Angesichts der jüngsten Verbesserungen der Kosteneffizienz, und dem wachsenden Vertrauen in die Cloud-Sicherheit gab es eine signifikante Verschiebung der Unternehmens-IT in die Cloud. Laut der Unternehmensberatung BCG wächst Software as a Service (SaaS) dreimal schneller als lokale Software.[1] Dies geschieht, weil Cloud Computing mehrere Vorteile hat. Unternehmen können ihre Investitionen zu den Betriebskosten verlagern und haben somit mehr Geld für Kernprojekte. Das Finanzieren von Projekten wird mit einem Abomodell viel einfacher. Und - Cloud-Services sparen auch IT-Ressourcen und bieten eine schnellere Wertschöpfung, weil es keine Software zu installieren oder Geräte zu verwalten gibt.

Viele Unternehmen nutzen die Cloud für E-Mail und Produktivitätsanwendungen, und zum Speichern von Buchhaltungs- und Finanzinformationen, Abrechnungsdaten, Patientenabrechnungsinformationen, Verwaltungsinformationen, Patientenakten sowie des geistigen Eigentums. IT-Teams, die traditionellen Hüter der Unternehmensdaten, müssen nicht nur die Preisgabe dieser Daten verhindern, sondern auch das geistige Eigentum des Unternehmens sichern und schützen, falls ein Gerät einmal verloren geht oder gestohlen wird, ein Mitarbeiter das Unternehmen verlässt oder für eDiscovery im Falle von Rechtsstreitigkeiten.

Organisationen sehen enorme Kosten-, Flexibilitäts- und Skalierbarkeitsvorteile beim Sichern der Daten von Laptops, Mobiltelefonen und anderen Endpunktdaten in der Cloud; aber andererseits haben sie Bedenken, einem Cloud-Service-Anbieter ihre Daten anzuvertrauen, speziell im Hinblick auf den Datenschutz, Sicherheit und die Verfügbarkeit von sensiblen Daten über unzählige Geräte und Netzwerkverbindungen hinweg. Je nach Branche oder geographischer Lage eines Unternehmens kann es verschiedenen Vorschriften wie HIPAA oder Datenspeicherortgesetzen unterliegen und muss dann dafür sorgen, dass es mit all diesen Vorschriften auch kompatibel bleibt, wenn die Daten in der Cloud gespeichert sind. Die Unternehmen wollen auch sicherstellen, dass die Produktivität der Endbenutzer nicht durch Ausfallzeiten der Cloud-Dienste beeinträchtigt wird, und dass das Unternehmen keinen permanenten Datenverlust riskiert, wenn einem Dritten sensible Unternehmensdaten anvertraut werden.



1. Von der Cloud profitieren: So gehen Sie mit Software as a Service (SaaS) um

Anforderungen an die Compliance mit den Datenspeicherortgesetzen

Viele Länder haben Regelungen eingeführt, um Unternehmensdaten, einschließlich der personenbezogenen Daten (PII), privaten Gesundheitsinformationen (PHI), persönlichen und Unternehmenssteuer-Informationen, Unternehmensfinanz-Informationen und Telekommunikations-Informationen rechtlich zu schützen. Ein Verstoß gegen diese Bestimmungen kann zu Geldstrafen und strafrechtlicher Verfolgung der Personen führen, die für die nicht geschützten Daten verantwortlich sind. Der Aufstieg von Cloud-Datenspeicherung und -Backup zwingt mit Datenschutz und Datensicherheit befasste IT-Führungskräfte dazu, Möglichkeiten zu finden, die rechtlichen und regulatorischen Verpflichtungen zu minimieren, und gleichzeitig die Aufgaben und Anforderungen ihrer Betriebsdatenspeicherung zu

erfüllen.[2]

Je nach Standort können Unternehmen Datenspeicherortgesetzen und -vorschriften unterliegen, wonach sie ihre Daten nur in einer bestimmten geografischen Region speichern dürfen. Globale Unternehmen mit Mitarbeitern in verschiedenen Ländern benötigen Zugriff auf Rechenzentren in vielen Regionen und näher an ihren Nutzern. Cloud-Anbieter sollten in der Lage sein, regionale Datenzentren auf der ganzen Welt zu nutzen, sodass sie regionale Unterschiede bei den Datenschutzvorschriften angehen und den Bedürfnissen der globalen Unternehmen anpassen können.

Zum Beispiel haben einige Anbieter ihre Rechenzentren in Europa, aber die USA haben Zugriff auf die dort gespeicherten Daten oder Metadaten. Dies ist ein wesentliches Anliegen für Unternehmen, die in Ländern mit strengen regionalen Datenspeicherortgesetzen Geschäfte machen. Microsoft hat sich kürzlich mit diesem Thema vor Gericht befassen müssen. Im Dezember 2013 präsentierten die US-Bundesstaatsanwälte einen Durchsuchungsbefehl, um im Zusammenhang mit einer Untersuchung wegen eines Medikaments die Inhalte und Metadaten eines Microsoft-Benutzerkontos ausgehändigt zu bekommen. Während die Metadaten in den USA gelagert wurden, waren die Inhalte der E-Mails in Irland gespeichert. Microsoft weigerte sich, die E-Mails zu übergeben, und gab als Begründung an, dass die US-Regierung ein Unternehmen nicht zwingen kann, in einem anderen Land gespeicherte Daten auszuhändigen. Laut InformationWeek „streitet sich Microsoft darum, das Zugriffsrecht auf die auf ihren Servern gespeicherten Daten zu behalten, ohne die Daten auf Anforderung herausgeben zu müssen. Ein verlorener Prozess vor Gericht könnte bedeuten, dass als einzige praktikable Option für Cloud-Computing-Unternehmen bleibt, eine Unwissenheitspolitik (Zero-Knowledge-Policy) zu verfolgen - um dadurch nicht in der Lage zu sein, Zugriff auf Kundendaten in der Cloud zu geben. Eine Haltung, die Apple und Google bereits für Daten auf dem Handy angenommen haben."[3]

Das europäische Datenschutzgesetz (Data Protection Act, DPA) unterscheidet zwischen „Datenkontrolleuren" - Personen oder Organisationen, welche den Zweck und die Art und Weise bestimmen, mit der alle persönlichen Daten verarbeitet werden sollen - und „Datenverarbeitern" - natürlichen oder juristischen Personen, welche die Daten im Namen der Datenkontrolleure verarbeiten.[4] Der wesentliche Unterschied zwischen den beiden ist, dass der eine die Befugnis hat, Daten zu verarbeiten, und der andere die Befugnis hat, zu entscheiden, wer die Daten verarbeiten darf. Diese Trennung ermöglicht es Organisationen und Gremien, im Fall eines Datenmissbrauchs, die Verantwortlichen zu bestimmen.[5]

Entsprechend diesem Modell bieten einige Cloud-Anbieter verschiedene Ebenen des Administratorzugriffs, je nach Abteilung des Administrators und individueller Rolle. Auf einer Ebene haben Administratoren Gesamt-Admin-Rechte in allen Bereichen des Service, und können den Zugriff von anderen Administratoren jederzeit widerrufen. Auf einer anderen Ebene haben Administratoren eingeschränkte Rechte, entsprechend dem Benutzerprofil oder regionalen

2. Fünf Cloud-Datenspeicherort-Probleme, die nicht ignoriert werden dürfen
3. Microsoft gewinnt Verbündete gegen die US-Datenherausgabe
4. Information Commissioner's Office Leitfaden zum Datenschutz
5. Die Datenkontrolleure und Datenverarbeiter: Was der Unterschied ist und wo die Governance- Implikationen liegen

getrennten administrativen Rechten. Diese delegierten Verwaltungsfunktionen ermöglichen es Unternehmen, Privatsphäreeinstellungen eindeutig zu konfigurieren, und trotzdem immer noch ein einheitliches System zur Datenerhebung zu haben, das vom Unternehmen verwaltet wird.

Warum ist es wichtig, die Privatsphäre - und nicht nur die Sicherheit zu adressieren

Ein Großteil der Datenschutzdebatte findet im Rahmen der Netzwerksicherheit und der Verteidigung gegen Bedrohungen von außen statt. Wenn man über gefährdete Daten nachdenkt, dann in der Regel im Rahmen eines Internet-Sicherheitsangriffs durch eine böswillige externe Einheit, die herausfindet, wie man Systeme hackt und Daten stiehlt; das führt zu Verwirrung bei Sicherheit im Gegensatz zu Privatsphäre. Es ist zwar wichtig, sich vor Cyber-Angriffen zu schützen, es ist es aber ebenso wichtig, zu verstehen, wie viele sensible Informationen relativ frei innerhalb von Organisationen und ohne wirkungsvolle Kontrollen fließen, um den Missbrauch von Unternehmens- und Mitarbeiterdaten zu vermeiden.

„Der Schutz von Daten ist wichtig, aber ohne Berücksichtigung angemessener Datenschutzmaßnahmen sind Daten - und Unternehmen - gefährdet. Mehr als je zuvor müssen heute globale Organisationen regionalen Datenvorschriften entsprechen," erklärt Jaspreet Singh, CEO bei Druva. „Datenschutzrechtliche Bedenken werden in die Top- Prioritäten der IT gezwungen. Das ausschließliche Konzentrieren auf die Sicherheit kann die Privatsphäre gefährden, für Organisationen für negative Publicity sowie mögliche rechtliche und regulatorische Maßnahmen sorgen."[6]

Datenschutz ist ein vielschichtiges Thema. Es beginnt mit der Speicherung und Sicherung von Daten, schließt aber auch Prozesse und Steuerungsmaßnahmen zur Adressierung weitergehender Privatsphäreanliegen mit ein. Cloud-Anbieter adressieren Datenschutz und Datensicherheit typischerweise durch Authentifizierung und Zugriffssteuerung. Dadurch wird sichergestellt, dass nur die richtigen Personen Zugriff auf Unternehmensdaten haben. Verschlüsselung hält die Daten sicher, aber sie garantiert nicht unbedingt, dass die Daten privat bleiben. Was wirklich zählt ist, wo die Schlüssel für die Verschlüsselung gespeichert werden, und wer Zugang zu ihnen hat. Wenn ein Cloud-Service-Provider Zugriff auf Verschlüsselungsschlüssel eines Unternehmens hat, entweder direkt oder über einen Treuhandanbieter, kann er Zugriff auf die Daten dieses Unternehmens ermöglichen. Und wenn der Anbieter einmal vorgeladen wird, kann er die Daten ohne Zustimmung des Kunden zur Verfügung stellen. Bei diesen Modellen kann es einen hohen Grad an Sicherheit geben, aber die Daten werden nicht wirklich privat gehalten.

Manchmal werden Verschlüsselungsschlüssel auf dem Server hinter der Firewall gespeichert. Während dies verhindert, dass der Service-Provider auf die Schlüssel zugreift, bedarf es zusätzlichen Hardware-Managements oder eines Schlüsselservers vor Ort, der den Grund für die Auswahl eines Cloud-Service negiert, und einen „Single Point of Failure" für den Zugriff auf Ihre Daten bereitstellt.

Mit den heutigen mobilen Arbeitsmethoden möchten die Benutzer jederzeit und überall auf ihre Daten zugreifen können. Dies bedeutet, dass sie die Möglichkeit zur Selbstwiederherstellung ihrer Daten benötigen, falls etwas schiefgehen sollte. Bei den meisten Implementierungen können die Benutzer nur dann eine Selbstwiederherstellung durchführen, wenn das Endbenutzergerät den Verschlüsselungsschlüssel besitzt. Aber die Speicherung des Schlüssels auf dem Gerät kann zu zusätzlichen Sicherheitsrisiken führen. Wenn das Gerät samt dem gespeicherten Schlüssel verloren geht oder gestohlen wird und das Gerät selbst nicht verschlüsselt ist, kann von einem Außenstehenden auf den Schlüssel zugegriffen werden.

Geschäftsszenario für bessere Systeme mit besserer Unterstützung des Datenschutzes

Da immer mehr Daten in die Cloud verschoben und Benutzeranwendungen von den Unternehmensmitarbeitern

6. Druva kündigt Cloud-Datenschutz-Framework an

angenommen werden, gibt es zusätzliche und neue Bedenken hinsichtlich der Privatsphäre innerhalb der Organisationen. Vertrauliche Finanzdaten, PII, und andere Daten, finden ihren Weg auf Geräte und Netzwerke außerhalb der Aufsicht der IT. Trotz dieser Fragmentierung und mangelnder Transparenz, sind Organisationen nach den Datenschutzbestimmungen moralisch und rechtlich verpflichtet, die Vertraulichkeit der Daten ihrer Benutzer zu schützen. Während viele Unternehmen über die Weitsicht verfügen, Richtlinien und Verfahren einzurichten, um die Datensicherheit und den Datenschutz zu gewährleisten, bedeutet dies nicht, dass diese Vorschriften auch befolgt werden. Es ist unrealistisch, diese Verantwortung in die Hände von Menschen zu legen, und dann von ihnen zu erwarten, sich streng an die Leitlinien zu halten. Technologien wie Verschlüsselung, Datentrennung und Richtlinienerstellung können die Lücken füllen, um Unternehmen beim Erzwingen der Einhaltung der Vorschriften und der Einhaltung von Datenschutzrichtlinien zu unterstützen. Bei der Entwicklung von Datenschutzrichtlinien ist es für Unternehmen wichtig, zu prüfen, wie Systeme den Datenschutz mittels den verschiedenen Funktionen innerhalb der verwendeten Produkte unterstützen.

Laut Rick Kam, Präsident und Mitbegründer von ID-Experts, sollten Unternehmen eine aktive Haltung einnehmen und Datenschutz als Teil der täglichen Arbeit wahrnehmen, statt zu warten, bis es zu einem Datenvorfall kommt. „Aufgrund neuer Risiken, wie BYOD, Cloud Computing, Informationsaustausch über Gesundheitsdienstleister und so weiter, müssen die Richtlinien, Verfahren und Technologien diese Risiken adressieren“, sagt Kam. „Neben der Anwendung von Standardrisiko-Managementpraktiken, wie jährliche Risikobewertung und Zeitpunkt-Risikobewertungen für neue Anwendungen, müssen diese neuen Risiken auf eine ganzheitliche Art und Weise angegangen werden.“ [7]

Unternehmen erkennen, dass die Nutzer durch den Einsatz von BYOD und File Sharing-Lösungen immer produktiver werden. Während die IT es auf den Schutz und die Sicherung von Daten sowie einen Einblick in die gespeicherten Daten anlegt, sind Mitarbeiter mehr an Komfort, Produktivität und Schutz ihrer personenbezogenen Daten interessiert. Um diese Bedenken auszuräumen, benötigen Unternehmen einen IT-geführten Weg, um den Zugriff auf Mitarbeiterdaten zu vermeiden, die sich auf Geräten neben den Unternehmensdaten befinden können. Mitarbeiter in Unternehmen mit einer BYOD-Politik haben das Recht, ihre Geräte für persönliche und Unternehmensdaten zu benutzen. Der Arbeitgeber hat Zugriff auf alle Daten auf diesen Geräten, muss aber darauf achten, dass er personenbezogene Daten der Mitarbeiter nicht kopiert oder anzeigt, damit die Privatsphäre gewahrt bleibt; dies ist vor allem auf globaler Ebene ein Problem.

Wie Druva inSync den Datenschutz in der Cloud gewährleistet

Unternehmen erkennen, dass sie sich auf Lösungen verlassen müssen, die speziell für die Zwecke der Aufrechterhaltung der Privatsphäre und der Sicherheit von Unternehmensdaten entwickelt wurden, und dass Sicherheit allein nicht den heutigen globalen Anforderungen genügt. Endpoint-Backup-, Datenverlustvorsorge-, File Sharing- und Data Governance-Werkzeuge können einen umfassenden Schutz von Unternehmensdaten gewähren, indem strenge Normen für den Datenschutz und die Sicherheit in der Cloud angewendet werden.

Druva inSync zentralisiert und steuert Geschäftsdaten auf Desktops, Laptops, Tablets und Smartphones der Mitarbeiter, über integrierte Datensicherung, Schutz vor Datenverlust, IT-verwaltetes File Sharing und Data Governance-Steuerungen. inSync spiegelt kontinuierlich Mitarbeiter-Gerätedaten und schafft eine zentrale, überwachbare Ablage von Unternehmensinformationen. Dies ermöglicht die Datenwiederherstellung für verlorene oder gestohlene Geräte, gestattet für Remote-Benutzer von jedem Gerät aus den Zugriff auf eine Datei oder einen Ordner, und unterstützt eDiscovery-, Compliance- und Forensik-Bedürfnisse.

inSync besitzt eine Kombination von Sicherheitsvorkehrungen zum Schutz von Organisationen gegen unerlaubten Zugriff und zur Verhütung von Missbrauch von Mitarbeiterdaten durch autorisierte

7. Ponemon: Die Quantifizierung des Wertes des Unified Endpoint Data Management

Benutzer und zur Sicherstellung der Datenintegrität für rechtliche und Compliance-Initiativen. Regionale Speicherung bietet Unterstützung für 11 globale regelkonfigurierbare Admin-wählbare Regionen, um sicherzustellen, dass Daten entsprechend DPA-Anforderungen gespeichert werden. Einzelinstanzobjektlagerung von Blockdaten hält Daten von Metadaten getrennt, und liefert eine Datenverwürfelung nach der es keine Querverweise unter gespeicherten Objekten mehr gibt. Metadaten und Blöcke werden mit einem einzigartigen Umschlag-Key-Verschlüsselungsmodell verschlüsselt, das den Datenschutz gewährleistet; niemand - nicht einmal Druva unter Gerichtsbeschluss - kann Zugriff auf Kundendaten freigeben. Endbenutzer-Sicherheitseinstellungen können je nach regionalen Anforderungen auf privat eingestellt werden, um sicherzustellen, dass Administratoren keine Einsicht in ihre Daten haben.

Eine Datenschutzregelung für Führungsmitglieder, die eventuell mit sensiblen Materialien umgehen müssen, verhindert, dass ihre Daten durch andere Personen in der Organisation eingesehen werden können. Audit-Trails für Endbenutzer und Administratoren stellen sicher, dass alle Datenzugriffe und File Sharing-Aktivitäten mit manipulationssicheren Überwachungsprotokollen nachverfolgt werden, sodass die Datenschutzverletzungen und Störungen der Datenintegrität für Forensik-, Regulatoren-, eDiscovery- und Compliance-Untersuchungen identifiziert werden. Und inSync bietet Unternehmen die Möglichkeit, einen Rechts/Compliance-Administrator zu benennen, der nach bestimmten Richtlinien die Privatsphäre außer Kraft setzen kann, damit vom General Counsel ausgewählte Personen die Data Governance durchsetzen können.

Die Möglichkeiten delegierter Administration umfassen Geo-definierte Governance-Funktionen, die den Datenschutz gewährleisten. Kunden können vielfältige regionale Datenschutzanforderungen in einer einzigen Cloud-Lösung unterstützen, indem sie den Datenzugriff auf Benutzer oder Administratoren in bestimmten Regionen beschränken. Diese geo-spezifischen Möglichkeiten sind für globale Unternehmen mit z. B. Betrieben in Deutschland entscheidend, da DPA dort strenge Vorschriften für Mitarbeiterdaten enthält, darunter ein Verbot von Datenspeicherung außerhalb des Landes.

Die Nutzung von Amazons AWS Cloud-Infrastruktur bietet inSync-Kunden die Möglichkeit, ihre Daten in acht verschiedenen Regionen der Welt, einschließlich Nordamerika, Europa, Asien-Pazifik und Südamerika zu lagern. Beispielsweise würde ein Kunde mit Nutzern in Deutschland, die AWS-Cloud in Deutschland für die Datensicherung nutzen. Dieser Kunde kann einen Admin delegieren, der physisch in Deutschland sitzt, und dort die Gruppe der deutschen Mitarbeiter verwaltet. Ein globaler Administrator hebt die Sichtmöglichkeiten auf, sodass sie die Daten in Deutschland nicht sehen können. Es kann auch ein deutscher Administrator bestimmt werden, der keinen Einblick in die Daten hat, aber Backup und Recovery kontrollieren kann. Dies erlaubt es uns, strenge regionale Anforderungen für die private Aufbewahrung der Daten zu befolgen, und sie dort zu speichern, wo es sein muss, sodass Unternehmen ihr Geschäft weltweit ausführen können.

Fazit

In der heutigen sich ändernden globalen Landschaft des Datenschutzes ist es entscheidend, die wichtigsten Fragen zu kennen, um den Datenspeicherortgesetzen zu entsprechen und den Datenschutz für Unternehmens- und Mitarbeiterdaten zu berücksichtigen. Unternehmen müssen jetzt nicht nur Daten regeln und schützen, sondern auch dafür sorgen, dass Cloud-Service-Provider strenge Datenschutzrichtlinien für die Speicherung von Daten in der Cloud befolgen. Cloud-Anbieter bemühen sich, diese Herausforderungen zu erfüllen, und die Privatsphäre und die Sicherheit von sensiblen Unternehmensdaten sicherzustellen, sodass Ihr Unternehmen von den neuesten Vorteilen von Cloud- und Mobile-basierten Geschäftstransaktionen profitieren kann sowie schwerwiegende Reputations-, Finanz- und rechtliche Folgen vermieden werden.

Datenschutz-Bereitschaftstest

Lesen Sie die folgenden Anforderungen an den Datenschutz für alle in der Cloud gespeicherten Daten.

Wie gut ist Ihr Unternehmen?

Regionaler Datenschutz

Datenspeicherort: Hat Ihr IT-Administrator die Möglichkeit, Regionen für den Datenspeicherort zu bestimmen?

- ○ Ja
- ○ Nein
- ○ Ich weiß nicht

Lokaler Admin: Können IT-Administratoren getrennt und Ihnen vordefinierte granulare Zugriffsrechte übertragen werden?

- ○ Ja
- ○ Nein
- ○ Ich weiß nicht

Produktion mit Anbietern: Wird verhindert, dass Anbieter Zugriff auf gespeicherte Daten oder Metadaten haben?

- ○ Ja
- ○ Nein
- ○ Ich weiß nicht

Privatsphäre der Mitarbeiter

Individuelle Privatsphäre: Können Anwender die Privatsphäreeinstellungen steuern oder Admin-Daten, Metadaten oder Audit-Trail-Einsicht abwählen?

- ○ Ja
- ○ Nein
- ○ Ich weiß nicht

Datenabgrenzung: Sind die Daten auf Laptops und Smart Devices in Containern?

- ○ Ja
- ○ Nein
- ○ Ich weiß nicht

Mitarbeiter (DPA): Gibt es ausschließende Einstellungen für die Datensicherung und das Sammelverfahren, wobei die Admin-Sichtbarkeit bei Audit-Trails über Regeln beschränkt wird?

- ○ Ja
- ○ Nein
- ○ Ich weiß nicht

Fortsetzung auf der nächsten Seite

Datenschutz-Bereitschaftstest

Unternehmensdatenschutz

Daten für Führungskräfte: Gibt es Gruppeneinstellungen für Klassen über Active Directory (Führungskräfte, Rechtsabteilung etc.), um die Datensichtbarkeit einzuschränken?

- Ja
- Nein
- Ich weiß nicht

Datenprüfung: Können Daten für die Überwachung der Compliance für PHI und PII vollständig auditiert werden?

- Ja
- Nein
- Ich weiß nicht

Tracking & Überwachung: Ist die Überwachung aktiv und auf Basis von Datenklassifikationen?

- Ja
- Nein
- Ich weiß nicht

Szenario-basierter Datenschutz

Compliance: Gibt es delegierte Rollen für die Compliance- und Rechtsabteilung?

- Ja
- Nein
- Ich weiß nicht

Untersuchungen & eDiscovery: Gibt es vollen Daten- und Audit Trail-Zugriff für die Bewältigung der einzigartigen Datenschutzanforderungen für Compliance, Ermittlungen und Rechtsstreitigkeiten?

- Ja
- Nein
- Ich weiß nicht

Wenn Ihre Antwort bei mehr als ein paar dieser Fragen „**Nein**“ oder „**Ich weiß nicht**“ lautete, ist es Zeit, sich mit der Stärkung Ihres Datenschutzes zu befassen.

Über Druva

Druva ist führend im Bereich Datensicherheit und Governance an vorderster Front, und bringt so im zunehmend mobilen und verteilten Unternehmen Transparenz und Steuerungsmöglichkeiten in die Geschäftsinformationen. Entwickelt für öffentliche und private Clouds, verhindern Druvas preisgekrönte inSync- und Phoenix-Lösungen Datenverluste und adressieren Governance-, Compliance- und eDiscovery-Anforderungen auf Laptops, intelligenten Geräten und Remote-Servern. Als der am schnellsten wachsende Edge Data Protection-Anbieter der Branche vertrauen mehr als 3.000 globale Unternehmen mit mehr als 3 Millionen Geräten Druva. Erfahren Sie mehr unter **www.druva.com** und beteiligen Sie sich an der Unterhaltung auf **twitter.com/druvainc.**

© Copyright 2015 Druva, Inc. Alle Rechte vorbehalten
Q415-CON-10460

Druva, Inc.
Amerikas: +1 888-248-4976
Europa: +44(0)20,3750,9440
APJ: +919886120215
sales@druva.com
www.druva.com