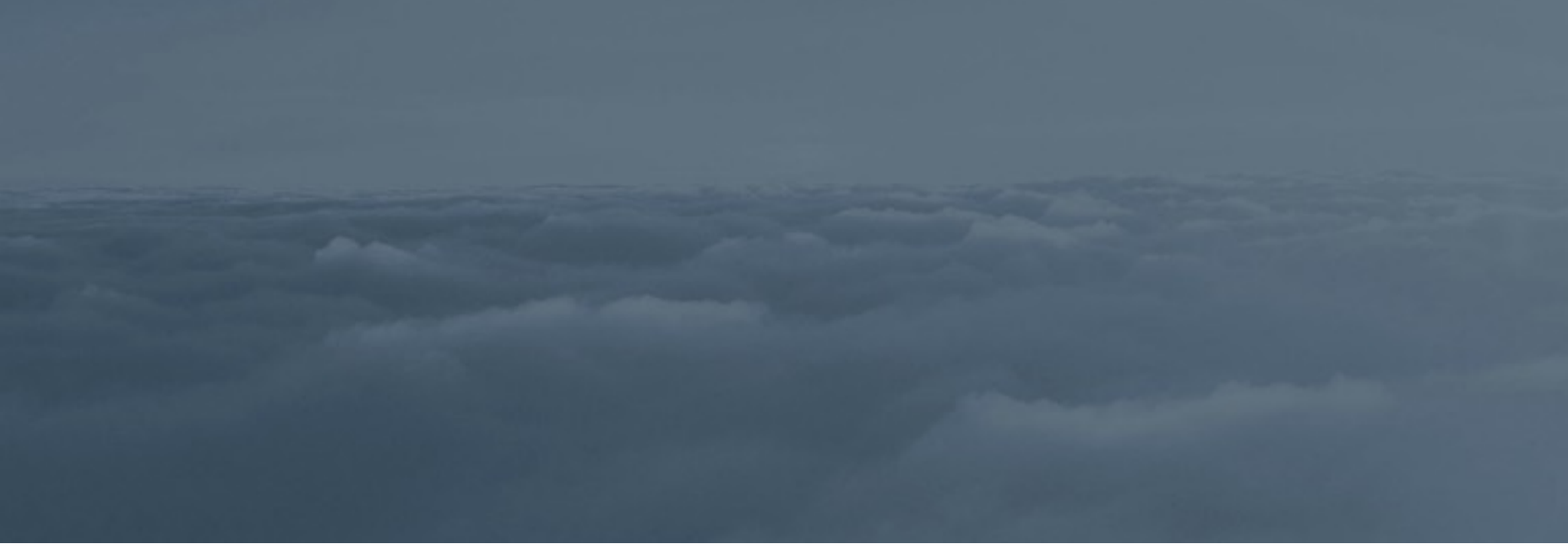
Checkliste für die Datensicherheit im Unternehmen

So erkennen Sie, ob Ihre sensiblen Daten in der Cloud sicher sind



ownCloud

Einführung

Immer mehr Anwender greifen für den Austausch und die Speicherung sensibler Unternehmensdaten auf Dienste wie Dropbox zurück, die ursprünglich für Verbraucher entwickelt wurden. Doch eigentlich können es sich Unternehmen nicht leisten, sich den Risiken auszusetzen, die mit der Nutzung dieser Dienste verbunden sind.

Da die Kosten infolge von Verstößen gegen den Datenschutz in die Millionen gehen können, müssen Sie sich folgende Fragen stellen: Bieten diese Cloud-Services ausreichenden Schutz für die sensiblen Daten Ihres Unternehmens? Zunehmend wichtig sind auch die genaue Kenntnis und lückenlose Einhaltung der Datenschutzvorschriften, die für Ihr Unternehmen gelten. Hält Ihr Cloud-Serviceprovider (CSP) alle relevanten Datenschutzvorschriften ein?

In Deutschland haben Datenschutzgesetze sowohl auf Bundes- als auch auf Landesebene eine lange Tradition. Nachdem das Safe-Harbor-Abkommen zwischen der EU und der USA im Oktober 2015 vom Europäischen Gerichtshof für ungültig erklärt wurde, sollte sich jeder IT-Manager ausführlich mit dem Thema Datenschutz, den dazugehörigen Kontrollmechanismen sowie den jeweils geltenden deutschen Datenschutzvorschriften auseinandersetzen. Kennt auch Ihr Cloud-Serviceprovider diese Vorschriften, und hält er sie ein?

Dieses Whitepaper soll Ihnen helfen, Antworten auf diese Fragen zu finden. Die verschiedenen Checklisten gehen auf die einzelnen Aspekte des Themas Datenschutz ein, unterstützen Sie bei der Bewertung Ihrer Risiken und Ihrer Risikoposition und helfen Ihnen, das nötige Maß an Sicherheit, Compliance und Governance zu gewährleisten.

Warum ist Datenschutz so wichtig?

Als IT-Manager haben Sie die Aufgabe, alle sensiblen Daten des Unternehmens zu schützen, einen angemessenen Schutz nachzuweisen und für die Einhaltung von Compliance-Anforderungen zu sorgen. Im Mittelpunkt stehen dabei folgende Aspekte:

- **Datenhoheit**: Das Konzept der Datenhoheit basiert darauf, dass Daten, die in digitalem Format gespeichert werden, den Gesetzen des Landes unterliegen, in dem sich die Daten befinden. Sie tragen Verantwortung für die Einhaltung dieser Gesetze, unabhängig davon, ob Ihre Dateien lokal oder in der Cloud gespeichert sind. Bei technologischen Entscheidungen ist es deshalb äußerst wichtig, auch die entsprechenden gesetzlichen Pflichten zu kennen.

- **Sicherheit**: Die Sicherheit Ihrer Daten muss höchste Priorität genießen. Bei sämtlichen Anwendungsfällen müssen Sicherheitsprotokolle und -prozesse berücksichtigt werden, beispielsweise die Mechanismen für eine effektive Zugriffskontrolle, der Speicherort von Metadaten und die Verwaltung von Keys. Viele Content Delivery Networks (CDNs), Protokolle wie WebDAV und andere Zugriffstechnologien arbeiten nicht mit verschlüsselten Daten. Sie müssen wissen, welche Sicherheits- und Verschlüsselungstechniken verfügbar sind und verwendet werden, um Ihre Daten schützen zu können.

- **Kontrolle**: Wenn Sie Ihre Daten einem externen Anbieter anvertrauen, ist nicht mehr gewährleistet, dass die Sicherheitsprotokolle und -prozesse Ihres Unternehmens eingehalten werden.

Der Anbieter sollte nicht nur den Zugriff kontrollieren, sondern auch sämtliche Zugriffsaktivitäten umfassend verwalten, überwachen und protokollieren. Wichtig sind außerdem Backup- und Rollback-Funktionen.

Wird der Anbieter Ihren Sicherheitsanforderungen in einem oder mehreren dieser Bereiche nicht gerecht, kann dies einen enormen Schaden für Ihr Unternehmen nach sich ziehen, beispielsweise den Verlust geistigen Eigentums oder des Markenwerts. Selbst wenn kein Verstoß gegen Datenschutzvorschriften vorliegt, kann das Nichtbestehen einer behördlichen Prüfung zu hohem Schaden und Bußgeldern in Millionenhöhe führen.

Um den Schutz Ihrer Daten und Ihres Unternehmens gewährleisten zu können, müssen Sie kritische Fragen stellen.

Haben Sie die Kontrolle über Ihre Hardware?

Checkliste für Ihre Hardware

- ✓ Wo befindet sich Ihre Hardware, und wer hat Zugriff darauf?
- ✓ Wie werden physische Zugangsrechte erteilt und entzogen?
- ✓ Wer verfügt über Administratorzugriffsrechte, und wie werden diese verwaltet?
- ✓ Wie erfolgen Kontrolle, Überprüfung und Protokollierung des Zugriffs?
- ✓ Werden auch Ihre Governance-Richtlinien befolgt?
- ✓ Welchen Gesetzen zur Datenhoheit unterliegen Sie?
- ✓ Wie erfolgen Backup und Aktualisierung der Hardware oder das Einspielen von Patches?

Sicherheit beginnt zunächst bei der Hardware. Wenn Sie die Kontrolle über Ihre Hardware einem Dritten überlassen, müssen Sie für die Einhaltung von Sicherheitsstandards sorgen – sowohl Ihrer eigenen als auch der gesetzlich vorgeschriebenen Standards. Sie müssen außerdem sicherstellen, dass Ihre Service-Level-Agreements für die Anwender weiterhin eingehalten werden.

Und schließlich müssen Sie jederzeit nachweisen können, wer aus welchem Grund Zugriff auf Ihre Server hat.

Lesen Sie das Kleingedruckte, fordern Sie die entsprechenden Nachweise an, und machen Sie sich nach Möglichkeit selbst ein Bild von den Einrichtungen des Anbieters. Prüfen Sie alle Aspekte so wie Sie es tun würden, wenn die Hardware bei Ihnen im Unternehmen wäre oder sie neu validieren würden. Nach deutschem Gesetz liegt die Sicherheit der Daten in Ihrer Verantwortung, selbst wenn die Daten auf der Hardware eines Dritten im Rechenzentrum eines externen Anbieters gespeichert sind.

Was passiert mit Ihren Daten?

Checkliste für Ihr Netzwerk

- ✓ Wo befinden sich die Endgeräte, und wer hat Zugriff darauf?
- ✓ Welchen Weg nehmen Ihre Daten bei der Übertragung, und wie werden sie dabei geschützt?
- ✓ Was passiert bei einer Disaster Recovery bzw. einem Failover?
- ✓ Entspricht das Netzwerk Ihren Richtlinien?
- ✓ Wie erfahren Sie von unbefugten Zugriffen?
- ✓ Wird Ihr Netzwerkverkehr abgehört/analysiert?
- ✓ Nutzen Sie CDNs zur Beschleunigung des Netzwerkverkehrs? Falls ja, welche?
- ✓ Kann der Netzwerkverkehr in Ihrem CDN verschlüsselt werden

Die Fragen zum Netzwerk sind den Fragen zur Hardware ähnlich, jedoch noch komplexer.

Ein Aspekt, der oftmals außer Acht gelassen wird, sind Content Delivery Networks (CDNs). Dabei ist es durchaus möglich, dass die Nutzung eines CDN in der Übertragungskette dazu führt, dass eine Datei unverschlüsselt im Rechenzentrum eines externen Anbieters gespeichert wird. In diesem Fall müssen Sie alle Punkte innerhalb der Kette überprüfen und herausfinden, ob an irgendeinem Punkt ein unverschlüsselter Zugriff auf die Datei möglich ist.

Die Netzwerküberwachung sollte Ihnen die nötigen Informationen zur Einhaltung von Compliance-Anforderungen liefern. Denken Sie stets daran, dass Sie auch ohne explizite Datenschutzverletzung Risiken ausgesetzt sein können. Es kann schon ausreichen, dass Sie nicht wissen, ob Ihre Daten gefährdet sind.

Wo werden Ihre Daten gespeichert?

Checkliste für Ihre Speichersysteme

- ✓ Wo sind Ihre Dateien gespeichert, und wer hat Zugriff darauf?
- ✓ Werden die Dateien vor der Speicherung überprüft?
- ✓ Welche Methoden der Aufbewahrung und Nachverfolgung werden eingesetzt?
- ✓ Was passiert, wenn Sie Ihre Dateien nicht mehr hosten lassen, sondern wieder lokal speichern möchten?
- ✓ Was passiert, wenn Sie Ihre Daten Behörden offenlegen müssen?
- ✓ Wie werden die Daten verschlüsselt? Wer verwaltet die Keys?
- ✓ Was passiert, wenn Sie Dateien löschen oder deduplizieren

Aspekte im Zusammenhang mit der Datenspeicherung sind besonders komplex. Zunächst stellt sich die Frage, wem die Daten gehören. Manche Endbenutzer-Lizenzverträge sehen vor, dass der Serviceprovider Eigentümer der Daten ist. In diesem Fall muss der Serviceprovider Daten auf Wunsch von Behörden offenlegen. Bei manchen Vorschriften zur Datenhoheit liegt das Risiko bei Ihnen, selbst wenn Ihre Daten von einem externen Anbieter gehostet werden. Sie müssen zum einen Ihre Rechte kennen, zum anderen aber auch Ihre Risiken.

Andere Aspekte sind technischer Natur. Manche Cloud-Anbieter greifen zur Überprüfung und Deduplizierung auf Dateien zu. In einigen Ländern und Rechtssystemen ist ein solcher Zugriff bei bestimmten Dateitypen untersagt. Stellen Sie sicher, dass die Verwaltung der Keys umfassend kontrolliert wird. Und lassen Sie Sorgfalt beim Löschen von Dateien walten – es kann vorkommen, dass Dateien nicht wirklich gelöscht werden oder Dateikomponenten beim Deduplizieren erhalten bleiben. In solchen Fällen kann es nach wie vor Datenschutzverletzungen geben.

Wer verwendet Ihre Daten?

Checkliste Benutzer und Administratoren

- ✓ Wie erfolgt die Bereitstellung und Authentifizierung von Benutzern? Wird SSO unterstützt?
- ✓ Wie werden Administratoren geschult, überprüft und überwacht?
- ✓ Befolgen Administratoren Ihre Richtlinien oder eigene?
- ✓ Wie werden Benutzer überwacht und überprüft?
- ✓ Welche Benutzerprotokolle stehen für die Warnung vor unbefugten Zugriffen zur Verfügung?
- ✓ Können Benutzer oder Administratoren Ihre IT-Richtlinien umgehen?
- ✓ Wie werden die Keys der Benutzer verwaltet? Wie erfolgt eine Wiederherstellung? Wer hat Zugriff auf die Keys

Serviceprovider schulen ihre Mitarbeiter zwangsläufig nach einem einheitlichen Schema. Damit kennen sie sich vermutlich gut mit den Prozessen und Verfahren des Providers aus, nicht jedoch mit **IHREN** Richtlinien und Prozessen. Wenn Sie besondere Anforderungen an Hardware, Netzwerk, Speichersysteme, Backup, Benutzer und Administration haben, kann Ihr Provider diesen ziemlich sicher nicht gerecht werden.

Sie benötigen Zugriff auf Benutzerprotokolle und müssen in der Lage sein, diese in Ihre eigenen Tools zu integrieren. Wenn Sie sich dabei auf Ihren Serviceprovider verlassen, kann die Nichteinhaltung von Vorschriften bei einem Audit Ihnen angelastet werden. Wichtig ist auch, dass Sie die Kontrolle über Ihre Keys haben, da diese ausschlaggebend dafür sein können, wer die Kontrolle über Ihre Daten hat.

Wie funktioniert das Zusammenspiel?

Checkliste für die Integration

- ✓ Werden Ihre Governance-Richtlinien eingehalten?
- ✓ Müssen Ihre Daten in die Cloud hochgeladen werden, damit Sie darauf zugreifen können?
- ✓ Wie nutzen Sie bisherige IT-Investitionen weiter?
- ✓ Wie können Sie vorhandene IT-Tools und Prozesse weiter nutzen?
- ✓ Welche Datenbanken können Sie für Ihre Daten verwenden?
- ✓ Welche Speichersysteme können Sie für Ihre Daten nutzen?
- ✓ Entsteht dadurch ein neues Datensilo, das verwaltet werden muss?
- ✓ Wie können Sie zukünftige Anforderungen unterstützen?

Ihre IT-Organisation hat unter Umständen viele Jahre gebraucht, um ihre Prozesse und Strukturen auf behördliche Anforderungen, Aufbewahrungsrichtlinien, Löschprozesse und die hohen Standards Ihres Unternehmens abzustimmen.

Wenn Sie die so entstandenen Lösungen nicht auch für den Austausch von Dateien nutzen können, waren viele Ihrer Investitionen umsonst. Zudem entsteht ein neues Datensilo.

Zwar können Sie Ihre Firewall ein Stück weit öffnen, um Services externer Anbieter zu integrieren, doch ist dies mit Sicherheit keine ideale Lösung. Auch wird es immer Daten geben, die das Unternehmen nicht verlassen dürfen. Eine Trennung zwischen dem Cloud-Service und Ihren internen Prozessen ist damit unvermeidbar.

Wenn Sie wissen, welche Lösungen auch Ihre zukünftigen Anforderungen unterstützen, können Sie die optimale Entscheidung für Ihr Unternehmen treffen.

Halten Sie alle einschlägigen Gesetze ein?

Checkliste für die Einhaltung gesetzlicher Vorschriften

- ✓ Wissen Sie, wer für die Sicherheit Ihrer sensiblen Daten verantwortlich ist?
- ✓ Sind Sie ein internationales Unternehmen, für das in unterschiedlichen Ländern auch unterschiedliche Regeln gelten?
- ✓ Hält Ihr Provider die für Ihr Unternehmen geltenden Vorschriften ein?
- ✓ Ist Ihr Provider eine hundertprozentige Tochtergesellschaft eines US-Konzerns?
- ✓ Kann Ihr Provider die Einhaltung des BDSG/der EU-Datenschutzrichtlinie/des FISA bzw. den Schutz vor PRISM nachweisen?
- ✓ Sind Sie Eigentümer der Dateien, die Ihr Provider für Sie hostet?
- ✓ Sind Sie in der Lage, Datenschutzgesetze lückenlos einzuhalten?
- ✓ Können Sie nachweisen, dass Sie die Kontrolle über Ihre Daten haben?

Abschließend geht es um die zentrale Frage, die sich jedes Unternehmen stellen muss: Können Sie nachweisen, dass Sie die Kontrolle über Ihre Daten haben? Falls ja, sind Sie auf der sicheren Seite. Falls nein, sollten Sie eine erneute Bewertung Ihrer Risikoposition vornehmen.

In den gesetzlichen Vorschriften ist geregelt, dass Sie Kontrolle über Ihre Daten haben und wissen müssen, wo sich diese Daten befinden. Wenn Sie zu irgendeinem Zeitpunkt keine Kontrolle mehr über eine bestimmte Datei haben, könnte dies bei einem Audit zum Problem werden – und bei einem Verstoß gegen Datenschutzvorschriften ernsthafte Konsequenzen nach sich ziehen.

Bei der Einhaltung von Gesetzesvorschriften sind viele Aspekte zu berücksichtigen. Unter anderem müssen Sie auch wissen, welche Folgen die Gesetze anderer Länder auf den

Datenschutz in Ihrem Unternehmen haben. Ein Beispiel hierfür sind Tochtergesellschaften von US-Konzernen. Unabhängig davon, wo sich der Standort eines Unternehmens außerhalb der USA befindet, kann der „US Patriot Act“ Anwendung finden, wenn die Muttergesellschaft ein US-Unternehmen ist. Damit wird der Schutz Ihrer personenbezogenen Daten gefährdet.

Auch müssen sowohl Rahmenvereinbarungen der EU als auch konkrete deutsche Vorschriften berücksichtigt werden. Der Schutz personenbezogener Daten ist in landesspezifischen Gesetzen wie dem Bundesdatenschutzgesetz (BDSG) sowie einzelnen Abschnitten des Strafgesetzbuches geregelt. Zudem gibt es in allen 16 Bundesländern jeweils eigene Datenschutzregelungen.

Zu den EU-weit gültigen Vorschriften zählen die EU-Datenschutzrichtlinie, in der die Erhebung und Übertragung personenbezogener Daten außerhalb der EU geregelt ist, und das Safe-Harbor-Abkommen zwischen der EU und den USA. Das Safe-Harbor-Abkommen wurde im Oktober 2015 vom Europäischen Gerichtshof für ungültig erklärt. Nach diesem Urteil müssen deutsche Datenschutzbehörden die Übertragung von Daten an US-Unternehmen untersagen, die im Rahmen von Programmen wie PRISM und FISA überwacht werden.

Für die Sicherheit und Kontrolle Ihrer Daten ist es entscheidend, dass Sie wissen, mit welchen Maßnahmen Ihr Serviceprovider die Einhaltung der für Ihr Unternehmen geltenden Datenschutzvorschriften sicherstellt.

Serviceprovider sind bestrebt, die Sicherheit Ihrer Daten durch entsprechende Maßnahmen zu gewährleisten. Es geht jedoch um Ihre Daten. Wenn Sie die Kontrolle über diese Daten einem externen Anbieter anvertrauen, können Sie Risiken niemals vollständig ausschließen.

Ein alternatives Konzept

Für Unternehmen, für die eine vollständige Kontrolle über ihre Daten wichtig bzw. unabdingbar ist, gibt es ein alternatives Konzept, bei dem Sie nicht auf die Vorteile der Cloud verzichten müssen.

Bei diesem Konzept ist die Kontrollebene für Filesync und -share im unternehmenseigenen Rechenzentrum oder im Rechenzentrum eines vertrauenswürdigen lokalen Serviceproviders angesiedelt. Dies bedeutet, dass die Keys für die Verschlüsselung, die Metadaten und die Zugriffskontrolle unabhängig vom Speicherort der Daten in Ihrer lokalen Umgebung verbleiben. Selbst wenn Sie zur Offenlegung von Daten verpflichtet sind, können Sie nicht gezwungen werden, auch die zur Entschlüsselung benötigten Keys preiszugeben. Als einziger Anbieter von EFSS-Lösungen bietet ownCloud Unternehmen die Wahl, wo Daten und Keys gespeichert werden.

Die Lösung basiert auf einer skalierbaren Plattform mit umfassenden Funktionen für das Filesharing im Unternehmen und lässt sich flexibel in die bestehenden Systeme, Richtlinien und Standards der IT-Organisation integrieren.

Für die Anwender, die möglichst einfach Daten mit ihren Kollegen oder externen Geschäftspartnern austauschen und effizienter kommunizieren möchten, bietet das System den Bedienkomfort gängiger Public Cloud-Services, während aber gleichzeitig Sicherheitsrichtlinien eingehalten werden können. Dies fördert die Akzeptanz der Anwender für eine sichere Filesharing-Lösung, die den Sicherheits- und Compliance-Anforderungen deutscher Datenschutzgesetze voll und ganz gerecht wird.

Weitere Informationen zu diesem Konzept finden Sie unter www.owncloud.com/de.

Anhang

Links zu Datenschutzgesetzen:

Gesetze im Internet
http://www.gesetze-im-internet.de/bdsg_1990/index.html

Gesetze zum Online-Datenschutz: Deutschland
http://www.loc.gov/law/help/online-privacy-law/germany.php

Deutsche Rechtsvorschriften zum Datenschutz
https://www.ldi.nrw.de/mainmenu_Datenschutz/index.php

Blog zu Datenschutz- und Informationssicherheitsgesetzen in Deutschland
https://www.huntonprivacyblog.com/tag/germany/

Blog zum Thema Speicherort von Daten und Datenhoheit
https://owncloud.com/de/data-residency-data-sovereignty-and-the-mad-scramble/