

FORTRA™



EBOOK (GoAnywhere)

Kontrolle in der Cloud: MFT zur sicheren Handhabung Ihrer Daten



Intro

In den letzten Jahren hat der rasche und unerwartete Wandel des Geschäftsbetriebes neue Herausforderungen für die Sicherheit mit sich gebracht. Während viele Unternehmen mit der Sicherheit der Daten und deren Logistik bei einer Einführung von Cloud-Technologien haderten, erkannten andere hierbei den Wert einer professionellen Managed File Transfer-Lösung. Wir haben darüber mit einer Gruppe von Fachleuten aus verschiedenen Unternehmen und Branchen gesprochen. Sie teilten uns ihre Erfahrungen mit, wodurch Ihre Cloud-Initiative so reibungslos, sicher und effektiv als nur möglich verlaufen wird.

(Reza Alavi | Senior Manager, Technology and Digital Risk | [LinkedIn](#))

Die digitale Transformation hat die Art und Weise, wie wir ein Unternehmen führen, grundlegend verändert. Ein Großteil dieses Wandels vollzieht sich im Cloud-Ökosystem. Cloud-Implementierungen finden bereichsübergreifend in allen Branchen statt. Mit der Cloud haben wir begonnen den Nutzen von Mehrwertdiensten zu verstehen, die im Cloud-Ökosystem durch ein effizientes Datenmanagement implementiert werden.

Kosteneinsparungen, Flexibilität, Mobilität, verbesserte Informationssicherheit, verbesserte Zusammenarbeit und neue Erkenntnisse innerhalb des Datenbestandes eines Unternehmens sind nur wenige Vorteile einer Verwaltung und Speicherung von Daten in einer Cloud-Umgebung.

(Matthew Hankinson | Infrastructure manager | [LinkedIn](#))

Die Arbeit von zu Hause hat die Einführung der Cloud-Technologie beschleunigt. Aber während die Zahl der Cloud-basierten Anwendungen für eine Zusammenarbeit stetig zunimmt, haben sich die Methoden der Dateiübertragung nicht wirklich verändert. Dies scheint eher auf die Notwendigkeit zurückzuführen zu sein, ein bestimmtes System zu erweitern oder zu ersetzen und es in die Cloud zu verlagern. Das war für uns der Auslöser. Wir haben ein geschäftskritisches On-Premises System in ein Cloud-System verlagert, wobei die Sicherheit der Daten gewährleistet sein musste. Managed File Transfer lässt uns Dateien mit der notwendigen Flexibilität und Kontrolle transferieren, so wie wir es benötigen.



Frage 1: On-prem-Herausforderungen

Was sind einige der wichtigsten Herausforderungen bei der Datenübertragung On-Premises und in der Cloud? Wie hilft die richtige Technologie, wenn es um Produktivität, Sicherheit und Compliance geht?

Funso Richard | Information Security Officer | [LinkedIn](#)

Die größte Herausforderung für Unternehmen ist die ineffiziente Verwaltung der Daten. Die Verwendung von On-Premises-Protokollen zur Übertragung von Dateien innerhalb des Unternehmens sowie an externe Partner bzw. Parteien birgt große Herausforderungen wie die einer mangelnden Sicherheit, fehlende Mobilität, Performanceprobleme, Wartungskosten, Produktivitätseinbußen und fehlende Nutzerkenntnis. Eine Alternative hierzu besteht darin, die Datenübertragung in die Cloud zu verlagern. Jedoch sind eine unzulängliche Planung, die Kosten, Fehlkonfigurationen und fehlende Kenntnisse nur einige der Herausforderungen hierbei. Infolge mangelnder Kenntnis verwenden Mitarbeiter dann häufig nicht genehmigte Lösungen, um Dateien auszutauschen. Dies ist ein ernsthaftes Risiko, welches Unternehmen möglichen Datenverlust und Datenschutzverletzungen aussetzt.

Um sowohl Produktivität als auch Datenschutz zu gewährleisten, ist die Investition in die richtige Dateiübertragungstechnologie für einen effektiven und effizienten Geschäftsbetrieb entscheidend. Angesichts der Zunahme von Heimarbeit und der Abhängigkeit von funktionierenden Lieferketten benötigen Unternehmen eine dynamische, zuverlässige und flexible Übertragungstechnologie, um Daten und Dateien über verschiedene Protokolle, Plattformen und Umgebungen hinweg sicher zu übertragen. Eine solche Technologie ist Managed File Transfer (MFT). MFT verfügt über Kontroll- und Sicherheitsmechanismen, ohne die Produktivität und Leistung zu beeinträchtigen. Zu den Vorteilen einer MFT Lösung zählen Kosteneinsparungen, zentralisierte Verwaltung, Skalierbarkeit, flexible Integration, Regelkonformität, zeitkonformer Datenzugriff sowie Benutzerfreundlichkeit zur verbesserten Entscheidungsfindung.

Gary Hibberd | Security Consultant | [LinkedIn](#)

Es gibt eine grundlegende Herausforderung bei der Datenübertragung, ob sie nun On-Premises oder in der Cloud stattfindet - und das ist die Frage der Kontrolle: Wer hat Zugriff auf die Daten und wie werden diese übertragen? Sicherlich nimmt die Menge der von uns verarbeiteten Daten stetig zu. Die sichere und gemeinsame Nutzung dieser Daten in unserer Infrastruktur ist für jedes Unternehmen von zentraler Bedeutung.

Die Herausforderungen mit denen wir konfrontiert sind, liegen in der Verwaltung und Kontrolle dieser Übertragungen. Wo dieses geschieht, sollten wir geeignete technische Lösungen wie Managed File Transfer (MFT) einsetzen. Mit einer Managed File Transfer-Lösung wird sichergestellt, dass die Daten regelkonform, überwacht und sicher am Ziel ankommen. Eine gute MFT-Lösung verringert die Risiken von Regelverstößen, da sie die Integrität der Daten sicherstellt. Darüber hinaus erhöht sie die Produktivität, da die Netzauslastung durch Optimierung verringert und die Geschwindigkeit sowie die Zuverlässigkeit der Übertragung erhöht wird.

Michael Barford | Solutions Engineer | [LinkedIn](#)

Bei On-Premises Datentransferlösungen sehen wir die größte Herausforderung nach wie vor in der hohen Komplexität, die mit der Entwicklung und Pflege von benutzerdefinierten Lösungen im Umgang mit großvolumigen und hochkomplexen Transfers verbunden ist. Dennoch verlassen sich heute viele Unternehmen auf Skripte oder selbst entwickelte Lösungen zur Umsetzung interner Übertragungen. Dies ist mit hohen Wartungs- und Betriebskosten verbunden. Ein großer Teil der Kosten basiert dabei gewöhnlich auf Fehlern. Wenn eine Datei verloren geht, merken das viele erst Tage später. Um herauszufinden, was passiert ist und wo sich die Datei befindet müssen verschiedene IT-Ressourcen mobilisiert werden. Es wird manuell nachbearbeitet und das "Skript" muss korrigiert werden, damit sich das Problem in Zukunft nicht wiederholt. Die Problematik verschärft sich, wenn die Mitarbeiter als Entwickler dieser benutzerdefinierten Lösung in andere Funktion oder in ein anderes Unternehmen wechseln oder wenn diese Lösung für neue Anwendungsfälle erweitert werden muss. Dies betrifft auch mehr und mehr die Cloud.

Eine weitere Herausforderung ist mit den Anforderungen an Sicherheit oder die Compliance verbunden. Diese einzuhalten ist schwer und kostspielig, sofern man nicht über eine speziell entwickelte Lösung verfügt, die die jeweils neuesten Sicherheitsprotokolle unterstützt und eine umfassende Verschlüsselung, Nachvollziehbarkeit, Protokollierung sowie Rollenkonzepte bietet.

Bei einer Migration in die Cloud ist es wichtig zu prüfen, ob eine MFT-Lösung mit einer Vielzahl an Cloud-Plattformen interagieren kann und auch REST-APIs unterstützt, damit deren ständige Weiterentwicklung zukünftige Anwendungsfälle abdecken kann. Aufgrund der Vielzahl von Plattformen und Schnittstellen mit denen Unternehmen heute arbeiten, werden Sicherheit, Nachvollziehbarkeit und Wartbarkeit von Datenübertragungen immer schwieriger.

Traditionell werden Dateiübertragungsprozesse konfiguriert und einfach laufen gelassen, was in einer Zeit, in der es nur SFTP- oder FTP-Übertragungen gab auch ganz gut funktionierte. Man konnte denselben Prozess für mehrere Handelspartner verwenden. Schwierig wird es dann, wenn der Prozess angepasst werden muss. Dies ist in der Regel der Wendepunkt, an dem sich Kunden für eine MFT-Lösung entscheiden.

Der Einsatz der richtigen Technologie ermöglicht es Unternehmen, sich leichter an die sich ständig ändernden Anforderungen an die Dateiübertragung anzupassen.

Ray Sutton | Technical Consultant | [LinkedIn](#)

Bei der Datenübertragung gibt es zahlreiche Herausforderungen, vor allem wenn es darum geht, diese Dienste beispielsweise über das Internet für externe Partner bzw. Parteien zugänglich zu machen. Diese Herausforderungen bestehen darin, eine gute und sichere Umgebung bereitzustellen. Um nun die Netzwerke und Systeme innerhalb Ihres Unternehmens zu schützen, müssen die Lösungen überarbeitet werden.

Man muss jedoch auch zugeben, dass diese Herausforderung auch in der Cloud besteht. Die Sicherheit der verbundenen Cloudplattform und der Schutz der Daten muss sogar stärker berücksichtigt werden.

Das richtige Gleichgewicht ist hierbei der Schlüssel, um sicherzustellen, dass die Produktivität der Mitarbeiter, die Sicherheit und die Anforderungen an die Compliance erfüllt werden. Für jeden, der mit Ihren Systemen interagiert, muss gewährleistet sein, dass Sie alle Sicherheitsanforderungen erfüllen, aber dennoch ein einfaches Verfahren für die Datenübertragung haben. Dies ist entscheidend für die Aufrechterhaltung eines hohen Sicherheitsniveaus.

Wenn Sie diesen Schritt versäumen, schwierige Prozesse oder Systeme einführen, könnte dies dazu führen, dass sich einige Mitarbeiter nach schnelleren Alternativen umsehen, was wiederum zu einem höheren Risiko in der Art Ihrer Cloud- oder On-Premises-Lösungen führt.

Matthew Hankinson | Infrastructure manager | [LinkedIn](#)

Die Herausforderung bei einer sicheren Datenübertragung besteht darin, ein Gleichgewicht zwischen den Anforderungen und Wünschen des Unternehmens sowie den Anforderungen an die Cybersicherheit herzustellen. Sie muss geschäftlichen Anforderungen bei gleichzeitiger Einhaltung aller Vorschriften und Vorgaben erfüllen. Eine sichere Datenübertragung muss allen Beteiligten gerecht werden, wobei die Cybersecurity nicht nur aus praktischer Sicht, sondern auch aus regulatorischer Sicht berücksichtigt werden muss.

In der Vergangenheit lag der Hauptunterschied zwischen dem Datentransfer On-Premises oder in einer Cloud-Umgebung immer in der Kontrolle. Bei der Cloud gibt es das unbekannte Terrain, bei dem man in gewisser Hinsicht einem Dritten vertrauen muss. Sie müssen sich vergewissern, dass der Cloud-Anbieter Ihre Sicherheitsstandards einhält. Weiter müssen Sie sich über die Art der zu transferierenden Daten im Klaren sein. Sind personenbezogene Daten enthalten (Personally Identifiable Information (PII)), müssen Sie sicherstellen, zusätzliche Schutzmaßnahmen zu ergreifen. Allzu oft stellt sich niemand die Frage, was überhaupt übertragen wird. Sie werden lediglich gebeten, eine Datei von einem Ort zum anderen zu transferieren, aber was ist eigentlich in diesen Daten enthalten? Handelt es sich um etwas, das für das Unternehmen ein größeres Problem darstellen könnte, sofern es nach außen gelangt? Es ist wichtig, eine verlässliche Managed File Transfer-Lösung zu haben, die all diese Sicherheitsaspekte mit berücksichtigt. Ein großer Teil der Herausforderung besteht darin, mit alten Gewohnheiten zu brechen. Man hat viele Jahre lang ungehindert Informationen übertragen, aber jetzt müsse man über die Daten nachdenken, die in diesen Dateien enthalten sind, um nicht gegen Datenschutzgesetze zu verstoßen. Wir arbeiten daran die Nutzer aufzuklären, über das was Sie versenden auch nachzudenken. Wir bemühen uns um ein Standardverfahren und initiale Überprüfung der angeforderten Daten.

Soulos Panagiotis | Global Information Security Manager | LinkedIn



Einige der wichtigsten Herausforderungen im Bereich der On-Premises Datenübertragung sind:

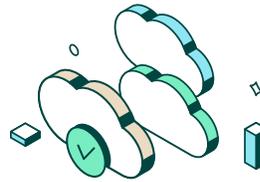
Sicherheitslücken: Herkömmliche On-Premises Lösungen für die Dateiübertragungen wie FTP und SFTP/FTPS, decken nicht alle aktuellen Sicherheitsanforderungen der Unternehmen ab. FTP wurde noch nicht unter dem Aspekt der Sicherheit entwickelt, denn es fehlt an grundlegenden Sicherheitskontrollen, unter anderem einem verschlüsselten Authentifizierungskanal. Verschlüsselung zum Schutz der Daten während der Übertragung oder auf den Speichersystemen, ist eine nachträgliche Maßnahme, die zusätzliche Schritte und IT-Fachwissen erfordert, welche den Transfer und das sichere Speichern von Dateien schwierig, kostenintensiv und zeitaufwändig macht. Auch die Verwendung der Benutzeranmeldedaten wird von diesen Lösungen nicht verwaltet und sollte mit externen und in der Regel manuellen Verfahren durchgeführt werden, denen es aber an Sicherheitsvorkehrungen mangelt, was wiederum die Möglichkeit der Offenlegung erhöht.

Automatisierung: Herkömmliche Lösungen bieten keine Automatisierung oder zeitliche Planungen von Dateiübertragungsvorgängen. In der Regel sind manuelle Skripte oder zusätzliche Lösungen erforderlich, um solche Anforderungen zu erfüllen, was zu erhöhten Kosten führt und spezielle Fachkenntnisse der IT-Mitarbeiter voraussetzt.

Automatisierte Benachrichtigungen: Herkömmliche Lösungen bieten keine automatisierten Benachrichtigungen und sollten mit anderen Lösungen kombiniert werden, um Benutzer bei Fehlern während der Dateiübertragung zu informieren.

Fortlaufender Betrieb: Disaster-Recovery-Pläne sollten manuell entworfen und umgesetzt werden, da herkömmliche Lösungen keine automatisierten DRP-Mechanismen enthalten. Auch die Wiederherstellungsverfahren bei Ausfällen werden manuell durchgeführt.

Kapazitätsengpässe: On-Premises Lösungen können Problemen bei der Übertragung großer Dateien haben, was durch kleinere Netzwerkausfälle und Fehler verursacht werden kann.



Wichtige Herausforderungen bei der Datenübertragung in der Cloud sind:

Einhaltung von Vorschriften: Je nach Art der Organisation müssen möglicherweise bestimmte Vorschriften und/oder Branchenstandards eingehalten werden. Auch die Datenhoheit sollte bei der Speicherung und Übertragung von Daten in der Cloud berücksichtigt werden.

Datenlecks/Verletzungen: Wenn der Cloud-Anbieter kompromittiert wird, kann es zu Datenlecks oder Datenschutzverletzungen kommen.

Zugriffsprobleme/Denial-of-Service: Der Zugang zu den Diensten kann gestört sein, wenn der Cloud-Anbieter einem Denial-of-Service-Angriff ausgesetzt ist oder auch der Internetzugang der Organisation unterbrochen ist.

Gefahren durch Malware: Es sollte Anti-Malware-Sicherheit zur Minimierung des Risikos vorhanden sein, dass in der Cloud gespeicherte und übertragene Dateien mit Malware infiziert werden.

Anbieterbindung und Übertragbarkeit von Diensten: Bei der Nutzung von Cloud-Diensten sollte darauf geachtet werden, dass eine Anbieterbindung vermieden wird und die Dienste möglichst leicht zu einem anderen Anbieter/Cloud-Dienstleister übertragbar sind. Eine Anbieterbindung liegt vor, wenn die Kosten für einen Anbieterwechsel so hoch sind, dass das Unternehmen an den aktuellen Anbieter gebunden bleibt. Ein Vendor-Lock-Out liegt vor, wenn der Anbieter seine Geschäftstätigkeit einstellt und die angebotenen Dienste einstellt.

Mit der richtigen Technologie kann ein Unternehmen diese Herausforderungen begegnen, indem es sicherstellt, dass die gewählte Technologie die Produktivität und Effizienz des Unternehmens verbessern kann. Cloud-Lösungen nutzen die Eigenschaften der Cloud wie Ressourcen-Pooling, Elastizität und messbare Leistungsparameter. Außerdem werden Cloud-Lösungen mit Blick auf die Sicherheit konzipiert, implementiert und bieten geeignete Verschlüsselungsmechanismen zum Schutz der Daten während der Übertragung und auf den Speichersystemen. Einige Aspekte der Regelkonformität werden durch entsprechende Zertifizierungen, Audit-Funktionen und transparente Verfahren der Cloud-Lösungen erreicht.

Anwendungsfälle

Es mag einfach erscheinen, rein theoretisch über die Vorteile einer professionellen Managed File Transfer Lösung zu sprechen. Bezüglich GoAnywhere MFT in der Cloud gibt es jedoch interessante Anwendungsfälle, welche das Thema auch mit Leben füllen. Die folgenden drei Use-Cases sollen dies veranschaulichen.

Großes, global agierendes Unternehmen aus dem Gesundheitswesen

Eine der wichtigsten IT-Maßnahmen für dieses international tätige Unternehmen aus der Gesundheitsbranche bestand darin, Dienste in die Cloud zur Entwicklung eines hybriden Modells zu migrieren.

Als wir das erste Mal mit dem Unternehmen sprachen, bestand eine langfristige Anforderung darin, MFT zu aktualisieren, da es mit veralteten und unüberschaubaren Prozessen übersät war. Würde man dies nicht zeitnah angehen, könnten potentielle Sicherheitsrisiken nicht ausgeschlossen werden. Außerdem sollte die Cloud-Infrastruktur weiter ausgebaut werden, was für die nächsten 12 Monaten ein priorisiertes Projekt bleiben sollte.

Die derzeitige MFT-Lösung wurde nicht mehr unterstützt und war am Ende ihrer Laufzeit angelangt, was die Aktualisierung bestehender Prozesse und Aufgaben erschwerte. Weiter war die Cloud-Unterstützung begrenzt und stellte ein echtes Problem für die Strategie des Unternehmens dar, mehr Dienste in die Cloud zu migrieren. Daher haben wir Anfang dieses Jahres die Implementierung von GoAnywhere in ihre private Cloud-Umgebung umgesetzt.

Gasversorger

Als wir mit diesem Unternehmen sprachen, wählten sie GoAnywhere MFT als ihre MFT-Lösung aus dem einfachen Grund. Wir besaßen ein Angebot für die Cloud.

Das Unternehmen verfolgte als internes Ziel, so viele Services wie möglich in ihren DevOps-Workflows zu integrieren. Das bedeutete, dass jeder neue Service, den es bereitstellte, mit ihren Containern oder der AWS-Infrastruktur kompatibel sein musste.

Unser Angebot an Docker-Container war zu diesem Zeitpunkt noch nicht ausreichend entwickelt und in Großbritannien fehlte es noch an Know-How, so dass wir uns für die Bereitstellung in AWS entschieden.

Einer der wichtigsten Vorteile der Nutzung von AWS bestand für sie darin, dass sie einen großen Teil des Deployment mit bestehenden Prozessen automatisieren konnten.

Internationales Vertriebsunternehmen

Eine anderes Unternehmen wollte den Platzbedarf für ihre eigene Hardware minimieren und entschied sich für einen SaaS-Ansatz mit MFTaaS.

Sie nutzten GoAnywhere Agents im Rahmen eines hybriden Modells, um eine sichere und vertrauenswürdige Verbindung zwischen der On-Premises Landschaft und der Cloud herzustellen, was ihre langfristige Strategie in der Abschaffung von On-Premises-Diensten unterstützte.

Eine wichtige Anforderung war die Sicherheit, welche wir jedoch auch dank unserer SOC-2 Typ 1 Zertifizierung mit MFTaaS erfüllen konnten. Bei einem Großteil unserer Produktpräsentationen ziehen Kunden MFTaaS oder ein Deployment in ihre private Cloud ernsthaft in Erwägung.





Frage 2: Herausforderungen der Cloud

*Welche Auswirkungen hat eine Cloud-Transformation auf Managed-File-Transfer?
Welche Bereiche des Unternehmens müssen Sie berücksichtigen?*

Funso Richard | Information Security Officer | LinkedIn

Um Störungen im Tagesgeschäfts bzw. Geschäftsbetrieb zu vermeiden, erfordert die Einführung einer Cloud-Strategie eine gründliche Planung. Zieht ein Unternehmen eine Managed File Transfer (MFT) Migration in die Cloud in Betracht, verhält sich das nicht anders. Eine schlecht umgesetzte MFT-Migration in die Cloud kann zu Datenverlusten, regulatorischen Verstößen, Bußgeldern, erheblichen finanziellen Kosten, ineffizienter Entscheidungsfindung aufgrund fehlender Datenbasis, Leistungs- und Produktivitätseinbußen, Unterbrechungen der Lieferkette und negativen Nutzererfahrungen führen. Um all diese negativen Effekte zu vermeiden, ist es wichtig eine gut durchdachte Strategie zu haben.

Die Verlagerung von Daten in die Cloud ist eher eine geschäftliche Entscheidung als ein IT-Prozess. Auch wenn die IT-Abteilung über die grundlegende Technologie verfügt, gibt es Auswirkungen auf den Geschäftsbetrieb, die vor der Datenmigration berücksichtigt werden müssen. Ein wichtiger Gesichtspunkt sind die geschäftlichen Anforderungen. Ja, Daten ist der Treibstoff, der den Geschäftsmotor antreibt, aber um eine optimale Leistung zu erzielen, muss dieser Treibstoff die richtige Qualität haben. Von der Datenerfassung, deren Speicherung, deren Schutz, deren Übertragung, deren Zugriff und Verwaltung sowie deren Vernichtung müssen die geschäftlichen Anforderungen und Bedürfnisse bei der Auswahl eines MFT's und der Datenmigrationsstrategie berücksichtigt werden. Dies ist nicht verhandelbar. Es steht außer Frage, dass MFT in der Cloud die Skalierbarkeit, Mobilität, Transparenz, Interoperabilität und Nutzerfreundlichkeit von Daten in einem hochgradig flexiblen und vernetzten Unternehmens-Ökosystem bietet. Allerdings sind Implementierungskosten und Ressourcen wichtige betriebswirtschaftliche Faktoren. Bei stark regulierte Unternehmen spielen die Anforderungen an die Compliance bei der Verlagerung von Daten in die Cloud eine wichtige Rolle. Um Bedenken an die Compliance zu begegnen, sollten Unternehmen MFT-Lösungen mit integrierten Compliance- und Sicherheitskontrollen wählen.

Soulos Panagiotis | Global Information Security Manager | LinkedIn

Bei der Umstellung auf eine MFT Lösung in der Cloud sollten einige wichtige Punkte berücksichtigt werden. Die Sicherheit der Daten – bei Speicherung und während der Übertragung – sowie die Einhaltung von Vorschriften stehen ganz oben auf der Liste. Es sollte sich keine Möglichkeit bieten, dass die Einführung einer Cloud-MFT Lösung zu rechtlichen, regulatorischen oder sonstigen Compliance-Verstößen führt. Auch die Leistungsfähigkeit des Dienstes sollte berücksichtigt werden. Interoperabilität und Übertragbarkeit sind Schlüsselfaktoren für die Einführung einer Cloud-Lösung. Sie sollten sicherstellen, dass die Migration des Dienstes die geringsten bzw. falls möglich keinerlei Auswirkungen auf den Geschäftsbetrieb des Unternehmens hat, einschließlich aller laufenden Kommunikationskanäle mit kooperierenden Unternehmen und Kunden. Die Service Level Agreements (SLAs) sollten alle Geschäftsanforderungen abdecken, gründlich geprüft und vertraglich verankert werden.

Auch die Schulung der Nutzer, sowohl Anwender als auch IT-Mitarbeiter, sollte berücksichtigt werden, um das Risiko von operativen Störungen aufgrund mangelnder Kenntnis zu minimieren und um das volle Potenzial des Cloud-Dienstes nutzen zu können.

Die Nutzer des Dienstes, Mitarbeiter aus Informationssicherheit, für operationelle Risiken, Compliance und Recht sowie das technische IT Personal sollten mit einbezogen werden, um sicherzustellen, dass der Cloud-Dienst alle Geschäftsanforderungen abdeckt.

Gary Hibberd | Security Consultant | LinkedIn

Damit MFT effektiv funktionieren kann, muss das Unternehmen wissen, welche Daten es besitzt und wie diese verwendet werden. Sobald das verstanden ist, muss eine Strategie zur Umsetzung von MFT entwickelt und im gesamten Unternehmen kommuniziert werden, da wahrscheinlich alle Bereiche des Unternehmens auch mit berücksichtigt werden müssen.

Unternehmensbereiche die derzeit große Mengen personenbezogener oder sensibler Daten per E-Mail oder auch FTP übertragen, sollten priorisiert behandelt werden, da hier die Vorteile und Kontrollmechanismen sichtbar werden. Eine gute MFT-Lösung wird den Datenschutz und die Sicherheit der Daten verbessern.

Durch die Implementierung einer MFT-Lösung können Unternehmen über eine zentral Plattform Datenübertragungen konsolidieren, steuern und überwachen. Dies bietet Transparenz darüber, welche Daten wann und von wem übertragen werden. Da ein solches Monitoring vorhanden ist, unterstützen MFT-Systeme als ein Bestandteil belegbar den internen Auditprozesses.

Ray Sutton | Technical Consultant | [LinkedIn](#)

Wenn Sie Dienste in die Cloud verlagern, müssen Sie auf Risiken, Sicherheit und Leistung achten. Falls das System bei der Verlagerung in die Cloud Performanceprobleme oder hohe Latenzen aufweist, könnte dies dazu führen, dass Ihre Kunden und Anwender den Dienst nicht mehr nutzen oder in dem schlimmsten Fall alternative Möglichkeiten zum Austausch und Kopieren von Dateien verwenden. Dies würde zu Problemen in Bezug auf die Sicherheit und möglicherweise zur Preisgabe vertraulicher Informationen führen. Migration auf eine Cloud-Lösung ist kein einfaches Unterfangen, insbesondere wenn es um personenbezogene oder vertrauliche Daten geht. In jüngster Zeit haben wir einige Sicherheitsverletzungen erlebt, die – vielleicht bei entsprechender Planung und dem Verständnis der Risikofaktoren – hätten vermieden werden können.

Einige Schlüsselbereiche, die Sie berücksichtigen müssen, sind das Verständnis über Ihre Daten und welche Sicherheitsvorkehrungen getroffen werden müssen. Dabei spielt es keine Rolle, ob Sie in die Cloud migrieren oder Ihre Daten On-Premises speichern; die Regeln sind die gleichen. Es ist wichtig, einen Sicherheitsrahmen für Daten zu schaffen und in der Lage zu sein, diese Daten zu verarbeiten und zu sichern. Suchen Sie zum Beispiel nach einer Lösung, die Ihre Daten während der Übertragung und im gespeicherten Zustand verschlüsselt. Achten Sie auf den Schutz dieser Daten, wenn sie den Endpunkt erreichen bzw. im Ziel abgelegt werden. Schauen Sie auch über diesen Endpunkt hinaus und überlegen Sie, wie Sie eine Art Lebenszyklus auf Ihre Daten anwenden können, bei dem Sie kontrollieren, wer sie ansehen, bearbeiten und vielleicht sogar drucken darf.

Die Cloud bietet viele Möglichkeiten, aber es ist wichtig, dass Sie die Art Ihrer Daten verstehen und wissen, wie Sie dieses wertvolle Gut schützen müssen.

Fragen und Antworten: Michael Barford | Solutions Engineer | [LinkedIn](#)

Die Umstellung auf die Cloud ist kein einfaches Projekt. Es gibt verschiedene Faktoren, die dieses geschäftsfördernde Vorhaben beeinflussen werden. Ein Teil der erforderlichen Due-Diligence-Prüfung besteht darin, die richtigen Fragen zu stellen, um auch die beste Lösung für Ihre Unternehmensvision zu finden:

– **Wo finden unsere wichtigsten Prozesse statt: On-Premises oder in der Cloud?**

Das könnte Ihnen helfen, sich für MFT in der Cloud, On-Premises, als Hybridlösung oder auch beides zu entscheiden.

– **Benötigen wir eine MFT-Lösung, die "transparent" ist, unabhängig davon, ob der Informationsfluss in der Cloud, On-Premises oder in einem Hybridsystem stattfindet?**

Heutzutage ist es üblich, dass automatisierte Workflows traditionelle Technologien wie SFTP und FTPS mit gängigen Cloud-Service-Anbietern kombinieren. Sie möchten wahrscheinlich in der Lage sein, komplexe Automatisierungen abstrahiert vom Technologie-Stack zu erstellen, so dass keine IT-Ressourcen mit Kenntnissen rein innerhalb dieser einzelnen Technologien erforderlich sind.

– **Gehen wir zu einer reinen Cloud-Infrastruktur über oder werden wir mittel- bis langfristig weiterhin hybrid arbeiten?**

Die überwiegende Mehrheit der Unternehmen wird Anwendungsfälle haben, bei denen On-Premises und Cloud miteinander verbunden sind. In diesen Fällen kann die Möglichkeit MFT einzusetzen, wann immer wir wollen (On-Premises oder in der Cloud), und die Automatisierung von Prozessen durch Agenten die entscheidende Fähigkeit sein. MFT mit Agenten ermöglicht eine transparente Automatisierung von Workflows mit On-Premises Systemen, in der Cloud und sogar in Kunden- bzw. Partnernetzwerken. Diese Strategie ermöglicht eine reibungslose Migration in die Cloud, die nicht an einem Tag stattfinden kann.

– **Brauchen wir ein MFT als Cloud-Service oder sollten wir es selbst betreiben?**

Falls Sie sich für den Eigenbetrieb entscheiden, sollten Sie prüfen, ob die Lösung zu Ihrer bestehenden Deployment-Strategie passt. Dies bedeutet, es unterstützt ein Deployment als Docker-Container, es ist skalierbar, unterstützt Load-Balancing, usw.

– **Welche Arten von Daten werden wir verarbeiten?**

Sie müssen sich vergewissern, dass die Datenübermittlung auf einem angemessenen Sicherheits- und Compliance-Niveau erfolgt. In der Cloud kann dies eine größere Herausforderung sein. Daher können Sie von Anbietern profitieren, die Zertifizierungen sowie Funktionen wie Verschlüsselung und andere Merkmale anbieten, die Ihren geschäftlichen Anforderungen entsprechen.

Gute und schlechte Praktiken

Wie bei allen Sicherheitsinitiativen gibt es auch Wege Vorschriften einzuhalten, ohne wirklich sicher zu sein. Manchmal ist es einfach eine Checkliste für die Einhaltung von Vorschriften zu erfüllen, aber dennoch bleibt das Unternehmen gefährdet. Um die richtigen Schritte zu unternehmen, geben unsere Experten Ratschläge, was man vermeiden und was man anstreben sollte.

✗ **BAD PRACTICES:** Christos Syngelakis | Chief Information Security Officer | [LinkedIn](#)

Bei der Arbeit mit einer sicheren Dateiübertragungen gibt es viele Herausforderungen zu bewältigen. Die Herausforderung besteht nicht so sehr innerhalb eines einzelnen Unternehmens, eher wenn das Unternehmen auch Aktivitäten außerhalb seiner Umgebung durchführen muss. Zum Beispiel eine medizinische Einrichtung, die große Dateien an Patienten übertragen muss oder auch ein Marketingunternehmen, das Dateien außerhalb des Unternehmens teilt.

In vielen Unternehmen gibt es kein spezielles IT-Personal oder Mitarbeiter, die für diese Art von Transaktionen zuständig sind. Häufig hat der Empfänger nur ein öffentliches E-Mail Konto und sonst nichts. Die angebotenen Lösungen eines Unternehmens, solche Arten von Transaktionen im Rahmen der Unternehmensrichtlinien zu handhaben, passen nicht so recht in dieses Szenario.

Teilweise existieren Möglichkeiten ein Konto einzurichten, um dem Empfänger Zugang über einer der von Ihnen verwendeten Sicherheitslösungen zu gewähren, aber im Allgemeinen sind diese „spontan-Kommunikationsmittel“ nicht bezahlbar. Sie verursachen für diese Art von Aktivitäten nicht nur Personalkosten, sondern vielleicht auch Lizenzkosten. Große, unternehmensinterne Tools für die Zusammenarbeit können den Dateitransfer von Unternehmen zu Unternehmen unterstützen, da es etablierte Mechanismen zwischen den beiden Parteien gibt, aber die On-Demand-Kapazität kann eine große Hürde darstellen.

Eine weitere Herausforderung sind die unterschiedlichen Befugnisse innerhalb der Unternehmen. Manchmal handelt es sich bei der anderen Partei um eine Regierungsbehörde, die Daten übermitteln möchte, aber keine geeignete und sichere Möglichkeit hierfür hat. Jedoch wird darauf bestanden, die Übermittlung in dieser Form dennoch durchzuführen. Mitunter gibt es auch Probleme zeitlicher Natur, jedoch besteht die Unternehmensleitung auf einen sofortigem Transfer. In diesem Falle wird der Anwender jede beliebig verfügbare Software nutzen, um die Aufgabe auch durchzuführen.

Es besteht ein enormer Bedarf an einer Lösung, die einfach zu implementieren und zu nutzen ist, ohne dass der Anwender oder die Gegenseite etwas tun muss. Es gibt zwar einige Lösungen, aber sie sind unbezahlbar, sehr komplex und nicht einfach zu bedienen. Jedes Unternehmen benötigt eine solche Lösung, da eine Vielzahl an verschiedene Dokumenten mit Informationen existieren, von denen man nicht möchte, dass sie für jeden zugänglich sind.

✓ **GOOD PRACTICES:** Chris Hodgson | Business Development Manager | [LinkedIn](#)

Es gibt eine Vielzahl von Protokollen und Methoden für die Datenübertragung mit Kunden und Handelspartnern, die alle ihre Vor- und Nachteile haben. All diese unterschiedlichen Methoden Daten zu teilen kann unübersichtlich, schwer zu handhaben, zu pflegen und nicht regelkonform sein. Eine Lösung wie GoAnywhere bietet eine zentralisierte Secure File Transfer-Lösung, mit der Daten von jedem Endpunkt zu jedem anderem Endpunkt übertragen werden können, sei es von On-Prem zu On-Prem, von Cloud zu Cloud oder eine Mischung aus beidem. GoAnywhere bietet Benutzern und Administratoren einen rollenbasierten Sicherheitsrahmen für Anmeldungen und dem Zugriff auf das System, mit Zwei-Faktor-Authentifizierung und Verschlüsselung aller Dateien und Daten während der Übertragung und bei Speicherung. Dies hilft Unternehmen, den Austausch sensibler Daten zu automatisieren und zu rationalisieren und gleichzeitig die Einhaltung von Branchenstandards zu gewährleisten.

Die Verlagerung in die Cloud ist oft der Auslöser dafür, dass man sich nach einer Lösung für einen gesicherten Dateitransfer umsieht. Cloud-Plattformen bieten einige wirklich gute Möglichkeiten für die Übertragung von Daten innerhalb ihrer eigenen Umgebung. Aber was ihnen fehlt, ist die Möglichkeit Daten zwischen verschiedenen Cloud-Strukturen zu übertragen. Eine Lösung wie GoAnywhere kann helfen, den Datenaustausch zwischen verschiedenen Cloud-Plattformen von einer zentralen Benutzeroberfläche aus zu ermöglichen und zu optimieren. Auch für die Finanzbereiche im Unternehmen, die auf neue Cloud-basierende ERP-Systeme migrieren wollen und eine sichere Methode zur Integration von Dateien und Daten mit nachgelagerten Systemen oder Handelspartner suchen, gibt es gute Gründe die Vorteile einer Secure File Transfer Lösung zu sondieren.

Schlussfolgerung

Daten- und Dateiübertragung ist ein vielschichtiges Thema. Wir haben heute viele Möglichkeiten, Daten und Dateien zu übertragen. Hierüber den Überblick zu behalten ist jedoch eine besondere Herausforderung. Wir verabschieden uns von den Zeiten des File Transfer Protocol (FTP) und des Secure File Transfer Protocol (SFTP) und haben uns neuen Methoden und Produkten zugewandt, bei denen all die Anbieter Cloud-basierend sind. Dies führt zu unterschiedlichen Faktoren. Einige Unternehmen verwenden ältere Methoden, benutzen SFTP, andere wiederum verwenden APIs, die permanent Daten an verschiedene Drittanbieter, Cloud- und SaaS-Lösungen weitergeben. Angesichts der Komplexität all dieser verschiedenen Facetten und der unterschiedlichen Arbeitsweisen gibt es keine Einheitslösung für alle und alles. Die Verfechtung einer einheitlichen Methode ist eine große Herausforderung, da jedes Unternehmen ihren eigenen Weg hat, das zu tun, was es hierbei für richtig hält.

Wichtig ist auch eine Möglichkeit, die Integrität der übertragenen Daten und Dateien zu überprüfen. Es gibt einige gute Lösungen, die Daten und Dateien validieren können. Nehmen Sie viele Daten und Dateien an, stellen Sie Webservices mit hohen Datenaufkommen bereit, können Sie diese vor Übertragung mit einer Online-Scanning-Lösung untersuchen.

Bei der Übertragung von Daten und Dateien geht es nicht immer nur um das Verschieben einer Datei von Ort A nach Ort B. Sie müssen die Sicherheit bei jedem Schritt der Transaktion gewährleisten. Wenn der Vorstandsvorsitzende Sie bittet, die Haushaltsplanungen an einen anderen Standort zu senden, werden Sie das nicht per E-Mail tun. Es gibt einige gute Lösungen, mit denen Sie die Datei klassifizieren und gezielt sperren können.

(Goher Mohammad | Head of InfoSec | [LinkedIn](#))

"Die Dateiübertragung ist komplex, unabhängig davon, ob sie in der Cloud, On-Premises oder hybrid erfolgt. Schränken Sie die Übertragung auf Basis von Dateiendungen ein oder scannen Sie alle eingehenden Daten auf Malware, um die Integrität Ihrer Daten und anderer Komponenten sicherzustellen? Neben der Geltendmachung verschiedener Sicherheitsregularien, wie dies zu geschehen hat, ist es ebenso wichtig, wiederverwendbare Schemata zu haben, um für diese bei Projekten und Maßnahmen, die eine solche Dateiübertragungslösungen entwickeln müssen, eine konsistente Implementierung haben. Ganz gleich, ob es sich um herkömmliches SFTP oder um die Verwendung des SDK und der API-Suite eines Anbieters für die Übergabe an einen S3-Bucket mit strengen Zugriffskontrollen handelt - keine Implementierung ist eine einfache „Verschiebefunktion“. Die Klassifizierung der Daten, ihr Speicherort und die Sicherheitsüberprüfungen im Zusammenhang mit der Implementierung sind alle gleichermaßen wichtig."

(Lidia Guiliano | Information Security Professional | [LinkedIn](#))

Unabhängig davon, ob Ihr Unternehmen gerade erst in die Cloud einsteigt oder bereits eine starke Cloud-Präsenz aufgebaut hat, sollte die Sicherheit ein übergreifendes Unternehmensanliegen sein. Sicherheit ist mehr als nur Sorge zu tragen, dass Ihre Daten nicht dem Internet ausgesetzt sind. Daten sind weder eine statische Entität noch auf einen einzigen Bereich beschränkt. Sie müssen sich bewegen, damit das Unternehmen funktionieren kann. Die Bedeutung einer Managed-File-Transfer Lösung kann nicht hoch genug eingeschätzt werden. Unsere Experten haben viele Denkanstöße gegeben, damit Ihr Unternehmen in der Cloud erfolgreich und sicher wachsen kann.

Wenn Sie mehr darüber erfahren möchten, wie Sie die Sicherheit Ihrer Daten- und Dateiübertragungen bewerkstelligen und steuern können, kontaktieren Sie uns [hier](#).

FORTRA

Fortra.com/de

Fortra ist ein Cybersicherheitsunternehmen wie kein anderes. Wir schaffen eine einfachere, stärkere Zukunft für unsere Kunden. Unsere vertrauenswürdigen Experten und unser Portfolio integrierter, skalierbarer Lösungen sorgen für Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Wir sind der positive Veränderer und Ihr unermüdlicher Verbündeter, der Ihnen bei jedem Schritt Ihrer Cybersecurity-Reise ein sicheres Gefühl gibt. Erfahren Sie mehr unter [fortra.com](#).

Über Fortra