WHITEPAPER

RISIKEN BEIM DATENAUSTAUSCH

GEFAHREN ERKENNEN UND EFFIZIENT VERMEIDEN

inklusive Handlungsempfehlungen

FTAPI

Inhalt

1. Einleitung 3

2. Gefahrenquelle Datentransfer 4

3. Lösungen für den Datenaustausch 6

4. Entscheidende Kriterien für eine sichere Datenaustausch-Lösung 8

5. Handlungsempfehlungen 9

6. Ausblick 10

7. Risiken beim Datentransfer minimieren mit FTAPI 11

8. Fazit 12

1. Einleitung

Die sichere Übertragung von Daten ist in der heutigen Geschäftswelt von entscheidender Bedeutung. Getrieben von Digitalisierung und Globalisierung steigt das Volumen der digitalen Datenmengen weltweit seit Jahren exponentiell an. Der Trend zu Home Office und Hybrid Work hat die virtuelle Zusammenarbeit weiter verstärkt - und das auch weit über Firmen- und Landesgrenzen hinaus. Doch gerade der Austausch von unternehmenskritischen, sensiblen und personenbezogenen Daten stellt hohe Anforderungen an Datenschutz und IT-Sicherheit.

Eine effiziente Zusammenarbeit erfordern einen reibungslosen Datentransfer. Unternehmen, aber auch Behörden und Organisationen sind auf sichere Übertragungswege angewiesen, um den Schutz sensibler Informationen zu gewährleisten.

Dennoch besteht beim Thema sicherer Datentransfer weiter Nachholbedarf. Das ist das Ergebnis des **Secure Data Reports von FTAPI**. Demnach nutzen nur 35 Prozent der befragten Unternehmen eine Lösung für einen sicheren Datentransfer. Zu den Gründen zählen neben mangelnder fachlicher Kompetenz vor allem die zu hohen Kosten. Obwohl das Bewusstsein um Cyberrisiken kontinuierlich steigt und der Schutz von Daten „at rest" in Unternehmen und Behörden inzwischen zum Standard gehört, wird der Schutz der Daten „in motion" immer noch vernachlässigt.

Dieses Whitepaper hat das Ziel, die verschiedenen Risiken beim Datentransfer zu identifizieren, zu analysieren und bewährte Praktiken zur Minimierung dieser Risiken vorzustellen, um sichere und effektive Datentransferpraktiken in ihrer Unternehmensinfrastruktur zu implementieren und so langfristig in die Sicherheit von Systemen und Daten zu investieren.

2. Gefahrenquelle Datentransfer

Ein unbefugter Zugriff Dritter auf Daten und Informationen stellt eine erhebliche Bedrohung für die Datensicherheit dar. Daten können nicht nur unbemerkt abfließen, sondern auch manipuliert werden. Das beeinträchtigt die Integrität der Daten und kann dazu führen, dass aufgrund der Manipulation falsche Entscheidungen getroffen werden, die mitunter gravierende Konsequenzen für das Unternehmen haben können.

Die Auseinandersetzung mit diesen Datensicherheitsrisiken erfordert eine umfassende Sicherheitsstrategie, die sowohl technologische als auch organisatorische Maßnahmen beinhaltet.

Technologische Risiken

Die technologischen Risiken beim Datentransfer umfassen verschiedene Aspekte, die die Integrität und Verfügbarkeit von Daten beeinträchtigen können. Es ist entscheidend, diese Risiken zu verstehen und geeignete Maßnahmen zu ergreifen, um einen sicheren Datentransfer zu gewährleisten.

Die Integration von Systemen mit unterschiedlichen Technologien kann zu Inkompatibilitäten führen, die den Datentransfer beeinträchtigen. Eine umfassende Planung und Standardisierung sind erforderlich, um reibungslose Integrationen zu gewährleisten.

Auch Systemausfälle können den Datentransfer erheblich beeinträchtigen. Die Implementierung von Redundanzmechanismen und Notfallwiederherstellungsplänen ist wichtig, um Ausfallzeiten zu minimieren. ine mögliche Maßnahme ist der verstärkte Einsatz von On-Demand-Services, der es ermöglicht, Kernservices zu dezentralisieren und somit die Resilienz gegenüber externen Angriffen zu stärken. So sind Unternehmen besser in der Lage, Ausfälle durch Cyberangriffe zu minimieren und ihre Geschäftskontinuität auch im Falle eines erfolgreichen Angriffs zu wahren.

Darüber hinaus bieten Cloud-Plattformen automatisierte Sicherheitsfunktionen, die kontinuierlich Bedrohungen überwachen, erkennen und darauf reagieren. Dies ermöglicht eine schnellere Reaktion auf potenzielle Angriffe, ein automatisiertes Einspielen von Sicherheitsupdates und -Patches und schont damit die knappen Ressourcen in den IT-Abteilungen.

Compliance und Datenschutz

Die Einhaltung von Datenschutzbestimmungen und gesetzlichen Vorgaben ist für Unternehmen von zentraler Bedeutung, um rechtliche Konsequenzen zu vermeiden und das Vertrauen der Kunden zu wahren. Die Compliance-Risiken beim Datentransfer umfassen verschiedene Aspekte, die sorgfältige Aufmerksamkeit erfordern.

Dabei kann die Nichterfüllung von Datenschutzbestimmungen wie der EU-DSGVO zu rechtlichen Konsequenzen führen. Unternehmen müssen sicherstellen, dass ihre Datentransferpraktiken den geltenden nationalen und internationalen Datenschutzvorschriften entsprechen, denn Verstöße gegen Datenschutzvorschriften können zu erheblichen finanziellen Strafen und einem massiven Reputationsschaden und Vertrauensverlust bei Kunden und Geschäftspartnern führen.

Sicherheitsfaktor Mensch

Auch menschliche Faktoren spielen bei einem sicheren Datentransfer weiterhin eine entscheidende Rolle und erfordern besondere Aufmerksamkeit und Maßnahmen zur Risikominderung.

Schon eine übereilt versendete E-Mail kann zu einem unbeabsichtigten Datenleck führen, beispielsweise dann, wenn die Informationen an den falschen Empfänger geschickt oder personenbezogene Daten nicht verschlüsselt übertragen werden. Um die Risiken durch Flüchtigkeitsfehler zu minimieren, sollten Unternehmen darauf achten, dass Mitarbeitende regelmäßig geschult werden, um sie für mögliche Datenlecks zu sensibilisieren, das Bewusstsein für Sicherheitsrisiken zu schärfen und sie im Umgang mit entsprechenden Lösungen für einen sicheren Datenaustausch zu schulen. Klare Zugriffsrichtlinien können die Sicherheit von Daten zusätzlich erhöhen.

Voraussetzung ist, dass Lösungen für einen sicheren Datentransfer überhaupt zur Verfügung stehen. Gibt es solche Lösungen nicht, greifen die Mitarbeitenden auf nicht genehmigte Anwendungen und Dienste zurück. Was entsteht, ist die sogenannte Schatten-IT, also ein Wildwuchs an nicht-autorisierten Lösungen - und damit eine zusätzliche Sicherheitslücke in der Unternehmens-IT. Um die Entstehung zu vermeiden, lohnt es sich, konkrete Richtlinien zur Nutzung von IT-Ressourcen aufzustellen und alternative, benutzerfreundliche, sichere Lösungen anzubieten, um die Entstehung von Schatten-IT zu minimieren.

Die Benutzerfreundlichkeit hat einen entscheidenden Einfluss auf die Akzeptanz sicherer Datentransferlösungen. Benutzerfreundliche Schnittstellen, eine intuitive Benutzeroberfläche und eine nahtlose Integration in das bestehende Arbeitsumfeld tragen dazu bei, dass Sicherheitsrichtlinien effektiv umgesetzt werden.

Die Datensicherheit ist von zentraler Bedeutung für den sicheren Datentransfer. Verschiedene Risiken können die Integrität, Vertraulichkeit und Verfügbarkeit von Daten gefährden. Dennoch werden hochsensible Daten oder personenbezogene Informationen häufig unverschlüsselt versendet.

3. Lösungen für den Datenaustausch

Nachteile gängiger Datentransfer-Lösungen

Unverschlüsselte E-Mail: Häufig werden Dateien unverschlüsselt per Mail aus der gewohnten Umgebung heraus erfolgt verschickt. Das ist nicht nur unsicher, oft gibt es auch Größenbeschränkungen beim Sender oder Empfänger, die die Übermittlung unmöglich machen. Zudem besteht die Gefahr, dass Firewalls und Spamfilter Anhänge blockieren oder entfernen.

Physische Datenträger: Die Übermittlung umfangreicher Datenmengen auf physischen Medien wie Festplatten, CDs oder USB-Sticks durch Kurierdienste, Postversand oder persönliche Übergabe steht nicht nur im klaren Widerspruch zur Digitalisierung, sondern bringt auch erhebliche Risiken mit sich, etwa durch möglichen Verlust oder Diebstahl. Darüber hinaus gestaltet sich diese Art der Datenübertragung als äußerst umständlich und zeitaufwendig.

Cloud Services außerhalb der EU: Für die unkomplizierte Übertragung großer Datenmengen, die nicht mehr in den E-Mail-Anhang passen, werden oft internationale Cloud Anbieter genutzt, im Internet verwendet - insbesondere dann, wenn die Unternehmens-IT keine geeignete Lösung für einen sicheren Datentransfer zur Verfügung stellt. Die Server stehen dabei allerdings häufig außerhalb der EU, sodass die Nutzung der Services unter Umständen gegen die EU-DSGVO verstößt.

FTP-Server: Diese Übertragungsmethode, die den Transfer von Datenmengen ohne Größenbeschränkungen ermöglicht, weist zwar höhere Sicherheitsstandards als Cloud Services auf, allerdings ist die Bedienung kompliziert und umständlich.

Anforderungen an eine sichere Datentransfer-Lösung

Ende-zu-Ende-Verschlüsselung
Überall dort, wo Sicherheit und Nachvollziehbarkeit bei der Übertragung vertraulicher Daten gefragt sind, kommen Unternehmen an einer Ende-zu-Ende-Verschlüsselung der Daten nicht vorbei. Sie umfasst eine sichere Verschlüsselung des Transportweges sowie die Verschlüsselung der Nachricht und der angehängten Dateien.

Die Ende-zu-Ende-Verschlüsselung beginnt auf dem Endgerät des Versenders und erstreckt sich über den gesamten Übertragungsweg bis hin zum Empfänger. Dabei gilt das Zero-Knowledge-Prinzip, das unter Sicherheitsexperten als wirksamstes Mittel gegen Cyberkriminalität gilt.

Das heißt, nicht einmal der Anbieter und Betreiber einer Verschlüsselungslösung, eines Datentransfer-Systems oder eines Cloud-Speicherdienstes darf an den zur Entschlüsselung benötigten Key herankommen und so Einblick in die Daten seiner Kunden erhalten.

Dabei spielt die eingesetzte Verschlüsselungstechnologie eine wichtige Rolle. Bei der Auswahl einer optimalen Lösung sollten Unternehmen darauf achten, dass wichtige Kriterien erfüllt werden: Die Ende-zu-Ende-Verschlüsselung muss BSI-konform und der verwendete Algorithmus als sicher eingestuft sein. Zudem muss sie eine dem aktuellen Standard entsprechende Schlüssellänge verwenden.

Einfache Bedienbarkeit sorgt für Akzeptanz
Auch die einfache Bedienbarkeit ist von zentraler Bedeutung. Denn eine Software-Lösung kann nur dann ihren Zweck erfüllen, wenn sie von allen Beteiligten genutzt und als fester Bestandteil des Alltags akzeptiert wird. Lange Zeit war die Ende-zu-Ende-Verschlüsselung von Nachrichten und Dateien allerdings eine sehr komplexe Angelegenheit, die aufwendige Schulungen der Mitarbeiter erforderte.

Heute gibt es Lösungen, die sehr einfach zu handhaben, rasch in bestehende Systeme integrierbar und individuell an die Erfordernisse von Unternehmen anpassbar sind. Eine intuitive Benutzeroberfläche, die leicht verständlich und gut strukturiert ist, ermöglicht es allen Nutzern, die Lösung ohne lange Schulungen und Einarbeitungszeiten zu verwenden. Die komplexe Sicherheitstechnologie bleibt somit für die Anwender im Hintergrund verborgen und macht den verschlüsselten Versand von sensiblen Daten so einfach wie das Versenden einer ganz normalen E-Mail.

Nur, wenn die Verschlüsselungslösung so einfach zu bedienen ist wie ein E-Mail-Programm und nahtlos darin integriert werden kann, wird sie auch von Mitarbeitern, Partnern und Kunden akzeptiert und genutzt. Im einfachsten Fall benötigt der E-Mail- Empfänger keine spezielle Software, um die Nachricht zu öffnen.

Weitere Anforderungen
Darüber hinaus sollte sich eine Softwarelösung für den sicheren Datentransfer unbedingt nahtlos in bestehende Systeme integrieren lassen, individuell an die Erfordernisseder Unternehmen anpassbar, nachvollziehbar und Kosten-transparent sein, sowie die Übertragung hoher Datenmengen ohne Größenlimit sicherstellen. Selbstverständlich müssen auch die DSGVO-Konformität und die Einhaltung von Compliance-Vorgaben (z.B. Zertifizierungen nach BSI C5 und ISO 27001) gewährleistet werden. Zudem garantiert eine optimale Lösung einen geringen Verwaltungsaufwand und entlastet die IT-Administratoren.

Die Einsatzmöglichkeiten für sichere Datentransferlösungen sind äußerst vielfältig und gehen weit über die Kernfunktionen des E-Mail-Versandes oder von Transferplattformen hinaus. An den richtigen Stellen eingesetzt helfen sie, die Digitalisierung in Unternehmen mit einfachen Mitteln voranzutreiben und die Effizienz von Arbeitsprozessen erheblich zu steigern. Enorme Potenziale lassen sich ohne großen Aufwand besonders im Inputmanagement, Rechnungseingang, Bewerbermanagement, einem sicheren Hinweisgeber-System für Whistleblower oder dem Versand von Gehaltsabrechnungen heben.

4. Entscheidende Kriterien für eine sichere Datenaustausch-Lösung

1. Maximaler Nutzer-Komfort

Eine intuitive Bedienbarkeit sowie ein minimaler Einführungsaufwand erhöhen die Akzeptanz gegenüber der neuen Lösung.

2. Höchste Sicherheit

Eine durchgehende Ende-zu-Ende-Verschlüsselung schützt Ihre Daten vor dem Zugriff Dritter und gewährleistet Ihnen höchste Sicherheit bei der digitalen Kommunikation.

3. Kein Größenlimit

Dateien jeglicher Art und Größe müssen sicher aus einer Lösung übertragen werden können.

4. Nahtlose Integration in bestehende Systeme

Fügt sich die Lösung problemlos in bestehende Systeme ein, können die Mitarbeitenden direkt in ihrer gewohnten Umgebung weiterarbeiten.

5. Datensouveränität und Nachvollziehbarkeit

Jederzeit die Kontrolle über den Datenfluss im eigenen Unternehmen zu behalten und die Souveränität der Daten zu gewährleisten, ist heute essentiell für den Unternehmenserfolg.

6. Geringer Verwaltungsaufwand

Eine schnelle Implementierung vermeidet zusätzlichen Admin-Aufwand und schont personelle Ressourcen in Ihrer IT-Abteilung.

7. Kosten

Anfallende Kosten müssen transparent und leicht nachvollziehbar sein. Für externen Empfänger:innen dürfen keine Extrakosten oder zusätzlicher Aufwand enstehen.

8. Automatisierungen

Zeit und Kosten sparen Sie durch die Automatisierung von analogen Prozessen oder den Ausbau bereits bestehender Prozesse.

9. Deutscher Lösungsanbieter

Entwicklung, Support und Hosting in Deutschland sowie ein einsehbarer Kundenstamm sind Grundvoraussetzung für einen glaubwürdige Lösungsanbieter.

10. Transparenz durch Zertifizierungen

Zertifizierungen nach ISO beispielsweise zeigen wie hoch der Sicherheitsaspekt gewichtet wird und wie viel Wert das Unternehmen darauf legt den eigenen Anspruch an die Sicherheit auch nach außen zu demonstrieren.

5. Handlungsempfehlungen

Die Herausforderungen beim Datentransfer erfordern eine ganzheitliche Sicherheitsstrategie, die technologische, organisatorische und menschliche Aspekte berücksichtigt. Basierend auf den analysierten Risiken, bewährten Praktiken und Fallstudien bietet sich eine Kombination aus technischen und organisatorischen Maßnahmen an, um die Sicherheit des Datentransfers zu erhöhen und Risiken beim Datenaustausch zu minimieren.

Technologische Maßnahmen

1. Implementierung robuster Verschlüsselungstechnologien
Nutzen Sie Ende-zu-Ende-Verschlüsselung für alle Datentransfers, insbesondere in Cloud-Umgebungen.

2. Umfassendes Berechtigungsmanagement
Definieren Sie klare Zugriffsrechte für Benutzer basierend auf ihren Rollen und Aufgaben und implementieren Sie eine regelmäßige Überprüfung und Aktualisierung von Berechtigungen.

3. Usability-orientierte Sicherheitslösungen
Entwickeln Sie Sicherheitslösungen, die benutzerfreundlich sind und nahtlos in die täglichen Arbeitsabläufe integriert werden können. Bieten Sie klare Anweisungen und Schulungen zur Nutzung sicherer Funktionen.

4. Zwei-Faktor-Authentifizierung
Nutzen Sie zusätzliche Maßnahmen, um die Sicherheit Ihrer Systeme zu erhöhen. Führen Sie eine Zwei-Faktor-Authentifizierung für alle Benutzerkonten ein und schulen Sie Ihre Mitarbeitenden in der Nutzung.

Organisatorische Maßnahmen

1. Schulungen und Sensibilisierung der Mitarbeiter
Führen Sie regelmäßige Schulungen durch, um Mitarbeiter über Sicherheitsrisiken und bewährte Praktiken zu informieren, sensibilisieren Sie Mitarbeiter für die Gefahren von Schatten-IT und fördern Sie die Nutzung genehmigter Alternativen.

2. Klare Richtlinien für sicheren Datentransfer
Erstellen Sie klare Richtlinien für den sicheren Datentransfer und stellen Sie sicher, dass sie von allen Mitarbeitern verstanden werden.

3. Notfallvorsorge und Wiederherstellung
Entwickeln Sie umfassende Notfallwiederherstellungspläne, um auf technische Ausfälle vorbereitet zu sein.

4. Förderung einer Sicherheits- und Fehlerkultur
Etablieren Sie eine Unternehmenskultur, die Sicherheit als gemeinsame Verantwortung aller Mitarbeiter betrachtet.

Die Kombination dieser technologischen, organisatorischen und menschlichen Maßnahmen bildet eine umfassende Sicherheitsstrategie, um Risiken beim Datentransfer zu minimieren. Unternehmen sollten diese Empfehlungen an ihre spezifischen Anforderungen anpassen und regelmäßig überprüfen, um auf sich entwickelnde Bedrohungen vorbereitet zu sein.

6. Ausblick

Die Zukunft des Datentransfers steht vor verschiedenen Herausforderungen und Chancen, die maßgeblich von technologischen Fortschritten, gesellschaftlichen Entwicklungen und sich wandelnden Sicherheitsanforderungen geprägt werden.

Beispielsweise kann der Aufstieg von Quantencomputern die herkömmliche Verschlüsselungstechnologie in Frage stellen. Organisationen müssen sich auf die Integration quantensicherer Verschlüsselungsstandards, beispielsweise durch den Einsatz kryptoagiler Verschlüsselungsverfahren, vorbereiten, um die Sicherheit ihrer Daten langfristig zu gewährleisten.

Die Weiterentwicklung von Künstlicher Intelligenz (KI) wird durch die Erkennung und Abwehr von Cyberangriffen eine Schlüsselrolle in der IT-Sicherheit einnehmen. Durch den Einsatz von fortschrittlichen KI-Algorithmen können Unternehmen Anomalien in Echtzeit identifizieren und automatisierte Reaktionen auf Sicherheitsvorfälle implementieren.

Die Datenschutzgesetzgebung wird voraussichtlich weiterhin verschärft werden, um den wachsenden Herausforderungen im Bereich des Datentransfers gerecht zu werden. Eine aktuelle Entwicklung ist **NIS 2**, eine neue Richtlinie zur Steigerung der Cybersicherheit in Europa, die bis Oktober 2024 in den Unternehmen umgesetzt werden muss.

Das Europäische Parlament reagiert damit auf die zunehmenden Digitalisierung die damit einhergehende Verschärfung der Bedrohungslandschaft für Cybersicherheit. NI2 2 ist eine Erweiterung von NIS 1, die bereits besteht, und umfasst deutlich mehr Anwendungsbereiche der Cybersicherheitsvorschriften und wird auf neue Sektoren und Einrichtungen erweitert.

Gesetzliche Änderungen wie NI2 2 und die angespannte Lage der Cybersicherheit in Europa erfordern es, dass Organisationen ihre Datenschutzpraktiken kontinuierlich anpassen müssen, um sicherzustellen, dass sie mit den aktuellen und zukünftigen rechtlichen Anforderungen konform sind.

Angesichts der zunehmenden Globalisierung und Vernetzung wird die internationale Zusammenarbeit im Bereich der Cybersicherheit entscheidend sein. Die Entwicklung von internationalen Standards und Vereinbarungen wird dazu beitragen, gemeinsame Ansätze zum Schutz des Datentransfers zu fördern.

Insgesamt wird die Zukunft des Datentransfers von einer ständigen Anpassung an technologische, regulatorische und gesellschaftliche Veränderungen geprägt sein. Organisationen, die proaktiv auf diese Entwicklungen reagieren, haben die Möglichkeit, ihre Datentransferpraktiken zu optimieren und ihre Daten effektiv zu schützen.

7. Risiken beim Datentransfer minimieren mit FTAPI

Ein erfahrener Spezialist für den sicheren und einfachen Transfer sensibler Daten ist das Münchener IT-Unternehmen FTAPI. Der IT-Experte hilft Unternehmen aller Größen und Branchen dabei, eine sichere digitale Kommunikation einzuführen und damit Arbeitsabläufe effektiver und kostensparender zu gestalten.

Ein erfahrener Spezialist für den sicheren und einfachen Transfer sensibler Daten ist das Münchener IT-Unternehmen FTAPI. Der IT-Experte hilft Unternehmen aller Größen und Branchen dabei, eine sichere, digitale Kommunikation einzuführen und dadurch Arbeitsabläufe effektiver und kostensparender zu gestalten.

Im Kern stehen die Produkte **FTAPI SecuMails** und **FTAPI SecuRooms**, die den hochsicheren Datenaustausch mit unbegrenzter Größeüber eine Ende-zu-Ende-Verschlüsselung möglich machen. FTAPI zählt zu Deutschlands wachstumsstärksten Technologieunternehmen und wurde mit dem Deloitte Fast 50 Award ausgezeichnet.

FTAPI bietet eine umfassende Plattform für einfache und sichere Daten-Workflows und Automatisierung. Damit verbindet FTAPI Menschen, Daten und Systeme sicher, schnell und einfach. Seit 2010 vertrauen über 2.000 Unternehmen und mehr als eine Million aktive Nutzer:innen auf die Produkte SecuMails, SecuRooms, SecuForms und SecuFlows — egal ob es um das Senden oder Empfangen von Daten, den strukturierten Dateneingang, das Teilen von vertraulichen Informationen oder die sichere Automatisierung von Daten-Workflows geht: mit der Secure Data Workflow Plattform von FTAPI sind sensible Daten jederzeit DSGVO-konform geschützt.

Die FTAPI Plattform:
Ein umfangreiches Angebotsspektrum für Ihre Bedürfnisse

FTAPI SecuMails

Dateien jeder Größe einfach und sicher per Mail senden und empfangen

FTAPI SecuForms

Dateneingänge einfach, sicher und strukturiert managen

FTAPI SecuRooms

Dateien einfach und sicher speichern, teilen und gemeinsam nutzen

FTAPI SecuFlows

Sensible Daten-Workflows aus einer Hand einfach und sicher automatisieren

8. Fazit

Die Absicherung des E-Mail-Verkehrs und darüber hinaus der sichere Datentransfer wird immer mehr zum entscheidenden Erfolgsfaktor für Unternehmen, gerade auch im Mittelstand. Datenverluste führen zu hohen Kosten und können sogar die Existenz der Firma gefährden. Dabei ist der sichere Austausch von Daten kein Hexenwerk. IT und Datenschutz sind gefordert, professionelle Lösungen bereit zu stellen, die den Sicherheitsanforderungen in Unternehmen genügen und den Versand von Dateien für die Mitarbeiter so einfach wie möglich machen.

Mit der richtigen Software-Lösung wird eine Ende-zu-Ende-Verschlüsselung und eine einfache Handhabung für alle Beteiligten sichergestellt. Dabei lassen sich sichere Datentransferlösungen auch für Aufgaben jenseits des klassischen E-Mail-Versandes einsetzen, um weitere Potenziale zu heben. Ein digitales Inputmanagement, der digitaleRechnungseingang oder die digitale Gehaltsabrechnung sind schnell auf höchstem Sicherheitsniveau eingerichtet. Damit lassen sich standardisierte, aufwendige Arbeitsabläufe wesentlich effizienter gestalten und Kosten sparen.

Vorteile von FTAPI

Höchste Sicherheit
Vom sicheren Downloadlink bis hin zur durchgehenden Ende-zu-Ende-Verschlüsselung.

DSGVO-konform
Versenden und empfangen Sie personenbezogene Daten datenschutzkonform und sicher.

Personalisierbarkeit
Passen Sie Farben, Logos und Texte der CI Ihres Unternehmens an und schaffen Sie so Vertrauen.

Einfache Bedienung
Die Nutzung aller unserer Produkte ist leicht verständlich und intuitiv.

Zertifizierungen und Pentest
FTAPI ist ISO-zertifiziert und unterzieht sich jährlich einem unabhängigen Pentest.

Zentrale Administration
Verwalten Sie SecuMails, SecuRooms, SecuForms bzw SecuFlows inkl Add-Ons an einer zentralen Stelle.

Größenbeschränkung
Tauschen Sie auch besonders große Datenmengen sicher und verschlüsselt aus.

Transparenz
Empfangs- und Downloadbestätigungen machen Ihre Datenaustauschprozesse transparent.

Automatisierungen
Mit FTAPI SecuFlows atomatisieren Sie aufwendige manuelle, wiederkehrende Prozesse in Ihrem Unternehmen.

Zertifizierungen

SySS THE PENTEST EXPERTS. Certified Product Approved Security TESTED 10.2022

TÜVRheinland ZERTIFIZIERT Management System ISO/IEC 27001:2013 www.tuv.com ID 9000015007

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft

Software Hosted in Germany Bundesverband IT-Mittelstand e.V.

BSI-C5-TESTAT

Unsere Kunden

Kundenzitate

Andreas Hallemann

Leitung BO/IT und Statistik, Verband der Versicherungsunternehmen Österreichs

Mit der Möglichkeit externe Partner einfach in den Geschäftsprozess einzubinden sowie dem ansprechenden Design und dem für den VVO optimalen Lizenzmodell sind wir froh uns für FTAPI entschieden zu haben.

Mike Felber

IT-Administrator, Kommunaler Sozialverband Sachsen

Datensicherheit spielt bei der Kommunikation zwischen Behörden, externen Stellen und Bürgern eine wichtige Rolle. FTAPI hat uns dabei unterstützt Digitalisierung und Datensicherheit in Einklang zu bringen.

Gregorio Aversa

Sales & Account Management / Leiter DSAG Personalwesen Schweiz

Wir stellen unseren Kunden HR-Komplettlösungen rund um den Employee Lifecycle bereit. Das effiziente Management und die Weiterverarbeitung von personenbezogenen Daten spielt dabei eine wichtige Rolle. Wir freuen uns mit FTAPI einen vertrauensvollen Partner gefunden zu haben, um die digitale Transformation im Personalmanagement weiter voranzutreiben.

Alexander Glöckler

Gesellschafter & Kaufmännischer Leiter; CNC-Fertigung Glöckler KG

Wir nutzen zur Verschlüsselung unserer E-Mails und Daten das Produkt von FTAPI. Wir sind sehr zufrieden, auch in Bezug auf die Abwicklung und den Support. Eine super Anwendung.

FTAPI

FTAPI GmbH
Steinerstraße 15f
81369 München

T: +49 89 230 69 54 0
F: +49 89 230 6954 10
info@ftapi.com
www.ftapi.com