Telefax - Sicherheitslösungen

- Whitepaper -

- Rechtliche Situation
- Technische Realisierung
- Auswahlkriterien

GTC®
TeleCommunication GmbH

Inhalt

Die Sicherheit der Daten spielt heutzutage in jedem Unternehmen eine übergeordnete Rolle – nicht zuletzt durch die DSGVO. Eine besondere Herausforderung stellt dabei die Übermittlung der Daten an Dritte dar. Denn hier verlassen die Daten den geschützten Bereich des Unternehmens.

Natürlich ist die E-Mail für den Austausch von Informationen in Unternehmen heute unabdingbar geworden. Allerdings: wenn man sicher sein möchte, dass etwas beim Empfänger ankommt, erweist sich die E-Mail oft als äußerst ungeeignet: viele erwünschte Mails landen regelmäßig – unerkannt – im Spam-Filter des Empfängers und erreichen diesen nie. Hier ist die Übermittlung per Fax eine schnelle und praktikable Alternative – denn das Fax kommt garantiert viren- und trojanerfrei direkt beim Empfänger an.

Datensicherheit kann eine E-Mail aber schwer bieten – es sei denn, man verschlüsselt sie. Aber dann müssen Sender und Empfänger sich auf eine Verschlüsselungsmethode einigen und alle Beteiligten diese korrekt nutzen. Ein Medium, das eine einfache, schnelle Kommunikation mit hoher Sicherheit bietet, ist das Fax - nicht als verstaubtes Thermofaxgerät, sondern als Übertragungsweg. Denn die Daten werden bei der traditionellen Fax-Übertragung nicht in „Klarschrift“ über das Internet geschickt – für jeden einsehbar. Bei der Fax-Übertragung wird das Bild zunächst codiert, versandt und dann decodiert. Das macht das Fax während der Übertragung nicht ohne erheblichen Aufwand abhör-/abfangbar. Ganz anschaulich gesprochen: eine Bildinformation ist einfach schwerer zu scannen/lesen als eine reine Textinformation wie bei einer E-Mail.

Welche Möglichkeiten bestehen, das Fax als sicheren Kommunikationsweg zu nutzen und wie man diese Sicherheit noch zusätzlich erhöhen kann, beschreiben wir im Folgenden.

1. Rechtliche Möglichkeiten bei der Kommunikation von Daten per Fax

Ein Dokument, das per Fax übermittelt wird, gilt gemäß deutschem Recht prinzipiell als rechtlich bindend. Das Fax eignet sich dabei bei allen Erklärungen, die keine besondere Formerfordernis haben bzw. für die die einfache Schriftform ausreicht. Dadurch eignet sich das Fax gut für den normalen Geschäftsalltag mit dem Versand von Bestellungen, Auftragsbestätigungen und sogar Rechnungen. Für den Nachweis des Versandes/Empfanges dienen Sende- und Empfangsprotokolle. Wenn allerdings die Übersendung eines unterschriebenen Originaldokumentes per Gesetz zwingend vorgeschrieben ist, reicht das Fax nicht – dann muss man auf die Briefpost zurückgreifen.

2. Besondere Daten, die per Fax sicher kommuniziert werden können

Das Fax eignet sich vor allem für den Austausch von Daten mit Empfängern, mit denen keine separate, gesicherte Datenkommunikation (Austausch per EDI) eingerichtet ist. Die Nutzung der Fax-Übertragung als Kommunikationskanal ermöglicht es damit, jedem Empfänger, der über einen Fax-Anschluss verfügt, die Daten einfach zu übermitteln und doch mit einem höheren Schutzgrad als eine normale E-Mail.

Besonders schützenswerte Daten sind dabei vor allem:

- **Kundendaten** (Adressdaten, Preise, Konditionen, u.v.m) - Schutz vor Zugriff auf die Konkurrenz
- **Personenbezogene Daten** (Namen, E-Mail-Adressen, persönliche Informationen) – Verpflichtung zum Schutz gemäß DSGVO
- Besonders schützenswert: **Kreditkartendaten** – bspw. bei Bestellungen oder Reservierungsbestätigungen
- Besonders schützenswert: **Gesundheitsdaten** im Speziellen – bspw. bei der Übermittlung von Labor- und Untersuchungsergebnissen, die schnell übermittelt werden müssen

Sobald solche Informationen versandt werden, müssen sie entsprechend auch bei der Übermittlung besonders geschützt werden.

3. Wie läuft die Fax-Übertragung beim Fax ab?

Bei der Übertragung von Dokumenten per Fax erfolgt eine Umcodierung in ein Tonsignal, das über normale Telefonleitungen übertragen wird. Dabei baut der sendende Fax-Anschluss eine direkte Wahlverbindung zum empfangenden Faxgerät auf. Diese „begrüßen" sich per Tonsignal – und erst dann erfolgt die Übertragung. Auf der Empfängerseite werden die Tonsignale wieder decodiert und in das ursprüngliche Fax-Bild umgewandelt. Diese Verbindung ist eine End-to-End-Verbindung. Prinzipiell kann diese abgehört werden – aber mit dem gleichen Aufwand wie eine Telefonverbindung abgehört werden kann, also nur mit entsprechendem technischem und rechtlichem Aufwand.

Zusätzlich zum übertragenen Fax tauschen Sender und Empfänger außerdem eine Sendekennung aus, die von den Systemen entsprechend dokumentiert wird. Dadurch lassen sich Sender wie Empfänger über die Sendekennung identifizieren.

Heutzutage erfolgt die Fax-Übermittlung teilweise auch per VoIP (Voice over IP – also per Internet). Hierbei werden die Tonsignale der Faxübertragung zunächst digitalisiert, in einzelne Pakete aufgeteilt und per Internet versandt. Die Empfängerseite empfängt die Pakete, sortiert und wandelt sie wieder in ein Tonsignal um – das als Fax ausgewertet werden kann. Auch hier erfolgt keine Übertragung in Klartext.

4. Wo sind die „Angriffspunkte" beim Fax?

Prinzipiell erfolgt die Übermittlung bei einem Standardfax von Faxgerät zu Faxgerät über eine Telefonleitung. Dieser Weg ist zwar nicht verschlüsselt - allerdings können die so übermittelten Daten genauso einfach oder schwer abgehört werden wie eine normale Telefonleitung: mit richterlichem Beschluss und entsprechender Technik sowie Zugang. Im Gegensatz zu einer E-Mail ist das Mitlesen somit deutlich schwieriger.

Bei der Nutzung über VoIP erfolgt die Übertragung der Fax-Daten in Paketen über das Internet. Die Übertragung erfolgt dabei in der Regel automatisch bereits verschlüsselt – im Gegensatz zu einer normalen unverschlüsselten E-Mail. Der Zugriff auf die Datenpakete ist hierbei prinzipiell einfacher als bei einer klassischen End-to-End-Wählverbindung – allerdings müssen die so empfangenen Datenpakete aber vom Abfangenden entsprechend sortiert, decodiert und ausgewertet werden; im Gegensatz zu einer E-Mail ein größerer Aufwand.

Das größte Risiko liegt wie immer vor allem im Menschen begründet: eine falsch eingegebene Nummer – und das Fax erreicht den falschen Empfänger. Und physische Faxgeräte können zudem ein Sicherheitsrisiko darstellen, wenn sie auch für Unbefugte zugänglich sind. Eingehende Faxe könnten somit in die falschen Hände geraten

5. Welche Sicherheitslösungen gibt es

a. Internet-Fax allgemein

Im Gegensatz zu einem festinstallierten Fax-Gerät bietet eine Internet-Fax-Lösung den Vorteil, dass eingehende wie ausgehende Faxe nicht in Papierform vorliegen. Sie können nicht versehentlich liegengelassen werden, nicht versehentlich in falsche Hände geraten. Der gesamte Versandvorgang wird genau protokolliert und Faxe wie Protokolle können digital zum Nachweis beliebig aufbewahrt werden.

Bei der Nutzung über eine Mail-to-Fax-Lösung erfolgt die Übermittlung des Dokumentes zunächst per E-Mail an den Provider. Ist diese Mail unverschlüsselt, stellt dies prinzipiell das gleiche Sicherheitsrisiko wie eine unverschlüsselte Mail dar. Sollen sensible Daten übermittelt werden, dann sollten weitere Sicherheitsmaßnahmen ergriffen werden.

b. Internet-Fax verschlüsselt

Als zusätzliche Sicherheitsmaßnahme kann bei der Nutzung einer Mail-to-Fax-Lösung die Übergabe an den Provider über eine verschlüsselte E-Mail erfolgen. Dabei wird einmalig eine Public Key Signatur zum Provider eingerichtet. Alle Faxe, die dann an den Provider per E-Mail übermittelt bzw. von diesem als E-Mail empfangen werden, werden dann verschlüsselt übermittelt. Gleiches gilt für Faxversand- und Faxempfangsbestätigungen, die man per E-Mail erhalten möchte. Die Verbindung zum Provider ist damit jederzeit geschützt.

c. Internet-Fax über geschützten Kundenbereich

Bei der Nutzung des Internet-Fax-Versandes und -Empfangs über den geschützten Kundenbereich erfolgt die Übermittlung des zu versendenden bzw. das Herunterladen des empfangenen Faxes beim Provider über einen geschützten Kundenbereich. Dies erhöht die Sicherheit im Vergleich zu unverschlüsselter Mail-to-Fax/Fax-to-Mail-Lösung erheblich.

d. PCI-DSS-konforme Lösungen

Für die Übermittlung von Kreditkartendaten haben die Kreditkartenunternehmen einen höheren Sicherheitsstandard eingeführt: der PCI DSS (Payment Card Industry Data Security Standard) ist der Sicherheitsstandard für den Umgang mit Kreditkartendaten. Er soll sicherstellen, dass der Umgang mit Kreditkartendaten sorgfältig und gegen Zugriff von außen geschützt erfolgt. Sobald Kreditkartendaten gespeichert und/oder verarbeitet werden, ist die Einhaltung dieses Standards Pflicht.

InterFAX bietet eine PCI-DSS-konforme Fax-Lösung an. Unternehmen, die diese Lösung einsetzen, sorgen für maximale Sicherheit ihrer Daten und können diesen Schutz auch den Kreditkartenunternehmen gegenüber im Zweifelsfall nachweisen.

Die Abwicklung erfolgt komplett innerhalb der InterFAX-Systeme: die Übermittlung der Daten erfolgt über einen geschützten Kundenbereich. Nutzt auch der Empfänger die PCI-DSS-konforme Lösung, so erhält er das Fax auch nur im geschützten Kundenbereich, kann es dort nicht ausdrucken oder abspeichern. Jeder Zugriff auf die Dokumente wird komplett dokumentiert und kann entsprechend eingeschränkt werden. Zusatzfeatures wie diese, dass das Fax nach dem Versand automatisch gelöscht werden kann, können zusätzlich sicherstellen, dass die versandten Dokumente nicht länger als nötig auf den Systemen gespeichert werden.

Die Nutzung des Weges als Ganzes – also von Sender- bis zu Empfängerseite ist somit maximal gegen den Zugriff von außen geschützt. Um Kreditkartendaten PCI-DSS-konform zu empfangen, reicht die Buchung einer entsprechenden Empfangsnummer bei InterFAX – wie der Versender die Kreditkartendaten auf den Weg bringt, ist dabei prinzipiell ihm überlassen, wenn es nur darum geht, als Empfänger einen Missbrauch auszuschließen.

e. Fax im Gesundheitssystem - HIPAA-konforme Lösungen

Daten im Gesundheitssektor sind um ein Vielfaches sensibler als in vielen anderen Bereichen. In den USA unterliegen daher alle Unternehmen, die mit persönlichen oder vertraulichen Daten im Gesundheitssektor zu tun haben, dem Regelwerk **HIPAA**, das den Datenschutz und die Sicherheit dieser Daten sicherstellt. Diesen Anforderungen gerecht zu werden, ist gerade bei der Datenübermittlung nicht einfach.

Europäische Unternehmen, die keinen Kontakt mit Patientendaten aus den USA haben, unterliegen diesem Regelwerk zwar rechtlich gesehen nicht - können es aber freiwillig anwenden und somit ihre Daten maximal schützen. Die Übermittlung per Fax macht die Kommunikation mit allen Beteiligten sehr einfach - und stellt gleichzeitig sicher, dass ihre Daten stets optimal geschützt sind.

Die GTC Internet-Fax Lösung erfüllt die HIPAA-Anforderungen mit diesen Sicherheitsfeatures:

- **Verschlüsselung** - Sämtliche Fax-Nachrichten können verschlüsselt übertragen werden (via SSL oder signierter E-Mail (PKI - Public-Key-Infrastruktur), so dass Patienten-Informationen immer maximal geschützt sind.
- **Protokollnachweis** - Versand und Empfang sämtlicher Telefaxe über das System wird genauestens protokolliert. Das Protokoll steht online zur Verfügung oder kann per E-Mail an den Absender einzelner Faxe gesandt werden.
- **Physikalische Sicherheit** - Sämtliche Daten liegen auf redundanten Servern, die in streng abgesicherten Serverräumen untergebracht sind. Diese können nur von autorisiertem Fachpersonal mit entsprechender Zutrittsberechtigung betreten werden.
- **Benutzer-Authentifizierung** - Der Zugriff auf die Daten erfolgt geschützt mit Benutzernamen und Passwort; Zugriffsrechte können individuell konfiguriert werden.
- **Automatische Löschung** - Je nach der individuellen Einstellung können Nachrichten mit vertraulichen Informationen nach erfolgreicher Übertragung automatisch gelöscht werden. So kann niemand mehr diese vertraulichen Informationen einsehen.

6. Worauf muss man achten bei der Auswahl der Lösung?

Um eine maximale Sicherheit der Daten bei der Übermittlung sicherzustellen, müssen diese sowohl auf der Sender- und auf der Empfängerseite sowie dem Versandweg gesichert sein. Um hier sämtliche Eventualitäten (wie z.B. das Abhören von Telefax-Verbindungen) auszuschließen, ist ein hoher technischer Aufwand auf Sender- wie Empfängerseite nötig. Je nach Anzahl der Übermittlungen, technischem und zeitlichem Aufwand, ist hier eine Abwägung der Möglichkeiten sicher sinnvoll.

Diese Punkte spielen eine Rolle:

- **Einfach zu integrieren**
  Wichtig ist, die technischen Schnittstellen auf Sender- wie Empfängerseite genau abzuklären. Wie liegen die Daten vor? Wie müssen/können diese konvertiert werden? Wie können sie an den Provider übergeben werden? Wie kann der Empfänger sie erhalten und speichern? Der zeitliche wie finanzielle Aufwand für die Integration sollte mit in die Entscheidungsfindung einfließen.

- **Einfach zu nutzen durch betroffene Mitarbeiter**
  Der Knackpunkt vieler Sicherheitslösungen ist am Ende des Tages der Mensch: nur, wenn die Mitarbeiter die eingesetzte Sicherheitslösung auch nutzen, ist sichergestellt, dass die Daten auch sicher bleiben. Daher ist es wichtig, die Abläufe im Unternehmen genau zu eruieren: wie werden Daten erzeugt? Wieviel Aufwand muss der Mitarbeiter betreiben, um diese zu übermitteln? Wieviel Aufwand ist es für den Mitarbeiter auf der Empfängerebene, diese zu empfangen, sicherheitskonform abzuspeichern? Wie wird ggf. ausgeschlossen, dass Daten auf parallelem (unsicheren Weg) doch noch zusätzlich ausgedruckt, gespeichert, versandt werden?
  Wichtig ist es, diese Wege genau zu betrachten und die Mitarbeiter dabei ins Boot zu nehmen. Dazu gehört die Sensibilisierung der Mitarbeiter für die Themen, das Berücksichtigen aller Anforderungen (z.B. an Einfachheit) und ggf. eine Schulung.

- **Dokumentationen und Zertifikate**
  Die Sicherheit der Daten spielt auch aus marketingtechnischen Gründen eine Rolle: viele Kunden erwarten entsprechende Nachweise über die Sicherheitsstandards im Unternehmen. Dabei sind entsprechende Sicherheitskonzepte und -Dokumentationen unterstützend. Zusätzlich kann es hilfreich sein, Dienstleister mit entsprechenden Zertifikaten zu beauftragen. Bei der Nutzung der GTC InterFAX-Produkte greifen Sie z.B. automatisch auf Produkte zurück gemäß ISO 27001 Standards, PCI-DSS-Konformität oder dem HIPAA-Standard. Bei der Datenübermittlung werden durch die Nutzung dieser Dienste automatisch die entsprechenden Standards erfüllt – ohne eigene Zertifizierungen.

- **Auftragsdatenverarbeitungsvertrag** bei Arbeit mit einem Dienstleister:
  Bei jeder Übermittlung personenbezogene Daten benötigen Unternehmen mit dem eingesetzten Versanddienstleister einen Auftragsdatenverarbeitungsvertrag. In diesem garantiert der Versender ein hohes Maß an Sicherheit für die durch ihn verarbeiteten Daten. GTC InterFAX hält diesen bspw. für seine Kunden bereit.

Dabei sind unter anderem die Implementierungskosten von Maßnahmen, Art und Umfang der Datenverarbeitung und die Eintrittswahrscheinlichkeit von Risiken zueinander ins Verhältnis zu setzen.

Anhang

Sollten Sie Fragen haben oder Unterstützung benötigen, so wenden Sie sich gerne an unsere freundlichen Kundenberater.

Hotline – Telefon: +49 (0) 7 11-4 90 90-82
Während unserer Geschäftszeiten

GTC Gutacker TeleCommunication GmbH
Zimmermannstr. 15
D-70182 Stuttgart
Telefon: +49 (0) 7 11-4 90 90-0
Telefax: +49 (0) 7 11-4 90 90-15
E- Mail: interfax@gtc.net
Internet: www.gtc.de