Spontanverschlüsselung für den geschützten Austausch vertraulicher Daten

Röntgenbilder, Rechnungen & Co. sicher per E-Mail verschicken

Vor Kurzem hat die Datenschutzgrundverordnung (DSGVO) ihr zweijähriges Bestehen gefeiert. Bedenkt man, wie viel Aufwand betrieben wurde, um die Implementierung zu bewerkstelligen, ist der Umsetzungsgrad im Bereich E-Mail-Verschlüsselung noch immer ausbaufähig. Aufgrund des vermeintlichen Aufwands verzichten viele Firmen, Arztpraxen, Organisationen etc. darauf, überhaupt auf elektronischem Wege mit Kunden oder Patienten zu kommunizieren. Dabei existieren bereits Lösungen, die einfach in den Arbeitsalltag zu integrieren sind.

E-Mail-Verschlüsselung hat nach wie vor ein schlechtes Image. Die Technologie wird von vielzähligen Unternehmen als kompliziert und instabil erachtet. Dabei kann es mit einer passenden Secure-E-Mail-Lösung so einfach sein, sicher mit jedermann zu kommunizieren. Sobald eine E-Mail als »vertraulich« markiert wurde, kümmert sich eine entsprechende Appliance um den Rest. Dafür sind lediglich die Mailadresse und Handynummer des Empfängers notwendig. Was spricht also dagegen, medizinische Befunde, Rechnungen, Verträge und Ähnliches digital zu versenden, anstatt stapelweise Papier zu produzieren und als Brief oder Paket zu verschicken?

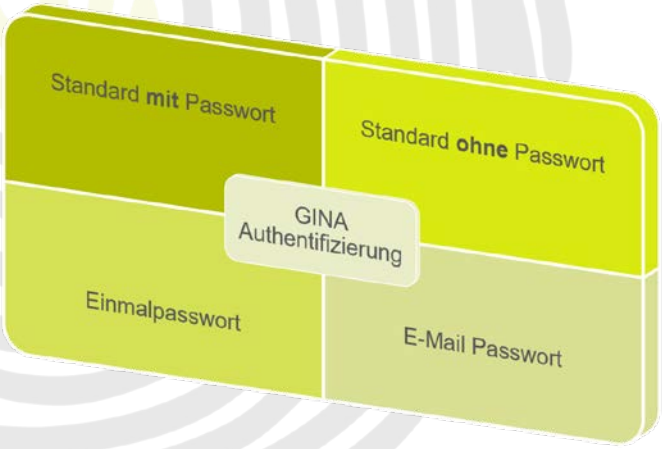
Moderne Lösung zur elektronischen Spontankommunikation. Oftmals ist es äußerst wichtig, dass Dokumente wie beispielsweise Untersuchungsergebnisse, die entscheidend für den weiteren Behandlungsverlauf, das Stoppen von Infektionsketten oder Ähnlichem sind, möglichst schnell ihren Empfänger erreichen. In bestimmten Krankheitsfällen zählt jede Minute. Kommt eine geeignete Verschlüsselungslösung zum Einsatz, ist es kein Problem, solch zeitkritische Unterlagen sofort zu übermitteln.

Unverschlüsselte E-Mails gleichen einer Postkarte. Sie können ohne weiteres von Dritten abgefangen werden und eignen sich somit keinesfalls für den Versand sensibler Daten. Auch konventionelle Verfahren wie die PDF-Verschlüsselung sind nur bedingt sicher. Stattdessen bedarf es einer professionellen, DSGVO-konformen Verschlüsselungsmethode, die sich intuitiv bedienen lässt und keinen Mehraufwand verursacht.

Auf der Suche nach einer passenden Lösung sollte unter anderem darauf geachtet werden, dass die eingesetzte Hard- und Software auf der Empfängerseite keine Rolle spielt und eine komplette Auslieferung der E-Mail inklusive aller Dateianhänge jeglicher Größe erfolgt. Selbst bei übergroßen Dateien wie Röntgenbilder, Videodokumentationen oder RAW-Bildmaterial sollte das Empfängersystem der eingehenden E-Mail nicht die rote Karte zeigen. Des Weiteren muss die Möglichkeit bestehen, dass der Empfänger verschlüsselt auf eingegangene E-Mails antworten kann, um Rückfragen zu stellen – auch dann, wenn er selbst über kein eigenes Schlüsselmaterial verfügt. Fortschrittliche Lösungen nutzen dafür ein intelligentes Gateway, das die erforderlichen Prozesse für die Spontankommunikation unterstützt.

Umsetzung in der Praxis. Mittels eines Secure-E-Mail-Gateways sind in der Praxis einige Szenarien durchführbar, die sich auf die Anforderungen des Anwenders abstimmen lassen. Insge-

Passwortvergabe



Durch das patentierte GINA-Verfahren ist es den Nutzern des Secure E-Mail Gateways möglich, E-Mails verschlüsselt an Empfänger zu übermitteln, die keine Verschlüsselungssoftware einsetzen und keinen Schlüssel besitzen. Das GINA Verfahren verschlüsselt unter Anwendung der sicheren Public-Key-Standards und benötigt keine Software-Installation weder beim Sender noch beim Empfänger. Die E-Mails können im gewohnten E-Mail-Programm empfangen werden und werden durch Eingabe eines Passworts entschlüsselt.

Spontanverschlüsselung

Das patentierte GINA-Verfahren von SEPPmail

Um die E-Mail per GINA-Technologie zu verschlüsseln genügt es, die E-Mail im Mail-Programm als vertraulich zu deklarieren oder ein bestimmtes Schlüsselwort in den Betreff zu schreiben. Dabei spielt es keine Rolle, ob schon je eine Kommunikation mit dem Empfänger stattgefunden hat oder nicht. Das Secure E-Mail Gateway prüft, ob für den betroffenen Benutzer schon ein Schlüssel vorhanden ist. Falls nein, wird ein neuer Schlüssel generiert. Der Sender braucht nichts weiter zu unternehmen.

Die E-Mail wird mit dem Schlüssel verschlüsselt und dem Empfänger übermittelt. Bei der ersten Übertragung wird auf einem anderen Kanal (SMS, Telefon, Fax etc.) ein Passwort übermittelt. Nur mithilfe dieses Passwortes wird der Schlüssel freigeschaltet, um die E-Mail zu entschlüsseln.

Der Empfänger öffnet den Anhang der verschlüsselten E-Mail, gibt sein Passwort ein und die E-Mail wird automatisch im Hintergrund entschlüsselt. Der Empfänger braucht nichts weiter zu unternehmen. Selbstverständlich hat er die Möglichkeit verschlüsselt zu antworten.

samt ist es wichtig, dass die Prozesse einfach und größtenteils automatisiert ablaufen, damit sie fließend in den gewohnten Arbeitsablauf integriert werden können. Dies erhöht die Nutzerakzeptanz und führt dazu, dass Verschlüsselung als Standard akzeptiert und eingesetzt wird. Zudem läuft man damit keine Gefahr, gegen die Richtlinien der DSGVO zu verstoßen.

Typische denkbare Szenarien sind zum Beispiel:

- Initialpasswort per SMS oder Telefonat zum Sender
- Einladungsmail zur Registrierung (ohne Initialpasswort)
- externe Anmeldung per Webseiten-Link
- Einmalpasswort per SMS (nach jeder Öffnung einer gesicherten E-Mail)
- E-Mail-Passwort ohne Registrierung (jede E-Mail hat ein eigenes Passwort)

Mit einer professionellen Appliance ist es möglich, eine E-Mail zu verschlüsseln und als HTML-Anhang mit einer Träger-Mail zu versenden. Um den verschlüsselten Anhang zu öffnen, eignet sich jedes internetfähige Gerät mit Browser, über den ein Passwort eingegeben und die Nachricht entschlüsselt wird. Wie oben beschrieben, sollten hierfür mehrere Passwortoptionen zur Verfügung stehen.

Die Appliance kann beispielsweise ein Initialpasswort für den Absender erstellen, das dieser dem Empfänger über einen zweiten Übertragungsweg, etwa per Telefon, mitteilt. Alternativ sollte unter anderem die Funktion des Einmalpasswortes zur Verfügung stehen, für das der Absender lediglich zwei Informationen vom Empfänger benötigt: E-Mail-Adresse und Handynummer. Daraufhin lässt sich jede beliebige E-Mail seitens des Absenders verschlüsseln, und der Empfänger erhält per SMS ein einmaliges Kennwort zur Entschlüsselung. Ohne vorherigen Registrierungsprozess kann der Empfänger die E-Mail so problemlos abrufen, indem er das SMS-Passwort nutzt. Bei erneutem Öffnen dieser oder einer weiteren E-Mail erfolgt die Vergabe und der Versand eines neuen Einmalkennwortes per SMS. Dies erlaubt einen unkomplizierten Prozess, der sich in jede E-Mail-Infrastruktur integrieren lässt und sensible Informationen vor dem Zugriff Fremder schützt. Für den seltenen oder einmaligen Versand von vertraulichen Nachrichten eignet sich ein E-Mail-Passwort, das einer spezifischen Mail zugeordnet ist und ohne Registrierung funktioniert. Empfänger, die häufiger verschlüsselte E-Mails bekommen, sollten sich beim Versender registrieren und im Anschluss mittels Abstufungen (mit oder ohne Login) sichere E-Mails empfangen können.

Fazit. Inzwischen ist es nicht mehr vonnöten, vertrauliche Dokumente auf postalischem Wege zu verschicken. Die verschiedenen Optionen einer Spontanverschlüsselung bieten einiges an Flexibilität und gleichzeitig an Sicherheit, sodass sich Dateien geschützt elektronisch übertragen lassen. Davon profitieren nicht nur Unternehmen, Praxen, Organisationen & Co., sondern vor allem auch Kunden, Mandanten, Nachbarabteilungen, Patienten etc., da sie deutlich schneller Dokumente erhalten – und das sowohl DSGVO-konform als auch ohne großen Aufwand.

Günter Esch,
Geschäftsführer der SEPPmail
Deutschland GmbH