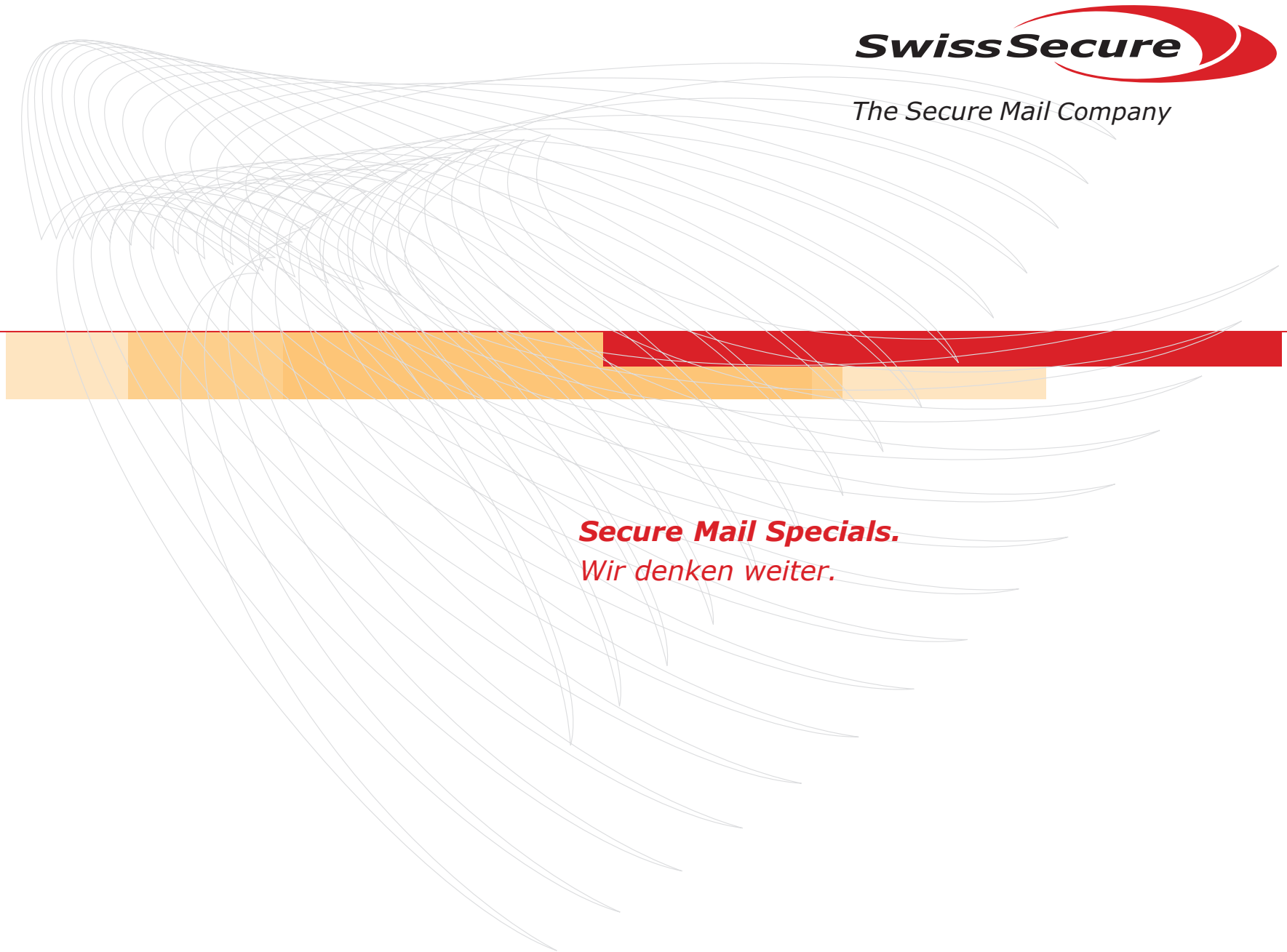
SwissSecure
The Secure Mail Company
Secure Mail Specials.
Wir denken weiter.

Secure Mail Specials

Für jedes Unternehmen die perfekt passende Lösung.

Lösungen

Secure Mail ist als 1:1-Funktion aufgebaut: Jeder Benutzer sendet Mails an einen oder mehrere definierte Empfänger, und jeder User kann nur die für ihn bestimmte Post lesen.

Sollen die heute üblichen Mail-Funktionen auf Secure-Mail-Lösungen abgebildet werden, müssen ein paar weitere Fragen beantwortet werden.

- Was geschieht mit Shared Mailboxen?
- Wie funktionieren das Weiterleiten und die Delegation?
- Funktionieren vorhandene Distributionslisten noch?
- Wie funktionieren Backup und Restore?
- Wie archiviert man Mails?

Und ein besonderer Fall:

- Kann Secure Mail auch von weiteren Anwendungen genutzt werden?

Back-Up

Secure Mail Back-Up und Restore.

Werden Mails verschlüsselt gesendet, werden sie meist auch verschlüsselt im Sent-Ordner des Mail-Clients abgelegt und sind damit auf dem normalen Tages-Backup geschützt. Die Probleme beginnen später.

Restore von verschlüsselten Mails ist notwendig

- Nicht nur jede Mail, auch das Schlüsselmaterial muss sicher gebackuped werden. So zuverlässig, dass keine Daten in falsche Hände geraten.
- Wie die Schlüssel während des normalen Betriebs gelagert werden, hängt von der Lösung ab. Ein Restore kann damit auch von Client-Versions abhängig sein.
- Die Prozesse für den Schlüssel-Restore müssen recht ausgeklügelt sein. Damit nicht jeder den Schlüssel eines anderen restoren kann.
- Das Schlüsselmaterial kann in der Phase zwischen Backup und Restore ungültig geworden sein. Darauf reagiert jeder Mail-Client anders.

Mails sind auch nach Austritt des Mitarbeiters wichtig

- Das Schlüsselmaterial ist für jeden User individuell definiert, jemand anders kann nichts damit anfangen.
- Tritt ein Mitarbeiter aus, ist er länger abwesend, oder gibt es einen Notfall, muss man unter Umständen auf verschlüsselte Mail-Daten zugreifen. Das kann je nach Lösung sehr schwierig sein.
- Alle dafür nötigen Prozesse und technischen Vorkehrungen müssen zwingend vorher festgelegt und realisiert werden. Ein nachträgliches Entschlüsseln ohne Vorbereitung ist prinzipiell unmöglich. Nur so kann man sich vor dem Ausspionieren schützen.

Secure Mail Archivierung

Archivierung

Mails werden archiviert – wie andere geschäftsrelevante Dokumente auch.

Gewisse Mails gelten heute als geschäftsrelevante Dokumente. Sie haben zwar nicht zwingend Rechtsverbindlichkeit wie ein Vertrag, aber es gelten für sie die gesetzlichen Aufbewahrungspflichten.

Die meisten Firmen archivieren ihre Mail-Daten noch nicht. Oft wird rigoros gelöscht, um Speicherplatz zu sparen. Darum kann heute auch kaum jemand mehr zuverlässig auf ältere Mails zugreifen. Doch was, wenn beispielsweise genau diese eine Mail über mehrere Tausend Franken Schadenersatz entscheiden und zur Beweisführung dienen könnte?

Wie auch immer: Organisiertes Archivieren von elektronischer Post wird schon bald zur Regel. Verschlüsselte Mails vereinfachen die Problematik nicht. Im Gegenteil, denn die Fragen über Zugriffsberechtigung bekommen mit der Verschlüsselung eine neue Dimension.

- Da das Schlüsselmaterial persönlich einem Mitarbeiter zugeordnet ist, kann ein anderer Mitarbeiter, z.B. der Archivar, nichts damit anfangen.
- Damit ein Archivsystem optimal funktioniert, muss man auf den Klartext von Mails zugreifen können. Und für optimale Sicherheit muss die Nachricht verschlüsselt bleiben.
- Suchfunktionen funktionieren bei verschlüsselten Mails ungenügend oder gar nicht.
- Viele Secure-Mail-Systeme können nicht an Archivsysteme angeschlossen werden. Gängige Mail-Systeme anzuschliessen, ist ungenügend: Die Schlüssel sind nicht archiviert, und ohne Schlüssel kann man später nichts mit der Mail anfangen.

Secure Mail Distributionslisten

Verteiler

Secure Mail muss auch mit Verteilerlisten möglich sein

Heute kann man Mails an mehrere Personen gleichzeitig senden – über Verteiler- oder Distributionslisten: Eine Mail wird nur an eine «Person» geschickt, eben diese Liste, und erst später in Mails an die einzelnen Empfänger zerlegt.

Eine gute Idee, die Zeit spart. Nur: Sie lässt gewisse Secure-Mail-Funktionen nicht zu. Hier hilft nur eine enge Zusammenarbeit mit dem Mail-Betreiber weiter.

- Persönliche Verteilerlisten werden von den meisten Secure-Mail-Programmen unterstützt.
- Oft stellen Mail-Server Informationen über Mitglieder von Verteilerlisten nicht zur Verfügung. Eine Client-Verschlüsselung ist so nur mit Umwegen möglich.
- Verteilerlisten kann man auch extern verwalten. Sie lassen sich aber nur in Zusammenarbeit mit dem Verwalter und/oder den Teilnehmern in ein Secure-Mail-System integrieren.
- Öffentliche Mailing-Listen brauchen keine Verschlüsselung, eine digitale Unterschrift kann aber sinnvoll sein.

Secure Mail mit Shared Mailboxen

Secure Mail soll Shared Mailboxen unterstützen können.

Für den Support ist es häufig sinnvoll, Mail-Konten einzurichten, auf die verschiedene User Zugriff haben. Dabei sind alle Personen gemeinsam für die per Mail eintreffenden Anfragen zuständig.

Derartige Mails können durchaus vertraulich sein, da der Support auch bei Applikationen hilft, die schützenswerte Daten verwalten.

Gängige Secure-Mail-Systeme können mit solchen Mails nicht umgehen. Die Forderung, Shared Mailboxen ebenfalls mit Secure-Mail-Systemen zu unterstützen, dürfte für die meisten Firmen ein Sonderfall sein. Eine individuelle Abklärung ist nötig.

- Um Mails zu verschlüsseln, braucht es einen öffentlichen Schlüssel des Empfängers. Im vorliegenden Fall wäre dies jener der Shared Mailbox, auf den User der Mailbox in der Regel jedoch keinen Zugriff haben.
- Mails lassen sich auch für mehrere Empfänger verschlüsseln. Wer Post erhält, muss aber nicht grundsätzlich mit dem tatsächlichen Empfänger des Mails identisch sein (Mail-Adresse des Empfängers). Es können Mails so verschlüsselt werden, dass sie alle User der Shared Mailbox lesen können, solange diese der Gruppe der Shared Mailbox angehören. Übliche Secure-Mail-Systeme kennen diese Funktion nicht.
- Auch Rückantworten der Shared Mailbox sollten sinnvollerweise verschlüsselbar sein. Und die Absenderinformationen so beschaffen, dass auch Anfrager korrekt antworten können.
- Abzuklären ist, wie weit man die Liste der Personen mit Zugriff auf eine Shared Mailbox verändern kann, und ob neue User auch frühere Mails lesen können sollen.

Secure Mail Weiterleitung und Delegation

Delegation

Zunehmend genutzt, darum besser gesichert.

Weiterleiten und Delegieren von Mails wird vor allem in grossen Unternehmen sehr häufig genutzt. Nicht nur persönliche Assistenten, auch Kollegen bei Ferienabwesenheit sollen Mails bearbeiten können.

Das Problem mit Secure Mail: Auf verschlüsselte Mails hat der Stellvertreter keinen Zugriff. Darum machen auch automatische Weiterleitungsfunktionen, ohne dass ein Stellvertreter die Bearbeitung übernehmen kann, keinen Sinn mehr.

In der Regel kann auch ein persönlicher Assistent verschlüsselte Mails weder lesen, noch im Namen des Vorgesetzten senden. Die Delegationsfunktion in Mail-Programmen würde damit viele Vorteile verlieren.

- Schlüssel sind immer eindeutig einem Mitarbeiter zugeordnet. Vertritt ihn jemand, sind ohne zusätzliche technische Hilfsmittel keine Mails lesbar. Oder aber man lässt sich das Mail erneut zustellen – verschlüsselt für den Stellvertreter. Für einzelne Firmen mag dies vernünftig sein. Aber jeder Manager sollte selber entscheiden können, wer was lesen darf oder nicht. Es gibt leider nur wenige Möglichkeiten, Mails auf verschiedene Vertraulichkeitsstufen zu setzen (privat, nur Geschäftsleitung usw.).
- Im Idealfall wird bereits dem Mail-Client des Senders mitgeteilt, dass der Empfänger Mails weiterleitet. Dies ist in der Regel nur im eigenen Netzwerk möglich, eine interne Lösung reicht aber oft aus.
- Bereits in unverschlüsselten Situationen sind Delegationen schwer zu bewältigen, und es braucht Assistenten mit Fingerspitzengefühl, um abzuschätzen, ob ein Brief oder eine Mail gelesen werden soll oder nicht.
- Mit Verschlüsselungen wird es noch heikler. Die Technik kann nur entschlüsseln, nimmt einem also nie die Entscheidung ab. Dazu braucht es differenzierte Informationen über Vertraulichkeitsstufen im Mail. Entsprechende Lösungen, die in einem solchen Fall entschlüsseln, sind erhältlich.

Secure Mail für Applikationen

Applikationen

Applikationen sollten auch verschlüsselte Mails senden können.

Bilanz- und Erfolgsrechnungen, Vermögensübersichten und Lohnausweise: Sie alle werden mit verschiedenen Programmen erstellt, ausgedruckt und per Post verschickt.

Ein Mail-Versand ist aus Vertraulichkeitsgründen nicht möglich, bleibt aber wünschenswert, selbst wenn sich die Software im Normalfall nicht anpassen lässt.

- Das Konzept der technischen Benutzer (z.B. der Login-Name der Applikation) muss so erweitert werden, dass auch dieser User zum Schlüsselmaterial kommt.
- Ist eine Mail digital signiert, garantiert sie Unveränderlichkeit. Trotzdem muss diskutiert werden, wie nah eine «automatische» digitale Unterschrift an eine handschriftliche herankommt, wie es bereits bei Bankauszügen Usus ist.
- Bestehende Software lässt sich oft nur mit grossen Kosten an Secure Mail anpassen. Das muss ausserhalb der Applikation erfolgen. Nur so wird die gewünschte Sicherheit nicht eingeschränkt.

Möchten Sie weitere Details?
Kontaktieren Sie uns. Wir beraten Sie gerne.

Hier können wir nur aufzeigen, worauf grundsätzlich zu achten ist. Die technischen Details sind wie immer abhängig von der individuellen Situation vor Ort. Gerne diskutieren wir mit Ihnen über passende Lösungsansätze. Ein gemeinsamer Workshop kann aufzeigen, wie Sie Secure Mail auch in Ihrem Unternehmen richtig einsetzen.

SwissSecure AG

Höhtalstrasse 25, 5408 Ennetbaden, Switzerland

Phone *+41 44 77 55 111*
Fax *+41 44 77 55 101*
E-Mail *info@swisssecure.ch*
www.swisssecure.ch