iQ.Suite WebCrypt Pro

- Einsatzszenarien -

E-Mail-Verschlüsselung für Jedermann

Expertise matters

Inhalt

1 Damit vertrauliche Daten vertraulich bleiben: Zentrale E-Mail-Verschlüsselung mit iQ.Suite WebCrypt Pro

In jüngster Zeit schaffen es Datenpannen und -diebstähle großen Ausmaßes erschreckend häufig in die Schlagzeilen - national sowie international. Die Folgen von Datenverlust gleich welcher Natur sind verheerend. Kunden und Geschäftspartner haben in der Regel kein Verständnis. Im schlimmsten Fall fallen vertrauliche Informationen in die falschen Hände.

Im Visier der Datenspione befindet sich auch der allseits beliebte und etablierte Kommunikationskanal „E-Mail“. Das wundert kaum. Denn noch nie hatten es Kriminelle leichter, auf die Kommunikation Dritter zuzugreifen. Die Beschaffenheit des Kommunikationsweges via Internet macht es möglich. Elektronische Nachrichten können abgefangen, während ihres Transportes von Mail-Server zu Mail-Server manipuliert und schließlich auch unbemerkt gelesen werden.

Die Vertraulichkeit, Integrität und Authentizität von per E-Mail übermittelten Informationen spielen angesichts der jüngsten Entwicklungen eine immer größere Rolle in der geschäftlichen E-Mail-Kommunikation. Um diesen Anforderungen – schon in eigenem Interesse – gerecht zu werden, führt kein Weg am Einsatz einer E-Mail-Verschlüsselungslösung vorbei.

1.1 Komplexität als Herausforderung

Allerdings stellt sich das Vorhaben, die eigene E-Mail-Kommunikation per Verschlüsselung abzusichern, für viele Unternehmen als sehr komplex dar. Es beginnt schon bei der Wahl der Verschlüsselungsmethode: PGP, GnuPG oder S/Mime? Das sind berechtigte Fragen: Immerhin erfordert der verschlüsselte elektronische Briefwechsel in der Regel die Teilnahme beider Parteien – sprich: des Absenders und des Empfängers einer E-Mail – am selben Verfahren. Dies lässt sich jedoch nicht immer durchsetzen. Insbesondere in der unmittelbaren Kommunikation mit Endkunden lassen sich die genannten Verfahren nur schwer oder gar nicht etablieren.

1.2 Die neue Generation: Web-basiert und effizient

Neue Lösungen eröffnen alternative Wege, sich dem Thema E-Mail-Verschlüsselung zu nähern. GBS Software bietet mit iQ.Suite WebCrypt Pro eine solche Lösung: web-basiert und zentral implementierbar, ermöglicht sie den Austausch verschlüsselter E-Mails mit Geschäftspartnern und Kunden, die über keine eigene Verschlüsselungslösung verfügen. Damit kann auch in solchen Szenarien der Datenschutz bei der Übertragung sensibler Inhalte zuverlässig sichergestellt werden. Die Lösung arbeitet sowohl mit IBM Domino als auch Microsoft Exchange/SMTP zusammen.

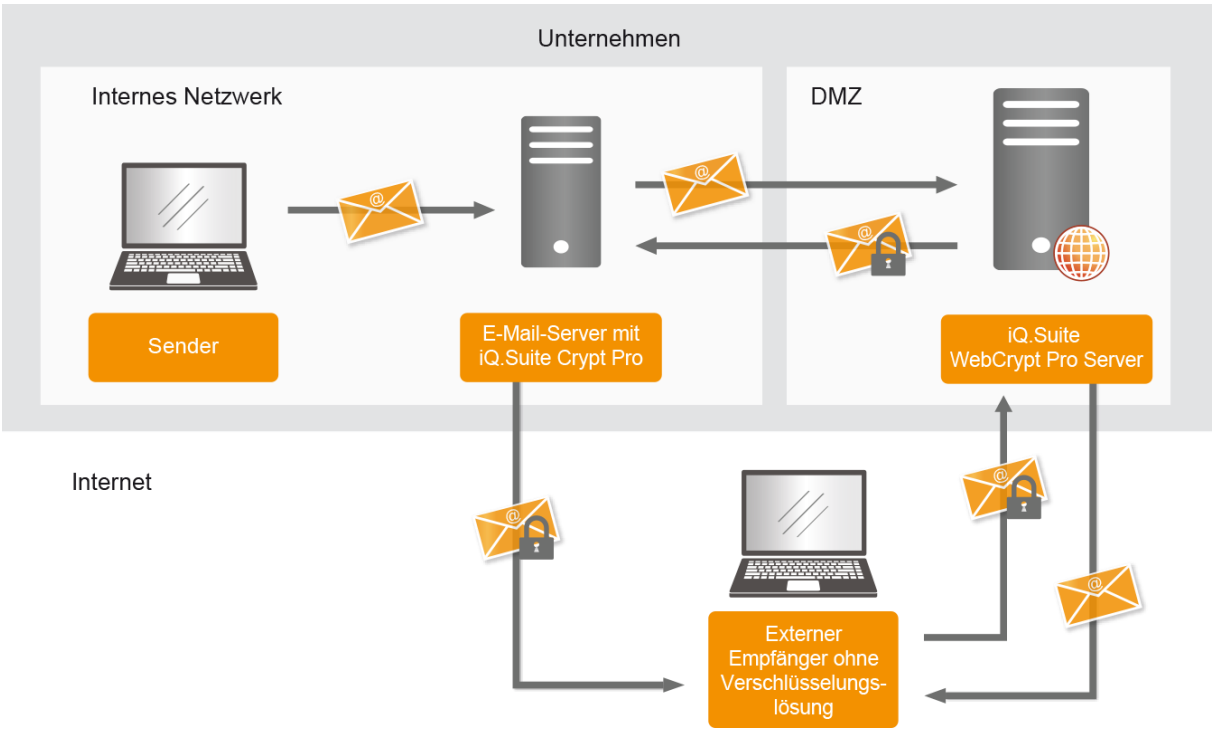

Abbildung 1: iQ.Suite WebCrypt Pro Infrastruktur

Zur Funktionsweise unserer neuartigen Verschlüsselungslösung:

1. Der Absender versendet, wie gewohnt, die zu verschlüsselnde E-Mail an seinen Kommunikationspartner.
2. Die erzeugte WebCrypt Pro Nachricht wird dem Empfänger als verschlüsselter HTML-Anhang in einer herkömmlichen E-Mail zugesendet.
3. Mit Hilfe des im lesbaren Teil der E-Mail befindlichen Web-Links gelangt der Empfänger zum über HTTPS gesicherten WebCrypt Pro Internet-Portal und muss sich dort mit seiner E-Mail Adresse und dem auf separatem Weg übermittelten Passwort anmelden.
4. Der verschlüsselte Anhang wird nach dem automatischen Hochladen mit dem persönlichen Schlüssel des Empfängers entschlüsselt und dargestellt.
5. Der Empfänger hat nun die Möglichkeit im WebCrypt Pro Internet-Portal die Nachricht gesichert (verschlüsselt) zu beantworten, oder diese lokal und unverschlüsselt auf seinem Computer zu speichern.

In der Kommunikation beim Absender zwischengeschaltet ist stets der WebCrypt Pro-Server, der als Ergänzung zum Mail-Server (IBM Domino, Microsoft Exchange/SMTP) die Ver- und Entschlüsselung der gesendeten E-Mails übernimmt. Zur Absicherung der Kommunikation zwischen Empfängern und WebCrypt Pro-System kommt eine abgesicherte HTTPS-Verbindung zum Einsatz. Es empfiehlt sich für diese Verbindung ein Zertifikat von einem offiziellen Trustcenter zu verwenden, damit die Kommunikationspartner keine Sicherheitswarnung des Browsers/E-Mail-Clients erhalten.

iQ.Suite WebCrypt Pro ermöglicht dem Empfänger zusätzlich ein sicheres Antworten auf verschlüsselte E-Mails. Die elektronischen Nachrichten werden dabei auf dem WebCrypt Pro-Server nicht dauerhaft gespeichert, sondern lediglich zur Anzeige gebracht.

Die eigentlichen Inhalte verbleiben stets im Besitz des Kunden beziehungsweise des Kommunikationspartners – sprich: dem Empfänger der verschlüsselten E-Mail. Somit entsteht keine zusätzliche Aufbewahrungspflicht durch den Einsatz der Lösung (Compliance). Das heißt letztlich für den Absender einer solchen verschlüsselten Nachricht: er kann ohne jedwede Hard- oder Softwareinstallation auf Empfängerseite sicher kommunizieren.

2 iQ.Suite WebCrypt Pro im Einsatz

Im Fokus des unter Punkt 2.1 beschriebenen Szenarios steht der sichere und zugleich einfache Austausch vertraulicher Informationen über das Medium E-Mail im Finanzsektor. Eine Software- oder Hardwareinstallation auf Empfängerseite ist dafür nicht notwendig. Die Lösung kann sowohl in der unternehmenseigenen IT implementiert werden als auch im Hosting-Betrieb eines externen Rechenzentrums.

Aufgrund seiner hohen Flexibilität lässt sich iQ.Suite WebCrypt Pro in einer Vielzahl weiterer Einsatzszenarien nutzen:

- Touristik: Versand von Buchungsunterlagen, Rechnungen, Vouchers, eTickets
- Öffentlicher Bereich: elektronischer Versand von Unterlagen, wie Rentenbescheiden
- Onlineshops: Versand von Rechnungen, Lieferscheinen, Lizenzschlüsseln
- Gesundheitswesen: Kommunikation zwischen Krankenhaus und niedergelassenen Ärzten sowie Ärztekammer und Ärzten
- Pharmazeutische Industrie: Austausch mit externen Forschungspartnern und Laboratorien
- Automotive: Kommunikation mit Zulieferern und Ingenieurbüros
- Energieversorger und Telekommunikation: Rechnungsversand
- etc.

2.1 Anwendungsfall 1: Kundenberater schickt erste WebCrypt Pro E-Mail

Die iQ.Suite auf dem Mail-Server der Bank hat einen Job implementiert, welcher E-Mails eines beliebigen Kundenberaters der Bank per WebCrypt Pro verschlüsselt und dem Empfänger als E-Mail mit verschlüsseltem Anhang zustellt. Dieser Anhang heißt immer secure.htm.

Damit E-Mails verschlüsselt werden, muss eine Zeichenfolge wie z.B. „WebCrypt Pro“ im Betreff der E-Mail auftauchen. Alternativ kann die Mailschablone der Kundenberater um eine Option „Per WebCrypt Pro verschlüsseln“ erweitert werden, um den Bedienkomfort am Client zu erhöhen.

Sollte für den Adressaten der E-Mail noch kein Benutzerkonto auf dem WebCrypt Pro-Server vorhanden sein, wird automatisch ein zur Empfänger-Adresse gehörender neuer symmetrischer Schlüssel und ein Passwort erzeugt. Das Passwort und die E-Mail-Adresse werden dem Kundenberater der Bank per E-Mail zugesandt.

Diese E-Mail mit den Login-Daten wird nur bei der Erst-Verwendung von WebCrypt Pro für eine E-Mail-Adresse generiert.

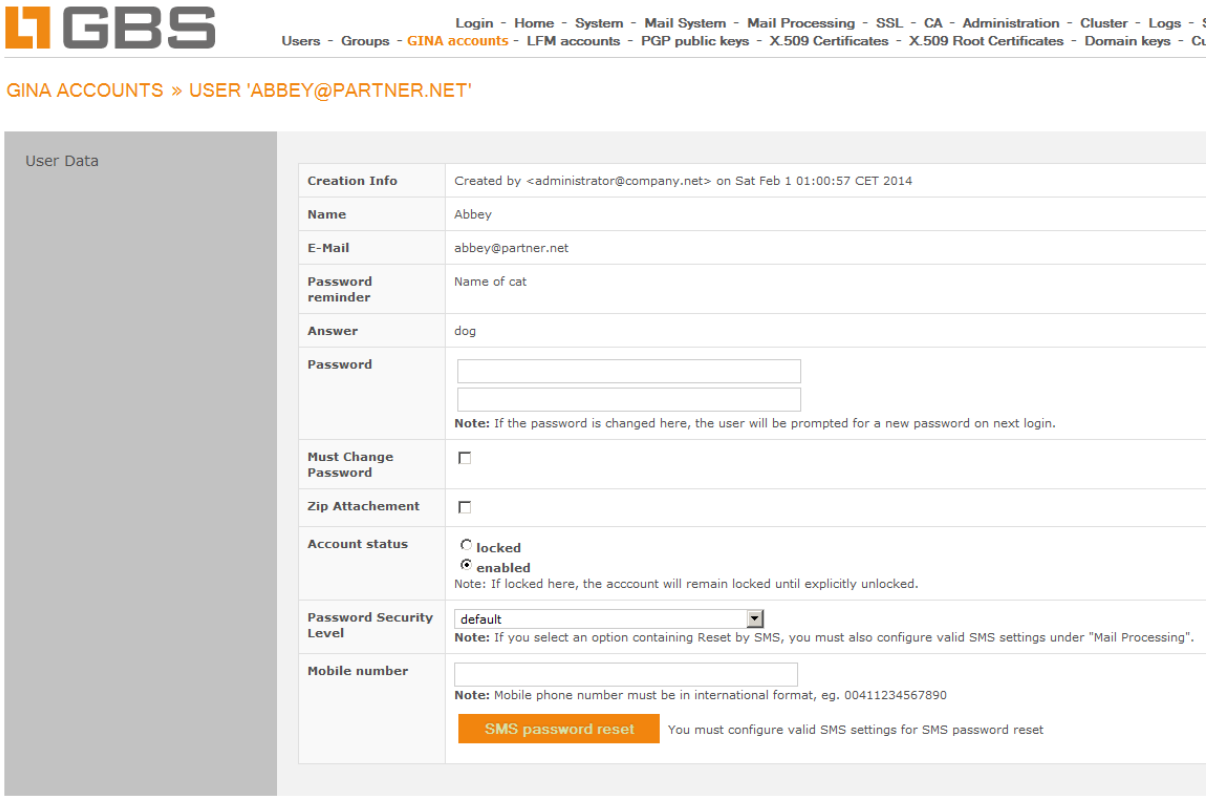

Abbildung 2: iQ.Suite WebCrypt Pro Nutzerverwaltung

Der Kundenberater übergibt dem Kunden die Login-Daten. Alternativ bekommt der Kunde diese Informationen auf postalischem Weg. Der Kunde kann per WebCrypt Pro-Konfiguration dazu angeleitet werden, nach dem erstmaligen Login ein neues Passwort zu wählen.

2.2 Anwendungsfall 2: Kunde antwortet auf WebCrypt Pro-E-Mail

Hat sich der Kunde erfolgreich authentifiziert und seine E-Mail gelesen, besteht die Möglichkeit dem Kundenberater direkt aus der WebCrypt Pro-Oberfläche zu antworten. Diese Mails werden ebenfalls über eine abgesicherte Verbindung (SSL, TLS) übertragen.

2.3 Anwendungsfall 3: Kunde hat sein Passwort vergessen

a. Weiß der Kunde die Antwort auf seine geheime Frage, die individuell vergeben werden kann, so wird ihm im Browser sein neu generiertes Passwort angezeigt.

b. Hat der Kunde die Antwort auf seine geheime Frage vergessen, muss der WebCrypt Pro-Administrator das Passwort per Web-Frontend zurücksetzen. Daraufhin erhält der Kunde die neuen Login-Informationen automatisch per E-Mail.

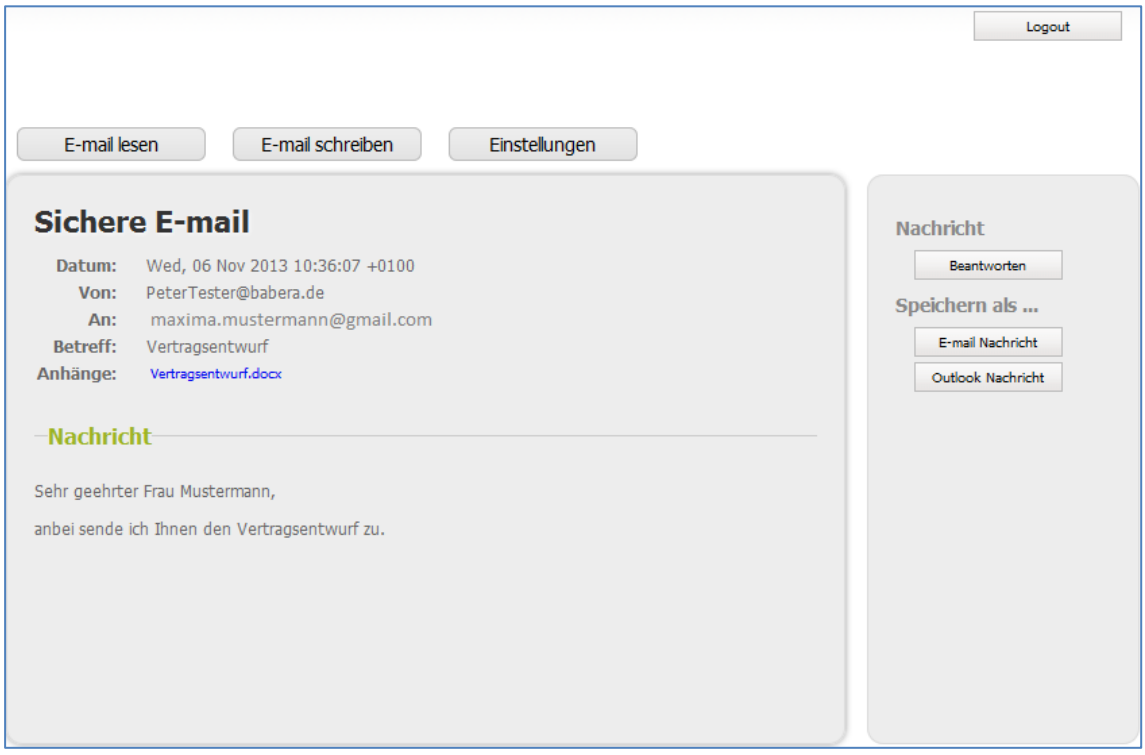

Abbildung 3: Anwender Oberfläche

2.4 Anwendungsfall 4: Der Kunde hat eine neue E-Mail Adresse

Beim nächsten Versand einer per WebCrypt Pro verschlüsselten E-Mail an die neue Adresse wird für den Kunden automatisch ein neuer Zugang angelegt.

Genereller Hinweis: Voraussetzung für den Einsatz eines WebCrypt Pro-Servers ist, dass der einmal gewählte Domänen-/Server-Name nicht mehr geändert wird, da er in den verschlüsselten Attachments hinterlegt ist. Andernfalls können Kunden den Server nicht mit Ihrer verschlüsselten E-Mail erreichen. Daher wird empfohlen, dass die Bank der Eigentümer der WebCrypt Pro-Domänenadresse ist. Sollte sich die Domäne aus organisatorischen Gründen ändern, muß dafür gesorgt werden, dass der alte Domänename auf den neuen Domänenamen referenziert. Alternativ wird der alte Name beibehalten.

3 Fazit

Nur der Einsatz einer effizienten E-Mail-Verschlüsselungslösung bietet die nötige Sicherheit beim elektronischen Briefwechsel. iQ.Suite WebCrypt Pro bietet in Szenarien, in denen Empfänger über keine geeignete Verschlüsselungslösung verfügen, die sichere und zugleich einfache Übermittlung vertraulicher Inhalte. Das flexible Web-Frontend ermöglicht ein schnelles Roll-Out und lässt sich optisch und inhaltlich an die Vorstellungen des Kunden anpassen.

3.1 Die wesentlichen Vorteile im Überblick

- Schutz des geistigen Eigentums bei gleichzeitig hoher Effizienz der Kommunikation
- Sichere und vertrauliche E-Mail-Korrespondenz ohne PGP, S/Mime oder PKI-Strukturen
- Keine zusätzlichen Installationen bei Ihren Kommunikationspartnern
- Zentrales, integriertes Benutzermanagement
- Skalierbare und flexible Architektur mit Web-Oberfläche
- Anpassbar an das Corporate Design des Kunden

3.2 Die Technologie im Überblick

- WebCrypt Pro-Server
  - Linux
  - Apache-Webserver
  - MySQL-Datenbank (alternativ: Oracle, MS SQL, Postgres)
  - Unterstützt Load Balancing
- Verschlüsselungsmethode
  - Blowfish-Algorithmus

3.3 Die Funktionen im Überblick

- Generell
  - Web Portal
  - Sicheres Login
  - Abgesicherte Verbindung
- Administrator
  - Grundeinstellungen (Netzwerk, Load Balancing etc.)
  - User Management (Passwort zurücksetzen, Nutzer deaktivieren/löschen etc.)
  - Interface-Konfiguration (Corporate Identity)
  - E-Mail-Konfiguration (Größenlimits etc.)
  - Monitoring
- Anwender
  - Entschlüsselung
  - Download der Inhalte und lokale Ablage
  - Sicheres Antworten
  - Profilinformationen (letztes Login, Gültigkeit des Accounts etc.)
  - Passwort und Sprache ändern

Über GBS

GROUP Business Software ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die IBM und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Weitere Informationen unter www.gbs.com