iQ.Suite Crypt Pro Grundlagen

- Zentrale E-Mail-Verschlüsselung -

Serverbasierte Verschlüsselung für umfassende E-Mail-Inhaltssicherheit

Expertise matters

Inhalt

1 Zusammenfassung

Über 2,5 Mrd. E-Mail-Benutzer sind heute weltweit registriert. Ein bedeutender Teil des E-Mail-Aufkommens besteht aus Geschäftsdokumenten. Die meisten Unternehmen haben sich ans Internet angeschlossen und nützen seine globalen Fähigkeiten, Informationen auszutauschen, um so im Konkurrenzkampf vorne zu bleiben.

Je mehr Mitglieder es jedoch in einer strukturierten Einheit gibt, desto mehr muss auf den Schutz der Rechte des Einzelnen geachtet werden. Dieser Schutz bezieht sich ganz besonders auf die Daten, die der Betreffende im Netz verbreitet und/oder verarbeitet. Gerade im kommerziellen Sektor würde keine multinationale Firma daran denken, sensible Daten wie interne Bilanzen, Betriebs- und Erfolgsberichte innerhalb ihrer Firmenstruktur über das Internet zu transportieren, wenn nicht sichergestellt ist, dass diese Daten auch geschützt und sicher ankommen.

Geschützt und sicher heißt in diesem Zusammenhang, dass nur von autorisierten Personen auf die Daten zugegriffen und nur von ihnen gelesen werden können. Bekanntlich gibt es viele Wege, im Netz Daten zu transportieren. Man kann sie lokal in einer Datenbank ablegen und den Zugriff durch das Netzwerk ermöglichen. Manchmal ist es jedoch nötig, dass Datensätze und Informationen selbst gesendet werden müssen. Dies kann unter anderem auch mittels elektronischer Post geschehen.

Auf dem Weg vom Sender zum Empfänger durchläuft eine E-Mail sowohl im Internet als auch im Intranet unterschiedlichste Computersysteme. Der jeweilige Weg einer E-Mail ist nicht vorhersagbar und richtet sich nach Indikatoren wie Netzwerkverkehr und Bandbreite. Gleich einer Postkarte ist der Inhalt einer E-Mail während des Transports durch das Internet nicht geschützt und grundsätzlich von Jedermann les- und veränderbar.

Unsichere E-Mail Kommunikation:

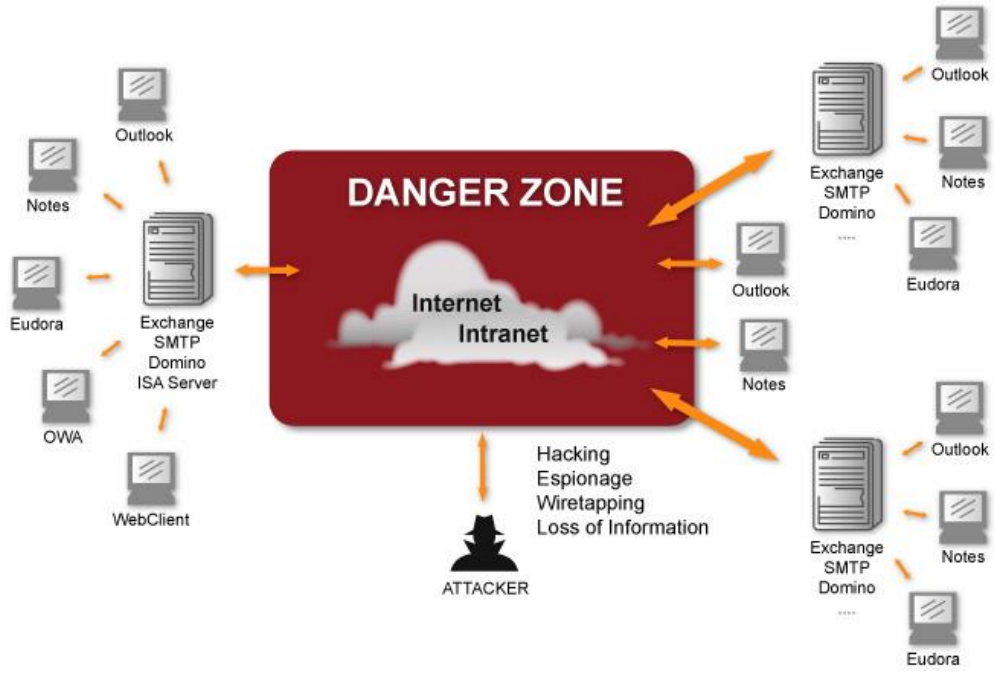

Abbildung 1: Der unsichere Weg einer E-Mail zum Empfänger

Durch den Einsatz von E-Mail-Verschlüsselung wird aus der eben beschriebenen Postkarte ein chiffrierter Brief mit Echtheitssiegel. Das vorliegende White Paper beschäftigt sich mit der Alternative zu einer Public-Key-Infrastruktur (PKI).

Näheres zur Kryptographie finden Sie im White Paper „Kryptographie“. Mit den Grundlagen der PKI beschäftigt sich das White Paper „PKI-Grundlagen“. Beide White Paper können Sie auf unserer White Paper-Website runterladen.

2 Clientbasierte Verschlüsselung

Bei einer clientbasierten Verschlüsselung (auch: Ende-zu-Ende-Verschlüsselung) ist die E-Mail vom Absender-PC bis zum Empfänger-PC verschlüsselt. Das bedeutet, dass der Inhalt der E-Mail auf ihrem kompletten Weg für Dritte nicht lesbar ist.

Eine solche Ende-zu-Ende-Verschlüsselung des E-Mail-Verkehrs mag auf den ersten Blick als eine gute Lösung erscheinen. In der Praxis hat sich jedoch gezeigt, dass clientbasierte Verschlüsselung in vielen Fällen zu unerwünschten Effekten führt. Warum?

Hier spielen mehrere Faktoren eine Rolle, auf die im Folgenden eingegangen wird.

2.1 Benutzergebundene Schlüssel(paare)

Jeder E-Mail-Benutzer erhält bei clientbasierter Verschlüsselung ein individuelles Schlüsselpaar für seine E-Mail-Kommunikation. Dieses Schlüsselpaar bezieht sich auf den gesamten verschlüsselten E-Mail-Verkehr dieses Benutzers.

Verlässt nun dieser Benutzer beispielsweise das Unternehmen, so ist die E-Mail-Kommunikation dieses Benutzers nicht mehr zugänglich. Sollte nun ein Zugriff auf die vergangene E-Mail-Kommunikation notwendig werden, so stellt die fehlende Zugriffsmöglichkeit eine nicht unerhebliche Gefahr für das Unternehmen dar, es sei denn, das Schlüsselpaar wurde zusammen mit dem Passwort zentral abgelegt, so dass in diesen Fällen darauf zugegriffen werden kann.

2.2 Komplexität

Die Einführung einer unternehmensweiten clientbasierten Verschlüsselung ist mit erheblichem Aufwand verbunden. Zunächst benötigt jeder E-Mail-Benutzer einen eindeutigen Schlüssel bzw. Schlüsselpaar. Es entstehen sehr schnell Hunderte und Tausende von Schlüssel(paaren). Diese Schlüssel bzw. Schlüsselpaare müssen erstellt, verteilt und administriert werden. Mit zunehmender Anzahl von E-Mail-Benutzern entsteht hier immenser Aufwand. Die Schlüssel(paare) werden in der Regel über eine autorisierte Zertifizierungsstelle beantragt. Hier entstehen ebenfalls Kosten pro Schlüssel(paar).

Darüber hinaus bedeutet die Einführung der clientbasierten Verschlüsselung auch, dass neben der reinen Schlüsselverwaltung durch die Administration noch weitere Aufgaben zu erfüllen sind. Zunächst einmal muss die entsprechende Verschlüsselungssoftware auf jedem Rechner der E-Mail-Benutzer installiert werden.

Dies ist ebenfalls mit nicht unerheblichem Aufwand verbunden. Damit jedoch nicht genug. Die E-Mail-Benutzer, die oft bereits mit der Bedienung der E-Mail-Software ihre Mühe haben, müssen nun auch noch die korrekten Arbeitsschritte für die Verschlüsselung ihrer E-Mails durchführen. Selbstverständlich sind auch für die Entschlüsselung eingehender E-Mails entsprechende Interaktionen durch die Benutzer erforderlich.

Selbst die Durchführung von Benutzerschulungen garantiert keine reibungslose Ver- und Entschlüsselung, da Fehlbedienungen bei der Nutzung durch den Anwender nicht ausgeschlossen werden können. Außerdem entstehen natürlich Kosten für die Schulung der Benutzer.

Selbstverständlich fallen hier auch der fortlaufende Support und die Softwarewartung als Kostenfaktoren ins Gewicht. Denn jedes Update der Verschlüsselungssoftware muss wiederum auf alle Benutzer-PCs verteilt werden.

Bedingt durch die Notwendigkeit der Benutzerinteraktion fehlt es bei Benutzern immer wieder an ausreichender Akzeptanz gegenüber der Verschlüsselung. Die Benutzer betrachten die mit der Verschlüsselung verbundenen notwendigen Arbeitsschritte als eine zusätzliche Bürde, die ihnen von der Unternehmensführung oder den IT-Verantwortlichen auferlegt wird. Mangelnde Akzeptanz führt zwangsläufig dazu, dass die objektiv notwendige Sicherheit des E-Mail-Verkehrs auf der Strecke bleibt.

2.3 Probleme durch clientbasierte Verschlüsselung

Für viele Unternehmen umfasst die Sicherheit der E-Mail-Kommunikation nicht ausschließlich die Verschlüsselung derselben. Themen wie Virenschutz, Schutz vor Spam- und Junk-Mail, Schutz vor Informationsverlust und unerwünschten Inhalten stehen ganz oben auf den To-Do-Listen der IT-Abteilungen und Sicherheitsbeauftragten.

Betrachten wir nun die clientbasierte Verschlüsselung, so stellen wir fest:

Clientbasierte Verschlüsselung verhindert umfassende E-Mail-Inhaltssicherheit

Der Grund: Eine verschlüsselte Mail kann von Antiviren-Programmen und anderen E-Mail-Sicherheitsprogrammen auf den Mail-Servern nicht geschützt werden, denn die gesamte Mail ist für diese Programme nicht lesbar, so dass alle Schutzmechanismen, die auf den Mail-Servern implementiert sind, nicht greifen. Dies ist eine prekäre Situation. Haben sich doch die meisten Unternehmen aus gutem Grund dazu entschlossen, E-Mail-Sicherheitsanwendungen zentral auf den Servern zu betreiben, da dadurch die Administration in vielerlei Hinsicht wesentlich erleichtert wird. Die clientbasierte Verschlüsselung widerspricht damit der Notwendigkeit, E-Mail-Infrastrukturen und die entsprechenden Sicherheitsmechanismen zentral und unternehmensweit einheitlich zu implementieren und zu administrieren.

3 Serverbasierte Verschlüsselung

Eine serverbasierte Lösung zur E-Mail-Verschlüsselung bietet sehr gute Möglichkeiten, die in Kapitel 2 Clientbasierte Verschlüsselung beschriebenen Probleme zu vermeiden.

3.1 Einfache Implementierung

Im Gegensatz zur clientbasierten Verschlüsselung lässt sich eine serverbasierte Lösung mit einem Unternehmensschlüssel sehr viel schneller realisieren.

Bei serverbasierter Verschlüsselung benötigt nicht jeder E-Mail-Benutzer individuelle Schlüssel(paare), sondern das Unternehmen besitzt einen zentralen Unternehmensschlüssel bzw. ein Schlüsselpaar.

Stattdessen ist es möglich, einen Unternehmensschlüssel für die gesamte E-Mail-Kommunikation zu verwenden. Dadurch lässt sich die Verwaltung der Schlüssel wesentlich reduzieren. Die Kosten für Beantragung, Verteilung und Administration der Schlüssel sind im Vergleich zur clientbasierten Verschlüsselung ungleich geringer. Bei diesem Konzept steht das Unternehmen als juristische Person im Vordergrund. Der verwendete Unternehmensschlüssel stellt hier stellvertretend für die beteiligten E-Mail-Benutzer des Unternehmens sicher, dass die entsprechende E-Mail aus diesem Unternehmen gesendet wurde. Da letztlich das Unternehmen für den Inhalt der E-Mails der Mitarbeiter haftet, ist es zunächst unerheblich, ob eine E-Mail von Mitarbeiter A oder Mitarbeiter B versendet wurde. Daher lässt sich feststellen: Ein Unternehmensschlüssel ist für die rechtliche Sicherheit des Unternehmens ausreichend. Davon unbeschadet ist es natürlich dennoch möglich, für einzelnen Mitarbeiter personenbezogene Schlüssel einzusetzen. Für die Mehrzahl der Mitarbeiter bietet die Verschlüsselung mit einem Unternehmensschlüssel die notwendige Sicherheit.

Ein weiterer Vorteil der serverbasierten Verschlüsselung: Die aufwändige Implementierung einer Public Key Infrastruktur (PKI) ist nicht notwendig. Denn durch die Verschlüsselung zwischen zwei dedizierten E-Mail-Servern ist eine ebenso sichere „partielle“ Public Key Infrastruktur (PKI)-Lösung für Verschlüsselung von E-Mails realisierbar. Für die Realisierung einer Verschlüsselung zwischen zwei Unternehmen sind also nur folgende Dinge notwendig:

- ein Schlüssel pro Unternehmen,
- der Austausch dieser Schlüssel zwischen den Unternehmen,
- der Eintrag der Schlüssel in die zentrale Schlüsselverwaltung.

Mit diesen wenigen Arbeitsschritten ist die gesamte Kommunikation zwischen diesen beiden Unternehmen geschützt.

3.2 Keine Client-Softwareverteilung

An der Stelle, an welcher bei clientbasierter Verschlüsselung umfangreiche Maßnahmen zur Softwareverteilung notwendig sind, gestaltet sich dies bei der serverbasierten Variante sehr viel einfacher und daher kostengünstiger. Alle erforderlichen Softwarekomponenten befinden sich hier auf den E-Mail-Servern.

Die notwendige Installation auf den E-Mail-Servern ist nur mit sehr wenig Aufwand verbunden. Dies verringert nicht nur die Initialkosten, sondern verursacht auch bei der Softwarewartung wesentlich geringeren Aufwand.

3.3 Benutzertransparente Verschlüsselung

Bei serverbasierter Verschlüsselung ist keine Interaktion mit den E-Mail-Benutzern notwendig. Der E-Mail-Benutzer versendet und empfängt seine E-Mails in der für ihn bekannten Art und Weise. Die Ver- und Entschlüsselung findet für den Benutzer unbemerkt auf den E-Mail-Servern statt, erfordert daher keinen zusätzlichen Aufwand für Benutzerschulungen und spart entsprechend erhebliche Kosten. Selbstverständlich ist auch die Akzeptanz einer serverbasierten Verschlüsselung bei den E-Mail-Benutzern wesentlich höher, da sich für diese keine Änderungen in ihren Arbeitsabläufen ergeben.

Darüber hinaus lassen sich die eingesetzten Verschlüsselungsmethoden auf den E-Mail-Servern sehr einfach und für die Benutzer transparent kombinieren bzw. austauschen. Diese Flexibilität ist insbesondere dann von Bedeutung, wenn neue Unternehmens- oder Industriestandards eingeführt werden.

3.4 Zentrale, regelbasierte Verschlüsselung

Die Verlagerung der Verschlüsselung von den Clients auf den Server ermöglicht eine zentral gesteuerte, über Regeln definierte Verschlüsselung. „Regelbasiert“ bedeutet zunächst einmal, es wird eine Anzahl von „Wenn-Dann“ Bedingungen definiert. Wobei sowohl das „Wenn“ mehrere Bedingungen enthalten kann, als auch das „Dann“ mehrere auszuführende Aktionen beinhalten darf. Im Fall der Verschlüsselung könnten beispielsweise folgende Regeln definiert werden:

Wenn ...,	*dann ...*
eine E-Mail an abc@xyz.com gesendet wird	verschlüssele diese Mail mit dem PGP-Schlüssel abc
eine E-Mail von *@test.com empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
eine E-Mail an tom@jerry.com und mit der Betreffzeile „S/MIME“ gesendet wird	verschlüssele diese Mail mit S/MIME Zertifikat 4711

Durch diese regelbasierte Methode ist ein Höchstmaß an Flexibilität für das Unternehmen gewährleistet. Über eine zentrale Benutzeroberfläche werden die Regeln verwaltet.

3.5 Zentrale Schlüsselverwaltung

Die Schlüsselverwaltung erfolgt entsprechend in den jeweiligen Verschlüsselungsanwendungen (PGP und/oder S/(MIME) auf den E-Mail-Servern. Die PGP-Schlüssel lassen sich automatisch in den Schlüsselring importieren. Der zentrale Ansatz vereinfacht nicht nur die Implementierung, sondern auch die fortlaufende Wartung im Unternehmen.

3.6 Lösung mit iQ.Suite Crypt Pro

3.6.1 Flexible serverbasierte Ver- und Entschlüsselung

Auf den jeweiligen E-Mail-Servern werden iQ.Suite Crypt Pro und PGP und/oder S/MIME installiert. Eine clientseitige Installation ist nicht notwendig [siehe 3.2 Keine Client-Softwareverteilung].

Unbeschadet der serverbasierten Verschlüsselung mit iQ.Suite Crypt Pro im Unternehmen, können die Kommunikationspartner selbstverständlich sowohl serverbasiert als auch clientbasiert verschlüsseln. Entscheidend ist dabei nur, dass die gleichen Verschlüsselungsmethoden von beiden Partnern verwendet werden. iQ.Suite Crypt Pro unterstützt die beiden Industriestandards PGP und S/MIME.

3.6.2 Integrierte Verschlüsselung und Inhaltssicherheit

Für eine umfassende Sicherheit des E-Mail-Verkehrs ist Verschlüsselung alleine nicht ausreichend. Zentraler Virenschutz, Schutz vor Spam- und Junk-Mails, Schutz vor Informationsverlust und unerwünschten Inhalten spielen hier eine sehr wichtige Rolle. Die serverbasierte Verschlüsselung mit iQ.Suite Crypt Pro bietet hier als einziges Produkt die Möglichkeit, die Anforderungen für Verschlüsselung und Inhaltssicherheit zu erfüllen.

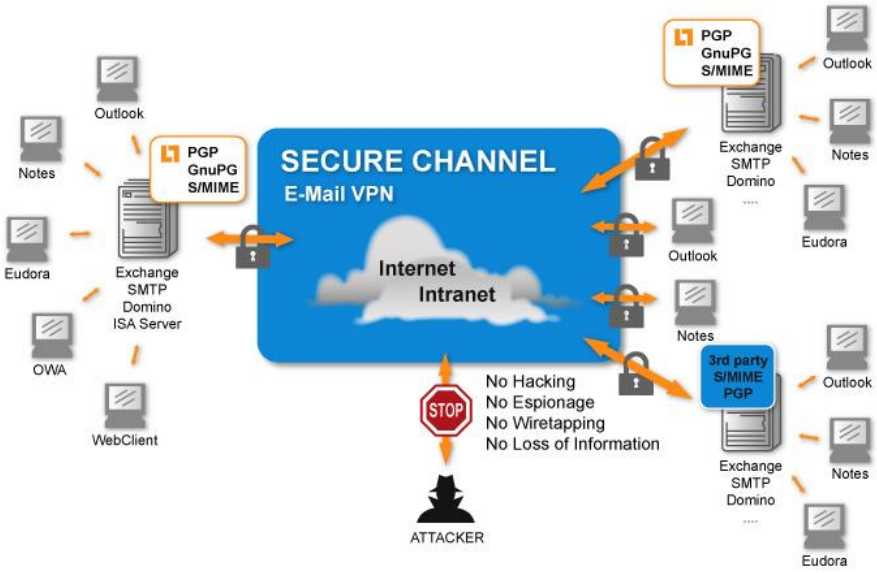

Abbildung 2: Sichere E-Mail Kommunikation mit iQ.Suite Crypt Pro

Durch die Kombination von iQ.Suite Crypt Pro mit weiteren Modulen der iQ.Suite sind mehrstufige Sicherheitsmaßnahmen realisierbar:

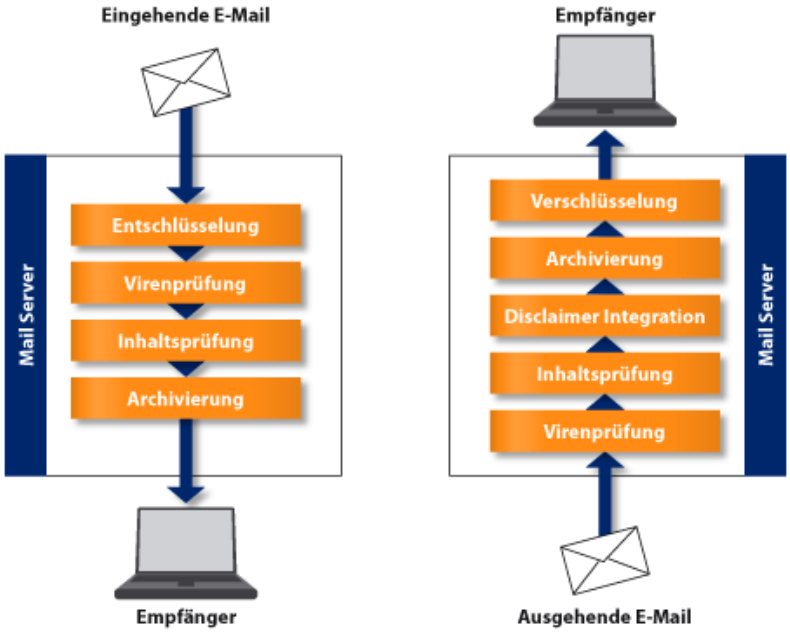

Abbildung 3: Mehrstufige Sicherheitsmaßnahmen der iQ.Suite für eingehende und ausgehende E-Mails

Mit iQ.Suite Crypt Pro muss sich ein Unternehmen nicht entscheiden, ob es Verschlüsselung oder serverbasierten Virenschutz, Spam- und Junk-Schutz, etc. einsetzt.

Bei iQ.Suite Crypt Pro heißt es: Verschlüsselung **und** serverbasierter umfassender Inhaltsschutz.

3.7 Überblick: Serverbasierte vs. clientbasierte Verschlüsselung

	Serverbasierte Verschlüsselung mit iQ.Suite Crypt Pro	*Clientbasierte Ende-zu-Ende Verschlüsselung*
Initialer Softwareverteilungsaufwand	gering	hoch
Supportaufwand	gering	hoch
Aufwand für Softwarepflege	gering	hoch
Zentrales, serverbasiertes Schlüsselmanagement	Ja	Nein
Aufwand für Schlüsselverwaltung im Unternehmen	gering	hoch
Implementierungsaufwand	gering	hoch
Benutzerakzeptanz	hoch	gering
Benutzertransparenz	Ja	Nein

	Serverbasierte Verschlüsselung mit iQ.Suite Crypt Pro	*Clientbasierte Ende-zu-Ende Verschlüsselung*
Schulungsaufwand	gering	hoch
Ermöglicht serverbasierten Virenschutz	Ja	Nein
Ermöglicht serverbasierten Schutz vor Spam- und Junk-Mail	Ja	Nein
Regelbasierte E-Mail-Sicherheit auf Basis von Domänen, Organisatorischen Einheiten, Gruppen und Benutzern	Ja	Ja, aber unverhältnismäßig aufwändig
Installation der Verschlüsselungssoftware	nur E-Mail-Server	auf allen Clients
PKI-Infrastruktur erforderlich	Nein	Ja
Kosten für gesamte Implementierung	gering	hoch
Kosten für den fortlaufenden Betrieb	gering	hoch
Unterstützung von E-Mail-Vertreterregelungen	Ja	Nein
Ermöglicht zentrale E-Mail Archivierung verschlüsselt und/oder unverschlüsselt	Ja	Nein

4 Szenarien

4.1 Client-zu-Server-Verschlüsselung

Ein Unternehmen beschäftigt neben fest angestellten Mitarbeitern an verschiedenen Standorten auch eine Anzahl von freien Mitarbeitern. Die freien Mitarbeiter arbeiten in der Regel nicht im Firmengebäude, sondern z.B. zu Hause. Von dort sind die freien Mitarbeiter über unterschiedliche Internet-Provider in der Lage, per E-Mail mit dem Unternehmen zu kommunizieren. Das Medium E-Mail nimmt hier bei der Kommunikation den größten Stellenwert ein.

Hierbei werden neben Informationen wie Absprachen und Terminvereinbarungen auch „kritische“ Informationen wie beispielsweise Preislisten, Verträge, Kunden- und Lieferantendaten ausgetauscht.

Um die E-Mail-Kommunikation umfassend zu schützen, werden nun geeignete Lösungen eruiert. Hierbei stehen neben der Sicherheit auf den Kommunikationswegen auch Virenschutz und Inhaltsprüfung im Vordergrund.

Anforderungen

1. Da die freien Mitarbeiter mit unterschiedlichsten E-Mail-Programmen über die verschiedensten Internet-Provider mit dem Unternehmen kommunizieren, muss die Verschlüsselung auf den dortigen Clients erfolgen. Dies allerdings unter Berücksichtigung der unterstützten Verschlüsselungsstandards des Unternehmens.
2. Das Unternehmen möchte seinen Mitarbeitern im Firmengebäude die Nutzung von E-Mails durch E-Mail-Verschlüsselung nicht erschweren. Daher ist eine für die Benutzer transparente Verschlüsselungslösung notwendig.
3. Wichtig ist eine kostengünstige Lösung, die sich leicht implementieren lässt. Daher sollen aufwändige Softwareverteilung und Benutzerschulungen vermieden werden. Gleichzeitig ist der Schlüsselverwaltungsaufwand des Unternehmens zu minimieren.
4. Parallel zur Einführung der E-Mail-Verschlüsselung ist die Implementierung einer serverbasierten Lösung für Virenschutz und Inhaltsprüfung geplant. Die Verschlüsselungslösung muss sich also so in das gesamte E-Mail-Sicherheitskonzept integrieren lassen, dass auch verschlüsselte E-Mails serverbasiert geschützt werden können.

Lösungsansätze

1. Die freien Mitarbeiter werden mit dem Verschlüsselungsprogramm PGP ausgestattet. PGP ist für unterschiedliche E-Mail-Clients verfügbar, so dass es für alle freien Mitarbeiter nutzbar ist. Jeder Mitarbeiter erhält einen PGP-Schlüssel.
2. Es wird ein Unternehmensschlüssel für das Unternehmen erstellt. Der öffentliche Unternehmensschlüssel wird allen freien Mitarbeitern zur Verfügung gestellt.
3. Die freien Mitarbeiter pflegen den öffentlichen Schlüssel in ihr PGP-Programm ein.
4. Auf dem E-Mail-Server des Unternehmens wird iQ.Suite Crypt Pro und PGP installiert. Auf den Clients des Unternehmens ist **keine** Softwareinstallation notwendig.
5. Die öffentlichen Schlüssel der freien Mitarbeiter werden auf dem E-Mail-Server in PGP eingepflegt.
6. In iQ.Suite Crypt Pro werden die entsprechenden Verschlüsselungsregeln erstellt:

Wenn ...,	*dann ...*
eine E-Mail von freier.mitarbeiter1@t-online.de empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
eine E-Mail von freier.mitarbeiter2@aol.com empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
eine E-Mail an freier.mitarbeiter3@hotmail.com gesendet wird	verschlüssle diese Mail mit PGP-Schlüssel FM3
etc.	etc.

7. Um nun auch den Virenschutz und die Inhaltsprüfung zu gewährleisten, werden mit iQ.Suite Watchdog (Virenschutz) und iQ.Suite Wall (Inhaltsprüfung) zwei weitere Module auf dem E-Mail-Server implementiert und in die bestehenden Regeln integriert.

	Wenn ...,	*dann ...*
STUFE 1	eine E-Mail von freier.mitarbeiter1@t-online.de empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
	eine E-Mail von freier.mitarbeiter2@aol.com empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
	etc.	etc.
STUFE 2 und 3	Wenn Mails aus dem Internet empfangen werden, unabhängig vom Absender	starte den Virenschutz und die Inhaltsprüfung

4.2 Server-zu-Server-Verschlüsselung

Ein Unternehmen unterhält Geschäftsbeziehungen zu einer größeren Anzahl von Lieferanten. Aufgrund der Schnelligkeit und der niedrigen Kosten wird mittlerweile mehr als 80% der Kommunikation über E-Mail abgewickelt. Wobei alle beteiligten Geschäftspartner die E-Mail-Plattformen IBM Notes/Domino oder Microsoft Exchange einsetzen. Im Rahmen der E-Mail-Kommunikation werden vor allem auch „kritische“ Informationen versandt, darunter beispielsweise Aufträge, Konstruktionszeichnungen, Analysen und Preisvereinbarungen. Gerieten solche Informationen in die falschen Hände, so hätte dies für das Unternehmen fatale Folgen.

Daher soll in Zukunft die E-Mail-Kommunikation zwischen den Geschäftspartnern verschlüsselt werden

Anforderungen

1. Für die Umsetzung der Verschlüsselung sollen keine weiteren Kosten für Hardwareanschaffungen entstehen.
2. Um den Aufwand und die Kosten zu minimieren, soll eine zentrale Verschlüsselung implementiert werden.
3. Da die beteiligten Unternehmen unterschiedliche Verschlüsselungsmethoden favorisieren, muss die Verschlüsselungslösung die Industriestandards PGP und S/MIME unterstützen.

Lösungsansätze

1. Die beteiligten Unternehmen installieren auf Ihren jeweiligen E-Mail-Servern iQ.Suite Crypt Pro und die gewünschten Verschlüsselungsprogramme (PGP oder S/MIME)
2. Für jeden Geschäftspartner wird ein Unternehmensschlüssel erstellt.
3. Die Unternehmensschlüssel werden auf den jeweiligen E-Mail-Servern in die Verschlüsselungsprogramme (PGP oder S/MIME) eingepflegt.
4. In iQ.Suite Crypt Pro werden die entsprechenden Verschlüsselungsregeln erstellt:

Wenn …	*Dann …*
eine E-Mail von Lieferant1@supplier.com empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
eine E-Mail von Lieferant2 @supplierxyz.com empfangen wird	entschlüssle diese Mail mit dem PGP-Unternehmensschlüssel
eine E-Mail anLieferant3@suppliernet.com gesendet wird	verschlüssele diese Mail mit S/MIME Zertifikat LF3

5 Daten und Fakten

iQ.Suite Crypt Pro Unterstützung	
Unterstützte E-Mail-Systeme	■ IBM Notes / Domino ■ Microsoft Exchange / SMTP
Unterstützte Verschlüsselungsmethoden	■ PGP ■ PGP/MIME[1] ■ S/MIME
Unterstützte Modi	■ Verschlüsseln ■ Entschlüsseln ■ Signieren ■ Signatur prüfen ■ Schlüsselimport

[1] **iQ.Suite für Exchange**

6 iQ.Suite Crypt Pro auf einen Blick

Highlights

- Unternehmensweite Verschlüsselungs-Richtlinien
  Die flexible Konfiguration von Absender-Empfänger-Kombinationen und E-Mail-Domänen erlaubt gezielte Verschlüsselungsbeziehungen zwischen Personen, Gruppen und Unternehmen. Zentrale Richtlinien ermöglichen beispielsweise das Einrichten permanenter E-Mail-Verschlüsselung oder deren Begrenzung auf bestimmte Personengruppen.
- Transparente Wirkungsweise
  Der Einsatz standardisierter Verfahren und die zentrale Verarbeitung auf dem Server stellt Transparenz gegenüber dem Benutzer und Unabhängigkeit vom E-Mail-Client sicher. Alle Kombinationen der Verschlüsselungspartner, wie Client-Client, Server-Server und Client-Server, sind frei konfigurierbar.
- Unterschiedliche Verschlüsselungs-standards
  Die gleichzeitige Verwendung von unterschiedlichen Verschlüsselungsverfahren wie PGP und S/MIME bietet höchste Sicherheit für unterschiedliche Einsatzzwecke und Kommunikationspartner.
- Flexibles Regelwerk
  Durch den Einsatz eines intelligenten, frei definierbaren Regelwerks zur gezielten Verschlüsselung von E-Mail-Inhalten bietet iQ.Suite Crypt Pro höchste Flexibilität und Sicherheit.
- Integrierte und zentrale Administration

Features

- Vergabe zentraler Verschlüsselungs-Richtlinien für die Kommunikation über Internet und öffentliche Netze
- Transparente E-Mail-Verschlüsselung unabhängig vom E-Mail-Client für den Benutzer
- Gezieltes Verschlüsseln durch Adressprüfung beliebiger Absender-Empfänger-Kombinationen, Empfängergruppen und Internetdomänen
- Integrierbar in jede Schlüsselverwaltung und Public Key Infrastructure (PKI)
- Zentrale Ablage von personen- und firmenbezogenen Public-Keys auf dem Server
- Keine Schlüsselverwaltung beim End-benutzer
- Gleichzeitige Verwendung unterschiedlicher Verfahren mit langen Schlüsseln, z.B. PGP, S/MIME
- Detaillierte Protokollfunktionen
- Konfigurierbare Benachrichtigungen an Absender, Empfänger und Administrator
- Multiplattformsupport für alle Betriebs-systeme
- Optimiertes Multiprozessing und Multithreading auch für Partitioned Server und Cluster
- Skalierbare Architektur
- „Ready to go“ für Application Service Providing (ASP)
- Einfache Erweiterung mit weiteren iQ.Suite Produkten

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