Sichere E-Mail

Aufgrund der unsicheren Übertragung von E-Mails ist es für viele Anwendungen unabdingbar, weitere Schutzmechanismen hinsichtlich Integrität und Vertraulichkeit anzuwenden. Hierbei kommt es auch aus Haftungsgründen darauf an, dass definierte Sicherheitsrichtlinien zentral eingerichtet und zuverlässig durchgesetzt werden.

Wer liest Ihre elektronische Post ?

Als vor über 30 Jahren die elektronische Post entwickelt wurde, wollten die Entwickler über eine Reihe universitär genutzter Rechner miteinander Nachrichten austauschen. Da es sich um ein in sich geschlossenes Netzwerk handelte, wurde eine missbräuchliche Nutzung nicht in Betracht gezogen.

Heute ist dies anders: Das Internet ist ein offenes Netz geworden und über das E-Mail-Protokoll SMTP werden milliardenfach Nachrichten verschickt. Darunter auch ein hoher Anteil mit sensiblen, privaten oder wertvollen Informationen. Leider hat das E-Mail-Protokoll immer noch keine eingebaute Sicherheit. E-Mail-Nachrichten werden als Klartext übertragen. Damit können sie auf jedem Rechner, den die Nachricht auf Ihrem Weg vom Absender zum Empfänger passiert, gelesen werden. Ebenso einfach lassen sich E-Mails mit falschen Absenderadressen versenden.

Daher gilt:

Ohne zusätzliche Schutzmechanismen, können Sie als Empfänger einer E-Mail weder dem Absender noch dem Inhalt einer E-Mail vertrauen! Darüber hinaus kann der Inhalt Ihrer E-Mails einfach gelesen werden.

Digitale Signatur und Verschlüsselung für den E-Mail-Verkehr des gesamten Unternehmens.

Bei der Kommunikation über E-Mail legen die Kommunikationspartner zunehmend Wert auf die eindeutige Authentisierung des Absenders und die Vertraulichkeit des Nachrichteninhalts. Für den Absender einer E-Mail bedeutet dies, dass er in die Lage versetzt werden muss, einerseit seine Nachricht digital zu signieren und andererseits auch zusätzlich bei Bedarf zu verschlüsseln. Gleichzeitig müssen alle Voraussetzungen geschaffen werden, dass der Empfänger der E-Mail die Authentizität der digitalen Signatur prüfen und die Nachricht wieder entschlüsseln kann.

Realisierungskonzept:
Zentrale Signatur/Verschlüsselung.

Am Übergang zum öffentlichen Netz wird ein Verschlüsselungs-Gateway eingerichtet, bei dem Schlüssel möglicher Kommunikationspartner hinterlegt sind. Technisch gesehen befindet sich das Gateway in der Demilitarisierten Zone (DMZ) zwischen Firewall und E-Mail-Server.

Eingehende E-Mail wird vom Gateway automatisch entschlüsselt und hausintern unverschlüsselt weitergeleitet. Die digitale Signatur des Absenders wird ebenfalls direkt auf dem Gateway geprüft. Ausgehende E-Mail wird automatisch digital signiert und,

enbiz • engineering and business solutions
Mozartstraße 25 • 67655 Kaiserslautern
http://www.enbiz.de/
info@enbiz.de

falls für den Empfänger ein Schlüssel hinterlegt ist, zusätzlich vor der Weiterleitung mit diesem Schlüssel verschlüsselt. Innerhalb des Unternehmens werden E-Mails nicht verschlüsselt.

Ob und mit welchen Mechanismen eine bestimmte E-Mail signiert und verschlüsselt wird, lässt sich auf dem Gateway **anhand von Regeln** hinterlegen. Regeln können hierbei sowohl generell als auch abhängig von den Kommunikationspartnern definiert werden.

Vorteile gegenüber E-Mail-Verschlüsselung auf individueller Ebene:

- Das Verschlüsselungs-Gateway ist für den hausinternen Absender/Empfänger vollständig transparent. Der Absender/Empfänger muss sich nicht mit der Signatur/Verschlüsselung auseinandersetzen, da das Gateway alle Aufgaben übernimmt.
- Problemlose, sichere und zuverlässige Umsetzung von Sicherheitsrichtlinien: die Regeln für die Signatur bzw. Verschlüsselung werden zentral formuliert, ein Benutzer kann nicht "vergessen", seine Mail zu signieren oder zu verschlüsseln.
- Das Verschlüsselungs-Gateway unterstützt mehrere Verschlüsselungsverfahren und damit auch unterschiedliche Verschlüsselungsprogramme beim externen Partner. Damit ist die Investitionssicherheit gegeben.
- Zentrale Verwaltung der Schlüssel: Aufwand nur an einer Stelle, einfache Datensicherung und -wiederherstellung.
- Content- und Virenfilter arbeiten unbeeinträchtigt, da im internen Netz keine verschlüsselten E-Mails übermittelt werden

Realisierung mit "Z1 SecureMail Gateway"

Das Z1 SecureMail Gateway der Firma Zertificon arbeitet wie eine zentrale Poststelle, die eingehende Post öffnet und ausgehende Briefe kuvertiert. Weil es alle E-Mails einer Organisation sichert und entsichert, wird es vom Hersteller auch als "virtuelle Poststelle" bezeichnet. Je nach Policy verschlüsselt, entschlüsselt, signiert bzw. überprüft es Signaturen automatisch auf Gültigkeit.

Das Z1 SecureMail Gateway unterstützt sowohl die Signatur/Verschlüsselung nach S/MIME als auch PGP (Pretty Good Privacy).

Eine PKI (Public Key Infrastructure) kann unmittelbar angebunden werden, so dass benötigte Schlüssel direkt durch das Gateway bei der Zertifizierungsstelle abgerufen bzw. beantragt werden.

Die zentrale Sicherheitspolitik wird vom Administrator vollständig über eine browserbasierte Management-Konsole (Admin Webclient) konfiguriert.

enbiz ist zertifizierter Partner von Zertificon Solutions und Competence Center für das Z1 SecureMail Gateway

Wir bieten Ihnen folgende Dienstleistungen im Bereich Secure Mail Gateway:

- Analyse von Netzwerk und E-Mailsystem, Beratung bei Aufbau und Absicherung
- Implementierung und Betrieb SecureMail Gateway
- Installationsworkshops und Adminschulung
- Anwenderschulung