Cesario
Informationstechnologie

PGP VERSCHLÜSSELUNG

SICHERE KOMMUNIKATION

E-Mail Versand sicher ...

Nutzung von E-Mail zur sicheren Nachrichtenübermittlung

Der E-Mail Datenverkehr kann auf vielfältige Weise abgehört werden.

Der Versand von E-Mail wird in der Regel über das nicht gesicherte Internet abgewickelt. Diese Datenkommunikation kann leicht mit im Internet erhältlichen Tools mitgehört und gespeichert werden. Dies ist für den sogenannten Angreifer völlig risikolos.

Warum verschlüsseln?

Als Versender von persönlichen Daten, sind Sie verpflichtet dritten den Zugang zu erschweren.

Die Verbreitung und Weiterentwicklung digitaler Kommunikationsmittel lässt bei vielen Unternehmen die wichtige Frage des Datenschutzes und der Datensicherheit in den Hintergrund treten.

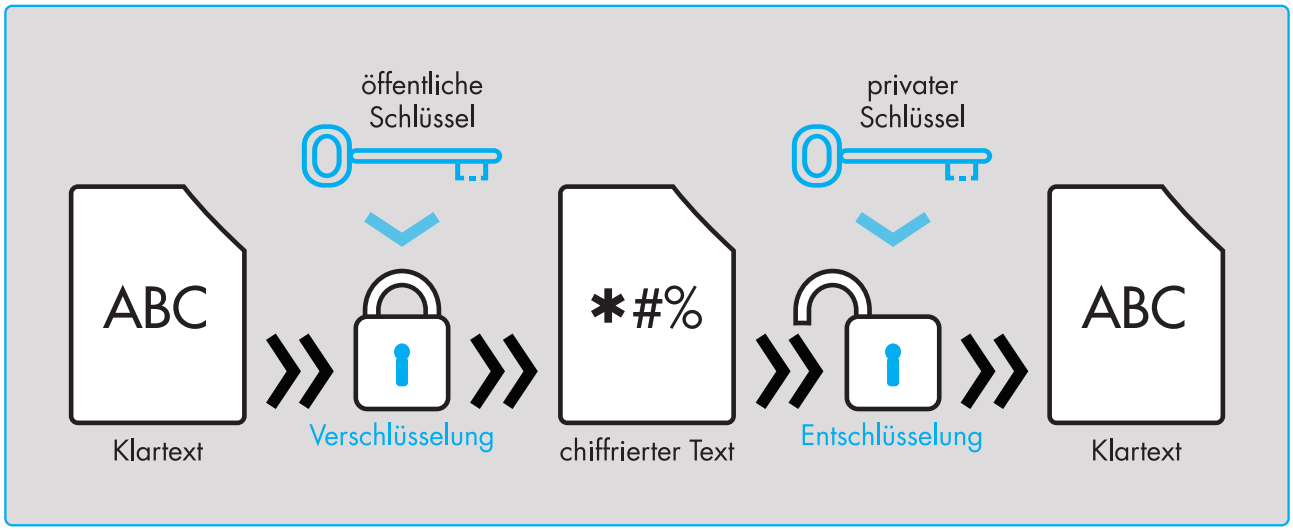
Viel zu selten drängt sich den Verantwortlichen, gerade in der heutzutage alltäglich gewordenen E-Mail-Kommunikation, die Frage nach dem Schutz ihrer Nachrichten und Daten während der Übertragung auf.

Ein Großteil der Unternehmen sendet eigene Daten und, viel schlimmer, die Daten von Kunden ohne besondere Vorkehrungen per E-Mail über das Internet.

Es erscheint daher durchaus gerechtfertigt den Versandt einer E-Mail mit dem einer Postkarte zu vergleichen. Die Verletzung der Vertraulichkeit ist möglich, ohne dass Spuren hinterlassen werden.

Verschlüsselung mit PGP

OpenPGP ist in der Informationstechnik ein Standard
für Verschlüsselungs-Software und im Rahmen der RFC 4880 standardisiert.



Funktionsweise der PGP Verschlüsselung

Statt wie bei einem symmetrischen System nur einen Schlüssel sowohl für Ver- als auch Entschlüsselung zu verwenden, besteht bei einem asymmetrischen System ein Schlüsselpaar aus zwei zusammengehörigen Schlüsseln. Daten, die mit einem Schlüssel verschlüsselt wurden, können ausnahmslos nur mit dem anderen Schlüssel wieder entschlüsselt werden; es ist nicht möglich, die Verschlüsselung mit demselben Schlüssel aufzuheben, mit dem sie erstellt wurde.

Das Hauptproblem der ansonsten sehr sicheren symmetrischen Verfahren, den einzigen existierenden Schlüssel sicher zum Kommunikationspartner zu übermitteln, stellt sich somit nicht, denn das Schlüsselpaar kann in einen sogenannten privaten oder geheimen Schlüssel und einen öffentlichen Schlüssel geteilt werden.

Um Daten zu verschlüsseln, benötigt der Absender nur den öffentlichen Schlüssel des Empfängers. Dieser öffentliche Schlüssel kann auch auf unsicherem Wege zum Kommunikationspartner gebracht werden, denn Nachrichten, die mit diesem Schlüssel verschlüsselt wurden, können nur mit dem privaten Schlüssel, der bei seinem Besitzer verblieben ist, wieder entschlüsselt werden. Somit ist ausgeschlossen, dass die Daten in falsche Hände geraten.

In der Regel ist sogar eine möglichst weite Verbreitung des öffentlichen Schlüssels wünschenswert, um sicherzustellen, dass keine öffentlichen Schlüssel unter falschem Namen eingeschleust werden.
Da die asymmetrische Verschlüsselung sehr rechenaufwendig ist, verwendet OpenPGP eine Mischung (Hybrid) aus asymmetrischer und symmetrischer Verschlüsselung:

Im ersten Schritt werden die zu verschlüsselnden Daten mit einem symmetrischen Einmal-Schlüssel, der nur für diese eine Verschlüsselung erzeugt wurde und nie wieder verwendet wird (Sitzungsschlüssel), verschlüsselt.

Im zweiten Schritt wird dieser Sitzungsschlüssel wiederum mit einem Schlüssel des asymmetrischen Schlüsselpaares verschlüsselt. Um umgekehrt die Daten wieder zu entschlüsseln, muss zuerst der symmetrische Schlüssel mit dem Bruder des asymmetrischen Schlüssels entschlüsselt werden.

Da der symmetrische Schlüssel im Verhältnis zu den zu verschlüsselnden Daten sehr kurz ist, hält sich auch der Rechenaufwand zur asymmetrischen Verschlüsselung in Grenzen und ist deutlich geringer, als wenn die Daten selbst asymmetrisch verschlüsselt würden.

Unser Angebot für Sie

PGP Pretty Good Privacy

- kostengünstig
- allgemein verfügbar
- geringer technischer Aufwand
- geringer administrativer Aufwand
- leichte Nutzung
- kein „offline“ Schlüsseltausch

Installation zum Festpreis

Nutzung von E-Mail zur sicheren Nachrichtenübermittlung

- lokale Installation von Thunderbird
- Installation von PGP Plugin für Thunderbird
- Erzeugung eines Schlüsselpaares
- speichern des Schlüssels
- Einrichtung in Ihrem Unternehmen
- Einweisung Ihrer Mitarbeiter
- Versand von Testnachrichten

Innerhalb des Berliner Rings 229€ zzgl. 19% MwSt.