De-Mail

Schlüssel zum Erfolg

[10.07.2015] Bislang war die Ende-zu-Ende-Verschlüsselung von De-Mails umständlich. Einfacher macht es jetzt das so genannte Pretty-Good-Privacy-Verfahren: Senden und empfangen kann nur ein Nutzer mit dem jeweils passenden Schlüssel.

De-Mails ohne zusätzliche Inhaltsverschlüsselung sind für das Sicherheitsniveau hoch zugelassen. Immer wieder aber gab es Diskussionen rund um die Datenübermittlung, für die ein sehr hohes Schutzniveau verlangt wird. Mit der Einführung des Pretty-Good-Privacy-Verfahrens (PGP) ist es jetzt einfacher, De-Mails zusätzlich Ende-zu-Ende (E2E) zu verschlüsseln. Seit Anfang April kann ein Nutzer mit einem Klick ein Zusatzprogramm in Form einer Erweiterung für die Browser Firefox und Chrome im De-Mail-Postfach vom De-Mail-Anbieter herunterladen, installieren und nach wenigen Einstellungen starten. Bis die E2E-Verschlüsselung auf PGP-Basis startklar ist, sind etwa 20 Schritte weniger erforderlich als bei der klassischen E-Mail-Kommunikation. Dem Vorgang wird damit die Komplexität genommen – zumindest für private Nutzer, die sich die Browser-Erweiterung heruntergeladen haben. Wenn größere Firmen und Behörden De-Mails zusätzlich verschlüsseln wollen, müssen sie sich mit der IT-Infrastruktur auseinandersetzen. Sie haben unterschiedliche Möglichkeiten, die E2E-Verschlüsselung zu nutzen. Am einfachsten ist der Einsatz eines so genannten Security Gateways. Diese Systeme übernehmen zentral die Ver- und Entschlüsselung der Nachrichten, sodass keine weiteren Eingriffe in die Infrastruktur erforderlich sind. Wer ein solches System bereits einsetzt, sollte prüfen, ob es auch für PGP geeignet ist. Dann sind in der Regel keine weiteren Anschaffungen erforderlich, um es mit De-Mail zu nutzen.

Add-In für den E-Mail-Client

Alternativ kann jeder Arbeitsplatz mit einem so genannten Add-In für den E-Mail-Client ausgestattet werden. Damit wird jede De-Mail nicht zentral, sondern erst am Arbeitsplatz ver- und entschlüsselt. Im Gegensatz zu Security-Gateway-Lösungen ist diese Variante mit mehr Aufwand bei der Einführung und Nutzung verbunden. Welche Methode sinnvoller ist, hängt von den jeweiligen Anforderungen ab. Unabdingbar für die Nutzung ist, dass sowohl beim Empfänger als auch beim Sender PGP-Verschlüsselungstechnologien vorhanden sind – entweder die Webbrowser-Erweiterung, ein zentrales Security Gateway oder eine dezentrale Erweiterung der E-Mail-Clients über entsprechende Add-Ins. PGP ist ein asymmetrisches Verschlüsselungsverfahren: Es werden immer zwei zusammengehörende Schlüssel genutzt. Dabei dient ein öffentlicher Schlüssel dazu, die Nachrichten zu verschlüsseln. Der Nutzer darf diesen Schlüssel frei weitergeben. E2E-verschlüsselte De-Mails kann nur ein Absender schicken, dem der Empfänger den Schlüssel weitergegeben hat. Somit kann auch niemand unfreiwillig eine PGP-verschlüsselte Nachricht erhalten. Der zweite, private Schlüssel ist geheim. Er wird zur Entschlüsselung genutzt und ist nur dem Eigentümer bekannt. Verliert der Besitzer ihn, kann er keine E2E-verschlüsselten Nachrichten mehr lesen. Der private Schlüssel lässt sich aus der Browser-Erweiterung exportieren und sollte unbedingt auf einem Datenträger gesichert werden.

Sicherer Austausch

Für die praktische Nutzung muss zunächst ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, generiert werden. Das ist simpel: Nach Installation der PGP-Browser-Erweiterung

erzeugt der Nutzer per Mausklick ein Schlüsselpaar. Dieses Paar wird im Schlüsselbund der Browser-Erweiterung lokal gespeichert. Im Anschluss lädt der Nutzer Personen oder Institutionen für die verschlüsselte Kommunikation ein. Dabei wird der öffentliche Schlüssel an die Eingeladenen gesendet. Die Herausforderung besteht darin, die Schlüssel zwischen Empfänger und Sender sicher auszutauschen. Bislang funktioniert das semiautomatisch, etwa indem der Sender dem Empfänger seinen öffentlichen Schlüssel per De-Mail mitteilt. Im Gegensatz zur E-Mail-Verschlüsselung steht hinter einer De-Mail-Adresse eine eindeutig identifizierte Person. Somit lässt sich auch der Schlüssel eindeutig zuordnen. Security Gateways unterstützen in der Regel bei der Schlüsselverwaltung. Künftig soll der Austausch automatisch erfolgen – über den öffentlichen Verzeichnisdienst von De-Mail (ÖVD). Davon profitieren insbesondere Verwaltungen und Kommunen, da sie die öffentlichen Schlüssel dann nicht mehr manuell verwalten müssen.
Künftig sind alle De-Mail-Nutzer in der Lage, im ÖVD ihren öffentlichen PGP-Schlüssel hochzuladen. Bereits heute ist das für die S/MIME-Verschlüsselung möglich. Da sie für Bürger nicht praktikabel ist, wird sie in erster Linie von Behörden und Unternehmen genutzt. Im ÖVD kann sich jeder De-Mail-Nutzer wie in einem Telefonbuch freiwillig mit seiner De-Mail-Adresse und weiteren Kontaktdaten eintragen. Verwaltet wird das Verzeichnis von den De-Mail-Diensteanbietern. Das ÖVD ist fester Teil der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten De-Mail-Infrastruktur. Mit einem Klick sind die Nutzer in der Lage, anbieterübergreifend nach Teilnehmern und öffentlichen Schlüsseln zu suchen. Damit steht künftig eine standardisierte Infrastruktur für den Schlüsselaustausch zur Verfügung – ein Meilenstein gegenüber der heutigen E-Mail-Kommunikation mit Pretty-Good-Privacy-Verfahren. Das ÖVD lässt sich theoretisch beliebig erweitern. Dort könnten zum Beispiel weitere Bürgerdaten vom Nutzer gespeichert und von Kommunen angewendet werden.

Klares Alleinstellungsmerkmal

Der Schritt, den die De-Mail-Diensteanbieter mit der Einführung des PGP-Verfahrens gegangen sind, ist richtig. Er zeigt, wie wichtig ihnen das Thema Sicherheit ist und wie konsequent die Erweiterungen umgesetzt werden, die bereits zur Einführung der De-Mail angekündigt wurden. Privatpersonen, Firmen und Behörden sollen für eine sichere digitale Kommunikation sensibilisiert werden, damit sie auf die De-Mail setzen. Mit dem automatischen Austausch der öffentlichen Schlüssel über das ÖVD in Verbindung mit den weiteren Eigenschaften der De-Mail-Infrastruktur erhält die De-Mail sogar ein klares Alleinstellungsmerkmal.

()

http://www.telekom.com

Stichwörter: IT-Sicherheit, De-Mail