ReddFort
M-Protect

reddFort

M-Protect

ReddFort M-Protect ist die „Personal End2End Encryption“ der ReddFort Software GmbH. Für zentral verwaltete Teilnehmer von E-Mail-Kommunikation, die Microsoft Outlook® verwenden, bietet ReddFort M-Protect höchste Sicherheit und garantiert Langzeitvertraulichkeit der zu übermittelnden Inhalte, bei einfachster Handhabung.

Warum ReddFort M-Protect?

Eine repräsentative Studie von Corporate Trust zum Thema Industriespionage[1] stellt fest, dass nur 16 % der deutschen Unternehmen E-Mail-Verschlüsselung als Instrument der IT-Sicherheit nutzen. Gleichzeitig geben aber mehr als die Hälfte der befragten Unternehmen an, bereits einen nachweislichen Spionagefall oder begründeten Verdacht auf Spionage gehabt zu haben, wobei nahezu jedes zweite der betroffenen Unternehmen das „Abhören/Abfangen von elektronischer Kommunikation“ als bewiesene oder vermutete Handlung des Angreifers angibt.

Dies zeigt deutlich, wie zunehmend wichtig der Schutz und die Verschlüsselung der Unternehmenskommunikation, insbesondere von E-Mails, für Unternehmen heutzutage sind.

Neben dem unter Sicherheitsaspekten ungünstigsten Fall der Übermittlung von E-Mails im Klartext trifft man in der Praxis häufig eine Transportverschlüsselung via TLS zwischen den Mailclients und dem Mailserver an. Worüber sich Anwender jedoch häufig nicht im Klaren sind: Trotz TLS können E-Mails auf den Mailservern frei gelesen werden. Die Transportverschlüsselung sorgt lediglich für die Vertraulichkeit der E-Mails auf dem Weg durch das Internet, nicht aber auf den Mailservern selbst. Zudem hängt die Haltbarkeit der Vertraulichkeit von der Stärke der Verschlüsselung in TLS ab. Hier zeigen bekannt gewordene Angriffe von Geheimdiensten, dass TLS dazu gebracht werden kann, nur ganz schwache Verschlüsselung anzuwenden, die faktisch keinen Schutzwert hat.

Einen besseren Schutz bietet eine durchgehende Ende-zu-Ende-Verschlüsselung, z.B. via PGP. PGP wird jedoch in der Praxis relativ selten eingesetzt, was zumeist auf die Komplexität der Einrichtung zurückgeführt wird. Der häufigste Kritikpunkt ist die umständliche und aufwändige Einrichtung und Benutzung, denn PGP leidet – wie alle PKI-basierten Systeme – unter der Schwierigkeit, die Echtheit und Gültigkeit der öffentlichen Schlüssel sicher und einfach zu gewährleisten.

Die Haltbarkeit der Verschlüsselung hängt von der Länge der RSA-Schlüssel, der Steigerung der Rechenkraft und Fortschritten bei Algorithmen zur Faktorisierung ab. Nach heutigem Stand können 2048/4096-RSA-Schlüssel noch drei bis fünf Jahre halten.

[1] Corporate Trust-Business Risk & Crisis Management GmbH: „Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co?“ **(www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf)**

Wo liegen die Unterschiede zur herkömmlichen E-Mail-Verschlüsselung?

ReddFort M-Protect geht einen ganz neuen Weg beim Schutz der Vertraulichkeit von E-Mail-Kommunikation. Eine E-Mail wird im ersten Schritt symmetrisch AES-256-verschlüsselt, wobei alle Teilnehmer paarweise verschiedene Schlüssel haben, die nur ein einziges Mal verwendet werden. Bei der symmetrischen Verschlüsselung, wie eben beim AES-Standard, wird derselbe Schlüssel zum Ver- und Entschlüsseln der Daten genutzt. Die Sicherheit ist an die Geheimhaltung des Schlüssels gebunden. AES gilt als sehr sicher. Eine „Brute Force Attack“, bei der alle möglichen Kombinationen durchgerechnet und ausprobiert werden, ist in diesem Fall nutzlos.

Im zweiten Schritt wird die bereits verschlüsselte E-Mail ein zweites Mal mit einem Random-One-Time-Pad (ROTP) verschlüsselt, wobei alle Teilnehmer das gleiche ROTP haben. Die Haltbarkeit der Vertraulichkeit unter den Teilnehmern hängt von der Haltbarkeit von AES-256 ab. Nach heutigem Wissen wird AES-256 mindestens 50 Jahre halten.

Die Haltbarkeit der Vertraulichkeit gegenüber Dritten hängt von der Qualität des ROTP ab. Ist das ROTP perfekt zufällig, dann kann die Verschlüsselung NIE gebrochen werden – sie hält ewig. Bei dem Zufallszahlengenerator von ReddFort M-Protect kann die Zufälligkeit als perfekt angesehen werden. ReddFort M-Protect garantiert damit die Vertraulichkeit der E-Mails über Jahrhunderte. Zusammen mit der einfachen Verwaltung und Benutzung ist M-Protect damit der perfekte E-Mail-Schutz für zentral verwaltete Teilnehmer.

Wie wendet man ReddFort M-Protect an?

ReddFort M-Protect integriert sich bei der Installation als Add-in nahtlos in Microsoft Outlook®. Für den Benutzer ergeben sich durch den Einsatz von M-Protect keine Beeinträchtigungen im gewohnten Umgang mit seinem Mailprogramm.

- Nach dem Kauf von ReddFort M-Protect legt eine Person des Vertrauens im Verwaltungsmodul des Programms zunächst den vorgesehenen Benutzerkreis mit den zugehörigen E-Mail-Adressen an. Dazu sind keine tiefer gehenden technischen Kenntnisse erforderlich.
- Für diesen Benutzerkreis werden durch ReddFort M-Protect automatisch Schlüssel und ROTP-Bänder zusammen mit einer Setup-Datei generiert. Diese werden in Verzeichnissen abgelegt, für jeden Benutzer auf einen USB-Stick kopiert und den Teilnehmern des Benutzerkreises ausgehändigt.
- Jeder Benutzer führt am eigenen Rechner die Setup-Datei aus. Damit wird ReddFort M-Protect als Add-in für Microsoft Outlook® installiert.
- Nun können durch den Benutzer E-Mails an andere Teilnehmer des Benutzerkreises verschlüsselt verschickt und verschlüsselte E-Mails (samt Dateianhängen) im Klartext gelesen werden.
- Neue Teilnehmer können in den vertraulichen Benutzerkreis aufgenommen oder Teilnehmer aus diesem Kreis entfernt werden, ohne dass jedes Mal neue Schlüssel oder ROTP-Bänder für den Rest des Kreises generiert werden müssen.

Ihre Vorteile?

- Lebenslange Vertraulichkeit der verschlüsselten Inhalte
- Höchste Sicherheit bei einfachster Handhabung
- Schlüsselerzeugung erfolgt im eigenen Haus, keine dritte Stelle ist involviert
- Nahtlose Integration in Microsoft Outlook 2010®/2013®/2016®
- ReddFort M-Protect ist konfigurierbar und damit individuellen Sicherheitsvorgaben anpassbar

Nahtlose Integration in Microsoft Outlook 2010®/2013®/2016®

Verfügbar für iOS und Android

Auf Smartphones können mit M-Protect verschlüsselte E-Mails NUR gelesen werden.

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

ReddFort Software GmbH

Neuensaaler Str. 70, 51515 Kürten Fon:
+49 2206 3096, Fax: +49 2206 4756
E-Mail: info@reddfort.de

www.reddfort.de