Kommentar: De-Mail - Rettungsversuch mit end-to-end-Verschlüsselung

13.03.2015, 18:47 | IT, New Media & Software

Pressemitteilung von: *KuppingerCole*
Presseagentur: *KuppingerCole*

Wiesbaden, 12. März 2015 – Seit der Einführung von De-Mail im Jahr 2012 kämpft, der Anbieter um die Akzeptanz der deutschen Öffentlichkeit. Nach den jüngsten Berichten nutzen nur rund 1 Mio. Privatpersonen diesen Service, was weit unter dem ursprünglichen Plänen von De-Mail liegt. Für eine Privatperson hat der Dienst kaum Vorteile im Vergleich zum normalen Postweg. Die größten Kritikpunkte bei De-Mail sind die Unvereinbarkeit mit regulären E-Mail- und sonstigen elektronischen Kommunikationsdiensten, Datenschutzbedenken im Anmeldeverfahren, sowie ein unzureichendes Sicherheitsniveau. Die deutsche Regierung versucht nun durch die Einführung von Ende-zu-Ende-Verschlüsselung die letztgenannten Probleme anzugehen. Der Plan ist es, De-Mail auf OpenPGP-Standard zu bringen, welcher in Mai 2015 von allen kooperierenden Anbietern eingeführt wird. Laut Innenminister Thomas de Maizière bietet die Einführung von PGP eine einfache und benutzerfreundliche Möglichkeit zur Erhöhung der Sicherheit des De-Mail-Services. Sicherheitsexperten und die Öffentlichkeit reagierten auf diese Maßnahme jedoch nicht besonders positiv.

Auch Alexei Balaganski, Analyst bei KuppingerCole sieht diese Änderung kritisch: „Um diese neue Funktionalität zu aktivieren, müssen Benutzer ein Browser-Plugin installieren. Diese Lösung basiert auf einer Open Source JavaScript OpenPGP-Unterstützung und steht derzeit nur für Chrome und Firefox-Browser zur Verfügung. Somit werden die Browser von mehr als 60% aller deutschen Internetnutzer nicht unterstützt. Noch größer ist das Problem des Mangels an Unterstützung für mobile Anwendungen oder Desktop-Mail-Clients."

Leider ist keine Einbindung des Plugins in das De-Mail-Benutzer-Verzeichnis möglich. Das bedeutet, dass die Benutzer vor der großen Herausforderung stehen eine sichere und zuverlässige Methode des Key Management (wie sie bei jeder Ende-zu-Ende-Verschlüsselungslösung benötigt wird) alleine finden zu müssen. In dieser Hinsicht ist De-Mail also nicht besser als jeder andere herkömmliche E-Mail-Service, da PGP-Verschlüsselung bereits von vielen Mail-Anwendungen in einer völlig Provider-unabhängige Art und Weise unterstützt wird.
Ein weiteres Thema ist die Benutzerfreundlichkeit der neuen Verschlüsselungslösung. De-Mail bietet bereits Verschlüsselung auf Basis von S/MIME an. Diese reicht aber nicht aus, da der Prozess "zu kompliziert" ist. Wenn man allerdings den Aufwand für sicheres Key Management vergleicht, ist PGP kaum eine einfachere Alternative.

Schließlich gibt es nach Alexei Balaganski noch eine grundlegende Frage mit vielen möglichen Rechtsfolgen: Wie kann man Ende-zu-Ende-Verschlüsselung mit der Forderung nach dem Dritten (dem Staat) kombinieren, um ihre Legitimität zu überprüfen?
Nach Meinung von Balaganski wird der Dienst von De-Mail auch in Zukunft erhalten bleiben, zumindest solange dieser aktiv von der Regierung unterstützt wird. „Allerdings habe ich ernsthafte Zweifel, dass De-Mail durch diese Unternehmungen einen spürbaren Einfluss auf ihre Popularität hat. Der einzig richtige Weg zur Implementierung einer Ende-zu-Ende-Verschlüsselung ist nicht zu versuchen, weiter auf der alten E-Mail-Infrastruktur aufzubauen, sondern neue Protokolle mit Rücksicht auf die Sicherheit, von Anfang an zu implementieren. Dafür muss man das Rad nicht neu erfinden, sondern sich ein Beispiel an bestehenden Entwicklungen, wie zum Beispiel der Dark Mail Technical Alliance, nehmen. Was die Industrie braucht, ist einen gemeinsam entwickelten Standard für die verschlüsselte Kommunikation zu erreichen."

Auch eine einheitliche Ansicht über die Verschlüsselung innerhalb der Regierung würde nach Balaganski helfen. Durch das Vorantreiben von NSA-ähnliche Massenüberwachung aller Internet-Kommunikationskanäle, sowie die Verwendung von Hintertüren und Exploits von denselben Personen, die zurzeit eine erhöhte Sicherheit und Privatsphäre der staatlichen Dienstleistungen versprechen, können weder Sicherheitsexperten noch die breite Öffentlichkeit überzeugt werden, so Balaganski.

Den vollständigen Blogbeitrag von Alexei Balaganski finden Sie unter www.kuppingercole.com/blog.

Journalisten können diesen Artikel sowie alle weiteren KuppingerCole-Analysen kostenlos bei KuppingerCole anfordern. Um die Zusendung von Belegexemplaren oder Links zu Online-Publikationen bei Veröffentlichungen mit Bezug auf diesen Beitrag wird gebeten.

Portrait

Über KuppingerCole
KuppingerCole, gegründet im Jahr 2004, ist ein führendes globales Analystenunternehmen mit Hauptsitz in Europa mit Schwerpunkt auf Information Security und Identity & Access Management (IAM). Ein weiterer Kernbereich des KuppingerCole Researchs bildet Governance, Risk Management and Compliance (GRC). Unsere sehr erfahrenen Analysten wissen, wie mit Informationssicherheits- und Privacylösungen ein signifikanter Mehrwert für Unternehmen generiert werden kann - für on-premise-Anwendungen, Cloud-Lösungen, mobile Zugriffe und Social Computing-Plattformen.
KuppingerCole steht für Expertise, Thought Leadership, Neutralität und für einen ausgeprägten Praxisbezug und unterstützt damit Anwenderunternehmen, Integratoren und Softwarehersteller sowohl bei taktischen als auch strategischen Herausforderungen. Die Balance zwischen unmittelbarer Umsetzbarkeit und Zukunftssicherheit prägt das Handeln von KuppingerCole.
Gemeinsam mit dem Unternehmensgründer Martin Kuppinger beobachten die hoch qualifizierten und weltweit angesehenen KuppingerCole Analysten kontinuierlich den Markt und stellen ihre Expertise in Form von aktuellen Research Notes und durch herstellerneutraler Beratung („Trusted Advisory“) zur Verfügung.
Zu den Analysten gehören neben Martin Kuppinger unter anderen der Identity & Access Management Experte Matthias Reinwarth, die Informationssicherheitsexperten Mike Small, Amar Singh, Dr. Eric Cole und Alexei Balaganski, die Infrastruktur- und Projektexperten Dr. Horst Walther, Dr. David Goodman und Rob Newby, die Privacy und Datenschutzexperten Dr. Karsten Kinast und Dr. Scott David sowie das Identity Management-Urgestein Dave Kearns.
Als unabhängige Analystengruppe organisiert KuppingerCole Konferenzen, Seminare, Workshops und Webcasts im Bereich Informationssicherheit, IAM und GRC und ist Ausrichter der European Identity & Cloud Conference, die sich als die führende Veranstaltung für Meinungsführerschaft und Best Practices für Identity & Access Management, Cloud und Digital Risk in Europa etabliert hat.
Erfahren Sie mehr auf unserer Website:
https://www.kuppingercole.com
https://www.id-conf.com

News-ID: 844237 • Views: 126 (Stand: 04.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/844237/Kommentar-De-Mail-Rettungsversuch-mit-end-to-end-Verschluesselung.html