

Sichere Mail-Verschlüsselung vom BSI. Präsident Schönbohm: „E-Mails und Online-Formulare weitgehend automatisiert verschlüsseln.“

Mit der quelloffenen Browser-Erweiterung Mailvelope können Anwender unter Verwendung des Verschlüsselungsstandards OpenPGP auch ohne spezielles E-Mail-Programm verschlüsselte E-Mails austauschen. Im Rahmen eines seit Januar 2018 laufenden Projekts hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mailvelope mit dem Ziel weiterentwickelt, die Installation, Konfiguration und Anwendung von Ende-zu-Ende-Verschlüsselung deutlich nutzerfreundlicher zu gestalten und damit eine größere Verbreitung von Verschlüsselung beim E-Mail- und Formular-Austausch zu erreichen. Zukünftig kann die Software auch genutzt werden, um vertrauliche Anfragen, zum Beispiel an Ärzte oder Banken, über Web-Formulare zu stellen.



Eingang Dienstgebäude des BSI, Godesberger Allee 185-189, 53175 Bonn Quelle: Bundesamt für Sicherheit in der Informationstechnik

Dazu Arne Schönbohm, Präsident des BSI: „Mehr Verschlüsselung bedeutet mehr Privatsphäre in der Kommunikation. Dies sollte kein nice-to-have, sondern ein absolutes must-have sein. Unser Ziel als Cyber-Sicherheitsbehörde ist es deshalb, Verbraucherinnen und Verbrauchern einfach anwendbare Lösungen an die Hand zu geben, mit denen sie ihre Privatsphäre besser schützen können. Deshalb haben unsere Expertinnen und Experten Mailvelope erweitert. Jeder kann sich dieses Tool als Add-on für den Browser herunterladen und damit E-Mails und Online-Formulare weitgehend automatisiert verschlüsseln.“

Ein konkretes Beispiel: Ärztinnen und Ärzte bieten Online-Formulare als Alternative zu Anrufen an. In der Regel ist es dabei notwendig, auch persönliche und vertrauliche Informationen anzugeben und diese somit über das Internet zu versenden. Mit einem verschlüsselten Kontaktformular können die Patientendaten besser geschützt werden. Der für die Verschlüsselung notwendige Austausch von öffentlichen Schlüsseln läuft dabei automatisiert ohne Nutzerinteraktion ab. Dazu müssen Anbieter von Kontaktformularen, in diesem Fall also die Arztpraxis, das Formular entsprechend konfigurieren

Anwenderinnen und Anwender müssen lediglich einmalig die Mailvelope-Anwendung installieren und konfigurieren. So wird Kommunikation im digitalen Alltag sicherer.

Die Erweiterungen von Mailvelope im Einzelnen

- Web-Formularinhalte können unabhängig vom Betreiber der Webseite bis zum Empfänger der Formularende-Zu-Ende verschlüsselt übertragen werden,
- die verwendete Kryptographie-Bibliothek OpenPGP.js ist durch das BSI-Projekt erweitert worden, um Kompatibilität mit dem OpenPGP-Standard herzustellen,
- es kann eine lokale GnuPG-Installation eingebunden werden, sodass Nutzer auf Wunsch native Anwendungen (z.B. zur Schlüsselverwaltung) verwenden können und
- für den Nutzer kann ein möglichst transparentes Schlüsselaustauschverfahren etabliert werden: Verteilung des öffentlichen Schlüssels durch Web Key Directory (WKD) über HTTPS-Abfrage

Um das Vertrauen in die Entwicklungen zu stärken, hat das BSI darüber hinaus ein Audit der Sicherheitseigenschaften des Produkts Mailvelope in Auftrag gegeben. Neben der Umsetzung der kryptographischen Verfahren wurden dabei auch die Existenz von Routinen zur Nutzerüberwachung oder Kompromittierung privater Daten überprüft. Hierdurch konnte nicht nur ein hohes Maß an Qualität gewährleistet werden, sondern Probleme wurden direkt im Anschluss an die Entwicklung erkannt und vor der Freigabe im Rahmen des Koordinierten Schwachstellenmanagements mit den Entwicklern erfolgreich gelöst.

Das vollständige Ergebnis des Audits ist in einem umfangreichen, englischsprachigen Bericht auf der Webseite des BSI verfügbar. **KLICKEN Sie HIER, um ihn aufzurufen.**

HIER gelangen Sie zur Projektseite ‚Weiterentwicklung von Mailvelope‘

Pressestelle BSI
www.bsi.bund.de



Mmh, Zuckerrohr ...

... das kleine süße Glück!

Für das größere Glück im Leben braucht Samir eine Schule und eine gute Grundbildung.

Sie können uns beim Schulbau helfen!

www.deswos.de



DESWOS

Deutsche Entwicklungshilfe
für soziales Wohnungs- und
Siedlungswesen e.V.

Spendenkonto DESWOS 660 22 21
Sparkasse KölnBonn, BLZ 370 501 98