Verschlüsselung – Ende-zu-Ende oder Transportverschlüsselung?

Dortmund, 06.07.2023 [Mit Aktualisierung vom 06.03.2024 zur Empfehlung des BSI zur Transportverschlüsselung und Hinweis auf das MECSA des JRC der Europäischen Kommission]: Inhalte von E-Mails können mit verschiedenen Maßnahmen gegen Einsichtnahme oder Manipulation geschützt werden. Wir geben einen kurzen Einblick in die Verschlüsselungsmöglichkeiten bei der E-Mail-Kommunikation

Die sicherste Methode zur sicheren Übermittlung von Daten ist die Ende-zu-Ende-Verschlüsselung (E2E) der E-Mails. Nur der Absender und der Empfänger haben Zugriff auf den Inhalt der E-Mail. Die E-Mail wird vor dem Versand, im E-Mail-Programm des Absenders verschlüsselt und erst im E-Mail-Programm des Empfängers wieder entschlüsselt. Während der Übertragung der E-Mail sowie auf dem E-Mail-Server liegt die E-Mail verschlüsselt vor und ist vor dem Zugriff Unberechtigter geschützt. Es sind Produkte am Markt erhältlich, die die E2E Ver- und Entschlüsselung auf einem vorgelagerten E-Mail-Gateway durchführen. Dies verlagert zwar das Ver- und Entschlüsseln der E-Mail vom Anwender auf das Gateway, aber die E-Mail liegt bei der Gateway-basierten Implementierung unverschlüsselt im Postfach des Senders bzw. Empfängers.

Für die E2E-Verschlüsselung haben sich 2 Standards etabliert. Diese beiden Standards, S/MIME und PGP, funktionieren nach dem gleichen Prinzip mit öffentlichen und privaten Schlüsseln, sind aber nicht kompatibel miteinander. Beide Standards werden von allen gängigen E-Mail-Programmen entweder direkt oder durch entsprechende Plug-ins unterstützt.

In Organisationen wird die E2E-Verschlüsselung in der Regel durch IT-Abteilungen implementiert. Es findet eine Einweisung der Nutzer statt, wie die Verschlüsselung zu verwenden ist.

In der E-Mail-Kommunikation mit Privatpersonen oder bei Privatpersonen untereinander, fehlt häufig die Möglichkeit der E2E-Verschlüsselung. Im privaten Bereich wird der Aufwand für die Integration von E2E-Verschlüsselung häufig gescheut oder das Wissen über Verschlüsselung und deren technische Umsetzung fehlt. Für den Versand von sensiblen Informationen haben sich im privaten Bereich Alternativen etabliert wie z. B. das Verschlüsseln von Anhängen (Passwortschutz) oder die Nutzung von sicheren Cloud-Diensten.

Für alle gängigen E-Mail-Programme finden sich gute Anleitungen und/oder Plug-ins, die die Einrichtung und Verwendung von E2E im privaten Bereich einfach gestalten und den Anwender durch alle notwendigen Schritte führen. Von der Erstellung der Schlüssel bis zum Versand und Empfang von verschlüsselten E-Mails.

Wie der Name beinhaltet, bietet die Transportverschlüsselung (Transport Layer Security – TLS) eine Verschlüsselung des Transportweges der E-Mail an. Ist TLS auf dem E-Mail-Server aktiviert und korrekt implementiert, wird der Transport der E-Mail verschlüsselt und schützt die E-Mail während der Übermittlung vor Einsicht und Manipulation.

Die E-Mail liegt bei der ausschließlichen Verwendung von TLS im Postfach des Senders und des Empfängers sowie auf dem E-Mail-Server in unverschlüsselter Form vor. Es gibt Administratoren, die konfigurieren E-Mail-Server bewusst unsicher, um die Kommunikation mit älteren oder nicht korrekt konfigurierten E-Mail-Servern weiter zu ermöglichen. Dadurch entsteht regelmäßig ein Sicherheitsrisiko, da Angriffe gegen die Verschlüsselung erfolgreich sein und E-Mails eingesehen oder manipuliert werden können.

Die korrekte Implementierung von TLS obliegt dem Betreiber des E-Mail-Servers. Der Sender oder Empfänger einer E-Mail kann in der Regel nicht nachvollziehen, ob die E-Mail TLS-gesichert übertragen wurde. Ebenso hat der Anwender auch keine Möglichkeit der Einflussnahme, ob TLS als Verschlüsselung verwendet werden soll oder nicht.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat in seiner technischen Richtlinie TR-02102-2 (Version 2023-1) Empfehlungen für die Verwendung von Transport-Layer-Security (TLS) als Transportverschlüsselung veröffentlicht. TLS ist nach der Empfehlung des BSI nur in den Versionen TLS 1.2 und TLS 1.3 als sicher einzustufen.

Das Joint Research Center (JRC) der Europäischen Kommission hat auf seiner Webseite den kostenlosen Service „My Email Communications Security Assessment“ (MECSA) bereitgestellt. Dieser Service bietet die Möglichkeit, die Sicherheit der E-Mail-Kommunikation zwischen Providern bewerten lassen.

Als Alternative, um mit Firmen oder Organisationen in Kontakt zu treten und Daten oder Dateien verschlüsselt zu übertragen, haben sich Webformulare etabliert. Wird die Formularseite mittels „https“ / TLS abgesichert, ist für die Übermittlung der Daten ein verschlüsselter Kommunikationsweg vorhanden. Der Inhalt ist nur für den Anwender sichtbar und für den Betreiber des Servers, auf den die Daten mit dem Webformular abgelegt werden.

Oft wird auch für den Austausch von Informationen eine Webseite mit Benutzername und Log-in verwendet. Der Benutzername wird von der Organisation vorgegeben oder selbst vergeben. Das Passwort wird üblicherweise durch den Anwender selbst vergeben. Die Kommunikation ist bei dieser Methode ebenfalls „https“ / TLS geschützt und einer Kommunikation per E-Mail ohne Verschlüsselung, aufgrund der Transportverschlüsselung der Webseite, bevorzugt zu verwenden.

Wie bei allen Zugängen ist es wichtig, dass die gewählten Passwörter ausreichend sicher sein sollten, und das für jeden Dienst ein eigenes, sicheres Passwort vergeben wird. Siehe dazu auch die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik:

BSI Information „Sichere Passwörter erstellen“

BSI Information: „Passwörter Schritt-für-Schritt merken“