++++ PRESSEMITTEILUNG ++++

LEIPZIG, 18.05.2018

E-Mail-Versand trotz Schutzvorkehrungen unsicher?

Aktuell wurde eine Sicherheitslücke beim Mail-Verkehr entdeckt / Von zentraler Bedeutung sind dabei technische Einstellungen und das Nutzerverhalten

In den letzten Tagen ging eine Meldung durch die Medienwelt: „E-Mails können nicht mehr sicher durch das Internet geschickt werden. Bisher verwendete Verschlüsselungsverfahrungen wurden geknackt." Sollten vertrauliche Informationen daher nicht mehr über die allseits beliebte Form der digitalen Briefe versendet werden? Doch, sagen Experten des Clusters IT Mitteldeutschland e. V. Die nun aufgedeckte Sicherheitslücke bezieht sich nicht auf die Verschlüsselung selbst, sondern betrifft den Transportweg und das Verhalten der Nutzer. Mit einer korrekten Implementierung und Anwendung der Schutzmechanismen lassen sich die versendeten Daten gut schützen.

Grundsätzlich gleichen E-Mails – wenn keine Vorkehrungen getroffen werden – einer Postkarte, die durch das Internet schwebt. Mit nicht allzu großem Aufwand und dem entsprechenden technischen Wissen kann im Prinzip jeder die darin enthaltenen Informationen mitlesen. Um E-Mails deshalb vor ungewollten Zugriffen zu schützen, wird klassischerweise ein Verschlüsselungssystem verwendet. Nur der Sender und der Empfänger können die Nachricht korrekt lesen. Während des Transportweges werden die Inhalte als lose, unverständliche Zeichenfolgen dargestellt.

Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun mitteilte, haben Wissenschaftler der Fachhochschule Münster, der Ruhr-Universität Bochum sowie der Universität Leuven (Belgien) eine Sicherheitslücke bei den gängigen E-Mail-Verschlüsselungsstandards OpenPGP und S/MIME aufgedeckt. Dabei ist es gelungen, E-Mails nach der Entschlüsselung durch den Empfänger an einen fiktiven Cyber-Angreifer weiterzuleiten. Um die Schwachstelle ausnutzen zu können, sind der Zugriff auf den Transportweg, den Mailserver oder das E-Mail-Postfach des Empfängers notwendig.

„Die nun aufgedeckte Sicherheitslücke betrifft nicht die Verschlüsselungsverfahren selbst. Diese können weiterhin bedenkenlos eingesetzt werden und liefern einen effektiven Schutz vor Cyber-Angriffen", sagt Andreas Liefeith, Leiter des Arbeitskreises IT-Sicherheit im Cluster IT Mitteldeutschland und Leiter Marketing der procilon GROUP, „Das eigentliche Sicherheitsproblem entsteht erst, wenn die Schutzvorkehrungen nicht richtig und umfassend implementiert werden und wenn sie von Seiten der Nutzer falsch angewendet werden. Hier gilt es, gegebenenfalls zu überprüfen, ob der aktuelle Schutz ausreichend ist."

So muss die Verwendung eines Verschlüsselungsverfahrens in ein Gesamtkonzept für sicheres Kommunizieren über das Web eingebettet sein. Das beinhaltet zum einen die technische Komponente, das heißt, dass Vorkehrungen und Einstellungen über die eigentlichen Mail-Inhalte hinaus gedacht und umgesetzt werden müssen – und zum Beispiel auch Maßnahmen zum Schutz von Postfächern und Mailservern umfassen. Dazu zählt zum Beispiel die zwingend erforderliche Durchführung von Sicherheitsupdates. Wichtig ist auch, dass vor Entschlüsselung geprüft wird, ob die E-Mail unversehrt ist oder ob zum Beispiel auf dem Weg durch das Internet schadhafte Elemente an ihr angeheftet wurden (Integritätsprüfung). Diese werden häufig nach der Entschlüsselung aktiv. Besondere Gefahr geht dabei von so genannten aktiven Inhalten aus. Dazu gehören Inhalte in HTML-Mails wie Bilder oder nach Klick auf Links aktivierte Inhalte. Häufig sind Mailprogramme, besonders auch auf Smartphones, so eingestellt, dass aktive Inhalte automatisch angezeigt werden. Für den sicheren E-Mail-Verkehr sollten diese deaktiviert werden.

Neben den technischen Maßnahmen ist es von zentraler Bedeutung, die Nutzer für sicheres Agieren im Internet zu sensibilisieren. „Ein klassisches Beispiel stellt der Umgang mit Passwörtern dar“, so Liefeith, „Gelingt es Angreifern, über das Internet oder auch direkt vor Ort durch eine fahrlässige Verwendung Passwörter für Mail-Accounts abzugreifen, ist es für sie ein Leichtes, Zugang zu Mail-Postfächern zu gewinnen. Und dann kann auch keine Technologie wirkungsvoll schützen. Im Arbeitskreis IT-Sicherheit des Clusters IT Mitteldeutschland weisen wir deshalb immer wieder sehr umfangreich und detailliert auf technische und menschliche Sicherheitslücken hin.“

Wie die Sicherheitslücke funktioniert, erklärt anschaulich (für jedermann) ein Sicherheitsexperte von procilon: https://bit.ly/2INaukH.

Zum Cluster IT Mitteldeutschland e. V.

Der Cluster IT ist das Branchennetzwerk der IT-Wirtschaft in Sachsen, Sachsen-Anhalt und Thüringen mit der Zielsetzung, die Aktivitäten der Branche zu koordinieren und sichtbar zu machen. Gegründet wurde der Verein im Jahr 2009 und besitzt mittlerweile knapp 50 Mitglieder. www.it-mitteldeutschland.de.