Bitkom e.V. |

Nutzer sollten ihre E-Mails weiterhin verschlüsseln

- Entwarnung zu jüngsten Veröffentlichungen über gehackte E-Mails
- Bitkom gibt Hinweise für eine sichere E-Mail-Kommunikation

Berlin, 18. Mai 2018 - Trotz der jüngsten Veröffentlichungen zu Angriffen auf verschlüsselte E-Mails: Der Digitalverband Bitkom rät dazu, E-Mails weiterhin mit den bekannten Verfahren S/MIME oder OpenPGP zu schützen. „Eine verschlüsselte E-Mail ist in jedem Fall sicherer vor ungewollten Blicken, als nicht-geschützte E-Mails“, sagt Dr. Nabil Alsabah, Bitkom-Experte für IT-Sicherheit. „Nicht alle Hackerszenarien, die unter Laborbedingungen stattfinden, sind auch in der Praxis leicht umsetzbar.“

Europäische Sicherheitsforscher hatten kürzlich gezeigt, wie Angreifer gängige Sicherheitsmechanismen bei der E-Mail-Verschlüsselung aushebeln können. In den veröffentlichten Szenarien waren E-Mail-Programme betroffen, die Nachrichten mit den standardisierten Verfahren S/MIME oder OpenPGP verschlüsseln. Eine der Voraussetzungen für einen erfolgreichen Angriff ist dabei, dass ein Angreifer in den Besitz einer verschlüsselten E-Mail kommt. Gelingt ein solcher Datenklau, müsste der Angreifer diese verschlüsselte Nachricht in eine E-Mail mit HTML-Schadcode einbetten und diese wiederum an den Empfänger der zuvor verschlüsselten Nachricht schicken. Unter bestimmten Voraussetzungen wird diese E-Mail dann automatisch entschlüsselt und lesbar an den Angreifer zurück verschickt. „Es besteht keine akute Gefahr für Nutzer, die ihre E-Mails verschlüsseln“, so Alsabah. Die jüngst veröffentlichten Forschungsergebnisse deuteten jedoch darauf hin, dass die S/MIME- und OpenPGP-Standards mittelfristig zu aktualisieren sind.

Bitkom gibt Tipps für eine sichere E-Mail-Kommunikation.

E-Mails richtig verschlüsseln

Moderne E-Mail-Verschlüsselung basiert auf dem Prinzip der asymmetrischen Kryptographie. Dabei nutzen Anwender ein sogenanntes Schlüsselpaar: einen Schlüssel zum Kodieren und einen zum Dekodieren von Nachrichten. Die zugrunde liegenden mathematischen Verfahren garantieren, dass so geschützte Nachrichten nur mit dem privaten Schlüssel zu entziffern sind. Der öffentliche Schlüssel soll und kann deshalb publik gemacht werden. Mit diesem können E-Mail-Sender ihre Nachrichten an den Empfänger verschlüsseln. Der andere Schlüssel muss jedoch privat und geheim aufbewahrt werden. Denn damit lassen sich alle Nachrichten und Daten entschlüsseln, die an den Empfänger verschickt werden. S/MIME und PGP sind die am weitesten verbreiteten Standards für die asymmetrische Verschlüsselung. Sie arbeiten nach ähnlichen Prinzipien. Ein zentraler Unterschied betrifft die Generierung des Schlüsselpaars: Bei S/MIME werden Schlüssel von einer vertrauenswürdigen Zertifikats-Autorität ausgestellt, PGP kommt jedoch ohne aus. Für PGP und für S/MIME gibt es kostenlose, quellcodeoffene, aber auch kommerzielle Lösungen – als Softwarepaket oder als Online-Dienst. Damit generieren Nutzer ein Schlüsselpaar und erweitern Mailprogramme um Verschlüsselungsfunktionen, sofern diese nicht nativ unterstützt werden. Nutzer könne nun ihren öffentlichen Schlüssel an Bekannte verschicken und im Netz veröffentlichen. Ebenso können sie öffentliche Schlüssel von weiteren Anwendern herunterladen, um ihnen verschlüsselte E-Mails zu versenden.

Kein automatisches Laden von aktiven Inhalten

Aktive Inhalte sind vor allem in E-Mails im HTML-Format beliebt. Sie erlauben dem Verfasser Texte zu formatieren, Bilder einzufügen und dadurch ein lebendiges Erscheinungsbild zu kreieren. Diese Inhalte werden durch HTML-Code eingebettet. Der Nachteil: In diesen aktiven Inhalten lässt sich Schadcode verstecken. Wer aktive Inhalte in HTML-basierten E-Mails grundsätzlich laden lässt, läuft Gefahr, dass damit Schadcode empfangen und ausgeführt wird. Vor allem bei unbekannten Absendern sollten aktive Inhalte in E-Mails nicht ausgeführt werden. In der Regel lässt sich über das

genutzte E-Mail-Programm einstellen, wann und ob HTML-Inhalte dargestellt werden.

Sichere Verbindung zum Mailserver nutzen

Wer seine E-Mails über eine Weboberfläche abruft, sollte auf eine sichere Verbindung zum Mailserver achten. Dies ist daran zu erkennen, dass die Adresse im Browser mit „HTTPS“ anfängt. Eine HTTPS-Verbindung sorgt dafür, dass die Kommunikation zwischen dem Rechner des Nutzers und dem E-Mail-Server verschlüsselt wird und bietet dadurch zusätzliche Sicherheit.

Sicherheitsupdates immer installieren

Nutzer sollten die Update-Hinweise ihres Betriebssystems, im Browser, bei Add-Ons und anderen Programmen ernst nehmen. Gleiches gilt für Virenscanner. Ohne sie kann es sehr gefährlich sein, sich im Internet zu bewegen – gleich ob per Desktop-Computer oder Smartphone. Umso wichtiger ist es, die Virensoftware immer aktuell zu halten.

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org

Felix Kuhlenkamp
Referent Sicherheitspolitik
Nachricht senden

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/Nutzer-sollten-ihre-E-Mails-weiterhin-verschluesseln.html