Cryptshare®
Making e-mail better

Kommentar

Efail: Nicht E-Mail ist das Problem, sondern der Transportweg

Eine Einschätzung von Matthias Kess, CTO der auf Kommunikationslösungen spezialisierten Befine Solutions AG

Freiburg im Breisgau, 22. Mai 2018. Sicherheitsforscher haben die Verschlüsselung von E-Mail-Systemen ausgehebelt und Details über Sicherheitslücken in den beiden Verschlüsselungsverfahren PGP und S/MIME veröffentlicht. Unter bestimmten Bedingungen lassen sich E-Mails entschlüsseln, auch nachträglich. Damit dürfte das Vertrauen in verschlüsselte E-Mails zumindest auf absehbare Zeit verloren sein, so die Forscher, schlimmer noch: E-Mail sei kein sicheres Kommunikationsmedium mehr. Müssen sich Unternehmen nun, wenige Tage vor Inkrafttreten der Europäischen Datenschutzgrundverordnung, Gedanken machen? Ja! Ist Panik angebracht? Nein! Beides hat gute Gründe.

Die Forscher der Fachhochschule Münster, der Ruhr-Universität Bochum und der belgischen Universität Leuven haben kritische Schwachstellen bei der Entschlüsselung von S/MIME- und PGP-verschlüsselten Nachrichten in E-Mail-Clients entdeckt. Sie können nachweisen, wie man mit aktiven Inhalten von HTML-E-Mails wie beispielsweise einem geschickt gefälschten Befehl zum Laden von externen Bildern die entschlüsselten Inhalte einer E-Mail abgreifen kann.

E-Mail: Kein sicheres Kommunikationsmedium mehr?

Das Angriffsszenario besteht darin, in eine verschlüsselte E-Mail einen neuen Befehl einzubetten, wodurch der Text vom Empfänger nicht nur automatisch entschlüsselt, sondern dabei auch automatisch an den Angreifer gesendet wird. Das Szenario, das auf Unzulänglichkeiten in der E-Mail-Client-Software basiert, erfordert deutlich weniger Hacker-Know-how als man erwarten könnte.

Die Folgerung der Forscher – E-Mail sei kein sicheres Kommunikationsmedium – ist erst mal nichts Neues. Was zugleich die gute und die schlechte Nachricht ist. Im Prinzip entspricht eine E-Mail einer Postkarte: Sie ist günstig und schnell zuzustellen, ihr Inhalt ist aber für jeden lesbar und auch modifizierbar, der sie transportiert. Was auf dem Transportweg der einzelnen E-Mails passiert, welche Stationen beteiligt sind, bleibt dem Anwender verborgen.

Verschlüsselung: Ja oder nein?

Soll man also vorerst auf die Verschlüsselung in E-Mail-Clients verzichten, wie es die Forscher geraten haben? Wäre das nicht in etwa so, als ob man grundsätzlich seine Haustüre offenstehen lässt, weil es ohnehin zu viele Einbruchsdelikte zu beklagen gibt?

Nein, keine Verschlüsselung ist auch keine Lösung. Daher weist auch das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) darauf hin, dass OpenPGP und S/MIME weiterhin sicher eingesetzt werden könnten, wenn sie korrekt implementiert und sicher konfiguriert werden. Dies erfordert allerdings Aktivitäten sowohl von Software-Herstellern, Standardisierungsgremien und Endbenutzern und wird sich in der Summe der notwendigen Maßnahmen voraussichtlich noch Monate hinziehen.

Überhaupt gilt es, gerade den Punkt der Verschlüsselung nochmals grundlegend zu überdenken: Denn in wenigen Tagen, am 25. Mai, tritt die Europäische Datenschutz-Grundverordnung nach einer zweijährigen Übergangszeit endgültig in Kraft. Während die DS-

GVO in vielen Fällen bewusst vage vom „Stand der Technik“ spricht, so auch in Artikel 32 („Sicherheit der Verarbeitung“), fordert sie dort explizit die „Verschlüsselung personenbezogener Daten“.

DS-GVO: Welche Rolle spielt die Verschlüsselung personenbezogener Daten?

Damit ist natürlich nicht gemeint, dass Unternehmen nur noch über verschlüsselte E-Mails kommunizieren dürfen. Wohl aber, dass Faktoren wie der Schutzbedarf der Daten zu berücksichtigen sind. Die Verordnung bezieht sich ausschließlich auf personenbezogene Daten, aber auch andere vertrauliche Daten sollten diesen Schutz erfahren. Um beispielsweise Patentgeheimnisse, Forschungsergebnisse oder Kundeninformationen abzusichern, bleibt Verschlüsselung alternativlos.

Laut einer vor wenigen Tagen vorgestellten Bitkom-Umfrage werden drei Viertel der deutschen Unternehmen mit der Umsetzung der Vorgaben nicht rechtzeitig fertig – ihnen bleibt nun gar nichts anderes mehr übrig als Prioritäten zu setzen. Durch E-Mail-Verschlüsselung lässt sich ein vergleichsweise kleiner Posten der Liste schnell abarbeiten.

„E-Mail 2.0“: Warum hat der Ansatz Schwächen?

Überhaupt spielt E-Mail bei den bisher erörterten Fragen eine zentrale Rolle: Sie hat sich speziell im Unternehmensumfeld seit vielen Jahren als Hauptkommunikationsmittel etabliert, ist einfach zu bedienen und universell verfügbar – und ist andererseits seit langem ein bevorzugtes Angriffsziel von Kriminellen, Hackern und Wirtschaftsspionen.

Auch im Zuge der aktuellen Diskussion werden Forderungen nach „E-Mail 2.0“ laut. Besser wäre es, von „SMTP 2.0“ zu sprechen. SMTP (Simple Mail Transfer Protocol) zählt zu einer kleinen und ausgewählten Gruppe von universellen Standards, welche die Geschäftskommunikation unterstützen, den heutigen Anforderungen an Sicherheit jedoch weit hinterherhinken. SMTP ist ein Protokoll, das festgelegte Regeln beschreibt, wie ein bestimmter Vorgang abläuft – das Versenden und Weiterleiten einer E-Mail im Internet. Die E-Mail geht dabei, für den Anwender unsichtbar, durch verschiedene Hände und passiert mehrere Stationen, die als potentielle Angriffspunkte für Cyber-Kriminelle dienen können. Das erst ist die Basis für bestimmte Arten von Angriffen.

Der andere (Transport-)Weg

Cryptshare wählt daher einen anderen (Transport-)Weg als S/MIME und PGP: Die Idee dahinter ist es, die Nachteile des E-Mail-Systems zu überwinden und die Vorteile zu nutzen. Der Ablauf ist bewusst einfach gehalten: Die verschlüsselt zu übertragenden Daten – auch die E-Mail-Nachricht – werden verschlüsselt auf einen unternehmenseigenen Server hochgeladen und abgelegt. Der Empfänger wird per E-Mail lediglich über die Bereitstellung seiner Nachricht informiert und erhält vom Absender separat ein einmaliges Passwort. Das kann auf unterschiedliche Arten stattfinden – beispielsweise telefonisch, per Brief, Fax oder auch persönlich. Welches Maß an Sicherheit angewendet wird, hat der Anwender selbst in der Hand.

Mit dem Passwort kann er die Daten direkt und verschlüsselt von diesem Server herunterladen. Die Nachricht samt Anhängen findet sich dann automatisch im E-Mail-Client des Empfängers wieder. Hundertprozentige Sicherheit gibt es nicht, auch hier nicht: Aber während bei S/MIME und PGP mehrere Server im Spiel sind, ist es hier nur einer – der des Unternehmens, in dessen Rechenzentrum der Inhalt der empfangenen Nachricht abliegt. Die vertrauliche Nachricht wird also von E-Mail-Client zu E-Mail-Client übertragen, ohne dass ein E-Mail-Server oder -Provider mit den sensiblen Informationen in Berührung kommt.

Zudem entfallen auf diesem Wege die Größenlimitierungen für Dateianhänge, und alle Versand- und Empfangsvorgänge werden vollständig protokolliert. Klare Benachrichtigungen an den Absender, wann E-Mails und Dateien versandt und an den beabsichtigten Empfänger zugestellt worden sind, unterstützen Unternehmen, Richtlinien und Compliance-Vorgaben wie

die DS-GVO einzuhalten. So können auch auffällige Aktivitäten im Zusammenhang mit der E-Mail-Kommunikation besser festgestellt werden.

Weitere Informationen

Informationen zur Funktionsweise der Lücke und das dazugehörige Forschungspapier von Forschern der Fachhochschule Münster, der Ruhr-Universität Bochum sowie der belgischen Universität Leuven lassen sich hier abrufen.

Über Matthias Kess
Matthias Kess ist CTO der Befine Solutions AG mit Sitz in Freiburg im Breisgau, die Kommunikationslösungen für Unternehmen entwickelt und vertreibt.

Über Cryptshare und Befine Solutions
Die inhabergeführte Befine Solutions AG entwickelt und vertreibt Softwarelösungen für Unternehmen, die damit ihre Prozesse unterstützen, optimieren und überwachen können. Hauptsitz und Entwicklungsstandort des im Jahr 2000 gegründeten Unternehmens mit über 50 Mitarbeitern ist Freiburg im Breisgau. Vertriebsstandorte gibt es in Großbritannien sowie den Niederlanden, eine Tochtergesellschaft in den USA.
Im Mittelpunkt steht Cryptshare, eine Kommunikationslösung für den sicheren Austausch von Informationen. Mit ihr lassen sich E-Mails und Dateien jeder Größe und Art ad-hoc austauschen – einfach und sicher, nachvollziehbar und kostengünstig. Sie ist in mehr als 1.400 Unternehmen in über 30 Ländern bei rund 3 Millionen Anwendern im Einsatz. Cryptshare wurde 2017 mit dem „Cybersecurity Excellence Award“ in der Kategorie „E-Mail Security“ ausgezeichnet.
Weitere Informationen finden sich unter www.cryptshare.com. Anwender können sich auch im Blog informieren.

Pressekontakt:
phronesis PR GmbH
Marcus Ehrenwirth, Marcus Wenning
Kobelweg 12 ¼
D-86156 Augsburg
Telefon: +49 821 444800
E-Mail: info@phronesis.de
Web: www.phronesis.de

Befine Solutions AG – The Cryptshare Company
Oliver Gäng – Chief Marketing Officer
Schwarzwaldstraße 151
D-79102 Freiburg im Breisgau
Telefon: +49 761 389130
E-Mail: oliver.gaeng@cryptshare.com
Web: www.cryptshare.com