Vertrauliches wieder als Brief schicken???

17.05.2018 17:03 CEST

Über den Unterschied von geknackt und angreifbar – ein Interview zu EFAIL

Aktuell grassieren unter dem Stichwort ‚efail' Meldungen, die die Wirksamkeit von verschlüsselter Kommunikation prinzipiell in Frage stellen. Als Experte für dieses Thema möchte procilon zur Aufklärung einen Beitrag leisten. Dazu einige Fragen an Oliver Kube, Leiter Qualitätssicherung der Leipziger Unternehmensgruppe.

F: Herr Kube, verzichten Sie ab sofort auf verschlüsselte E-Mails?

OK: Natürlich nicht! Vertrauliches gehört nach wie vor nicht auf eine

Postkarte. Außerdem kann von geknackter E-Mail-Verschlüsselung nicht die Rede sein. Die für die Verschlüsselung genutzte Technologie ist weiterhin sehr sicher. Unsere erste Analyse der inzwischen unter https://efail.de veröffentlichten Angriffsvektoren hat ergeben, dass vielmehr eine Schwachstelle bei E-Mail-Programmen, konkret der E-Mail-Clients, Ziel von Cyber-Attacken werden könnte.

F: Wie sieht sowas konkret aus?

OK: Ich will es mal anschaulich beschreiben: Sie sind Getränkehersteller und erhalten von einem Forscher eine geheime, erfolgversprechende Rezeptur. Der Forscher schickt seine Rezeptur mit einem versiegelten Brief (verschlüsselte E-Mail) direkt an Sie. Auf dem Postweg (über das Internet) gelingt es dem Spion eines anderen Getränkeherstellers einen Spionageroboter an den versiegelten Briefumschlag zu heften. Wenn Sie nun den Briefumschlag öffnen, ohne zu prüfen, was alles noch am Briefumschlag hängt (Integritätsprüfung), kann der Spionageroboter heimlich ein Bild von der geheimen Rezeptur schießen, wenn Sie diese aus dem Briefumschlag genommen haben (entschlüsseln). Mit diesem Bild macht sich dann der Spionageroboter auf den Weg zu seinem Auftraggeber. Der kann das Geheimnis ohne weitere Mühe einfach mitlesen.

Der Spion muss sich also gar nicht die Mühe machen den versiegelten Brief zu öffnen (die Verschlüsselung zu knacken), sondern braucht nur ein wenig Geduld und muss hoffen, dass er nicht entdeckt wird. Wie man an diesem Beispiel sieht, besteht das Problem nicht beim sicheren Transport des Briefes (der verschlüsselten E-Mail), sondern entsteht erst bei der sorglosen Öffnung.

F: Besteht diese Gefahr bei allen E-Mails?

OK: Nein. Das Problem besteht hauptsächlich dann, wenn sog. aktive Inhalte aus dem Internet nach der Entschlüsselung geladen werden.

Um bei unserem Spionageroboter zu bleiben, kann man sich das etwa so vorstellen : wenn er beim Adressaten des versiegelten Briefes angekommen ist, muss er erst einmal nachschauen, wo er ist und wie er zu seinem Auftraggeber zurückkommt. Dazu beschafft er sich z. B. eine Karte und ein paar Hilfsmittel aus einem Versteck. Ohne diese hat er keine Chance.

F: Und, um auch im Bild zu bleiben, was heißt das für den Getränkehersteller (Anwender)?

OK: Nun zum einen rate ich ihm prinzipiell seine Post auf Unversehrtheit (Integrität) zu prüfen. In unserem Sprachgebrauch ist das dann E-Mail-Signatur und entsprechend protokollierte Prüfung.

Zum anderen sollte der Getränkehersteller den Rückweg des Spionageroboters verstellen.

Wieder in unsere Welt übersetzt. Es kann erst mal nicht viel passieren, wenn man z.B. Bilder in HTML-Mails, die oft erst einmal als Link eingefügt sind und entweder automatisch (oft bei Mobile-Clients) oder nach „Klick“ nachgeladen werden, verzichtet. Sieht nicht schön aus, ist aber in der aktuellen Gefährdungslage sicherer.

Darüber hinaus sind natürlich die Hilfsmittel, die der Getränkehersteller benutzt um seine Post zu öffnen und zu verwalten (E-Mail-Clients) gefragt eine „Spionageroboterüberprüfung“ zu machen.

Mit anderen Worten: ein E-Mail-Client-Update ist dringend empfohlen, sobald es verfügbar ist.

Natürlich sollte er sich generell bei der Implementierung einen Experten für Informationssicherheit hinzuziehen. Wir helfen da auch gern weiter.

F: Wenn wir nun die Welt der geheimen Rezeptur verlassen, gibt es für procilon Handlungsbedarf?

OK: Natürlich haben wir uns die Angriffsvektoren nach der Veröffentlichung sehr genau in Bezug auf unsere proGOV-Plattform angeschaut. Die Ergebnisse sind inzwischen auf unserer Web-Site unter https://www.procilon.de/support/infos veröffentlicht. In unserem System sehen wir keinen direkten Handlungsbedarf. Aber wir werden unseren Kunden im integrierten Regelwerk Hilfsmittel zur Verfügung stellen, die sie bei der Identifizierung solcher Angriffe unterstützen. Damit kann jeder Anwender individuell nach eigener Policy Gegenmaßnahmen ergreifen.

Seit Jahrzehnten gilt die procilon GROUP als verlässlicher Ansprechpartner, wenn es um den Auf- und Ausbau einer sicheren digitalen Kommunikation im deutschen Rechtsraum geht.

Sowohl Unternehmen als auch Behörden setzen zur sicheren Identifizierung, Übertragung und Aufbewahrung ihrer Daten auf Lösungen der Anbietergruppe. Ihr SaaS- und On-Premises-Portfolio ermöglicht es ihnen, digitale Inhalte sicher, niederschwellig, vertraulich, nachvollziehbar und beweisbar zu signieren, auszutauschen und zu archivieren. Die Stärke der procilon GROUP-Produktpalette basiert dabei zum einen auf der strikten Einhaltung deutscher und europäischer Richtlinien und Vorgaben, zum anderen auf dem Einsatz kryptografischer Spitzentechnologien made in Germany, sowie – last but not least – auf seiner Cloud First-Strategie.

Ein wichtiges Mitglied der Anbietergruppe ist die intarsys GmbH. Sie entwickelt und vertreibt qualitativ hochwertige und technologisch führende Softwareprodukte und -komponenten zur Erzeugung und Prüfung von elektronischen Signaturen, Siegeln und Zeitstempeln sowie zur beweissicheren Langzeitarchivierung von digitalen Dokumenten.

Gemeinsam haben es sich die Mitglieder der Anbietergruppe zum Ziel gesetzt, die procilon GROUP zu einem der führenden deutschen Anbieter elektronischer Vertrauensdienstanwendungen auszubauen.

Sie möchten mehr über die procilon GROUP erfahren? Klicken Sie hier – oder abonnieren Sie den procilon Newsletter.

Kontaktpersonen

Kafka Kommunikation GmbH & Co KG
Pressekontakt
Dr. Torben Gülstorff
procilon@kafka-kommunikation.de
+49 (0) 89 7474705824