Kundeninformation zu EFAIL

Möglicherweise haben Sie bereits von *Efail* (*https://efail.de*) gehört und fragen sich nun, ob die Kommunikation über DICOM EMAIL davon betroffen ist?

Das wichtigste zuerst - wir können Ihnen versichern, dass der Datenschutz und die Datenintegrität der im Westdeutschen Teleradiologieverbund übermittelten Daten davon nicht betroffen und somit die Daten auch nicht gefährdet sind. Die von VISUS erstellte *DICOM MAIL Software* ist gegen diesen Angriff *immun*.

Was steckt hinter Efail?

Den Autoren des Papers *„Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels“* (https://efail.de/efail-attack-paper.pdf) ist es gelungen, mittels OpenPGP (DICOM EMAIL) beziehungsweise S/MIME verschlüsselte Emails so zu manipulieren, dass es für einen Angreifer möglich wird an Informationen aus dem verschlüsselten Teil solcher Emails zu gelangen.

Dazu verschickt ein Angreifer manipulierte Emails und lässt das Opfer diese Emails entschlüsseln. Dies geschieht durch den erneuten Versand bereits schon einmal versendeter Nachrichten oder Teilen daraus. Zur Durchführung des Angriffs benötigt der Angreifer daher vom Opfer bereits in der Vergangenheit verschickte Emails. Durch die Manipulation wird das Emailprogramm des Opfers angehalten, die entschlüsselten Emailanteile im Hintergrund an den Angreifer im Klartext zu übermitteln.

Für einen erfolgreichen Angriff müssen demnach die beiden folgenden Voraussetzungen erfüllt sein:

1.) Der Angreifer muss bereits im Besitz der verschlüsselten Mails sein, die er dechiffriert haben möchte
2.) Das Opfer muss die präparierten Emails durch ein Email Programm öffnen, der das automatische Nachladen von Bildern erlaubt und eingestellt hat.

Warum ist nun DICOM EMAIL nicht davon betroffen?

Zunächst ist es für einen Angreifer nur *extrem schwer* möglich überhaupt an die verschlüsselten Emails *heranzukommen*. Sämtliche Email Kommunikation des Westdeutschen Teleradiologieverbundes erfolgt *ausschließlich* über *verschlüsselte Protokolle*. Das bedeutet, dass selbst beim Abhören der Internetverbindungen ein *Angreifer* nur einen *verschlüsselten Datenstrom* erhält mit dem er in der Regel nichts anfangen kann.

Sollte der Angreifer dennoch aus irgendeinem Grund an diese verschlüsselten Nachrichten gelangen und sie manipuliert erneut versenden, spielt das für die DICOM Email Gateways überhaupt keine Rolle.

Die Software der DICOM MAIL Gateways verfügt nicht über die für den Angriff benötigten Funktionen.

Dementsprechend kann *Efail* auch *keinen Schaden* anrichten. Der Datenschutz und die Datenintegrität sind daher auch beim Empfang manipulierter Emails zu keinem Zeitpunkt in Gefahr.

Wichtig ist, dass Sie die OpenPGP Schlüssel der DICOM MAIL Gateways ausschließlich auf diesen nutzen.

Für die Verschlüsselung Ihrer *übrigen Email Kommunikation* verwenden Sie bitte *separate Schlüssel*. Denn selbst durch Efail ist es noch immer besser Emails zu verschlüsseln, als darauf zu verzichten.

Für Rückfragen wenden Sie sich bitte an
Herrn Hauke Scheer aus unserem Supportteam
email trv-support@visus.com
fon +49 234 93693-200