Cryptshare®
Making e-mail better

Comment

Efail: The problem is not e-mail, but the transport method.

An estimation of Matthias Kess, CTO of Befine Solutions AG, specialized in communication solutions

Freiburg im Breisgau, May 22, 2018: Security researchers have undermined encryption of e-mail systems and published details about security gaps in the two encryption methods PGP and S/MIME. Under certain conditions, e-mails can be decrypted, even subsequently. According to the researchers, this means that confidence in encrypted e-mails will probably be lost at least for the time being. Even worse, e-mail is no longer a secure communication medium. Should companies now, a few days before the entry into force of the basic European Data Protection Regulation, think about it? Yes! Is panic called for? No! There are good reasons for both.

Researchers at Münster University of Applied Sciences, Ruhr University Bochum and Leuven University in Belgium have discovered critical vulnerabilities in the decryption of S/MIME- and PGP-encrypted messages in e-mail clients. You can demonstrate how to access the decrypted content of an email with active content from HTML emails, such as a cleverly forged command to load external images.

E-mail: No longer a secure communication medium?

The attack scenario consists of embedding a new command in an encrypted e-mail, whereby the text is not only automatically decrypted by the recipient, but also automatically sent to the attacker. The scenario, which is based on shortcomings in the email client software, requires significantly less hacker know-how than you might expect.

The researchers' conclusion - that e-mail is not a secure communication medium - is nothing new for the time being. Which is good news and bad news at the same time. In principle, an e-mail corresponds to a postcard: it is cheap and fast to deliver, but its content can be read and modified by anyone who transports it. What happens on the transport route of the individual e-mails, which stations are involved, remains hidden from the user.

Encryption: Yes or no?

So should encryption be dispensed with in e-mail clients for the time being, as the researchers have advised? Wouldn't that be like leaving your front door open because there are too many burglary offences to complain about anyway?

No, no encryption is no solution either. The German Federal Office for Information Security (BSI) therefore also points out that OpenPGP and S/MIME could continue to be used securely if they were correctly implemented and configured. However, this requires activities by software vendors, standardization bodies and end users and is expected to take months in the sum of the necessary measures.

In general, we need to reconsider the point of encryption once again: in a few days' time, on 25 May, the basic European data protection regulation will finally come into force after a two-year transitional period. While in many cases the GDPR deliberately vaguely speaks of the "state of the art", as also in Article 32 ("Security of processing"), it explicitly requires the "encryption of personal data".

GDPR: What role does the encryption of personal data have?

Of course, this does not mean that companies may only communicate via encrypted e-mails. However, factors such as the need for data protection must be taken into account. The Regulation applies only to personal data, but other confidential data should also be protected. In order to protect patent secrets, research results or customer information, for example, encryption remains without alternatives.

According to a Bitkom survey presented a few days ago, three quarters of German companies cannot complete the implementation of the requirements in time - they now have no choice but to set priorities. E-mail encryption allows a comparatively small item in the list to be processed quickly.

"E-mail 2.0": Why are there weaknesses in the approach?

In general, e-mail plays a central role in the questions discussed so far: it has established itself as the main means of communication especially in the corporate environment for many years, is easy to use and universally available - and has long been a preferred target of attack by criminals, hackers and business-spy.

Demands for "E-Mail 2.0" have also been raised in the course of the current discussion. It would be better to speak of "SMTP 2.0". SMTP (Simple Mail Transfer Protocol) belongs to a small and selected group of universal standards that support business communication but are far behind today's security requirements. SMTP is a protocol that describes defined rules for how a certain process takes place - sending and forwarding an e-mail on the Internet. The e-mail passes through different hands, invisible to the user, and passes through several stations that can serve as potential targets for cyber criminals. This is the basis for certain types of attacks.

The other (transport) way

Cryptshare therefore uses a different (transport) route than S/MIME and PGP: The idea behind it is to overcome the disadvantages of the e-mail system and to take advantage of the benefits. The procedure is deliberately kept simple: The data to be transmitted in encrypted form - including the e-mail message - is uploaded and stored in encrypted form on a company server. The recipient is informed by e-mail only about the provision of his message and receives a unique password separately from the sender. This can take place in different ways - for example by telephone, letter, fax or personally. The user has control over the level of safety applied.

With the password he can download the data directly and encrypted from this server. The message and its attachments are automatically found in the recipient's e-mail client. There is no such thing as 100% security, not even here: But while several servers are involved in S/MIME and PGP, here it is only one - that of the company in whose data center the content of the received message is stored. The confidential message is therefore transmitted from e-mail client to e-mail client without an e-mail server or provider coming into contact with the sensitive information.

In addition, the size limits for file attachments are eliminated in this way, and all dispatch and reception processes are logged in full. Clear notifications to the sender of when emails and files have been sent and delivered to the intended recipient help companies to comply with policies and compliance requirements such as GDPR. This makes it easier to identify conspicuous activities in connection with e-mail communication.

Further infromation

Information on how the gap works and the associated research paper by researchers from the Münster University of Applied Sciences, the Ruhr University Bochum and the Belgian University of Leuven can be found here.

About Matthias Kess
Matthias Kess is CTO of Befine Solutions AG, based in Freiburg im Breisgau, which develops and sells communication solutions for companies.

About Cryptshare and Befine Solutions
The owner-managed Befine Solutions AG develops and supplies software solutions that help companies support, optimise, and secure their processes. Founded in the year 2000, the company with now over fifty employees has its headquarter and development site located in Freiburg im Breisgau, Germany. There are sales locations in the UK and the Netherlands. In 2017, a subsidiary in America was established: Cryptshare Inc.
The focus is on Cryptshare, a communication solution for the exchange of sensitive business information. It makes it possible to send and receive e-mails and large files ad-hoc – securely, easily and at low cost. Cryptshare also offers auditability which helps companies follow compliance rules and regulations. Today more than 1400 companies use Cryptshare with about 3 million users in over 80 countries. This success is underlined by the award of the “Cybersecurity Excellence Award 2017” to Befine Solutions AG.
Further information is available on www.cryptshare.com. Users may inform themselves on the blog.

Press contact:
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