syracom
business efficiency engineering

CYBER SECURITY AND REQUEST-TO-PAY

A new channel for issuing requests to pay

The new European Request-to-Pay (R2P) standard permits a payee to send a standardized payment request to the payer, for instance to his mobile device. The payer can approve or reject such a request for payment immediately. Strong client authentication must be ensured for this process to be safe. The approval then directly initiates a SEPA transfer without any additional inputs.

CHALLENGE

At the moment, your customers primarily receive payment requests as invoices in paper form or per e-mail. Recurring payments are also often implemented as direct debits. In the near future, Request-to-Pay can be used to request many of these payments directly from your customers via the banking infrastructure. This will not only provide more convenience and control when initiating payments, but will also present banks with completely new challenges in the area of cyber-security.

Fraud attempts involving payment transactions have increased significantly both online and offline in recent years. These include phishing, i.e. attempts to induce customers to enter their PIN and TAN on fake websites, or methods that directly induce bank customers to trigger payments, whether by sending fake invoices (spoofing) or social manipulation (social engineering).

EXAMPLE 1

A trickster pressures an accounting employee over the telephone to quickly make a payment on behalf of the managing director ("CEO fraud"). With Request-to-Pay, the fraudster can further lower the victim's inhibition threshold for payment.

Request-to-Pay now creates the new situation that bank customers can in principle receive a payment request from any bank account within the SEPA area. Since it is delivered via the banking infrastructure and displayed in secure online banking, it is generally considered more trustworthy than, for example, an e-mail. This increases both the risk for the customer of releasing fraudulent payment requests without careful examination and the risk for the bank of suffering damage to its reputation as a result.

EXAMPLE 2

An impostor buys lists of leaked account numbers on the dark net and sends fake payment requests via Request-to-Pay, which at first glance resemble those of a large biller and therefore look legitimate.

HOW WE CAN HELP

Step 1

CONCEPT

We check existing security measures and identify gaps.

Step 2

CONSULTING

We will advise you in a personal meeting and propose solutions for closing these gaps.

Step 3

IMPLEMENTATION

We use many types of cyber-security measures.

WHY SYRACOM?

syracom has many years of experience in the area of cyber security and banking. With a comprehensive network of partners, the consulting firm optimally bundles experts and know-how. syracom provides independent consulting to find solutions and sees itself as an integrated companion in the design and implementation of solutions. You benefit from comprehensive security know-how that includes social engineering as well as other essential components for increasing information security.

ABOUT SYRACOM

syracom is an independent business and IT consulting firm. We develop tailor-made, future-proof solutions with functional and technical know-how and guide our clients on their way through digital transformation: *business efficiency engineering* – safe, sustainable, efficient.

The consulting firm was founded in 1998 and is part of the Consileon Group.

Frank Hoffmann

Head of IT Security

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)
Phone: +49 6122 9176 0

frank.hoffmann@syracom.de
www.syracom.de