SPAM, SCAM, EXTORTION

October 2017

Probably everybody has heard about companies falling victim to scam attacks caused by e-mails sent by criminals with faked e-mail addresses asking to use a new bank account for the next transaction. When these instructions are followed, the money is usually lost. Scammers do this by gaining access to someone's daily business information, especially to the e-mail traffic of one party of a business relationship. This is done by "phishing" e-mails or other sorts of malware.

- Use System 5's Black & Whitelist
- Take "Faked Sender" warning seriously.
- Verify all bank account changes via phone
- Use complex passwords

Once the intrusion was successful, the attackers register an internet domain which looks very similar to the one used by the party who usually receives funds within this business relation. As a final step, they send an e-mail to the other party with instructions to use a new bank account for the next outstanding payment. This e-mail looks almost like a genuine one and references the correct business case - only the sending e-mail address is slightly different. You will have to look twice to spot the difference.

If you received a message from Mail@Systen5.de, would you spot the error during hectic business hours?

System 5 protects you!

- System 5 features a built-in **Black & White** List. The "Whitelist" contains e-mail addresses or domain names which you have actively acknowledged to be "good". E-Mails from these addresses will be routed to your journals. The "Blacklist" works the other way around, addresses on that list are considered as "bad" and won't be distributed.

- **Spam messages** are in-between. They cannot be ignored, but you have to be cautious. System 5 displays such messages in a separate journal. **Attachments and links are disabled automatically, the risk to install ransomware or other malware by opening attached files is reduced**. Someone in your organization with appropriate rights needs to decide whether this sender is "good" or "bad".

- It's technically quite easy to pretend to be someone else. An e-mail with a sending address Mail@System5.de, but with a "Reply To" address Mail@Systen5.de would look genuine to most available e-mail applications – but not to System 5. System 5 checks whether discrepancies between the "From" and "Reply To" address exist and warns you with a big red "p**ossibly faked Sender**" label when viewing the e-mail.