Watch out, Danger from Imposters!

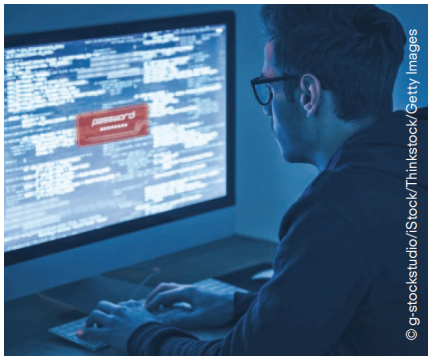
Corporates are vulnerable to attack at any time - from inside and outside. Payment transactions in particular are the target of cybercriminals. The right solution suite can help to protect the corporate. By Gregor Opgen-Rhein

In times of increased cybercrime, fraud prevention is a central task for every corporate. One of the most popular targets of attackers is and remains payment transactions. The reason: the promising profit margins. Attacks from "inside" must be catered for just as much as attacks from "outside", designed to gain media attention. Because even "dissatisfied" employees who open company accounts, change powers of attorney or close accounts without being noticed can cause considerable damage.

Companies have many ways to protect themselves against attacks on payment processes. The first pillar of any comprehensive security concept consists of technical precautions such as the encryption of all data streams and the use of anti-spyware programs. Organizational measures such as raising employee awareness of CEO fraud attempts and the introduction of a consistent dual control principle for manual payments and maintaining master data form the second pillar.

Keeping accounts in view

The third pillar comprises functional options, for example in administrative account management. The focus here is on both the corporate's own accounts and the accounts of its business partners. The highest level of security when opening and closing accounts and when changing powers of attorney and account numbers can be achieved through a structured, predefined process with distributed organizational responsibilities.


© g-stockstudio/iStock/Thinkstock/Getty Images

A cyber attack is one of the biggest dangers.

In addition, the bank details of the business partners are subject to further, much stricter regulatory requirements. In the light of the statutory money laundering and sanctions provisions, this is not just a matter of subjecting the business partner to an audit. The business partner's bank, or the payee, could also be on a list and must also be permanently and verifiably subject to sanctions screening.

At the same time, corporates should also check the beneficiaries of the payment files against a positive list in order to allow payments only to internal, pre-validated payees. This security measure against fake-president attacks protects the company's own employees who are the target of such attacks.

Another administrative measure to prevent losses is to monitor of account statements. For instance, if statements or transactions are missing, this could be due to technical errors at the bank delivery the details, but equally could be caused by deliberate concealment of suspicious transactions. A well-designed solution suite should uncover such suspicious items and provide the relevant warnings.

By combining of technical, organizational and functional measures, it is possible to link operational payment processes and administrative account management processes, including so-called denied party checks, to form a close-meshed network of fraud prevention.

Any solution suite for electronic Bank Account Management must support all these features for account lifecycle management and at the same time offer the opportunity to centralize, standardize and digitize sensitive processes. In this way, a corporate can protect itself from fraud attacks.

Translation of „Achtung, Betrüger!" in „DerTreasurer Printausgabe 4-2019"

Gregor Opgen-Rhein

Gregor Opgen-Rhein is Key Account Manager at Omikron Systemhaus in Cologne.

gor@omikron.de