German Competence Centre against Cybercrime e.V.

3 QUESTIONS FOR...RONNY WOLF, CASH SERVICES, FRAUD PREVENTION – COMMERZBANK

1. Mr. Wolf, what is meant by CEO fraud and how successful are the perpetrators?

The term "CEO fraud" denotes a procedure used by cyber criminals whereby the fraudster claims to be the boss of a company which he is in fact planning to defraud. By means of an (apparently) internal email, the fake executive confides a strictly confidential matter to a member of staff in "his" company. In order to gain the victim's confidence, a third person is introduced whose function is to monitor the contractual part. One of the two fraudsters then tells the staff member to instruct the bank to make a payment. The supposed reasons for this scenario can vary: a planned company takeover, fines due to public authorities, or an imminent tax fraud investigation within the firm.

The fraudsters insist on absolute discretion – and even threaten possible punishment. They manipulate their victims in writing and by telephone. Their aim is to secure large money transfers and if the ploy is successful it is repeated with the same victim until the swindle comes to light. Since 2013 criminals have pocketed around €150 million from German companies in just under 70 different cases. More than 180 reported attempts remained unsuccessful.

2. How can management advise personnel not to fall for these fraudulent tricks?

The most important thing is to teach staff about these fraudulent scenarios, so that they will recognize them if and when they occur. Companies should require employees to treat internal knowledge responsibly – and this also applies to the social media.

Those areas in which checks and controls are necessary can clearly be seen from the prevention and information measures that are taken. These controls must be carried out whatever the circumstances! This includes clear absence regulations if the CEO is not present in the company. Managers should instruct their personnel to use common sense when assessing an unusual situation which has arisen. This ensures that would-be fraudsters are thwarted before any damage can be done.

3. What can companies do if they have in fact been defrauded?

The first step is to get in touch with the company's bank immediately – especially if the payment has already been made. Companies can only be sure of recovering their money if it hasn't yet been booked to the recipient's account. Once the money has been lodged to their account, the only course available is to take legal action.

At the same time, it is important to undertake an inhouse investigation. The executives affected should only pass on the fraudulent emails to the police and their own IT department and should only use PDFs or printouts to give notice of the fraud internally. And a number of questions need to be answered: Have other members of staff received this email or telephone instructions? Is there possibly someone now working in the firm, in a subsidiary, or in the parent company who is taking instructions from the fraudster?

In many cases the staff member who triggered payment is wrongly suspected in the company of being some kind of "perpetrator". This simply serves to increase the degree of

mental stress, which is already extreme. Instead, it is advisable to provide the staff member with psychological support and to draw up a detailed report from memory, after which this person should only be involved in the affair to the extent required by the ongoing inquiry.

With this as with all other cybercrime activities, the rule must be: the more companies which share their experiences, the easier it will be for them to protect themselves against attacks in the future.