Ein ungewöhnlicher Zahlungsauftrag vom Chef? Besser nochmal nachfragen!

05.10.2017
von
Redaktion, Verbraucher

Immer wieder verleiten Betrüger Angestellte dazu, Firmengelder auf fremde Konten zu überweisen – mit einer perfiden Masche, dem „CEO-Fraud“. Der Bankenverband weist im Rahmen des European Cyber Security Month (ECSM) darauf hin, wie wichtig es ist, am Arbeitsplatz besonders aufmerksam zu bleiben.

Ungewöhnlich war die E-Mail schon, die Markus Schmidt (Name geändert), Buchhalter in einem mittelständischen Unternehmen, von der Führungsetage erhalten hat. Er solle die Überweisung einer hohen Summe auf ein Konto im Ausland in die Wege leiten, schreibt der Geschäftsführer, die Sache sei absolut vertraulich zu behandeln. Doch weil Schmidt regelmäßig E-Mails mit Überweisungsaufträgen von seinen Vorgesetzten erhält, schöpft er keinen Verdacht: Er gibt die Zahlung in Auftrag. Bald ist klar: Der Buchhalter ist auf eine üble Betrugsmasche hereingefallen – dem sogenannten CEO-Fraud.

„CEO“ steht für Chief Executive Officer, also Geschäftsführer; „fraud“ heißt „Betrug“. Kriminelle haben es dabei auf das Geld von Firmen abgesehen. Sie fälschen so geschickt Zahlungsanweisungen, dass selbst erfahrene

Kurzgefasst

„CEO-Fraud“ heißt die Betrugsmasche, mit der Kriminelle immer wieder Firmen um viel Geld bringen. Die Betrüger verleiten Angestellte durch falsche Informationen, die scheinbar von der Geschäftsführung stammen, zu Überweisungen auf fremde Konten. Der Bankenverband rät, ungewöhnliche Zahlungsaufträge gründlich zu prüfen.

Mitarbeiter manipuliert werden und Geld auf die Konten der Betrüger überweisen.

Dabei gehen die Gauner teils akribisch vor: Sie spionieren ein Unternehmen über einen langen Zeitraum aus, bis sie mit den internen Abläufen vertraut sind. Indem sie Bezug auf konkrete Geschäfte oder geplante Investitionen nehmen, gelingt es ihnen, Zahlungsaufträge sehr echt erscheinen zu lassen. Es gibt auch Fälle, in denen die eigentlich korrekte Bankverbindung des Empfängers durch die des Täters ersetzt wird („Mandate-Fraud"). Zum Beispiel, indem per E-Mail eine angeblich neue Bankverbindung eines Geschäftspartner bekannt gegeben wird.

Das müssen Sie tun, wenn Sie in die Falle getappt sind

Wenn klar ist, dass eine falsche Zahlung ausgelöst wurde, muss die Firma so schnell wie möglich handeln und die Bank informieren. Kreditinstituten gelingt es immer wieder, betrügerische Zahlungen zu stoppen – dies ist aber nur möglich, wenn diese dem Empfängerkonto noch nicht gutgeschrieben worden sind. Egal ob die Zahlung gestoppt werden konnte oder nicht: Firmen sollten unbedingt die Daten des Täterkontos an die Bank weitergeben und bei der Polizei Anzeige erstatten.

Ganz wichtig ist auch eine gute „Human Firewall". Unternehmen sollten ihre Mitarbeiter so gut schulen und für die Risiken sensibilisieren, dass Gauner möglichst keine Chance haben.

Die Firma von Markus Schmidt hatte Glück: Nachdem der Buchhalter die Überweisung seinem Chef bestätigt hatte, flog der Betrug auf – rechtzeitig genug, um die Zahlung aufzuhalten. Was Schmidt und seine Kollegen aus dem Vorfall gelernt haben: ungewöhnliche Aufträge für Geldtransfers im Vorfeld immer gründlich prüfen! Der Bankenverband rät: Scheuen Sie sich nicht, noch mal bei Ihrem Vorgesetzten nachzufragen und sich den Zahlungsauftrag bestätigen zu lassen.