German Competence Centre against Cybercrime e.V.

3 FRAGEN AN… RONNY WOLF, CASH SERVICES, FRAUD PREVENTION – COMMERZBANK

1. Herr Wolf, was ist ein CEO-Fraud und wie erfolgreich sind die Täter damit?

Ein CEO-Fraud – zu Deutsch „Chefbetrug“ – bezeichnet eine Vorgehensweise von Cyberkriminellen, bei denen sich der Betrüger als Chef der Firma ausgibt, an der er den Betrug plant. Hierbei betraut der „vermeintliche“ Vorgesetzte in einer scheinbar internen E-Mail einen Mitarbeiter „seines“ Unternehmens mit einer streng vertraulichen Angelegenheit. Um Vertrauen beim Opfer aufzubauen, wird eine dritte Person ins Spiel gebracht, die den vertraglichen Teil begleiten soll. Von einem der beiden erhält der Mitarbeiter dann eine Zahlungsanweisung, die er bei der Bank beauftragen soll. Die vorgetäuschten Hintergründe können verschieden sein: eine geplante Firmenübernahme, Strafzahlungen an Behörden oder aber auch eine Steuerfahndung im eigenen Haus.

Die Betrüger drängen auf absolute Diskretion – bis hin zu Strafandrohungen. Sie manipulieren ihre Opfer auf schriftlichem und telefonischem Weg. Das Ziel sind Überweisungen meist größerer Beträge und die Masche wird bei Erfolg am selben Opfer oft solange wiederholt, bis der Betrug auffällt. Seit 2013 erbeuteten Kriminelle so rund 150 Millionen Euro von deutschen Unternehmen in knapp 70 Fällen. Mehr als 180 gemeldete Versuche blieben erfolglos.

2. Wie kann man seine Mitarbeiter instruieren, damit sie nicht auf die Täter hereinfallen?

Das wichtigste ist die Schulung der Mitarbeiter zu Betrugsphänomenen, damit diese vom Mitarbeiter erkannt werden können. Firmen sollten von ihren Mitarbeitern einen verantwortungsvollen Umgang mit firmeninternem Wissen einfordern, auch in den sozialen Medien.

Maßnahmen zur Prävention und Aufklärung machen deutlich, wo Kontrollen erforderlich sind. Diese Kontrollen sind unter allen Umständen einzuhalten! Klare Abwesenheitsregeln, wenn sich der Geschäftsführer nicht im Haus befindet, gehören in jedem Fall dazu. Führungskräfte sollten ihre Mitarbeiter dazu anhalten, jede ungewöhnliche Situation mit ihrem gesunden Menschenverstand zu prüfen. Dann kommen viele Betrüger schon sehr früh in ihrem Prozess nicht weiter.

3. Was können Firmen tun, wenn der Schadensfall doch eingetreten ist?

An erster Stelle steht, sofort die Hausbank zu kontaktieren – insbesondere, wenn die Zahlung bereits getätigt wurde. Unternehmen können nur dann sicher sein, ihr Geld zurückzuerhalten, wenn dies dem Empfängerkonto noch nicht gutgeschrieben wurde. Nach einer Gutschrift greifen nur juristische Wege.

Gleichzeitig gilt es, interne Prüfungen einzuleiten. Betroffene Unternehmer sollten die Betrugsmails nur an die Polizei und die eigene IT weitergeben und zur Bekanntmachung des Betrugs im Haus nur PDFs bzw. Ausdrucke verwenden. Zugleich müssen die Fragen geklärt werden: Haben noch mehr Mitarbeiter diese E-Mail oder telefonische Anweisungen bekommen? Arbeitet vielleicht ein anderer Mitarbeiter im Unternehmen, in einer Tochter- oder Muttergesellschaft aktuell auch nach den Anweisungen des Täters?

Derjenige Mitarbeiter, der die Zahlung ausgelöst hat, bekommt im Unternehmen oft fälschlicherweise eine Art „Täterrolle“ zugeschrieben. Damit wird die ohnehin extreme psychische Belastung noch verstärkt. Stattdessen empfiehlt sich eine psychologische Unterstützung des Mitarbeiters und die Aufnahme eines Gedächtnisprotokolls. Danach sollte der Mitarbeiter im Vorgang möglichst nur soweit eingebunden sein, wie es die Situation noch erfordert.

Bei diesem wie bei allen anderen Cyber Crime-Aktivitäten gilt: Je mehr Unternehmen ihre Erfahrungen teilen, umso besser können sie sich vor weiteren Angriffen schützen.