CEO-Fraud

Enkeltrick 4.0 oder: Dringende Anweisung vom Chef

Freitagnachmittag, kurz vor Feierabend: Die Buchhaltung erhält eine E-Mail vom Chef. Kurzfristig muss eine höhere Geldsumme auf ein Konto ins Ausland transferiert werden. Es ist absolute Vertraulichkeit zu gewährleisten. Schließlich soll nun das lange geplante, bislang geheim gehaltene Projekt erfolgreich zum Abschluss gebracht werden. Die Zeit drängt.

So lässt sich die übliche Vorgehensweise der CEO-Fraud genannten Betrugsmasche grob beschreiben. Eine Person im Unternehmen, die berechtigt ist, Zahlungen zu tätigen, erhält per E-Mail eine Mitteilung. Der Absender gibt sich als Vorgesetzter, Geschäftsführer oder Vorstand aus. Die Person wird angewiesen, eine höhere Summe schnell und ohne weitere Personen zu informieren, auf ein Konto ins Ausland zu überweisen. Die Absenderadresse scheint auf den ersten Blick zu stimmen. Auch das Design der Mail stimmt mit dem aus der Chefetage überein.

Undenkbar, dass die Zahlungen dann auch tatsächlich erfolgen? Nein, leider nicht. Eine offizielle Statistik liegt zwar nicht vor, aber das Bundeskriminalamt hat Ende 2017 Zahlen bekanntgegeben, wonach eine Tätergruppierung von 2014 an rund 800 Versuche mit dieser Masche unternommen hat. Etwa 100 davon waren erfolgreich, so dass dadurch 175 Millionen Euro erbeutet wurden. Und das ist sicher nur die Spitze des Eisbergs.

Der CEO-Fraud unterscheidet sich elementar von den bislang bekannten Betrugsversuchen per Mail, die allein schon aufgrund der Tippfehler, der zugrunde gelegten Geschichte oder auch der Absenderadresse leicht als Fälschung zu erkennen waren. Die aktuelle Masche ist dagegen erheblich professioneller und zeitaufwändiger. Die Ziele werden genauer beobachtet, die Unternehmenswebseite ausgewertet und Informationen über Mitarbeiter bspw. durch Social-Media-Kanäle gesammelt. Dazu wird ausgekundschaftet, wer die Berechtigung für finanzielle Transkationen hat. In einigen Fällen wird sogar telefonisch vorab Kontakt aufgenommen, um weitere Details zu verifizieren. Dabei werden zum Teil Techniken eingesetzt, die den Angerufenen eine bekannte Rufnummer vortäuschen. Mit diesem Wissen ausgestattet, wird dann ein maßgeschneiderter Angriff ausgeführt, der nicht so einfach zu durchschauen ist.

Enkeltrick 4.0

Eine wichtige Komponente: Es wird Druck auf den Mitarbeiter ausgeübt, der die Transaktion veranlassen soll. So wird dieser in der Mail zur Verschwiegenheit verpflichtet und ihm bei Verstoß Strafzahlungen angedroht. Gerade in Betrieben, in denen der Austausch mit der Chefebene nicht gepflegt wird, trifft diese Herangehensweise auf fruchtbaren Boden.

Auch der Zeitpunkt spielt eine Rolle: Am Freitag, kurz vor dem Wochenende, muss die Zahlung noch schnell erledigt werden. Wenige Mitarbeiter sind noch am Platz, um ggfs. eine Kontrollfunktion zu übernehmen, manch einer möchte nach einer langen Arbeitswoche schnell ins Wochenende; das Anliegen wird nur oberflächlich geprüft und nicht hinterfragt. Dazu werden die Mailangriffe unter Umständen noch durch Telefonate flankiert, bei denen sich der Anrufer als Rechtsanwalt des Vorgesetzten ausgibt. Zum Teil wird dies in der ersten Mail bereits angekündigt. Dadurch wird noch einmal im persönlichen Gespräch auf die Notwendigkeit eines zeitnahen Handelns verwiesen und versichert, dass alles seinen rechtmäßigen Gang geht. Der Enkeltrick 4.0 sozusagen. Der hohe Aufwand der seitens der Kriminellen betrieben wird, erklärt sich mit der Höhe der Summen, die durch ein solches Vorgehen erzielt werden können. Laut Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden so in Einzelfällen bereits Schäden in Millionenhöhe realisiert.

Was können Unternehmen dagegen tun?

Die erste, wirksame Maßnahme ist fast schon trivial: Bei den Mails nicht auf den Antwortbutton klicken. Denn die Absenderadressen sehen den originalen zum Teil sehr ähnlich und variieren nur um einen oder wenige Buchstaben. Das wird dann schnell überlesen. Also besser bei entsprechenden Anfragen die Mailadresse händisch eingeben oder per Telefon die entsprechenden Anweisungen verifizieren lassen. Grundsätzlich sollten bestimmte Kontrollmechanismen installiert sein, so dass nicht eine Person alleine die Zahlungsanweisungen tätigen kann. Das Vier-Augen-Prinzip ist leicht umzusetzen und kann weiterhelfen. Auch für vertrauliche Projekte sollten Regelungen getroffen werden. Die Mitarbeiter im Unternehmen – vor allem in der Buchhaltung - sollten grundsätzlich hinsichtlich dieser Variante des Betrugs sensibilisiert werden. Ist das Unternehmen dann ins Visier eines solchen Angreifers geraten, gilt es zügig die Polizei zu informieren und Anzeige zu erstatten. Ziel ist es, den Täter zu ermitteln und zu verurteilen. Denn: Der Internetzugang in den Justizvollzugsanstalten reicht für kriminelle Handlungen in der Regel nicht aus.

IHK NRW – Die Industrie- und Handelskammern in Nordrhein-Westfalen e.V. führt zum sechsten Mal den IT-Sicherheitstag NRW durch, der am 4. Dezember 2018 von 09.00 Uhr bis 17.00 Uhr in der Historischen Stadthalle Wuppertal stattfindet. Der Fachkongress zum Thema Daten-, Informations- und IT-Sicherheit bietet für den Mittelstand mit Impulsvorträgen, parallelen Basic- und Expertenforen sowie Seminaren und einer begleitenden Fachausstellung an einem Tag alles rund um sicherheitsrelevante Themen. Zudem haben Teilnehmer in einer „Hack-Academy“ die Möglichkeit, sich in die Lage eines Angreifers zu versetzen und so ggf. Sicherheitslücken direkt zu erkennen. Die Teilnahme kostet 99 Euro inkl. MwSt. Alle weiteren Informationen und die Anmeldung gibt es im Netz unter: www.it-sicherheitstag-nrw.de

Jan Borkenstein, IHK zu Essen