carmasec

security. done. right.

Whitepaper 02/2020

CEO-Fraud:
So erkennen und vermeiden Sie den gezielten Unternehmensbetrug

Was ist ein CEO-Fraud?

„Fraud“ ist das englische Wort für Betrug und der CEO (Chief Executive Officer) ist die oberste Führungskraft eines Unternehmens. Wobei die Abkürzung CEO hierbei nur als Platzhalter dient, denn genauso können die Namen anderer Führungskräfte missbraucht werden. Alternative Bezeichnungen für derartige Betrugsmaschen lauten daher auch BEC (Business E-Mail Compromise), Bogus Boss E-Mail, FPF (Fake Presidental Fraud) oder schlicht und einfach E-Mail-Fraud.

Die Täter nutzen bei einem CEO-Fraud Informationen, die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Website oder in Werbebroschüren veröffentlichen. Die Betrüger legen ihr Augenmerk insbesondere auf Angaben zu Geschäftspartnern und künftigen Investments. Für das Beschaffen von Erstinformationen über das Unternehmen sind in erster Linie soziale Netzwerke eine Goldmine. LinkedIn ist für Betrüger besonders interessant, da dort Informationen über geschäftliche Beziehungen oder die Identität und Funktion von Mitarbeitenden zu finden sind. Sind die benötigten Daten nicht online verfügbar, kontaktieren die Betrüger direkt die Firma, um die Betrugsmasche trotzdem durchführen zu können.

Wie akut ist CEO-Fraud?

Die CEO-Fraud genannte Betrugsmasche, bei der Mitarbeiter großer Firmen dazu gebracht werden, erhebliche Geldbeträge auf ausländische Konten zu überweisen, entwickelt sich zum Massendelikt. Das zeigt die neunte Studie „Wirtschaftskriminalität“ der Wirtschaftsprüfungs- und Beratungsgesellschaft PwC, eine repräsentative Befragung unter 500 deutschen Unternehmen.

So berichteten 40 Prozent der befragten Firmen, sie seien innerhalb der vergangenen 24 Monate zumindest einmal zum Ziel einer CEO-Fraud Attacke geworden – wobei die Kriminellen in fünf Prozent der Fälle Erfolg hatten. Die durchschnittliche Schadenssumme dieser Angriffsmethode, die technische Elemente mit dem sogenannten „social engineering“ kombiniert, liegt deutlich höher als bei der typischen Cyber-Kriminalität. Das FBI schätzt, dass durch genannte Attacken jährlich knapp 3 Milliarden Dollar den Besitzer wechseln – mit zum Teil gravierenden Folgen für das betroffene Unternehmen. In einer Vielzahl von Fällen waren die Täter jedoch nicht erfolgreich, da die kontaktierten Mitarbeiter aufmerksam waren und sich von den professionell vorgehenden Tätern nicht täuschen ließen.

Wie läuft eine CEO-Fraud-Attacke ab?

Zu den gesuchten Daten gehören hauptsächlich die Mailadressen der Mitarbeitenden in der Buchhaltung, die am Ende die Zahlungen für die Betrüger vornehmen sollen. Mit den Angaben aus diesen Erstkontakten werden dann gezielte E-Mails mit für das jeweilige Unternehmen plausiblen Angaben verschickt. Für den Versand von E-Mails, die auf den ersten Blick täuschend echt scheinen, verwenden die Betrüger häufig unternehmensähnliche Domainnamen. Auch ein Berater oder eine falsche oder kompromittierte Anwaltskanzlei sind ebenfalls oft Teil des Szenarios.

AUF EINEN BLICK

- CEO-Fraud bezeichnet eine Betrugsmasche, bei der Mitarbeiter von einem vermeintlichen CEO angewiesen werden, Geldbeträge auf ausländische Konten zu überweisen
- Kriminelle recherchieren Daten über ein Unternehmen und geben sich bei Mitarbeitern aus Buchhaltung oder ähnlichen Abteilungen als Geschäftsführer aus
- CEO-Fraud ist ein sehr relevantes Thema - das FBI schätzt, dass jährlich durch diese Art von Betrug 3 Milliarden Dollar den Besitzer wechseln
- CEO-Fraud betrifft große, aber auch mittelständische und kleine Unternehmen
- Häufig treten die Betrüger via Mails an Mitarbeiter heran und versuchen so sozialen Druck aufzubauen und technische Schwächen auszunutzen
- Unternehmen können entgegenwirken, indem sie Mitarbeiter sensibilisieren, öffentliche Unternehmensinformationen überprüfen, klare Regelungen und Kontrollmechanismen schaffen sowie Hilfe von Profis einholen

So haben die Täter die Möglichkeit, mit Mitarbeitenden Kontakt aufzunehmen und sich als Leitende Angestellte, Geschäftsführer oder Handelspartner auszugeben. Dabei fordern sie z.B. unter Hinweis auf eine angebliche Unternehmensübernahme oder angeblich geänderte Kontoverbindungen den Transfer eines größeren Geldbetrages auf Konten in China und Hong Kong, aber auch in osteuropäischen Staaten.

Die Kontaktaufnahme erfolgt in der Regel über E-Mail oder Telefon, wobei E-Mail-Adressen verfälscht und Telefonnummern verschleiert werden. Als Alternative zur E-Mail werden auch immer wieder gefälschte Briefe verschickt. Dazu wird das offizielle Briefpapier eines Unternehmens ebenso kopiert wie zum Beispiel ein Stempel. CEO-Fraud-Täter recherchieren nicht nur die Namen der Führungsriege, sondern auch den Aufbau ihrer E-Mail-Adresse, ihren Schreibstil, die Signatur usw.

Die Strategie der Betrugsmasche ist klar auf die Umgehung bzw. unautorisierte Nutzung von vorhandenen Prozessen durch geschickte Täuschung eines Mitarbeiters der Abteilung Finanzen oder der Buchhaltung ausgelegt. Der soziale Druck auf Mitarbeitende ist hierbei keineswegs nebensächlich - in der Nachricht des vermeintlichen CEO wird oftmals betont, dass die Angelegenheit streng vertraulich sowie besonders zeitkritisch ist. Außerdem wird gewarnt, dass die erhaltene E-Mail nicht mit dem direkten Vorgesetzten besprochen werden darf, da geheime Informationen wie beispielsweise eine Firmenübernahme o.ä. unter Verschluss bleiben müssen. Es handelt sich hierbei also einerseits um ein technisches Delikt, andererseits aber auch um die Manipulation von Menschen. So machen sich Kriminelle gleich zwei potenzielle Schwachstellen von Unternehmen zunutze.

Was können Unternehmen tun?

Auch wenn das Angriffsmuster selbst nicht neu ist, so ist dennoch Dynamik rund um dieses Risiko entstanden. Bei Versicherungsunternehmen rangiert der CEO-Fraud auf den obersten Rängen der aktuellen Betrugsszenarien. Einige Versicherungsunternehmen reagierten mit der Anpassung ihrer Bedingungswerke auf das erneute Aufflammen der alten Betrugsmasche.

Der Gestaltung sicherer Zahlungsprozesse fällt in Unternehmen daher eine entsprechende Bedeutung zu. Aktuelle Diskussionen sind nach wie vor zu stark auf die eher trivialen Angriffsszenarien fokussiert. Der besonderen Situation eines in den Vorfall involvierten Mitarbeiters wird damit nicht ausreichend Rechnung getragen.

CEO-Fraud-Attacken werden oftmals nicht erkannt, da Kriminelle versuchen möglichst perfekte Fälschungen zu versenden, die weder auf den ersten noch auf den zweiten Blick von Mitarbeitenden erkannt werden können. Das wird mit der „Angst“ der Mitarbeiten-

den vereint, die Entscheidungen des obersten Chefs zu hinterfragen. Ein Angestellter aus der Buchhaltung kann sich nicht leisten, bei jeder Zahlung, die er buchen soll, viele Fragen zu stellen, statt unverzüglich der Aufforderung nachzukommen. Zudem gelten für Führungskräfte oft Ausnahmen von der Regel. Der CEO selbst wird in vielen Unternehmen keinen Kostenantrag stellen oder von anderen Personen freigeben lassen müssen. Wenn er sagt, dass Summe X an Partei X gezahlt werden soll, wird das auch so gemacht. Besonders gefährdet sind daher vor allem Unternehmen, in denen noch sehr hierarchische und von Autorität geprägte Strukturen bestehen.

Diese Unternehmen wurden Opfer von CEO-Fraud:

Die Redaktion des IT-Magazins t3n berichtet allerdings in ihrem Artikel „Bitte zahlen. Gruß, Chef" detailliert, wie sie selbst Opfer einer CEO-Fraud Attacke wurde. Im Jahr 2016 wurde außerdem der bayrische Automobilzulieferer Leoni AG durch E-Mail-Fraud um 40 Millionen Euro erleichtert. Noch einmal zehn Millionen mehr kostete eine solche Attacke den Luftfahrtzulieferer FACC. In dem Beitrag Safer Internet Day: Christina und der vermeintliche CEO zeigt sich außerdem, dass ein CEO-Fraud auch kleine und mittelständische Unternehmen treffen kann und nicht ausschließlich Summen in Millionen- oder Milliardenhöhe gefordert werden.

Prinzipiell kann aber jedes Unternehmen Opfer einer CEO-Fraud Attacke werden. Um aber die Gefahr zu minimieren oder entsprechende Angriffe zu erkennen, bevor Zahlungen angewiesen werden, beachten Sie die folgenden Tipps:

1. Mitarbeiter sensibilisieren

Der Faktor Mensch ist immer noch ein Risiko, das keine Sicherheitssoftware der Welt lösen kann. Informieren Sie Ihre Mitarbeiter daher in regelmäßigen Abständen über aktuelle Betrugsmaschen und erstellen Sie einen Sicherheitsleitfaden, den jeder Angestellte lesen muss. Die Maßnahme sollte rollenspezifisch sein und zumindest Geschäftsführung, höheres Management und Mitarbeiter der Abteilung Finanzen und der Buchhaltung sprichwörtlich an einen Tisch bringen.

Entscheidend im Rahmen der Schulungsmaßnahme ist die moderierte Diskussion – idealerweise einschließlich Rollenspiel – der psychologischen Eigenschaften eines Angriffsszenarios. Durch die unmittelbare emotionale Erfahrung wird das Problembewusstsein aller Teilnehmer geschärft und mögliche Barrieren durch Hierarchien werden abgebaut.

Im Ergebnis sollte das Bewusstsein dafür geschärft werden, dass es sich um ein komplexes Angriffsszenario handeln kann, dessen Vorbereitung möglicherweise über einen längeren Zeitraum stattfindet.

2. Öffentliche Unternehmensinformationen überprüfen

Achten Sie in diesem Zusammenhang außerdem darauf, welche Informationen über Ihr Unternehmen öffentlich sind und was Sie und Ihre Mitarbeiter*innen im Zusammenhang mit Ihrem Unternehmen publizieren.

3. Klare Abwesenheitsregelungen und interne Kontrollmechanismen schaffen

Hierbei kann die Etablierung eines Freigabekonzepts für Zahlungen nützlich sein. Bedeutet: Egal ob die weitergeleitete Rechnung oder Zahlungsanweisung vom CEO oder vom Praktikanten kommt – die Buchhaltung muss jeden einzelnen Fall prüfen. Am einfachsten geht das, wenn sich das Prinzip des vier Augen Prinzips zunutze gemacht wird. Beispiel: Der CEO leitet der Buchhaltung per E-Mail eine hohe Rechnung weiter; der Mitarbeiter sucht den CEO entweder persönlich auf, um sich die finale Freigabe zu holen oder schickt ihm eine SMS auf sein Firmenhandy. Damit nicht das gesamte Unternehmen im Freigabeprozess-Chaos untergeht, legen Sie eine Mindestsumme fest, ab der eine zweite Freigabe eingeholt werden muss (zum Beispiel 5.000 €). Besonders wichtig: E-Mail-Absender prüfen. Schon die kleinste Abweichung in der E-Mail-Adresse ist ein Zeichen dafür, dass am anderen Ende nicht die eigene Führungskraft, sondern ein Betrüger sitzt.

4. Vermeiden von öffentlichen WLAN-Netzen

Besonders Führungskräfte sollten die Nutzung öffentlicher WLAN-Netze nach Möglichkeit vermeiden. Über sogenannte Fake-Access-Points verschaffen sich Cyberkriminelle nämlich nur allzu gern Zugang zu mobilen Geräten.

5. Hilfe von Profis einholen.

Cybersicherheit ist ein hochspezielles Kompetenzfeld, das Expertenwissen bereithält. Daher ist es sinnvoll, Unterstützung von Profis einzuholen, die Schwächen im Unternehmen feststellen können und Lösungen mitbringen. CEO-Fraud-Attacken zeigen, dass die Herausforderungen nicht nur in der IT eines Unternehmens liegen. Im Fokus stehen auch die Optimierung von Prozessen sowie die Schulung von Mitarbeitern und Führungskräfte.

Auch Carsten Marmulla, Partner der Beratungsboutique carmasec im Themenfeld Cybersicherheit und Datenschutz, empfiehlt, Fragen rund um das Thema Cybersicherheit außerdem mit professioneller Hilfestellung anzugehen. Ein Geheimtipp von ihm: „Wir arbeiten mit der Awareness-Plattform SoSafe zusammen, um interessierten Kunden effektiv und spielerisch die Themen der IT-Sicherheit näher zu bringen.“ Die E-Learning Module beinhalten praktische Anleitungen, ein Quiz und simulierte Angriffe, die Mitarbeitenden helfen, sich auf eine mögliche Bedrohung vorzubereiten.

Sie haben weitere Fragen zu dem Themenkomplex CEO-Fraud oder wünschen sich eine Beratung zur Cybersicherheit in Ihrem Unternehmen? Wir sind gerne für Sie da!

Carsten Marmulla
Jan Sudmeyer
Timm Börgers

carmasec
security. done. right.

IHRE ANSPRECHPARTNER

Carsten Marmulla
Managing Partner
Senior Trusted Advisor

Jan Sudmeyer
Managing Partner
Senior Trusted Advisor

Timm Börgers
Managing Partner
Senior Trusted Advisor

www.carmasec.com
xing.carmasec.com
contact@carmasec.com
twitter.carmasec.com
+49 (0) 201 426 385 900
linkedin.carmasec.com

Behalten Sie Ihre Cybersicherheit im Blick

Melden Sie sich für unseren Newsletter an:
www.carmasec.com/newsletter