Bild: Albert Hulm

„Überweisen Sie sofort 1,5 Millionen Euro“

CEO-Betrug in Deutschland

Ein wenig Social-Media-Recherche, einige gut gemachte E-Mails – und schon überweisen unbedarfte Mitarbeiter sechsstellige Summen an Kriminelle. Diese CEO-Betrug getaufte Masche ist die prominenteste Spielart von Business E-Mail Compromise und deutsche Unternehmen erleiden dadurch jährlich Schäden in zweistelliger Millionenhöhe. Was machen Unternehmen richtig, die diese Attacken erfolgreich abwehren konnten?

Von Uli Ries

Business E-Mail Compromise (BEC) bezeichnet Betrügereien, bei denen sich Kriminelle beispielsweise als Chef ausgeben, so Mitarbeiter täuschen und durch angeordnete Überweisungen hohe Geldbeträge ergaunern. Die CEO-Masche ist aber nur eine Variante von BEC. Die Charakteristika davon sind: Kriminelle geben sich per E-Mail als privilegierte Person – CEO, Anwalt, Kunde – aus und verlangen Informationen beziehungsweise Aktionen von Mitarbeitenden der Finanzabteilung.

Eine CEO-Betrüger-Mail an die Buchhaltung könnte etwa so aussehen: „Hallo XYZ, wir stehen kurz vor der Übernahme eines Unternehmens. Aufgrund Ihrer tollen Arbeit und Ihrer Diskretion werden Sie den buchhalterischen Teil des Projekts übernehmen. Viele Grüße, ZZZ.“

Wobei XYZ der Vorname eines existierenden Mitarbeitenden der Finanzabteilung des attackierten Unternehmens ist und ZZZ der Name des Geschäftsführers beziehungsweise Vorstandsvorsitzenden (CEO, Chief Executive Officer) oder des Finanzchefs (CFO, Chief Financial Officer). Absender der Nachrichten sind aber nicht CEO oder CFO, sondern Kriminelle, die zuvor zumeist per Social Media recherchiert haben, wie die Mitarbeiter in der Finanzabteilung heißen, und dann mit gefälschtem Absender im Namen von CEO oder CFO Anweisungen per E-Mail senden.

Allen Nachrichten gemeinsam ist, dass sie den Empfängern schmeicheln

(„Sie sind mir als besonders zuverlässige, leistungsfähige Kollegin in Erinnerung") und sie auf absolute Verschwiegenheit einschwören. Niemand im Unternehmen dürfe etwas vom „strategischen Projekt" wissen, an dem die Unternehmensführung derzeit arbeitet. Die jeweiligen Mitarbeitenden dürfen nur mit dem Absender – dem vermeintlichen Geschäftsführer oder Finanzchef – kommunizieren und das auch nur per E-Mail, keinesfalls per Telefon. Der Vertraulichkeit und – ironischerweise – besseren Dokumentation der Kommunikation wegen: „Compliance-Vorschriften, Sie verstehen sicher". Der wahre Grund ist aber ein anderer: Greifen die Angesprochenen zum Telefonhörer, um sich beim angeblichen Absender rückzuversichern, fliegt der Betrugsversuch sofort auf.

Keine Massenware

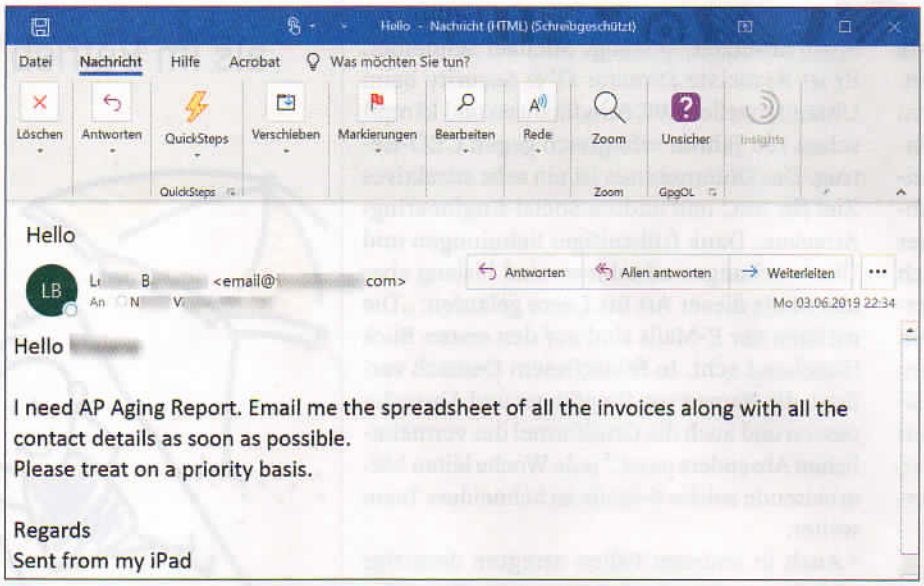
Da die betrügerischen E-Mails gezielt an einzelne Mitarbeitende gehen, haben Spam-Filter in der Regel keine Chance: Die Nachrichten verschwinden schlicht im Grundrauschen der täglichen E-Mail-Kommunikation. Dazu gesellt sich die soziale Komponente: Die Betrüger-Mails sind zumeist überzeugend formuliert und spielen durch die Mischung aus Schmeichelei, Geheimniskrämerei und Druck geschickt mit menschlichen Schwächen. Daher fallen Mitarbeiter immer aufs Neue auf den Betrug herein und klemmen sich hoch motiviert hinter die Überweisungsaufträge.

Dass die im Rahmen eines CEO-Betrugs verschickten E-Mails sich qualitativ vom üblichen Nigeria-Connection-, Viagra- und Dating-Spam absetzen, bestätigt Michael Schneider. Er ist Associate Director IT & Security beim Uhrenhersteller IWC Schaffhausen und kämpft schon seit Jahren erfolgreich gegen CEO-Betrug. Das Unternehmen ist ein sehr attraktives Ziel für BEC und andere Social-Engineering-Attacken. Dank frühzeitiger Schulungen und Überwachungsmaßnahmen sind bislang aber alle Mails dieser Art ins Leere gelaufen: „Die meisten der E-Mails sind auf den ersten Blick täuschend echt. In fehlerfreiem Deutsch verfasst, die Namen von Empfänger und Absender passen und auch die Grußformel des vermeintlichen Absenders passt." Jede Woche leiten Mitarbeitende solche E-Mails an Schneiders Team weiter.

- Auch in anderen Fällen erregten derartige Mails erst einmal kein Misstrauen. Sie griffen beispielsweise die im jeweiligen Unternehmen übliche Ansprache per Du oder Sie korrekt auf. Dies lässt auf Insider-Wissen schließen, wie es beispielsweise aus geleakten E-Mails gewonnen wird oder durch Trojaner-Infektionen. Wie eine Sprecherin des Bundeskriminalamts (BKA) gegenüber c't erklärt, nutzten Kriminelle in der Vergangenheit zur Vorbereitung ihrer Taten Informationen, die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Homepage oder in Werbebroschüren veröffentlichen. „Sie legen ihr Augenmerk insbesondere auf Angaben zu Geschäftspartnern und künftigen Investments", so die Sprecherin. Selbst Abwesenheitsmails seien von Interesse. Oder könnte sie/er die angefragten Daten selbst ohne großen Aufwand zusammentragen? Auch dann ist Vorsicht angesagt.
- An der Anrede und der Grußformel: Sind Absender und Empfänger per Sie, ist ein „Hallo XYZ" verdächtig. Das Gleiche gilt für die Grußformel: Unterzeichnet der echte Absender seine E-Mails mit seinem vollen Namen? Oder nur mit seinen Initialen oder dem Vornamen? Bei einer Abweichung hiervon gilt: Keinesfalls auf die E-Mail antworten.
- Rückfragen: Bevor Mitarbeiter finanzielle Transaktionen freigeben, sollten sie vorab immer persönlichen Kontakt zur Geschäftsführung suchen und explizit nachhaken. Das gilt auch bei der Preisgabe von brisanten Informationen nach außen.
- An der Absenderadresse: Klickt man auf „Antworten", zeigen E-Mail-Clients typischerweise neben dem Namen des vermeintlichen Absenders auch die E-Mail-Adresse an, von der die Nachricht stammt. Ist hier eine nicht zum Unternehmen gehörende Adresse zu sehen, sollte man aufhorchen. Angreifer können jedoch auch die wahre E-Mail-Adresse verschleiern, sodass dies kein allgemein gültiges Merkmal ist.
- An der Anfrage: Hat die betreffende Person jemals zuvor eine ähnliche Bitte gestellt?

CEO-Betrug erkennen und im Keim ersticken

Es gibt diverse Faktoren, anhand derer Mitarbeiter die Chef-Masche erkennen können:



Die Vorstufe für einen CEO-Betrug: So versuchen Kriminelle an Firmen-Interna zu kommen, um daraus überzeugende Betrüger-Mails zu stricken.

resse, da sich daraus die Systematik von Erreichbarkeiten herleiten lässt. Soziale Netzwerke, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben, sind laut BKA ebenfalls eine wichtige Informationsquelle.

Opfer: Google, Facebook und Bäcker

Die Liste der Arbeitgeber, deren Mitarbeiter auf die Masche reinfielen, ist lang und prominent besetzt. Den High Score aus Sicht der Kriminellen hat sicherlich der heute knapp 50-jährige litauische Betrüger Evaldas Rimasauskas inne: Er hat im Lauf von zwei Jahren gemeinsam mit unbekannten Komplizen Facebook und Google um über 120 Millionen US-Dollar gebracht. Und zwar durch eine weitere Variante des BEC: Die Betrüger gaben sich als Mitarbeiter eines legitimen Lieferanten der Opferunternehmen aus. In diesem Fall der taiwanische Computerhersteller Quanta Computer, der im wirklichen Leben wahrscheinlich maßgeschneiderte Server an die Internetgiganten liefert. Mittels fingierter Rechnungen und E-Mail-Adressen, deren Absender-Domain dem Original-Domainnamen ähnelte, erschlichen sich die Kriminellen gut 100 Millionen US-Dollar von Facebook und über 20 Millionen US-Dollar von Google.

Auch deutsche Unternehmen sind betroffen. So beispielsweise die in Südbayern bekannte Bäckereikette Hofpfisterei: Eine Buchhalterin überwies 1,9 Millionen Euro auf das Konto der Trickbetrüger bei einer Bank in Hongkong. Der Autozulieferer Leoni AG musste sogar 40 Millionen Euro abschreiben, die durch den CEO-Betrug den Besitzer wechselten. Wie ein Vertreter des Spezialversicherers Euler Hermes dem Wirtschaftsmagazin Capital sagte, bewegen sich die in Deutschland von Betroffenen gemeldeten Schadenssummen zwischen 750 000 und 15,5 Millionen Euro.

Die US-Bundespolizei schätzt, dass im Jahr 2018 weltweit 12 Milliarden US-Dollar durch CEO-Betrug ergaunert wurden. Auf Deutschland entfielen im Jahr zuvor dem jüngsten Bundeslagebild Wirtschaftskriminalität des BKA aus dem Jahr 2017 zufolge Schäden in Höhe von rund 24 Millionen Euro. Angesichts der latent hohen Dunkelziffer – viele Opfer erstatten aus Angst vor Imageverlust keine Anzeige – ist jedoch davon auszugehen, dass die tatsächliche Schadenssumme höher ausfällt. Das BKA ist überzeugt, dass sich an der steigenden Zahl der Straftaten, die im Versuchsstadium stecken bleiben, die Wirksamkeit der bisher seitens der Strafverfolgungsbehörden durchgeführten Sensibilisierungsmaßnahmen ablesen lässt. „In den dem BKA bekannten Erfolgsfällen konnte durch schnelles Handeln verschiedener Institutionen und der grenzüberschreitenden polizeilichen Kooperation verhindert werden, dass betrügerisch erlangte Gelder in Höhe von 26 Millionen Euro tatsächlich bei den Täter ankamen“, erläutert eine BKA-Sprecherin.

Die Variante: „Einmal alle Rechnungen, bitte“

Trotz eventuell niedrigerer Erfolgsaussichten versuchen es Täter nach wie vor. Bei IWC Schaffhausen schafften es in jüngster Zeit E-Mails in die Postfächer, die ebenfalls vermeintlich vom Finanzchef stammten. Sie baten jedoch nicht um Überweisungen im Rahmen einer Firmenübernahme, sondern um eine Aufstellung aller in den letzten vier Wochen eingegangenen Rechnungen. Warum das Ganze? Mittels dieser BEC-Variante gelangen Kriminelle an eine Übersicht der gelisteten Lieferanten und bekommen ein Gefühl dafür, in welchen Regionen sich die in Rechnung gestellten Leistungen befinden.

Diese Informationen sind unabdingbare Grundlage für den nächsten Schritt der Betrüger: Sie geben sich per E-Mail – ähnlich wie der litauische Kriminelle – als Mitarbeiter eines der viel versprechenderen Lieferanten aus und bitten um Änderung der beim Opferunternehmen gespeicherten Stammdaten. Konkret: die Bankverbindung. Kommt die Buchhaltung der Bitte nach, müssen die Trickbetrüger lediglich auf die nächste Rechnung des legitimen Lieferanten warten. Das Geld kommt dann automatisch auf ihr Konto. Typischerweise fliegt dies erst dann auf, wenn der eigentliche Lieferant die Überweisung anmahnt. Dass diese Methode selbst bei an sich gut informierten Unternehmen Erfolg hat, zeigt das Beispiel eines in Europa ansässigen Anbieters von Antiviren-Software: Die Buchhaltungsmitarbeiter schöpften keinen Verdacht und nahmen die Stammdatenänderung im SAP-ERP-System vor wie von den Kriminellen gewünscht.

Rüstzeug gegen CEO-Betrug

Wer einmal mit den Methoden hinter dem CEO-Betrug vertraut gemacht wurde, sollte das Muster künftig sofort erkennen. Daher ist das Informieren der Belegschaft über diese und andere Betrugsmaschen für Michael Schneider von IWC unabdingbar: „Wir betreiben seit einigen Jahren eine Informationskampagne rund um Cyber-Sicherheitsthemen. Im Rahmen dieses Awareness-Programms vermitteln wir beispielsweise durch Blog-Beiträge im Intranet oder Live-Hackings das Wissen, das zur Abwehr der entsprechenden Attacken nötig ist“, erläutert Schneider. Der IT-Sicherheitsverantwortliche ist überzeugt, dass die Belegschaft aufgrund der Schulungen hinreichend sensibilisiert

wurde, um Betrugsversuche zu erkennen und entsprechende E-Mails an die IT-Sicherheitskollegen weiterzuleiten. Finanziellen Schaden hat IWC durch CEO-Betrug laut Schneider jedenfalls bislang keinen erlitten.

Darüber hinaus müssen Unternehmen auch verbindliche Prozesse einführen, um den Betrugsversuch im Keim zu ersticken. Beispielsweise, indem sich Mitarbeitende der Finanzabteilung in jedem Fall telefonisch bei CEO, CFO oder den entsprechenden Assistenzen rückversichern, ob die Anfrage legitim ist.

Einen anderen Weg wählte Sonja Catani, Geschäftsführerin des schwedischen Tierbedarfsanbieters Hugo & Celine AB: Zu Anfang eines jeden Monats vereinbart sie mit den Mitarbeitern im Controlling mündlich ein Codewort aus dem Bereich Nahrung wie beispielsweise „Schokoladenspinat". Nur wenn sich dieses Codewort in einer per E-Mail an die Buchhaltung übermittelten Überweisungsaufforderung findet, geht das Geld raus.

Außerdem können Mitarbeiter laut Schneider schon vorab verhindern, dass betrügerische Nachrichten überhaupt in ihrem Postfach landen. „Die Kolleginnen und Kollegen müssen darauf achten, welche Daten sie von sich im Internet preisgeben. Also beispielsweise bei Facebook Details über Arbeitgeber, Aufgaben oder Geschäftsreisen öffentlich posten, sodass die Infos auch für Nutzer außerhalb ihres direkten Freundeskreises sichtbar sind", führt er aus.

Details über Reisen können missbraucht werden, um Mails an die Mitarbeiter in der Finanzabteilung glaubwürdiger aussehen zu lassen. Datensparsamkeit sollte auch für Profile bei den Business-Netzwerken LinkedIn und Xing gelten. Hier sollten keine Hinweise auf die spezifische Abteilungszugehörigkeit gegeben werden, um sich nicht selbst ins Fadenkreuz von CEO-Betrügern zu manövrieren. Der komplette Verzicht auf Profile in den Business-Netzwerken ist aber auch nicht zielführend: Denn dann könnten Betrüger Fake-Profile der Personen erstellen und in deren Namen mit echten Bekannten und Geschäftspartnern in Kontakt treten, um diese auszuhorchen.

Auch wenn CEO-Betrug kein technisch anspruchsvoller und ausgefuchster Angriff ist – Behörden wie das BKA sortieren die Masche in der Abteilung Wirtschaftskriminalität ein und nicht bei den Cyber-Verbrechen – so gibt es doch technische Abhilfe: Signieren Unternehmen alle E-Mails per S/MIME oder PGP, sind betrügerische Nachrichten schnell zu erkennen. Egal wie überzeugend der oder die vermeintliche CEO den Auftrag formuliert. *(des@ct.de)* c't