CEO-FRAUD – Die rechte Hand des Geschäftsführers erhält die Aufforderung per Mail kurz vor Arbeitsende an einem Freitag: Spätestens um 15.30 Uhr sollen 20 000 Franken als Anzahlung für eine neue Werkzeugmaschine auf ein Bankkonto in England überwiesen werden, schreibt der sich auf Geschäftsreise weilende Inhaber eines 50-Mann-Betriebs der Metallverarbeitungsbranche …

Der Fake-President-Trick

Cyberattacken bedrohen unsere KMU in der Schweiz zusehends. Leider ist es heutzutage nicht mehr die Frage *ob,* sondern *wann* man gehackt wird. Egal leider auch, ob es sich um einen kleinen Familienbetrieb, einen internationalen Konzern oder eine systemrelevante Institution handelt. Kleinste Nachlässigkeiten in der IT, Versäumnisse bei der Informationssicherheit oder ungenügende Awareness der Mitarbeitenden führen schnell zum Erfolg der böswilligen Hacker oder geldgierigen Kriminellen.

… Wenn das Geld nicht rechtzeitig überwiesen werde, erhalte die Konkurrenz den Zuschlag für die dringend benötigte Maschine, der Deal sei dann geplatzt. Der langjährige Angestellte verzichtet auf Rückfragen und zahlt das Geld übers E-Banking ein. Letztlich hat er die Kompetenz zur Auslösung der Zahlung für solche Beträge und es ist bereits 15.20 Uhr. Ausserdem hat er bis jetzt noch jeden Auftrag seines Chefs pflichtbewusst erfüllt und das Qualifikationsgespräch steht an …

Der Fake-President-Trick funktioniert leider immer wieder. Bild: 123RF

Der Schaden ist angerichtet

Fatal, wie sich am Montag früh herausstellt, nicht der Geschäftsführer, sondern ein unbekannter Internet-Betrüger hatte per Mail die Überweisung veranlasst. Der Schaden lässt sich nicht beheben, eine Strafanzeige bei der Polizei bringt kaum etwas und die Spur zum Konto in Grossbritannien lässt sich – wenn überhaupt – nur langwierig ermitteln. An die überwiesene Geldsumme kommt man nicht mehr heran. Wie sich Tage später herausstellt, wurde der Betrag bereits abgehoben und das Konto aufgelöst.

Mit raffinierten Methoden erzeugen Kriminelle Hektik und Druck, die Firmen zu einer Vielzahl von Fehlern verleiten können. Nachlässigkeiten sowie unkritisches und gutgläubiges Verhalten der Mitarbeitenden werden nicht nur bei der Industrie- und Wirtschaftsspionage ausgenutzt, sondern sind leider bestens geeignet zur schnellen und anonymen monetären Bereicherung.

Das Geld ist meistens verloren

Beim CEO-Fraud, auch Fake-President-Trick oder allgemein auch als Variante «Phishing Mail» bekannt, handelt es sich um eine Betrugsmasche, bei der sich Cyberkriminelle meist als Chef eines Unternehmens ausgeben und ihre Opfer in fingierten E-Mails dazu auffordern, hohe Geldsummen ins Ausland zu überweisen. Die Unbekannten erlangen vorgängig mittels Social-Engineering-Methoden *(vgl. sgz vom 23. April 2021)* jegliche Art von Informationen über die Firma und ihre Mitarbeitenden und adressieren danach sehr gezielt jene Mitarbeitenden, die Zugang zu sensiblen Daten haben oder berechtigt sind für Zahlungstransfers. Diese erhalten dann eine E-Mail, die den Namen eines eigenen Chefs als vermeintlichen Absender trägt. In der Nachricht wird meist eine dringliche, vertraulich zu behandelnde Transaktion angekündigt, für die eine umgehende Überweisung eines höheren Geldbetrags ins Ausland nötig sei. Einmal überwiesene Geldbeträge können meist nicht mehr zurückgeholt werden! Dieser Bedrohung sind wir aber nicht einfach schutzlos ausgesetzt. Es gibt einige Gegen- und Präventionsmassnahmen, vor allem im Bereich der Awareness, welche hochwirksam sind und mit wenig Aufwand angehoben werden können. In der nächsten Kolumne *(Ausgabe vom 18. Juni)* gehe ich praxisbezogen und konkret darauf ein.

Chris Eckert

DER AUTOR

Autor **Chris Eckert** ist Founding Partner der Swiss Business Protection AG und verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich und der Bundeskriminalpolizei.

www.fh-hwz.ch
www.swissbp.ch