

FALSCHHE CHIEFS UND FALSCHHE TECHNIKER WOLLEN GELD UND DATEN

„So blöd kann doch kein Mensch sein“, lautet schnell die Reaktion, wenn wieder ein Bericht veröffentlicht wird, dass Beschäftigte Geld auf fremde Konten überwiesen haben. Doch wer sich intensiver mit den einzelnen Fällen befasst, kommt häufig zu Erkenntnis, dass die Täter in vielen Fällen so geschickt vorgehen, dass man in dieser Situation möglicherweise auch falsch reagiert hätte. Damit es dazu nicht kommt, erfahren Sie hier, mit welchen Angriffsmethoden Kriminelle an das Geld und auch an Daten gelangen wollen.

Die Cheffalle – CEO Fraud

Bei der Cheffalle (CEO Fraud, CEO = Chief Executive Officer, Geschäftsführer/Vorstand) geht es im Prinzip darum, dass ein Beschäftigter mit Kontovollmacht vom vermeintlichen Vorgesetzten dazu gebracht wird, Geld zu überweisen. Der Weg der Kontaktaufnahme variiert dabei, wobei die meisten Angreifer bislang wohl häufig die Textform wählen und die Anweisungen per E-Mail senden.

Nun gab es aber die ersten Meldungen, dass die Täter mithilfe von Stimmenimitation per Telefon ihre Opfer kontaktiert haben.

Anruf vom vermeintlichen Chef: „Bitte Geld überweisen“

Wohl mit dem Einsatz von selbstlernender Software zur Imitation von Stimmen wurde ein Mitarbeiter eines britischen Tochterunternehmens vom vermeintlichen Chef aus Deutschland angerufen. Grund war eine angeblich dringende Überweisung, welche unbedingt noch ausgeführt werden sollte. Da eine Überweisung in Deutschland erst am nächsten Werktag ausgeführt werden würde, sollte das Geld vom Tochterunternehmen aus England überwiesen werden. Aufgrund der Zeitverschiebung sollte es somit möglich sein, die Überweisung am

beStock

© SurfupVector



damaligen Tag noch auszuführen. Nach der Mitteilung des Versicherungsunternehmens Euler Hermes landeten so 220.000 € auf einem Konto in Ungarn. Gut war nur, dass der Täter gierig wurde und später Fehler beging. Ansonsten hätte es kaum einen Nachweis über den Anruf gegeben.

Neue Technik – neue Möglichkeiten

Da die Stimmimitationssoftware aktuell am besten in Englisch funktioniert, sind Unternehmen mit Sitz oder Filialen in den nicht deutschsprachigen Ländern derzeit am ehesten bedroht. Es wird wohl aber nur eine Frage der Zeit sein, bis auch deutschsprachige Anrufe oder sogar gefälschte Videoanrufe möglich sind.

Täuschend echt: Täter nutzen interne Korrespondenz

Während einige Angreifer öffentliche Informationen, wie die Namen und Funktionen

>

der Ansprechpartner, nutzen, investieren andere mehr Zeit, um ihre Opfer zu überzeugen. So erhielt ein Buchhalter eine E-Mail von seinem vermeintlichen Chef mit der Bitte, Geld für eine Investition zu überweisen. In der E-Mail befand sich neben der Kontonummer des Kriminellen auch die alte und echte Korrespondenz zwischen dem Geschäftsführer und dem Steuerberater des Unternehmens, bei dem es um diese echte geplante Investition ging.

Kein Freund und Helfer: der falsche Techniker

Im Regelfall zielen die falschen Helfer darauf ab, an das Geld ihrer Opfer zu gelangen. Häufig verleiten sie ihre Gesprächspartner dazu, eine vermeintliche Schutzsoftware zu installieren, welche dann zum Kauf teurer Lizenzen führt, oder es handelt sich um Schadsoftware, welche z. B. die Daten auf dem Computer oder im Netzwerk verschlüsselt. Teilweise lassen sich die Täter einen Fernwartungszugang geben, um direkt die Schadsoftware zu installieren oder in gezielten Einzelfällen auch um Daten zu stehlen.

Zwischenzeitlich sind ganze Callcenter für Kriminelle aktiv, die sowohl Privatpersonen als auch Selbstständige und Unternehmen telefonisch kontaktieren. Die Anrufer geben sich häufig als Techniker von Microsoft oder einem Partnerunternehmen aus. Weigern sich die Benutzer, wird ihnen auch mit Konsequenzen, wie einer Meldung an die Polizei, gedroht. Als Grund wird dann beispielsweise genannt, dass die angebliche Schadsoftware auf dem Rechner des Benutzers die IT-Infrastruktur von Behörden angreife und der Benutzer mitverantwortlich gemacht werden könnte.

Opfer rufen die Täter an

Clevere Täter lassen sich zwischenzeitlich einfach von ihren Opfern anrufen. Dazu schalten diese beispielsweise Online-Werbeanzeigen, die wie Windows-Systemmeldungen aussehen. Nach dieser Meldung hat der Computer einen Virus und fordert den Benutzer auf, die Techniker unter der

angezeigten Rufnummer zu kontaktieren. Um den Eindruck zu verstärken, dass es sich um die Hotline von Microsoft oder Ähnlichen handelt, investieren die Täter auch in kostenfreie Service-Rufnummern.

Checkliste: Merkmale für einen Angriff

Merkmale	
Zeitdruck	●
keine Rückfragen	●
Vertraulichkeit	●
Druck durch Drohung	●

Durch den Zeitdruck soll möglichst wenig Zeit zum Überlegen und für eventuelle Rückfragen verbleiben, sofern diese nicht gleich sowieso ausgeschlossen werden. Zudem wird im Regelfall Vertraulichkeit eingefordert oder die Opfer werden unter Druck gesetzt, wenn sie die Anweisungen nicht befolgen.

Schutz mit individuellen Regelungen

Da allgemein gültige Regeln dazu führen würden, dass Kriminelle diese auch kennen und ausnutzen würden, sollten alle Unternehmen für sich eigene individuelle Regelungen treffen.

Wichtig für die Beschäftigten ist in allen Fällen, sich nicht unter Druck setzen zu lassen. Im Zweifel sollten bei Angriffen durch falsche Techniker die bekannten IT-Ansprechpartner kontaktiert werden. Bei verdächtigen Anweisungen durch vermeintliche Vorgesetzte, wie dringend Geld zu überweisen, sollte die bzw. der echte Vorgesetzte kontaktiert werden.

Bei der Kontaktaufnahme sollte ein anderer, möglichst von außen nicht bekannter und beeinflussbarer Kanal gewählt werden, z. B. ein persönliches Gespräch oder ggf. ein Anruf auf dem Mobiltelefon.