

30.04.2024

CEO-Betrug 2.0

Beim klassischen CEO-Betrug werden Mitarbeitende eines Unternehmens per E-Mail vom angeblichen Chef angewiesen, eine Zahlung sofort auszulösen. Dem Bundesamt für Cybersicherheit wurde nun ein Fall gemeldet, der noch einen Schritt weiter geht.

Der Fall, der dem Bundesamt für Cybersicherheit (BACS) gemeldet wurde, hebt sich von den bis jetzt bekannten Angriffen ab. Im Gegensatz zur üblichen Vorgehensweise wurde das Opfer nicht davon abgehalten, Kontakt mit dem Chef aufzunehmen. Stattdessen erhielt der Mitarbeitende mit direkter Zahlungsermächtigung einen Anruf von einem angeblichen Anwalt, der ihn zu einer Videokonferenz mit dem Chef einlud. Als der Mitarbeitende sich dann zur Konferenz einwählte, konnte er tatsächlich den vermeintlichen Chef auf dem Bildschirm sehen und mit ihm sprechen. Dieser versuchte ihn dann während dem Gespräch zu überzeugen, Finanztransaktionen auszulösen.

Das gefälschte Video des Chefs wurde mit Hilfe von Künstlicher Intelligenz (KI) erstellt. Es ist unklar, woher die Kriminellen das Material dafür bezogen haben. Es wird vermutet, dass öffentlich verfügbares Videomaterial zur Erstellung des sogenannten Deepfake-Videos genutzt wurde.

Eine weitere Möglichkeit, insbesondere zum Kopieren der Stimme, ist das Tätigen von Telefonanrufen im Vorfeld. So wurde in letzter Zeit von verschiedenen Unternehmen berichtet, dass Unbekannte telefonisch Informationen über das Unternehmen erfragt haben, die für gezielte Angriffe genutzt werden könnten. Mit der aufgezeichneten Stimme des Chefs ist es möglich, diesen mittels KI und Deepfake zu kopieren.

Der Vorfall zeigt, dass Kriminelle zunehmend das Mittel der Künstlichen Intelligenz (KI) nutzen, auch wenn deren Anwendung noch nicht perfekt ist. Im aktuellen Fall wurde der Betrug aufgedeckt. Die Betrüger beschränkten sich bei der Manipulation auf das Gesicht des Chefs. Die Kleidung entsprach nicht den Gewohnheiten des Chefs, und auch die Stimme war nicht besonders gut imitiert.

So erkennen Sie einen Deepfake:

- Lippenbewegungen sind nicht synchron zum Text
- Aussprachefehler
- Merkwürdige Formulierungen
- Schlechte Videoqualität
- Verwendetes Material aus anderem Zusammenhang

Weitere Informationen zu CEO-Betrug und insbesondere, wie Sie sich schützen können, finden Sie unter:

www.ebas.ch/ceofraud (<http://www.ebas.ch/ceofraud>)

Den Originalartikel des BACS finden Sie [hier](https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/wochenrueckblick_14.html) (https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/wochenrueckblick_14.html).