Betrug mit Computerstimme, die klingt wie der eigene Chef?

André Zand-Vakili

Hamburger LKA schildert, wie Betrüger Unternehmen am Telefon dazu bringen könnten, ihnen hohe Summen zu überweisen.

Hamburg. Mit neuester Computertechnologie versuchen Kriminelle offenbar, Unternehmen um hohe Summen zu betrügen. Davor hat jetzt das Hamburger Landeskriminalamt gewarnt. Die Polizei geht davon aus, dass die Betrüger schon bald eine spezielle Software einsetzen werden – diese ist in der Lage, bei Telefonanrufen jede beliebige Stimme nachzuahmen, etwa auch die von Unternehmenschefs.

Mehrere Firmen haben bereits solche Programme entwickelt, die bekannteste kommt von der kanadischen Firma Lyrebird. Der Name ist der eines australischen Vogels, der nahezu jedes Geräusch imitieren kann. Auch das Computerprogramm besitzt diese Fähigkeit: Hat es von einem bestimmten Menschen eine Stimmprobe, kann es beliebige Sätze so klingen lassen, als seien sie von ihm gesprochen.

Der Polizei macht die Technik große Sorgen

Andreas Dondera, Experte für Cybercrime im Hamburger LKA, nennt als Beispiel folgendes Szenario: Der vermeintliche "Chef" könnte einen

Buchhalter telefonisch anweisen, so schnell wie möglich eine hohe Summe auf ein Konto im Ausland zu überweisen. Ahnungslos führt der Mitarbeiter den Auftrag des "falschen" Vorgesetzten aus. Wenn der Betrug auffliegt, ist das Konto längst leer geräumt.

Das Vorgehen der Täter fällt für die Polizei unter den Fachbegriff CEO Fraud (Unternehmenschef-Betrug) – eine Masche, mit der Betrüger schon jetzt Millionensummen erbeuten. Bisher wurde hierbei per E-Mail kommuniziert. Die Täter spähen zunächst Firmen aus, um gezielt an Angestellte in der Buchhaltung heranzukommen. Diese werden dann angeschrieben. Dabei werden E-Mail-Adressen benutzt, die jener der Firma ähneln, oft ist nur ein Buchstabe anders. So wird das, was in der vermeintlichen Chef-E-Mail steht, auch ausgeführt.

2015 zählte das LKA 14 Fälle von CEO Fraud – in den ersten zehn Monaten des Jahres 2016 schnellte ihre Zahl auf 84 hoch. Seitdem liegt sie auf hohem Niveau. Bei der Polizei geht man davon aus, dass die Firmen nur einen Bruchteil der Fälle anzeigen. Laut Bundeskriminalamt sind es lediglich etwa 17 Prozent.

Was die Polizei Firmen und Mitarbeitern rät

Jede Firma ist von Cyberkriminalität bedroht. Da ist sich der Erste Kriminalhauptkommissar Andreas Dondera sicher. Oft fehlt allerdings bei Chefs und Mitarbeitern das Bewusstsein dafür. Das macht es den Tätern leicht. Andreas Dondera und seine Kollegen von der Zentralen Ansprechstelle Cybercrime sind deshalb unermüdlich unterwegs, um Unternehmen zu informieren. So wie beim Wirtschaftsverein für den Hamburger Süden, dort kamen sie im Ingenieurwerk in Wilhelmsburg zusammen. Die rund 100 Zuhörer waren in vielen Fällen überrascht, woher die Gefahr drohen kann. Einerseits ist es der unbekümmerte Umgang mit Daten. Kaum ein Mitarbeiter hat dafür ein Bewusstsein, dass er mit jedem Word-Dokument auch Meta-Daten mitschickt, die versierten Betrügern das Ausspähen von Firmen erleichtern. Gefahr droht aber auch von innen. In einigen Fällen haben sich bereits entlassene Mitarbeiter gerächt, indem sie ganze Netzwerke lahmlegten. Das kann Firmen in den Ruin treiben.

Der Code zur Entschlüsselung wird nur gegen Zahlung geliefert

Gefahr kommt aber auch aus Richtung der Konkurrenz, die gezielt die Rechner von Firmen überlasten. Das betrifft vor allem Betreiber von Internetshops oder von Bestellservices.

Gängig ist es zudem, durch eingeschleuste Programme alle Daten auf Rechnern, meist ganze Netzwerke, zu verschlüsseln. Der Code zur Entschlüsselung wird nur gegen eine Zahlung geliefert. Gezahlt werden muss immer in Bitcoin. Die Täter zu ermitteln, ist schwierig. Sie sitzen fast immer im Ausland und agieren unter falschen Identitäten. Zahlungen in Kryptowährungen lassen sich nicht nachverfolgen.

Darüber hinaus gibt es die herkömmliche Spionage, bei der es darum geht, an Firmengeheimnisse zu kommen. Die Täter können sich dabei in der Regel Zeit lassen. Durchschnittlich 210 Tage dauert es, bis ein Unternehmen bemerkt, dass es gehackt wurde. Der Tipp von den Cybercrime-Experten: Regelmäßig müssen Daten extern gesichert werden. Im Unternehmen sollte man zudem sorgsam mit Berechtigungen umgehen. Kommt eine Späh- oder Verschlüsselungssoftware über einen Mitarbeiter ins Firmennetz, kann sie nur auf die Bereiche zugreifen, auf die es auch der Mitarbeiter darf.