Als Chef getarnt fordern Internet-Kriminelle Geld von Firmen

Mit psychologischen Tricks machen sich Straftäter im Internet an zuvor gezielt ausgesuchte Mitarbeiter von Firmen heran. Es geht um Geld oder Geschäftsgeheimnisse. Das Social Engineering hat aber noch mehr Facetten.

Der Leiter des Rechnungswesens einer Büdinger Firma stoppte in letzter Minute eine Überweisung von mehr als 300.000 Euro. Er war kurz vor knapp misstrauisch geworden. Denn sein Chef, der vermeintliche Absender der Mail mit dem Überweisungs-Auftrag an eine Anwaltskanzlei in Luxemburg, war eigentlich im Urlaub. Und die E-Mail-Adresse hatte einen Schreibfehler.

Dieses Beispiel von versuchtem Betrug von Geschäftsleuten über das Internet hat die Polizei in Friedberg öffentlich gemacht. Die Masche ist nach Einschätzung von Fachleuten auf dem Vormarsch. Der Sprecher des Landeskriminalamtes (LKA), Christoph Schulte, warnt: "Das kann eine Firma in den Ruin treiben."

Beim Social Engineering verwenden Kriminelle persönliche Informationen aus dem Internet vor allem, um an Geld zu kommen, aber auch um Geschäftsgeheimnisse in Erfahrung zu bringen. Wie viele Fälle es im Jahr in Hessen ungefähr gibt, weiß allerdings niemand genau.

Keine Anzeige aus Scham

"So eine Mail an sich ist noch keine Straftat", erläutert die Sprecherin der Friedberger Polizei, Sylvia Frech. Solange es wie in dem Fall aus Büdingen gut ausgehe, wendeten sich viele Firmen deshalb erst gar nicht an die Polizei.

Aber auch viele geschädigte Unternehmen erstatteten keine Anzeige, heißt es beim LKA. Aus Scham oder wegen eines befürchteten Imageverlusts. Ebenso unklar wie das Ausmaß sei daher die Schadenshöhe, sagt Schulte. Oft ist der Schaden auch erstmal nicht zu beziffern, weil es um Geschäftsgeheimnisse oder -abläufe geht.

Unter Social Engineering fallen auch Täter, die am Telefon Passwörter oder interne Firmendaten ausspionieren wollen. Manchmal geht es ihnen nach Darstellung von Fachleuten dabei auch darum, Vorlieben der Angerufenen in Erfahrung zu bringen. Dann folgen als Informationen getarnte E-Mails, die mit Schadsoftware gespickt sind.

Online-Speisekarte als Einfallstor

Der Präsident des Bundesamtes für Verfassungsschutz, Hans-Georg Maaßen, nannte kürzlich noch ein anderes Beispiel. Dabei konnten sich Angreifer in eine Firma einhacken, weil sie die Online-Speisekarte eines italienischen Restaurants präparierten, das der Chef des Unternehmens gerne besucht. Als dieser dann noch seinen privaten Rechner für dienstliche Zwecke nutzte, war es zu spät.

Ein Beschäftigter einer Friedberger Firma war sofort skeptisch, als er eine Mail seines Vorgesetzten bekam, in der es um ein angeblich sehr geheimes Dossier zur Übernahme einer ausländischen Firma ging. Von einem Geheimhaltungsvertrag war die Rede, der Mitarbeiter wurde außerordentlich gelobt und aufgefordert ausschließlich – auch mit seinem Chef – nur per E-Mail über das Thema zu kommunizieren. Da der Absender der ungewöhnlichen Mail auch noch einen Buchstabendreher im Namen des Absenders enthielt, wandte sich der Beschäftigte sofort an die Firmenleitung und die Polizei.

X-bliebige E-Mail-Adresse vorgaukeln

Woher haben die Täter ihre Informationen? "Firmenauftritte im Internet liefern zumeist umfassende Informationen über die Hierarchieverhältnisse in den Unternehmen", warnt die Polizei. Meist würden Beschäftigte angemailt, die berechtigt sind, Geld zu überweisen. "Über Anonymisierungsdienste lässt sich dann eine X-beliebige E-Mail-Adresse vorgaukeln, die in der E-Mail-Flut manches Firmenmitarbeiters schnell als eine echte Mitteilung des Chefs angesehen werden kann."

Der Betrug sei oft nur schwer zu erkennen: Nicht immer hilft ein Rechtschreibfehler oder eine falsche Signatur. "Das Spiel der Betrüger mit der Vertraulichkeit macht es für Mitarbeiter zudem schwer sich mit ihren Kollegen auszutauschen, da sie nicht in die Missgunst des vermeintlichen Chefs fallen wollen."

Social Engineering via Facebook

Wie anfällig soziale Netzwerke für Social Engineering sind, habe schon vor Jahren die Kunstfigur Robin Sage gezeigt, sagt Schulte. Die vermeintlich attraktive Frau war 2009/2010 zwei Monate lang auf Internet-Kommunikationskanälen wie Facebook, Twitter und LinkedIn präsent. Das Ergebnis: "300 zum Teil hochrangige Kontakte aus Militär und Wirtschaft".

"Immer mehr Leute sind auf immer mehr Kanälen im Internet erreichbar", sagt Schulte. Wer in sozialen Netzwerken 2000 oder 3000 Freunde habe, verliere leicht den Überblick über einzelne Kontakte. Gefahr berge auch der Austausch über bestimmte Gruppen in sozialen Netzwerken. Straftäter könnten sich leicht Zugang verschaffen und unbemerkt Interna ausspähen.

Holzauge sei wachsam

Das LKA nennt mehrere Gründe, weshalb Social Engineering funktioniert: Das Ausnutzen von Freundlichkeit und Hilfsbereitschaft, Autoritätshörigkeit, mangelndes Gefahrenbewusstsein und fehlende Sicherheitsstandards. Und: "Die Opfer fühlen sich überrumpelt und wollen in einer ungewohnten Situation keine Fehler machen." Vielen potenziellen Opfern sei auch nicht bewusst, "wie wertvoll die Informationen in ihrem Besitz sind". Eine 100-prozentige Sicherheit gebe es nicht, generell gelte aber: "Vorsicht bei E-Mails die unaufgefordert eingehen!"
(des)

Erschienen am 16.05.2016 um 10:46 Uhr auf heise.de

Permalink: http://heise.de/-3208796