Geschichten mit vielen wahren Details? Vorsicht vor Fallen!

«Fast kein Cyberangriff funktioniert ohne eine gewisse Beteiligung des Opfers»: Max Klaus, stellvertretender Leiter der Melde- und Analysestelle Informationssicherung MELANI, erklärt, wie man sich vor «Social Engineering» schützt.

Im Namen des Firmenchefs eine E-Mail an die in der Buchhaltung tätige Person senden: So funktioniert CEO-Fraud. Das erste Schweizer Opfer war ein KMU im Kanton Freiburg, das durch diesen Vorfall eine Million Schweizer Franken verlor. *Bild: Shutterstock*

Cyberbedrohungen sind allgegenwärtig und können alle treffen. Dies gilt für Privatpersonen genauso wie für KMU, Grossunternehmen oder Regierungsbehörden auf allen Stufen.

Täter sammeln möglichst viele Informationen über potenzielle Opfer

Fast kein Cyberangriff funktioniert ohne eine gewisse Beteiligung des Opfers. Die Täter sind meistens darauf angewiesen, dass das Opfer beispielsweise ein Passwort verrät, einen Link auf eine schadhafte Internetseite anklickt oder ein per E-Mail zugeschicktes Dokument öffnet. Die Angreifer versuchen deshalb zuerst, möglichst viele Informationen über ihre möglichen Opfer zusammenzutragen. Diese Informationen werden dann verwendet, um dem potenziellen Opfer eine möglichst glaubwürdige Geschichte mit vielen wahren Details aufzutischen. Dadurch wirkt die durch den Angreifer verschickte E-Mail glaubwürdiger und erhöht die Chance, dass das potenzielle Opfer einen Fehler macht.

Der Gemeindeangestellte ist auch als Privatperson ein mögliches Ziel

Social Engineering – also das Beeinflussen von möglichen Opfern – kann in verschiedensten Formen erfolgen. Häufig geschehen die erwähnten Recherchen online, ohne dass das Opfer etwas davon merkt. Es ist aber auch denkbar, dass ein Angreifer herausfindet, dass ein Gemeindeangestellter in seiner Freizeit eine bestimmte Sportart ausübt. Der Angreifer sucht auf dem Sportplatz persönlichen Kontakt zum potenziellen Opfer, baut ein Vertrauensverhältnis auf und versucht, auf diesem Weg an Informationen zu kommen.

CEO-Fraud kann Millionen kosten

Vor wenigen Jahren haben die Cyberangreifer ein neues «Geschäftsmodell», den sogenannten «CEO Fraud» entdeckt.

Nationales Zentrum für Cybersicherheit NCSC.ch

Um die Bevölkerung und die Wirtschaft beim Schutz vor Cyberrisiken zu unterstützen und die Sicherheit der eigenen Systeme zu verbessern, hat der Bundesrat am 30. Januar 2019 die Schaffung eines Nationalen Zentrums für Cybersicherheit (NCSC.ch) beschlossen. An das NCSC können sich alle Personen und Unternehmen wenden, die sich über Cybergefahren informieren wollen oder die einen Cybervorfall melden möchten.
Das NCSC wird zurzeit auf der bisherigen Melde- und Analysestelle Informationssicherung MELANI aufgebaut. Auf der Website www.melani.admin.ch finden sich zahlreiche Anleitungen und Checklisten zum Thema Cyberbedrohungen, beispielsweise eine Anleitung, wie das Gäste-WLAN auf der Gemeindeverwaltung richtig konfiguriert wird.
Seit dem 1. Januar 2020 ist die Nationale Anlaufstelle des NCSC in Betrieb (www.ncsc.ch). Sie nimmt Meldungen zu Cybervorfällen entgegen und informiert über aktuelle Gefahren.

Dabei geben sich die Angreifer als Firmenchef aus und versuchen, die Finanzabteilung zur Überweisung eines hohen Betrages anzuweisen. Das erste Schweizer Opfer war ein KMU im Kanton Freiburg, das durch diesen Vorfall eine Million Schweizer Franken verloren hatte. In Österreich kostete ein solcher Angriff das betroffene Unternehmen sogar 42 Millionen Euro.

Die Angreifer überlegen sich dabei in einem ersten Schritt, welches Unternehmen oder welche Behörde sie um ihr Geld erleichtern wollen. Danach besuchen sie die entsprechende Website und suchen dort gezielt nach Namen von Personen, die in der Geschäftsleitung tätig sind sowie von Personen, die in der Buchhaltung arbeiten. In einem nächsten Schritt versuchen die Angreifer über Businessnetzwerke wie z. B. XING oder LinkedIn ausfindig zu machen, wie sich das Mitglied der Geschäftsleitung ausdrückt, wenn es Texte verfasst. Das Ziel ist es, im Namen des Firmenchefs oder eines Mitglieds der Geschäftsleitung eine E-Mail an die in der Buchhaltung tätige Person zu senden.

Kollektivunterschriften schützen besser vor Manipulationen
Während die ersten Mails vom vermeintlichen Chef noch relativ harmlos sind, wird der Druck auf die Person in der Buchhaltung im Laufe des Mailverkehrs immer weiter erhöht. In der E-Mail wird eine sehr heikle finanzielle Transaktion erwähnt, über die mit niemandem gesprochen werden dürfe. Zum Schluss bringen die Angreifer die Person in der Buchhaltung so weit, dass sie bereit ist, die entsprechende Zahlung auszulösen. Um sich vor solchen Angriffen zu schützen, sollten für Zahlungen unbedingt Kollektivunterschriften verwendet werden. Dadurch muss der Angreifer mindestens zwei Personen manipulieren, was deutlich schwieriger ist. Es sollten zudem niemals interne Informationen an unbekannte Personen weitergegeben werden. Schliesslich sollte unbedingt bei Vorgesetzten nachgefragt werden, wenn ausdrücklich verboten wird, jemanden über den «Geschäftsvorgang» zu informieren.

Daten klassifizieren und verschlüsseln
Gemeindebehörden, kantonale Stellen und Behörden auf Bundesebene sind besonders interessante Ziele für einen Datendiebstahl. In allen Behörden werden vertrauliche Informationen wie beispielsweise Steuererklärungen oder Gesundheitsdaten bearbeitet. Diese Informationen können für Cyberangreifer sehr lukrativ sein, weil sie sich unter Umständen für viel Geld weiterverkaufen lassen. Es ist daher von zentraler Bedeutung, solche Daten entsprechend zu schützen.
Eine Klassifizierung der Daten (z. B. «intern», «vertraulich» und «geheim») beschreibt die Sensibilität und den entsprechenden Umgang mit diesen Daten. In der Bundesverwaltung dürfen als «vertraulich» klassifizierte Daten ausschliesslich verschlüsselt per E-Mail übermittelt werden. Als «geheim» klassifizierte Daten dürfen nur durch einen Kurier überbracht werden und müssen auf komplett isolierten Geräten gespeichert sein.

Max Klaus
Eidg. Finanzdepartement EFD
Informatiksteuerungsorgan Bund ISB
Stv. Leiter der Melde- und Analysestelle Informationssicherung MELANI

«cyber-safe.ch», das Gütesiegel der Cybersicherheit für kleine und mittlere Organisationen

Der Schutz vor Cyberattacken ist für kleinere Unternehmen und Gemeinden oft kompliziert. Faktoren wie die Kosten für IT-Sicherheitsprüfungen, keine oder zu komplexe Standards oder fehlende interne Kompetenzen halten davon ab, entsprechende Massnahmen zu ergreifen. Deshalb hat der Schweizer Verband für das Gütesiegel der Cybersicherheit (ASLaC) das Label «cyber-safe.ch» lanciert, das eine IT-Sicherheitsprüfung wesentlich vereinfacht und vergünstigt. Um den Erwartungen kleiner und mittlerer Organisationen gerecht zu werden, hat der in der Westschweiz gegründete Verband Vertreter von Wirtschaftsverbänden aus der Waadt, Genf, Neuenburg, Freiburg und Wallis mit dem Verband der Waadtländer Gemeinden, Berufsverbänden wie der Schweizer Kader Organisation sowie Vertretern der Zivilgesellschaft und Hochschulen zusammengebracht. Gemeinsam haben sie eine Reihe von Anforderungen ausgearbeitet, die eine Organisation für den Erhalt des Labels erfüllen muss. Der junge Verband, der vom Center for Digital Trust (C4DT) der ETH Lausanne unterstützt wird und Mitglied des Steuerungsausschusses der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» ist, hat zudem einen automatisierten Prozess zur Bewertung von Organisationen im Hinblick auf die von den Partnern definierten Anforderungen eingerichtet. In der Deutschschweiz wird das Label von der Information Security Society Switzerland (ISSS) vertreten.
Der Onlinefragebogen ist kostenlos. Für den nachfolgenden Prozess liegen die Preise zwischen 3000 Franken für kleine Organisationen und 9990 Franken für ein Unternehmen mit 250 Mitarbeitenden.

Weitere Informationen und Anmeldung unter www.cyber-safe.ch.