Social Engineering: Jeder hat eine Schwachstelle

Cyber-Bedrohungen sind allgegenwärtig. Dabei stehen technische Sicherheitslücken oftmals im Vordergrund. Der Faktor Mensch geht häufig vergessen. Die Nutzer und Nutzerinnen sind aber häufig das schwächste Glied in der Sicherheitskette. Social Engineering nutzt menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen oder Angst aus, um technische Sicherheitsvorkehrungen zu umgehen. Philipp Leo erklärt im Interview die Mechanismen und Vorgehensweisen erfolgreicher Hacker.

Hptm Frederik Besse im Interview mit dem Cyber-Security-Experten und Milizoffizier Philipp Leo

Was macht Social Engineering so gefährlich?

Philipp Leo: Es kann jeden treffen. Man braucht dafür weder besonders naiv oder einfältig zu sein. Jeder hat eine Schwachstelle. Wenn man diese findet, kann man jeden Menschen hacken. Social Engineering ist an sich nichts Neues. Trickbetrug gibt es schon seit Menschengedenken.

Wie muss man sich so einen Angriff vorstellen?

Leo: Es wird Vertrauen zu den Opfern aufgebaut, nur um diese anschliessend auszubeuten. Was sich aber im Zeitalter der digitalen Kommunikation geändert hat, sind die neuen und äusserst effektiven Möglichkeiten, potenzielle Opfer erreichen zu können.

Die Kommunikation über digitale Kanäle bietet ein besonders günstiges Umfeld für Social Engineering. Während ein Akteur sein Gegenüber in einer realen Gesprächssituation über alle Sinne hinwegtäuschen muss, ist die Komplexität in der digitalen Kommunikation deutlich geringer.

Zudem können bereits im Vorfeld wichtige Hintergrundinformationen über die Opfer zusammengetragen werden, deren Kenntnis für einen Vertrauensaufbau hilfreich sein können.

Wo wird Social Enginnering am häufigsten eingesetzt? Etwa bei grossen Unternehmen?

Leo: Mit Social Engineering muss man überall rechnen. Aber die bekannteste Form ist sicherlich das Phishing. Durch meist sehr echt wirkende E-Mails sollen Personen dazu gebracht werden, auf einen Link zu klicken und nachfolgend auf authentisch wirkenden, aber gefälschten Websites ihre Logins und Passwörter einzugeben.

Diese werden dann von den Akteuren abgegriffen. Neben dem massenhaften Versand von Phishing-Mails lässt sich aber auch vermehrt die gezieltere Variante dieser Methode beobachten. Dabei spricht man von Spear-Phishing. In dieser Vorgehensweise werden die E-Mails nach vorausgegangener Recherche speziell auf kleine Gruppen oder einzelne Personen ausgerichtet.

Durch diese Fokussierung versucht man die Erfolgswahrscheinlichkeit zu erhöhen.

Also zum Beispiel bei einflussreichen Personen wie einem CEO?

Leo: Genau,beim CEO Fraud versuchen Akteure gezielt Mitarbeiter oder Mitarbeiterinnen aus den Finanzabteilungen so zu manipulieren, dass diese vermeintlich im Auftrag des Managements Überweisungen von hohen Geldbeträgen an die Akteure veranlassen.

Solche Manipulationen finden zwischenzeitlich auch schon über Telefon statt. Dabei wird die Stimme des Anrufers durch künstliche Intelligenz in Echtzeit synthetisiert und lässt sich dann nicht mehr von der echten Stimme des Vorgesetzen unterscheiden. Die Stimmmuster, die für das Antrainieren der künstlichen Intelligenz notwendig sind, stammen dabei oft aus Unternehmens- oder YouTube-Videos mit der jeweiligen Person.

Gibt es auch bekannte Vorfälle aus dem militärischen oder behördlichen Umfeld?

Leo: Davon gibt es viele. Als Beispiel: Im Jahr 2015 hat ein britischer Teenager Kane Gamble aus politischen Motiven den privaten E-Mail-Account von CIA-Direktor John Brennan gehackt. Bei seiner Recherche ist er auf die Mobilfunknummer des CIA-Direktors gestossen und hat sich anschliessend beim Provider als interner Techniker ausgegeben. Dabei konnte er viele persönliche Details in Erfahrung bringen.

Mit dieser Information konnte er den E-Mail-Account von Brennan zurücksetzen lassen und nachfolgend auf dessen private Korrespondenz zugreifen. Diese hat der Teenager dann auf verschiedenen Plattformen veröffentlicht. Aber wir brauchen gar nicht so weit in die Ferne zu schweifen. Es gibt auch bekannte Fälle von Social Engineering bei der Schweizer Armee.

2018 gab sich der Schweizer Journalist Cedric Schild über das Telefon als militärischer Vorgesetzter aus und brachte Angehörige der Armee dazu, ihm vertrauliche Wachtpläne über E-Mail zuzusenden. Er hat seine Vorgehensweise auf Video dokumentiert und nachfolgend veröffentlicht. Auch wenn dieser Beitrag als journalistischer Telefonscherz ausge-

legt war, zeigte seine Aktion in beeindruckender Weise die destruktiven Möglichkeiten von Social Engineering auf. Meines Erachtens war das eine echte Meisterleistung.

Nun, die Soldaten, die Opfer von Cedric Schild wurden, waren bemüht, das Richtige zu tun. Zielt Social Engineering auf unser soziales Wesen ab?

Leo: Social Engineering instrumentalisiert Menschen und nutzt ihre Schwächen schamlos aus. Wie diese Überzeugungsarbeit funktioniert, wissen wir vor allem aus der Psychologie, der Kriminologie oder dem Marketing.

Im Wesentlichen basiert Social Engineering auf der Ausnutzung grundlegender psychologischer Eigenschaften wie Autorität, Gruppenverhalten, Sympathie, Gutgläubigkeit, Vertrauen, sexuelle Attraktivität, Hilfsbereitschaft, Angst, Gier oder einfach nur Neugier. Diese Verhaltensweisen sind tief in uns verankert und sind das, was uns menschlich macht.

Wie kann man sich gegen etwas schützen, das tief in uns verankert ist? Ist das überhaupt möglich?

Leo: Der wirksamste Schutz vor Social Engineering ist der Einsatz des gesunden Menschenverstands. Wichtig ist es, aufmerksam zu sein und Unregelmässigkeiten nicht einfach hinzunehmen, sondern diese aktiv zu hinterfragen.

Wenn etwas zu gut klingt, um wahr zu sein, dann ist es oftmals auch nicht wahr. Das gilt in der realen, wie auch in der digitalen Welt. Ausserdem sollte mit der Preisgabe von Informationen in sozialen Netzwerken vorsichtig umgegangen werden. Diese werden häufig von Akteuren missbraucht, um das Vertrauen des Opfers zu gewinnen.

Gerne möchte ich noch eine letzte Frage an Sie als Milizoffizier richten. Wie erleben Sie persönlich den Einbezug der Miliz in der Cyber-Abwehr der Armee?

Leo: Ich werde als Milizoffizier, wie viele andere meiner Kameraden auch, vertieft in der Weiterentwicklung unserer Armee in diesem Themenbereich involviert. Ich erlebe diesen Einbezug als einen Austausch auf Augenhöhe. Unter anderem durfte ich bereits an der Konzeption für das Kommando Cyber mitarbeiten, die Führung an internationalen Cyber-Übungen begleiten oder auch an der Ausbildung unserer Cyber-Spezialisten mitwirken. Es erfüllt mich mit Stolz und Dankbarkeit, dass ich auf diese Weise Dienst leisten darf.

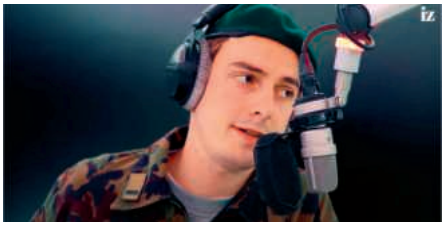

Bild: izzy

2018 gab sich der Schweizer Journalist Cedric Schild über das Telefon als militärischer Vorgesetzter aus und brachte Angehörige der Armee dazu, ihm vertrauliche Wachtpläne über E-Mail zuzusenden.

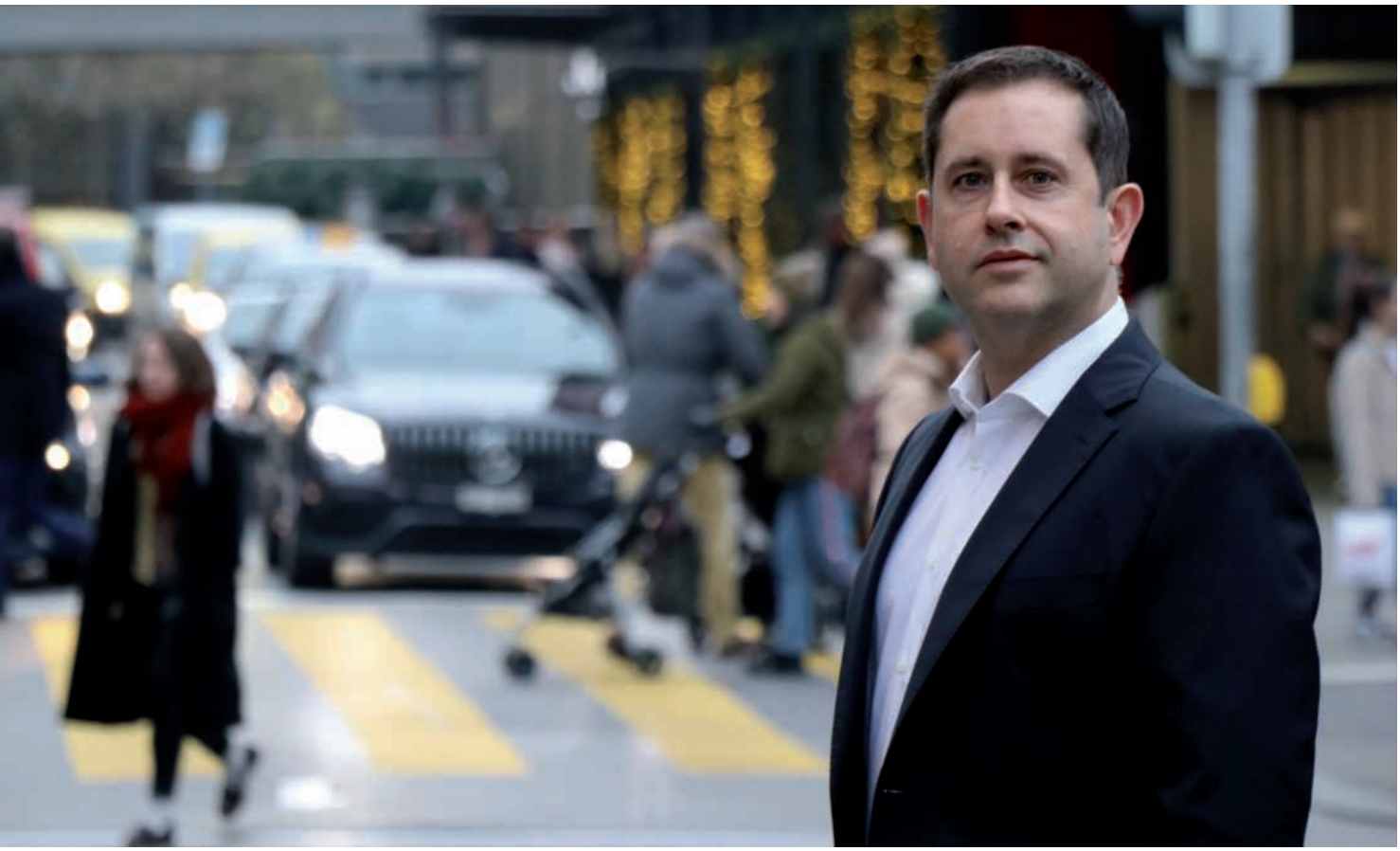

Bild: SCHWEIZER SOLDAT

«Wichtig ist es, aufmerksam zu sein und Unregelmässigkeiten nicht einfach hinzunehmen, sondern diese aktiv zu hinterfragen. Wenn etwas zu gut klingt, um wahr zu sein, dann ist es oftmals auch nicht wahr. Das gilt in der realen – wie auch in der digitalen Welt», Philipp Leo – Cyber-Security-Experte.