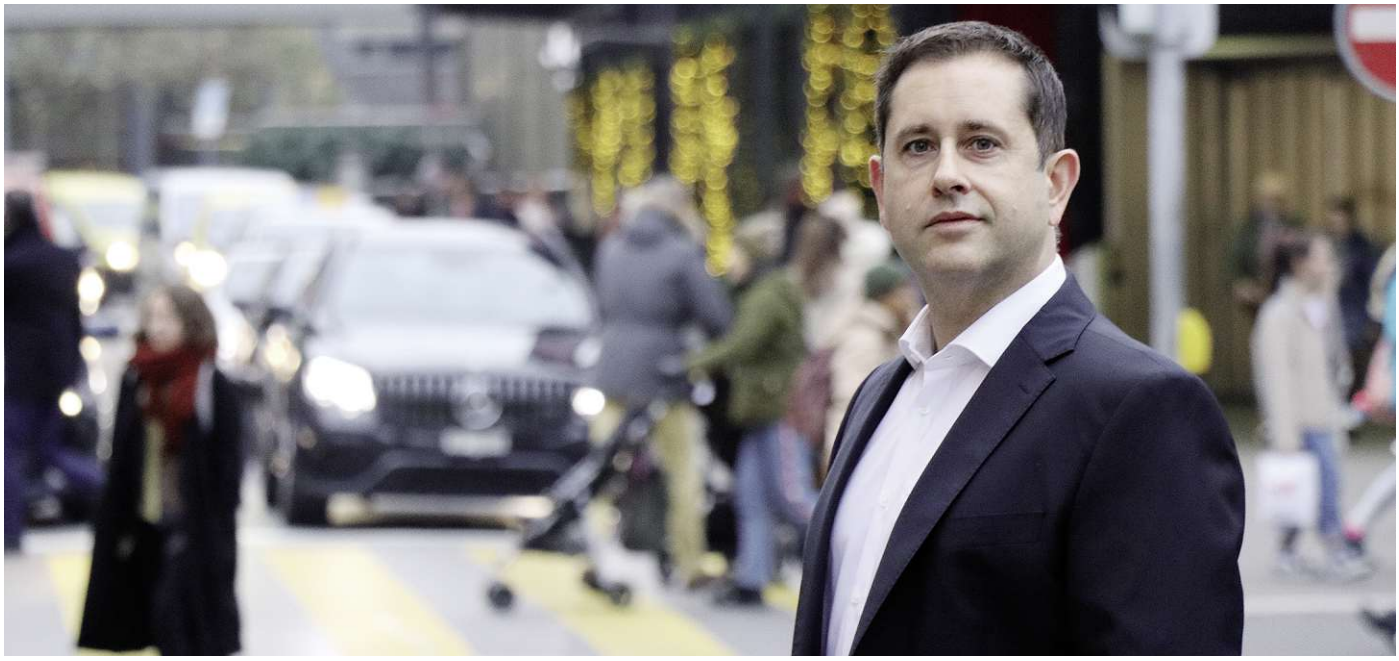

Philipp Leo: Berater zahlreicher Behörden und Organisationen und ausgewiesener Experte für Cyber Risiken und Digitalisierung.

Das wäre?
Leo: Wir können Muster anhand der nationalen Interessen erkennen. Die USA haben ein ganz anderes Einsatzspektrum als China. Während in China wirtschaftliche Interessen höher stehen, sind die USA stärker im militärischen Rahmen. Dort will man, ganz nach dem Motto «Kampf der verbundenen Waffen», die Cyberkräfte stärker in die Streitkräfte integrieren.

Sie unterrichten am Cyber Lehrgang der Armee. Wie würden Sie diesen aus Ihrer Sicht beschreiben?
Leo: Grundsätzlich bildet die Armee drei Funktionen aus. Diese heissen Spezialist CNO, Spezialist milcert und Spezialist Cyber Defence. Sie operieren in den Bereichen Defensiv, Offensiv und Nachrichtenbeschaffung. Hierbei ist anzumerken, dass wir die «Offensive» Tätigkeit ausbilden, um ein besseres Verständnis für die Verteidigung zu gewinnen. Diese Ausbildung und das Praktikum verlaufen nach ganz klar definierten ethisch moralischen und gesetzlichen Grundlagen.

Als Trainer spielen Sie dabei auch oft die Gegenseite im Kriegsspiel. Warum?
Leo: Das gehört zu meinen Kernkompetenzen. Ich unterrichte, wie die Gegenseite funktioniert und welche Vorgehensweisen möglich sind. Eine rein «blaue» Ausbildung ist limitiert, allein schon durch die Vorgaben und die Ethik. Der Gegner kann jedoch von allen Mitteln Gebrauch machen. Wer das nicht versteht, riskiert eine böse Überraschung. Ich bin jedoch meistens Teil eines Teams und agiere nicht als Einzelgänger.

Die Stärke liegt also im Teamplay?
Leo: Genau. Die Stärke liegt in der Kombination verschiedener Aspekte. Technik, Kreativität und Psychologie zum Beispiel. In den Teams, in denen ich beteiligt war, hatte ich vielfältige Personen zur Verfügung. Das sind Sprachspezialisten, Regisseure und Juristen zum Beispiel. Es geht darum, die besten Leute für eine spezifische Aufgabe einzusetzen.

Wieso Kreativität. Inwiefern kann ich als Angreifer kreativ sein?
Leo: Nun, das Ziel soll in eine Geschichte eingebunden werden. Eine solche Geschichte wird auf verschiedenen Kanälen erzählt. Das führt dazu, dass für das Ziel die fiktive Geschichte immer realer wird. Eine solche Geschichte ist zum Beispiel der CEO, welcher zur Rettung des Unternehmens eine grosse Summe zahlen muss. Kombiniert mit verschiedenen Inputs wie Telefongesprächen, einem Brief oder einer E-Mail wird die erfundene Geschichte zur erlebten Realität. Das wurde dem Angestellten im Finanzbereich des Unternehmens zum Verhängnis. Er glaubte die fiktive Geschichte.

Und was dann?
Leo: Dann wird er bereit sein etwas zu tun, was er sonst nie tun würde. Aus eigenem Antrieb: Denn es erscheint ihm logisch so zu handeln.

Im militärischen Bereich geht es dabei kaum um die Kreditkarte, oder?
Leo: Informationen zu Truppenstandorten können sehr lukrativ sein. Als militärisches Beispiel gibt es die Geschichte von israelischen Soldaten, die zum Download einer App überlistet wurden. Dies von gefakten Profilen israelischer Frauen.

Wenn ich einen Soldaten zum Installieren eines Trojaner bringe, kann ich eine Vielzahl von Informationen beziehen. Es gibt Beispiele, in denen mittels einer Fitness-App Militärstützpunkte sichtbar wurden. Dies, weil die Soldaten innerhalb der Basis joggen gingen.

Was können Angehörige der Armee und Privatpersonen tun, um dagegen gewappnet zu sein?
Leo: Sicherheit im Netz ist eine Illusion. Niemand ist sicher. Dessen muss man sich bewusst sein. Halte deine Systeme immer aktuell und beziehe alle Updates. Nutze lange Passwörter.

Überlege vor jedem Klick, was du tust. Benutze Sicherheitstools und sichere Messengers. Schränke die Rechte deiner Apps ein.

«Du wirst bereit sein etwas zu tun, was du sonst nicht tun würdest»

Im Wettrüsten zwischen Hacker und Cyberspezialisten werden immer bessere Programme geschrieben und Schwachstellen gesucht. Eine Komponente ist jedoch seit dem ersten Computervirus gleichgeblieben: Der Mensch. Philipp Leo, Berater zahlreicher Behörden zeigt im Exklusiv-Interview die Gefahren von Social Engineering auf und erzählt von einer simulierten Attacke auf einen Schweizer Offizier.

Hptm Frederik Besse im Interview mit Philipp Leo, unabhängiger Berater von Behörden

Was ist Social Engineering?
Philipp Leo: Der Ansatz ist einfach: Wieso sollte ich mich durch sieben Sicherheitsschichten durchkämpfen, wenn mir auch jemand einfach die Tür aufmachen kann? Social Engineering will genau das erreichen und ist somit Trickbetrug. Wie finde ich bei der Schnittstelle Mensch Schwachstellen? Mittels psychologischen Tricks geht es dann darum, Menschen dazu zu bringen, etwas zu tun was sie nicht wollen. Meistens ist ein Angriff eine Kombination zwischen menschlicher Interaktion und technischer Attacke. Dieser Trickbetrug ist laut Studien in vielen Fällen ein Bestandteil der Angriffsstrategie.

Wie kann man sich das im Alltag vorstellen?
Leo: Stellen Sie sich vor, Sie erhalten im Geschäft ein Mail mit der Aufforderung, eine grosse Summe an einen unbekannten Empfänger zu überweisen. Der Absender ist Ihnen bekannt und nur kurze Zeit später ruft dieser auch an und bestätigt die Transaktion. Im Finanzbereich gab es einen Fall, in dem ein Mitarbeiter aufgefordert wurde eine solche Zahlung durchzuführen. Er war sich zu 100 Prozent sicher, dass die Stimme zu seinem CEO gehörte, den er kennt. Es stellte sich später heraus, dass eine künstliche Intelligenz die Stimme des CEO aus verfügbaren Proben analysiert hatte und in Echtzeit kopieren konnte.

Wer Menschen täuschen will, muss diese auch kennen. Was muss man über Kulturen wissen?
Leo: Richtig. Wer Menschen angreift und nicht technische Systeme muss die kulturellen Begebenheiten kennen. Diese gibt es ganz klar auch im Cyber Bereich. Ein Amerikaner reagiert auf eine unterschiedliche Weise als ein Schweizer. Diese Aspekte spielen eine wichtige Rolle.

Apropos unterschiedliche Kulturen: Sie waren zwei Jahre lang für die Schweizer Armee in Korea stationiert.
Leo: Genau.

Was haben Sie dort erlebt?
Leo: Ich habe in einem internationalen Kontext gesehen, was Informationen ausmachen. Es ist so weit gekommen, dass mich ein Nachrichtendienst, auch mittels Social Engineering, für seine Sache gewinnen wollte.

Waren es die Nordkoreaner?
Leo: Meiner Meinung nach werden die Nordkoreaner überschätzt. Ich denke, dass sie ihre Angriffe in China einkaufen. Sie sind eine schwache Macht im Cyber Raum, werden jedoch als Gefahr wahrgenommen. Es kann durchaus helfen, wenn ausschliesslich die Reputation über die eigene Cybertruppe stark ist. Dieses aufgeblasene Image eines starken Cyber-Nordkorea bringt allen Parteien etwas. Aber: Aufgrund der abgeschotteten Bevölkerung und dem mangelnden Zugang zu Bildung sind die Kapazitäten der Nordkoreaner in Bereich Cyber beschränkt. Die Rekrutierung ist schon in der Schweiz schwierig genug.

In der Schweiz waren Sie an einer Aktion beteiligt, bei der Social Engineering bei einem Offizier ausprobiert wurde.
Leo: Ich war Teil eines Teams, dass einen Höheren Stabsoffizier in einer Simulation gehackt hatte. Bei diesem Angriff kam Social Engineering ebenfalls zum Zug.

Was hat es mit diesem Angriff auf sich?
Leo: Im Rahmen einer Sensibilisierung Kampagne hat sich ein Höherer Stabsoffizier bereiterklärt das Ziel eines simulierten Angriffes zu sein. Wir haben einen Angriff geplant und umgesetzt. Dabei ging es in einer ersten Phasen darum Informationen zu sammeln. Aus diesen Daten konnte schlussendlich ein Angriffsplan entwickelt werden. Im Rahmen eines Seminars haben wir die Resultate präsentiert.

Wie war die Reaktion?
Leo: Die Auswirkung auf das Publikum war sehr hoch. Die Offiziere waren überrascht wie stark sie als Führungsperson in den Fokus geraten können.

Hätten die Verteidiger Sie überhaupt als Angreifer identifizieren können, wenn es ein realer Angriff gewesen wäre?
Leo: Wohl kaum. Das nennt man Attribution und gehört zu den schwierigsten Aspekten im Cyberbereich. Natürlich hinterlässt alles Spuren im Cyberraum. Die Zuweisung ist jedoch komplex und hat oft auch politische Komponenten. Eine einwandfreie Attribution wird dadurch ein Ding der Unmöglichkeit. Ich würde hinter jede Zuweisung von digitalen Angriffen immer ein Fragezeichen setzen. Etwas ist jedoch gut analysierbar