Social Engineering

«Die geringe Büropräsenz hilft uns sehr»

Immer mehr Unternehmen lassen sich von Social Engineers angreifen, um Sicherheitslücken aufzudecken, sei es in der IT, sei es beim Personal. Computerworld sprach mit Ivano Somaini, Regional Manager Zürich bei Compass Security, der genau solche Aufträge ausführt.

→ INTERVIEW UND BILDER: JENS STARK

ZUR PERSON

Ivano Somaini
hat an der ETH Zürich Informatik mit Schwerpunkt Informationssicherheit studiert. Im Studium vertiefte er Themen wie kryptographische Protokolle, Network Security und E-Privacy. Für seine Masterarbeit befasste er sich mit dem theoretischen Aspekt der Sicherheit. Er modellierte und verifizierte das kryptographische Protokoll Kerberos. Seit März 2011 ist Somaini bei Compass Security als Security Analyst tätig. 2013 gründete er deren Berner Filiale, welche er bis September 2017 leitete. Heute führt er die neue Filiale in Zürich. 2015 hat sich Somaini bei Christopher Hadnagy, dem weltbesten Social Engineer, als Advanced Social Engineer weitergebildet. Ein Jahr später folgte die Weiterbildung im Bereich Open Source Intelligence bei Mike Bazell, dem ehemaligen FBI-Undercover-Agent und Osint-Experten.

Der «Faktor Mensch» wird immer wieder als wunder Punkt in der IT-Security genannt. Das mahnen nicht nur Cybersicherheitsspezialisten immer wieder an, das wissen auch Wirtschaftsspione und Hacker. Schliesslich verlassen sie sich auch zu einem Grossteil bei ihren Angriffen auf ihre Social-Engineering-Künste. Sie manipulieren also Personen gezielt, um diese dazu zu bewegen, Informationen herauszugeben oder um sich auch ganz physisch unautorisierten Zugang zu Gebäuden zu verschaffen. Auf Social Engineering hat sich auch Ivano Somaini von Compass Security spezialisiert. Er bricht – natürlich stets und strikt im Kundenauftrag – in Firmengebäude ein oder lanciert Phishing-Kampagnen, mit der Absicht Lücken im Sicherheitsdispositiv aufzudecken und Mitarbeitende zu sensibilisieren. Wie er dabei vorgeht, verrät Somaini im Interview mit Computerworld.

Computerworld: Welche Social-Engineering-Methoden sind Ihrer Meinung nach erfolgsversprechender, um bei einem Eindringungsversuch Informationen einer Firma zu entwenden: Eher digitale wie Phishing oder doch eher physische Methoden wie telefonieren oder in Person vor Ort erscheinen?

Ivano Somaini: Die schwierigste der drei erwähnten Methoden, bei denen also die Leute am skeptischsten sind, ist meiner Erfahrung nach das Telefonat. Hier muss man als Social Engineer am besten schauspielern können. Das liegt daran, dass man bei einem Anruf eigentlich nur einen Kommunikationskanal zur Verfügung hat – die eigene Stimme. Wenn man dagegen vor Ort erscheint, steht einem auch noch die Körpersprache und der Augenkontakt zur Verfügung. Darüber hinaus kann man sich vorher verkleiden, etwa als Service-Techniker. Das schafft Vertrauen und die Hemmschwelle des Gegenübers wird erhöht, das Vorhaben in Frage zu stellen und mit gesunder Skepsis auf die Situation zu reagieren.

Beim Phishing hat man den Vorteil, sehr viele Empfänger zu erreichen. Bei hundert Mails reicht es eigentlich, wenn ein Mitarbeitender in die Falle tappt und beispielsweise einen verseuchten Link anklickt. Allerdings ist Phishing aus technischer Sicht in letzter Zeit immer schwieriger geworden. Denn die Firmen benutzen heutzutage häufig cloudbasierte Lösungen, bei denen Anti-Phishing-Mechanismen standardmässig aktiviert und nur mit Mühe auszuhebeln sind. Vor ein paar Jahren konnten wir noch eine Domain reservieren und mit dieser eine Phishing-Mail-Kampagne erstellen. Heute wird elektronische Post von Domains, die erst vor Kurzem reserviert wurden, oft geblockt. Als Konsequenz müssen wir meist von den Administratoren verlangen, uns auf die Whitelist zu setzen.

CW: Mich erstaunt noch, dass Telefonieren als Methode so schwierig eingestuft wird. Ich hätte jetzt gedacht, mit einem Telefonat erhält man mehr Aufmerk- →

Bild: Jens Stark

Ivano Somaini von Compass Security hat sich auf Social Engineering spezialisiert

samkeit, da heutzutage die Verwendung dieses Kommunikationsmittels abnimmt…

Somaini: Die zunehmende Skepsis gegenüber Anrufenden ist unter anderem auch auf die vielen Telefonate von Verkäufern und Marktforschern in den letzten Jahren zurückzuführen. Darüber hinaus wissen viele um die typische Betrugsmasche, bei der jemand anruft und sich als Microsoft-Supporter ausgibt. Hier haben die vielen Warnungen etwa auch von der Polizei Wirkung gezeigt.

VORTEIL LEERE BÜROS

CW: Auch als Social Engineer müssen die letzten zwei Jahre speziell gewesen sein. Was waren Ihre Erfahrungen während der Pandemie, als viele Belegschaften mehrheitlich im Home-Office waren? War es einfacher oder mühsamer für einen Social Engineer?

Somaini: Während der Pandemie haben wir ehrlich gesagt weniger Aufträge erhalten für physische Eindringungsversuche. Schliesslich wollte man keine solche Szenarien anhand einer Aussnahmesituation testen. Denn wichtig sind ja die Ergebnisse für den Normalfall in Hinblick auf Awarenesskampagnen. Viele Auftraggeber haben daher die Pandemie für einen schlechten Zeitpunkt gehalten, da ungewiss war, wie lange diese anhalten würde. Die Ausnahmesituation hätte ja nach wenigen Wochen vorbei sein können. Zudem hätten Betroffene mit Verweis auf die Covid-Krise eine gute Ausrede gehabt, warum sie im Sinne der Security falsch gehandelt haben.

Auch wollten wir keine Phishing-Mails entwerfen, die die Pandemie thematisieren. Schliesslich kann man davon ausgehen, dass viele Mitarbeitenden selbst oder im näheren Umfeld Krankheitsfälle oder gar Opfer zu beklagen hatten. Unser Ziel als Social Engineer ist es, das Sicherheitsbewusstsein zu schärfen und nicht bei den Betroffenen schlechte Gefühle hervorzurufen. Dies wäre bei Corona aber unweigerlich der Fall gewesen. Darum müssen wir immer Szenarien entwerfen, bei denen die Betroffenen sich zwar ärgern oder betroffen sind, dass sie in die von uns gestellte Falle getappt sind, aber nicht mehr.

CW: Was wäre ein solches Szenario?

Somaini: Beispielsweise migrieren derzeit viele Firmen auf Office 365 und sind dabei die Zweifachauthentifizierung zu implementieren. Hier schreiben wir dann ein Mail im Namen des Supports und fordern die Angeschriebenen auf, für die Änderung der Konfiguration auf einen Link zu klicken, der auf eine Seite führt, auf die Login-Daten abgefangen werden können. Es handelt sich somit um ein relativ emotionsloses Thema, es geht schlicht um IT.

Ein weiteres Beispiel: Zur Zeit kann man Mitarbeitenden im Mail als Fringe-Benefit Tankgutscheine versprechen, wenn die Benzinpreise wieder steigen. Es werden also positive Köder ausgelegt, was moralisch weniger problematisch ist.

CW: Wie gut funktionieren physische Eindringungsversuche derzeit, da viele Mitarbeitende nur noch teilweise im Büro anzutreffen sind?

Somaini: Was die jetzige geringe Büropräsenz angeht, so hilft dies bei Social-Engineering-Angriffen. Wir können uns gegenüber früher freier bewegen, weil in den Grossraumbüros nur noch die Hälfte der Mitarbeitenden anwesend sind. In der Regel können wir uns an einen verwaisten Arbeitsplatz setzen und in aller Seelenruhe unsere weiteren Schritte planen. Auch wird man seltener angesprochen und fällt generell weniger auf. Besonders in grossen Konzernen wissen viele Angestellte gar nicht mehr, wer aktuell genau für das Unternehmen tätig ist und wie all die Mitarbeitenden aussehen, die dort arbeiten. Somit kann man recht locker die Rolle als neuer Mitarbeiter spielen.

GUTE SOCIAL ENGINEERS SPIELEN SICH SELBST

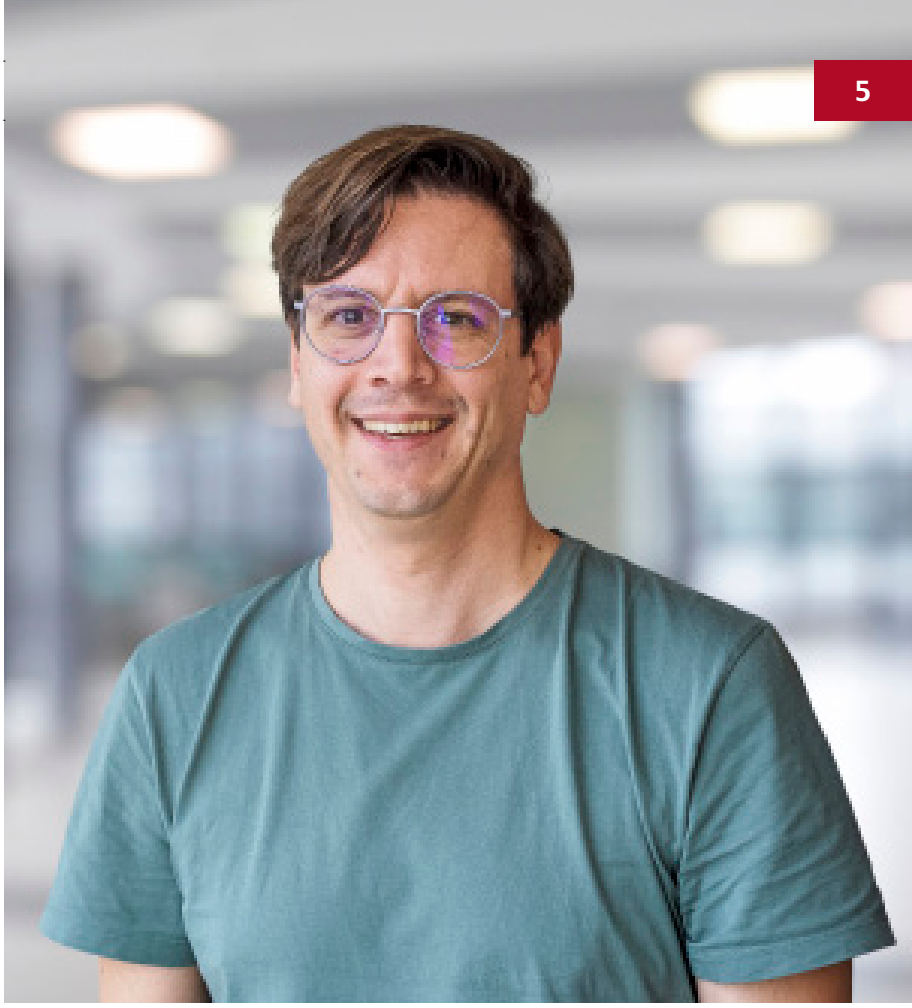
CW: Was braucht es, um ein erfolgreicher Social Engineer zu sein, welche persönliche Eigenschaften und Charakterzüge sind von Vorteil?

Somaini: Wichtig ist, dass man gut weiss, wie man gegen aussen wahrgenommen wird. Mich selbst beurteile ich beispielsweise vom Aussehen her als eher wenig autoritär. Ich witzle oft, dass ich auf andere wirke wie jemand, der Hilfe benötigt. Daher kann ich diese Rolle auch am besten spielen. Ich trete dann meistens mit einer grossen Schachtel in der Hand auf, sodass die Leute mir ohne weiteres die Türe aufhalten. Wenn ich dann gleich auch noch vorgebe, in ein wichtiges Telefonat vertieft zu sein, werden auch keine Fragen über meine Anwesenheit gestellt. Ich könnte zwar auch den autoritären und bösen Boss raushängen. Aber ich befürchte, das würden die Umstehenden mir weniger abnehmen. Auch kann ich als ausgebildeter Informatiker mich am natürlichsten beispielsweise in der Rolle eines IT-Supporters bewegen. Denn hier kann ich sehr spontan auf Fragen kompetent reagieren, sodass ich als jemand rüberkomme, der etwas von der Sache versteht. Das gelingt mir sicher weniger in einem Umfeld, das mir fremd ist.

Was die Charaktereigenschaften anbelangt, so ist sicher Empathie sehr wichtig. Dies gilt nicht nur für Besuche und Auftritte in Person, sondern auch für den Versand von Phishing-Mails. Hier muss man sich gut in den anderen versetzen können und wissen, wie das Gegenüber tickt.

«Die jetzige geringe Büropräsenz hilft bei Social-Engineering-Angriffen.»

Bild: Jens Stark



Ivano Somaini leitet die neue Zürcher Filiale von Compass Security

CW: Da müssen Sie die Person aber bereits gut kennen, damit das funktioniert…
Somaini: Ja, das stimmt. Meist muss sich hier der Social Engineer über die anzugreifende oder auszutricksende Person anhand öffentlich zugänglicher Informationen und Quellen ein Bild machen, mit Hilfe so genannter Osint-Methoden (Open Source Intelligence) also. Das gelingt bei den meisten Zielpersonen immer besser, da heutzutage viel von sich selbst preisgegeben wird, und sei es durch Posts in sozialen Medien.

Beim Auftauchen vor Ort muss man dagegen oft das Gegenüber schnell einschätzen können und entsprechend reagieren. Das geschieht üblicherweise in Sekundenbruchteilen und unbewusst.

CW: Welche Rollen haben ihrer Erfahrung nach mehr Erfolg, unauffällige Rollen, wie der vermeintliche Service-Techniker der Druckerfirma, oder ausgeklügeltere und auffälligere?
Somaini: Beides funktioniert. Allerdings ist die unauffällige Rolle oft einfacher durchzuführen, da sie weniger aufwendig ist in der Vorbereitung und dennoch sehr oft zum Erfolg führt. Gerade kürzlich haben Kollegen von mir zwei Szenarien am selben Tag und am selben Ort durchgespielt. Das erste war sehr durchdacht und mit grossem Rechercheaufwand verbunden. So fanden sie heraus, wer die Gebäudeverwaltung für die Büros der Zielfirma – in diesem Fall eine Bank – war. Danach gaben sie sich als deren Techniker aus, meldeten sich vorab an und kamen zum vereinbarten Termin perfekt verkleidet, mit Namensschildern und Mäppchen versehen. Darüber hinaus hatten sie einen erfundenen Report eines angeblichen Besuchs vor einem Jahr dabei. Trotz dieses Aufwands riefen sie eher Skepsis hervor und wurden sehr genau beobachtet, bei allem, was sie vor Ort verrichteten. Danach kehrten sie zurück, tauschten das Gebäudetechniker-Tenue gegen normale Anzüge und besuchten das Geldinstitut als normale Bankangestellte. Sie schlichen sich hinter Mitarbeitenden durch noch geöffnete Türen ein und konnten sich recht frei in der Bank bewegen, weil sie in ihrem Outfit überhaupt nicht auffielen.

KULTURELLE UNTERSCHIEDE

CW: Gibt es auch gesellschaftliche Unterschiede? Funktionieren gewisse Social-Engineering-Tricks beispielsweise in der Schweiz besser als in anderen Ländern oder Kulturen? Was sind hier Ihre Erfahrungen?
Somaini: Auf jeden Fall! Es gibt Szenarien, die in der Schweiz funktionieren, aber in Italien oder auch in Deutschland nicht. In der Schweiz ist man generell nett, zuvorkommend und hilfsbereit. Das macht meinen Job tendenziell einfacher. Wenn Leute sehen, dass ich Probleme habe, wird mir geholfen. Auch beobachte ich bei sogenannten Tailgating-Versuchen, wo ich also hinter jemandem durch die noch offene Türe schlüpfe, dass in der Schweiz und besonders in der Deutschschweiz die Hemmschwelle sehr hoch ist, mich anzusprechen und zu fragen, wer ich bin und ob ich überhaupt berechtigt sei, mich hier aufzuhalten. Letzteres passiert in Deutschland und Italien übrigens öfter als in der Schweiz. Hierzulande erntet man zwar skeptische Blicke, aber zur Rede wird man selten gestellt.

Dafür kann man in Italien und Deutschland die Leute mit Titeln mehr beeinflussen, da diese in der Alltagskultur eine grössere Rolle spielen als bei uns. Hier ist also definitiv ein auf die Hierarchie abzielendes Szenario erfolgversprechender als bei uns.

CW: Welche Rolle spielt auch die Firmenkultur und -struktur dabei, ob ein Social-Engineering-Angriff erfolgreich ist? Ist es beispielsweise einfacher in einem autoritär geführten Unternehmen an Infos zu kommen als in einer Firma mit flacher Hierarchie?
Somaini: Ob es einfacher ist, kann nicht gesagt werden. Es ist aber sicherlich so, dass Szenarien, die auf die Hierarchie setzen, in Organisationen wie dem Militär oder der Polizei, aber auch bei gewissen Grossbanken sehr gut funktionieren. Hier reicht es oft aus, mit Hilfe eines hohen Dienstgrads oder einer hohen Position im Management an die benötigten Informationen zu kommen.

Auf der anderen Seite hätten Sie damit bei Start-ups überhaupt keinen Erfolg. Dies sind ja Firmen, die sehr offen und neugierig sind und Know-how aufsaugen möchten. Sie suchen geradezu neue Kontakte, so dass es nicht sonderlich schwierig ist mit ihnen anzubandeln und sich zu treffen sowie offen auszutauschen.

Bei grösseren Unternehmen kann dagegen einerseits die Anonymität ausgenutzt werden, um sich beispielsweise ins Gebäude einzuschleusen. Andererseits sind hier Phishing-Aktionen meist erfolgreich, wenn man die Hierarchie-Karte spielt und sich etwa als Verkaufschef ausgibt. Allerdings braucht es gute vorgängige Osint-Recherchen wie das gründliche Studium des Organigramms.

CW: Wie wenden Sie die Informationen an, reicht das simple nennen des Namens eines leitenden Managers?
Somaini: Meist nicht einmal nur das. Ein Trick etwa besteht darin, jemanden ein Mail mit einem Auftrag oder einer Bitte zu schreiben und die Adresse des Chefs oder Vorgesetzten ins «CC:» zu nehmen, aber so, dass diese einen Schreibfehler enthält. Dadurch meint zwar der Angeschriebene, dass der Chef das Mail ebenfalls erhalten habe. Es ist aber wegen der falschen Adresse nicht angekommen.

Ivano Somaini empfiehlt gegenüber Unbekannten zwar skeptisch zu sein aber auch höflich zu bleiben

Daneben gibt es noch ganz andere Spielarten. Einmal durfte ich einen Politiker angreifen. Hier zielte ich dann auf das Ego des Betreffenden ab, indem ich mich als Zeitungsredaktor ausgab und erklärte, dass ich an einem Porträt über ihn arbeitete, das morgen gedruckt werde und ihm den Text zur Durchsicht im Mail angehängt habe. Die Wahrscheinlichkeit, dass diese Person die Datei öffnet, ist dann sehr hoch.

CW: Politiker könnte man auch mit bewussten Falschaussagen aus der Reserve locken…
Somaini: Nicht nur Politiker! Falsche Angaben sind oft hilfreich, um an richtige Informationen zu kommen. Letztens haben wir die Rezeption einer Bank angerufen, um herauszufinden, wie der Prozess zur Ausstellung von Besucher-Badges abläuft. Gegenüber dem Mitarbeitenden erklärten wir am Schluss als Bestätigung, dass wir diesen somit anrufen, wenn wir einen Badge bräuchten. Worauf dieser dies verneinte und uns die richtige Kontaktperson samt Mailadresse und Telefonnummer verriet. Schlussendlich konnten wir in Erfahrung bringen, wie und mit welchen Informationen ein Formular ausgefüllt werden musste, um den Badge zu erhalten.

DEN LERNEFFEKT VOR AUGEN

CW: Wie gehen Sie vor, wenn Sie einen «Einbruchsauftrag» erhalten?
Somaini: Zunächst versuche ich herauszufinden, was dem Auftraggeber am meisten bringt, um später auch die Mitarbeitenden entsprechend sensibilisieren und generell die Sicherheit erhöhen zu können. Denn oft werde ich von den Auftraggebern schon mit sehr konkreten Plänen konfrontiert, die zwar erfolgreich wären, aber nicht unbedingt die Awareness steigern würden. Ich halte somit Ausschau nach Szenarien, die dieser Firma auch passieren könnten.

CW: Das heisst, Sie haben von Anfang an den Lerneffekt vor Augen…
Somaini: Genau, dies ist das Endziel, das zudem in meiner «Karriere» im Laufe der Zeit einen höheren Stellenwert erhalten hat. Als ich als Social Engineer angefangen habe, verspürte ich mehr Druck, wirklich in ein Ziel einzudringen. Heute ist es mir dagegen wichtiger, einen Mehrwert für die Auftraggeber zu erzielen. Ein Einbruch ist nämlich in den meisten Fällen möglich, aber doch nicht wahrscheinlich, da das eingegangene Risiko und der Ertrag in keinem Verhältnis stehen. Besser ist es da, auf generelle, auch kulturell begründete Sicherheitsmängel hinzuweisen. So musste ich vor Kurzem bei einer Firma einbrechen, die ein zweistufiges Badge-System implementiert hatte. So musste man sich zunächst für den Zutritt zum Gebäude ausweisen und dann in jedem Stock nochmals. Interessant war hier, dass ich, nachdem ich die erste Hürde überwunden hatte, mich quasi frei bewegen konnten. Auf Stock-Ebene wurden mir die Türen aufgehalten, weil die Leute das Gefühl hatten, ich sei sicherlich autorisiert. Die gute Absicherung des Gebäudes verursachte also ein falsches Gefühl der Sicherheit, das dann im Awareness-Training thematisiert werden konnte.

Ein anderes Mal konnte ich Fehler in den Prozessen aufdecken. Mir war nämlich bei einem früheren Besuch aufgefallen, dass mir der Besucherbadge bereits ausgestellt wurde, als ich 40 Minuten vor dem eigentlichen Termin mit einem Mitarbeitenden an der Rezeption erschien. Als wir dann einen Einbruchsauftrag erhielten, nutzten

Bild: Jens Stark

wir dies aus. Ich erschien wieder zu früh, erhielt den Badge und begab mich unter dem Vorwand, noch eine Zigarette rauchen zu wollen, nach draussen. Dort übergab ich den Besucherbadge an einen Kollegen, der sich mit diesem ungeniert in dem Unternehmen umsehen konnte, während ich mit einer Attrappe wieder in die Lobby begab. Der Hinweis auf diese prozessuale Lücke war dann ein Mehrwert für die Firma und half dabei, die Sicherheit zu erhöhen.

CW: Gibt es auch Angriffsversuche, bei denen Sie gescheitert sind?
Somaini: Gescheitert in dem Sinne, dass wir nicht in eine Firma eindringen konnten, sind wir noch nie. Allerdings gelang uns dies nicht immer beim ersten Mal. Dann reicht es aber in der Regel aus, auf die nächste Gelegenheit zu warten. So traf ich vor kurzem auf einen skeptischen Mitarbeitenden, der mich zur Rede stellte. Beim nächsten Versuch klappte es dann. Solche Hindernisse sind aber für den Schlussbericht genauso wichtig wie erfolgreiche Einbruchsversuche. Denn man kann schliesslich anhand solcher Beispiele aufzeigen, wie man sich im Sinne der Sicherheit korrekt verhalten hätte. Darum bin ich heute auch mehr ein Fan von sehr einfach gestrickten Angriffsversuchen, bei denen man aufzeigen kann, dass man diesen eigentlich hätte merken und abwenden können. Dagegen bieten sehr ausgeklügelte und technisch ausgefeilte Versuche einen weniger grossen Lerneffekt, da deren Wahrscheinlichkeit in Abrede gestellt werden kann.

SKEPTISCH, ABER HÖFLICH

CW: Sie plädieren also für eine gesunde Skepsis. Sollen wir schlussendlich – etwas provozierend gefragt – alle unhöflich werden, wenn beispielsweise jemand hinter uns durch die Türe möchte?
Somaini: [Lacht] Das ist eine berechtigte Frage. Viele befürchten tatsächlich, dass man unhöflich und asozial werden könnte. Dem versuche ich entgegenzuhalten, dass man einerseits, wenn etwas nicht stimmt, durchaus seinem Bauchgefühl folgen und Skepsis an den Tag legen darf. Andererseits gibt es ja auch einen höflichen Weg, um auf solche Situationen zu reagieren. So könnte man einen Fremden durchaus anständig ansprechen, beispielsweise wie folgt: «Ich kenne Sie nicht. Sind Sie neu hier? Bei uns sollte man einen Badge haben. Wenn Sie wollen, kann ich Sie zur Rezeption begleiten, um einen solchen auszustellen.»

CW: Was geschieht eigentlich nach einem Einbruch?
Somaini: Das hängt ganz vom Auftraggeber ab. Wir schreiben immer einen Bericht, in dem wir unsere Schritte dokumentieren. In der Regel können wir unsere Ergebnisse auch in Form von Vorträgen präsentieren. Dabei ist es meist von Vorteil, dass wir als Externe auf die Missstände aufmerksam machen, besonders wenn es um die Verbesserung der IT-Sicherheit geht. Denn oftmals sind Mitarbeitende offener gegenüber Verbesserungsvorschlägen, wenn diese nicht von der eigenen IT-Abteilung kommen, sondern von aussen. Häufig werden wir von Firmen auch gebeten, ein Awareness-Training zu organisieren, besonders dann, wenn beispielsweise ein Phishing-Versuch unsererseits besonders erfolgreich war.

> «Es gibt Szenarien, die in der Schweiz funktionieren, aber in Italien oder auch in Deutschland nicht.»

CW: Gibt es Rezepte für mehr oder weniger erfolgreiche Awareness-Kampagnen?
Somaini: Meiner Erfahrung nach ist es am erfolgreichsten, wenn ein Thema ins private Umfeld getragen wird. Wenn wir den Beteiligten aufzeigen können, wie sie sich zu Hause richtig verhalten, um etwa den Online-Banking-Zugang oder die privaten Familienfotos besser zu schützen, übertragen viele dieses Verhalten auch auf den Umgang mit Firmen-Ressourcen. Wenn man dagegen rein geschäftlich argumentiert, ist dies weniger erfolgreich. Denn schliesslich geht es nicht um das eigene Geld oder die eigenen Informationen. Wenn ich dagegen die Gefahren in Bezug auf das Privatleben aufzeigen kann, ist das Interesse grösser und die Awareness steigt auch in Bezug auf die eigene Firma.

CW: Wie viele Firmen setzen unterdessen auf Awareness-Kampagnen?
Somaini: In Bezug auf mittlere und grosse Unternehmen sind es wohl mittlerweile alle, die in irgendeiner Form Awareness-Kampagnen fahren, und seien es automatisierte Tools, die zum Einsatz kommen. Vor zehn Jahren, als ich mit diesen Angeboten anfing, waren es noch sehr wenige Firmen. Unterdessen stelle ich fest, dass auch immer mehr KMU Awareness-Kampagnen einsetzen.

Das hängt natürlich auch mit dem Angebot zusammen. Zum Beispiel bietet heute Microsoft im Rahmen von Office 365 eine Phishing-Simulation als Dienstleistung an. Für Firmen, die sowieso schon auf Office 365 setzen, ist es dann sehr einfach, regelmässig Phishing-Tests durchzuführen, die dann auch das Budget nicht allzusehr belasten. ←

ZUR FIRMA

Compass Security wurde 1999 durch Walter Sprenger und Ivan Bütler gegründet. Das Schweizer IT-Security-Unternehmen ist mit über 55 Mitarbeitenden an Standorten in der Schweiz, in Deutschland und in Kanada präsent. Zu den Dienstleistungen der Firma gehören unter anderem Penetration Tests, Red Teaming, Security Reviews sowie Digital Forensics und Incident Response.
→ **compass-security.com.**