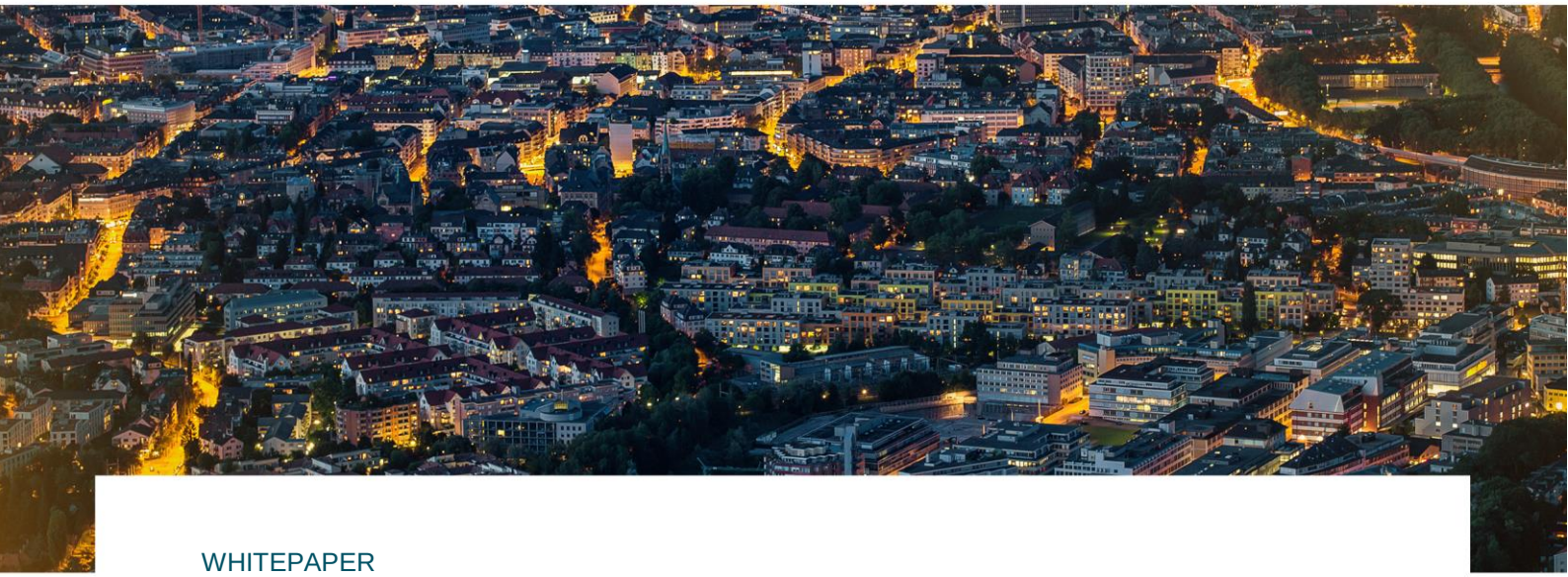
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WHITEPAPER

«Social Engineering» – die wirksamen Gegenmassnahmen

Reto Amstad | Senior Security Consultant | Steinhausen, 5. Juli 2019

Der Begriff «Social Engineering» wird für eine Vielzahl von Aktivitäten verwendet. Der passende deutsche Begriff heisst «soziale Manipulation» und zielt darauf ab, durch zwischenmenschliche Beeinflussung von Zielpersonen bestimmte Verhaltensweisen hervorzurufen, wie zum Beispiel die Opfer dazu zu bewegen, vertrauliche Informationen oder Abläufe einer Organisation bekanntzugeben.

Bislang kennen wir das traditionelle «Conventional Social Engineering» und das «Mass Social Engineering» oder «Social Engineering 2.0». Dabei stellt das Zweite eine Erweiterung des Ersten dar. Mit beiden Ansätzen spähen die «Social Engineers» das persönliche Umfeld ihrer Opfer aus, können Identitäten vortäuschen oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um eigentlich klassifizierte Informationen bzw. Informationsfragmente davon zu erlangen oder Dienstleistungen zu missbrauchen.

Die nachfolgende Abbildung zeigt schematisch den groben Prozess des Social Engineerings auf. Dabei korrespondieren die Phasen des «Conventional Social Engineering» mit dem allgemeinen Prozess. Einzelne Phasen können auch mittels «Mass Social Engineering»-Ansätzen ausgeführt werden. Oft wird aber ein kombinierter Ansatz aus beiden Methoden angewendet. Die einzelnen Phasen und ihre Ansätze sind darum in der nachfolgenden Abbildung mit der gleichen Farbe dargestellt.

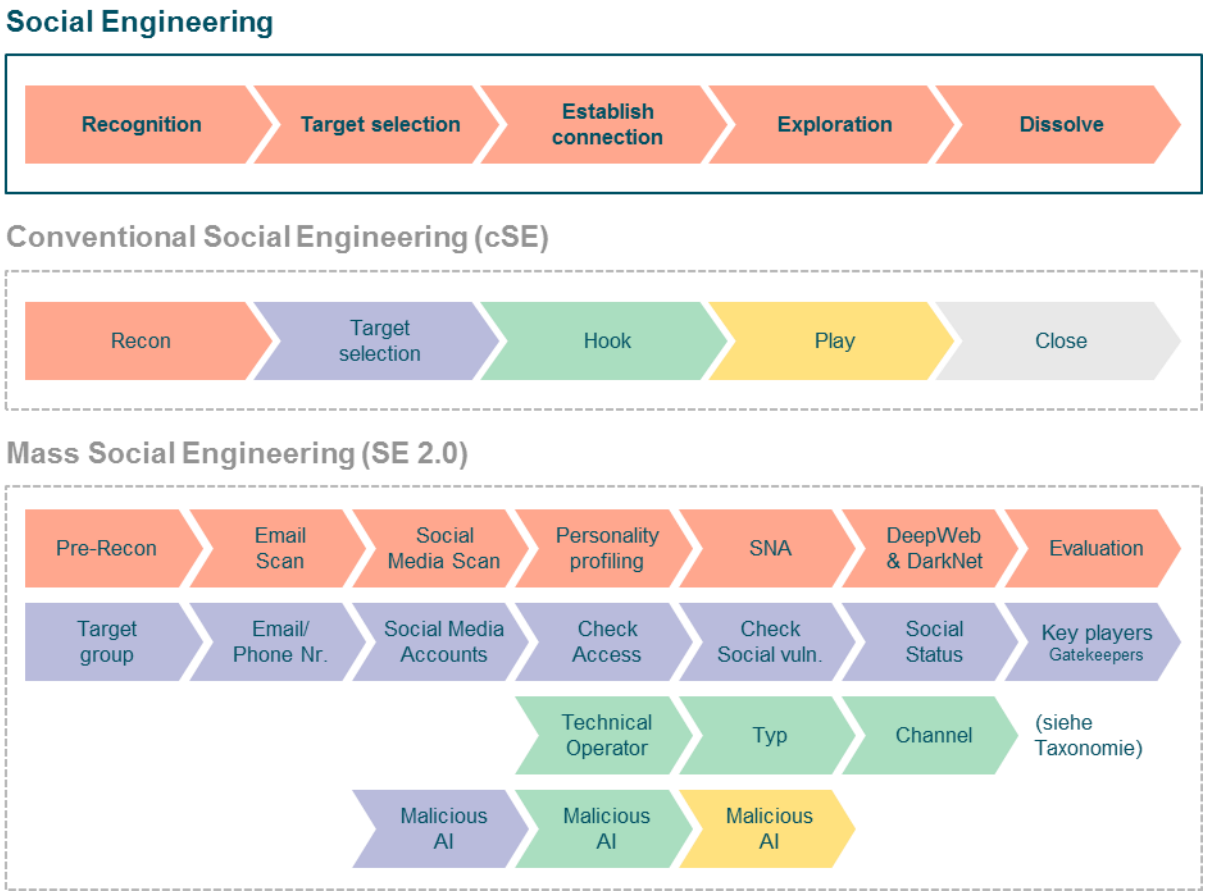


Abbildung 1: Übersicht Social Engineering mit beiden Methoden

Wichtig ist zu wissen, dass unter dem Begriff «Social Engineering» in beiden sich ergänzenden Ausprägungen unzählige verschiedene technische und nicht technische Methoden einzeln oder in Kombination zum Einsatz kommen können. Damit sollen Cyber-Angriffsmethoden entlang der «Cyber-Kill Chain» erfolgreich und zielgerichtet ermöglicht werden. Social Engineering ist in diesem Sinne also ein «Enabler».

Conventional Social Engineering (cSE)

Um eine ungefähre Übersicht über «Conventional Social Engineering» zu bekommen, hilft die nachfolgende Taxonomie.

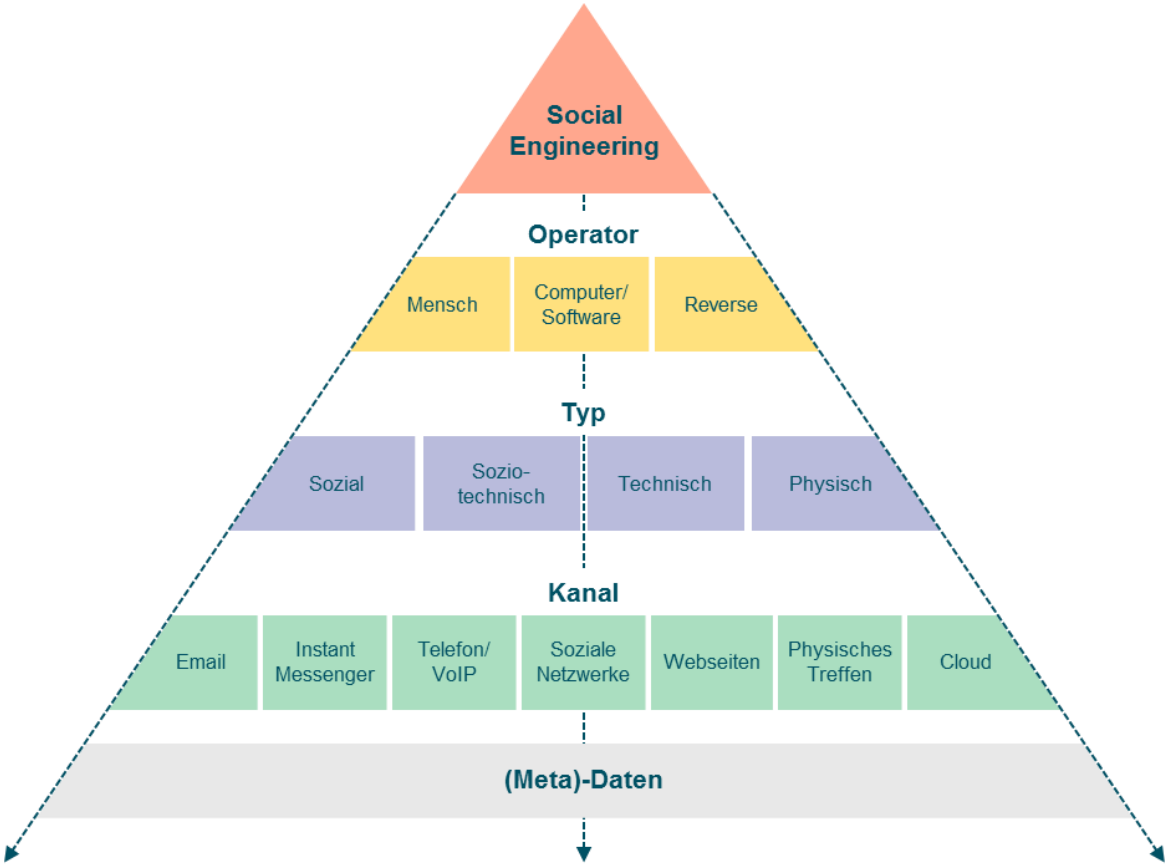


Abbildung 2: Taxonomie von klassischem Social Engineering (Conventional Social Engineering)

Ausgehend von verschiedenen Operatoren (gelb) lassen sich die in den nachfolgenden Kapiteln beschriebenen konventionellen Social-Engineering-Techniken auch jeweils einem Typ (blau) und einem klassischen Kanal (grün) zuordnen. Dabei sind die in der Abbildung aufgelisteten Kanäle nicht abschliessend und unterliegen stark der technologischen Entwicklung im ICT-Umfeld.

Mensch: Human Based Social Engineering

Dies umfasst alle Ansätze, bei denen zielbringende Informationen auf nicht technischem Weg beschafft werden. Diese Methoden zielen auf die Naivität, Hilfsbereitschaft und Unvorsichtigkeit von Menschen ab. Hier besteht bei einigen Formen ein direkter Kontakt zwischen Opfer und Täter, weshalb der Täter in seinem Verhalten besonders darauf achtet, seinen Angriff nicht zu offensichtlich durchzuführen. Typische Vertreter von «Human Based»-Social Engineering sind:

Dumpster Diving	Hierbei handelt es sich um das systematische Durchwühlen von Abfall einer Organisation oder Zielperson zwecks Beschaffung ausrangierter Informationen, die von Wert sind oder die dem Angreifer nützliche interne Informationen vermitteln, die er für seinen Cyber-Angriff (inkl. weiterer Social-Engineering-Aktivitäten) verwenden kann. Es ist nicht die eleganteste Art der Informationsbeschaffung, in ihrer Effektivität jedoch nicht zu unterschätzen. Diese Attacke ist legal, sobald sie auf öffentlichem Gelände stattfindet.

Tailgating	Eine einfache und zielführende Methode, sich unautorisiert Zutritt zu einer eingeschränkt zugänglichen und verschlossenen Örtlichkeit (Gebäude oder Raum) zu verschaffen. Einerseits kann sich der Angreifer hierbei unauffällig in der Nähe des verschlossenen Eingangs aufhalten, bis sich ihm die Möglichkeit bietet, die verschlossene Örtlichkeit zu betreten. Öffnet ein Zutrittsberechtigter die Tür, folgt ihm der Angreifer unauffällig hindurch, bevor sich die Tür schliesst. Ebenso kann er offensiver, z. B. durch einen grossen Gegenstand in den Händen, provozieren, dass ihm die Tür breitwillig aufgehalten wird, oder er kann sich als Service-Mitarbeiter getarnt zusammen mit Angestellten zum Eingang bewegen. Dabei sind die passende Bekleidung, Ausdrucksweise und Pretext sowie richtiger Aufdruck bei Ausweisen Schlüsselelemente.
Shoulder Surfing	Dies bezeichnet den Vorgang, eine Zielperson beim Eintippen an einer Tastatur zu beobachten, um sensitive Informationen (Passwort, PIN, User-Informationen etc.) ausfindig zu machen und zu stehlen. Situationen für die Verwendung dieser Methode sind all jene, bei der eine Zielperson personenbezogene, vertrauliche oder gar sensible Daten in ein Gerät eintippt oder diese bearbeitet. Die Auswahl eines Ziels kann dabei für den Angreifer geplant, aber auch spontan geschehen. Anhand von Aufklebern, die von Geschäften und Behörden gerne auf Notebooks angebracht werden, ist es für einen Social Engineer einfach, schnell zu erkennen, ob es sich um ein potenzielles Ziel handelt.
People Watching	Dieser Angriff erfordert Routine und Erfahrung seitens des Angreifers. Hier tritt dieser nicht direkt in Kontakt mit der Zielperson, sondern beobachtet sie nur. Es handelt sich um eine klassische Profilerstellungsmethode, weil hier auf Besonderheiten der Kleidung, des Verhaltens, mögliche Begleitpersonen, verwendete Aufschriften etc. von Zielpersonen geachtet wird. Zudem werden Vorlieben oder Tätigkeiten beobachtet und wenn nötig mittels technischer Hilfsmittel (z. B. Suchmaschine) genauer bestimmt. Sind alle Eigenschaften der Zielperson analysiert und in einen gemeinsamen Kontext gebracht, kann der Angreifer ein Profil erstellen und entscheiden, welche weiteren zielführenden Methoden oder welche Zielpersonen lohnenswert sind.
Quidproquo	Bei diesem Ansatz sucht der Angreifer direkten Kontakt zur Zielperson und bietet ihr eine Gegenleistung für die Bekanntgabe von interessanten Informationen. Zur Vorbereitung muss der Social Engineer vorgängig vielversprechende Informationsträger ausfindig machen (Screening), entsprechende Hintergrundabklärungen (z. B. Social Media) durchführen und sich dann für eine Methode, das Medium sowie die Gegenleistung entscheiden. Die Kontaktaufnahme kann anschliessend über jedes erdenkliche Kommunikationsmedium erfolgen. Überraschend häufig werden bei diesem Angriff die vom Angreifer gewünschten Informationen preisgegeben. Der Angreifer nützt dabei geschickt die vorhandenen Wünsche, ein mögliches Frustrationspotenzial oder einen Geltungsdrang der Zielperson aus. Diese Methode wird u. a. professionell von Nachrichtendiensten oder Geheimdiensten verwendet.

Pretexting	Der Angreifer kreiert hier ein plausibles, aber falsches Szenario und gibt sich gegenüber der Zielperson als eine autoritäre, vertraute, höhergestellte oder geschulterte Person aus. Mit diesem Verhalten erhofft sich der Angreifer, Einfluss auf die Zielperson ausüben zu können und auf diese Weise Zugang zu sensiblen Daten zu bekommen. Diese Art von Angriff kann über jede Kommunikationsplattform durchgeführt werden, oft erfolgt sie aber telefonisch. Es wird dabei versucht, das Opfer infolge der vorgegaukelten höheren Position, Ausnutzung der Naivität oder durch das erschlichene Vertrauen dazu zu bewegen, die Information preiszugeben.
Badge Surveillance	Ein offiziell aussehender Ausweis mindert das Misstrauen der Menschen drastisch, selbst wenn er an sich nur ein kleines Accessoire ist. Der Begriff «Badge Surveillance» beschreibt die Tätigkeit des Kopierens eines solchen Identifikationsnachweises. Dabei wird der Angreifer unterstützt durch die Tatsache, dass viele Mitarbeiter auch abseits des Firmengeländes ihre Zutrittsausweise sichtbar mit sich tragen. Dadurch erhält er leicht die Gelegenheit, dieses Verhalten zu beobachten und die Ausweise zu fotografieren. So erhält er eine gute Vorlage für seine Kopie, welche er z. B. bei einem «Tailgating» optimal einsetzen kann.
Diversion Attack/ Theft	Diese Art von Angriff wird meist von sehr professionellen Social Engineers durchgeführt. Für dieses Vorgehen ist eine fundierte und vollständige Informationsgrundlage über eine Organisation als Ganzes und ihre vorhandenen und gelebten Prozesse notwendig. Hierbei geht es Kriminellen darum, in existierende Prozesse einzugreifen und dadurch eine finanzielle Bereicherung zu erzielen (z. B. Umleitung eines Geldtransports). Unter diesem Begriff können aber auch nachrichtendienstlich geprägte Angriffe auf ganze Logistikprozesse verstanden werden. Diese Methode erlaubt dem meist staatlichen Angreifer, entsprechende Schadkomponenten hardwarebasiert oder softwarebasiert (Malware) bereits vor der Auslieferung in eingekaufte Produkte (z. B. Arbeitsplatzstationen, Routers und Firewalls etc.) platzieren zu können (klassischer Angriff auf die Supply Chain einer Organisation).

Maschine: Computer Based Social Engineering

Bei dieser Variante wird der Computer als Kontakt- und Täuschungswerkzeug verwendet oder es wird mittels Computer technisch versucht, sensible Daten aus Kommunikationsverfahren oder aus Speicherorten zu extrahieren. Ausserdem können infolge von Social Media extrem viele und wertvolle Randdaten, sogenannte Metadaten, einfach gesammelt werden. Der Social Engineer kann den Computer dazu benutzen, Kontakt mit dem Opfer herzustellen oder eine Täuschung durchzuführen. Ein direkter Kontakt zwischen Täter und Opfer ist hierbei nicht zwingend notwendig. Dadurch ist es für den Angreifer einfacher, seine Identität und somit seinen Angriff zu verschleiern. Trotzdem werden weiterhin menschliche Schwächen ausgenutzt, um an die sensiblen Daten der Opfer zu gelangen.

Typische Vertreter von «Computer Based»- Social Engineering sind:

Evil Twin	Bei diesem Verfahren generiert der Täter ein WLAN mit derselben Kennung (SSID) wie eines, das an dieser Örtlichkeit bereits real verfügbar ist. Dabei übernimmt dieser auch sämtliche weiteren Einstellungen des zu kopierenden Zugangs. Loggt sich ein Nutzer fälschlicherweise in das vom Täter kontrollierte drahtlose Netzwerk ein, kann dieser hier Login-Daten (z. B. Passphrase des richtigen Wireless-Netzwerks) und verwendete IP- und MAC-Adressen der Zielperson auslesen. Auch kann der Angreifer unter Umständen den DNS-Cache der Zielperson verändern und dadurch auf eine gefälschte, aber sehr ähnlich aussehende Webseite weiterleiten.
Typo Squatting	«Typo Squatting» ist eine Abwandlung des Markendiebstahls. Dabei registrieren Betrüger Webdomains, deren URL ähnlich lautet wie die bekannter Marken. Meist ersetzen, entfernen oder vertauschen sie Zeichen, fügen eines hinzu oder ergänzen einen Bindestrich. Dort bauen die Betrüger das Original täuschend echt nach und greifen über falsche Login-Masken Zugangsdaten ab oder leiten Mitarbeitende auf mit Malware infizierte Seiten weiter.
Badge Com Surveillance	Schliesssysteme von Organisationen bestehen immer häufiger aus rein elektronischen Komponenten. Bei diesem Vorgehen findet eine Authentifizierung mittels RFID oder NFC der Zugangsgeräte (Badge, Smartphone etc.) mit einem Lesegerät neben der entsprechenden Türe statt. Nach erfolgreicher Authentifizierung kann die Entriegelung des Schlosses vorgenommen werden. Durch den Besitz des richtigen Zugangsgeräts (wie z. B. des richtigen Badges) wird nur autorisierten Personen Zutritt zu einem Gebäude oder einem Raum gewährt. Bei dieser Methode wird versucht, die Kommunikation zwischen den Zutrittsapparaturen und den mobilen Zugangsgeräten abzufangen und zu kopieren. Hat der Angreifer die genannten Geräte frei zur Verfügung oder befindet er sich in Reichweite der drahtlosen Übertragungstechnologie, kann er entweder den Speicher des vorhandenen Geräts auslesen oder die Übertragung bei einer erfolgreichen Anmeldung abfangen und im Nachgang analysieren und zu brechen versuchen. Ausgehend von einer unzureichenden Verschlüsselung oder zu schwach eingesetzten Schlüsseln ist anschliessend die Kopie mit einem passenden Schreibgerät möglich.
Baiting	Diese Angriffsmethode zielt auf die Neugier und/oder die Gratiskultur (Habgier) von Menschen ab. Dabei werden mobile Speichermedien (USB-Sticks, Speicherkarten etc.) oder sogar ein ganzes Smartphone absichtlich an einem Ort gelassen, wo die Zielperson oder mögliche Zielpersonen einer Organisation diese auffinden können. Um den Anreiz zur Mitnahme zu erhöhen, werden die Datenträger mit Firmenlogos (Konkurrenz oder von exklusiven Organisationen) oder mit attraktiven Begrifflichkeiten versehen (Jahresabschluss – vertraulich, geplante Personalmutationen etc.). Zur Vorbereitung einer «Baiting»-Attacke werden die Datenträger vorgängig mit einer sich automatisch installierenden Schadsoftware (Malware), welche von den verwendeten Anti-

	Virenprogrammen nicht erkannt wird, versehen. Dieses Programm ist meist ein Türöffner zur Herstellung des Kontakts zum Angreifer, damit dieser weitere und zumeist persistente Schadsoftware nachinstallieren kann.
Forensic Analysis	Hier werden die ausrangierten Speichermedien einer Zielperson oder einer Organisation wiederhergestellt und forensisch ausgewertet. Dies meistens im Nachgang zu einer durchgeführten «Dumpster Diving»-Aktion. Ebenfalls denkbar ist bei dieser Methode der gezielte Kauf von Datenträgern über Online-Auktionen oder andere Angebote. In beiden Fällen erhofft sich der Angreifer wichtige Erkenntnisse (elektronische Dokumente, Passwörter, Konfigurationen etc.) der Zielperson oder der anzugreifenden Organisation.
Phishing-E-Mails	Beim klassischen «Phishing» via E-Mail werden elektronische Nachrichten an viele Zielpersonen (zum Beispiel Informatik-Helpdesk oder Finanzabteilung), möglicherweise sogar an alle Kunden einer Organisation verschickt. Diese E-Mails sind nicht personalisiert.
Whaling	Analog zum klassischen Phishing werden unter diesem Begriff aber Angriffe gegen hochrangige Mitarbeitende zusammengefasst. Der Angreifer verspricht sich aufgrund der weitreichenden Entscheidungskompetenzen (inkl. der finanziellen Mittel) sowie der meist weitreichenden Zugriffsberechtigungen dieses Personenkreises einen grossen Erfolg für seinen Angriff.
Clone Phishing	Eine bereits vorher von einer Person oder einer Organisation versandte E-Mail (inklusive Link oder Anhang) wird von einem Angreifer kopiert. Dabei ersetzt der Täter die zusätzlichen Informationen (z. B. den Anhang) durch eine schadhafte Version und schickt die Nachricht ein weiteres Mal an den (die) Empfänger. Dabei wird der Absender verfälscht und zusätzlich eine Art «Update-Hinweis» gegeben, sodass der oder die Nutzer nur die neuere E-Mail beachten.
Spear Phishing	Unter diesem Begriff laufen alle personalisierten Phishing-Angriffe. Oft täuscht der Angreifer dabei vor, Vertrauter oder Freund des Opfers zu sein. Denkbar ist auch eine Rundmail an eine gesamte Gruppe, die einen Bekannten haben (z. B. Mitarbeiter einer Abteilung). In beiden Fällen sind Hintergrundinformationen über das Angriffsziel notwendig, um eine plausible E-Mail verfassen zu können. Dabei wird der Inhalt der Nachricht personalisiert und enthält wiederum einen schadhaften Link oder ein wichtiges mit Schadsoftware versehenes Dokument im Anhang. Infolge des vertrauensvollen Absenders und des personalisierten Inhalts soll die Zielperson auf den Link klicken oder den Anhang öffnen.
Phone Phishing (Vishing)	Hier erhält die Zielperson die Aufforderung, eine bestimmte Telefonnummer zu wählen (z. B. via E-Mail). Ist die Verbindung hergestellt, wird sie entweder durch eine intelligente Interactive Voice Response (IVR) oder von einem Social Engineer aufgefordert, entsprechende sensitive Daten (z. B. Kontoangaben, Passwörter etc.) bekanntzugeben. Wichtig

bei dieser Art von Angriff ist der richtige und konsistente Kontext der Aufforderung und der nachfolgenden IVR-Logik (z. B. Ansage). Diese müssen für die Zielperson plausibel und stimmig sein (z. B. Verwendung des richtigen Banknamens oder der Helpline einer Organisation).

Waterholing

Bei dieser Art von Angriff wird das Ziel bzw. die Zielgruppe vorgängig einem intensiven Profiling-Prozess unterzogen. Ziel dieses Prozesses ist, via Hintergrundabklärungen der Ziele ein gemeinsames (leichter) verwundbares Ziel ausserhalb der anzugreifenden Infrastruktur zu finden (z. B. webbasiertes Onlinereservierungssystem eines gemeinsamen oft frequentierten Restaurants). Danach wird diese externe Infrastruktur für einen Angriff auf die Zielgruppe missbraucht. Dazu wird in einem ersten Schritt mittels entsprechender Exploits die externe Infrastruktur für das Hosting des entsprechenden Ziel-Exploits vorbereitet. Wenn eine der anvisierten Zielpersonen diese präparierte externe Infrastruktur von der anzugreifenden Ziel-Infrastruktur aus (z. B. von der Ziel-Organisationsinfrastruktur aus) mit dem Firmenrechner besucht, wird der Ziel-Exploit für diesen Zielrechner angewendet und nachfolgend eine entsprechende Malware über den infizierten Organisationsrechner in die Ziel-Organisationsinfrastruktur eingeschleust.

Beides: Reverse Social Engineering

Diese Kategorie beinhaltet Methoden, die sowohl mit als auch ohne technische Hilfsmittel auskommen. Das Ziel besteht hier darin, sich die gewünschten Informationen über das Opfer nicht selbst zu beschaffen, sondern die Zielperson dazu zu bringen, diese freiwillig und aktiv an den Social Engineer zu übermitteln. Dazu gibt es grundsätzlich drei «Reverse Social Engineering»-Ansätze:

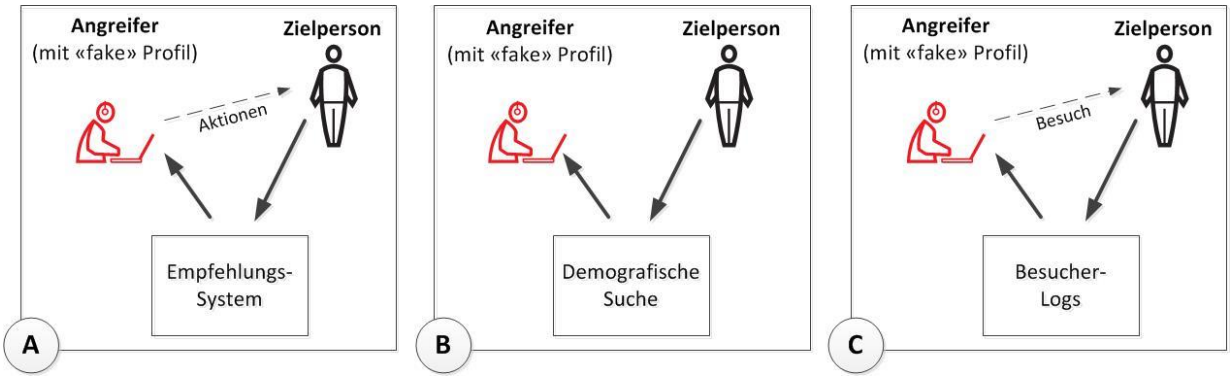


Abbildung 3: Drei Referenzansätze für «Reverse Social Engineering»

(A) Empfehlungssystem

Bei diesem Ansatz wird durch den Angreifer zuerst bei der Zielperson eine Aktion ausgelöst, welche diese in irgendeiner Art und Weise einschränkt. Das Ziel dieser Aktion besteht darin, die Zielperson über ein Empfehlungssystem (z. B. durch ein entsprechendes Pop-up) dazu zu zwingen, den Angreifer zu kontaktieren, damit dieser dabei hilft, das bei der Zielperson hervorgerufene Problem zu beheben. Die tatsächliche Absicht des Angreifers tritt dabei überhaupt nicht in Erscheinung. Klassische Erscheinungen sind hier im Helpline-Umfeld zu finden.

(B) Demografische Suche — In diesem Szenario kennt der Angreifer bereits die Problemstellung, für welches die Zielperson oder die Zielorganisation eine Lösung sucht. Gezielt kann sich der Angreifer jetzt als Lösungsanbieter präsentieren und wird daher durch die entsprechenden Suchanfragen der Zielperson auch gefunden. Somit kann der Kontakt hergestellt werden und entsprechende klassifizierte Informationen, die für die fiktive Problemlösung benötigt werden, können durch den Angreifer erfragt werden.

(C) Besucher-Logs — Hier hat der Angreifer Zugriff auf die entsprechenden Besucher-Logs der Zielorganisation und weiss, mit welchen Kontakten diese in Verbindung stehen und mit welchen Problemstellungen sich die Zielorganisation aktuell beschäftigt. Der Angreifer kann jetzt aktiv einerseits eine bereits etablierte Kundenbeziehung vortäuschen und so an die benötigten Informationen gelangen. Andererseits kann er sich als möglicher Problemlöser bei der entsprechenden Zielorganisation präsentieren und aktiv in einen Dialog treten.

Selbstverständlich können die drei Ansätze auch abgeändert oder in Kombination zum Einsatz kommen. Dies unterliegt ganz der Innovations- und Adaptionskraft des Social-Engineering-Teams.

Mass Social Engineering (SE 2.0)

Der allgegenwärtige Trend der heutigen Gesellschaft, soziale Informationen über private, meist ausländische Anbieter teilen zu müssen, führt zu grossen Mengen von verfügbaren personenbezogenen Daten im Netz. Dieser Trend ist vor einiger Zeit auch in der Industrie angekommen und findet, wenn auch etwas abgeschwächt, bei Behörden Einzug. Zu gross sind die geschäftlichen Vorteile für beide Gruppen, sich damit auf einfache und relativ kostengünstige Art und Weise Präsenz auf ihrem Markt verschaffen zu können, geschäftsrelevante Netzwerke etablieren oder Ansprechgruppen gezielt und schnell erreichen zu können.

Diese neuen Wege, sich schnell privat und geschäftlich kostengünstig vernetzen zu können, haben aber auch eine dunkle Seite. Diese Daten sind im Netz verfügbar und können Social Engineers wertvolle Inhaltsdaten und eine Unmenge kleinerer Randdatenfragmente liefern. Oft argumentieren die Betroffenen damit, dass die preisgegebenen Daten unkritisch bzw. zu unbedeutend sind. Zudem sehen sie die so produzierten Metadaten-Fragmente als wertlose unstrukturierte Datenmengen an, ohne jeglichen Nutzen.

Diese Ansicht stimmt jedoch nur bedingt, denn diese Daten-Puzzleteile sind sehr einfach durch Maschinen les- und bearbeitbar. Damit können diese Unmengen scheinbar zusammenhangloser Daten unter dem Begriff «Big-Data-Analyse» sehr effizient durch Rechenmaschinen zu einem sehr individuellen und aussagekräftigen Gesamtbild einer Person, einer Organisationseinheit oder einer Unternehmung zusammengefügt werden. Dies gilt sowohl für Privatpersonen und Unternehmen aus der Industrie als auch für Personen und Organisationseinheiten von Behörden.

Diese neuen verfügbaren Daten und effizienten maschinellen Verarbeitungsmöglichkeiten führten in den letzten Jahren auch im Social Engineering zu einer adaptiven Weiterentwicklung. Infolge dieser immens grossen verfügbaren Datenmengen verwenden die Experten für diese Erweiterungsansätze auch den Begriff «Mass Social Engineering» oder sprechen kurz von SE 2.0 (Social Engineering 2.0). Zusammenfassend beinhaltet modernes SE 2.0 nachfolgende Charakteristika:

Beschreibung Charakteristika
… fast vollständig automatisiert
… basiert auf grossen Mengen von maschinenlesbaren Daten
… ist interdisziplinär (verwendet verschiedenste Wissenschaften)
… läuft nach wirtschaftlichen Grundsätzen ab
… beinhaltet weiterhin das klassische Social Engineering
… ist auch auf Remote-Targets anwendbar
… ist noch besser auf das individuelle Ziel abgestimmt (targeted)

Tabelle 1: Charakteristika von SE 2.0

Automatisiert und Interdisziplinär

Wie aus der oben stehenden Tabelle ersichtlich ist, beinhaltet das heutige moderne Social Engineering sowohl die klassischen Ansätze des «Conventional Social Engineering» als auch neue Social-Engineering-Ansätze, welche diese massenhaft verfügbaren organisations- und personenbezogenen Daten gezielt berücksichtigen und fast vollständig automatisiert be- bzw. aufarbeiten können.

Während früher die klassischen Social Engineers meistens aus dem technischen Umfeld stammten, bestehen heutige erfolgreiche Teams aus Vertretern vieler unterschiedlicher Berufsbilder, welche eng miteinander zusammenarbeiten. So kann ein heutiges Social-Engineering-Team beispielsweise auch eine Fachperson mit abgeschlossenem Psychologie-Studium und/oder Marketingexperten umfassen, die eng mit Datenanalysten und Machine-Learning-Experten zusammenarbeiten.

Durch diese Team-Diversität und den Einsatz computergestützter Verfahren werden die bisherigen traditionellen Ansätze verbessert, vervollständigt, automatisiert und dadurch enorm erweitert.

Aufklärungsphasen (Recon)

Die Aufklärungsphase ist eine der wichtigsten Phasen und basiert innerhalb des SE 2.0 hauptsächlich auf öffentlich verfügbaren Quellen (sog. OSINT), auf der Auswertung von sozialen Medien (sog. SOCMINT) und auf anderen Datenanalyse-Techniken. Folgender Ablauf kommt dabei typischerweise zur Anwendung:

Pre-Recon	Sie dient dazu die Zielperson oder -Organisation kennenzulernen. Der Angreifer möchte dabei die nachfolgenden Informationen aufspüren: • Organisationsstruktur • Angebotene Produkte und Dienstleistungen • Vorhandene Geschäftsmodelle • Partnerlandschaft (Fokus auch auf zukünftige) • Mitbewerber • Finanzielle Hintergründe • Aktuelle/ehemalige Mitarbeitende • Stellenausschreibungen
Google Advanced Search	Viele zusätzliche Informationen können via spezielle Suchoperatoren im Netz gefunden werden. Dazu gehören eine grosse Varietät von Advanced Google Searches, Reverse Image Lookups und sogenannten «Google Dorks». Hierzu existieren entsprechende Dokumentationen bei Google Support und bei MIT. Entsprechende Google Dorks können in der Google Hacking Data-

	base ermittelt werden. Mittels eines individuellen Scripts können so Suchoperationen zielbringend kombiniert und automatisiert werden und somit im Netz schwer auffindbare Informationen gezielt gefunden werden.
Robot Exclusion Protocol	Das Robot Exclusion Protocol (robots.txt) wird standardmässig von Webcrawlern genutzt. Dieses spezifiziert, welche Informationen von einer Suchmaschine auf einer Zielwebsite automatisch gesucht und von ihr heruntergeladen werden sollen.
Metadaten-Analyse	Um Metadaten von einer Zielperson oder Organisation extrahieren und analysieren zu können, eignet sich das öffentlich verfügbare **F**ingerprinting **O**rganisation with **C**ollected **A**rchives (FOCA). Das Tool scannt die populären Search Engines (z. B. Google, Bing etc.) und sucht nach Dateien mit einer Beziehung zur Webdomain der Organisation. Danach werden diese Dateien heruntergeladen und lokal auf interessante Metadaten hin analysiert.
System- und Infrastruktur-Analyse	Hier werden voll automatisiert mit verschiedensten kombinierten «Fingerprinting-Tools» entsprechende Informationen über die vorhandene IT-Infrastruktur der im Einsatz stehenden Systeme und benutzten Applikationen gesammelt. Je nach Sicherheits-Awareness des aufzuklärenden Ziels können dabei rein passive Scanner oder auch halb-aktive Programme zum Einsatz kommen.
E-Mail-Adressensuche	Mit einem intelligenten «E-Mail crawler» werden die «Anti-crawling»-Erkennungsmechanismen der modernen Suchanbieter umgangen. Diese Intelligenz beinhaltet typischerweise emulierte Webbrowser Sessions mit wechselnden User-Agents und entsprechenden zufälligen Zeitverzögerungen. So können indexierte Webseiten-Inhalte und dazugehörige Dokumente automatisch nach Domänen-spezifischen E-Mail-Adressen von aktuellen und ehemaligen Mitarbeitenden abgesucht werden. Hierbei ist es wichtig, dass nicht nur die Organisationsdomain-Namen untersucht werden, sondern auch mögliche private Domainnamen.
Identifikation von Mitarbeitenden und ihren Social Media Accounts	Nachdem die E-Mail-Adressen bekannt sind, können diese in einem ersten Schritt auf die Verwendung in den diversen Social-Media (LinkedIn, Facebook, Xing, Twitter etc.) hin überprüft werden. Dies kann automatisiert mit entsprechenden angepassten FOSS-Tools geschehen (z. B. Scythe etc.). Dieser erste Schritt kann dem Social-Engineering-Team wertvolle zusätzliche psychologisch verwertbare Informationen vermitteln. Zudem ist es neben der allfälligen E-Mail-Adresse ein zweiter effektiver Social-Media-Kanal, welcher zu einem späteren Zeitpunkt für eine gezielte Phishing-Kampagne genutzt werden kann. In einem zweiten Schritt werden die gefundenen Social Media Posts der Mitarbeiter (meistens mittels KI) auf verschiedene

	Personalitätsmerkmale hin analysiert. Diese Merkmale umfassen mehrheitlich Offenheit, Extravertiertheit, Neurotizismus, Bescheidenheit und Gewissenhaftigkeit, und das Machine Learning wird innerhalb von professionellen Social-Engineering-Teams von Experten mit fundiertem psychologischem Background begleitet.
Social Network Analysis (SNA)	Bei diesem Schritt werden alle Verbindungsdaten der gefundenen Social Media Accounts systematisch innerhalb der gleichen Organisation analysiert und grafisch dargestellt (z. B. mit i2 Analyst Notebook). Danach werden innerhalb dieser gefundenen Strukturen die Muster mit allfälligen Schwachstellen extrahiert. Solche Schwachstellen können nachfolgende Strukturen aufweisen: • (A) Zentraler Node: Person mit zahlreichen sternförmig ausgeprägten Verbindungen. • (B) Privilegierter Node: Ziel, an welchem viele anderer Nodes hierarchisch angehängt sind. • (C) Individueller Node: mögliche Zielperson, welche zu mehreren Nodes Verbindungen aufweist, wo aber die anderen Nodes keine direkten Verbindungen zueinander aufweisen.

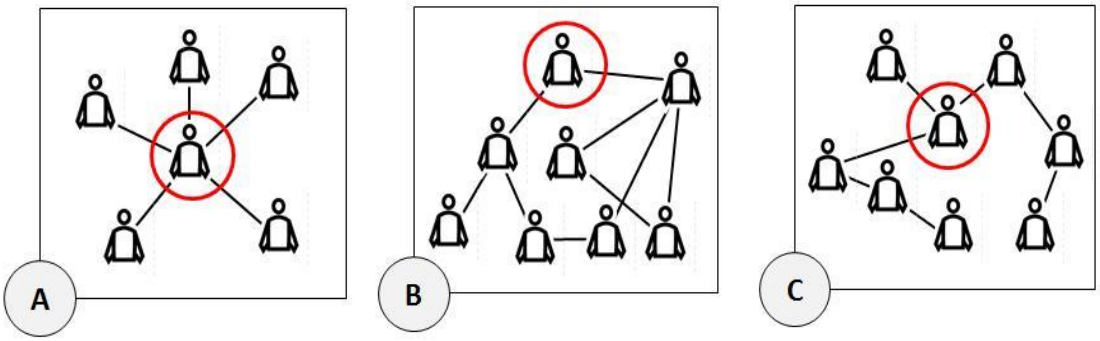


Abbildung 4: A-C – Schwachstellenmuster innerhalb von Social-Media-Strukturen

Deep-Web- & Darknet-Suche	Dabei wird im Deep Web & Darknet gezielt nach allfälligen zusätzlichen Informationen über Organisationen und Personen gesucht, welche sonst nicht öffentlich auffindbar sind. Dazu werden automatisiert Foreneinträge, WayBack Machines und Seiten wie «Pastebin» durchforstet. Die so gefundenen Erkenntnisse sollen das bereits erhaltene Bild bestmöglich ergänzen.

Zielauswahlprozess (Target selection)

Nachdem sämtliche verfügbaren Informationen über die Zielperson(en) oder die Organisation gesammelt und voranalysiert wurden, geht es beim nächsten Schritt darum, geeignete Ziele zu finden. Dazu wird der nachfolgende Selektionsprozess (siehe Tabelle 2 und Abbildung 1 «Target selection») durchgeführt. Dabei werden die Erkenntnisse der Aufklärungsphase zusammengeführt.

Schrittname	Task	Recon-Aggregation
Zielgruppe(n) identifizieren	Identifikation von Zielgruppen innerhalb und allenfalls ausserhalb (z. B. Partner/Lieferanten) der Zielorganisation	• Pre-Recon • Google Dorks • FOCA • SNA-Analyse
Extrahieren von: • E-Mails • Telefonnummern • Infrastrukturdaten • ID Social-Media-Konten	Anhand der festgelegten Zielgruppen werden die dazugehörigen und verwendeten elektronischen Kommunikationsmittel eruiert. Zusätzlich werden die vorhandenen Infrastrukturdaten (Hardware und Software), in welche diese Mittel eingebettet sind, zugeordnet.	• Pre-Recon • FOCA • E-Mail-Adressensuche • Identifikation Social Media • Fingerprinting • Deep Web / Darknet
Prüfen der Zugänge • Infrastruktur • Social Media Accounts	Bei diesem Schritt werden die gefundenen Mittel und Infrastruktur-Geräte auf ihre Zugänglichkeit hin geprüft. Dies beinhaltet die Überprüfung, ob die Konten zugänglich sind und die vorhandene Infrastruktur verwundbar ist (z. B. durch Abgleich der eigenen Exploit-DB).	• Pre-Recon • Fingerprinting • SNA-Scan
Psychologische Profilerstellung	Anhand der aufgefundenen Social Media Accounts, der Verbindungen und abgegebenen Informationen (Posts) wird ein psychologisches Profil der verbliebenen Zielpersonen erstellt und beurteilt.	• SNA-Post-Analyse • SNA-Strukturanalyse • Deep Web / Darknet
Bestimmen des Status • Innerhalb der Organisation • Sozialer Status	Anhand der Organisationsstruktur, der SNA-Struktur (welche auch die gelebte Struktur innerhalb einer Organisation wiederspiegeln können) und des psychologischen Profils wird bzw. werden die vielversprechendste(n) Zielperson(en) definiert.	• Pre-Recon • SNA-Strukturanalyse • psychologische Profile
Definieren von Zielpersonen (Gatekeepers)		

Je nachdem welche Absichten und welche Zielsetzung der Angreifer hat, kann er nun den geeigneten Angriffskanal wählen und z. B. personifiziert entsprechende Phishing-E-Mails vorbereiten oder bei einer Diversion-Attacke entsprechende Schlüsselpersonen mit konventionellen Social-Engineering-Methoden angehen (Hook-Phase) und versuchen, in den Logistikprozess einzugreifen.

Schutzmassnahmen (Mitigation)

In vielen Unternehmen und Organisationen existieren bereits etablierte Sicherheitsprozesse, die Mitarbeitenden helfen sollen, sich gegen Cyber-Angriffe (inkl. Social Engineering-Ansätze) zu schützen. Häufig sind diese aber von IT-Abteilungen aus der technischen Perspektive heraus entwickelt und lassen die Möglichkeit der kontinuierlichen Verbesserung des Menschen ausser Acht. Zudem sind diese Security-Direktiven oft für die Mitarbeitenden unverständlich oder umständlich in der Anwendung, sodass sie die vorgegebenen Prozesse am Ende nicht einhalten – sprich nicht leben. Es gilt also, diese Abläufe genau zu prüfen und sie im Dialog mit den Anwendern auf die Praktikabilität, aber auch auf die Effektivität hin zu optimieren. Dafür sind Soft Skills essentiell.

Mitarbeitende aus dem Sicherheitsteam mit technischem Hintergrund stecken meist sehr tief in der Materie. Es fällt ihnen daher manchmal schwer, die Perspektive des anderen Mitarbeitenden einzunehmen. Aus unserer Erfahrung sind Sicherheitsprogramme schneller erfolgreich, wenn kommunikationsstarke Mitarbeitende mit nicht technischem Hintergrund Teile dieses neu zu etablierenden Sicherheitsprozesses sind. Hier eignen sich beispielsweise Kollegen aus den Marketing- oder Kommunikationsabteilungen oder aber ein externer Dienstleister besser.

Es ist zudem empfehlenswert, die Organisation von aussen einem Social Engineering Scan zu unterziehen. Einerseits kann so initial festgestellt werden, welchen «Footprint» das Unternehmen aktuell hat und in welchem Bereich angesetzt werden muss. Andrerseits kann mit einem solchen Aussen-Scan auch beurteilt werden, ob die etablierten Massnahmen greifen.

Die eigentlichen internen Eindämmungsmassnahmen selbst müssen sich an einer Mischung aus individuellen Schulungen, Trainings, Simulationen und Tests orientieren. Sie sollen vor allem die technischen IT-Sicherheitsmassnahmen des Unternehmens optimal ergänzen können. Sie sollen so gestrickt sein, dass sie das Sicherheitsniveau verbessern und dauerhaft von Mitarbeitenden akzeptiert werden. Dazu ist es wichtig, die Massnahmen individuell auf die Zielgruppen zuzuschneiden. Dabei sind Mitarbeitende mit starken Soft Skills in die einzelnen Zielgruppenprogramme zu integrieren.

Je nach Position und Funktion sollten dabei für die Tests dezidierte Social-Engineering-Vektoren eingesetzt werden. Finanzabteilungen sind beispielsweise begehrte Ziele von «CEO-Fraud» oder gefälschten E-Mail-Rechnungen und sollten verstärkt dafür sensibilisiert werden. Personalabteilungen sollten beispielsweise über Malware in E-Mail-Anhängen wie Lebensläufen und über Phishing-Attacken auf sensible Mitarbeiterinformationen informiert werden. Mitarbeitende in einem Warenlager oder im Einzelhandel sollten zudem auch auf physische Sicherheitsmassnahmen geschult werden.

Eines ist bei diesem Prozess klar: Persönliches Engagement in Sachen Sicherheit seitens der Belegschaft ist nicht selbstverständlich und lässt sich auch nicht erzwingen. Es ist eine kulturelle Entwicklung, die langfristig aktiv gefördert und gelebt werden muss.

CyOne Security ist der vertrauensvolle Partner für Social Engineering Optimierung

Die Schwachstelle Mensch gegen die steigende Flut von Social-Engineering-Attacken abzudichten, ist eine vielschichtige Angelegenheit. Es gilt, alle Ebenen – von der Geschäfts- und Organisationsführung bis zu den einzelnen Abteilungen – zu involvieren, eventuelle interne Hürden zu überwinden und die dafür notwendige Security Awareness als strategisches Ziel zu etablieren.

Die CyOne Security unterstützt Sie dabei, eine angepasste Awareness-Kampagne zusammenzustellen sowie eine neutrale aussagekräftige Aussen-Analyse Ihres Social Engineering «Footprints» durchzuführen. Dies abgestimmt auf die Sicherheitsbedürfnisse Ihrer Organisation.

Setzen Sie auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau.

Beginnen Sie noch heute, Ihre Organisation gegen die steigenden Gefahren der neuen Social-Engineering-Methoden zu schützen.

Machen Sie den ersten Schritt: Analysieren und verbessern Sie gemeinsam mit unseren Cyber-Security-Experten die Social-Engineering-Resilienz Ihrer Organisation.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.