Bundeskriminalamt

Social Engineering / CEO-Fraud

Aufbereitung aktueller nationaler Forschungsbeiträge und Publikationen

IZ 34

Heike Bruhn

Stand: Oktober 2017

BKA

Inhaltsverzeichnis

1. EINLEITUNG 1

2. METHODIK 1

3. AUFBEREITUNG AKTUELLER NATIONALER FORSCHUNGSBEITRÄGE UND PUBLIKATIONEN 2

3.1 Studien und Bücher 2

known_sense (Beratungsunternehmen): Bluff me if U can – gefährliche Freundschaften am Arbeitsplatz (Studie 2015) sowie: Gefahren und Abwehr bei Social Engineering - Selbst mal ein Schwein sein...(Fachartikel 2015) 2

3.2 Fachartikel zum Thema Social Engineering (SE) 7

Hellerforth, Michael: Wirtschaftskriminalität: Social Engineering - So manipulieren Industriespione ihre Opfer. In: WirtschaftsWoche (2015) 7

Schumacher, Stefan: Die psychologischen Grundlagen des Social Engineerings (2013/2014 und 2011) 11

3.3 Fachartikel zum Thema CEO-Fraud 14

Kunze, Dirk: „Millionenbeute durch clevere Betrüger“ (2016) sowie „Enkeltrick 4.0 - Wenn der falsche Chef Geld will (2016) 14

3.4 Laufende Forschungsprojekte 18

Scholl, Margit u.a.: Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg. TH Wildau, 2017 sowie Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt (2016) 18

3.5 Relevante Veranstaltungen, Experten und sonstige Veröffentlichungen 2017 22

3.6 Europol Erkenntnisse 24

4. FAZIT 25

LITERATURVERZEICHNIS 27

Ausgewertete Publikationen 27

Zusätzliche Quellen 28

1. Einleitung

Der vorliegende Bericht hat das Ziel, den aktuellen Forschungsstand zum Thema „Social Engineering (SE)“ und „CEO-Fraud“ der letzten fünf Jahre (2012 – 2017) in Deutschland wiederzugeben.

2. Methodik

Im Mai und Juni 2017 wurde u.a. zu dieser Thematik eine internetbasierte Literaturrecherche durchgeführt. Zu den Schlagworten „President Fake“ und „Social Engineering“ gab es in den durchsuchten Datenbanken[1] für den Zeitraum 2012 – 2017 sehr wenige Treffer. Zum Schlagwort „CEO-Fraud“ fanden sich bei SpringerLink 465 Treffer, die überwiegend englisch-sprachige Studien anboten. Die meisten deutschsprachigen Studien, die sich, überwiegend mit den psychologischen und sozialwissenschaftlichen Grundlagen zum Phänomenbereich beschäftigen, lagen vor 2012.[2] Letztendlich konnten 12 Treffer zur Kurzbewertung und Sichtung im deutschsprachigen Raum identifiziert werden. Daher wurde im September 2017 zusätzlich eine OSINT-Recherche zu den Schlagworten durchgeführt. Ziel war, neben den wissenschaftlichen Texten, die aktuellen Publikationen und den aktuellen Diskussionsstand zur Thematik zu finden, auch, wenn dieser nicht in wissenschaftlichen Datenbanken dokumentiert ist. Somit konnte die wissenschaftliche Basis sinnvoll mit aktuellen praxisnahen (Phänomen-) Erkenntnissen abgerundet und ein realitätsnahes Gesamtbild aufgezeigt werden. Insbesondere Publikationen von Autoren aus der Sicherheitsbranche, die konkret für Unternehmen als Zielgruppe schreiben, Verbänden und ein aktuelles Projekt wurden so gefunden.

Im vorliegenden Bericht wurden nur deutschsprachige Veröffentlichungen berücksichtigt. Die Betrachtung der englischsprachigen Literatur müsste, bei Bedarf, in einem gesonderten Bericht erfolgen. Die Reihenfolge der zusammengefassten Werke, falls in einer Kategorie mehrere bearbeitet wurden, orientiert sich am Erscheinungsdatum.

Wenn es auch wenig spezielle deutsche Literatur zu SE gibt, so findet man Ausführungen dazu traditionell häufig in Werken über Spionage, da hierbei schon immer der Mensch als Angriffsziel im Mittelpunkt stand. Früher durch Direktkontakte, heute häufig über elektronische Medien oder Telefon. Daher lohnt bei Beschäftigung mit SE auch immer der Blick in Werke zur Spionagethematik oder allgemein zum Thema Innentäter in Unternehmen.[3]

[1] Diese waren: SpringerLink, KrimDok, Bibliothekskatalog des MPI, KrimLit, COD und OPAC des BKA und Bibliothekskatalog der Uni Mainz.
[2] Aus diesem Grund wurde auch ein Artikel von Schumacher aus dem Jahr 2011 miteinbezogen. Die Aussagen fassen den diesbezüglichen Forschungsstand sehr gut zusammen und die Literaturliste ist umfassend.
[3] In diesem Zusammenhang wird auf den Monitoringbericht „Innentäter in Unternehmen“, IZ 34, Julia Weber, Stand 08/17, verwiesen.

3. Aufbereitung aktueller nationaler Forschungsbeiträge und Publikationen

3.1 Studien und Bücher

known_sense (Beratungsunternehmen): Bluff me if U can – gefährliche Freundschaften am Arbeitsplatz (Studie 2015) sowie: Gefahren und Abwehr bei Social Engineering - Selbst mal ein Schwein sein...(Fachartikel 2015)

Gegenstand: Die Studie verdeutlicht die Aktualität der Gefahren für SE und erforscht passende Awareness-Maßnahmen. In dem Fachartikel wird über die Studie und die Ergebnisse berichtet.

Der Studie liegt die *Definition* des Verfassungsschutzes Brandenburg zugrunde: „Social Engineering ist der Versuch unter Ausnutzung menschlicher Eigenschaften Zugang zu Know-how zu erhalten. Der Angreifer nutzt dabei Dankbarkeit, Hilfsbereitschaft, Stolz, Karrierestreben, Geltungssucht, Bequemlichkeit oder Konfliktvermeidung aus. Dabei bieten häufig soziale Netzwerke oder auch Firmenwebseiten Möglichkeiten, um sich auf sein Opfer gründlich vorzubereiten. Zu diesen „Vorfeldermittlungen" können auch Anrufe im Unternehmen gehören. Professionelle Angreifer versuchen dabei nicht, mit einem Anruf alle gewünschten Informationen zu erlangen, dies könnte misstrauisch stimmen. Der Angerufene wird dabei im Gespräch nach vermeintlich nebensächlich erscheinenden Informationen gefragt*." Kurzfassung Definition Studie*: Social Engineering ist eine zwischenmenschliche Manipulation, bei der ein Unbefugter unter Vortäuschung falscher Tatsachen versucht, unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen.

Die *Autor*en: *Dietmar Pokoyski* ist Fachbuchautor und Geschäftsführer der Kommunikationsagentur known_sense, die seit 2005 Awareness-Maßnahmen für Kunden wie T-Systems, Deutsche Telekom, E.ON oder auch Bosch durchführt. *Ivona Matas* ist Dipl.-Psychologin, Therapeutin, Marktforscherin und Gutachterin. Bei known_sense u.a. verantwortlich für die Durchführung von tiefenpsychologischen Security-Wirkungsanalysen, Begleitung von Kampagnen mithilfe qualitativer Wirkungsforschung, Führungskräfte-Entwicklung, Präsenztrainings und Social-Engineering-Maßnahmen bzw. Awareness im Kontext personeller Sicherheit. *Dirk Fleischer* ist Kriminologe und seit mehr als 25 Jahren im Bereich der öffentlichen und privaten Sicherheit tätig.

Projektpartner: Technische Hochschule Wildau (Fachbereich Wirtschaft, Informatik, Recht (WIR), Prof Dr. Margit Scholl), LANXESS Deutschland GmbH (Corporate Security), <kes> - Die Zeitschrift für Informations-Sicherheit

Ziele: Konkrete Gefahren des SE identifizieren, konkrete Awareness-Maßnahmen für Unternehmen entwickeln.

Forschungsfragen: Aus dem Blickwinkel der Informationssicherheit und mit dem Ziel der Verwertbarkeit innerhalb der Corporate Security von Unternehmen wurde in dieser Studie das konkrete Kommunikationsverhalten von Beschäftigten betrachtet, um Erkenntnisse zu folgenden Fragen zu gewinnen:

- Welche Kommunikationslandkarten lassen sich bei der privaten und beruflichen Kommunikation erstellen?

- Wie sind die Themen Sicherheit, Cybercrime und insbesondere Social Engineering in den Unternehmen verankert? Sind Methoden der Sozial-Ingenieure bekannt - und wie schützt man sich vor ihnen?
- Welche Umgangsformen mit Kommunikation, Informationssicherheit und Risiken bzw. Angriffen lassen sich beschreiben und welche typologischen Konsequenzen daraus ableiten?
- Welche Rolle spielen Sicherheits- und Führungskultur und lassen sich hinsichtlich Größe oder Branche Unterschiede zwischen den Unternehmen erkennen?
- Welche psychologischen Eigenheiten lassen sich im Kontext Social Engineering beschreiben bzw. welche „Vorteile" erwachsen Mitarbeitern, die Angriffsflächen bieten?
- Welche Awareness-Maßnahmen für diese Form der Wirtschaftsspionage sind bekannt und wie sind die verschiedenen Instrumente hinsichtlich Impact und Nachhaltigkeit zu bewerten?
- Welche Empfehlungen lassen sich ableiten, um die Mitarbeiter von Unternehmen vor den Methoden des Social Engineering zu schützen, und welche Awareness-Maßnahmen werden von den Mitarbeitern selbst „gewünscht" oder als sinnvoll angesehen?

Zur *Methodik*[4]: Die Studie nennt sich im Untertitel: „Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr". Die Ergebnisse beruhen auf zwei Interviewreihen, bei denen jeweils 90- bis 120minütige tiefenpsychologische Interviews durchgeführt wurden:

- eine interne Wirkungsanalyse bei einem known_sense-Kunden im Juli 2012, bei der 20 Mitarbeiter explizit zum Thema Social Engineering befragt wurden,
- eine Befragung von 15 berufstätigen Personen im November und Dezember 2014 zu ihrem beruflichen und privaten Kommunikationsverhalten, wobei vorausgesetzt wurde, dass digitale Kommunikationsmedien sowohl im Beruf wie auch privat täglich und aktiv genutzt werden.

Alle Probanden

- nutzten beruflich einen PC mit Internetanschluss,
- telefonierten häufig in ihrem beruflichen Kontext,
- verfügten zu Hause über einen Internetanschluss und nutzten diesen regelmäßig,
- verfügten über ein internetfähiges Mobiltelefon und nutzten dieses häufig.

Explizit zum Thema Social Engineering befragt wurden 35 Personen:

- 14 Frauen und 21 Männer
- 12 Führungskräfte und 23 Mitarbeiter ohne Leitungsfunktion, verteilt über drei Altersklassen (20 bis 30 Jahre, 30 bis 45 Jahre, 45 bis 65 Jahre)

[4] Die Begriffe „morphologische Markt- und Medienforschung" sowie „psychologische Tiefeninterviews" werden folgendermaßen erläutert: „Auf Basis der morphologischen Psychologie, die an der Universität Köln entwickelt worden ist, analysieren Diplom-Psychologen die unbewussten seelischen Einflussfaktoren und Sinnzusammenhänge, die das Handeln mitbestimmen. Mit oft überraschenden Ergebnissen. Beim psychologischen Tiefeninterview wird so tief „gegraben", bis die Psychologen in der Lage sind, die psychologische Wurzel eines Phänomens erkennen und beschreiben zu können. Eine damit verbundene Darstellung gerät so breit und umfassend, wie es die jeweilige Fragestellung pragmatischer Weise erfordert. In den hier 2012 und Ende 2014 in zwei Samples durchgeführten 35 zweistündigen Einzelinterviews konnten so die unbewussten seelischen Wirkungen und Einflussfaktoren evaluiert werden, die das Verhalten aller von Social Engineering betroffenen Personen men." Pokoyski, Dietmar (2015): Url: https://www.it-finanzmagazin.de/tiefenpsychologische-cybercrime-studie-bluff-me-if-u-can-es-fehlt-an-notfallplaenen-und-awareness-12927/ .

- Branchen: Telekommunikation, Auto, Pharma, Chemie, öffentlicher Dienst, Banken, Dienstleister

Untersuchungszeitraum:

- Sample 1 im Juli 2012 (20 Interviews)
- Sample 2 im November/Dezember 2014 (15 Interviews)

Untersuchungsraum:

- Deutschlandweit mit Schwerpunkt im Raum Köln-Bonn

Methodik der Untersuchung

- Morphologische Markt- und Medienforschung

Psychologische Projektleitung:

- Dipl. Psychologin Ankha Haucke
- Dipl. Psychologin Ivona Matas.

Ergebnisse:

- Der Begriff ist (etwa im Gegensatz zu Phishing) allen Befragten unbekannt - und wird fälschlicherweise oftmals mit positiven Assoziationen verbunden. Es wird sogar nach konkreten „Weiterbildungsmöglichkeiten zum Social Engineer“ gefragt. Die Vorlage der o. a. Definition führt bei vielen Befragten zu Enttäuschung und Unmut: Es wird Ärger über den irreführenden englischen Begriff laut.
- Der vordergründig souveräne Umgang mit allen digitalen Kommunikationskanälen führt zunehmend zu einer Auflösung der Unterscheidung von analoger und digitaler Kommunikation. Diese Vermischung führt zu Risiken, da die zusätzliche Prüfung des Gegenübers in einer Face-to-Face-Situation (Mimik, Gestik, Gesamtperformance) wegfällt.
- Vormals klar definierte Grenzen zwischen privat und öffentlich verwischen - eine neue Definition von Privacy (Informationssicherheit/ Datenschutz) ist für viele (noch) nicht präsent. Es herrschen z. T. nur noch kleine Unterschiede zwischen beruflichem und privatem Kommunikationsverhalten.
- Der „erfolgreiche" Social Engineer ist insgesamt sowohl technisch versiert und kennt die richtigen psychologischen Kniffe. Wobei das technische Know-how nicht unbedingt auf Hacker-Niveau sein muss, es reichen zunächst gute Kenntnisse über soziale Netzwerke.
- SE funktioniert, weil normale menschliche Eigenschaften ausgenutzt werden.
- In der Studie wurden fünf gefährdete Mitarbeiter-Typen herausgearbeitet. Diese Typen entsprechen nicht einem konkreten Menschen, sondern typischen Umgangsformen. So können durchaus einzelne Personen mehrere Typen in sich tragen und - je nach Verfassung - zwischen diesen switchen:
    - Naive Dauersender (lieben ständigen Kontakt zu bekannten und weniger bekannten Menschen, fühlen sich aber selber als zu unbedeutend, um für einen Social Engineer interessant zu sein) -> sehr hohes SE-Risiko, bieten eine große Angriffsfläche; mittlere Awareness-Eignung

    - Unbekümmerte Mitläufer (offen für Neuerungen, wollen immer dabei sein. SE „versaut“ diese schöne, heile Kommunikationswelt und weckt Schamgefühle) -> hohes SE-Risiko, aber auch hohe Awareness-Eignung
    - Versierte Netzjunkies (bewegen sich souverän auf dem neuesten Stand der Technik, sind durch „Menschliches" allerdings schnell überfordert) -> hohes SE-Risiko, geringe Awareness-Eignung
    - Skeptische Verweigerer (bewegen sich kritisch in der Kommunikationslandschaft und machen keinesfalls überall mit. SE ist das Problem der anderen, die zu unkritisch waren) -> hohes SE-Risikopotential aufgrund der Anfälligkeit in analogen Kommunikations-Settings, mittlere Awareness-Eignung
    - Vorsichtige Pragmatiker (betrachten die Möglichkeiten der modernen Kommunikation sorgfältig auf ihren Nutzen hin. SE führt entweder zu selbstkritischen Einsichten oder Resignation) -> geringes SE-Risiko, hohe Awareness-Eignung
- Es wurden 6 soziale Einfallstore und Mental Shortcuts identifiziert:
    - Hilfsbereitschaft
    - Leichtgläubigkeit
    - Neugier
    - (Wunsch nach) Anerkennung
    - Druck
    - Angst.
- Den Unternehmen fehlt es an Methoden-Wissen und an Gespür für das Menschliche. Awareness-Maßnahmen sind häufig nur kognitiv ausgerichtet.
- Der Führungsstil beeinflusst die SE-Abwehr: Führung als ein intentionaler, sozialer Beeinflussungsprozess verwendet auch SE-Prinzipien. Wenn der Social Engineer weiche Methoden benutzt, können Manager diese auch nutzen. Denn je unwohler sich ein Mitarbeiter fühlt, desto größer die Hoffnung, dass Einfluss bzw. Beziehungen von außen kommen („...dumm gelaufen, wenn der Social Engineer der netteste Mensch am Arbeitsplatz meiner Mitarbeiter ist.“)
- Führungskräfte sind oftmals keine Vorbilder: Manager glänzen in punkto Auftritt, Performance und kognitiver Fähigkeiten - nicht als Sicherheits-Vorbilder. Es fehlt an Bewusstsein für Sicherheitsthemen sowie für die Einbindung von Social Skills (Anerkennung). Unternehmen müssen Manager stärker als Multiplikatoren für Sicherheit involvieren und spezielle Tools implementieren.
- Sinnvoller SE-Schutz auf 3 Ebenen:
    - 1. Bewusstsein für das eigene Kommunikationsverhalten entwickeln (mental shortcuts)
    - 2. Identifikation von relevanten sozialen Eigenschaften
    - 3. Entwicklung einer geeigneten Sicherheits- und Unternehmenskultur (u. a. Awareness, Simulationen, Rollenspiele etc.)
- Maßnahmen für Unternehmen:
    - Tragfähiges Incident-Management, das, aufgrund der sozialen Komponente und den schambesetzten Reaktionen der Opfer, den Opfern einen besonders geschützten Raum zur Verarbeitung anbieten muss
    - Erarbeitung von Clustern, die zeigen, wie SE in ein Unternehmen gelangt
    - Authentizität und Glaubwürdigkeit derer, die das Thema vermitteln
    - Serious Games, projektive Übungen und Rollenspiele.

Bewertung: Im 20-seitigen offenen Abstract werden keine konkreten Maßnahmen zur Prävention und Bekämpfung veröffentlicht. Lediglich im Presseartikel werden Maßnahmen angedeutet. Die gesamte 78-seitige Auswertung der Studie muss käuflich erworben werden.

Positiv zu bewerten ist, dass das Unternehmen eine eigene Studie vorangesetzt hat, auf die sich die zu empfehlenden Maßnahmen und Informationen für Unternehmen beziehen. Die Anzahl der durchgeführten Interviews (35) kann als ausreichend für eine aussagefähige, explorative Datenbasis erachtet werden, ungeachtet der Tatsache, dass die Art der Auswahl der Interviewpartner, zumindest in der offenen Abstractversion, nicht angegeben wird. Repräsentativität kann insofern nicht unterstellt werden. Zu allen Forschungsfragen wurden, soweit im Abstract ersichtlich, Erkenntnisse generiert.

Andere Unternehmen, die in diesem Sektor tätig sind, vernachlässigen dies häufig und beziehen ihr Wissen aus Sekundäranalysen oder verarbeiten lediglich die im Kundenunternehmen gemachten Erfahrungen. Dies ist natürlich insofern angemessen und sinnvoll, wenn ein Vorfall in einem Unternehmen geschehen ist, diesen für die anderen Mitarbeiter zu Schulungszwecken aufzubereiten. Allerdings könnte der sachkundige und thematische Bezugsrahmen für eine umfassende effektive Maßnahmenstrategie zu kurz kommen.[5]

Das Unternehmen known_sense ist auch Kooperationspartner im von der Horst Görtz Stiftung geförderten Forschungsprojekt unter Leitung von Prof. Dr. Scholl, TH Wildau, und verfügt durch diese intensive Beschäftigung mit der Thematik zusätzlich über entsprechende Expertise. [6]

Neu in Bezug zu anderen Veröffentlichungen ist der Präventionsansatz, dass der Mitarbeiter sich zunächst selbst seiner eigenen Stärken und Schwächen bewusst werden soll, um möglichen SE-Angriffen gegenüber gewappnet zu sein. Nach dem Motto: „Erkenne Dich selbst“ steht an erster Stelle einer effektiven Präventionsarbeit die Analyse der eigenen sozialen Eigenschaften, die als Einfallstor ausgenutzt werden können (Hilfsbereitschaft, Neugier etc. s.o.). Ebenso gilt es, das eigene Kommunikationsverhalten zu reflektieren und zu üben sowie kommunikative Footprints zu überdenken. Erst dann folgt die Aufgabe der Organisation und der Führungskräfte, mit entsprechenden Maßnahmen und einer geeigneten Unternehmenskultur, den regulativen Sicherheitsrahmen zu schaffen.

[5] Zuletzt wurde diese Vorgehensweise gegenüber Uzin im Gespräch mit zwei Beratungsfirmen, die anlässlich des 16. Frankfurter Symposium „Compliance & Unternehmenssicherheit“ am 21.09.17 als Aussteller anwesend waren, bestätigt.
[6] Eine Zusammenfassung des Projektes siehe unter Punkt 3.4 in diesem Bericht.

3.2 Fachartikel zum Thema Social Engineering (SE)

Hellerforth, Michael: Wirtschaftskriminalität: Social Engineering - So manipulieren Industriespione ihre Opfer. In: WirtschaftsWoche (2015)

Gegenstand: Der Autor richtet seinen Fokus auf das Delikt „Spionage“, unabhängig davon, ob der Angriff durch staatliche oder andere Akteure durchgeführt wird und fasst unter Social Engineering nur Manipulationen, die im oder über das Internet und sozialen Medien stattfinden. Er schildert den Tatablauf und die einzelnen Tatphasen einer „Operation“ sehr ausführlich und fast im Stil einer „Tatanweisung“.

Der *Autor* ist Rechtsanwalt in Mülheim an der Ruhr, ehemaliger Abteilungsleiter bei der Nato und Dozent an der Ecole de Guerre Economique (Schule für Wirtschaftskrieg, EGE) in Paris. Schwerpunkt seiner Tätigkeit ist die Betreuung von Mittelständischen Unternehmen, Großunternehmen und öffentlichen Akteuren.

Ziele: Der Beitrag wurde als „Gastbeitrag“ in der Wirtschaftswoche abgedruckt. Ein konkretes Ziel nennt der Autor nicht. Zu vermuten ist, dass er mit dem Beitrag seinen Bekanntheitsgrad bei Unternehmen steigern und für die EGE werben möchte sowie Sensibilität wecken.

Forschungsfragen: entfällt

Ergebnisse:

- Jede Auseinandersetzung mit dem Thema Industriespionage leidet unter einem doppelten Handicap: Zum einen wird das Delikt mit Vorstellungen aus der Filmwelt assoziiert und hat damit etwas Fantastisches, Unwirkliches oder Realitätsfernes, wird aber nicht mit den Wirklichkeiten des geschäftlichen Alltags in Verbindung gebracht. Zum anderen betrachten Unternehmen es zuallererst als ein technisches bzw. kriminelles Problem. D.h. ein krimineller Mitarbeiter im Unternehmen handelt bewusst kriminell.
- Konsequenz: Sicherheitsstrategien werden darauf ausgerichtet und der Faktor Mensch als Schwachstelle wird ausgeklammert.
- In der deutschen Sprache existieren keine adäquaten Bezeichnungen für „Intelligence“ oder „Social Engineering“. Dies erschwert die Auseinandersetzung mit der Thematik.
- Definitionen:
    - Intelligence ist die gezielte und geplante Erkenntnisgewinnung durch Beschaffung, Auswertung und Aufbereitung von Informationen. Die Spionage ist dabei eine Form der Intelligence.
    - Social Engineering ist die aktive Manipulation von Informationen im Internet und sozialen Medien zwecks Beeinflussung einer Zielperson oder Zielorganisation um von dieser Informationen zu gewinnen und/oder diese zu einem bestimmten Verhalten zu bewegen.
- Phasen des Social Engineering und Organisation:[7]

  In der Praxis durchläuft eine solche Operation mehrere aufeinander aufbauende Phasen[8]:

[7] Es bleibt unklar, woher der Autor die folgenden Informationen bezieht. Eine Quelle wird nicht benannt.
[8] Die Phasen werden in dem Artikel ausführlich mit Hinweisen für ein Gelingen der „Operation“ beschrieben.

- Vorbereitung
- Kreation von Avataren und Aufbau von Legenden
- Kontaktaufnahme
- Informationsabschöpfung.

Laut Autor werden diese Operationen häufig von einer oder zwei Personen durchgeführt, obwohl es aus Praxissicht sinnvoller sei, ein eingespieltes Team einzusetzen.

Idealtypischer Weise besteht ein Team aus mehreren Spezialisten mit klar abgegrenzten Aufgabenbereichen:

- Ein Teamleiter als Manager und zentraler Entscheider
- Ein IT-Analyst, der Informationen aus offenen Quellen über die Ziele sammelt und bündelt. Gleichzeitig erstellt er ein aktuelles Lagebild über den Auftritt der eigenen Avatare im Netz sowie über das Bild, das das Ziel von diesen gewinnen kann.
- Ein Fachmann für das Informationsgebiet aus dem die Informationen gewonnen werden sollen.
- Ein Fachmann für Social Media sowie sämtliche eingesetzten Seiten, Blogs, Medien und Applikationen.
- Ein Kommunikationsspezialist als Redakteur für die im Netz sowie im direkten Kontakt zu veröffentlichenden Elemente, Kommentare, Texte sowie persönliche Nachrichten. Dieser muss sowohl über psychologisches Gespür, schreibendes Talent sowie den notwendigen sprachlichen und kulturellen Background verfügen.

- Diese Branchen sind am häufigsten von Computerkriminalität betroffen[9]:
  - der Automobilbau
  - die Chemie- und Pharmabranche
  - das Finanz- und Versicherungswesen
  - die Medien- und Kulturbranche
  - der Handel.
- Ergebnisse aus einer Studie von E&Y aus dem Jahr 2015[10]:
  - *Wer wurde angegriffen?* Jedes fünfte Unternehmen mit mehr als einer Milliarde Euro Umsatz hat in den vergangenen drei Jahren einen Angriff auf die eigenen Daten bemerkt. 18 Prozent der Betroffenen registrierten sogar mehrere Attacken. Mittlere (ab 50 Millionen Euro Umsatz) und kleinen Unternehmen (bis zu 50 Millionen Euro Umsatz) erlebten seltener Angriffe: 16 beziehungsweise zehn Prozent haben Hinweise auf Spionage oder Datenklau entdeckt.
  - *Welche Branche ist im Visier der Hacker?* Unternehmen der Energie- (17 Prozent) und der Finanzbranche (16 Prozent) werden am häufigsten Opfer von Spionage und Datenklau.
  - *Wer sind die Hacker?* In den meisten Fällen (48 Prozent) ließ sich der Täter nicht zuordnen. In 18 Prozent der Fälle konnten Hackergruppen als Täter

[9] Hier bezieht sich der Autor auf eine Umfrage des Branchenverbandes Bitkom aus dem Jahr 2015, in der 1074 Unternehmen ab 10 Mitarbeitern gefragt wurden, ob das jeweilige Unternehmen innerhalb der letzten zwei Jahre von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen war. Gut die Hälfte der befragten Unternehmen gab an, tatsächlich Opfer von IT-gestützter Wirtschaftskriminalität geworden zu sein.

[10] Hier bezieht sich der Autor auf die Studie „Datenklau 2015“ von der Prüfungs- und Beratungsgesellschaft Ernst & Young. Geschäftsführer sowie Führungskräfte aus IT-Sicherheit und Datenschutz von 450 deutschen Unternehmen wurden 2015 vom Marktforschungsinstitut Valid Research befragt.

identifiziert werden. In 15 Prozent war es ein konkurrierendes ausländisches Unternehmen.
    - *Von welchen Hackern geht die größte Gefahr aus?* Die größte Gefahr geht aus Sicht der Manager von China aus: „46 Prozent nennen das Land als Region mit dem höchsten Risikopotenzial, dahinter folgen Russland (33 Prozent) und die USA (31 Prozent)".
    - *Was sind die Motive?* Hinter den Angriffen vermuten die Manager in erster Linie den Versuch an Wettbewerbsvorteile oder finanzielle Vorteile (je 29 Prozent) zu gelangen. Reputationsschädigung (8 Prozent), Racheaktion (6 Prozent) und die Störung des Geschäftsbetriebs (3 Prozent) werden deutlich seltener hinter den Attacken vermutet.
    - *Welchen Schaden verursachen die Angriffe?* In drei von vier Fällen (74 Prozent) handelte es sich bei den Attacken um Hackerangriffe auf die EDV-Systeme, in 21 Prozent wurden IT-Systeme vorsätzlich lahmgelegt. Deutlich seltener wurden Kunden- oder Arbeitnehmerdaten abgegriffen (elf Prozent), Mitarbeiter abgeworben oder Datenklau durch eigene Mitarbeiter begangen (jeweils zehn Prozent).
- Social Engineering ist ein Problem, das schwerpunktmäßig außerhalb des Unternehmens auftritt, so dass Mittel des Betriebsschutzes nur schwer oder überhaupt nicht greifen. Das eigentliche Ziel einer Operation „das Gehirn des Opfers" kann von seinem Arbeitgeber weder kontrolliert noch überwacht werden. Hinzu kommt, dass das Ziel im - vermeintlich - privaten Umfeld unterwegs ist, so dass hier gesetzliche Regelungen zu Daten- und Persönlichkeitsschutz greifen.
- Fünf aktive, vorbeugende Maßnahmen zum Schutz gegen Social Engineering:
    - Überwachung der eigenen Webpräsenz und von im Zusammenhang mit dem Unternehmen und seinen Produkten, Techniken und Strategien stehenden Postings.
    - Steigerung des Gefahrenbewusstseins der Mitarbeiter.
    - Aus- und Weiterbildung der Mitarbeiter.
    - Einrichtung einer proaktiven Unternehmenspolitik, um Mitarbeiter im Falle einer erfolgten Operation einzubinden und nicht zu verängstigen.
    - Aktive Verschleierung und Desinformation (Aktive Verschleierung und Desinformation sind ein zweischneidiges Schwert. Werden diese aufgedeckt, kann das dem Image des Unternehmens empfindlich schaden. Eine Desinformationskampagne wird daher in der Regel nur im Falle eines konkreten Anlasses und zeitlich begrenzt erfolgen).

Bewertung: Der Autor beschreibt und bewertet das Phänomen Spionage und Social Engineering sehr stark aus einer geheimdienstlichen Perspektive. Er spricht davon, dass „Gegenspionage" die „gangbarsten Lösungen" zur Verhinderung bietet. Den deutschen Rechtsrahmen behält er dabei aber immer im Auge. Dennoch fällt der Artikel insofern aus dem Rahmen der sonstigen Publikationen, dass er eine Szenerie beschreibt, die eher an einen Spionagefilm erinnert als an reales Wirtschaftsleben. Das Selbstbild eines deutschen Unternehmensermittlers dürfte daher im Duktus nicht getroffen werden, sondern ihn eher überfordern. Man spürt in seinen Aussagen die Zugehörigkeit zur École de guerre économique (deutsch Schule für Wirtschaftskrieg, EGE) in Paris. Diese wurde „1997 von General Jean Pichot-Duclos, Christian Harbulot und Benoît de Saint-Sernin gegründet. Sie ist die erste europäische Institution, die eine Ausbildung für Angriffs- und Verteidigungsmethoden anbie-

tet, denen die Unternehmen im Wettlauf der Globalisierung ausgeliefert sind.“[11] Die Gründer stammen alle aus der Geheimdienst- und Nachrichtendienst- Szene und vertreten die Auffassung eines herrschenden „Wirtschaftskrieges“.

Die Aussagen zum Täterverhalten oder zu Täterorganisationen werden nicht belegt. Es bleibt zu vermuten, dass diese Anschauungen auf den Erkenntnissen beruhen, die an der Ecole gelehrt werden.

Die Ansätze zur Prävention mit entsprechenden Konzeptionsangeboten kommen im Artikel zu kurz und sind wenig hilfreich.

[11] Vgl hierzu: Wikipedia. Url: https://de.wikipedia.org/wiki/%C3%89cole_de_guerre_%C3%A9conomique. (Stand: 19.09.17)

Schumacher, Stefan: Die psychologischen Grundlagen des Social Engineerings (2013/2014 und 2011)

Gegenstand: Der Artikel zeigt, wie SE aus psychologischer Sicht funktioniert und erklärt die zugrundeliegenden Tricks anhand sozialpsychologischer Studien und Experimente. Außerdem werden Beispiele, Warnsignale und Gegenmaßnahmen vorgestellt.

Definition: SE ist eine Angriffsstrategie, die auf eine psychologische Manipulation von Menschen abzielt. Dabei versucht der Angreifer, fundamentale menschliche Verhaltensweise auszunutzen, um Zugriff auf sensible Daten zu bekommen.

Der *Autor* ist geschäftsführender Direktor des Magdeburger Instituts für Sicherheitsforschung und Mitherausgeber des Magdeburger Journals zur Sicherheitsforschung. Er befasst sich mit Fragen der Informations- und Unternehmenssicherheit und erforscht Sicherheitsfragen aus pädagogisch/ psychologischer Sicht. Darüber hinaus berät er Unternehmen bei der Umsetzung von Sicherheitsmaßnahmen und der Etablierung unternehmensweiter IT-Sicherheitsstrategien.

Ziele: Der Artikel richtet sich an Sicherheitsverantwortliche und Systemadministratoren, die verstehen wollen, wie Social Engineering funktioniert und dieses Wissen in ihre Sicherheitsmaßnahmen integrieren möchten.

Forschungsfragen: Forschungsfragen stellt der Autor explizit keine, da er keine eigene empirische Untersuchung durchführt. Es lassen sich aber folgende Fragen ableiten:

- Wie funktioniert Social Engineering? Welche sind die psychologischen Grundlagen der Manipulation?
- Welche Maßnahmen können aus diesen Erkenntnissen abgeleitet werden, um Social Engineering zu verhindern?

Ergebnisse:

- Social-Engineering ist äußerst erfolgreich, wenn größere Organisationen wie Unternehmen, Behörden oder Universitäten angegriffen werden sollen.
- Human Based Social Engineering setzt zum Großteil auf soziale Beziehungen als Angriffsvektor. Phishing dagegen, als Variante des SE, benötigt lediglich technische Voraussetzungen (Webspace).
- Auch zunächst unverfänglich erscheinende Informationen (z.B. Telefonnummern, E-Mailadressen, Aufgabengebiete, Fotos) können nach Freigabe im Netz missbraucht werden.
- Kontaktanbahnung durch:
    - Sympathie-Aufbau (z.B. gleiches Hobby)
    - Verbrüderung mit dem Opfer (z.B. vermeintlich gleicher Gegner)
    - Vorspiegelung von Autorität (funktioniert in strengen Hierarchien, wie Polizei oder Armee, sehr gut. Aber auch wichtiger Kunde, hoher Verantwortlicher einer anderen Filiale etc.)
    - Aufbau einer Drohkulisse („Wenn das ihr Chef erfährt, dann…“)
- Der Mensch reagiert auf bestimmte Auslösemerkmale mit *automatisiertem Sozialverhalten*. Regeln mit solch hoher gesellschaftlicher Durchschlagkraft lassen sich leicht missbrauchen:

    - Die Regel der *Reziprozität* (Wechselseitigkeit, d.h. wir müssen uns für erhaltene Gefälligkeiten, Geschenke etc. revanchieren. Auf Zugeständnisse müssen wir mit Zugeständnissen reagieren). Falls aber durch Bewusstheit/ Sensibilität erkannt wird, dass der Gefallen oder das Geschenk in Wirklichkeit nur ein Manöver war, um Vorteile zu erlangen, verliert die Reziprozitätsregel ihre Durchschlagskraft.
    - Das Kontrastprinzip (Kontraste erscheinen durch eine geschickte Präsentation größer als sie unter anderen Umständen erscheinen würden).
    - Die Regel des *Commitments* und der *Konsistenz* (d.h. den Menschen wohnt ein geradezu zwanghaftes Verhalten inne, in Konsistenz mit ihren früheren Handlungen zu erscheinen - also konsequent zu sein. Wurde eine Entscheidung getroffen, treten intra- und interpsychische Vorgänge in Kraft, die uns dazu drängen, konsistent zu bleiben. In der Sozialpsychologie und dem Marketing arbeitet man daher mit der sog. „Fuß-in-der-Tür-Taktik“. Man beginnt mit einer kleinen Bitte und arbeitet sich dann zur großen vor oder verändert das Selbstbild des Gegenübers in die gewünscht Richtung. Hat man das Selbstbild einer Person erst einmal in eine neue Rolle manipuliert, tut die Person nahezu alles um mit dem neuen Selbstbild konsistent zu bleiben). Zumeist spürt der Mensch, dass er betrogen oder ausgenutzt werden soll, achtet aber nicht auf dieses „Bauch-Gefühl“. Durch Awareness-Training kann hier, als Gegenmaßnahme, eingegriffen werden.
    - Das Prinzip der sozialen Bewährtheit (Das Verhalten anderer wird als richtig angenommen und gegebenenfalls kopiert bzw. adaptiert).
    - Sympathie (Uns sympathische Menschen können uns eher zu einem bestimmten Verhalten verleiten). Sympathie verstärkt alle anderen eingesetzten Überzeugungstricks. Dazu gehören auch Attraktivität, Ähnlichkeit, gleiche Herkunft, ähnliche Interessen, Schmeicheleien, Sympathiebekundungen, Flirts.
    - Autorität (Autoritätssymbole: Titel, Uniform, Luxus).
    - Knappheit (je knapper eine Ware ist, desto mehr gewinnt sie an Wert).
- Fazit:
    - Es gibt keinen »Abwehrzauber« gegen Social-Engineering, denn dabei handelt es sich um Verhalten, das in der Regel sozial erwünscht ist. Technische Maßnahmen sind nicht in der Lage, derartige Vorfälle zu verhindern, da es sich um ein soziales Problem handelt. Zur Abwehr wird die Fähigkeit benötigt, soziale Beziehungen und Kontexte zu deuten. Es ist notwendig, in Organisationen ein Sicherheitsbewusstsein im Rahmen einer Sicherheitskultur zu schaffen.
    - Erfolgreiches Social-Engineering setzt oft bei der mangelnden Authentifizierung des Angreifers an. Daher ist es notwendig, *sinnvolle Authentifizierungsmechanismen* (z. B. Dienstausweise, Anruf-Parolen o. ä.) zu etablieren. Dabei gilt es aber, derartige technische Lösungen sozial akzeptabel zu machen.

Bewertung: Der Artikel erläutert und veranschaulicht mit vielen Beispielen und Experimentbeschreibungen, auf welchen sozialpsychologischen Grundlagen Social Engineering beruht und wie Manipulation gezielt angewandt werden kann. Es wird deutlich, dass die vorgestellten Grundlagen des Social-Engineerings sich weder verhindern noch ausschalten lassen, da sie auch die Grundlagen unseres sozialen Zusammenlebens darstellen. Sozial adäquates und erwünschtes Handeln sowie tiefverwurzelte menschliche Interaktionsmechanismen werden missbraucht. Es ergibt sich ein ähnliches Dilemma wie bei der Korruption. Letztendlich lassen sich diese Phänomene nur durch eine gezielte Bewusstheitsschulung und dauerhafte

Awareness eingrenzen. Technische Kontrollsysteme und Sicherheitsvorschriften können Vorfälle nicht verhindern, aber ein Warnsignal für den Mitarbeiter bieten, dass hier ein Missbrauchsversuch vorliegt und eine bewusste Verhaltensentscheidung hervorrufen.

3.3 Fachartikel zum Thema CEO-Fraud

Kunze, Dirk: „Millionenbeute durch clevere Betrüger“ (2016) sowie „Enkeltrick 4.0 - Wenn der falsche Chef Geld will (2016)

Gegenstand: Der Autor hat 2016 zwei Artikel zur Thematik veröffentlicht, einen in der Zeitschrift „der kriminalist“, einen in der „Kriminalistik“. Die Inhalte beider Artikel werden hier zusammen dargestellt, da sie sich inhaltlich weitreichend überschneiden. Die Artikel beschreiben das Phänomen aus polizeilicher Sicht. Es wird ein Überblick über Modi operandi, Kooperation von LKA, BKA, Banken und Unternehmen, Ratschläge des LKA NRW für Maßnahmen der Betroffenen sowie polizeiliche Erfahrungen bei den Ermittlungen gegeben.

Der *Autor* ist Kriminalrat beim LKA NRW, Leiter D 42, Zentrale Internetrecherche/ Ermittlungskommissionen.

Ziele: Die Artikel richten sich an ermittelnde Polizeibeamte. Ziel ist eine Weitergabe der in NRW gemachten Erfahrungen bei Ermittlungen zum CEO-Fraud.

Forschungsfragen: entfällt

Ergebnisse:

- Dieser Modus Operandi, in den USA als Business E-Mail Compromise/Scam (BEC) bezeichnet, ist seit 2009 festzustellen. Die ersten Fälle wurden in der Schweiz registriert. Diese zunächst in der französischsprachigen Schweiz beginnenden Taten verlagerten sich 2010 nach Belgien und Frankreich.
- Schäden:
    - Im frankophonen Sprachraum wurden seitdem ca. 1200 vollendete Taten mit einer Gesamtschadenssumme von über 500 Millionen Euro registriert.[12]
    - Für Deutschland weist die aktuelle Statistik einen Schaden von ca. 88 Millionen Euro bei 51 vollendeten Taten aus.[13] Dazu kommen 78 rechtzeitig erkannte Versuche mit einer Schadenssumme von ca. 70 Millionen Euro. Der höchste Einzelschaden wurde in Belgien mit 70 Millionen Euro zum Nachteil einer Bank registriert. Weltweit verzeichnete das FBI zwischen Oktober 2013 und Juni 2016 insgesamt 22.143 Geschädigte und Schäden von 3,1 Milliarden US-Dollar.[14]
- Vorgehensweise: Die qualifizierten Täter spähen ihre Ziele sorgfältig aus und bereiten ihre Taten detailliert vor. Die beobachtete Vorgehensweise gliedert sich in zwei Phasen:
    1. Das Ziel wird durch Recherche im Internet (Open Source INTelligence - OSINT) und erste persönliche/ telefonische/ schriftliche Kontaktaufnahme oder Kompromittieren der IT-Systeme (APT) aufgeklärt und alle verfügbaren Informationen gesammelt. Die Täter tragen die erforderlichen Informationen und Unterschriften zur Begehung der Tat teils über Monate zusammen.
    2. Mit den erlangten Informationen beginnt die zweite Phase, der eigentliche Angriff: Mit den durch Spear-Phishing, Social Engineering und OSINT-

[12] Stand März 2016.
[13] Stand März 2016.
[14] Url: https://www.ic3.gov/media/2016/160614.aspx (letzte Prüfung 29.6.2016 durch den Autor, Stand am 26.09.17 unverändert)

Maßnahmen gewonnenen Informationen erfolgt, zeitlich teils deutlich versetzt, die eigentliche Tatausführung. Die Geschädigten ziehen dadurch in der Regel keine Verbindung zu den Anrufen und E-Mails. Nun wird durch Vortäuschen mittels E-Mail des „Chefs“ eine Zahlungsaufforderung getätigt. Dabei wird Druck (hierarchisch, zeitlich) aufgebaut, Geheimhaltung geboten, an Loyalität appelliert etc.. Die Tat ist so angelegt, dass die Überweisung häufig kurz vor Geschäftsschluss der Banken oder vor europäischen Feiertagen erfolgt. So sollen Maßnahmen von Banken zur Rückgewinnung des Geldes erschwert werden. Auf dem Empfängerkonto angekommen erfolgt meist zeitnah eine Weiterleitung des Geldes, in der Regel in den asiatischen Raum. Spätestens hier wird das Geld in Tranchen weiter verteilt, um so die Nachverfolgung zu erschweren.

- Die Täter scheinen arbeitsteilig, hierarchisch organisiert und strukturiert zu arbeiten. Sie nutzen alle Möglichkeiten der modernen Kommunikation, insbesondere die zur Anonymisierung und Verfolgung ihrer eigenen Korrespondenz.
- Die Art und Weise der Kommunikation legt einen muttersprachlichen Hintergrund zumindest eines Teils der Täter nahe.
- Häufig werden nicht nur große Unternehmen, sondern auch Mittelständler, sogenannte „hidden champions", oder andere solvente Unternehmen ausgewählt. Die Erfolgsquoten der Täter variieren dabei. Während bei DAX Unternehmen nur ca. 10 Prozent der Versuche erfolgreich sind, steigt diese Zahl bei klein- und mittelständischen Unternehmen bis auf 50 Prozent an. Insbesondere in patriarchalisch geführten, mittelständischen Unternehmen scheint die Erfolgsquote besonders hoch zu sein.
- Eine schnellstmögliche Alarmierung der Polizei nach Tatvollendung ermöglicht häufig eine durch die polizeilichen Finanzermittlungsdienststellen initiierte Sicherung des abgeflossenen Geldes noch in Europa.
- Gleichzeitig ist die Einbindung der Außenhandelskammern, der Botschaften der Bundesrepublik Deutschland oder von lokalen Anwälten zur Sicherung und Rückführung des Geldes im Ausland sinnvoll.
- Der unmittelbare umfassende Austausch ist erfolgskritisch, um die Chance auf die Überwachung aktiver Täterkommunikation zu erhalten und Verbindungen festzustellen.
- Aufgrund der weiten Streuung der Taten erscheint eine landeszentrale Bearbeitung zum Erkennen von Zusammenhängen zielführend.
- Der enge Austausch unter Einbindung von Europol und des BKA bietet gute Möglichkeiten, Maßnahmen europaweit eng abzustimmen und Informations- und Bedarfsträger zu verknüpfen. Die Einbindung des Focal Points hat sich in NRW als wertvoll erwiesen. Dem LKA NRW ist es in enger Zusammenarbeit mit der Financial Intelligence Unit des BKA und den beteiligten Banken gelungen, seit Übernahme der landeszentralen Ermittlungen im Dezember 2015 mehr als 20 Millionen Euro für die geschädigten Firmen Ausland zu sichern (Stand 2016). Die Zusammenarbeit zwischen dem LKA NRW, dem BKA, den Banken und den Firmen war dabei eng und kooperativ.
- Am 02.03.16 führte das BKA ein koordinierendes Treffen der sachbearbeitenden Dienststellen durch. Durch den Abgleich der bekannten Daten und Vorgehensweisen kristallisierten sich neben „Trittbrettfahren“ zwei unterschiedliche Tatbegehungsweisen heraus.
- Am 06. 07. 16 hat das LKA NRW unter Beteiligung des FBI, Europol, des BKA, verschiedener LKÄ, des Branchenverbandes Bitkom e. V. und des Verbandes der IT-

Anwender VOICE e. V. sowie des Deutschen Industrie- und Handelskammertages, der Industrie- und Handelskammern und der Allianz für Sicherheit in der Wirtschaft (ASW) einen internationalen Präventionstag durchgeführt. Vertreter von Verbänden, Banken und der Polizei stellten die Möglichkeiten der Erkennbarkeit und der Prävention dieses Phänomens dar. Im Anschluss daran wurden im Rahmen einer Sachbearbeitertagung, an der auch Vertreter der norwegischen Polizei und Staatsanwaltschaft teilnahmen, die Möglichkeiten der Zusammenarbeit und des Informationsaustausches thematisiert.

- *Kritik*:
    - Ein fortwährend aktualisiertes, bundesweites Lagebild inklusive festgestellter technischer Adressen und Konten würde ein frühzeitiges Erkennen von Tatzusammenhängen und die Zuordnung zu einzelnen Tätergruppen ermöglichen. Das Fehlen erschwert das Generieren und Verfolgen von Ermittlungsansätzen. Ein Erkennen von Zusammenhängen ist aufgrund des Fehlens der Daten nicht gewährleistet.
    - Das Bedienen des Meldedienstes nach Abschluss der Ermittlungen bei Abgabe an die Staatsanwaltschaft ist in diesem hoch dynamischen Bereich allein nicht zielführend.
- Das LKA NRW gibt folgende *Präventionshinweise* an die Unternehmen:
    - Kontrollieren Sie die öffentlich einsehbaren Informationen ihres Unternehmens, achten Sie auf Publikationen durch Sie und Ihre Mitarbeiter.
    - Führen Sie Unterscheidungsmerkmale ein, mit denen Mitarbeiter Autorisierungen/ Unterschriften von den im Netz verfügbaren unterscheiden können.
    - Führen die Regeln für Abwesenheiten ein und schaffen Sie interne Kontrollmechanismen.
    - Klären Sie Mitarbeiter an neuralgischen Stellen über die Gefahren von „CEO-Fraud" und „Social Engineering" auf.
    - Weisen Sie Ihre Mitarbeiter darauf hin, dass die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) keine Zahlungsanweisungen oder Verschwiegenheitserklärungen versendet oder einzelne Zahlungen autorisiert.
    - Prüfen Sie die Möglichkeiten kontrollierter E-Mail-Verwaltung (Konfiguration des E-Mail-Servers - z. B. Prüfen auf Eintrag einer E-Mail-Adresse im angezeigten Namensfeld, Prüfen von Vorname und Nachname von Funktionsträgern auf externe Domains etc.).
    - Sprechen Sie mit Ihrer Bank, wie Sie im Fall der Fälle vorgehen können. Etablieren Sie Kommunikationskanäle.
    - Legen Sie Kommunikations- und Entscheidungswege für Krisenfälle fest.
    - Im Falle von Zahlungsanweisungen sollten Sie vor Veranlassung der Zahlung:
        - den Absender- und die Antwortadresse und Schreibweise der E-Mail prüfen,
        - bei einer Antwort die E-Mail-Adresse des Empfängers von Hand eingeben,
        - die Zahlungen per Rückruf/persönlicher Rückfrage beim Auftraggeber verifizieren.
- Im Falles des Schadenseitritts rät das LKA NRW:
    - Wenden Sie sich umgehend an Ihren Vorgesetzten und schildern das Problem.

- Treten Sie mit Ihrer Bank und IHK in Kontakt und versuchen Sie gemeinsam, das Geld „anzuhalten".
- Erstatten Sie schnellstmöglich Anzeige, nur dann können die Strafverfolgungsbehörden Sie, neben der Strafverfolgung, bei der Rückgewinnung der Gelder unterstützen.

Bewertung: Die Artikel bieten eine wertvolle Erkenntnisgrundlage für ermittelnde PVB und fassen den polizeilichen Erkenntnistand zusammen. Deutlich wird die Wichtigkeit eines raschen Sammelns und Zusammenführens von Daten und Informationen zu einem neuen Modus operandi oder einer neuen Tatvariante rasch nach erstem Bekanntwerden für Präventionsmaßnahmen und einen späteren polizeilichen Erfolg. Da die Erstellung eines bundesweiten Lagebildes mit aktuellen Zahlen, Daten und Fakten bei Auftreten einer neuen Tatbegehungsweise bisher oftmals nicht zeitnah gelingt, können die entsprechenden Lageerkenntnisse nicht „automatisch“ zur Verfügung gestellt werden. Daher ist der vielversprechendere Weg, zeitnah Workshops und Tagungen zu veranstalten, um alle erforderlichen Akteure an einem Tisch zu versammeln, Lageerkenntnisse zu bündeln und schnell eine Öffentlichkeit für die neue Betrugsvariante herzustellen. Zusätzlich wäre die Veröffentlichung auf der Kommunikationsplattform www.wirtschaftsschutz.info der Initiative Wirtschaftsschutz zielführend. Denn Kenntnisse über aktuelle Tatbegehungsweisen bilden die beste Präventionsgrundlage für Unternehmen, um Mitarbeiter entsprechend zu sensibilisieren. Darüber hinaus können verfahrensrelevante Informationen ausgetauscht, Zusammenarbeitsabsprachen und Zuständigkeiten geklärt sowie eine ressourcenschonende Arbeitsaufteilung zur Vermeidung von Doppelarbeit besprochen werden.

3.4 Laufende Forschungsprojekte

Scholl, Margit u.a.: Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg. TH Wildau, 2017 sowie Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt (2016)

Gegenstand: Die fortschreitende Digitalisierung durchdringt zunehmend alle Lebensbereiche und erfordert ein stärkeres Bewusstsein sowie verbesserte Kompetenzen im Bereich der Informationssicherheit sowohl im Privat- als auch im Arbeitsleben. Bisherige IT-Sicherheitsmechanismen stoßen an ihre Grenzen und Zuverlässigkeit und Beherrschbarkeit können nicht vorausgesetzt werden. Die fortschreitende digitale Transformation in allen gesellschaftspolitischen und wirtschaftlichen Bereichen führt zu einer Zunahme der Bedeutung von Informationssicherheit und IT-Sicherheit sowie Datenschutz und Datensicherheit. Das Projekt SecAware4job dient der *Steigerung des Informationssicherheitsbewusstseins* von Studierenden an der TH Wildau. Der Beitrag skizziert Methoden und Übungen, die in dem Fach „Sensibilisierung für Informationssicherheit“ zur Anwendung kommen. Diese innovativen Lehr- und Lernmethoden basieren auf dem Game-based-Learning-Ansatz, denn durch die Einbeziehung spielerischer Elemente kann insbesondere die Motivation gefördert werden und lassen sich Verhaltensänderungen anregen. Damit widmet sich SecAware4job aktuellen Forschungsfragen zum spielebasierten und kooperativen Lernen im Bereich der Awareness/ Bewusstseins-Förderung.

Zum Projekt:

Leiterin: Prof. Dr. rer. nat. Scholl, Margit. Professorin für Wirtschafts- und Verwaltungsinformatik: Informationstechnologie und Projekt-/Prozessmanagement, betriebliche und multimediale Anwendungen, Informationssicherheit und Bewusstsein. Forschungsschwerpunkte: E-Government und Projektmanagement sowie IT-Sicherheit; IT und Didaktik, Lernförderliche Infrastrukturen & spielebasierte Szenarien, Individual- und Organisationslernen, Digitale Medien in der Bildung; Verwaltungsinformatik an Fachhochschulen.[15]

Mitarbeiter: Frauke Fuhrmann, Denis Edich, Peter Ehrlich, Peter Koppatz

Kooperationspartner: known_sense

Mittelgeber / Förderprogramm / Art der Finanzierung: Horst Görtz Stiftung

Projektvolumen: 199.805 Euro

Laufzeit: 2015 – 2017

Projektabschlussbericht: Fachbuch: Informationssicherheitsbewusstsein für den Berufseinstieg (SecAware4job). ISBN: 978-3-8440-5466-8. Buch in Vorbereitung für September 2017.[16]

Ziele: Ziel des von der Horst Görtz Stiftung finanzierten Forschungsprojektes „Informationssicherheitsbewusstsein für den Berufseinstieg: SecAware4job“ ist es, bei den Studierenden der TH Wildau, insbesondere der nicht technischen Studiengänge, ein stärkeres Bewusst-

[15] Vgl: Url: https://typo3.tfh-wildau.de/mitarbeiter/mitarbeitersuche/detailseite.html?uid=mscholl. Stand 27.09.17

[16] Buch ist noch nicht verfügbar. Stand: 26.09.17.

sein für Informationssicherheit und Datenschutz unter besonderem Einsatz von didaktischen Kreativmethoden - spielebasierten analogen und digitalen Lernszenarien - zu entwickeln. So sollen sie als zukünftige Mitarbeiter/innen für die alltäglichen Herausforderungen des Schutzes von sensiblen Informationen und der digitalen Infrastruktur sensibilisiert werden und ihr Sicherheitsbewusstsein soll fundiert gefördert werden. In SecAware4job liegt darüber hinaus ein Schwerpunkt in der Entwicklung einer nachweisbaren, stufigen Qualifizierung in Informationssicherheit für Studierende für den Berufseinstieg in Unternehmen, Verwaltungen und Institutionen. In der höchsten Qualifizierungsstufe können die Studierenden zertifizierte Kompetenzen erwerben, um in der Organisation als IT-Sicherheitsbeauftragter eine Leitlinie vorzubereiten, die Einführung eines Informationssicherheitsmanagements in Unternehmen bzw. Verwaltung zu begleiten und Kollegen für Informationssicherheit zu sensibilisieren.

Forschungsfragen:

Übergreifend: Wie kann auf innovative Weise mittels einer Kombination aus spielerischen analogen und digitalen Lernszenarien Bewusstsein für Informationssicherheit und entsprechende Verhaltensweisen gefördert werden?

- Welche Faktoren des „Game-Based Learning Design Model" von Shi und Shih (2015) sollten in welcher Weise bei der Entwicklung und Anwendung (a) der analogen spielebasierten Lernszenarien und (b) der digitalen Varianten berücksichtigt werden?
- Durch welche spielerischen Elemente (z. B. Belohnung, Feedback, Wettbewerb) lässt sich (a) das Engagement, (b) die Motivation und (c) der Lernprozess der Studierenden fördern?
- Wie lassen sich (a) analoge und digitale spielebasierte Lernszenarien effektiv verbinden, so dass (b) ihre eigenständigen Einsatzbereiche sinnvoll erhalten werden?
- Wie lassen sich die spielebasierten Lernszenarien in ein zeitgemäßes Lehr- und Lernkonzept integrieren?
- Wie (a) motiviert sind die Studierenden, die angebotene Zertifizierungshierarchie zu absolvieren? Wie (b) erfolgreich absolvieren sie welche Stufe?
- Wie lassen sich (a) die Wirksamkeit der Lernszenarien sowie (b) der Lernerfolg und (c) das Informationssicherheitsbewusstsein der Lernenden messen?

Methodik:

Im Zuge der Durchführung von Sec-Aware4job wurden analoge Lernszenarien auch englischsprachig aufbereitet, international vorgestellt und in Auszügen mit einem internationalen Publikum getestet. Durch systematische Versuchsreihen sollen so die Forschungsfragen am Ende von SecAware4job umfassend beantwortet werden können. Studenten der TH Wildau, an denen die Methoden getestet wurden, wurden wöchentlich mittels Feedbackbogen befragt (Evaluation).

Erste Forschungsergebnisse:

- Die Ergebnisse zeigen, dass zwar ein gewisses Bewusstsein für Informationssicherheit bei den Studierenden vorhanden ist, sich dies aber nicht zwingend in dem Verhalten der Befragten widerspiegelt. Zudem sind neuere Bedrohungen noch nicht ausreichend bekannt und somit können die damit verbundenen Gefahren nicht kompetent abgewehrt werden.

- Es wurde ein Modell in Form einer Spirale entwickelt, mit dem die transformative Wechselwirkung zwischen top-down Vorgaben einer Organisation und der bottom-up Beeinflussung durch Mitarbeiter zur Entwicklung einer gelebten Sicherheitskultur erläutert wird.
- Ein Szenario wirkt umso besser, desto spezifischer die eingesetzten Materialien die berufliche Situation der Zielgruppe simulieren bzw. abbilden.
- Folgende Spielemechanismen wurden im Rahmen des Projektes entwickelt:
  - Lerneinheit Strafgesetzbuch (StGB)
  - ABC-Liste
  - BINGO
  - Netzwerk-Domino
  - Schutzspiel - Gefahrenabwehr mit begrenztem Budget
  - Interaktive Übung „Phishing“
  - Folgende Spielemechanismen wurden im Rahmen des Projektes entwickelt:
  - App „CBubbles“
- Das Fach mit dem angewandten methodischen Ansatz - bestehend aus einer Kombination aus Vortrag, analogen und digitalen spielebasierten Lernszenarien sowie interaktiven Übungen wurde von den Studierenden sehr gut bewertet.
- Das Ziel des Projektes, Informationssicherheitsbewusstsein und entsprechende Kenntnisse zu verbessern sowie idealerweise Verhaltensänderungen auszulösen, wurde bei den Teilnehmenden im Sommersemester 2016, insbesondere für das Arbeitsleben, erreicht.
- Um Aussagen zu den Wirkungsweisen der einzelnen Methoden, zum Lernerfolg und zur Nachhaltigkeit fundiert treffen zu können, ist es allerdings noch zu früh, da die empirische Basis bisher zu gering ist.
- In Planung ist die Entwicklung eines umfangreicheren Spieles zum Thema Social Engineering. In dem geplanten Lernszenario sollen der Tagesablauf eines fiktiven Charakters sowie potentielle Angriffspunkte und Risiken dargestellt und als Rollenspiel erlebt werden. Mit konkreten Gefahren der Digitalisierung konfrontiert, sollen Lernende die Notwendigkeit des Schutzes sensibler Daten begreifen lernen.

Bewertung: Das Forschungsprojekt und die Umsetzung der Erkenntnisse in Aus- und Fortbildungsmaßnahmen greift die wirkungsvollste Präventionsmaßnahme zur Verhinderung von SE auf, die Sensibilisierung von Mitarbeitern. Somit bieten die wissenschaftlichen Ergebnisse wertvolle Impulse für die Gestaltung und Entwicklung effektiver Schulungsmaßnahmen. Nur die Kombination von Technik und handelndem Mensch kann das Sicherheitsniveau steigern. Zur Etablierung einer gelebten Sicherheitskultur in Organisationen ist daher eine Kombination aus institutionellen Vorgaben und freiwilligem Engagement der Beschäftigten zur Gewährleistung von Informationssicherheit erforderlich. Die Selbstverpflichtung der Mitarbeiter, die Sicherheitsvorgaben des Unternehmens zu leben, kann nur gelingen, wenn die Emotionen der Beschäftigten angesprochen werden. Eine praktische, effektive und lebensnahe Vermittlung von Bedrohungen und Sicherheitsmaßnahmen kann daher ein nachhaltiges Bewusstsein schaffen. Insofern ist der Forschungsansatz an der TH Wildau geeignet und zeitgemäß.

Obwohl zunächst der Gedanke auftaucht, ob der „spielerische“ Ansatz der gewählten Methoden in der Erwachsenenbildung angemessen ist, erscheint die Einbindung solcher Schulungselemente nach den vorliegenden Ergebnissen als effektiv. Die Methodik, dass die Studierenden in Teams kooperativ lernen, ihr vorhandenes Wissen im Erfahrungsaustausch

vertiefen und durch gemeinsame Besprechung der Ergebnisse ein direktes Feedback zu ihrem Lernerfolg erhalten, scheint, zumindest bei jungen Menschen, die aber die Zukunft der Arbeitswelt stellen, erfolgreich.

Außerdem tut eine wissenschaftliche Evaluation bestehender Schulungsmethoden im Bereich Awarenessbildung not, da auf dem Beratungs- und Schulungsmarkt für die Wirtschaft eine Vielzahl von Privatanbietern tätig ist, deren Maßnahmen teuer von Unternehmen eigekauft werden, eine Evaluation aber selten stattfindet. Auch die Hinwendung zu jungen Menschen, die erst auf den Arbeitsmarkt streben oder Berufsanfängern ist sinnvoll, da die Bedeutung von Informationssicherheit so schon früh im Bewusstsein verankert wird. Dies entspricht auch der Forderung von Europol, das Thema Informationssicherheit schon frühzeitig in die Erziehung und Bildung einfließen zu lassen[17], um wehrhafte und sicherheitsbewusste Mitarbeiter auszubilden.

[17] Vgl: INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2016, S: 34: “Education and awareness on cyber-security and safety should be introduced as ‘life skills’ from an early age.”

3.5 Relevante Veranstaltungen, Experten und sonstige Veröffentlichungen 2017

Am 14.09.17 hat in Berlin die *Social Engineering Konferenz „Bluff City 2017"*[18] stattgefunden. Aktuelle Forschungsergebnisse, bewährte und innovative SE-Awareness-Methoden sowie Defense-Praxisbeispiele und Konzepte für SE-Kampagnen, -Simulationen und SE-Tools wurden dort präsentiert.

Interessante Referenten (Aufzählung ohne Unternehmensvertreter und Journalisten):

- *Holger Berens* (Rheinische Fachhochschule Köln, Leiter Kompetenzzentrum Internationale Sicherheit (KIS): Studiengangsleiter für Wirtschaftsrecht und Leiter des Studiengangs Compliance und Corporate Security (LL.M.) an der Rheinischen Fachhochschule Köln. Autor entsprechender Fachbücher sowie Berater im Bereich Compliance und Security. Darüber hinaus ist er Mitglied des Vorstandes von ASIS Germany e.V., dem deutschen Chapter von ASIS International. ASIS International ist mit mehr als 37.000 Mitgliedern die weltweit größte Organisation für Fragen der Sicherheit in der privaten Wirtschaft. Das Hauptquartier befindet sich in Alexandria VA in den USA, es existieren zudem mehr als 200 Landesverbände (sogenannte Chapters) in aller Welt.
- *Ankha Haucke*. Diplom Psychologin und Therapeutin mit eigener Praxis für Einzel- und Paartherapie in Köln. Bei known_sense ist sie u.a. für Konzeption und Feldarbeit von tiefenpsychologischen Security-Wirkungsanalysen verantwortlich Darüber hinaus ist sie Co-Autorin des psychologischen Fachbuchteils von Security Awareness, erschienen bei Vieweg Springer.
- Dipl. Psychologin Ivona Matas (known_sense)., s. Punkt 3.1
- Team Prof. Margit Scholl mit Frauke Fuhrmann u.a. (TH Wildau), s. Punkt 3.4.

Weitere Experten:

- Dr. Sandro Gaycken, Direktor des Digital Society Institute Berlin, ESMT Berlin, zählt zu den führenden Experten im Bereich IT-Security und befasst sich mit den Auswirkungen der Informationstechnologien auf unsere Gesellschaft.[19]
- Fred Maro, Geschäftsführer von FM-nospy. Fred Maro gilt international als Experte, wenn es um die Themen Ausspähen, Wirtschaftsspionage und Social Engineering geht. Maro ist Autor einiger themenbezogenen Fachbücher[20], berät zahlreiche Unternehmen und lehrt an mehreren Fachinstituten.[21]

Leitblätter des ASW zum Thema Social Engineering (2017) und CEO-Fraud (2016)

Mit Stand Juli 2017 hat der ASW ein *Leitblatt zum Thema Social Engineering* herausgegeben. Dort werden auf 2 Seiten komprimiert Informationen zur Definition, Vorgehen der Angreifer, Rollen des Social Engineer sowie Hinweise zur Prävention für Unternehmen und Mitarbeiter angeboten. Dieses Leitblatt dient als Erstinformation für Unternehmen, um über-

[18] Nähere Informationen zur Veranstaltung unter: Url: http://www.bluff-city.net/ . (Stand: 27.10.17)

[19] U.a. Keynote Speaker am 15. Juni 2017 im Auswärtigen Amt bei einer Informationsveranstaltung zur Gefährdungslage rund um CyberAngriffe und Social Engineering. Vgl.Url: https://www.stiftung-nv.de/de/veranstaltung/sven-herpig-moderiert-expertenpanel-zu-social-engineering-im-ausw%C3%A4rtigen-amt (Stand: 27.10.17)

[20] Das bekannteste in diesem Zusammenhang ist das bereits 2012 erschienene Buch: „Von netten und anderen Menschen", Verlag: epubli GmbH; Auflage: 1 (17. Oktober 2012), ISBN-10: 3844232095, ISBN-13: 978-3844232097.

[21] U.a. war Maro als Leiter des VDI-Spezialtages SE – Risikofaktor Mensch am 20.06.17 vorgesehen. Vgl. Url: https://www.vdi-wissensforum.de/industrie-40-weiterbildung/social-engineering/. (Stand: 27.10.17)

haupt Sensibilität für diese Thematik zu wecken und eine Richtung für Lösungsansätze vorzugeben.

Bereits 2016 hat der ASW ein *Leitblatt zum Thema CEO-Fraud* herausgegeben. Dort werden Charakteristika der Tatbegehungsweise, Identitätscheck als Gegenmittel sowie Fallbeispiele samt konkrete Verhaltensempfehlungen für Mitarbeiter gegeben. Solche Informationen eines Verbands mit entsprechender Zielgruppenerreichbarkeit, zeitnah herausgegeben, sind wichtige Bausteine einer effektiven Präventionsarbeit.

3.6 Europol Erkenntnisse

Im *IOCTA 2016* ist dem Themenfeld SE ein eigenes Kapitel gewidmet, mit einem Schwerpunkt auf CEO-Fraud (neben PHISHING und Advanced Fee Fraud). Der Modus operandi wird zusammenfassend beschrieben und in seiner weltweiten Ausbreitung dargestellt. Über die Festnahme von 60 Verdächtigen im Rahmen der Operation Triangle wird berichtet. Europol sieht ein Ansteigen der Gefahr in dem Maße als dass die Verbreitung sozialer Netzwerke und „social apps" wächst. Die Vorteile dieser Kommunikationswege können und werden von potentiellen Tätern erkannt und genutzt. Die Empfehlungen Europols beziehen sich hauptsächlich auf folgende Punkte:

- Einrichtung effizienterer Meldewege für diese Massendelikte
- Beim Auftreten dieser Massenphänomene Konzentration auf eine effektive Prävention durch Sensibilisierung und Veröffentlichung von Gegenmaßnahmen. Insbesondere konkrete Hinweise, auf welchem Weg und wo, Anzeige erstattet werden kann.
- Frühzeitige Vermittlung der Thematik Informationssicherheit bereits in jungen Jahren als Lebenskompetenz („life skill")
- Frühzeitige Koordination der Präventionskampagnen auf nationaler und internationaler Ebene, um Doppelarbeit zu vermeiden.
- Die Erfahrung hat gezeigt, dass ein konstruktives Zusammenwirken von Wirtschaft und Strafverfolgung erfolgreiche Ermittlungen bedingt. Dazu gehören auch die zeitnahe Anzeige und ein frühzeitiger Informationsaustausch.
- Kontrollregularien wie das „Vier-Augen-Prinzip" oder die „Zwei-Unterschriften-Forderung" sind ein wirksames Präventionsmittel.

Im *SOCTA 2017* ist SE im Kapitel „Fraud" unter „Investment Fraud" kurz erläutert und es wird auf die immensen Gewinne bzw. Schadenssummen hingewiesen. Da hier die Opfer keine Unternehmen sind sondern Privatpersonen lautet die Definition folgendermaßen: „Social engineering techniques are a key element to many different types of fraud. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes." Es wird über die Operation BATEO berichtet, in der mehr als 50.000 Opfer in 34 Ländern identifiziert werden konnten und der Schaden auf mehr als 3 Milliarden € beziffert wird.

Weitere beschriebene Modi operandi sind: Mass Marketing Fraud[22] und Payment Order Fraud (als Spielart des CEO-Fraud).

Es gibt ein einschlägiges laufendes *„Operational Analysis Project" (AP)* mit Beteiligung Deutschlands:

- AP Apate (Betrugsdelikte), Ziel: Unterstützung bei Straftaten (Betrugsdelikten), welche durch bewusst falsche Angaben, einen freiwilligen aber daher auch ungesetzlichen Transfer von Geldbeträgen und/oder Waren bewirken und dem Täter so einen unzulässigen Vorteil verschaffen.

[22] Trickbetrug z.N. älterer Menschen, wobei sich die Täter am Telefon als Polizisten ausgeben und so an vertrauliche Daten, Geld oder Wertgegenstände ihrer Opfer gelangen.

4. Fazit

Trotz weniger wissenschaftlicher Funde im festgelegten Zeitraum sind die psychologischen Grundlagen des Phänomens SE gut erforscht. Die meisten Studien liegen zeitlich schon länger zurück, sind aber, aufgrund der zeitlosen Aussagekraft psychologischer und sozialer menschlicher Verhaltensgrundlagen als Basis gesichert und als Grundlage weiterer Forschung geeignet. In der neueren Zeit finden sich vermehrt Abhandlungen über SE im Zusammenhang mit dem Thema Wirtschaftsschutz. Autoren sind Unternehmensberater, Verbände, Polizei. Hierbei handelt es sich um praxisnahe Fallschilderungen, Präventionsansätze, Bekämpfungsmaßnahmen und erfolgreiche best practise-Ansätze z.B. für eine erfolgreiche Zusammenarbeit. Ebenfalls wurde ein Forschungsprojekt identifiziert, das Wissenschaftler in enger Zusammenarbeit mit der Wirtschaft bzw. einer Beratungsfirma durchführen, um kreative Schulungsmaßnahmen zu entwickeln.

Wie bereits erwähnt, sind die psychologischen Grundlagen weitestgehend erforscht, insbesondere im englischsprachigen Raum und den USA existieren die meisten Studien und Veröffentlichungen und es wird permanent zu aktuellen Entwicklungen und Tatbegehungsmöglichkeiten weiter geforscht und veröffentlicht, z.B. speziell zum Thema Anfälligkeit für SE in sozialen Netzwerken am Beispiel Facebook.[23] Die Beachtung der angloamerikanischen Forschung ist folglich für eine weiterführende Bearbeitung des Themas geboten.

Die sozialwissenschaftlichen Untersuchungen ergeben, dass sechs unterschiedliche soziale Prinzipien eine Manipulationshandlung erleichtern. Zu diesen gehören die Autorität, die Zuneigung und soziale Bestätigung, das Revanchieren, die Konsequenz und der Mangel/ die Knappheit.[24] Darüber hinaus hat es sich gezeigt, dass die Auskunftsbereitschaft von Mitarbeitern im Rahmen von persönlich durchgeführten Abschöpfungsversuchen, lässt man IT-basierte Angriffe unberücksichtigt, mit der räumlichen Entfernung zum Arbeitsplatz zunimmt.[25]

Die Vorgehensweise, dass „normale“ soziale Verhaltensmuster ausgenutzt bzw. missbraucht werden, um illegal an Informationen zu kommen bzw. Menschen zu einem bestimmten Verhalten zu bewegen, erschweren die Prävention und Tatverhinderung. Neu sind immer wieder die Tatbegehungsweisen. Funktioniert eine nicht mehr, wird die Tatvariante abgewandelt. Diese neuen Formen zeitnah zu erkennen, zu melden, aufzubereiten und bekannt zu machen scheint erfolgskritisch. Schon 2012 wurden in der Zeitschrift „der kriminalist“ eine Vielzahl neuer Erscheinungsformen des Trickbetrugs von einem Ermittlungsbeamten bekannt gemacht. Damals noch z.B. folgende Modi operandi, die zum Teil auch heute noch aktuell sind: Skimming-Straftaten, Enkeltricktaten meist z.N. älterer Menschen, Kriminalität rund um Glücksspiel und Call-Center-Betrug.[26]

Prognostisch bleibt zu befürchten, dass SE-Fälle in Zukunft eher ansteigen als abnehmen werden und die Aufklärung problematisch bleibt. Gründe hierfür sind insbesondere:

[23] S. hierzu: Algarni, Abbdullah u.a. (2017): An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. In: European Journal of Information Systems (2017).
[24] Vgl. hierzu Kirsch, S. 135.
[25] Ebd., S. 135.
[26] Vgl. hierzu Dase (2012).

- Die Betrügereien werden weiterhin und zunehmend aus dem Ausland oder von nicht zu identifizierenden Rechnern oder Personen begangen. Dadurch sinkt das Entdeckungsrisiko.
- Scham oder die Angst vor Reputationsverlust kann die Anzeigebereitschaft hemmen.
- Die Aussicht auf immense (schwer abzuschöpfende) Gewinne erhöht den Tatanreiz.
- Die Verfügbarkeit relevanter offener Informationen, die für einen SE-Angriff genutzt werden können, wird eher ansteigen als abnehmen. Dadurch werden Manipulationen erleichtert.
- Der Druck auf einzelne Mitarbeiter in der heutigen Arbeitswelt steigt eher als dass er sinkt und der notwendige Rückhalt/ das Vertrauen in die Organisation, sich vermeintlichen Anweisungen zunächst zu widersetzen, ist nicht immer vorhanden.
- Die „Europäisierung des Betruges“ wir nicht adäquat mit der Europäisierung der Strafverfolgung beantwortet und „die internationale Rechtshilfe ist in hohem Maße defizitär“.[27]

Ganz aktuell erschien in der Süddeutschen Zeitung am 18.10.17 ein Artikel, in dem davor gewarnt wird, dass derzeit immer häufiger mittelständische Unternehmen als Opfer des CEO-Fraud/ Fake President Fraud in den Fokus rücken.[28]

[27] Vgl. hierzu Dase (2012), S. 23.

[28] Vgl.: Süddeutsche Zeitung vom 18.10.17: Die Masche mit dem Chef. Mittelständler werden immer öfter Opfer von Betrügern, die sich als Geschäftsführer ausgeben. Wie Unternehmen sich davor schützen können. Url: http://www.sueddeutsche.de/wirtschaft/fake-president-die-masche-mit-dem-chef-1.3710605.

Literaturverzeichnis

Ausgewertete Publikationen

ASW Bundesverband - Allianz für Sicherheit in der Wirtschaft e.V.(2016): Leitblatt CEO-Fraud. Url: https://asw-bundesverband.de/fileadmin/user_upload/leitfaden_-blatt/Leitblatt_CEO-Fraud_final.pdf (Stand: 29.09.17)

ASW Bundesverband - Allianz für Sicherheit in der Wirtschaft e.V.(2017): Leitblatt Social Engineering. Url: https://asw-bundesverband.de/fileadmin/user_upload/leitfaden_-blatt/17_07_14_-Leitblatt_Social_Engineering.pdf (Stand: 29.09.17)

Europol (2016): IOCTA 2016. S. 32 – 34.

Hellerforth, Michael (2015): Social Engineering - So manipulieren Industriespione ihre Opfer. In WirtschaftsWoche am 09.09.15. Url: http://www.wiwo.de/technologie/digitale-welt/social-engineering-so-manipulieren-industriespione-ihre-opfer/12296134.html (Stand: 18.09.17)

Known_sense (2015): Bluff me if U can – gefährliche Freundschaften am Arbeitsplatz . Url: http://known-sense.de/BluffMeIfUCanAuszug.pdf (Stand: 28.09.17)

Known_sense (2015): Gefahren und Abwehr bei Social Engineering - Selbst mal ein Schwein sein... . In: WIK - Zeitschrift für die Sicherheit der Wirtschaft 2015/4. SecuMedia Verlags-GmbH. Ingelheim. S. 29 – 33.

Kunze, Dirk (2016): Enkeltrick 4.0 - Wenn der falsche Chef Geld will. In: Kriminalistik 8-9/2016, S. 541 - 545.

Kunze, Dirk (2016): Millionenbeute durch clevere Betrüger. In: der kriminalist 11/2016 Bund Deutscher Kriminalbeamter, S. 19-22.

Scholl, Margit u.a. (2017): Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg. In: Wissenschaftliche Beiträge 2017. TH Wildau. Url: https://liveweb.th-wildau.de/files/2_Dokumente/Berichte/WB_2017.pdf (Stand: 26.09.17)

Scholl, Margit u.a. (2016): Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt. In: Detlef Rätz [et. al.] (Hrsg.): Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016, S. 101 – 111.

Schumacher, Stefan (2014): Die psychologischen Grundlagen des Social Engineerings. In: Information, Wissenschaft & Praxis 2014; 65(4-5), S. 215 – 230. DGI-Forum Wittenberg 2013. De Gruyter Verlag.

Schumacher, Stefan (2011): Die psychologischen Grundlagen des Social Engineerings. In: Magdeburger Journal zur Sicherheitsforschung. Magdeburg 2011. Meine Verlag - Wissenschafts-, Sach- und Fachbuchverlag. Url: http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS-001.pdf (Stand: 19.09.17)

Zusätzliche Quellen

Dase, Siegbert (2012): Trickbetrug - neue Erscheinungsformen (Teil 1). In: der kriminalist 4-2012 Bund Deutscher Kriminalbeamter, S. 22 – 27.

Dase, Siegbert (2012): Trickbetrug - neue Erscheinungsformen (Teil 2). In: der kriminalist 5-2012 Bund Deutscher Kriminalbeamter, S. 18 -23.

Fox, Dirk (2014): Social Engineering im Online-banking und E-Commerce. In: DuD – Datenschutz und Datensicherheit 5 – 2014. Springer Verlag. S. 325 – 328.

Hadnagy, Christopher (2014): Social Engineering enttarnt. mitp-Verlags GmbH & Co.KG. ISBN: 978-3-8266-9664-0.

Hesse, Carsten (2013): Keine Geheimnisse mehr. In: WIK - Zeitschrift für die Sicherheit der Wirtschaft 2013/5. SecuMedia Verlags-GmbH. Ingelheim. S. 22 – 26.

Kirsch, Simon (2014): Informationsschutz im Unternehmen – Prävention von Wissensabfluss und die Erkennung von Innentätern anhand derer Verhaltensmerkmale. Norderstedt. BoD-Books on Demand.

Pokoyski, Dietmar (2015): Tiefenpsychologische Cybercrime-Studie „Bluff me if U can“: es fehlt an Notfallplänen und Awareness. In: IT-Finanzmagazin am 14.04.15. Url: https://www.it-finanzmagazin.de/tiefenpsychologische-cybercrime-studie-bluff-me-if-u-can-es-fehlt-an-notfallplaenen-und-awareness-12927/.