Social Engineering (SE)/ CEO-Fraud

Kurzfassung einer Aufbereitung aktueller nationaler Forschungsbeiträge und Publikationen zum Thema SE und CEO-Fraud

Der Bericht hat das Ziel, den aktuellen Forschungsstand zum Thema „Social Engineering (SE)“ und „CEO-Fraud“ der letzten fünf Jahre (2012 – 2017) in Deutschland wiederzugeben. Bei dem vorliegenden Tex handelt es sich um eine gekürzte Fassung. Der Gesamtbericht kann auf der Kommunikationsplattform Wirtschaftsschutz unter www.wirtschaftsschutz.info eingesehen werden.

Die Ergebnisse beruhen auf einer internetbasierte Literaturrecherche[1] im Mai/ Juni 2017 sowie einer zusätzlichen Open-Source-Recherche im September 2017. Zu den Schlagworten „President Fake“ und „Social Engineering“ gab es in den durchsuchten Datenbanken für den Zeitraum 2012 – 2017 sehr wenige Treffer. Zum Schlagwort „CEO-Fraud“ fanden sich bei SpringerLink mehrere hundert Treffer, die überwiegend englischsprachige Studien anboten. Die meisten deutschsprachigen Studien, die sich zum größten Teil mit den psychologischen und sozialwissenschaftlichen Grundlagen zum Phänomenbereich beschäftigen, lagen vor 2012. Im Bericht werden u.a. Studien, Fachartikel, ein laufendes Forschungsprojekt sowie Europol-Erkenntnisse zusammengefasst und bewertet.

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.

Insbesondere im englischsprachigen Raum und den USA existieren die meisten Studien und Veröffentlichungen. Dort 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. 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. Darüber hinaus hat

[1] Recherchiert wurde mit den Schlagworten „President Fake“, „Social Engineering“ und „CEO-Fraud“ in den folgenden Datenbanken: SpringerLink, KrimDok, Bibliothekskatalog des MPI, KrimLit, COD und OPAC des BKA sowie im Bibliothekskatalog der Uni Mainz.

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.

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. Zusätzlich sollte an eine frühzeitige Vermittlung der Thematik Informationssicherheit in der Schule/ Ausbildung bereits in jungen Jahren als Lebenskompetenz („life skill“) gedacht werden. Prognostisch bleibt zu befürchten, dass SE-Fälle in Zukunft eher ansteigen als abnehmen werden und die Aufklärung problematisch bleibt. Gründe hierfür sind insbesondere:

- 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“. [2]

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.[3]

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

[3] 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.