St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

Automated Social Engineering Tools

Overview and comparison with respect to capabilities and detectability

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Dominik Dana, BSc
1910619805

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuer: FH-Prof. Dipl.-Ing. Peter Kieseberg

Ort, TT.MM.JJJJ	(Unterschrift Autor/Autorin)	(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehr- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, TT.MM.JJJJ

(Unterschrift Autor/Autorin)

Zusammenfassung

Postings und Profile in Social-Media-Plattformen beinhalten sehr viele private Informationen, über die man sich in vielen Fällen mit wenig Aufwand in kurzer Zeit einen Eindruck über eine Person verschaffen kann. Schlecht konfigurierte Privatsphäreneinstellungen eröffnen zudem der breiten Öffentlichkeit Zugang zu privaten Bildern, zu Freundeslisten, geben Aufschluss über Arbeits-, Beziehungs- und Familienverhältnisse und enthalten nicht selten weitere private Informationen. Was für die betreffenden Personen meist als harmlose Angaben angesehen und bezeichnet wird, ist in den falschen Händen möglicherweise Gold wert, denn harmlos erscheinende, persönliche Daten und Informationen können weiter genutzt werden, beispielsweise im Rahmen von Social-Engineering-Angriffen gegen die betroffene Person, oder ihr nahestehenden Personen.

Social Engineering wird von vielen Quellen als die Kunst, Menschen durch gezielte psychologische Manipulationen zu bestimmten Handlungen zu bewegen, beschrieben. Der Mensch rückt, nachdem IT-Systeme aus technischer Sicht und mit fortschreitender Zeit immer besser geschützt werden, immer mehr als Angriffsziel in den Mittelpunkt, denn im Unterschied zu den IT-Systemen, können die Menschen nicht so einfach gepatcht und mit Sicherheitsupdates versorgt werden.

Mit einer falschen Identität und entsprechend guten Vorwänden, machen sich Angreifer, ausgestattet mit einfachen technischen Hilfsmittel und dem nötigen psychologischen Nachdruck, an potenzielle Opfer heran. Nicht selten gelten Angriffe auf Privatpersonen nur als ein erster Schritt, als Einstieg und Hilfsmittel, um an weitere Informationen einer anderen Zielperson, oder einer Organisation, der die Zielperson angehört, zu kommen.

Der manuelle Aufwand, der von Social Engineers betrieben wird, um diese Informationen einzuholen, ist teilweise sehr hoch. Sie sind daher bestrebt, Abläufe so weit als möglich zu automatisieren. So ist es Social Engineers, mit dem richtigen Toolset, mit bereits wenigen Menüeingaben und Auswahlen möglich, E-Mail-Adressen aus Social-Media-Profilen zu exportieren, sowie Freundschaftsanfragen und Phishing-Nachrichten an eine Vielzahl von Personen zu senden. Die Nachrichten beinhalten beispielsweise Anhänge, die beim Öffnen bereits unbemerkt Schadsoftware auf dem Gerät der Empfänger ausführen, oder auch Links zu einer vertraut wirkenden Internetseite, die im Hintergrund die einzugebenden Zugangsdaten an ein, von den Social Engineers vorbereitetes System, senden. Das Opfer merkt von all dem nicht viel, im ersten Moment, ab Bestätigen der Anmeldedaten, sieht es so aus, als hätte es sich nur im Passwort vertippt.

In dieser Arbeit wird aufgezeigt, inwieweit Abläufe in einem Social-Engineering-Prozess bereits tatsächlich automatisierbar sind. Es wird dargestellt, welche Möglichkeiten aktuelle, frei verfügbare Tools bieten und wie zuverlässig diese funktionieren, indem sie in der Anwendung miteinander verglichen werden. Das Clustering der Werkzeuge wurde anhand der Phasen eines technischen Social-Engineering-Modells, das sich aus den gängigsten Social-Engineering-Frameworks ableitet, vorgenommen. Jede Sektion enthält zudem am Ende eine tabellarische Aufstellung der erwähnten Werkzeuge.

Abstract

Postings and profiles on social media platforms contain a great amount of private information, which in many cases, can be used to gain an impression of a person in a short time with little effort. Poorly configured privacy settings also provide the general public access to private pictures, friend lists, information about work, relationship and family relationships, and often contain further private information. What is usually considered and described as harmless information for the persons concerned, is potentially worth its weight in gold in the wrong hands, because seemingly harmless personal data and information can be used further, for example in the context of social engineering attacks against the person concerned, or persons close to them.
Social engineering is described by many sources as the art of persuading people to take certain actions through targeted psychological manipulation. As IT systems become better protected from a technical point of view and as time goes on, people are increasingly becoming the focus of attack because, unlike IT systems, people cannot be patched and provided with security updates so easily.
With a false identity and appropriate pretexts, attackers, equipped with simple technical tools and the necessary psychological emphasis, approach potential victims. It is not uncommon for attacks on private individuals to be seen as just a first step, an entry point and a means of obtaining further information from another target, or an organization to which the target belongs.
The manual effort required by social engineers to obtain this information is sometimes very high. They therefore strive to automate processes as much as possible. For example, with the right toolset, it is possible for social engineers, with just a few menu entries and selections, to export email addresses from social media profiles, as well as send friend requests and phishing messages to a variety of people. The messages contain, for example, attachments which, when opened, already execute malware on the recipient's device without being noticed, or links to a familiar-looking website which, in the background, sends the credentials, which had been entered, to a system prepared by the social engineers. The victim does not notice much of all this, in the first moment, after confirming the login data, it looks as if he has only mistyped the password.
This paper shows to what extent procedures in a social engineering process can actually be automated. It is presented which possibilities current, freely available tools offer and how reliably they work by comparing them in use. The clustering of tools was done based on the phases of a technical social engineering model, derived from the most popular social engineering frameworks. Each section also includes a tabular listing of the tools mentioned at the end.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einführung

1.1. Die Begrifflichkeit und Bedeutung des Social Engineering

Der Begriff Social Engineering (SE) ist, spätestens seit der Zeit des pandemiebedingt vermehrten Homeoffices, bekannter denn je, weisen doch etliche Firmen in zahlreichen internen Veranstaltungen zur Steigerung der Awareness, Newslettern, virtuellen Informationskampagnen und vielem mehr, eindringlich auf Möglichkeiten und Folgen eines Social Engineering Angriffs, hin. Es wird größtenteils davor gewarnt, verdächtige E-Mails zu öffnen, keine unbekannten Links anzuklicken, keine unbekannten Anhänge auszuführen und auch keine sensiblen Informationen am Telefon preiszugeben. Zur Unterstützung gegen angewandte Teile des Social Engineerings, werden diverse Tools und Addins in die gewohnte Office Umgebung installiert, welche beispielsweise Phishing Angriffe abwehren sollen, für die Belegschaft aber mehr verwirrend als hilfreich sind. Die Maßnahmen werden daher von eben dieser auch gerne als übertrieben angesehen und belächelt. Aussagen wie „Bis jetzt ist ja eh noch nie etwas passiert“, oder „Früher haben wir das auch nicht gebraucht“, sind dabei nur ein kleiner Ausschnitt aus den Gesprächen in Kaffee- und Teeküchen, oder den Raucherbereichen.
Dabei sind die Unternehmen, die großen Wert darauf legen, dass der angriffsfreie Zustand noch weiter anhält, an dieser Stelle keineswegs paranoid, da fast alle Angriffe mittels Social Engineering in Situationen stattfinden, in denen man sich sicher und gut fühlt. Neben dem gewohnten Büroumfeld, oder während Urlauben sind dies aber auch die eigenen vier Wände [1], [2], [3]. Und daher gelten diese Hinweise, gerade in der aktuellen Zeit, besonders und gerade auch im Homeoffice, wo es zusätzlich noch wichtiger ist, die elektronischen Gerätschaften bei Nichtverwendung entsprechend zu sperren und vor unbefugtem Zugriff zu schützen. Gerne werden Folgen eines unbefugten Zugriffs unterschätzt, denn ein unbefugter Zugriff kann sogar schon innerhalb des eigenen Haushaltes durch fremde, oder aber auch Mitglieder der eigenen Familie stattfinden, wenn das vom Arbeitgeber überlassene Gerät beispielsweise das aktuell einzige im Haushalt befindliche, oder in dem Moment funktionierende, oder eventuell auch zugängliche Gerät ist. Social Engineering bezieht sich dabei weniger auf den Computer, das Smartphone, oder Tablet selbst, als eher auf den Anwender direkt. Social Engineering ist die Kunst des Ausnutzens des schwächsten Glieds der Informationssicherheitssysteme: Die Menschen, die sie benutzen [4].
Je nachdem, welche Ziele die angreifende Seite verfolgt, kann eine Täuschung und Verleitung zu einer bestimmten, meist zum Nachteil der jeweiligen Anwenderinnen und Anwender, Handlung erfolgen. Einer der bekanntesten Experten im Bereich Social Engineering, Kevin Mitnick, beschreibt in Zusammenarbeit mit William Simons, in seinem Buch *„The Art of Deception: Controlling the Human Element of Security“* Social Engineering wie folgt:

> „*Social Engineering ist die Kunst, Menschen zu täuschen oder auszutricksen, um Angreifern zu helfen, ihre Ziele zu erreichen, Informationen von ihnen zu erhalten, oder sie zu einer Handlung zu überreden, aus der Angreifende in irgendeiner Weise profitiert*.“ [1]

und

> „*Social Engineering nutzt Einfluss und Überredung, um Menschen zu täuschen, indem man sie davon überzeugt, dass der Social Engineer jemand ist, der er nicht ist, oder durch Manipulation. Als Ergebnis ist der Social Engineer in der Lage, Menschen auszunutzen. Menschen auszunutzen, um Informationen zu erhalten, mit oder ohne den Einsatz von Technologie*.“ [1].

Wie es zu dazu kommt, dass Social Engineering so an Bedeutung gewinnen konnte, lässt sich wie folgt beschreiben. Social Engineering (SE) ist eine aufkommende Bedrohung, die sich zusammen mit Netzwerken und sozialen Medien entwickelt hat und in den letzten Jahren immer mehr Aufmerksamkeit auf sich gezogen hat. Betrug gab es schon lange vor dem Aufkommen der modernen Technologie. Die weit verbreitete Nutzung von sozialen Medien und des Cyberspace bietet einen fruchtbaren Boden für traditionellen Betrug, da immer mehr persönliche Informationen weitergegeben werden, aber nur wenig Bewusstsein und Maßnahmen zum Schutz dieser Informationen vorhanden sind [5]. Gerade die weit verbreiteten und ständig verfügbaren sozialen Medien und Netzwerke, sogenannte „Social Networking Sites“ (SNS), sind eine Spielwiese um verschiedene Formen von Phishing Angriffen durchzuführen [6].
Arten und Ansätze von Social Engineering haben sich allerdings nicht erst durch, oder mit der Entwicklung der Technologie mitentwickelt, so gab es, neben dem berühmten Trojanischen Pferd um 1184 B.C., erste Formen

bereits in den frühen 1900er Jahren, wo George Parker Social-Engineering-Techniken dazu verwendete, um Touristen zum Kauf berühmter Sehenswürdigkeiten wie der Brooklyn Bridge, zu bewegen [7], oder Victor Lustig, der 1925 den Eiffelturm in Paris sechs Schrotthändlern zum Verkauf anbot und mit dem Interessenten André Poisson einen Kaufvertrag über den aus etwa 7000 Tonnen Eisen bestehenden Turm abzuschließen [8]. Frank Abagnale, in den 1960er Jahren Checks fälschend und später einen Co-Piloten der Airline Pan-Am vortäuschend, ist ein weiteres Beispiel, dessen gelungene Täuschungen sogar von Stephen Spielberg unter dem Titel „*Catch Me If You Can*“ verfilmt wurden [9].
Es drängt sich die Frage auf, warum Social Engineering erst jetzt immer mehr an Bedeutung gewinnt, wenn es doch bereits seit einiger Zeit vor der technologischen Entwicklung der letzten Jahre bestand. Antworten darauf liefern unter anderem Studien und Experimente, wie beispielsweise von Yuki Kano und Tatsuo Nakajima [10] an der Waseda University durchgeführt, worin Vertrauensfaktoren bei Angriffen in sozialen Netzwerkdiensten (SNS) untersucht wurden:

- Mit der Entwicklung der Informationstechnologie in den letzten Jahren haben sich SNSs, wie Twitter und Facebook, entwickelt und die Menschen sind im Internet immer aktiver geworden [10].
- SNSs sind Onlineplattformen, die es erlauben, Inhalte, Wissen und Erfahrungen mit anderen zu teilen und Onlineaktivitäten zu fördern [11].
- Es gibt gezielte Angriffe, bei denen Nutzer, die für ein bestimmtes Unternehmen arbeiten, ausgegeben als Geschäftspartner, identifiziert und über SNSs kontaktiert werden und ihre vertraulichen Informationen über Direktnachrichten gestohlen werden [12].
- Es gibt fortgeschrittene Phishing-Angriffe, die sich über das Teilen von SNS-Posts verbreiten, die zu einem Informationsverlust führen können [6].
- Und nicht zuletzt führen auch Gewöhnungseffekte dazu, dass diverse Links (speziell Shortlinks) angeklickt, Beiträge kopiert, gelikt, geteilt und eingefügt werden, welche schlussendlich ein Social Engineering begünstigen [6].

Dass Social Engineering in den sozialen Netzwerkdiensten so erfolgreich ist, begründet Mironela Pirnau in [13] mit den wichtigsten sieben menschlichen Schwächen:

- Gier (Greed)
- Angst (Fear)
- Gefühl der Wichtigkeit (The feeling of urgency)
- Neugierde (Curiosity)
- Sympathie (Sympathy)
- Respekt vor Authoritäten (Respect towards authorities)
- Vertrauen in bestimmte Personen (Trust in certain person)

Im Vergleich dazu spricht der US-amerikanische Psychologe Robert Cialdini in [14] von den Prinzipien der Beeinflussung durch:

- Das Prinzip der Reziprozität (Reciprocation)
- Das Prinzip des Commitment und der Konsitenz (Commitment and Consistency)
- Das Prinzip der sozialen Bewährtheit (Social Proof)
- Das Prinzip der Sympathie (Liking)
- Das Prinzip der Authorität (Authority)
- Das Prinzip der Knappheit (Scarcity)

Diese Prinzipien wurden in [15] bereits um das Prinzip der Einheit (Unity) und das Prinzip des ständigen Einflusses (Instant Influence) erweitert.
Schlussendlich benötigt es für ein erfolgreiches Social Engineering auch die enstprechend situativen Rahmenbedingungen. Diese werden durch die Covid-19 Pandemie begünstigt, wie die Studie von Kristjan Kikerpill und Andra Siibak [16], die den Anstieg von Social Engineering Angriffen in den ersten vier Monaten der

Pandemie untersucht haben, veranschaulicht. Die Studie zeigt, dass einerseits mit fortschreitender Dauer der Pandemie auch die fortgeschritteneren Angriffe zugenommen haben und diese darauf abzielten, Vorteile aus dem Verlangen nach aktuellen Informationen zu ziehen und andererseits, dass es hauptsächlich zwei primäre Kommunikations Strategien („Good Samaritan“ und „Shock and Awe“) gegeben hat, wovon die Strategie „Good Samaritan“, also die helfen wollende Strategie, mehr zur Anwendung gekommen ist.

1.2. Arten von informationsunterstützem Social Engineering

Nach einer kurzen Einführung in die erhöhte Bedeutung, Entwicklung und die Hintergründe, warum Social Engineering funktioniert, fehlt für ein gesamtheitliches Bild noch die Art und Weise, wie dies aus technischer Sicht funktionieren, aussehen und ablaufen kann. Nachfolgend wird dieses, durch Listung und Beschreibung der Arten von Social Engineering, mit Bezug auf die Nutzung von IT-Systemen, ergänzt. Die Arten und Taxonomien, wie Social Engineering durchgeführt werden kann, sind sehr vielfältig und haben sich über die letzten Jahre technologisch ständig weiterentwickelt. Während einerseits die meisten dieser Typen weiterhin mit physischen Anwesenheiten, oder vielen einzelnen Schritten manueller Tätigkeiten verbunden sind, wurden bereits auch Werkzeuge entwickelt, die diese unterstützend automatisiert ablaufen lassen können. Entsprechende Unterscheidungen zwischen „Human based“ und „Computer based“ oder „Technology based“ finden sich auch in den Arbeiten [17], [18], [19] wieder. Die vorliegende Arbeit thematisiert die aktuell verfügbare Automatisierung in den Social-Engineering-Tools, daher werden im Folgenden nur die jeweils geeigneten Arten des Social Engineering beschrieben, die mit Unterstützung von Informationssystemen durchgeführt werden können und mit Automatisierung den Prozess des Social Engineering vereinfachen, oder zumindest Möglichkeiten für eine Automatisierung bieten.

1.2.1. Phishing

Phishing Attacken wurden erstmals in den frühen 2000er Jahren beobachtet [20] und die Gefährdung durch Phishing nimmt weiter zu [21]. Allein in Österreich wurden, mit Stand August 2021, um 88 Prozent mehr Phishing Attacken in den Homeoffices [22] verzeichnet. Weltweit wurden, basierend auf dem Sophos Phishing Insights Report 2021, Steigerungen um 70 Prozent ausgewiesen [22], [23]. Das Zentrum für sichere Informationstechnologie – Austria (A-SIT) hat die Daten der Trend Reports von der Anti-Phishing Workgroup der letzten Jahre aufbereitet und auf deren Internetseite veröffentlicht. Das Diagramm in Abbildung 1 veranschaulicht den Anstieg von Phishing in E-Mails und Phishing über Webseiten in dem Zeitraum zwischen dem ersten Quartal 2018, bis zum aktuell vorliegenden Report aus dem zweiten Quartal 2021.

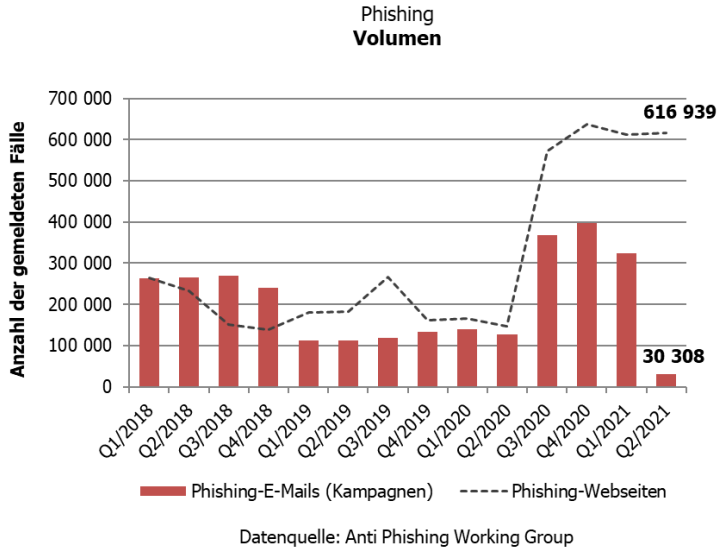


Abbildung 1: Phishing Volumen Q1/2018 – Q2/2021, Grafik [21], Datenquellen [24]

Für Phishing direkt gibt es keine durchgängige und einheitliche Begriffsdefinition. Das Ziel ist allerdings immer das selbe, mit Links zu manipulierten Webseiten, an persönliche Informationen und Anmeldedaten zu gelangen,

beziehungsweise diese zu „erfischen“. Die Phishing-Nachrichten selbst sind dabei in großer Anzahl an unbestimmte Empfänger der Allgemeinheit gerichtet, deren Daten entweder generiert, oder aus Databreaches stammen und sind zumeist E-Mail-Nachrichten mit einem entsprechenden Vorwand, der teilweise auch als „Vorschussbetrug“, oder „419 Scam“ [25] bekannt ist.
Von dem Social-Engineering-Typ Phishing gibt es wiederum verschiedenste Klassifikationen, beispielsweise Spear-Phishing (Phishing Nachrichten, die speziell an eine Person, oder Organisation angepasst wurden), Smishing (ein Kunstwort, generiert aus dem Wort SMS und Phishing), Vishing (abgeleitet aus Voice und Phishing, im Grunde handelt es sich dabei um persönliche Anrufe), und Whaling (Phishing Nachrichten, die gezielt an wichtigere Schlüsselpersonen gerichtet werden). Eine in den letzten Jahren entstandene Version wird auch SPIM genannt, worunter Spear-Phishing via Instant Messenger oder Instant-Messaging-Scams, verstanden wird. Smishing war gerade in der Zeit, in der die vorliegende Arbeit verfasst wurde, ein sehr aktuelles Thema in der Öffentlichkeit. Im Frühjahr des Jahres 2021 wurden häufig SMS mit Notifikationen verschickt, dass ein vermeintliches Paket zur Abholung bereit wäre. Im darauffolgenden Herbst wurden die Nachrichten von der Benachrichtigung über vermeintliche Pakete zur Abholung, auf hinterlassene Sprachnachrichten abgeändert.

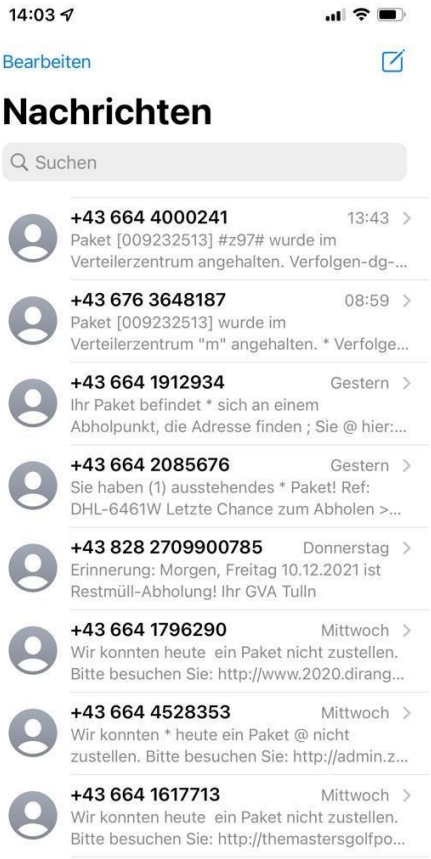


Abbildung 2: Zugestellte Smishing-Nachrichten im Zeitraum einer Woche (KW49/2021)[26]

Um Smishing-Angriffe einzudämmen, ergreifen Mobilfunkprovider Maßnahmen zur Filterung der Nachrichten. Diese bieten allerdings keine vollständige Schutzfunktion, da Nachrichten manchmal absichtlich Buchstabendreher, Schreibfehler oder zufällige Zeichenketten enthalten, um die Spam-Filter der Mobilfunkbetreiber zu umgehen [27]. Sprachnachrichten sind für die Mobilfunkbetreiber, wie die absichtlich mit Fehlern versehenen Textnachrichten, ebenfalls schwer filterbar. Der Provider T-Mobile Austria beobachtet, laut eigenen Angaben, ebenfalls einen starken Anstieg der Phishing Aktivitäten und führt in einem eigenen Blog [28] online verschiedene Beispiele, die in deren Namen im Zeitraum zwischen Dezember 2013 und November 2021 durchgeführt und bekannt geworden sind, an.

1.2.2. Baiting

Hinter dem Begriff Baiting verbergen sich Köderangriffe auf potenziell neugierige Opfer. Falsche Versprechen, verlockende Texte, oder vermeintlich erzielte Gewinne bei Websitebesuchen, wecken Begehrlichkeiten bei den späteren Betrugsopfern. Meist erfolgt das sogenannte Baiting mit infizierten USB-Sticks, mit präparierten Werbegeschenken, oder anderen (auch gerne als „vertraulich“ und alternativen, die Neugierde erweckenden, Beschriftungen versehenen) Datenträgern, auf denen sich Malware befindet, die geschickt versteckt ist, sodass diese nicht sofort auffällt. Viele, zumeist mit Windows betriebene, Computersysteme haben per Default die automatische Wiedergabe von Wechselmedien aktiviert, welche beim Auslesen der Datenträger unbemerkt im Hintergrund die versteckte Malware ausführt und so den Rechner des neugierigen Opfers infiziert. Diese speziell präparierten Datenträger werden gerne an häufig frequentierten Orten ausgelegt, wo sie garantiert entdeckt und mitgenommen werden. Ein Security Consultant namens Steve Stasuikonis machte ursprünglich diese Art von Social Engineering vor vielen Jahren populär und ihre Beliebtheit hält noch heute an [7]. Die Taktik des Baiting beschränkt sich dabei nicht nur auf physische Medien, sie kann auch mit einem Download und neben der Installation von Software direkt aus dem Internet (beispielsweise über Werbeeinblendungen) erfolgen.

1.2.3. Water-Holing

Hinter dem sogenannten „Water-Holing“ verbirgt sich eine weitere, aber subtilere Version des zuvor beschriebenen Phishing. Hierbei kann es vorkommen, dass bereits vonseiten der Social Engineers Informationen über Kunden, Lieferanten und Partner eines Unternehmens eingeholt wurden und deren Internetauftritte oder Portale dahingehend manipuliert wurden, dass Links auf vertrauten Webseiten zu manipulierten Webseiten umgeleitet werden. Damit dies den späteren Opfern nicht so einfach auffällt, werden Domains, die für diese Verlinkungen genutzt werden, nach Typo- und Cybersquatting Methoden [29] reserviert. Dies bedeutet, dass Domains registriert werden, in denen beispielsweise Zeichen innerhalb des Domainnamens verdreht werden, Buchstaben gegen Ziffern ausgetauscht werden, oder gar einzelne Zeichen weggelassen werden und so sogenannte „Doppelgänger Domains“ entstehen. Zur Veranschaulichung könnte so beispielsweise abgeleitet von www.google.at eine Doppelgänger Domain www.g00gle.at, oder www.goog1e.at reserviert werden. Damit Domains, die nach Typo- und Cybersquatting Methoden reserviert wurden, nicht von diversen WebCrawlern und Blacklists abgefangen werden, werden diese einige Zeit vor deren produktiver Nutzung mittels CNAME-Records zu den „richtigen“ Seiten verlinkt. Finden WebCrawler die Verlinkungen im Internet, werden sie richtig umgeleitet und klassifizieren die Doppelgänger Domains als sicher. Diese Klassifizierung kann mitunter auch den Versand von Phishing-Nachrichten via E-Mail begünstigen [30].
Es existieren alternativ zu dem Registrieren von Domains via Typo- und Cybersquatting, aber auch Plattformen, die demnächst ablaufende, oder auch kürzlich gelöschte Domainnamen, listen. Eine solcher Plattformen ist, betrieben von Marco Schmidt, ExpiredDomains.net [31]. So kann im besten Fall sogar eine kürzlich noch für nicht bösartige Zwecke genutzte Domain die Seite wechseln und für Water-Holing genutzt werden.
Sobald die Water-Holing-Seite und die entsprechende Verlinkung zu einer solchen publiziert ist, muss auf der Seite der Social Engineers nurmehr abgewartet werden, bis jemand auf den Link klickt und diese aufruft. Gerne wird, sollte eine Water-Holing-Seite über ein Spear-Phishing-E-Mail verlinkt werden, in Formularfeldern bereits die E-Mail-Adresse der Spear-Phishing Opfer hinterlegt, sodass für diese der Eindruck entsteht, diese Seite bereits einmal besucht zu haben [30].

1.2.4. Scareware und Rogue Security Software

Die beiden Typen „Scareware“ und „Rogue Security Software” (auch als „Rougeware“ bezeichnet) sind sich grundsätzlich sehr ähnlich. Während die als Scareware bezeichnete Version aus Popups, Einblendungen oder auch Werbebannern besteht, die sich sehr schwer wegklicken lassen [32], wird die Rogue Security Software meist auf dem Gerät des Opfers direkt installiert. Beide haben gemein, dass sie Anwenderinnen und Anwender mit falschen Alarmen vor angeblichen Sicherheitsproblemen, oder Viren auf dem Gerät des Opfers warnen und damit einschüchtern wollen. Scareware verleitet, mit geschickt formulierten Texten und Buttons auf Internetseiten dazu, diese angeblichen Probleme mit einem Klick zu beheben, oder eventuelle Vollversionen der präsentierten Software zu beziehen. Ein beispielhafter Screenshot ist in der nachfolgenden Abbildung 3 angeführt. Grafiken und Logos, in teilweise auch optisch nachgestellten Fehlermeldungen, entsprechen dabei bewusst und weitgehendst denen namhafter Hersteller, damit die Chancen höher sind, diese leichter zu verwechseln. Bei einem Klick auf einen solchen Button wird erst recht Schadsoftware heruntergeladen.

Rouge Security Software tarnt sich oft als Antivirus- oder Antimalwareprogramm, das ebenfalls mit der Entfernung von Schadsoftware wirbt, oder auch als Tweaking-Tool, das eine Optimierung des als langsam bewerteten Systems vornehmen soll, wenn dieses installiert wird. Jedoch wird, bei Installation der vermeintlichen Security Software, Schadsoftware, wie Spyware, Malware, oder Trojaner, auf das Gerät des Opfers geladen [33]. Beispiele für Rogue Software können, neben den „Security Suites“ auch 3rd Party Browser Plugins, Bilder und Zip-Archive aus E-Mails, oder Drive-By-Downloads sein, die auch bei Installation von beispielsweise Multimedia Codecs, unbemerkt heruntergeladen werden können, sein.

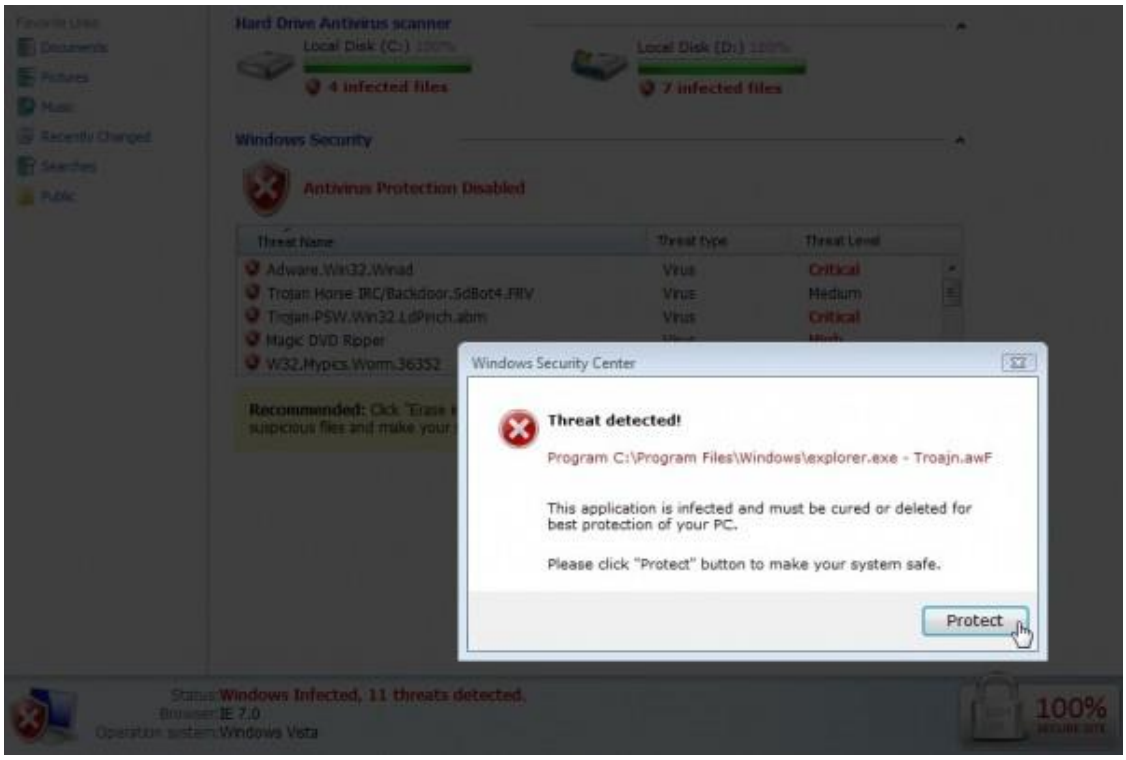


Abbildung 3: Scareware Beispiel Popup Fenster [34]

1.2.5. Pretexting und Impersonation

Unter Pretexting und Impersonation wird, wortwörtlich jeweils der Vorwand, oder die Ausrede und das Nachahmen, oder der Wechsel einer Identität, verstanden. Pretexting ist damit die Geschichte, die den Social-Engineering-Opfern vorgespielt wird, wenn ein physisches Zusammentreffen der Social-Engineering-Seite und der Opfer-Seite zustande kommt. Christopher Hadnagy beschreibt Pretexting als Schaffung eines erfundenen Szenarios, um ein Opfer dazu zu bringen, Informationen preiszugeben, oder eine Handlung vorzunehmen. Es geht um mehr als nur eine Lüge, in einigen Fällen kann es sich um die Schaffung einer völlig neuen Identität handeln [2]. Impersonation hängt mit dem Pretexting sehr oft zusammen, da in einer der Geschichten und Vorwände, die sich in einer Social-Engineering-Attacke abspielen, meist auf jemand Prominentes, Namhaftes, oder Bekanntes, berufen wird. So wird eine Social-Engineering-Attacke gerne so vorbereitet, als dass der Pretext im Auftrag einer autoritären, oder vorgesetzten Stelle, von gerade nicht verfügbaren Kolleginnen und Kollegen, eines Servicedienstes, des IT-Supports, aber auch von Kunden, Lieferanten, oder von gesetzlicher Seite her, stattfindet. Pretexting und Impersonation sind umso erfolgreicher, je genauer und je mehr Informationen zuvor über das, oder die jeweiligen Opfer eingeholt werden konnten [2].
Pretexting und Impersonation finden nicht nur auf der physischen Ebene, sodass die Social Engineers vor Ort kommen, statt. Pretexting und Impersonation sind jeweils auch eine wichtige Grundlage von funktionierenden Phishing-, Vishing- und Smishing-Angriffen.

1.3. Automation und Automationsmöglichkeiten bei Social Engineering

Die Erfolgsquote und Effizienz von Social-Engineering-Angriffen nimmt zu. Viele Informationen über die Opfer können manuell, oder durch automatisierte Tools zur Informationsbeschaffung gesammelt werden. Das Hinzufügen von Informationen über die Zielpersonen erhöht die Wahrscheinlichkeit, dass sie Opfer eines Phishing-Angriffs werden [35], [36]. Social Engineering erfordert jedoch viel Zeit für die Pflege von Beziehungen, den Aufbau von Vertrauen und die anschließende Ausnutzung der Benutzerinnen und Benutzer, um an geheime Informationen zu gelangen [37]. Social Engineers verwenden Kombinationen der zuvor erwähnten Social-Engineering-Techniken, um jegliche, digital hinterlassenen Arten von Spuren ihrer Angriffsziele und späteren Opfer aufzuspüren, zu verwerten und um gegebenenfalls Passwörter, Sicherheitsabfragen umgehen, oder herausfinden zu können. Die dazu genutzten Tools sind, hinsichtlich der grundlegenden Informationsbeschaffung, größtenteils im Open Source Intelligence (OSINT) Bereich angesiedelt. OSINT ist eine Entwicklung aus dem, während des 2. Weltkrieges durch William Donovan gegründeten, „Office of Strategic Services“, das später zur „Central Intelligence Agency (CIA)“ wurde [38]. Neben dem Social Engineering wird OSINT auch für zahlreiche andere Anwendungsgebiete genutzt, beispielsweise für die Suche von Vermissten, im Geheimdienst, für journalistische Arbeiten, Recruiter greifen bei Bewerbungen darauf zurück, Strafverfolgungsbehörden, während Penetrationtests, oder auch im Zivil- und Katastrophenschutz [38]. Die OSINT-Tools greifen dazu auf eine große Sammlung an im Internet öffentlich zugänglichen Informationen über Personen, Organisationen und anderen Gebieten zurück. Unter Verwendung dieser Tools ist es mit etwas Suchaufwand beispielsweise auch abseits von kostenpflichtigen Informationsquellen und des Darknets möglich an geleakte Benutzerdaten von beispielsweise vergangenen Databreaches zu gelangen.
Es lässt vermuten, dass für die manuellen Tätigkeiten bei der Informationsbeschaffung, bei der Vorbereitung und Ausarbeitung von Vorwänden für passende Angriffsarten sehr viel Zeit aufgewendet werden muss. Zeit, die die angreifende Seite entweder im konkreten Fall nicht hat, oder aber auch nicht aufwenden möchte, da diese Aufwände mit dem Ergebnis und Ziel des Angriffs, in keinem lukrativen Verhältnis stehen. Diese Zeit lässt sich mit automatisierten und teilautomatisierten Werkzeugen erheblich verkürzen. Aus der Sicht der Social Engineers müssen die Angriffe automatisiert werden, um viele Opfer zu erreichen und er sollte menschenähnlich sein, damit mehr Opfer darauf hineinfallen [39].
Automatisierungsmöglichkeiten bieten sich in der Information-Gathering, oder auch Reconnaissance-Phase genannt, an. In dieser Phase ist die Möglichkeit der Automatisierung groß, da es eine große Vielzahl an verschiedensten OSINT-Tools gibt, die Suchen erheblich vereinfachen. Es gibt dazu nicht nur eine große Community an OSINT-Interessierten und Begeisterten, sondern auch unzählige Linklisten, die in versteckten Foren und Social-Media-Gruppen geteilt werden und auf online verfügbare, sowie direkt ausführbare Webapplikationen zur Informationsgewinnung führen. Während, beispielsweise im Rahmen einer ersten Information-Gathering-Phase, nach bekannten Benutzern stundenlang manuell auf verschiedenen Plattformen und Social-Media-Kanälen gesucht werden müsste, kann diese Aufgabe bereits von eigenen Suchmaschinen, quer über hunderte von Plattformen, mit wenigen Mausklicks erledigt werden. Ähnlich verhält es sich mit dem Erstellen von Phishing-Nachrichten, oder Phishing-Sites. Anstatt selbst Websites zu gestalten, die für Water-Holing oder Phishing-Angriffe genutzt werden, oder anstatt selbst eine hohe Anzahl an Phishing-Nachrichten via E-Mail auszusenden, genügen ein paar Menüauswahlen oder Klicks in den jeweiligen Tools und Toolsets. Diese Tools sind teilweise sogar bereits in eigenen Betriebssystemumgebungen vorkonfiguriert und einsatzbereit, beziehungsweise mit grundlegend vorhandenen Linux Betriebssystemkenntnissen einfach nachlad- und konfigurierbar. Dafür bekannte Umgebungen sind Kali Linux mit dem bereits integrierten Social Engineering Toolkit (SET), aber auch BlackArch mit dem Social Package. Etwas neuer sind beispielsweise die Distributionen CSI-Linux [40] und Tsurugi-Linux [41], die ebenfalls einen großen Umfang an Werkzeugen, die für automationsunterstütztes Social Engineering genutzt werden können, beinhalten.
Weitere Möglichkeiten der Automation bietet bereits auch die Interaktion mit Menschen. Es gab bereits einige Experimente, wo Social Engineering mit Robotern oder Chat-Bots durchgeführt wurden. Mit dem iCub Experiment [3] wurde veranschaulicht, dass es durchaus möglich ist, dass Menschen zu Robotern im Dialog ein Vertrauen aufbauen und die Roboter dieses aufgebaute Vertrauen anschließend ausnutzen können. Andere Beispiele für die bereits automatisierte Interaktion zwischen einem Menschen und einem Chat-Bot sind „ELIZA“ [42], ein Chat-Bot der 1966 von Joseph Weizenbaum entwickelt wurde und einen Psychotherapeuten imitiert und damit auch als einer der ersten einen eingeschränkten Turing Test [43] bestanden hat, oder auch „TayandYou“, ein Twitter-Chat-Bot mit künstlicher Intelligenz aus dem Hause Microsoft [44]. Während Microsofts Bot Tay am 23.03.2016 online ging und nach 16 Stunden bereits wieder abgeschalten werden musste, da Tay dynamisch von Twitter-Postings moralisch und ethisch verwerfliche Antworten gelernt und gepostet hatte und ein weiterer Versuch eine Woche später ebenso misslang [45], sind Ableger von Eliza hingegen aufgrund der sehr einfachen Kommunikation, noch immer online verfügbar [46]. Ein weiteres Exemplar ist das Experiment

von Markus Huber et al., wo am Beispiel einer Implementierung eines Automated Social Engineering (ASE) Bots [4] gezeigt wird, dass Social Engineering in den Chats der sozialen Netzwerke mit einem automatisierten Chat-Bot, bereits zur damaligen Zeit (2009) möglich war. Das Experiment, respektive der ASE-Bot, wurde ebenfalls einem Turing Test unterzogen.
Die Studie von Priya Kaul und Deepak Sharma beschreibt Automated Social Engineering ebenfalls mit Bots, als automatisierte Form des traditionellen Social Engineering, das unter Zuhilfenahme von Bots, SNS attackiert [47]. Die beiden Autoren sind außerdem der Meinung, dass ASE-Bots einfach unter Verwendung von OpenSource-Web-Automation und Web-Scraping-Tools entwickelt werden können [47]. Und weiter, dass diese Tools in Kombination mit einer geeigneten Chat Logik mit fortgeschrittener Intelligenz, eine große Bedrohung für die Sicherheit von SNS darstellen [47].
Eine fortgeschrittenere und technisch aufwändigere Art von Social-Engineering-Automation kann auch in den über Social-Media-Plattformen durchgeführten Angriffen mit KOOBFACE [48] und Honeybot [39] gesehen werden. Während sich hinter KOOBFACE ein ganzes Botnet befunden und bösartige Absichten verfolgt hat, fungierte Honeybot als ein Forschungsprojekt, in der virtuellen Unterhaltung zwischen zwei echten Personen, als Chat-Bot, als „Bot in the Middle (BITM)“.
Eine typische Infektion mit KOOBFACE begann immer mit einer Spam Nachricht, die über SNSs verschickt wurde und einen vermeintlichen YouTube-Videolink enthalten hat. Wurde der Link angeklickt, so wurde man auf eine nachgestellte YouTube-Seite (die in Wirklichkeit „YuoTube“ hieß) geleitet, auf der zum Abspielen des Videos noch eine ausführbare `*.exe` Datei nachgeladen werden musste. Diese ausführbare Datei, ein vermeintlicher Codec, war der Downloader für die restlichen KOOBFACE Komponenten [47], [48]. KOOBFACE hatte eine Variante der TROJ_LDPINCH Malware implementiert, die von den infizierten Rechnern der Opfer digitalen Windows IDs, Internet-Profile, E-Mail-Benutzerdaten, FTP-Benutzerdaten und Instant Messaging (IM) Benutzerdaten abgegriffen hat. KOOBFACE war außerdem in der Lage, Nachrichten an andere Freunde zu senden und konnte über das Durchsuchen von Offlinedaten und Cookie-Einträge innerhalb der jeweiligen SNS filtern. KOOBFACE war entsprechend schwierig aufzufinden, da die ASE-Attacken sehr menschenähnlich und damit sehr schwierig aufzufinden waren. Facebook selbst hat zum Cracken des KOOBFACE Botnets drei Jahre gebraucht [49].
Mit dem Chat-Bot Honeybot gehen Tobias Lauinger et al. in einem 74-tägigen Experiment in dem Bereich des automatisierten Social Engineering einen Schritt weiter und zeigen, dass es mit einem Chat-Bot möglich ist, automatisch ein Gespräch zwischen zwei menschlichen Benutzern zu starten, das Gesprächsthema zu beeinflussen, die Gesprächsteilnehmer dazu zu bringen, die Links, die von der Forschergruppe in die Konversationen eingefügt wurden, anzuklicken und Techniken anzuwenden, die die Konversationen der beiden Teilnehmer verlängern [39]. Honeybot könnte auch für eine Version des durchgeführten Tinder Social Engineering Attack [50] Experiments von Anthony Zboralski eingesetzt werden.
Andere Automationsmöglichkeiten sind über Plattformen im Dark Web zu finden. Mit einer monatlichen Gebühr von 250 $ kann ein „Social Engineering as a Service“ Dienst abonniert werden, der Opfer mit automatisierten Robocalls sensible Finanzdaten am Telefon entlockt [51]. Einen, in dem ASE-Bereich noch weiteren, bedeutenden Schritt, macht die zwischenzeitliche Weiterentwicklung der künstlichen Intelligenz. So kann diese mittlerweile dazu genutzt werden, um ASE-Bots zu entwickeln, die selbstständig Onlinezeiten von Benutzern in sozialen Netzen auswerten [52], [53], oder um Spear-Phising-Postings in sozialen Netzwerken zu tätigen, wie beispielsweise das auf der DEF CON24 vorgestellte Projekt *„Social Network Automated Phishing with Reconnaissance“: SNAP_R* [54] [55]. Die Weiterentwicklung kann von Social Engineers aber auch dazu genutzt werden, Deepfakes (ein mit Hilfe künstlicher Intelligenz erstelltes Bild oder Video, das authentisch wirkt, es aber nicht ist [56]) zu entwickeln. Wo es vor zehn Jahren noch schwierig war, die Stimme und das Auftreten einer Person im Internet nachzuahmen, ist es heute dank ausgefeilter Technologie nicht nur möglich, sondern in einigen Fällen auch ziemlich überzeugend. Nach Angaben des FBI werden ab März 2021 böswillige Akteure in den nächsten 12 bis 18 Monaten mit ziemlicher Sicherheit synthetische Inhalte für Cyber- und ausländische Beeinflussungsoperationen nutzen [57].

2. Ziele und Rahmen der Arbeit

2.1. Aufbau der Arbeit

Die vorliegende Arbeit beginnt mit einer kurzen Einführung unter Kapitel 1, die an das Thema und den Begriff des Social Engineering oberflächlich heranführen soll. Dabei soll verdeutlicht werden, warum Social Engineering und die Möglichkeiten der Automatisierung bei Social-Engineering-Angriffen, von großer Bedeutung sind. In dem aktuellen Kapitel wird auf die Struktur, die Ziele, aber auch auf den Rahmen der Arbeit eingegangen. Den Abschluss des Kapitels bilden die Formulierungen der Forschungsfragen, anhand dieser die Arbeit verfasst wurde. Während der Recherche zum aktuellen Stand der Forschung wurden verwandte Arbeiten aufgefunden, welche in dem nächsten Kapitel untersucht und analysiert werden.
Rechtliche und ethische Aspekte, die bei, oder bereits vor der Verwendung von Werkzeugen im Social-Engineering-Kontext, wie beispielsweise bei Anwendung von OSINT-Tools, entstehen, werden in der Sektion 4 thematisiert. Da sowohl rechtliche, als auch ethische Aspekte Auswirkungen auf die Ergebnisse der vorliegenden Arbeit haben, werden auch gewählte Umgänge anderer Autoren in anderen Publikationen angeführt. Das Kapitel 5, „Social-Engineering-Phasenmodelle und Frameworks“, widmet sich verschiedenen Ansätzen, wie Social Engineering in einer Art Framework abgebildet werden kann. Dieser Part ist ein wichtiger Bestandteil, da mit der Arbeit ergründet werden soll, welche Phasen eines Social-Engineering-Angriffs bereits mit automatisierten Werkzeugen unterstützt stattfinden können und wie diese Werkzeuge zusammenspielen. Die Werkzeuge, die während der Recherche analysiert, getestet und bewertet wurden, werden in Kapitel 6, Toolunterstütze Automation , gelistet und vorgestellt. Den Abschluss der Arbeit bilden ein zusammenfassendes Conclusio mit Erkenntnissen, die während dem Verfassen der Arbeit gewonnen werden konnten, der Beantwortung der Forschungsfragen, sowie mit Möglichkeiten für weiterführende Arbeiten, unter Sektion 7.

2.2. Ziele der Arbeit

Social Engineering ist quer durch die Unternehmenshierachien, aber auch in privater und persönlicher Umgebung, eine ernstzunehmende und ansteigende Bedrohung, die gerade in dem Zeitalter des mobilen Arbeitens und vermehrt ermöglichten Homeoffice nicht zu unterschätzen ist. Zumeist befindet sich gerade im beruflich bedingten Homeoffice niemand, der Kolleginnen und Kollegen in der unmittelbaren Umgebung (an dem jeweiligen Standort, beziehungsweise zuhause), die entweder bei Unsicherheit schnell konsultiert werden, oder die bei Erkennen einer stattfindenden Attacke (beispielsweise einem gerade stattfindenden Tailgaiting, verdächtigen Phishing-Nachrichten, oder einem eingehenden Vishing-Anruf) unterstützen können. Der Hauptunterschied zwischen Social-Engineering-Angriffen und anderen Angriffen auf die Informationssicherheit besteht darin, dass sie auf jede Person in einem Unternehmen abzielen können, unabhängig von ihrem Rang, ihrem Wissen, ihrem Gehalt oder anderen Merkmalen [58]. Diese Angriffe können, je nach Kreativität der Angreifer sehr unterschiedlich ausfallen und basieren zu einem großen Teil auf dem wichtigsten Part, dem Auffinden von Informationen über das Angriffsziel. Da diese sogenannte Information-Gathering-Phase in manueller Durchführung sehr zeitaufwändig ist, gibt es mittlerweile eine Vielzahl an unterstützenden Tools, die den Zeitaufwand minimieren können.
Die Ziele der Arbeit sind einerseits Automatisierungs-Tools zu analysieren, deren Anwendung zu testen und die Qualität der Ergebnisse zu bewerten. Andererseits soll dabei auch ein Überblick geschaffen werden, wie weit Automation bei Social-Engineering-Tools bereits vorhanden ist und ob, beziehungsweise welche Phasen eines Angriffs bereits automatisiert ablaufen können. Weitere Ziele dieser Arbeit sollen auch die Darstellung der Zuverlässigkeit, sowie die Verfügbarkeit und das Zusammenspiel dieser Tools sein. Darunter ist einerseits zu verstehen, ob die Tools kostenfrei und uneingeschränkt verwendbar sind, andererseits wie und ob Tools in Kombination verwendet werden können. Erwähnung sollen neben den auffindbaren Tools und Toolsuites auch verfügbare Livesysteme finden.

2.3. Methodik, Rahmen und Eingrenzungen

Grundlegende Social Engineering Basics, Abläufe und Herangehensweisen wurden den Werken von Kevin Mitnick [1], [59], Christopher Hadnagy [2], [25], Peter Kim [30] und Jeremiah Talamantes [7] entnommen. Der aktuelle Stand der Forschung und verwandte Arbeiten facheinschlägiger Literatur, wurden unter Zuhilfenahme von digitalen Bibliotheken erhoben. In Verwendung standen dazu größtenteils Onlinebibliotheken von IEEEXplore, ScienceDirect, ACM Digital Library und offene Publikationen von Springer. Die Onlinebibliotheken wurden im Zeitraum von August 2021 bis Januar 2022 nach Arbeiten, die Kombinationen und Keywords, welche mit „Automated Social Engineering“ in Verbindung stehen und beinhalten, durchsucht. Sämtliche verwendbare Literatur aus den Suchergebnissen wurde im Literaturverzeichnis der vorliegenden Arbeit aufgenommen.
Die Tools, die Automatisierung im Social Engineering ermöglichen, wurden explorativ erforscht, die Suchbereiche waren dabei, wie auch die späteren Anwendungsbereiche, bis auf die Vermeidung der Nutzung des Deep Webs, nicht eingegrenzt. Verwendet wurden unterschiedliche Suchmaschinen, um einer eventuellen Einschränkung von Suchergebnissen nicht zu unterliegen. Zur Recherche genutzt wurden die Suchmaschinen Google, DuckDuckGo und vereinzelt Bing. Ebenfalls miteinbezogen in die Suchen wurden facheinschlägige Foren, Communities, zugriffsbeschränkte Gruppen innerhalb der gängigen Social-Media-Kanäle, sowie Repositories auf GitHub. Aktive Recherchen im Deep Web und Darknet wurden vermieden, Verlinkungen in verwendeten Literaturen und Berichten wurden allerdings berücksichtigt.
Der primäre Anwendungsbereich der recherchierten Tools umfasst allerdings nicht direkt Anwendungen für, oder auf Smartphones, da dies den Umfang und Rahmen der Arbeit aufgrund der Vielfalt der verschiedenen Plattformen, erheblich erweitern und sprengen würde. In den verschiedenen Bereichen des Phishing sind diese aber dennoch, bedingt durch die Verwendung der mobilen Endgeräte zum Empfang von Nachrichten (SMS, E-Mail, diverse Messenger) und Anrufen, als mögliche der Angriffsziele, generisch miteinbezogen.

2.4. Problemstellung und Forschungsfragen

Zu Beginn der Arbeit, sowie auch während einer ersten Recherche im Bereich des Social Engineerings, hat sich die Frage gestellt, welche Möglichkeiten für eine Automatisierung aktuell bestehen und wie zuverlässig deren Endergebnisse ausfallen. Während der ersten Literaturanalyse, sowie Recherche und Analyse von verwandten Arbeiten, wurden die Fragestellungen erweitert, welche und wie weit Phasen des Social Engineerings bereits automatisierbar sind und wie sich das Zusammenspiel verschiedener Tools gestaltet. Bei der Recherche nach ersten geeigneten Tools hat sich herausgestellt, dass einige der Tools kostenpflichtig und nur mit entsprechendem Hintergrund beziehbar sind, sowie dass die Funktionalitäten bei vielen Tools auf Bundesstaaten der USA eingeschränkt waren. Ebenfalls ist aufgefallen, dass die Verfügbarkeit und die Funktionalitäten, bedingt durch die Einführung der Datenschutz-Grundverordnung (DSG-VO) innerhalb der Europäischen Union (EU), limitierter ist. So führten beispielsweise Links auf nicht mehr vorhandene Internetseiten, oder auf Seiten zu Tools, deren letzte Releases Jahre zurück lagen. Die Erkenntnisse während der Toolrecherche haben die Forschungsfrage RQ1 um den Teil der freien Verfügbarkeit und die Bedeutung auf das Social Engineering, erweitert.

RQ1	Wie weit sind frei verfügbare Social Engineering unterstützende Tools bereits automatisiert und was bedeutet dies in Bezug auf das Social Engineering?
RQ2	Welche Phasen des Social Engineering können mit den Tools bedient werden?
RQ3	Wie spielen die verschiedenen Tools zusammen, gibt es Toolsuites die einen kompletten Social-Engineering-Prozess an- und begleiten?
RQ4	Wie zuverlässig sind die Ergebnisse der Tools?

Tabelle 1: Forschungsfragen

Am Ende der vorliegenden Arbeit sollen die unter Tabelle 1 gelisteten Forschungsfragen RQ1 bis RQ4 beantwortet und ein Überblick über einen, zum Zeitpunkt der Verfassung der Arbeit, aktuellen Stand an verfügbaren Werkzeugen, geboten werden.

3. Literaturanalyse und verwandte Arbeiten

3.1. Techniken und Tools

Wer sich mit dem Bereich des Social Engineerings beschäftigt, kommt an Publikationen von Kevin Mitnick nicht vorbei. Er beschreibt in einem seiner bekanntesten Bücher [1] Richtungen und Grundlagen eines erfolgreichen Social Engineerings, sowie Techniken, die bei der Durchführung angewandt werden und zeigt, welche Ziele für Social Engineers von besonderem Interesse sind. Der Fokus liegt eher auf physischen Anwendungen und ist technologisch nicht mehr ganz aktuell, dadurch in dieser Arbeit in geringem Umfang verwertbar. Aktueller sind hingegen Blogeinträge auf seiner Internetseite, wo er von der Geschichte des Social Engineerings schreibt, über Typen, gängigste Angriffe und die größten Angriffe in der Geschichte, aber auch Gegenmaßnahmen beschreibt [59] und wie Technologie aus seiner Sicht die Zukunft des Social Engineering verändern wird [57].
In ähnlichem Maße sind auch die Literaturen von Christopher Hadnagy [2], [25] gehalten, wobei in der neueren Ausgabe „*The Science of Human Hacking*“ bereits OSINT-Techniken und eine kleine Auswahl an Social-Engineering-Tools Erwähnung finden. Weitere erste nutzbare Tools und Techniken führt Peter Kim in „*The Hacker Playbook 2*“ [30] in einem eigenen Kapitel, das sich nur auf Social Engineering bezieht, an.
Jeremiah Talamantes bezieht sich in „*The Social Engineer's Playbook*” [7] insgesamt ebenfalls eher allgemein auf das Thema Social Engineering, führt aber, neben physischen Werkzeugen und Möglichkeiten zum Social Engineering via Telefon, die Anwendung von speziellen Google Suchoperatoren („Google Hacking“), sowie SET (Social Engineering Toolkit) und Maltego aus. Die beiden Tools SET und Maltego zählen zu den etabliertesten und umfangreichsten Tools der Social-Engineering-Szene, da sie im weiteren Verlauf in mehreren Publikationen Erwähnung, oder Anwendung, gefunden haben. Aufgrund der beinhalteten Automation wurden sie ebenfalls in die Liste der, in dieser Arbeit thematisierten Tools, mitaufgenommen.
Wang et al. sind nicht nur der Meinung, dass technische Angriffe zunehmend schwieriger werden und Angreiferinnen und Angreifer daher immer mehr in Richtung Social Engineering gehen, sie bieten in [18] auch einen sehr umfangreichen Überblick über Angriffsmotivationen, -ziele und -strategien. Weiters fassen sie in dem Paper die Wirkung von Social Engineering in sechs Aspekten zusammen und unterscheiden zwischen Angriffen der Kategorie „Human-Based“ und „Computer-Based“. Sie fassen die Top 3 der menschlichen Vulnerabilitäten in Leichtgläubigkeit, Hilfsbereitschaft und Konformität, die Top 3 der Angriffsmedien in E-Mail, Website und Telefon, zusammen. Dass diese auch die häufigsten Angriffsmethode darstellen, die in Phishing-, Vishing- und Smishing-Angriffen resultieren, berichten auch Bilikis Banire et al. in [60].
Eine ähnliche, wie zuvor von Wang et al. dargestellte Unterscheidung der Angriffe in „Human-Based“ und „Technology-Based“, treffen Hussain Aldawood und Geoffrey Skinner in [19]. Sie kommen in dem Paper weiters zu dem Schluss, dass virtuelle Communities, nachdem in diesen Plattformen oft persönliche Daten gespeichert werden, die größte Quelle für Social-Engineering-Angriffe darstellen, da wenig technologisches Know-How benötigt wird, sobald mit den Opfern ein Vertrauen aufgebaut worden ist. Diese Erkenntnis wiederum deckt sich auch mit den Ergebnissen der in Kenya durchgeführten Studie aus [61], wo ebenfalls Phishing und Smishing als die prominentesten Angriffsmethoden identifiziert wurden.
Katharina Krombholz et al. unterscheiden in dem Paper *„Advanced social engineering attacks“* [17] bei der Anwendung nicht nur ähnlich, wie zuvor erwähnt, zwischen „Software“ und „Human“, sie klassifizieren auch die Angriffskanäle in E-Mail, Instant Messenger, Telefon und VoIP, soziale Netze, Cloud, Website und in Physisch, sowie die Angriffsvektoren in Dumpster Diving, Advanced Persistent Threat (APT), Baiting, Phishing, Shoulder Surfing, Reverse Social Engineering und Waterholing und stellen diese in einer Tabelle gegenüber, um zu zeigen, dass verschiedene Angriffsvektoren über verschiedene Techniken und Kanäle bedient werden können. Auch in diesem Paper findet sich die Aussage und Erkenntnis, dass die sozialen Medien und Netzwerke eine gute Quelle für Social Engineering darstellen, da in der Welt der allgegenwärtigen Kommunikation die Menschen in diesen nach Belieben Inhalte veröffentlichen, ohne sich dabei viele Gedanken über Sicherheit und Datenschutz zu machen. Sie teilen dabei hochsensible Dokumente und Informationen mit anderen virtuellen Nutzern rund um den Globus und halten diese, aufgrund ihrer Profile oder angegebenen E-Mail-Adressen, für vertrauenswürdig.

Das eBook von Nihad A. Hassan und Rami Hijazi [62] thematisiert Methoden und Werkzeuge, die größtenteils im OSINT-Bereich, welcher als ein Teil des Information-Gathering-Prozesses innerhalb des Social Engineerings angesehen werden kann, angesiedelt sind. In der Publikation wird neben einer generellen Einführung über Onlinebedrohungen und Gegenmaßnahmen, auf die Bereiche Social Media Intelligence (SOCMINT) und People Search Engines eingegangen. Es werden zwar eine Vielzahl an Methoden und (webbasierenden) Tools erwähnt, der Hauptanwendungsbereich dieser liegt allerdings in den USA. Bedingt durch die DSG-VO sind diese innerhalb der EU größtenteils nicht nutzbar. Dass viele dieser Werkzeuge in den meisten Fällen auf die USA zugeschnitten sind, wird auch in der Publikation *„Open source intelligence“* von Isabelle Böhm und Samuel Lolagar [38] erwähnt.
Wie sich OSINT-Techniken und Tools mit der DSG-VO verändern und vertragen, wird von Ludo Block in einem Artikel in [63] und in einer Publikation von Leonore ten Hulson [64] thematisiert. Letzteres verschafft eine sehr gute Übersicht über rechtliche Unterschiede und die Möglichkeiten, die sich mit OSINT ergeben. So wird beispielsweise das Auffinden von, einem der in den Niederlanden meistgesuchten Verbrecher, Shahin Gheiybe [65], [66], mittels verwendeter OSINT-Techniken innerhalb der Social-Media-Plattform Instagram beschrieben und dies auch aus rechtlicher und ethischer Sicht beleuchtet. Anhand des Fallbeispiels und der veränderten Landschaft der strafrechtlichen Ermittlungen sieht Leonore ten Hulson die Rolle der Zivilbevölkerung bei strafrechtlichen Ermittlungen gestärkt und eine neue hervorkommende Art der Justiz.
Chancen und Risiken für die Polizeiarbeit der Zukunft sieht Julia Fricke in einer Kombination von OSINT und Polizeiarbeit in [67]. So könnten Systeme um öffentliche Informationen aus den Social-Media-Plattformen erweitert werden und damit in Kombination mit polizeilichen Daten in Big Data-Analysen dazu genutzt werden, um Verhaltensmuster, Trends, oder auch künftige Straftaten, abzuleiten.

3.2. Fortgeschrittenere Angriffe und Automationen

Neben den Literaturen, die schwerpunktmäßig von Techniken und Tools handeln, wurden während der Recherche auch verwandte Arbeiten ausgemacht, die sich mit fortgeschritteneren Angriffsmöglichkeiten und Automation im Bereich des Social Engineerings auseinandersetzen.
Mit vergangenen und zukünftigen Formen der Automatisierung der menschlichen Interaktionen, inklusive den daraus resultierenden ethischen und sozialen Dilemmas, setzt sich [68] auseinander und definiert Automation simpel und naiv als Systeme, die die Ausführung von Aufgaben von Menschen übernehmen und dadurch einfach den Arbeitsaufwand, oder die Aufmerksamkeit, die Menschen für diese Aufgaben aufwenden müssen, reduzieren. Weiter werden in einem Venn-Diagramm Online-Chat-Bots als Schnittmenge zwischen „Automated System“ und „Non-professional user“ dargestellt.
Wang et al. sind in [35] der Meinung, dass die breite Anwendung und Verfügbarkeit von SNSs, dem Internet der Dinge (IoT), industriellem Internet und mobilen Geräten, größere Angriffsflächen für Social Engineering geschaffen haben. Sie begründen dies mit riesigen Datenmengen, die durch deren Nutzung entstehen und dass Menschen in der heutigen Zeit mehr Informationen über deren persönliche Identität, deren Aktivitäten, Beziehungen, Standorten und persönliche Interessen, aber auch über deren Arbeit und Arbeitsumgebungen, in den sozialen Medien teilen, sowie mit der Verbreitung von Social-Engineering-Tools und deren offener Quellcodes, die groß angelegte Social-Engineering-Angriffe erleichtern. Die Anwendung neuer Technologien, wie beispielsweise dem maschinellen Lernen oder der künstlichen Intelligenz, in Kombination mit neuen Bedrohungsformen, wie beispielsweise APTs, ermöglichen es, hocheffiziente, zielgerichtete und intelligente Social-Engineering-Angriffe durchzuführen. SET und Maltego finden, neben Phishing Frenzy und Gophish, auch in dieser Arbeit Erwähnung, mit der Bemerkung, dass diese auch von nicht professionellen Hackern und Script-Kiddies einfach für halbautomatische Angriffe angewandt werden können. Wang et al. beschreiben und führen in dem Paper weiter, neben Möglichkeiten zur Umgehung von Phishing- und Deeplearningdetection, auch die automatisierten Chat-Bots von Markus Huber (ASE-Bot) [69], Tobias Lauinger et al. (Honeybot) [39], sowie John Seymour und Philip Tully (SNAP_R) [54], an. Der ASE-Bot, Honeybot und zusätzlich der sich als Malware über die Social-Media-Plattform Facebook verbreitete Bot Koobface, werden auch in der Studie von Priya Kaul und Deepak Sharma [47] als automatisierte Social-Engineering-Tools angeführt.

Davide Ariu et al. definieren und verwenden damit, in Kombination mit dem, hauptsächlich in SNSs naiven Verhalten der Menschen, in [70] dafür den Begriff „Social Engineering 2.0“, welches unter anderem aus einem Malware Ecosystem 2.0, modernem OSINT, der Weiterentwicklung der Angriffsvektoren und automatisierten Social-Engineering-Angriffen, sowie der Nutzung von bereits bekannten Methoden (auch aus Human- und Sozialwissenschaften) besteht.
In den Arbeiten von und mit Markus Huber et al. [4], [69] wird der zuvor bereits erwähnte ASE-Bot beschrieben. Dieser wird allerdings nur auf der Social-Media-Plattform Facebook angewandt und interagiert auf dieser mit Studenten einer, nach bestimmten Kriterien ausgewählten Gruppe, an schwedischen Universitäten. Das Experiment wird aufgrund ethischer Bedenken und fehlender PTA (Permission to Attack) Dokumente abgeändert. In der Abänderung wurden die Zielpersonen schlussendlich nur einem Turing-Test unterzogen und danach befragt, ob sie sich entscheiden können, ob sich hinter den zwei genutzten Testaccounts ein Mensch, oder der ASE-Bot verbirgt.
Tobias Lauinger et al. gehen mit Honeybot in [39] nach eigenen Angaben einen Schritt weiter als der ASE-Bot. Sie lassen Menschen nicht direkt mit einem Bot kommunizieren, sondern initiieren eine Unterhaltung zwischen zwei echten Personen und schalten Honeybot als „Bot in the Middle“, dazwischen. Das Verhalten von Honeybot ist in dieser Position dabei mit dem Verändern, Ersetzen oder Löschen von Nachrichtenteilen, individuell steuerbar. Auf der jeweiligen Seite des Gegenübers ist das Vertrauen, sowie auch die Chance, beispielsweise durch Honeybot eingefügte, oder veränderte Links aufzurufen, im Vergleich zu anderen Chat-Bots stark erhöht.
Eine weitere Möglichkeit für Automatisierung im Social Engineering demonstrieren John Seymour und Philip Tully mit dem Projekt „*Social Network Automated Phishing with Reconnaissance*“ (SNAP_R) [54], das auf der Social-Media-Plattform Twitter aufsetzt. Twitter ist ihnen zufolge ein guter Ort für automatisiertes Spear-Phishing, da die Plattform über eine Bot-freundliche API verfügt und aufgrund der Zeichenbeschränkung in Postings auch Shortlinks und gebrochenes Englisch akzeptiert werden. Nachdem SNAP_R ein Ziel ermittelt hat, wird an dieses ein maschinell erzeugter Tweet gesendet, welcher unter Verwendung von Markov Models [71] und Long Short-Term Memory (LSTM) rekurrent neuronalen Netzen [72], generiert wird und zumeist einen Shortlink enthält. SNAP_R, das ursprünglich für Sicherheits- und Awarenessmaßnahmen, oder auch die Werbebranche entwickelt wurde, wird als Erweiterung zu SET beschrieben, da es bislang noch keine automatisierte Software gibt, die Phishing-Nachrichten in der Art an eine größere Zielgruppe verteilen kann.

3.3. Vertrauensfaktoren als Grundlagen für die Funktionalität von Automation

Während der Recherche, dem Lesen und Analysieren von Literaturen zu dem aktuellen Stand hinsichtlich Automation im Social-Engineering-Bereich, stellte sich die Frage, welche Vertrauensfaktoren es ermöglichen, dass automatisierte Social-Engineering-Angriffe ebenfalls funktionieren können, da Social-Engineering-Angriffe doch oft sehr dynamisch und nicht exakt durchplanbar sind.
Yuki Kano und Tatsuo Nakajima kommen nach einem Experiment in *„Trust Factors of Social Engeineering Attacks on Social Networking Sites”* [10] zu dem Schluss, dass es darauf ankommt, ob auf Postings positiv oder negativ reagiert wird und ob diese von vertrauensvollen Personen geteilt wurden. Dass die Menschen verdächtige Links in Nachrichten von Facebook-Freunden eher öffnen als beispielsweise von ihrer Bank, thematisiert auch Aron Stern bei Kaspersky [73], sowie Edwin Frauenstein und Stephen Flowerday in [6]. Letztere führen in ihrem Paper weiter aus, dass es auch weit verbreitet ist, nicht eingeschränkte Facebook-Profile zu klonen und Freundschaftsanfragen an Freunde dieses originalen Profils zu senden. Ziel ist es, mit dem geklonten Profil überzeugende Phishing-Nachrichten zu versenden, oder die Facebook-Freunde dazu zu bringen, Phishing-Links anzuklicken. Die Chancen, dass diese bösartigen Links angeklickt werden, sind hoch, da den Autoren zufolge die Menschen sich mit der ständigen Aktualisierung der SNSs daran gewöhnen, Nachrichten, Beiträge und Links anzuklicken, zu liken und zu teilen, sowie diverse Medieninhalte hoch- und herunterzuladen. Dies führt dazu, dass Nutzerinnen und Nutzer anfälliger für Social-Engineering-Angriffe in SNSs werden, da sie diese Nachrichten nicht aus der Sicherheitsperspektive heraus betrachten.
Yazan Boshmaf et al. berichten in [74], dass die meisten „Online Social Network“ Nutzerinnen und Nutzer nicht vorsichtig genug sind, wenn sie Verbindungsanfragen von Fremden bekommen, speziell dann nicht, wenn sie bereits gemeinsame Verbindungen haben. Diese Annahme wird durch ein Experiment mit einem Socialbot-

Network untermauert, das die Gruppe über die Dauer von acht Wochen mit 102 Socialbots und einem Botmaster, auf Facebook losgelassen hat. Die Ergebnisse haben gezeigt, dass zu dem Zeitpunkt, wo das Experiment durchgeführt wurde, es möglich war, Facebook mit einer Erfolgsquote von bis zu 80 Prozent zu infiltrieren, es abhängig von den Privatsphäreneinstellungen möglich war, private Daten in großem Umfang zu sammeln und dass das Facebook Immune System (FIS) diesen Angriff nicht effektiv genug stoppen konnte. Yazan Boshmaf et al. führen in dem Paper weiter aus, dass die nächste Generation an Social-Engineering-Angriffen noch trügerischer sein werden und beziehen sich dabei auf ein experimentelles Projekt namens „Realboy“ [75], das darauf abzielt glaubwürdige Twitter-Bots zu entwerfen, die richtige Twitter-Nutzerinnen und Nutzer, imitieren können. Ihr Experiment vergleichen sie am Ende des Papers mit dem Botnet Koobface [48].
Eine andere Art des automatisierten Social Engineering stellt das Experiment mit dem Roboter iCub [76] dar. Alexander Mois Aroyo et al. nutzen in [3] einen Social-Engineering-Bot, entwickelt von dem Italian Institute of Technology, der das Vertrauen von Teilnehmerinnen und Teilnehmern während eines Schatzsuchspiels gewinnen möchte. Das Experiment baut auf Kevin Mitnicks Social-Engineering-Modell auf. iCub versuchte verschiedene Arten von persönlichen Informationen in einer Art Eingewöhnungsphase mit den Teilnehmerinnen und Teilnehmern des Experiments zu sammeln, die normalerweise manuell von Social Engineers mit einer Reihe von Fragen gesammelt werden. iCub versuchte damit das Vertrauen der Teilnehmerinnen und Teilnehmer zu gewinnen und eine Beziehung zu diesen aufzubauen, indem er hilfreiche Hinweise, während des zeitlich begrenzten Schatzsuchspiels, innerhalb eines Testraumes gab. Am Ende des Spiels versuchte iCub das gewonnene Vertrauen auszunutzen, indem er die Teilnehmerinnen und Teilnehmer dazu brachte, das gewonnene Geld zu verspielen. Das Experiment hat primär gezeigt, dass die Menschen tatsächlich dazu tendieren, Vertrauen und Beziehung zu einem Roboter aufzubauen und dabei auch sensible, persönliche Informationen von sich preisgeben.

3.4. Alternative Fameworks

Neben den klassischen Frameworks und Social-Engineering-Modellen, auf die in der nachfolgenden Sektion 5, Social-Engineering-Phasenmodelle und Frameworks, eingegangen wird, wurden während der Recherche auch alternative Ansätze entdeckt, die Social-Engineering-Angriffe auf neuem Wege klassifizier- und vergleichbar machen sollen.
Tong Wu et al. entwickeln in [5], nach einer umfassenden Analyse über den aktuellen Stand an wissenschaftlichen Arbeiten, Modellen und Frameworks zu Social Engineering, ein eigenes, neues Framework, das auf dem Konzept von Social-Engineering-Sessions (SES) und Social-Engineering-Dialogen (SED) aufsetzt. SES bestehen hierbei aus zumindest einem oder mehreren SEDs. SEDs beziehen sich hier auf spezifische Angriffsphasen und stellen in diesem Framework eine atomare Einheit, die einzelne Verbindungen zwischen den Angreifern und dem Ziel darstellen, dar. Die Anwendbarkeit des Frameworks wird anhand dreier, bereits stattgefundenen und bekannten Social-Engineering-Angriffen, geprüft und gezeigt.
Kristjan Kikerpill und Andra Siibak entwerfen in [16], in Anlehnung an eine alte arabische Fischereitechnik „Almadraba“ das Konzept des „Mazephishing“, wo es für einen erfolgreichen Fang auf die drei Kriterien des richtigen Zeitpunktes (timing), des richtigen Ortes (place) und der richtigen Technik (trap-setting technique), ankommt. Sie verbinden die Erkenntnisse aus der Fischerei, in der es unter Beachtung der drei Kriterien wichtig ist zu verstehen, warum Fische zu einem bestimmten Zeitpunkt in großer Anzahl unterwegs sind, wo es für die Fischer am günstigsten ist, die Fischwanderungen zu unterbrechen und mit welcher Technik die Fische gefangen werden können, mit der Welt des Social Engineering, während der ersten Monate der weltweit vorherrschenden Covid-19 Pandemie. Die Erkenntnisse zeigen, dass das Element „timing“ mit der Covid-19 Pandemie, aber auch mit anderen aktuellen Zeitgeschehen (beispielsweise Weihnachten) begründet werden kann, dass das Element „place“ die Medien, mit denen verschiedene Betrügereien durchgeführt werden, umfasst und unter dem Element „technique“ die Art und Weise, wie diese Betrügereien, basierend auf Robert Cialdinis Prinzipien der Beeinflussung [14], [15], durchgeführt werden, verstanden wird. Das Konzept soll dabei, so die Verfasser des Papers, die zu wenig beachtete Bedeutung des sozialen Kontextes bei Social-Engineering-Angriffen erfassen.

In einer noch sehr frühen Anfangsphase eines anderen Ansatzes, um die angewandten und eingesetzten Taktiken von Social Engineers zu verstehen, befindet sich die Studie *„Understanding Social Engineers Strategies from the perspective of Sun-Tzu Philosophy“* [77]. In dieser wird versucht, Social Engineering aus der Sicht und Richtung der Erklärungen des Philosophen, Militärstrategen und Schriftstellers Sun-Tzu, verständlich zu machen. Die Sun-Tzu Philosophie besteht in dem Paper aus fünf fundamentalen Faktoren für den Erfolg im Krieg, aus sechs Prinzipien für Angriffsstrategien und fünf Prinzipien für Verteidigungsstrategien, die nacheinander und beispielhaft mit Social-Engineering-Szenarien, erklärt werden. Eine tabellarische Übersicht stellt die fünf fundamentalen Faktoren Moral (Morality), Klima (Climate), Umgebung (Terrain), Führung (Generalship) und Lehre (Doctrine), den Bedeutungen in Krieg, betrieblichem Umfeld und innerhalb des Social Engineerings, gegenüber.

4. Rechtliche und ethische Aspekte

4.1. Rechtliche Aspekte

4.1.1. Datenschutz-Grundverordnung

Bei dem Zusammenstellen und Suchen nach Informationen im Rahmen des Social Engineerings (in einschlägigen Foren und in der SE- und OSINT-Community auch als „Doxing“ [78], [25] bezeichnet) wird mit Daten und Informationen von und über bestimmte Personen gearbeitet. Daten und Informationen, die auf Personen rückführbar sind, gelten in der aktuellen Fassung der Datenschutz-Grundverordnung (DSG-VO), unter Artikel 4, als personenbezogene Daten [79]. Weiters wird von der Verordnung als Verarbeitung

> „*jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung*“ [79]

bezeichnet.
Die Verarbeitung von personenbezogenen Daten gilt als rechtmäßig, wenn die betroffene Person ihre Einwilligung (nachweisbar und widerrufbar) zu der Verarbeitung der sie betreffenden Daten für einen oder mehrere bestimmte Zwecke, gegeben hat [79]. Bei der Verarbeitung muss der Grundsatz der Datenminimierung eingehalten werden und die Erhebung

> „*dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.*“ [79].

Die Menge und Speicherdauer der Daten sollen somit, neben der Zweckbindung, auf das Notwendigste reduziert werden. Als Regel kann gesagt werden, so viel wie nötig, so wenig wie möglich. [63]. Eine Empfehlung der Autoren von ebenfalls [63] lautet, ein Untersuchungsprotokoll anzulegen, in dem die Datenverarbeitungsschritte nachvollziehbar und der Umgang mit den Grundsätzen und den verarbeiteten Daten beschrieben werden. Auf die Korrektheit der verarbeiteten Daten bezogen, fordert die Datenschutz-Grundverordnung weiter, Personenbezogene Daten müssen

> *„sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)*;“ [79].

Hinsichtlich der Speicherung der verarbeiteten Daten gilt es ebenfalls zu beachten, dass der Verarbeiter, neben der Form und erforderlichen Speicherdauer, auch für den entsprechend Schutz verantwortlich ist. Als Regel kann hierzu angeführt werden

> „*If you cannot protect it, don’t collect it*“ [63].

4.1.2. Strafgesetzbuch

Nachdem bei der vorliegenden Arbeit keine Angriffe auf Computersysteme stattfinden, keine Störungen dieser ausgelöst werden und auch nicht durch Umgehen von Zugangsbeschränkungen oder technischen Sperren in

fremde Systeme eingedrungen wird, sind die „Hacker-Paragraphen“ 118a, 119a und 126a bis 126c des österreichischen Strafgesetzbuchs (StGB) [80] hier nicht anwendbar und damit auch nicht relevant.
Ebenfalls werden und wurden mit der vorliegenden Arbeit keine betrügerischen Absichten, welche die Paragraphen 146 und 147 des österreichischen Strafgesetzbuchs betreffen, verfolgt.

4.2. Ethische Aspekte

Neben den erwähnten rechtlichen Aspekten gibt es bei der Arbeit mit Daten und Informationen fremder Personen oder Institutionen, auch ethische Aspekte zu bedenken. Auch wenn Informationen über Personen und Institutionen frei im Internet auffindbar sind, kann und sollte grundsätzlich nicht davon ausgegangen werden, dass diese auch frei zur Verwendung stehen. Was rechtlich gesehen erlaubt ist, bedeutet nicht, dass es ohne Weiteres auch aus ethischer Sicht machbar und erlaubt ist. Aufgefundene Daten und Informationen könnten beispielsweise aus veröffentlichten Databreaches oder Datendiebstählen stammen, über deren öffentliche Verfügbarkeit die jeweilige Person oder Institution zu dem jeweiligen Zeitpunkt noch gar keine Kenntnis hat. Es könnte sich aber auch um Daten handeln, die die betreffende Person oder Institution auch weiterhin geheim gehalten haben möchte, diese hier allerdings plötzlich der Allgemeinheit frei zugänglich wären. Das Amsterdam Law Forum schreibt hier in einer Publikation von einem Privatsphären-Paradoxon: Die Informationen sind öffentlich verfügbar und für alle zugänglich, also nicht von Natur aus privat, aber gleichzeitig handelt es sich oft um (sensible) persönliche Informationen, die daher von Natur aus privat sind [64].
Informationen können allerdings in der falschen Kombination auch anders interpretiert und so zu ungewollten und ungünstigen Ergebnissen für die jeweiligen Betroffenen werden. [62] beschreibt, ein weiteres Dilemma besteht darin, dass die OSINT-Stichprobe je nach den Bedürfnissen des Sammlers minimiert oder ausgewählt wird. Sie könnten tatsächlich wichtige Quellen absichtlich vernachlässigen, um ein bestimmtes Ergebnis zu erzielen. Weiters stellt sich gerade auch im Hinblick auf die Automatisierung von Social-Engineering-Werkzeugen die Frage, inwieweit den Ergebnissen automatisierter Maschinen vertraut werden kann und ob diese sie genauso behandeln wie die von Menschen gesammelten Daten? Was, wenn ein Softwarefehler in der Software vorliegt, der ungenaue Ergebnisse erzeugt, die schädliche Folgen haben [62]?
Die Frage nach der zulässigen Anwendung zur Evaluierung von automatisierten Social-Engineering-Tools ist aus ethischer Sicht damit nicht so einfach beantwortbar. Diese Werkzeuge auf Funktionalität und Zuverlässigkeit zu prüfen, funktioniert natürlich am besten, wenn die Rolle eines Angreifers, oder einer Angreiferin eingenommen wird und eine ausgewählte „Person of Interest“ nicht über einen, beispielsweise Phishing-Angriff, informiert ist. Die Chancen stünden hierbei am höchsten, dass ein Phishing-Link angeklickt wird. Dies macht jedoch Personen unwissentlich zu Teilnehmern in einer Versuchsreihe [4] und könnte eventuell Daten liefern, die auf keinen Fall gewollt bekanntgegeben werden möchten. So könnte sich eines der Opfer beispielsweise tatsächlich mit einem, von seinem Umfeld bewusst geheim gehaltenen, Social-Media-Konto anmelden und damit Daten zu diesem Profil und eventuell auch sensiblen Unterhaltungen liefern. Hingegen würde eine vorherige Information den Versuch möglicherweise verfälschen, da nicht sichergestellt werden kann, ob das Phishing nur dem Versuch zuliebe funktioniert hat, oder tatsächlich funktioniert haben könnte. Eine ähnliche Sicht würde für einen zu Versuchszwecken eingesetzten Chat-Bot gelten.

4.3. Gewählter Umgang mit beiden Aspekten in anderen Arbeiten

Jeremiah Talamantes empfiehlt in „*The Social Engineers Playbook*” bei Penetration-Tests, die Social Engineering beinhalten, die Verwendung eines “Rules of Engagement (RoE) Plans”. Dies ist ein mit dem Social-Engineering-Team und dem Kunden vereinbarter Plan für die Durchführung eines Social-Engineering-Tests. Die RoE müssen jeden Social-Engineering-Test begleiten und sie müssen von allen Teammitgliedern strikt befolgt werden [7]. Ähnliches ist in den Literaturen von Christopher Hadnagy [2], [25] und in der Literatur von Ian Mann [81] unter einer „Get Out of Jail Free Card“, oder auch bei Markus Huber et. al. unter „Permission to Attack (PTA)“ [4], zu finden. Diese Vereinbarungen decken sowohl die rechtlichen, als auch die ethischen Aspekte ab und grenzen dabei auch den Rahmen bei Social Engineering ein.

Markus Huber versuchte in [69] und [4] vorab für Experimente mit einem selbstentwickelten ASE (Automated Social Engineering) Bot bei drei verschiedenen schwedischen Universitäten, Permission to Attack Genehmigungen zu bekommen. Die Annahme, dass die Chancen diese Genehmigungen im akademischen Bereich zu bekommen, höher sind als anderwärtig, konnte sich zu der Zeit der Anfragen nicht bestätigen, da keine der kontaktierten Universitäten über einen Ausschuss für Forschungsethik verfügt hat. Die Genehmigungen konnten daher nicht eingeholt werden, das Experiment wurde daraufhin in zwei unterschiedliche ASE-Experimente verändert und abgewandelt durchgeführt. Der ASE-Bot wurde so nur mit einem Facebook-Dummyprofil dazu genutzt, um potenzielle Opfer innerhalb dieser Social-Media-Plattform zu finden und in einer weiteren Phase, diese einem Turing Test [43] zu unterziehen, in welchem die Teilnehmerinnen und Teilnehmer entscheiden mussten, ob sie sich mit einem Computer oder einer realen Person unterhielten.

In [39] wurden von Tobias Lauinger et al. bei dem Experiment mit Honeybot eine Risikoabwägung einerseits hinsichtlich der Testinteressen im Sinne der Forschung in einer möglichst natürlichen Umgebung und andererseits dem Schutz der Testpersonen durchgeführt. Neben den Restrisiken hinsichtlich verlorener Zeit und emotionalen Konsequenzen während den Unterhaltungen, wurden zum Schutz der Testpersonen Mechanismen in Honeybot implementiert, welche die Anonymität der Teilnehmer gewährleistet haben. In dem Paper wird das Unterbinden eines Austausches von persönlichen Nutzerinformationen, sowie auch ein Vorbeugen gegen eventuelle Angriffe von dem Dialogpartner beschrieben. Alle Daten, die während des Experiments gesammelt wurden und den Autoren zufolge weitgehend anonymisiert gehalten wurden, wurden am Ende der Evaluierungsphase gelöscht. Eine Nachbesprechung mit den Testteilnehmern wurde, den Forschungsergebnissen von [82] folgend, in welchen Peter Finn und Markus Jakobsson zu der Erkenntnis gelangt sind, dass ein Nachbesprechen mehr Schaden als Nutzen herbeiführt, nicht durchgeführt.

Der achtwöchige Einsatz des Socialbot Networks [74] wurde von Yazan Boshmaf et al. von der University of British Columbia, nach eigenen Angaben sorgfältig geplant, um ebenfalls Risiken auf der Seite der Nutzer zu reduzieren. Neben der Überzeugung, dass risikominimierte und realistische Experimente die einzige Möglichkeit sind, um Angriffe in der realen Welt abschätzen zu können, gibt es in diesem Experiment auch eine Freigabe der Ethikkommission für Verhaltensforschung von deren Universität. Die teilnehmenden Personen in dem Experiment mussten vorab nicht informiert werden.

Hingegen wurden, zwei Wochen vor Beginn eines anderen Social-Engineering-Experiments mit dem humanoiden Roboter iCub [76], den Teilnehmern verschiedene Fragebögen vorab zugeschickt. Unmittelbar vor dem Experiment im Institut unterzeichneten alle Teilnehmer eine von der örtlichen Ethikkommission genehmigte Einverständniserklärung, in der sie darauf hingewiesen wurden, dass sie mit Kamera und Mikrofon aufgezeichnet werden können und in der sie der Verwendung ihrer Daten für wissenschaftliche Zwecke zustimmten [3]. Die Kameras und Mikrofone wurden den Versuchsteilnehmern allerdings erst am Ende in der Debriefing Phase gezeigt, um während des Experiments möglichst natürliches Befinden und natürliche Interaktionen einzufangen.

Auch Yuki Kano und Tatsuo Nakajima informierten die 35, via Twitter Posts rekrutierten, Teilnehmer ihres Experiments zu Vertrauensfaktoren von Social-Engineering-Angriffen auf soziale Netzwerkdienste [10], vor dessen Beginn über den Ablauf des Experiments und die Daten, die im Zuge dessen erhoben werden sollten. Die jeweiligen Zustimmungen zur Teilnahme wurden anschließend eingeholt.

Zustimmungen haben sich auch John Seymour und Philip Tully eingeholt, während sie auf der DEF CON24 in dem Talk „*Weaponizing Data Science for Social Engineering*“ [83] den Bot SNAP_R, für automatisiertes Spear-Phishing auf der Plattform Twitter vorgestellt haben. Sie gaben dem Publikum die Möglichkeit, freiwillig an einer Demonstration von SNAP_R während der Präsentation teilzunehmen. Dazu wurden die Rahmen- und Teilnahmebedingungen in der Präsentation kurz umrissen, jede Teilnehmerin und jeder Teilnehmer aus dem Publikum konnte einen Tweet mit *#SNAP_R* absetzen, um an der Vorführung des Twitter Social Engineering Bots teilzunehmen. Ob die von SNAP_R ebenfalls in dem Talk präsentierten und zuvor stattgefundenen Test- und Vergleichsläufe mit anderen Begriffen, wie beispielsweise *#cat*, *#pokemongo*, oder *#infosec* ebenfalls angekündigt wurden, wurde nicht erwähnt.

Nicht erwähnt wurde auch in der Case Study „*Passive and Active Reconnaissance*” [84], ob die Teilnehmer von dem durchführenden Team darüber informiert wurden, dass sie unter Verwendung von mehreren Social-Media-

Fakeprofilen nach persönlich indentifizierbaren Informationen (PII) gefragt wurden. Eine Art Debriefing im Nachhinein fand in der Case Study ebenfalls keine Erwähnung.

4.4. Gewählter Umgang mit beiden Aspekten in dieser Arbeit

Der Umgang mit ethischen und rechtlichen Aspekten ist, wie in dem zuvor ausgeführten Abschnitt, in den verschiedenen Papers recht unterschiedlich. Dieser reicht von vorab angefragten Genehmigungen und Fragebögen und bis hin zur einfachen Durchführung von Versuchen. Ein Debriefing mit den Teilnehmerinnen und Teilnehmern der Versuche wird selten abgehalten. Mit Bedacht auf diese Umgänge wurde auch der Umgang mit beiden Aspekten in der vorliegenden Arbeit entwickelt. Personen unwissentlich zu Versuchspersonen in einem Experiment zu machen, wirft natürlich erste ethische Bedenken auf, wie auch bereits in [4] bemerkt wurde. Daher wurden für erste Tests mit den Tools nach eigenen, veralteten und bereits bekannten, geleakten Daten gesucht. Für die weitere Anwendung von den in den Recherchen zusammengestellten automatisierten Tools, die online frei verfügbare Informationen abrufen, wurde in erster Linie versucht an eigene (persönliche) Informationen, über die in dem vorab informierten Bekanntenkreis, über die der FH St. Pölten, des Familienbetriebs und an Informationen über ein ebenfalls vorab informiertes, international tätiges Großunternehmen, zu kommen.
Insofern die getesteten Tools in der Lage waren personenbezogene Daten aufzufinden, wurden diese, rein zu Dokumentationszwecken in der Arbeit eingefügten Screenshots, entsprechend stark anonymisiert, sodass daraus keine Rückschlüsse gezogen werden können und auch keine Personen, beziehungsweise Institutionen, erkennbar sind, da die Verfügbarkeit und Einsicht der vorliegenden Arbeit nicht durchgängig kontrolliert oder eingeschränkt werden kann. Bei der Verarbeitung der aufgefundenen Daten und Informationen wurde trotz Automatisierung versucht, so weit als möglich auf das Prinzip der Datenminimierung und Zweckbindung Rücksicht zu nehmen. Auf entstehbare und möglicherweise nachteilige Kombinationen der Ergebnisse wurde geachtet. Die Erkenntnisse und Ergebnisse bei der Verwendung der Tools werden im Verlauf des Kapitel 6, Toolunterstütze Automation in, so weit als möglich anonymisierter Form, beschrieben. Die Such- und Versuchsergebnisse wurden nach der Anwendung nicht gespeichert. Vereinzelt wurden von den Tools automatische Protokolldateien angelegt, welche die Ergebnisse aus den Suchabfragen beinhalten haben. Diese Protokolldateien wurden am Ende des Versuchs ebenfalls gelöscht. Die gelisteten Social-Engineering-Werkzeuge wurden alle gesamt in mehreren virtuellen Maschinen auf einem mittels Bitlocker verschlüsseltem System installiert, welche ebenfalls nach Fertigstellung der vorliegenden Arbeit, gelöscht wurden.
Möglicherweise schädliche und aus rechtlicher Sicht bedenkliche Angriffe via DDoS (Distributed Denial of Service), Bruteforce, Netzwerkscans und dergleichen wurden weder angedacht noch durchgeführt und somit auch nicht durchgetestet. Die entsprechenden Funktionalitäten in den Werkzeugen wurden soweit vorhanden, immer übersprungen.
Der Fokus der vorliegenden Arbeit liegt primär darauf, die Werkzeuge, die mit Automation im Social-Engineering-Umfeld unterstützen können, deren Schwierigkeiten bei der Verwendung und auch die Zuverlässigkeit der Ergebnisse, aufzuzeigen und nicht direkt deren Ergebnisse. Die Listung und Beschreibung der Werkzeuge ist für wissenschaftliche und bewusstseinsbildende Zwecke gedacht und soll in keinster Weise kriminelle Energien und Aktivitäten mit böswilligem Hintergrund unterstützen.

5. Social-Engineering-Phasenmodelle und Frameworks

Eine standardisierte Formulierung eines Social-Engineering-Angriffs, sowie der Ablauf und die zeitlichen Ereignisse, ermöglichen es Forschern verschiedene Social-Engineering-Angriffe miteinander zu vergleichen [85]. Eine wirklich durchgängig standardisierte Formulierung, beziehungsweise eine Art einheitliches Framework für Abläufe von Social-Engineering-Angriffen, lässt sich allerdings nur schwer finden und auch nur näherungsweise umsetzen. Social Engineering ist so dynamisch, dass es annähernd unmöglich ist, jede Phase zu planen [25]. Im nachfolgenden Teil dieses Kapitels werden die gängigsten Phasenmodelle und Frameworks thematisiert und verglichen, mit denen es näherungsweise möglich ist, Social-Engineering-Angriffe in Phasen zu unterteilen. Die gelisteten Frameworks wurden während der Literaturrecherche analysiert und zusammengestellt, einige davon wurden auch in den beschriebenen Papers auf publik gewordene Social-Engineering-Angriffe angewandt. Die Listung der Frameworks entspricht dabei grundsätzlich keiner Reihung und keiner Wertung. Der Beginn erfolgt mit der klassischen Cyber Kill Chain, die bereits aus der Anwendung und Klassifizierung anderer Angriffe der Cyberwelt bekannt ist, führt über bereits länger etablierte Modelle von Kevin Mitnick und Christopher Hadnagy, bis hin zu neueren und individuelleren Ansätzen.

5.1. Cyber Kill Chain nach Lockheed

Aus dem militärischen Bereich, mit ursprünglich definierten Maßnahmen zur Erkennung und Abwehr von Angriffen kommend, wurde von Lockheed Martin die Cyber Kill Chain [86] entwickelt. Ziel war es, die Handlungsmaßnahmen aus dem militärischen Bereich auch in dem digitalen Bereich zu etablieren. Seit der Überführung dieser im Jahr 2011, ist diese unter „Cyber Kill Chain“, oder „Intrusion Kill Chain“ bekannt [87]. Die in Abbildung 4 dargestellte Grafik der Cyber Kill Chain wurde bereits mehrmals adaptiert, so beispielsweise von IBM Security in [88]. Bei Internetrecherchen ist diese auch in Kreisdiagrammen [89] und mit zusätzlichen Ergänzungen zu den einzelnen Phasen dargestellt [88], aufzufinden. Die Phasen und deren Beschreibungen sind dabei allerdings zumeist die gleichen. Kritikern zufolge ist die Lockheed Martin Cyber Kill Chain zu sehr auf Malware Angriffe ausgelegt.
Die einzelnen Phasen der Cyber Kill Chain werden aus der Täterperspektive wie folgt definiert:

- **Phase 1: Reconnaissance**

  In der Reconnaissance-Phase werden Angriffsziele (Personen, Institutionen, oder bestimmte Personen in Institutionen) ausgewählt und so viele Informationen wie möglich über diese eingeholt. Jede noch so kleine und als unwichtig erscheinende Information kann für den weiteren Verlauf von Bedeutung sein.

- **Phase 2: Weaponization**

  In dieser Phase wird ein Angriff, basierend auf den zuvor eingeholten Informationen, vorbereit. Es werden zum einen ein zu dem Angriffsziel passender Pretext entworfen und zum anderen dazu nutzbare Tools zusammengestellt.

- **Phase 3: Delivery**

  In der Phase Delivery wird die Durchführung eines Angriffs begonnen. Es werden dafür bereits vorbereitete Phishing-Nachrichten an ausgewählte Ziele versandt, präparierte Datenträger deponiert, oder aber auch Water-Holing Seiten aktiv geschalten.

- **Phase 4: Exploitation**

  In der Exploitation Phase werden Sicherheitslücken und Schwachstellen des Angriffsziels ausgenutzt. Hier finden auch Vishing-Anrufe statt, die das Angriffsziel zur Mitwirkung und Mithilfe bewegen können.

- **Phase 5: Installation**

  In dieser Phase wird unbemerkt Schadsoftware auf den Geräten der Angriffsziele installiert. Dies kann durch die zuvor präparierten Datenträger, oder aber auch über eine der aktivierten Water-Holing-Seiten passieren.

- **Phase 6: Command and Control**

  In dieser Phase der Cyber Kill Chain werden die zuvor installierten Schadprogramme genutzt um an Daten, weitere persönliche Informationen, oder Zugangsdaten zu gelangen.

- **Phase 7: Actions on Objectives**

  In der letzten Phase der Cyber Kill Chain werden die Angriffe konkretisiert, Systeme kompromittiert und erlangte Daten und Zugangsdaten ausgenutzt, um den Angriff zu vollenden.

Abbildung 4: Lockheed Cyber Kill Chain [86]

5.2. Social Engineering Cycle nach Mitnick und Simon

Kevin Mitnick beschreibt in „*The Art of Deception*“ [1], von Kapitel 2 bis Kapitel 14 anhand praxisnaher Beispiele, wie Social-Engineering-Angriffe aus seiner Sicht und Erfahrung ablaufen können und wie Social Engineers dabei agieren. Er veranschaulicht, wie scheinbar harmlose Informationen zusammengetragen und einfach erfragt werden können. Er geht darauf ein, wie Beziehungen zu Social-Engineering-Zielen aufgebaut werden und diese, sowie auch recherchierte Informationen, ausgenutzt und genutzt werden, wer für Angriffe am ehesten anfällig ist und wie mit geschicktem Einsatz von Sympathie, Schuld und Einschüchterung Opfer zu Handlungen bewegt werden, die ganz im Interesse von Social Engineers stehen.
Dies fasst er am Ende als einen vierphasigen Kreislauf, bestehend aus den folgenden Elementen, zusammen:

Abbildung 5: Mitnick Social Engineering Cycle [1]

Der Einstieg in das Framework erfolgt mit der Phase **Recherche**, in welcher Informationen eingeholt und Nachforschungen über das jeweilige Angriffsziel angestellt werden. Dies kann über alle möglichen Kanäle erfolgen (beispielsweise öffentliche Quellen, Jahresberichte, Marketingunterlagen, Zeitungsartikel, Websites, Inhalte aus sozialen Medien). Mit detaillierteren Informationen und Insider-Informationen, werden Identitäten angenommen und auf, dem Opfer bekannte, Personen verwiesen. Es werden damit in der nächsten Phase **Beziehungen und Vertrauen entwickelt**, die in der darauffolgenden Phase ausgenutzt werden. In der Phase **Ausnutzung des Vertrauens** wird das Opfer um Gefallen und Handlungen gebeten. Es kommt hier auch zu einer Sonderform des „Reverse Sting“, in der das Opfer die angreifende Seite um Hilfe bittet. In der letzten Phase werden die zusammengetragenen **Informationen genutzt**. Stellt es sich in dieser Phase heraus, dass noch etwas zum endgültigen Erreichen des Ziels fehlt, kann noch einmal in eine frühere Phase des Kreislaufs zurückgekehrt werden. Dies erfolgt so lange, bis die angreifende Seite ihr Ziel erreicht hat.

5.3. Social Engineering Lifecycle nach Imperva

Bei der Recherche nach Social-Engineering-Lifecycles oder Phasenmodellen findet sich in den Suchergebnissen oftmals auch der Social-Engineering-Lifecycle des international tätigen IT-Sicherheitsunternehmens Imperva (siehe dazu nachfolgend Abbildung 6) [90].
Imperva verwendet, um den Lebenszyklus von Social-Engineering-Angriffen darzustellen, ähnlich dem Modell von Kevin Mitnick, ebenfalls ein 4-Phasen-Modell, allerdings mit unterschiedlichen Phasen und Bezeichnungen:

- **Phase 1: Investigation**
  In der Investigation-Phase werden die Grundlagen für einen Angriff vorbereitet. Es werden die Angriffsopfer ausgewählt, Hintergrundinformationen über diese gesammelt und geeignete Angriffsmethoden ausgewählt.

- **Phase 2: Hook**
  In der Hook-Phase geht es darum, die Angriffsopfer zu täuschen und bei diesen Fuß zu fassen. Mit den Zielpersonen wird in Kontakt getreten, diese mit einer erfundenen Geschichte getäuscht und Kontrolle über Interaktionen übernommen.

- **Phase 3: Play**
  Die Play-Phase des Lifecycles dreht sich um Informationen, die über einen gewissen Zeitraum abgerufen werden. Die Einnistung aus der vorhergehenden Phase wird vertieft, Angriffe ausgeführt, Geschäftsabläufe gestört und/oder Daten abgeschöpft.

- **Phase 4: Exit**
  In der Exit-Phase wird der Angriff abgeschlossen, idealerweise ohne Verdacht zu erregen. Hierzu werden jegliche Spuren verwischt, Malware wieder entfernt und der Vorwand, die Geschichte, die in der Hook-Phase erfunden wurde, zu einem natürlichen Ende gebracht.

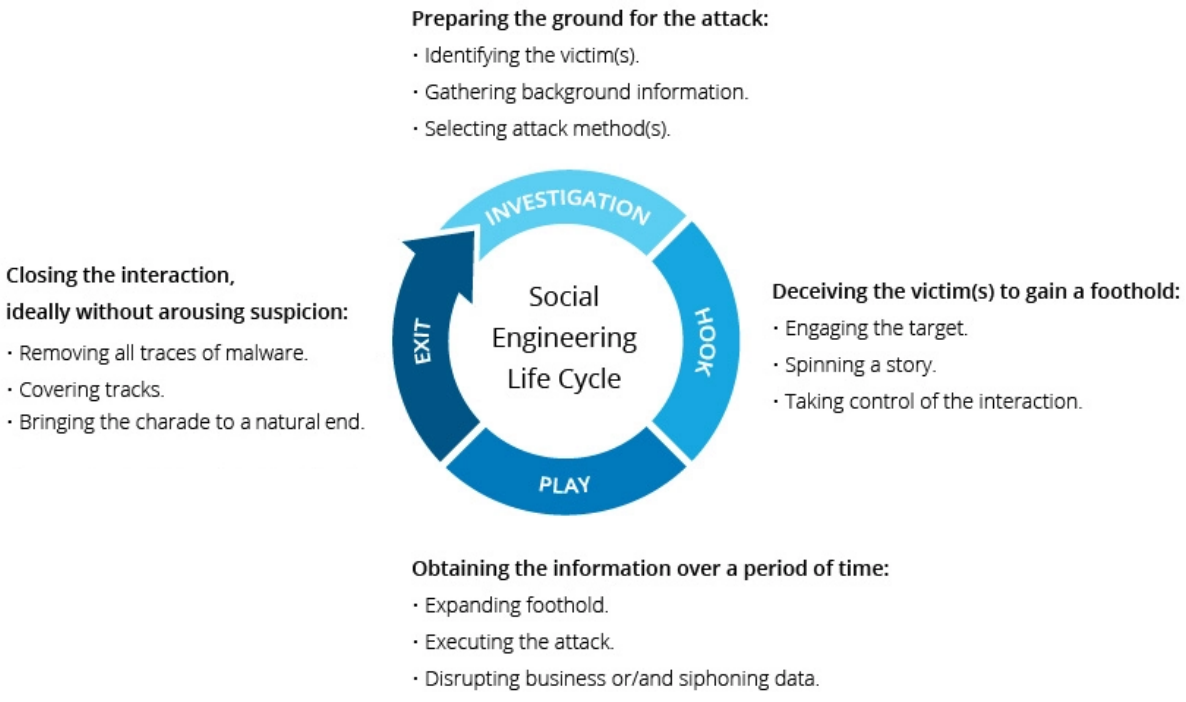


Abbildung 6: Imperva Social Engineering Lifecycle [90]

5.4. Social Engineering Pyramide nach Hadnagy

Christopher Hadagny definiert in [25] die Stufen des Social Engineerings in Form einer Social-Engineering-Pyramide (siehe Abbildung 7). Er führt als erste und wichtigste Stufe die Stufe der **Informationsbeschaffung** an, da diese seiner Meinung nach, die wichtigste Stufe darstellt, immer an erster Stelle steht und erst im Anschluss daran ein Angriff richtig geplant werden kann. Im Anschluss an die Stufe der Informationsbeschaffung ist aus dieser bereits abschätzbar, welche Szenarien und Pretexts funktionieren können, daher folgt als nächste Stufe die **Entwicklung von Vorwänden** beziehungsweise Pretexts. Im Anschluss daran wird, als nächste Stufe, basierend auf den gewonnenen Informationen und den entwickelten Vorwänden, ein konkreter **Angriff geplant** und dieser in der darauffolgenden Stufe **ausgeführt**.
Christopher Hadnagy erwähnt in [25] mehrmals, dass Social Engineering nicht genau geplant werden kann und Spielraum für Flexibilität miteingerechnet werden sollte. Ein Zurückkehren in vorherige Stufen, beispielsweise zurück in die Informationsbeschaffung, während einer bereits begonnenen Angriffsplanung, ist in seinem Framework, laut eigenen Hinweisen, durchaus möglich.

Abbildung 7: Hadnagy Social Engineering Pyramide [25]

Die Pyramide endet mit der Stufe **Reporting**. Aufgrund dessen, dass Christopher Hadnagy die Social-Engineering-Pyramide für Penetration Tests in Kundenaufträgen verwendet, ist für eine Nachvollziehbarkeit von Social-Engineering-Arbeiten auch ein entsprechendes Reporting von großer Wichtigkeit.

5.5. Social Engineering Attack Framework nach Mouton et al.

Das in Abbildung 8 dargestellte „*Social Engineering Attack Framework*" von Mouton et al. [85] basiert auf dem Attack Cycle von Kevin Mitnick und ist, den Autoren zufolge, eine Erweiterung dessen, um Unzulänglichkeiten aus dem Attack Cycle schrittweise genauer zu beleuchten.
Was auf den ersten Blick bei diesem Framework auffällt ist, neben ähnlichen und feineren Begrifflichkeiten der Phasen innerhalb des Frameworks, die am Schluss angesiedelte Debriefing-Phase, in der die Zielpersonen wieder in einen normalen emotionalen Zustand versetzt werden sollen (Maintenance-Prozess). Die Idee, die hierbei verfolgt wird, ist den Zielpersonen ein gutes Gefühl zu vermitteln, sodass diese sich nicht fühlen, als wären sie angegriffen worden, um dadurch Schuldgefühlen von (unbefugten) Weitergaben von Informationen entgegenzuwirken und somit unvorhergesehene Folgen zu vermeiden. In dem Transition-Prozess innerhalb der letzten Phase wird entschieden, ob das Angriffsziel erreicht wurde, oder ob nochmals in ein früheres Stadion zurückgekehrt werden muss (beispielsweise um mehr Informationen zu beschaffen).

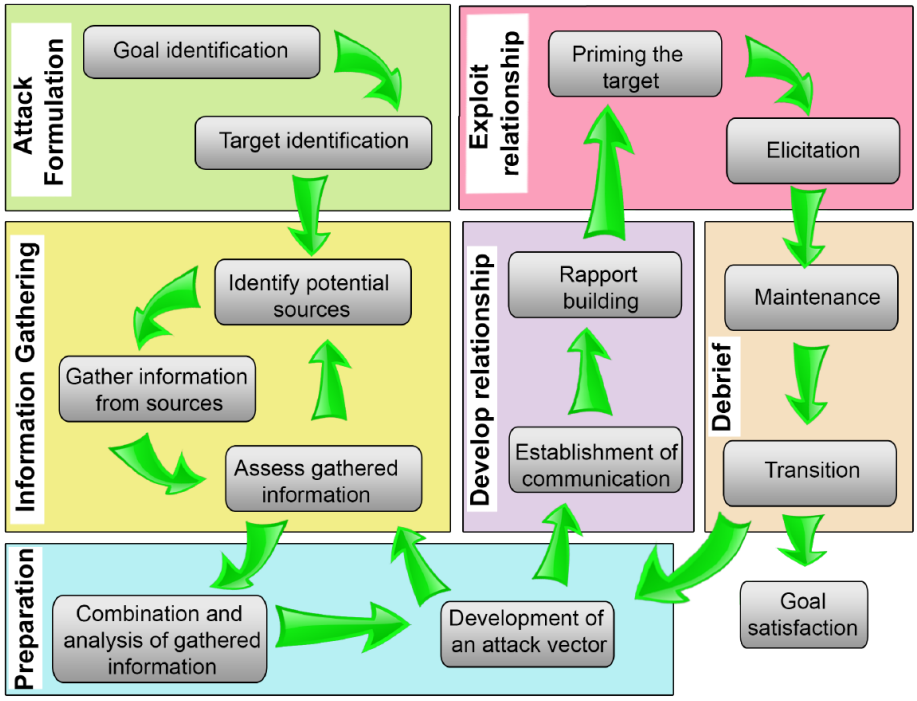


Abbildung 8: Mouton et al. Social Engineering Attack Framework [85]

Das Social Engineering Attack Framework besteht generell, verglichen mit dem Social Engineering Cycle nach Mitnick und Simon, aus mehreren Phasen mehr und ist gerade am Beginn detaillierter gehalten, da am Anfang das Ziel des Angriffs noch nicht eindeutig festgesetzt werden kann, beziehungsweise auch noch nicht definiert ist, welche Zielpersonen eventuell dabei behilflich sein könnten, um das gewünschte Ziel zu erreichen. Daher wurde hier von Mouton et al. eine zusätzliche Phase „**Attack Formulation**" eingeführt. Weiters ist die Phase **„Information Gathering"** um die Bewertung von gesammelten Informationen detaillierter, da diese für den weiteren Verlauf des Angriffs von großer Wichtigkeit sind und die nachfolgend aufzubauenden Vertrauensverhältnisse erheblich von der Qualität der lukrierten Informationen aus dieser Phase abhängig sind. Eine weitere wichtige und zusätzliche Phase **„Preparation"**, in welcher Daten aufbereitet und Angriffsvektoren auserkoren werden, findet sich vor der Phase **„Develop Relationship"**, welche sehr ähnlich gehalten ist, sich aber in dem Einstiegspunkt unterscheidet. Auch die Phase **„Exploitation Relationship"** wurde in diesem Framework detaillierter ausgeführt. Abschließend findet sich die zusätzliche und bereits eingangs erwähnte Debriefing Phase.

5.6. Cycle of Deception nach Nohlberg und Kowalski

Der „*Cycle of Deception*“ [91] ist ein Social-Engineering-Framework, das nicht nur die Phasen aus der Sicht der Angreifer beinhaltet, sondern auch die aus Sicht der Angriffsopfer und deren Verteidiger. Das Modell wurde entwickelt, da die bis zu diesem Zeitpunkt vorhandenen Frameworks als zu einfach und gleichzeitig zu undurchsichtig empfunden wurden. Es soll, den Autoren nach, unter anderem als Hilfe für Schulungszwecke, aber auch als Modell für eine ganzheitliche Schutzstrategie gegenüber Social Engineering dienen.

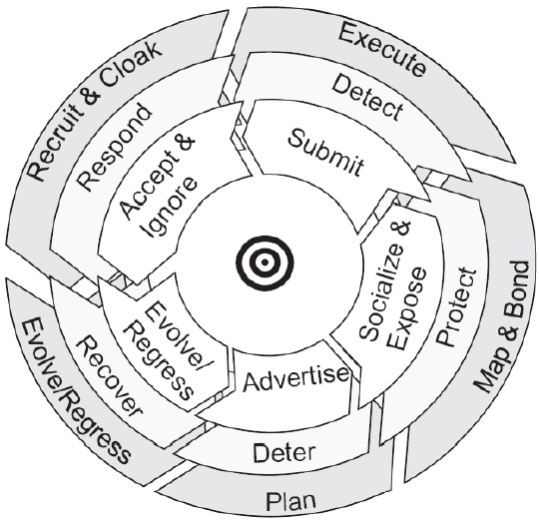


Abbildung 9: Cycle of Deception [91]

Der in Abbildung 9 dargestellte Cycle of Deception besteht aus der Zusammenführung des Angriffsziels in der Mitte, sowie dreier einzelner Kreisläufe, die nachfolgend, inklusive kurzer Phasenbeschreibung, dargestellt werden. Der **Attack Cycle**, der in dem Cycle of Deception ganz außen ersichtlich ist, widmet sich mit seinen beinhaltenen Phasen dem Verhalten und den Aktionen der Angreifenden.

Abbildung 10: Attack Cycle [91]

- **Phase 1: Goal & Plan**
  Beinhaltet Ziel, Zweck und Begründung des Angriffs.
- **Phase 2: Map & Bond**
  Unter Verwendung verschiedener Suchtechniken suchen sich Angreifer Informationen über die Angriffsziele zusammen.
- **Phase 3: Execute**
  Die Angreifer vollziehen eine nicht erlaubte, oder strafbare Handlung.
- **Phase 4: Recruit & Cloak**
  Bezeichnet alle Aktivitäten um Spuren nach einem erfolgten Angriff zu verschleiern.
- **Phase 5: Evolve/Regress**
  Die Angreifer lernen von dem Prozess und schafft eine interne Rechtfertigung für das was passiert ist.

In Richtung der Mitte, dem Angriffsziel, befindet sich als nächstes der **Defense Cycle**, welcher sich phasenweise den Optionen, die den Verteidigenden zur Verfügung stehen, widmet. Die Rolle der Verteidigenden können in manchen Fällen entweder von den Opfern selbst, oder von IT-Professionisten, eingenommen werden.

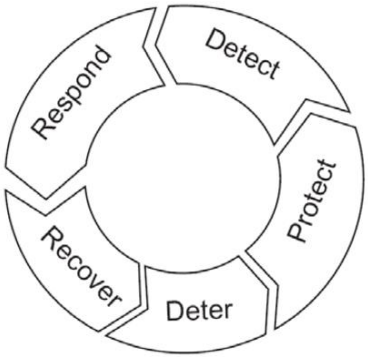


Abbildung 11: Defense Cycle [91]

- **Phase 1: Deter**
  Abschreckende Wirkung durch entsprechende Vorgaben und Wahrnehmungen über gute Meldelinien bei Vorfällen.
- **Phase 2: Protect**
  Wenige sensible Daten zur Verfügung stellen, Schulungsmaßnahmen für Mitarbeitende und eine entsprechende Policy schützen in dieser Phase.
- **Phase 3: Detect**
  Phase 3 beschreibt die Angriffserkennung durch aufmerksame Mitarbeitende oder durch technische Einrichtungen.
- **Phase 4: Respond**
  Schaffen von Möglichkeiten zur einfachen Meldung von Social-Engineering-Angriffen oder Versuchen von diesen.
- **Phase 5: Recover**
  Die Phase Recover beinhaltet das Wissen um den Wert der eigenen Daten, gute vorhandene Policies und gut dokumentierte, gemeldete Angriffe, um daraus zu lernen.

Der **Victim Cycle** wurde direkt um das Angriffsziel gelegt und fokussiert sich auf das Verhalten der individuellen Opfer, welchen den Autoren zufolge beim Analysieren von Angriffen zu wenig Aufmerksamkeit geschenkt wird.

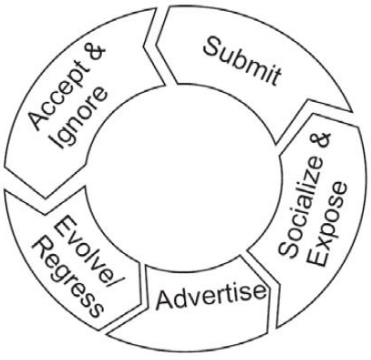


Abbildung 12: Victim Cycle [91]

- **Phase 1: Advertise**
  Das Opfer besitzt (wissentlich oder unwissentlich) etwas an Wert, das es zum Ziel macht.
- **Phase 2: Socialize & Expose**
  Durch Interaktion mit den Angreifern lässt sich das Opfer täuschen und gibt seine Wertgegenstände, beziehungsweise Zugang zu diesen, preis.
- **Phase 3: Submit**
  In dieser Phase erfolgt die Herausgabe von beispielsweise geheimen Informationen.
- **Phase 4: Accept & Ignore**
  Bezeichnet das Verhalten des Opfers nach stattgefundem Angriff, indem dieser akzeptiert, ignoriert, oder gar nicht bemerkt wurde.
- **Phase 5: Evolve/Regress**
  Beschreibt die Entwicklung des Angriffsziels in die Rolle des daraus Lernenden, oder in die Rolle des Opfers.

5.7. Social Engineering Attack Spiral nach Cullen und Armitage

Andrea Cullen und Lorna Armitage entwickeln mit der „*Social Engineering Attack Spiral*“ (SEAS) [92] ein Modell direkt anhand einer Serie von zwei beschriebenen Angriffsszenarien, das auf zuvor bereits vorhandene Frameworks verwandter Arbeiten, beispielsweise dem Social Engineering Cycle von Mitnick und Simon, oder dem Cycle of Deception von Nohlberg und Kowalski, aufsetzt. Das Modell soll ein besseres Verständnis für den Angriffsprozess des Social Engineerings schaffen und sowohl auf simple und gezielte, als auch auf hoch komplexe Angriffe, angewandt werden können.

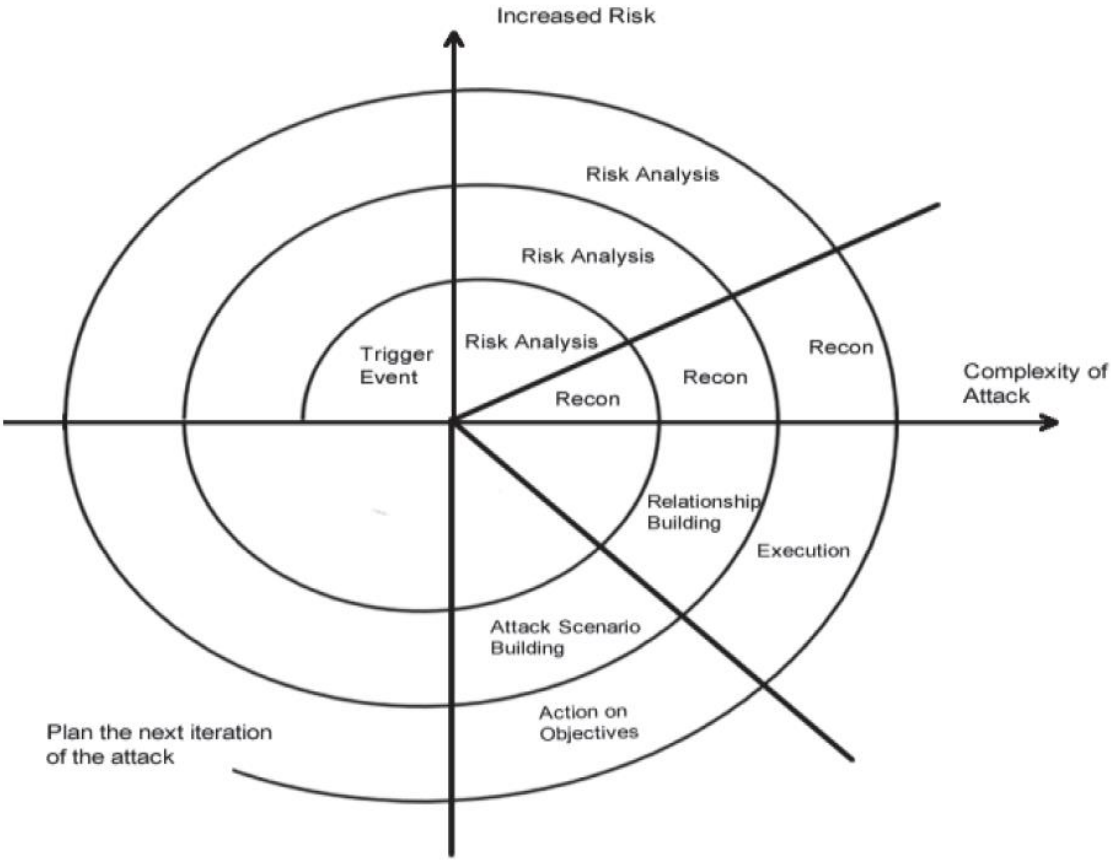


Abbildung 13: Social Engineering Attack Spiral [92]

Jeder Social-Engineering-Angriff, beziehungsweise damit Durchlauf der SEAS (siehe Abbildung 13), hat einen bestimmten **Auslöser (Trigger Event)**, nach diesem eine erste **Risikoanalyse (Risk analysis)** und **Reconnaissance (Recon)** durchgeführt wird. Die Risikoanalyse- und Reconnaissance-Phasen finden sich in diesem Modell durchgängig, wobei die Risiken und die Komplexität im Angriffsverlauf mit jeder Runde zunehmen.
Im weiteren Verlauf der SEAS wird geplant, wie zu den Angriffsopfern **Beziehungen aufgebaut (Relationship Building)** werden können und erste **Angriffsszenarien entwickelt (Attack Scenario Building)**, welche in den weiteren Phasen **Execution** und **Action on Objectives**, aktiv angewandt werden.
Cullen und Armitage sehen in dem Modell vor, dass die Angreifenden bei jeder Iteration der SEAS die nächste Phase bereits planen und dass Interaktionen zwischen Angreifern und Opfern während des gesamten Verlaufs stattfinden können.

5.8. Session und Dialog basierendes Framework nach Wu et al.

Die Gruppe Kangfang Zheng, Tong Wu, Xiujuan Wang, Bin Wu und Chunhua Wu bemerkt, dass fast alle phasenbasierten Social-Engineering-Modelle als Kreislauf dargestellt werden und ist der Meinung, dass die zirkuläre Form, auf Kosten einiger Details, den sich wiederholenden Prozess des Social-Engineering-Angriffs, um sein Endziel zu erreichen, zeigt. Sie schlägt daher in ihrer Arbeit „*A Session and Dialogue-Based Social Engineering Framework*“ [93] ein alternatives Framework vor, das Social-Engineering-Angriffsphasen als „**Social-Engineering-Sessions**“ (SES) vorsieht. Mehrere gut organisierte SESs werden in dem Modell dann zu einem sogenannten „**Social-Engineering-Dialog**“ (SED) zusammengeführt. Abbildung 14 visualisiert die schematische Darstellung einer SES, Abbildung 15 die eines SED:

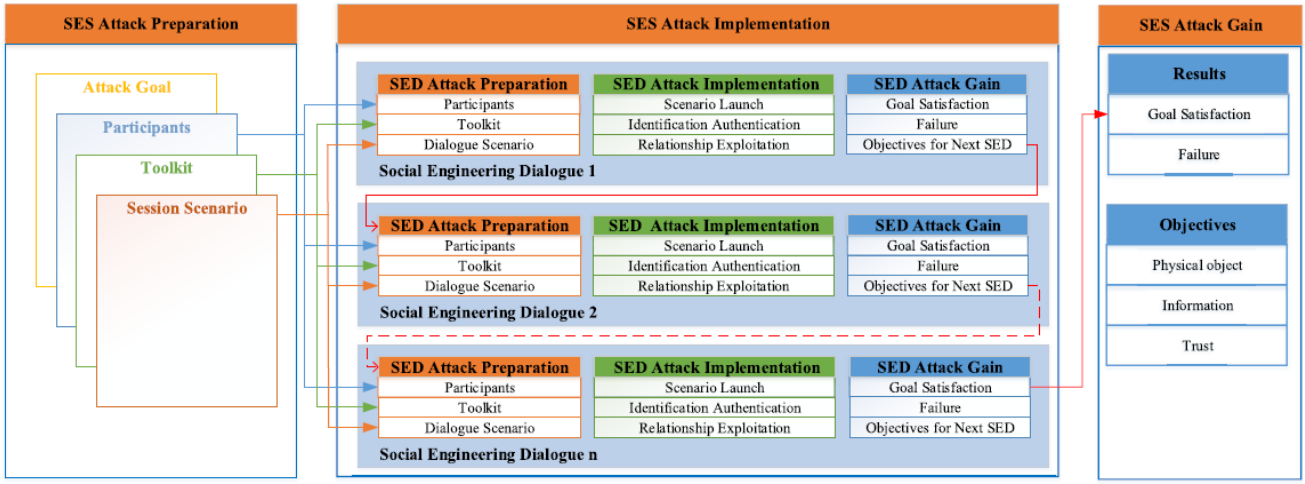


Abbildung 14: Social Engineering Session [5]

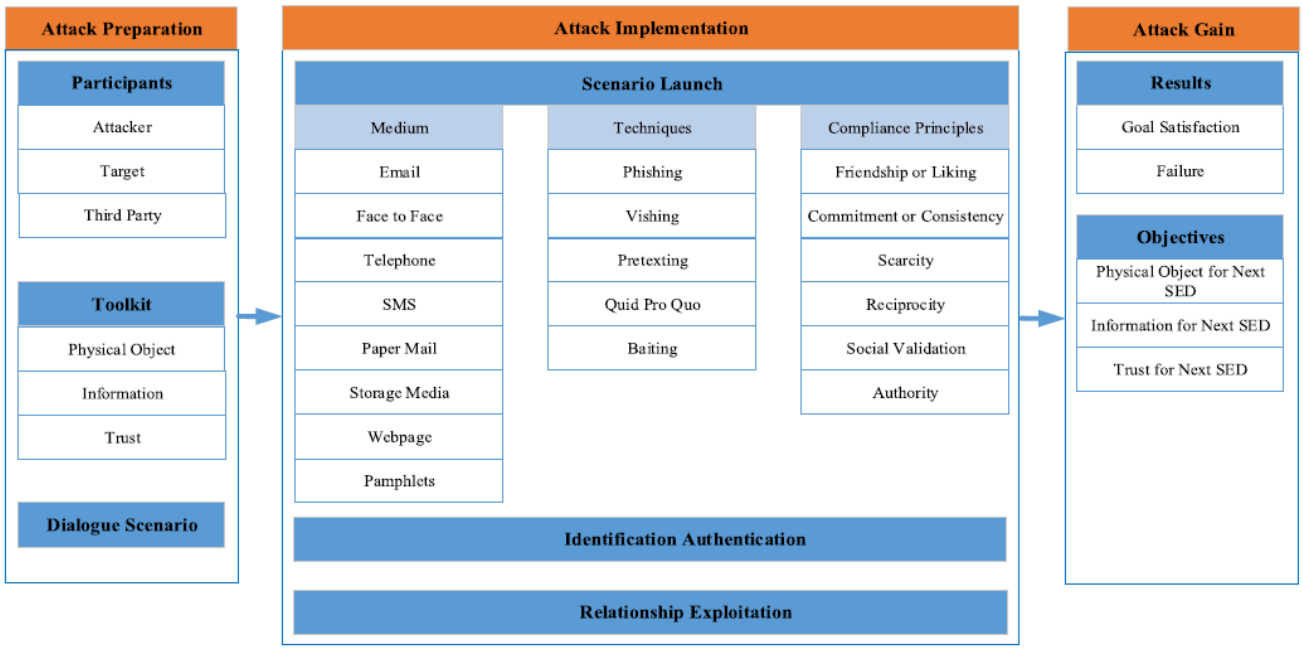


Abbildung 15: Social Engineering Dialog [5]

Per Definition ist ein SED ein atomarer Teil in einem gesamten Social-Engineering-Angriff, der eine einzelne Verbindung zwischen den Angreifenden und dem Ziel darstellt. Die Kombination von mehreren SEDs ergibt am Ende einen kompletten Angriffsprozess. Jeder SED ist ein für sich eigenes und integriertes System, welcher jeweils die Angriffsvorbereitung (**Attack Preparation**), die Angriffsdurchführung (**Attack Implementation**) und das Angriffsziel (**Attack Gain**), umfasst. Am Beginn eines jeden solchen SEDs, in der Vorbereitungsphase, werden die Teilnehmenden, die benötigten Werkzeuge, sowie die Dialog-Szenarien für den nächsten Schritt festgelegt. In der Angriffsdurchführungsphase werden die Angriffe, entsprechend den entwickelten Angriffsszenarien und unter Verwendung von verschiedenen Medien, Techniken und Prinzipien (siehe Abbildung 15, Clustering Scenario Launch), durchgeführt. Das Aufbauen und Ausnutzen von Beziehungen findet ebenfalls in dieser Phase statt (siehe Abbildung 15, Identification Authentication und Relationship Exploitation). Per Definition besteht ein SES ebenfalls aus den drei Phasen Attack Preparation, Attack Implementation und Attack Gain und stellt einen schrittweisen Prozess des Ausnutzens von Vertrauen, zum Erreichen der Angriffsziele, dar. Innerhalb der SES ist die richtige Abfolge der einzelnen SEDs von großer Wichtigkeit, ebenso wie die Bewertung der Ergebnisse am Ende. Letzteres entscheidet über die Erreichung der Ziele, oder die Abfolge des nächsten SEDs.

5.9. Phasen- und Quellmodelle nach Algarni und Xu

Im Gegensatz zu den anderen, vorhergehenden Frameworks präsentieren Abdullah Algarni und Yue Xue in ihrem Paper „*Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models*“ [94] ein phasenbasierendes Modell und als Ergänzung dazu ein ursprungsorientiertes Modell. Die Anwendungen beider Modelle beziehen sich primär auf soziale Netzwerkdienste. Die SNSs weisen, den Autoren zufolge, im Vergleich zu Social Engineering im „realen Leben“, andere spezifische und einzigartige Charakteristiken auf.
Das in Abbildung 16 dargestellte phasenbasierte Modell zeigt die auf acht Phasen zusammengefassten Schritte, die Social Engineers in SNSs bis zum Angriff durchlaufen, um ihre Opfer auszutricksen:

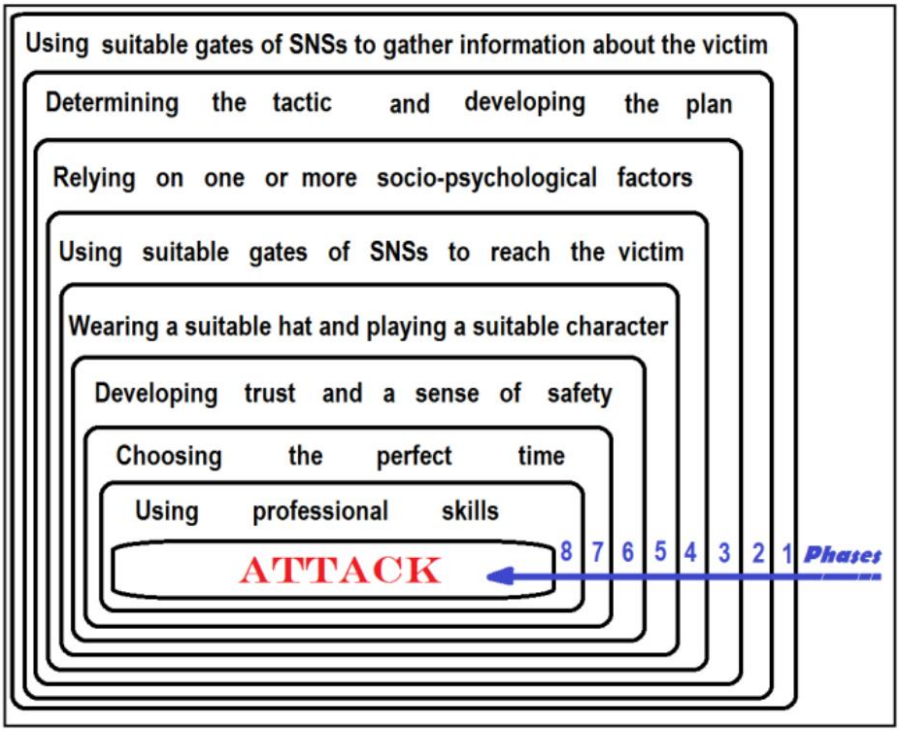


Abbildung 16: Phase-Based Model [94]

- ***Phase 1: Using suitable gates of SNSs to gather information about the victim.***

  Einholen von Informationen über die Opfer und verstehen von deren Schwächen, oder Informationen die zur weiteren Recherche verwendet werden.

- **Phase 2: Determining the tactic and developing the plan**

  Auswählen der als am passendsten und erfolgreichsten angesehenen Taktiken und Entwicklung von Plänen, um die Opfer zu täuschen.

- **Phase 3: Relying on one or more socio-psychological factors**

  Einsatz von sozio-psychologischen Faktoren, die das Verhalten von Menschen beeinflussen (beispielsweise Faktoren nach Robert Cialdini [15]).

- ***Phase 4: Using suitable gates of SNSs to reach the victim***

  Mit den Opfern in Kontakt treten durch die, beispielsweise bereits häufig integrierten Messaging-Funktionen innerhalb der SNSs.

- **Phase 5: Wearing a suitable hat and playing a suitable character**

  Eine passende und überzeugende Figur in einem vorbereiteten Pretext, basierend auf den gesammelten Informationen, den ausgewählten Taktiken und sozio-psychologischen Faktoren.

- **Phase 6: Developing trust and a sense of safety**

  Aufbauen von Beziehungen, Vertrauen und einem Gefühl der Sicherheit zwischen den Angreifenden und den Opfern.

- **Phase 7: Choosing the perfect time**

  Den bestmöglichen Zeitpunkt für einen Angriff auswählen durch Beobachten von Aktivitäten der Opfer (beispielsweise Postings, Statusmeldungen und Kommentare)

- **Phase 8: Using professional skills**

  Entscheidet über den Erfolg der vorhergehenden Phasen. Es wird ein gutes, zuvor entwickeltes Szenario durchgeführt und mit dem Opfer interagiert.

Innerhalb von Phase 1 und Phase 4 gibt es verschiedene Arten von Einfallstoren (**gates**), um Informationen über Opfer zu erhalten, oder diese zu erreichen. Aufgrund dessen wurde als weiteres Modell zur Unterscheidung der Herkunft, beziehungsweise des Ursprungs von Social-Engineering-Angriffen, ein Ergänzungsmodell erschaffen, welches in der nachfolgenden Abbildung 17 dargestellt ist. In diesem Ergänzungsmodell, dem Source-Based Model, werden die drei hauptsächlichen Ursprünge, aus denen die Bedrohungen für SNSs ausgehen, in Form eines Venn-Diagramms miteinander geschnitten.

- **Privacy Setting**

  Falsch konfigurierte Privatsphäreneinstellungen auf Social-Media-Seiten mit detaillierten, privaten Angaben, machen es Angreifenden leicht, an private Inhalte zu kommen (beispielsweise komplett öffentlich einsehbare Profile, oder nur leicht eingeschränkte Berechtigungen, beispielsweise beschränkt auf nur die Freunde von Freunden). Dies bedroht nicht nur die jeweiligen Nutzenden selbst, sondern auch deren Freunde, oder auch deren betriebliches Umfeld.

- **Friendship & Connection with strangers**

  Das Annehmen von unbekannten Freundschafts- und Verbindungsanfragen, aus verschiedenen psychologischen Motiven heraus, wird in dem Diagramm ebenfalls als eine Haupteinfallsquelle für Social Engineering gesehen, da die Personensuche und Kontaktaufnahme in den SNSs sehr einfach möglich ist. Aufgrund dessen, dass die SNSs bei der Erstellung von Profilen freie Hand bei Vergabe von Namen, Fotos, Alter, Schulangaben

und diversen anderen persönlichen Informationen lassen, ist es für die Social Engineers sehr leicht, eine beliebige Identität nachzuahmen, um sich das Vertrauen der Opfer zu erschleichen.

Durch das Feature, dass SNSs, basierend auf Gemeinsamkeiten (gemeinsame Freunde, Schulen, oder Gruppen) Personen als Freundschaftsvorschläge anzeigen, kann es auch zu einer sogenannten „Reverse Attack" kommen, in der das jeweilige Opfer selbst dazu verleitet wird, mit den Social Engineers, die zuvor Freunde der Zielperson mit angenommenen Freundschaftsanfragen kontaktiert haben, in Kontakt zu treten [95].

- **Insecure Dealing with Content**

  Inhalte auf SNSs können bösartige Software, Viren und Würmer enthalten, die beispielsweise durch Hyperlinks in Nachrichten eingebettet werden, oder Hyperlinks enthalten, die zu Seiten mit direkt ausführbaren Dateien führen, die durch die dazu verleiteten Opfer heruntergeladen werden [96]. Phishing- und Spam-Nachrichten zählen ebenfalls zu dieser Kategorie.

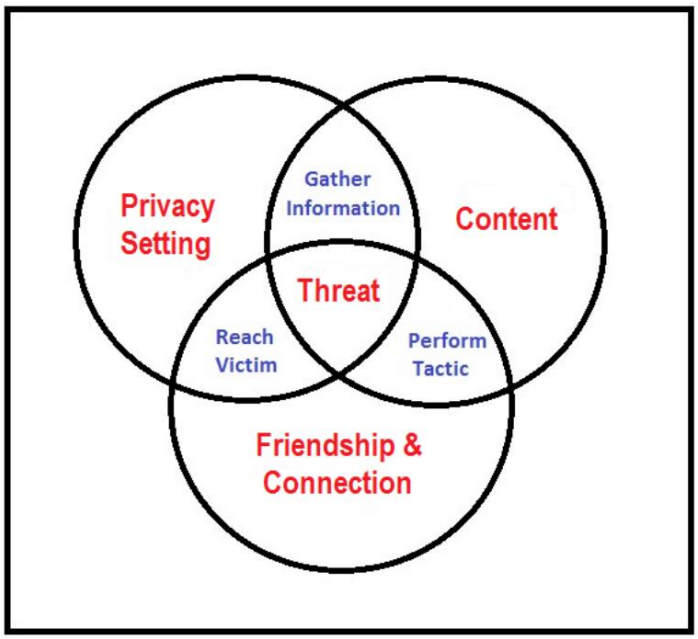


Abbildung 17: Source-Based Model [94]

Die Kombination aller drei Gates ergeben insgesamt eine Bedrohung, die in dem Modell in Abbildung 17 zentral dargestellt ist. Unzureichende Privatsphäreneinstellungen und ein unsicherer Umgang mit Inhalten innerhalb der SNSs führt zur Begünstigung von **Information Gathering**, in Kombination mit unsicherem Umgang mit Freundschafts- und Verbindungsanfragen wird die Erreichbarkeit zwischen Zielpersonen und Social Engineers begünstigt (**Reach Victim**). Der unsichere, oder falsche Umgang mit Inhalten in Kombination mit dem Handhaben von Freundschafts- und Verbindungsanfragen, führt zur Begünstigung von Social-Engineering-Angriffstaktiken (**Perform Tactic**).

5.10. Zusammenfassender Vergleich und technisches Social-Engineering-Modell

In diesem Kapitel wurden verschiedene Phasenmodelle und Frameworks beschrieben, die im Zusammenhang mit Social-Engineering-Angriffen recherchiert wurden. Die Modelle unterscheiden sich am deutlichsten in Richtung der Darstellung, so sind die Modelle 5.1 (Cyber Kill Chain nach Lockheed), 5.4 (Social Engineering Pyramide nach Hadnagy), 5.8 (Session und Dialog basierendes Framework nach Wu et al.) und 5.9 (Phasen- und Quellmodelle nach Algarni und Xu) in nacheinander folgenden Prozessschritten, die Modelle 5.2 (Social Engineering Cycle nach Mitnick und Simon), 5.3 (Social Engineering Lifecycle nach Imperva), 5.5 (Social Engineering Attack Framework nach Mouton et al.), 5.6 (Cycle of Deception nach Nohlberg und Kowalski) und

5.7 (Social Engineering Attack Spiral nach Cullen und Armitage) in Kreisläufen dargestellt. Dass der Großteil der erforschten Frameworks eine zirkuläre Struktur verwendet, um Social-Engineering-Angriffe zu beschreiben, die meist die Phasen der Informationsbeschaffung, Ausnutzung von Vertrauen, Angriffsentwicklung und Zielerfüllung beinhalten, wird auch bereits in [1], sowie in [5], beschrieben. Die zirkulären Formen bieten die Darstellung der Möglichkeit, vorherige Phasen zu wiederholen, wenn mehr Informationen benötigt werden, oder das Ziel nicht in einer einzigen Phase erreicht wird [1].
Das Modell von Nohlberg und Kowalski [91] sieht ein Zurückkehren in einzelne, vorhergehende Phasen nicht vor, dafür aber eine Abfolge von mehreren Cycles sphärisch „übereinander“, was dieses Framework auf den ersten Blick, gerade auch in Kombination mit der Miteinbeziehung von Risiken als dreidimensionale Komponente, als sehr komplex erscheinen lässt.

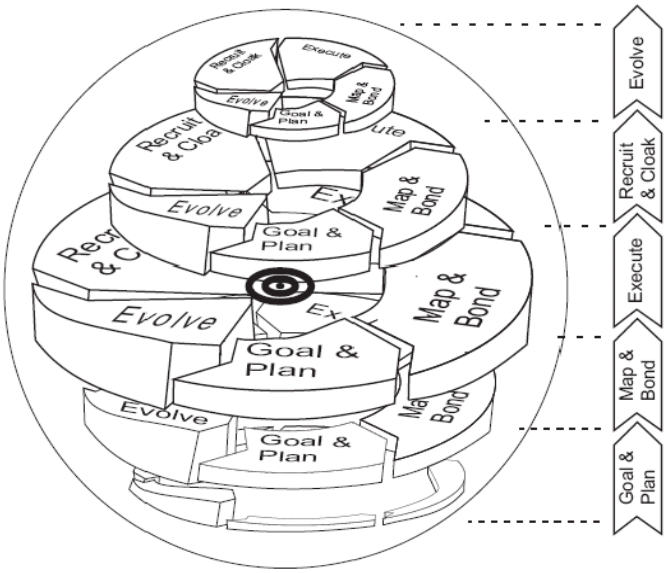


Abbildung 18: Cycle of Deception, sphärisch [91]

Die angeführten Modelle und Frameworks unterscheiden sich weiters auch hinsichtlich der Anzahl an Ablaufphasen, so wurden bis auf zwei Modelle, alle anderen Modelle mit weniger als acht Phasen entworfen.
Von der klassischen Cyber-Kill-Chain, so wie sie unter 5.1 beschrieben wurde, konnte zum Zeitpunkt der Recherche, noch keine auf den Bereich des Social Engineerings ausgerichtete Version aufgefunden werden. Für Social-Engineering-Angriffe ist sie allerdings nur bedingt geeignet, da diese Art von Angriffen nicht zwangsweise alle Phasen des Frameworks durchlaufen müssen. Ebenso fehlt diesem Modell der komplette Bereich in dem Beziehungen und Vertrauen aufgebaut, sowie ausgenutzt werden.
Die Pyramide von Christopher Hadnagy zeigt fünf Phasen und ist das einzige Modell, das als letzten Schritt ein Reporting, zur Nachvollziehbarkeit und Dokumentation des Ablaufs und der Ergebnisse, vorsieht. Der Social-Engineering-Lifecycle von Imperva, sowie das Modell nach Kevin Mitnick beschränken sich auf insgesamt nur vier Phasen bei ähnlichen Bezeichnungen. Das Modell von Mitnick wird im Vergleich mit dem Modell von Mouton et al. als gute Basis, allerdings als zu oberflächlich gesehen, es lässt [85] zufolge zu viel Spielraum für Interpretationen und beinhaltet keine Debriefing-Phase, welche in dem Modell von Mouton et al. vorgesehen ist, um Zielpersonen wieder zurück in normale emotionale Zustände zu bringen.
Unabhängig davon, wieviele Phasen die jeweiligen Modelle und Frameworks jedoch aufweisen, ändert sich nichts daran, dass am Beginn einer jeden erfolgreichen Social-Engineering-Attacke eine ausführliche und gründliche Phase zur Informationsbeschaffung stattfinden muss. Die Qualität der erlangten Informationen innerhalb dieser Phase trägt entscheidend zu den Erfolgen der nachfolgenden Phasen, so fein sie auch granuliert werden, bei. Während der Recherche und Analyse von verwandten Arbeiten, zu erfolgreichen Social-Engineering-Angriffen, aber auch zu verwendbaren, automatisierten Werkzeugen, hat sich gezeigt, dass entsprechende Suchergebnisse aus der Phase der Informationsbeschaffung im letzten Moment ursprünglich

geplante Angriffsszenarien abändern, schlimmstenfalls sogar als obsolet erscheinen lassen können. Generell ist Social Engineering aber so dynamisch, dass es weder exakt geplant werden kann noch ein wirklich zu 100 Prozent passendes Modell dazu gibt.
Basierend auf den beschriebenen Modellen und Frameworks wurde das nachfolgende technische Social-Engineering-Modell (TSE) entworfen, das auf nur drei Gemeinsamkeiten reduziert wurde, innerhalb dieser mit Toolunterstützung automatisiert werden kann. Die Reduzierung wurde auf die in Abbildung 19 dargestellten Phasen vorgenommen:

Abbildung 19: Technisches Social-Engineering-Modell

Eine entsprechende Zuordnung, welche Phasen der in diesem Kapitel beschriebenen Phasenmodelle und Frameworks zu welcher der reduzierten Phasen passen, ist der nachfolgenden Tabelle 2 entnehmbar. Zur besseren Darstellung und Lesbarkeit dieser wurden die in dieser Sektion beschriebenen Phasenmodelle und Frameworks in der darauffolgenden Tabelle 3 durchnummeriert.

Modell	Informationsbeschaffung	Angriffsvorbereitung	Angriffsausführung
M1	Reconnaissance	Weaponization, Delivery	Exploitation, Installation, Command & Control, Actions on Objectives,
M2	Research	Developing Rapport and Trust, Exploiting Trust	Utilize Information
M3	Investigation	Hook	Play
M4	Information Gathering	Attack Planning	Perform Attacks
M5	Information Gathering	Preparation	Exploit Relationship
M6	Map & Bond	Execution	
M7	Recon	Relationship Building, Attack Scenario Building	Execution, Action on Objectives
M8	Attack Preparation		Attack Implementation
M9	Using suitable gates of SNSs to gather information about the victim	Using suitable gates of SNSs to reach the victim	Attack

Tabelle 2: Phasenzuordnung zu technischem Social-Engineering-Modell

Nummer	Social-Engineering-Modelle und Frameworks
M1	Cyber Kill Chain nach Lockheed
M2	Social Engineering Cycle nach Mitnick und Simon
M3	Social Engineering Lifecycle nach Imperva
M4	Social Engineering Pyramide nach Hadnagy
M5	Social Engineering Attack Framework nach Mouton et al.
M6	Cycle of Deception nach Nohlberg und Kowalski
M7	Social Engineering Attack Spiral nach Cullen und Armitage
M8	Session und Dialog basierendes Framework nach Wu et al.
M9	Phasen- und Quellmodelle nach Algarni und Xu

Tabelle 3: Zuordnung Kurzbezeichnungen zu Social-Engineering-Modellen und Frameworks

6. Toolunterstütze Automation im Social Engineering

In diesem Abschnitt werden verschiedene Tools, mit welchen eine Automatisierung, oder eine Möglichkeit zur Automatisierung von verschiedenen Phasen oder Aufgaben, innerhalb eines Social Engineering Angriffs möglich sind, gelistet und vorgestellt. IBM beschreibt Automatisierung als einen Begriff, bei dem menschliche Eingaben minimiert werden und untergliedert diesen in grundlegende Automatisierung, zur Übernahme von einfachen, rudimentären Aufgaben, Prozessautomatisierung im Sinne von Workflow-Automatisierung, Integrationsautomatisierung, wo Maschinen menschliche Aufgaben nachahmen und wiederholen, sobald entsprechende Regelungen definiert wurden und in Automatisierung durch künstliche Intelligenz [97].
Die Gruppierung der Tools wird nach dem im vorherigen Kapitel entworfenen TSE-Modell vorgenommen. Signifikante Unterschiede im Vergleich mit anderen und ähnlichen Tools, sowie bei der Anwendung evaluierte Stärken und Schwächen, werden ebenfalls in den folgenden Unterkapiteln behandelt. Die gelisteten Tools wurden im Laufe der Recherche zusammengestellt, der Reihenfolge der Listung ist dabei keine besondere Rangfolge, Wertung oder Bewertung beigemessen. Alle gelisteten Werkzeuge unterliegen den Bedingungen, dass sie für die Bildung von Awareness, für Schulungszwecke, oder nur im Rahmen der rechtlichen und ethischen Gegebenheiten genutzt und angewandt werden dürfen.

6.1. Tools in der Phase Informationsbeschaffung

Die Werkzeuge in der Phase der Informationsbeschaffung dienen der Beschaffung von Informationen aller Art über ein Angriffsziel. Umfasst sind in dieser Phase jene Arten von Tools, die in diversen Information-Gathering-Phasen, in der Reconnaissance und in den verschiedensten Ausprägungen der Intelligence-Formen, beispielsweise das einleitend bereits erwähnte OSINT, oder eine davon abgeleitete Form der Social Media Intelligence (SOCMINT), zur Anwendung kommen.
Erste Informationen über ausgewählte Zielpersonen, die dem Social Engineering dienlich sind, können bereits ohne lokaler Installation von speziellen Tools, über verschiedene Webanwendungen, in Erfahrung gebracht werden. Die Ergebnisse aus der Verwendung dieser Tools können die Basis für die Verwendung von weiteren, spezifischeren Tools, darstellen.

6.1.1. Webapplikationen und Linklists für erste schnelle Suchergebnisse

6.1.1.1. Google Dorking

Die Internetsuchmaschine Google bietet, neben der gewöhnlichen und gewohnten Suche nach einfachen Begriffen, auch die Möglichkeit mittels Verwendung von speziellen Suchparametern, die Suchergebnisse genauer zu spezifizieren [98]. Dafür hat sich der Begriff des „Google-Dorking“ (früher auch als „Google-Hacking“ bezeichnet) durchgesetzt. Eine Vielzahl vorgefertigter und verwendbarer Suchabfragen ist beispielsweise in der Exploit-DB [99] aufzufinden. Zum Zeitpunkt der Recherche lag der aktuelle Stand der Exploit-DB bei verfügbaren 7.341 Google Dorks. Mittels der Google Programmable Seach Engine [100] ist es weiters möglich, Suchabfragen online zu Custom Search Engines (CSE) zu speichern. Diese CSEs sind auch öffentlich für die Allgemeinheit zugänglich und verwendbar.
Eine speziell auf Social-Media-Plattformen abgestimmte CSE von Brijesh Singh [101] ist unter [102] verfügbar, Stefanie Proto listet in den Zusammenstellungen [103] und [104] zum Zeitpunkt der Recherche über 130 weitere, verfügbare und direkt verwendbare CSEs.

6.1.1.2. OSINT Linklists

Während der Recherche zu automatisierten Social-Engineering-Werkzeugen wurden in einschlägigen Foren oftmals Verlinkungen zu Listen mit hunderten von Links zu Webapplikationen zur Verfügung gestellt, die für

OSINT Zwecke genutzt werden, welche aber auch den Information-Gathering-Prozess innerhalb des Social Engineerings unterstützen können.
Bellingcat [105], eine in den Niederlanden ansässige Gruppe investigativer Journalisten, die sich auf OSINT-Ermittlungen spezialisiert hat, bietet unter [106] und [107] eine Zusammenstellung nützlicher Webapplikationen zur Verwendung an. Ähnliches ist auch auf der Homepage des OSINT-Forschers mit dem Pseudonym „Technisette“ [108] zu finden, sowie in den weiteren auszugsweise in Tabelle 4 angeführten Quellen.

Seite	Kurzbeschreibung	Verweis
Technisette Tools	Webbasierende OSINT-Tools und Webapplikationen zur Unterstützung von Onlinercherchen, Links zu weiteren Partnerplattformen, Social-Media-Onlinesuchmaschinen.	[108]
Bellingcat’s Online Investigation Toolkit	Zusammenstellung von mehreren hundert webbasierenden Tools zur Unterstützung beim Information-Gathering, gruppiert nach Einsatzbereichen (beispielsweise Bildersuchmaschinen, Social Media, Peoplesearch und vieles mehr).	[106] [107]
OSINT for Journalists	Media-Map und Linklist mit Verlinkungen zu verschiedensten OSINT-Onlinesuchmaschinen, Toolsammlungen, Verlinkungen zu weiteren umfänglichen Linklisten, zu Webapplikationen und Datenbanken.	[109]
Search Social Media	Zahlreiche, nach Social-Media-Plattformen (Twitter, Reddit, Periscope, Tumblr, Facebook, Instagram, YouTube, LinkedIn, TikTok, Telegram, Snapchat, Pinterest) gruppierte, Onlinesuchmaschinen. Verlinkungen zu weiteren Linklisten und Suchmaschinen für Informationen zu Personen, Benutzernamen, Telefonnummern und E-Mailadressen.	[110]
Ph055a GitHub Repository	GitHub Repositories „Domains_OSINT_Collection” und “OSINT_Collection” beinhalten Linklisten mit zahlreichen Verlinkungen zu online verfügbaren OSINT-Ressourcen, beispielsweise Suchmaschinen für Benutzer über mehrere hundert Social-Media-Plattformen, Suchmaschinen für Informationen über Unternehmen, Suchmaschinen zum Durchsuchen von Leaks, aber auch Links zu Onlineressourcen um Domains und IoT-Produkte zu untersuchen, beispielsweise Subdomain-Enumerator und -Crawler, Link-Checker, DNS-Info, Similar-Site-Search und vieles mehr.	[111]
OSINT Framework	Eine animierte OSINT-Tool-Linksammlung, die neben frei verfügbaren Suchmaschinen und Webapplikationen zur Suche und Enumeration von und nach Benutzernamen, Domains, E-Mailadressen, Archiven auch Dokumentations- und Trainingsmaterial anbietet.	[112]

Tabelle 4: Zusammenstellung OSINT Linklists

Die Anzahl der Verlinkungen ist derartig umfangreich, dass eine genaue Nachprüfung im Rahmen dieser Arbeit nicht möglich war. Bei der stichprobenartigen Verwendung hat sich gezeigt, dass nicht alle Verlinkungen funktional waren, sowie nicht alle Tools automatisiert funktionierten. Es hat sich ebenfalls herausgestellt, dass Verlinkungen auf ähnliche Seiten beinhalten sind, die wiederum eine Vielzahl an Toolverlinkungen beinhalten. Ebenfalls hat sich gezeigt, dass sich die gelisteten Tools, Suchmaschinen und Browser-Plugins sehr oft gleichen.

6.1.1.3. Suche nach Benutzerdaten

Die Webapplikation *CheckUsernames* [113] ermöglicht es, innerhalb von ein paar Sekunden und Mausklicks auf 160 Social-Media-Plattformen gleichzeitig nach Benutzernamen zu suchen. In der Premiumversion ist der Suchumfang auf 300 Plattformen erweitert. Gesucht wird allerdings nur nach Benutzernamen in genau der eingegebenen Form, indem ein Teil der Profil-URL der Social-Media-Pattformen um den eingegebenen Benutzernamen erweitert wird. Am Ende der animierten Suche werden positive Suchergebnisse ausgegraut, mit einem Klick wir das jeweilige Social-Media-Profil aufgerufen.
ReconTool [114] bietet diese Möglichkeit ebenfalls und verlinkt bei der Nutzung der Suche nach Benutzernamen (in Abbildung 20 unter „>_Username“ dargestellt) sogar auf die Seite von CheckUsernames, der Funktionsumfang ist allerdings erheblich erweitert. So ist es hier nicht nur möglich eine Mindmap zu zeichnen und die einzelnen Nodes mit einem Mausklick in die jeweiligen Suchfunktionen zu übernehmen und Ergebnisse daraus direkt auswählen zu können, sondern auch direkt mit dem Entwickler zu chatten.

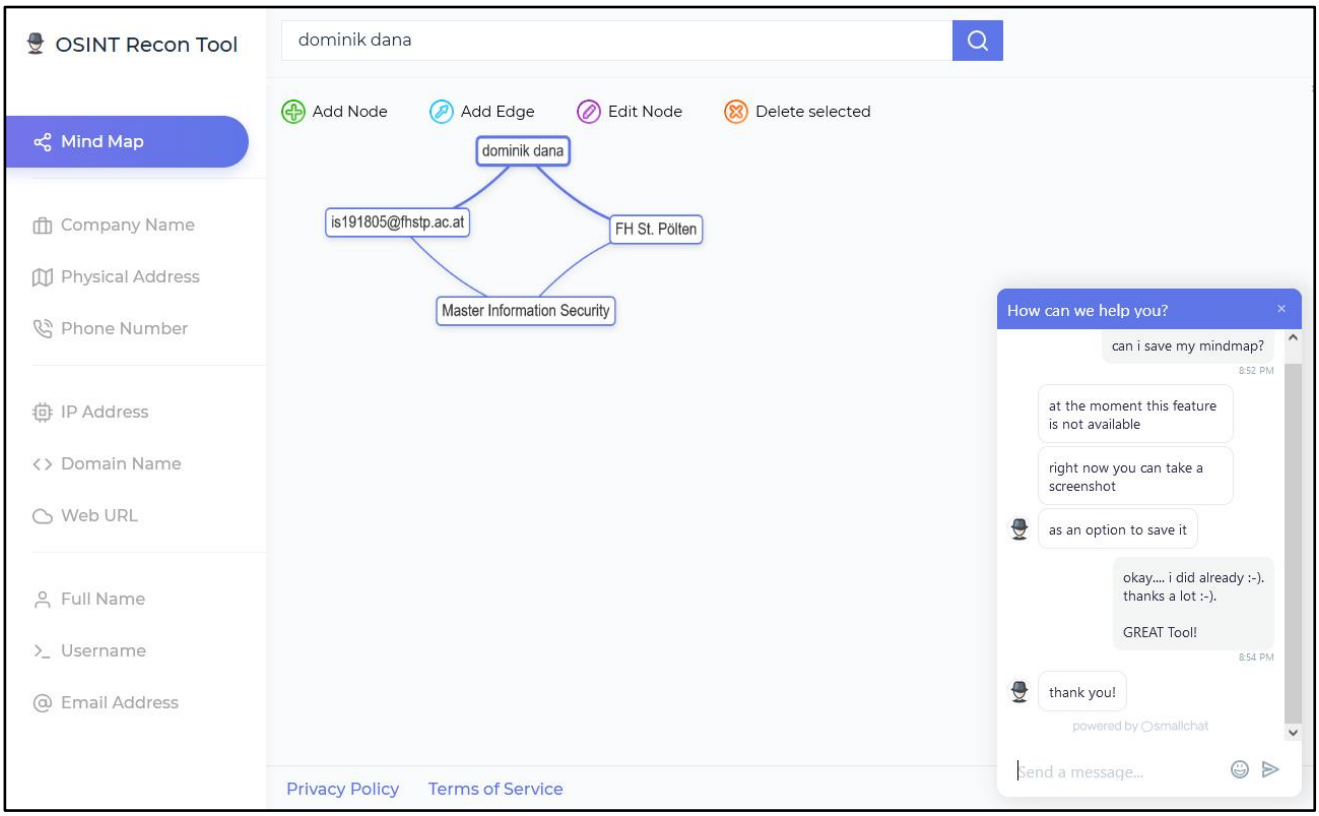


Abbildung 20: ReconTool Anwendungsbeispiel [114]

Ähnlich in der Handhabe und Funktionsweise agieren die *HOPain Tools* [115], die nicht nur interaktiv online zur Verfügung stehen, sondern auch über ein GitHub-Repository lokal geklont und genutzt werden können. Der Funktionsumfang ist im Vergleich zu ReconTool nochmals erweitert, da innerhalb dieser Webapplikation auch nach Bildern, Videos, detaillierten Inhalten auf den Social-Media-Plattformen (beispielsweise Postings innerhalb eines Zeitbereichs, mit bestimmten Textinhalten, nach Lokation, oder auch nach Anzahl der Likes), aber auch nach Bitcoin-Adressen, gesucht werden kann. Die Suchfunktionen innerhalb der Suchkategorien (beispielsweise Facebook Posts by User, Facebook Posts by Date) sind jeweils einzeln nutzbar, mit einem Klick auf „Populate All“ kann aber auch in allen Suchfunktionen ein Suchbegriff für Suchen übernommen werden.
Für die Suchergebnisse (bezogen auf die Suchen auf den SNSs) ist es nötig ein entsprechendes Social-Media-Konto innezuhaben. Die Ergebnisse gleichen den Suchen innerhalb der jeweiligen SNSs, die Handhabe ist in den HOPain Tools allerdings vereinfacht.

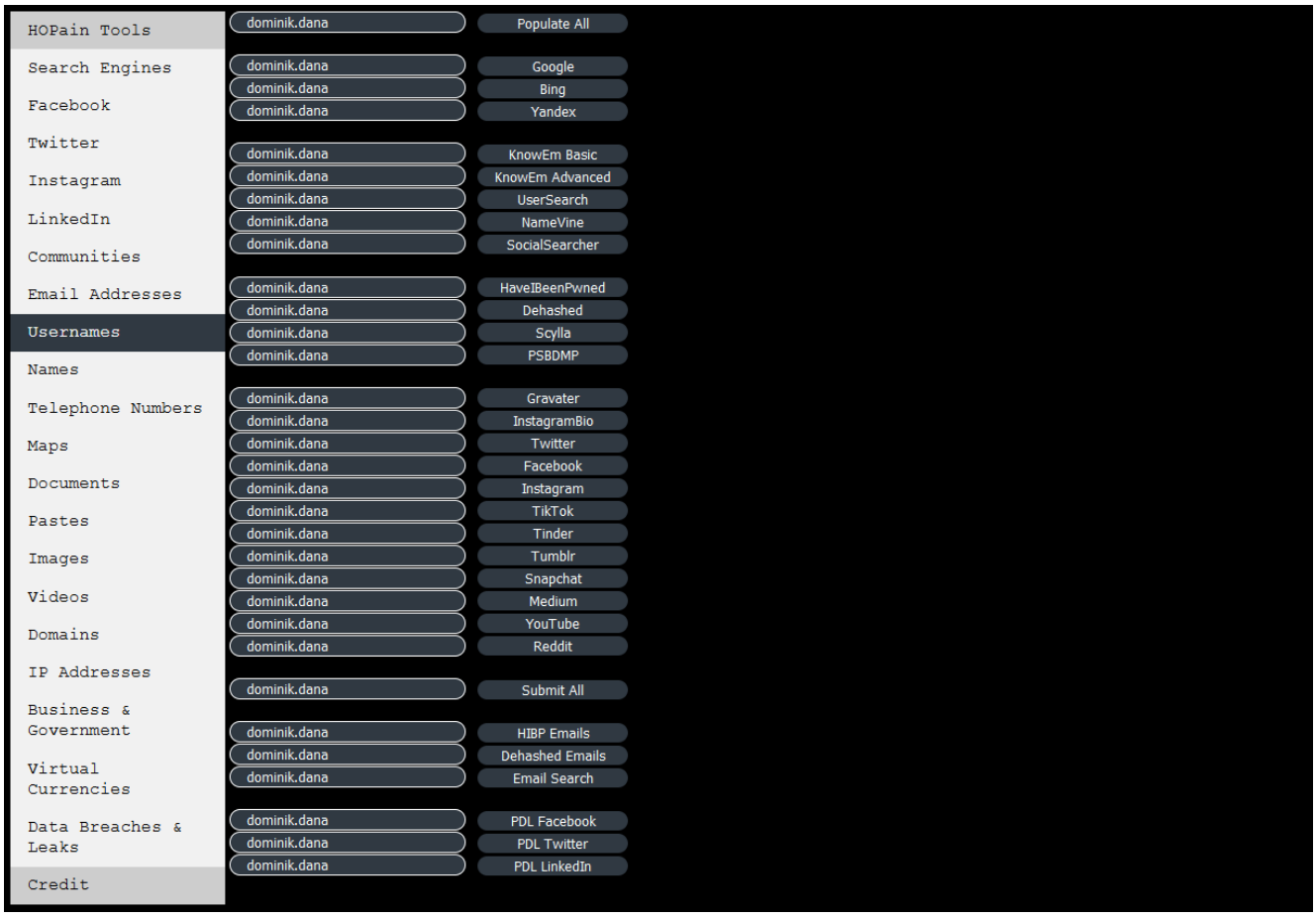


Abbildung 21: HOPain Tools SNS-Benutzersuche [115]

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
CheckUsernames	Automatisierte Benutzersuche auf 160 Plattformen gleichzeitig.	[113]
OSINT Recon Tool	Suche nach Benutzernamen, E-Mail-Adressen, Namen, Domains, Firmen, Telefonnummern, etc. Mindmap Unterstützung mit „Click-to-Search“ Funktion, Chat mit Entwickler möglich.	[114]
HOPain OSINT Search Tools	Parallele Suchen in verschiedenen Suchmaschinen, Social-Media-Plattformen, nach Dokumenten, Data Breaches und Leaks, sowie nach Bitcoin-Adressen. Suchen sind genauer spezifizierbar, mit einem Klick können Suchen über alle Suchmaschinen in der jeweiligen Kategorie verteilt werden. GitHub-Repository vorhanden.	[115] [116]

Tabelle 5: Zusammenstellung Suche nach Benutzerdaten

6.1.1.4. Technologiecheck

Um die Möglichkeiten der Pretexts und Impersonationen für Social Engineering in Organisationen zu erweitern, kann es auch hilfreich sein, die bestehenden Internetauftritte auf verwendete Technologien und eventuelle Schwachstellen zu untersuchen. Als Alternative zu, durch höhere Lizenz- und Betriebskosten, erheblich teurere Systeme, können die nachfolgenden Tools genutzt werden.
Das Ergebnis eines Scans mit *BuildWith* [117] zeigt nicht nur verwendete Technologien des jeweiligen Webauftritts, verwendete Plugins und auch den genutzten Hostingprovider, sondern auch weitere Webauftritte, die den gleichen Hostingprovider nutzen, sowie die Dauer und die jeweilige öffentliche IP-Adresse, unter welcher diese erreichbar waren. Die Ergebnisse sind in der freien Version allerdings nur eingeschränkt einsehbar, für die Suche nach CVEs (Common Vulnerabilities and Exposures) und zur Entwicklung von Pretexts aber ausreichend.
Technologische Informationen, Telefonnummern, E-Mail-Adressen, CVE-Schwachstellen mit der entsprechenden CVE-Nummer, genutzte öffentliche IP-Adressen, offene Ports, Domainnamen, sowie Cybersquatting-Domains und vieles mehr, um weitere Angriffsflächen und Risiken eines Webauftrittes zu ermitteln, lassen sich auch sehr komfortabel mit *SpiderFoot* [118] herausfinden. Die Version *SpiderFoot HX* [119] bietet einen noch erweiterten Umfang und eine intuitive, grafische Oberfläche, die all diese Infos mit wenigen Klicks in Form eines Node-Graphs (siehe Abbildung 22) darstellen kann. Jeder Node ist einzeln auswählbar und bietet nicht nur die Möglichkeit die Ergebnisse detailliert einzusehen, sondern auch von hier aus eine neue Investigation zu starten.

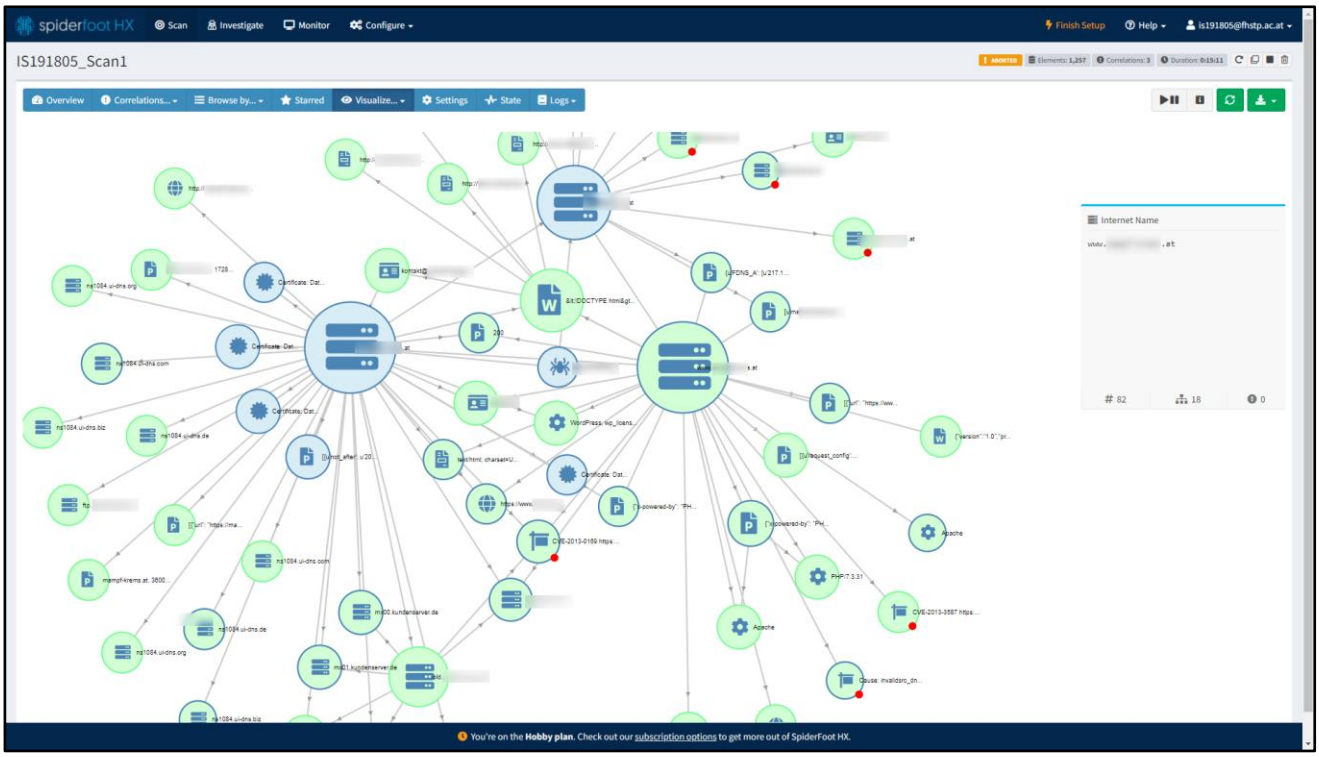


Abbildung 22: SpiderFoot HX Scan Anwendungsbeispiel (anonymisiert) [119]

In der Basisversion (Hobby Plan) unterliegt man allerdings auch hier einigen Einschränkungen, beispielsweise sind Investigationen in den Nodes in dieser Version nicht freigeschalten, Scans enden nach einem 15-minütigen Zeitlimit und nach einer bestimmten Höchstanzahl an Scans pro Tag und Ziel. Die Scanergebnisse waren in der Kürze der Zeit und in Anbetracht der genutzten Basisversion überraschend umfänglich und durchgängig korrekt.

Neben *Shodan* [120], einer der bekanntesten Suchmaschinen, die Informationen über jedes im Internet verfügbare Gerät sammelt, wurden in Zusammenhang mit der Suche nach technischem Information-Gathering in einschlägigen Foren die Systeme *ZoomEye* [121], *Spyse* [122] und *Chaos.* [123] genannt.
Shodan ist in der Handhabe mit den vielen Filtermöglichkeiten am Beginn etwas unübersichtlich und verlangt, neben einer Registrierung, eine Einarbeitungszeit, um mit der Suche brauchbare Ergebnisse zu erzielen. Die Suchergebnisse sind abhängig von der Zeit, in der Shodan das Zielsystem gescannt hat, beinhalten dafür einen hohen Detailgrad über das gescannte Zielsystem, sind allerdings auch hier in der Basisversion eingeschränkt.
ZoomEye war zum Zeitpunkt der Recherche, trotz sprachlicher Barrieren, mit Übersetzungssoftware verwendbar und erinnerte in der Darstellung der Suchergebnisse sehr an Shodan. Während dem Verfassen der Arbeit und detaillierterem Betrachten der einzelnen Tools erforderte es allerdings eine Registrierung, die aber nicht durchgeführt wurde.
Spyse konnte währen der Anwendung und unter Verwendung identer Zielsysteme, überraschenderweise nur wenige Ergebnisse liefern und ist für Social-Engineering-Zwecke damit wenig geeignet. Chaos. befand sich zum Zeitpunkt der Recherche noch in einem frühen Entwicklungsstadium, auch während dem Verfassen der Arbeit war eine Registrierung zur Nutzung noch nicht möglich.

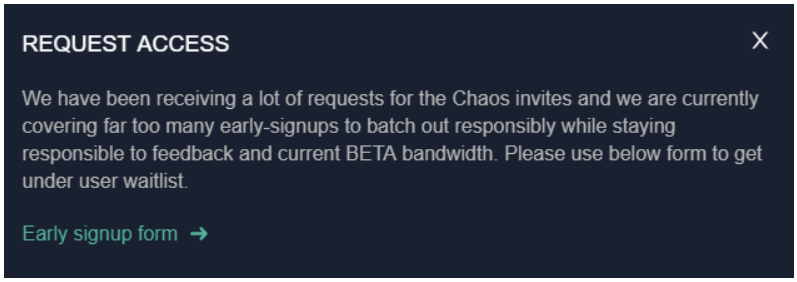


Abbildung 23: Request Access to Chaos. [123]

Ein hingegen durchgängig frei verfügbares Werkzeug, das ebenfalls in diese Kategorisierung passt, ist *SynapsInt* [124]. SynapsInt liefert Suchergebnisse zu Domains, IP-Adressen, SSL-Zertifikaten, E-Mail-Adressen, Telefonnummern und auch zu Twitter-Accounts. SynapsInt bietet auch die Möglichkeit nach Ransom-Bitcoin-Adressen und nach CVE-Nummern zu suchen. Die Ergebnisse eines Scans mit den selben Eingaben wie zuvor, lieferte in kurzer Zeit korrekte Ergebnisse, einen aktuellen Screenshot der Seite, eine VirusTotal-Analyse, den letzten verfügbaren Eintrag in dem Internetarchiv Wayback-Machine, offene Ports und Informationen zu dem genutzten Hosting-Provider.
Weiters wurden sämtliche Domains, die unter derselben IP-Adresse erreichbar sind, sämtliche Subdomains, internen Verlinkungen und verwandte Social-Media-Verknüpfungen gelistet und geprüft, ob (am Beispiel einer eingegebenen Domain) diese in diversen Blocklists beinhalten ist. Die Blacklist-Prüfung funktioniert auch mit eingegebenen E-Mail-Adressen. Die Leak-Prüfung, sowie die Twitter-Account-Prüfung hat mit einer bereits oftmalig geleakten privaten E-Mail-Adresse nicht funktioniert.

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
BuiltWith	Technologie-Scan von Webauftritten, Auflistung von verwendeten Plugins, Providern und verwendeter IP-Adressen. Eingeschränkter Funktionsumfang in der frei nutzbaren Version. In kostenpflichtigen Versionen größere Anzahl an Scans und detailliertere Ansicht der Suchergebnisse, sowie Ansteuerung via API möglich.	[117]

Tabelle 6: Zusammenstellung Technologiecheck Teil 1

Tool	Kurzbeschreibung	Verweis
SpiderFoot HX	Ermittlung von technischen Schwachstellen bei Scans von Webauftritten. Node-Graph-Darstellung von Suchergebnissen mit Möglichkeit zu direkt weiteren Investigationen, oder zu detaillierteren Ansichten. Findet nicht nur technische Schwachstellen, inkludiert in Scans (Module in Untermenü „State“ einsehbar) auch Suche nach E-Mail-Adressen, Telefonnummern, ähnlichen Domains und vieles mehr.	[118] [119] [125]
Shodan	Umfangreiche Suchergebnisse von Geräten, die mit dem Internet verbunden sind. Erfordert Registrierung und Einarbeitung in die Handhabe. Ergebnisse sind abhängig von dem Zeitpunkt des Scans des jeweiligen Systems. Developer-API und Browser-Toolbar verfügbar. Basisversion limitiert Suchergebnisse.	[120]
ZoomEye	Ähnlich wie Shodan, allerdings durchgängig chinesisch. Während der Recherche gesetzte Limitierung auf 400 Abfrageergebnisse, während der Verschriftlichung nurmehr mit Anmeldung nutzbar.	[121]
Spyse	Liefert bei gleichen Suchabfragen weniger Ergebnisse als andere Tools in der freien Ausführung.	[122]
Chaos.	Beta-Version, Registrierung nicht möglich.	[123]
SynapsInt	Durchgängig Freeware, liefert unter Verwendung verschiedener Suchmaschinen im Hintergrund Ergebnisse zu Domain, IP-Adressen, Metadaten, zu Social-Media-Verknüpfungen, Internetarchivdaten und bietet den Service um auf Phishing zu prüfen. Liefert auch Suchergebnisse zu Bitcoin-Adressen und CVE-Datenbanken.	[124]

Tabelle 7: Zusammenstellung Technologiecheck Teil 2

6.1.1.5. E-Mail-Adressformate ableiten

Um genutzte E-Mail-Formate eines Angriffsziels, beispielsweise einer Zielperson in dessen Unternehmensumfeld, herauszufinden, eignen sich die Suchmaschinen *Email-Format* [126], *Hunter.io* [127], sowie *Finder.app* [128].
Während bereits bei der ersten Abfrage mit Finder.app das Limit erreicht wurde, werden bei den beiden anderen Suchmaschinen mehrere Abfragen gestattet. Hunter bietet 25 Abfragen pro Monat, Email-Format gibt auf deren Webpräsenz zwar kein Limit an, startet bei den Pricing-Modellen in dem kleinsten Tarif allerdings mit einer Limitierung von bis zu 200 täglichen Abfragen. Hunter, als auch Email-Format leiten, aus einer Vielzahl an via Webscans gesammelten E-Mail-Adressen, Muster für entsprechende E-Mail-Adressformate ab. Von den testweise eingegebenen Zieldomänen lieferte rund ein Drittel keine Suchergebnisse. Die in beiden Webapplikationen abgeleiteten E-Mail-Adressformate erscheinen richtig, es werden in beiden Applikationen auch Beispieldaten frei angezeigt, deren Aktualität allerdings nicht durchgängig gegeben ist.
Email-Adressformat bietet, neben den identifizierten Konventionen, eine größere Liste an repräsentativen E-Mail-Adressen, sowie (je nach Bezahlplan) auch die Möglichkeit diese herunterzuladen. Im Vergleich zu Email-Format limitiert Hunter die Ausgabe zwar eher, zeigt jedoch, neben aktuelleren Datensätzen, auch das Vorkommen der repräsentativen E-Mail-Adressen auf, anhand dieser die Logiken für die E-Mail-Adressen abgeleitet werden.
Die Ergebnisse der Tools sind nachfolgend, in Abbildung 24 und Abbildung 25, gegenübergestellt.

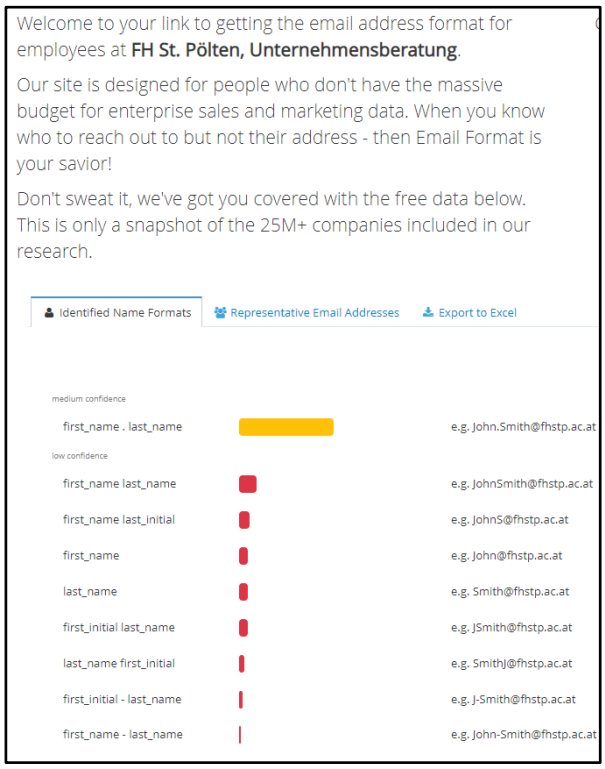


Abbildung 24: Email-Format Anwendungsbeispiel [126]

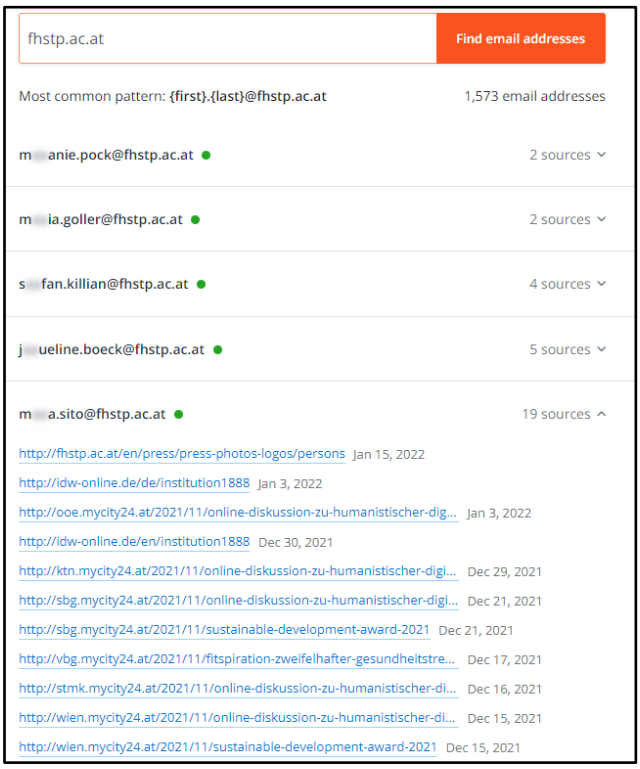


Abbildung 25: Hunter.io Anwendung (anonymisiert) [127]

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
Email-Format	Ableitung von E-Mail-Adressformaten aus vorhandenen E-Mail-Adressen. Eingeschränkte Nutzung, höhere Leistung (API-Ansteuerung, mehr erlaubte Suchabfragen und -ergebnisse, sowie umfänglichere Suchdatenbanken) durch entsprechende Bezahlpläne. 30 Tage Geld-Zurück-Garantie.	[126]
Hunter.io	Ableitung von E-Mail-Adressformaten aus gescannten E-Mail-Adressen mit Verlinkung der Herkunft.	[127]
Finder.app	„50 free credits/month“ funktionierten nur einmalig.	[128]

Tabelle 8: Zusammenstellung E-Mail-Adressformate ableiten

6.1.1.6. Durchsuchen von Databreaches und Dataleaks

Die Plattform *_IntelligenceX* [129] präsentiert bei Suchanfragen nach beispielsweise E-Mail-, Bitcoin-, MAC- und IP-Adressen, Domänen, URLs, Telefonnummern, Kreditkartennummern und vielem mehr, Ergebnisse aus Dataleaks, aus Wikileaks, Paste-Sites und sogar aus dem Darknet. _IntelligenceX bietet eine sogenannte „Third Party Search“, in welcher der Suchumfang nochmals auf mehrere Suchmaschinen (gleichzeitig via Popups) ausgedehnt werden kann und beispielsweise auch nach Fahrzeugidentifikationsnummern (VIN) gesucht werden kann. Es gibt eigene Suchfunktionen für Social-Media-Kanäle, Verlinkungen zu OSINT-Linklists, sowie File- und Encoding-Tools.

Die abgesetzten Testsuchen lieferten überraschend genaue Ergebnisse. Eine privat genutzte, wissentlich bereits geleakte und nicht mehr in Verwendung befindliche E-Mail-Adresse konnte, inklusive zu der Zeit der Nutzung verwendetem Kennwort, aufgefunden werden. Eine für eine weitere, noch privat genutzte E-Mail-Adresse, konnte herausgefunden werden, in welchem Databreach die E-Mail-Adresse aufgetaucht ist, beziehungsweise welche Plattform von dem Breach betroffen war.

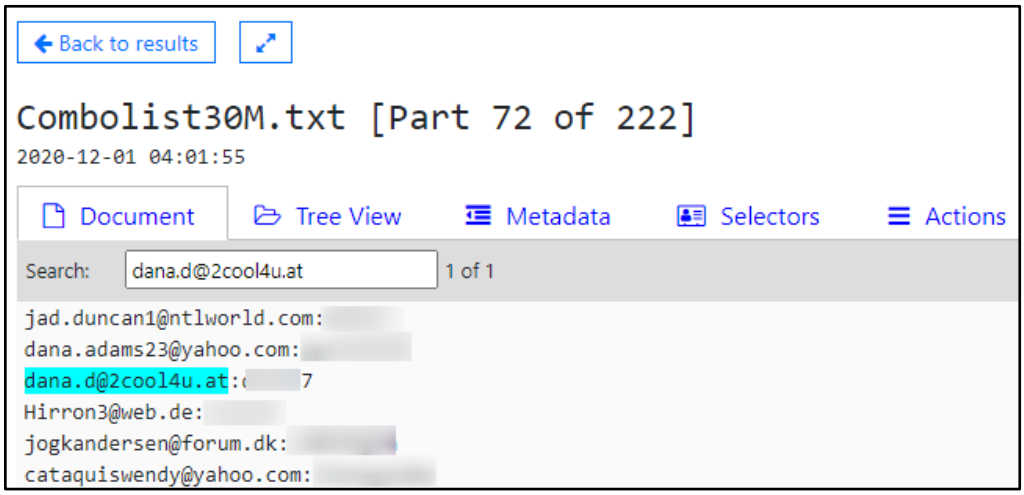


Abbildung 26: IntelX Suchergebnis Databreach 1 (anonymisiert) [129]

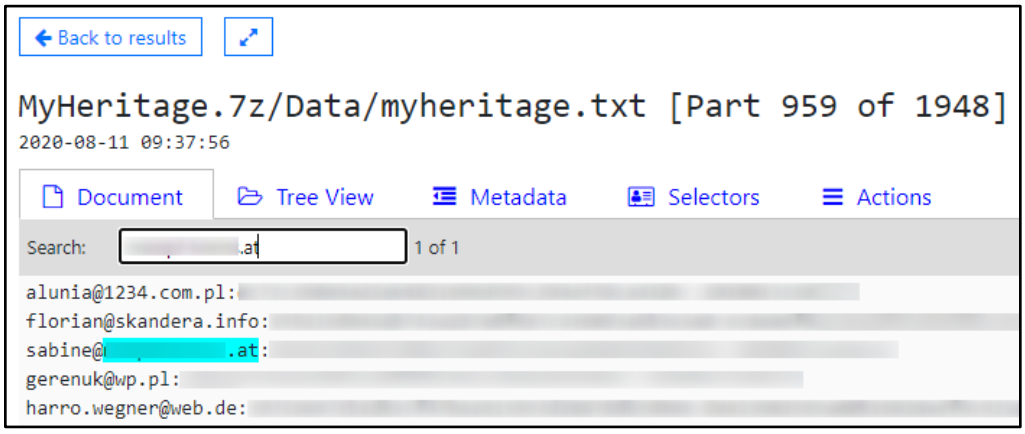


Abbildung 27: IntelX Suchergebnis Databreach 2 (anonymisiert) [129]

Für weitere E-Mail-Adressen im privaten Umfeld konnten ebenfalls gültige Zugangsdaten aufgefunden werden, die betroffenen Personen wurden im Rahmen der innerhalb dieser Sektion durchgeführten Suchen, darüber informiert und um Änderung ersucht, sollte diese nicht bereits erfolgt sein.
Testweise ebenfalls durchgeführte Reverse-Image-Searches aus der Kategorie Third-Party-Search, mit wahllos hochgeladenen Bildern aus Privatbestand und schneller Google-Suche, verwiesen allerdings größtenteils auf Adobe-Stock Grafiken, von zehn hochgeladenen Bildern wurden drei gefunden. Ebenfalls getestet wurde die VIN-Suche mit zwei verschiedenen VIN-Nummern aus eigenem Bestand, die Suche blieb jedoch ohne Ergebnis.
_IntelligenceX ist in der freien Version auf zehn Abfragen pro Tag limitiert und zensiert dabei teilweise Ergebnisse mit schwarzen Balken. In der angebotenen und registrierten Universitäts-Lizenz waren die schwarzen Zensurbalken nicht mehr zu sehen, die erlaubten Abfragen wurden auf 100 Abfragen pro Tag angehoben.

6.1.1.7. Onlinezeiten auswerten

Im Rahmen der Recherche nach entsprechend automatisierten Social-Engineering-Werkzeugen wurden zwei Tools analysiert, die eine Überwachung, beziehungsweise Auswertung von Onlinezeiten potenzieller Social-Engineering-Opfer ermöglicht.
Für die SNS-Plattform Twitter wurde *SleepingTime* [52] analysier und mit mehreren Twitter-Accounts erfolgreich genutzt. SleepingTime wertet die letzten 1000 Tweets eines Twitter-Accounts aus und leitet aus den Zeitstempel der jeweiligen Tweets einen geschätzten „Schlafplan“ ab, in dem der Account am wenigsten aktiv und in Verwendung ist. Für den offiziellen Twitter-Account der Fachhochschule St. Pölten ist das das Zeitfenster zwischen 23:00 Uhr und 07:00 Uhr, exemplarisch unter Abbildung 28 dargestellt:

Abbildung 28: SleepingTime Analyse Twitter-Account [52]

Um ein ähnliches Tool, das mit Browser-Notifikationen arbeitet, wenn ein bestimmter WhatsApp-Kontakt online verfügbar ist, handelt es sich bei dem *WhatsApp-Monitor* [53]. Die Verwendung des Tools klang während der Recherche sehr interessant, konnte allerdings zum Zeitpunkt der Tests nicht verwendet werden, da für die Inbetriebnahme auf die Seite http://wpmonitor.tech/online verwiesen wurde, die zu dem Zeitpunkt der Tests nicht aufrufbar war und das Laden der Seite durch den Browser mit der Fehlermeldung „*ERR_CONNECTION_REFUSED*“ abgebrochen wurde.

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
Sleeping Time	Auswertung Inaktivitätszeiten von Twitter-Accounts durch Analyse der Zeitstempel der 1000 letzten Tweets.	[52]
WhatsApp-Monitor	Browser-Notifikationen für verfügbare WhatsApp-Kontakte.	[53]

Tabelle 9: Zusammenstellung Onlinezeiten auswerten

6.1.1.8. Suche nach Personendaten

Webmii [130] ist eine Personensuchmaschine, die öffentlich auffindbare Informationen über Personen im Internet zusammenstellt und daraus einen Online-Score generiert, der die Verfügbarkeit der jeweiligen Person im Internet darstellen soll.

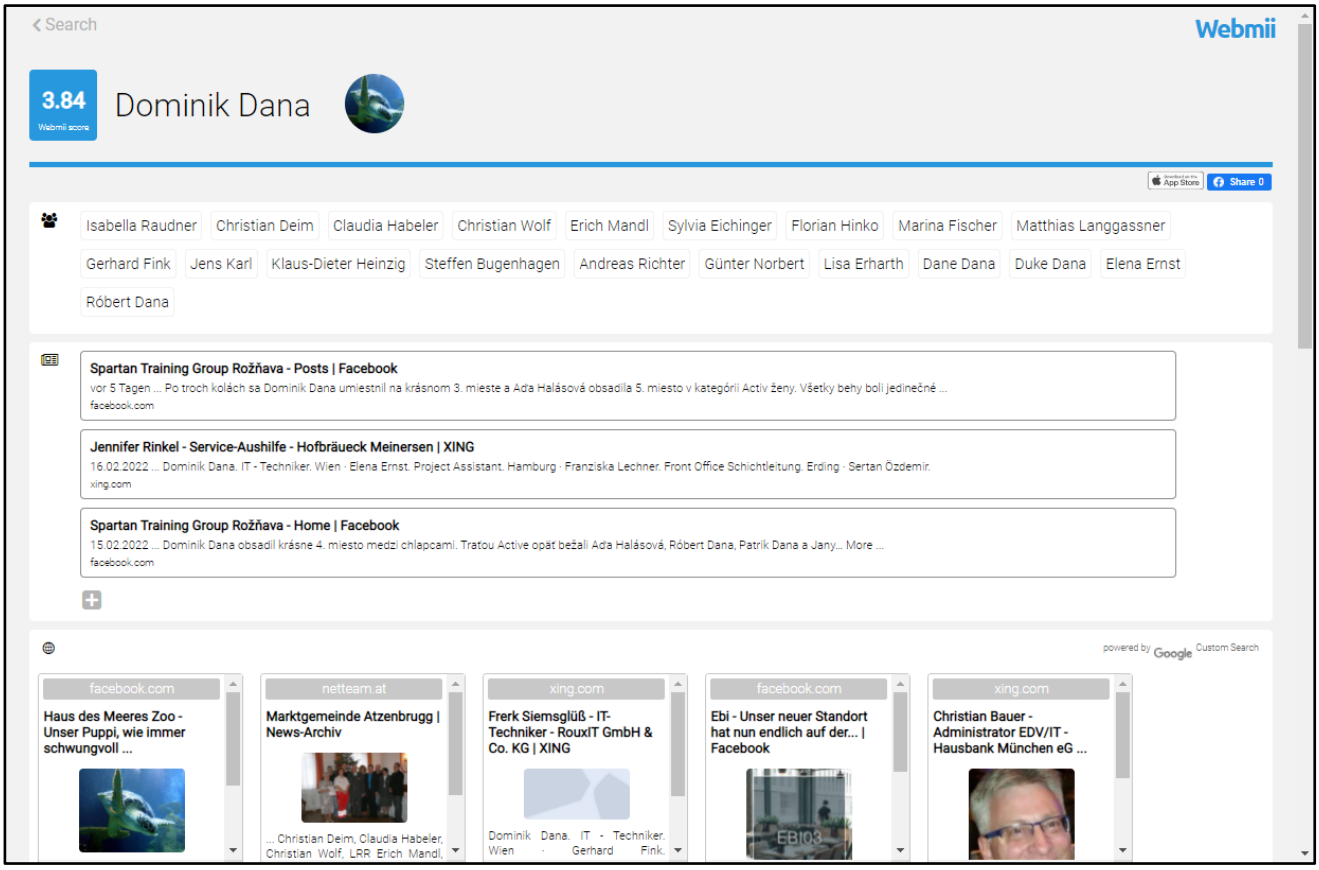


Abbildung 29: Webmii Suchergebnisse [130]

Webmii listet die Ergebnisse zumeist in vier Bereichen. In dem ersten Bereich der Ergebnisliste werden Namen von Personen, die in den Social-Media-Kanälen mit der Zielperson interagiert haben, gelistet. Bei Anklicken eines Namens in der Ergebnisliste wird dieser direkt in eine neue Suche übernommen. In dem zweiten Bereich finden sich Suchergebnisse aus diversen Zeitungsartikeln. In dem dritten Bereich finden sich Suchergebnisse aus verschiedenen Social-Media-Kanälen und in dem letzten und vierten Bereich lassen sich weitere, durch eine Google-CSE eingeholte, Suchergebnisse durchsehen.
IDCrawl [131] bietet auf den ersten Blick einen größeren Funktionsumfang, da hier nicht nur nach Namen von Personen gesucht werden kann, sondern auch nach Benutzernamen quer durch 17 SNSs. Ebenfalls angeboten wird eine Reverse-Phone-Suche. Praktisch ist, dass IDCrawl die Möglichkeit eines „Opt-Out“ anbietet, wo man sich aus Suchergebnissen mit entsprechender Begründung exkludieren lassen kann. Bei dem Test und der Suche nach eigenen auffindbaren Informationen konnte bei IDCrawl nur ein Suchergebnis als korrekt verifiziert werden, die Aktualität des Ergebnisses war allerdings zu bezweifeln, da in dem konkreten Fall das Benutzerprofilbild nicht übereingestimmt hat und bereits längere Zeit ersetzt wurde. Die Korrektheit der Daten ist aber auch bei Webmii nicht in großer Menge gegeben, da auch in dieser Suchmaschine nur Teile der Informationen als korrekt angesehen werden konnten. Der überwiegende Teil der Suchergebnisse war nicht verwendbar, Links von Ergebnissen ließen sich vereinzelt auch gar nicht öffnen.

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
Webmii	Webbasierende Personensuche mit Darstellung eines Online-Scores und namentliche Darstellung von mit der Zielperson interagierenden Personen.	[130]
IDCrawl	Webbasierende Personensuche mit Möglichkeit eines begründeten Opt-Outs, Suchmöglichkeit nach Benutzeraccounts in 17 verschiedenen SNS-Plattformen, sowie Möglichkeit der Suche nach Telefonnummern.	[131]

Tabelle 10: Zusammenstellung Suche nach Personendaten

6.1.2. Lokale Tools mit Installationsbedarf

6.1.2.1. Alternative zu Maltego

Das Data-Mining-Tool *Maltego* [132] ist eines der bekanntesten Toolsuites in der OSINT-Umgebung zur Informationsbeschaffung und in seinem Funktionsumfang annähernd einzigartig. Je nach Lizenzierung und hinzugefügten Plugins, die in dem Maltego Transform Hub bei Programmstart auswähl- und installierbar sind, ändert sich der Leistungsumfang der Software. Maltego, als auch die wählbaren Plugins unterliegen herstellerabhängig individuellen Lizenzmodellen, deren Bezugsmöglichkeiten teilweise auch auf bestimmte Institutionen eingeschränkt sind und deren Hauptunterschiede sich in der Anzahl der Entitäten in einem Diagramm und in der Anzahl an Transformationen, bewegen. Für die Tests und den Toolvergleich mit einem ähnlichen Tool wurde die registrierte, freie Community Edition mit acht freien Plugins genutzt, welche je nach genutzter Abfrage (innerhalb von Maltego als Transformationen bezeichnet) eine bestimmte Anzahl an Credits zur Verfügung stellt. Ein Suchlauf kann aus vielen hintereinander abfolgenden Transformationen bestehen, es empfiehlt sich daher den Umfang und die Plugins gerade am Beginn der Suche noch klein zu halten und die Suchen in spezifischen Richtungen zu vertiefen. Der Beginn einer neuen Investigation hängt von bereits vorhandenen Informationen über das Zielunternehmen oder die Zielperson ab. In dem nachfolgenden Beispiel wurde via Drag-and-Drop die Entität „Person“ in den Graphen gezogen, mit dem Firmenwortlaut versehen und von diesem aus mit den Transformationen begonnen.
In dem Suchgraph, dargestellt in der nachfolgenden Abbildung 30, sind die Ergebnisse der durchgeführten Transformationen für ein reales Unternehmen im persönlichen Umfeld, in anonymisierter Form, ersichtlich. Mit sechs von einhundert zur Verfügung gestandenen Credits war es bereits möglich Domaininformationen, Whois-Einträge, Firmeninhaberdaten, E-Mail-Adressen, Telefonnummern, öffentliche IP-Adressen, alle verwendeten Plugins des Internetauftritts, sowie archivierte Versionen davon seit dem Jahr 2009 aufzufinden. Ebenfalls aufgefunden wurden Prüfberichte von amerikanischen Betrieben der gleichen Unternehmenssparte in der Maltego Documentcloud. Diese standen allerdings in keinem Bezug zu dem exemplarischen Zielunternehmen.
Im Rahmen der Recherche konnte eine vergleichbare Alternative, beziehungsweise Ergänzung, zu Maltego recherchiert werden, die trotz kritischer Stimmen [133], ausgeführt und zum Vergleich lizenziert und getestet wurde: *Lampyre* [134]. Lampyre ist nur auf Windows-Plattformen verfügbar und bietet in der sogenannten „List of requests“ (siehe Abbildung 32) eine ähnliche Übersicht wie Maltegos Transformation Hub. Der Vorteil der Software ist, dass die Plugins nicht einzeln installiert werden müssen, eine Auswahl (und ebenfalls, wie bei Maltego, die Eingabe eines entsprechenden API-Keys) der zu nutzenden Module, der darunterliegenden und gewünschten Aufgaben, sowie der erforderlichen Parameter dazu, reicht für den Start aus. Auch Lampyre bringt in der Grundversion, von der Anzahl der Abfragen her, eine Deckelung mit die bei „100 Ph“ (Photons) liegt. Der aktuell verfügbarer Stand ist in dem Onlineportal einsehbar, in der Übersicht „List of requests“ wird auch berechnet, wieviel von dem verbleibenden Ph-Guthaben bei Abfragenausführung in Abzug kommen wird.

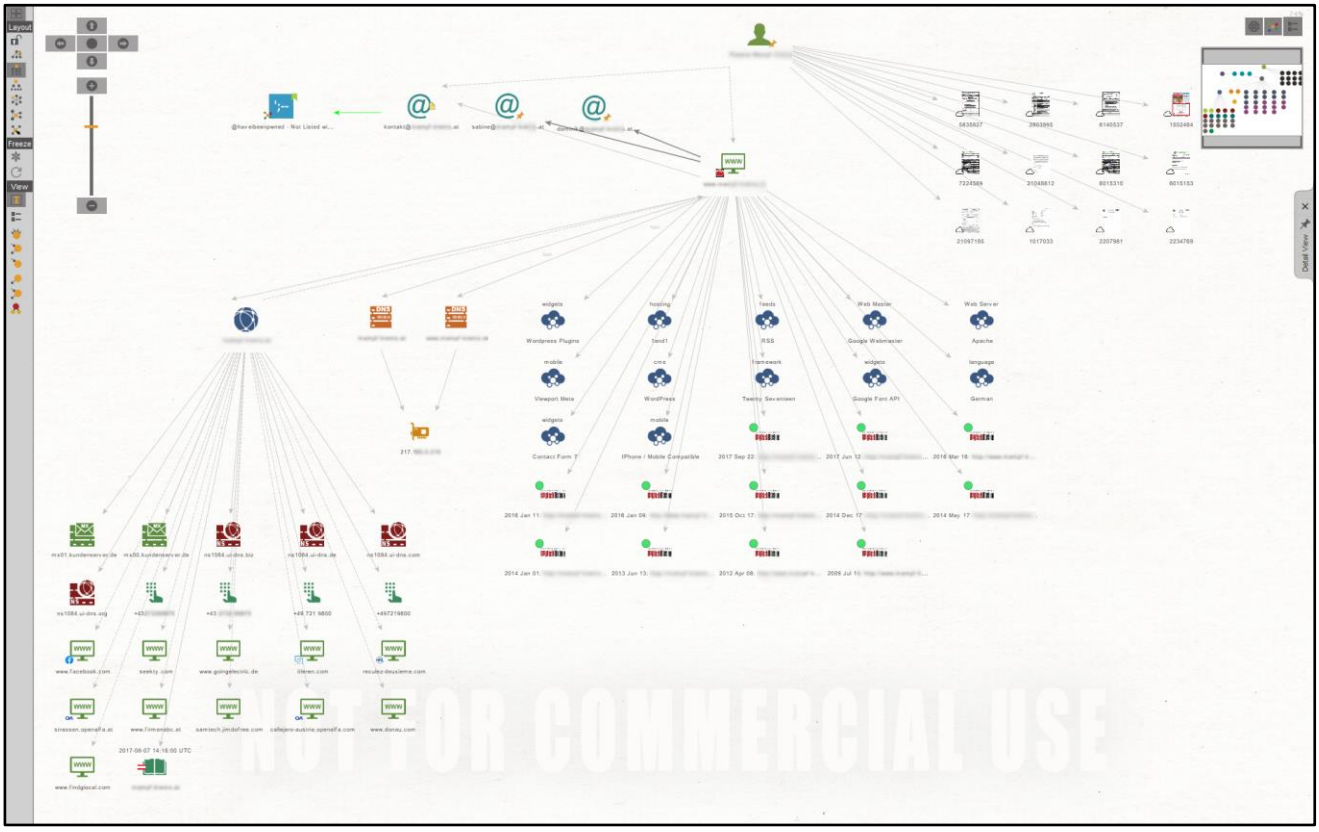


Abbildung 30: Maltego Graph Suchergebnisse (anonymisiert) [132]

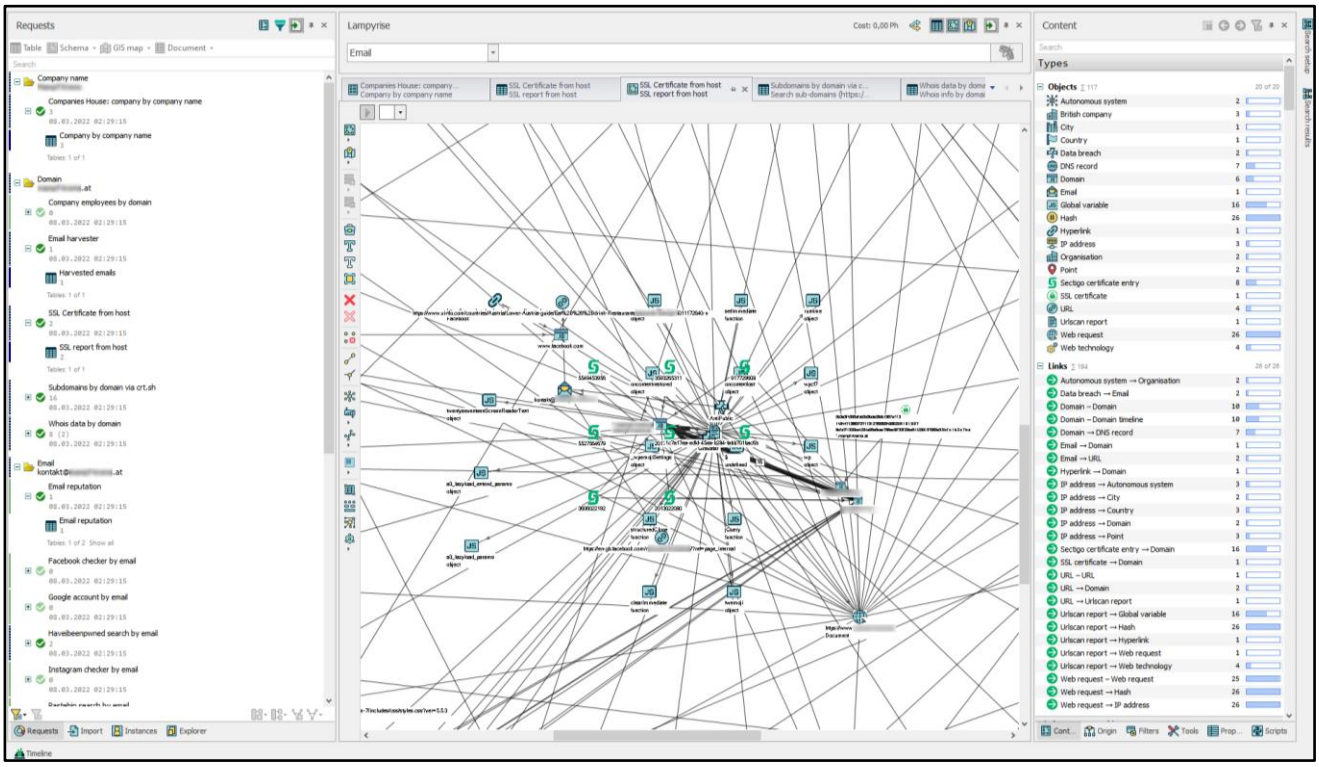


Abbildung 31: Lampyre Schema Suchergebnisse (anonymisiert) [134]

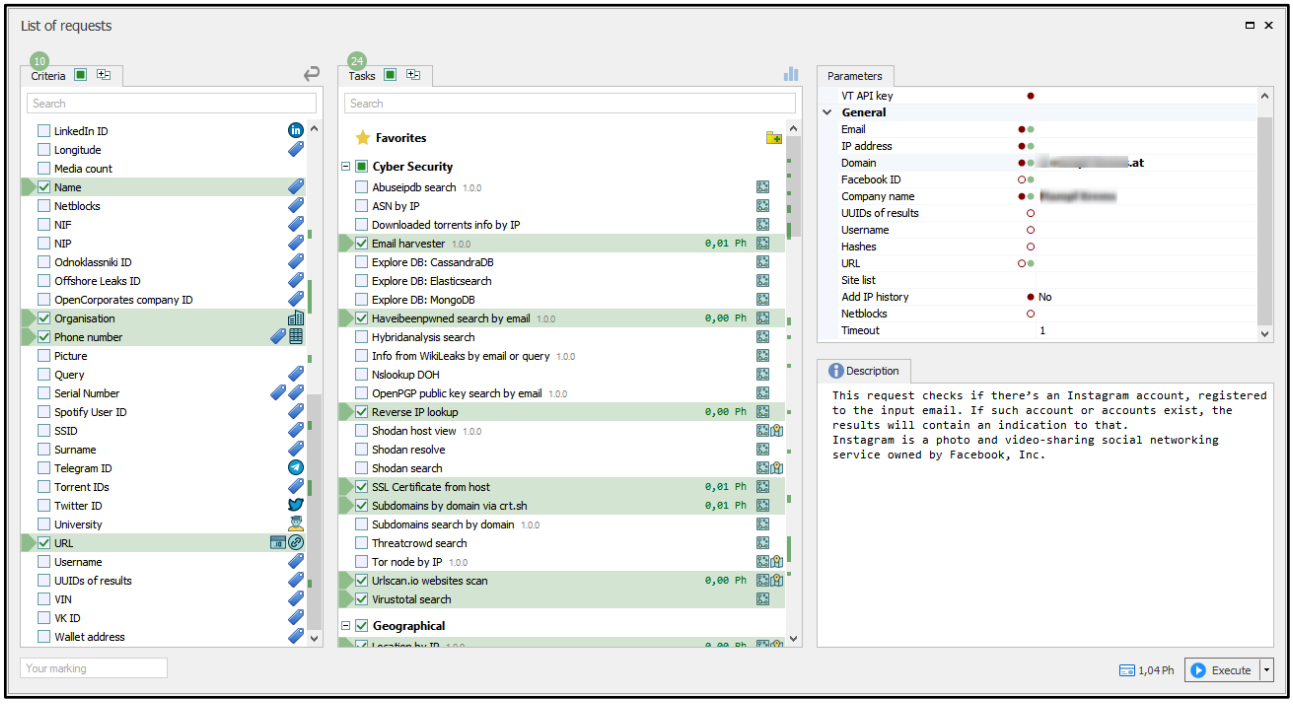


Abbildung 32: Lampyre List of Requests Suchparameter (anonymisiert) [134]

Im direkten Vergleich ist Maltego in der Anwendung übersichtlicher und strukturierter. Lampyre ist im Hinblick auf die Bedienbarkeit einfacher gehalten, die Darstellung der Ergebnisse erfolgt größtenteils in tabellarischer Form, graphische Abhängigkeiten sind nur vereinzelt möglich. Weiters ist die Applikation in der Anwendung teilweise instabil. So reagierten während der Anwendungstests unterschiedliche Ergebnis-Tabs plötzlich nicht mehr und waren nicht mehr auswählbar, die Ergebnisse somit nicht mehr einsehbar. Von den bereits beinhaltenen Plugins bietet Lampyre eine Auswahl an Suchkriterien, die in Maltego noch nicht auffindbar waren und umgekehrt. Darunter fielen bei Lampyre beispielsweise die Suche nach IMEI-Nummern, WLAN SSIDs, oder auch KFZ-Fahrgestellnummern (VIN), bei Maltego dafür beispielsweise die Wayback-Machine, Movie Database, Blockchain.info, oder Google Maps Geocoding, wobei diese in beiden Applikationen regelmäßig aktualisiert und erweitert werden. Innerhalb von Maltego sind die Herkünfte der Suchergebnisse und die Nutzung der Suchprovider nachvollziehbar. Woher Lampyre die Ergebnisse der Transformationen bezieht, ist auf den ersten Blick nicht zu erkennen, wenn der Suchprovider nicht in den Tasks beschrieben ist.
Bei den Transformationen zu der selben Zielorganisation konnten mit Maltego mit weniger bekannten Daten mehr Suchergebnisse erzielt werden. Die Zuverlässigkeit der Daten war ebenfalls in Maltego höher, so konnte beispielsweise der öffentliche Unternehmens-Facebook-Account mit Maltego aufgefunden werden, Lampyre hingegen lieferte bei diesen Transformationen Fehlermeldungen.

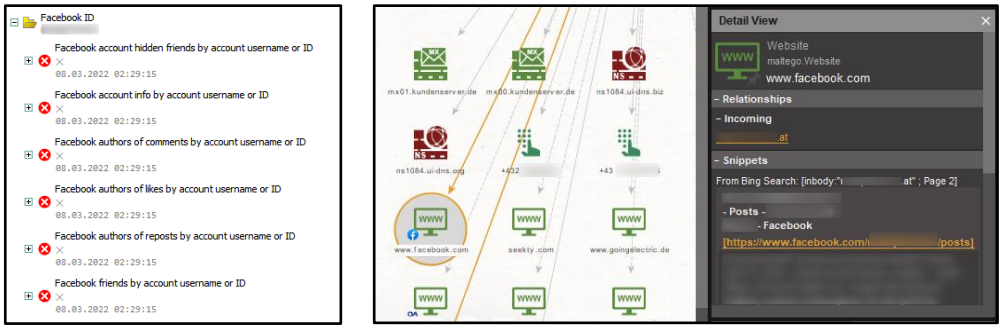


Abbildung 33: Vergleich Suchergebnisse Facebook-Unternehmensaccount (anonymisiert) [134], [132]

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
Maltego	Data-Mining-Tool mit einer Vielzahl an (automatisierten) Erweiterungsmöglichkeiten, die herstellerabhängig, separate Nutzungskosten für den Erhalt der API-Keys, zusätzlich zu den Lizenzkosten von höherwertigen Editionen von Maltego, auslösen können. Übersichtliche Darstellung und intuitives Handling, Exportmöglichkeit von Ergebnissen. Zuverlässigkeit und Anzahl der Suchergebnisse bereits in freien Lizenzmodellen sehr hoch.	[132]
Lampyre	Alternative zu Maltego. Wurde von einer OSINT-Community auf Twitter, nach einer Dekompilierung und Traffic-Analyse, sehr kritisch beurteilt. Intuitivität, Darstellung der Suchergebnisse und Performance haben Verbesserungspotenzial. Die Tabs der einzelnen Suchergebnisse reagieren manchmal nicht. Suchkriterien, die in Maltego nicht zur Verfügung stehen (beispielsweise VIN, Spotify User IDs, IMEI-Nummern).	[134] [135] [133]

Tabelle 11: Zusammenstelung Alternative zu Maltego

6.1.2.2. Suche nach Benutzer- und Personendaten

Um quer durch die diversen SNS-Plattformen nach Benutzernamen und Personendaten zu suchen, eigenen sich nicht nur die unter 6.1.1 beschriebenen Webapplikationen. Es gibt eine Reihe an Tools, die in einschlägigen Foren und Communities präsentiert und geteilt werden, welche gezielte Suchen über mehrere Suchmaschinen im Internet verteilen und die Ergebnisse automatisiert aufbereiten.
Das Enumerations-Tool *CrossLinked* [136] übernimmt die automatisierte Suche nach Personen und Benutzernamen innerhalb der Plattform LinkedIn. Die Suchergebnisse werden allerdings nicht direkt über die Plattform selbst, sondern über das Durchfiltern von Suchmaschinen-Ergebnissen, einem sogenannten „Search-Engine-Scraping“, zusammengestellt. Dies ermöglicht die Verwendung des Tools abseits der Plattform selbst, ohne Nutzung von API-Keys und ohne benötigte Anmeldedaten. Für die beispielhafte Anwendung des Tools wurde nach der Fachhochschule St. Pölten (fhstp) gesucht, da mit dieser eine größere Ergebnisanzahl erwartet wurde. Die Suche warf 242 Suchergebnisse aus, ein Ausschnitt davon ist, inklusive der Suchparameter, die zum Search-Engine-Scraping an die Suchmaschinen Google und Bing gerichtet wurden, in Abbildung 35 ersichtlich. Bei der Verifizierung der Ergebnisse zeigte sich, dass diese zwar plausibel (durch stichprobenartigen Vergleich der Ergebnisse mit dem online einsehbaren Mitarbeiterverzeichnis) waren, in den Suchergebnissen aber nicht nur Namen von Mitarbeiterinnen und Mitarbeitern gelistet wurden, sondern auch die von jeder Person, die in ihrem LinkedIn-Profil die Fachhochschule St. Pölten angegeben hat, was die Prüfung auf Korrektheit und Zuverlässigkeit erschwerte. Bei der Suche nach einer weiteren Organisation ohne Ergebnisse stellte sich heraus, dass auch Links der Suchmaschinen als Ergebnisse gewertet wurden (siehe Abbildung 34).

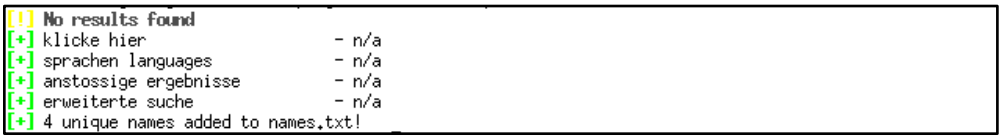


Abbildung 34: CrossLinked Suchergebnisse 1 (anonymisiert) [136]

Abbildung 35: CrossLinked Suchergebnisse 2 (anonymisiert) [136]

Die beiden ähnlich klingenden Tools *UserReCon* [137] und *Userrecon-py* [138], *Nexfil* [139], *Sherlock* [140], *Us3R-F1nD3R* [141] und *Thorndyke* [142] versprechen ähnliche Funktionalitäten, deren Suchumfänge sich über mehrere Hundert Social-Media-Plattformen erstrecken. Aus den tooleigenen Beschreibungen und Kommandoreferenzen geht hervor, dass Sherlock die einzige Applikation ist, die neben einer Sucheingabe auch mehrere, sowie vorbereitete Listen, in einem Suchlauf verarbeiten kann.
In der Anwendung und dem Aussehen sind sich die Tools sehr ähnlich, ebenso in den Ergebnissen, die sie während des Suchlaufes liefern (auszugsweise in Abbildung 38 bis Abbildung 40 dargestellt). Neben existenten Social-Media-Accounts konnte auch der Instagram-Testaccount *@dominikhatkeininsta*, den Suchergebnissen zufolge als registrierter Benutzer auf mehreren Plattformen aufgefunden werden. Da der Testaccount nur für Instagram erstellt wurde, kann davon ausgegangen werden, dass die Suchergebnisse, bis auf die Plattform Instagram, nicht valide sind. Dies bestätigte sich bei der Prüfung der Suchergebnisse, exemplarisch für die Plattformen Twitter und Reddit, in Abbildung 36 und Abbildung 37, dargestellt.

Abbildung 36: Verifikation der Ergebnisse auf Twitter [143]

Abbildung 37: Verifikation der Ergebnisse auf Reddit [144]

Abbildung 38: Exemplarische Suche in UserReCon (Auszug) [137]

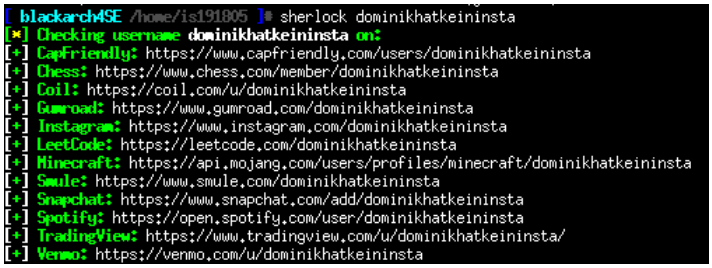


Abbildung 39: Exemplarische Suche in sherlock [140]

Abbildung 40: Exemplarische Suche in userrecon-py [138]

Buster [145] kann ebenfalls Benutzer auf Social-Media-Plattformen auffinden, der Suchumfang ist hier aber erweitert um die Enumeration und Generation von E-Mail-Adressen, die aus möglichen Databreaches, Pastes und Revers-Whois-Abfragen zur Verfügung gestellt werden. Buster zeigt in den Suchergebnissen auch die Quellen der Suchergebnisse an, da im Hintergrund unter anderem die Dienste von Hunter.io genutzt werden. Buster bietet laut eigener Beschreibung 200 Validationen pro Tag, diese waren allerdings zum Zeitpunkt der Versuche sehr schnell verbraucht. Die Validationen können, mit dem Hinterlegen der entsprechenden API-Keys der jeweils im Hintergrund genutzten Anbieter, erweitert werden.

Abbildung 41: buster Suchergebnisse (anonymisiert) [145]

Abbildung 41 zeigt die Anwendung von buster zur Enumeration von drei verschiedenen E-Mail-Adressen. Die Suchergebnisse im ersten Durchgang standen in keinem Zusammenhang mit der Suche. Die Suchergebnisse im zweiten Durchgang waren korrekt. Zu dem dritten Durchlauf konnten keine Ergebnisse erzielt werden.

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
CrossLinked	LinkedIn Benutzerenumerationstool. Funktionell vergleichbar mit einer Google-CSE, Suche nur innerhalb LinkedIn und nur via Google und Bing. Suchergebnisse plausibel, zur Weiterverwendung in der Datei `names.txt` im Anwendungsverzeichnis zwischengespeichert.	[136]
UserReCon	Suchen nach Benutzernamen in über 200 SNSs.	[137]
Userrecon-py	Suchen nach Benutzernamen in 187 SNSs.	[138]
Nexfil	Suchen nach Benutzernamen in 351 SNS. Verarbeitet auch mehrere kommagetrennte Eingaben und Listen mit Benutzernamen.	[139]
Sherlock	Suchen nach Benutzernamen in 323 SNSs.	[140]
Us3R-F1nD3R	Suchen nach Benutzernamen in 30 SNSs.	[141]
Thorndyke	Suchen nach Benutzernamen in 200 SNSs.	[142]
buster	Suchen nach Benutzeraccounts und Breaches in SNSs, inklusive Angabe des Fundortes, Generieren von Benutzernamen- und E-Mail-Adresskombinationen, Auffinden von registrierten E-Mail-Adressen in Social-Media-Accounts.	[145]

Tabelle 12: Zusammenstellung Suche nach Benutzer- und Personendaten

6.1.2.3. Technologiecheck

Auch in dieser Sektion gibt es, als Ergänzung oder Alternative zu den in 6.1.1 beschriebenen Webapplikationen, Werkzeuge, die technische Details zu Internetauftritten und Informationssystemen von potenziellen Social-Engineering-Angriffszielen liefern können, um entsprechende Pretexts und Impersonationen vorzubereiten.
TheHarvester [146] ist unter Kali-Linux-Distributionen bereits vorinstalliert und bietet Suchen nach Domaininformationen, sowie Google-Dorks in 38 verschiedenen Suchmaschinen, darunter Bing, Crtsh, DuckDuckGo, Google, Hunter.io, IntelX, securityTrails, Sublist3er, Virustotal, oder auch Zoomeye, an. Zur Nutzung werden entsprechende API-Keys benötigt, die Suchergebnisse können im Umfang eingeschränkt werden. Im Test haben unter der Version 4.0.3 die Suchmaschinen, trotz erneuter Installation des Tools, nicht einwandfrei funktioniert, unter Version 3.2.2 konnten zumindest via Google Suchergebnisse erzielt werden, die allerdings überwiegend nicht valide waren (Gegenüberstellung siehe nachfolgend unter Abbildung 42 und Abbildung 43).
Bei *Raccoon* [147] handelt es sich grundsätzlich eine Erweiterung des Tools *nmap* [148]. Das Tool ist noch im Entwicklungsstadium, der Fokus liegt auf Einfachheit. Der Komfort bei der Nutzung von Raccoon besteht darin, dass die Parametrisierung der nmap-Scans bereits durch das Tool vorgegeben ist. Neben den Möglichkeiten von nmap-Scans und der Subdomain-Enumeration soll Raccoon auch Cookies durchsuchen, Web-Application-Firewalls erkennen und Informationen zu CMS, Web-Server und Whois-Abfragen liefern können. In dem Test (ohne nmap-Scan) hat dies jedoch nicht funktioniert.
Eine stimmige Subdomain-Enumeration konnte, unter Verwendung von drei verschiedenen Domains, darunter die der Fachhochschule St. Pölten, mit *Sublist3r* [149], *Sn0int* [150] und *Frogy* [151] durchgeführt werden, wobei Frogy in den Enumerationen Sublister mitnutzt. Sublister bietet auch die Möglichkeit eines Portscans und eines Bruteforce-Scans, welche nicht ausgeführt wurden. Unter Sn0Int stellt die Subdomain-Enumeration nur einen kleinen Teil der Funktionalitäten dar, die mittels integriertem Paketmanager ständig erweitert werden können. Die Handhabe ist für Anfänger am Beginn nicht selbstverständlich, der Haupteinsatzzweck liegt den Entwicklern zufolge, aber auch im Penetration-Testing, des Bug-Bounties und der Schwachstellenanalyse.

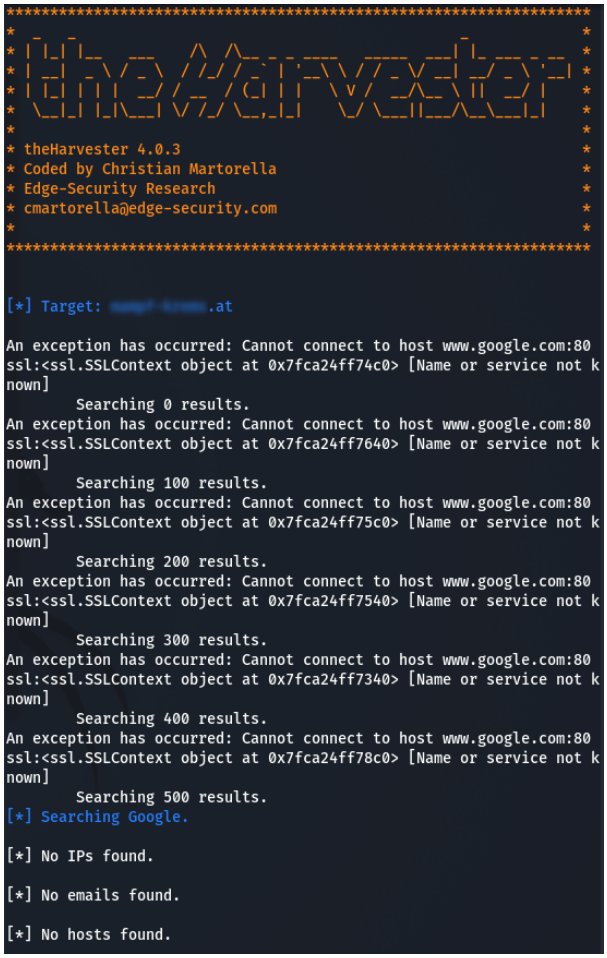


Abbildung 42: theHarvester 4.0.3 Suchergebnis (anonymisiert) [146]

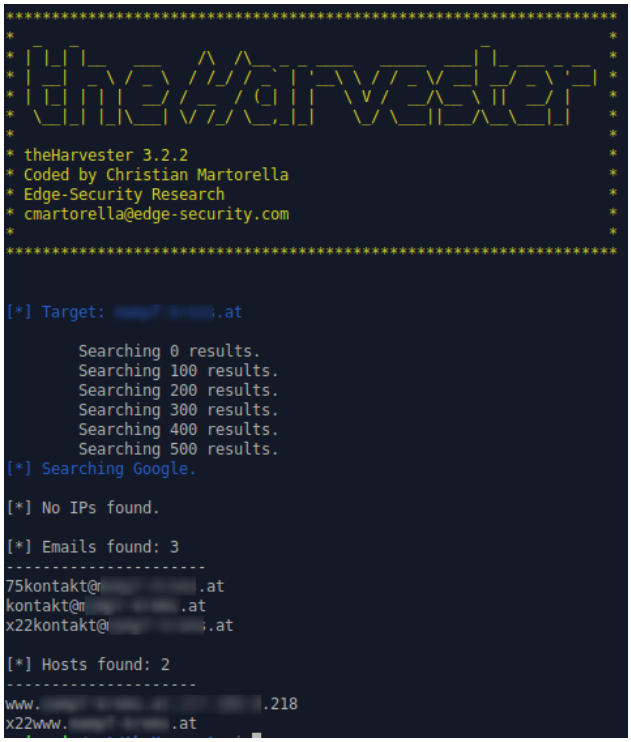


Abbildung 43: theHarvester 3.2.2 Suchergebnis (anonymisiert) [146]

Frogy befand sich, zum Zeitpunkt der Recherche und der Tests, ebenfalls noch in Entwicklung. Neben dem Auffinden von IPs, Domains und Subdomains soll es auch Live-Websites und Anmeldeportale auffinden. Besonders interessant ist an diesem Tool, dass es auf die Datenbank von Chaos. zugreifen kann, in welcher in dem vorhergehenden Kapitel 6.1.1.4 keine Registrierung ermöglicht werden konnte. Alle, durch die von Frogy verwendeten Plugins, werden am Ende in einer Datei „output.csv“ zusammengefasst.

Ein weiteres, in den sich mit Informationsbeschaffung beschäftigenden Communities und in dieser Sektion angeführte, vorgeschlagene Tool ist *ReconSpider* [152]. ReconSpider steht für die Kombination aus Reconnaissance und Spider und ist ein Tool zum automatisierten Scannen von IP- und E-Mail-Adressen, Webauftritten, Telefonnummern, DNS- und Domain-Informationen, aber auch zum Durchsuchen von Databreaches.

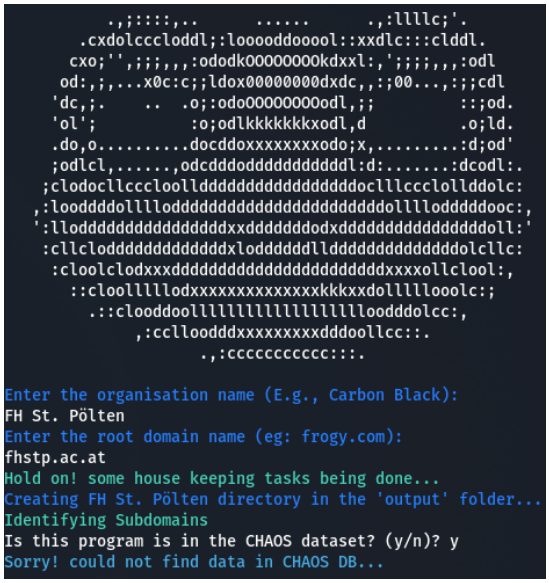


Abbildung 44: Frogy Abfrage in Chaos.-Datenbank [151]

ReconSpider konnte bei den Testeingaben durchgängig korrekte Daten zurückliefern, stürzte allerdings vereinzelt bei Eingaben in den Menüs zu Whois- und Domain-Abfragen mit Python-Fehlern ab.

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
theHarvester	Enumeration von Subdomains, findet E-Mail-Adressen, Virtualhosts, geöffnete Ports und Namen	[146]
Raccon	Enumeration von Subdomains, zeigt offene Ports und WAFs	[147]
Frogy	Attack-Surface-Management-Solution, scannt nach Domains, Subdomains, Websites und Login-Seiten.	[151]
Subli3ter	Subdomainlister, sucht nach Subdomains in Google, Yahoo, Bing, Baidu und Ask, enumeriert Subdomains mit Hilfe von Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.	[149]
ReconSpider	Ein Mix aus Reconnaissance-Tool und WebCrawler. Sucht beispielsweise nach IP-Adressen, Domains, Telefonnummern, Benutzernamen und Mailbreaches.	[152]
Sn0int	OSINT-Framework zum Sammeln von Domain-, DNS-, und E-Mail-Informationen aus Logs, Scans, aus Whois-Abfragen, oder Databreaches. Kann auch nach Benutzerprofilen auf Internetplattformen, sowie nach Telefonnummern und Bildern suchen.	[150]

Tabelle 13: Zusammenstellung Technologiecheck

6.1.2.4. Daten aus Social-Media-Profilen exportieren

ReconSpider, aus der vorherigen Sektion, kann bereits Informationen zu Facebook-, Twitter- und Instagram-Accounts anzeigen, diese sind allerdings auf den Namen, die Anzahl der Follower und die Profilbeschreibung limitiert und nicht exportierbar. Der Export von Informationen aus Social-Media-Profilen kann für Social-Engineering-Zwecke, zur weiteren Nutzung und Verarbeitung, erforderlich sein und kann mit den nachfolgend ausgewählten Werkzeugen erfolgen.
OSINTGram [153] erfordert das Hinterlegen eines gültigen Instagram-Accounts in den Konfigurationseinstellungen unter `/opt/Osintgram/config/credentials.ini`, um verwendbar zu sein. Das in der Anwendung sehr einfach gehaltene und intuitive Tool verlangt bei Start direkt nach einem Instagram-Zielaccount, um mit den Exporten beginnen zu können. Exportierbar sind, wahlweise in `*.txt` und `*.json` Dateiformate, alle Adressen, die aus gepostetem Bildmaterial ausgelesen werden können, alle Texte und Kommentare, die zu geposteten Bildern hinzugefügt wurden, die Anzahl der Follower des Zielaccounts, sowie die Anzahl der Accounts, welchen der Zielaccount folgt, Accountinformationen, sowie die Anzahl aller Likes, Hashtags, eine Liste aller Verlinkungen des Zielaccounts und eine Liste aller Accounts, die zu beliebiger Zeit Beiträge des Zielaccounts kommentiert haben. Besonders einfach ist mit dem Tool auch der Download von Stories und Multimedia-Inhalten des Zielaccounts. Gerade für Social-Engineering-Zwecke interessante Features stellen die Funktionen „*fwersemail*“, „*fwingsemail*“, „*fwersnumber*“ und „*fwingsnumber*“ dar, die jeweils eine Liste mit Telefonnummern und E-Mail-Adressen (insofern in den jeweiligen Accounts angegeben) der Followers, sowie der Followings, erstellt. In der Testanwendung mit dem Instagram-Account der Fachhochschule St. Pölten wurden mehrere Tausend Daten aufgefunden, der Export aus Zeitgründen abgebrochen. Mit einem privaten Testaccount konnten die durchgängig korrekten Informationen innerhalb kurzer Zeit in Listen bereitgestellt werden (anonymisiert dargestellt in Abbildung 45).

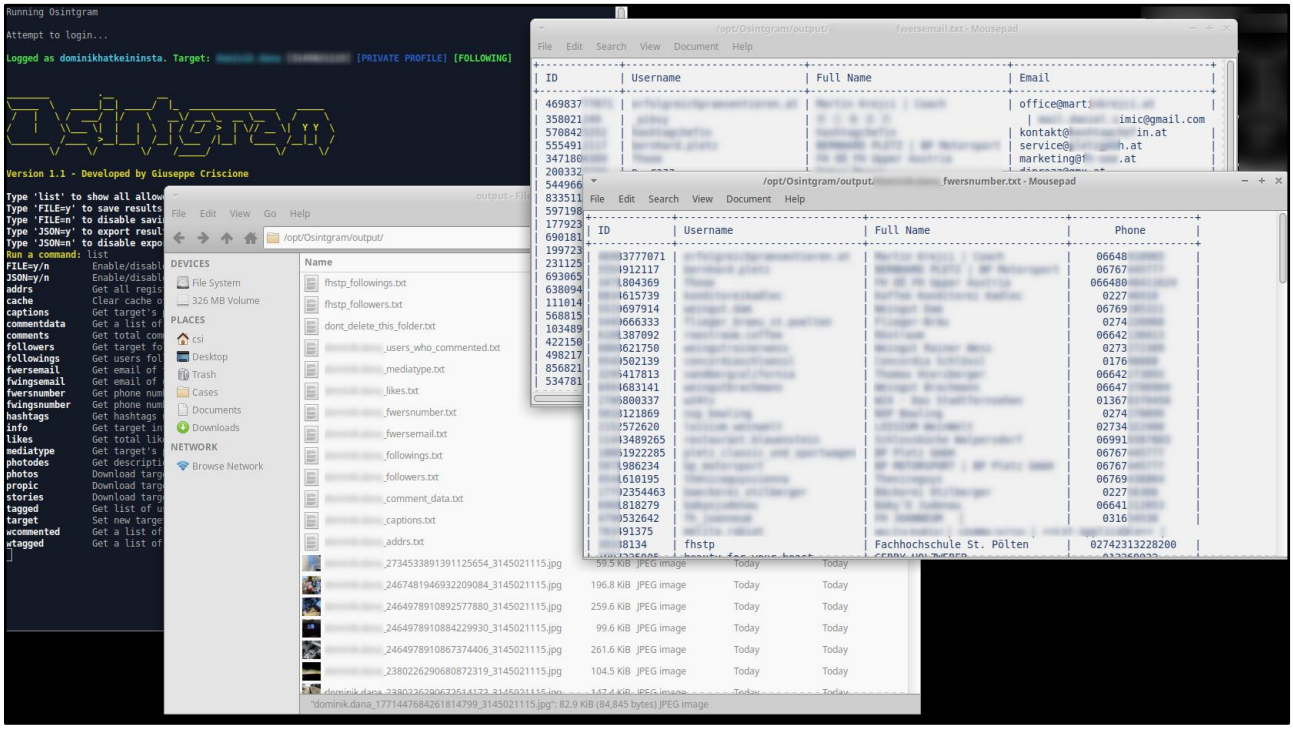


Abbildung 45: OSINTGram Suchergebnisse (anonymisiert) [153]

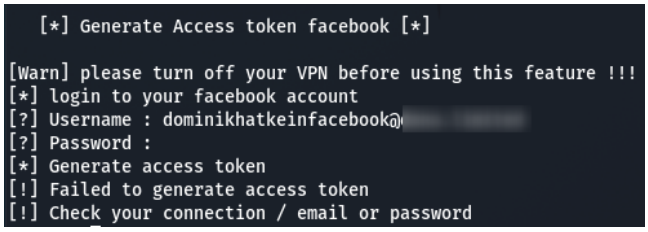


Abbildung 46: FBI Token-Generierung über Facebook-Graph-API (nicht funktional) [154]

In, zu OSINTGram ähnlicher Weise, hätte auch mit dem Tool *FBI* (Facebook Information) [154] auf der Social-Media-Plattform Facebook gearbeitet werden sollen. Es scheiterte im Test allerdings an der Generierung eines aktuellen und gültigen Access-Tokens für die Facebook-Graph-API, die von FBI angesteuert wird. Eine alternative Anmeldung anstatt des Access-Tokens war nicht möglich (laut Meta for Developers wird dazu ein Entwicklerkonto bei Facebook benötigt).

Sterra [155] exportiert ebenfalls Follower- und Following-Accounts, inklusive deren Account-ID, Benutzernamen, angegebenen Namen, der Biografie, Anzahl der Postings und Verlinkungen zu dem jeweiligen Account in CSV-Dateien. Innerhalb der Applikation ist es auch möglich Follower-Listen miteinander abzugleichen und so zu filtern, dass nur Gemeinsamkeiten, oder Unterschiede, übrigbleiben. Sterra ist in der Anwendung sehr komplex, daher gibt es auch ein eigenes Benutzerwiki dafür, in welchem die Funktionalitäten erklärt und anhand eines Beispiels gezeigt werden. Nachdem auch Sterra direkt mit der API von Instagram arbeitet, ist die Zuverlässigkeit der Daten gegeben.

Listenvergleiche können mit dem Python-Tool *Insta-Extract* [156] ebenfalls durchgeführt werden, diese sind in der Anwendung allerdings einfacher als innerhalb von Sterra, dafür nicht so umfangreich.

Was auf der Social-Media-Plattform Instagram in den Testanwendungen gut funktioniert, funktioniert mit zwei weiteren Applikationen auch auf der Plattform Twitter. *Twi1tter0s1nt* [157], auch unter den Bezeichnungen *TWINT* und *twosint* bekannt, bietet ziemlich die gleichen Funktionen auf der Commandline, die auch *TinfoLeak* [158], in einer GUI-Umgebung (Graphical User Interface) bietet. Dazu zählen das allgemeine Suchen nach Benutzernamen, suchen nach geocodierten Tweets (so sich die Geolokationsdaten in den Tweets auslesen lassen), Tweets in einem bestimmten Zeitfenster, Filtern nach speziellen Begriffen, aber auch das Exportieren der Anzahl an Followern. TWINT bietet, neben Exporten in mehrere Dateiformate, auch an, Tweets mittels

Google-Translate direkt in andere Sprachen zu übersetzen. Für das Scraping von Tweets kann mit dem Parameter „*min-wait-time*“ auch ein Zeitlimit zwischen den einzelnen Scrapes eingestellt werden.
TinfoLeak ist in der Anwendung mit der grafischen Oberfläche angenehmer zu bedienen, hier werden die gewünschten Operationen einfach angehakt und mit entsprechenden Werten oder Daten versehen. Abbildung 47 zeigt die exemplarische Analyse des Twitter-Accounts der Fachhochschule St. Pölten im Zeitraum zwischen 26. Februar bis 13. März 2022. Um den Report in einer ansehnlichen Größe zu halten, wurde die Anzahl der „Operations“ jeweils nur auf den Wert 50 beschränkt.

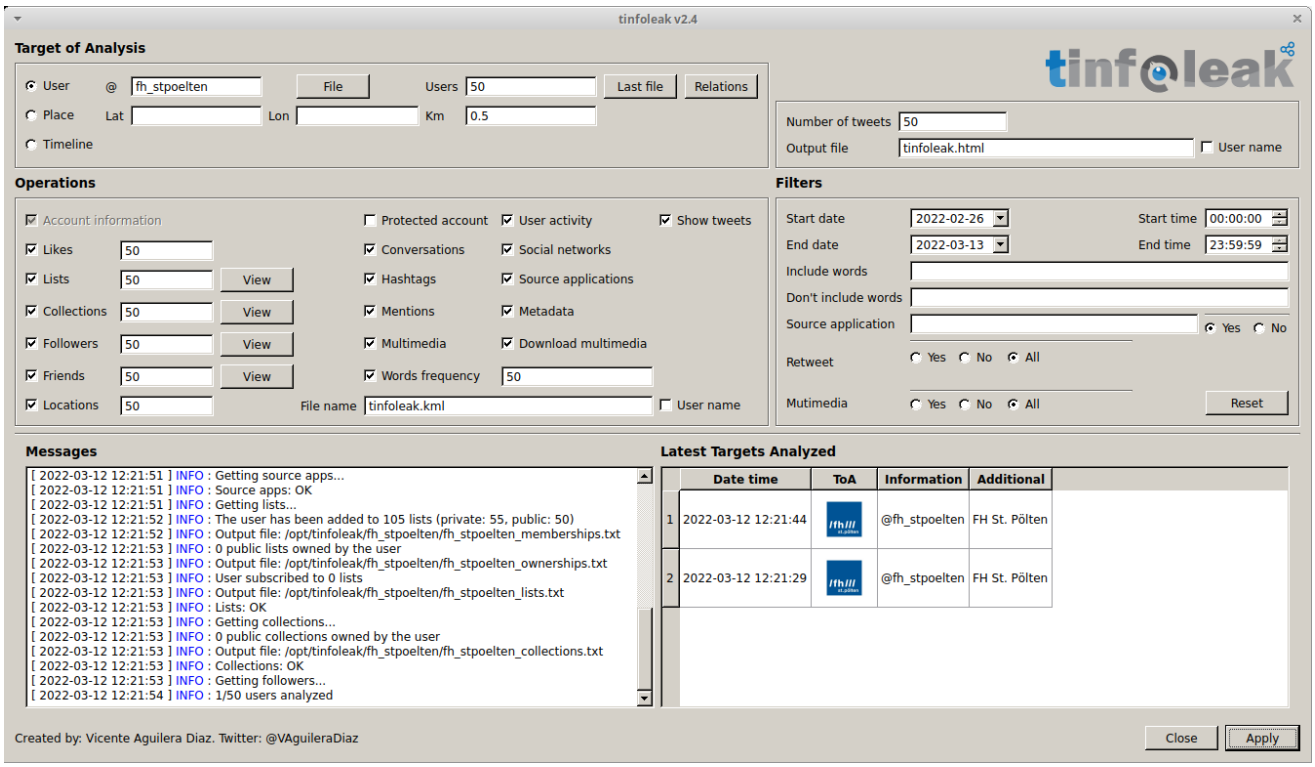
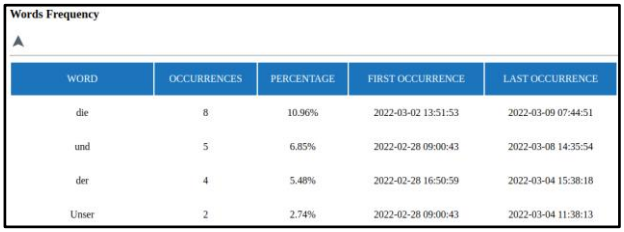


Abbildung 47: TinfoLeak Twitter-Analyselauf (anonymisiert) [158]

TinfoLeak stellt am Ende des Durchlaufes einen Report zusammen, in dem die Daten analysiert und aufbereitet einzusehen sind.
Am Beispiel des Twitter-Accounts *@fh_stpoelten* ist zu erkennen, dass in dem analysierten Zeitfenster die häufigsten Tweets um 13:00 Uhr getätigt wurden (siehe Abbildung 50), die drei am häufigsten vorkommenden Wörter „*die*“, „*und*“, sowie „*der*“ waren (siehe Abbildung 48) und mehr getweetet, als gelikt wurde (siehe Abbildung 49).



WORD	OCCURRENCES	PERCENTAGE	FIRST OCCURRENCE	LAST OCCURRENCE
die	8	10.96%	2022-03-02 13:51:53	2022-03-09 07:44:51
und	5	6.85%	2022-02-28 09:00:43	2022-03-08 14:35:54
der	4	5.48%	2022-02-28 16:50:59	2022-03-04 15:38:18
Unser	2	2.74%	2022-02-28 09:00:43	2022-03-04 11:38:13

Abbildung 48: Am häufigsten verwendete Wörter in den Tweets von @fh_stpoelten [158]

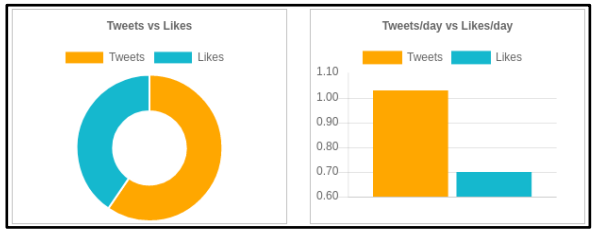


Abbildung 49: Verhältnis Tweets vs. Likes von @fh_stpoelten [158]

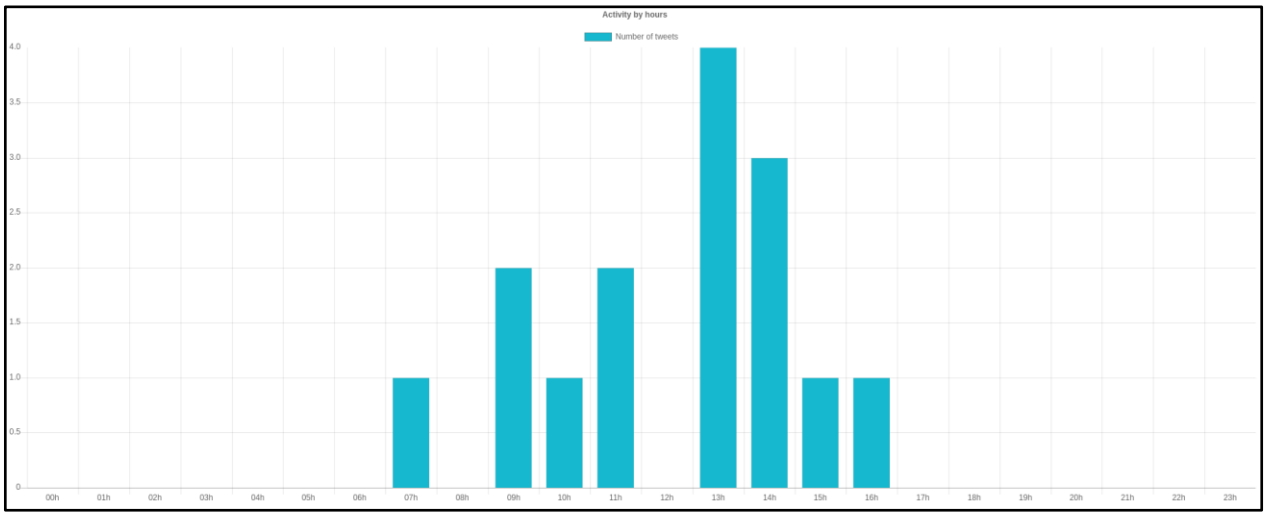


Abbildung 50: Aktivität nach Uhrzeit von @fh_stpoelten [158]

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
OSINTGram	Instagram Information-Gathering-Tool zum Sammeln und Downloaden von Instagram-Profilinhalten (Bildbeschreibungen, Followers und Followings, inklusive hinterlegter E-Mail-Adressen, Hashtags, Herunterladen von Fotos, Stories, Profilbildern, Kommentaren und Tags) via Commandline-Interface (CLI).	[153]
Sterra	Exportieren von Followers und Followings, sowie gemeinsame Kontakte in CSV-Dateien. Analyse-, Filter- und Vergleichsmöglichkeiten zwischen verschiedenen Follower-Exports.	[155]
Insta-Extract	Commandline-Tool zum Scrapen und Exportieren von allgemeinen Benutzerinformationen, Postings, den Benutzernamen der Follwers und der Followings.	[156]
Tw1tter0s1nt / TWINT	Suchen nach Twitter-Benutzern (auch gesperrten), Suchen nach Keywords, nach Telefonnummern und E-Mail-Adressen. Scrapen von Tweets und Antworten, Auslesen von Followern und Followings eines Zielaccounts.	[157]
Tinfoleak	Grafische Anwendung zum Extrahieren und Erstellen eines Reports über Twitter-Accounts. Extrahiert Kontoinformationen und -aktivitäten, Hashtags, Erwähnungen, Likes, Worthäufigkeiten, Medien, Metadaten, Geo-Location, markierte Benutzer und Follower.	[158]

Tabelle 14: Zusammenstellung Daten aus Social-Media-Profilen exportieren

6.1.3. Betriebsfertige Systemumgebungen

Die Phase der Informationsbeschaffung ist durch eine Vielzahl an verfügbaren Applikationen sehr umfangreich. Automation wird größtenteils versucht, innerhalb einer Anwendung zu schaffen, um Zeit und Aufwände durch wiederkehrende Tätigkeiten und Abfragen, zu automatisieren (beispielsweise die gleichen Suchen nach verschiedenen Benutzernamen auf Social-Media-Plattformen) und positiv zu beeinflussen.
Anwendungen wie Maltego und Lampyre versuchen mit Plugins verschiedener Hersteller und Entwickler, Automation mit verschiedenen und unterschiedlichen Suchabfragen, innerhalb der eigenen Applikation zu bieten.
Während der Recherche nach Social-Engineering-Tools mit Automation und Möglichkeiten dafür, konnten auch zwei Linux Distributionen ausfindig gemacht werden, mit denen zwar keine vollständige Automation in dem Prozess der Informationsbeschaffung geschaffen werden kann, allerdings die Aufwände durch die komfortable Bedienung damit stark vereinfacht wird.

6.1.3.1. Tsurugi-Linux

Ähnlich wie die Linux-Distributionen Kali und BlackArch, ist die betriebsfertige Distribution des *Tsurugi-Linux-Projekts* [41] aufgebaut. Die Distribution ist vollständig kostenlos und beinhaltet eine Vielzahl an Werkzeugen, die für Zwecke der Digitalforensik und Malwareanalyse genutzt werden können. Die Distribution setzt auf Ubuntu 20.04 LTS auf und wird in drei Versionen zum Download angeboten. Zwei der drei Versionen stehen als Live-System zur Verfügung, die dritte Version kann als fertiges Image für Oracle VirtualBox heruntergeladen werden. Unter Tsurugi wird ein von japanischen Mönchen verwendetes Doppelklingenschwert verstanden. Die Metapher der Doppelklinge wurde auch in die Distribution übertragen, so gibt es einen Profile-Switcher, der von der Digitalforensik-Umgebung zur OSINT-Umgebung umschaltet und damit bequem zahlreiche Werkzeuge für Informationgathering- und Reconnaissancezwecke im Startmenü mit nur wenigen Mausklicks zur Verfügung stellt.
Eine Liste vorinstallierter Tools ist unter [41] einsehbar, einige davon wurden, unabhängig von dieser Distribution, auch in der vorliegenden Arbeit thematisiert. Die Werkzeuge müssen, ähnlich wie bei Kali und BlackArch, zwar manuell gestartet werden, der Bedienkomfort durch den Profile-Switcher ist allerdings erhöht und vereinfacht so den Prozess der Informationsbeschaffung.

6.1.3.2. CSI-Linux

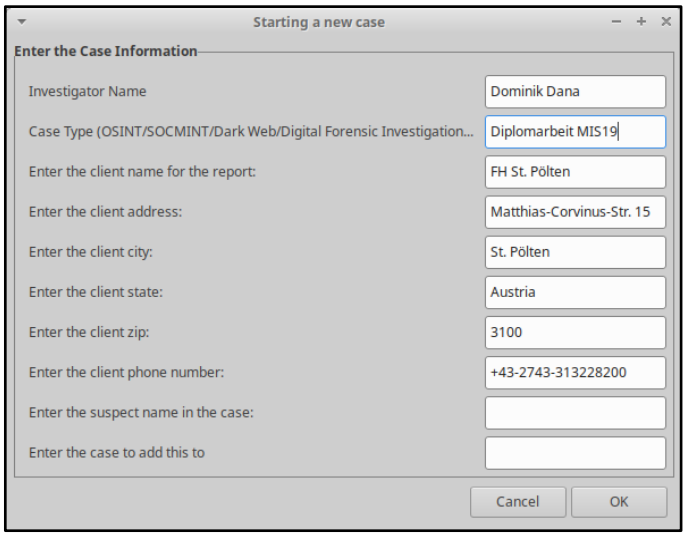


Abbildung 51: CSI-Linux Neuer Case

Ebenfalls auf Digitalforensik ausgelegt ist die Linux Distribution *CSI-Linux* [40]. CSI-Linux optimiert die Zeit und den Aufwand innerhalb des Prozesses der Informationsbeschaffung, indem es über mehrere, ebenfalls in dieser Arbeit bereits thematisierte Werkzeuge, mit einem sogenannten „Case Management“ ein bereits vorparametrisiertes Starten von Applikationen ermöglicht und mit diesem auch die Suchergebnisse übersichtlich in einer entsprechenden Ordnerstruktur ablegt.
Jeder neue Investigationsprozesses startet mit dem Anlegen eines neuen Casefiles (Abbildung 51), nach dem die gewünschte Art der Investigation ausgewählt wird.

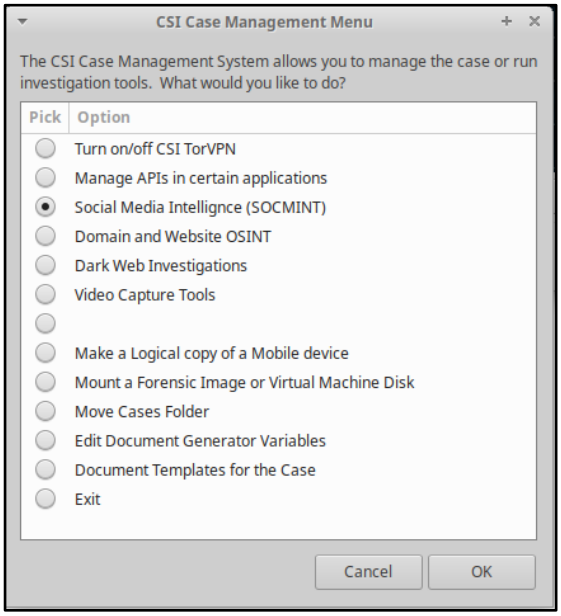


Abbildung 52: CSI-Linux Case-Management

Dies kann beispielsweise „Social Media Intelligence (SOCMINT), wie in Abbildung 52 dargestellt sein.
Der jeweilige Launcher ist dabei, auch bei Auswahl einer anderen Investigation (beispielsweise „Domain and Website OSINT“), so einfach gehalten, dass nur ausgewählt werden muss, wonach gesucht werden möchte.
Eine spezielle Kenntnis an und in Programmen und Anwendungen, sowie an zur Verwendung nötigen Parameter, ist damit nicht erforderlich. Exemplarisch ist der Launcher für eine SOCMINT-Investigation nachfolgend in Abbildung 53 dargestellt.
Einfach und übersichtlich gehalten ist mit dieser workflowähnlichen Bedienoberfläche auch das Handling von teilweise kostenpflichtigen API-Keys. Ein Hinzufügen, Austauschen, oder Entfernen von Keys ist komfortabel mit wenigen Mausklicks möglich.

Abbildung 53: CSI-Linux SOCMINT Investigation

CSI-Linux ist ebenfalls als importierfertiges Image für Oracle VirtualBox verfügbar. Zusätzlich wird es auch als bootfähiges Image, in Form eines forensischen RAW-Images, angeboten. Zur Unterstützung gibt es unter [40] auch Anleitungsvideos und Walkthrougs zu verschiedenen Anwendungszwecken.

6.2. Tools in der Phase Angriffsvorbereitung

In der Phase der Angriffsvorbereitung sind jene Tools inbegriffen die, abhängig von dem gewählten Angriffsszenario, für tatsächliche Angriffe vorbereitend wirken können. Beispielsweise zählt hierzu das Vorbereiten von Payloads, die dann in der tatsächlichen Angriffsphase genutzt werden. Auch das Vorbereiten von Texten, für im weiteren Verlauf auszusendende Phishing-Nachrichten, oder das Vorbereiten von Bots, kann hier erfolgen. Die Auswahl der nachfolgenden Möglichkeiten wurden im Zuge der Recherchen für Tools, Angriffe und Angriffstechniken im Social Engineering, als vorbereitend bewertet und geclustert.

6.2.1. Payloads vorbereiten

Um, bereits in der Einführung beschriebenes, Baiting für Social-Engineering-Zwecke einsetzen zu können, bedarf es einer Vorbereitung von entsprechenden Payloads, die auf beispielsweise USB-Datenträger aufgespielt werden. Die Payload bezeichnet in diesem Fall den Schadcode, der sich bei Auslesen des Datenträgers selbstständig aktiviert, oder sich hinter einer Datei verbirgt und ausgeführt wird, sobald die Zielpersonen diese versucht auszuführen oder zu öffnen.
Um entsprechende Payloads vorzubereiten, können einerseits bereits fertig generierte und zur Verfügung gestellte Versionen, wie beispielsweise unter [159], gelistet, genutzt werden, oder mit eigenen Tools neue generiert werden. Dafür eignet sich, neben einem der bekanntesten Tools, dem Social-Engineering-Toolkit (SET) [160], auch das von Matt Nelson und Matt Robinson entworfene PowerShell-Skript [161], welches nach Durchlauf ein Excel-Dokument erstellt, das bei Aufruf auf dem Zielsystem eine Meterpreter-Shell erstellt. Weiters persistiert es sich in der Windows-Registry und im Benutzerverzeichnis, um bei Systemneustarts erneut ausgeführt zu werden. Eine Verbindung zu dem infizierten System kann via Meterpreter Reverse HTTP und HTTPS hergestellt werden.
Das Tool *MacroPack* von Emeric Nasi [162] ist aktueller und im Funktionsumfang, verglichen mit dem PowerShell-Skript, erweitert und benötigt auf dem System, auf dem die Payload in eine Office-Datei integriert werden soll, eine funktionierende und registrierte Office-Installation. Das Tool bietet zusätzlich den Service von Code-Obfuscation, sodass der Schadcode in den Office-Markos nicht so einfach erkennbar ist und unterstützt in der Community-Version sämtliche Microsoft Office-Dokumentenversionen und Verknüpfungsdateien. Die Pro Version bietet noch einen erweiterteren Funktionsumfang, sowie die Anwendung auf bereits bestehenden Office Dateien.
Bei den Tests hat das Generieren der Payloads mit dem PowerShell-Skript, trotz Änderung in den Ausführungsrichtlinien, welche die Ausführung des Skripts ursprünglich unterbunden haben, nicht funktioniert. Für die Ausführung und Verwendung von MacroPack empfiehlt es sich, die Windows-Sicherheitseinstellungen anzupassen, da diese eine Ausführung verhindern und das Tool als schwerwiegende Bedrohung einstufen.

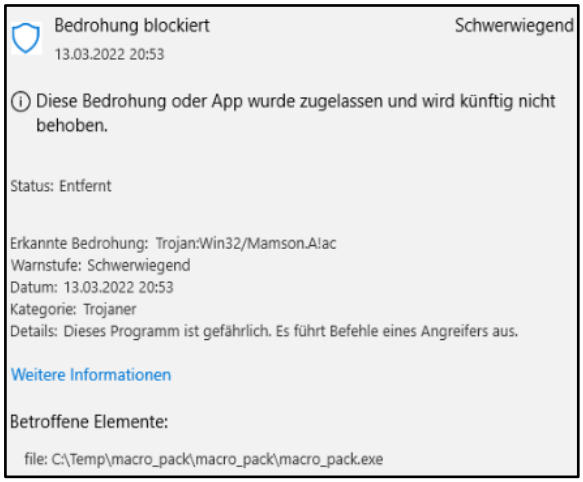


Abbildung 54: Blockierung MacroPack durch Windows Sicherheit

Das Erstellen einer geeigneten Payload für den Test von MakroPack, konnte im Praxistest, aufgrund einer fehlenden Microsoft Office-Lizenz auf dem Testsystem, nicht durchgeführt werden.
Das, während der Recherche in einem Forum erwähnte, Tool *Social_X* [163], welches Trojaner mit einer eigenen Reverse-Shell und in Form einer `*.exe` Datei generieren und das Icon nach Wunsch anpassen können sollte, konnte unerwartet nicht korrekt installiert werden und terminierte bei mehreren Startversuchen. Dokumentationen zu dem Tool waren, zum Zeitpunkt der Tests, nicht vorhanden und ein dazu verlinktes YouTube-Video nicht mehr verfügbar. Social_X wird daher an dieser Stelle nur als weitere Möglichkeit aufgezählt, da der letzte Commit auf GitHub nur wenige Monate alt war und der Fehler möglicherweise in einem nächsten Commit behoben sein könnte.
SET [160], welches in jeder aktuellen Installation von Kali-Linux beinhalten ist, bietet in dem Untermenü „*1) Social-Engineering Attacks*“ die Möglichkeit, automatisiert Datenträger so zu manipulieren, dass Schadcode auf Wechseldatenträgern über die Autorun-Funktion automatisch ausgeführt werden kann (Submenü „3) *Infectious Media Generator*“). Dies kann über eine ausführbare Datei, die über die auf dem Wechseldatenträger beinhaltene Datei `autorun.inf` ausgeführt werden, oder über einen Dateiformat-Exploit, um eventuelle Sicherheitswarnungen zu umgehen. TrustSec stellt unter [164] eine detaillierte Dokumentation zu SET bereit, in der jede Funktion durchgegangen, gezeigt und beschrieben wird. Die Anwendung von SET war zum Zeitpunkt der Verfassung der Arbeit bereits bekannt und in Kombination mit der Dokumentation von TrustSec einfach und zuverlässig möglich.

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
SET - Social Engineering Toolkit	Eines der bekanntesten OpenSource Social-Engineering-Werkzeuge, für Social-Engineering- und Penetration-Tests entwickelt. Integrierter Infections-Media- und Payload-Generator.	[160] [164] [165]
PowerShell Skript zur Generierung von Excel-VBA-Makro	PowerShell-Skript, das Excel-Dateien mit einem VBA-Makro mit Persistenz erzeugt. Zugriff mit Meterpreter über HTTP und HTTPS.	[161]
Office VBA MacroPack	Macro-Pack-Build-Tool, das automatisiert Office-Dateien nach Wahl mit integrierten Payloads für Zugriffe über Meterpreter erstellt. Inkludiert Obfuscation-Funktionen im VBA- und VBS-Code.	[162]
USB-Rubber-Ducky Payloads	USB-Rubber-Ducky Vorlagen für Windows 7-11 (zirka 70 Stück) und Mac OSX (zirka 15 Stück).	[159]
Social_X	Generator für Trojaner, der ausführbare `*.exe` Dateien mit entsprechenden Icons von Bild-, oder Officedateien generiert.	[163]

Tabelle 15: Zusammenstellung Payloads vorbereiten

6.2.2. Tonfälle und Emotionen in Texten prüfen und bewerten

Um Nachrichten, oder schriftlich verfasste Vorwände, auf die Wirkung von Emotionen zu prüfen, wurde während der Recherche zu automatisierten Social-Engineering-Werkzeugen der Tone Analyzer [166], [167] von IBM getestet.
Der Tone Analyzer ist online in einem Webformular frei testbar und erkennt über, via MachineLearning-Analyse eines eingegebenen Textes, die darin vorkommenden Emotionen und Tonfälle. Die Node.js-Version des Tone Analyzers [167] bietet, nach Registrierung in der IBM Developer Cloud, für die ersten 1000 API-Aufrufe im Monat kostenfreie Analysen und Unterstützung von mehreren Sprachen und Dateien, direkt an.

Zum Testen der Analyse wurden die nachstehenden Beispieltexte zur Analyse eingegeben:

- Positive Emotion: *"Dominik likes doing his master thesis all night long :-)"*
- Negative Emotion: *"Dominik does not like doing his master thesis all night long :-("*

Die Analysen, dargestellt in Abbildung 55 bis Abbildung 57, nahm Tone Analyzer mit den Bereichen „*Confident*", „*Joy*" und „*Sadness*" vor und klassifizierte die Stärke der Ausdrücke in den Nachrichten mit unterschiedlich starken Farben.

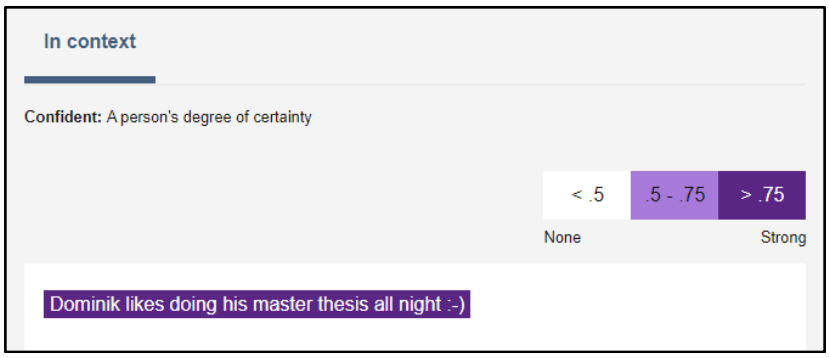


Abbildung 55: Tone Analyzer Analyse „Confident" [166]

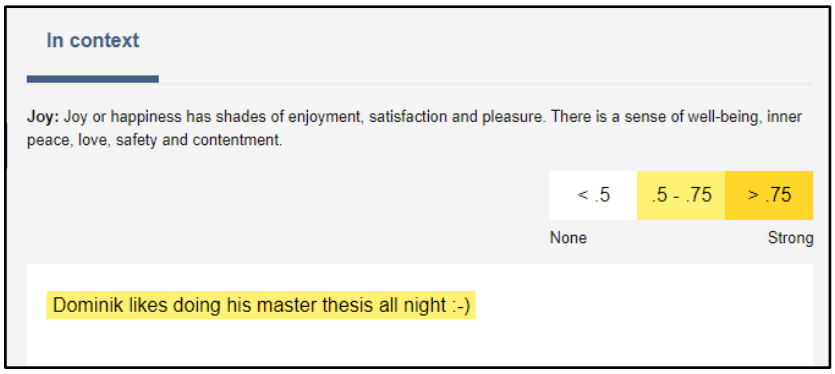


Abbildung 56: Tone Analyzer Analyse „Joy" [166]

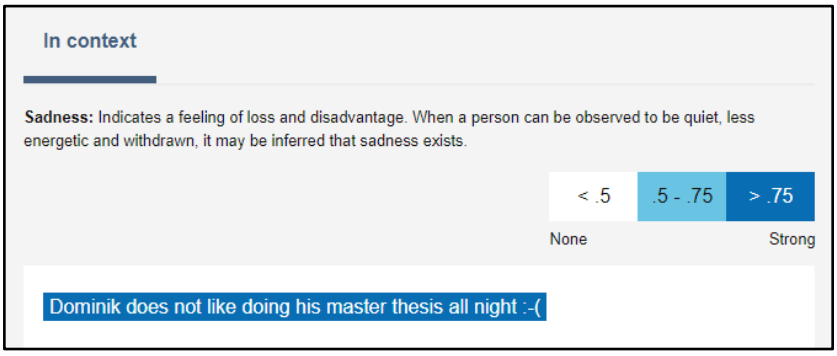


Abbildung 57: Tone Analyzer Analyse „Sadness" [166]

In weiteren Tests, mit unterschiedlichen Textfragmenten, klassifizierte Tone Analyzer auch in Richtung „Analytical“ und „Tentative“. Die Node.js-Version des Tone Analyzers wurde in dieser Versuchsreihe, mangels IBM Developer Account, nicht getestet.

6.2.3. Vorbereiten von Bots

Teile eines Social-Engineering-Angriffs können, je nachdem welches Ziel und welches Angriffsszenario ausgewählt wurde, auch durch Bots übernommen werden. Die nachfolgenden Nennungen stellen dar, wie und dass dies bereits möglich ist, sind aber weder für bösartige Einsatzzwecke entwickelt noch für einen solchen Einsatz angedacht worden.
Ähnliche Implementierungen von Twitter-Bots, nach Vorlage von beispielsweise *Realboy* [75], oder *SNAP_R* [55], können in der Phase der Angriffsausführung zum automatisierten Streuen von Phishing-Links genutzt werden. In der Phase der Angriffsvorbereitung können entsprechende Twitter-Accounts erstellt, mit Content gefüllt und mit einem Netzwerk an Followern und Follows ausgestattet, zu mehr Glaubhaftigkeit geführt werden. Beide Bots, Realboy als auch SNAP_R, wurden in der Arbeit nicht getestet und evaluiert, da dies bereits in verwandten Arbeiten, welche in der Literaturanalyse am Beginn der Arbeit bereits Erwähnung fanden, gemacht wurde.

Erwähnte Bots in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
Realboy	Twitter-Bot der auf Twitter selbst agiert.	[75]
SNAP_R	Twitter-Bot der auf bestimmte Hashtags reagiert, auf Unterhaltungen antworten und Phishing-Links verteilen kann.	[55]

Tabelle 16: Zusammenstellung Vorbereiten von Bots

6.3. Tools in der Phase Angriffsausführung

In der Phase der Angriffsausführung finden sich all diejenigen Tools, die direkt ausgeführt einen Social-Engineering-Angriff durchführen können. Während der Recherche zu entsprechenden Tools hat sich herausgestellt, dass bei den Angriffstools Automation fast nur in Richtung Phishing mit Website-Cloning, Massenmails und vereinzelt auch dem Einsatz von Bots, beschrieben wird.

6.3.1. Phishing mit Website-Cloning

SET [160] bietet im Hauptmenü unter „*1) Social-Engineering Attacks*“, in dem Untermenü „*2) Website Attack Vectors*“ die Möglichkeit, entweder mit Auswahl „*3) Credential Harvester Attack Method*“, oder mit Auswahl „*6) Multi-Attack Web Method*“, eine beliebige Website in eine Internetseite mit Phishing, oder mit multiplen Angriffsmethoden, zu klonen. Die geklonte Seite ist direkt nach Eingabe einsatzbereit, die eingegebenen Benutzerdaten werden direkt auf der Commandline eingefärbt eingeblendet (siehe Abbildung 58).
Ähnlich, auch in Bezug auf das Website-Cloning, funktioniert *Zphisher* [168], welcher exemplarisch und zum Vergleich der Ähnlichkeit mit SET in Abbildung 59, Benutzerdaten von einer von Netflix geklonte Internetseite übertragen bekommt und diese in einer Protokolldatei im Arbeitsverzeichnis abspeichert.
Im Unterschied zu SET bietet Zphisher allerdings nur fertige Vorlagen für Phishing-Seiten an und kein Klonen von individuellen Seiten. Dies ist auch bei *phishEye* [169] so der Fall.

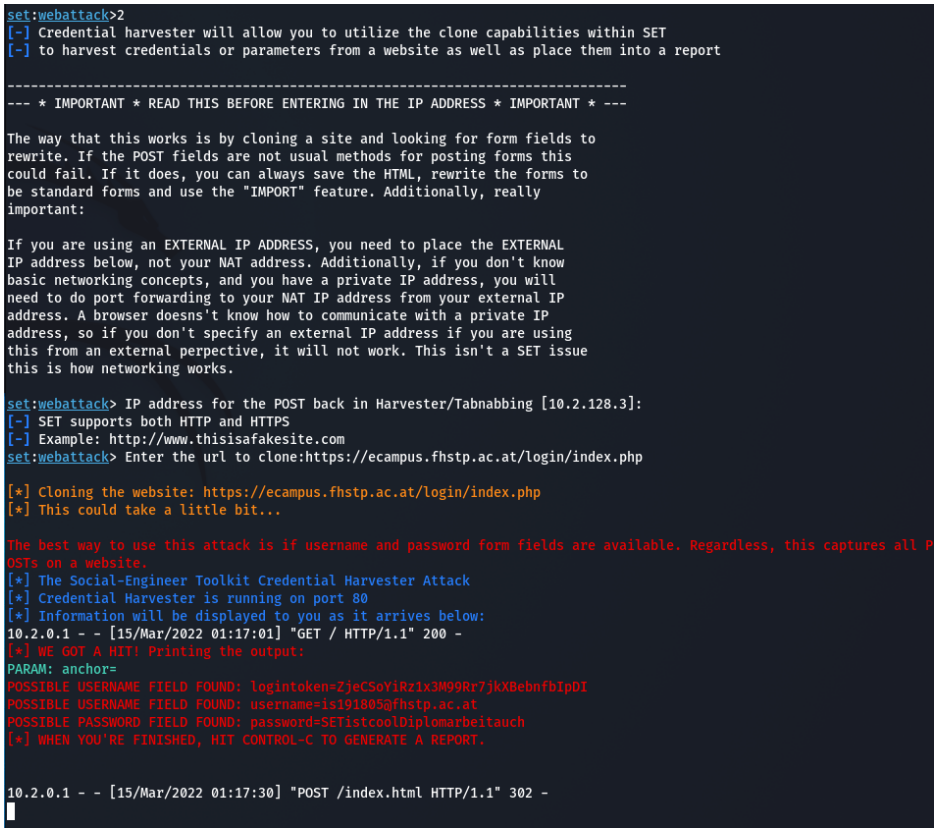


Abbildung 58: SET Siteclone mit Credential-Harvesting [165]

Abbildung 59: Zphisher Siteclone mit Credential-Harvesting [168]

PhishEye bietet allerdings, als einziges der gelisteten Tools, die Möglichkeit Websites auch für mobile Geräte zu klonen.
Bei den Anwendungstests konnte festgestellt werden, dass *Blackeye* [170] zwar eine Reihe an Vorlagen der Social-Media-Plattformen mitbringt, diese konnten jedoch nicht direkt getestet werden, da bei der Generation der Phishing-Links immer ein Fehler aufgetreten ist und keine Links generiert, beziehungsweise für die Nutzung ausgegeben, wurden. *SocialFish* [171] konnte ebenfalls nicht zur Gänze getestet und evaluiert werden, da es bei Start der Applikation, trotz aller installierten Requirements und Abhängigkeiten, zu Modul-Error-Meldungen innerhalb der Hauptanwendung gekommen ist. Die Dokumentation zu der App ist in dem Repository nur sehr kurz und rudimentär gehalten, daher konnte der Fehler nicht behoben werden. Ein erneutes Klonen des GitHub-Repository brachte ebenfalls keine Abhilfe.
Mit *StormBreaker* [172] wird die Liste der in diesem Unterkapitel genannten Phishing-Tools um ein Tool erweitert, das zwar keine Websites, wie die anderen bislang genannten Tools klonen kann, dafür aber mit maximal zwei Eingaben, Seiten und Links mit Hilfe von Ngrok generiert, die den Zugriff auf Kamera, Mikrofon und Lokationsdaten der Endgeräte ermöglichen. Die Lokationsdaten werden mit einer Google-Maps-Verknüpfung zurückgeliefert. Abbildung 60 zeigt StormBreaker bei Zugriff auf die Kamera des Endgerätes einer potenziellen Zielperson.

Abbildung 60: Storm-Breaker Zugriff auf Kamera [172]

Zusätzlich bietet StormBreaker eine Funktion „*OS Password Grabber*“, die eingegebene Passwörter übertragen soll. Während der Tests gab es in diesem Funktionsteil Schwierigkeiten, da entweder die zu verschickenden Links nicht generiert wurden oder die Anwendung nicht auf Eingaben reagiert hat.
Die Funktionalität der Zugriffe auf Mikrofon, Kamera, sowie auf die Positionsdaten des Endgeräts der potenziellen Zielperson, sind allerdings nur dann möglich, wenn bei Aufruf der Seite sämtliche angezeigte Phishing-Warnungen der aktuellen Browsergenerationen ignoriert, sowie die Berechtigung zum Zugriff auf Mikrofon, Kamera oder Standort, entsprechend gewährt wird.

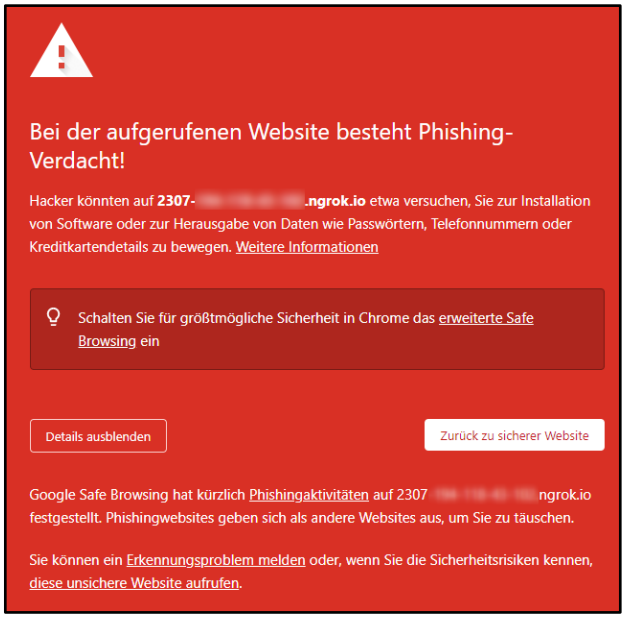


Abbildung 61: Browser Phishing-Warnung (Chrome)

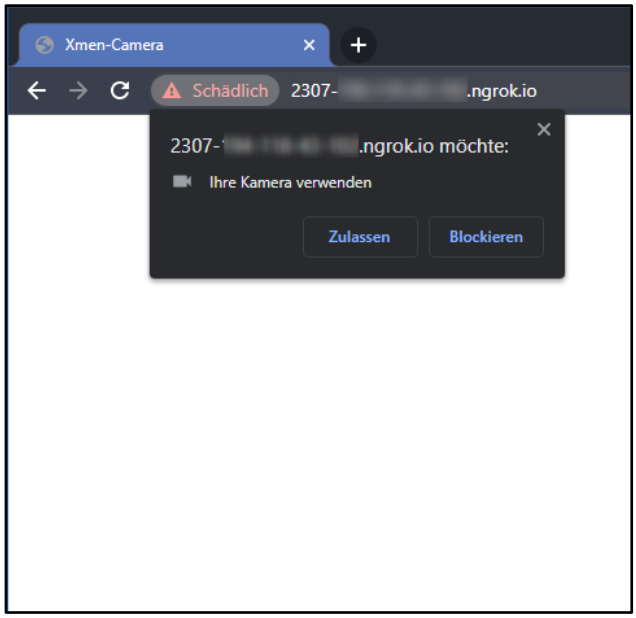


Abbildung 62: Browser Zugriffswarnung (Chrome)

Genutzte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
SET - Social Engineering Toolkit	Eines der bekanntesten OpenSource Social-Engineering-Werkzeuge, für Social-Engineering- und Penetration-Tests entwickelt. Integriertes Website-Cloning, Spear-Phishing und Mass-Mail-Attack-Framework.	[160] [164] [165]
StormBreaker	Zugriff auf Kamera, Mikrofon, Tastenanschläge und Positionsdaten über Versenden eines Links. Payload und fertiger Link zum Versand automatisiert.	[172]
Zphisher	Automatisiertes Phishing-Tool mit Website-Cloner für viele populäre Internetseiten (Facebook, Google, Netflix und vieles mehr). Generiert automatisch funktionierende Cloud-Links zum Direktversand.	[168]
SocialFish	Generiert automatisiert Phishing-Site-Clones von Facebook, Google, SnapChat, Twitter und Microsoft.	[171]
Blackeye	Upgrade von vormaligem Tool „ShellFish“, generiert mehr Phishing-Site-Clones von PayPal, eBay, Verizon, Dropbox, Adobe ID, Shopify, Messenger, Twitch, MySpace, Badoo, Yandex und devianART	[170]
phishEye	Automatisiertes Phishing-Tool mit Website-Cloner für Facebook, Twitter, Instagram, LinkedIn, GitHub, Dropbox. „Click-and-Phish“ mit funktionierendem Ngrok-Link.	[169]

Tabelle 17: Zusammenstellung Phishing mit Website-Cloning

6.3.2. Massenmailer

Mit dem Social Engineering Toolkit *SET* [160] lässt sich, neben einzelnen (Spear-)Phishing-Nachrichten auch unter "*1) Social-Engineering Attacks*" und dem weiteren Untermenü "*5) Mass Mailer Attack*", ein Versand von Massenmails einrichten. Die E-Mail-Adressen der Empfänger können dabei über eine separate Textdatei bereitgestellt werden. Zum Versenden kann ein eigener Mail-Server oder das Versenden über Google-Mail (gmail) ausgewählt werden. Die Nachrichteninhalte werden sowohl in HTML-, als auch in reiner Textformatierung akzeptiert.
Eine Test-Aussendung mit SET wurde unter Verwendung eines eigenen Mailservers durchgeführt. Erwartungsgemäß wurde die E-Mail-Nachricht als SPAM klassifiziert und entsprechend gefiltert.

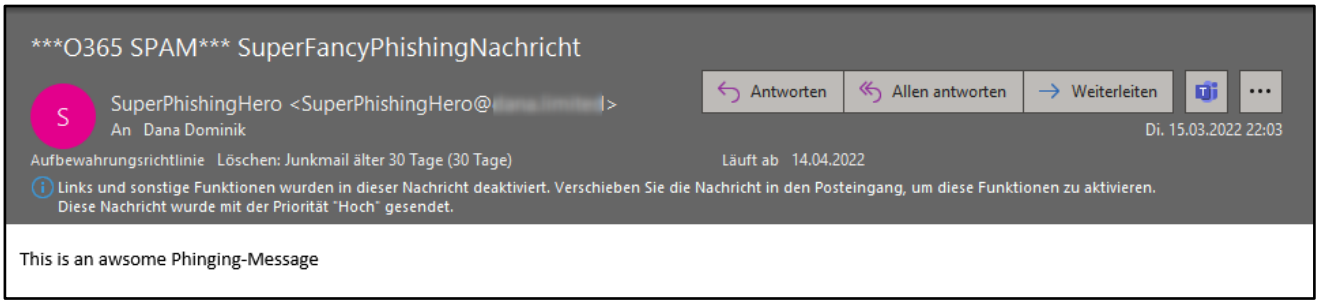


Abbildung 63: Massenmail mit SET

In vielen Fällen ist vor dem Senden einer Nachricht nicht klar, ob diese von einem Mailserver geblockt wird, oder ob diese anstandslos zugestellt werden wird. Um das Verhalten von Mailservern bei Erhalt einer Nachricht zu prüfen, kann vorab eine Prüfung mit *Phishious* [173] durchgeführt werden. Phishious ist, eigenen Angaben zufolge, das bislang einzige Werkzeug, das es ermöglicht Phishing-Angriffe via E-Mail zu scannen. Phishious wertet dazu Headerdaten aus Unzustellbarkeitsmeldungen aus und kann damit vorhersagen, ob eine Nachricht zugestellt, oder als Spam, beziehungsweise Junk-Mail, klassifiziert wird.
Ein weiteres Massenmailer-Tool kann in *Catero* [174] gesehen werden. Catero bietet, neben ebenfalls der Möglichkeit Websites zu klonen, verschiedene Arten zum Versand von automatisierten Nachrichten und ist komplett über das Commandline-Interface (CLI) steuerbar. Catero unterstützt das Senden von Nachrichten über Twillo-Konten zum Versenden von SMS-Nachrichten, das Versenden über LinkedIn-Konten und WebMail-Diensten, Google Voice, sowie iMessage. Catero wurde, aufgrund des größeren Funktionsumfanges und der unterschiedlichen Konfigurationen der jeweiligen Messaging-Typen, sowie der für die Arbeit begrenzten Zeit, keiner praktischen Anwendung zugeführt.

Genutzte und erwähnte Tools in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
SET - Social Engineering Toolkit	Eines der bekanntesten OpenSource Social-Engineering-Werkzeuge, für Social-Engineering- und Penetration-Tests entwickelt. Integriertes Website-Cloning, Spear-Phishing und Mass-Mail-Attack-Framework.	[160] [164] [165]
Catero	Mailer, Webmailer, Twillo, LinkedIn, GoogleVoice und iMessage für (Massen)versand ist die Kernkomponente des Tools. Bietet auch Website-Cloning. Auf Kommandozeilenebene verwaltbar.	[174]
Phishious	Prüft ob und wie sich E-Mail-Gateways beim Erhalt von Phishing-Nachrichten verhalten und ob diese geblockt, oder duchgelassen werden.	[173]

Tabelle 18: Zusammenstellung Massenmailer

6.3.3. Einsatz von Bots

Eine weitere Art der Automation von Social Engineering mittels Bots, stellt die Vorbereitung der Nutzung von *SMSRanger* [175] dar, der auf einem Telegram-Bot basiert. SMSRanger sendet automatisierte Nachrichten an Personen, jeweils im Auftrag einer Bank und fordert diese auf, OTP-Codes (One Time Password) in entsprechenden Websites, oder in einem automatisierten Anruf über einen Voice-Bot, über die Telefontastatur einzugeben. Der Service enthält tägliche Updates, ist in verschiedenen Sprachen erhältlich und ist kostenpflichtig. Zum Zeitpunkt der Recherche waren für aufgerufene 425 USD pro Monat auch Anrufe aus und in verschiedene Länder, unter anderem auch in deutschsprachige, beinhalten. Gesteuert wird SMSRanger über einen Telegram-Chat. Auch dieser Bot wurde, aus sicherheitstechnischen, sowie aus rechtlichen und auch ethischen Gründen, nicht aktiviert.

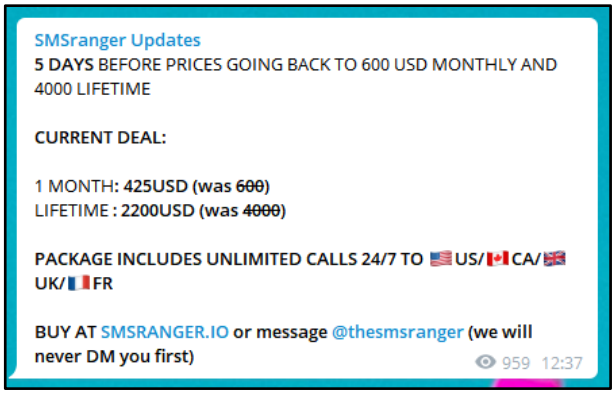


Abbildung 64: SMSRanger Pricing (Screenshot Telegram Channel)

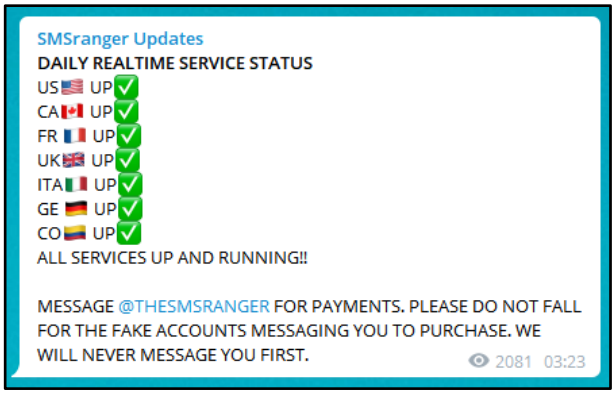


Abbildung 65: SMSRanger Daily Service Status (Screenshot Telegram Channel)

Mit *Honeybot* [39] wurde von Tobias Lauinger et al. bereits gezeigt, dass Konversationen zwischen zwei Menschen gestartet und durch den Bot-in-the-Middle beeinflusst und gesteuert werden können. Der Einsatz einer ähnlichen Implementierung kann ebenfalls unter dieser Sektion genannt werden. Honeybot hat in dieser Sektion nur erwähnenden Charakter und wurde in der vorliegenden Arbeit nicht getestet oder evaluiert, da dies bereits in verwandten Arbeiten, welche innerhalb der Literaturanalyse am Beginn der Arbeit, bereits Erwähnung fanden, beschrieben wurde.

Erwähnte Bots in dieser Sektion:

Tool	Kurzbeschreibung	Verweis
Honeybot	Chatbot, der eine Unterhaltung mit zwei realen Menschen als Bot-in-the-Middle beeinflussen kann.	[39]
SMSRanger	Eine auf einem Telegram-Bot basierende Lösung, die automatisiert im Auftrag eines Geldinstituts, oder einer anderen Impersonation, OTP-Codes, oder auch Kreditkartendaten von Personen sammelt.	[175]

Tabelle 19: Zusammenstellung Einsatz von Bots

7. Schlussfolgerungen

7.1. Zusammenfassung und Erkenntnisse

In der vorliegenden Arbeit wurde ein einführender Einblick in die Welt des Social Engineerings gegeben. Es wurde dargelegt, wie und warum Social Engineering funktionieren kann, welche Vertrauensfaktoren dazu nötig sind und weiters Beispiele für die Nutzung von IT-Systemen für Social-Engineering-Zwecke, gegeben. Es wurde anhand von Beispielen aus der Vergangenheit gezeigt, dass Social Engineering keine neue Bedrohung ist, es sich aber mit dem Fortschritt der technologischen Entwicklung mit weiterentwickelt hat und erfolgsversprechender ist, als die ebenfalls immer besser werdenden, technischen Hürden für Angriffe zu umgehen. In der Einführung wurde auch darauf eingegangen, welche Automationen im Social Engineering bereits bestehen und welche Möglichkeiten sich dafür bieten können

In der Literaturanalyse wurde der aktuelle Stand der Forschung über alle analysierten und verwendeten Literaturen zum Thema Social Engineering und Automation im Social Engineering zusammengefasst und auf verwandte Arbeiten eingegangen. Aufgrund der großen Menge an Literaturen wurden diese in die Bereiche „*Techniken und Tools*“, „*Fortgeschrittenere Angriffe und Automationen*“, „*Vertrauensfaktoren als Grundlagen für die Funktionalität von Automation*“ und in „*Alternative Fameworks*“ aufgeteilt.

Da die Arbeit mit Social-Engineering-Werkzeugen in der praktischen Anwendung ethische, aber auch rechtliche Problematiken mit sich bringen kann, wurde daher in Kapitel 4 auf rechtliche Aspekte hinsichtlich der Datenschutz-Grundverordnung und des Strafgesetzbuches, aber auch auf die ethischen Aspekte eingegangen. Der Umgang mit diesen Aspekten und Gegebenheiten in anderen Arbeiten wurde im Anschluss angeführt und basierend darauf ein eigener Ansatz für die Anwendung in der vorliegenden Arbeit abgeleitet und beschrieben.

Um Automation im Bereich des Social Engineerings besser zu verstehen und um nach geeigneten Werkzeugen und Toolsuites suchen zu können, aber auch um Automation in verschiedene Phasen des Social Engineerings einordnen zu können, war es unerlässlich verschiedene Social-Engineering-Frameworks zu analysieren und miteinander zu vergleichen. Dazu wurden alle Frameworks, die während der Recherche aufgefunden werden konnten, in Kürze beschrieben. Dabei hat sich herausgestellt, dass sich die verschiedenen Modelle in der Anzahl der Phasen häufig unterscheiden und ein Einordnen von automatisierten Tools zu einzelnen Phasen in dieser Weise nicht zielführend ist. In dem zusammenfassenden Vergleich aller Modelle wurde daher eine Komprimierung der Phasen aus den angeführten Social-Engineering-Modellen und Frameworks, auf gemeinsame Phasen vorgenommen und daraus das „Technische Social-Engineering-Modell“, das nurmehr aus den drei Phasen der Informationsbeschaffung, Angriffsvorbereitung und der Angriffsausführung besteht, vorgenommen. Ein vergleichbares abstraktes Modell konnte, während der Verfassung der Arbeit, nicht gefunden werden. Mit einem Phasen-Mapping wurden weiters die einzelnen Phasen der beschriebenen Frameworks aus anderen Arbeiten, den Phasen des technischen Social-Engineering-Modells zugeordnet. Für die Listung und das Clustering des aktuellen Standes der recherchierten und automationsunterstützen Social-Engineering-Werkzeuge, wurden in Kapitel 6 die einzelnen Phasen des technischen Social-Engineering-Modells herangezogen.

Das Clustering der entsprechenden Werkzeuge zeigt in der Phase der Informationsbeschaffung die Vielfältigkeit und die große Anzahl der Werkzeuge mit den meisten Automatisierungsmöglichkeiten, da es hier eine große Community an Interessierten und Mitwirkenden aus dem OSINT-Bereich gibt. Dies zeigte sich nicht nur in den kurzen Abständen, in denen Tools und Updates zu bestehenden Tools veröffentlich werden, sondern auch in der sprachlichen Vielfältigkeit, in der die Applikationen gehalten sind. Die kurzen Zeitabstände machen es unmöglich, alle Tools zu listen und zu testen. Aufgrund dessen wurde eine Auswahl von über 140 deutsch- oder englischsprachigen Tools zusammengestellt, welche einer praktischen Anwendung und einem Vergleich unterzogen wurden.

Bei den Tests und Anwendungen hat sich herausgestellt, dass sich die Informationsbeschaffung innerhalb der Europäischen Union, seit Einführung der Datenschutz-Grundverordnung, erschwert hat und dass speziell Webapplikationen zur Informationsbeschaffung, größtenteils nur in den Bundesstaaten der USA Ergebnisse liefern. Auch sind in den kostenfrei verfügbaren Applikationen oftmals Abfragelimits implementiert, die nur eine

geringe Anzahl an Abfragen innerhalb eines bestimmten Zeitraums erlauben. Die Registrierung zum Erhalt eines API-Keys, verschiebt die Abfragelimits, je nach gewähltem Tarif und Tool, aber auch die Aktualität, sowie den Umfang an zur Verfügung gestellten Daten. Da der Fokus in der vorliegenden Arbeit primär auf frei zugänglichen Tools liegt, wurden nur freie Tools und API-Keys genutzt.
Bei der Verwendung der Tools zur Informationsbeschaffung zeigt sich, dass Ergebnisse vor einer weiteren Verwendung manuell auf Plausibilität und Validität geprüft werden müssen, da die Ergebnisse der automatisierten Tools, mit Ausnahme dieser, die Informationen direkt aus Social-Media-Plattformen auslesen, nicht zwangsläufig korrekt, oder passend sein müssen. Für die Anwendung der Tools zur Informationsbeschaffung in Social-Media-Plattformen wird von den meisten Plattformen ein registrierter Account verlangt, wofür es sich empfiehlt, einen eigenen Social-Media-Account zu nutzen, da nicht gewährleistet werden kann, ob es durch die Verwendung der Tools zu einem Abfluss an Benutzerdaten kommt. Während der testweisen Anwendungen der Tools wurden die Testaccounts der Plattformen Facebook und Instagram mehrmals aufgrund unberechtigter Zugriffe gesperrt und erforderten jeweils manuelle Reaktivierungsprozedere inklusive Passwortwechsel.
Bei der Verwendung der Tools zur Vorbereitung von Angriffen hat sich gezeigt, dass Automation auf die vorbereitende Generation und Erstellung von Payloads und Bots, sowie auf die Unterstützung bei der Formulierung von Texten zusammengefasst werden kann. Tools, die Websites klonen und als Phishing-Websites zur Verfügung stellen, wurden in die Phase der Angriffsausführung übernommen, da die Seiten direkt nach dem Klonen bereits aktiv und verwendbar waren. Eine gesonderte Vorbereitung ist bei diesen Tools daher nicht nötig.
Bei der Verwendung der Tools in der Phase der Angriffsausführung konnten die recherchierten und genannten Tools in die Kategorien „*Phishing mit Website-Cloning*“, „*Massenmailer*“ und den „*Einsatz von Bots*“ zusammengefasst werden. Tools, die für awarenessbildende Phishing-Kampagnen in Unternehmen eingesetzt werden können, beispielsweise *CanIPhish* [176], *KingPhisher* [177], oder *GoPhish* [178] wurden in dieser Sektion nicht betrachtet.
Eine komplett durchgängig automatisierte Software, die einen kompletten Social-Engineering-Angriff in all seinen Phasen abbilden kann, konnte nicht aufgefunden werden. Die beiden Tools Maltego und SET sind, nach Abschluss der Tests und Vergleiche, die funktionalsten und zuverlässigsten Werkzeuge.

7.2. Beantwortung der Forschungsfragen

7.2.1. Beantwortung RQ1

> ***Wie weit sind frei verfügbare Social Engineering unterstützende Tools bereits automatisiert und was bedeutet dies in Bezug auf das Social Engineering?***

Die frei verfügbaren Social-Engineering-Werkzeuge sind dahingehend automatisiert, als dass wiederkehrende Abfrage- und Sucharbeiten automatisiert durchgeführt werden können und der manuelle Aufwand damit erheblich reduziert werden kann. Dazu zählt bei der Beschaffung von Informationen über eine Zielperson, oder Zielorganisation, die Suche über beispielsweise CSEs, die Suche nach Informationen in Social-Media-Plattformen, die Suche nach E-Mail-Adressen, nach Informationen und Daten in verschiedenen Databreaches, aber auch die Suche nach Informationen technischer Natur, beispielsweise einem Webauftritt, Informationen über verwendete Technologien, Versionen und Provider.
Suchen können dabei über Webapplikationen, aber auch lokal installierte Tools durchgeführt werden. Webapplikationen glänzen mit einfacheren Bedienungen und mit schneller Verfügbarkeit. Die Automationsmöglichkeiten sind allerdings unter Verwendung der APIs der Suchanbieter und -plattformen, größer, da die Ergebnisse bei entsprechender Ausgabe automatisiert weiterverarbeitet werden können. Eine komplett durchgängige und automatisierte Lösung konnte, zum Zeitpunkt der Recherche und Verfassung der Arbeit, nicht aufgefunden werden. Die Entwicklung einer solchen Lösung gestaltet sich allerdings als entsprechend schwierig, da einerseits Social Engineering sehr dynamisch ablaufen kann und andererseits, als

dass Teilergebnisse immer wieder validiert und verifiziert werden müssen. Eine Entscheidung, ob Daten zu einem aktuellen Ziel in einem aktuell vorbereiteten Social-Engineering-Szenario passen, muss von den jeweiligen Social Engineers manuell selbst getroffen werden.
Automation ist bei der Durchführung von Angriffen und in der entsprechend Vorbereitung ebenfalls bereits vorhanden, entsprechende Tools sind auch in der Bedienung schon sehr einfach gehalten. So ist es bereits mit wenig Aufwand und ohne detaillierten Kenntnissen möglich, Phishing-Seiten mit Abbildern von echten Websites, zu erstellen und diese einzusetzen. Ein Versenden von automatisiert generierten und schädlichen Anhängen ist mit diesen ebenfalls bereits sehr einfach und ohne spezieller Kenntnisse möglich.
Es hat sich, während dem Verfassen der Arbeit gezeigt, dass die Auswahl und Verfügbarkeit von automatisierten Social-Engineering-Tools, zum Zweck der Informationsbeschaffung und Reconnaissance, am größten ist. Als eine Begründung dessen kann die Verfügbarkeit einer großen Community aus dem OSINT-Bereich genannt werden, die ihr Knowhow auch für Suchen nach beispielsweise vermissten Personen bei sogenannten „Search Partys“ [179] einsetzen und entsprechende Tools aus dieser Motivation heraus entwickeln. Eine andere Begründung kann in der größeren Verfügbarkeit dieser Tools, unter anderem zu awarenessbildenden Maßnahmen, gesehen werden.
Frei verwendbare Tools haben oftmals Themen mit Qualität und Verfügbarkeit. Hinsichtlich der Qualität wurde in der Arbeit angeführt, dass der Suchumfang und die Anzahl der zugelassenen Suchen, je nach Plattform gewissen Limitierungen unterliegen und erst mit kostenpflichtigen Subskriptionen erhöht werden. Dies wirkt sich auch auf die Zuverlässigkeit der Suchergebnisse aus. Hinsichtlich der Verfügbarkeit konnten während der Recherchephase interessante Tools gesammelt werden, die allerdings während der Test- und Anwendungsphase einige Wochen später, nicht mehr verfügbar und nicht mehr anwendbar waren. Die Verfügbarkeit, speziell die freie Verfügbarkeit, von automatisierten Social-Engineering-Tools bedeutet, dass diese Werkzeuge jeder Person zur Verfügung stehen, von jeder Person genutzt werden kann und dass sich somit auch jede Person, ohne viel Aufwand und ohne vertiefenden Kenntnissen, auf einfache Weise den Techniken des Social Engineerings bedienen kann. Durch die Verfügbarkeit von betriebsfertigen Systemumgebungen, wie die in Kapitel 6.1.3 beschrieben Linux-Distributionen, werden bereits vorkonfigurierte Systeme zur Verfügung gestellt, welche mit einer vereinfachten grafischen Oberfläche, auch Einsteigern innerhalb kurzer Zeit brauchbare Ergebnisse liefern können.

7.2.2. Beantwortung RQ2

Welche Phasen des Social Engineering können mit den Tools bedient werden?

Bei der Nennung der Phasen, die durch automatisierte Social-Engineering-Tools bedient werden können, kommt es darauf an, welches Phasenmodell für die Zuordnung der Phasen in Betracht gezogen wird. Die verschiedenen Frameworks und Phasenmodelle unterscheiden sich hinsichtlich der Anzahl an Phasen, sowie auch hinsichtlich der Abläufe innerhalb der Phasen selbst. Generisch formuliert, können die Phasen der Reconnaissance und die Phasen, innerhalb dieser Angriffe stattfinden, am besten mit Automation bedient und unterstützt werden.
Aufgrund der vielen Unterschiede zwischen den verschiedenen Social-Engineering-Modellen konnte keine, auf alle Modelle passende, Zuordnung der automatisierten Tools durchgeführt werden. Daher wurde unter Kapitel 5.10 das abstrakte technische Social-Engineering-Modell, das sich aus den in Kapitel 5.1 bis Kapitel 5.9 beschriebenen Frameworks ableitet, vorgestellt.
Die Phasen des technischen Social-Engineering-Modells können von allen, in dieser Arbeit genannten Tools, bedient werden. Dies wurde auch anhand der Aufgliederung der Tools innerhalb von Kapitel 6 verdeutlicht.

7.2.3. Beantwortung RQ3

Wie spielen die verschiedenen Tools zusammen, gibt es Toolsuites die einen kompletten Social-Engineering-Prozess an- und begleiten?

Die in dieser Arbeit gelisteten Tools spielen nur auf manuellem Wege zusammen. Datensätze müssen manuell ausgewählt, validiert und dem nächsten Tool entsprechend formatiert, übergeben werden. Toolsuites, die mehrere Möglichkeiten bieten und deren Funktionalitäten mit Plugins erweitert werden können, wie beispielsweise die genannten Tools Maltego, Lampyre, oder auch Spiderfoot HX, können Ergebnisse in neue Suchen am einfachsten übernehmen. Diese Tools können zwar keinen kompletten Social-Engineering-Prozess anleiten, begleiten aber einen großen Teil dessen, mit Informationsbeschaffung, auf sehr zuverlässige Weise. Komplette Toolsuites konnten im Rahmen der Arbeit keine aufgefunden werden. Eine selbst entwickelte Verbindung zwischen mehreren Tools, über Scripts oder weitere Tools, wurde zwar angedacht, im Rahmen dieser Arbeit aber nicht durchgeführt, da dies den Umfang der Arbeit erheblich erweitern würde. Die Entwicklung eignet sich erweiternd als Future Work.

7.2.4. Beantwortung RQ4

Wie zuverlässig sind die Ergebnisse der Tools?

Die Ergebnisse, die bei der praktischen Anwendungen der genannten und gelisteten Tools geliefert werden, hängen sehr von der Funktionsweise des jeweiligen Tools selbst ab. Während einige der Tools, zur Lieferung von Suchergebnissen, sich der Suche in Archivdatenbanken oder dem Durchsuchen von gecrawlten und gescannten Internetseiten bedienen, greifen einige Tools direkt auf Livedaten zu. Livedaten wurden in freien Programmversionen nur von Tools, die Social-Media-Plattformen durchsuchen, beispielsweise Tinfoleak oder OSINTGram, ausgewertet und setzten eine Registrierung, beziehungsweise einen vorhandenen Benutzeraccount auf der jeweiligen Plattform, voraus. Gecrawlte Seiten zu durchsuchen, wie es in den Tests beispielsweise von dem Tool Crosslinked gemacht wurde, erfordert zwar keine bestehenden Benutzeraccounts, die Zuverlässigkeit der Ergebnisse wird dadurch aber ein Stück weit vernachlässigt, da die Aktualität der aufgefundenen Daten nicht restlos bestimmt werden kann und damit Suchergebnisse zum Zeitpunkt des Auffindens bereits veraltet sein können.

7.3. Future Work

Im Rahmen dieser Arbeit wurde ein Überblick und aktueller Stand an frei erhältlichen Social-Engineering-Tools geboten. Diese wurden, so sich deren Anwendungen im Rahmen der ethischen und rechtlichen Möglichkeiten bewegt haben, auch getestet und miteinander verglichen, die Unterschiede hervorgehoben und die Zuverlässigkeit der Ergebnisse bewertet. Als erweiternde Arbeit können, anstatt der freien und für Studenten zur Verfügung gestellten API-Keys, kostenpflichtige API-Keys der Applikationen, die höherwertige Subskriptionen anbieten, erworben werden und die Ergebnisse zwischen den Premium-Versionen miteinander verglichen werden. Unter entsprechender rechtlicher und ethischer Deckung ist ein erweiterter Einsatz der Tools, auch zu Awareness- und Schulungszwecken, denkbar. Ebenfalls zu Schulungs- und Awarenesszwecken kann es, gerade auch im Hinblick auf das steigende Aufkommen von Phishing-Nachrichten, von Vorteil sein den Einsatz und die Unterschiede von professionellen Social-Engineering-Tools, beispielsweise CanIPhish, GoPhish, oder auch SET, im Unternehmenskontext zu bewerten. Daraus können, in einem weiteren Schritt, auch zu der jeweiligen Organisation passende, organisatorische Gegenmaßnahmen abgeleitet werden und nach Möglichkeit ein Anti-Social-Engineering-Framework, entworfen werden.
Bei Anwendung und Nutzung der kostenfreien Tools konnte festgestellt werden, dass Suchplattformen, darunter beispielsweise Hunter.io, Shodan.io, sowie _IntelX, in mehreren Tools im Hintergrund genutzt wurden. Basierend auf dieser Erkenntnis könnte im Rahmen einer weiteren Arbeit verglichen werden, welche und

wieviele Suchmaschinen und -datenbanken im Hintergrund von den verschiedenen Tools gemeinsam genutzt werden und ob sich die Ergebnisse, trotz Verwendung gleicher Quellen, am Ende unterscheiden.
Wie auch bereits in der vorhergehenden Beantwortung der Forschungsfrage RQ3 erwähnt, kann eine weiterführende Arbeit auch die Entwicklung einer automatisierten Social-Engineering-Applikation hervorbringen, welche die Anwendungen und Ergebnisse verschiedener Social-Engineering-Tools, ähnlich den geführten Case-Management-Dialogen in CSI-Linux, miteinander verknüpfen kann.

Literaturverzeichnis

[1] K. D. Mitnick und W. L. Simon, The Art of Deception: Controlling the Human Element of Security, Indianapolis, Indiana: Wiley Publishing Inc., 2002.

[2] C. Hadnagy, Social Engineering: The Art of Human Hacking, Indianapolis, Indiana: Wiley Publishing Inc., 2010.

[3] A. M. Aroyo, F. Rea, G. Sandini und A. Sciutti, „Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?," in *IEEE Robotics and Automation Letters*, 2018.

[4] M. Huber, S. Kowalski, M. Nohlberg und S. Tjoa, „Towards Automating Social Engineering Using Social Networking Sites," in *International Conference on Computational Science and Engineering*, 2009.

[5] K. Zheng, T. Wu, X. Wang, B. Wu und C. Wu, „A Session and Dialogue-Based Social Engineering Framework," in *IEEE Access vol. 7*, 2019.

[6] E. D. Frauenstein und S. V. Flowerday, „Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats?," IEEE, University of Fort Hare, East London, South Africa, 2016.

[7] J. Talamantes, The Social Engineer's Playbook - A Practical Guide To Pretexting, Woodbury, MN: Hexcode Publishing, 2014.

[8] R. Pöhner, „Wie man Al Capone über den Tisch zieht," Tagesanzeiger.ch, 09 01 2018. [Online]. Available: https://blog.tagesanzeiger.ch/historyreloaded/index.php/2202/wie-man-al-capone-ueber-den-tisch-zieht/. [Zugriff am 31 10 2021].

[9] Wikipedia, „Frank Abagnale," Wikipedia.org, 01 09 2021. [Online]. Available: https://de.wikipedia.org/wiki/Frank_Abagnale. [Zugriff am 06 11 2021].

[10] Y. Kano und T. Nakajima, „Trust Factors of Social Engineering Attacks on Social Networking Services," in *2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech)*, Nara, Japan, 2021.

[11] M. N. Hajli, „The role of social support on relationship quality and social commerce," in *Technological Forecasting and Social Change, Volume 87*, 2014.

[12] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler und S. Goluch, „Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam," in *IEEE Internet Computing, vol. 15, no. 3*, 2011.

[13] M. Pirnau, „CONSIDERATIONS ON PREVENTING SOCIAL ENGINEERING OVER THE INTERNET," Memoirs of the Scientific Sections of the Romanian Academy, Tome XL, Bucharest, Romania, 2017.

[14] R. B. Cialdini, PhD., „INFLUENCE The Psychologiy of Persuasion, Revised Edition," HarperCollins e-books, 2009.

[15] R. B. Cialdini, PhD, INFLUENCE, NEW AND EXPANDED The Psychology of Persuasion, HarperCollinsPublishing, 2021.

[16] K. Kikerpill und A. Siibak, „MAZEPHISHING: THE COVID-19 PANDEMIC AS CREDIBLE SOCIAL CONTEXT FOR SOCIAL ENGINEERING ATTACKS," in *Trames Journal of the Humanities and Social Sciences 25(4):371*, Tartu, 2021.

[17] K. Krombholz, H. Hobel, M. Huber und E. Weippl, „Advanced social engineering attacks," in *Journal of Information Security and Applications Vol.22*, 2014.

[18] Z. Wang, H. Zhu, P. Liu und L. Sun, „Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," SpringerOpen, 2021.

[19] H. Aldawood und G. Skinner, „An Advanced Taxonomy for Social Engineering Attacks," in *International Journal of Computer Applications (0975 - 8887), Volume 177 - No. 30*, 2020.

[20] K. Ilker, „DON'T BITE THE BAIT: PHISHING ATTACK FOR INTERNET BANKING (E-BANKING),“ in *Journal of Digital Forensics, Security and Law: Vol. 16, Article 5*, 2021.

[21] Onlinesicherheit.gv.at, „Services > Cybermonitor > Phishing,“ A-SIT Zentrum für sichere Informationstechnologie - Austria, 24 09 2021. [Online]. Available: https://www.onlinesicherheit.gv.at/Services/Cybermonitor/Phishing.html. [Zugriff am 21 11 2021].

[22] W. Franz, „88 Prozent mehr Phishing-Attacken in österreichischen Homeoffices,“ COMPUTERWELT, 27 08 2021. [Online]. Available: https://computerwelt.at/news/88-prozent-mehr-phishing-attacken-in-oesterreichischen-homeoffices/. [Zugriff am 21 11 2021].

[23] A. Molder, „Weltweit 70 Prozent mehr Phishing-Attacken im Home-Office,“ LANline.de, 31 08 2021. [Online]. Available: https://www.lanline.de/it-security/weltweit-70-prozent-mehr-phishing-attacken-im-home-office.253437.html. [Zugriff am 21 11 2021].

[24] APWG - Anti Phishing Workgroup, „Phising Activity Trends Reports 2004-2021,“ APWG, 2021. [Online]. Available: https://apwg.org/trendsreports/. [Zugriff am 21 11 2021].

[25] C. Hadnagy, Social Engineering - The Science of Human Hacking, Indianapolis, Indiana: Wiley Publishing Inc., 2018.

[26] D. Niederberger, „Smishing Nachrichten KW49,“ WhatsApp Nachrichtenverlauf 11.12.2021, 2021.

[27] BSI - Bundesamt für Sicherheit und Informationstechnik, „"Smishing" - SMS-Phishing im Herbst 2021 mit neuen Betrugsmaschen,“ BSI, 14 10 2021. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html. [Zugriff am 17 10 2021].

[28] T-Mobile Austria GmbH, „Phishing - Aktuelle Fälle und Tipps gegen Phishing-Attacken im Blick,“ Magenta, 15 11 2021. [Online]. Available: https://blog.magenta.at/2021/11/15/phishing-attacken/. [Zugriff am 24 11 2021].

[29] Kaspersky, „What is Typosquatting? – Definition and Explanation,“ Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting. [Zugriff am 02 12 2021].

[30] P. Kim, The Hacker Playbook 2 - Practical Guide To Penetration Testing, North Charleston, South Carolina: Secure Planet LLC, 2015.

[31] M. Schmidt, „Expired Domain Name Search Engine,“ [Online]. Available: https://www.expireddomains.net/. [Zugriff am 12 12 2021].

[32] NortonLifeLock Inc., „What is scareware? And how to spot online scareware scams,“ NortonLifeLock Inc., 15 09 2021. [Online]. Available: https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html. [Zugriff am 04 12 2021].

[33] Panda Security S.L.U., „Rogueware: Sie meinen Geräte in Gefahr?,“ Panda Security S.L.U., 2019. [Online]. Available: https://www.pandasecurity.com/de/security-info/rogueware/. [Zugriff am 04 12 2021].

[34] Unsicherheitsblog.de, „Scareware, Rogueware, Rogue Softwarec, falsche Antiviren-Tools,“ Unsicherheitsblog.de, [Online]. Available: https://unsicherheitsblog.de/basiswissen/scareware-rogueware. [Zugriff am 12 12 2021].

[35] Z. Wang, L. Sun und H. Zhu, „Defining Social Engineering in Cybersecurity,“ in *IEEE Access (Volume: 8)*, 2020.

[36] W. R. Flores, H. Holm, G. Svensson und G. Ericsson, „Using phishing experiments and scenario-based surveys to understand security behaviours in practice,“ in *Information Management & Computer Security, Vol. 22 No. 4, pp. 393-406*, 2014.

[37] C. Shah und A. Gawde, „Study of Automated Social Engineering bots,“ in *International Journal of Computer Science and Information Technologies, Vol. 5 (1)*, 2014.

[38] S. Lolagar und I. Böhm, „Open source intelligence,“ in *Int. Cybersecur. Law Rev.*, 2021.

[39] T. Lauinger, V. Pankakoski, D. Balzarotti und E. Kirda, „Honeybot, Your Man in the Middle for Automated Social Engineering," in *3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats*, Sophia-Antipolis, France, 2010.

[40] J. Martin, Medlin Richard, M. Swenson, N. Sharma, C. Perini, M. Martinez und D. Traci, „CSI Linux," CSI Linux, 2021. [Online]. Available: https://csilinux.com/. [Zugriff am 27 12 2021].

[41] G. Rattaro, M. Giorgi, D. Gabrini, F. Picasso, M. Dal Cero, A. Broi und C. Matteuzzi, „TSURUGI Linux," TSURUGI Linux, 2021. [Online]. Available: https://tsurugi-linux.org/index.php. [Zugriff am 27 12 2021].

[42] J. Weizenbaum, „ELIZA — a computer program for the study of natural language communication between man and machine," in *Communications of the ACM, Volume 9, Issue 1*, Massachusetts, 1966.

[43] A. M. Turing, „I.—COMPUTING MACHINERY AND INTELLIGENCE," in *Mind, Volume LIX, Issue 236*, 1950.

[44] SPIEGEL Netzwelt, „Künstliche Intelligenz - Vom Hipster-Mädchen zum Hitler-Bot," Der Spiegel, 24 03 2016. [Online]. Available: https://www.spiegel.de/netzwelt/web/microsoft-twitter-bot-tay-vom-hipstermaedchen-zum-hitlerbot-a-1084038.html. [Zugriff am 12 12 2021].

[45] Wikipedia, „Tay (Bot)," Wikipedia.org, 09 11 2017. [Online]. Available: https://de.wikipedia.org/wiki/Tay_(Bot). [Zugriff am 12 12 2021].

[46] Medical Artificial Intelligence, „ELIZA," med-ai.com, [Online]. Available: http://www.med-ai.com/models/eliza.html.de. [Zugriff am 11 12 2021].

[47] P. Kaul und D. Sharma, „Study of Automated Social Engineering, its Vulnerabilities, Threats and Suggested Countermeasures," in *International Journal of Computer Applications, Vol. 67 (7)*, 2013.

[48] J. Baltazar, J. Costoya und R. Flores, „The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained," Trend Micro Threat Research, 2009.

[49] J. Drömer und D. Kollberg, „The Koobface malware gang exposed," SophosLabs, 2012.

[50] A. Zboralski, „Tinder Social Engineering Attack," medium.com, 25 08 2016. [Online]. Available: https://medium.com/@zboralski/tinder-social-engineering-attack-fb239d8c4c34. [Zugriff am 13 10 2021].

[51] L. Franceschi-Bicchierai, „This Dark Web Site Creates Robocalls to Steal People's Credit Card PINs," VICE Media Group, 30 06 2017. [Online]. Available: https://www.vice.com/en/article/3knz98/dark-web-site-robocalls-to-steal-credit-card-pins. [Zugriff am 19 12 2021].

[52] A. Agarwal, „Sleeping Time," digital inspiration, 2014. [Online]. Available: http://sleepingtime.org/. [Zugriff am 27 12 2021].

[53] R. Ahmad, „WhatsApp Monitor - WhatsApp Contact Online Monitoring Tool," Github, 2021. [Online]. Available: https://github.com/rizwansoaib/whatsapp-monitor. [Zugriff am 28 12 2021].

[54] J. Seymour und P. Tully, „Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter," Blackhat, USA, 2016.

[55] J. Seymour und P. Tully, „GitHub - zerofox-oss/SNAP_R: A machine learning based social media pen-testing tool," 13 08 2016. [Online]. Available: https://github.com/zerofox-oss/SNAP_R. [Zugriff am 13 12 2021].

[56] Gabler Wirtschaftslexikon, „Deepfake Definition," Gabler Wirtschaftslexikon, 25 07 2019. [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/deepfake-120960/version-370918. [Zugriff am 13 12 2021].

[57] K. Mitnick und Global Ghost Team, „How Technology is Changing the Future of Social Engineering," mitnicksecurity.com, [Online]. Available: https://www.mitnicksecurity.com/blog/how-technology-is-changing-the-future-of-social-engineering. [Zugriff am 14 10 2021].

[58] S. Kaushalya, R. M. R. S. B. Randeniya und A. D. S. Liyanage, „An Overview of Social Engineering in the Context of Information Security," in *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, Bangkok, Thailand, 22-23 Nov. 2018.

[59] K. Mitnick und Global Ghost Team, „The History of Social Engineering & How to Stay Safe Today," mitnicksecurity.com, [Online]. Available: https://www.mitnicksecurity.com/the-history-of-social-engineering. [Zugriff am 13 10 2021].

[60] B. Banire, D. Al Thani und Y. Yang, „Investigating the Experience of Social Engineering Victims: Exploratory and User Testing Study," in *Electronics, vol. 10, no. 21*, 2021.

[61] J. Obuhuma und S. Zivuku, „Social Engineering Based Cyber-Attacks in Kenya," in *IST-Africa 2020 Conference Proceedings*, Uganda, 2020.

[62] N. A. Hassan und R. Hijazi, Open Source Intelligence Methods and Tools - A Practical Guide to Online Intelligence, SpringerLink, Hrsg., New York: Springer Science+Business Media, 2018.

[63] L. Block und MW-OSINT, „How GDPR affects OSINT," keyfindings.blog, 11 06 2019. [Online]. Available: https://keyfindings.blog/2019/06/11/how-gdpr-effects-osint/. [Zugriff am 25 12 2021].

[64] L. ten Hulson, „OPEN SOURCING EVIDENCE FROM THE INTERNET - THE PROTECTION OF PRIVACY IN CIVILIAN CRIMINAL INVESTIGATIONS USING OSINT (OPEN-SOURCE INTELLIGENCE)," in *Amsterdam Law Forum, 12(2), pp.3–48*, Amsterdam, 2020.

[65] Politie.nl, „Shahin Gheiybe," 05 03 2019. [Online]. Available: https://www.politie.nl/en/wanted-and-missing/most-wanted/2019/maart/shahin-gheiybe.html. [Zugriff am 22 01 2022].

[66] H. Van Ess, „Locating The Netherlands' Most Wanted Criminal By Scrutinising Instagram," Bellingcat, 19 03 2019. [Online]. Available: https://www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/. [Zugriff am 21 01 2022].

[67] J. Fricke, „Big Data und künstliche Intelligenz - Chancen und Risiken für die Polizeiarbeit der Zukunft," Recklinghausen, 2019.

[68] C. P. Janssen, S. F. Donker, D. P. Brumby und A. L. Kun, „History and future of human-automation interaction," in *International Journal of Human-Computer Studies 131*, 2019.

[69] M. Huber, *Automated Social Engineering Proof of Concept,* Stockholm, 2009.

[70] D. Ariu, E. Frumento und G. Fumera, „Social Engineering 2.0: A Foundational Work: Invited Paper," in *CF'17: Proceedings of the Computing Frontiers Conference*, 2017.

[71] Wikipedia, „Markov chain," Wikipedia.org, 26 01 2022. [Online]. Available: https://en.wikipedia.org/wiki/Markov_chain. [Zugriff am 29 01 2022].

[72] F. A. Gers, J. Schmidhuber und F. Cummins, „Learning to Forget: Continual Prediction with LSTM," in *Technical Report IDSIA-01-99*, Lugano, Switzerland, 1999.

[73] A. Stern, „Social Networkers Beware: Facebook is a Major Phishing Portal," Kaspersky, 23 06 2014. [Online]. Available: https://www.kaspersky.com/blog/1-in-5-phishing-attacks-targets-facebook/5180/. [Zugriff am 30 01 2022].

[74] Y. Boshmaf, I. Muslukhov, K. Beznosov und M. Ripeanu, „The Socialbot Network: When Bots Socialize for Fame and Money," in *ACSAC '11: Proceedings of the 27th Annual Computer Security Applications Conference*, 2011.

[75] Z. Coburn und G. Marra, „Realboy - Believeable Twitter Bots," 2008. [Online]. Available: http://ca.olin.edu/2008/realboy/. [Zugriff am 30 01 2022].

[76] G. Metta, L. Natale, F. Nori, G. Sandini, D. Vernon, L. Fadiga, C. von Hofsten, K. Rosander, M. Lopes, J. Santos-Victor, A. Bernardino und L. Montesano, „The iCub humanoid robot: An open-systems platform for research in cognitive development," in *Neuronal Networks Volume 23, Issues 8-9*, 2010.

[77] A. R. F. Yasin, L. Liu*, J. Wang und R. Ali, „Understanding Social Engineers Strategies from the perspective of Sun-Tzu Philosophy," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Madrid, Spain, 2020.

[78] Wikipedia, „Doxing," Wikipedia.org, 18 11 2021. [Online]. Available: https://de.wikipedia.org/wiki/Doxing. [Zugriff am 26 12 2021].

[79] EUR-Lex, „VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTES UND DES RATES vom 27. April zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung),“ 2016.

[80] RIS - Rechtsinformationssystem des Bundes, „Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Strafgesetzbuch, Fassung vom 30.12.2021,“ 30 12 2021. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296. [Zugriff am 31 12 2021].

[81] I. Mann, Hacking the Human - Social Engineering Techniques and Security Countermeasures, Hampshire: Gower Publishing Limited, 2008.

[82] P. Finn und M. Jakobsson, „Designing ethical phishing experiments,“ in *IEEE Technology and Society Magazine (Volume: 26, Issue: 1, Spring 2007)*, 2007.

[83] *DEF CON 24 - Delta Zero, KingPhish3r - Weaponizing Data Science for Social Engineering.* [Film]. YouTube, 2016.

[84] S. N. H. Zulkifflia, M. N. A. Zawawi und F. A. Rahim, „Passive and Active Reconnaissance: A Social Engineering Case Study,“ in *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, Selangor, Malaysia, 2020.

[85] F. Mouton, M. M. Malan, L. Leenen und H. Venter, „Social engineering attack framework,“ in *2014 Information Security for South Africa*, Johannesburg, South Africa, 2014.

[86] Lockheed Martin Corporation, „Cyber Kill Chain,“ Lockheed Martin Corporation, [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Zugriff am 05 12 2021].

[87] Hornetsecurity GmbH, „Die Cyber Kill Chain im Detail,“ Hornetsecurity GmbH, 2019. [Online]. Available: https://www.hornetsecurity.com/de/wissensdatenbank/cyber-kill-chain/. [Zugriff am 05 12 2021].

[88] P. Pathak, „Is Your SOC Overwhelmed? Artificial Intelligence and MITRE ATT&CK Can Help Lighten the Load,“ SecurityIntelligence.com, 28 11 2018. [Online]. Available: https://securityintelligence.com/is-your-soc-overwhelmed-artificial-intelligence-and-mitre-attck-can-help-lighten-the-load/. [Zugriff am 12 02 2022].

[89] A. TU, „The Cyber Kill Chain: A Detailed Study,“ akshaycnet, 10 01 2021. [Online]. Available: https://akshaycnet.com/the-cyber-kill-chain-a-detailed-study.html. [Zugriff am 12 02 2022].

[90] imperva, „What is social engineering,“ imperva, [Online]. Available: https://www.imperva.com/learn/application-security/social-engineering-attack/. [Zugriff am 19 10 2021].

[91] M. Nohlberg und S. Kowalski, „The Cycle of Deception - A Model of Social Engineering Attacks, Defences and Victims,“ in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)*, 2008.

[92] A. Cullen und L. Armitage, „The Social Engineering Attack Spiral (SEAS),“ in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, London, UK, 2016.

[93] Z. Wang, L. Sun und H. Zhu, „Defining Social Engineering in Cybersecurity,“ in *IEEE Access (Volume: 8)*, 2020.

[94] A. Algarni und Y. Xu, „Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models,“ in *International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 3, No. 6, December 2013*, Brisbane, Australia, 2013.

[95] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda und C. Pu, „Reverse Social Engineering Attacks in Online Social Networks,“ in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Berlin/Heidelberg, 2011.

[96] G. Hogben, „Securty Issues and Recommendations for Online Social Networks,“ ENISA Position Paper No.1, 2007.

[97] „What is automation?,“ IBM.com, [Online]. Available: https://www.ibm.com/topics/automation. [Zugriff am 27 02 2022].

[98] Google, „Websuchen optimieren - Google Suche-Hilfe,“ [Online]. Available: https://support.google.com/websearch/answer/2466433. [Zugriff am 02 03 2022].

[99] Exploit Database by Offensive Security, „Google Hacking Database,“ [Online]. Available: https://www.exploit-db.com/google-hacking-database. [Zugriff am 28 02 2022].

[100] Google, „Programmable Search Engine,“ [Online]. Available: https://programmablesearchengine.google.com/about/. [Zugriff am 28 02 2022].

[101] Sector035, „Week in OSINT #2021-41,“ 18 10 2021. [Online]. Available: https://sector035.nl/articles/2021-41?fbclid=IwAR1sRn_HDJco7UJRVo_ZJN6pqj5tFT_mdCxEbvUlv2sLf5oypeK9hIdq5nA. [Zugriff am 02 03 2022].

[102] B. Singh, „One-Stop CSE for Social Media,“ 18 10 2021. [Online]. Available: https://cse.google.com/cse?cx=73dda67fd05b4405f#gsc.tab=0. [Zugriff am 02 03 2022].

[103] S. Proto, „Stefanie Proto's Custom Search Engines,“ [Online]. Available: https://docs.google.com/spreadsheets/d/1fBPz6KHsFXryhu6JNrj1l-Rl04bEKLfinyCgCIqTyzU/edit?fbclid=IwAR3niqdKoD6Zx1DL4ZPvM9yXMUo8Hhr6zK2MpELKvyvegQ2Ea7xWqLELiM0#gid=436019663. [Zugriff am 28 02 2022].

[104] S. Proto, „Sprp77's OSINT Resources,“ [Online]. Available: https://drive.google.com/drive/folders/1CBcemFdorkAqJ-Sthsh67OVHgH4FQF05. [Zugriff am 02 03 2022].

[105] bellingcat, „bellingcat - the home of online investigations,“ [Online]. Available: https://www.bellingcat.com/. [Zugriff am 04 03 2022].

[106] Bellingcat, „Bellingcat's Online Investigation Toolkit [bit.ly/bcattools],“ [Online]. Available: https://docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit?fbclid=IwAR2gnqA0CUujpYiS4Kg6Jvwch0Sg-tR1g9_s9gfofwRyIz75ioy-PzdQRto#gid=1919065780. [Zugriff am 02 03 2022].

[107] Bellingcat, „Bellingcat OSINT Landscape - start.me,“ [Online]. Available: https://start.me/p/ELXoK8/bellingcat-osint-landscape. [Zugriff am 04 03 2022].

[108] Technisette, „Tools - Technisette website,“ [Online]. Available: https://technisette.com/p/tools. [Zugriff am 02 03 2022].

[109] „16.OSINT-IO,“ start.me, [Online]. Available: https://start.me/p/1kOJ9N/16osint-io. [Zugriff am 02 03 2022].

[110] „Search Social Media,“ start.me, 16 07 2020. [Online]. Available: https://start.me/p/RMKeQv/search-social-media. [Zugriff am 02 03 2022].

[111] Ph055a, „Ph055a (Ph055a) / Repositories,“ [Online]. Available: https://github.com/Ph055a?tab=repositories. [Zugriff am 02 03 2022].

[112] J. Nordine, „OSINT Framework,“ [Online]. Available: https://osintframework.com/. [Zugriff am 02 03 2022].

[113] KnowEm, „CheckUsernames,“ [Online]. Available: https://checkusernames.com/. [Zugriff am 04 03 2022].

[114] „OSINT Recon Tool,“ [Online]. Available: https://recontool.org/#mindmap. [Zugriff am 04 03 2022].

[115] HOPain, „HOPain OSINT Search Tools,“ [Online]. Available: https://osint.hopain.cyou/. [Zugriff am 04 03 2022].

[116] HOPain, „GitHub - HOPain Complex OSINT Search Tools,“ 22 09 2021. [Online]. Available: https://github.com/HOPain/OSINT-Search-Tools. [Zugriff am 04 03 2022].

[117] BuiltWith Pty Ltd, „BuiltWith Technology Lookup,“ BuiltWith Pty Ltd, [Online]. Available: https://builtwith.com/. [Zugriff am 05 03 2022].

[118] S. Micallef, „SpiderFoot,“ [Online]. Available: https://www.spiderfoot.net/about/. [Zugriff am 05 03 2022].

[119] S. Micallef, „SpiderFoot HX,“ [Online]. Available: https://sf-c824cc8.hx.spiderfoot.net/scaninfo?id=48f74883e9c61198ca1d8356ad0d38e9cc42584e208317542c21b56afbbbb890.

[120] Shodan Search Engine, „Shodan Search Engine,“ [Online]. Available: https://www.shodan.io/dashboard. [Zugriff am 05 03 2022].

[121] KnownSec, „ZoomEye,“ [Online]. Available: https://www.zoomeye.org/. [Zugriff am 05 03 2022].

[122] SPYSE, „Spyse - Internet Assets Search Engine,“ [Online]. Available: https://spyse.com/. [Zugriff am 05 03 2022].

[123] projectdiscovery.io, „Projectdiscovery.io | Chaos.,“ [Online]. Available: https://chaos.projectdiscovery.io/#/. [Zugriff am 05 03 2022].

[124] M. Garciaguirre, „SynapsInt,“ [Online]. Available: https://synapsint.com/index.php. [Zugriff am 06 03 2022].

[125] S. Micallef, „GitHub - smicallef/spiderfoot,“ [Online]. Available: https://github.com/smicallef/spiderfoot?ref=d. [Zugriff am 05 03 2022].

[126] „Email-Format,“ [Online]. Available: https://www.email-format.com/. [Zugriff am 06 03 2022].

[127] Hunter Web Services, Inc., „Find email addresses in seconds - Hunter,“ [Online]. Available: https://hunter.io/. [Zugriff am 06 03 2022].

[128] L. Maldonado und F. Maldonado, „Finder.app,“ [Online]. Available: https://finder.app/about. [Zugriff am 06 03 2022].

[129] Kleissner Investments s.r.o, „_IntelligenceX,“ [Online]. Available: https://intelx.io/. [Zugriff am 06 03 2022].

[130] „Webmii People Search Engine,“ [Online]. Available: https://webmii.com/. [Zugriff am 06 03 2022].

[131] IDCrawl, „IDCrawl Free People Search,“ [Online]. Available: https://www.idcrawl.com/.

[132] Maltego Technologies, „Maltego,“ [Online]. Available: https://www.maltego.com/. [Zugriff am 06 03 2022].

[133] M. Krüger, „Be careful what you OSINT with,“ Keyfindings.com, 23 03 2020. [Online]. Available: https://keyfindings.blog/2020/03/23/be-careful-what-you-osint-with/. [Zugriff am 06 03 2022].

[134] DATA TOWER Kft., „Lampyre: Data analysis & OSINT tool for everyone,“ [Online]. Available: https://lampyre.io/. [Zugriff am 08 03 2022].

[135] wondersmith_rae, „Using Lampyre for Basic and Phone Number OSINT,“ 21 07 2019. [Online]. Available: https://wondersmithrae.medium.com/using-lampyre-for-basic-email-and-phone-number-osint-e0e36c710880. [Zugriff am 06 03 2022].

[136] m8r0wn, „GitHub - m8r0wn/CrossLinked: LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping,“ [Online]. Available: https://github.com/m8r0wn/crosslinked. [Zugriff am 10 03 2022].

[137] vijaysahuofficial, rly0nheart und HanslettTheDev, „GitHub - vijaysahuofficial/UserReCon: This is a simple username recognition tool. It can search a username from over 200 different social media platforms.,“ GitHub, [Online]. Available: https://github.com/vijaysahuofficial/UserReCon?fbclid=IwAR0NAexz0KEyNDvJSOfSyOzsw9Z0Hc9j7AtB38ZK5AsI-5vupj46Dh95o-o. [Zugriff am 10 03 2022].

[138] lucmski, „GitHub - lucmski/userrecon-py: Recognition usernames in 187 social networks.,“ GitHub, [Online]. Available: https://github.com/lucmski/userrecon-py. [Zugriff am 10 03 2022].

[139] thewhiteh4t, „GitHub - thewhiteh4t/nexfil: OSINT tool for finding profiles by username,“ GitHub, [Online]. Available: https://github.com/thewhiteh4t/nexfil?fbclid=IwAR0NAexz0KEyNDvJSOfSyOzsw9Z0Hc9j7AtB38ZK5AsI-5vupj46Dh95o-o. [Zugriff am 10 03 2022].

[140] sherlock-project, „GitHub - sherlock-project/sherlock: 🔎 Hunt down social media accounts by username across social networks,“ GitHub, [Online]. Available: https://sherlock-project.github.io/. [Zugriff am 10 03 2022].

[141] machine1337, „GitHub - machine1337/userfinder: An OSINT tool to find user's all over the internet including social media platforms,“ GitHub, [Online]. Available: https://github.com/machine1337/userfinder?fbclid=IwAR3sCrgnkLvCUuLHP5VT6X8pVUvfyb8W0DZPenHVDA-VTIq3Et3zwMldWL0. [Zugriff am 10 03 2022].

[142] rly0nheart, „GitHub - rly0nheart/thorndyke: Lightweight username enumeration tool that checks the availability of a specified username on over 200 websites.,“ GitHub, [Online]. Available: https://github.com/rly0nheart/thorndyke?fbclid=IwAR1qnLkHJOC0a-OdlRXk1svN8ypAo6BvuQTrA8L5E4VYxbgI4UzVXLUz6PE. [Zugriff am 10 03 2022].

[143] Twitter, Inc., „Profil / Twitter,“ [Online]. Available: https://twitter.com/dominikhatkeininsta. [Zugriff am 11 03 2022].

[144] Reddit, „Reddit - Entdecke ohne Ende,“ [Online]. Available: https://www.reddit.com/user/dominikhatkeininsta. [Zugriff am 11 03 2022].

[145] sham00n, „GitHub - sham00n/buster: An advanced tool for email reconnaissance,“ GitHub, [Online]. Available: https://github.com/sham00n/buster. [Zugriff am 10 03 2022].

[146] C. Martorella, „theHarvester | Kali Linux Tools,“ Edge-Security Research, [Online]. Available: https://www.kali.org/tools/theharvester/. [Zugriff am 11 03 2022].

[147] E. Meged, „GitHub - evyatarmeged/Raccoon: A high performance offensive security tool for reconnaissance and vulnerability scanning,“ GitHub, [Online]. Available: https://github.com/evyatarmeged/Raccoon. [Zugriff am 11 03 2022].

[148] G. Lyon, „Nmap: the Network Mapper - Free Security Scanner,“ nmap.org, [Online]. Available: https://nmap.org/. [Zugriff am 11 03 2022].

[149] aboul3la, „GitHub - aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers,“ GitHub, [Online]. Available: https://github.com/aboul3la/Sublist3r. [Zugriff am 11 03 2022].

[150] kpcyrd, „GitHub - kpcyrd/sn0int: Semi-automatic OSINT framework and package manager,“ GitHub, [Online]. Available: https://github.com/kpcyrd/sn0int. [Zugriff am 11 03 2022].

[151] Iamthefroggy, „GitHub - iamthefrogy/frogy: My subdomain enumeration script. It's unique in the way it is built upon.,“ GitHub, [Online]. Available: https://github.com/iamthefrogy/frogy. [Zugriff am 11 03 2022].

[152] bhavsec, „GitHub - bhavsec/reconspider: 🔎 Most Advanced Open Source Intelligence (OSINT) Framework for scanning IP Address, Emails, Websites, Organizations.,“ GitHub, [Online]. Available: https://github.com/bhavsec/reconspider. [Zugriff am 11 03 2022].

[153] G. Criscione, „GitHub - Datalux/Osintgram: Osintgram is a OSINT tool on Instagram. It offers an interactive shell to perform analysis on Instagram account of any users by its nickname,“ GitHub, [Online]. Available: https://github.com/Datalux/Osintgram. [Zugriff am 12 03 2022].

[154] Hak9, „GitHub - xHak9x/fbi: Facebook Information,“ GitHub, [Online]. Available: https://github.com/xHak9x/fbi. [Zugriff am 12 03 2022].

[155] Novitae, „GitHub - novitae/sterraxcyl: Instagram OSINT tool to export and analyse followers | following with their details,“ GitHub, [Online]. Available: https://github.com/novitae/sterraxcyl. [Zugriff am 12 03 2022].

[156] J. M. Sánchez, „GitHub - JavideSs/insta-extract: Instagram OSINT Tool to scraping user information,“ GitHub, [Online]. Available: https://github.com/JavideSs/insta-extract. [Zugriff am 12 03 2022].

[157] falkensmz und L. Zaccagnini, „GitHub - falkensmz/tw1tter0s1nt: Python tool that automates the process of Twitter OSiNT investigation using twint,“ GitHub, [Online]. Available: https://github.com/falkensmz/tw1tter0s1nt. [Zugriff am 12 03 2022].

[158] V. A. Diaz, „GitHub - vaguileradiaz/tinfoleak: The most complete open-source tool for Twitter intelligence analysis," GitHub, [Online]. Available: https://github.com/vaguileradiaz/tinfoleak. [Zugriff am 12 03 2022].

[159] D. Kitchen, „Payloads · hak5darren/USB-Rubber-Ducky Wiki · GitHub," GitHub, [Online]. Available: https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads. [Zugriff am 13 03 2022].

[160] D. Kennedy, „The Social-Engineerin Toolkit (SET)," TrustedSec, LLC, [Online]. Available: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/. [Zugriff am 13 03 2022].

[161] M. Nelson und M. Robinson, „GitHub - enigma0x3/Generate-Macro: This Powershell script will generate a malicious Microsoft Office document with a specified payload and persistence method," GitHub, [Online]. Available: https://github.com/enigma0x3/Generate-Macro/. [Zugriff am 13 03 2022].

[162] E. Nasi, G. Michel und J. Goldberg, „GitHub - sevagas/macro_pack: macro_pack is a tool by @EmericNasi used to automatize obfuscation and generation of Office documents, VB scripts, shortcuts, and other formats for pentest, dem…," GitHub, [Online]. Available: https://github.com/sevagas/macro_pack. [Zugriff am 13 03 2022].

[163] A. Kaplan, „GitHub - AzizKpln/Social_X: "Socialx" is a Social Engineering And Remote Access Trojan Tool. You can generate fud backdoor and you can embed any file you want inside of the exe file.," GitHub, [Online]. Available: https://github.com/AzizKpln/Social_X?fbclid=IwAR2NFR2Xr0NY4EdwZGdTY6Y-gUF0K-ryMW0-T2mrkrC0iwGqR_QyF4OlKt8. [Zugriff am 13 03 2022].

[164] D. Kennedy, „SET User Manual made for SET 6.0," TrustedSec, LLC, [Online]. Available: https://github.com/trustedsec/social-engineer-toolkit/raw/master/readme/User_Manual.pdf. [Zugriff am 13 03 2022].

[165] D. Kennedy, „GitHub – trustedsec/social-engineer-toolkit: Das Social-Engineer Toolkit (SET)-Repository von TrustedSec – Alle neuen Versionen von SET werden hier bereitgestellt.," GitHub, [Online]. Available: https://github.com/trustedsec/social-engineer-toolkit. [Zugriff am 13 03 2022].

[166] IBM Watson Developer Cloud, „Tone Analyzer Demo," [Online]. Available: https://tone-analyzer-demo.ng.bluemix.net/. [Zugriff am 13 03 2022].

[167] IBM Watson Developer Cloud, „GitHub - watson-developer-cloud/tone-analyzer-nodejs: Sample Node.js Application for the IBM Tone Analyzer Service," GitHub, [Online]. Available: https://github.com/watson-developer-cloud/tone-analyzer-nodejs. [Zugriff am 13 03 2022].

[168] T. Rayat, „GitHub - htr-tech/zphisher: An automated phishing tool with 30+ templates. This Tool is made for educational purpose only ! Author will not be responsible for any misuse of this toolkit !," GitHub, [Online]. Available: https://github.com/htr-tech/zphisher. [Zugriff am 14 03 2022].

[169] A. Kumar, „GitHub - sky9262/phishEye: phishEye is an ultimate phishing tool in python. Includes popular websites like Facebook, Twitter, Instagram, LinkedIn, GitHub, Dropbox, and many others. Created with…," GitHub, [Online]. Available: https://github.com/sky9262/phishEye?fbclid=IwAR1hdh_rgxK24YB4gi_2FYtY4D7Qrxt05WPwU2ZKGa1gXCh7ln7MF0RfmyI. [Zugriff am 14 03 2022].

[170] An0nUD4Y, „GitHub - An0nUD4Y/blackeye: The ultimate phishing tool with 38 websites available!," GitHub, [Online]. Available: https://github.com/An0nUD4Y/blackeye. [Zugriff am 14 03 2022].

[171] UndeadSec, „GitHub - UndeadSec/SocialFish: Phishing Tool & Information Collector," GitHub, [Online]. Available: https://github.com/UndeadSec/SocialFish. [Zugriff am 15 03 2022].

[172] A. Moghaddas, „GitHub - ultrasecurity/Storm-Breaker: Tool social engineering [Access Webcam & Microphone & Os Password Grabber & Location Finder] With Ngrok," GitHub, [Online]. Available: https://github.com/ultrasecurity/Storm-Breaker?fbclid=IwAR2HX8B5RRQ2f-yRlWndAjxZM1PKfZxVZq-GM-9C_f317IFWGjdAVhcRHaY. [Zugriff am 14 03 2022].

[173] Reis, „GitHub – Rices/Phishious: Ein Open-Source-Evaluierungs-Toolkit für Secure Email Gateway (SEG), das für Red-Teamer entwickelt wurde.," [Online]. Available:

https://github.com/Rices/Phishious?fbclid=IwAR2OhR2kRNkAyyGS7skSzOwlRPEWDcxzFwzohAFuj_coiQFlMdq7t9wlh_k. [Zugriff am 15 03 2022].

[174] Section9Labs, „GitHub - Section9Labs/Cartero: Cartero - Social Engineering Framework," GitHub, [Online]. Available: GitHub - Section9Labs/Cartero: Cartero - Social Engineering Framework. [Zugriff am 15 03 2022].

[175] smsranger.io, „SMSranger is the most advanced SMS capture bot on the market," smsranger.io, [Online]. Available: https://smsranger.io/. [Zugriff am 14 03 2022].

[176] Can I Phsish Pty Ltd., „Free Phishing Simulation Software & Tools | CanIPhish," caniphish, [Online]. Available: https://caniphish.com/. [Zugriff am 15 03 2022].

[177] RSM US LLP, „GitHub - rsmusllp/king-phisher: Phishing Campaign Toolkit," RSM US LLP, [Online]. Available: https://github.com/rsmusllp/king-phisher. [Zugriff am 15 03 2022].

[178] Gophish, „Gophish - Open Source Phishing Framework," Gophish, [Online]. Available: https://getgophish.com/#. [Zugriff am 15 03 2022].

[179] Trace Labs, „Trace Labs | Search Party," [Online]. Available: https://www.tracelabs.org/initiatives/search-party. [Zugriff am 17 03 2022].

[180] A. S. Alazri, „The awareness of social engineering in information revolution: Techniques and challenges," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015.

[181] N. Pavkovic und L. Perkov, „Social Engineering Toolkit — A systematic approach to social engineering," in *2011 Proceedings of the 34th International Convention MIPRO*, Opatija, Croatia, 2011.

[182] A. Algarni, Y. Xu und T. Chan, „Social Engineering in Social Networking Sites: The Art of Impersonation," in *2014 IEEE International Conference on Services Computing*, Anchorage, AK, USA, 2014.

[183] S. Sun, C. Yan und J. Feng, „Analysis of Influence for Social Engineering in Information Security Grade Test," in *2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, China, 2012.

[184] L. J. Janczewski und L. R. Fu, „Social Engineering-Based Attacks: Model and New Zealand Perspective," in *Proceedings of the International Multiconference on Computer Science and Information Technology*, Wisla, Poland, 2010.

[185] R. Winter, S. Scheinert, M. Stanfill, A. Salter, O. B. Newton, J. Song, S. M. Fiore, W. Rand und I. Garibay, „A Taxonomy of User Actions on Social Networking Sites," in *31st ACM Conference on Hypertext and Social Media (HT'20)*, New York, USA, 2020.

[186] K. Nielsen und B. Kristensen, „End-to-end mapping of a spear-phishing attack," in *Proceedings of the European University Information Systems Conference 2021, Volume 78, Pages 89–97*, Denmark, 2021.

[187] H. J. Williams und I. Blum, „Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise," 2018. [Online]. Available: https://www.rand.org/pubs/research_reports/RR1964.html. [Zugriff am 13 11 2021].

[188] APWG - Anti Phising Workgroup, „Phishing Activity Trends Report 2nd Quarter 2021," 22 09 2021. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf. [Zugriff am 21 11 2021].

[189] A. S. L. Kowta, K. Bhowmick, J. R. Kaur und N. Jeyanthi, „Analysis and Overview of Information Gathering & Tools for Pentesting," in *2021 International Conference on Computer Communication and Informatics (ICCCI -2021)*, Coimbatore, India, 2021.

[190] M. H. K. T. Comia, J. S. R. Cruz, G. A. A. Ngceen und S. M. B. Gutierrez, „Social Engineering: Exploring Social Engineering Toolkits," 2017.

[191] S. Uebelacker und S. Quiel, „The Social Engineering Personality Framework," in *4th Workshop on Socio-Technical Aspects in Security and Trust 2014*, Vienna, Austria, 2014.

[192] T. Bakhshi, „Social Engineering: Revisiting end-user awareness and susceptibility to classic attack vectors," in *13th International Conference on Emerging Technologies (ICET)*, 2017.

[193] O. Jaafor und B. Birregah, „Multi-layered graph-based model for social engineering vulnerability assessment," in *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Paris, France, 2015.

[194] C. Freitas, F. Benevenuto, S. Ghosh und A. Veloso, „Reverse Engineering Socialbot Infiltration Strategies in Twitter," in *ASONAM '15: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, 2015.

[195] Z. Doffman, „Why Your Dating App Might Be Dangerous," Forbes Media LLC, 29 07 2020. [Online]. Available: https://www.forbes.com/sites/zakdoffman/2020/07/29/dating-app-dangerous-cyber-warning-iphone-android-update/?sh=407a73957775. [Zugriff am 20 12 2021].

[196] F. Salahdine und N. Kaabouch, „Social Engineering Attacks: A Survey," in *MDPI Jounals, Future Internet 2019, Volume 11, Issue 4*, 2019.

[197] A. C. Bahnsen, I. Torroledo, L. D. Camacho und S. Villegas, „DeepPhish: Simulating Malicious AI," 05 2018. [Online]. Available: https://albahnsen.files.wordpress.com/2018/05/deepphish-simulating-malicious-ai_submitted.pdf. [Zugriff am 28 12 2021].

[198] H. Böck, „Wissenschaft: Auf der Suche nach den Social Bots," Golem.de, 04 01 2022. [Online]. Available: https://www.golem.de/news/wissenschaft-auf-der-suche-nach-den-social-bots-2201-162154.html. [Zugriff am 05 01 2022].

[199] IVRE.rocks, „IVRE - Network recon framework," [Online]. Available: https://ivre.rocks/. [Zugriff am 05 03 2022].

[200] pinterest, „Pinterest - Profile," [Online]. Available: https://www.pinterest.at/search/users/?q=dominikhatkeininsta&rs=rs&eq%3D%3D=&etslf=1199&term_meta%5B%5D=dominikhatkeininsta%7Crecentsearch%7C0. [Zugriff am 11 03 2022].

[201] th3unkn0n, „GitHub - th3unkn0n/osi.ig: Information Gathering Instagram.," GitHub, [Online]. Available: https://github.com/th3unkn0n/osi.ig. [Zugriff am 12 03 2022].

[202] B. McCann, T. McCarthy, A. Ringwood, A. Dalton, M. Orru und A. Johnson, „Phishing Frenzy - Manage Email Phishing Campaigns - Penetration Tes," Phishing Frenzy, [Online]. Available: https://www.phishingfrenzy.com/. [Zugriff am 15 03 2022].