Co-funded by the Erasmus+ Programme of the European Union

InCyT-Trainingsmodule

Informationssicherheit für Mitarbeiter **Einheit Nr.: (4) Woche 7** **Name der Einheit (Modul): (Social Engineering)**	
Lernaktivitäten	❑ **Webinar** ❑ **Übungen** ❑ **Workshop** ❑ **Präsentation** ❑ **Sonstiges** Streaming Webinar, Text, Übungen zur Selbsteinschätzung, Übungen mit Antworten in Diskussionsforen und in den organisierten Sitzungen mit dem Trainer/Mentor, E-Portfolios
Lehrverantwortliche	• David Sommer • Ileana Hamburg
Ziele der Lernaktivitäten	1. Social-Engineering-Angriffstechniken 2. Die Bedeutung von Social Engineering Training 3. Wie man sich vor Phishing-Angriffen schützt 4. Social Engineering aus interdisziplinärer Sicht
Zu erwerbende Fertigkeiten	• **TS3 Netzsicherheit** • **TS4 Penetrationstests (ausnutzbare Sicherheitslücken)** • **SS3 Kognitions- und Verhaltensanalyse**
Dauer der Lernaktivität	2 Wochen
Lernenanforderungen	***Was wird benötigt?*** • Zugang zum Internet • Internet-Browser • MS Office365

Co-funded by the
Erasmus+ Programme
of the European Union

Kurze Informationen zum Modul

Beschreibung
Social Engineering ist eine wichtige und sehr häufige Bedrohung für die Informationssicherheit. Dieses Modul erklärt kurz den Lebenszyklus von Social Engineering, wie ein Angriff erfolgt und wie er verhindert werden kann. Insbesondere wird Phishing beschrieben, als einer der beliebtesten Social Engineering Angriffe. Viele Unternehmen setzen technische Lösungen ein, um Angriffe zu verhindern, aber technische Maßnahmen sind nicht sehr effektiv, wenn die Mitarbeiter nicht entsprechend geschult sind. Dies ist eines der Ziele dieser Einheit. Die Lernenden können sich über diese Aspekte informieren, indem sie den entsprechenden Text lesen, sich Streaming-Webinare ansehen und Übungen im eigenen Tempo lösen. Alle diese Dokumente befinden sich auf der digitalen interaktiven Projektplattform. Die Lernenden können ihre Antworten in den Selbsteinschätzungsübungen testen. Die Antworten auf die anderen Übungen sollten im entsprechenden Diskussionsforum gespeichert und mit dem Mentor bei dem wöchentlich stattfindenden gemeinsamen Treffen besprochen werden. Die Lernenden können vor allem während der Treffen mit anderen und dem Mentor kooperativ zusammenarbeiten. Sie werden dabei unterstützt, ein E-Portfolio zu erstellen, das für die Reflexion und Bewertung der Ausbildung wichtig ist.

Inhalt des Lernmaterials

Was ist Social Engineering?

Social Engineering kann definiert werden als die Manipulation von Menschen, meist mit Hilfe psychologischer Methoden, um Zugang zu Daten, Dokumenten und Informationen zu erhalten, zu denen der Angreifer keinen Zugang haben sollte. Schon vor Jahren gab es verschiedene Formen von Social Engineering, aber durch den zunehmenden Einsatz von Technologie in den wichtigsten Aspekten der Wirtschaft und des Lebens wachsen die Bedrohungen und werden zu einem komplexen Prozess, der schwer zu stoppen ist. Social Engineering ist heute eine der größten Bedrohungen für die Informationssicherheit und eine effektive Form der Internetkriminalität. Die möglichen Auswirkungen eines erfolgreichen sozialen Angriffs können für Menschen und Organisationen sehr gefährlich sein. Im Jahr 2019 war beispielsweise Phishing, eine Form der Social-Engineering-Kriminalität, für viele Datenschutzverletzungen verantwortlich, mehr als jede andere Art von Angriff.

Viele Social-Engineering-Angriffe haben finanziellen Schaden angerichtet und Organisationen erhebliche Geldbeträge gekostet. Im Jahr 2020 zum Beispiel, USA Verluste 4,2 Milliarden Dollar, nach dem FBI (Abbate, 2020).

Unternehmen könnten unter Betriebsunterbrechungen leiden - Produktivitätsverlust, sinkende Arbeitsmoral und Schwierigkeiten für die Organisation, sich zu erholen. Dieser Prozess kann Folgen haben: Oft wird ein Reaktionsteam entlassen, Sicherheitssoftware zur Verhinderung künftiger Angriffe sollte bereitgestellt werden und Mitarbeiter müssen neu qualifiziert werden. Unternehmen können im Falle eines Social-Engineering-Angriffs auch einen Imageschaden erleiden, weil die Kunden nicht davon überzeugt sind, dass das Unternehmen sich selbst schützen kann.

Die Bedeutung von Social Engineering Training

Es ist schwierig, sich gegen Social Engineering zu schützen, denn die Taktiken der Angreifer basieren auf dem Verhalten des Einzelnen, und wenn die Mitarbeiter nicht entsprechend geschult sind, um Social-Engineering-Angriffe zu erkennen, ist das Risiko, Opfer zu werden, groß.

Social-Engineering-Schulungen könnten in Programme zur Sensibilisierung für Sicherheitsfragen aufgenommen werden und geben den Mitarbeitern das Wissen und die Werkzeuge an die Hand, die sie benötigen, um diese Arten von Angriffen zu erkennen und sowohl sich selbst als auch ihr Unternehmen zu schützen (Weßelmann, 2008).

Aufgrund der Bedeutung von Social-Engineering-Schulungen für die Minimierung von Bedrohungen sollten viele Organisationen, insbesondere KMUs, die über weniger Ressourcen verfügen, dabei unterstützt werden, Cyber-Awareness-Schulungen einschließlich Social-Engineering sehr ernst zu nehmen und ihren Mitarbeitern die Möglichkeit zu bieten, daran teilzunehmen (Mimecast Contributing Writer, 2021).

Bis 2022 sollen beispielsweise 60 % der großen Unternehmen über Sicherheitsbewusstsein nachdenken (Gartner Magic Quadrant für SAT 2019).

Lebenszyklus eines Social Engineering-Angriffs

Social-Engineering-Angriffe werden oft in mehreren Schritten durchgeführt. Der Angreifer untersucht zunächst das vorgesehene Opfer, um die notwendigen Hintergrundinformationen zu sammeln, wie z. B. Einstiegspunkte und schwache Sicherheitsprotokolle, die für den Angriff benötigt werden. Dann versucht der Angreifer, das Vertrauen des Opfers zu gewinnen und Anreize für Handlungen zu schaffen, die normalerweise nicht zu den Sicherheitspraktiken gehören, wie z. B. die Preisgabe sensibler Informationen oder die Gewährung des Zugangs zu wichtigen Ressourcen. Abbildung 1 erläutert den Lebenszyklus eines Angriffs.

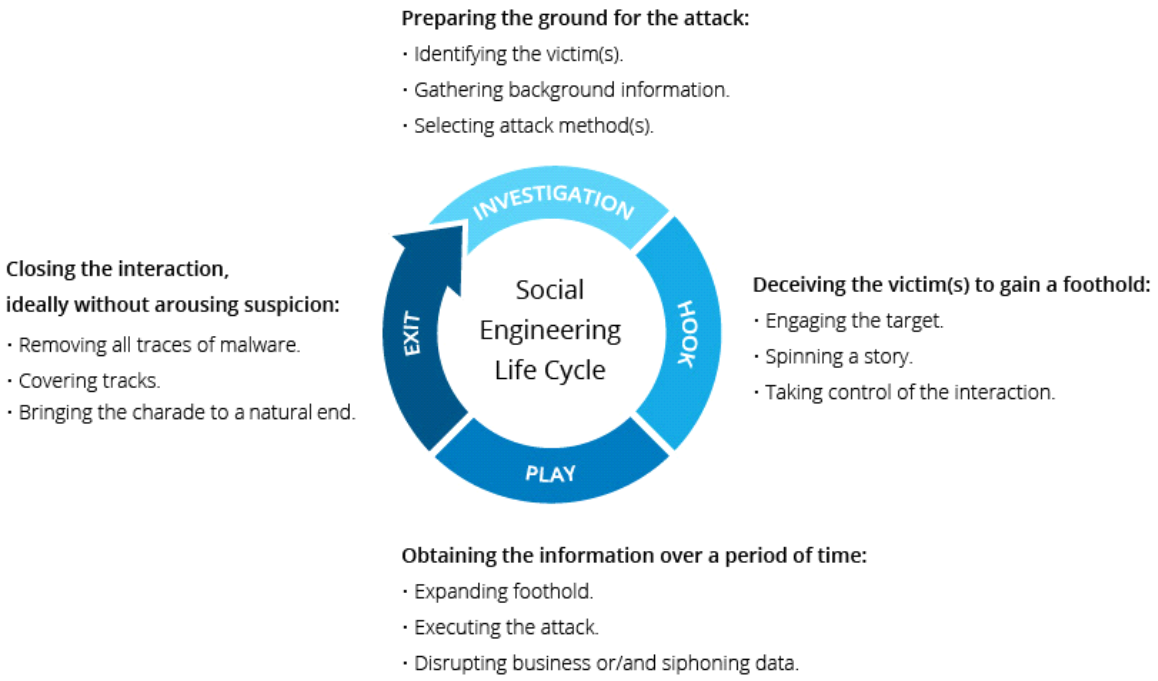

Abbildung 1: Lebenszyklus eines Angriffs (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Social Engineering ist besonders gefährlich, weil es eher auf menschlichem Versagen als auf Schwachstellen in Software und Betriebssystemen beruht. Es ist schwieriger, Fehler von legitimen Nutzern vorherzusehen, zu erkennen und zu stoppen als ein Eindringen mit Malware.

Social-Engineering-Angriffstechniken

Social-Engineering-Angriffe haben verschiedene Formen und können überall dort durchgeführt werden, wo menschliche Interaktion im Spiel ist. Die häufigsten Formen digitaler Social-Engineering-Angriffe sind die folgenden:

Köder

Köderangriffe versuchen, die Neugierde des Opfers zu wecken. Sie locken die Nutzer in eine Falle, um ihre persönlichen Daten zu stehlen oder ihre Systeme mit Malware zu infizieren. Die häufigste Form des Köderns verwendet physische Medien, um Malware zu verbreiten. So werden z. B. mit Malware infizierte Flash-Laufwerke an auffälligen Orten platziert, an denen sie von potenziellen Opfern mit Sicherheit gesehen werden (z. B. in Toiletten, Aufzügen oder auf dem Parkplatz des Zielunternehmens). Der Köder sieht authentisch aus, z. B. mit einem Etikett, das ihn als Gehaltsliste des Unternehmens ausgibt. Die Opfer nehmen den Köder auf und setzen ihn in einen Arbeits- oder

Heimcomputer ein, was zu einer automatischen Malware-Installation auf dem System führt. Köderangriffe müssen nicht unbedingt in der realen Welt stattfinden. Online-Formen von Köderangriffen bestehen aus verlockenden Anzeigen, die zu bösartigen Websites führen, die die Benutzer zum Herunterladen einer mit Malware infizierten Anwendung verleiten.

Scareware

Die Opfer werden zu Fehlalarmen und fiktiven Bedrohungen. Die Benutzer denken, dass ihr System mit Malware infiziert ist und sie Software installieren müssen, die nur für den Angreifer von Nutzen ist oder selbst Malware ist. Scareware wird als Täuschungssoftware, Rogue-Scanner-Software und Betrugsware bezeichnet. Ein gängiges Beispiel für Scareware sind die legitim aussehenden Popup-Banner im eigenen Browser beim Surfen im Internet mit Texten wie "Ihr Computer ist möglicherweise mit schädlichen Spyware-Programmen infiziert". Sie bieten entweder an, das Tool zu installieren (das oft mit Malware infiziert ist), oder leiten das Opfer auf eine bösartige Website, auf der der eigene Computer infiziert wird. Scareware wird auch über Spam-E-Mails verbreitet, in denen Benutzern der Kauf wertloser/schädlicher Dienste angeboten wird.

Pretexting

Der Angreifer erlangt Informationen durch eine Reihe von Lügen. Der Schwindel (Betrug) wird oft von einem Täter initiiert, der unterstellt, sensible Informationen von einem Opfer zu benötigen, um eine wichtige Aufgabe zu erfüllen. Der Angreifer beginnt in der Regel damit, Vertrauen zu seinem Opfer aufzubauen, indem er sich als Mitarbeiter, Polizist, Bank- und Steuerbeamter oder andere Personen ausgibt, die berechtigt sind, die Informationen zu erhalten. Der Angreifer stellt Fragen, die erforderlich sind, um die Identität des Opfers zu bestätigen, und gelangt so an wichtige persönliche Daten. Auf diese Weise können viele wichtige Informationen und Unterlagen erlangt werden, z. B. Sozialversicherungsnummern, persönliche Adressen und Telefonnummern, Telefondaten, Urlaubsdaten von Mitarbeitern, Bankdaten und sogar Sicherheitsinformationen zu einer Anlage.

Phishing

Phishing ist eine der beliebtesten Arten von Social-Engineering-Angriffen. Phishing-Betrügereien (Betrügereien) sind E-Mails und SMS-Kampagnen, die darauf abzielen, die Opfer neugierig zu machen oder zu verängstigen und sie dazu zu bringen, vertrauliche Informationen preiszugeben, auf Links zu bösartigen Websites zu klicken oder Anhänge zu öffnen, die Malware enthalten. Ein Beispiel ist eine E-Mail, die an die Benutzer eines Online-Dienstes geschickt wird und sie auf einen Verstoß gegen die Richtlinien hinweist, der sofortiges Handeln erfordert, wie z. B. eine erforderliche Passwortänderung. Sie enthält einen Link zu einer nicht legitimen Website, die fast genauso aussieht wie die legitime Version, und der Benutzer gibt seine aktuellen Anmeldedaten und sein neues Kennwort ein. Die Informationen werden an den Angreifer gesendet. Da bei Phishing-

Kampagnen identische oder nahezu identische Nachrichten an viele Benutzer gesendet werden, ist es für Mailserver, die Zugang zu Plattformen zur gemeinsamen Nutzung von Bedrohungen haben, einfacher, sie zu erkennen und zu blockieren.

Speer-Phishing

Hierbei handelt es sich um eine besondere Form des Phishing-Angriffs, da ein Angreifer bestimmte Personen oder Unternehmen auswählt. Die Angreifer passen ihre Nachrichten an Merkmale, berufliche Positionen und Kontakte ihrer Opfer an, um ihren Angriff unauffälliger zu gestalten. Spear-Phishing erfordert einen größeren Aufwand seitens des Täters (der Person, die die illegale Handlung begeht) und kann Wochen und Monate der Vorbereitung in Anspruch nehmen. Solche Angriffe sind viel schwieriger zu erkennen und haben eine höhere Erfolgsquote. Bei einem Spear-Phishing-Szenario beispielsweise gibt sich ein Angreifer als IT-Berater eines (bestehenden) Unternehmens aus und sendet eine E-Mail an einen oder mehrere Mitarbeiter. Sie ist genau so signiert, wie es der Berater normalerweise tut, und die Empfänger halten sie für eine authentische Nachricht. In der Nachricht werden die Opfer aufgefordert, ihr Kennwort zu ändern, und sie erhalten einen Link, der sie auf eine bösartige Seite weiterleitet, auf der der Angreifer ihre Anmeldedaten stiehlt.

Phishing erkennen

Betrüger (Personen, die betrügerische Geschäfte machen) verwenden E-Mails oder Textnachrichten, um Personen dazu zu bringen, ihre persönlichen Daten mitzuteilen. Sie versuchen, Passwörter, Kontonummern oder Sozialversicherungsnummern zu stehlen. Wenn sie diese Informationen erhalten, können sie sich Zugang zu E-Mail-, Bank- oder anderen Konten verschaffen. Täglich starten Betrüger Tausende von Phishing-Angriffen - und sie sind oft erfolgreich. Betrüger aktualisieren ihre Taktiken häufig, aber es gibt einige Anzeichen, die Opfern helfen, eine Phishing-E-Mail oder -SMS zu erkennen, wie die folgenden:

- Phishing-E-Mails und -SMS können so aussehen, als kämen sie von einem Unternehmen, das Sie kennen oder dem Sie vertrauen. Sie sehen aus, als kämen sie von einer Bank, einem Kreditkartenunternehmen, einem sozialen Netzwerk, einer Online-Zahlungswebsite oder -App oder einem Online-Shop.

- Phishing-E-Mails und -SMS erzählen oft eine Geschichte, um die Opfer dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen. Sie behaupten, dass sie verdächtige Aktivitäten oder Anmeldeversuche bemerkt haben, dass es ein Problem mit dem Konto oder den Zahlungsinformationen gibt, dass die Person einige persönliche Informationen bestätigen muss, fügen eine gefälschte Rechnung bei, wollen, dass die Person auf einen Link

klickt, um eine Zahlung zu leisten, sagen, dass die Person berechtigt ist, sich für eine staatliche Rückerstattung zu registrieren, usw.

Abbildung 2 zeigt ein reales Beispiel für ein Phishing.

Die E-Mail sieht aus, als käme sie von einem Unternehmen, das die Person kennt und dem sie vertrauen kann: Netflix. Sie verwendet sogar ein Netflix-Logo und eine Kopfzeile.

In der E-Mail heißt es, dass das eigene Konto wegen eines Abrechnungsproblems auf Eis liegt.

Die E-Mail hat eine allgemeine Begrüßung: "Hallo, mein Lieber". Wenn die Person ein Konto bei dem Unternehmen hat, würde es wahrscheinlich nicht eine solche allgemeine Begrüßung verwenden.

In der E-Mail wird die Person aufgefordert, auf einen Link zu klicken, um ihre Zahlungsdaten zu aktualisieren.

Diese E-Mail sieht vielleicht echt aus, ist es aber nicht. Die Betrüger, die E-Mails wie diese verschicken, haben nichts mit den Unternehmen zu tun, für die sie sich ausgeben. Phishing-E-Mails können reale Folgen für Personen haben, die den Betrügern ihre Daten geben. Und sie können den Ruf der Unternehmen, die sie vortäuschen, schädigen.

Schutz vor Phishing

Eigene E-Mail-Spamfilter können viele Phishing-E-Mails vom eigenen Posteingang fernhalten. Aber Betrüger versuchen immer wieder, Spam-Filter zu überlisten, daher ist es sinnvoll, zusätzliche Schutzmaßnahmen zu ergreifen.

Methoden zum Schutz:

- Um den eigenen Computer mit Sicherheitssoftware zu schützen, sollte die Software automatisch aktualisiert werden, um Sicherheitsbedrohungen zu begegnen.
- Um das eigene Mobiltelefon zu schützen, sollte die Software automatisch aktualisiert werden.
- Um die eigenen Konten zu schützen, sollte eine Multi-Faktor-Authentifizierung verwendet werden.

Die zusätzlichen Anmeldedaten für die Anmeldung beim eigenen Konto können in Gruppen zusammengefasst werden:

- Einen Passcode erhält man über eine Authentifizierungs-App oder einen Sicherheitsschlüssel.
- Ein Scan des eigenen Fingerabdrucks, der Netzhaut oder des Gesichts.

Die Multi-Faktor-Authentifizierung erschwert es Betrügern, sich bei anderen Konten anzumelden, wenn sie an den entsprechenden Benutzernamen und das Passwort gelangen. Es ist wichtig, die eigenen Daten durch Backups zu schützen, die nicht mit dem eigenen Heimnetzwerk verbunden sind. Eigene Computerdateien sollten auf eine externe Festplatte oder einen Cloud-Speicher kopiert werden. Auch die Daten auf dem eigenen Telefon sollten kopiert werden.

Verhalten bei Verdacht auf einen Phishing-Angriff

- Wenn Sie eine E-Mail oder eine Textnachricht erhalten, in der Sie aufgefordert werden, auf einen Link zu klicken oder einen Anhang zu öffnen, fragen Sie nach: Habe ich ein Konto bei diesem Unternehmen oder kenne ich die Person, die mich kontaktiert hat?
- Wenn die Antwort "Nein" lautet, könnte es sich um einen Phishing-Betrug handeln. Lesen Sie die Tipps unter "Wie man Phishing erkennt", achten Sie auf Anzeichen für einen Phishing-Betrug, melden Sie die Nachricht und löschen Sie sie.
- Wenn die Antwort "Ja" lautet, kontaktieren Sie das Unternehmen über eine Telefonnummer oder eine echte Website, ohne die Informationen in die E-Mail aufzunehmen, da Anhänge und Links schädliche Malware installieren können.

Reagieren auf eine Phishing-E-Mail

Auf der Grundlage der verlorenen Informationen sind bestimmte Schritte zu unternehmen

- Führen Sie einen Scan durch.
- Wenn Sie eine Phishing-E-Mail oder -SMS erhalten, melden Sie sie.

Social Engineering aus interdisziplinärer Sicht

Die vernetzte Welt von heute und die intensive Nutzung des Internets und der Technologie sind Katalysatoren für Social Engineering-Angriffe. Systemschutzmaßnahmen sind hilfreich, um einige Social-Engineering-Angriffe zu entschärfen, aber sie reichen nicht aus. Das Federal Bureau of Investigation's Internet Crime unterstreicht den zunehmenden Einsatz von Social Engineering und E-Mail-Betrug in Unternehmen, der in den letzten Jahren zu Verlusten in Milliardenhöhe geführt hat (Abbate, 2020). Auch bei den Methoden der Hacker ist ein interdisziplinärer Ansatz erforderlich, um dieses Phänomen mit all seiner Komplexität zu verstehen, insbesondere im Zusammenhang mit den Auswirkungen auf Unternehmen. In Literaturübersichten werden Perspektiven aus verschiedenen Disziplinen aufgezeigt: Informationstechnologie, Psychologie, Wirtschaft und Ethik. Abbildung 3 veranschaulicht diese Sichtweise (Washo, 2021).

Disziplin der Informationstechnologie

Social Engineering kann nur im Zusammenhang mit den eigentlichen Informationssystemen und deren Einsatz im Unternehmen diskutiert werden. Technische Schutzmaßnahmen können als eine Form der Risikominderung eingesetzt werden, und es wird empfohlen, Kontrollstrategien zu verwenden. Die Multi-Faktor-Authentifizierung ist eine gängige und oft wirksame Methode für Unternehmen, um zu bestätigen, dass die Person, die auf die Systeme zugreift, auch tatsächlich über diesen Zugang verfügen sollte. Ein Anmeldeverfahren mit einem Benutzernamen und einem Kennwort wäre zum Beispiel eine Möglichkeit, den Benutzer zu authentifizieren. Ein zusätzlicher

Faktor könnte die Verwendung einer Anmeldung über ein virtuelles privates Netzwerk (VPN) sein, um den Benutzer weiter zu validieren.

Disziplin Psychologie

Da Social Engineering mit Täuschung verbunden ist, ist ein psychologischer Ansatz zum Verständnis des Konzepts wichtig, um die Gedanken und Verhaltensweisen sowohl des Angreifers als auch des Opfers zu verstehen. Der Einsatz psychologischer Methoden ist für Social Engineering wichtig, da sie zur Unterstützung von Schutzmaßnahmen wie Firewalls und Systemen zur Identifizierung von Eindringlingen eingesetzt werden (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). Das gesamte informationstechnische Netzwerk eines Unternehmens ist nur so stark wie der einzelne Nutzer eines bestimmten Systems. Tatsächlich sind das Verhalten und die Handlungen der Mitarbeiter eine der Hauptursachen für Datenverletzungen.

Geschäftsperspektive

Social Engineering wirkt sich auf viele Arten von Unternehmen aus und hat Auswirkungen auf die Art und Weise, wie Organisationen strukturiert und verwaltet werden. Das Thema kann aus der Unternehmensperspektive betrachtet werden, um die Faktoren zu ermitteln, die sich auf Social Engineering-Angriffe auswirken. Diese Sichtweise ist von Vorteil, wenn sie sich auf die folgenden Unternehmensbereiche bezieht: Schulung und Entwicklung, dokumentierte Richtlinien, interne Prüfverfahren, Budgets und Organisationskultur. Ein Mangel in einem dieser Bereiche kann zu Angriffen beitragen.

Ethische Perspektive

Ethik ist im Zusammenhang mit Social Engineering und der damit verbundenen Forschung zu diesem Thema wichtig. Die Idee, einen anderen Menschen zu manipulieren, verstößt gegen viele ethische Grundsätze. Im Falle eines Social-Engineering-Vorfalls kann die Behandlung der Opfer unterschiedlich sein, aber oft werden sie nicht ausreichend behandelt, um den Angriff zu ermöglichen. Leider sind die Eigenschaften, die man normalerweise bei idealen Mitarbeitern findet, wie Vertrauen, die Bereitschaft, es anderen wie Managern, Kunden, Kollegen und Besuchern recht zu machen, und die Bereitschaft, Autoritäten zu gehorchen, in der Regel dieselben, die eine Person für Social Engineering anfällig machen (Mouton, Malan, Kimppa, & Venter, 2015).

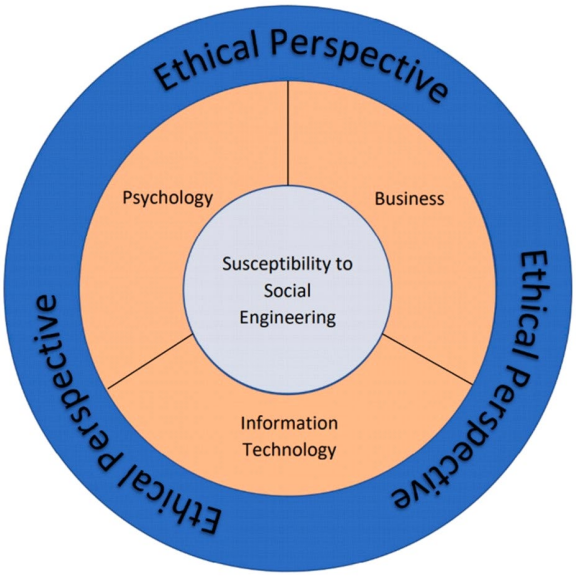

Abbildung 3: Social Engineering aus interdisziplinärer Sicht (Washo, 2021)

Der Literaturüberblick aus verschiedenen Disziplinen verdeutlicht die Notwendigkeit eines integrierten Ansatzes zur Untersuchung des komplexen Themas Social Engineering. Jede Disziplin liefert Informationen darüber, wie das Thema zu verstehen und zu interpretieren ist, wie man sich gegen verschiedene Arten von Angriffen schützen kann und wie man die Auswirkungen von Social Engineering sowohl aus menschlicher als auch aus organisatorischer Sicht versteht. Die Interpretation des Themas durch die einzelnen Disziplinen ist jedoch nur sinnvoll, wenn sie im Kontext der anderen Disziplinen betrachtet wird.

Fragen:

Fragen Diskussionsforum, die mit einer kurzen Erklärung beantwortet werden müssen. Die Antworten werden mit dem Mentor während der Mentoring-Sitzungen besprochen

1. Wie man Phishing erkennt: Phishing-E-Mails und -SMS erzählen oft eine Geschichte, um die Opfer dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen.
2. Wie man sich vor Phishing-Angriffen schützt
3. Nennen Sie bitte einige Disziplinen, die mit Social Engineering verbunden sind, und erläutern Sie kurz diese Verbindungen

Anhänge:

1. Präsentation
2. Video-Filme

Referenzen:

Abbate, P., (2020). Bericht zur Internetkriminalität 2020
URL: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullee, J.W.H, Montoya, L., Pieter, W., Junger, M, Hartel, P. (2017). On the anatomy of social engineering attacks - A literature-based dissection of successcul attacks. *Journal of Investigative Psychology and Offender Profiling. 15. 20-45.*

Lee, T. (2020). Die richtigen Lehrkräfte für ein besseres Sicherheitsbewusstsein einstellen. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast Contributing Writer (2021). Social Engineering Awarness Training für Angestellte. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Die Notwendigkeit von Ethik in der Social-Engineering-Forschung. Computers & Security, 55, 114-127. https://doi.org/10.1016/j. HYPERLINK "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). Ein interdisziplinärer Blick auf das Social Engineering: Ein Aufruf zum Handeln für die Forschung. URL:
https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. In: Datenschutz und Datensicherheit. DuD. 601-604.