Social Engineering – Warum wir auch 2024 „gehackt" werden und was wir dagegen tun können

Dieses Vorlesungsskript ergänzt den am 8.1.2024 gehaltenen Gastvortrag an der Universität Regensburg. Der Inhalt ist ausschließlich für Hörer (m/w/d) des Gastvortrags bestimmt. Die aktuelle Version des Skripts ist unter bs83.de verfügbar.

Motivation

Für eine Privatperson kann es zunächst nicht trivial nachvollziehbar sein, warum man sich eigentlich mit Social Engineering auseinandersetzen sollte. Allerdings ist ganz klar jede Privatperson potenzielles Ziel eines Angreifers. Resultate eines Angriffs können beispielsweise sein:

- Jemand stiehlt uns Geld, unter Umständen sehr viel Geld.
- Jemand bestellt in unserem Namen Waren und bezahlt nicht. Dies kann sehr negative Folgen auf die eigene Bonitätsbewertung (Stichwort „Schufa") haben.
- Jemand übernimmt unsere Identität, um Dritte anzugreifen (Freunde, Familie, Arbeitgeber, Kollegen).
- Jemand verschlüsselt all unsere Dateien wie bspw. Fotos oder die wichtige Abschlussarbeit und erpresst uns (Stichwort „Ransomware").
- Jemand spioniert uns aus.

Für Unternehmen (vom kleinen Familienbetrieb bis zum Konzern) können erfolgreiche Social-Engineering-Angriffe in schmerzhaften bis existenzbedrohenden finanziellen Verlusten resultieren, wirken sich in der Regel aber ebenso negativ auf Vertrauens- und Geschäftsbeziehungen aus.

Insgesamt kann der durch Social Engineering verursachte Schaden immens sein, egal, ob man eine Privatperson, ein Familienbetrieb oder ein Konzern ist.

Was ist Social Engineering und betrifft mich das?

Social Engineering ist im weitesten Sinn die Manipulation eines menschlichen Opfers, um dieses Opfer zum gewünschten Handeln zu bewegen.

Definitionen

- Angreifer: Ein Angreifer ist in diesem Skript ein Oberbegriff für die Partei, die uns durch ihre Aktion schaden oder uns negativ zu ihrem Vorteil beeinflussen will. Bsp. Cyberkriminelle, Betrüger, „Hacker“.
- Social Engineering: Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. (BSI) Beim Social Engineering nutzt der Täter den „Faktor Mensch“ als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen. (BSI)

Betroffenheit

In den Medien gibt es fast täglich Dutzende Berichte zu erfolgreichen Social-Engineering-Angriffen. Typische Medienberichte sind bspw.:

- im Unternehmensbereich: Cyberangriff, Ransomwareangriff
- bei Privatpersonen: Enkeltrick, Telefonbetrug, Love Scam, Identitätsdiebstahl

Jeder Mensch kann Opfer von Social-Engineering-Angriffen werden, völlig egal, wie technisch versiert man ist. Social Engineering ist ein psychologisches, kein technisches Thema. Social Engineers nutzen unsere menschlichen Eigenschaften und unser unkontrolliertes Unterbewusstsein aus.

Unser Unterbewusstsein ermöglicht es uns, Dinge automatisch und schnell zu erledigen, wie bspw. Atmen und Gehen. Allerdings fehlt uns hierbei größtenteils die Kontrolle. Das zeigt sich bspw. bei spontaner Gestik und Mimik oder beim Wahrnehmen bekannter Muster wie „3+x = 5“. Obwohl in diesem Absatz nichts über Mathematik steht und auch keine Aufgabe gestellt wurde, erkennt unser Unterbewusstsein in „3+x = 5“ ein erlerntes Muster und berechnet die Aufgabe automatisch.

Wie arbeitet ein „Social Engineer“?

Social-Engineering-Angriffe können grob in vier Phase eingeteilt werden. Diese vier Phasen können beliebig lange dauern und sich wiederholen, auch sind Rücksprünge oder ein vorzeitiges Ende möglich. Ein erfolgreicher Social-Engineering-Angriff kann unmittelbar in einem neuen Angriff mit anderen Opfern resultieren. Siehe auch https://www.social-engineer.org/framework/attack-vectors/attack-cycle/.

Phase 1: Der Social Engineer sammelt und kombiniert Informationen über Opfer.

In der ersten Phase sammelt sammelt der Social Engineer Informationen über sein potenzielles Opfer. Das potenzielle Opfer kann dabei eine Einzelperson oder auch mehrere Personen (bspw. Beschäftigte eines Unternehmens) sein.

Social Engineers können heutzutage auf eine Vielzahl digitaler Ressourcen für die Phase 1 zurückgreifen. Quellen für Informationen können Suchmaschinen, soziale Netzwerke, Datenlecks, Webseiten, Instant-Messenger-Gruppen, exponierte Server sein.

Hier müssen Sie auch an „unsichtbare" Daten denken: Diensteanbieter im Internet sammeln häufig mehr Daten, als nur das, was wir eingeben (bspw. IP-Adressen, Informationen über Ihren Webbrowser, Login-Zeitpunkte und -Zeiträume, Standorte, persönliche Interessen, ...). Auch diese „unsichtbaren" Daten sind am Ende in Datenbanken gespeichert, die Angreifer erhalten könnten (und könnten öffentlich einsehbar sein).

Social Engineers kombinieren die Einzelinformationen nach und nach miteinander, analog zu einem Puzzle. Dabei unterstützen Tools wie Maltego. Auf diese Weise können aus unscheinbaren Einzelinformationen umfassende Profile der potenziellen Opfer werden. Findet ein Social Engineer jedoch kaum etwas oder nichts über das potenzielle Opfer, kann ein möglicher direkter Angriff unter Umständen in Phase 1 gestoppt werden.

Inwieweit eigene E-Mail-Adressen in Datenlecks enthalten sein könnten, kann man mit Have I Been Pwned oder dem HPI Identity Leak Checker prüfen.

Phase 2: Der Social Engineer interagiert mit potenziellen Opfern (Aufbau einer Vertrauensbeziehung aka „Rapport").

Nachdem potenzielle Opfer ermittelt und ausreichend Informationen beschafft worden sind, erarbeitet der Social Engineer Vorwände und Gründe, um dann mit einer ggf. falschen Identität mit dem Opfer zu interagieren.

Beispiel: Nachdem ein Social Engineer („Betrüger") mehrere alleinlebende ältere Damen und Herren als potenzielle Opfer des „Enkeltricks" identifiziert hat, bereitet er auf Basis vorhandener Informationen einen Vorwand vor. Beispielsweise soll es in letzter Zeit viele Einbrüche in der Straße gegeben haben, weshalb sich der Social Engineer mit der falschen Identität eines angeblichen Polizisten über die Sicherheitsmaßnahmen im Haus informieren will. Mit diesem Vorwand und einem

passenden Aussehen sucht der Social Engineer die Opfer zu Hause auf und interagiert mit diesen. Dabei wird eine Vertrauensbeziehung (hier bspw. über die Autorität, angeblich Polizist zu sein) aufgebaut.

Natürlich kann es aber auch sein, dass das Opfer misstrauisch wird und der Angriff in dieser Phase fehlschlägt oder der Social Engineer noch einmal zu Phase 1 zurückspringt, um sich noch besser über das Opfer zu informieren.

Phase 3: Der Social Engineer nutzt das Opfer aus, um eigene Ziele zu erreichen. Sobald ein ausreichendes Vertrauensverhältnis zwischen Social Engineer und Opfer besteht, nutzt der Social Engineer das Opfer aus. Da das Opfer in diesem Augenblick dem Social Engineer vertraut, schöpft es zunächst keinen Verdacht.

Beispiel von Phase 2: Der Social Engineer überzeugt eine alte Dame, zunächst ihr Haus betreten zu dürfen, um sich dort über Sicherheitsmaßnahmen zu informieren. Er erklärt dann, dass diese Sicherheitsmaßnahmen aktuell nicht ausreichen und empfiehlt der Dame, ihr Bargeld umgehend zur Bank zu bringen. In einem unbeobachteten Moment entwendet der Social Engineer Wertsachen.

Natürlich kann es aber auch sein, dass das Opfer misstrauisch wird und der Angriff in dieser Phase fehlschlägt oder der Social Engineer noch einmal zu Phase 1 oder 2 zurückspringt.

Phase 4: Der Social Engineer verwischt Spuren und hinterlässt einen unauffälligen, positiven Eindruck (es kommt zunächst oder nie Verdacht auf). Im idealen Fall hinterlässt der Social Engineer nach Erreichen der eigenen Ziele einen unauffälligen, positiven Eindruck und das Opfer bemerkt den erfolgreichen Angriff nie oder erst nach einigen Monaten.

Beispiel von Phase 2 und 3: Der Social Engineer fährt das Opfer zur Bank, wo es tatsächlich das Bargeld auf das eigene Konto einzahlt. Im Anschluss fährt der Social Engineer das Opfer wieder nach Hause und überreicht ihr noch eine echte Broschüre der Polizei über Einbruchsprävention. Er verabschiedet sich freundlich. Das Opfer bemerkt den erfolgten Diebstahl einige Zeit nicht.

Hier muss man beachten: Selbst wenn das Opfer irgendwann den Angriff als solchen erkennt und „das Kind schon im Brunnen ertrunken ist“, verschweigen oder verbergen ausgenutzte Opfer dies oder können sich nicht mehr an Details erinnern, die zur Strafverfolgung notwendig wären.

Wie sehen echte Social-Engineering-Angriffe aus?

Je nach Literatur und Quelle werden eine Vielzahl an Angriffstechniken und -mustern dem Social Engineering zugeordnet. Nachfolgend einige häufige Techniken heutzutage sowie historisch erfolgreiche Social Engineers zur weiteren Recherche.

Beispiel: Sextortion

- Situation: Der Angreifer behauptet, das Opfer beim Pornokonsum gefilmt zu haben. Dazu sei Schadsoftware auf dem Gerät des Opfers installiert oder das Gerät gehackt worden. Als „Beweis“ schickt der Angreifer oft ein echtes Passwort des Opfers mit. Wenn das Opfer nicht zahle, werde das Videomaterial veröffentlicht.
- Mögliches Ziel des Angreifers: Geld vom Opfer erhalten.
- Hinweis: Oftmals sind Datenlecks Ausgangspunkt dieser Angriffe. Wenn in einem Datenleck E-Mail-Adressen und Passwörter enthalten sind, schreibt der Angreifer (automatisiert) alle enthaltenen E-Mail-Adressen inkl. des jeweiligen Passworts an.

Beispiel: Romance Scams, Love Scams, Dating-Betrug, Tinder-Trading-Scam

- Situation: Der Angreifer baut über einen verhältnismäßig langen Zeitraum eine enge Vertrauensbeziehung zum Opfer auf.
- Mögliches Ziel des Angreifers: Geld vom Opfer erhalten. Oftmals in Form kleinerer Beträge mit Vorwänden über einen langen Zeitraum, teils in Form von Wertkarten, Gutscheinen oder Kryptowährung.
- Hinweis: Das Opfer kann nach einem solchen Vorfall stark traumatisiert sein. Dieser Angriff kann also nicht „nur“ finanzielle Folgen haben.

Beispiel: „Hallo Mama, ...“

- Situation: Der Angreifer sendet an potenzielle Opfer bspw. SMS, um sich als Sohn oder Tochter des Opfers auszugeben. Oft wird behauptet, das Telefon sei defekt oder die SIM-Karte gesperrt, weshalb das vermeintliche Kind dringend finanzielle Unterstützung des Opfers brauche (bspw. anstehende Überweisung).
- Mögliches Ziel des Angreifers: Geld vom Opfer erhalten. Oft in Form einer Überweisung (drei- bis vierstelliger Betrag).

Beispiel: Loverboy, Cybergrooming

- Situation: Der Angreifer baut eine enge Vertrauensbeziehung zum jungen Opfer auf, gibt sich als liebender (erster) Freund aus.
- Mögliches Ziel des Angreifers: Ultimativ hat diese Angriffsart oft Prostitution als Ziel.

Beispiel: Phishing

- Situation: Der „Klassiker“ im IT-Bereich, bei dem sich der Angreifer als vertrauenswürdiger Kommunikationspartner ausgibt. Funktioniert heutzutage oft ebenso per Instant Messenger, SMS oder Sprachanruf. Hierbei wird eine gigantische Bandbreite an Gründen und Vorwänden hervorgebracht, damit das Opfer etwas tut. Beispiele: DHL-Paket verfolgen, Steuerrückzahlung erhalten, Gewinn ausschütten, Passwortablauf verhindern, kostenlosen Speicherplatz sichern, ...
- Mögliches Ziel des Angreifers: In der Regel wird das Opfer auf nachgeahmte Login-Seiten weitergeleitet, um das Passwort zu „phishen“. Es gibt allerdings ebenso Varianten, wo Opfer Schadsoftware installieren oder Informationen preisgeben sollen.

Beispiel: Baiting

- Situation: Ein Angreifer legt einen „Köder“ (= Bait) aus, um die Neugierde des Opfers auszunutzen. Beispiele sind herrenlose USB-Sticks an von potenziellen Opfern frequentierten Orten (bspw. Parkplätze, Verkehrsmittel).
- Mögliches Ziel des Angreifers: Über Schadsoftware oder spezielle Hardware (siehe auch „USB Rubber Ducky“) Fernzugriff auf Geräte des Opfers erhalten oder Informationen stehlen.

Beispiel: Water holing

- Situation: Der Angreifer präpariert einen von Opfern genutzten Onlinedienst mit Schadsoftware. Opfer infizieren sich anschließend darüber. Es wird die Vertrauensbeziehung zwischen Opfern und dem bereits genutzten Onlinedienst ausgenutzt.
- Mögliches Ziel des Angreifers: Über Schadsoftware Fernzugriff auf Geräte des Opfers erhalten oder Informationen stehlen.

Beispiel: Impersonation

- Situation: Ein Angreifer täuscht die Identität einer anderen Person vor, um damit schadhafte Aktionen durchzuführen. Dies kann sehr lange negative Folgen für das Opfer haben.
- Mögliches Ziel des Angreifers: Alles. Letztendlich ist „Impersonation“ eine Art Multitool für den Social Engineer.

Historisch bekannte Social-Engineering-Angriffe

In der Geschichte der Menschheit (keine Sorge, so weit geht es nicht zurück) gab es lange vor iPhones und Computern erfolgreiche und weit bekannte Social-Engineering-Angriffe. Nachfolgend einige Beispiele:

- George C. Parker (* 1870; † 1936) verkaufte unter Vorwänden Sehenswürdigkeiten in New York City an Touristen und Einwanderer.
- Victor Lustig (* 1890; † 1947) verkaufte 1925 einem französischen Schrotthändler den Eiffelturm.
- „Bernie“ Madoff (* 1938; † 2021) schädigte durch Anlagebetrug nach dem Ponzi-Schema mindestens 4800 Klienten bei einer Schadenssumme von mindestens 51 Milliarden Euro.
- Frank William Abagnale Jr. (* 1948) gab sich lange als Pilot aus, um so vertrauenswürdiger zu erscheinen und Geld/Privilegien zu erhalten. Dies wurde als „Catch Me If You Can“ (2002) verfilmt.
- Kevin David Mitnick (* 1963; † 2023) nutzte SE für Angriffe auf IT-Systeme.

Zu den jeweiligen Personen existieren teils umfangreiche Wikipedia-Artikel und Literatur.

Für das Selbststudium

Im Internet gibt es eine Vielzahl an Ressourcen, um sich über gängige Social-Engineering-Angriffe zu informieren. Im Privatbereich können dies Behörden-Auftritte (bspw. Polizei, BKA) sein. Nachfolgend einige leicht verdauliche Videos:

- Enkeltrick: https://www.youtube.com/watch?v=tErPkPB-8TY
- Trickbetrüger am Telefon: https://www.youtube.com/watch?v=5-nnqmxqsow
- Prävention Trickbetrug: https://www.youtube.com/watch?v=cqoJ51krkGE
- Schockanrufe: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/230524_Schockanrufe.html
- Cybergrooming: https://www.youtube.com/watch?v=kYOfqKkPxb0
- Loverboys: https://www.youtube.com/watch?v=P75SwvN5TWU

Wie hilft Information Security Awareness?

Nach der Betrachtung der Angreiferseite, also was Social Engineering ist, wie es funktioniert und wie Angriffe aussehen, widmen wir uns der Verteidigung dagegen.

Ein zentraler Bestandteil ist Bewusstsein für Social Engineering zu entwickeln. Im Unternehmensbereich können Awarenessmaßnahmen vermitteln, wie Beschäftigte Social Engineering erkennen, verhindern und ggf. korrekt darauf reagieren.

Natürlich können und sollten wir alle gemeinsam ebenso im Privatbereich Familie, Freunde und Bekannte auf gängige Social-Engineering-Angriffe hinweisen (siehe bspw. „Hallo Mama“-Nachrichten oder den „Enkeltrick“).

Zunächst folgen einige Überlegungen, was man selbst tun kann, um Social Engineering zu verhindern oder zu erschweren.

Tipps gegen Social Engineering

- Überlegen Sie vor Registrierung bei jedem Onlinedienst, ob Sie diesen wirklich brauchen. Informationen, die Sie gar nicht erst über sich selbst preisgeben, können auch nicht gestohlen und gegen Sie verwendet werden.
- Seien Sie sich bewusst, welche „unsichtbaren“ Daten ein Anbieter über Sie sammelt. Teilweise speichern Anbieter viel mehr Daten über uns, als wir wirklich direkt eingeben.
- Teilen Sie nicht alles offen im Internet: Setzen Sie Ihre Profile auf „privat“. Entfernen Sie sensible Daten und Metadaten aus Dateien.
- Pro Tipp: Verfahren Sie in Anlehnung an *Schnelles Denken, langsames Denken* gemäß **Vollbremsung und Kontext prüfen**, wenn Sie in eine unbekannte oder seltsame Situation geraten — auch offline. Bremsen Sie Ihr Unterbewusstsein und denken Sie logisch nach! Handeln Sie **nicht** automatisch und schnell!

Tipps im Umgang mit Zugangsdaten

Auch wenn „passwordless“-Verfahren langsam im Kommen sind, sind Zugangsdaten wie Passwörter weiterhin im Alltag in Verwendung. Seit Jahren gibt es Hilfsmittel wie Passwortmanager, um uns beim *Managen* unserer Passwörter zu unterstützen.

- Nutzen Sie kostenlose Passwortmanager wie bspw. KeePassXC (Windows, Linux, macOS), KeePassDX (Android), Keepassium (iOS). Diese funktionieren ohne „Cloud“.
- Alternativ gibt es Bitwarden.

Informieren Sie sich, wie diese Passwortmanager funktionieren, insbesondere, welche Features es gibt und was Sie brauchen. Diese Tools können bei richtiger Verwendung den Umgang mit Passwörtern erheblich vereinfachen und gleichzeitig in verbesserter Sicherheit resultieren.

Zusätzlich zur Verwendung von klassischen Passwörtern bieten immer mehr Dienste Multi-Faktor-Authentifizierung (MFA). Auch dies sollte man stets aktivieren und nutzen. Gängige Verfahren sind OATH-TOTP, U2F und WebAuthn bzw. Zwei-

Schritt-Verifizierung. MFA kann teils mithilfe eines Passwortmanagers genutzt werden oder greift auf zusätzliche Hardware zurück, wie beispielsweise das eigene Smartphone oder YubiKeys.

Weitere Empfehlungen:

- Setzen Sie je Onlinekonto ein individuelles Passwort. Hintergrund: Wenn ein Anbieter Ihr Passwort nicht ausreichend sicher speichert (bspw. im Klartext in einer Datenbank) und dies Dritten bekannt wird, ist nur ein einziges Ihrer Konten betroffen.
- Ändern Sie umgehend Ihr Passwort, wenn ein Datenleck beim dazugehörigen Anbieter bekannt wird. Teilweise können Tage, Wochen oder Monate dauern, bis der Anbieter einen Sicherheitsvorfall wie ein Datenleck vollständig untersucht hat. In dieser Zeit könnten Angreifer mit Ihren Zugangsdaten Schaden anrichten.
- Löschen Sie Onlinekonten, die Sie nicht mehr brauchen. Was nicht mehr da ist, kann auch nicht angegriffen werden. Beachten Sie aber, dass teils gesetzliche Aufbewahrungsfristen bestehen, sodass manche Informationen über Sie teils erst nach Jahren oder Jahrzehnten gelöscht werden können.
- Setzen Sie niemals erratbare Informationen bei „Passwort vergessen“-Fragen. Die „Passwort vergessen“-Funktion war lange Zeit eine beliebte Hintertür für Angreifer, um Ihr (starkes) Passwort einfach zu umgehen!
- Machen Sie ausreichend Backups Ihrer Passwortdatenbanken. Eine Backup-Faustregel ist 3-2-1: Drei Kopien der Originaldaten, auf zwei unterschiedlichen Medienarten (bspw. USB-Stick, externe Festplatte) und eine Kopie an einem anderen vertrauenswürdigen Ort (bspw. bei Eltern oder in der „Cloud“).

Für Fortgeschrittene:

- Nutzen Sie je Onlinekonto auch individuelle E-Mail-Adressen bzw. E-Mail-Aliase. Dies ermöglicht bei einem plötzlichen Aufkommen von Spam oder Angriffsversuchen die Ursache schneller zu ermitteln, auch wenn der betroffene Anbieter noch gar nicht öffentlich über ein Datenleck berichtet hat.
- Dokumentieren Sie bei jedem Eintrag im Passwortmanager, welche personenbezogenen Daten Sie bewusst angegeben haben (bspw. IBAN, physische Adresse, Mobiltelefonnummer). Diese Informationen können bspw. als Tags hinterlegt werden. Auf diese Weise wissen Sie ungefähr, welche Informationen bei einem Datenleck abhanden gekommen sein könnten.

Für das Selbststudium

Lesen Sie sich die nachfolgenden Situationen durch und machen Sie jeweils Vorschläge, welche Maßnahmen in einer verbesserten Sicherheit resultieren könnten. Diese Übung soll das Erarbeiten von Awarenessmaßnahmen trainieren.

- Finn ist Student und Gamer seit seiner Kindheit. Er hat seinen PC selbst zusammengestellt und nutzt immer noch ein raubkopiertes Windows 7, weil das sowieso besser als Windows 11 ist und was soll schon passieren? Für ein manche Singleplayer-Spiele hat er „Cracks“ installiert. Weil es manchmal Probleme beim Starten der Spiele gibt, hat er die Windows Firewall laut irgendeinem Forum deaktiviert.
- Sophia ist begeisterte Shopperin im Internet und kauft seit sieben Jahren bei Dutzenden Onlineshops alles Mögliche ein. Den einen oder anderen Account hat sie schon vergessen, aber ihr Passwort nicht. Das ist MaX-2017!. Max ist ihr treuer Hund, der auf Insta einen großen Fanclub hat. Sie postet dort ihren halben Alltag.

Wie kann ich Awareness im Unternehmen umsetzen?

Information Security Awareness in Normen und Standards

Information Security Awareness findet sich in gängigen Normen und Standards wie der ISO/IEC 27001 (7.3 Awareness; A.7.2; A.7.2.2) oder auch im BSI IT-Grundschutz (ORP.3 Sensibilisierung und Schulung zur Informationssicherheit). *Aus rechtlichen Gründen wird an dieser Stelle nicht aus dem Normen zitiert.*

Eine Awarenesskampagne durchführen

Wiederkehrende, abwechslungsreiche Awarenesskampagnen können das Bewusstsein für Social-Engineering-Angriffe, Sicherheitsbedrohungen und geltende Richtlinien und Gesetze steigern.

Gründe für eine Awarenesskampagne sind unter anderem:

- Ein Unternehmen kann niemals einen 100-prozentigen technischen Schutz erreichen. Es gibt demnach immer Situationen, in denen Menschen nicht durch Technologie geschützt werden können.
- Ein Unternehmen kann niemals das individuelle Handeln jedes Menschen umtrainieren, weshalb mit der Missachtung von Sicherheitsvorgaben oder dem fehlenden Bewusstsein für Bedrohungen gerechnet werden muss.
- Zahlreiche Statistiken, Untersuchungen und Berichte der letzten Jahre und

Jahrzehnte zeigen immer wieder, dass der „Faktor Mensch“ durch Leichtsinn, Unsicherheit oder Unwissenheit Ursache von erfolgreichen Cyberangriffen ist.

Ziele einer Awarenesskampagne könnten sein:

- Beschäftigten vermitteln, dass sie in manchen Situationen selbst für die Informationssicherheit des Unternehmens verantwortlich sind.
- Beschäftigten Grundlagen der Informationssicherheit vermitteln.
- Beschäftigten Risiken und Gefahren aufzeigen, sowohl dienstlich als auch privat.
- Beschäftigten die internen Regelungen und Richtlinien in Auszügen vorstellen und bekannt machen.

Zutaten für eine erfolgreiche Awarenesskampagne

Bei der Gestaltung einer Awarenesskampagne sollten die nachfolgenden fünf Elemente berücksichtigt werden:

- **Kontinuität**: Vertiefen Sie das Wissen der Beschäftigten und fördern Sie erwünschtes Handeln durch Wiederholungen.
- **Modularität**: Gruppieren Sie Beschäftigten in geeignete Zielgruppen und vermitteln Sie relevante Inhalte.
- **Kreativität**: Erkennen Sie Altersstrukturen und nutzen Sie geeignete Kanäle für diese Zielgruppen.
- **Interaktivität**: Begrüßen Sie Feedback und Diskussion, um den Teamgeist zu fördern.
- **Metriken**: Verbessern Sie kommende Kampagnen und Maßnahmen durch Erhebung und Analyse passender Metriken.

Außerdem sollte den folgenden vier Aspekten Aufmerksamkeit geschenkt werden:

- **Vorbereitung**: Definieren Sie ein Ziel für Ihre Kampagne unter Berücksichtigung der Strukturen im Unternehmen.
- **Organisation**: Binden Sie frühzeitig Führungskräfte und Organisationseinheiten wie HR ein. Bitten Sie um Unterstützung.
- **Inhalt**: Setzen Sie ein starkes Leitmotiv („Wir gegen den Angreifer“) und übersetzen Sie komplexe technische Sachverhalte in einfach verständliche Sprache.
- **Umsetzung**: Setzen Sie Ihre Maßnahmen anhand eines überschaubaren Zeitplans kontinuierlich um, damit Sie Ihr Ziel erreichen können.

Modulbeispiele

Wenn Sie Module für Ihre Awarenesskampagne entwickeln, könnten folgende Themen vorkommen:

- Sicheres Arbeiten von zu Hause (bspw. VPN-Nutzung, SASE-Nutzung, sicherer Internetzugang)
- Social Engineering (siehe dieser Gastvortrag)
- Melden von Sicherheitsvorfällen (Was sind Sicherheitsvorfälle? An wen sollen Beschäftigte potenzielle Sicherheitsvorfälle melden?)
- Umgang mit sozialen Medien (Was darf geteilt werden, was nicht?)
- Klassifizierung von Informationen (bspw. öffentlich, intern, vertraulich)
- Umgang mit Wechselmedien (bspw. USB-Sticks, SSDs)
- Nutzung öffentlicher Netzwerke (bspw. öffentliches Wi-Fi im Zug oder Hotel)

Kanalbeispiele

Neben Modulen (relevante Module geeigneten Beschäftigtengruppen zu vermitteln) können ebenso Präferenzen bei der Mediennutzung der Beschäftigten eine wichtige Rolle spielen. Sie müssen als Autor Ihrer Awarenesskampagne die für Ihre Zielgruppe relevanten Medien identifizieren und diese gezielt „bespielen“. Solche Medienkanäle könnten sein:

- Internes soziales Netzwerk des Unternehmens
- Intranet-Seite des Unternehmens
- E-Learning
- Toolgestützte Schulungen, bspw. Tools für Phishing-Kampagnen
- Interne Zeitschriften und Zeitungen
- Unternehmensblog
- Printmedien wie Poster oder Flyer
- Workshops mit Fachbereichen und Zielgruppen

Beachten Sie insbesondere, dass manche Kanäle eher von älteren Beschäftigten, andere von jüngeren Beschäftigten genutzt werden könnten.

Zwischen zwei Kampagnen ...

Mit einer einzigen Awarenesskampagne pro Dekade ist leider nicht viel erreicht. Letztendlich ist Awareness wie Fitness: Ein sinnvolles, kontinuierliches Maß ist besser als ein Marathon im Monat und sonst nichts.

Beispiele für „Awareness zwischendurch“:

- Interne Präsenz-Schulungsangebote für Beschäftigte anbieten
- E-Learning für Beschäftigte anbieten
- Schulungsmaterial für Führungskräfte bereitstellen und diese Schulungen via Geschäftsführung/HR verpflichtend machen
- In sozialen Netzwerken des Unternehmens regelmäßig über Sicherheitsthemen berichten und moderierte Diskussionen zulassen

Was sollten wir im Kopf behalten?

- Jeder Mensch kann Opfer von Social Engineering werden, völlig egal, wie sehr technisch versiert man ist. Social Engineering ist ein psychologisches, kein technisches Thema.
- Um Bewusstsein privat und dienstlich zu schaffen, müssen wir mit Menschen umgehen können und ggf. technische Sachverhalte einfach erklären können. Deshalb kann es gerade im Unternehmen sehr wichtig sein, Führungskräfte, die Geschäftsführung oder HR in Kampagnen und Maßnahmen einzubinden, statt die Erläuterungen komplizierter Sachverhalte der IT zu überlassen.
- Alles, was wir über uns im Internet veröffentlichen, kann gegen uns verwendet werden. Datensparsamkeit, strikte Datenschutzeinstellungen und starke Passwörter sind gute Bausteine gegen Social Engineering. Nutzen Sie deshalb einen Passwortmanager und setzen Sie Ihre Onlineprofile (Facebook, Twitter, Reddit, LinkedIn, Garmin, ...) auf privat!

Literatur

- Gray: Practical Social Engineering, 2022
- Hadnagy: Social Engineering: The Science of Human Hacking, 2018
- Kahneman: Schnelles Denken, langsames Denken, 2012

Links

Definitionen und Hintergründe

- Social Engineering allgemein
- The Social Engineering Framework
- Phasen des Social Engineerings

Ressourcen für den Selbstschutz und Awareness

- Watchlist Internet (Aktuelle Angriffe auf Privatpersonen)
- Verbraucherzentrale Phishing-Radar

Social Engineering im echten Leben

- „Echter“ Fake-Charakter Robin Sage

Berufliche Zertifizierungen

- The SANS Security Awareness Professional (SSAP)