Der Faktor Mensch

Social Engineering und Information Security Awareness

Benjamin Süß

Gastvortrag am 09.01.2023

Was wollen wir heute erreichen? 🤔

Bildquellen: Meme Generator

Organisatorisches 🙋

- Bekommen wir die Präsentation?
  ✅ Ja, die **Präsentation wird verteilt**.
- Darf ich Fragen stellen?
  ✅ Ja, bitte **gerne jederzeit Fragen stellen**!
- Werden hier nur Folien vorgelesen?
  ❌ Nein, **ich zeige auch Dinge live**!

Warum schauen wir uns Social Engineering an?

Verizon: 82% der Sicherheitsverletzungen entstanden durch den Faktor Mensch

Blackhat: At the core of almost every successful cyberattack, one thing remains constant

BSI: … der Faktor „Mensch“ für Cyber-Angriffe immer bedeutsamer.

Quellen: https://www.verizon.com/business/de-de/resources/reports/dbir/, https://www.blackhat.com/sponsor-posts/10052021-five-social-engineering-trends-to-watch.html, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=5

Was kann uns schon passieren? 🤷

- Jemand stiehlt uns Geld, viel Geld.
- Jemand bestellt in unserem Namen Waren und bezahlt nicht.
- Jemand übernimmt unsere Identität, um unsere Familie, Freunde, Bekannte anzugreifen.
- Jemand spioniert uns aus.
- Jemand greift „dank uns“ erfolgreich unseren Arbeitgeber an.
- …

Agenda

- Was ist Social Engineering und betrifft mich das?
- Wie arbeitet ein „Social Engineer“?
- Wie sehen echte Social Engineering Angriffe aus?
- Wie hilft Information Security Awareness?
- Wie kann ich Awareness im Unternehmen umsetzen?
- Was sollten wir im Kopf behalten?

Was ist Social Engineering und betrifft mich das?

Definitionen von 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)

Quellen: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html

Warum sind wir alle potenziell betroffen?

- 🤔 These: Unser menschliches „Betriebssystem“ läuft den Großteil des Tages per Autopilot. Wir haben uns dann **nicht selbst unter Kontrolle**, auch wenn wir das denken.

- 🤔 These: Wir handeln die meiste Zeit automatisch, schnell, unbewusst und haben eine verzerrte Wahrnehmung.

Siehe auch https://de.wikipedia.org/wiki/Schnelles_Denken%2C_langsames_Denken

Beispiel einer Beeinflussung

🤔 *Haben Sie noch die Kontrolle?*

89249 + 72665 = ?

Anlehnung an *Schnelles Denken, langsames Denken* (Kahneman)

Beispiel einer Beeinflussung

Anlehnung an *Schnelles Denken, langsames Denken* (Kahneman), Bildquelle: https://unsplash.com/photos/UxxUi-ApVwM

Betrifft mich Social Engineering?

- 😲 **Ja!** Selbst wenn wir denken, wir seien „immun“, bleiben wir trotzdem mehr oder weniger beeinflussbar.

- ☺️ Kontinuierliches „Anti-Social-Engineering“-Training bringt zwar keine 100-prozentige Sicherheit, kann aber immens gegen Social Engineering helfen.

- 👮 **Fazit:** Wir müssen verstehen, wie typische Social-Engineering-Angriffe aussehen.

Wie arbeitet ein „Social Engineer“?

Phasen eines SE-Angriffs

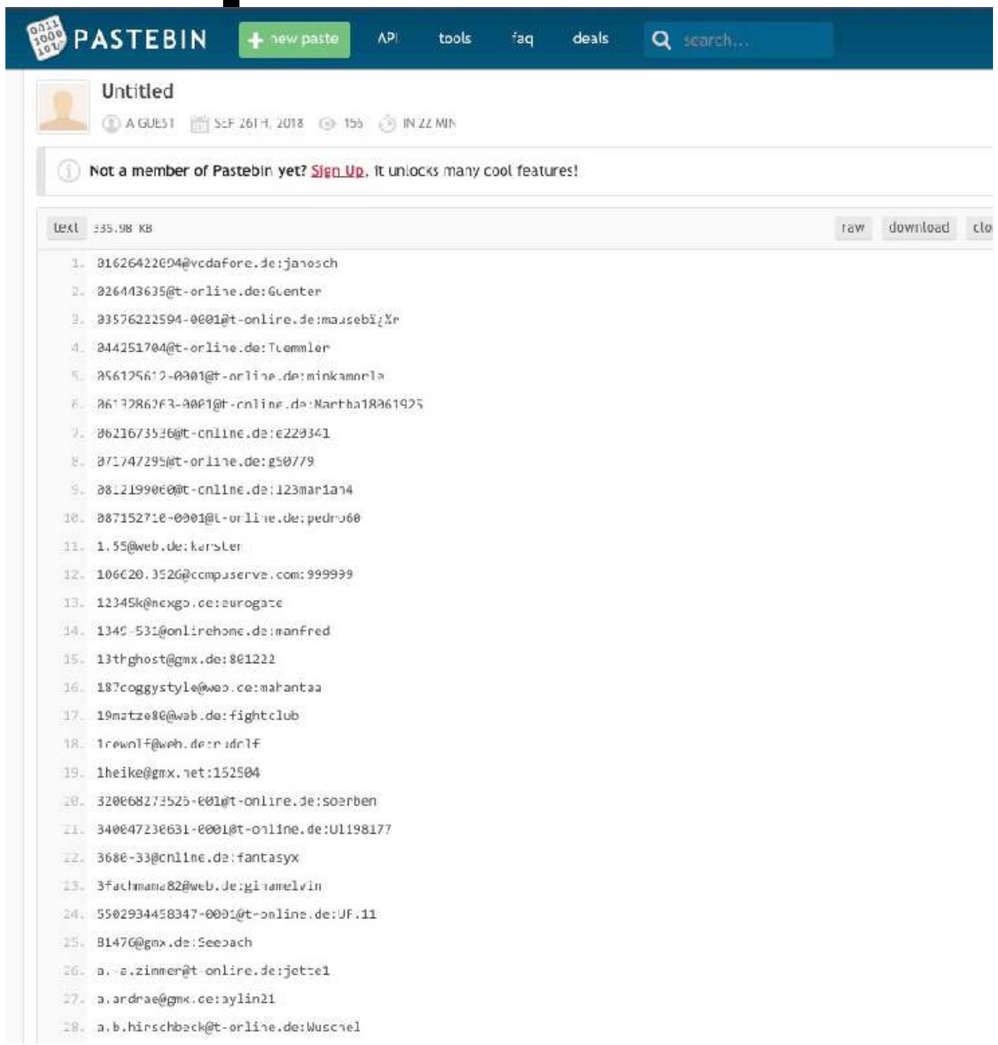
- Phase 1: Der Social Engineer sammelt und kombiniert Informationen über Opfer.
- Phase 2: Der Social Engineer interagiert mit potenziellen Opfern (Aufbau einer Vertrauensbeziehung).
- Phase 3: Der Social Engineer nutzt das Opfer aus, um eigene Ziele zu erreichen.
- Phase 4: Der Social Engineer verwischt Spuren und hinterlässt einen unauffälligen, positiven Eindruck (es kommt zunächst oder nie Verdacht auf).

Siehe auch https://www.social-engineer.org/framework/attack-vectors/attack-cycle/

Phase 1 eines SE-Angriffs

- Die Phase 1 (Informationen über Opfer beschaffen und kombinieren) kann bereits über **Erfolg oder Misserfolg** des Angriffs entscheiden.
- Social Engineers können heutzutage auf eine **Vielzahl digitaler Ressourcen** für die Phase 1 zurückgreifen (bspw. Suchmaschinen, soziale Netzwerke, Datenlecks, Webseiten, Messenger Gruppen, exponierte Server), umgangssprachlich auch als OSINT (= Open Source Intelligence) bezeichnet.
- Unscheinbare Einzelinformationen können in Kombination zu neuen Schlüssen führen und Angriffe begünstigen.

Beispiel Datenleck als Quelle



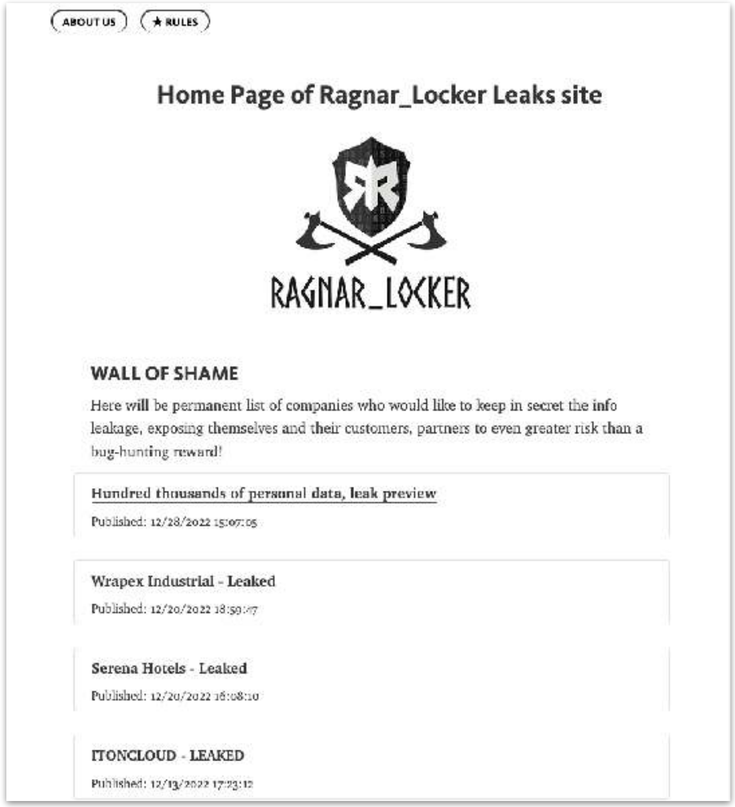
- Have I Been Pwned listet **12,4 Milliarden** geleakte Nutzerkonten, der HPI Identity Leak Checker **12,8 Milliarden**.

- Täglich gibt es weitere Datenlecks, auf die wir als Nutzer kaum Einfluss nehmen können.

Bildquelle: https://twitter.com/cyb3rops/status/1045061014683885569

Beispiel Datenleck als Quelle

🤓🍿 Kurze Demonstration



- „Moderne“ Ransomware kopiert vor Verschlüsselung oft massenhaft Daten. Opfer werden doppelt erpresst (Zahlung für Entschlüsselung, Zahlung für Nichtveröffentlichung).
- Diese Daten werden entweder verkauft oder einfach veröffentlicht.

Bildquelle: Ransomware Leak Seiten (Ragnar Locker et al.)

Beispiel soziale Medien als Quelle

- Öffentliche Profile, Posts und Kommentare sind teils eine Goldgrube für Social Engineers.

- Beispiele: **Reddit** und **Twitter**

🤓🍿 Kurze Demonstration

- Auch an „sekundäre“ Profile denken, wie bspw. Garmin Connect

Beispiel exponierte Server (hier Kameras)

🤓🍿 Kurze Demonstration

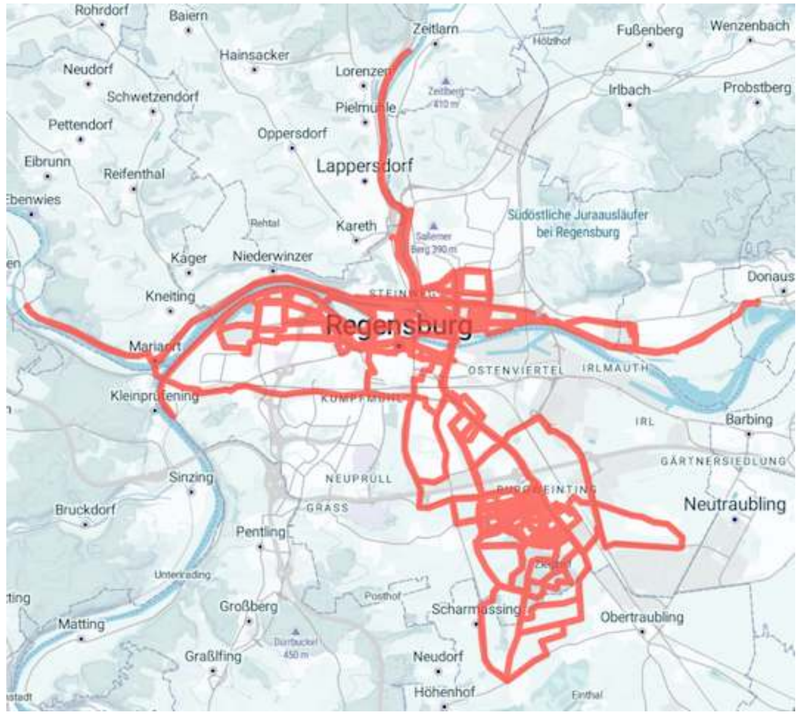
Bildquelle: Exponierter Videostream auf insecam.org

Denken Sie auch an “unsichtbare” Daten

- 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).

- Beispiel rechts: GPS-Daten von Workouts



Bildquelle: Eigene Aufnahme

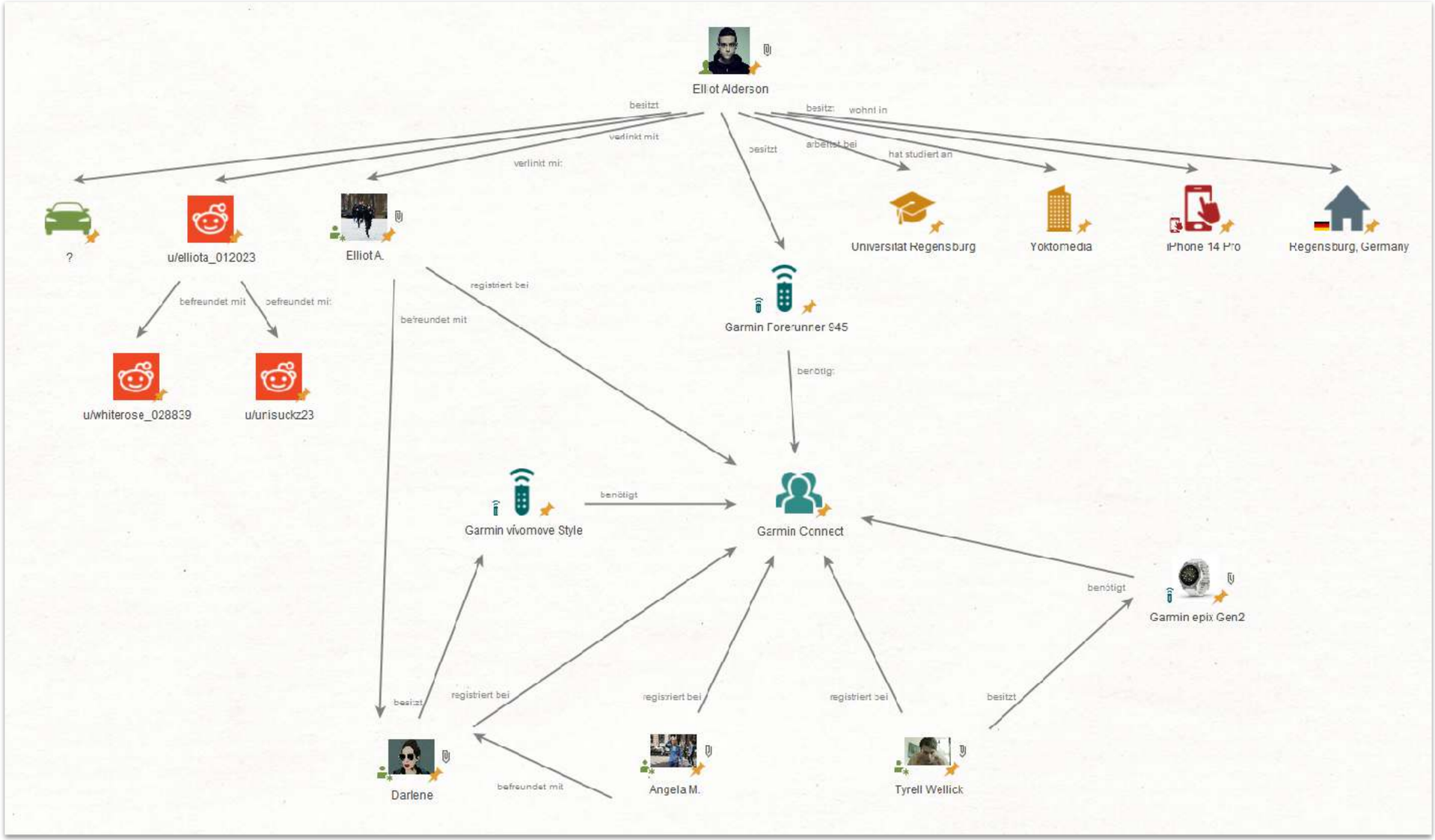
Beispiel „unsichtbare“ Metadaten in Dateien

- Viele Dateiformate wie PNG, JPG, PDF oder DOCX enthalten standardmäßig Metadaten.
- Metadaten können Informationen preisgeben, die Sie nicht preisgeben wollen.

🕵️ Was entdecken Sie in den Metadaten?

Bildquelle: Eigene Aufnahme

Beispiel Datenaufbereitung in Maltego



Bildquelle: Eigene Aufnahme

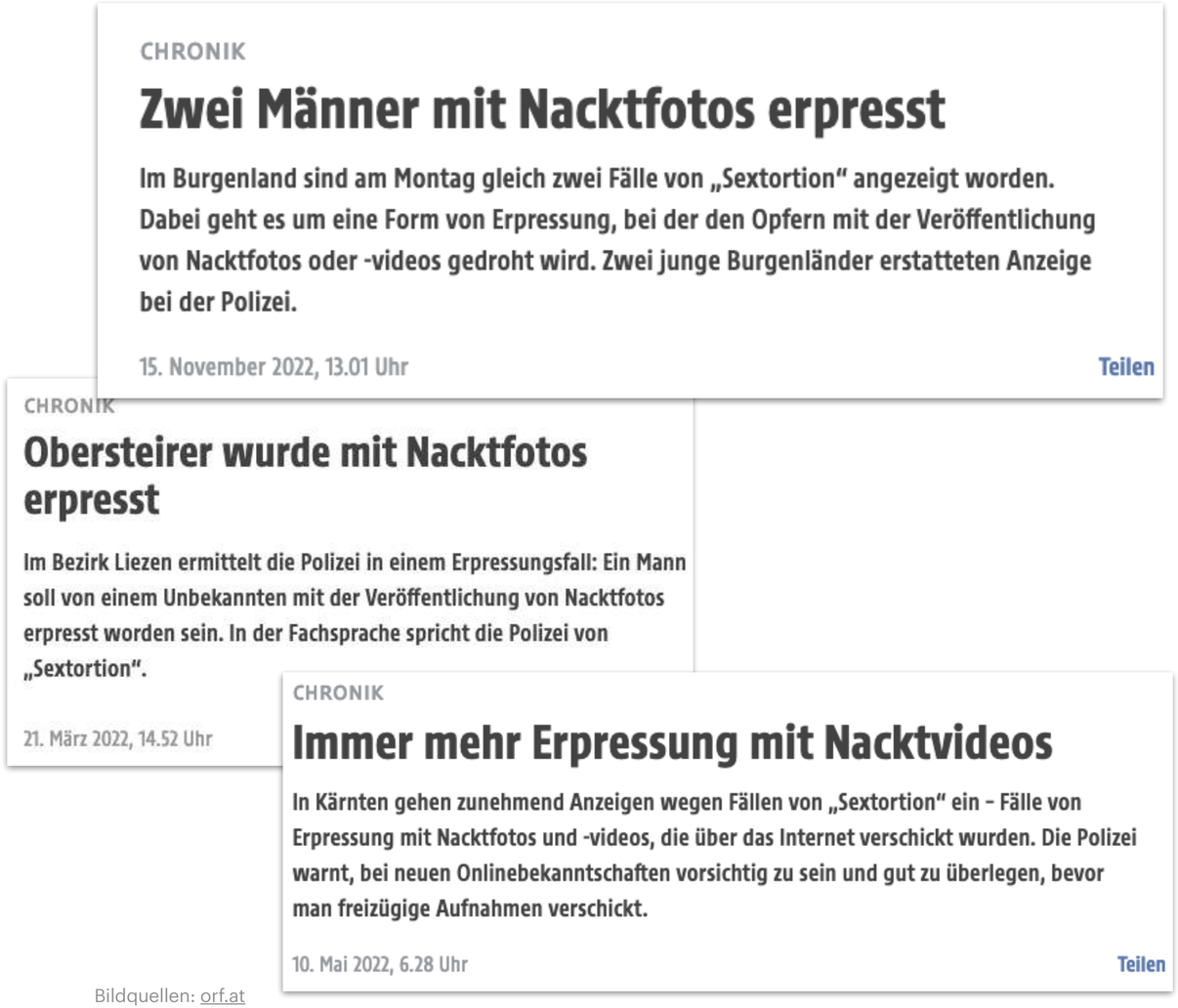
Wie sehen echte Social Engineering Angriffe aus?

Historisch bekannte SE-Angriffe

- 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.
- Kevin David Mitnick (* 1963) nutzte SE für Angriffe auf IT-Systeme.

Quellen: https://de.wikipedia.org/wiki/George_C._Parker, https://de.wikipedia.org/wiki/Victor_Lustig, https://de.wikipedia.org/wiki/Bernard_L._Madoff, https://de.wikipedia.org/wiki/Frank_Abagnale, https://de.wikipedia.org/wiki/Kevin_Mitnick

Beispiele: Sextortion



CHRONIK

Zwei Männer mit Nacktfotos erpresst

Im Burgenland sind am Montag gleich zwei Fälle von „Sextortion“ angezeigt worden. Dabei geht es um eine Form von Erpressung, bei der den Opfern mit der Veröffentlichung von Nacktfotos oder -videos gedroht wird. Zwei junge Burgenländer erstatteten Anzeige bei der Polizei.

15. November 2022, 13.01 Uhr Teilen

CHRONIK

Obersteirer wurde mit Nacktfotos erpresst

Im Bezirk Liezen ermittelt die Polizei in einem Erpressungsfall: Ein Mann soll von einem Unbekannten mit der Veröffentlichung von Nacktfotos erpresst worden sein. In der Fachsprache spricht die Polizei von „Sextortion“.

21. März 2022, 14.52 Uhr

CHRONIK

Immer mehr Erpressung mit Nacktvideos

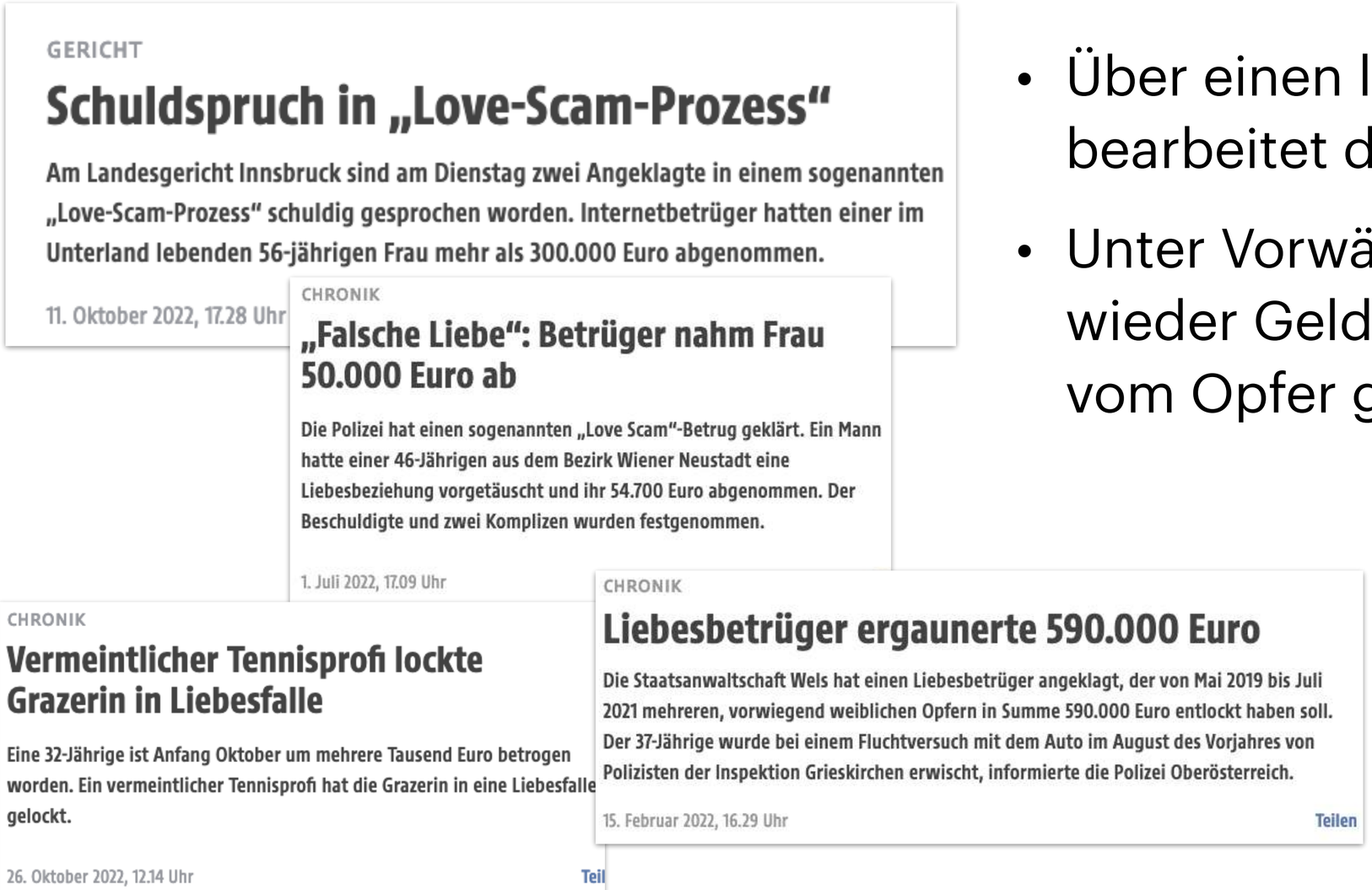
In Kärnten gehen zunehmend Anzeigen wegen Fällen von „Sextortion“ ein – Fälle von Erpressung mit Nacktfotos und -videos, die über das Internet verschickt wurden. Die Polizei warnt, bei neuen Onlinebekanntschaften vorsichtig zu sein und gut zu überlegen, bevor man freizügige Aufnahmen verschickt.

10. Mai 2022, 6.28 Uhr Teilen

Bildquellen: orf.at

- Ein Angreifer gibt vor, das Opfer sei über Schadsoftware beim Pornokonsum gefilmt worden.
- Als „Beweis“ schickt der Angreifer oft ein gültiges Passwort mit, das in einem öffentlichen Datenleck enthalten war.
- Der Angreifer verlangt Geld, sonst werde die Videoaufnahme veröffentlicht.

Beispiele: Romance Scans, Love Scams



GERICHT

Schuldspruch in „Love-Scam-Prozess“

Am Landesgericht Innsbruck sind am Dienstag zwei Angeklagte in einem sogenannten „Love-Scam-Prozess“ schuldig gesprochen worden. Internetbetrüger hatten einer im Unterland lebenden 56-jährigen Frau mehr als 300.000 Euro abgenommen.

11. Oktober 2022, 17.28 Uhr

CHRONIK

„Falsche Liebe“: Betrüger nahm Frau 50.000 Euro ab

Die Polizei hat einen sogenannten „Love Scam“-Betrug geklärt. Ein Mann hatte einer 46-Jährigen aus dem Bezirk Wiener Neustadt eine Liebesbeziehung vorgetäuscht und ihr 54.700 Euro abgenommen. Der Beschuldigte und zwei Komplizen wurden festgenommen.

1. Juli 2022, 17.09 Uhr

CHRONIK

Vermeintlicher Tennisprofi lockte Grazerin in Liebesfalle

Eine 32-Jährige ist Anfang Oktober um mehrere Tausend Euro betrogen worden. Ein vermeintlicher Tennisprofi hat die Grazerin in eine Liebesfalle gelockt.

26. Oktober 2022, 12.14 Uhr Teil

CHRONIK

Liebesbetrüger ergaunerte 590.000 Euro

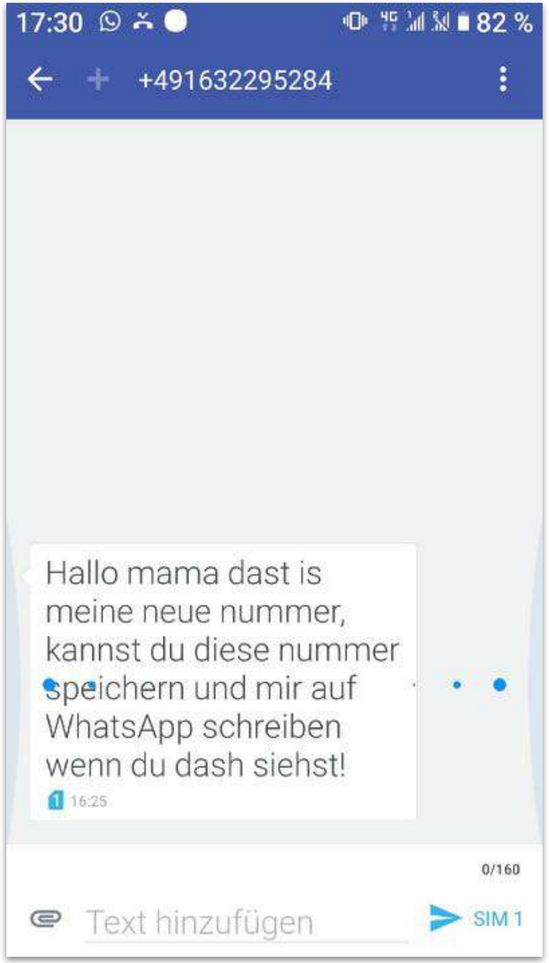
Die Staatsanwaltschaft Wels hat einen Liebesbetrüger angeklagt, der von Mai 2019 bis Juli 2021 mehreren, vorwiegend weiblichen Opfern in Summe 590.000 Euro entlockt haben soll. Der 37-Jährige wurde bei einem Fluchtversuch mit dem Auto im August des Vorjahres von Polizisten der Inspektion Grieskirchen erwischt, informierte die Polizei Oberösterreich.

15. Februar 2022, 16.29 Uhr Teilen

Bildquellen: orf.at

- Über einen langen Zeitraum bearbeitet der Angreifer sein Opfer.
- Unter Vorwänden werden immer wieder Geldsummen erbettelt und vom Opfer gezahlt.

Beispiele: „Hallo Mama, …“



Bildquellen: Privat, Reddit

Beispiele: Loverboy, Cybergrooming

"Loverboy-Methode"

Häufige Tatbegehungsform ist die "Loverboy-Methode". Betroffene hiervon sind oft minderjährige Mädchen und junge Frauen aus allen Gesellschaftsschichten. Sie werden von "Loverboys" angesprochen, die ihnen zunächst vorgaukeln, sie seien in sie verliebt. Die "Loverboys" geben ihnen Aufmerksamkeit, Komplimente, Zuneigung und oft auch Geschenke. Gleichzeitig machen sie die Opfer emotional abhängig und entfremden sie ihrem Verwandten- und Bekanntenkreis. Später verleiten oder zwingen sie sie zur Prostitution. Oft gaukeln sie ihren Opfern vor, das so verdiente Geld zum Aufbau einer gemeinsamen Zukunft verwenden zu wollen. Die Opfer sind oft schwer zu erkennen, da sie sich häufig selbst nicht als Opfer wahrnehmen. Besondere Bedeutung kommt der „Loverboy-Methode" in sozialen Netzwerken und Dating-Portalen zu.

POLIZEI
KRIMINALPRÄVENTION

SCHUTZ VOR (CYBER-)GROOMING

Was ist Grooming?

Bei Grooming handelt es sich um das gezielte Ansprechen von Kindern, um sexuellen Kontakt anzubahnen. Es ist eine besondere Form der sexuellen Belästigung, die bis zum sexuellen Missbrauch führen kann. Die Anbahnung findet hauptsächlich in Chaträumen und sozialen Netzwerken statt.

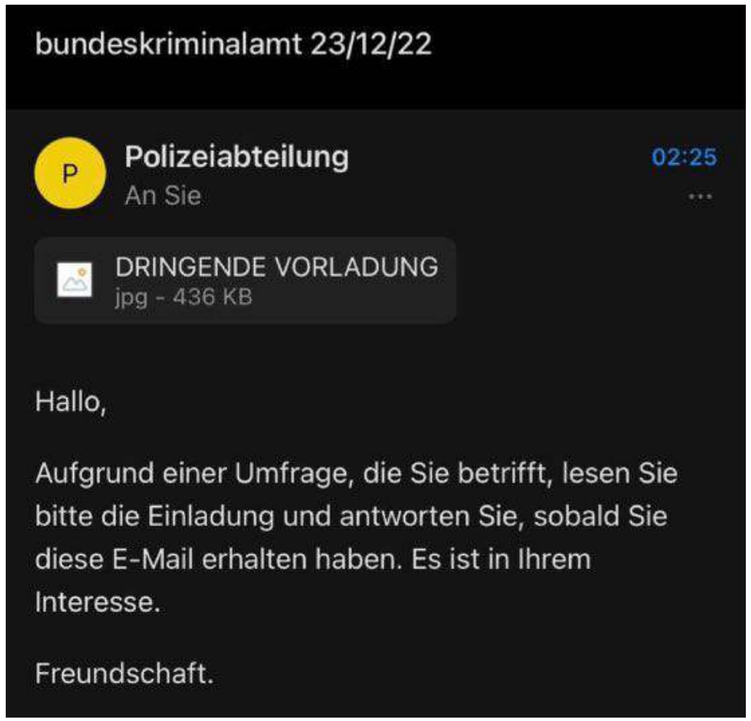
Bildquellen: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/VerdachtDesMenschenhandels/verdachtDesMenschenhandels_node.html, https://www.lka.polizei-nds.de/praevention/aktuelles_und_kampagnen/die-masche-der-loverboys-wenn-aus-liebe-zwang-wird-115322.html, https://www.bundeskriminalamt.at/202/Internet_kennen/files/Grooming_Juni2015.pdf

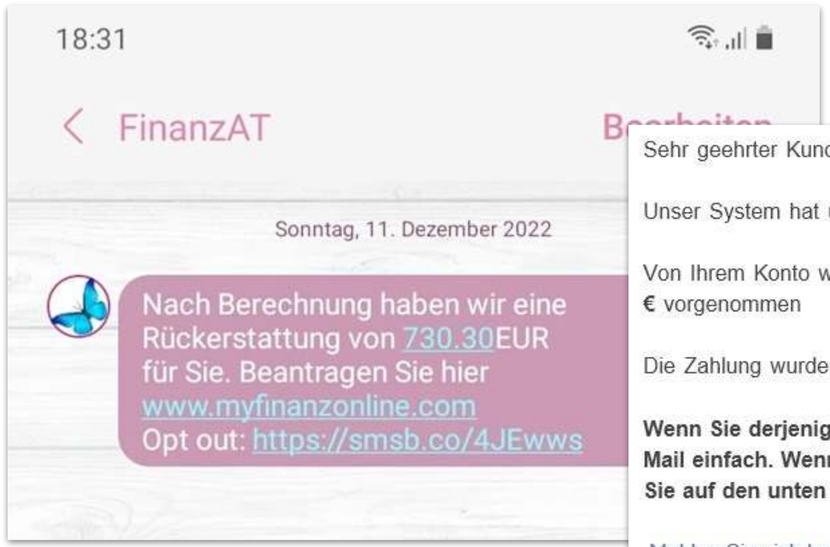
Für das Selbststudium ... 💻🍿

- 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.deutschlandfunk.de/kriminelles-geschaeft-mit-schockanrufen-100.html
- Cybergrooming: https://www.youtube.com/watch?v=kYOfqKkPxb0
- Loverboys: https://www.youtube.com/watch?v=P75SwvN5TWU

Übliche SE-Techniken

- **Phishing**: Der „Klassiker“ im IT-Bereich, bei dem sich der Angreifer als vertrauenswürdiger Kommunikationspartner ausgibt. Funktioniert auch per Instant Messenger, SMS oder Sprachanruf.





Bildquellen: Privat, https://www.watchlist-internet.at

Übliche SE-Techniken

- **Water holing**: Der Angreifer präpariert einen von Opfern genutzten Onlinedienst mit Schadsoftware. Opfer infizieren sich anschließend darüber. Es wird die Vertrauensbeziehung zwischen Opfern und dem Onlinedienst ausgenutzt.
- **Impersonation**: Ein Angreifer täuscht die Identität einer anderen Person vor, um damit schadhafte Aktionen durchzuführen. Dies kann sehr lange negative Folgen für das Opfer haben.
- **Baiting**: Ein Angreifer legt einen “Köder” (= Bait) aus, um die Neugierde des Opfers auszunutzen (bspw. herrenloser USB-Stick oder verlorenes Smartphone).

Wie hilft Information Security Awareness?

Was ist mit Awareness gemeint? 🤔

- Es soll **Bewusstsein** für Gefahren in der Informationssicherheit geschaffen werden. Dies schließt Social Engineering ein.

- Durch Awarenessmaßnahmen soll vermittelt werden, wie wir Social Engineering **verhindern, erkennen** und ggf. darauf **reagieren** können.

Beispiele Awarenessmaßnahmen im Alltag

Bildquellen: https://www.runtervomgas.de/aktuelles-und-downloads/aktionsmaterial/, https://www.behance.net/gallery/98639073/Environmental-Awareness-Poster, https://publikationen.dguv.de/widgets/pdf/download/article/3787

Welche Maßnahmen könnten hier helfen? 🤔

- **Finn** ist Student und Gamer seit seiner Kindheit. Er hat seinen PC selbst zusammengestellt und nutzt 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 sechs 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.

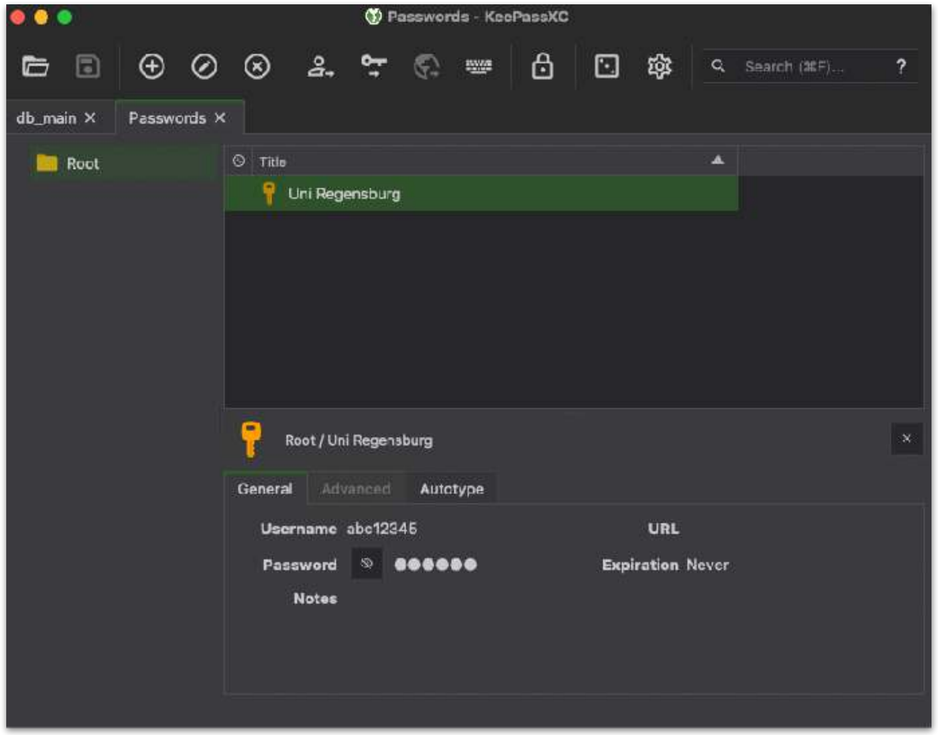
👨‍💼 Was schlagen Sie vor? Sie sind Experte!

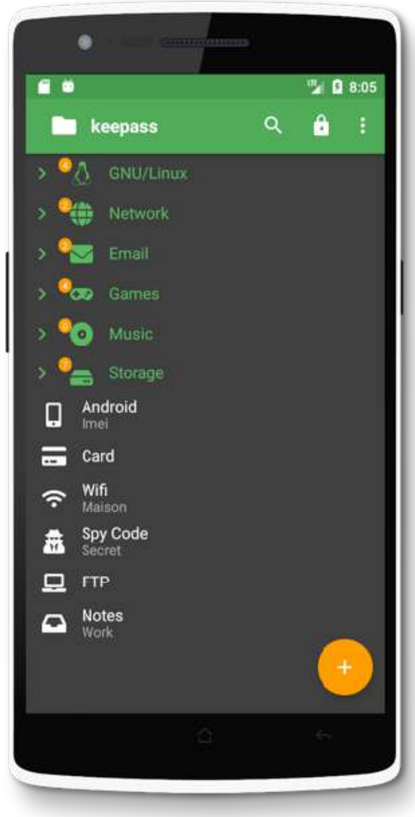
Tipps gegen Social Engineering

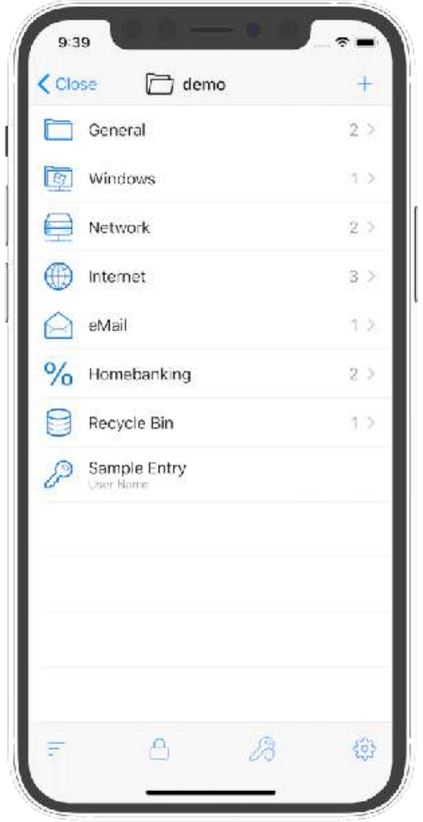
- Überlegen Sie vor Registrierung bei jedem Onlinedienst, ob Sie diesen wirklich brauchen.
- Seien Sie sich bewusst, welche „unsichtbaren“ Daten ein Anbieter über Sie sammelt.
- Teilen Sie nicht alles offen im Internet: Setzen Sie Ihre Profile auf „privat“. Entfernen Sie sensible Daten und Metadaten 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!

Tipps im Umgang mit Passwörtern

Nutzen Sie kostenlose Passwortmanager wie bspw. KeePassXC (Windows, Linux, macOS), KeePassDX (Android), Keepassium (iOS).







Bildquellen: Eigenes Bild, https://www.keepassdx.com/, https://keepassium.com/img/view-group_flat.png?t=20191121T2359

Tipps im Umgang mit Passwörtern

Nutzen Sie Zwei-Faktor-Authentifizierung (bspw. OATH-TOTP, U2F, WebAuthn) bzw. Zwei-Schritt-Verifizierung.

Bildquellen: Eigene Bilder

Tipps im Umgang mit Passwörtern

- Immer gut:
  - Setzen Sie je Onlinekonto ein individuelles Passwort.
  - Nutzen Sie Zwei-Faktor-Authentifizierung bzw. Zwei-Schritt-Verifizierung.
  - Ändern Sie umgehend Ihr Passwort, wenn ein Datenleck bei einem Anbieter bekannt wird.
  - Löschen Sie Onlinekonten, die Sie nicht mehr brauchen.
  - Setzen Sie niemals erratbare Informationen bei „Passwort vergessen“-Fragen.
- Für Fortgeschrittene:
  - Nutzen Sie je Onlinekonto auch individuelle E-Mail-Adressen bzw. -Aliase.
  - Dokumentieren Sie bei jedem Eintrag im Passwortmanager, welche personenbezogenen Daten Sie bewusst angegeben haben (bspw. IBAN, physische Adresse, Mobiltelefonnummer).

Awareness hört bei uns nicht auf

Bildquellen: Meme Generator, Polizei Bayern

Wie kann ich Awareness im Unternehmen umsetzen?

Awareness in der ISO/IEC 27001

7.3 Awareness

Persons doing work under the organization's control shall be aware of:
a) the information security policy;
b) their contribution to the effectiveness of the ISMS [...]; and
c) the implications of not conforming with the ISMS requirements.

A.7.2 Human resource security – During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

A.7.2.2 Information security awareness, education and training

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Awarenesskampagne als Marketing

- Motivation
  - 100-prozentiger technischer Schutz ist unmöglich, ebenso 90 % oder 80 %.
  - Menschen sind überall in einem Unternehmen und tauschen Informationen über vielfältige Kanäle aus.
  - Viele Sicherheitsvorfälle entstehen durch den „Faktor Mensch“, oft durch Leichtsinn, Unsicherheit oder Unwissenheit.

- Ziele
  - Eigenverantwortung der Mitarbeiter stärken.
  - Wissen über Informationssicherheit vermitteln.
  - Bewusstsein für Risiken und Gefahren schaffen (dienstlich und privat).
  - Interne Regelungen und Richtlinien bekannt machen.
  - Einbindung der Führungskräfte in den Fachabteilungen.

Fünf Elemente einer erfolgreichen Kampagne

- **Kontinuität**: Vertiefen Sie das Wissen der Mitarbeiter und fördern Sie erwünschtes Handeln durch Wiederholungen.
- **Modularität**: Gruppieren Sie Mitarbeiter 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.

Weitere Tipps für eine erfolgreiche Kampagne

- **Vorbereitung**: Definieren Sie ein Ziel für Ihre Kampagne unter Berücksichtigung der Strukturen im Unternehmen.
- **Organisation**: Binden Sie frühzeitig Führungskräfte und andere Fachbereiche 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.

Awarenesskampagnen: Modulbeispiele

- Sicheres Arbeiten im Home Office (bspw. VPN-Nutzung, sicherer Internetzugang)
- Social Engineering
- Melden von Sicherheitsvorfällen (an wen was wie 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. WLAN im Zug oder Hotel)

Awarenesskampagnen: Kanalbeispiele

- 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

Zwischen zwei Kampagnen …

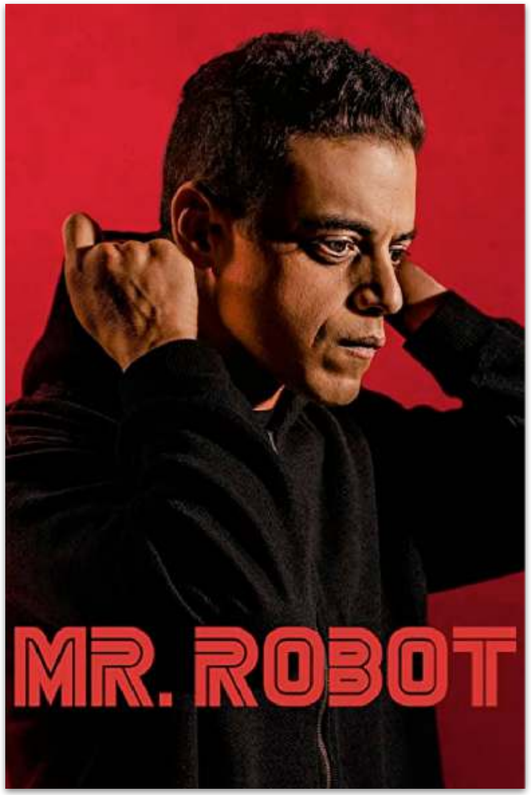
- Awareness ist wie Fitness: Ein sinnvolles, kontinuierliches Maß ist besser als ein Marathon im Monat und sonst nichts.
- Beispiele für „Awareness zwischendurch“:
  Interne Präsenz-Schulungsangebote für Mitarbeiter, E-Learning-Angebote, aktuelles Schulungsmaterial für Führungskräfte, Posts und moderierte Gruppen im sozialen Netzwerk des Unternehmens, …

Was sollten wir im Kopf behalten?

Zusammenfassung 🤔💡

- Social Engineering ist ein psychologisches, kein technisches Thema.
- Für erfolgreiche Information Security Awareness müssen wir mit Menschen umgehen können und ggf. technische Sachverhalte einfach erklären können.
- Alles, was wir über uns im Internet veröffentlichen, kann gegen uns verwendet werden.
- Nutzen Sie einen Passwortmanager und setzen Sie Ihre Onlineprofile (Facebook, Twitter, Reddit, LinkedIn, Garmin, ...) auf privat!

Empfehlung zum Schluss 🎬🍿



Schauen Sie Mr. Robot.

- Vier Staffeln, 45 Episoden
- Behandelt „echtes“ Hacking realitätsnah, vor allem auch Psychologie.

Bildquelle: https://www.imdb.com/title/tt4158110/mediaviewer/rm9147905/

🤔 Finale Fragen?

Vielen Dank für Ihre Aufmerksamkeit

LinkedIn: https://www.linkedin.com/in/bs83de/

E-Mail: bs83de@blakemail.de

Links und Literatur 📚🤓

- „Echter“ Fake-Charakter Robin Sage: https://en.wikipedia.org/wiki/Robin_Sage
- Social Engineering allgemein: https://en.wikipedia.org/wiki/Social_engineering_(security)
- The Social Engineering Framework: https://www.social-engineer.org/framework/general-discussion/
- Phasen des Social Engineerings: https://www.social-engineer.org/framework/attack-vectors/attack-cycle/
- The SANS Security Awareness Professional (SSAP) Zertifizierung: https://www.sans.org/security-awareness-training/career-development/credential/
- BSI IT-Grundschutz, ORP.3 Sensibilisierung und Schulung: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2022.pdf?__blob=publicationFile&v=3
- Watchlist Internet (Aktuelle Angriffe auf Privatpersonen): https://www.watchlist-internet.at/
- Verbraucherzentrale Phishing-Radar: https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059

- Gray: Practical Social Engineering, 2022, https://nostarch.com/practical-social-engineering
- Hadnagy: Social Engineering: The Science of Human Hacking, 2018.
- Kahneman: Schnelles Denken, langsames Denken, 2012.