Der Faktor Mensch

Social Engineering und Information Security Awareness

Benjamin Süß

Gastvortrag am 24.01.2022

Organisatorisches 🙋

- Bekommen wir die Folien?
  ✅ Ja, die **Folien werden 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?

Wer allerdings so bequem ist, dass er auch noch das Denken abschaltet und auf Phishing-Mails reinfällt oder sich Spionage-Trojaner installiert, der darf sich nicht beklagen, wenn PIN und TANs bösen Menschen in die Hände fallen.

🤔 *Was denken Sie darüber?*

Zitat von https://www.heise.de/ct/artikel/Wir-sind-selbst-schuld-290140.html

Warum schauen wir uns Social Engineering an?

85% of breaches involved a human element (2021)

Social Engineering Threats Rose 270% in 2021

während der Pandemie eine erhebliche Anzahl von Social Engineering-Kampagnen beobachtet

Quellen: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf,
https://securityboulevard.com/2021/10/social-engineering-threats-rose-270-in-2021-indicating-a-shift-to-multi-channel-phishing-attacks-as-apps-and-browsers-move-to-the-cloud/,
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2021-11-spoc-wirtschaft-und-wissenschaft-schuetzen.pdf?__blob=publicationFile&v=4

Was kann mir schon passieren? 🤷

- Dritte stehlen Ihnen Geld, viel Geld.
- Dritte bestellen in Ihrem Namen Waren; Sie tragen die Konsequenzen (offene Forderungen, rechtliche Auseinandersetzungen, Bonität!).
- Dritte übernehmen Ihre Identität, um Ihre Familie, Freunde, Bekannte anzugreifen (kann Beziehungen nachhaltig beeinträchtigen).
- Dritte “spionieren” Sie aus (bspw. durch Schadsoftware auf Ihrem Smartphone).
- Sie helfen Dritten, Ihren Arbeitgeber anzugreifen, was wiederum berufliche Konsequenzen für Sie haben kann.

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. Auch wenn wir denken, uns selbst unter Kontrolle zu haben, ist das nicht so.

- 🤔 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?*

29287 + 77549 = ?

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

Beispiel einer Beeinflussung

Anlehnung an *Schnelles Denken, langsames Denken* (Kahneman), Bildquelle: https://unsplash.com/photos/r-enAOPw8Rs

Betrifft mich Social Engineering?

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

- ☺️ Wie immer in der Informationssicherheit bringt auch ständiges “Anti-Social-Engineering”-Training keine 100-prozentige Sicherheit, kann aber immens gegen Social Engineering helfen.

- 👮 **Fazit:** Wir müssen verstehen, wie Social Engineering abläuft.

Wie arbeitet ein „Social Engineer“?

Phasen eines SE-Angriffs

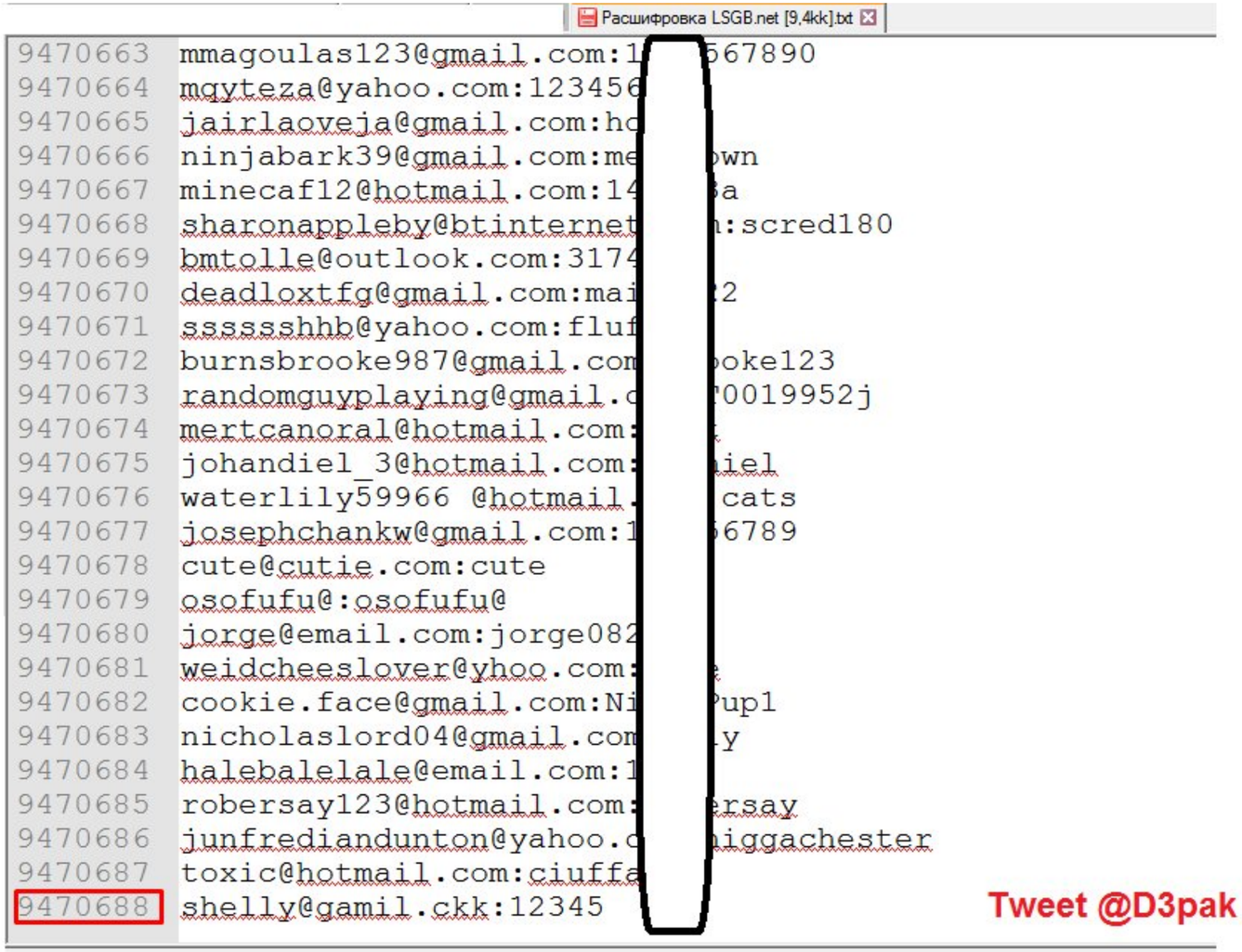
- Phase 1: Der Social Engineer sammelt und kombiniert Informationen über Opfer.
- Phase 2: Der Social Engineer interagiert mit potenziellen Opfern (Aufbau einer Vertrauensbeziehung).
- Phase 3: Der Social Engineer nutzt das Opfer aus, um eigene Ziele zu erreichen.
- Phase 4: Der Social Engineer verwischt 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



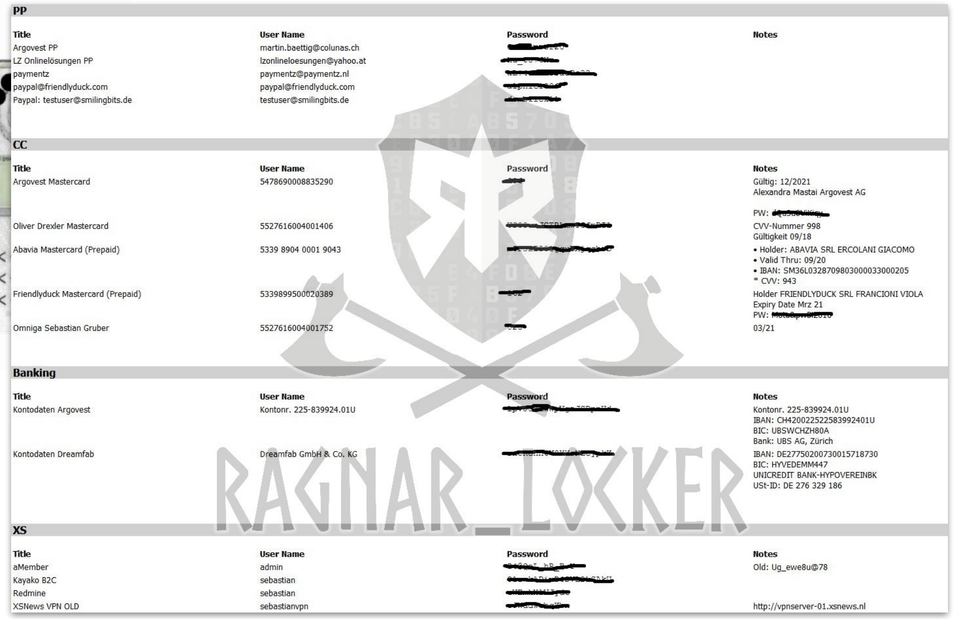
- Have I Been Pwned listet **11,7 Milliarden** geleakte Nutzerkonten, der HPI Identity Leak Checker **12,7 Milliarden**.

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

Bildquelle: https://twitter.com/d3pak/status/957984061892435968

Beispiel Datenleck als Quelle

Kurze Demonstration



- “Moderne” Ransomware zieht oft massenhaft Daten von Opfern vor Verschlüsselung ab, um dann mit deren Veröffentlichung zu drohen, sollte das Opfer nicht zahlen.
- 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

Beispiel soziale Medien als Quelle

🤔 *Was sehen Sie?*

Bildquelle: Reddit

Beispiel soziale Medien als Quelle

Bildquelle: Reddit

Beispiel exponierte Server (hier Kameras)

🤓🍿 Kurze Demonstration

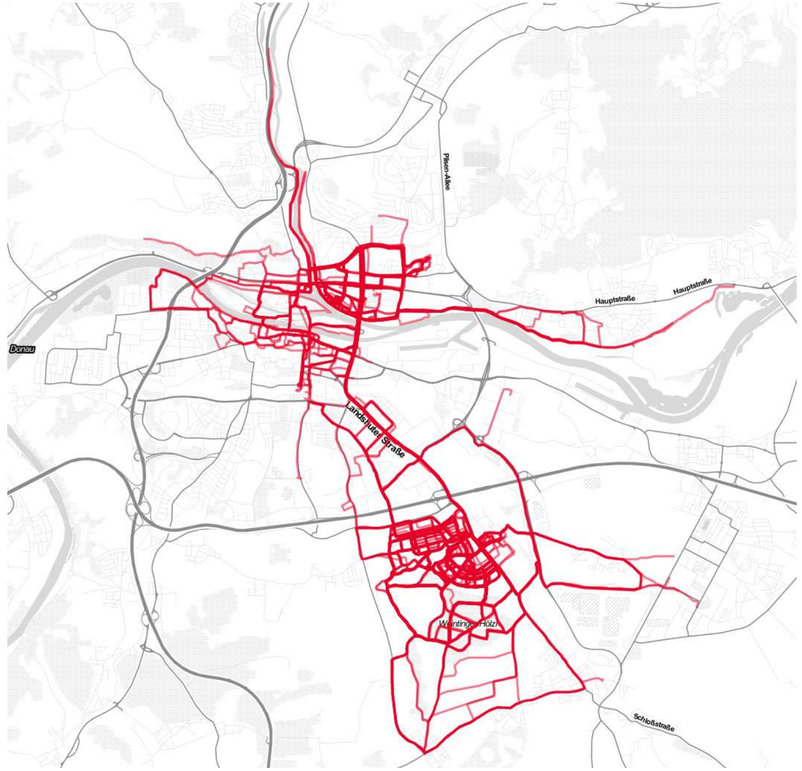
Bildquelle: Exponierter Videostream auf insecam.org

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.

- 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

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

Aktuelle SE-Angriffe

Hacker tarnen Malware-USB-Sticks als "Geschenke"

09.01.2022

Die gut getarnten Päckchen sollen Mitarbeiter*innen dazu bringen, die USB-Sticks an die Rechner anzustecken.

Mann fällt auf Fake-SMS rein: 900 Euro Handyrechnung

Arbeiterkammer und Landeskriminalamt warnen vor dem Öffnen von Links in Fake-SMS. Es drohe saftiger finanzieller Schaden.

CHRONIK

Betrugsmasche mit Online-Verkaufsplattformen

Durch eine Betrugsmasche, vor der die Polizei seit zwei Monaten warnt, sind zuletzt österreichweit nochmals mehr als 70 Menschen um ihr Geld gebracht worden. Der Gesamtschaden beläuft sich laut Polizei auf rund 50.000 Euro.

Online seit heute, 8.00 Uhr

Die Betrüger suchen sich ihre Opfer auf Online-Verkaufsplattformen wie willhaben oder eBay und geben vor, den angebotenen Gegenstand kaufen zu wollen. Dann gaukeln sie vor, dass sie nicht persönlich kommen können, um das Verkaufsobjekt abzuholen. Sie schieben eine Quarantäne oder eine Erkrankung vor. Sie haben auch schon eine Lösung parat: ein Postkurier solle die Ware abholen. Die angeblichen Käufer wollen aber, dass der Verkäufer diese Versandkosten vorstreckt. Nach dem Erhalt der Lieferung bekomme er diese Versandkosten rückerstattet und den Kaufpreis für den Artikel bezahlt.

CHRONIK

In Falle gelockt: 20.000 Euro weg

Ein Linzer, der geglaubt hat sein Geld gewinnbringend in Kryptowährung anzulegen, ist einem Betrüger aufgesessen. Der 35 Jahre alte Mann verlor gut 20.000 Euro. Der Lockvogel war eine Frau aus Tschechien, die er über eine Online-Datingapp kennengelernt hatte.

19. Jänner 2022, 6.00 Uhr Teile

Hacking group also used an IE zero-day against security researchers

By Lawrence Abrams February 4, 2021 12:07 PM 0

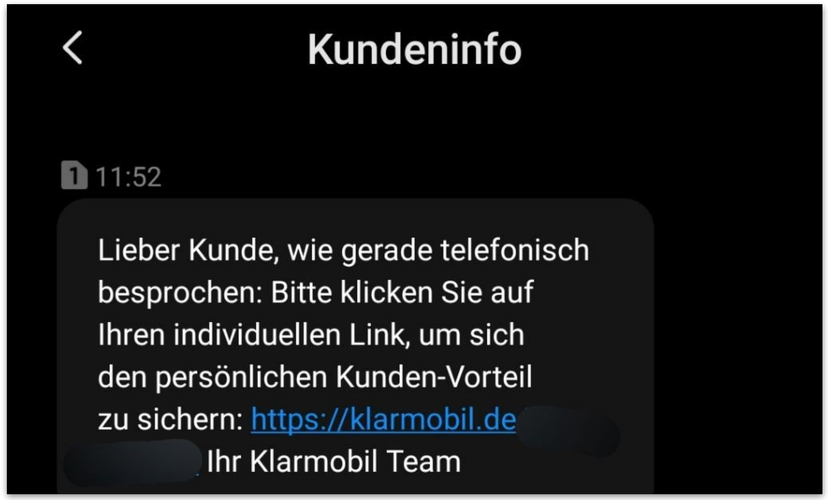
Frau verlor durch Online-Betrug Tausende Euro

Die Polizei verzeichnet erneut zahlreiche Fälle von Online-Betrügen, bei welchen sich die Täter Zugriff auf die Computer ihrer Opfer verschaffen. Eine 57-Jährige aus dem Bezirk Eferding ist so um knapp 14.000 Euro gebracht worden.

8. Jänner 2022, 16.44 Uhr (Update: 9. Jänner 2022, 10.53 Uhr) Teilen

Quellen: https://futurezone.at/digital-life/hacker-usb-stick-malware-geschenk-firmen-cyberkriminelle-fbi/401865719, https://ooe.orf.at/stories/3139184/, https://ooe.orf.at/stories/3137752/, https://ooe.orf.at/stories/3139852/, https://futurezone.at/digital-life/fake-sms-schaden-900-euro-handyrechnung/401435521, https://www.bleepingcomputer.com/news/security/hacking-group-also-used-an-ie-zero-day-against-security-researchers/

Beispiele echter Angriffsversuche



Bildquellen: Spammer via Signal, https://www.verbraucherschutz.com/warnungsticker/abzocke-sms-im-namen-von-dhl-fuehrt-in-abofalle/, anderer Spammer

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 (siehe Vishing, Smishing usw.)
- **Sextortion**: 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.

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? 🤔

- Wie der Name impliziert, 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 10/11 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 fünf 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.

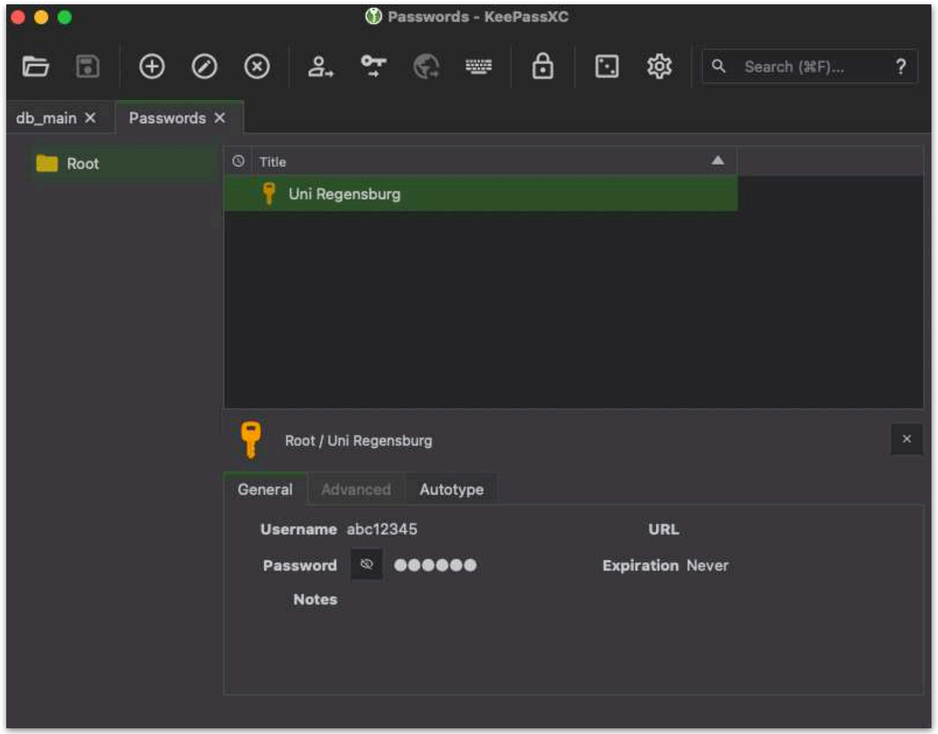
👨‍💼 Was schlagen Sie vor? Sie sind Experte!

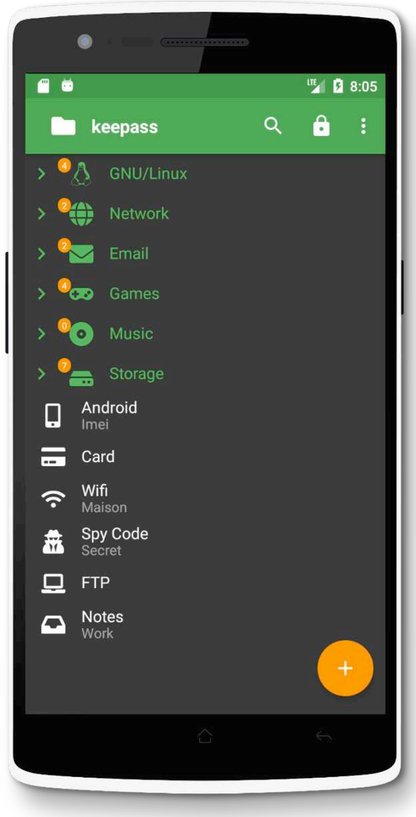
Tipps gegen Social Engineering

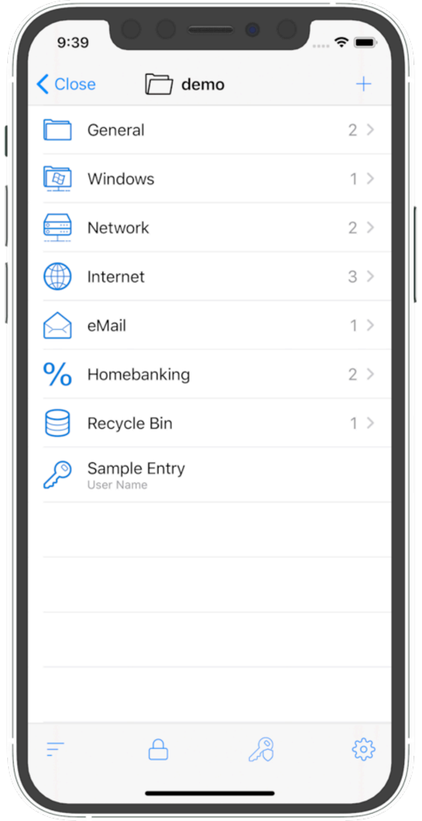
- Überlegen Sie vor Registrierung bei jedem Onlinedienst, ob Sie diesen wirklich brauchen.
- Seien Sie sich bewusst, welche “unsichtbaren” Daten ein Anbieter über Sie sammelt.
- Teilen Sie nicht alles offen im Internet: Setzen Sie Ihre Profile auf “privat”. Entfernen Sie sensible Daten und Metadaten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



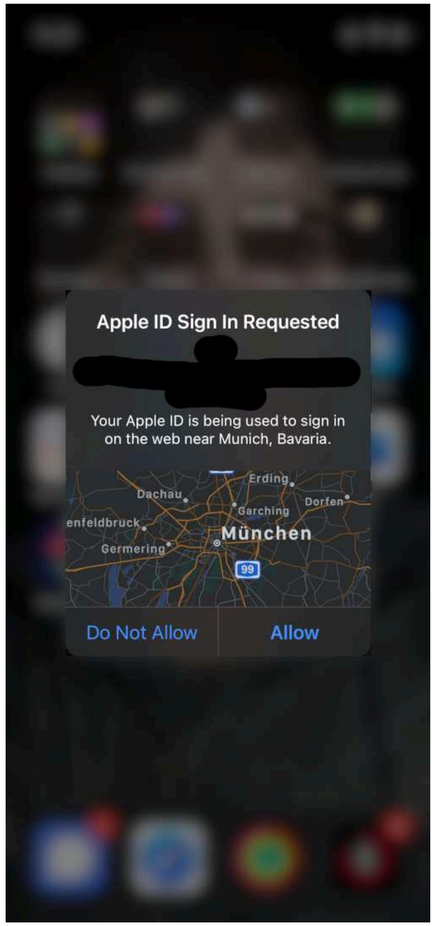


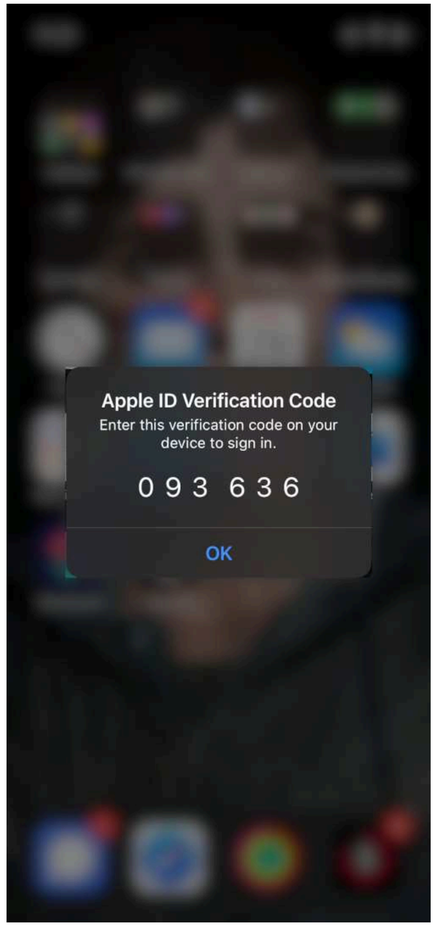


Bildquellen: Eigenes Bild, https://www.keepassdx.com/, https://keepassium.com/img/view-group_flat.png?t=20191121T2359

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).

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
  - Sie können Informationen und IT niemals zu 100 % technisch schützen, auch nicht zu 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.

Awarenesskampagnen: Modulbeispiele

- Sicheres Arbeiten im Home Office
- Social Engineering
- Melden von Sicherheitsvorfällen
- Umgang mit sozialen Medien
- Klassifizierung von Informationen
- Clean-Desk-Policy
- Umgang mit Wechselmedien
- Nutzung öffentlicher Netzwerke (bspw. WLAN)

Awarenesskampagnen: Kanalbeispiele

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

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.

Zwischen zwei Kampagnen ...

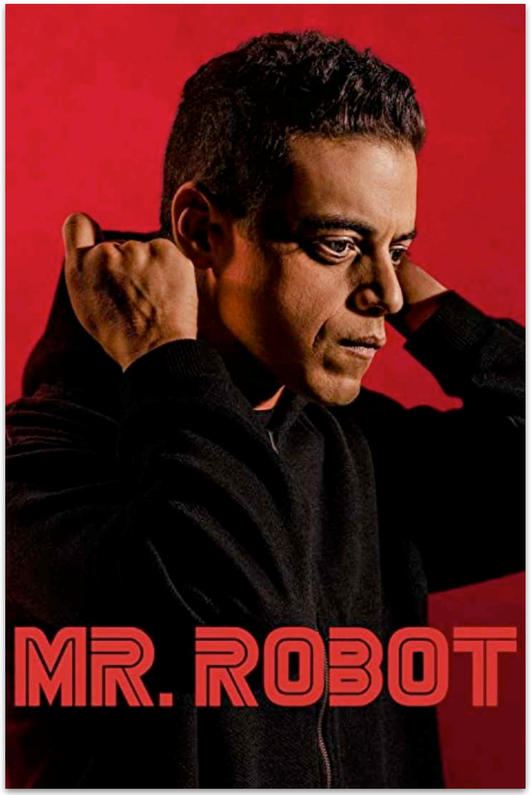
- Sehen Sie Awarenesskampagnen nicht als Einmalaktivität, denn das Bewusstsein der Mitarbeiter schwindet auf natürliche Weise mit der Zeit.
- Sensibilisieren Sie Mitarbeiter kontinuierlich, aber seien Sie weder aufdringlich noch langweilig.
- Beispiele für “Awareness zwischendurch”: Interne Präsenz-Schulungsangebote 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 bedeutet, uns zu manipulieren. Das 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 und wird im Zweifel von Social Engineers und anderen gegen uns verwendet werden.
- Nutzen Sie einen Passwortmanager und setzen Sie Ihre Onlineprofile auf privat!

Empfehlung zum Schluss 🎬🍿



Schauen Sie Mr. Robot.

- Vier Staffeln, 45 Episoden
- Behandelt “echtes” Hacking realitätsnah, vor allem auch Psychologie.
- Kein GoT-Ende!

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

Vielen Dank für Ihre Aufmerksamkeit

🤔 Finale Fragen?

📫 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/Kompendium_Einzel_PDFs/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2020.pdf?__blob=publicationFile&v=1
- Watchlist Internet (Aktuelle Angriffe auf Privatpersonen): https://www.watchlist-internet.at/

- Helisch, Pokoyski: Security Awareness, 2009, E-Book: https://link.springer.com/book/10.1007/978-3-8348-9594-3
- Hadnagy: Social Engineering: The Science of Human Hacking, 2018.
- Kahneman: Schnelles Denken, langsames Denken, 2012.