

# Cyber Security Awareness Training

Erstellt von <https://security-companion.net/>

Version 1.6

# Über dieses Training

- Veröffentlicht unter Open Source Lizenz (Creative Commons Zero v1.0 Universal)
  - > Training steht zur freien Verfügung
  - > Verwendung, Änderungen und Vervielfältigung ist gestattet
- Aktuelle Version kann [hier](#) heruntergeladen werden

# Übersicht

- Motivation
- Social Engineering
- Sicherheit im Internet
- Passwörter
- 2-Faktor Authentifizierung
- WiFi / VPN
- Backups
- Allgemeine Hinweise
- Weiterführende Informationen

# Motivation

- Hackerangriffe auf Firmen und Organisationen sind in letzter Zeit stark angestiegen
- Alle technischen Absicherungen sind nutzlos wenn die Personen, die diese bedienen diese bewusst oder unbewusst umgehen
- Mitarbeiter einer Organisation sind oft das schwächste Glied in der Kette.
- Diese Präsentation soll dazu dienen, Mitarbeiter für die Zukunft zu rüsten und für die Themen der Cyber Security zu sensibilisieren.

# Schützenswerte Daten

- Adressen von externen oder internen Kontakten
- Kontoverbindungen
- Benutzernamen/Passwörter
- Finanzberichte
- in der Organisation verwendete Hardware und Software
- etc.

- Sozialversicherungsnummer
- Geburtstag, Geburtsort, Name der Mutter (wird oft verwendet um Passwörter wiederherzustellen)
- Emailadresse
- usw.

# Social Engineering

- Definition: Methoden, die Angreifer nutzen um Vertrauen zu Personen/Mitarbeitern aufzubauen und ihnen so sensible Informationen zu entlocken, oft unter Einsatz von Druck und dem Versuch, Mitleid zu erregen (Phishing)
- Beispiele:
  - wenn nicht sofort die vom vermeintlichen Chef angeordnete Überweisung erfolgt drohen hohe Mahungskosten
  - Angreifer gibt sich als neuer Kollege aus und bittet um Mithilfe in Form der telefonischen Übermittlung von Passwörtern

- weitere Beispiele:
  - Angreifer gibt sich als technischer Support von z.B. Microsoft aus und gibt an, ein Problem auf dem Computer lösen zu müssen
  - Angreifer gibt sich als Enkel aus und gibt vor, in großer Not zu sein und (finanzielle) Unterstützung zu benötigen
  - Angreifer senden eine E-Mail und bitten um einen dringenden Rückruf beim Kundendienst eines genannten Unternehmens. Die Telefonnummer ist allerdings nicht die tatsächliche sondern eine von den Angreifern kontrollierte (Callback Phishing)



# Sicherheit im Internet


- Browser und E-Mail Clients sind direkt dem Internet ausgesetzt  
-> immer aktuell halten um gegen neue Angriffe möglichst gut geschützt zu sein
- Vor Anklicken einen Links aus E-Mail, Chat-App, SMS etc. immer prüfen
  - Habe ich diesen Link erwartet?
    - Link eines Paketzustellers obwohl gar kein Paket erwartet wird
    - Link einer Bank bei der gar kein Konto vorhanden ist

- Ist mir die URL(=Linkadresse) bekannt?
- Ist die Übersetzung der Webseite oder E-Mail mangelhaft?
- Ist in der URL wirklich kein Buchstabe geändert?  
<https://amazon.com> und <https://amaz0n.com> sind komplett verschieden
- Bin ich auf der offiziellen Seite oder gehört der hintere Teil der Domain zu einem anderen Land? .ru, .uk, .cn etc.??
  - Beispiel: <https://firma.com.mx> oder <https://firma.de> anstatt <https://firma.com>

- Vor dem Anklicken eines Links auf diesen mit der Maus zeigen (auf Tablets lange draufdrücken) und in der Statusleiste dessen Korrektheit überprüfen
  - Ist anstatt einer URL eine IP-Adresse (93.235.136.159) sichtbar?
- Gekürzte Links mit Diensten wie <https://urlex.org/> oder <https://unshorten.me/> überprüfen (den ganzen Link anzeigen lassen)

- Beim Besuch von unbekanntem Seiten diese kritisch hinterfragen und im Zweifelsfall den Besuch abbrechen
- Ist das Design verschoben oder fehlt es gänzlich?
- Webseiten können mit <https://virustotal.com> auf Viren überprüft werden
- Adresse einer Webseite besser direkt im Browser eingeben anstatt Link in E-Mail anzuklicken

- Auf Verkaufsplattformen immer nur die offiziellen Nachrichtenkanäle verwenden
  - Falls sich ein potenzieller Käufer per Messenger meldet immer besonders vorsichtig und mißtrauisch sein
  - Eine häufige Masche ist, vorzugeben, einen Artikel kaufen zu wollen und zusätzlich noch Gutscheinkarten die der Verkäufer zusätzlich im Namen des Käufers erwerben soll
  - Nicht unter (zeitlichen) Druck setzen lassen sondern Kontakt abbrechen

- Wenn eine E-Mail mit verdächtigem Anhang von einem Freund/Bekanntem kommt vor Öffnen des Anhangs telefonisch beim Absender nachfragen ob E-Mail legitim ist
- Auf Schloss in der Browserleiste achten 
  - Achtung! Das Schloss bedeutet nur, dass die Verbindung zwischen Browser und Client verschlüsselt ist.
  - Ein Schloss bedeutet nicht automatisch, dass die Seite sicher ist bzw. nicht von einem Angreifer betrieben wird.

- Niemals Software installieren die in einem Browser Pop-Up beworben wird
- Auf öffentlichen Rechnern (Hotel-Lobby, Bücherei etc.) nicht in E-Mail Konto oder Online-Banking einloggen da Angreifer Daten mitschneiden können
- Macros in Microsoft Word, Excel etc. bei verdächtigen Anhängen niemals aktivieren!

# E-Mail

- Viele E-Mail Programme zeigen nur den Namen des Absenders und nicht dessen komplette E-Mail Adresse an
- Angreifer verändern E-Mails so, dass sie legitim aussehen obwohl sie ein Fake sind (Forged E-Mails)
- Überprüfen der Domain: Nur [service@paypal.com](mailto:service@paypal.com) ist legitim, [kundenservicepaypal@gmail.com](mailto:kundenservicepaypal@gmail.com) hingegen nicht
  - Die zweite E-Mail Adresse wird nicht durch Mail-Server und Spamfilter ausgefiltert und wird deswegen gerne von Angreifern verwendet



- Nicht dieselbe E-Mail Adresse beruflich und privat verwenden
- Eigene E-Mail Adresse für Online-Shopping verwenden
  - Viele Shopping-Seiten fügen E-Mail Adressen unerlaubterweise zu Mailinglisten hinzu
  - Wenn der Account nach einer gewissen Zeit zu viel Spam erhält kann einfach ein neuer erstellt werden
  - -> Persönlicher E-Mail Account erhält deutlich weniger unerwünschte E-Mails

# Passwörter

- Angreifer haben [lange Passwortlisten](#) mit Millionen von Passwörtern zur Verfügung. Diese probieren sie auf Login-Seiten aus bis sie Erfolg haben
- Beispiele für schlechte Passwörter:
  - P@ssw0rd
  - Sommer2021
  - Geheim1
  - abc123

- Mindestvoraussetzungen für Passwörter:
  - Mindestens 12 Zeichen mit Kombination aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen verwenden
  - Je länger ein Passwort desto schwieriger ist es, dies zu knacken
  - Kein Passwort wiederverwenden

- Möglichst folgende Wörter in den Passwörtern vermeiden da Angreifer diese leicht recherchieren können:
  - Name des Haustieres oder der Kinder, zweiter Vorname
  - Geburtstag, Adresse
  - Wörter die im Zusammenhang mit dem Arbeitgeber stehen (Gebäudename etc.)
  - Aktuelle Jahreszahl

- Besser die Anfangsbuchstaben eines Satzes verwenden
  - Beispiel: legPmS55: Ich esse gerne Pizza mit Salami 55
- Niemals Passwörter direkt im Klartext auf der Festplatte speichern oder mit Zettel an den Bildschirm heften
- Mithilfe von [haveibeenpwned.com](https://haveibeenpwned.com) oder [HPI Identity Leak Checker](#) prüfen ob eigene E-Mail Adresse/Passwort-Kombination bereits Teil eines Datenlecks war

# Passwortmanager

- Digitaler Safe für alle Benutzer-Passwort Kombinationen
  - Passwörter werden verschlüsselt gespeichert und sind durch ein Master-Passwort gesichert
- Synchronisierung zwischen mehreren Geräten möglich
- Bieten oft die Möglichkeit, zufällig generierte Passwörter zu erzeugen

- Kostenlose OpenSource-Varianten: KeepassXC und Bitwarden
  - Browser-Erweiterungen erhöhen den Komfort durch automatisches Ausfüllen von Login-Feldern
- Viele kommerzielle Anbieter bieten auch kostenlose Varianten an
  - Allerdings können bei einem Hackerangriff auf den Anbieter dann auch die eigenen Passwörter entwendet werden

# 2-Faktor Authentifizierung

- Logins zusätzlich zur Benutzernamen/Passwort Kombination mit einem weiteren zweiten Faktor absichern
  - Beispiel: zeitlich ablaufende Ziffernfolge auf dem Handy (Token)
  - Nur mit diesem ist ein Login möglich, schützt effektiv vor Missbrauch des Zugangs
- Wo möglich aktivieren



- Tokens die per SMS verschickt werden vermeiden, stattdessen Tokens die im Handy generiert und sich minütlich ändern vorziehen
- Eventuell QR-Code/Einrichtcode im Passwortmanager hinterlegen um bei Verlust des Handys nicht aus Diensten ausgesperrt zu werden

# W-LAN

- Hacker können leicht ein eigenes W-LAN aufspannen das gleich heißt wie das ursprüngliche (z.B. Bücherei- oder Zug-WLAN)
  - Öffentliche, unverschlüsselte W-LAN meiden
  - stattdessen nur verschlüsselte W-LANs und/oder VPN verwenden
- Wo möglich Kabel- statt W-LAN-Verbindungen verwenden

# VPN

- VPNs machen eine Verbindung nicht automatisch sicherer da heutzutage eh schon viele Verbindungen schon durch SSL/TLS verschlüsselt sind
- VPN ist hilfreich wenn
  - vor dem Internetprovider/Hoster versteckt werden soll welche Seiten man besucht
  - Vor dem Betreiber einer Webseite versteckt werden soll aus welchem Land man kommt (und somit Inhalte frei schalten möchte die sonst nicht verfügbar wären)

- Kommerzielle VPN-Anbieter versprechen zwar, die Benutzer-Daten zu verschlüsseln und deswegen nicht auf sie zugreifen zu können. Dies zu überprüfen ist aber schwierig
- Kostenlose VPN-Anbieter meiden

# Datenschutz

- Regelmäßig darüber nachdenken welche Datentypen man bei der Arbeit und privat nutzt und wie man diese schützen kann wenn sie verloren gehen bzw. gestohlen werden und sich in den Händen von jemandem befinden der mir nicht freundlich gesinnt ist
- Computer: Obwohl man sich einloggen muss um sie verwenden zu können kann man die Daten auslesen wenn man die Festplatte in einen anderen Computer einsteckt oder einen USB-Stick mit einem alternativen Betriebssystem einsteckt

- Deshalb Computer mit Tools wie Bitlocker/VeraCrypt (Windows), FileVault (Mac) oder LUKS (Linux) verschlüsseln
- Das gleiche gilt für externe Festplatten und USB-Sticks: Sobald sie an einen Computer angeschlossen werden kann man ihre Daten auslesen wenn sie nicht verschlüsselt sind

# Cloud-based/online Storage

- Viele Anbieter von Cloudspeicher verschlüsseln Daten auf deren Servern - allerdings besitzen sie den Master-Schlüssel um die Daten entschlüsseln und lesen zu können
- Stattdessen besser Anbieter suchen die Zero-knowledge unterstützen
  - Dies bedeutet dass die Daten lokal auf dem Rechner verschlüsselt werden bevor sie ins Internet übermittelt werden
  - Niemand außer Ihnen selbst kann sonst die Daten lesen
- Alternativ Daten lokal mit Tools wie Cryptomator oder BoxCryptor verschlüsseln bevor man sie an z.B. Dropbox versendet

# Backups

- Regelmäßig Backups von wichtigen Daten erstellen, beispielsweise über NAS oder (verschlüsselten) USB-Stick
- Mehrere Versionsstände vorhalten, z.B. nach Schema Großvater, Vater, Kind
- Nur Backups, die nicht mit einem Computer oder Netzwerk verbunden sind (Offline-Backups) schützen vor Verschlüsselung durch Trojaner o.ä.
- Regelmäßig Wiederherstellen der Daten üben um für den Ernstfall vorbereitet zu sein



# Allgemein

- Es gibt keinen 100% Schutz vor Angriffen. Es ist nur möglich, Maßnahmen zu ergreifen um das Risiko möglichst gering zu halten
- Regelmäßig überprüfen ob das was man gestern tat auch heute und morgen noch sinnvoll und sicher ist

- bei Produkten die man kostenlos nutzen kann ist man oft selbst das Produkt
  - Anbieter nutzen Kundendaten und verkaufen diese an Werbepartner weiter
  - Freeware kann sich als Spyware entpuppen die sensible Benutzerinformationen an die Entwickler des Programmes verschickt
  - Manchmal ist es besser, für ein Produkt zu zahlen und so Datensammelei einzudämmen
- Nur notwendige Software installieren und diese nur aus vertrauenswürdigen Quellen installieren

- Immer Betriebssystem und verwendete Software aktuell halten
- Virens Scanner aktuell halten
- Sich dessen bewusst sein, das Software-Suiten die versprechen gegen "alle" Angriffsmöglichkeiten zu schützen auch ihre Grenzen haben
- Keine unbekanntes USB-Sticks die man beispielsweise auf dem Parkplatz gefunden hat an Rechner anschließen
  - Programme können selbstständig, unbemerkt und ohne Nutzeraktion starten
  - Angreifer können diese Methoden gezielt nutzen um in ein Netzwerk einzudringen

# Weiterführende Informationen

- [Kurse des Hasso-Plattner-Instituts](#)
- [BSI Leitfaden für Politiker](#) - nicht nur für Politiker relevant