Cyber Security Awareness Training

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

Version 1.2

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
- 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.

Social Engineering

- Methoden, die Angreifer nutzen um Mitarbeitern sensible Informationen zu entlocken, oft unter Einsatz von Druck und dem Versuch, Mitleid zu erregen
- 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

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 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 (192.168.178.1) sichtbar?
- Gekürzte Links mit Diensten wie https://urlex.org/ oder https://unshorten.me/ überprüfen (den ganzen Link anzeigen lassen)

- Beim Besuch von unbekannten 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

- Wenn eine E-Mail mit verdächtigem Anhang von einem Freund/Bekannten 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!

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: IegPmS55: 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 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: KeepassX 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 immer aktivieren!
- 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
- Kommerzielle VPN-Anbieter versprechen zwar, die Benutzer-Daten zu verschlüsseln und deswegen nicht auf sie zugreifen zu können. Dies zu überprüfen ist aber schwierig

Datenschutz

- bei Produkten die man kostenlos nutzen kann ist man oft selbst das Produkt
  - Anbieter nutzen Kundendaten und verkaufen diese an Werbepartner weiter
  - Manchmal ist es besser, für ein Produkt zu zahlen und so Datensammelei einzudämmen

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-Backps) schützen vor Verschlüsselung durch Trojaner o.ä.
- Regelmäßig Wiederherstellen der Daten üben um für den Ernstfall vorbereitet zu sein

Allgemein

- Immer Betriebssystem und verwendete Software aktuell halten
- Virenscanner aktuell halten
- Keine unbekannten 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