Handout von Daniel Moßbrucker & Albrecht Ude zum Vortrag bei #nr19

So schützen sich Journalist:innen gegen Doxing

Was ist Doxing?

- Veröffentlichung personenbezogener Daten im Internet, die entweder durch unrechtmäßige Attacken (z.B. Hacking) erlangt wurden oder bereits offen im Netz waren und für einen Dox aggregiert werden.

Welche Journalist:innen sind besonders gefährdet?

- Journalist:innen, die in Ihrer Berichterstattung Haltung zeigen, insbesondere
  - die für die öffentlich-rechtlichen Sender oder großen Medienhäuser arbeiten,
  - die sich regelmäßig kritisch über Rechtspopulist:innen äußern,
  - YouTuber,
- und jeweils das persönliche und berufliche Umfeld all‘ dieser Journalist:innen
- weibliche Journalist:innen sind häufig besonders betroffen.

Drei Schritte, um sich gegen Doxing präventiv zu schützen:

1. Phishing erkennen

- Das können Journalist:innen z.B. hier, hier und hier trainieren
- Grundregeln
  - keine Emails öffnen, die man nicht kennt oder nicht erwartet
  - nie dem Anzeigenamen vertrauen, sondern die Email-Adresse ansehen
  - bei Verdacht auf Phishing Infos über Suchmaschinen recherchieren
  - niemals auf einen Link klicken, ohne ihnen genau angesehen zu haben
    - Domain recherchieren: von rechts nach links lesen
    - https-Zertifikat ansehen
  - niemals Anhänge öffnen bei Verdacht auf Phishing

2. starkes Passwort wählen & sinnvoll verwalten

- Die Länge eines Passworts ist wichtiger als die Komplexität, aber nur ein langes, komplexes Passwort ist sicher (kein Passwort sollte weniger als zwölf Zeichen haben)
- Passwörter, die sich Menschen einfach merken können, sind unsicher
- Es geht nicht mehr ohne Passwort-Manager heute!
  - z.B. Keepass, Apple Keychain, 1Password, Dashlane, Lastpass
- niemals Passwörter bei mehreren Diensten verwenden, weil Doxxer:innen dann diverse Accounts übernehmen

3. Zwei-Faktor Authentifizierung

- Idee: Neben dem Passwort ist ein zweiter Log-in-Schritt nötig, falls ein:e Angreifer:in das Passwort stiehlt
- Möglichkeiten
  - zweiter Code per SMS an Handynummer
  - zweiter Code per Code-Generator-App auf zuvor registriertem Smartphone (z.B. Google Authenticator)
  - Security Key als zweiter Schritt, der physisch ins Gerät gesteckt werden muss (z.B. YubiKey)

Hinweise zum Datenmanagement für Journalist:innen

Welche Daten haben im Netz nichts verloren?

Viele Daten "normaler" Nutzer, die im Netz zum Kauf angeboten werden, wurden nicht bei diesen Nutzern selbst gestohlen, sondern bei den Diensten (soziale Netze, Online-Shops, Mailprovider...), die diese Menschen in gutem Glauben genutzt haben. Diese Firmen haben die Daten ihrer Kunden mangelhaft geschützt. Wir leben im Zeitalter der Massen-Hacks, bei denen Millionen von Kundendaten erbeutet werden.

Bestimmte Daten müssen Journalist:innen deswegen besonders schützen, wenn diese auf sie als Person hinweisen.

- Geburtsdatum: geben Sie niemals ihr echtes Geburtsdatum im Netz ein. In vielen Fällen dient es nur der Alterskontrolle.
- Ihr Name und Ihr echtes Geburtsdatum sind die wichtigsten Identifikatoren für Sie.
- Telefonnummer, Mobilfunknummer, private E-Mail-Adresse: geben Sie diese nur dort bekannt, wo Sie auch kontaktiert werden wollen.
- Kontonummern, PINs, TANs, usw. sollten Sie nur dort eingeben, wo sie benötigt werden, also etwa bei der entsprechenden Bank.
- Achten Sie bei der Dateneingabe immer darauf, dass die Verbindung verschlüsselt ist.
- Denken Sie immer daran, wenn Sie einer App oder einem Netz Zugriff auf Ihr Adressbuch gewähren - Sie liefern dann die Daten Ihrer Konrakte an die App oder das Netz aus.

Zwei Datenbanken, in denen man nachschauen kann, ob man von einem Datenleak betroffen ist:

- HIBP - ';--have i been pwned? Datenbank von Troy Hunt:https://haveibeenpwned.com/
- ILC - Identity Leak Checker des Hasso-Plattner-Institutes https://sec.hpi.de/ilc/search

Kontakt

- Daniel Moßbrucker – Journalist & Trainer für digitale Sicherheit
  - mail@daniel-mossbrucker.de I twitter: @damossb I web: daniel-mossbrucker.de
- Albrecht Ude – Journalist, Researcher, Trainer
  - albrecht@ude.de I @Aude_berlin I web: ude.de