Kryptografie

Grundbegriffe

- Vertraulichkeit: Unbefugte können nicht mitlesen
- Integrität: Nachricht ist unverändert
- Authentizität: Urheber/Autor der Nachricht steht eindeutig fest
- Schlüsselaustausch: sensibler Prozess. Oft wird extra Kanal zum Austausch von Schlüsseln bzw zur Verifikation der Echtheit verwendet - um einen man-in-the middle auszuschließen

- Anonymität: aus einer (verschlüsselten) Nachricht kann keinerlei Rückschluss auf den Autor geschlossen werden. Bei 2 (zwei) verschiedenen Nachrichten desselben Autors kann dies nicht festgestellt werden
- Pseudonymität: Trotz Unkenntnis des konkreten Autors können 2 (verschiedenen Nachrichten) für Dritte auf denselben Autor zugeordnet werden

- Transport-Verschlüsselung: der Transport zwischen relevanten Servern ist geschützt. Der Betreiber eines Servers kann mitlesen!
- Ende-zu-Ende Verschlüsselung: auch Server Betreiber können NICHT mitlesen

- Symmetrische Verschlüsselung: alle Parteien einer Kommunikation haben denselben (geheimen) Schlüssel
  - Ver- und Entschlüsselung erfolgt mit demselben geheimen Schlüssel zzgl dem Algorithmus
- Einfachste oder Pseudo-Verschlüsselungen, von denen abzuraten ist, wie u.a.:
  - Leetspeak
  - ROT-13

- Asymmetrische Verschlüsselung: jede Partei hat ein Schlüsselpaar
  - öffentlicher Schlüssel: kann und wird frei veröffentlicht. Es gibt auch öffentliche Verzeichnisse (Keyserver)
  - privater Schlüssel: wird nicht weitergegeben. Zugriff oft mit Kennwort geschützt
  - zur Vertraulichkeit wird eine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt
    - der Empfänger entschlüsselt mit seinem privaten Schlüssel
  - zur Integrität und Authentizität kann Sender die Nachricht mit seinem privaten Schlüssel signieren
    - der Empfänger kann die mitgeschickte Signatur mit dem öffentlichen Schlüssel des Absenders verifizieren
  - im Folgenden wird dieser Fall weiter erörtert

- “Nachrichten” können verschiedene Arten von Dokumenten sein:
  - E-Mails
  - Dateien
  - Texte (auf Webseiten)

- Zentrale/hierarchische Schlüsselverzeichnisse, z.B. https/SSL, über Trustcenter
- Web-of-Trust: durch Signieren des öffentlichen Schlüssels wird die Authentizität, ggf inkl Ausweis Kontrolle bekundet. Es entstehen selbstorganisierte Netze des Vertrauens. Siehe auch Keysigning-Parties.

Anwendungen

- Vertrauliche/verschlüsselte Kontaktaufnahme (mit Journalisten)
- Sicherstellen, dass derselbe (pseudonyme) Autor/Whistleblower Kontakt aufnimmt
- Datenträger/Festplatten Verschlüsselung
- Verschlüsselung von Dateien vor hochladen in Cloud-Speicher, z.B. Dropbox

E-Mail

E-Mail Provider / Anbieter

Hier eine kleine Auswahl:

- Posteo
- Proton Mail
- Web.de
- GMail

PC Linux/Windows

Mit Addons (GnuPG aka “gpg” bzw. gpg4win unter Windows) zum E-Mail Client Thunderbird

Browser

Als Email Client wird die Web-Schnittstelle des E-Mail Anbieters, z.B. web.de oder posteo, verwendet. Browser-Erweiterung (Add-On) Mailvelope erlaubt die lokale Ver- und Entschlüsselung auf dem eigenen Rechner - innerhalb des Browsers.

In diesem Fall müsste man mMn dem E-Mail Provider soweit vertrauen, dass dieser Mailvelope korrekt einbindet - und einem Daten, Passwörter oder Schlüssel abgreift. Insbesondere das Sicherheits-Backup, welches auf web.de teilweise zwingend notwendig ist, sehe ich persönlich sehr problematisch; siehe Web.de Verschlüsselte Kommunikation einrichten. Auf posteo ist ein solcher Schritt nicht notwendig.

Android / Smartphone

Email Client K9 zzgl. OpenKeyChain

Unverschlüsselt

Die E-Mail Adressen von Empfänger und Absender sind immer zwingend unverschlüsselt. Der Betreff ist oft ebenfalls unverschlüsselt; hierüber muss man sich im Klaren sein!

Thunderbird bietet die Möglichkeit, den Betreff ebenfalls zu verschlüsseln. Allerdings kann dann der Empfänger den Betreff oftmals ebenfalls nicht lesen. Des weiteren erschwert bzw verlangsamt sich die Sortierung von E-Mails ebenfalls. Daher würde ich persönlich keinen Gebrauch von dieser Einstellung machen.

Messaging

Threema

Siehe https://threema.ch/de/faq/why_secure

Empfehlung! Obwohl kommerziell.

Signal

Lt. https://support.signal.org/hc/de/articles/360007318911-Woher-wei%C3%9F-ich-dass-meine-Kommunikation-vertraulich-ist " Signal ist darauf ausgelegt, niemals sensible Informationen zu sammeln oder zu speichern. Nachrichten und Anrufe in Signal können weder von uns noch von Dritten eingesehen werden, da sie immer Ende-zu-Ende-verschlüsselt, privat und sicher sind. "

Telegram

Lt. https://www.datenschutz.org/telegram/ " Telegram verschlüsselt zwar die Übertragung zwischen Endgerät und Cloud-Server, eine Ende-zu-Ende-Verschlüsselung bietet die App jedoch nur bei geheimen (Einzel-)Chats als Option. In der Cloud hinterlegte Informationen und Chats können so sowohl von Telegram als auch potentiell von Dritten eingesehen werden. "

WhatsApp

siehe https://www.dr-datenschutz.de/die-ende-zu-ende-verschluesselung-bei-whatsapp/

Anonymität vs Spuren

Viele Webseiten, wie z.B. Email Provider könn(t)en die IP Adressen protokollieren. Daher wird die Verwendung über ein VPN - zur Wahrung der Anonymität - dringend angeraten.

Mögliche Angriffsvektoren

Kennwort-Attacken

- Zu einfaches Kennwort, siehe z.B. Meistgenutzte Passwörter
- Abhören einer Funktastatur, siehe z.B. Keysniffer auf Golem.de

Physikalischer Zugriff

Auch temporärer Zugriff auf den Computer kann ausreichend sein, z.B. die Festplatte auszubauen oder um einen (unscheinbaren) Keylogger zwischen Computer und Tastatur einzustecken, um die Passwort-Eingabe mitzuschneiden!

Nachgestelltes Netzwerk/WLAN und Webseite

Webseiten können täuschend echt aussehen, wo man zur Eingabe des Kennworts aufgefordert wird .. siehe z.B. Wikipedia zu Phishing, wo man z.B. mittels E-Mails auf gefälschte Webseiten gelenkt wird.

Alternativ können Angreifer auch freie WLANs bereitstellen, auf die Nutzung warten und auch die originären URLs von Dienste-Anbietern faktisch umleiten. Hier müsste man auf die SSL Verschlüsselung des Browsers achten.

Social Engineering

Anruf von vermeintlichen Mitarbeitern oder Kollegen .. siehe Wikipedia Artikel

Zugriff beim E-Mail Provider

Unverschlüsselt empfangene sowie gesendete E-Mails liegen beim E-Mail Provider i.d.R. ebenfalls unverschlüsselt im IMAP Postfach. Folglich könnte der Provider auf ihre E-Mails zugreifen. Eine Ausleitung/Kopie an Behörden ist grundsätzlich denkbar.

Des Weiteren besteht auch immer die Möglichkeit von Hacker Angriffen auf ihr E-Mail Konto. Oft sind sensible Daten in den E-Mails gespeichert, z.B. Bestätigungen für Bestellungen und Konteninformationen, die für Betrüger interessant sind.

Darüberhinaus ist auch die Bestechung von Mitarbeitern des E-Mail Providers im Rahmen des Denkbaren ..

Es gibt wiederum Email Provider wie z.B. Posteo, die alle ankommenden E-Mails automatisch mit dem öffentlichen Schlüssel zum Konto verschlüsseln, bevor sie die Daten speichern. Den privaten Schlüssel braucht der Provider nicht. Somit kann der Provider die verschlüsselt gespeicherten E-Mails nicht mehr lesen. Auch eine Weitergabe an Behörden macht wenig Sinn - außer, die Behörden kommen z.B. über eine Hausdurchsuchung/Beschlagnahme an den privaten Schlüssel ran. Mittels Beugehaft könn(t)en Richter auch die Herausgabe eines Kennworts erzwingen. Dies gilt entsprechend auch für Kennwörter von verschlüsselten Festplatten.

Quellen / Links

- https://cloudogu.com/de/blog/crypto-101-grundlagen
- https://lehrerfortbildung-bw.de/u_matnatech/imp/gym/bp2016/fb3/i03_iud/1_hintergrund/2_verlauf/2_assym/

- BSI: E-Mail Verschlüsselung
- BSI: Verschlüsselte Kommunikation

- https://de.m.wikipedia.org/wiki/Alice_und_Bob
- https://cryptocouple.com/

- https://www.heise.de/hintergrund/Einfach-erklaert-E-Mail-Verschluesselung-mit-PGP-4006652.html
- https://riseup.net/de/security/message-security/openpgp/gpg-best-practices
- https://www.privacy-handbuch.de/index.htm

- VPN