Crypto macht Schule

Bedrohungsmodelle

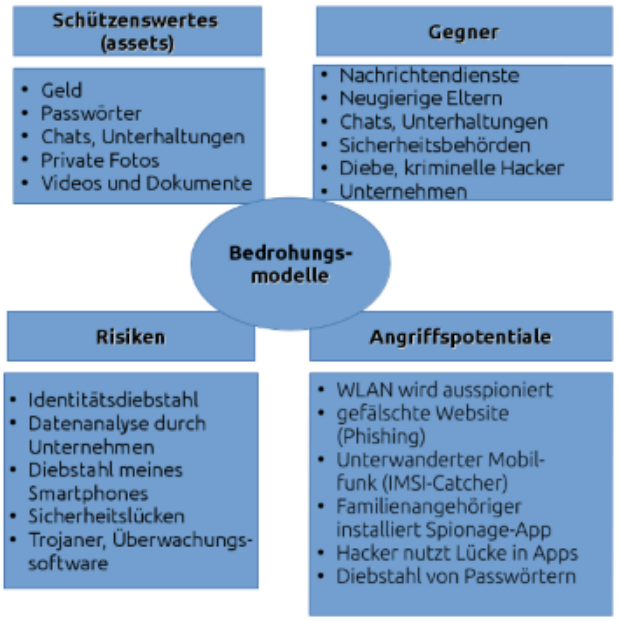

Abbildung 1: Übersicht Bedrohungs-modelle zum Einschätzen von Risiken der IT-Sicherheit.

Allgemeine Tipps

- Never trust anyone
- Datensparsamkeit: möglichst wenige (reale) Informationen Preis geben
- Alternative Suchmaschinen verwenden
- Für jede App, jedes Konto ein eigenes, starkes Passwort verwenden
- unterschiedliche Identitäten: unterschiedliche Nutzernamen, und E-Mail-Adressen

Allgemeine Tipps

Datenspuren beim digitaler Kommunikation und beim Surfen im Web werden durch Tracking- Verfahren zu Profilen verdichtet. Grundlage dafür sind u. a. Cookies, eingebettete JavaSkripte und Fingerabdrücke. Überprüfung mit `https://panopticlick.eff.org/` möglich.

Ende-Zu-Ende-Verschlüsselung

Bei der Ende-zu-Ende-Verschlüsselung ist der Kommunikationskanal aller Teilnehmer direkt vom jedeweiligen Ende verschlüsselt. Zentrales Verfahren ist die Perfect Forward Secrecy. OTR[1] und Double Ratchet[2] sind zwei Protokolle, die Perfect Forward Secrecy umzusetzen versuchen.

[1] Off the Record

[2] Siehe `https://whispersystems.org/blog/advanced-ratcheting/`

Übersicht der Messenger-Apps für Mobilgeräte mit Ende-zu-Ende-Verschlüsselung

	Signal	Wire	SnapChat	Facebook	WhatsApp	Threema
Empfehlung	✓	✓	✗	✗	✗	✗
Chats vollverschlüsselt	✓	✓	✗	✗	✓	✓
Videotelefonie verschlüsselt	✓	✓	✗	✗	✗	✗
Desktop Client	✓	✓	✗	✗	✓	✗
Keine Telefon-Nr. notwendig	✗	✓	✓	✗	✗	✓

Tabelle 1: Kriterien zur Bewertung von Crypto-Messengern (Auswahl)

Anwendungen für Sofortnachrichten (Instant Messenger) bei PCs und Laptops

App	Website	Bemerkung
CryptoCat	https://cryptocat.im/	OMEMO-Verschlüsselung Gruppenchats
Ricochet	http://ricochet.im/	verschleiert Kommunikationsdaten, keine Gruppenchats
Matrix IM	http://matrix.org/	Double Ratched Verschlüsselung

Tabelle 2: Auswahl von Messengern für PCs und Laptops

Transportverschlüsselung

Beim Abruf von Webseiten, E-Mails und auch einiger Apps sollte immer auf SSL/TLS-Verschlüsselung geachtet werden. Viele Seiten verwenden veraltete Verschlüsselung.[3] Höchste Sicherheitsstufe hat derzeit die HSTS-Verschlüsselung.[4] Beim Online-Banking Zertifikat prüfen.

[3] Der aktuellste Standard ist TLS 1.3, der immer noch von sehr wenigen Seiten unterstützt wird.

[4] Webseiten könnten mit `https://www.ssllabs.com/ssltest/` geprüft werden.

Weitere Informationen

Literatur

S. Gutwirth, R. Gellert, and Bellanova. *Appendix: Types of privacy, benefits & harms.* Fraunhofer ISI, 1. auflage edition, 2011.

Tobias Rademacher. Termine für cryptoparties. `http://crpytoparty.in/leipzig`, June 2017a.

Tobias Rademacher. Cryptoparty-forum für fragen, antworten, diskussionen. https://forum.privacy-leipzig.org/, June 2017b.

Tobias Rademacher. Materialien zur cryptoparty. https://privatsphaere-leipzig.org/cryptoparties/crypto-macht-schule-cryptoparty-montessori-06-juni-2017-programme-materialien-links/, June 2017c.

Tobias Rademacher. Präsentationsfolien zur cryptoparty. https://privatsphaere-leipzig.org/cryptoparty/crypto-macht-schule/montessori/2017/juni/, June 2017d.

Roberto Simanowski. *Facebook-Gesellschaft*. Matthes & Seitz, 1. auflage edition, May 2016. ISBN 978-3-95757-057-4.