Helmut Reimer, Christoph Wegener

# Kryptographie und Benutzerfreundlichkeit

„Kryptographie muss benutzerfreundlich sein" ist eine oft gehörte Forderung und auch in Medien jeglicher Couleur wird die zögerliche Verbreitung von „sicheren Anwendungen" nur zu oft und zu gern mit mangelnder Benutzerfreundlichkeit begründet. Völlig unabhängig von der Frage, ob diese Forderung technisch überhaupt realistisch umsetzbar ist, gilt es zu klären, was Benutzerfreundlichkeit überhaupt meint.

Denn bereits der Begriff selbst ist unbestimmt und vor allem stark von der Benutzergruppe und der konkreten Situation abhängig. Dazu einführend ein paar Beispiele:

- Ein professioneller Benutzer einer Anwendung ist über die verfügbaren Sicherheitsfunktionen und das mit der Verarbeitung der Daten einhergehende Risiko informiert. Er wird alle notwendigen Verfahrensschritte bewusst und geduldig ausführen und Sicherheitsrisiken allenfalls nach sorgsamer Abwägung in Kauf nehmen sowie zugleich akzeptieren, dass die Sicherheitsvorgaben letztendlich in einem erhöhten Zeitaufwand resultieren.
- Anders der Gelegenheitsnutzer einer Anwendung: Er wird zusätzliche Sicherheitsfunktionen, die den Ablauf der Anwendung verzögern, ignorieren oder -falls dies nicht ohne weiteres umsetzbar ist- versuchen, diese zu umgehen. Etwaige „Sicherheitsprobleme" -wie bspw. abgelaufene Gültigkeitszeiträume von Zertifikaten- nimmt dieser Benutzertyp (unbewusst) in Kauf und er trägt so -ebenfalls unbewusst- zu einer wachsenden Unsicherheit und Instabilität der IT-Sicherheitsinfrastruktur bei.
- Hinzu kommt, dass Sicherheitsanwendungen üblicherweise nicht zum Arbeitsalltag gehören und keine Routineaufgaben darstellen. Sie müssen stattdessen -wie übrigens ganz praktisch auch alle Behördengänge- quasi jedes Mal neu erlernt werden. Man kann dann davon ausgehen, dass die Anwendung häufig mit der Begründung „zu benutzerunfreundlich" abgebrochen werden wird. Als Alternative kommen dann häufig übrigens wesentlich benutzerunfreundlichere, weil nicht medienbruchfreie, Lösungen ins Spiel, die dem Nutzer aber scheinbar Handlungsautonomie bieten und so gegenüber der digitalen Lösung häufig als benutzerfreundlicher empfunden werden.
- Zudem werden sicherheitskritische Anwendungen oft auch über (mobile) Apps vermittelt, PayPal ist ein populäres Beispiel für die Unterstützung von finanziellen Transfers im Internet. Diese Tools sind auf den ersten Blick benutzerfreundlich und haben eine große Reichweite – bis hin zu globalen Einsatzmöglichkeiten. Der Benutzer dieser Apps bleibt jedoch -insbesondere hinsichtlich des Schutzes seiner Privatsphäre- im Ungewissen. Trotzdem werden solche Apps oft und gern von Benutzern verwendet und das mit ihnen einhergehende Risiko -aufgrund der hohen Benutzerfreundlichkeit- schlichtweg akzeptiert.

Diese Beispiele zeigen bereits, dass die Benutzerfreundlichkeit im Zusammenhang mit der Informationssicherheit vor allem situationsabhängig zu beurteilen ist.

Die Komplexität von IT-Sicherheitsanwendungen wird zudem, insbesondere, wenn sie auf Kryptographie mit den dann unverzichtbaren Infrastrukturen beruhen, gern durch „benutzerfreundlich" vor dem Benutzer verdeckt. Mit anderen Worten: Aufgrund der allgegenwärtigen Forderung, Anwendungen müssten immer maximal benutzerfreundlich gestaltet sein, werden wichtige Details, die zur Bewertung der Sicherheit notwendig sind, vom Nutzer ferngehalten. Oder noch plakativer ausgedrückt: Man traut auch dem (geschulten) Benutzer einfach nicht zu, mit der Komplexität sinnvoll umgehen zu können.

Bei der Umsetzung von „Benutzerfreundlichkeit" im Kontext von sicherheitskritischen Anwendungen und im Rahmen der Beurteilung der Sicherheit von Anwendungen und den zugrundeliegenden Infrastrukturen stellen sich daher grundsätzlich einige wichtige Fragen:

- Was sollte der Benutzer wissen, um einer Kryptoanwendung vertrauen zu können? Neben den Anwendungen selbst geht es dabei ja auch um die Sicherheitsparameter der genutzten Infrastrukturen (insbesondere bei Einsatz von Cloud-basierten Lösungen) und der beteiligten Institutionen (bis hin zu den am Prozess beteiligten natürlichen Personen).
- Was sollen eigentlich die Ziele von benutzerfreundlichen Lösungen sein? Geht es vorrangig um die Entlastung von „lästigen", im Sicherheitskontext aber oft notwendigen „Routineaufgaben" und um die Erzeugung eines Sicherheitsgefühls und ist dabei ein „Verdrängen" von Risiken schlichtweg zu akzeptieren? Oder sollte auch dem nicht-Experten die Möglichkeit gegeben werden, die Sicherheit -zumindest grob- beurteilen und sein Handeln daran ausrichten zu können?
- Wird ein Benutzer durch hohe „Benutzerfreundlichkeit" sogar angreifbar, beispielsweise weil ihm die Beurteilung von Risiken aufgrund mangelnder Informationen nicht mehr möglich ist, und gefährdet er dadurch gegebenenfalls sogar weitere Beteiligte?

„Was ich nicht weiß, macht mich nicht heiß." Diese Alltagsregel darf nicht unter dem Deckmantel der Benutzerfreundlichkeit zum Standard beim Design von Benutzerschnittstellen werden. Vielmehr braucht es aufgeklärte und risikobewusste Benutzer, damit die IT-Sicherheitsinfrastrukturen auch in Zukunft „sicher" bleiben.