2 Gesellschaftlicher Kontext

Dieses Kapitel beschreibt die Bedeutung der Thematik eines sicheren Mobiltelefons für das Leben in einer demokratischen Gesellschaft. Zu diesem Zweck werden sowohl private als auch staatliche Akteure als Beispiel für potentielle Angreifer dargestellt. Darüber hinaus wird die mögliche Modifikation des Nutzerverhaltens eingeordnet und die Thematisierung in der Schule in Abschnitt 2.4 als ein Vorschlag für einen verbessertes Sicherheitsbewusstsein vorgestellt.

2.1 Bedrohung durch private Akteure

Die Bedrohung durch private Akteure gewinnt durch günstiges Equipment und zum Teil fertige Software zum Durchführen von Angriffen vermehrt an Bedeutung. Die Hardware zur Durchführung von Angriffen bei GSM, z. B. Man-in-the-middle, ist für unter 2000 € erhältlich[1] und damit im Rahmen einer privaten Anschaffung. Sofern eine Sicherheitslücke von einem Jeden ausgenutzt werden kann, steigt die Relevanz der Angriffsproblematik und erhöht damit als Seiteneffekt den Druck auf den Personenkreis, welchem die Möglichkeit der Schließung einer solchen Lücke obliegt.

2.2 Bedrohung durch staatliche Organisationen

Die Bedrohung der Privatsphäre einzelner Nutzer kann jedoch nicht nur von privaten, sondern insbesondere auch staatlichen Organisationen ausgehen. Insbesondere beim Einsatz von teurem Equipment oder wenn Informationen benötigt werden, die staatlichen Organisationen exklusiv zur Verfügung stehen, wie z. B. bei der Mobilfunkortung, spielt der Staat eine zentrale Rolle in Bezug auf Sicherheit und Datenschutz. Die Tatsache, dass es sich bei staatlichen Maßnahmen in der Regel um legale Vorgänge handelt, schließt rechtliche Schutzmaßnahmen aus und unterstreicht die Relevanz technischer Methoden zur Abwehr datenschutzkritischer Eingriffe. Selbst wenn die Legalität eines staatlichen Eingriffs nicht

[1] `http://www.heise.de/security/meldung/IMSI-Catcher-fuer-1500-Euro-im-Eigenbau-1048919.html` [30.09.14]

P. Gewald, *Sicherheitsaspekte von Mobiltelefonen,* BestMasters,
DOI 10.1007/978-3-658-12612-4_2, © Springer Fachmedien Wiesbaden 2016

gegeben ist, beispielsweise bei der Übertretung der Befugnisse bei Geheimdiensten, bleibt dem Einzelnen in der Regel kaum die Möglichkeit rechtlicher Gegenmaßnahmen, sondern lediglich der Einsatz technischer Mittel. Dies meint nicht die Unterstützung krimineller Handlungen, sondern viel mehr den Schutz des Einzelnen vor einem Generalverdacht oder der Willkür von Behörden, dessen Handlungen im Vergleich zu ihren Befugnissen im Fall der Geheimdienste als unverhältnismäßig zu bezeichnen sind. Dabei kann zwischen zwei Arten von Behörden unterschieden werden:

Polizeiliche Ermittlungsbehörden

Die Anzahl der durchgeführten Überwachungsmaßnahmen ist im Laufe der Jahre gestiegen[2]. Dabei handelt es sich sowohl um Ortungs- als auch um Abhörmaßnahmen. Dies zeigt sich einerseits in Abschnitt 4.1.6 über die Thematik der Silent-SMS, aber auch beim Einsatz von IMSI-Catchern, wie Abschnitt 4.1.7 zeigt. Besteht „Gefahr im Verzug“ können Behörden für diese Ermittlungsschritte auf eine richterliche Anordnung im Vorfeld verzichten.

Geheimdienste

Die NSA-Affäre[3] hat das Ausmaß der geheimdienstlichen Tätigkeiten gezeigt und dient als Beispiel für die Notwendigkeit technischer Gegenmaßnahmen. Insbesondere die Kooperation mit großen Softwareunternehmen bzw. Mobilfunkprovidern[4] unterstreicht die Notwendigkeit technischer Schutzmaßnahmen im Mobilfunkbereich. Jeder Nutzer hat ein Recht auf informationelle Selbstbestimmung, welches m. E. nicht nur politisch, sondern vor allem technisch verteidigt werden muss.

2.3 Verhaltensänderung

Sobald ein gesellschaftliches Bewusstsein über die Überwachung von mobilen Kommunikationswegen entsteht, wirkt sich dies m. E. auf die Verhaltensweise der Betroffenen aus. Ein Teil der Nutzer versucht nach Möglichkeit seine Kommunikation durch diverse Verschlüsselungsmethoden zu verschleiern, während andere Nutzer bestimmte Dienste oder Kommunikationswege gänzlich meiden. Dies kann auch das Unterlassen bestimmter Schlüsselwörter in Texten umfassen oder die Beschränkung auf einige unkritische Themen,

[2] http://www.heise.de/newsticker/meldung/Bessere-Handy-Ortung-fuer-die-deutsche-Polizei-2289542.html [06.09.14]
[3] http://www.heise.de/extras/timeline/[01.11.14]
[4] http://www.heise.de/newsticker/meldung/Bericht-NSA-sammelt-Telefondaten-von-Millionen-US-Buergern-1883586.html [06.09.14]

was m. E. einer Simulation staatskonformer Kommunikation gleicht. Eine dritte Nutzergruppe hat „nichts zu verbergen“ und ist sich potentieller Konsequenzen von Überwachungsmaßnahmen entweder nicht bewusst oder misst diesen eine nur geringe Bedeutung zu. Letzte Nutzergruppe fördert mit ihrem gleichgültigen Verhalten implizit ein Fortführen und Ausbauen von Überwachungsmaßnahmen. Auch ein Schüler kann beispielsweise im Rahmen der Recherche für den Politikunterricht auf politisch extremen Webseiten zum Zweck der Recherche automatisch ins Visier der Ermittlern geraten. Wer nichts zu verbergen hat, benötigt weder geheimen Passwörter, noch Türschlösser oder Pseudonyme. Um die Konsequenzen von Überwachungsmaßnahmen abschätzen zu können, wird zunächst das Wissen über mögliche Angriffe benötigt. Zu diesem Zweck ist eine Thematisierung in der Schule ein Ansatz, um möglichst früh ein Bewusstsein für diese Problematik zu schaffen.

2.4 Thematisierung in der Schule

Insbesondere Schüler sind in sozialen Netzwerken aktiv und nutzen Mobiltelefone meist in vollem Umfang ihrer Funktionen. Damit wickeln sie einen Großteil der private Kommunikation über die Schnittstellen und Protokolle eines Mobiltelefons ab. Eine Sensibilisierung für eine Angriffsproblematik sollte m. E. aufgrund der intensiven Nutzung und eines frühen „Lernalters“ das Interesse der Zielgruppe Schüler wecken. Das in Kapitel 3 näher formulierte Ziel zur Aufklärung beizutragen und ein gesellschaftliches Bewusstsein zu schaffen soll auch bzw. insbesondere über den Schulweg umgesetzt werden. Zu diesem Zweck ist es wichtig, die vorliegenden Angriffe nicht nur zu nennen, sondern deren Ablauf und Funktion zu erläutern, um deren Erkennung und Prävention zu verdeutlichen. Eine Visualisierung vorliegender Angriffe trägt nicht nur zum allgemeinen Verständnis bei, sondern soll vor allem Lehrkräfte und Schüler motivieren sich mit dieser Thematik zu beschäftigen.

http://www.springer.com/978-3-658-12611-7

Sicherheitsaspekte von Mobiltelefonen
Erkennung und Visualisierung von Angriffsvektoren
Gewald, P.
2016, XIII, 98 S. 53 Abb., Softcover
ISBN: 978-3-658-12611-7