Presseinformation

Warum der Abhörskandal wirklich jeden betrifft

München, 23. September 2013. Die amerikanische Bürgerrechts-Organisation „American Civil Liberties Union“ (ACLU) klagt, unterstützt selbst von konservativen US-Juristen, vor einem US-Gericht gegen die Abhörpraktiken der National Security Agency (NSA). Eine wichtige Aussage in der Klageschrift ist, dass die von der NSA betriebene Speicherung von Metadaten zu Telefonanrufen und SMS keineswegs harmlos sei, sondern erlaube, quasi automatisch ein detailliertes Profil aller Bürgerinnen und Bürger zu erstellen.

Zu Beginn des Skandals um die NSA wurde zur Beruhigung von der US-Regierung verlautbart, dass ihre riesige Datenbank von inländischen Anrufen „nur" Metadaten enthalte. Niemand würde die Telefonate mithören oder die SMS lesen. Die UCLA-Klage legt hingegen offen, dass die "Metadaten" viele private Informationen enthielten.

Prof. Edward Felten, der an der renommierten Universität Princeton Informatik lehrt, belegte im Rahmen der Prozessvorbereitung, warum "Metadaten" quasi alles über die Bürgerinnen und Bürger verraten. (1) Metadaten seien sehr einfach automatisch zu analysieren im Gegensatz zu den komplizierten Einzelheiten eines Anrufs mit seinen Variationen in Sprache, Stimme und Gesprächsstil. Moderne Analyse-Software ermöglicht, aus Metadaten Beziehungen, persönliche Daten, Gewohnheiten und Verhaltensweisen herauszulesen. Es gibt bereits Programme, die für Strafverfolgung und Geheimdienste solche Daten analysieren, etwa IBM Analyst‘s Notebook. IBM bietet sogar Kurse an, die lehren, wie man Anrufdaten mit IBM Analyst‘s Notebook auswertet. (2) Im Gegensatz zum tatsächlichen Inhalt der Anrufe, SMS und E-Mails lassen sich die Metadaten zu diesen Anrufen kaum schützen. Dafür sind diese Metadaten oft aufschlussreicher als der eigentliche Inhalt.

Der deutsche Sicherheitsexperte Hubert Jäger, Geschäftsführer des IT-Sicherheitsdienstleisters Uniscon (3), bestätigt das: „Zu wissen, wer wen wann und wie oft anruft oder anschreibt, enthüllt privateste Informationen. Je mehr Daten man sammelt, desto aufschlussreicher wird das Ergebnis.“ Zum Beispiel weist ein Anruf von einem Buchmacher wahrscheinlich auf eine Wette hin. Die Analyse der Metadaten im

Presseinformation

Laufe der Zeit könnte zeigen, dass die angerufene Person ein Problem mit Glücksspielen hat, insbesondere wenn die Anruflisten auch eine Reihe von Anrufen von Kreditfirmen, Inkassofirmen und Pfandleihern aufweist.

Ein hypothetisches Beispiel verdeutlich die Gefahren, denen Bürger sich gegenüber sehen, wenn die Metadaten ihrer Kommunikation gesammelt und ausgewertet werden. Ein Deutscher ruft regelmäßig die Handynummer eines in Deutschland geduldeten Roma-Flüchtlings an, dessen Abschiebung ins Kosovo ansteht. Nach kurzer Zeit kommen häufige Telefonate mit einem Anwalt hinzu, der auf Ausländerrecht spezialisiert ist. Der Mann telefoniert in den nächsten Tagen darauf mit einer Menschenrechtsorganisation, einer Kirchengemeinde und einem Stadtverordneten, von dem bekannt ist, dass er sich mit Asylrecht sehr gut auskennt und dann mit einer Zimmervermittlung in Berlin. Die Metadaten dieser Anrufkette, mit der richtigen Software ausgewertet, erzählen eine so deutliche Geschichte, dass kein Abhören von Telefonaten mehr nötig erscheint. Anhand einer mehrere Jahre umfassenden Datenbank mit „Metadaten“ lassen sich ganze Lebensläufe ohne viel Mühe eruieren.

Aber auch politische Gegner lassen sich so ganz einfach ausspionieren.
Durch das Sammeln von Daten einer Bürgerrechtsorganisation wie der ACLU könnte die Regierung die Strategie bei der Klage gegen verfassungswidrige Geheimdienst-Machenschaften ermitteln, indem sie Verbindungen zu bestimmten Experten, Protestbewegungen oder Einzelpersonen offenlegt.

„Unternehmen sind sich der Tatsache des Ausspionierens durch die Metadaten noch wesentlich stärker bewusst“, sagt Jäger. Deshalb würden sie sich vermehrt nach Möglichkeiten umsehen, die Metadaten zu schützen. Jäger hat Einblick in die Bedürfnislage der Unternehmen, denn Uniscon betreibt den Online-Kommunikationsdienst IDGARD für Unternehmen, der auch die Metadaten schützt.

In vielen Medien aber wird dieses Thema derzeit noch wenig beachtet, vielleicht auch deshalb, weil die Werbewirtschaft mit ganz ähnlichen Methoden Profile von Internetnutzern anlegt, um ihre Werbung daraufhin zu optimieren.

Presseinformation

(1) http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf
(2) http://www-03.ibm.com/software/products/de/de/analysts-notebook/
(3) http://www.uniscon.de/firmenprofil/

Über Uniscon GmbH –

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service ID|GARD für Unternehmen basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

Pressekontakt
Uniscon GmbH/Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 110
presse@uniscon.de
www.uniscon.de

PR-Agentur Xpand21 GmbH
Doris Loster
Romanstr. 10
80639 München
089 / 71 68 07 35
uniscon@xpand21.com
www.pr-agentur-xpand21.de