Das EU-geförderte Projekt TABULA RASA hat konkrete Gegenmaßnahmen entwickelt, damit europäische Unternehmen derartige Angriffe abwehren können.

Seit drei Jahren erforscht und bewertet das TABULA RASA-Konsortium, das aus zwölf Partnern aus sieben Ländern besteht, Schwachstellen in biometrischen Sicherheitssystemen. Dazu hat es eine umfangreiche Liste mit möglichen sogenannten Spoofing-Attacken erstellt und fünf konkrete Gegenmaßnahmen an Unternehmen übermittelt. Beim Spoofing werden durch die Verwendung alltäglicher Mittel wie Make-up, Fotos und Sprachaufzeichnungen biometrische Systeme untergraben oder direkt angegriffen.

Die EU investierte 4,4 Millionen Euro in das Projekt, das TABULA RASA-Konsortium weitere 1,6 Millionen Euro, um die umfangreichen Forschungen und Tests durchführen zu können.

Dr. Sébastien Marcel, Koordinator des Projekts TABULA RASA, erklärte:

„Ohne die Investition der Europäischen Union wäre es unmöglich gewesen, dieses Forschungsprojekt so groß anzulegen und mit so vielen Partnern aus der EU zusammenzuarbeiten. Die Vorteile der verbesserten Software sind nicht nur sicherere Geräte und Informationen, sondern auch kürzere Anmeldezeiten für IT-Geräte sowie schnellere und präzisere Grenz- und Reisepasskontrollen. Wir glauben, dass viele verschiedene Unternehmen Interesse an unseren Forschungsergebnissen zeigen werden. Insbesondere Technologieunternehmen, Postämter, Banken, Hersteller von Mobilgeräten oder Anbieter von Onlinediensten können davon profitieren."

Weitere Informationen: *http://www.tabularasa-euproject.org*

## Partnerschaft: Bundesverband IT-Sicherheit e.V. (TeleTrusT) und Bund Deutscher Kriminalbeamter e.V. (BDK)

Der Bundesverband IT-Sicherheit e.V (TeleTrusT) und der Bund Deutscher Kriminalbeamter e.V. (BDK) haben am 11.10.2013 die Partnerschaft beider Verbände vereinbart, um Expertise insbesondere auf den Gebieten IT-Sicherheit und IT-Forensik auszutauschen.

Ermittlungen bei IT-Kriminalität setzen besondere Kenntnisse, Befähigungen und Werkzeuge in der kriminalpolizeilichen Arbeit voraus. Die technische Beweissicherung bedingt vertieftes Verständnis von IT-gestützten Bedrohungsszenarien. TeleTrusT und BDK können wechselseitig Nutzen aus dem Erfahrungsaustausch ziehen, um im Ergebnis die Abwehrtechnologie zu optimieren.

Der BDK vertritt die beruflichen und sozialen Belange aller Angehörigen der Kriminalpolizei. Der Verband zählt die überwiegende Mehrheit aller Kriminalbeamtinnen und -beamten zu seinen Mitgliedern. Durch das Wirken im politischen Raum, in der Öffentlichkeit und in der polizeilichen Organisation leistet er seinen Beitrag zur Entwicklung einer praxisnahen, realistischen und fortschrittlichen Kriminalitätskontrolle.

## App-Security-Check für iOS, Android & Co.

Jede App, die ein Mitarbeiter auf einem mobilen Gerät installiert, stellt für sein Unternehmen ein Sicherheitsrisiko dar. Fraunhofer SIT hat deshalb „Appicaptor" entwickelt, ein Testwerkzeug, das prüft, ob Apps die Sicherheitsanforderungen von Unternehmen erfüllen. Das Testwerkzeug wird gegenwärtig zur Analyse von iOS und Android Apps verwendet, ist jedoch auf andere Plattformen erweiterbar.

Wie wichtig eine solche Prüfung ist, zeigen Probeläufe mit Pilotkunden für iPhone-Apps: Von den 400 beliebtesten Business-Apps, die mit Appicaptor geprüft wurden, erfüllten über 300 nicht die Sicherheitsanforderungen des Unternehmens.

Anwender-Unternehmen oder App-Entwickler können unter *www.sit.fraunhofer.de/appicaptor* einen kostenlosen Beispielbericht anfordern.

## Fraunhofer SIT: Forschungsroadmap zum Schutz von Privatsphäre und Vertraulichkeit

Die Enthüllungen von Edward Snowden haben deutlich gezeigt, wie umfangreich und weitreichend Geheimdienste das Internet überwachen können. Ein effektiver Schutz von Bürgern, Wirtschaft und Verwaltung vor Massenüberwachung erfordert eine Kombination von rechtlichen und technischen Maßnahmen. Viele technische Fragen sind allerdings noch nicht zufriedenstellend beantwortet. Das Fraunhofer-Institut für Sichere Informationstechnologie hat die zwölf wichtigsten Forschungsfragen zum Schutz von Privatsphäre und Vertraulichkeit im Internet in einem Trend- und Strategiebericht zusammengestellt und erläutert. Noch fehlt es etwa an Verfahren, mit denen Internetnutzer kryptografische Schlüssel auf einfache Art und Weise austauschen können. Auch gibt es noch keine Möglichkeit, die Sicherheitseigenschaften von Cloud-Diensten nachzuprüfen bzw. nachzuweisen. Ein fundamentales Problem ist die Vermeidung von Hintertüren und Schwachstellen in Soft- und Hardware. Das Dokument steht im Internet unter *http://www.sit.fraunhofer.de/forschungsfragen* zum kostenlosen Download bereit.

„Die massenhaften Ausspähung im Internet war in der Fachwelt seit langem als eine Möglichkeit bekannt, aber erst die Enthüllungen von Edward Snowden haben uns vor Augen geführt, dass es sich hier um eine sehr reale, uns alle betreffende Gefahr handelt", sagt Michael Waidner, Leiter des Fraunhofer SIT. „Neben der Politik sind auch die Forschung und Industrie gefragt, das IT-Sicherheits- und Datenschutzniveau im Internet zu erhöhen."

Der Trend- und Strategiebericht entstand mit Unterstützung des im Rahmen des LOEWE-Programms vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) geförderten Forschungszentrums CASED (*http://www.cased.de*) und des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Cybersecurity-Kompetenzzentrums EC SPRIDE (*http://www.ecspride.de*).

## Hohes Risiko bei Verlust von mobilen Geräten

11 Prozent der mobilen Geräte (Laptop, Smartphone oder Tablet) gingen in Deutschland zwischen Juni 2012 und 2013 irreparabel defekt, wurden verloren oder gestohlen. Das ist das Ergebnis einer weltweiten Umfrage unter Verbrauchern, die Kaspersky Lab zusammen mit B2B International durchgeführt hat. Die befragten Nutzer beklagten dabei zu sieben Prozent einen irreparablen Schaden, zu zwei Prozent ein verlorenen gegangenes Gerät und zu zwei Prozent einen Diebstahl.

Der materielle Wert der Geräte ist oft zweitrangig gegenüber dem Schaden, den der Missbrauch der darauf gespeicherten Da-