Verschlüsselung für alle

(Mynewsdesk) Nach den Enthüllungen zu Massenüberwachungen durch Geheimdienste suchen Wirtschaft und Gesellschaft nach praktikablen Verschlüsselungslösungen, die Unternehmen und Bürger schützen. Bisherige Technik scheiterte im Alltag an mangelnder Benutzerfreundlichkeit oder hohen Kosten. Mit der Volksverschlüsselung startet Fraunhofer jetzt eine offene Initiative, um Ende-zu-Ende-Verschlüsselung in der breiten Bevölkerung zu etablieren. Auf der CeBIT stellen die Forscher einen Prototypen der laientauglichen Software sowie ihr Konzept zur Infrastruktur dahinter vor (Halle 9, Stand E40).

Verschlüsselung ist das wirksamste Mittel gegen die anlasslose massenhafte Ausspähung von Bürgern, Unternehmen und Behörden. Programme, etwa für die Absicherung von E-Mail-Kommunikation, gibt es zwar viele, dennoch werden sie kaum genutzt, weil sie für Normalbürger meist zu aufwendig sind. Aus diesem Grund fordert die Bundesregierung in ihrer Digitalen Agenda die Möglichkeit einer durchgängigen und laientauglichen Verschlüsselung. Ein Forschungsteam vom Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt entwickelte ein Konzept für die Volksverschlüsselung, das Benutzerfreundlichkeit von Anfang an berücksichtigt. Die Software platziert die kryptografischen Schlüssel auf dem eigenen Computer automatisch an den richtigen Stellen. Zusätzlich arbeiten die Wissenschaftler an einer Infrastruktur, die allen Nutzern zur Verfügung steht und auch bestehende Verschlüsselungsangebote unterstützt.

»Mit der Initiative und den konkreten Entwicklungen unterstützt Fraunhofer die Bundesregierung in ihren Bemühungen, die Sicherheit von Bürgern und Unternehmen zu erhöhen«, sagt Prof. Michael Waidner, Institutsleiter des Fraunhofer SIT. Dementsprechend soll die Volksverschlüsselungssoftware als Open-Source zur Verfügung gestellt werden.
Schlüsselverteilung für LaienDie Software ist das Kernstück der Lösung. Sie nimmt dem Nutzer die bislang schwierigen Verteilungsvorgänge ab: Sie erkennt, welche Anwendungen ? zum Beispiel verschiedene Mailprogramme ? auf dem Computer, dem Smartphone oder Tablet Kryptografie nutzen können und stellt ihnen die entsprechenden Schlüssel automatisch zur Verfügung. Außerdem erzeugt sie auch kryptografische Schlüssel, mit denen sich etwa E-Mails oder Dateien verschlüsseln lassen. Damit der Absender einer E-Mail die Nachricht für den Empfänger verschlüsseln kann, braucht er dessen öffentlichen Schlüssel. Bei der Volksverschlüsselung stellt eine zentrale Infrastruktur diese Schlüssel zur Verfügung. »Sie funktioniert wie ein Telefonbuch«, sagt Projektleiter Michael Herfert. »Hier kann jeder öffentliche Schlüssel nachschlagen und herunterladen. Die zentrale Infrastruktur sorgt außerdem dafür, dass die Schlüssel auch wirklich zu der fraglichen Person gehören und verhindert, dass jemand eine Identität vortäuschen kann.« Auf der CeBIT zeigen die Fraunhofer-Forscher zunächst, wie man sich mit Hilfe der eID-Funktionalität des neuen Personalausweises anmelden kann. Später sollen aber auch andere Verfahren möglich sein. Damit wirklich die breite Bevölkerung die Infrastruktur der Volksverschlüsselung nutzen kann, muss sie im Idealfall mit vielen Millionen Schlüsseln umgehen können. Deshalb sollte sie gleichermaßen leistungsfähig wie sicher sein. Geplant ist derzeit, sie am Fraunhofer-Institutszentrum in Birlinghoven auf einem Hochsicherheitsserver zu betreiben. Mittelfristig sollen sich jedoch auch weitere, vertrauenswürdige Partner beteiligen können. Die Ergebnisse der Volksverschlüsselung ? insbesondere die Software - kommt auch Unternehmen zu Gute. Vor allem kleine und mittlere Unternehmen können die im Projekt entwickelten Lösungen nutzen, um Verschlüsselung leichter einzusetzen und Firmengeheimnisse so besser zu schützen.

Einen Prototyp der Software stellen die Forscher vom 16. bis 20. März auf der CeBIT in Hannover in Halle 9 am Stand E 40 vor. Dabei handelt es sich um eine Software für Windows-Desktop-Rechner. Weitere Versionen für andere Betriebssysteme und Mobilgeräte sind geplant. Außerdem arbeitet das Forschungsteam auch an diversen Erweiterungen, unter anderem an einer Ergänzung, die eine Ad-hoc-Verschlüsselung ermöglicht.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/rv98j2

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/verschluesselung-fuer-alle-22807

=== Volksverschlüsselung ermöglicht sichere Ende-zu-Ende-Verschlüsselung für alle. (Bild) ===

Shortlink:
http://shortpr.com/261psw

Permanentlink:
http://www.themenportal.de/bilder/volksverschluesselung-ermoeglicht-sichere-ende-zu-ende-verschluesselung-fuer-alle

Pressekontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

presse@sit.fraunhofer.de

Firmenkontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

sit.fraunhofer.de

presse@sit.fraunhofer.de

Die Informationstechnologie hat bereits weite Teile unseres Alltags durchdrungen: Ob Auto, Telefon oder Heizung ohne IT-Einsatz sind die meisten Geräte und Anlagen heute nicht mehr denkbar. Insbesondere Unternehmen nutzen ---IT-Systeme zur effektiven Gestaltung ihrer Arbeitsprozesse. Das Fraunhofer-Institut für Sichere Informationstechnologie beschäftigt sich mit dem Schutz dieser Systeme vor Ausfällen, Angriffen und Manipu-lationen.

Das Fraunhofer-Institut SIT ist Teil des größten Cybersicherheitsforschungszentrums Deutschlands in Darmstadt und zählt auch weltweit auf vielen Gebieten zu den führenden Forschungseinrichtungen zur Cybersicherheit weltweit.

Anlage: Bild