Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

PRESSEINFORMATION
16. Oktober 2012

Von bösartigen Apps, verräterischen Stromzählern und sicherer Software-Entwicklung

Alle Bereiche des täglichen Lebens werden zunehmend vernetzt. Angreifer finden in Computersystemen immer häufiger Sicherheitslücken und können so Bürger, Unternehmen und Staaten bedrohen. Seit 2011 fördert das Bundesministerium für Bildung und Forschung daher drei nationale Kompetenzzentren für IT-Sicherheit. Sie sind angesiedelt an der Technischen Universität Darmstadt, der Universität des Saarlandes in Saarbrücken und am Karlsruher Institut für Technologie und erforschen diverse Fragen zur IT-Sicherheit. Erste Ergebnisse präsentieren sie vom 16. bis 18. Oktober auf der IT-Security-Messe „it-sa“ in Nürnberg.

Private E-Mails und geschäftliche Unterlagen sind nicht mehr auf dem eigenen Rechner abgespeichert, sondern bei einem Anbieter im World Wide Web. Die aktuellen Verbrauchsdaten des intelligenten Stromzählers finden sich dort ebenfalls, damit man sie bequem mit dem internetfähigen Telefon abrufen kann und zum Beispiel die Waschmaschine zum richtigen Zeitpunkt preisgünstig laufen lässt. Diese fortschreitende Vernetzung weckt nicht nur die Begierde von Datendieben und digitalen Vandalen, sondern wirft auch Fragen auf, die neben der Technologie auch die Gesetzgebung und die Gesellschaft betreffen. Mit diesen setzen sich die drei Kompetenzzentren für IT-Sicherheit auseinander, die das Bundesministerium für Bildung und Forschung seit 2011 mit insgesamt rund 17 Millionen Euro über vier Jahre hinweg fördert. Erste Ergebnisse und Ansätze sind nun auf der IT-Security-Messe in Nürnberg zu sehen.

Gegenspionage auf dem Smartphone
Halle 12, Stand 666

Das „Center for IT-Security, Privacy and Accountability“ (CISPA) an der Universität des Saarlandes präsentiert einen Ansatz, der bösartige Mini-Programme auf Smartphones entlarvt. Die dazu entwickelte und ebenfalls gezeigte App namens „Appguard“ analysiert, auf welche Daten und Dienste die installierten Miniprogramme zugreifen und zeigt dies dem Anwender an. Dieser kann bei verdächtigem Verhalten der jeweiligen App deren Rechte und Zugriffe einschränken.

Wenn der intelligente Stromzähler plaudert
Halle 12, Stand 668

Kann der intelligente Stromzähler missbraucht werden, um die Privatsphäre von Bewohnern auszuspähen? Dieser Frage geht das Kompetenzzentrum für

Redaktion
Oliver Küch | Fraunhofer-Institut für Sichere Informationstechnologie | Telefon +49 6151 869-213
Rheinstraße 75 | 64295 Darmstadt | www.sit.fraunhofer.de | presse@sit.fraunhofer.de

PRESSEINFORMATION
16. Oktober 2012

Angewandte Sicherheitstechnologie (KASTEL) am Karlsruher Institut für Technologie nach. Anhand einer prototypischen Wohnung, deren Haushaltgeräte und Energieversorgung komplett über das Internet gesteuert werden, identifizieren sie mögliche Gefahren und stellen Gegenmaßnahmen vor.

Werkzeug für sichere Software-Entwicklung
Halle 12, Stand 213

Das European Center for Security and Privacy by Design (ECSPRIDE), an dem sich neben der Technischen Universität Darmstadt auch das Fraunhofer-Institut für Sichere Informationstechnologie beteiligt, setzt auf Fehlervermeidung statt auf das Suchen von Programmierfehlern. Das am Fraunhofer SIT entwickelte „Operational Threat Analysis Tool“ (OTA-Tool) unterstützt Entwickler ohne großes Sicherheits-Know-how bereits in der Design-Phase. Das Werkzeug gibt Handlungsempfehlungen für typische Problemfelder der Software-Entwicklung. Zusätzlich lassen sich mit dem OTA-Tool auch sicherheitsrelevante Aktivitäten dokumentieren.

Weitere Informationen:

Center for IT-Security, Privacy and Accountability
(CISPA)
www.cispa-security.de

Redaktion
Oliver Küch | Fraunhofer-Institut für Sichere Informationstechnologie | Telefon +49 6151 869-213
Rheinstraße 75 | 64295 Darmstadt | www.sit.fraunhofer.de | presse@sit.fraunhofer.de