Sichere Netzknoten für das Internet der Dinge

Sichere Netzknoten für das Internet der Dinge
Fraunhofer SIT zeigt auf der CeBIT 2014 erstmals eine Lösung zur Schaffung vertrauenswürdiger IT-Netze, die auch Schutz vor den jüngst von britischen Forschern entwickelten Router-Viren bietet. Das "Trusted Core Network" (TCN) prüft den Zustand von Routern oder anderen Netzwerkkomponenten, erkennt Manipulationen und isoliert manipulierte Geräte so, dass diese keinen Schaden mehr anrichten können. Die Entwicklung des Fraunhofer SIT wurde für Industrie-Umgebungen entwickelt, kann aber generell auf Netzkomponenten eingesetzt werden. Fraunhofer SIT zeigt das "Trusted Core Network" in Hannover in Halle 9 am Stand E40. Weitere Informationen im Internet unter www.sit.fraunhofer.de/tcn .
Das "Trusted Core Network" wurde für industrielle Umgebungen entwickelt, um Maschinen und Anlagen vor IT-basierten Angriffen zu schützen. Die Wirkweise des TCN schützt Netzkomponenten aber auch vor der jüngst von der Universität Liverpool entwickelten und im Labor demonstrierten Schadsoftware "Chamäleon", die Einstellungen eines Routers manipulieren, eine eigene Firmware installieren und sich selbstständig verbreiten kann. In aktuellen Netzen lässt sich ein Angriff von solchen WLAN-Viren nicht ohne weiteres feststellen und die Schadsoftware könnte sich über drahtlose Netze verbreiten. Im "Trusted Core Network" können Netzknoten sich gegenseitig identifizieren und prüfen, ob Änderungen an Software und Einstellungen vorgenommen wurden. Dadurch lassen sich infizierte Netzknoten ausfindig machen und von der Kommunikation ausschließen.
Die von Fraunhofer SIT entwickelte Lösung verwendet das standardisierte Trusted Platform Modul TPM als Vertrauensanker, um Gerätezustand und -identität verlässlich prüfen zu können. Auf jedem Gerät befindet sich ein TPM, auf dem Informationen zur erlaubten Software und anderen relevanten Teilen der Konfiguration gespeichert sind. Router können mit diesen Informationen alle Geräte in der Nachbarschaft prüfen. Weicht der Ist-Zustand vom Soll-Zustand ab, erkennt das System die Veränderung und schlägt Alarm. So lassen sich mögliche Angriffe schnell erkennen und besser abwehren. Werden vom Hersteller Referenzwerte für die Firmware zur Verfügung gestellt, können auch in offenen Netzen (zum Beispiel zwischen unterschiedlichen Wi-Fi-Netzen) Angriffe erkannt und die Verbreitung der Schadsoftware verhindert werden.
Die von Fraunhofer SIT entwickelten Prototypen verwenden diese Technologie für sichere mobile Ad-Hoc Netze und als "Trusted Core Network" für Industrienetze. Über Protokolle, wie zum Beispiel das standardisierte Trusted Network Connect, können auch Smartphones und andere Geräte in das Sicherheitsmonitoring einbezogen werden. Das "Trusted Core Network" wird auf der CeBIT 2014 als Teil eines Industrie 4.0-Demonstrators gezeigt.

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Rheinstrasse 75
64295 Darmstadt
Deutschland
Telefon: +49 6151 869-292
Telefax: +49 6151 869-224
URL: www.sit.fraunhofer.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=559134" width="1" height="1">

Pressekontakt

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

64295 Darmstadt

sit.fraunhofer.de

Firmenkontakt

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

64295 Darmstadt

sit.fraunhofer.de

Weitere Informationen finden sich auf unserer Homepage