Starthilfe

Wege zum selbstheilenden Internet of Things

Die beim Adressverwalter Réseau IP Européens zusammenkommenden Netzwerk-Administratoren blicken mit Sorge auf die vielen Dinge des Internet, die bald ihre Netze bevölkern werden. Die Organisation trägt daher Konzepte für ein sicheres Internet of Things zusammen – Selbstheilungsfunktionen inklusive.

Von Monika Ermert

Das Internet der Dinge ist immer noch Teil des Internet. Und damit es funktioniert, entwickelt die Selbstverwaltungsorganisation RIPE Regeln für die Vergabe von IP-Adressen an Netzbetreiber, die IoT-Geräte und -Dienste anbieten wollen. Beispielsweise wollen Mobilfunkper Funk auslesbare Zähler und passende Dienste anbieten und entwickeln dafür LTE-Erweiterungen wie Narrow-Band IoT.

Die Fachleute diskutieren aber auch über Peering und die Sicherheit beim Routing im Zusammenhang mit IoT. Damit das zielgerichtet abläuft, hat das RIPE Ende Oktober bei seinem 75. Treffen in Dubai eine IoT-Arbeitsgruppe gegründet. Die Gruppe soll die rund 17.000 RIPE-Mitglieder über Entwicklungen informieren und IoT-Neulingen unter die Arme greifen.

Das S in IoT

Zum Thema Sicherheit hielt Ivana Tomic, eine Wissenschaftlerin des Londoner Imperial College, einen Vortrag zu ihrer Forschung über Sensoren mit Selbstheilung (siehe ct.de/yncf). Tomic simulierte ein Netz aus 100 Nodes und untersuchte den Datenfluss in Abhängigkeit von netzinternen Attacken und Selbstheilungsfunktionen. Die Nodes ermittelten den Normalzustand anhand von Parametern wie Verkehrsaufkommen oder Paketlaufzeiten zu verschiedenen Zielen im Netz. Anschließend wurden Angriffe und kompromittierte Nodes simuliert. Als Beleg für erfolgreiche Angriffe gilt beispielsweise sprunghaft erhöhter IP-Verkehr. Solche Auffälligkeiten meldeten die Nachbar-Nodes der Basis. Brave Knoten wählten dann einen Pfad um den verdächtigen Nachbarn herum.

Deutlich größer ist das 2010 gestartete Atlas-Netz des RIPE, das aus weltweit verteilten

Kleinstroutern von TP-Link besteht (TL-MR 3020). Die rund 10.000 Router-Sensoren erfassen eine Vielzahl von Daten und bewerten, wie gut der IP-Verkehr durch das Internet läuft. So detektieren sie Störungen und deren Quelle.

Die Entwickler hatten von Anfang an ein offenes System geplant, das RIPE-Mitglieder und Forscher für Messungen nutzen können, das aber zugleich gegen Missbrauch gewappnet ist.

Deshalb haben die Sensoren einen Satz individueller Schlüssel und sind beim RIPE registriert. Firmware-Updates spielen sie nur ein, wenn sie von einer authentifizierten Quelle stammen und wenn sich die signierten Dateien validieren lassen. Außerdem detektieren schon die Atlas-Nodes Ausreißer anhand des Kommunikationsverhaltens und melden das. Beim RIPE NCC arbeitet man gerade daran, alle Sicherheitsfeatures als Beitrag zur Security-Debatte zu dokumentieren.

IoT und Blockchain

Die IoT-Gruppe soll auch die Positionen des RIPE in der IoT-Diskussion vertreten. Dabei scheint nun Streit mit anderen Arbeitsgruppen vorprogrammiert: Manche Fachleute sind mit den aktuellen Funktionen des Adressierungs- und Namenssystems unzufrieden (Internet-IP-Adressen und Domain Name System, DNS) und wünschen sich eine Semantik, die gut nachvollziehbar und sicher ist.

Bei der ITU prüft man, ob sich die Digital Object Architecture (DOA) als Management-Tool für IoT eignet. DOA gründet auf einer eigenen Rootzone mit Identifiern, ist jedoch eine Closed-Shop-Veranstaltung und nicht dezentralisiert. Einen ersten Test über DNS zeigte jüngst ausgerechnet die Internet Corporation for Assigned Names and Numbers, die das DNS verwaltet.

Der Ethereum Name Service setzt hingegen auf Blockchain und verspricht sich davon mehr Sicherheit und Transparenz; Ethereum hat schon 180.000 „.eth“-Namen auktioniert. Dabei bilden IP-Adressen und DNS den Basis-Layer. Und die ITU Study Group 20 will einen IoT-Adressplan auf IPv6-Basis erstellen, was man beim RIPE mit Argwohn verfolgt.

(dz@ct.de) **ct**

IoT-Forschungs-Dokumente: ct.de/yncf

Anzeige