Antrag A-01

Jusos Sachsen

Contains Internet

Der Landesparteitag möge beschließen und an den Bundesparteitag der SPD weiterleiten:

Wir fordern eine verpflichtende Kennzeichnung aller netzwerkfähigen Geräte, die auf dem europäischen Markt verkauft werden, mit einem EU-weit einheitlichem Etikett, dass auf die Netzwerkfähigkeit hinweist.

Diese Kennzeichnung soll neben der allgemeinen Netzwerkfähigkeit die Fähigkeit zur Verschlüsselung der Übertragungswege unter Angabe der verwendeten Standards enthalten.

Begründung

Wir leben in einer Zeit, in der nicht mehr nur PC und Smartphones im Internet sind, sondern immer mehr und mehr Geräte aller Art, z. B.: Kühlschränke, Fernseher, Bügeleisen, Autos und so weiter.

Oftmals ist für die VerbraucherInnen beim Kauf eines neuen Gerätes gar nicht zu erkennen ob es „Internet enthält", also eine IP-Adresse hat und übers Internet kommunizieren kann.

Warum ist das wichtig?

Netzwerkfähige Geräte müssen gepflegt werden, d.h. es müssen (Sicherheits-)Updates installiert werden, es muss geschaut werden, dass sich das Gerät keine einfängt und dadurch bspw. an einem Botnetz teilnimmt.

Auch stellen solche Geräte oftmals eine Gefahr für die Privatsphäre dar. Meist schicken die Geräte die Daten, die sie sammeln höchst selbst nach draußen in die weite Welt. Ist dies nicht der Fall, besteht immer die Gefahr fremden Übernahme, so dass sämtliche Daten, die das Gerät gesammelt hat, in die falschen Hände geraten.

IoT-Geräte (Internet of Things – Internet der Dinge) sind oft eine Sicherheits-Schwachstelle für die eigene IT-Landschaft. Rechner und Router sind in der Regel mit Firewalls und Antiviren-Programmen geschützt, aber wenn dann im selben Netzwerk bspw. noch eine Kaffeemaschine eingehängt ist, dann wird diese mit einem Trojaner infiziertund von dort aus wird das Netzwerk infiltriert.

Im Weiteren stellt die fehlende Sicherheit von IoT-Geräten auch eine Gefahr für unbeteiligte Dritte dar. Da bspw. die Kontrolle über entsprechende Geräte übernommen und in Botnetze integriert werden können. Anschließend sind auch Massenangriffe auf Dritte über sogenannte DDoS-Angriffe (Distributed Denial of Service) oder Bruteforce-Methoden zur Entschlüsselung möglich.

Empfehlung der Antragskommission: Konsensliste