Angriffe auf Steuerungs- und eingebettete Systeme

Die Sensibilisierung für die Angreifbarkeit kritischer Infrastrukturen, industrieller Steuerungs- oder eingebetteter Systeme hat in den vergangenen Monaten deutlich zugenommen. Das schlägt sich auch in den Sicherheitskonferenzen nieder. Und während an einigen Flughäfen noch getestet wird, ob der Einsatz von Körperscannern dort einen Sicherheitsgewinn bringt, trugen Teilnehmer der „Hack In The Box Amsterdam", der europäischen Ausgabe der malaysischen Hackerkonferenz vor, wie man trotz aller Sicherheitsmaßnahmen ein Linienflugzeug in seine Gewalt bekommen oder anderweitig die Sicherheit bedrohen könnte.

Ersteres beschrieb Hugo Teso, Berufspilot und Sicherheitsberater, in seinem Vortrag „Aircraft Hacking". Bei eBay hatte er für 500 US-$ das nötige Equipment gekauft, um die Kommunikation eines üblichen Linienflugzeugs im Labor nachzubauen. Das Cockpit wurde über einen Flugsimulator nachgebildet, wie er zur Ausbildung von Piloten benutzt wird. Mit dieser Ausstattung war es Teso möglich, über die Kommunikationswege zwischen Flugzeug und Bodenstation Befehle an das Flight-Management-System zu senden und von dort in weitere Systeme vorzudringen. In seiner Testumgebung konnte er sogar ein Framework in die Systeme einschleusen, über das sich das Flugzeug mittels einer Android-App steuern lässt. Auch wenn Teso dies noch nicht an einem echten Flugzeug testen konnte, verließen die Zuhörer den Vortrag mit einem mulmigen Gefühl.

In einem Vortrag über das „Terminal Cornucopia" zeigte Evan Booth anhand eindrucksvoller Videos, wie sich in einem Flughafen auch nach der Sicherheitskontrolle dank der zahlreichen Einkaufsmöglichkeiten potenziell gefährliche Waffen bauen lassen. Es war ihm sogar möglich, mittels der gekauften Artikel ferngesteuert einen Brand im Handgepäck auszulösen, der zudem nur sehr schwer zu löschen war.

Hacker trifft Paparazzi

Fotoreporter sind seit jeher bestrebt, ihre Aufnahmen möglichst schnell an die Presse weiterzureichen. Dazu haben hochpreisige Kameras mitunter sogar Funkschnittstellen integriert. Daniel Mende führte in seinem Vortrag live vor, wie er per WLAN auf eine Fotokamera zugreifen und Fotos hoch- oder herunterladen kann. Selbst zur Liveüberwachung lässt sich eine solche Kamera missbrauchen, ohne dass der Besitzer das Geringste merkt.

Sergey Sheykan und Artem Harutyunyan demonstrierten an einer handelsüblichen Netzwerkkamera, wie sie zu Tausenden in Privathaushalten oder Unternehmen eingesetzt wird, wie leicht ein Angreifer über eine CSRF-Schwachstelle (Cross-Site Request Forgery) auf die Kamera zugreifen kann. So ließen sich über auslesbare Kernel-Dumps Zugangsdaten zur Kamera extrahieren. Über einen schnell nachinstallierten Webproxy für das lokale Netzwerk ließ sich die Kamera sogar zur Netzwerküberwachung aufrüsten.

Manuel Moser (ur)