Neuland

Am 19.06.2013 äußerte Bundeskanzlerin Angela Merkel in einer Pressekonferenz mit dem damaligen US-Präsidenten Barack Obama, dass das Internet „für uns alle Neuland“ sei – und musste für diese Formulierung viel Hohn und Spott einstecken. Dabei ging ihr Satz weiter: Das Internet „ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen.“

Die Äußerung war zweifellos im Kontext der NSA-Überwachung gemeint, doch brachte Frau Merkel damit (wenn auch womöglich unwillentlich) eine empfindliche Wahrheit auf den Punkt, die auch vier Jahre danach, während die „Digitalisierung“ in aller Munde und Thema von Regierungserklärungen ist, leider noch immer Gültigkeit besitzt: Nach wie vor versehen Hersteller mit einer erschütternden Naivität ihre Produkte mit digitalen Schnittstellen und schaffen dabei mit unausgereiften und offenbar unzureichend getesteten Lösungen gefährliche neue Angriffspunkte. Mit geradezu voraussehbarer Regelmäßigkeit werden derzeit dieselben Fehler wiederholt, die sich die Hersteller von Betriebssystemen und Internet-fähigen Programmen in den vergangenen zwanzig Jahren mühsam abgewöhnt haben: Administrative Zugänge mit (oft trivialen) voreingestellten Standard-Passwörtern, Update-Mechanismen ohne Authentifikation und Integritätsprüfung oder ungeschützte „Remote-Zugänge“ für dringende Fernwartungszugriffe, um nur drei der schlimmsten zu nennen. Die zunehmende Vernetzung der Anwendungen und Systeme sorgt zugleich dafür, dass erfolgreiche Angriffe auf einzelne Komponenten unter Ausnutzung derartiger Schwachstellen meist gleich das gesamte IT-System und womöglich sogar weitere, mit diesen verbundene kompromittieren können. Kleine Ursachen mit meist großer Wirkung.

Solange es sich bei den von solchen Anfängerfehlern betroffenen Systemen um via Internet zugängliche Überwachungskameras handelt, mag das noch als handwerkliche Ungeschicklichkeit mit Spaßfaktor durchgehen. Inzwischen erfasst die von Sicherheitsaspekten unbelastete und von IT-Sicherheitskompetenz befreite Digitalisierung allerdings immer mehr Produkte, bei denen Angriffe eine unmittelbare Gefahr für Leib und Leben darstellen. Und spätestens da hört der Spaß nun einmal auf.

Blieb der Angriff auf ein motorisiertes Skateboard Anfang 2015 noch eher unbeachtet, sorgte die von einem Journalisten im Selbstversuch dokumentierte Attacke auf einen Chrysler Cherokee im Juli 2015 immerhin für etwas Wirbel. Gelernt haben daraus allerdings noch lange nicht alle Hersteller, wie der im Juli 2017 bekannt gewordene Angriff auf einen Segway MiniPro zeigte, dessen Smartphone-Steuerung von einem beliebigen Dritten übernommen werden konnte.

Seit Jahren unterwerfen wir jedes Fahrzeug vor der Zulassung strengen Untersuchungen. Jeder Sicherheitsgurt, jeder Reifen und jeder Stoßdämpfer muss einen Sicherheitstest absolvieren, bevor er eine Straßenverkehrszulassung erhält. Aber Komponenten mit IT-Schnittstellen – Radio, Navigationssystem, Lüftungssteuerung etc. – bei denen Implementierungsfehler einem Angreifer Eingriffe in die Fahrzeugsicherheit mit gegebenenfalls dramatischen Folgen ermöglichen können, dürfen ohne vertiefte Prüfung verbaut werden (und dabei denke ich noch gar nicht an Algorithmen zum autonomen Fahren). Schlimmer noch: Wir haben nicht einmal anerkannte und standardisierte Testverfahren, mit denen wir solche Systeme verlässlich prüfen könnten.

Neuland eben.

Mit herzlichen Grüßen, Ihr

Dirk Fox