Über das Restrisiko

Während der Bahnstreiks in den letzten Monaten häuften sich die Zeitungsartikel, die die Möglichkeiten eines automatisierten Bahnbetriebs diskutierten. Die meisten waren sich sicher, dass die Bahn nun umso schneller und intensiver die notwendigen Investitionen im Angriff nimmt, um Züge ohne Lokführer fahren lassen zu können. Dass das technisch möglich, bezweifelt eigentlich niemand mehr. Tatsächlich fahren ja schon mehrere U-Bahnen, z. B. die in Nürnberg, ohne Lokführer und irgendwie scheint die Aufgabe ja auch wirklich beherrschbar zu sein, wenn alle namhaften Automobil-Hersteller bereits sehr konkret an Prototypen von fahrerlosen Automobilen arbeiten. Die einzige Frage ist anscheinend: Ist das denn wirklich sicher genug?

Beim fahrer- oder führerlosen Fahren wird sehr deutlich, dass funktionale Sicherheit inzwischen hochgradig von Informationssicherheit abhängt. Deswegen freue ich mich sehr, dass wir diesem Thema in dem Artikel von **Christof Ebert** und **Armin Happel** etwas tiefer auf dem Grund gehen können. „Maßnahmen müssen sowohl im Produkt als auch im Entwicklungsprozess und im Feld umgesetzt werden. Architekturen, Systeme und Protokolle müssen spezifisch entwickelt werden, bereichsübergreifende Kompetenzen aufgebaut, und die Mitarbeiter einzeln für Informationssicherheit entlang des gesamten Lebenszyklus trainiert werden“, schreiben die Autoren.

Stephan Kaps geht in seinem Artikel „Einstieg in Secure-Coding und Continuous-Security-Testing“ noch einen Schritt weiter. Neben vielen wertvollen Tipps für sicheres Codieren gibt er uns den – aus meiner Sicht – zentralen Satz mit auf den Weg: „Nur wenn sich Security-Testing nahtlos in den Entwicklungs-Workflow integriert, indem Security-Bugs genauso aufgespürt, verwaltet und behoben werden wie andere Bugs, wird dieses Instrument auch von Entwicklern akzeptiert und die Art und Weise, wie sichere Software entwickelt wird, positiv beeinflusst.“ Soll heißen: Sicherheit ist nur konzeptionell durch Regeln zu gewährleisten, praktisch brauchen wir automatisierte Verfahren, die uns helfen, Sicherheitslücken aufzudecken und zu schließen. In genau diesem Sinne beschreibt **Tam Hanna** die „Honey-Files“, die bewusst Hacker und ihre Werkzeuge anlocken und auf ihren „Leim gehen lassen“.

Etwas anders ist der Tenor im Bereich der Gefährdungen durch moderne Datensammel-Verfahren wie Big Data. **Yvonne Hofstetter** mahnt in dem bemerkenswerten Interview, das **Johannes Mainusch** mit ihr geführt hat: „Der Mensch wird zum Objekt gemacht, obwohl er von Rechts wegen das Subjekt wäre. In der Sphäre der Maschinen wird er genauso behandelt wie eine Maschine ohne Rechte, weil eine Maschine keine Rechte hat.“ Im weiteren Verlauf des Gesprächs zeigt die Juristin und Expertin für Künstliche Intelligenz eine Reihe von daraus resultierenden Grundrechtsverletzungen auf.

Kerstin Dittert fordert in ihrem Artikel über autonome Akteure: „Es gilt, Gesetze weiterzuentwickeln, wirksame Sanktionen gegen Verstöße zu etablieren und dem Bürger durchsetzbare Rechte an die Hand zu geben. Ein Recht auf informelle Selbstbestimmung, das nur mit langem Atem und hohen Prozesskosten durchgesetzt werden kann, widerspricht dem Gedanken eines Grundrechts für alle Bürger.“

Irgendwie scheinen wir den staatlichen und vor allem den kommerziellen Datensammlern und automatischen Akteuren mehr oder weniger hilflos ausgeliefert zu sein. Der Ruf nach gesetzlichen Regelungen ist lauter als der nach organisatorischen oder technischen Lösungen. Das Problem scheint zu sein, dass es bereits heute organisatorische und technische Möglichkeiten gibt, die Sammelwut der Beteiligten einzuschränken, dass die kurzfristigen Vorteile der Preisgabe der eigenen Daten die oft abstrakt erscheinenden langfristigen Nachteile aber bei den meisten beteiligten Menschen überwiegen. Dieses Phänomen kennen wir ja schon aus der letzten industriellen Revolution – sowohl aus dem Bereich der Atomkraft als auch aus dem des CO_2-Ausstoßes. Hier wie dort sind Gesetzgebungsverfahren zu langsam und zu regional, um wirksamen Schutz zu bieten. Außerdem wird schon in aktuellen Konflikten deutlich, dass gerade despotische Herrscher sich der neuen Werkzeuge für ihre Zwecke bedienen werden, um Freiheiten und Rechte anderer einzuschränken. Müssen wir also an diesem Sicherheitsdilemma verzweifeln? Müssen wir in eine apokalyptische Depression fallen?

Ich glaube nicht. Wir werden durch die Möglichkeiten der Daten viele neue Chancen und Annehmlichkeiten bekommen. Wir werden zum Beispiel staufrei Auto und streikfrei Bahn fahren, wir werden stressfrei einkaufen und CO_2-frei kommunizieren. Aber wir werden eben auch das gesellschaftliche Bewusstsein für die Risiken dieser Technologie ausbilden müssen. Denn nur, wenn die beteiligten Menschen Grenzen und Schutz wünschen, entsteht Raum für politische, aber erst recht für die von uns heute zu entwickelnden technischen Schutzmaßnahmen gegen die Risiken im Haifischbecken der Datensammler.

Ihr Thorsten Janning,
Chefredakteur OBJEKTspektrum