Null-Fehler-Sicherheit

Es ist enorm, was Software auf Basis einer soliden Hardware alles vollbringen kann. Software spielt Schach wie ein Großmeister. Software ermöglicht Menschen, im virtuellen Raum real zusammenzuarbeiten und setzt dabei geschäftliche Regeln durch. Und Software soll schließlich in Zukunft auch selbständig Auto fahren. Würde mein Schachprogramm seinen nächsten Zug ein wenig später ausführen oder nicht optimal spielen; ich würde es vermutlich nicht einmal merken. Das gleiche gilt für unzählige andere Anwendungen.

Doch wir kennen auch diese Fälle: Die Software reagiert einfach nicht mehr. Änderungen an Daten werden erst beim zweiten oder dritten Mal übernommen. Ein Software-Update drängt sich dazwischen; mit Mühe kann ich noch meine Daten speichern. Eine unverständliche Fehlermeldung verhindert das Weiterarbeiten; ich verstehe nicht, was ich angeblich falsch gemacht habe. Der Bildschirm friert ein. Hacker stehlen Informationen. Erpresser verschlüsseln die Festplatte. Irgendjemand bringt den Server zum Absturz; oder war es doch nur ein Hardware-Fehler?

An viele dieser Abstürze, Fehlfunktionen und Hacks haben wir uns fast gewöhnt. Doch während solche Mängel bei meinen übrigens völlig zuverlässig arbeitenden Schachprogrammen noch tolerierbar wären, würde ich heutzutage sicher zögern, in ein Auto ohne Lenkrad und Bremse zu steigen. „Update; das System steht Ihnen in wenigen Augenblicken wieder zur Verfügung.“ „Aufgrund eines Fehlers steht das System 4711 gerade nicht zur Verfügung. Bitte lesen Sie im Handbuch nach.“ Doch bei solchen Fehlermeldungen kann man ja noch davon ausgehen, dass das Programm weiß, was los ist. Anders sieht es meist bei erfolgreichen oder angeblich abgewehrten Angriffen aus. Im besten Fall weiß das Auto, dass etwas nicht stimmt. Integritätsverletzung! Oder war es doch nur ein unglückliches Zusammentreffen von Ereignissen, die der Programmierer nicht vorhersehen konnte?

Was wir brauchen, ist Qualität in der IT und der IT-Sicherheit! Doch die gibt es in Zeiten raschen Wandels weder durch Worte noch durch Kontrolle und Korrekturen. Qualität in der IT-Sicherheit entsteht nicht einmal durch wirklich ehrliches Bemühen, es endlich besser zu machen. Was wir brauchen, sind neue Methoden und Werkzeuge.

Wer sich Qualität zum Ziel setzt, macht nicht gleich zu Anfang Abstriche! Er nimmt das Endziel ins Visier! Wollen wir IT-Sicherheit erreichen, so kann die Devise daher nur „Null-Fehler-Sicherheit“ heißen! Dies ist ein ambitioniertes Vorhaben, dem sich namhafte Experten im Schwerpunktthema dieses Heftes mit sechs Beiträgen zu nähern versuchen. Sie werden diverse Entwicklungen und Trends untersuchen und dort nach Lösungen Ausschau halten. Denn Notwendigkeiten sind der beste Lehrmeister: Die zunehmende Digitalisierung bringt neue IT-Architekturen hervor (wie das Internet-der-Dinge). Die Arbeitsteilung in der IT nimmt massiv zu (Lieferketten werden komplexer). Die Künstliche Intelligenz tritt auf den Plan. Security und Safety wachsen zusammen; die eine Sicherheit entscheidet auch über die andere. Gleichzeitig wird die Abhängigkeit von qualifiziertem Personal spürbar (zum Beispiel Kompetenz statt nur Knowhow).

Ein weiterer Beitrag im Heft befasst sich mit einem innovativen Konzept für die Gewährleistung von Sicherheit & Vertrauen im Post-Quantum Umfeld.

Eberhard von Faber