IT-Sicherheit 5.0

Die Informationstechnologie (IT) und ihre Anwendungsgebiete entwickeln sich so rasant, dass es Zeit für Informationssicherheit 5.0 wird. Die IT-Sicherheit muss nachziehen. Fünf-Punkt-Null? Ist es schon so weit? Bis in die 1980er Jahre war die Technik von zentralem Computing und von mehr oder minder eigenständigen oder lokal vernetzten PCs geprägt. Regierungen entwickelten erste Kriterien für die IT-Sicherheit wie das Orange-Book und die ITSEC auch für den privatwirtschaftlichen Bereich (1.0). Anfang der 1990er Jahre wurden die PCs mobil und den Nutzern wurde klar, dass sie für die Sicherheit der Daten sorgen müssen (2.0). In der zweiten Hälfte der 1990er Jahre kam das Internet, und mehr oder minder alle Rechentechnik und viele Anwendungen wurden vernetzt. Unternehmen entwickelten neue Sicherheitskonzepte für vernetzte IT, und sie gestalteten ihre Sicherheitsorganisationen zu Managementsystemen um (3.0). Mitte bis Ende der 2000er Jahre kamen Virtualisierung und Cloud-Geschäftsmodelle auf, und anfängliche IT-Silos wichen global vernetzten Infrastrukturen. Die IT-Sicherheit setzte mehr und mehr auf grundlegende Lösungen zur Abwehr und schnelle Reaktion im Angriffsfall (4.0).

Keine der Aufgaben ist heute obsolet geworden. Doch selbst wenn wir diese Aufgaben hervorragend meistern könnten, wären wir nur schlecht gerüstet für das was kommt. Komplexität und Arbeitsteilung in der IT nehmen massiv zu (Lieferketten werden komplexer). Die Industrialisierung der IT-Herstellung schreitet voran. Die Diversität der Geschäftsmodelle steigt an, und ihr Einfluss auf die IT-Sicherheit wird immer deutlicher (zum Beispiel Workload versus Infrastruktur). Die Globalisierung drückt auf die Kosten und verlangt neue Methoden und Standards. Und gleichzeitig werden das Business und die Behörden immer abhängiger von sicher funktionierender IT.

Das alles muss zu einer Weiterentwicklung der Methoden der Informationssicherheit führen: eben zu IT-Sicherheit 5.0. – Worum es dabei primär geht, sind nicht neue Sicherheitstechnologien und -produkte. Was wir brauchen, sind Methoden für mehr Qualität! Architekturen sind zu nutzen, um die Komplexität beherrschen zu können. Modularisierung und Standards für Sicherheitsspezifikationen helfen dabei, für IT-Sicherheit in der arbeitsteiligen Lieferkette zu sorgen. Die Entkopplung von IT-Funktionalität und IT-Service-Management ermöglicht es uns, bei allen Geschäftsmodellen das Ganze zu sehen. Die Integration von IT-Sicherheit in die Herstellungsprozesse im Sinne von „Secured by definition" ist ein Mittel, die Kosten zu senken und die Sicherheit zu verbessern.

Sind Architekturen, Modularisierung, Vereinheitlichung, Strukturen und IT-Herstellungsprozesse die aktuellen Themen der IT-Sicherheit, die alle bewegen? Ich kann dies leider nicht erkennen. Solche Themen zu adressieren und neue Methoden und Werkzeuge im Sinne von IT-Sicherheit 5.0 zu entwickeln sollte uns aber ein wichtiges Anliegen sein. Denn ohne sie könnten die Digitalisierung zum gefährlichen Ritt und das IT-Sicherheitsmanagement schon bald vollends zur Sisyphos-Arbeit werden.

Prof. Dr. Eberhard von Faber