Vertrauen ist gut ... Zertifizierung ist besser!

Der grundsätzliche Wert einer Zertifizierung der IT-Sicherheit von Produkten und Lösungen ist aufgrund langjähriger Praxis unbestritten – schließlich sind viele unserer täglichen Begleiter, ob Personalausweis, Reisepass oder Gesundheitskarte, nach speziellen Sicherheitsvorgaben zertifiziert und mit ISO/IEC 15408 hat sich ein einschlägiges, international abgestimmtes Normenwerk (auch bekannt als „Common Criteria“) fest etabliert.

Andererseits erreicht die Methodik der Common Criteria aus nachvollziehbaren Gründen nur einen kleinen Teil der uns umgebenden IT Infrastruktur. Ein wenig ist das – bitte verzeihen Sie das plumpe Bild – als würden nur wenige ausgewählte Fahrzeuge auf unseren Straßen TÜV-geprüft. Unter anderem mit dem Ziel, diese unbefriedigende Situation zu verbessern, hat die Europäische Kommission im September 2017 im Rahmen ihres Cybersecurity Packages einen Vorschlag für einen sogenannten „Cybersecurity Act“ veröffentlicht. Dieser stellt zum einen eine gute Chance für die Verbesserung der Cybersicherheit in Europa dar, zugleich soll er der europäischen IT-Sicherheits-Industrie neue Möglichkeiten eröffnen.

Den inhaltlichen Schwerpunkt des vorliegenden Heftes bildet eine Reihe von Beiträgen zu dem oben angesprochenen Komplex. *Miguel Bañón* führt in die ISO/IEC 15408 Normenfamilie ein, diskutiert das Erreichte und das Wünschenswerte und gibt einen Ausblick auf die derzeit intensiv vorangetriebene Weiterentwicklung der Common Criteria.

Andreas Mitrakas beleuchtet im Anschluss den „Cybersecurity Act“ aus Sicht der ENISA und diskutiert die angestrebte neue Rolle der ENISA im Zusammenspiel mit den bereits existierenden Aktivitäten und Spielern auf dem Feld der Zertifizierung von IT-Sicherheit in Europa.

Der Beitrag von *Bernd Kowalski* und *Matthias Intemann* bildet hierzu einen Gegenpol und setzt sich entsprechend kritisch mit dem „Cybersecurity Act“ auseinander.

Edward Humphreys gibt einen Einblick in seine Erwartungen hinsichtlich der Weiterentwicklung der überaus erfolgreichen ISO/IEC 27001 Normenfamilie. Er beleuchtet markt- wie technologiegetriebene Herausforderungen und diskutiert möglicherweise notwendig werdende Anpassungen im Angebot der ISMS Standards.

Neben der IT-Sicherheit sind Vertrauensdienste – wie sie durch die eIDAS-Verordnung definiert sind – ein bereits bewährtes Anwendungsfeld für Zertifizierungen. Mit *Kim Nguyen* und *Herbert Leitold/Daniel Konrad* erläutern ausgewiesene Experten die positiven sowie in Deutschland und Österreich auch unterschiedlichen Erfahrungen in diesem Bereich.

Arno Fiedler und *Christian Thiel* runden den Schwerpunkt des Heftes mit einer kritischen Sicht auf nationale, regionale und gesellschaftliche Aspekte einer Zertifizierung von IT-Sicherheit ab.

Zwei Aufsätze gehen darüberhinaus auf spezifische Themen ein, die sich aus der Datenschutzgrundverordnung ergeben. *Olga Kieselmann* und *Arno Wacker* behandeln mit einem neuen Lösungsansatz das nach wie vor spannende Thema „Löschen im Internet“ und *Susan Gonscherowski*, *Marit Hansen* und *Martin Rost* greifen Resilienz als eine neue Anforderung aus der Datenschutz-Grundverordnung auf.

Wir hoffen, das Spektrum der Beiträge in diesem Heft findet auch diesmal Ihr Interesse.

Walter Fumy und Helmut Reimer