Kernforderungen zu Cybersecurity und Datenschutz

1. Cybersecurity von digitalen Dienstleistungen und IT-vernetzten Produktionsanlagen sowie kritischen Infrastrukturen stärken! Vertrauen in die digitale Welt durch Zertifikate unabhängiger Dritter fördern!
2. Security by Design-Standards und Interoperabilität vorantreiben! Sie sind die Voraussetzung für den Erfolg der Digitalisierung. Hierfür müssen einheitliche europäische Standards für die digitale Vernetzung übergreifend definiert werden.
3. Die Prüfung von IoT-Produkten muss stets erweiterte Funktionalitäten wie Kommunikationsfähigkeit und Interoperabilität sowie die Aspekte Safety und Security umfassen!
4. Die Akzeptanz und Vertrauenswürdigkeit von Cloud-Lösungen durch international anerkannte Sicherheitsstandards und Datenschutzregelungen verbessern! Sie sind die Grundlage für Zertifizierungen und ein allgemein anerkanntes neutrales Prüfsiegel, das Seriosität, Qualität und Sicherheit einer Cloud-Dienstleistung vermitteln kann.
5. Schaffung eines unabhängigen und fachkompetenten Zulassungs- und Zertifizierungssystems für vertrauenswürdige und sichere Software-Lösungen vernetzter Geräte. Voraussetzung ist hierfür der diskriminierungsfreie Zugang zu Steuerungs- und Softwaredaten zu Prüfzwecken.
6. Die Verfügungsgewalt des Nutzers über seine personenbezogenen Daten muss gewährleistet bleiben! Diese Anforderungen an den Datenschutz sollten vor der Vermarktung digital vernetzter Produkte und Webservice-Anwendungen durch ein unabhängiges und qualifiziertes Audit und Zertifikat nachgewiesen werden.
7. Digitale Kompetenz der Gesellschaft durch gezielte Aus- und Weiterbildungsangebote bereits in der Schulausbildung stärken! Zur Steigerung der Beurteilungskompetenz bedarf es umfangreicher Sensibilisierung zu den Themen Cybersicherheit und Vertrauenswürdigkeit aller Mitarbeiter in Unternehmen und Behörden.