



Pressemitteilung

Sicherheit als Marktvorteil: wird zur Pflicht:

Wie Unternehmen den Cyber Resilience Act pragmatisch meistern

Aktuelle EU-Vorgaben verändern die Spielregeln für vernetzte Produkte grundlegend: Wer digitale Komponenten entwickelt, integriert oder vertreibt, steht vor verbindlichen Sicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg. Wie Unternehmen diesen Wandel strategisch für sich nutzen können, beleuchtete die Transformationslounge des Transformationsnetzwerks (TraFoNetz) Nordschwarzwald im IHK-Bildungszentrum Nagold.

Eine verantwortliche Person benennen, Produkte erfassen, Meldewege festlegen: Mit diesen drei Schritten lasse sich der Cyber Resilience Act (CRA) im Betrieb sinnvoll anpacken. **Maria Rill**, Abteilungsleiterin im Forschungsbereich Cybersecurity and Law am FZI Forschungszentrum Informatik in Karlsruhe, erläuterte, wen die Verordnung betrifft, die Anfang September 2026 in einer ersten Stufe gestartet ist: Hersteller von Produkten mit digitalen Elementen, speziell mit vernetzter Hardware und Software. Sie müssten schon beim Design mögliche Risiken bewerten, Schwachstellen behandeln und die Konformität nachweisen.

Auslöser für die Vorgabe der EU war unter anderem die Sicherheitslücke in der Java-Bibliothek „Log4j“, die in unzähligen Produkten steckte, ohne dass die Hersteller es wussten. Deshalb gehört nun eine Software Bill of Materials (SBOM) zu den Pflichten.

Das Stimmungsbild bei den Teilnehmenden zum Veranstaltungstitel „CRA – Fluch oder Segen“ fiel geteilt aus. **Jochen Protzer**, Geschäftsführer der Wirtschaftsförderung Nordschwarzwald GmbH (WFG), die das Projekt TraFoNetz federführend betreut, macht unterdessen deutlich: Cybersicherheit dürfe in der betrieblichen Praxis nicht als lähmende Pflicht verstanden werden, sondern als unverzichtbares Fundament für Marktfähigkeit und digitale Innovationskraft. „Mit TraFoNetz eröffnen wir mittelständischen Unternehmen gangbare Pfade, um regulatorische Hürden strukturiert zu meistern und nachhaltiges Vertrauen bei Kunden aufzubauen“, so der WFG-Geschäftsführer.

In der lebhaften Debatte mit den anwesenden Fach- und Führungskräften kamen handfeste betriebliche Reibungspunkte zur Sprache. Eine Software-Entwicklerin schilderte die schwierige Abhängigkeit von internationalen Komponenten: Viele Zulieferer und Plugin-Entwickler aus den USA oder Asien zeigten bislang wenig Bereitschaft, sich an europäische Zeitpläne anzupassen. Dadurch würden hiesige Integratoren unweigerlich in die Herstellerrolle mit voller Konformitätshaftung geraten.

FZI-Abteilungsleiterin Rill riet zu strukturiertem Risikomanagement: „Nicht jedes Produkt braucht die verrückteste und krasseste Krypto oben drauf.“ Man müsse die Maßnahmen entsprechend dem Risiko auswählen. Zudem stellte sie klar, dass bewährte und bestehende Schutzkonzepte anerkannt

Pressekontakt:

Wirtschaftsförderung Nordschwarzwald GmbH

Jutta Effenberger, Tel.: (+49) 7231 / 15 43 69-31, E-Mail: jutta.effenberger@nordschwarzwald.de



würden. So müssten Branchen mit bereits etablierten Standards, etwa Automotive (UN ECE R155) oder Medizinprodukte (MDR), keine Doppelregulierung fürchten.

Ein Kleinunternehmer schilderte, dass allein Überwachung und Konformitätsaufwand für viele seiner Kunden monatlich bis zu zwei Stunden bedeuten würden. Rill appellierte, die Herausforderungen über Verbände und das BSI (Bundesamt für Sicherheit in der Informationstechnik) zu melden, denn kleine und mittlere Unternehmen hätten in Brüssel wenig Lobby.

Dämpfen konnte die Expertin die Sorge vor harten Sanktionen. Beim FZI Open House im Februar habe die BSI-Referatsleiterin betont, dass bei nachweisbarer Auseinandersetzung mit dem Thema zunächst Beratung im Vordergrund stehe. Nach Rills Erfahrung würden die Marktüberwachungsbehörden vor allem auf den Nachweis aktiver Prozesse statt auf pauschale Strafen zum Stichtag setzen. Wichtig seien vor allem die Erstellung einer transparenten Software-Stückliste (SBOM), geregelte Update-Pfade sowie klare Zuständigkeiten im Schadensfall.

TraFoNetz-Projektleiter **Daniel Fissl** zeigte im zweiten Teil der Veranstaltung auf, wie Unternehmen unmittelbar ins Handeln kommen. Mit einem kostenfreien Cybersicherheitscheck erhielten kleine und mittlere Unternehmen eine strukturierte Standortbestimmung in zentralen Themenfeldern. In enger Kooperation mit der Cybersicherheitsagentur Baden-Württemberg würden konkrete Handlungsempfehlungen abgeleitet, flankiert von Workshops und Schnittstellen zu regionalen Hochschulen. Ergänzend decke ein Digitalisierungsscheck breitere Innovationspotenziale ab, sodass regulatorische Vorgaben und unternehmerisches Wachstum Hand in Hand gingen.

Den praxisnahen Abend in Nagold resümierte TraFoNetz-Teilprojektleiter und Event-Organisator **Matthias Friedrich** so: „Wer Sicherheitsstrukturen frühzeitig im Produktentstehungsprozess verankert, schützt sensible Werte und sichert sich zudem entscheidende Wettbewerbsvorteile.“

Link zum Bildmaterial:

<https://www.dropbox.com/scl/fo/5bvuguzpnsxc3bx2k22w/ACj44a1Qvcaireme8crkK14?rlkey=wh0v0mr snak2eue3g0hvmc46d&st=2n1uhgxf&dl=0>

Bildbeschreibung:

Bild 1: Von links: Daniel Fissl, TraFoNetz Projektmanager, Referentin Maria Rill vom FZI sowie TraFoNetz-Teilprojektleiter und Event-Organisator Matthias Friedrich.

Bild 2: Maria Rill vom FZI informierte im IHK-Bildungszentrum Nagold über die neue EU-Verordnung „Cyber Resilienz Act“ (CRA).

Bild 3: TraFoNetz-Projektmanager Daniel Fissl stellte den Cybersicherheitscheck und den Digitalisierungsscheck vor.

Bild 4: Begrüßte als Hausherr des IHK-Bildungszentrums die Teilnehmenden: Geschäftsstellenleiter Patrick Walz.

Bildrechte: Gerd Lache

Pressekontakt:

Wirtschaftsförderung Nordschwarzwald GmbH

Jutta Effenberger, Tel.: (+49) 7231 / 15 43 69-31, E-Mail: jutta.effenberger@nordschwarzwald.de