

CIRES stärkt resiliente Konnektivität für KRITIS in Europa

Artikel vom **6. Oktober 2026**

ITK und Dienstleistungen

Giesecke+Devrient beteiligt sich am EU-Projekt »CIREs«. Ziel ist ein Edge-Computing-Stack, der kritische Infrastrukturen bei Cyberangriffen, Stromausfällen oder Netzstörungen funktionsfähig hält und sichere Kommunikation ermöglicht.



Bernd Müller, Head of Technology & Innovation. (Bild: G+D)

Giesecke+Devrient beteiligt sich als Technologiepartner am europäischen Forschungs- und Innovationsprojekt »CIREs«, das im Rahmen von Horizon Europe Chips JU gestartet ist. Über 36 Monate arbeiten 17 Partner aus fünf europäischen Ländern daran, die Resilienz kritischer Infrastrukturen in Europa zu stärken. Im Fokus stehen vor allem Energieversorgung und digitale Infrastruktur. Das Projekt entwickelt einen

durchgängigen Technologie-Stack für resilientes Edge Computing. Kritische Systeme sollen damit auch bei Cyberangriffen, Stromausfällen, Kommunikationsstörungen oder Störungen in der Lieferkette lokal weiterarbeiten und sich kontrolliert erholen können. Dafür werden unter anderem eingebettete KI für schnelle lokale Entscheidungen, fehlertolerante Kommunikation über heterogene Netze, belastbare Zeit- und Synchronisationsmechanismen sowie verteilte Edge-to-Cloud-Architekturen kombiniert.

Sichere Identitäten für vernetzte Systeme Ein zentraler Beitrag liegt in der Entwicklung und Integration post-quantenfähiger »eSIM«- und »iSIM«-Lösungen für Kommunikationssysteme in kritischen Infrastrukturen. Die Technologien sollen als Hardware-Vertrauensanker dienen und Identitäten, Authentisierung sowie sichere Kommunikation unterstützen. Geplant ist ein krypto-agiles Betriebssystem für eUICC- und iUICC-Plattformen, das in Multi-RAT-Umgebungen eingesetzt werden kann. Damit lassen sich Konnektivitätsprofile über den gesamten Lebenszyklus eines Geräts flexibel und sicher verwalten. Betreiber kritischer Infrastrukturen können so auf Netzstörungen, Betreiberwechsel oder neue Sicherheitsanforderungen reagieren, ohne Geräte im Feld physisch anpassen zu müssen. Resiliente Backend-Systeme übernehmen dabei das sichere Lifecycle- und Connectivity-Management der jeweiligen Implementierungen.

Kommunikation auch bei gestörten Netzen Die entwickelten Lösungen zielen darauf ab, Kommunikation und Authentisierung auch dann verfügbar zu halten, wenn zentrale Netze ausfallen oder angegriffen werden. Unterstützt werden unterschiedliche Kommunikationswege, darunter 4G, 5G und nicht-terrestrische Netze. Offene Standards, interoperable Sicherheitsarchitekturen und europäische Technologiebausteine sollen dazu beitragen, Abhängigkeiten zu reduzieren und die technologische Souveränität Europas zu stärken. Ein wichtiger Baustein ist die Integration von Post-Quanten-Kryptographie. Sie soll den Übergang zu künftigen kryptographischen Standards unterstützen und kritische Infrastrukturen besser gegen neue Bedrohungen absichern. Krypto-agile Mechanismen ermöglichen es, Sicherheitsverfahren anzupassen, wenn sich Anforderungen oder Risiken verändern.

Demonstratoren für reale Einsatzfelder Die im Gesamtprojekt entwickelten Technologien werden in mehreren Demonstratoren unter realitätsnahen Bedingungen validiert. Vorgesehen sind unter anderem drohnengestützte Infrastrukturinspektionen, Smart-City- und Smart-Building-Services, resiliente digitale Zwillinge für Lieferketten, robuste Energiesysteme sowie das Monitoring digitaler Infrastrukturen. Das Forschungsprojekt wird durch das Chips Joint Undertaking unter Grant Agreement No. 101253052 sowie durch das deutsche Bundesministerium für Forschung, Technologie und Raumfahrt unter Fördervereinbarung Nr. 16MEE1145K gefördert und von der Europäischen Union kofinanziert.

Hersteller aus dieser Kategorie
