Pressemitteilung – 11. März 2026

Start des ENFORCERS-Projekts zur Förderung der europäischen Zusammenarbeit im Bereich der Cybersecurity für industrielle Software und Automatisierung

- **Eine koordinierte Zusammenarbeit aller Stakeholder ist entscheidend für eine Cyber-Resilienz in der Industrie.**
- **ENFORCERS zielt darauf ab, Aufgaben der Vorfallserkennung (Incident Detection) und koordinierter Reaktion sowie die Zertifizierung und Bereitstellung sicherer Updates zu automatisieren.**
- **Der Fokus liegt auf der Stärkung der industriellen Automatisierung in OT-Umgebungen durch die Überwachung und Verfolgung von Schwachstellen in Softwarelieferketten.**
- **Die WIBU-SYSTEMS AG koordiniert das Projekt, das von der Europäischen Union kofinanziert wird.**

Ein europäisches Konsortium startet ein dreijähriges Projekt zum Schutz von Softwarelieferketten, zur koordinierten Reaktion auf Vorfälle (Incidents) und zur Lebenszyklus-Resilienz im Rahmen der neuen EU-Cybersecurity-Vorschriften

Karlsruhe – **Das europäische Forschungs- und Innovationsprojekt ENFORCERS (Enhanced Cooperation for Cybersecurity) ist offiziell gestartet. Es vereint ein starkes Konsortium aus Industrieherstellern und Anbietern von Cybersecurity-Technologien, das von angewandten Forschungseinrichtungen unterstützt wird. Gemeinsam wollen sie eine der drängendsten Herausforderungen Europas angehen: die Sicherstellung robuster und vertrauenswürdiger Software während des gesamten Lebenszyklus industrieller Automatisierungssysteme.**

Das offizielle Kick-off-Meeting fand am 10. und 11. Februar 2026 bei der WIBU-SYSTEMS AG in Karlsruhe statt. Bei diesem Treffen kamen die Konsortialpartner erstmals persönlich zusammen, um die nächsten Schritte und den strategischen Fahrplan für die kommenden drei Jahre zu besprechen. Das Treffen markierte den operativen Startpunkt von ENFORCERS und schuf die Voraussetzungen für eine enge, durch EU-Fördermittel kofinanzierte grenzüberschreitende Zusammenarbeit.

Von der Vorfallserkennung bis zur sicheren Wiederherstellung: So werden Cybersecurity-Lücken geschlossen

ENFORCERS geht über isolierte Schutzmaßnahmen hinaus. Das zentrale Ziel besteht darin, die Lücke zwischen der Erkennung von Cybersecurity-Vorfällen und koordinierten Reaktionen sowie der Zertifizierung und sicherer Softwareverteilung in industriellen Umgebungen zu schließen. Dies ist besonders relevant für die Bereiche Automatisierung und Fertigung, in denen Software häufig über segmentierte, teilweise voneinander getrennte oder heterogene Operational Technology (OT)-Netzwerke aktualisiert werden muss.

Das Projekt basiert auf einer Cybersecurity-Systemplattform, die mehrere vertrauenswürdige Instanzen zu einem sicher verketteten „System Circle“ verbindet. Dazu gehören:

- Private **Security Operation Center (SOC)**, die Daten zu Vorfällen und Schwachstellen sammeln, verknüpfen und klassifizieren.
- **Secure Elements,** die als Vertrauensanker an OT-Endpunkten und Gateways fungieren.
- **Automatisierte Playbooks** zur Schwachstellenbehebung, Zertifizierung und für sichere Software-Updates.
- **Grenzüberschreitende Datenaustauschmechanismen**, die es SOCs und Stakeholdern ermöglichen, unter Wahrung der Souveränität über ihre Daten zusammenzuarbeiten.

Dieser technische Ansatz unterstützt die Einhaltung von **NIS2** und antizipiert die Anforderungen des **Cyber Resilience Act**. Gleichzeitig kann er an zukünftige gesetzliche und technologische Entwicklungen angepasst werden.

> *„ENFORCERS vereint Technologien, Prozesse und Stakeholder in einem operativen Cybersecurity-Framework“, erklärte **Alvaro Forero**, **Projektkoordinator bei der WIBU-SYSTEMS AG**. „Als Koordinator ist es unsere Verantwortung, sicherzustellen, dass wir ein kooperatives System aufbauen, in dem Reaktionen auf Vorfälle, Vertrauensanker und sichere Softwarebereitstellung über organisatorische und nationale Grenzen hinweg zusammenwirken. Das Kick-off-Meeting hat das gemeinsame Verständnis bestätigt, dass Cybersecurity-Resilienz in den gesamten Lebenszyklus von Industriesoftware integriert werden muss.“*

Genaue Rollenverteilung in einem starken europäischen Konsortium

ENFORCERS bringt Partner mit sich ergänzenden Fachkenntnissen aus ganz Europa zusammen. Als Projektkoordinator steuert **Wibu-Systems** seine langjährige Expertise in den Bereichen Softwareschutz, Lizenzierung und sichere Update-Mechanismen für industrielle Umgebungen bei und sorgt gleichzeitig für die technische Kohärenz und die partnerübergreifende Integration im gesamten Projekt. Industrieunternehmen wie **Balluff** (Deutschland und Ungarn), **Schneider Electric** (Frankreich), **TTTECH Computertechnik** (Österreich) und **Technology Nexus Secured Business Solutions** (Schweden) liefern praktische Anforderungen aus den Bereichen Automatisierung, Fertigung und industrielle Vernetzung. Technologie- und Cybersecurity-Spezialisten wie **Infineon Technologies** (Deutschland), **Langlauf Security Automation** (Deutschland), **DYNAMIKI** (Griechenland), **AITAD** (Deutschland) und **ResilTech** (Italien) ergänzen das Projekt mit ihrem Fachwissen, das von KI und Embedded-Systemen über Secure Elements und Kryptografie bis hin zu SOC-Betrieb und Reaktion auf Vorfälle reicht. Die angewandte Forschung wird von dem **Fraunhofer-Institut für Sichere Informationstechnologie (SIT)** als Unterauftragnehmer unterstützt, während der **VDMA** sein industrielles Netzwerk und seine politische Präsenz einbringt.

Aus Sicht der Partner ist das Projekt auch ein Ausdruck ihres Engagements für die europäische Zusammenarbeit.

> *„Wir bei ResilTech freuen uns darauf, mit vollem Einsatz einen Beitrag zu leisten und gemeinsam mit so hochkarätigen Partnern daran zu arbeiten, die industrielle Cybersecurity in Europa zu stärken“, betonte* ***Francesco Brancati****,* ***Security Solution Manager und R&D Program Manager bei ResilTech Srl****. Er unterstrich dabei die Bedeutung der grenzüberschreitenden Zusammenarbeit als Voraussetzung für resiliente industrielle Systeme.*

Das Projekt integriert effektiv drei wesentliche Arbeitsebenen, die von strukturellen Aktivitäten wie Systemanforderungen und Architekturdesign über praktische Implementierungsmaßnahmen wie SOC-Integration, digitale Elemente und sichere Konnektoren bis hin zu qualitätsorientierten Aufgaben mit Schwerpunkt auf Verbreitung, Überwachung der Einhaltung von Standards und Schulungen reichen.

Die ersten Meilensteine umfassen die Definition der rechtlichen und technischen Anforderungen, die Konzeption der Cybersecurity-Systemarchitektur sowie die Einrichtung der ersten SOC- und Plattformkomponenten. In späteren Phasen folgen Demonstratoren und Validierungen.

Industriepartner betrachten ENFORCERS als strategische Investition in die langfristige Resilienz ihres Unternehmens.

> *Wie* ***Dr. Markus Jung****,* ***VP Engineering bei der Balluff GmbH****, bei der Projektvorstellung betonte: „ENFORCERS ist für Balluff eine hervorragende Gelegenheit, ein starkes Netzwerk mit führenden Partnern im Bereich Cybersecurity aufzubauen. Das Projekt wird uns dabei unterstützen, unsere Cybersecurity-Maßnahmen zu stärken und Best Practices für unsere industriellen Automatisierungsprodukte, Prozesse und Produktionsstätten zu optimieren. Das leistungsstarke Konsortium ermöglicht es uns, aufkommende Trends in den kommenden Jahren weit über die Anforderungen des Cyber Resilience Act hinaus*

> *zu antizipieren und letztlich unseren Kunden dabei zu helfen, ihre eigene Cybersecurity zu verbessern.“*

In den nächsten drei Jahren wird ENFORCERS technische Demonstratoren, bewährte Verfahren, Schulungsmaßnahmen und Impulse für Standardisierungs- und Zertifizierungsdiskussionen bereitstellen. Durch die Verbindung von industrieller Praxiserfahrung mit Fachwissen im Bereich Cybersecurity sollen Ergebnisse erzielt werden, die branchenübergreifend reproduzierbar sind. Diese sollen die digitale Souveränität Europas im Bereich industrielle Software und Automatisierung stärken.

Kofinanziert von der Europäischen Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Das Projekt wird vom Europäischen Kompetenzzentrum für Cybersecurity im Rahmen der Fördervereinbarung Nr. 101249745 unterstützt und durch die Europäische Union kofinanziert.

Die geäußerten Ansichten und Meinungen sind ausschließlich die der Autoren und spiegeln nicht unbedingt die der Europäischen Union oder des Europäischen Kompetenzzentrums für Cybersecurity wider. Weder die Europäische Union noch das Europäische Kompetenzzentrum für Cybersecurity können dafür verantwortlich gemacht werden.

8.279 Anschläge bei durchschnittlich 55 Zeichen pro Zeile

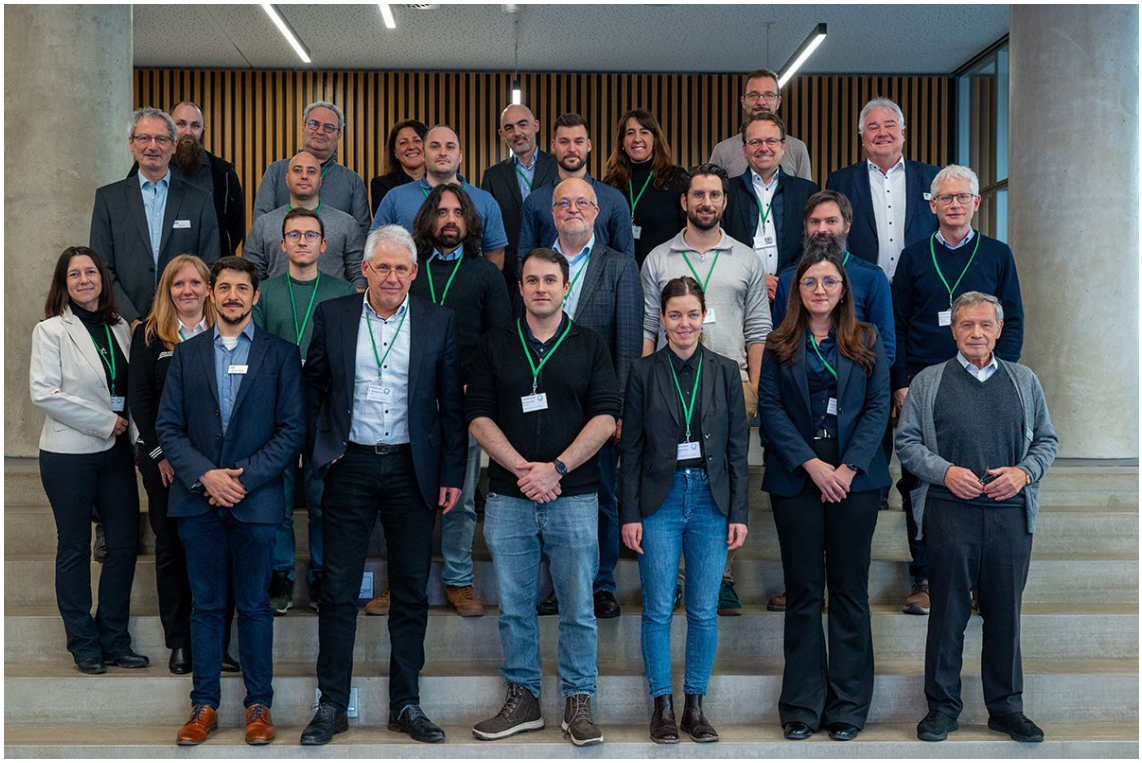

Bild: Konsortialpartner beim Kick-off-Meeting des ENFORCERS-Projekts im Februar 2026.

Weiterführende Informationen

- Details zum Forschungsprojekt: https://www.wibu.com/de/forschung-und-entwicklung/enforcers.html
- Die Pressemitteilung als Audiofile: https://www.wibu.com/fileadmin/Audiofiles/press_releases/WIBU-PR_ENFORCERS_DE.mp3
- Die Pressebilder stehen optimiert für den Druck und Online-Veröffentlichungen bereit: https://wibu.sharefile.com/public/share/web-sbab80e3b5c604ae2958f0ae407b2b739

Über WIBU-SYSTEMS AG

WIBU-SYSTEMS AG, www.wibu.com
Elke Spiegelhalter, Presse und Öffentlichkeitsarbeit
Tel.: +49-721-93172-11, elke.spiegelhalter@wibu.com

Wibu-Systems ist ein weltweit führendes Unternehmen in den Bereichen Cybersecurity und Softwarelizenzmanagement. Das Ziel ist, einzigartige, preisgekrönte und international patentierte Sicherheitslösungen zu liefern, die das in digitalen Assets eingebettete geistige Eigentum schützen und die Möglichkeiten der Monetarisierung von technischem Know-how erweitern. Die kompatiblen Hardware- und Softwaremodule der umfassenden CodeMeter Suite bieten Softwareherstellern und Herstellern intelligenter Geräte Schutz vor Piraterie, Reverse Engineering, Manipulationen, Sabotage und Cyberangriffen auf allen gängigen Plattformen und in verschiedenen Branchen.

Bildmaterial auf Anfrage oder https://www.wibu.com/de/pressearchiv.html.

In unseren Social-Media-Kanälen gibt es weitere Informationen: