No-Code-Plattform aus Bonn erhält offiziellen CNA-Status / Strukturiertes Schwachstellenmanagement als Antwort auf NIS2 und KRITIS-Dachgesetz

linqi erhält CNA-Status im CVE-Programm – als einer der wenigen Prozessanbieter weltweit

Bonn, den 03. Juni 2026 | Wer Software in sicherheitsrelevanten Umgebungen betreibt, trägt Verantwortung – auch für potenzielle Schwachstellen und dafür, wie sie erkannt, bewertet und kommuniziert werden. Die linqi GmbH aus Bonn, Anbieter einer No-Code-Plattform zur Prozessautomatisierung für Unternehmen und Behörden, schafft dafür nun die formale Grundlage, die bislang nur wenige Prozessanbieter weltweit erfüllen: **Das CVE™-Programm hat linqi offiziell als CVE Numbering Authority (CNA) autorisiert.** Damit gehört linqi zu den nur 25 Organisationen in Deutschland mit diesem Status und wird Teil eines internationalen Netzwerks aus großen Technologiekonzernen, Open-Source-Projekten und Sicherheitsspezialisten.

Dass das Thema Schwachstellenmanagement aktueller denn je ist, zeigen die Zahlen: Im ersten Quartal 2026 meldete das CVE-Programm – die weltweit führende Datenbank für bekannte IT-Sicherheitslücken – 15.176 CVE Records, ein Plus von 19 % gegenüber dem Vorjahresquartal.[1] Der BSI-Lagebericht 2025 verzeichnete durchschnittlich 119 neu bekannt gewordene Schwachstellen pro Tag – rund 24 % mehr als im Vorjahr.[2] Gleichzeitig wächst der regulatorische Druck: NIS2 und das KRITIS-Dachgesetz erhöhen die Anforderungen an Risikoanalysen, Meldepflichten und ein nachvollziehbares Schwachstellenmanagement – auch in der Lieferkette. Für Unternehmen und Behörden stellt sich damit immer dringlicher die Frage: **Wie stellen Softwareanbieter sicher, dass Schwachstellen erkannt, bewertet und gemeldet werden – und wie lässt sich das überprüfen?**

Prozessautomatisierung mit Verantwortung: linqi schafft Transparenz

Mit der No-Code-Plattform linqi können Unternehmen, Behörden und Konzerne wiederkehrende Geschäftsprozesse – von einfachen Freigabeprozessen bis hin zu vielschichtigen, abteilungs- und systemübergreifenden Abläufen – eigenständig, intuitiv und ohne IT-

[1] CVE Program: *CVE Program Report for Quarter 1 Calendar Year (Q1 CY) 2026*, 12. Mai 2026, https://www.cve.org/Media/News/item/blog/2026/05/12/CVE-Program-Report-for-Q1-2026.
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), 2025: *Lagebericht zur IT-Sicherheit in Deutschland*, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

Kenntnisse digitalisieren und automatisieren. Wer Dokumente und Formulare digitalisiert, Daten strukturiert erfasst und hinter Prozessgestaltungslogiken blickt, um sie zu automatisieren, verarbeitet hochsensible Daten. Der Umgang damit ist für linqi nicht nur eine technische, sondern eine grundsätzliche Frage der Verantwortung.

Was der CNA-Status konkret bedeutet

Das CVE-Programm (Common Vulnerabilities and Exposures) ist der weltweit anerkannte Standard zur Identifikation und Katalogisierung von Sicherheitslücken. Jede Schwachstelle erhält eine eindeutige CVE-ID, damit IT-Teams, Behörden und Sicherheitsdienste international einheitlich darüber kommunizieren und koordiniert reagieren können.

Als CVE Numbering Authority (CNA) ist linqi nun berechtigt, CVE-IDs für Schwachstellen im eigenen Zuständigkeitsbereich eigenständig zu vergeben und in der CVE-Liste zu veröffentlichen, ohne den Umweg über Dritte nehmen zu müssen. Dies setzt voraus, dass das Unternehmen über eigene Ressourcen, definierte Prozesse für den Umgang mit Schwachstellen sowie ein transparentes Vorgehen verfügt, insbesondere im Hinblick auf die eigene Software.

Cybersicherheit: linqi geht über die Mindestanforderungen hinaus

Der CNA-Status steht bei linqi nicht für sich allein. linqi bietet ein Sicherheitsportfolio, das in dieser Form als No-Code-Plattform nicht selbstverständlich ist und aus Überzeugung über die Mindestanforderungen hinausgeht:

- **DSGVO-konform: Entwickelt und gehostet in Deutschland**, ausschließlich in ISO 27001-zertifizierten, georedundanten Rechenzentren
- **Intrusion Detection** und kundenindividuelle Firewalls mit Geofencing
- **SAST (Static Application Security Testing)** – der Quellcode wird kontinuierlich automatisiert auf Schwachstellen geprüft
- **Automatisierte Tests**, Viren- und Malwarescans im laufenden Betrieb
- **WORM-Technologie** zum Schutz vor Ransomware
- **Sekundengenaue In-Point Recovery** und Helpdesk-Reaktionszeit unter einer Stunde
- **Bestandene Penetrationstests der NATO Security**
- **Und jetzt:** CNA-Status im CVE-Programm

„Als Entwickler von linqi tragen wir eine hohe Verantwortung gegenüber unseren Kundinnen und Kunden. Wir verstehen Datensicherheit als grundlegende Voraussetzung für ihr

Vertrauen und sind bereit, dafür auch zusätzliche Schritte zu gehen“, sagt Jörg Sager, CEO von linqi. *„Mit unserem Status als CNA schaffen wir nachvollziehbare Transparenz in Bezug auf unsere selbst definierten Prozesse, Ressourcen und die damit verbundene Kommunikation innerhalb der gesamten Security-Community.“*

Relevanz für linqi-Anwenderinnen und Anwender

Für Organisationen, die linqi einsetzen oder beschaffen, hat der CNA-Status eine konkrete Bedeutung: Er belegt, dass der Anbieter Schwachstellen eigenständig identifizieren, klassifizieren und standardkonform melden kann. Regulatorien wie NIS2 stellen diese Anforderung nicht nur an die Betreiber selbst – die Sorgfaltspflicht für die Lieferkette zieht zunehmend auch Softwareanbieter in die Pflicht. In Ausschreibungen und Sicherheitsaudits wird dieser Nachweis häufig aktiv eingefordert.

Über das CVE-Programm

Die Aufgabe des CVE™-Programms besteht darin, öffentlich bekannt gewordene Sicherheitslücken im Bereich Cybersicherheit zu identifizieren, zu definieren und zu katalogisieren. Für jede Sicherheitslücke im Katalog gibt es einen CVE-Eintrag. Die Sicherheitslücken werden von Organisationen aus aller Welt, die mit dem CVE-Programm zusammenarbeiten, entdeckt, zugeordnet und veröffentlicht. Die Partner veröffentlichen CVE-Einträge, um einheitliche Beschreibungen der Sicherheitslücken zu gewährleisten. Fachleute aus den Bereichen Informationstechnologie und Cybersicherheit nutzen CVE-Einträge, um sicherzustellen, dass sie über dasselbe Problem sprechen, und um ihre Bemühungen zur Priorisierung und Behebung der Sicherheitslücken zu koordinieren.

Über linqi

Die linqi GmbH ist ein 2020 gegründeter No-Code-SaaS-Anbieter aus Bonn. Die Plattform ermöglicht es Unternehmen und Behörden, interne Abläufe ohne Programmierkenntnisse zu digitalisieren und zu automatisieren – von Genehmigungsprozessen über Dokumentenmanagement bis hin zu Compliance-Workflows. Das Hosting erfolgt wahlweise in deutschen, ISO 27001-zertifizierten Rechenzentren, auf eigener Infrastruktur oder an einem frei wählbaren Standort. Über 500.000 aktive Nutzerinnen und Nutzer weltweit setzen linqi ein – in der Industrie, im Gesundheitswesen, in der Finanzbranche und in öffentlichen Einrichtungen. Weitere Informationen: www.linqi.de

Unternehmenskontakt:

linqi GmbH
Markt 26-32
53111 Bonn
Tel.: +49 228 92934510
buero@linqi.de

Pressekontakt:
Sophia Rosenblatt
rheinland relations GmbH
Gottfried-Claren-Str. 5
53225 Bonn
Tel.: +49 (0) 228 / 299 753-14
rosenblatt@rr-pr.com