

Weckruf zur rechten Zeit

Stand: 16. Oktober 2026, 7:29 Uhr - Uwe Steffin

Die deutsche Agrarwirtschaft muss hybride Bedrohungen ernst nehmen.

Kurzfassung

Der jüngste Cyberangriff auf die französische Lebensmittelkühllogistik alarmiert auch die hiesige Agrarwirtschaft. Bundeswehr-General Bodemann fordert angesichts steigender Sabotagegefahren ein radikales Umdenken beim Schutz kritischer Infrastrukturen. Auch zivile Betriebe müssten das „R-hoch-4“-Modell umsetzen: Robustheit der IT, Redundanzen wie Notstrom, materielle Reserven und schnelle Reparaturfähigkeiten.

FRANKFURT. Die zunehmende digitale Vernetzung der Agrar- und Ernährungswirtschaft wird nach Einschätzung von Experten immer mehr zum Sicherheitsrisiko für die zivile Versorgung. Der gezielte Cyberangriff auf Kühlsysteme der Lebensmittellogistik in Frankreich hat jetzt einmal mehr die Verwundbarkeit der Lieferketten offengelegt. Vor diesem Hintergrund fordert Generalleutnant **André Bodemann**, Stellvertreter des Befehlshabers des Operativen Führungskommandos der Bundeswehr, eine fundamentale Kehrtwende beim Schutz der kritischen Infrastruktur (KRITIS) in Deutschland. Im Zentrum des Krisenmanagements müsse ein sogenanntes „R-hoch-4“-Modell stehen, das als direkter Leitfaden auch für die Agrar- und Ernährungswirtschaft diene, erläuterte General Bodemann bei der Herbsttagung von Verbindung Landwirtschaft Industrie (VLI) am Donnerstag (15.10.) in Frankfurt am Main.

Der Sabotageakt in Frankreich verdeutlicht Bodemann zufolge die tückische Dynamik moderner Bedrohungen: Der Angriff erfolgte gezielt in den Nachtstunden, um eine sofortige Entdeckung zu verhindern, und führte zu unterbrochenen Kühlketten, tonnenweise verdorbenen Lebensmitteln sowie vereinzelt Bränden. „Unsere Lebensmittellieferketten werden zunehmend digital integriert und damit automatische Ziele“, warnte der General.

IT-Sicherheit darf kein Randthema mehr sein

Für landwirtschaftliche Betriebe, Genossenschaften, Verarbeiter und den Handel leiten sich aus dem militärischen Konzept Bodemann zufolge vier Kernbereiche für die betriebliche Praxis ab:

- **Robustheit:** Technische Systeme – von Fütterungsanlagen über Melkroboter bis zu digitalen Kühllagern – müssen von Grund auf gegen digitale Angriffe gehärtet werden. IT-Sicherheit darf in der Agrar- und Ernährungswirtschaft kein Randthema mehr sein.
- **Redundanzen:** Bei einem Ausfall der digitalen Steuerung müssen sofort analoge oder physische Ausweichsysteme greifen. Notstromaggregate und manuelle Überbrückungsmöglichkeiten sind essenziell, um einen Totalausfall von Systemen in der Nutztierhaltung oder Frischwarenlogistik zu verhindern.
- **Reserven:** Betriebe müssen materielle und personelle Puffer vorhalten. Da die Datenschutzgrundverordnung (DSGVO) die Abfrage des Reservistenstatus oder der für die Zivilverteidigung relevanten Ehrenämter – von THW bis Freiwillige Feuerwehr – von Mitarbeitern derzeit noch untersagt, empfiehlt Bodemann eine freiwillige

Copyright © by AGRA-EUROPE Presse- und Informationsdienst GmbH

Die Beiträge dieses Dienstes sind urheberrechtlich geschützt. Die Verbreitung, auch durch Film, Funk und Fernsehen, fotomechanische Wiedergabe, Tonträger jeder Art, auszugsweiser Nachdruck oder Einspeicherung und Rückgewinnung in Datenverarbeitungsanlagen jeder Art, ist nur mit Einwilligung des Herausgebers zulässig. Alle Informationen werden sorgfältig recherchiert und aufbereitet. Eine Haftung wird ausgeschlossen. ISSN 0515-6777

Erfassung im Betrieb, um zu wissen, welches Personal im Ernstfall tatsächlich zur Verfügung steht.

- Reparaturfähigkeiten: Wenn Systeme per Cyberangriff kompromittiert werden, zählt jede Minute. Die Agrarwirtschaft muss in der Lage sein, Kernprozesse schnell und autonom instand zu setzen oder auf Notbetrieb umzustellen, ohne auf externe Dienstleister warten zu müssen. AgE