Gastkommentar

Was der Cyberangriff auf Kälteanlagen in Frankreich bedeutet

Von **Gastbeitrag**

Dienstag, 20. Oktober 2026


Dolomitenconsult

Als Geschäftsführer von Dolomitenconsult ist Martin Döbler seit über 25 Jahren in der Gewerbekälte und für dessen Zulieferer in Europa tätig. Aufgrund seiner jahrelangen Tätigkeit für ein französisch-italienisches Unternehmen kennt er die französische Einzelhandelslandschaft näher. Er gilt als Befürworter nachhaltiger und energieeffizienter Maßnahmen im Lebensmittelhandel.

Cyberangriff auf Kälteanlagen: Was der französische Vorfall für den österreichischen Handel bedeutet, lesen Sie in diesem Gastbeitrag:

Als am Vorabend der europäischen Leitmesse für Kältetechnik, der Chillventa in Nürnberg, eine bislang beispiellose Attacke auf Kälteanlagen mehrerer großer französischer Lebensmittelhändler bekannt wurde, sorgte dies auch in der Branche für erhebliche Aufmerksamkeit. Dolomitenconsult nutzte die Messe, um mit Herstellern, Kälteexperten und Anbietern von Steuerungs- und Monitoring-Systemen über die Hintergründe des Vorfalls und die möglichen Konsequenzen für den Handel zu sprechen.

Was ist passiert?

In der Nacht vom 11. auf den 12. Oktober wurden zahlreiche französische Lebensmittelmärkte Ziel eines koordinierten Cyberangriffs. Betroffen waren nach übereinstimmenden Medienberichten und Brancheninformationen Märkte der Gruppen Intermarché/Netto (Groupement Les Mousquetaires), Coopérative U, E.Leclerc, Carrefour und Monoprix.
Die genaue Zahl der betroffenen Standorte ist auch mehrere Tage nach dem Vorfall nicht abschließend bekannt. Dies hängt unter anderem damit zusammen, dass ein Teil der betroffenen Handelsorganisationen als Händlerkooperationen oder Genossenschaften organisiert ist und die einzelnen Märkte von selbstständigen Kaufleuten betrieben werden.
Nach bisher veröffentlichten Informationen stehen bekannte Schwachstellen älterer Steuerungssysteme des Herstellers Danfoss im Verdacht, für den Angriff genutzt worden zu sein. Betroffen waren insbesondere die Controller-Generationen AK-SM800 und AK-SC355, auf denen teilweise veraltete Firmware-Versionen im Einsatz waren. Durch die Manipulation der Anlagen wurde in zahlreichen Fällen die Abtaufunktion aktiviert und dauerhaft aufrechterhalten. In der Folge stiegen die Temperaturen in Kühlmöbeln teilweise auf Werte weit über die zulässigen Lagerbedingungen hinaus.
Die Auswirkungen waren gravierend: Große Mengen verderblicher Ware mussten entsorgt werden. Neben den unmittelbaren Warenverlusten entstanden Kosten für Entsorgung, zusätzliche Personaleinsätze, externe IT- und Kältespezialisten sowie Betriebsunterbrechungen. Branchenkenner gehen insgesamt von Schäden in Millionenhöhe aus.

Was macht diesen Vorfall außergewöhnlich?

Anders als bei klassischen Cyberangriffen standen offenbar weder Datendiebstahl noch finanzielle Erpressung im Vordergrund. Ziel waren physische Infrastrukturen innerhalb des Lebensmittelhandels.
Besonders bemerkenswert ist die Breite des Angriffs. Mehrere Handelsunternehmen einer systemrelevanten Branche wurden nahezu zeitgleich betroffen. Damit rückt eine Entwicklung in den Vordergrund, die Sicherheitsexperten seit Jahren beobachten: Die zunehmende Vernetzung technischer Anlagen schafft neue Angriffsflächen, die weit über klassische IT-Systeme hinausgehen.
Der Vorfall zeigt eindrucksvoll, dass Cyberrisiken heute nicht nur Server und Datenbanken betreffen, sondern auch operative Anlagen mit unmittelbaren Auswirkungen auf Warenverfügbarkeit und Lieferketten.

Hätte man den Angriff verhindern können?

Nach Einschätzung vieler Experten wäre das Risiko deutlich reduzierbar gewesen, wenn die konsequente Umsetzung bewährter Cybersicherheitsmaßnahmen veranlasst worden wäre. Danfoss hat Kunden seit Jahren empfohlen, die Systeme immer mit der neuesten Firmware zu betreiben, Steuerungssysteme hinter Firewalls und über VPN-Verbindungen zu betreiben und nicht mehr unterstützte Systeme zu modernisieren. Für unterstützte Produkte hat das Unternehmen zudem Firmware- und Sicherheitsupdates bereitgestellt. Mehrere Medienberichte legen nahe, dass empfohlene Schutzmaßnahmen teilweise nicht vollständig umgesetzt waren.

Wer steckt hinter dem Angriff?

Derzeit gibt es keine belastbaren Erkenntnisse über die Urheber des Angriffs. Weder liegt ein Bekennerschreiben vor, noch wurden bislang Motive bekannt, die auf klassische Cyberkriminalität wie Erpressung oder finanziellen Betrug schließen lassen.
Fest steht jedoch: Der Vorfall demonstriert, wie verwundbar kritische Versorgungsstrukturen durch digitale Angriffe werden können. Genau deshalb untersuchen die zuständigen Behörden den Fall mit hoher Priorität.
Über die Hintergründe und mögliche politische oder geopolitische Motive kann derzeit nur spekuliert werden. Seriöse Schlussfolgerungen werden erst nach Abschluss der Ermittlungen möglich sein.

Könnte sich ein ähnlicher Vorfall in Österreich ereignen?

Ein Restrisiko lässt sich theoretisch nicht ausschließen. Dennoch ist die Wahrscheinlichkeit dafür in Österreich aufgrund verschiedener Umstände äußerst gering.
Der österreichische Lebensmitteleinzelhandel hat in den vergangenen Jahren massiv in moderne und energieeffiziente Kältetechnik investiert. Der hohe Innovationsdruck durch Energiepreise, Nachhaltigkeitsanforderungen und regulatorische Vorgaben hat dazu geführt, dass moderne Anlagen und Steuerungssysteme deutlich stärker verbreitet sind als in vielen anderen europäischen Märkten.
Darüber hinaus verfügen die großen Handelsunternehmen über etablierte Wartungs-, Monitoring- und Sicherheitsprozesse. Nach Bekanntwerden der Vorfälle in Frankreich wurden die bestehenden Schutzmaßnahmen zusätzlich überprüft und gegebenenfalls angepasst.
Insbesondere bei neueren Anlagen kommen hochentwickelte Steuerungs- und Überwachungssysteme zum Einsatz, die von spezialisierten Herstellern aus Deutschland, Österreich, Italien und weiteren europäischen Ländern geliefert werden.

Welche Lehren kann die Branche daraus ziehen?

Der Vorfall in Frankreich verdeutlicht eine grundlegende Erkenntnis: Sicherheit entsteht nicht durch Hoffnung, sondern durch vorausschauendes Handeln.
Das gilt gleichermaßen für Brandschutz, Einbruchsschutz und Cybersecurity. Investitionen in Prävention sind keine überflüssigen Kosten, sondern ein wesentlicher Bestandteil moderner Unternehmensführung. Gerade bei technischen Infrastrukturen entscheidet häufig nicht die Reaktion auf einen Vorfall, sondern die Qualität der Vorsorge darüber, ob ein Schaden überhaupt entstehen kann.
Für den österreichischen Lebensmittelhandel ist der Fall zugleich eine Bestätigung des eingeschlagenen Weges. Die kontinuierlichen Investitionen in moderne Kälteanlagen, digitale Überwachungssysteme, energieeffiziente Technologien und hochwertige Ladenausstattung erhöhen nicht nur die Nachhaltigkeit, sondern auch die Betriebssicherheit.
Letztlich profitieren davon die Konsumentinnen und Konsumenten. Eine verlässliche Lebensmittelversorgung, hohe Hygienestandards und moderne Technik sind keine Selbstverständlichkeit. Sie sind das Ergebnis langfristiger Investitionen in Qualität, Sicherheit und Infrastruktur.