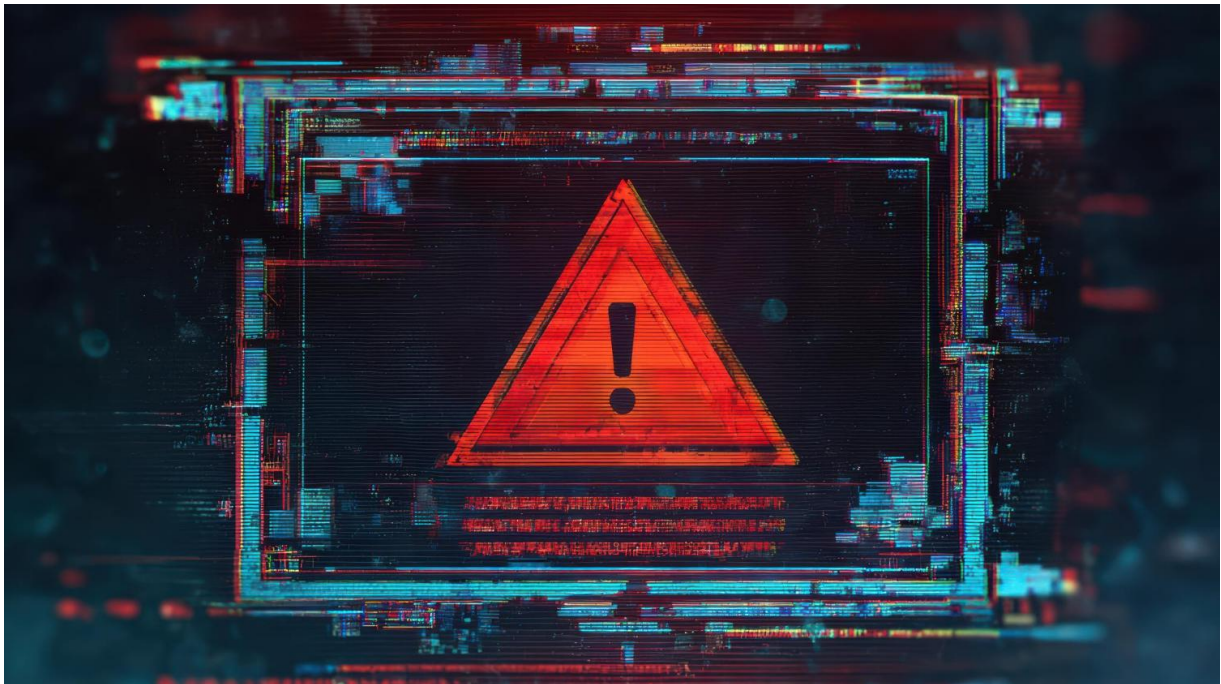


INSIDER PAPER

Französische Supermärkte leiden unter Kühlausfällen nach beispiellosem Cyberangriff

[AFP](#) Veröffentlicht: 12. Oktober 2026, 08:14 Uhr ET



Quelle: Magnific

Wichtigste Erkenntnisse aus dem Insider Paper

- Große französische Supermarktketten wurden von einem beispiellosen Cyberangriff getroffen, der dazu führte, dass Kühlsysteme abtauten und Lebensmittel verdarben.
- Mindestens 300 Intermarché- oder Netto-Filialen, über 100 Cooperative U-Filialen und mehrere E. Leclerc-Filialen waren betroffen.
- Der Angriff zielte auf ältere Kühltürschranksteuerungen von Danfoss mit veralteter Firmware ab, deren Aktualisierung Danfoss schon lange gefordert hatte.
- Nachdem Berichte über Brände im Zusammenhang mit dem Anschlag eingegangen waren, leitete die Pariser Staatsanwaltschaft Ermittlungen ein, und die Behörden alarmierten andere Länder und Lieferanten.

Große französische Supermarktketten gaben am Montag bekannt, dass sie von einem [Cyberangriff](#) betroffen waren, der in Hunderten von Filialen zu einem sprunghaften Anstieg der Temperatur in den Kühltürschränken führte. Dies zwang sie, verdorbene Lebensmittel wegzuerwerfen, und weckte Besorgnis über die Lebensmittelsicherheit.

Die führenden Einzelhändler E. Leclerc, Intermarché und Cooperative U bestätigten gegenüber der AFP, dass sie Opfer eines Cyberangriffs geworden seien, den der Vorstandsvorsitzende von Cooperative U als „beispiellos“ bezeichnete.

„Die Ernährungssicherheit erfordert mehr Aufmerksamkeit auf allen Ebenen“, sagte der EU-Kommissar für Ernährung und Landwirtschaft, Christophe Hansen, auf X und verurteilte den Anschlag. Er erklärte, eine solche „Ausbeutung von Lebensmitteln“ sei mittlerweile „Realität“.

Mindestens 300 Geschäfte von Intermarché oder deren Marke Netto, über 100 Filialen der Cooperative U und mehrere Geschäfte von E. Leclerc wurden angegriffen, teilten die Einzelhändler der AFP in separaten Erklärungen mit.

Die Pariser Staatsanwaltschaft bestätigte den Anschlag, bei dem Berichten zufolge auch andere große Handelsketten betroffen waren, und gab zudem an, dass es zu Bränden gekommen sei.

BFM TV berichtete, dass es Hackern gelungen sei, „in zahlreichen Geschäften die erzwungene Abtauung der Kühlsysteme aus der Ferne auszulösen“.

Die betroffenen Filialen müssen alle frischen und gefrorenen Produkte entsorgen, teilte Intermarché der AFP mit.

Laut der französischen Fachwebsite für den Einzelhandel, jebosseengrandedistribution.fr, seien auch andere Einzelhandelsriesen wie Carrefour Market und Monoprix betroffen, die Unternehmen hätten dies jedoch noch nicht bestätigt.

E. Leclerc bestätigte gegenüber AFP, dass ein Cyberangriff einen seiner Lieferanten von Kühlgeräten betroffen habe, was zu Beeinträchtigungen des Betriebs von Kühlsystemen in mehreren Filialen geführt habe.

Eine mit dem Vorgang vertraute Quelle gab an, dass Kältemittelregelungssysteme des dänischen Herstellers Danfoss im Visier der Angreifer waren.

Danfoss teilte der AFP in einer Erklärung mit, dass es sich bei den meisten betroffenen Geräten um ältere Produkte handele, die „keine Software- oder Sicherheitsupdates mehr erhalten“.

Das Unternehmen gab an, dass insbesondere seine Kühlschranksreglersysteme AK-SM800 und AK-SC355 betroffen seien, wobei eine Version des AK-SM800 veraltete Firmware verwende. Weiter hieß es, man habe Supermärkten schon lange empfohlen, diese Modelle zu aktualisieren. Danfoss machte keine Angaben zur Anzahl der betroffenen Systeme.

– Bemühungen zur Eindämmung des Hackerangriffs –

Eine dem französischen Premierminister Sébastien Lecornu nahestehende Person sagte, die französische Cybersicherheitsbehörde habe bereits „eine Sicherheitslücke in einer von einem dänischen Unternehmen gelieferten Software identifiziert und den Anbieter kontaktiert“.

„Man steht in Kontakt mit seinen europäischen Partnern, da auch andere Länder betroffen sein könnten“, und versucht, „weitere beteiligte französische Unternehmen zu identifizieren, um diese zu warnen“ und „die Ausbreitung zu verhindern“, fügte die Quelle hinzu.

Der Geschäftsführer von Cooperative U, Dominique Schelcher, bezeichnete den Angriff als „beispiellos“ und bestätigte, dass der Cyberangriff seit Sonntagabend Kühlsysteme beeinträchtigt habe.

„Die gezielte Bekämpfung von Geräten, die für die Konservierung frischer Produkte und die Lebensmittelversorgung der französischen Bevölkerung unerlässlich sind, ist äußerst besorgniserregend und beispiellos. Sie ist inakzeptabel“, schrieb er auf X.

Er fügte hinzu, dass die Teams des Unternehmens „vollständig mobilisiert“ seien, um die Situation so schnell wie möglich wiederherzustellen.

„Eine Untersuchung ist notwendig, um diesen Angriff vollständig aufzuklären“, fügte er hinzu.

Die Pariser Staatsanwaltschaft bestätigte gegenüber AFP, dass Ermittlungen zu dem „groß angelegten Cyberangriff auf die Kühlschränke mehrerer großer Lebensmittelhandelsketten in ganz Frankreich“ eingeleitet wurden.

Die Ermittlungen sollen dazu beitragen, „die Opfer zu identifizieren und den Zusammenhang zwischen den von ihnen gemeldeten Schäden in Bezug auf Lebensmittelverluste und Brandausbrüche herzustellen“, teilte die Staatsanwaltschaft mit.

Intermarché verurteilte die durch den Anschlag verursachte Lebensmittelverschwendung und die finanziellen Verluste, ohne jedoch Zahlen zu nennen.

Laut BFM TV wurden die Temperaturen „ferngesteuert verändert, was zur Vernichtung von Vorräten an frischen und gefrorenen Produkten führte“.

– Zunehmende Angst vor hybriden Angriffen –

Der Vorfall ereignet sich vor dem Hintergrund wachsender Besorgnis über das potenzielle Chaos, das in Europa in allen Sektoren durch Cyberangriffe böswilliger Akteure angerichtet werden kann.

Präsident Emmanuel Macron, ein starker Unterstützer der [Ukraine](#) in ihrem Kampf gegen die russische Invasion, ordnete im vergangenen Monat Maßnahmen zum Schutz der kritischen Infrastruktur Frankreichs vor russischen „hybriden Angriffen“ an.

Industrieanlagen wie Kühlturme, die lange Zeit vom Internet isoliert waren, sind jetzt über Sensoren oder Fernüberwachungssysteme vernetzt, sagte Antoine Hautin von der Cybersicherheitsberatungsfirma Almond gegenüber AFP.

Da der Angriff wahrscheinlich Hunderte von Einheiten gleichzeitig betraf, zeugte er von „einem gewissen Maß an Raffinesse“, fügte er hinzu.