cci ZEITUNG

* FÜHRENDE FACHZEITUNG FÜR DIE LÜFTUNGS-, KLIMA-, KÄLTEBRANCHE (LÜKK®)

13
26

23.11.2026
60. Jahrgang / E 55 27
Eine Publikation der cci Dialog GmbH
cci-dialog.de/zeitung

Anzeige

Belimo Webinar-Reihe

Neue Plattform für die interaktive Wissensvermittlung zu Themen der HLK aus der Praxis für alle Fachkräfte.

Mehr Infos und Anmeldung unter
https://cci-dialog.de/belimo-webinare

BELIMO

Cyberangriffe auf Supermarkt-Kühlanlagen decken Sicherheitslücken auf

Attacken durch offene Türen

Ein Cyberangriff auf Kühlanlagen von Hunderten französischen Supermärkten hat gezeigt, wie verwundbar vernetzte Kältetechnik sein kann. Inzwischen ist die Angriffswelle auch nach Deutschland geschwappt. Doch wie lassen sich solche Angriffe verhindern? Wer trägt die Verantwortung für die IT-Sicherheit? Und welche Anforderungen stellt seit kurzem der europäische Cyber Resilience Act (CRA) an die Branche? Ein Blick auf Risiken und Pflichten in einer zunehmend vernetzten Welt.



Cyber Resilience Act für vernetzte Produkte

Seit dem 11. September gibt der europäische Cyber Resilience Act (CRA) in einer ersten Stufe neue Cybersicherheitsanforderungen für Produkte mit digitalen Elementen vor. Davon können auch Steuerungen und Fernüberwachungssysteme vernetzter Kälte-, Klima- und Wärmepumpensysteme betroffen sein. Werden Schwachstellen aktiv ausgenutzt und kommt es zu schwerwiegenden Sicherheitsvorfällen, müssen Hersteller diese gemäß CRA nun melden. Ab dem 11. Dezember 2027 gibt der CRA Herstellern zudem weitere Anforderungen vor, einschließlich grundlegender Cybersicherheitsmaßnahmen vor dem Inverkehrbringen und der Schwachstellenbehandlung während des gesamten Lebenszyklus eines Produkts sowie Transparenz gegenüber den Nutzern. Ziel des Cyber Resilience Act ist es, innerhalb der Europäischen Union die Cybersicherheit zu erhöhen. Er gilt in allen EU-Mitgliedstaaten.

Während sich die Kältetechnikbranche Mitte Oktober auf der Chillventa in Nürnberg getroffen hat, mussten in Frankreich große Mengen aufgetauter Tiefkühlware entsorgt werden. Grund dafür war, dass Hacker die Kühlgeräte hunderter Supermärkte in einen kontinuierlichen Abtauzyklus gezwungen hatten. Als Einfallstore nannte die französische Melde- und Koordinierungsstelle für Cybersicherheitsvorfälle CERT-FR explizit Steuerungen von Danfoss und Systeme von Copeland. Inzwischen ist die Angriffswelle über die Beneluxländer und Schweden auch nach Deutschland geschwappt.

Die Frage ist: Wie kann das sein? Die Antwort: viel zu einfach. Gegenüber cci Zeitung hat Danfoss mitgeteilt, dass in Frankreich Controller verwendet wurden, auf denen keine aktuelle Firmware installiert gewesen sei. Zudem habe es weder eine Firewall noch eine VPN-Verbindung zur Absicherung gegeben. Das widerspricht grundsätzlich anerkannten Sicherheitspraktiken, erklärt dazu die CERT-FR. Copeland weist zudem darauf hin, dass Lebensmittel-Tiefkühlanlagen teils länger laufen, als Sicherheitsupdates für ihre Software bereitgestellt werden.

Über die Motive für die Attacken ist bislang nichts bekannt. Ein finanzieller Gewinn ist nicht erkennbar. Hier wird offensichtlich die Einladung zur Destabilisierung angenommen und Schaden angerichtet. Die Vorfälle zeigen: Vernetzte Kälteanlagen bieten zwar Vorteile bei Wartung, Energieverbrauch und Überwachung, öffnen aber auch Türen für Angriffsmöglichkeiten – und das nicht nur im Lebensmitteleinzelhandel. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Betreibern vernetzter Anlagen: direkten Zugriff aus dem Internet unterbinden, Zugriffe absichern, Systeme aktuell halten und Sicherheitsmaßnahmen zur Routine machen.

Doch wer ist dafür verantwortlich? Als Experte für den Lebensmitteleinzelhandel sagt Prof. Carsten Kortum von der Dualen Hochschule Baden-Württemberg (DHBW) Heilbronn dazu: „Die Verantwortung verteilt sich auf mehrere Beteiligte. Beim Handelsunternehmen liegt die organisatorische Verantwortung, Wartungs- und IT-Dienstleister müssen Fernzugänge absichern und Hersteller sind für die Sicherheit ihrer Produkte verantwortlich.“ Wer im Schadensfall hafte, hänge von vertraglichen Vereinbarungen und von der Schadensursache ab.

Ironie des Schicksals: Nur zwei Tage vor dem Bekanntwerden der Vorfälle in Frankreich hatte das BSI eine Empfehlung mit einfachen Maßnahmen zum Schutz internetverbundener OT-Systeme vor Cyberangriffen veröffentlicht. Was bleibt, ist die simple Erkenntnis, dass bei vernetzten Anlagen jederzeit größtmögliche Sorgfalt in Sachen Cybersicherheit geboten ist. Und das nicht nur bei solchen zur Kühlung von Lebensmitteln, sondern umso mehr, wenn es um Kritische Infrastruktur (KRITIS) geht. Auch dort hat es schon Cyberattacken gegeben, berichtet das BSI. (RP)

Anzeige



IN DIESER AUSGABE

NACHBERICHT CHILLVENTA 2026
Produkte, Kommentare, Branchengeschehen, 5

CHILLVENTA-STANDGEPLAUDER
Eindrücke von den Ausstellern vor Ort 18

CHILLVENTA-KONGRESS
Impulse für die Zukunft 24

GMODG-SERIE
Energetische Renovierung von Nichtwohngebäuden 25

NORM IM FOKUS
Neufassung der DIN EN 16798 Teil 3 27