NEDIK

An die Mitglieder des SVK
Schweizerischer Verband für Kältetechnik

Zürich, 12. November 2026

Cyberangriffe auf gewerbliche Kälteanlagen – wichtige Hinweise und Sofortmassnahmen

Sehr geehrte Damen und Herren,

Seit Mitte Oktober werden in mehreren europäischen Ländern und inzwischen auch in der Schweiz gewerbliche Kälteanlagen gezielt über das Internet angegriffen. Die Angreifer übernehmen die Steuerung, schalten die Kühlung ab und lassen die Anlagen aufheizen, teils auf weit über 50 °C. Die Folgen sind verdorbene Ware und Sachschäden. Betroffen sind zunehmend auch kleine Betriebe.

Die Voraussetzung für derartige Angriffe ist, dass die Steuerung der Kälteanlage über einen Netzwerkzugang, zum Beispiel aus dem Internet, erreichbar ist. Die Angreifer können gezielt Einstellungen des Steuerungsmechanismus angreifen und verändern, sodass die Anlage nicht mehr kühlt, sondern heizt.

Empfohlenes Vorgehen

- Internet- und Fernzugriff: Wenn die Anlage über einen Netzwerkzugang oder einen Internetzugang verfügt, sollte mit der Fachverantwortlichen Person geprüft werden, ob die Steuerung bis zu weiteren Prüfungen vom Netzwerk getrennt werden kann. Die Steuerung darf nicht direkt aus dem Internet erreichbar sein. Der Fernzugriff auf die Anlagen sollte nur über einen abgesicherten Netzwerkzugang erfolgen. Wenn dies kurzfristig nicht möglich ist, trennen Sie die Netzwerkverbindung der Steuerung, bis Sie geeignete Massnahmen getroffen haben. Die Kühlung läuft in der Regel lokal weiter.
- Zugangsdaten zur Kälteanlage: Stellen Sie sicher, dass der Zugang zu Ihrem System den heutigen Sicherheitsstandards entspricht (z. B. Standardpasswörter ersetzen, individuelle, starke Passwörter setzen, wo möglich Zwei-Faktor-Authentisierung nutzen und Zugänge von Dienstleistern prüfen).
- Geräte absichern: Stellen Sie zusammen mit dem Hersteller oder der zuständigen Fachperson sicher, dass Ihre Anlage auf dem aktuellen Stand ist. Dazu gehört, aktuelle Software einzuspielen, Geräte ohne Herstellersupport zu ersetzen oder in einem eigenen, abgeschotteten Netz zu betreiben, getrennt von der Büro-IT. Das Einspielen von Updates allein genügt nicht.
- Temperaturalarm unabhängig sicherstellen: Grenzwerte festlegen und die Alarmierung (z. B. per SMS) über ein von der Steuerung unabhängiges Gerät führen. Eine zuständige Person muss erreichbar sein und das Notfallkonzept kennen (Ausweich- bzw. Notkühlung).
- Sicherheitskonzept erarbeiten: Da immer wieder neue Schwachstellen entdeckt werden können, ist es wichtig, mit der IT-Fachperson ein Sicherheitskonzept auszuarbeiten.

Bei Verdacht auf einen Angriff

Ziehen Sie sofort den Kältefachbetrieb und die IT-Fachperson bei, betreiben Sie die Anlage wenn möglich manuell und sichern Sie die digitalen Spuren (Protokolle, Einstellungen) und setzen Sie das Gerät nicht zurück. Melden Sie den Vorfall umgehend der Polizei: bei laufendem Schaden über den Notruf 117, sonst über Ihre örtliche Polizeidienststelle.

Das Bundesamt für Cybersicherheit (BACS) hat eine Warnung mit weiteren Schutzmassnahmen veröffentlicht: www.bacs.admin.ch/de/warnung-kuehlanlagen-de.

Weitere Hinweise zum Thema Cyberkriminalität finden Sie auf cybercrimepolice.ch/de.

Freundliche Grüsse
Ihre Polizei / NEDIK (Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung)