

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 12.10.2026, 16:09 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	12.10.2026
Herausgeber	Maximilian Gilg, OT-Cyber.de, Rosenheim
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen
Online	https://ot-cyber.de/ot-lage/

Dieses Lagebild fasst öffentlich zugängliche Meldungen zusammen – automatisch zusammengestellt, ohne Gewähr. Die Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen in Deutschland, Österreich und der Schweiz.

Management Summary

Diese Ausgabe enthält 5 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

- **Kühlsteuerungen in französischen Supermärkten aus der Ferne verstellt

GESAMTBEWERTUNG

Hoch – vorrangig die Meldungen mit hoher Relevanz prüfen und umsetzen.

Lageübersicht

ID	Meldung	Relevanz
L-01	**Kühlsteuerungen in französischen Supermärkten aus der Ferne verstellt	HOCH
L-02	**Citrix NetScaler: weitere kritische Lücke CVE-2026-107406 bei SAML-Konfiguration (09.10.)**	MITTEL
L-03	**Windows 11 24H2: Patchday am 13.10. ist das letzte Update für Home und Pro**	MITTEL
L-04	**Update Japan: Bericht über einen „Notstand im Cyberraum“ nach einer Welle von Cyberangriffen (09.10.)**	MITTEL
L-05	**Erpressergruppe Redact (früher BlackFile) setzt auf Anrufe beim Helpdesk**	GERING

Meldungen im Detail

L-01 ****Kühlsteuerungen in französischen Supermärkten aus der Ferne verstellt**

Relevanz: **HOCH**

Sollwert bis 50 °C (11./12.10.)** – In der Nacht vom 11. auf den 12.10. wurden in Supermärkten mehrerer französischer Ketten die Kühl- und Tiefkühlschränke aus der Ferne verstellt. Les Mousquetaires (Intermarché) bestätigt gegenüber Radio France, dass die Temperatur auf 50 °C gestellt wurde; laut Les Mousquetaires wurde der Dienstleister Danfoss, der die Kühlschränke betreut, selbst Opfer des Angriffs. Coopérative-U-Chef Dominique Schelcher hat den Angriff bestätigt. Laut RTBF sind 150 bis 200 Intermarché-Märkte und weniger als etwa 100 Verkaufsstellen von Coopérative U betroffen, Frisch- und Tiefkühlware musste entsorgt werden. Die Pariser Staatsanwaltschaft ermittelt (OFAC) und nennt neben Warenverlusten auch Brandausbrüche. Danfoss gab laut Infosecurity Magazine zunächst kein Statement ab; Täter und Angriffsweg sind offen. Unsere Einschätzung: Kältetechnik ist OT – verstellte Sollwerte und eine dauerhaft ausgelöste Abtauung reichen für hohen Schaden. Betreiber von Supermärkten, Kühlhäusern und Lebensmittel-Produktionsstätten in DACH sollten prüfen, wer per Fernwartung auf ihre Kühlregler zugreifen kann (SANS Critical Control 4, Secure Remote Access). Laufender Stand im Vorfall-Lagebild: <https://ot-cyber.de/blog/vorfall-lagebild-hacker-stellen-danfoss-supermarktkuehlung-auf-50-c.html> –

Quelle: <https://www.infosecurity-magazine.com/news/french-supermarket-chains/>

Quelle: https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/des-magasins-systeme-u-et-intermarche-touche-par-une-cyberattaque-contre-leurs-installations-frigorifiques_8233720.html

Quelle: <https://www.rtbf.be/article/ils-ont-declenche-a-distance-le-degivrage-des-frigos-des-supermarches-francais-victimes-d-une-cyberattaque-sur-les-installations-frigorifiques-11798842>

L-02 ****Citrix NetScaler: weitere kritische Lücke CVE-2026-107406 bei SAML-Konfiguration (09.10.)****

Relevanz: **MITTEL**

Ein Speicherüberlauf kann laut BleepingComputer zu Remote Code Execution oder Denial of Service führen. Betroffen sind NetScaler ADC und Gateway, die als SAML Identity Provider (IdP) oder Service Provider (SP) eingerichtet sind. Behoben ist die Lücke ab 14.1-73.46 und 13.1-64.29, in den FIPS/NDcPP-Versionen ab 13.1.37.283. Citrix ist keine Ausnutzung bekannt. Shadowserver zählt über 21.000 IP-Adressen mit NetScaler-Fingerprint im Internet. Unsere Einschätzung: Wer NetScaler mit SAML als Remote-Access-Gateway nutzt, sollte den Versionsstand prüfen – auch wenn nach den Patch-Runden vom 27.09. und 04.10. schon aktualisiert wurde. Einordnung der ganzen Welle im Lagebild: <https://ot-cyber.de/blog/vorfall-lagebild-citrix-netscaler-adc-gateway-zwei-zero-days-mit-rem.html> –

Quelle: <https://www.bleepingcomputer.com/news/security/citrix-warns-admins-to-patch-new-netscaler-rce-flaw-immediately/>

L-03 **Windows 11 24H2: Patchday am 13.10. ist das letzte Update für Home und Pro**

Relevanz: MITTEL

Laut BleepingComputer endet die Versorgung mit Updates für Windows 11, Version 24H2, in den Editionen Home und Pro mit dem Patchday am 13.10.2026, danach gibt es keine Patches mehr; Enterprise und Education erhalten Updates bis 12.10.2027. Unsere Einschätzung: Prüfen Sie, ob auf Engineering-Workstations, HMI- oder Leitstellen-PCs eine Home- oder Pro-Edition mit 24H2 läuft – diese Rechner bekommen nach dem Patchday am 13.10. keine Patches mehr (SANS Critical Control 5, Risk-Based Vulnerability Management).

Quelle: <https://www.bleepingcomputer.com/news/microsoft/windows-11-24h2-home-and-pro-reach-end-of-support-in-90-days/>

L-04 **Update Japan: Bericht über einen „Notstand im Cyberraum“ nach einer Welle von Cyberangriffen (09.10.)**

Relevanz: MITTEL

Laut Gizmodo, das sich auf die Financial Times beruft, hat Japan nach einer Welle von Cyberangriffen auf wichtige Unternehmen einen „state of emergency in cyberspace“ ausgerufen. Gizmodo berichtet außerdem mit Bezug auf die Nachrichtenagentur Kyodo und die Nationale Polizeibehörde, dass mindestens 53 Unternehmen in Japan von Ransomware getroffen wurden; betroffen sind laut Berichten auch Organisationen aus Fertigung, Bau, Krankenhäusern und Schulen. Ein eigener Fall: Keio Railway hat am 26.09. einen Ransomware-Angriff auf Geschäftssysteme einzelner Konzernfirmen bestätigt; laut Keio gab es keine Störungen im Zugbetrieb. Unsere Einschätzung (eigene Einordnung): Die Häufung zeigt, wie viele Firmen Ransomware treffen kann – Betreiber in DACH sollten den Ausfall von Geschäfts-IT und von Dienstleistern in ihrem Incident-Response-Plan durchspielen, damit die Anlage weiterläuft (SANS Critical Control 1, ICS Incident Response).

Quelle: <https://gizmodo.com/we-have-entered-a-cybersecurity-hellscape-japan-warns-2000824268>

Quelle: <https://gbhackers.com/keio-railway-confirms-ransomware-attack/>

L-05 **Erpressergruppe Redact (früher BlackFile) setzt auf Anrufe beim Helpdesk**

Relevanz: GERING

Laut Cybermaxx geben sich die Angreifer am Telefon als IT oder Helpdesk aus und locken Mitarbeiter auf gefälschte MFA- oder Passkey-Seiten. Danach greifen sie auf Cloud-Dienste wie Microsoft 365, SharePoint und OneDrive zu, stehlen Daten und erpressen damit, verschlüsseln aber keine Systeme. Unsere Einschätzung (eigene Übertragung, Stadtwerke sind kein belegtes Ziel der Gruppe): Auch für Betreiber wie Stadtwerke in DACH lohnt sich ein Blick darauf, wie der Helpdesk Passwörter und MFA zurücksetzt – ein Rückruf über eine bekannte Nummer erschwert diese Masche deutlich.

Quelle:

<https://www.cybermaxx.com/resources/blackfile-becomes-redact-private-equity-firms-face-data-extortion/>

Einordnung und Unterstützung: OT-Cyber.de · Am Esbaum 12, 83022 Rosenheim · +49 8031 8603164 · akademie@ot-cyber.de · <https://ot-cyber.de/>