

**L A G E B I L D**

# OT-/Cyber-Lagebild

Ausgabe 25.10.2026, 16:10 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

|                        |                                                                           |
|------------------------|---------------------------------------------------------------------------|
| <b>Zielgruppe</b>      | Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS |
| <b>Datum</b>           | 25.10.2026                                                                |
| <b>Herausgeber</b>     | Maximilian Gilg, OT-Cyber.de, Rosenheim                                   |
| <b>Klassifizierung</b> | TLP:CLEAR – ausschließlich öffentliche Quellen                            |
| <b>Online</b>          | <a href="https://ot-cyber.de/ot-lage/">https://ot-cyber.de/ot-lage/</a>   |

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 4 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

- **\*\*Update: ConnectWise: Microsoft ordnet den Angriff der China-nahen Gruppe Storm-0940 zu (21./22.10.)\*\***: Microsoft geht davon aus, dass Storm-0940 hinter dem Supply-Chain-Angriff steckt. Die Gruppe ist staatsnah zu China und automatisierte die Angriffe mit dem KI-Pentest-Framework ARTEX. Betroffen ist eine Multi-Tenant-Anwendung von ConnectWise. Laut The Record blieb der Großteil der Angriffe nach Angaben von Microsoft erfolglos, eingedrungen ist die Gruppe dennoch bei vielen Organisationen, unter anderem aus Energie und Fertigung. Microsoft hat dazu Hinweise zur Absicherung veröffentlicht. Unsere Einschätzung: Stadtwerke und Dienstleister, die ConnectWise nutzen, sollten ihre Cloud- und Admin-Logs (z. B. Entra ID) zeitnah prüfen. Quellen: <https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/> · <https://therecord.media/china-cyber-connectwise-ai>

### GESAMTBEWERTUNG

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

## Lageübersicht

| ID   | Meldung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Relevanz |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| L-01 | <p><b>**BlackX-UEFI-Bootkit umgeht Secure Boot über „Baton Drop“ (CVE-2022-21894) (22./24.10.)**</b>: Kaspersky hat das Bootkit analysiert. Laut Kaspersky waren die angegriffenen Rechner vollständig gepatcht. Das Bootkit kam trotzdem durch, weil der Patch das Zertifikat „Windows Production PCA 2011“ nicht automatisch sperrt: Die Secure-Boot-Sperrung (Revocation) muss von Hand aktiviert werden. Das Zertifikat ist am 19.10.2026 abgelaufen, die anfälligen Boot-Dateien laden aber weiter, solange es nicht auf der Sperrliste steht. Ziele waren bisher diplomatische Stellen in Tadschikistan, Usbekistan und Turkmenistan, die Zuordnung zu APT41 gibt Kaspersky mit „medium confidence“ an. Unsere Einschätzung: Versorger sollten auf Windows-Engineering-Workstations, HMI- und SCADA-Servern prüfen, ob die Secure-Boot-Sperrungen aktiv sind. Patchen allein genügt hier nicht. Quellen: <a href="https://securelist.com/uefi-bootkit-blackx/121539/">https://securelist.com/uefi-bootkit-blackx/121539/</a> · <a href="https://www.bleepingcomputer.com/news/security/blackx-uefi-bootkit-exploits-baton-drop-flaw-to-bypass-secure-boot/">https://www.bleepingcomputer.com/news/security/blackx-uefi-bootkit-exploits-baton-drop-flaw-to-bypass-secure-boot/</a> · <a href="https://techcommunity.microsoft.com/blog/windows-it-pro-blog/revoking-vulnerable-windows-boot-managers/4121735">https://techcommunity.microsoft.com/blog/windows-it-pro-blog/revoking-vulnerable-windows-boot-managers/4121735</a></p> | MITTEL   |

| ID   | Meldung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Relevanz |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| L-02 | <p><b>**Kanton St. Gallen beschließt Strategie zum Schutz kritischer Infrastrukturen (SKIPD) (22.10.)**:</b> Die Regierung hat die Schutzstrategie für kritische Infrastrukturen, Prozesse und Dienstleistungen verabschiedet. Vorrang haben eine kantonale SKIPD-Koordinationsstelle als zentrale Anlaufstelle und kantonale Rechtsgrundlagen, die die Aufgaben von Kanton, Gemeinden und Betreibern festlegen. In einem Folgeprojekt sollen Leitfäden und Checklisten für Betreiber, ein gemeinsames Lagebild sowie gemeinsame Planungen und Übungen folgen. Als Beispiele für Bedrohungen nennt der Kanton einen Cyberangriff auf ein IT-System, Trinkwasserknappheit und Medikamentenengpässe. Unsere Einschätzung: Für Wasserversorger und Elektrizitätswerke im Kanton St. Gallen kommt mehr Abstimmung mit dem Kanton. Konkrete Cyber-Vorgaben nennt die Mitteilung noch nicht, sie dürften erst mit dem Folgeprojekt kommen. Quellen: <a href="https://www.sg.ch/news/sgch_allgemein/2026/10/koordinierter-schutz-fuer-kritische-infrastrukturen.html">https://www.sg.ch/news/sgch_allgemein/2026/10/koordinierter-schutz-fuer-kritische-infrastrukturen.html</a> · <a href="https://www.polizeinews.ch/2026/10/25/medikamentenengpaesse-cyberangriffe-wassermangel-kanton-verstaerkt-schutz/">https://www.polizeinews.ch/2026/10/25/medikamentenengpaesse-cyberangriffe-wassermangel-kanton-verstaerkt-schutz/</a></p> | MITTEL   |
| L-03 | <p><b>**Update: ConnectWise: Microsoft ordnet den Angriff der China-nahen Gruppe Storm-0940 zu (21./22.10.)**:</b> Microsoft geht davon aus, dass Storm-0940 hinter dem Supply-Chain-Angriff steckt. Die Gruppe ist staatsnah zu China und automatisierte die Angriffe mit dem KI-Pentest-Framework ARTEX. Betroffen ist eine Multi-Tenant-Anwendung von ConnectWise. Laut The Record blieb der Großteil der Angriffe nach Angaben von Microsoft erfolglos, eingedrungen ist die Gruppe dennoch bei vielen Organisationen, unter anderem aus Energie und Fertigung. Microsoft hat dazu Hinweise zur Absicherung veröffentlicht. Unsere Einschätzung: Stadtwerke und Dienstleister, die ConnectWise nutzen, sollten ihre Cloud- und Admin-Logs (z. B. Entra ID) zeitnah prüfen. Quellen: <a href="https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/">https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/</a> · <a href="https://therecord.media/china-cyber-connectwise-ai">https://therecord.media/china-cyber-connectwise-ai</a></p>                                                                                                                                                                                                                                   | HOCH     |
| L-04 | <p><b>**Windows Server 2016: Support endet am 12.01.2027 (23.10.)**:</b> Microsoft beendet den Extended Support für Windows Server 2016 am 12.01.2027, das ist der Januar-Patchday. Laut Microsoft ist das Januar-Update 2027 das letzte Sicherheitsupdate für diese Version. Unsere Einschätzung: In OT-Umgebungen finden sich häufig noch Leittechnik-, SCADA- und Historian-Server auf Windows Server 2016 oder älter. Jetzt ist ein guter Zeitpunkt, das Asset-Inventar zu prüfen und Migration oder Segmentierung zu planen. Quellen: <a href="https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2016">https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2016</a> · <a href="https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-2016-reaches-end-of-support-in-january/">https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-2016-reaches-end-of-support-in-january/</a> · <a href="https://www.microsoft.com/en-us/windows-server/blog/2026/02/25/planning-ahead-for-windows-server-2016-end-of-support/">https://www.microsoft.com/en-us/windows-server/blog/2026/02/25/planning-ahead-for-windows-server-2016-end-of-support/</a></p>                                                                                                                                                                                                    | MITTEL   |

## Meldungen im Detail

**L-01 \*\*BlackX-UEFI-Bootkit umgeht Secure Boot über „Baton Drop“ (CVE-2022-21894) (22./24.10.)\*\*:** Kaspersky hat das Bootkit analysiert. Laut Kaspersky waren die angegriffenen Rechner vollständig gepatcht. Das Bootkit kam trotzdem durch, weil der Patch das Zertifikat „Windows Production PCA 2011“ nicht automatisch sperrt: Die Secure-Boot-Sperrung (Revocation) muss von Hand aktiviert werden. Das Zertifikat ist am 19.10.2026 abgelaufen, die anfälligen Boot-Dateien laden aber weiter, solange es nicht auf der Sperrliste steht. Ziele waren bisher diplomatische Stellen in Tadschikistan, Usbekistan und Turkmenistan, die Zuordnung zu APT41 gibt Kaspersky mit „medium confidence“ an. Unsere Einschätzung: Versorger sollten auf Windows-Engineering-Workstations, HMI- und SCADA-Servern prüfen, ob die Secure-Boot-Sperrungen aktiv sind. Patchen allein genügt hier nicht. Quellen:

<https://securelist.com/uefi-bootkit-blackx/121539/> · <https://www.bleepingcomputer.com/news/security/blackx-uefi-bootkit-exploits-baton-drop-flaw-to-bypass-secure-boot/> · <https://techcommunity.microsoft.com/blog/windows-itpro-blog/revoking-vulnerable-windows-boot-managers/4121735>

Relevanz: MITTEL

**L-02 \*\*Kanton St. Gallen beschließt Strategie zum Schutz kritischer Infrastrukturen (SKIPD) (22.10.)\*\*:** Die Regierung hat die Schutzstrategie für kritische Infrastrukturen, Prozesse und Dienstleistungen verabschiedet. Vorrang haben eine kantonale SKIPD-Koordinationsstelle als zentrale Anlaufstelle und kantonale Rechtsgrundlagen, die die Aufgaben von Kanton, Gemeinden und Betreibern festlegen. In einem Folgeprojekt sollen Leitfäden und Checklisten für Betreiber, ein gemeinsames Lagebild sowie gemeinsame Planungen und Übungen folgen. Als Beispiele für Bedrohungen nennt der Kanton einen Cyberangriff auf ein IT-System, Trinkwasserknappheit und Medikamentenengpässe. Unsere Einschätzung: Für Wasserversorger und Elektrizitätswerke im Kanton St. Gallen kommt mehr Abstimmung mit dem Kanton. Konkrete Cyber-Vorgaben nennt die Mitteilung noch nicht, sie dürften erst mit dem Folgeprojekt kommen. Quellen: [https://www.sg.ch/news/sgch\\_allgemein/2026/10/koordinierter-schutz-fuer-kritische-infrastrukturen.html](https://www.sg.ch/news/sgch_allgemein/2026/10/koordinierter-schutz-fuer-kritische-infrastrukturen.html) · <https://www.polizeinews.ch/2026/10/25/medikamentenengpaesse-cyberangriffe-wassermangel-kanton-verstaerkt-schutz/>

Relevanz: MITTEL

**L-03 \*\*Update: ConnectWise: Microsoft ordnet den Angriff der China-nahen Gruppe Storm-0940 zu (21./22.10.)\*\*:** Microsoft geht davon aus, dass Storm-0940 hinter dem Supply-Chain-Angriff steckt. Die Gruppe ist staatsnah zu China und automatisierte die Angriffe mit dem KI-Pentest-Framework ARTEX. Betroffen ist eine Multi-Tenant-Anwendung von ConnectWise. Laut The Record blieb der Großteil der Angriffe nach Angaben von Microsoft erfolglos, eingedrungen ist die Gruppe dennoch bei vielen Organisationen, unter anderem aus Energie und Fertigung. Microsoft hat dazu Hinweise zur Absicherung veröffentlicht. Unsere Einschätzung: Stadtwerke und Dienstleister, die ConnectWise nutzen, sollten ihre Cloud- und Admin-Logs (z. B. Entra ID) zeitnah prüfen. Quellen: <https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/> · <https://therecord.media/china-cyber-connectwise-ai>

Relevanz: HOCH

**L-04 \*\*Windows Server 2016: Support endet am 12.01.2027 (23.10.)\*\*:** Microsoft beendet den Extended Support für Windows Server 2016 am 12.01.2027, das ist der Januar-Patchday. Laut Microsoft ist das Januar-Update 2027 das letzte Sicherheitsupdate für diese Version. Unsere Einschätzung: In OT-Umgebungen finden sich häufig noch Leittechnik-, SCADA- und Historian-Server auf Windows Server 2016 oder älter. Jetzt ist ein guter Zeitpunkt, das Asset-Inventar zu prüfen und Migration oder Segmentierung zu planen. Quellen: <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2016> · <https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-2016-reaches-end-of-support-in-january/> · <https://www.microsoft.com/en-us/windows-server/blog/2026/02/25/planning-ahead-for-windows-server-2016-end-of-support/>

Relevanz: MITTEL

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