Incident Brief: Osaki Electric Confirms Data Transfer After Ransomware Attack

The Japanese manufacturer says internal data was transmitted externally and plans a phased production restart; the scope of the information remains under investigation.

Vladimir Tsakanyan, Ph.D. · Center for Cyber Diplomacy and International Security

November 26, 2026

Cover image: AI-generated conceptual illustration; it does not depict Osaki’s actual facility or the incident.

Japan’s Osaki Electric said on November 25 that data had been transmitted from its internal systems to an external destination following a ransomware attack confirmed on November 17. The company said the content and scope of the transferred information, including whether personal information was involved, remained under investigation. [1]

Osaki plans to restart production in stages from November 27, subject to safety verification. It separately estimated that shipments for existing orders would resume from December 1; those dates are plans and may change. The company said the incident did not affect its production equipment and that it had identified no impact on products and services already in customers’ use. [1]

The manufacturer said unauthorized access also affected a group company through the same VPN device. It is working with external specialists and says it has consulted police and other relevant authorities. The disruption illustrates how an intrusion into business systems can interrupt manufacturing operations without establishing that production equipment itself was compromised. [1]

Sources and links

[1] Osaki Electric: Third report on ransomware and production resumption, November 25, 2026

https://www.osaki.co.jp/en/ir/news/auto_20261125586209/pdfFile.pdf

Read the original article online

https://cybercenter.space/insights/osaki-electric-ransomware-data-transfer-production-restart-november-2026/