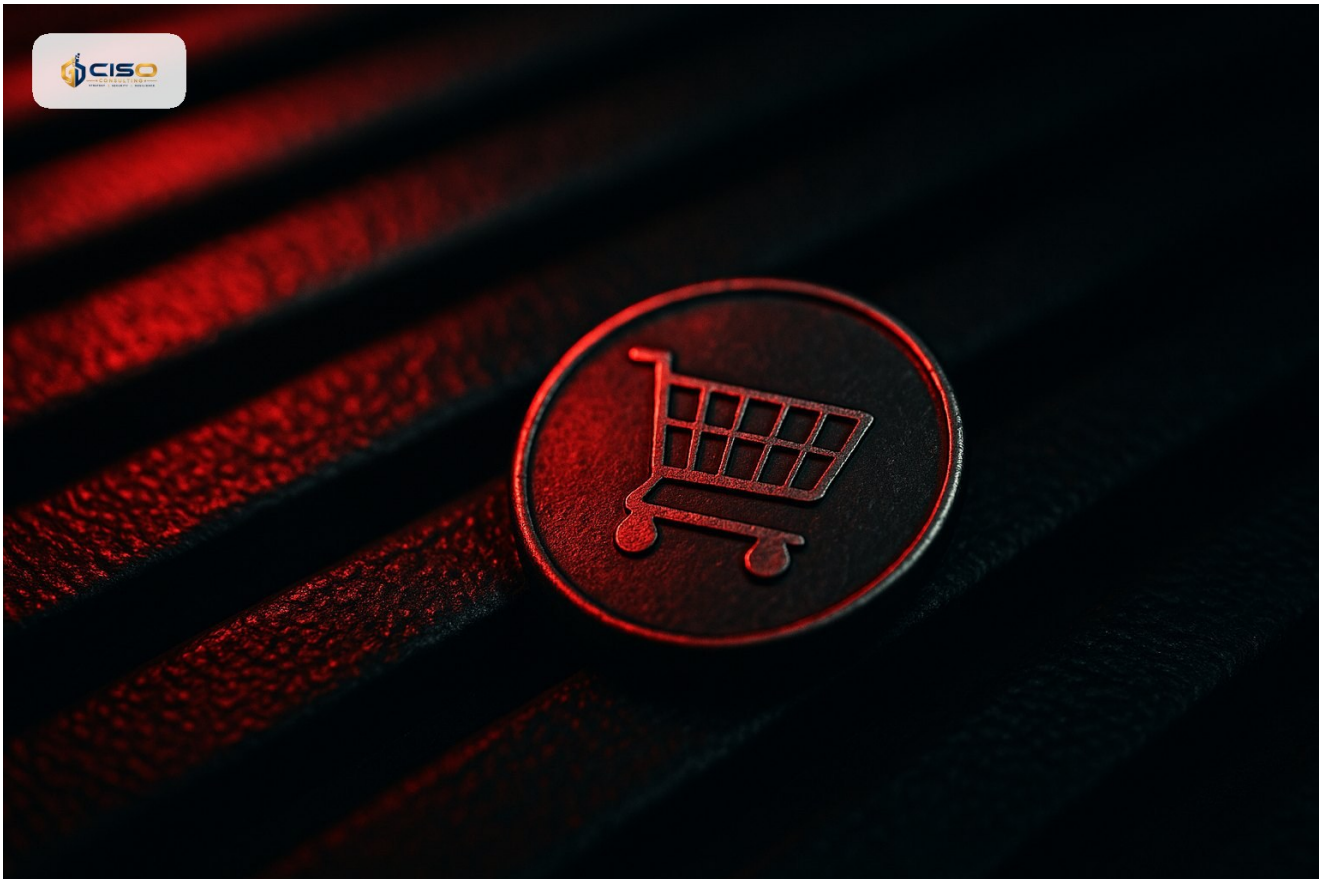


Ahold Delhaize Takes Systems Offline Following Cyberattack



Global retail giant Ahold Delhaize confirmed a cybersecurity incident forcing it to take systems offline, disrupting employee access and customer-facing platforms across multiple markets.

- Ahold Delhaize, operating over 9,400 stores globally with \$104 billion in annual sales, confirmed a cybersecurity incident on 12 October 2026
- The company took systems offline as a protective measure while stores remain open to customers
- Employees at Stop & Shop cannot access schedules or pay stubs; customer platforms disrupted at Albert Heijn, Etos, Gall & Gall and Delhaize stores
- Internal memos describe IT outages affecting order fulfilment capabilities at Food Lion locations
- This is the second major incident for Ahold Delhaize following a November 2024 ransomware attack affecting 2.2 million individuals

Incident Overview

Ahold Delhaize, one of the world's largest food retail chains, confirmed on 12 October 2026 that it experienced a **cybersecurity incident** requiring the company to take systems offline as a protective measure. The multinational retailer operates more than 9,400 stores across Europe, the United States and Indonesia, employs nearly 400,000 people, and serves approximately 60 million customers weekly. The company reported net sales exceeding \$104 billion in 2024.

In a brief statement, Ahold Delhaize said its teams are working to assess and mitigate the issue and that stores remain open and serving customers. The company stated that protecting its infrastructure in the best interest of customers, associates and partners is a top priority.

Operational Impact

The incident has caused disruptions across multiple markets. Employees at the Stop & Shop chain in the United States are unable to access their schedules and pay stubs. Customer-facing platforms including websites, apps and customer service systems are unavailable at Albert Heijn, Etos and Gall & Gall stores in the Netherlands, and at Delhaize locations in Belgium.

Internal communications at Food Lion stores in the United States described the situation as an IT outage, warning employees that stores may be unable to shop, stage or hand off orders. The company declined to provide details on whether the incident affected both corporate and store systems, the geographic scope of disruptions, or whether devices were encrypted.

Previous Incident

This marks the second significant cybersecurity event for Ahold Delhaize in recent years. In November 2024, the ransomware group INC Ransom compromised the company's U.S. systems, stealing personal, financial and health information belonging to more than 2.2 million individuals.

What to do now

1. Review and test business continuity plans for scenarios where core operational systems must be taken offline during an active incident
2. Verify that employee access to critical HR systems (payroll, scheduling) has documented offline or alternative access procedures
3. Assess customer-facing platform dependencies and establish communication protocols for service disruptions affecting digital channels
4. Evaluate segmentation controls between corporate networks and point-of-sale or store-level systems to limit lateral movement
5. Conduct tabletop exercises simulating prolonged IT outages affecting order fulfilment and supply chain operations

6. Review incident response playbooks to ensure clear escalation paths and decision criteria for taking systems offline versus maintaining availability