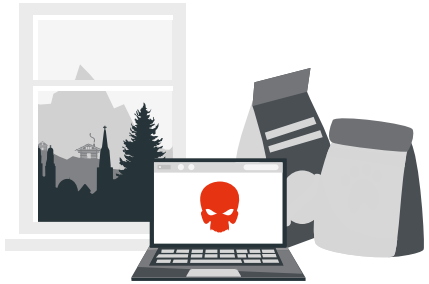
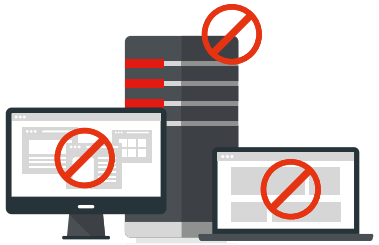
Containment without compromise



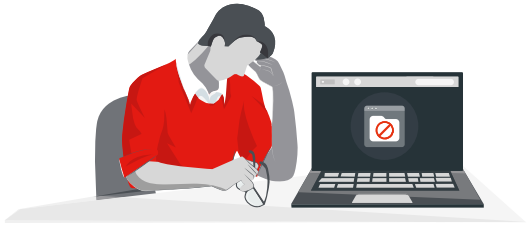
1. The Event

An animal food producer in Switzerland and Austria suffered a ransomware attack. The attack was perpetrated by a group that was believed to be “Akira”.



2. The Impact

The ERP and the entire IT environment had to be shut down. The network was infected with lateral movement, necessitating a complete re-setup. Additionally, production systems were impacted due to the encryption of data.



3. The Problem

The company’s IT infrastructure included systems of varying ages. There was a VPN connection to an Austrian production company within the group, which was also affected by the ransomware attack. No backups of the software for the controllers of the production were available.

4. The Solution

Chubb deployed an incident manager and forensic experts to support the IT team. Step-by-step recovery began after isolating safe systems. Old backups restored production, while critical controller software was sourced from third parties.

5. The Outcome

The efficient response minimised production loss, ensuring that the impact on the company remained immaterial. The operations of the company could be restored without material production loss. No ransom payment was made.

CHUBB®

UK9006-HS 09/25

Expert action, smooth recovery

Policy Triggered: Cyber

The Chubb difference:

- **Proactivity**
  Chubb acted swiftly by deploying an experienced incident response manager and a specialist forensic team, ensuring containment measures were initiated immediately. By proactively analysing system logs and identifying safe zones, the team prevented further spread and accelerated recovery from a complex, multi-site breach.
- **Technical Ability**
  The appointed forensic experts brought deep technical insight, identifying lateral movement across aged infrastructure and pinpointing the safest way to reintroduce systems.
- **Solutions Focussed**
  Despite significant challenges, Chubb and its partners found a way forward. With a clear recovery roadmap and third-party collaboration, the business resumed production quickly and avoided any material loss, without resorting to ransom payment.