Competenz
Your industry training partner

Competenz Recovery from a Cyber Attack

Background

Competenz is a New Zealand-based industry training organisation that provides skills development and workforce training across 37 key sectors.

In early June 2024, Competenz experienced a targeted intrusion by the LockBit cybercriminal group. The sustained ransomware cyberattacks aimed to steal sensitive customer data, disrupt business operations and force Competenz to pay a ransom to halt the attack.

Problem

The attack was initially identified when the Competenz Digital Team was alerted to unusual activity in their cloud environment. The team immediately started investigating and isolating affected systems and services.

Due to their quick reaction, the attack's effects were reduced. The servers' encryption, one of the characteristics of ransomware-type malware, was interrupted before it could be completed.

The team still needed to eliminate risks, safely restore service and minimise business impact.

Immediate response

Competenz established an independent team that immediately activated an incident response plan to restore the business to normal operations.

Equinox IT was asked to advise and help by providing solution architecture, cloud engineering and project management skills.

The initial need was to isolate any leftover infected systems to prevent the attack from spreading inside the Competenz network.

The team quickly needed to build clean environments to host the business applications. The contents of the system and data backup needed to be verified to ensure they could be safely restored to the new environments.

While performing these actions, the team had to make information available to assist authorities in investigating and identifying the attackers.

Recovery and remediation

The recovery and remediation steps taken by the Competenz Digital Team and Equinox IT involved the following activities:

- **Isolation:** The cloud environment where the affected services and data were hosted was isolated, with external network connectivity removed, services shut down and access restricted to a few engineers, preventing further attacks.
- **Comprehensive review:** Before any restoration of data or service could begin, a full review of Competenz's existing cloud environment and services was undertaken to identify the full impact of the attack.
- **Design and deploy:** Equinox IT designed and implemented a best-practice cloud landing zone to ensure Competenz recovered from the attack with a secure operational environment.
- **Data restoration:** Leveraging the existing Competenz data backups, the Equinox IT team validated the most recent clean backup and used it to restore data into the new landing zone.
- **Network security enhancement:** Equinox IT, working with the Competenz Digital team, strengthened the security of physical and cloud network infrastructure by implementing additional security measures.
- **End-user device replacement:** Equinox IT managed an end-user device replacement project, which included configuring a cloud-based endpoint management solution to reduce the risks of future attacks being successful.
- **Effective communication:** The Competenz leadership took a proactive and constructive approach to communications with internal and external stakeholders, including the relevant authorities.
- **Virtual CIO:** Throughout this engagement, an Equinox IT consultant acted as a vCIO, who assisted with technical leadership and supported the Competenz executive team in reviewing and updating their IT strategy, policies and procedures.

Long-term results

Competenz addressed the challenges presented by the attack by consulting with experts and implementing a proactive recovery strategy.

The prompt and coordinated response enabled Competenz to recover from the incident successfully, enhancing the business's resiliency and preparedness.

By streamlining technical management processes and embracing a modern, flexible environment, Competenz is well-positioned to respond quickly to strategic shifts and external influences, supporting its ability to create and deliver new, exciting digital experiences.

> *"Equinox rapidly moved from a gun for hire to help us recover from the incident to a trusted advisor who has been guiding not only on our infrastruture rebuild but with updating our processes and procedures to best practice. Ben and our GM of Corporate Services have formed a very tight working relationship that is beginning to make a real difference to our business."*

Amanda Wheeler, Competenz Executive Director

Get in touch

Find out how we can help you plan and keep your cloud safe and secure.