HACKNOWLEDGE

CASE STUDY

INCIDENT RESPONSE TEAM IN ACTION

CONTEXT

Cloud services have revolutionized the way we store data. Simplicity, speed, and accessibility all seem to be in the mix for the perfect solution. However, one small security breach and all the data can be exposed.

When one of our clients contacted us after a cyber-attack on their private cloud, our CSIRT - Incident Response Team had to combine speed and efficiency to eliminate the threat.

SETTING THE SCENE

Our customer offers its providers shared web hosting services with private cloud availability. The cyberattack began with the hacking of one of the client's privileged account.

From this gateway, intruders took control of the entire infrastructure by setting up backdoors, resulting in total paralysis of their system for several days.

OUR TEAM’S INTERVENTION

When this client contacted us, we immediately took action. Within 3 days of working tirelessly, the system was back on track and free of malware.

Together with an incident response team from another firm, we conducted a complete analysis of the situation. Understanding what happened is critical to remedy the problem.

Major actions were :

- Review of the entire Active Directory configuration;
- Analysis of the vulnerability points;
- Analysis of the network flow and the weakness of configuration with very few restrictions;
- Increased monitoring;
- Restoration of compromised machines to date identified as clean;
- Implementation of patches to avoid any recurrence.

When the company contacted us, their goal was to be back up and running as quickly as possible, which is understandable. Our CSIRT team's objective is similar, even though our experience has taught us one thing : acting quickly, without rushing - a job well done must ensure sustainability to avoid similar circumstances.
If you wish to benefit from the efficient intervention of Hacknowledge's CSIRT teams, contact us today.

Hacknowledge

www.hacknowledge.ch

info@hacknowledge.ch