+44 345 094 0945
www.waterstons.com

News article

Mar 2024

Attack Impacts 100 Romanian Hospitals: Cyber Incident Review

A cyber-attack on a healthcare provider platform used by hospitals in Romania has spread rapidly to around 100 hospitals and healthcare facilities.

What Happened

In February, the company that develops the Hipocrate Information System (HIS), a Healthcare management system used by hospitals in Romania to manage medical activities and patient data, was hit by a ransomware attack.

While the initial infiltration vector has not been disclosed, the Romanian National Cyber Security Directorate (DNSC) has reported threat actors deployed the 'Backmydata' ransomware to encrypt the production servers, taking the system offline. The threat actors were also able to spread to, and deploy ransomware on, the servers of 25 hospitals and healthcare facilities that use the HIS platform. A further 75 hospitals have been disconnected from the incident as authorities investigate the extent of the attack. While these actions are aimed at reducing the risk of data exfiltration, they have caused challenges for hospitals, some of which have been forced to turn to pen and paper to continue treating patients.

The unidentified ransomware group is demanding £135,000 to decrypt the HIS servers, however, it does not appear any of the impacted hospitals have paid. Fortunately, most of the impacted hospitals had the data on the encrypted servers backed up recently, enabling an easier recovery, with only one hospital so far having a backup older than three days available to restore from.

Currently there is no evidence that sensitive data was exfiltrated as part of the attack.

Wider Implications

Supply chain attacks continue to pose a significant threat to organisations as threat actors continue to target the complex digital supply chain. Over the past year multiple high profile supply chain attacks such as the MoveIT ,and 3CX incidents, have demonstrated the potential scale of supply chain attacks which can impact dozens of organisations. Threat actors have taken notice, and digital supply chain attacks are becoming more common and a significant challenge that organisations must confront.

Organisations Should:

- Use a risk-based process to review suppliers; assessing the security posture of the supplier, and the 'secure design' of the solution being procured. This review process should also identify critical dependencies which can be used to inform incident response and business continuity planning.
- Implement an incident response capability which is regularly tested to provide ongoing confidence in its effectiveness.
- Implement a comprehensive business continuity plan that is regularly tested to ensure all key personnel know their roles and responsibilities, and that the plan can be enacted quickly following an incident. The business continuity plan should take into account the Recovery Time Objective (RTO) of critical systems that support business functions, to ensure the plan can recover systems within a timeframe that will minimise impact.
- Ensure they have implemented a backup strategy which includes multiple copies of backups available, saved in different locations. At least one of these backups must be an immutable backup that cannot be modified or deleted by threat actors, and that can be deployed to production servers quickly.
- Ensure they have implemented a secure backup and recovery procedure, including regular testing of backups to ensure they meet the Recovery Time Objectives (RTO) and Recovery Point Objective (RPO), as well as the use of a modern backup solution that is designed to protect from modern security threats. The backup and recovery procedure should be designed to minimise the risk of human error during backup or recovery.
- Ensure that the backups solution is regularly maintained and patched to ensure it remains free of vulnerabilities. The VEAM Backup solution vulnerability discovered in March 2023 highlighted that regular software vulnerabilities still apply to backups solutions; and organisations can't set and forget their backups.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

Get in touch I 02 9160 8430