REMORA

CORPORATE CYBER DEFENCE

"Cryptolocker" attack recovery for a Shipping Company

Background

A Shipping company was infected by a "Cryptolocker" virus and attempts to remedy the situation by local IT staff had proven unsuccessful. Remora were urgently invited to resolve the situation.

Services performed

- Incident Response
- Risk Assessment to ensure the breach could not be repeated.

Time Taken: 7 days

Observations and Approach

We discovered that:

- An employee, with administrative privileges to their PC, had inadvertently downloaded the virus a day prior to the day of the attack, and this action rendered all company file data unusable over the weekend.
- An outdated and vulnerable version of Java was installed across the PC real-estate which allowed the virus to ultimately spread to the Windows server infrastructure.
- A restore from Tape Backup was not possible as backup jobs had been suspended by the order of Company's top management due to their impact on network bandwidth. The backup had not subsequently been re-enabled in a timely manner by the IT services provider.
- The financial impact to the firm being significant due to:
    - The "cryptolocker" ransom being paid twice due to connectivity difficulties during the original payment process.
    - SLA penalties paid to customers to compensate for lack of delivery.
    - Staff being sent home for the duration of the outage.

Deliverables and Conclusions

We identified to senior management the potential root causes for the breach and suggested a number of remediation measures. The combination of inappropriate and unnecessary user access privileges and a weak software patching regime had ultimately contributed to the "cryptolocker" infection causing significant financial loss to the firm.

Our findings ultimately led to:

- The recognition of Business Risk and the necessary prioritization of remediation, especially in light of the firms' strategic international expansion intentions
- A new process of internal staff oversight of the 3rd party IT Service Provider
- The contract of the 3rd Party IT Service Provider being renegotiated and Key Performance Indicators being tightened

Find out more :

hello@remora.co.uk

0203 617 6990

www.remora.co.uk