REMORA

CORPORATE CYBER DEFENCE

Penetration Testing and Follow-on Services for a Hedge Fund

Background

A London-based Hedge Fund received a request from its primary investor to run a vulnerability assessment for its IT systems and equipment. Remora were invited to perform the white box Penetration testing.

Services performed

- White box Penetration Testing (initially)
- Follow-on services: 24/7 incident response, data governance compliance monitoring.

Time Taken: 4 days (initially)

Observations and Approach

We discovered that:

- Outsourced IT services provider was using insecure and easily guessable passwords for switches and firewall administration.
- Wireless access controller was running an outdated software version. This version is prone to denial of service and privilege escalation attacks.
- Remote desktop protocol was accessible from the Internet - It was possible for anyone on the Internet to access the remote desktop protocol on a core server
- Network Printers were not locked down. Consequently, any attacker who has managed to gain access to the internal network would be able to disrupt these devices, obtain information that could aid further attackers.
- Internal exchange server prone to Mail spoofing - this would allow an attacker to anonymously transmit 'spam' or 'spoof' mail from a corporate email.

Deliverables and Conclusions

We have put through a message to senior management on the severity of issues identified and conducted work with outsourced IT services provider to resolve the problems identified and conducted a follow-on penetration testing relevant security controls were implemented.

Remora was then asked to provide ongoing services to the client that included:

- 24/7 Incident response service - cyber security monitoring, incident response and business continuity planning, regular staff trainings and drills;
- Data governance compliance monitoring to ensure sensitive corporate data, including personally identifiable information ('PII') of clients and employees, as well as company's intellectual property are protected at rest and during transfer, and subject access requests are carried out in line with the ICO requirements.

Our findings ultimately led to:

- Reduction of IT-security related risks;
- Increased levels of protection for valuable company data, including PII
- The contract of the 3rd Party IT Service Provider being renegotiated and controls being tightened

Find out more :

hello@remora.co.uk

0203 617 6990

www.remora.co.uk