REMORA

CORPORATE CYBER DEFENCE

Red Teaming for a Regulated Company

Background

A regulated business received a request from one of their lead investors to assess their current level of cyber security protection.

Remora was invited to perform Red Teaming exercise (multi-teared attack simulation designed to test whether company's network, people and security could combat a real-life adversary) to expose potential gaps in security.

Services performed

- Open Source Intelligence (OSINT) work;
- Advanced Email Phishing Campaign;
- Wireless Penetration Testing;
- Internal Infrastructure and Web Application Penetration Testing;
- Organisational Response Tests.

Observations and Approach

Remora designed a plan which would asses, execute and evaluate an attack simulation:

- Planning stage:
  - Reconnaissance and intelligence to obtain information on best possible way to perpetrate the target systems and mislead employees into disclosing valuable data.
  - Test baseline state of systems and services to measure attack efficiency.
  - Enumerate and identify external IT and physical office footprint.
- Analytical Red teaming stage:
  - Apply formal methods of modelling to identify course of actions which would impose risks to the business.
  - Create attack graphs and trees with reference to behavioural models to devise most efficient attack.
  - Undertake different scenarios simulations to identify the best vector of the attack.
- Operational Red Teaming stage:
  - Attack simulations executed to simulate execution of adversarial scenarios.
  - Compromise systems to achieve attack goals set.
  - Expose human security Issues to harvest information through advanced phishing emails and gain access to internal company networks.
  - Expose vulnerabilities of wireless connectivity.
  - Test various vulnerabilities of the IT and IT security infrastructure.

Deliverables and Conclusions

Remora discovered multiple risks and vulnerabilities in the cyber security systems with varying degrees of severity. The company did have policies and procedures in place that could have prevented attacks, but many of those needed to be more robust as they did not work during simulation. Penetration testing uncovered multiple technical vulnerabilities, many of those having high severity.
Management team and outsourced IT provider were educated in responding to an attack effectively and efficiently.
Our work ultimately led to:

- Improved levels of sophistication for policies, procedures and guidelines;
- Revised level of risks for organisation;
- Enhanced cyber security resilience;
- Improved awareness of cyber security protocols.

Find out more :

hello@remora.co.uk

0203 617 6990

www.remora.co.uk