REMORA

CORPORATE CYBER DEFENCE

Phishing and Penetration Testing for a Regulated Business

Background

A med-size Credit Union realised that they incurred expenses of £450,000 for services they did not solicit. Remora was invited to investigate possible causes and suggest solution that will address the problem going forward.

We found that there was a breach of confidentiality arising from an employee who provided personal information on malicious website after receiving email that seemed legitimate. As a result, sensitive information (full login credentials) was disclosed to a third-party with subsequent use of that information in fraudulent activities.

Remora was later asked to increase awareness of credit union personnel, identify possible deficiencies with the existing anti-malware protection and evaluate security of the business.

Services performed

- Investigate transactions and actions that lead to £450,000 being disseminated from Credit Union's account.
- Resolve situation with compromised credentials and procure that similar events don't happen again.
- Run phishing campaign simulation – use real life exercise involving mock phishing test to assess staff awareness.
- Train employees to spot malicious emails and raise cyber awareness.
- Run penetration testing to check infrastructure for known vulnerabilities.
- Upgrade cyber security architecture and cyber defences.

Observations and Approach

We discovered that an employee with access to the financial systems received an email that appeared as an email from the systems administrator asking to update his credentials. These credentials were used to make payments, and fraud was discovered only a week later.

Our phishing campaign simulation revealed that 44% of the employees would have been a victim of a phishing attack if they were sent similar email. We had to design series of training sessions to address that problem.

Penetration testing revealed multiple critical vulnerabilities in company infrastructure.

Deliverables and Conclusions

We have put through a message to senior management on the severity of issues identified and the rout-cause of the event.
We worked with the outsourced IT provider to resolve vulnerabilities and upgrade cyber security architecture as well as procure monitoring service to address the problem of cyber security.
We ensured all employee accounts have their passwords changed in accordance with stronger password policy, enabled double factor authentication for critical systems and procedural verification for transactions.
We recommended 24/7 monitoring and incident response service which was subsequently procured by the company.

Our work ultimately led to

- Reduction of IT-security related risks;
- Increased levels of employee awareness.

Find out more :

hello@remora.co.uk

0203 617 6990

www.remora.co.uk