REMORA

CORPORATE CYBER DEFENCE

A Charity has its Breached Website Successfully Restored

Background

Having had its customer-facing website breached and rendered unusable, a charity urgently invited Remora to remediate the situation.

Services performed

- Incident Response

Observations and Approach

We discovered that:

- An unstructured IT environment existed: server hardware located in the main office unprotected, exposed cabling, the lowest possible contractual Service Level Agreements with service providers, and hardware used beyond manufacturer's end-of-life.
- Due to the charity's chosen Service Levels, neither the hosting company nor the IT Service Provider were incentivised or compelled to resolve the situation.
- The original website had direct links back to behind-the-firewall infrastructure. It was using an old version of PHP ver4.0 with clear text passwords embedded in the code that could be easily accessed from any computer connected to the internet.
- Attempts by a technical representative of the charity to remedy the situation by deleting files had exacerbated the situation.

Remora restored the website and put in preventative safeguards by:

1) Encrypting all website passwords;

2) Removing all fraudulently injected content metadata, script, and the backdoor scripts;

3) Upgrading old versions of software to the currently used on the market.

Deliverables and Conclusions

We restored the website and enhanced security mechanisms to prevent further incidents.

Find out more :

hello@remora.co.uk

0203 617 6990

www.remora.co.uk