Determining what damage a targeted attack could inflict

Aware of his responsibility, under the Senior Manager Regime, to protect against data security breaches, the CEO of an international trading organisation commissioned Redscan’s Red Team to perform a real-world attack simulation. The three-month long, covert and exhaustive exercise revealed significant and fundamental information security vulnerabilities. With this insight, the organisation was able to subsequently prioritise security projects and improve board-level confidence in its ability to avert and detect a breach.

THE CHALLENGE

Improved cyber awareness for risk management

The CEO and board of directors were fully aware of the damage a cyber-attack could inflict to both the organisation’s operations and reputation. Like most senior executives in their position, however, they felt that, although significant cyber security investments had been made, they still had no real visibility of the effectiveness of these defences and how their organisation would respond to a real-world attack.

In addition to this, new legislation from the Financial Conduct Authority (FCA) is being implemented in phases from March 2016 that makes senior managers personally accountable for ensuring that regulatory requirements pertaining to IT security are met in full. So, the CEO and board of directors decided to engage Redscan’s Red Team to test the effectiveness of the company’s cyber security controls and its ability to both detect and respond to malicious behaviour.

The company was quick to recognise the high-value delivered by the investment in the Redscan Red Team engagement. It is less likely to face the potentially huge cost of remedying a major security breach and can also avoid fines and penalties from the FCA.
THE SOLUTION

A real-world attack simulation by Redscan’s Red Team

For this engagement, Redscan’s Red Team customised and employed modern adversarial tactics to emulate advanced threat actor activities within the organisation’s network environment. The project involved testing all facets of the financial company’s IT defences, including prevention, detection and response.

To ensure the engagement was conducted as realistically as possible, Redscan received no internal information or access to the client’s business. All knowledge was obtained leveraging open source threat intelligence gathering techniques to identify valuable information that was available within the public domain. The engagement was also carried out over a period of three months to ensure it replicated the stealthy approach adopted by real-world attackers.

THE RESULTS

The intelligence to implement real IT security improvements

At the end of the agreed simulated attack period, Redscan’s Red Team delivered a comprehensive report for the CEO and board of directors, highlighting all of the information security issues detected and ranking them according to the level of risk to the business. In each case, the Red Team provided clear guidance on how to mitigate the risk, recommending specific solutions, policies or training courses as appropriate. Consequently, the business is now putting in place new measures to better protect its data, employees and customers.

Some of the weaknesses the Red Team identified across the organisation’s technology, people and processes, include:

- Exposure to phishing attacks, which could be used to acquire remote log-in credentials for IT systems and access to client transactional data
- Failures in the company’s access permissions that could be exploited to disrupt multi-million dollar trading transactions
- Configuration issues in intrusion detection systems and a large number of false alerts, which made the company unable to detect Redscan’s deliberately “noisy” attempts to break-in
- Weak passwords used by many employees, demonstrating gaps in user education and training
- Inadequate responses to suspicious incidents
- No active monitoring of the internal network, so once the Red Team had successfully infiltrated there was no likelihood of discovery
The CEO and board members now have a far more enlightened view of cyber security weaknesses across the business and can better meet their information security obligations. They can provide documentary evidence that information security is of high priority; that they are aware of the risks; and that they are taking the appropriate action to mitigate them.

In reviewing the findings of the Red Team, the company was quick to recognise the high-value delivered by the investment in the Redscan Red Team engagement. It is less likely to face the potentially huge cost of remedying a major security breach and can also avoid fines and penalties from the FCA.

About Redscan Cyber Security Ltd
Redscan, is a Managed Security Services Provider (MSSP) that enables businesses to effectively manage their information security risks. Using a combination of security expertise, technology, processes and threat intelligence, the company’s rapid detection and monitoring services help defend against today’s sophisticated and targeted threats. Designed for businesses of every size, Redscan’s services include ThreatDetect, it’s affordable 24/7 Security Operations Centre as-a-service platform, CREST approved Penetration and Red Team Operations. Redscan’s management team bring over 50 years of combined experience in cyber security across a range of industries, including banking, accounting, legal services, construction, retail and leisure. Enabling clients to adhere to PCI and ISO, GPG13 and Cyber Essentials Plus, Redscan is proud of the certifications the team holds, such as Crest, CISSP, CEH, CISM, OSCE, CISA, OSCP and OSWP.

Contact Us
UK: +44 (0) 207 253 3020
HQ: 44 Paul Street, London EC2A 4LB
e: sales@redscan.com
www.redscan.com