



Using penetration testing to enhance security and reduce business risk ■

CASE STUDY

1



SECFORCE was contacted by a prominent UK insurance company. The company had suffered an incident whereby all their emails were treated as spam, and blocked by a number of large internet services providers and tier 1 carriers. The cause of this was identified to be an 'open mail relay' vulnerability on their mail server, which had been exploited by a spammer.

The discovery of this vulnerability raised grave concerns over the integrity of previous penetration testing results. The high level of business disruption caused by this incident made it clear to senior management that effective security measures needed to be implemented to protect them against this or any similar incident from re-occurring.

THE PROBLEM

2



A series of tests were commissioned with SECFORCE, as a new provider, to establish the following:

- What was the level of security in the Organisation's external infrastructure and web applications?
- How effective was the physical security at their 3 primary UK sites?
- What level of security awareness was held among their staff?
- How resilient was the internal network security to an unauthorised and low level user attack?
- What level of security protects the Organisation's information when stored on authorised thumb drives or laptops?

THE SOLUTION

In addition to these areas being challenged in isolation, senior management also wanted to know what level of impact might be achievable should information from any testing area be used to further attacks in others.

The following testing was conducted as part of this review:

- Penetration testing against all external infrastructure
- Application testing of all public facing web applications using the functionality and user levels available to any member of the public
- Physical penetration testing of the 3 primary UK locations
- Social engineering, both electronic in the form of spear phishing, over the phone and face to face
- Stolen laptop testing



External Infrastructure and Application Penetration Testing

identified that the systems were for the most part well configured and secure. The mail relay issue was indeed resolved. The applications tested had been well developed, and although there were a few security vulnerabilities identified, none would have put the organisation at an unacceptable level of risk.

The **Physical Testing** exercise identified significant issues with the organisation security processes. It was possible to enter and roam unchallenged in all three locations with little difficulty, utilising socially engineered entry and tail gating. Once inside the buildings there was no effective control or segregation of areas. At our Client's request, a wireless bridge was installed to a network socket behind a photocopier which was then successfully used to conduct internal testing from the car park. The wireless bridge required authentication and used strong encryption to ensure that only SECFORCE consultants could access it. The device went undiscovered for a three week period, whereupon our Client kindly returned it to us.

Internal Penetration Testing

discovered a number of procedural failings, with insecure services being used for administration, password policy being weakly enforced and patching policy not being enforced thoroughly. This led to a number of key servers being infiltrated, which in turn lead to the domain being fully compromised. This coupled with the wireless bridge represented a critical risk.

The Stolen Laptop Testing

demonstrated that data was securely encrypted when the laptop was powered down.

Social Engineering was used throughout the testing and contributed to facilitating entry to the buildings, extracting various passwords to the network.

The projected impact should this attack be carried out by a determined attacker is severe, **total compromise of confidentiality, integrity and availability** of the entire Organisation's system and data assets being achievable.

SECFORCE's comprehensive report was used as a baseline tool to enhance the security in the areas which needed it most. Our Client was able to arrange an emergency contingency budget from the board to address the significant issues which included:

- Installing card controlled access throughout the buildings
- Implementing an updated security awareness training programme
- Tightening policy control for the distribution of passwords
- Decommissioning legacy systems
- Enhancing network logging and monitoring
- Tightening policy on administration of key infrastructure

SECFORCE

SECFORCE is certified by CREST and ISO9001 to ensure the highest standards of security assessment services



CONTACT US

If you would like further details,
please get in contact:

SECFORCE UK
Suite 11, Beaufort Court
Admirals Way
E14 9XL London
TEL +44 (0) 845 056 8694

SECFORCE SOUTH AFRICA
Palazzo Towers W, Montecasino
William Nicol Dr, Johannesburg
Fourways, Gauteng, 2000
TEL +27 (0) 11 5100 161

www.secforce.com