DATA SHEET

Red Teaming:

A technical risk assessment conducted live and real-time.

Red Teaming involves a comprehensive replication of the behaviour of a real cybercriminal. This simulation is conducted via a multilayer approach to security testing that not only exploits vulnerabilities in technology, but also exploits the flaws in people and processes within the organisation and its supply chain.

"Red Teaming" originates from a military terminology with the Red Team being the attackers and the Blue Team being the defenders. This approach simulates more closely how unconstrained real-world attacks take place from key threat actors such as state-sponsored attackers, terrorists, organised crime gangs, corporate spies and other nefarious individuals. Your organisation and any outsourced IT services should be operating as the Blue Team – ideally defeating the attack as it occurs.

The results of such a test will allow you to create an independent, neutral view of the effectiveness of both security controls and the team responsible for identifying and reacting to security incidents.

Benefits of Red Teaming

A Red Team exercise is goal oriented.

Red Teaming focuses on what attackers may be interested in – whatever that is. It could be data, attaining access to a key administrative account/role with an application, the blue print to a strategic project, the decryption keys to highly sensitive protected documents, or it could be the controls to critical infrastructure.

While many penetration tests are narrow and system focused, the real "crown jewels" of the organisation are seldom targeted. Red Teaming is highly effective in exposing systemic weaknesses.

Adopting a Red Teaming approach means that you will be thinking and acting just like your worst enemy, allowing you not only to gain an understanding of the approach used by an adversary, but also ensuring that your security team will be prepared to create swift and decisive responses, even against the most complex attacks.

For organisations whose boards and directors are responsible for risk management of the business, this is one of the most effective validation measures of the capability of the business and its suppliers to demonstrate cyber resilience.

Why Red Team?

Corporate Australia is spending large sums of money protecting their networks, systems and applications – but is the money being spent wisely? Traditional approaches have focused on using targeted penetration testing to validate whether controls are working, and key information assets are protected.

Penetration testing is very narrow and even if the organisation gets good value from the test and fixes the issues there are likely *many other channels* through which an attack could occur.

An often-overlooked avenue is your physical security and the human factor. This is where a thorough holistic approach to information security testing is required - Red Teaming.

When it comes to red team testing, vulnerabilities and risks will be exposed across the business including:

1. Technology — networks, applications, routers, switches, appliances
2. People — staff, independent contractors, departments, business partners
3. Physical — offices, warehouses, substations, data centres, buildings
4. Business Processes – the relationship between roles within the organisation or the process flows that occur in the natural course of business
5. Supply Chains — the relationship between the organisation and its suppliers (networked, connected, process flows, help desks, ticketing services etc.)

Recent Case Study

Background

Our client operates critical infrastructure and appoints Sense of Security to deliver a goal phase objective of accessing/compromising:

- Key Corporate Data Store
- TLS certificates (Private Keys)
- Backend systems used to manage Critical Infrastructure.
- Active Directory domain

Collectively these are the “crown jewels” of the business.

The agreed methods for attack vectors include:

- Network (internal/corporate and external, and Wireless)
- Web application (client facing and corporate)
- Email (staff mailboxes and infrastructure)
- Tailgating (selected physical locations)
- Network drop boxes
- USB passive and active drops

Additional Testing for the Supply Chain of key outsourced IT Managed Services & Hosting Service Providers followed.

The following threat actors were identified as those most relevant to the business:

- Insider threat
- Identity unknown
- Individual
- Hacktivist
- Cyber terrorist
- State-sponsored

Stage 1

Unauthorised access to the network, critical systems and data was obtained through the testing performed.

Specifically, access was obtained to the external email platform (Office 365), the Active Directory Domain Administrator role, the nominated critical company data store, and the backend management system for the critical infrastructure including the TLS keys (and the passwords that protected them) which are paramount to the integrity and confidentiality of the system.

Access was obtained initially using tailgating techniques which permitted physical and network access. Once access was obtained it was trivial to laterally move through the network environment unobstructed, compromise other systems, and exfiltrate data due to the lack of outbound network filtering.

While the phishing attack as well as the creation of malicious mail rules were detected during the social engineering phase of the attack, the rest of the attacks (physical, external infrastructure as well as the internal access) went completely undetected and unhindered.

We determined that the systems and infrastructure reviewed were not configured and maintained in accordance with ICT security best practice standards, nor are staff adequately trained in how to challenge or deal with physical adversaries.

Improvements could be made to provide further protection against current and emerging threats by key actors.

Weaknesses were identified in relation to the key areas of security awareness, host and network configuration, endpoint security and monitoring, mail server and DNS configuration, physical access control, Windows configuration and hardening, password and account management and incident response.

Stage 2

Initially, SOS performed passive reconnaissance to map the organisation’s network exposure and enumerate potential external areas of attack. Information was also gathered about staff members, such as email addresses and other information, that could be used both in subsequent network as well as social engineering attacks.

External unauthorised access to staff mailboxes was obtained. Access was obtained by leveraging a combination of a misconfiguration of settings within the Office 365 platform, the weak password policy in place, as well as poor security awareness that allowed staff to use easily guessable passwords.

The passwords consisted of common dictionary words, combined with numbers and special characters using common patterns. A number of these passwords were also included in several compromised passwords lists. This has an implication for the entire organisation as an external party could gain access to all email messages of the compromised user accounts, including internal and system messages, including all information contained within.

SOS succeeded in physically tailgating staff members into an office. Remote access to the environment was obtained by subsequently plugging in a specially prepared device (LAN Turtle) to a network port which was not protected by network port-based access control solution. This device acted as a backdoor into the network and provided us with the same level of access as if we were physically sitting on site.

Once physical access was obtained, it was possible to boot the staff workstations, lacking BIOS or boot protections, using external USB drives. Due to the workstation hard drives not being encrypted, it was possible to extract cached domain credentials, which allowed domain level access to these as well as other domain attached machines.

Stage 3

As a separate attack, SOS conducted a successful phishing campaign which made use of a cloned login page to entice users to enter their Windows domain credentials. Even though the business had advised the users that a phishing attack was detected, and the external email gateway/security service flagged the phishing emails as suspect, we were still able to obtain several sets of credentials.

Lack of controls and procedures around content publishing allowed SOS to locate the target systems specified as the major goals for the engagement.

Insufficient network egress filtering allowed for unrestricted outbound network access. This created an easy channel to exfiltrate data from the network.

The industry leading DLP solution installed on workstations simply didn't work.

All the goal objectives of the assignment were achieved. Not all the attack methods succeeded; but we focused on those that did. The entire environment, right through to the crown jewels was compromised and nothing was detected.

Why choose Sense of Security

Sense of Security is Australia's leading Cyber resilience, information Security and Risk Management Consulting Firm.

As industry thought leaders for nearly 20 years, we provide expertise in governance & compliance, risk assessment, strategy & architecture through to, assurance & technical security testing.

Our strategic approach to security provides you with a capability to assess your risk and deliver qualified guidance on how to protect your information assets. Technically outstanding and exceptionally detail oriented, we view our accountability to our clients and the wider community extremely seriously and we do our utmost to conduct our business in a sustainable manner.

Working extensively with Australian based corporations and State and Federal Government agencies, SOS provides security services that deliver, no matter the standard or framework selected including NIST, CIS, ISO 27001, ISM and PCI DSS.

Sense of Security®

For help and tailored assistance, call Sense of Security right now on

info@senseofsecurity.com.au

1300 922 923 +61 2 9290 4444

senseofsecurity.com.au