Whitepaper: Social Engineering

Why companies are exposed to social engineering

Date: April 2016

Doc Ref: SOS-WP-SE-1210B

Author: Neville Gollan & Nathaniel Carew

Table of Contents

Introduction

Who presents the most dangerous threat inside your business? Most organisations would be surprised to know that overly helpful employees can be far more dangerous than the stereotypical "disgruntled employee".

This whitepaper explores the vulnerability of enterprises to social engineering, an attack that manipulates well-meaning or curious employees into unwittingly abetting the theft of corporate secrets.

Three aspects of social engineering will be discussed:

1. Relevance – the extent of exposure
2. Challenge – making the case
3. Protection – testing and procedures

While most CTOs and IT managers focus on the technical aspects of information security, highly publicised episodes overseas have shown that social engineering can sidestep the most advanced technological defences. Hardware solutions, with their reassuring rows of blinking lights, can be rendered ineffective once a social engineer has tricked an employee into giving privileged access to the internal network.

A cyber-security audit used a social engineering technique through placement of baited USB devices to penetrate the networks of eight state government agencies in Western Australia[1].

Social engineering is a type of insider threat. Insider threats are typically associated with the disgruntled employee who uses legitimate access to internal systems to steal, delete or manipulate information assets, or to disrupt operational systems dependent on IT such as SCADA control systems.

By comparison, a social engineering attack is carried out by an external assailant who deliberately manipulates an employee's good intention (i.e. their willingness to assist) or their general curiosity, such as enticing them to click on a link in an email to a malicious website. While social engineering and the disgruntled employee are both insider threats, defending against these respective attacks requires very different approaches.

The consequences of not protecting against social engineering can be disastrous, as breaches at network technology manufacturer Ubiquiti Networks and security vendor RSA have demonstrated. The viability of launching a social engineering attack has risen with the advent of social networking sites with a wealth of personal information that can greatly aid a social engineer.

One of the greatest challenges to enterprises defending against social engineering

[1] Western Australian Auditor General's Report, Information Systems Audit Report, Report 4 – June 2011

is coordinating a response from different departments, especially Human Resource Management. The answer to social engineering is not to buy another security appliance or software product. The best protection is ongoing security awareness training and a robust set of security policies that remind all employees of the important role they play in safeguarding their company's information assets.

Relevance – the potential exposure

2011 will be remembered for one of the biggest security breaches ever. Hackers broke into security company RSA's systems and stole very sensitive data relating to the operation of its security tokens which are used globally by financial institutions, enterprises and governments to authenticate network access and commercial transactions[2].

The hackers' first step in embarrassing one of the IT world's most impregnable companies was a phishing email targeting RSA staff with the subject line "2011 Recruitment Plan". The malicious spreadsheet it contained helped attackers record passwords remotely and penetrate the corporate network.

This was social engineering at work.

Advances in IT security have made it increasingly difficult to hack into a well-guarded enterprise. Network defences, encryption and smarter detection have forced cyber-attacks to look for easier targets which increasingly mean the soft underbelly represented by employees.

Ubiquiti Network Inc. disclosed in their quarterly financial report file[3] in August 2015, that they had been the victim of a social engineering that led to a substantive business fraud incident.

"On June 5, 2015, the Company determined that it had been the victim of a criminal fraud. The incident involved employee impersonation and fraudulent requests from an outside entity targeting the Company's finance department. This fraud resulted in transfers of funds aggregating $46.7 million held by a Company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties. As soon as the Company became aware of this fraudulent activity it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions".

Social engineering is often employed in the theft of data such as intellectual property, personal information or credit-card numbers. This is a growing problem locally and globally although the extent to which it exists in Australia is difficult to quantify.

Unfortunately, many businesses may not even know they have been the victim of social engineering. It can take several months to know that an incident has occurred, how it happened and what was stolen.

[2] http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html
[3] https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

The Risk of Insider Fraud: U.S. Study of IT and Business Practitioners report found that it took three months on average to recognise insider fraud had occurred and another three months to determine the root cause of the insider fraud incident and the consequences to the organisation[4].

One of the most widely used tactics is sending "phishing" emails. The email is disguised to appear as though it comes from a legitimate source and encourages the target to activate the attached malicious file or click on a link that directs the victim to a website hosting malicious code or requesting personal details.

The Verizon 2015 Data Breach Investigations Report [5] cited that the overall effectiveness of phishing campaigns resulted in 23% of recipients opening a phishing message and 11% clicking on attachments.

Sense of Security's research and experience gained from delivering social engineering assignments has demonstrated that a more realistic measure of an organisations ability to defend against the threat of phishing is to execute a well-crafted "spear phishing" assessment. Spear phishing assessment techniques require more research on the specific individual, or individuals that you intend to assess but the results are far more likely to be representative of the actual security risk posed by contemporary threat actors. The research focuses on a companies and an individual's publicly exposed information or OSINT (Open Source Intelligence), through mediums such as personal and corporate based social media platforms, Google indexing and misconfigured externally facing systems.

In a similar fashion to the results gained from spear phishing we have found that many employees of our clientele can be socially engineered over the phone to disclose sensitive information that can be used to further a security breach scenario. Masquerading as an IT support person or senior manager from another division (e.g. HR or Finance) can be applied to great effect if the person being socially engineered has not had any formal security awareness training.

Another practice with a high success rate is baiting. A social engineer leaves infected USB keys or other media in common areas such as lunch rooms, parking lots or foyers for employees to pick up and insert in their computers.

A USB key could contain a keylogger that grabs passwords and keystrokes from the employee's computer and relays the data back to the hacker's server on an external network. Connections could also be established out to the attacker, handing over control of the employee's computer.

It is possible that a hacker could use a compromised computer to move around the internal network using the access permissions of the user.

[4] The Risk of Insider Fraud: U.S. Study of IT and Business Practitioners by Ponemon Institute LLC, October 2011
[5] http://www.verizonenterprise.com/DBIR/

None of the social engineering methods described above are uncommon or require sophisticated technology and yet they can be extremely effective against many organisations, regardless of the number and complexity of their electronic defences.

The challenge for many security operations and risk management personnel is that social engineering is not perceived by their leadership teams to be a major concern and therefore the risk remains unaddressed. This mismatch between the effectiveness of a social engineering attack and the low understanding of the risk plays directly into the hands of a threat actor.

Challenge – making the case

Organisations in general are not doing enough to protect themselves against social engineering. While there is growing recognition that the human factor cannot be ignored, there is still a reluctance to extend traditional, technology-based penetration testing to include human elements.

Social engineering audits can face opposition from senior management. They may decide to confine a penetration test to a technology review rather than one that includes human factor tests, which may be perceived as too complicated or expensive.

The categorisation of social engineering as an insider threat can also cause confusion. A business may think it has done enough by installing anti-virus, firewalls, permission controls and patching to defend against the typical disgruntled-employee scenario but it would still be vulnerable to social engineering.

Today's strong focus on customer service can assist social engineers to take advantage of over-helpful receptionists who have access to sensitive information such as the home address of the CEO.

Social engineering has become easier thanks to the popularity of social networks which can give an attacker personal details such as maiden names, school history and favourite pastimes which can be used to construct a fake persona, or the perfect recipe for a password recovery attack that requires answers to "secret" questions. Instead of searching through rubbish bins or "dumpster diving", a hacker can profile a target within a few hours without leaving the desk.

Common difficulties in fighting social engineering include assigning responsibility for countermeasures, assessing vulnerability and admitting to the size of the threat. The solution is not a simple technical one. It requires co-operation among senior management, leadership in setting examples and development of policies and procedures from within the HR department.

Testing is the first step to analysing opportunities for social engineering, but this should include the involvement of HR Management during planning to avoid any potential staff related concerns following the review. An audit must be conducted covertly in a real-world environment but without embarrassing employees or damaging the organisation's productivity.

Social engineering is almost guaranteed to succeed against an unprepared organisation because it is a human issue, but despite this a breach will not reflect positively for the CRO or the CSO regardless.

While managing all personnel is not the sole responsibility of the CRO or CSO, the consequences of a duped employee surrendering access to the internal network can be.

Although the cost of assessment and preventative measures against social engineering are relatively low, a bad economic climate makes it difficult for companies to spend money on an assessment and security awareness training they may consider "non-essential" rather than spending it on technology which has a clearer return on investment.

An organisation must be open to the results of an assessment which can reveal vulnerabilities businesses would prefer to not to admit. The truth can often be uncomfortable and may stoke political opposition from managers who would rather ignore the problem.

Protection – testing for vulnerabilities

Ideally security reviews are scoped to be comprehensive and include testing the people, process and technology elements. Unfortunately, most reviews are limited and only assess technology, avoiding review of the people or process even though they can potentially present a greater threat.

Defending against social engineering is counter-intuitive in some senses. The classic insider threat of a disgruntled employee can be addressed with technology and permission controls. But the greatest threats in social engineering are helpful staff lacking security awareness.

Security organisations often discuss the "M&M approach" where an organisation has a hardened outer perimeter but a soft and vulnerable inside. Appropriate defences against social engineering involve "hardening" the attitudes of employees which also assists with ensuring a strong perimeter.

Furthermore, social engineering should provide a business with tangible technical solutions to reduce the threat that go beyond recommending social awareness training. These mitigations should include detailed email, DNS and web server configuration hardening techniques which decrease the legitimacy and effectiveness of many common social engineering attacks.

When defining the scope for a social engineering assessment, management should take into consideration the risk of not conducting a comprehensive review. A decision needs to be made on how thorough the review should be. Is baiting with USB sticks sufficient? Should other types of test methods be considered?

In most instances a review encompassing social engineering should be undertaken during a normal workday when employees, customers, suppliers and related

parties are going about their business as usual. For the review to be effective it must be covert and carried out in a realistic setting. The following assessment techniques should be considered as legitimate tests when defining the review scope.

Test Method	Description
Pretexting	Pretexting is the act of creating and using an invented scenario (the pretext) to engage a target victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.
Diversion	Diversion theft, also known as the "Corner Game" or "Round the Corner Game", is a technique used by malicious parties to persuade a person responsible for a legitimate delivery or materials or information, that the content is requested elsewhere.
Spear Phishing	Spear Phishing is a technique of fraudulently obtaining private information. Typically, the spear phisher sends an e-mail that appears to come from a legitimate source requesting "verification" of information and warning of some dire consequence if it is not provided.
Whaling	Whaling emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern or a request for a more junior level staff member to complete quickly and outside of normal business processes.
Baiting	Baiting is essentially a Trojan Horse that uses physical media. In this instance, an attacker leaves a malware infected media (e.g. USB drive) in a location which is likely to be found by employees and waits for the victim to use the device, activating the attack.
Quid Pro Quo	In a quid pro quo attack, an external party calls random numbers at a company claiming to be calling back from technical support. Eventually they will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and in the process have the user type commands that give the attacker access or launch malware.
Tailgating	An attacker, seeking entry to a restricted area where access is by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the

	door open for the attacker. The attacker may also fake the action of presenting an identity token.
Soft Target	A soft target attack often focusses on the more likely weak links in an organisations security. This could be a manager's mobile device or personal email account on Yahoo!, Gmail, or Hotmail etc; anywhere that an attacker might be able to harvest information for use in breaching the organisation that they work for.

Although a review needs to operate in a live environment it should not interrupt operations, cause loss of productivity or be performed in a manner disrespectful to the organisation or its employees. The review also should use repeatable methodologies and log all actions during the test. The resulting report should include meaningful and actionable findings and recommendations.

When an organisation moves to set up defences against social engineering it is important to consider that these will require regular attention; set-and-forget approaches will not work. Security awareness education is absolutely critical and needs to be frequently addressed. It should be part of the induction process and repeated on a 12-month basis for all staff.

Policies and frameworks help govern behaviour and explain responsibilities to all employees from the top down. If employees do not believe that their management are adhering to the same rules and regulations, they are likely to be less inclined to follow them themselves. Reactive processes also need to be addressed such as writing an incident response program that triggers an internal procedure after a social engineering attack.

The key to a successful and sustained defence against social engineering is enforcing behaviour throughout the company. CSOs may find positive reinforcement more effective than upbraiding lapses in behaviour.

A company which understands the importance of security at every level will present a much harder target to the social engineer.

Conclusion

Social engineering is a very serious threat that can quickly undo large investments in IT security and cause extreme damage to reputation, customer data and corporate IP.

The extent of data theft in Australia may be under-reported and underestimated, but reports from the US show that failing to defend against social engineering can present material financial and reputational risk.

Despite the evidence that social engineering can be more effective than external network attacks, many organisations exclude human factor reviews from their security test programme. This inadvertently presents their organisation with residual exposure.

Executive leadership and co-operation between departments are essential to gaining approval for social engineering reviews and helping ensure a company-wide change in behaviour.

Effective countermeasures to social engineering must be backed by company policies and procedures. Human resource management can play an active part in the improvement of an organisations security posture by ensuring all staff participate in security awareness training and developing a corporate culture that is aware of the risks.

About Sense of Security

Sense of Security Pty Limited is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides our clients with a capability to understand the security risks relevant to their organisation and knowledge to protect their information assets. We provide expertise in governance & compliance, strategy & architecture through to risk assessment, assurance & technical security testing.

For more information please contact us:

Web: www.senseofsecurity.com.au

Email: info@senseofsecurity.com.au

Phone: 1300 922 923

Sense of Security - Compliance, Protection and Business Confidence