Cybercrime Social Engineering Analysis Challenge

Security Nightmare 2015 Cloud Attack!

Social Engineering Proposal using MINDSPACE

Author: Peter Carmichael; Newcastle University UK; p.j.carmichael@ncl.ac.uk

Background

The attack presented partly relies upon the MINDSPACE framework which is an acronym that captures a set of behavioural effects used to influence human behaviour [1]. One such effect is *Messenger* which states that "we are heavily influenced by who communicates information to us". For example, in International Traders Limited (ITL) we can assume that the actor *Big* has greater influence over the trading department for advising about customer relations than *Cleo*, the cleaning personnel who is externally contracted.

Attack Scenario

Assumption 1: *Sydney*, *Terry* and *Ethan* have greater security awareness than *Finn*, *Cleo*, *Grey* and *Big*. Therefore, it requires a greater level of complexity to perform a social engineering attack towards them.
Assumption 2: *Grey* is an external employee.
Assumption 3: The laptop in ITL has the ability to manage access control rights which are not capable of being exploited from the outside world (internet) i.e. we need physical access.

Motivation: Server 1 is used for sensitive data which is directly accessed by *Ethan*. Server 2 is used for non-sensitive data and is accessed by *Finn*. Both of these employees have different goals. *Ethan* wants to maintain security; he is a Fraud Investigator and is interested in suspicious activities. *Finn* is a Finance Manager and is interested in productivity/efficiency. The role of Server 1 is to maintain integrity; the role of Server 2 is to be available. Compromising the availability of Server 2 will put pressure on *Finn*. If we can force Server 2 to be unavailable *Finn* will pressure *Sydney* the System Administrator to make it available. Therefore, the aim of this attack is to rearrange the structure of the system to ensure that only two VM's exist on one server. We present our final attack step first and decompose to explain how the final requirements are in place. S6 refers to Step 6 and so on:

S6: Acquire *FileX*;
Requirements: Finn's access details; *Cleo's* working hours; Server 2 stopped sending SSL messages;
Context: Physically break into ITL's open office through the front door. Using the information that Server 2 is no longer communicating with the outside world we can guarantee that all files are currently stored on Server 1. Using *Finn's* credentials, log in to the laptop and attempt to find *FileX*. We may need to perform some elevation of privileges to allow access to *VM1/FileX*. If these steps fail attempt to compromise the hypervisor on Server 1 to gain access to *VM1*.
Issues: We run out of time; the system is too secure and we can't compromise it from Finn's access. The attack is unsuccessful.
Discussion: By identifying *Cleo's* working hours we can maximise our time spent inside ITL as it may not be as straightforward as accessing *Finn's* account to get to *FileX*. We may need to perform some further actions to achieve our goal.

S5: Convince ITL to copy files from Server 2 to Server 1;
Requirements: Log files of SSL communication originating from Server 2;
Context: Impersonate official authorities and phone ITL asking to speak to the System Administrator. State that you have arrested a cybercriminal and have found suspicious logs originating from a server at ITL. Ask *Sydney* to perform a network analysis and look for outgoing SSL packets. When *Sydney* confirms, explain that the cybercriminal has compromised the server and that you recommend any integral files are backed up somewhere else, as you believe it to be open to further attacks so the server should be turned off.
Issues: *Sydney* identifies another solution as he/she realises the security concerns of storing sensitive information alongside non sensitive information. The attack breaks down.
Discussion: Phoning up and claiming to be the authorities, a system administrator needs some form of justification. By showing *Sydney* that the server is compromised, communications are encrypted and that *Sydney* can generate the logs himself/herself creates the environment where a computer savvy individual could be fooled. The recommendation to backup files and turn the server off will be combined by the thought that certain employees i.e. *Finn*, need regular access to their files. This *Norms* effect compounded with the *Messenger* effect will influence *Sydney* to co-locate all files on Server 1.

S4: Spear phish *Finn*
Requirements: *Grey’s* email address; *Finn’s* email address; *Grey’s* role
Context: Craft a spear phishing email to *Finn* spoofing *Grey*. Using the knowledge that *Finn* is the Finance Manager; provide him with an offer which risks him compromising his ITL credentials. Using the credentials remotely place a Trojan on the server which will activate once a system administrator logs in. The Trojan will open up an SSL connection and send encrypted messages to a pre-defined address (ours). The Trojan will continue to send messages until the server is switched off.
Issues: *Finn* does not take the bait, the attack breaks down.
Discussion: ITL is an open office area; if you send an email spoofing staff internally you cannot guarantee that it won’t be noticed. Spoofing an external employee gives a lot more certainty. It uses the *Messenger* effect as it communicates information coming from someone known and hopefully trusted, we can manage this when *Grey* is not at ITL. Targeting *Finn* is more likely than targeting *Sydney* or *Ethan* as *Finn* is less security conscious based on **Assumption 1,** by providing the right *Incentive* we can get his ITL credentials.

S3: Get *Finn’s* email address
Requirements: *Grey’s* role
Context: Phone ITL impersonating *Grey* asking for *Finn’s* email address. Explain why you don’t have it and why it’s necessary to have it.
Discussion: A little information on *Grey* should be enough to get the email address of *Finn*.

S2: Get *Grey’s* email address
Context: Approach *Grey* when he is leaving ITL and say that you are doing some work at ITL and was wondering what the best mode of transport is to get to ITL as it’s taken you along time today (*Affect*). Strike up conversation about *Grey*’s role at ITL, say that his line of work is rare to you and you have a friend who is interested in that area, would it be possible to have *Grey’s* email address to pass on (*Salience*).
Discussion: We can acquire *Grey’s* email address through another method. This is a trivial step.

S1: Get *Cleo’s* working hours
Context: Follow *Cleo* or approach her outside of ITL and offer her some work (*Incentive*). Ask for some contact details. Phone *Cleo* impersonating (*Messenger*) ITL and state that you a reviewing work and access hours to ITL. Ask her to confirm her exact hours at ITL.
Discussion: Just like S2 this is trivial and can be achieved in a variety of different ways.

Remarks: S1 to S5 is one example of how to work towards S6 which just has a set of requirements that must be in place. It doesn’t matter how the requirements for S6 are achieved, just that they are. The Social Engineering aspect of any attack always works towards that final step. The important aspect in this scenario is identifying that the security requirements of Server 1 and Server 2 are integrity and availability respectively and using it to our advantage.

Countermeasures + Experiment

In order to defend against behavioural affects we could provide counter effects. Policies such as Counter-*Incentive,* which ensure that no matter the circumstances, sensitive information should not be stored alongside non-sensitive information. Consider *Counter-Messenger* where external parties must verify through another communication channel, such as phoning back the authorities on a number advertised online to verify the authenticity of a call.

An ideal experiment would show how an adversary uses influential effects to nudge subjects into making adverse security decisions.

References

[1] Dolan, P. Hallsworth, M. Halpern, D. King, D. Metcalfe, R and Vlaev. I. Influencing behaviour: The mindspace way. Journal of Economic Psychology, 33(1):264{277, 2012.