Chad Ballay

Week 9 – 1

CYBR320-342

06/21/2020

**Human Factors & Social Engineering**

*On your own, develop a pretext that can be used to test the susceptibility of the CEO from your hypothetical Fortune 500 company. Include a paragraph that is describing what you are trying to achieve if this works, the results that can be gathered from this activity, and how those results can be used to prevent security risks.*

This one will require some assumptions about the working relationship at the company. In theory everyone should welcome the opportunity for being a part of an exercise that increases the security of the company. In practice that may not always be correct.

I would make my first engagement one that is low risk and establishes the rules and procedures around internal security reviews. With the CEO’s consent I would approach our HR/Security area with the scenario that it looks like the CEO is exfiltrating company information and that we would need to confirm this. Access logs, records, logins, etc.…. Again, this would be with the CEO knowing this tomfoolery was going on but HR/Security not being aware.

The goal is to review how the company handles delicate breaches like this. Do we establish a chain of custody? Can we definitively prove or disprove what someone was doing? Do we maintain operational security? How does our process on paper differ from in practice?

At the end of the engagement, and especially if successful there should be a very public announcement of the details of this engagement. One to clear up any rumors that may have been started. But to also telegraph that security is taken very seriously and that no one is above reproach.

Not much tactically is gained from this exercise but strategically it sets things up for the subsequent and more focused program. It should, and this is where the devil is in the details, demonstrate to the C-suite that security is a professional run organization and that we can be trusted.

Some of those later engagements:

* Auditing of two factor mechanisms to try and spoof the C-Suite’s cellphones for SMS verification challenges.
* Social Media. Both as to try and impersonate themselves as well as to impersonate someone contacting them.
* If allowed I would try to see if an onsite audit of their home network could be included. Their personal machines may be company owned but what about printing locally? Or web cameras in their office? Or any of the countless other ways that a persistent attacker could try to gain insight.

But this is all predicated on the idea that the relationship with the C-suite level requires some priming before going full on. If that relationship is already there, then most of the tests I can think of are around testing the CEO Fraud style engagements. The problem isn’t usually the single person with the CEO title. It’s how much that person’s name getting dropped in conversations cause people to make otherwise idiotic decisions. Ignoring routine verification on requests due to urgency. Or fear of upsetting the powers that be.

This one requires a strong backing because people will fail this test and it’s the go between people that need to be identified and “encouraged” to think more. The accounts payable manager that tells their underlying to handle the CEO’s email not the underling needs to be chastised. It’s the intermediary that is facilitating the work not the person who did the work. Those intermediaries are the central nervous system though. Most times their sense of urgency is how large things get moving quickly. It’s a very delicate needle to thread of retaining their usefulness to upper, upper management while course correcting their behavior.