Exercise 06: Social Engineering

Jan-Matthias Braun

29. of October, 2022

Social engineering plays an important role in a majority of real-world breaches. In summary,"Social Engineering is the art of convincing someone to do something, they normally wouldn't do, through psychological manipulation". As it targets humans, it poses the danger of bypassing all technological security features.

Introduction

Social Engineering in general can be seen as the approach to trick people into behaviours which are disadvantageous for them or their organisation. The tools of the trade goes from nudging the unconscious, over pushing and threatening to blackmail. Ways to influence, persuasion and convince people form the soft end of the tool box.

Potential attacks range from untargeted phishing campaings to targeted "spear fishing" attacks. For the latter, attackers will try to gain information about the individual's and organisation's processes and values to be better able to tailor the manipulation.

On the defender's side, therefore, you need provide technical as well as informative means to support people in withstanding attacks. Knowing about the attacker's techniques allows to explain why shortcuts must not be taken and prepare people how attacks will look like.

As an example: opening a door for someone else might be considered polite, but it should not obliterate your access policy, e.g., the use of key-cards or similar access control mechanisms.

Many of the keywords presented in the lecture will be digested best, when trying them out. Therefore, you have this exercise to do so and discuss the different tool boxes.

Defense

- †Which technical tools can be used to defend against social engineering attacks and against which?
- †Give examples on how you, as IT-experts, can either stop or mitigate Social Engineering.

Experiment: Attack & Defence

For this exercise, we will have two teams, the attackers and the defenders. In each team, form smaller groups of $2 - -4$ *Social Engineers* and *Defenders*.

The *Social Engineers* will

- †tailor an attack based on the information on our fictive victim DAN (see slides), based on the lecture materials. Discuss your choices.

The *Defenders* will

- †tailor a course to DAN, to make sure that he is aware of and protected in the best possible way against social engineering attacks. Optionally, you can think about a nice concept on how to do this, but this is not the essential part. Discuss your choices.

Afterwards, regroup to have small groups with both, *Social Engineers* and *Defenders*

- †Present your approaches and then discuss if your strategies are matched or if you could strengthen the defence or harden the attack.

If you participate in the exercises, the participants can simply split up into two teams and then into groups. If you are not participating in the exercises, please find yourself a (project-) group and try to have enough people together to split into a *Social Engineer* and a *Defender* group.