Social Engineering

Prevention and mitigation

Kaido Kikkas

No hope at all?

- ...considering the previous lectures
- Not ‘if’ but rather ‘when’
- Still, a full solution should address both:
  - Proactive/preventive measures trying to ward off attacks
  - Reactive/mitigating ones to minimize damages

Good old Mitnick...

- Security = technology x training x policy
- If one component is zero or very small, so will be the total!
- 2 out of 3 are people-oriented (social)

Hadnagy’s six steps (2011)

- Learning to identify social engineering attacks
- Creating a personal security awareness program
- Creating awareness of the value of the information that is being sought by social engineers
- Keeping software updated
- Developing scripts
- Learning from social engineering audits

- Develop a security awareness culture

Another version from Hadnagy 2018

- M.A.P.P., or Mitigation and Prevention Plan
  - Learn to identify Social Engineering Attacks
  - Develop Actionable and Realistic Policies
  - Perform Regular Real-World Checkups
  - Implement Applicable Security-Awareness Programs
- Some good points:
  - Do not assume that people ‘should know it’ (awareness starts from knowing that the danger in fact exists)
  - Scripted security policy can prevent excessive paranoia (“I do care and want to help you, we just need to follow some rules”)
  - Gamification might be an option (CtF games, safe pranks etc)

Discussion break

- Where should be the ‘balance point’ between prevention and mitigation (e.g. if you could spend a total of 1000€ on them, how much would you use on each)?
- In the Mitnick’s formula, all three components (tech, training, policy) count, but can have different weights. Find examples with (each) one prevailing (e.g. policy is the most important by far)
- Hadnagy has describe essentially the same thing in different ways in his 2011 and 2018 books. Which version would you prefer, and why?
- Find some risk factors / threats for each step in the Hadnagy’s M.A.P.P.

Awareness

- Generic, widespread knowledge instead of ‘educated elite’
- Following the news and learning from them
- Periodical checks/audits

A personal program

- The CTF game in several Defcons
- Fortune 500 companies with ample funds, yet fail spectacularly in security. Problem: not my personal business
- Training should ‘drop them into water’ (e.g. enter a password and see it cracked) – and draw a direct parallel with their personal safety (e.g. bank account)
- Should also include using phone

Information is valuable!

- The basic process in SE: obtain small pieces of information, use them to get bigger ones
- Small pieces are often not valued
- Examples: garbage management, cleaning service, cafeteria
  - Staff as targets (respect is scarce there, and can work wonders)
  - Staff as culprits (infiltration; e.g. drinking water provider or a cafeteria worker)
- Special notice: learn to withstand emotional requests and personal charm

Software updates...?

- (actually, should not be a topic at all)
- Yet in corporate settings, the problem is often a mix of technical glitches (e.g. incompatibilities), managerial stupidity (“do rather something useful!”) and “not my job” (initiative can be punished in several ways)
- Part of awareness: if everyone knows that “we are using Windows 10”, then a “Windows 11 fixer” could at least be repelled (if not uncovered)
- Should also be scripted (see next slide)

Scripting

- In (European) football, players use drills for standard situations (corners, throw-ins, free kicks, goal kicks etc)
- Similarly, simple standard situations should be scripted into drills (e.g. “someone calls and asks for account numbers”)
- Example:
  - Ask for ID
  - Ask for project information
  - If OK, answer the request. If not, say “call the boss”

Audits

- Audit strives to simulate real attack, with two differences
  - All actions within legal limits
  - No harm done
- Those two can limit the scope!
- Make right conclusions (e.g. firing the victims is not)
- No personal information

Simple examples

- Click on that link!
- Check out that site (and answer some questions)
- Use that USB stick!
- Phone and personal contacts (also off-site, e.g. gym)
- Physical perimeter security (cameras, guards)

Other things to include

- Phishing (and all its variants: smish, vish, spearphish...)
- Pretexting (different ones – law/rules, power, empathy)
- Baiting (besides USB sticks, could do a more ‘old school’ one with a planted (paper) book, a note with ‘some secret’ inside)
- Tailgating (an interesting idea: invite a celebrity)
- Physical entry (simulated theft)

A classification

Table 1: Classification of social engineering attacks according to our taxonomy.

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Attack	Baiting
Channel	E-Mail	✓			✓			
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓		✓

From: “Social Engineering Attacks on the Knowledge Worker” by Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl
https://www.sba-research.org/wp-content/uploads/publications/sig-alternate.pdf

Discussion break

- Let’s imagine you are tasked with carrying out a SE awaress training at our university. What kind of exercises would you include, and why?
- Suggest some SE mitigation scripts that could be used by the office manager / secretary at IT College
- How would SE training for top management (e.g. at the university, the Rector’s and Deans’ offices) differ from a similar training for ‘mere mortals’?

Advice by Johnny Long (“No Tech Hacking”)

- Go undercover (do not flaunt, e.g. stickers)
- Shred everything
- Get decent locks
- Put that badge away
- Check surveillance gear
- Shut down the surfers (e.g. viewing angles)
- Block tailgaters (policy! Quitting smoking also helps)
- Clean your car (stickers again, plus all kinds of paper)

Conclusion

- 2 out of 3 in Mitnick’s formula focus on people and SE
- Balance between training and policy
- Make it personal (both in knowledge and concern)
- Trust but test (regularly)

… and that’s it

- … for this run of the SE course
- The first big patch of people did pass the course last week already
- Today is also the last (CotW) seminar – we will try to find some time to wrap things up
- Hope that everyone enjoyed (we did, even if it was not a trivial effort)

Thanks