Topic 7: prevention and mitigation

Social Engineering (II909)

Kaido Kikkas

Some remarks

- Had to switch two last topics due to large workload
- Reminder: papers wanted for next Friday!

No hope?

- Considering the previous lectures
- Not ‘if’ but rather ‘when’
- Still, a full solution should address both:
  - Preventive measures trying to ward off attacks
  - Reactive ones to minimize damages

The Mitnick Formula

- 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)

6 steps (Christopher Hadnagy)

- 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

Learn to identify attacks

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

Personal awareness 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

Knowing the value of information

- The basic process in SE: obtain small pieces of information, use them to get bigger ones
- Small pieces are often not valued
- E.g. waste processing, dining places, cleaning service
- 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 and ‘not my job’
- Should also be scripted (see next slide)

Using scripts

- In (European) football, players use drills for standard situations (corners, 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”

Learn from audits

- Audit strives to simulate real attack, with two differences
  - All action 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

A sample audit

- 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)

Can also include

- Phishing
- Pretexting (in a controlled manner)
- Baiting
- Tailgating
- Physical entry (simulated theft)

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

Recommendations from Johnny Long

- 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)

Conclusions

- 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)

Thanks!

- Next time, some stories (and EOC)