Social Engineering
The devil is in the details

05. March 2015, Ivano Somaini
Hobby
Study
Work
WHO AM I
My first experience...
"Any act that influences a person to take an action that may or may not be in their best interest."
"Any act that influences a person to take an action that is not in their best interest."
New attack vectors
https://www.youtube.com/watch?v=F7pYHN9iC9I
Today I’ll present you

5 social engineering tests…
…which were successful!
Exploit 1 - Helpfulness/Authority
Mission

Goal

- Gain access to the restricted employee area of the building
- Gain access to the internal protected area
- Steal confidential information (i.e. USB sticks, documents etc.)

Information from the customer

- Company name
- Building address
Information Gathering

Information gathered

- Medium-sized private bank
- No public area
- Reception with security guard with full height turnstile with badge reader
- Garage entrance with badge reader
- And…
Coffee delivery service coming every day between 07:00 – 07:30

...has access to the garage and a badge for the secondary entrance
Quiet Place
Tailgating / Piggybacking
Simulate phone call

Very effective to indirectly communicate/suggest:

- Authority
- Need for help
- Internal Know-How – Pretexting
- Etc.
Countermeasures

- Every entrance should have the same level of protection
- Teach staff that transitions into further internal protected zones are as critical as the checks performed on the first entrance
- Never let a visitor alone roam through your organization
- Employees and external suppliers should be trained to ask for visitor badges
- Accompany the visitor to the person he is intended to meet
Exploit 2 - Curiousness

“Curiosity killed the cat” – Phishing/Baiting
Mission

Goal

- Gain confidential information from employees through indirect attacks

Information from the customer

- Company name
Information Gathering

Information gathered

- Swiss Bank
- 500 ~ 600 employee
- Mail address of 250 employee
- And…
75th anniversary of the Bank
...time for a bonus?!?
Wrong delivery address
Countermeasures

- Deny delivering emails containing dangerous / unexpected file types (especially executables)
- Macro Settings should be controlled by a GPO. Either disallow the execution of macros completely, or selectively allow the execution of signed macros only.
- The authenticity and the origin of mails – or in general every form of requests and inquiries – should be checked before any other action takes place
Exploit 3 - Holiday
Mission

Goal

- Get the IT support company to change a firewall rule

Information from the customer

- Company name
- Support company name
- Contact data of the responsible technician
Information Gathering

Information gathered

- Name of the boss of the responsible technician
- And…
Sehr geehrte Damen und Herren


Bei dringenden Angelegenheiten wenden Sie sich bitte an meine Stellvertreter:

Besten Dank für Ihr Verständnis.

Freundliche Grüße
Upload Generation
Other attack vector...

- Analyze social network activity
- Try to reach the target during school holidays
Weitere Informationen

Interessen
Bicycles, design, table soccer, music, movies, mountain biking
Fake e-mail

victim

+ 

URENTE

= PRETEXT

= STRESS!!!
PRETEXT + STRESS = 🚫
Countermeasures

- The authenticity and the origin of mails – or in general every form of requests and inquiries – should be checked before any other action takes place
- If possible, avoid automatic e-mail for 80% job
- Raise awareness about information disclosed on social network
Exploit 4 - BYOD
Mission

Goal
- Gain access to the confidential data of the CEO

Information from the customer
- Company name
- Name of the personal assistant of the CEO
Information Gathered

Information gathered

- Mobile phone number of CISO
- Mobile phone number of personal assistant of CEO
Attack Scenario

“Hi Martina, this morning during the evaluation of the weekly security scan result we noticed that a security hole allowed a virus to infect many machines. We are further analyzing the issue with an external company.

Ivano Somaini from Compass Security will show up in 15 min at the headquarter in order to analyze your PC. I'll call you in 2 hour to give you an update. Now I've a meeting about the incident. Cheers, Karl”
Countermeasures

- Call the initiator back to confirm his identity and request
- Create awareness that phones are as vulnerable to spoofing attack as e.g. emails
- The authenticity and the origin of the SMS and phone calls – or in general every form of requests and inquiries – should be checked before any other action takes place
- Ideally disable signature in response mail
- Ideally don’t insert mobile number in signature
Mission

Goal

✈ Gain access to the secured area of the building
✈ Steal confidential information (i.e. USB sticks, documents etc.)

Information from the customer

✈ Company name
✈ Building address
Information Gathering

Information gathered

- Traditional Swiss company
- No public area
- Single Point-of-Entry
- Full height turnstile with badge reader
Attack Scenario

It was the 5th of December...

Would you ask Santa Claus for an identification card?
Unintended consequences
Countermeasures

- Never let a visitor alone roam through your organization
- The receptionist, and ideally, also the internal employee has to verify the identity of every person who get access to the secured area of the company
- Request a valid badge to exit the building
Conclusions

PAY ATTENTION TO DETAIL

Thank you
Question?