Social Engineering in modern cyberspace and IT Security threats

When we discuss IT Security threats, the importance of human factor is increasing drastically. For IT professionals, it sounds counter-intuitive: the whole IT Security technology is trying to substitute human interaction and decision making with artificial intelligence (AI) and machine learning (ML). Today, IT administrators have many tools which not only suggesting the next steps, but sometimes executing them and just informing the person about what was done. If this is the case, why human factor instead of being under better control, becomes even more important?

The answer is simple: does not matter who decides, human or robot, does matter who creates and manages decision criteria and who and how handles exceptions. Yes, no rules can exist without dealing with extraordinary situations. So, human factor, i.e. psychology, plays crucial role when rules are defined or exceptions are handled.

In IT security, the User is the weakest link in the chain of the corporate infrastructure. Your greatest risk. At the same time, Users are the entire reason IT and security exist. Making it necessary to deal with their quirks and imperfections. It is for this reason that most IT security and policies are based on restrictions and violations.

Today's professional hackers are applied psychologists, business analysts and only then technologists. They know how to make an email appealing and trustworthy looking enough that user will open it and click on the attachment to infect his computer. They know what technique to use to get out of the person his/her administrative password to penetrate the organization. They know exactly how much ransom money to ask after crippling the company ability to operate, so it is cheaper to pay the intruder than to fix the issue. All of that lie in the area of social engineering, so our conclusion is simple: if you want to improve IT Security and mitigate digital threats, you better start learning more about human behavior in cyberspace.

Here is the list of discussion topics:

- What is behind "social engineering" attacks: attackers, potential targets, methods, goals
- "Hot Buttons" used by hackers:
    - Curiosity – make topic of the conversation or message interesting for

    - the potential target
    - Greed - convince the potential target of financial gains if he/she follows the advice in the message or during the conversation
    - Fear – convince the potential target of bad consequences if he/she does not do what the attacker conveys in the conversation or message
    - Pride – show the potential target that employer treats him/her unfairly and there is no reason to be loyal to the company

- Process flows used by attackers:
    - Ambiguity of business policies – convincing the potential target that he/she does not brake company policy due to not clear language
    - Poor handling of exceptions – introducing exception case with no clear way to handle it and proposing the solution which benefits the attacker
    - Company politics – using love/hate relationship between some of the business leaders and Subject Matter Experts to manipulate them making decisions in favor of the attacker cause
- Recommendations how to mitigate social engineering:
    - Improve trust between regular users, business managers and technical administrators, so people would prefer honest conversation in case of doubts instead of making compulsive decisions.
    - Better education of people involved in company business on all levels related to social engineering methods and goals
    - Better handling of policy exceptions – have a plan how to do it
    - Re-evaluate the company goals and effectiveness of the campaign to deliver them to the policy constituents. Again, honesty and openness are your two best friends.
- Role of psychology and psychology professionals in mitigating social engineering attacks and building better IT Security response.