Deutor Cyber Security Best Practice Conference 04-05. December 2019

Workshop Proposal

Christina Lekati (Cyber Risk GmbH)

Title:

“Social Engineering Workshop: Defending against human exploitation and removing attack verticals”

Bio:

Christina Lekati is a psychologist and a social engineer.

She has learned the mechanisms of behavior, motivation, decision making, but also manipulation and deceit. She became particularly interested in human dynamics and she is passionate about social engineering.

Contrary to typical career paths, her history and involvement in the cybersecurity field started quite early in her life. Being raised by George Lekatis, a sought-after cyber security expert, she found herself magnetized by the security field at a very young age. Growing up, she was able to get involved in projects that were often beyond her age but gave her an edge in understanding important areas of risk management in general, and cyber risk in particular.

Christina has participated among other things in penetration tests, in training to companies and organizations, and in needs and vulnerability assessments.

She is working with Cyber Risk GmbH as a social engineering expert and trainer.

Christina is the main developer of the social engineering training programs provided by Cyber Risk GmbH. These programs are based on lessons learned from real life cases in the fields of cybersecurity, psychology and counterintelligence. They often cover unique aspects that cannot be found in any other existing training program.

Christina Lekati

Abstract:

Social Engineering has become the most effective and efficient attack method used to initiate and enable attacks. We read in the news about large-scale security violations, where investigators are not able to understand the phase of initiation. These are often social engineering-initiated attacks. By design, this is the type of attack that moves in the shadows, delivered by criminals and state-sponsored agents that are able to blend in multiple environments and often leave no trace, making it very difficult to identify the point of initial compromise. Similar to warfare operations, these threat actors strive to create an asymmetrical advantage based on a carefully planned strategy.

How relevant is social engineering today, and which is the risk for companies and organizations? This workshop aims to discuss these questions and to provide insights on the methodology employed by attackers that gives them an asymmetrical advantage. We will take a look at the typical backbone and methodology of a social engineering attack strategy, as well as on what makes some targets more attractive than others.

Information is the lifeblood of most attacks. as their operations are primarily based on the quality of the information gathered. We will discuss the information that attackers commonly seek to gather, as well as the common methods of information harvesting. Being able to disrupt or minimize these verticals is critical for the defense of an organization.

Taking it a step further, we will also explore a methodology of profiling followed by attackers, in order to identify and select the best targets. This part helps attendees identify whether their own online presence or that of their co-workers, reveals potential vulnerabilities and exposes attack vectors.

Last but not least, attendees will be provided with examples of best practices that aim to increase their organizational security and create a human perimeter- one with employees that are able not only to identify but also deter attackers and notify the organization of potential threats.

Throughout the workshop, attendees will have the opportunity to engage in problem solving exercises and discussion.

Workshop Outline:

- How much of a threat is Social Engineering, realistically?
- Social Engineering Attack Kill-Chain: The pieces and the puzzle
- Criminal Mindset: Characteristics of targets that yield a high attack-ROI
- The information that makes you vulnerable
- Common Information Harvesting Techniques
  - OSINT
  - HUMINT
- Profiling, targeting, and victimizing
- Case Studies
- Best Practices & Building a Social Engineering defense strategy