IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

THE HUMAN ELEMENT IN CYBER SECURITY: EXPLORING BEHAVIORAL SCIENCE AND SOCIAL ENGINEERING THREATS

[1]Sheik Lalasha, [2]Yenugupalli Sowjanya, [3]Chevuru Dayakar [1]Assistant Professor, Dept. of MCA, BVC College of Engineering, Palacharla [2]Assistant Professor, Dept. of CSE, BVC College of Engineering,

Abstract: The role of the human factor in cyber security is increasing and playing the crucial role of robust cyber security practices. The Technology solutions in the mobile and digital Era are becoming more helpful in informing the population, education, system monitoring, tracking the individuals working and spending time from home. The other side of the coin the valuable information within such systems is positive to the risk of breaches at the individuals and also at an organizational level. One of the major threats in cyber security is social engineering. To protect from these social engineering attacks a fundamental work is to know what consists in the social engineering. To explore the importance of behavioral insights and training strategies in enhancing cyber security in the context of human behavior will be discussed in this paper. We delves into psychological factors influencing cyber security behavior such as cognitive biases, social engineering techniques and also human errors. To examine the application of behavioral insights including leveraging behavioral economics principles and nudging techniques to promote secure behaviors. Many security incidence and data breaches are associated with the human factor in cyber security it is one of the most significant topics in the present era. The third party emphasizes in the role of human factors in security and elaborates on the behavioral approaches to investigate behavioral sciences and understanding the influence of human factors in cyber security with the help of ontology. The domain ontology defines 11 concepts of core entities that significantly constitute or affect social engineering domain together with 22 kinds of relations describing how these entities are related to each other.

Keywords: Social Engineering, Human factors, ontology, behavioral, monitoring, population, cyber securities, constitute, economics, data breaches, tracking.

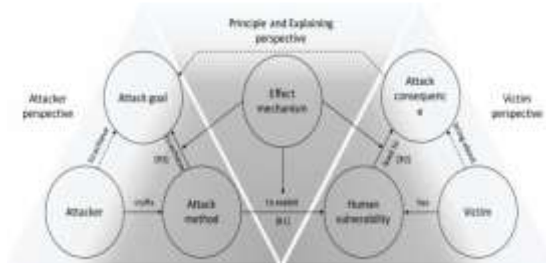
I. Introduction

In hacker community social engineering is required popular attack since 1970s. The social engineering is a type of attack in which the attacker exploits human vulnerability that means influence, deception manipulation and inducing to preach the security goals of Cyber elements like infrastructure, data, resource, user and operations. Many distinctive features make social engineering to be a quite popular attack in hacker community and a serious universal and persistent threat to cyber security. when compared to classical attack such as password cracking by brute force and software vulnerability exploit social engineering exploit human vulnerability to bypass or break through security barriers without having to combat with firewalls or antivirus software by Deep coding. For some attacks social engineering can be as simple as making a phone call and impersonating and inside it to elicit the classified information which is also called as sensitive information. Human vulnerability seems inevitable, after all there is not a cyber system don't rely on humans or involve human factors on the earth these human factors are vulnerable obviously or can be easily largely turned into security vulnerability by skilled attackers. social engineering gets not only large amounts of sensitive information about people network and devices but also more attack channels with the wide applications of Social Networking Sites (SNSs), IoT, industrial internet, mobile communication and wearable devices.

II. contributions:

To protect against social engineering attack and important work keys to understand how it works and take affect the contributions in this paper are as follows:

1. An interrogative and structural model to describe how social engineering a text works and take effect.
2. 3 core entities to get an inside to social engineering attacks.
3. 30 + effective mechanism involving 6 aspects.
4. 40 + human vulnerability involves 6 aspect s.
5. Case study of 16 social engineering attack scenarios including 30 type attack methods.



Social engineering attacks exploit a white range of human vulnerability the following aspects will discuss these vulnerabilities which are included in social engineering a text section:

1. Cognition and knowledge

Inertial thinking is a relatively rigid way, process or mode to think about something it can be also describe as a relatively stable behavior tendency and psychological readiness state the derived from previous experience and cognition.

2. Behavior and habit

When a person does not pay enough attention to the security contact or in unwilling to make necessary work or effort to prevent a security thread the person will be a target through whom a social engineering attack occur easily. Fixed action pattern exist in behaviors of both animal and humans which consists of series of relatively invent instinctive behavior started by a key stimulus this set of actions are automatic and involuntary and will go to completion even if the stimulus is removed.

3. Psychological factor

Psychological factors are individual level elements that influence thoughts, feelings and behaviors, affecting how people preserve process and react to situations. They encompass various aspects of mind and Psyche including personality, emotions, attitude, belief, motivation and learning.

4. Emotion and feeling

Emotions and feelings influence cognition attitude and diction making. Emotions and feelings are the all human factors can be exploit as security vulnerability in social engineering a text fare of getting into trouble with the superiors is often used in name dropping approach to a list sensitive information and fair arousing is presented.

III. Psychological Vulnerabilities:

The psychological vulnerabilities are further divided into three levels that is

1. Human nature

Human nature is a collection of psychological characteristics at the micro level, which describes the fundamental psychological characteristics shared naturally by the whole human being. Some human natures are security or notice exploitable in social engineering attacks. People who play close attention to themselves and their decides will magnify the ambient influence and increase the susceptibility to induce, persuade and manipulate in social engineering.

2. Personality traits

Individuals personality traits significantly contribute to their susceptibility to social engineering explore such as influence manipulation and deception. Social engineers treat human personality traits as vulnerability and use the language as their weapon to deceive, persuade and finally manipulate the victims.

3. Individual characteristics

Individual characters are psychologically characteristics that acquired with the influence of external environment and developed based on human nature and personality traits in the context of cyber security when some positive individual characteristics are emordinate or in inappropriate situation negative results can be generated if trust is sub situated by credulity, deception occurs easily.

From the evolution prospective of human wholeness to individuation.

That about able illustrate how to use the three core entities that is effect to mechanism human vulnerability and attack methods of conceptual model to get an inside into social engineering attacks. Some of these attack scenarios are based on cases in work and 13 types of social engineering attack methods are included in these 16 scenarios. The first column describe the attack method and scenario and second third column respectively show the corresponding effect mechanism and human vulnerabilities these items in the letter to column covers almost all effective mechanisms discussed about human vulnerability.

IV. Methodologies:

Ontology is a stretched formal representation of knowledge that define concepts properties and relationships within the domain. The following aspects are the methods of ontology.

1. Thread intelligence sharing
2. Risk assessment and management
3. Incident response

4. Automated reasoning and machine learning
5. Knowledge representation

In cyber security ontology provide structure way to represent and organize knowledge and share and standing of concepts like threats, vulnerability and attack vectors. This structure representation facilitates semantic analysis interoperability, and automatic reasoning, improving threat intelligence and incident response. There is no single correct way or methodology for developing ontologies since ontology design is a creative process and manufactures will affect the design choices such as the potential applications of ontology the designer understanding and view of the domain different domain features and anticipations of ontology to be more intuitive, general, detailed, extensible and maintainable.

One of the ontology methods is risk assessment and management. It involves identifying potential hazards and risk analyzing their likelihood and severity and developing strategies to mitigate or eliminate them. Risk management is a broader ongoing process that includes risk assessment as a key component. It's about proactively addressing potential issues before the cause harm or significant disruption.

V. Conclusion:

The human factor remains one of the most critical and vulnerable elements in the realm of cyber security. Cyber thread continue to evolve with increasing sophistication, particularly through social engineering attacks, it becomes imperative to deepen our understanding of human behavior and psychological dynamics in the context of cyber security. This paper highlights multifaceted nature of social engineering, emphasizing how attacker exploit cognitive biases, personality traits, emotional responses, and habitual behaviors to gain another access to sensitive systems and data.
By leveraging behavioral insights such as those rooted in behavioral economics and cognitive psychology organization scheme developed effective training programs and nudging strategies that promote secure behavior among individuals. The ontology based approach discussed in the study provides structured framework to identify and analyze the inter relationships between core entities mechanism of attack and human vulnerabilities. This not only aids in modeling and simulating potential attack scenarios but also supports improved thread detection, risk management and incident response strategies.
In conclusion the integration of behavioral sciences into cyber security practices represents a proactive and sustainable approach to mitigating human centric threats. As technological differences continue to advance equal emphasizes must be placed on strengthening the human firewall through education awareness and psychological resilience. Only by addressing both the technical and human dimensions of cyber security can we build a more robust and secure digital feature.

VI. References

1. Social engineering in cyber security: a domain ontology and knowledge graph application examples. https://doi.org/10.1186/s42400-021-00094-6

2. The Role of Human Factor In Cyber security: Behavioral Insights and Training

Strategies. Volume:06/Issue:03/March-2024, www.irjmets.com

3. Human Factors In Cyber security: Risks And Impacts, https://zagrebsecurityforum.com/Portals/0/SecurityScienceJournal/SSJ%202_2_4%20HUMAN%20FACTORS%20IN%20CYBERSECURITY%20RISKS%20AND%20IMPACTS.PDF

4. The Human Factor In Cyber Security, https://www.researchgate.net/publication/379430784

5. Social Engineering in Cyber security: Effect Mechanisms, Human Vulnerabilities and Attack Methods, https://ieeexplore.ieee.org/document/9323026

6. Ontology for Cyber security Governance of ICT Systems, https://ceur-ws.org/Vol-3260/paper4.pdf