Social Exploits

Micah L Wieburg

School Of Computer Information Sciences

University of the Cumberlands

MSCE-534: Principles of Cybersecurity

Dr. Eric Harmon

September 10 2023

Fall 2023

Social Exploits

The hacking of several high-profile Twitter accounts is documented to have occurred due to a social engineering attack against Twitter employees by leveraging existing relationships to gain access to an administrator panel, allowing hackers to hijack any Twitter account. According to NetworkChuck (2020), the belief is that the hackers gained access to this panel through the social engineering practices of manipulating a pre-existing relationship with a Twitter employee and bribery. These tactics verify that social engineering continues to be a significant security concern for organizations related to the susceptibility of their employees to fall for these tactics. Moreover, understanding the various social engineering strategies that hackers utilize is critical for recognizing these hacking attempts and creating ways to mitigate the associated risks.

Mechanisms used in Social Engineering

Social engineering attacks can be executed through various exploits to achieve success, which includes bypassing traditional security measures to gain access to the target system. Salahdine & Kaabouch (2019) state that these social engineering exploits can be social, technical, or physical-based attacks, with each attack type carrying its associated risks. These categories of social engineering assemble three forms of strategies that typically govern how they are executed. Furthermore, each form of social engineering exploit is performed to take advantage of the human element of cyber security.

A social-based social engineering attack can be cumbersome to prevent as it includes manipulating trust among humans. Salahdine & Kaabouch (2019) defines social-based attacks as the most dangerous type of social engineering attack because the attackers use relationships with the victims to play on their emotions and psychology through baiting and spear phishing attacks. This attack approach argues that human emotion will remain the most vulnerable element of security measures as people are needed to manage critical systems for organizations. Nevertheless, the technical-based social engineering attack is also a method that poses a risk for organizations.

Technical-based social engineering exploits tend to be more preventable as they deal with less of the social element of traditional human interaction. Salahdine & Kaabouch (2019) describes technical-based attacks as occurring on the internet through social networks and other online service websites to obtain the desired passwords, security question answers, and sensitive credit card information. The technical aspect of this attack verifies that social engineering can occur and be effective in one of the primary forms of online communication, which further increases the threat of such activity. Additionally, the physical-based social engineering attack is an exploit that organizations should understand.

Physical-based social engineering attacks can be viewed as the least risky form of social engineering attack as they involve bypassing physical barriers. According to Salahdine & Kaabouch (2019), physical-based attacks are conducted through physical actions executed by the attackers to obtain data about the target of the attack. This physical element of the attack proposes that physical security can not be discounted when defending against social engineering attacks. Consequently, mitigation efforts must be established to combat the risks associated with physical, technical, and social-based social engineering attacks.

Mechanisms for Mitigating Social Engineering

To combat an attacker's social engineering attempts, certain types of conditioning training using psychological principles can be applied to potential targets of these attacks. Schaab et al.

(2017) states that the inoculation defense mechanism can prepare users to resist social engineering attacks by exposing them to arguments that a social engineer may use and providing counterarguments to combat the attacker's persuasion. This familiarity with social engineers constructs a foundation for users to be prepared to recognize a social engineering attack and avoid being a victim of these attempts. Nevertheless, psychological preparation effectiveness would be hampered by some decision-making habits.

A user's decision-making capabilities during a social engineering attack can be the difference between success and failure for the attacker, solidifying decision-making training as a valuable defense mechanism. Schaab et al. (2017) mention that training through recurring exposure to various social engineering approaches aids in creating effective strategies against attacks by conditioning users from making intuitive or impulsive judgments. The benefits of decision-making training qualify as a viable option for preparing users against social engineering tactics. Furthermore, the best approach for defending against social engineering can be determined based on the nature of the attacks.

Best Approach for Mitigating Social Engineering

The exploitation of the human element of a system makes social engineering attacks challenging to defend against, as traditional cybersecurity areas tend only to defend the systems rather than its maintainers and must be supported through other means. Whitty (2019) comments that reducing the susceptibility to attacks, such as social engineering, must consider personality, sociodemographics, and routine activities. Considering numerous attributes when defending against social engineering defends the need to incorporate methods such as training through psychological principles as this approach goes beyond cybersecurity areas. Therefore, organizations must prepare their employees to deal with the persuasive nature of social engineering attacks to avoid an incident similar to the Twitter hack.

Conclusion

Social engineering attacks present complex challenges to corporations due to human nature, as seen in the hacking of high-profile accounts on Twitter. These attacks can exist in a social-based, technical-based, or physical-based form to gain access to a target system. To mitigate these attacks, increasing familiarity with social engineering attempts through training with psychological principles and situational responses can hamper the effectiveness of the attacks. This approach tends to show positive results as research has shown that multiple attributes of humans should be considered when determining susceptibility to scams and social engineering. By recognizing these attacks as a severe security risk, organizations can begin to foster the appropriate mitigation efforts.

References

NetworkChuck. (2020, July 21). *how a social engineering attack DESTROYED Twitter (feat. Marcus Hutchins) // Twitter Hack 2020*. Retrieved September 5, 2023, from https://www.youtube.com/watch?v=GE5J_26Ut1Q

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: a survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information and Computer Security*, *25*(2), 206–222. https://doi.org/10.1108/ICS-04-2017-0022

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *27*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095