Case Study: Twitter Bitcoin Scam

Introduction

An issue relevant to cybersecurity where social sciences play a significant role is the Twitter Bitcoin Scam of 2020. Twitter's internal systems were accessed by unauthorized attackers. Staff was maniuplated and other social engineering techniques were used against employees to gain tools and credentials.

Analysis

Attackers exploited psychological points to twitter staff to gain unauthorized access, attacking urgency, authority, trust, and expectation. Thinking was not rational due to the quick responses of staff as receiving and ignoring the possibility of unauthorized users. Impersonated staff and fake requests were used to gain trust of employees in which they fell for. Victims were expected to be rewarded for following attackers' directions.

Some sociological behavior experienced was rushed environment, network reactions, and social influence. Employees were not focused on noticing the attackers due to a fast past setting. A single post spread rapidly through the internet, and millions saw it immediately. Followers trusted the meesages that came from well-known accounts.

Solutions

Some comprehensive solutions that integrate technical cybersecurity measures with social science insights are advancing cybersecurity measures such as access controls based on roles. Employee access to tools should be limited to those only needed for their job. Multi-factor authentication is a way to have extra verification for employees who can access internal tools. Incident response should be created and effective for containing situations like this one. Some social scienceprecautions that can be taken are simulations for scams and attacks, social

engineering awareness training, and frequent reports, such as encouraging employees to report suspicious requests.

Barriers that may exist are economic issues such as training and tools advancement costs, human error regardless of training, employees not wanting to adjust to new rules, and the continued spread of misinformation such as users still falling for scams.

Reflection

The twitter bitcoin scam shows that human challenges are just as important as technical. Tools are not enough to prevent attacks, and human error needs to be decreased. The combination of social sciences and cybersecurity in this event shows the psychological aspect of how people fall for scams. Sociology, in how trust is achieved and spread. A multidisciplinary approach allows for multiple perspectives to be identified and strengthens people and system protection.

Some takeaways from this scam include “routinely monitor your social media channels, acknowledge you aren’t impervious to cyberthreats, and educate your team on social engineering tactics” (Mitnick 1).

Conclusion

This scam exemplifies how cyberattacks exploit social and technical aspects of society. The prevention of attacks like these cannot be overshadowed by thinking of technical solutions but also giving attention to social science perspectives as well.

Reference(s)

Security, Mitnick. “The 2020 Twitter Bitcoin Scam: How It Happened and Key Lessons from Whitehat Hacker Kevin Mitnick.” Mitnick Security Consulting, Mitnick Security Consulting, LLC, 12 Dec. 2022, www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam.