

Case Study - Cybersecurity and Social Sciences

Introduction

On July 15th, 2020, hackers compromised over a hundred and thirty high profile verified twitter accounts, which includes those of Elon Musk, Barack Obama, Joe Biden, Bill Gates, and even companies such as Apple and Uber. Using these accounts they posted Bitcoin scam tweets that promised to double any cryptocurrency sent to a specified wallet; this was framed as a charitable act during the COVID-19 pandemic. This attack ultimately gained approximately 118,000 dollars worth in Bitcoin before Twitter removed the postings.

Technologically, the breach involved no malware or exploits, but rather unauthorized access to the internal administrative tools of twitter. Socially, it succeeded through its coordinated phishing attacks which exploited human trust and the organization's vulnerabilities, thus showing how cybersecurity failures typically come from humans instead of mere technical weaknesses.

Analysis

Social science perspectives show how this attack succeeded in the first place. Firstly, from a psychological perspective, it is observed that the attackers used Robert Cialdini's principles of persuasion, particularly with regard to authority and urgency. This is because they had impersonated Twitter's IT help desk, therefore claiming to fix common VPN issues that were a real conundrum during the era of widespread remote work, and had employees go to fake login portals. This exploited their fear, trust, and compliance under seemingly legitimate pressure, thereby bypassing the technical safeguards they had in place like multi-factor authentication.

Furthermore, from a sociologically and business/organizational perspective, the cybersecurity attack showed several flaws in Twitter's security culture at large. Over a thousand employees had some kind of broad access to sensitive tools, and the shift to remote work during the era of the pandemic had eroded the typical verification norms that were setup, and increased reliance on communication via the phone. Additionally, without strong leadership at the head (Twitter didn't have a permanent CISO at this time), organizational trust became a great liability instead of being a strength. Finally, an interdisciplinary lens shows social engineering as a converged threat that intertwines technical access with human manipulation, thus resulting in the insufficiency of isolated IT defenses.

Solutions

For solutions to be effective they must implement technical controls and combine them with insights from social science. For technical purposes, integrate least privilege access, hardware based phishing resistant MFA for admin tools, real time monitoring, and regular access recertification. For social purposes, implement evidence based training programs that use behavioral psychology, like simulated phishing exercises and different kinds of nudges that counter cognitive biases such as authority bias, while at the same time fostering a security conscious organizational culture by leadership modeling and have clear verification protocols: never share credentials via phone, for example.

Barriers to said solutions include employees being fatigued by the training, them being resistant to the additional steps, these implementation costs being high for organizations that are smaller, and also the ever evolving nature of tactics. However, these and more can be overcome by a kind of gamified, metrics driven training, executive buy-ins that are tied to performance

incentives, and having the rollouts be phased with post incident audits to show the return on investment in the breach risk being reduced.

Reflection

It should be stated that combining cybersecurity with social sciences is quintessential because humans have continued to be the weakest and most powerful link in any system. Specifically, the Twitter case has shown that technical solutions by themselves will fail when attackers weaponize psychology and the dynamics of an organization. Significant insights received is the power of persuasion principles as well as the need for a proactive culture change. Moreover, a multidisciplinary approach will confer more resilient and ethical defenses by addressing the root behavioral causes instead of the symptoms, hence ultimately reducing both financial and societal harm that is caused by these cyber threats.

Conclusion

Overall, the 2020 Twitter incident showed that cybersecurity is ultimately inherently human centered. Thus, by integrating psychological, sociological, and technical strategies, organizations can better build their defenses in order to anticipate manipulation, thus turning human factors from vulnerabilities into strengths.

References

New York State Department of Financial Services. (2020). Report on investigation of Twitter's July 15, 2020 cybersecurity incident and the implications for election security.

https://www.dfs.ny.gov/Twitter_Report

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, 4, Article 100126.

<https://doi.org/10.1016/j.chbr.2021.100126>