BIZCOMMUNITY

Did Twitter ignore basic security measures? A cybersecurity expert explains a whistleblower's claims

By Richard Forno

2 Sep 2022

Twitter's former security chief, Peiter "Mudge" Zatko, filed a whistleblower complaint with the Securities and Exchange Commission in July 2022, accusing the microblogging platform company of serious security failings.

Source: www.unsplash.com

The accusations amplified the ongoing drama of Twitter's potential sale to Elon Musk.

Zatko spent decades as an ethical hacker, private researcher, government adviser and executive at some of the most prominent internet companies and government offices. He is practically a legend in the cybersecurity industry.

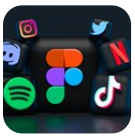
Because of his reputation, when he speaks, people and governments normally listen – which underscores the seriousness of his complaint against Twitter.

As a former cybersecurity industry practitioner and current cybersecurity researcher, I believe that Zatko's most damning accusations center around Twitter's alleged failure to have a solid cybersecurity plan to protect user data, deploy internal controls to guard against insider threats and ensure the company's systems were current and properly updated.

Zatko also alleged that Twitter executives were less than forthcoming about cybersecurity incidents on the platform when briefing both regulators and the company's board of directors. He claimed that Twitter prioritized user growth over reducing spam and other unwanted content that poisoned the platform and detracted from the user experience. His complaint also expressed concerns about the company's business practices.

Alleged security failures

Zatko's allegations paint a disturbing picture of not only the state of Twitter's cybersecurity as a social media platform, but also the security consciousness of Twitter as a company. Both points are relevant given Twitter's position in global communications and the ongoing struggle against online extremism and disinformation.



Social media ads are about to change - how new rules on content marketing will affect what you see and share

Rafaello Rossi and Agnes Nairn 1 Sep 2022

Perhaps the most significant of Zatko's allegations is his claim that nearly half of Twitter's employees have direct access to user data and Twitter's source code.

Time-tested cybersecurity practices don't allow so many people with this level of "root" or "privileged" permission to access sensitive systems and data. If true, this means that Twitter could be ripe for exploitation either from within or by outside adversaries assisted by people on the inside who may not have been properly vetted.

Zatko also alleges that Twitter's data centers may not be as secure, resilient or reliable as the company claims. He estimated that nearly half of Twitter's 500,000 servers around the world lack basic security controls such as running up-to-date and vendor-supported software or encrypting the user data stored on them.

He also noted that the company's lack of a robust business continuity plan means that should several of its data centers fail due to a cyber incident or other disaster, it could lead to an existential company ending event.

These are just some of the claims made in Zatko's complaint. If his allegations are true, Twitter has failed Cybersecurity 101.

Concerns over foreign government interference

Zatko's allegations might also present a national security concern. Twitter has been used to spread disinformation and propaganda in recent years during global events like the pandemic and national elections.

For example, Zatko's report stated that the Indian government forced Twitter to hire government agents, who would have access to vast amounts of Twitter's sensitive data. In response, India's at-times hostile neighbor Pakistan accused India of trying to infiltrate the security system of Twitter "in an effort to curb fundamental freedoms."

Given Twitter's global footprint as a communications platform, other nations such as Russia and China could require the company to hire its own government agents as a condition of allowing the company to operate in their country. Zatko's allegations about Twitter's internal security raise the possibility of criminals, activists, hostile governments or their supporters seeking to exploit Twitter's systems and user data by recruiting or blackmailing its employees may well present a national security concern.

Worse, Twitter's own information about its users, their interests and who they follow and interact with on the platform could facilitate targeting for disinformation campaigns, blackmail or other nefarious purposes. Such foreign targeting of prominent companies and their employees has been a major counterintelligence worry in the national security community for decades.

Fallout

Whatever the outcome of Zatko's complaint in Congress, the SEC or other federal agencies, it already is part of Musk's latest legal filings as he tries to back out of his purchase of Twitter.

Battle lines drawn in Musk Twitter battle

23 Aug 2022

Ideally, in light of these disclosures, Twitter will take corrective action to improve the company's cybersecurity systems and practices. A good first step the company could take is reviewing and limiting who has root access to its systems, source code and user data to the minimum number necessary.

The company should also ensure that its production systems are kept current and that it is effectively prepared to contend with any type of emergency situation without significantly disrupting its global operations.

From a broader perspective, Zatko's complaint underscores the critical and sometimes uncomfortable role cybersecurity plays in modern organisations. Cybersecurity professionals like Zatko understand that no company or government agency likes publicity for cybersecurity problems.

They tend to think long and hard about whether and how to raise cybersecurity concerns like these – and what the potential ramifications might be. In this case, Zatko says his disclosures reflect "the job he was hired to do" as head of security for a social media platform that he says "is critical to democracy."

For companies like Twitter, bad cybersecurity news often results in a public relations nightmare that could affect share price and their standing in the marketplace, not to mention attract the interest of regulators and lawmakers. For governments, such revelations can lead to a lack of trust in the institutions created to serve society, in addition to potentially creating distracting political noise.

Unfortunately, how cybersecurity problems are discovered, disclosed and handled remains a difficult and sometimes controversial process, with no easy solution both for cybersecurity professionals and today's organisations.

ABOUT THE AUTHOR

Richard Forno is the principal lecturer in computer science and electrical engineering, University of Maryland, Baltimore County