BUSINESS
INSIDER

Subscribe

Saudi Arabia reportedly paid Twitter employees to spy on users. Cybersecurity experts say insider spying is an issue that goes beyond Twitter.

Aaron Holmes 21 hours ago

Saudi Crown Prince Mohammed bin Salman, right. Reuters

US federal prosecutors have charged two former Twitter employees with spying on users on behalf of Saudi Arabia's government — and experts warn that it could happen again.

Three cybersecurity experts told Business Insider about broader "insider threats," or the risk of surveillance and data breaches carried out by people employed by tech companies.

The experts warned that tech companies should implement safeguards by addressing workplace culture, setting up ways to detect unusual behavior by employees, and more robustly protecting user data across the board.

Visit Business Insider's homepage for more stories.

Federal charges unsealed Wednesday allege that Saudi Arabia carried out a massive online spying operation, snooping on the accounts of more than 6,000 Twitter users — and prosecutors say the country did it with the help of two Twitter employees.

Now, cybersecurity experts warn that similar "insider threats" could surface again if tech companies don't make a concerted effort to ward them off.

Twitter responded to the federal charges Wednesday, saying the company was thankful for the investigation and would cooperate with future investigations. A representative added that Twitter "limits access to sensitive account information to a limited group of trained and vetted employees." The two employees in question no longer work for the company.

Three cybersecurity consultants told Business Insider that to protect against insider spying going forward, tech companies needed to vet employees and implement more rigorous protections of user data across the board.

Ryan Kalember, the executive vice president of cybersecurity strategy for Proofpoint, said companies like Twitter should focus on detecting abnormal behavior by employees. Kalember estimated that more than 30% of data breaches happened with the help of insiders.

"Stopping insider threats is one of the most challenging problems in security," Kalember said, adding: "Defending data requires the ability to detect insider accounts that are behaving oddly, including patterns of accessing and exfiltrating sensitive information."

"But detection isn't enough," he added. "With the complexity of an enterprise infrastructure like Twitter's, being able to respond quickly to any detected anomalies across cloud, email, and endpoints is at least as critical."

Kiersten Todt, the managing director of the Cyber Readiness Institute who previously served as an adviser to President Barack Obama, said the spying linked to the Twitter employees was "another example of how the tech platforms have repeatedly failed to protect the personally identifiable information" of users.

Whether personally identifiable information was "compromised and exposed through an accidental data breach or insider efforts to harvest data," Todt said, "the point is still the same: Tech platforms continue to fall short on their accountability and responsibility for data protection."

Kon Leong, the president, CEO, and cofounder of ZL Technologies, predicts that similar breaches will become more likely as the value of user data goes up.

"That draws ever more bees to the honey," Leong said. "Whether for political or economic advantage, expect more break-in attempts to get at the data."

Leong suggests that tech companies implement top-down "data control" policies, ensuring that data is managed centrally rather than stored in uncontrolled data silos, which he said could "also simultaneously solve many other pressing problems such as compliance, e-discovery, records-keeping, and analytics."

The accusations of spying by Saudi agents are just the latest case in which foreign governments are suspected of targeting users on US-owned platforms. A series of high-profile iPhone hacks earlier this year were linked to the Chinese government, while investigations by law enforcement and media have uncovered a series of hacks carried out by Russia in recent years meant to influence US policy.

SEE ALSO: Saudi Arabia allegedly recruited Twitter employees to spy on users. That's just one of many ways Saudi agents use tech tools to spy on critics. »

NOW WATCH:

More: Tech Politics Twitter Cybersecurity ⌄

Sitemap | Disclaimer | Commerce Policy | Coupons | Made in NYC | Stock quotes by finanzen.net

International Editions:

INTL | DE | AUS | FR | IN | IT | JP | MY | NL | SE | PL | SG | ZA | ES