Credit: iStock.com/Roman Tiraspolsky

Cyber professionals weigh in on Capital One's cloud security claims

Sam Clark | 13 August 2019

Cybersecurity professionals have largely backed up Capital One's claims that its use of the cloud was not to blame for a recent data breach and even helped it fix vulnerabilities more quickly, but warned that opting to shift data storage out of house may complicate security efforts.

When the bank announced in late July that an attacker had taken millions of records from an Amazon server that it was using, Capital One claimed that its use of cloud technology helped it to identify and fix the vulnerability more quickly.

Jeffrey Starr, an executive at network security company AlgoSec, said the claims could be true if the company "has the right security management tools in place".

"If they do, security teams can have visibility of their entire network, and execute change processes seamlessly and consistently across public clouds and on-premise networks from a single console," he said.

He added that the breach should not be used to argue that using cloud technology is insecure. "Instead, it highlights the need for centralised management and control over security in complex network environments," he said.

Capital One insisted after the attack that its use of cloud technology was not to blame for the attack. "The elements of infrastructure involved are common to both cloud and on-premises data centre environments," its press release said.

Information security technical experts and lawyers have told GDR that this claim is largely correct. AlgoSec's Starr said that Capital One was right to say that the incident wasn't specifically related to cloud security. "It was a misconfiguration, and these happen just as frequently in on-premise networks as in the cloud," Starr said.

David Kennefick, product architect at vulnerability management company edgescan, told GDR that the cloud and in-house systems are likely to have similar vulnerabilities. "Certain vulnerabilities may allow a malicious actor to access this data without authorisation or by completely bypassing any authorisation checks. Hosting in the cloud as opposed to in-house will not mitigate this vulnerability, as the cloud is just somebody else's computer."

But observers noted that Capital One's use of cloud infrastructure may have involved delegating responsibility for infrastructure security to Amazon.

Chia Ling Koh, a partner at OC Queen Street in Singapore, said: "Organisations tend to rely on the security expertise and security management features of the cloud services provider for infrastructural security, such as server, storage and network security."

"If an organisation relies on cloud services for its IT infrastructure, then it only makes sense for it to also rely on the accompanying security management features of the cloud services," Koh said. "It may also be that Capital One has found it effective to rely on the security features of the cloud environment rather than to build its own for diagnosing and fixing vulnerabilities."

But Javvad Malik, security awareness advocate at KnowBe4, said that companies are still responsible for data, platform and operating system security whether they use cloud or on-premise infrastructure.

Malik added that using cloud technology such as Amazon's can add extra security complexity because it is more easily accessible by employees, meaning that identity and access management and controls need to be considered. Amazon has itself been sued over its role in the Capital One data breach.

Capital One did not respond to a request for clarification about its comments.