Two-factor authentication oversight led to JPMorgan breach

The attackers stole an employee's access credentials and used them to access a serv that lacked a stronger authentication mechanism, report says

By Lucian Constantin

CSO Senior Writer, IDG News Service

DEC 23, 2014 3:43 AM PST

The attackers who stole information about 83 million JPMorgan Chase customers earlier this year gained a foothold on the company's network because a server reportedly lacked two-factor authentication.

The attackers stole the login credentials of a JPMorgan employee and were able to access the server, despite the company's practice of using two-factor authentication on most of its systems, the New York Times reported citing unnamed sources familiar with the internal and external investigations at JPMorgan.

Two-factor authentication combines the use of static passwords with one-time-use access codes generated by physical hardware devices or mobile apps.

[Related: Online privacy: Best browsers, settings, and tips]

The JPMorgan security team apparently neglected to deploy two-factor authentication on one of the company's many servers, leading to the absence of a security layer that might have otherwise prevented the attack, *The New York Times* reported.

Following the initial intrusion, the attackers were eventually able to gain access to more than 90 servers at the bank, but didn't manage to steal sensitive financial information before they were detected and blocked in August.

The attackers were able to compromise names, addresses, phone numbers and email addresses, along with information about which line of business the customers were affiliated with, JPMorgan said on its site in October.

The wider breach was discovered after a compromise was detected in August on an external website set up for a charitable race sponsored by the bank. JPMorgan then determined that the attackers had also had access to other systems for months, *The*

The story echoes the warnings of security experts over the years that the breach of a single server or employee computer can put an entire network at risk.

There have been numerous cases where attackers exploited a vulnerability on a public facing website and then used the underlying Web server to pivot to the company's internal network. Cyberespionage groups also often compromise the computers of low-level employees using simple attacks like spear phishing and then move laterally inside the network by exploiting the security holes in other systems and the credentials of those employees.

Strong access-management policies and network segmentation are key to limiting the extent of damage that attackers can do once they gain a foothold inside a network. However, for organizations like JPMorgan, implementing uniform security controls across their vast networks can be difficult because they often have to integrate large numbers of new systems with different levels of security as a result of acquiring other companies.