cfc

Case study

A vulnerable VPN

Hackers access a bank's system through a vulnerable VPN, holding data for ransom

Using a virtual private network (VPN) is common practice now for many businesses as we move towards more digitally accessible methods. Whilst VPNs are used commonly in the financial services sector and are often secure, they can be susceptible to bugs and errors in coding that allows hackers to impersonate, gain access and exploit an organisation's network. This means data and sensitive information can be at risk of being leaked or held ransom.

The past 20 years have seen huge advancements in the use of technology, and almost all modern businesses now have some dependence on their computer systems, and those operating in the financial services sector are no different.

In fact, financial institutions have been at the forefront of the technology revolution, embracing everything from online banking to direct-to-customer quoting platforms. This has allowed them to provide better services, expand their customer base and increase their revenues. However, this reliance on computer systems comes with a drawback, as financial services are increasingly vulnerable to malicious cyber attacks.

One of the main drivers of cyber losses is ransomware. Ransomware is a type of malicious software or encryption program that works by encrypting data on a network and then demands that a ransom be paid in exchange for a decryption key to regain access to the data. Ransomware, when combined with unintentional access via a VPN can devastate a company economically as well as legally. Financial services deal heavily in sensitive data usage and storage and therefore need to be hyper-aware of the security measures in place to protect against cyber threats.

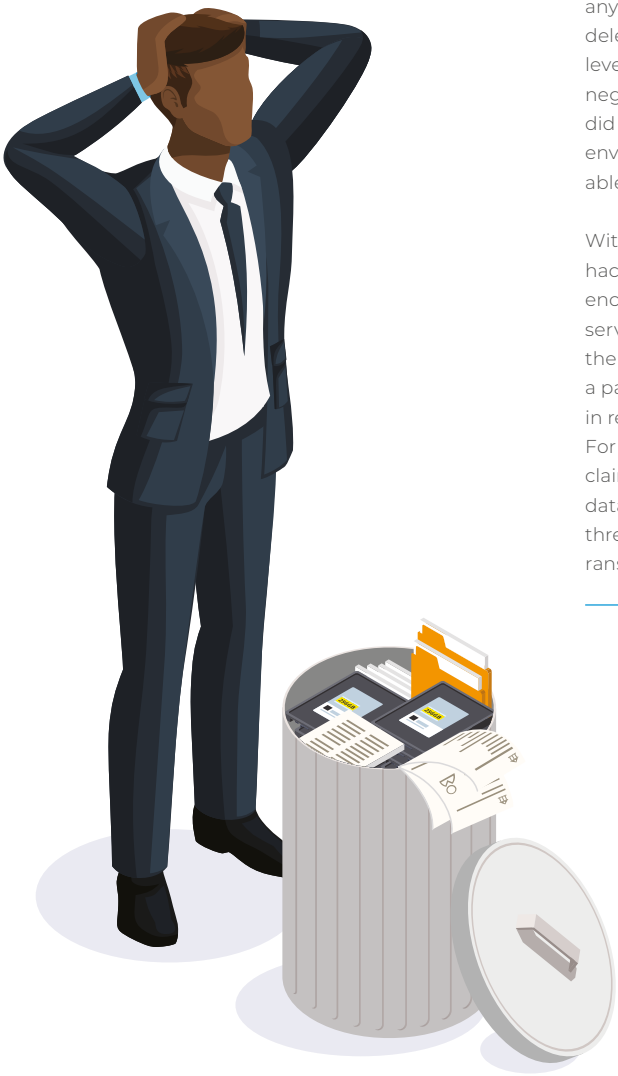
A VPN patch weakness gives hacker access

One of our policyholders who recently fell victim to a ransomware attack was a small bank who catered to both private and commercial customers with revenues of around $100 million.

The attack began when the hacker exploited a vulnerability in the insured's virtual private network (VPN). VPNs work by establishing an encrypted connection between two devices, meaning that anyone trying to intercept the connection only sees the encrypted version of the data. VPNs are often used as a remote access solution by organisations looking to allow employees to access their network whilst away from the workplace.

However, whilst VPNs are often a secure method for enabling remote access to the network, like any software asset VPNs can be susceptible to bugs and errors in coding that can allow imposters to gain access to an organisation's network. In this case, the bank's VPN had a vulnerability in place which allowed the attacker to read plain-text usernames and passwords for users of the bank's VPN application instead of the encrypted versions. Although a security patch was available from the VPN provider to fix this vulnerability, unfortunately the bank hadn't implemented it yet.

With these credentials at their disposal, the hacker was able to gain remote access to a legitimate user's account. Once the hacker was logged in, the next step was to escalate privileges. In order to do so, the hacker downloaded a password scraping malware from the internet onto the computer, which enabled them to obtain domain administrator account credentials, giving greater access across the network.



From here, the hacker used a scanning tool to gain information about what was on the bank's network. In particular, the hacker was searching for the location of any back-ups because if they could delete these, they might have more leverage in any future ransom negotiations. In this case, the bank did keep a back-up copy on its live environment and the hacker was able to locate and delete it.

With the preliminary work done, the hacker then went on to launch their encryption software across multiple servers, leaving a ransom note for the business and requesting that a payment of 60 Bitcoin be made in return for the decryption key. For good measure, the hacker also claimed to have stolen sensitive data from the organization and was threatening to release the data if the ransom wasn't paid.

A costly forensic investigation

Upon discovering the ransom note and realising that its computer systems and data were no longer accessible, the bank notified CFC's incident response team to determine the next step. The incident response team's first priority was to establish the status of the organisation's back-ups. Although the hacker had deleted a copy of the bank's back-ups that was stored on the organisation's live environment, fortunately the bank also had an offline back-up copy stored on a USB flash drive that was fully disconnected and inaccessible from the live environment. This meant that the bank was able to recover its data and systems within a short time frame and resume normal business operations.

Though the bank had managed to regain access to its computer systems, there was still a question mark over whether sensitive data had actually been accessed and stolen by the hacker. The bank stored a large amount of information on its customers, including bank details, payment card information, names, addresses and dates of birth. If this information had been accessed or exfiltrated during the course of the attack, a large scale notification process would have to be carried out to the effected customers.

CFC's in-house incident response team led a forensic investigation to find the root cause of the attack and discover what exactly the hacker had done while they had access to the bank's computer systems. This was a lengthy process as the bank had a fairly substantial network. After several weeks of investigations, it was determined that the hacker had not in fact accessed any sensitive information, and this was based on three factors: there was no evidence of large zip files being created, which are typically seen in cases of data exfiltration; the artifacts on the system relating to the attack appeared to be limited to harvesting password credentials, locating back-ups and encrypting files; and the amount of time the hacker spent on the system was not deemed to be long enough to carry out meaningful data exfiltration.

It appeared that the hacker's statement that they had stolen data appeared to be a bluff in order to encourage the bank to pay the ransom demand. Given that the bank had successfully recovered from back-ups and the forensic investigation had determined that no data exfiltration had occurred, the decision was made to not pay the ransom demand.

Despite avoiding paying the ransom demand, the cost of the attack was still significant. The forensic investigation alone came to some $113,897. This came on top of $22,000 in legal fees and $5,000 to engage a crisis communications consultancy to help deal with media relations following the attack, bringing to the total $140,897.

Update patches and back-up data

This incident highlights a few key points.

Updating computer systems as promptly as possible

Cyber criminals are constantly on the lookout for new vulnerabilities that they can exploit in order to gain access to organisations' computer systems. In this case, the hacker was able to gain access to the bank's systems because they had failed to patch its VPN for a critical security vulnerability. Had they implemented the patch as soon as it was released by the VPN provider, it's highly unlikely that the hacker would have gained access in the first place. It is therefore crucial that businesses make security patches as soon as is feasible.

Having offline back-ups

Organisations that keep their back-ups on their own live environments run the risk of these back-ups being deleted or encrypted by cybercriminals during the course of ransomware attacks, which can seriously weaken their leverage in ransom negotiations as well as causing significant disruption to business operations. In this instance, though the bank kept one back-up copy on the live environment which was deleted by the hacker, the organization had prudently chosen to store a copy offline too, allowing them to recover promptly and avoid any major operational disruption.

Finally, it highlights the value of cyber insurance. Though the bank was able to avoid paying a hefty ransom demand, the incident still resulted in expensive forensics, legal and crisis communication costs, all of which the bank would have had to absorb had it not been for their cyber insurance policy with CFC. Cyber insurance therefore provides a valuable safety net for organisations in the digital age.

cfcunderwriting.com