Armstrong Teasdale

June 29, 2021 • Advisory • www.atllp.com

COLONIAL PIPELINE: HOW HACKERS EXPLOITED A PASSWORD POLICY PROBLEM

A single password on an old, unprotected account – that's all it took for hackers to paralyze the largest fuel pipeline in the United States.

The account was no longer in use at the time of the attack, but the compromised password still worked – and with no other security measures in place, Colonial Pipeline was defenseless against the hackers that accessed its systems on May 7, 2021. Two days later, the federal government declared a state of emergency in 17 states and Washington, D.C., due to spiking gasoline prices, panic buying and thousands of empty gas stations on the East Coast, after Colonial shut down its pipeline operations to contain the cyberattack. After a six-day shutdown and a $4.4 million ransom paid to the attackers, Colonial's systems went back online. However, as high-profile cyberattacks and ransom payments provide incentives to other would-be hackers, similar ransomware attacks are likely to become even more frequent in the future.

Cyberattacks now pose a critical security threat in the United States. Payments to ransomware hackers totaled more than $350 million in 2020, an increase of 311% from 2019. While breaches at major corporations make the headlines, the majority of cyberattacks target small businesses, which are even less likely to employ adequate cybersecurity measures. With many businesses operating remotely due to the pandemic, the threat of cyberattacks has become even more dire. The account used by hackers in the Colonial attack was a virtual private network (VPN) account, the type of account widely used to allow employees to remotely access their employer's computer network.

However, basic cybersecurity standards could have foiled the Colonial hackers. To avoid falling prey to a similar attack, companies of every type and size should adopt the following fundamental security measures.

ENSURE THAT EMPLOYEES DO NOT REUSE THEIR PASSWORDS.

The Colonial hackers didn't need to use sophisticated software to guess the account's password. A Colonial employee had used that password on multiple independent websites prior to the cyberattack. When one of those websites became compromised, hackers likely obtained the employee's password, giving them everything they needed to access Colonial's systems.

PEOPLE

Lucas Amodio, C|EH

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

The security provided by complex, hard-to-guess passwords becomes entirely worthless once that password is compromised, and databases with millions of stolen passwords are available for sale online. Preventing employees from reusing passwords on multiple websites is one of the most important first steps in preventing security breaches.

EMPLOY MULTI-FACTOR AUTHENTICATION.

Once the Colonial hackers gained access to a compromised account, no secondary security measures stood in their way. That's why multi-factor authentication is necessary. Two-factor authentication would include having the user enter something they know (aka username and password) and prove that they have an object (such as their phone). For example, after correctly entering a username and password, users also have to enter a secondary security measure, such as a code texted to their mobile devices. While this won't foil every possible cyberattack, multi-factor authentication methods provide an extra layer of security that prevents bad actors like the Colonial hackers from strolling into an unprotected computer network with nothing more than a compromised password. President Biden's "Executive Order on Improving the Nation's Cybersecurity" strongly urged business leaders to mandate the use of multi-factor authentication methods in the wake of the Colonial attack.

DELETE OLD ACCOUNTS.

The compromised account used in the Colonial hack was tied to an inactive employee. However, the account itself remained active, which provided the attackers with access to Colonial's systems. To prevent this, company procedures for offboarding employees must include deleting the former employee's accounts. This also goes for old accounts from systems that are no longer in use. Otherwise, that account will forever be a potential target for hackers.

In the wake of the Colonial attack and the White House's Order, companies should analyze their own systems and look for similar security vulnerabilities that may be exploited. These proactive security measures are essential in safeguarding company systems against attack. Companies should look not only at their current cybersecurity practices, but also the legal implications of those cybersecurity practices. In a previous advisory on the Colonial Pipeline incident, Armstrong Teasdale's Privacy and Data Security attorneys discussed how companies can take proactive steps to prepare for prepare for potential cybersecurity intrusions.

Laurel Scott also contributed to this advisory.