Colonial Pipeline Ransomware Attack

Elijah Gartrell

Old Dominion University

CYSE 300 Introduction to Cybersecurity

Professor Malik Gladden

9/9/2023

Colonial Pipeline Ransomware Attack

Introduction

The Colonial Pipeline is a major pipeline on the East Coast that supplies more than half of the oil supply there. Making the Colonial Pipeline one of the most important critical infrastructures in the United States and one attack showed this. In May 2021 the entire East Coast of the United States went into a panic once Colonial Pipeline shut themselves down from attempting to stop a ransomware attack from spreading within their infrastructure. At this time the attackers DarkSide had already perceived to have stolen over 100 gigabytes of data in that time. This paper will cover the vulnerabilities that the Colonial Pipeline had, the aftermath of the situation, and how the incident could have been prevented.

Vulnerabilities

The initial "hack" of the Colonial Pipeline system was a compromised VPN account password that was said to be "Outdated". The password to this VPN account was leaked in a separate data leak, in which it has been concluded that this employee was using the same passwords for multiple accounts. Unable to find their security protocols before but the current website reads that Colonial Pipeline is NIST & ISO 200 compliant. Although VPNs are a semi secure way to log onto accounts there should have been MFA involved within that login process for an extra layer of security.

Aftermath

Once it was revealed that they were under a ransomware attack the pipeline shut down immediately following that. Making consumers along the East Coast anxious and worried along with spiking gas prices. Gas prices went up 18-21 cents along the East Coast and consumers were waiting in gas lines for up to an hour. This attack was so big on our critical infrastructure that President Biden called a State of Emergency. Post the Mandiant investigation of the

situation the CEO paid DarkSide a 4.4 million dollars in ransom for the data back. Following that the pipeline was back and running and in about a month's time 2.3 million of the 4.4 paid was recovered via a court order.

Preventative Measures

As stated in the Vulnerabilities section I could not find their exact security protocols beforehand, but here is a list of measures that could've helped this situation. MFA would have been a huge help within the initial access of the pipeline's network. If the attacker had only the account and password but no authorization DarkSide would have had a harder time getting in. Sectioning off the network and deploying a Zero Trust architecture for their network. This will help if the attacker already has access trying to escalate privileges and move through the network would be troubling. Implementing stronger password rules and requiring passwords to be changed every 3-6 months. Lastly, having an incident response team for cyber and an up to date cybersecurity department. It was reported that Colonial Pipeline was looking for a Cybersecurity manager role weeks before, possibly if we had the personnel and the protocols in place this would not happen.

Conclusion

The Colonial Pipeline Ransomware attack was one of the biggest attacks on US critical infrastructure to this day. The company now has implemented cybersecurity protocols and the Biden administration has been keen to improving cybersecurity within this space as well.

References

Amanda_M_Macias. (2021, June 8). *U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline Ransom*. CNBC. https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html

The attack on Colonial Pipeline: What we've learned & what we've done over the past two years: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2023, August 28). https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Author links open overlay panelTsvetan Tsvetanov, 7, A. M., AtkinsonBenjamin, ByrneDavid P., CoffeyMark, CrosignaniMatteo, & (EIA), E. I. A. (2021, October 12). *The effect of the colonial pipeline shutdown on gasoline prices*. Economics Letters. https://www.sciencedirect.com/science/article/abs/pii/S0165176521003992#:~:text=Within%20a%20week%20of%20the,country%20(Morris%2C%202021).

Cybersecurity Risk Management. Colonial Pipeline Company. (n.d.). https://www.colpipe.com/about-us/pipeline-operations-in-todays-world/cybersecurity-risk-management

Jones, D. (2022, May 17). *How the colonial pipeline attack instilled urgency in cybersecurity*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/#:~:text=Threat%20actors%20linked%20to%20the,at%20risk%20of%20remote%20takeover.

Kerner, S. M. (2022, April 26). *Colonial pipeline hack explained: Everything you need to know*. WhatIs.com. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know