PES2UG22CS556_SIRI_N_SHETTY_SOLUTIONS_AC

by Siri N Shetty

Submission date: 30-Oct-2024 09:15AM (UTC+0530)
Submission ID: 2502282455
File name: PES2UG22CS556_SIRI_N_SHETTY_SOLUTIONS_AC.pdf (365.5K)
Word count: 1096
Character count: 6468

UE22CS342AA4 – Applied Cryptography

Colonial Pipeline – Case Study

Siri N Shetty PES2UG22CS556

1. There was a dual role of cryptography in this case:

   Attackers used cryptographic techniques to encrypt Colonial Pipeline's data, preventing access to essential systems. The attacks employed a hybrid approach -encrypting most of the data using fast symmetric encryption first, and then encrypting them with asymmetric encryption for further security against decryption without having an appropriate private key. This technique ensured that only the attackers, holding the private key, could decrypt the files, effectively controlling access.

   The attackers demanded a ransom for the decryption key, using cryptography to gain financial power over the victim. This situation shows how, in ransomware, the secrecy of encryption keys becomes a bargaining tool. It complicates the victim's data recovery efforts and pressuring them into paying for key access.

2. The way in which Colonial Pipeline handles the crisis had its own strengths and weaknesses.
   Strengths: Colonial maintained closed systems within hours from the discovery of the attack and issued many public releases during the incident. This helped manage public opinion and kept stakeholders informed. Colonial involved federal agencies like the FBI to gather intelligence that would help understand what the DarkSide was and how the attack commenced and how to minimize damage.
   Although the impact, Colonial continued pipeline operations a couple of days after the accident, which indicates effective management of the crisis for fuel supply re-stabilization.
   Weaknesses: The Decision of Colonies to pay approximately $4.4 million in ransom which allowed them to retrieve their decryption keys was controversial. Payment of the ransom may facilitate further attacks as it

validates the business model of ransomware. Furthermore, it was not known if the data was going to be fully restored or other security issues were in the pipeline. The crisis highlighted Colonial's lack of a robust cybersecurity response plan. Questions arose about whether the company had adequate incident response and backup protocols. Some stakeholders expressed concerns over Colonial's lack of transparency during initial stages. A more transparent, structured communication plan might have helped better manage public concerns, especially around fuel shortages.

3. The company did well in the following aspects:
   - Upon detecting the ransomware, Colonial Pipeline quickly shut down operations to prevent further spread. This limited the attacker's reach and helped in reducing further data loss.
   - Involving FBI and other federal agencies helped Colonial gain immense support for assessing the threat and minimizing the damage. This also helped in indentifying DarkSide's tactics.
   - Colonial kept their stakeholders and the public updated, which helped in managing the information flow and also helped in addressing the concerns about fuel availability. This also helped in stabilizing public during the event.

   The company could improve in the following areas:
   - The incident highlighted the need for a more structured cybersecurity incident response plan. Colonial could streamline their efforts.
   - The way Colonial resented on paying the ransom suggests that the backup systems were either insufficient or not implemented properly. A robust backup and recovery strategy would help in avoiding this.
   - They could communicate more transparently to avoid public from panic.

   Lessons learnt from Incident
   - Importance of being prepared for a ransomware
   - Organisations should think about the further consequences before paying huge ransom. It can fuel the ransomware economy and can have long term negative effects.
   - Companies with high public impact must invest in cybersecurity measures. Regular security assessments must be conducted.

4. It can be done in the following ways:
   - Use Multi-Factor Authentication to access sensitive data. This adds an additional security layer.
   - Limit data access strictly to employees who need it for their roles, which minimizes the risk of internal breaches.
   - Use encryption both in transit and at rest to protect data.
   - Use a combination of symmetric and asymmetric encryption to balance efficiency and security.
   - Regularly audit systems for vulnerabilities, ensuring they meet the latest security standards.
   - Train employees to recognize phishing, social engineering and other common attack methods.
   - Conduct regular security simulations to prepare staff for breach scenarios, so that they can respond quickly and effectively.
   - Form an incident response team.
   - Invest in advanced security tools
   - Segment networks to prevent Lateral movement.
   - Backup data regularly with a Secure Strategy.
   - Ensure that antivirus and anti-malware solutions, as well as all software patches, are kept up to date to guard against evolving threats.

5. Blount's decision to pay the ransom to recover Colonial Pipeline's systems was a complex and controversial choice.
   Paying the ransom allowed Colonial to rapidly regain access to their data and resume operations. Given that the pipeline supplies fuel to a significant portion of the U.S. East Coast, restoring service quickly was crucial to avoid severe economic and public disruptions. Colonial's shutdown had immediate consequences, including fuel shortages and panic buying. With pressure from the government and the public, paying the ransom mitigated the risk of prolonged supply chain issues. Also, Colonial did not have an adequate backup system that could restore services without the decryption key.

   But, paying ransoms can encourage attackers by funding ransomware operations and encouraging more attacks on other organizations, contributing

to a cycle of cybercrime. There is no guarantee that attackers will honor their promise. Even after payment, Colonial faced issues with slow decryption and had to rely on its own resources to expedite the process. The decision to pay could negatively affect Colonial's reputation, as it suggests unpreparedness for cybersecurity incidents.

6. In general, organizations should avoid paying ransomware.

   Paying ransoms directly supports the ransomware economy and industry, providing cybercriminals with resources and incentives to continue their attacks. Each successful ransom payment leads to more sophisticated and frequent attacks targeting other organizations.

   Cybercriminals may not honor their promise to provide decryption keys, even after payment. Many cases have shown that victims either do not receive the promised decryption keys or receive keys that work only partially, leaving some data inaccessible.

   In some cases, paying ransomware may violate legal and regulatory guidelines. If the attackers are on government sanctions lists, payment could lead to fines or other legal consequences for the organization.

   Paying a ransom may make an organization a target for repeated attacks. Once criminals know a company is willing to pay, they or others might target it again, viewing it as a profitable victim.

   Beyond the immediate financial cost of the ransom, paying can tarnish an organization's reputation, leading stakeholders to question the company's security practices and readiness to handle cyber threats.

References:

1. Regular Security Assessments: Safety, Security and Risk https://link.springer.com/chapter/10.1007/978-3-658-37182-1_4
2. How to protect businesses from ransomware https://www.linkedin.com/pulse/ransomware-growing-threat-how-protect-your-business-prabhu-nerurkar-sib6f/

PES2UG22CS556_SIRI_N_SHETTY_SOLUTIONS_AC

ORIGINALITY REPORT

2%	0%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Indiana Wesleyan University Student Paper	2%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		