involve TECHNOLOGY

CASE STUDY: RANSOMWARE ATTACK ON EXCHANGE SERVER AND THE AFTERMATH AT A COMMERCIAL VEHICLE MANUFACTURER

Abstract

A medium-sized enterprise relied heavily on their on-premise Exchange server for communication and data storage. Despite their dependence on this system, the organization had not implemented a comprehensive disaster recovery as a service (DRaaS) solution, despite having received a proposal the previous year. They had a backup system in place but had not set up immutable backups, leaving their data vulnerable to cyberattacks.

Josh Lampe
lampe@involveITS.com – 610.216.3915

Case Study: Ransomware Attack on Exchange Server and the Aftermath at a Commercial Vehicle Manufacturer

Background

A medium-sized enterprise relied heavily on their on-premise Exchange server for communication and data storage. Despite their dependence on this system, the organization had not implemented a comprehensive disaster recovery as a service (DRaaS) solution, despite having received a proposal the previous year. They had a backup system in place but had not set up immutable backups, leaving their data vulnerable to cyberattacks.

In the midst of a successful cyberattack, the organization was forced to make critical decisions under pressure, ultimately opting to pay a hefty ransom rather than deal with the consequences of data loss. This case study explores the events leading up to the attack, the decisions made during the recovery process, and the lessons learned from this incident.

The Incident

1. Initial Compromise:

The cyberattack began with an undetermined method of entry, as the exchange system was compromised without immediate detection. It remains unclear how long the attacker had access before the breach was noticed. Given the lack of real-time monitoring and early warning systems, the compromise went undetected until the organization's administrator logged in to perform routine operations.

2. Malicious Script Execution:

Once the admin used their credentials to access the system, a malicious script was automatically triggered. This script began to propagate across other systems in the network, spreading the infection. The attack was sophisticated and automated, likely part of a ransomware campaign designed to cripple the organization’s operations and extract a ransom payment.

3. Backup Failure:

The organization’s backup strategy involved both on-site and online backups. However, a critical vulnerability was the lack of immutable backups for their online data. Once the attacker gained access to the network, they deleted the non-immutable online backups. This left the organization without a reliable means to restore their data, further complicating the situation.

4. Consultation with Insurance:

In the midst of chaos, the organization consulted with its cybersecurity insurance provider. After assessing the situation and the potential long-term impact of the attack, the decision was made to pay the ransom. The ransom demand was substantial, totaling

$400,000. While the amount was large, it was seen as a necessary expense to ensure business continuity.

Recovery Efforts

1. Migration to Microsoft 365 and the Cloud:

One of the first recovery steps taken was to migrate all users to Microsoft 365 and a cloud-based environment. This shift allowed the organization to regain access to email and critical communications, although some data may have been lost in the transition. The migration also marked the organization's first serious step toward adopting cloud technologies, which had been planned for some time.

2. Implementation of DRaaS:

In the wake of the attack, the organization realized the critical need for a robust disaster recovery plan. The proposal for a disaster recovery as a service (DRaaS) solution had been presented by a vendor, Involve, the previous year but had not been accepted due to cost concerns. However, given the magnitude of the breach and the ransom demand, the organization now recognized the importance of having a reliable, offsite backup and recovery system in place.

To prevent future incidents, the organization decided to implement DRaaS post-attack. The cost of implementing DRaaS was around $3,000 per month, significantly less than the ransom payment of $400,000. The decision to adopt DRaaS was seen as a key recovery strategy to ensure business continuity in the event of a future attack.

Key Lessons Learned

1. Importance of Immutable Backups:

The lack of immutable backups was a critical vulnerability that allowed the attacker to destroy the organization's data backups, significantly extending the recovery time. Immutable backups, which are write-once and cannot be deleted or altered, would have ensured that the organization could restore its data quickly, without having to rely on paying a ransom.

2. The Hidden Cost of Neglecting DRaaS:

The proposal for DRaaS, which had been presented a year earlier for $3,000 a month, was initially rejected due to budget constraints. However, the cost of not having a DRaaS solution in place ultimately led to a $400,000 ransom payment. This stark contrast between the cost of prevention and the price of recovery highlights the financial risks associated with neglecting disaster recovery solutions.

3. Ransomware Awareness and Planning:

The incident revealed the need for a more proactive approach to cybersecurity, including better detection mechanisms, regular vulnerability assessments, and a clear, well-rehearsed incident response plan. Ransomware attacks are becoming increasingly sophisticated, and organizations must be prepared to deal with such threats before they result in catastrophic losses.

4. Cloud Migration as a Contingency:
Migrating to Microsoft 365 and cloud-based services helped the organization restore communications and operations more quickly, demonstrating the value of cloud solutions as a contingency plan. This migration also gave the organization greater flexibility and scalability, reducing future risks associated with on-premise infrastructure.

5. Insurance Limitations:
While insurance can help mitigate the financial impact of a cyberattack, it does not provide the long-term solutions needed to prevent future incidents. Organizations must be cautious about relying too heavily on insurance as their primary defense against cyber threats. Comprehensive cybersecurity measures, including robust backups, training, and disaster recovery plans, are crucial.

Conclusion

This incident serves as a cautionary tale for organizations that have not fully embraced comprehensive backup and disaster recovery strategies. While the decision to pay the ransom may have seemed necessary at the time, the financial burden of that decision underscores the importance of preventive measures such as immutable backups, DRaaS, and proactive incident response planning. Had the organization implemented DRaaS at the proposal stage, they could have avoided paying the ransom altogether, saving valuable time, resources, and potentially millions of dollars.

For businesses looking to secure their operations, this case highlights the need for both technical preparedness and a mindset shift toward disaster recovery and cloud-based solutions. In today’s cyber threat landscape, taking steps to prevent an attack before it happens is far more cost-effective than dealing with the aftermath.