involve TECHNOLOGY

Case Study: Involve Helps Business Recover from Ransomware Attack and Migrate to Microsoft 365

A car dealership gets hit with Ransomware.
Involve triages and recovers all data and systems over one weekend.

Josh Lampe
Lampe@InvolveITS.com - 610.216.3915

Case Study: Involve Helps Business Recover from Ransomware Attack and Migrate to Microsoft 365

Client Background

The client, a mid-sized car dealership, had no prior business relationship with Involve. They were initially seeking assistance with migrating their infrastructure to Microsoft 365. Their needs dramatically shifted when a serious cybersecurity incident struck, ransomware crippled their entire IT environment, forcing them to seek urgent help.

The Challenge

Involve's initial engagement with the client was focused on facilitating a transition to Microsoft 365. However, during the scheduling of the migration, the client disclosed a significant issue: their network had been hit by ransomware, and their current Managed Service Provider (MSP) was unable to offer any support in resolving the situation.

Key challenges included:

1. Ransomware Attack: An employee had accidentally clicked on a malicious link, which allowed threat actors to gain administrative access and compromise the Exchange server.
2. Outdated Hardware: The client's storage hardware was no longer supported, further complicating recovery efforts.
3. Lack of Proper Security: Firewalls were not being updated or actively managed, creating an environment ripe for exploitation.
4. Widespread Compromise: The ransomware spread to all servers and endpoints across the network, disrupting operations entirely.

Given these severe challenges, the client was in a critical situation, with their entire IT infrastructure compromised, and no immediate means of restoring operations. Involve needed to act quickly and decisively.

Our Solution

Upon learning about the ransomware attack, Involve immediately mobilized a team and arrived on-site within an hour to assess the situation and begin mitigation efforts. The core objectives were clear:

- Contain the Damage: Prevent further spread of the ransomware.
- Restore Access: Retrieve essential data and restore operations as quickly as possible.
- Rebuild Infrastructure: Migrate to a more secure, modern environment to prevent future threats.

Key steps taken included:

1. Immediate Incident Response:
   - Involve's team began by isolating affected systems to prevent the ransomware from spreading further.

- We performed a full assessment of the compromised environment, which included servers, endpoints, and critical applications.

2. Data Recovery:
   - Thankfully, an off-site backup (albeit older) was available. This allowed us to restore critical data that had not been encrypted by the ransomware.
   - We used the backup to rebuild the organization's infrastructure and begin setting up a more secure environment.

3. Rebuilding the IT Environment:
   - Over the course of one weekend, Involve worked tirelessly to rebuild the client’s IT environment from scratch. The entire infrastructure was migrated to the cloud, including:
     - Domain Setup: We created a new domain to replace the compromised on-site infrastructure.
     - Microsoft 365 Migration: Microsoft 365 was implemented, providing a secure, cloud-based environment for email, file storage, and collaboration tools.
     - File Server in the Cloud: Critical files were securely migrated to cloud storage, ensuring redundancy and accessibility.

4. Disaster Recovery as a Service (DRaaS):
   - To ensure business continuity moving forward, we implemented Disaster Recovery as a Service(DRaaS). This solution replicated data to a secondary site, allowing for rapid recovery in case of future incidents.
   - The DRaaS solution was designed to be scalable, cost-effective, and fully managed, providing the client with peace of mind knowing that they were protected against future disruptions.

5. Ongoing Security Enhancements:
   - The client’s outdated firewalls were replaced, and we put in place proactive monitoring and management to ensure all security protocols were up to date.
   - Endpoint protection and additional layers of security were implemented across all devices to prevent further compromises.

6. Team Expansion and Coordination:
   - Involve brought in additional resources to speed up the recovery process. Our expanded team worked around the clock to ensure that the new environment was up and running smoothly, minimizing downtime and keeping the business operational.

Results

By the end of the weekend, the client was successfully operational again with a modernized IT infrastructure. The key outcomes of the project included:

- Full Recovery from Ransomware: Critical data was restored, and the client’s systems were no longer under threat. No data was permanently lost.
- Migrated to Microsoft 365: The migration to a secure, cloud-based platform ensured the client was operating in a more modern and scalable environment.
- New Disaster Recovery Solution: The implementation of DRaaS ensured that the client’s data was replicated and protected at a secondary site, providing a high level of business continuity in the event of future incidents.
- Enhanced Security Posture: The client’s security was drastically improved with updated firewalls, endpoint protection, and proactive monitoring, significantly reducing the risk of future cyberattacks.
- Minimal Downtime: Despite the extensive nature of the attack, Involve’s quick response meant that the client experienced minimal disruption and was able to continue operations throughout the recovery process.

Client Testimonial

"Involve was a lifesaver when our business was hit by a ransomware attack. We were completely overwhelmed, but their team responded quickly and professionally. Within hours, they had our systems isolated, and over the weekend, they not only recovered our data but completely rebuilt our IT environment. Thanks to them, we’re now more secure, and we have a reliable disaster recovery plan in place. We couldn’t be happier with the results."

Conclusion

Involve’s expertise in cybersecurity, cloud migration, and disaster recovery played a critical role in helping this client recover from a devastating ransomware attack. The incident highlighted the importance of proactive security measures, as well as the need for a modern, cloud-based infrastructure to mitigate risk and ensure business continuity.

This case serves as a testament to Involve’s commitment to client success and our ability to deliver comprehensive IT solutions in times of crisis. By acting quickly, implementing best practices, and leveraging cutting-edge technology, we were able to turn a potentially catastrophic situation into a long-term success.