MacroSoft™
An ISO 9001:2015 Company

Case Study: A Real-Life Ransomware Attack Mitigation for a Shipping and Transportation Company

Authors:

1. Scott Kalcic, Chief Security Officer
2. Todd Gerovac, Sr. Security Consultant
3. Joe Rafanelli, Director of Technical Solutions

Overview

The rise of cyberattacks has left businesses vulnerable to data breaches, system disruptions, and massive financial loss. One particularly devastating form of attack is ransomware, which can bring entire organizations to a standstill by encrypting critical files and demanding large payments for recovery.

A long-time client, a logistical shipping and transportation company has been working with our security team over 18 years. The client's IT infrastructure has grown increasingly complex over the years, prompting several proactive measures to strengthen their cybersecurity. The company's senior IT Director, oversees safeguarding the company's digital assets, supported by of expertise our cybersecurity consultants. Our team provides consulting in cybersecurity initiatives, disaster recovery, and IT infrastructure management.

In this case study, we explore the real-life ransomware experience of this client along with the methodology our team used to help mitigate the malicious attack. Through the dedicated efforts of our cybersecurity team, led by our Chief Security Officer, the attack was successfully mitigated in just a few days. Below, we dive deeper into the incident, the response strategy, and lessons learned to provide a comprehensive understanding of how businesses can combat ransomware effectively.

The Attack: A Sudden Crisis

The senior IT Director for the client, recalls the fateful moment when his team realized their systems had been compromised. As is often the case, the attack didn't occur during normal business hours but rather during off hours, causing a delay in identifying the attack.

He received an urgent off hour call from one of his colleagues reporting that files were missing, and that servers and systems were no longer functioning correctly. He quickly sprang into action, checking external connections such as the company's website, email and overall availability of data and systems and quickly realized that many networked systems were down. This was a clear sign that this was more than just a minor technical issue.

With his remote connectivity still operational, the senior IT Director was able to log in and access the company's internal servers. His worst fears were confirmed: all files had been encrypted. The company had fallen victim to a ransomware attack.

Recognizing the gravity of the situation, he knew that an organized and strategic response was essential and began execution of the companies Incident Response and Disaster Recovery plans, which our security experts helped create and implement a few months earlier. These plans included the implementation of a full Security Incident Response Team (SIRT).

Immediate Response: Executing Incident Response & Disaster Recovery Plans

The first step was to shut down internal and external network connectivity of systems to stop the ransomwares' ability to travel any further. The second step was to begin engaging the recovery team on site. This team consisted of the senior IT Director, key members of the company's executive management team and key members of our cybersecurity consulting team.

Once on site, the team began executing their pre-established incident and disaster recovery response plans. Members of the team immediately reached out to their DRAS (Disaster as a Recovery Service) to begin the recovery of systems. Other team members continued work to identify the source and extent of damage from the attack.

Escalation, Forensics & Mitigation: Damage Assessment and Recovery

Initial forensics indicated that the attack originated from a company users VPN account which had been compromised. The malicious actor had gained unauthorized access to the network by exploiting vulnerabilities within the VPN vendors remote access software. It was also discovered that the user that was compromised had access to a list of passwords to key business applications and systems which the bad actors were able to obtain. Recognizing this, the team immediately disabled all VPN services and systems and shut down all network account access.

As the SIRT team continued forensics, they engaged the internet service provider (ISP), who provides an SD-WAN solution to the company. They informed the ISP of the breach and provided a status of current forensic information. The ISP worked with the client to perform further forensics and network hardening to include the review and provisioning of logs, as well as the implementation of Geo Fencing to block communications from foreign countries and other undesirable external networks.

As the team identified sources of data and systems that were breached, they were quarantined, preventing any further spread of the ransomware. Simultaneously, critical event logs were collected for immediate and future forensic analysis, to develop a full understanding as it related to the scope and origin of the attack.

The client has a very stringent and secure DRAS service implemented which assisted in provisioning the full recovery of all systems. Unfortunately, it was discovered that the cloud portions of the DRAS system were compromised due the exposed password list. While this presented a challenge as it related to instant turn up of systems in the cloud, the overall solution is designed as a hybrid (on premise, replicate to cloud) model. Luckily the on-premises system is constructed with a secure segmented disk design, thus the DRAS vendor was able to provide a full recovery source for all systems from the local DRAS appliance. A secondary appliance was available to facilitate the recovery.

Once the SIRT team completed initial forensics and identified all the compromised assets, they began the recovery and replacement of compromised systems with the clean systems and data resident on the local DRAS appliance.

Due to proper incident and recovery planning, critical systems were brought online within 24 hours and the full recovery and turn up of all business systems was achieved within 2 days.

Lessons Learned: Enhancing Cybersecurity Pre & Post-Attack

Although the attacker was successful in their attack and the situation was mitigated, there are several lessons to be learned to help strengthen the company's cybersecurity posture moving forward.

1. Enhanced Security Policies: Although the company already had a solid cybersecurity framework, the attack revealed opportunities to implement more stringent written policies.
2. Enhanced Access Protection: While passwords were required for all systems access, the company culture did not enforce proper password complexity and change requirements. This alone may have helped avoid the attack. Post event, the password policies were hardened and enforced. While multi-factor authentication (MFA) was already in use, it had not been rolled out to every system and application. Post-attack, the client expanded the use of MFA across systems and applications wherever it was technically possible without inhibiting or creating an adverse effect on systems.

3. Managed Detection and Response (MDR) Solutions: Prior to the attack systems monitoring was only in place for network and virus monitoring and did not include a complete security monitoring of the entire environment. In the wake of the attack, the SIRT team opted to implement a Managed Detection and Response (MDR) solution, which provides continuous monitoring and threat intelligence. This new system offers real-time protection and alerting for unusual activities on the network, enabling faster and more automated responses to potential threats.

4. User Education: One of the lessons learned was the importance of educating users about cybersecurity best practices. Users often represent the weakest link in a company's defense, and educating employees on the importance of safe systems and online behaviour was implemented as part of the post-attack follow-up.

5. Proactive vs. Reactive Planning: Having a well-defined, tested, and rehearsed playbook in place was critical in handling the incident. Being proactive rather than reactive ensured that the company could avoid paying a ransom and minimize downtime. The incident response plan acted as a guide that helped the team stay focused during a stressful situation. The DRAS solution in place provided the ability to recover a full clean set of systems and return to service in just a few days. These solutions were highly effective during incident management and recovery and assisted in further identifying areas for improvement throughout the recovery phase.

6. Investment in Cybersecurity: Another key takeaway was the need for management buy-in when it comes to investing in cybersecurity tools and policies. This was not entirely the case until this event transpired. While implementing robust cybersecurity measures can be costly, the consequences of a successful ransomware attack can be far more expensive. The attack provided an opportunity to demonstrate the value of these investments to senior management, ensuring that additional resources were allocated to enhance security moving forward. The old "it won't happen to me, or we simply don't want to spend the money right now" narrative was put to rest.

Conclusion: The Importance of a Proactive Cybersecurity Approach

This event underscored the importance of preparation, teamwork, and continuous improvement in the face of cyber threats. Through the efforts of our cybersecurity team and the resilience of the senior IT Director's organization, the company was able to recover from a devastating attack without paying a ransom, losing critical data or suffering long-term operational damage. Further the company was able to execute a plan and recover fully from this event without exposing damage to their customers or reputation!

This case study serves as a reminder that cybersecurity is not a one-time investment but an ongoing process. Companies must remain vigilant, continuously update their security policies, and ensure that their incident and disaster recovery plans are in place, regularly tested and adapted to new threats. By staying proactive, businesses can not only recover from attacks but also prevent them from happening in the first place.

For businesses looking to enhance their cybersecurity defenses, this case study highlights the critical components of a successful strategy: comprehensive incident and disaster recovery planning, strong access controls, advanced threat detection, and ongoing employee training. With these measures in place, companies can mitigate the impact of ransomware and other cyber threats, safeguarding their operations and maintaining business continuity.

Macrosoft provides a full offering of Cybersecurity Consulting Services and welcomes you to reach out to our experts for a free 1-hour consultation to see how our services can help your business remain secure.

MacroSoft™
An ISO 9001:2015 Company

THANK YOU !

For More details please Contact Us.

Joe Rafanelli

Director of Migration Services

Macrosoft Inc

135 US-202/206 , Suite #9

Bedminster, NJ 07921.

EMail: jrafanelli@macrosoftinc.com

Cell: (973) 223 - 9717

www.macrosoftinc.com