Case Study
Ransomware Security Breach Summary: Food Production

Client

The client is a leading food producer that has been in business for many years and has experienced tremendous growth. The client has expanded to become a very important greenhouse vegetable producer—growing and selling tomatoes, peppers, and cucumbers. Being a rapidly growing business, they were looking for a service provider that would act as a trusted partner to rely on, help them securely address future growth needs, and modernize the way they are consuming IT.

Challenge	CBTS solution	Results
• Existing cloud and managed services provider targeted with a Ransomware email phishing attack • Unwitting employee downloaded malicious code that crippled their business • Cost of downtime is estimated at $200K/hour	• Managed security service that includes Security Information and Event Management (SIEM) tools capable of threat log organization • Log data is analyzed and correlated with the threat management tools to gain critical insight into the nature and scope of the attack and then begin containing the impact and recovery back to a steady state	• CBTS security experts contained and eliminated the Ransomware attack quickly and effectively • Production servers, databases, networks, computers, storage, backup and DR Environments were restored • With managed security services, in addition to managed cloud computing from CBTS, the client can rest assured that their business is being protected and that our team of experts is here to help in case of any incident

Security Challenge

Early on a Monday morning, the successful fruit and vegetable producer experienced a phishing e-mail security incident that very quickly resulted in a Ransomware attack that brought down their essential business infrastructure.

In a very common mistake, an employee opened an e-mail which downloaded malicious code that corrupted their systems, servers, and databases. This compromised all of their mission critical data that is required to run the business.

The cost of downtime for the client is estimated to be approximately $200K/hour, so the urgency to resolve the breach as quickly as possible was of the utmost importance to keep the business alive.

Security Solution

CBTS provides ongoing monitoring and management for the client's dedicated private cloud, including computer support, storage, networking backup and disaster recovery. In addition, to heighten the level of protection, CBTS delivers managed security services that include threat and log management based Security Information and Event Management (SIEM) tools.

Threat detection and log management from CBTS quickly identifies indicators of a compromise based on incident forensics and malicious activity monitoring. Log data is analyzed and correlated with the threat management activity to gain critical insight as to the nature of the attack, understand the breadth of scope, contain the impact, and start recovery back to a steady state.

Within minutes of being alerted to the anomalous activity in the client's environment, the CBTS security and operations team notified the client and immediately began to assess, contain, and mitigate the damage. CBTS brought the full weight of our experience and skill sets to help restore more than 140 production servers, and databases, as well as active directory, network, and remote desktop services.

CBTS' incident response pulled resources from multiple teams including engineering, computer, storage, backup, disaster recovery, and database as well as senior leadership.

In total, CBTS cloud operations engineers and management, collectively dedicated more than 750 person hours in this recovery and worked tirelessly 24x7 to help the customer regain operational status.

Results

Our security operations team has the industry experience and skill sets to quickly identify, alert, respond to, and recover from threats to client environments and minimize costly downtime or loss of essential information.

CBTS successfully restored the business back to normal operations and is able to move on to serving the needs of their clients and continue to grow the business.

With managed security services, in addition to managed cloud computing from CBTS, the client can rest assured that their business is being protected and that if there is an incident, our team of experts are here to help.

"Heartfelt thanks to CBTS for their continued assistance and dedication"

— Global IT Infrastructure Manager