OFFSITE
Cloud | Colo | Security | Managed IT

CYBERSECURITY SERVICES

Mitigating Vulnerabilities In The Face Of A Ransomware Attack

Case Study
Cybersecurity

Customer Profile
CPA Firm

Solutions Industry
Financial Services

Key Issues

- Network Vulnerability
- Data Loss Prevention and Recovery
- Cyberthreat Remediation

THE CHALLENGE

A large CPA firm with 5 offices in the United States, and over 500 employees fell victim to a cyber-attack. This company provides international tax services, business consulting, and accounting services to private and publicly traded companies around the globe. In 2018, they were confronted with a debilitating ransomware attack on their business. By the time OFFSITE was contacted, both their production and backup environments had been compromised. The client was managing their own passwords and policies for their Veaam backup environment running on OFFSITE's private cloud infrastructure. The bad guys were able to exploit this fact and delete all backup files after the attack encrypted all production data.

THE SOLUTION

Typically, when OFFSITE receives system backups into our private cloud environment, we replicate those files from the primary datacenter in Kenosha to our Denver datacenter. OFFSITE's Written Security Policies do not allow credentials for replicated backups to be shared with the customer personnel. This fact made recovery possible.

After a complete restoration of the customer's infrastructure into our private cloud environment, a team lead by OFFSITE's Chief Compliance Officer, who is a CISSP took a comprehensive approach to secure the customer's organization.

We designed and deployed a fully secure network with Palo Alto firewalls at each geographic location and redundant virtual firewalls in OFFSITE's private cloud. Going a step further, this customer opted in to have an air-gapped tape rotation put in place, where Iron Mountain transports the removable media to a remote location.

OFFSITE's 24x7 staffed Operations Center continues to provide MDR and SIEM monitoring of the network. Additionally, as part of our vCISO and CISO Support Services, we provide a weekly briefing that includes a static point-in-time snapshot for executive and regulatory reporting.

(262) 564-6400 • sales@off-site.com • off-site.com