Case Study: Project Ransom

Manufacturer Quickly Stops Bleeding of $1M/Day After Security Breach

BACKGROUND

A leading manufacturer of off-the-shelf, stable, dairy-based food and beverage products suffered a ransomware incident. The company, which has been in business for more than 75 years and has revenues of over $200 million, is a fast-growing, top-tier sourcing partner for large, Fortune 500 companies nationwide.

THE ASSESSMENT

A single ransomware incident caused this manufacturer to lose over $1 million a day due to business disruptions. The attack exposed all servers and endpoints and put the company at risk of losing data and access to raw materials. The company was forced to immediately shut down all production and operations, headquarters, and facilities - including servers and IT networks - to prevent further data loss. The magnitude of this breach required a specialized partner to help remedy the situation.

THE SOLUTION

The RKON incident response team rapidly investigated the incident and searched for the attack source to narrow down possible vectors. Our in-depth analysis discovered that the root cause of the attack was multifaceted caused by: an unsafe number of people using administrator accounts; misaligned leadership roles; incomplete backups; a lack of documentation, patching and consistent testing schedules; and a lack of a disaster recovery (DR) plan. Thus, the company was predisposed to extreme breach risks.

RKON took over IT control of the infrastructure and systems. Our team immediately disabled all accounts and thoroughly assessed the damage, while working with the data center provider.

In addition, RKON collaborated closely with the company's C-suite executives to quickly get the company back online. We explained the breach, worked alongside their IT department to remediate it, and recommended security solutions to not only restore business operations but also to protect the manufacturer from future attacks or breaches.

> *Our incident response team worked 24/7, both on-site and off-site, to secure our client's operations and get them back into production while preventing further damage or risk.*

THE OUTCOME

Our quick and effective recovery process saved more than just the company’s critical systems; it saved the company’s brand reputation as a trusted, reliable, and secure partner.

IMMEDIATELY STOPPED BLEEDING OF $1M/DAY

PROVIDED ROBUST INCIDENT RESPONSE

FUTURE-PROOFED SYSTEMS AGAINST FUTURE ATTACKS

RKON now plans to implement a security operations center (SOC), Office 365 migration, conduct holistic architecture reviews, and deploy ongoing vulnerability scans that will proactively safeguard information moving forward.

Our services will also strengthen security posture among all employees and vendors beyond just technology. Don't let a ransomware attack almost put you out of business before taking security seriously. The best way to protect your most valuable assets is to invest in IT and partner with a team of experts who have the experience and truly understand what it takes to keep your business safe.

BENEFITS ACHIEVED

- Immediately stopped the bleeding of $1 million per day
- Provided robust onsite & offsite incident response
- Protected Systems, business reputation & data
- Future-proofed systems against future attacks, breaches

ABOUT RKON

RKON has specialized in IT transformation since 1998, helping private equity and enterprise firms go from vision to execution and achieve "Quiet IT," in which IT seamlessly serves the business strategy versus getting in the way of execution.

Headquartered in Chicago, IL our team has developed a refined approach through years of experience. We deliver a clear vision of scalable, agile, secure, cost-optimized and low-risk end state.

To do this, RKON provides IT solutions in three stages: first building an advisory practice that sends the strategy in the right direction; an execution practice that ensures the vision is turned into reality; and a management practice that keeps the vision on track as IT evolved to best serve the business.

Need to secure your infrastructure and protect your business from cyberattacks? Let's chat!

CONTACT US