fit solutions
IT · CYBERSECURITY

Case Study: Rapid Ransomware Response for a Law Firm — Why Proactive Cybersecurity Monitoring is Critical

Client Overview

A mid-sized law firm specializing in civil litigation contacted us in crisis. They had fallen victim to a ransomware attack that encrypted most of their workstations, threatening sensitive client data, operations, and their reputation.

They were not under a cybersecurity monitoring agreement with us at the time, nor did they have any form of 24/7 threat detection or response capability in place.

The Challenge

The law firm reached out to our FIT Cybersecurity Operations Center (SOC) after discovering that their systems had been compromised and files across their network were encrypted. This attack effectively halted their operations and raised the risk of data exfiltration and extortion.

Key issues identified:

- No EDR/XDR solution in place.
- No 24/7 monitoring or alerting capability.
- Lack of segmentation allowed the ransomware to spread laterally.
- Backups were not offline or air-gapped but had not yet been impacted.

The Solution

- Upon engagement, our Incident Response team moved swiftly:
- Isolated compromised systems to prevent lateral movement. Secured and preserved backup systems, cutting off the ransomware's path before it could encrypt or delete those backups.
- Performed forensic analysis to identify initial access vector and timeline of compromise. Assisted with encrypted endpoint recovery using preserved backups. Provided detailed reporting to support insurance claims and regulatory requirements.
- Despite the encryption of numerous endpoints, our rapid containment prevented a full business catastrophe.

Outcome

- 100% of client data was recovered from backups.
- Zero data exfiltration was detected.
- Client avoided a full ransom payment, saving potentially hundreds of thousands of dollars.
- Downtime was significantly reduced thanks to a swift recovery plan.

Lessons Learned

This incident highlighted a harsh reality: reactive security is costly. If we had been monitoring the law firm's environment with proactive FIT Cybersecurity 24/7 SOC services, this breach likely would have been detected early — before any encryption occurred.

- Proactive Protection using our state of the art XDR Solution moving forward
- Implement deception technology across the environment, to setup tripwires for enhanced detection

Following the incident, the law firm enrolled in our Managed Detection & Response (MDR) services, including:

- 24/7 SOC monitoring
- Endpoint Detection & Response (EDR)
- Vulnerability Management
- Threat Intelligence & Threat Hunting
- Regular Incident Response Readiness Drills
- They now have peace of mind knowing a dedicated cybersecurity team is watching their environment around the clock.

The Cost of Inaction vs. the Value of Protection

1. Cyber threats are growing more advanced, and law firms are prime targets due to the sensitive nature of the data they hold. Ransomware actors are no longer simply encrypting data — they're stealing it and threatening public leaks.
2. Don't wait for a breach to discover the value of cybersecurity.
3. For less than the cost of hiring one full-time cybersecurity analyst, our team can provide your organization with:
4. Around-the-clock threat monitoring
5. Real-time alerting and response
6. Expert incident response support
7. Scalable cybersecurity protection tailored to your business

Are You Prepared?

Are your backups safe? Would you even know if you were breached right now?
Let's talk before it's too late.

Reach out today for a free consultation and find out how we can provide 24/7 cybersecurity protection at a fraction of the cost of building your own team.