Ransomware Case Study

Business Challenge

Things happen.
Viruses spread.
Proprietary company data is vulnerable.
How do I know my data is safe?

Solution

On a Thursday morning, IRIS Solutions received a monitoring alert regarding a client who was affected by malware. As soon as this alert was posted, our monitoring system isolated the malware on the infected computers by disabling shared drive.

IRIS Solutions confirmed the ransomware virus came in via email. Two staff members clicked on the malicious email.

Within minutes, an IRIS Solutions technician remediated the ransomware issue on the infected computers. The two workstations originally affected by the malicious email were addressed first. Next, the entire office network was scanned, cleaned, contained. The anti-malware software was already resident on the devices as a preventative measure for future events. The client's email solution was upgraded to Office365, which has built in preventative measures for malware.

But with other monitoring efforts, IRIS Solutions caught the issue before the potential business impact took off.

Results

Due to the reaction time, all of the office files on the server were safe from encryption. The only files affected by the malware initially were the local documents saved on the two workstations.

Following a predetermined recovery process a technician restored the files with minimal downtime.

Client

- A dental practice in the Greater Charlotte Area.

Challenge

- Ransomware infected two workstations on a networked office and had the potential to affect the entire business network.

Solution

- IRIS Solutions' response to the ransomware prevented the malware from encrypting proprietary company files on the server.
- IRIS Solutions' monitoring and response program functioned as designed.

Results

- The company did not suffer any severe downtime due to the ransomware virus.
- IRIS Solutions was able to stop and remove the infection before any files on the server were encrypted.

Best Practices

- Save documents on the server. Do not save documents on your local computer.
- Implement a multi-level security plan to reduce the risk of ransomware.
- Hire a Managed Service Provider to monitor your network.

IRIS Solutions
8700 Red Oak Blvd. Suite H
Charlotte, NC 28217