CASE STUDY

When Lightning Strikes Twice

How DiamondIT Prepares You for Inevitable Cyberattacks

John Balfanz Homes is a premier homebuilder based in Bakersfield. In business since 1989, the family-run operation is deeply involved in the community and has built in neighborhoods throughout the region. At the outset of working with together, John Balfanz Homes wanted to leverage DiamondIT's expertise and solutions to manage their IT systems.

We first introduced comprehensive, layered managed security through DiamondIT's SecureCentric, which combines tools, services and strategic consulting like network threat monitoring, antivirus protection and Dark Web scans for leaked credentials. Along with a holistic approach to security, John Balfanz Homes needed reliable backup and disaster recovery. We recognized BackupCentric as exactly what would ensure they could securely store applications and data, automate their backup process, replicate their systems offsite and, most importantly, manage access permissions to their backups, to keep their data from becoming compromised.

But two security challenges emerged early in DiamondIT's relationship with John Balfanz Homes: a cryptocurrency attack and the installation of a malicious Tor browser.

SAVED BY THE BACKUP: STOPPING A POTENTIALLY CRIPPLING CRYPTOCURRENCY ATTACK

The DiamondIT team completed offsite backups and had started implementing SecureCentric when a cryptocurrency attack encrypted the builder's on-premise servers. As a result, John Balfanz Homes restored their files without interacting with the cybercriminals. The incident caught the owner's attention, and he asked what other security measures should be in place. The DiamondIT team assured him that once SecureCentric was fully installed, it and BackupCentric would provide the comprehensive security tools required to protect John Balfanz Homes against current and emerging cyberthreats. This promise was tested when the Tor browser was installed.

DANGERS FROM THE DARK WEB HIT HOME

As we began to work together, DiamondIT discovered one of John Balfanz Homes' employees had credentials for sale on the Dark Web and told the builder to change their passwords. Shortly afterward, DiamondIT's breach-detection software identified dangerous software on their network. In one instance, a Windows magnify tool, which allows users to enlarge text to see better, had been replaced with an administrative backdoor program that gave anyone full access to everything on that server.

In addition, a Tor browser had been installed. This malicious software anonymizes user activity and is deployed by cybercriminals undetected, making their illegal actions untraceable. It insulates criminals from authorities and implicates innocent companies, while acting as a conduit for more malicious software.

HOW DIAMONDIT DISCOVERED AND SQUASHED THE THREAT

On a Friday, DiamondIT's breach-detection software confirmed the presence of malicious exploits on one of John Balfanz Homes' servers. Relying on their layered security and expertise, the DiamondIT team acted quickly, before the destructive code could be leveraged or exploited, notifying the client and stopping the attack in its tracks.

A report of the incident was sent including what happened, potential ways the attack occurred and how DiamondIT prevented the malware from successfully infiltrating the network.

SAVED BY THE BACKUP

The layered solutions included in SecureCentric kicked in when the Tor browser was installed and successfully, working backups, prevented the company from losing time or productivity trying to restore or re-create lost data. Their reputation remains intact because they took proactive measures to ensure managed security and had backups overseeing their network and sensitive files. Thanks to DiamondIT's heavyweight solutions, neither incident resulted in a loss of data, money or time.

Without this comprehensive security in place, John Balfanz Homes employees would have walked into their office on Monday morning and discovered a massive cybersecurity attack with a hefty ransom, requiring a long, arduous recovery process.

YOU'RE GOING TO BE ATTACKED

Cyberattacks are not a matter of if, they're a matter of when. With a security-focused IT provider like DiamondIT actively protecting your network, when that day comes, you'll be ready.

Contact us today:
www.diamondit.pro/contact/ or (877) 716-8324.

"I have learned that it is vitally important to be proactive rather than reactive about cybersecurity..."

"The first issue we had, which resulted in a little over a week of lost data once we were fortunate enough to get back up and running, took literally 2 to 3 months of rework to fully recover from. The last attempted hack was stopped and our network returned to normal before most of our company knew we had any problem at all."

– Justin Schweitzer
Controller, John Balfanz Homes

SECURECENTRIC INCLUDES:

- Advanced threat detection
- Around-the-clock monitoring
- Proactive network patching
- Responsive security support
- Employee cybersecurity training
- Essential security tools:
  - » Firewalls
  - » Antivirus
  - » Email encryption