WED2B Prevents Disruption from Ransomware Attack Using Rubrik

CHALLENGE

- 5 TB of data encrypted
- Antivirus solution failed
- Minimize damage to head office and retail locations

RESULTS

- $0 paid in ransom
- No data lost and 100% recovery from ransomware within 24 hours
- Zero impact to the business
- Restored critical SQL database and Active Directory immediately

> " I used to treat recovery with a laissez-faire attitude. The ransomware situation completely changed that. I cannot recommend the Rubrik platform enough. "

It was 11 PM on a Friday in November of 2019. WED2B IT systems administrator Jamie Jeeves started receiving a barrage of email alerts warning that antivirus (AV) clients were crashing in the company's central office. All prospects for a relaxing weekend vanished when Jeeves logged into the remote system to investigate the AV shutdowns.

WED2B operates as a retailer of wedding gowns, dresses, and accessories for brides and bridesmaids. With nearly 60 stores across the UK, Ireland, Belgium, and the Netherlands, WED2B was fearful the attack would ruin arguably the 'most important day' for countless brides.

While checking the network's file share, Jeeves noticed a mass encryption of data was underway. "This is when I knew we were in trouble. We had just been hit with ransomware," said Jeeves. "All WED2B website files, including text, videos, and high-res images, were being encrypted. 5 terabytes of critical NAS data had been initially encrypted, including the backups from a 3rd party system that used Azure to store backups."

RESPONDING AND RECOVERING WITHIN 24 HOURS

Jeeves knew he had to act fast. In the Retail business, time is money and downtime can be paralyzing for sales. Jeeves began by shutting down all servers and devices remotely. "Unfortunately, however, the remote software missed two machines, so I could not foil the attack completely," Jeeves remarked.

The next morning, working closely with his Rubrik team, he started the recovery process. "We generate the bulk of our weekly sales on weekends. Needless to say, time was of the essence. I immediately disconnected the network from all store locations so they could continue operating independently without impact," said Jeeves.

"Leveraging Rubrik Zero Trust Data Security, I focused on our most critical assets first. I restored Active Directory through Rubrik in less than 30 minutes. I then moved onto SQL databases, which took only an hour to recover 1 TB+ of data. I was pleasantly shocked at how quickly everything came back," said Jeeves. By early Saturday afternoon, all critical systems were back online.

"There were essentially two recoveries taking place: one for data managed by Rubrik and one for Azure backups. While our data on Rubrik was back up and running within 24 hours, it took weeks upon weeks to get NAS back up and running since it was not protected by Rubrik. One of them was painless, and the other one was not," Jeeves stated.

As a result of the successful and fast recovery, WED2B has further increased its investment in Rubrik: "All of our data, including NAS, are now being protected by Rubrik's Zero Trust Data Security. We have upgraded to a newer version and are considering future investments because with Rubrik, it just works."

BUSINESS OUTCOMES:

- **$0 paid in ransom**: "To be honest, it never even occurred to me to pay the ransom demand because I was that confident in Rubrik's ransomware recovery capabilities."

- **No data loss and 100% recovery from ransomware within 24 hours**: "If we didn't have Rubrik, not only would we have lost a lot of critical data, we would have no way of getting that data back. We would have had to either decrypt the data or start from scratch. I've always had confidence in Rubrik's immutability. "I never worried that the data on Rubrik would be reached or encrypted."

- **Zero impact to the business**: "There was minimal, close to zero, impact to the business because we were able to recover so quickly. There was no disruption to the WED2B website, and our bridal stores didn't even realize there was an issue. Everything was fixed before they noticed anything."

- **Restored SQL database and Active Directory immediately**: "Restoring Active Directory through Rubrik took less than 30 minutes. Our SQL databases took an hour to recover 1 TB+ of data. It just works."