Network Repairs

RANSOMWARE CASE STUDY

THE ISSUE

One of our clients from the Food Services industry got attacked by Ransomware a few months back. The client had subscribed to a basic back-up plan.

The Ransomware struck them on a weekday during regular business hours. The client reacted quickly and contacted us immediately. With their prompt response, we were able to restrict any major damage and recover their data.

Knowing how sophisticated ransomware attacks are becoming. We advised our client to ramp-up their back-up plan.

Unfortunately, the client didn't react to our recommendations on-time and got attacked once again. This time it happened overnight and as a result most of their database, backup and, applications got encrypted and formatted.

THE SOLUTION

Even with a basic back-up plan we offer a rotational backup policy that backs up data offline at a periodical interval of 24-48 hours. This became the saviour, this time around!

With a serious ransomware attack, data recovery isn't easy. In this case, the major challenge along with everything else was that ransomware even affected the Active Directory. To overcome this challenge, we had to recover data from the backup and then pull it back to the active directory.

THE OUTCOME

The client realized this after getting attacked twice in a gap of few months. Immediately after the second attack we helped the client create a solid back-up and recovery plan.

We performed multiple upgrades including a server upgrade with warranty and better Raid controller. Migrated all Virtual Machines on to the newly upgraded server.

The backup was designed to the repository along with a virtual standby. This way we make multiple copies with one kept turned-off and the other copy will be to be synchronized with the server across the VAN link to the datacentre. With this sophisticated backup plan, we now cover the client from on-premise disaster and also against ransomware attack, server and operating system failure.

This approach makes the client's backup plan more secure and enhances the recovery process.

IMPORTANT TIPS

We were able to bring this back in control! However, in order to limit the effects of ransomware attacks, limit vulnerabilities and improve recovery processes, businesses need a customized backup plan and monitoring in place.