Asigra.

Recovery is Everything™

Case Study

UK Backup Expediently Recovers Business Critical Data After Locky Ransomware Attack

- UK Backup provided a large UK retailer a cloud based data protection solution to protect their data
- Locky Ransomware attacks and encrypts over 350 sites, including entire network servers and file systems
  - Within a 20-minute time frame, approximately four million files were encrypted
- Asigra's scalable data protection software helped UK Backup decrypt and restore over 20 TB of data before the beginning of the next business day
- Granular restoration ensured all data was protected efficiently

UK Backup

Asigra.

Recovery is Everything™

SUMMARY

As one of the leading provider of cloud backup and disaster recovery services, UK Backup (a UK Based ISO27001 Certified Cloud Backup Provider) provides cloud backup services to the public and private sectors. Their Disaster Recovery as a Service (DRaaS) and Data Protection service is currently powered by Asigra's Cloud Backup™ and recovery solution, which enables UK Backup to guarantee an expedient recovery of business critical data, including data living within Office 365 as well as other on premise file systems using Asigra's cloud based backup solution.

In the summer of 2016, the Locky Ransomware virus attacked and encrypted 20TB of UK Backup's customer's data. UK Backup received the initial call at 5 p.m. that their client's files were all encrypted. Although the client did not know the origin of the encryption (e.g. whether an attachment was opened via email or if an employee visited a malicious website), the client was able to identify that the encryption took place at about 4:40 p.m., and it took a mere 20 minutes to encrypt files, network servers, systems and drives across the customer's 350 sites. The request from the client was clear: they needed UK Backup to minimize downtime by restoring their data and having their systems up and running for the start of the next business day.

BACKGROUND

Business data is at risk. Whether it's stored on the cloud or on site, data needs to be protected and backed up to give organizations the peace of mind that data will never be lost or compromised after a cyber-attack. With ransomware attacks rapidly increasing since 2015, and now considered the greatest data security threat to organizations in every industry, having only an anti-virus software in place is antiquated and risky. More organizations are taking a closer look at existing data protection and recovery strategies to ensure they can resume business operations quickly after a potential disaster.

After Locky encrypted all the customer's data on local area networks, servers, and computers (both laptops and PCs), UK Backup utilized Asigra's DRaaS solution to facilitate an expedient recovery. Already providing Asigra Cloud Backup™,

CHALLENGES

- Providing a comprehensive business continuity strategy that met the needs of the client and ensured that data can be protected after a ransomware attack
- Mitigating cybersecurity risks and being able to restore business critical information by the next business day after a disaster occured

ASIGRA CLOUD-BASED DATA RECOVERY DELIVERS

- Single integrated solution for all data protection needs
- Policy-based protection based on the user's IT environment and recovery requirements
- Optimization of IT resources for enhanced utilization
- Data encryption that secures data in-flight and at-rest with full support of compliance requirements
- High-performance data recovery

DRaaS, and Office 365 backup solutions to the client, UK Backup knew that Asigra's solutions could restore files quickly. Asigra's offerings are scalable, comprehensive and have the capabilities to recover all data, no matter where it resides (whether that's locally or on the cloud). The solution guaranteed that normal business operations would resume quickly (e.g. the following business day) and the scalability of the solution enabled UK Backup to decrypt all sites, consisting of four million files and over 20 TB of data.

SOLUTION

UK Backup's cloud based data recovery solution recovered all business critical information/data. This included application data retrieval from Microsoft Exchange servers, networks, SQL Servers, the company's internal systems, PST archive files on desktops and laptops as well as a large volume of file data. Using existing backup rules pre-determined by the client, UK Backup started the first restore at about 8 p.m. Automatic point-in-time data backups already pre-arranged proved to be valuable to the client, as it was an immediate available previous backup set that was used to help the client recover from the attack. With Asigra's intuitive user interface, UK Backup was able to quickly recover the data by pin-pointing the exact files that were encrypted as opposed to looking through every single file/network on the system.

> "We didn't have to wipe the whole system and start again. We could use the software to determine which files were actually affected so we could work out what needed to be removed or restored. We were able to use Asigra's solution to find exactly what files were infected to replace the infected files."
>
> **James Chillman, UK Backup**

RESULTS

What Chillman and his staff did to expedite a speedy recovery included working diligently with the client's internal IT staff to disconnect any suspected computers from the network, disabling all drives (as Locky encrypts all networks and shared drives connected to networks), updating and continuously running security software on all devices and software on the network, and reverting to a backed up version of data that was not encrypted. This lead to initial success within the first three hours.

Final restoration occurred at 3 a.m., the recovery time (RTOs) and point objectives (RPOs) of the organization were not only met, but exceeded. Never encountering a disaster of this scope, the client was impressed with the scalability of UK Backup's solution, recovery response time and ability to recover all data from both local and remote devices.

> "The reliability was the key thing that was a factor and the guarantee that we could recover the data within the required time frame."
>
> **James Chillman, UK Backup**

Other benefits provided by Asigra's solution included: the ability to recover data back to any system/device in the network (including physical servers, virtual machines and/or desktops), and its platform agnosticism ensuring that all enterprise data is protected. These features allowed the client to eliminate point solutions and consolidate backup operations, which helped in recovering data faster.

About UK Backup

UK Backup Limited are UK based providers of enterprise grade Cloud Backup and Disaster Recovery services. By utilizing a market leading technology, UK Backup has quickly established itself as one of the UK's leading Backup and Disaster Recovery providers. Established in 2010, UK Backup protects companies of all sectors and sizes, from public sector clients and enterprises through to SMEs.

About Asigra

Trusted since 1986, Asigra provides organizations around the world the ability to recover their data now from anywhere through a global network of partners who deliver cloud backup and recovery services as public, private and/or hybrid deployments. As the industry's first enterprise-class agentless cloud-based recovery software to provide data backup and recovery of servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, eliminates silos of backup data by providing a single consolidated repository, and provides 100% recovery assurance. Asigra's revolutionary Recovery License Model provides organizations with a cost-effective data recovery business model unlike any other offered in the storage market. In 2015, Asigra Cloud Backup was named the **Top Enterprise Backup Solution** and achieved silver in Storage Magazine's **Products of the Year**.

More information on Asigra can be found at www.asigra.com

Asigra.