What Businesses need to know about RansomCloud

Ransomware remains a pervasive threat to all Australian businesses. Ransomware continues to grow as the method of choice for cybercriminals to extort funds from their victims. Cybercriminals who carry out these attacks are incentivised to continually look for new ways to stay ahead of the curve to capitalise on vulnerable computer users on a mass scale – and it appears they have found their latest loophole: the cloud.

RansomCloud, What is it?

The cloud has risen to become the computing solution of choice for businesses. As businesses have migrated to the cloud, they have increased their reliance on cloud-based applications such as Microsoft Office 365 and collaboration tools to store and manage their critical business, vendor, and customer data.

Cybercriminals have recognised this monumental uptake of cloud. As a result, they see it as an opportunity to release new strains of ransomware. The latest strain that is anticipated to create new security problems for any business is RansomCloud.

How can RansomCloud affect my business?

When a RansomCloud attack occurs on a business' cloud-based applications, the impact can be extremely severe – often business ending.

Once a business' critical files and applications are encrypted, it's prevented from carrying out any further activities. A business will suffer immediate productivity and revenue losses.

What puts my business at risk of a RansomCloud attack?

There is a common market misconception that the cloud is secure. Typically, a public cloud infrastructure has its own secure barriers in place to prevent attacks from penetrating the actual servers and failovers. However, it's not entirely foolproof. In fact, even Microsoft recommends that backups be kept in an external, non-mapped or not synced storage.

Additionally, where there are humans involved, there is always risk. There is no way organisations can prevent people from deliberately or accidentally exposing a business to greater vulnerabilities.

How can my business recover from a RansomCloud attack?

- **DON'T** pay the ransom fee. There is no guarantee an attacker will release any encrypted files after the payment
- **DO** backup data that resides in the cloud
- **DO** integrate **both a disaster recovery and business continuity solution** to ensure you can get your organisation up and running in a timely manner if disaster strikes
- **DO continually test** the backup and disaster recovery solution. Doing so will ensure that when – not if – an attack strikes a business' systems will be ready to operate at optimal level.

79% of Managed Service Providers report clients have experienced some level of business-threatening downtime[1]

14% of a total 45% of SMBs that do pay ransom to a cybercriminal never recover their data[1]

Source

1. https://www.datto.com/au/blog/datto-state-of-the-channel-ransomware-report-anz

SOMA IT

For more information please contact:
Greg Nicholson | Business Development Manager
Phone: 1300131559
Email: greg@somait.com.au
Soma IT Pty Ltd | http://www.somait.com.au/
Level 5, Niecon Plaza, Victoria Avenue Broadbeach, QLD, 4218