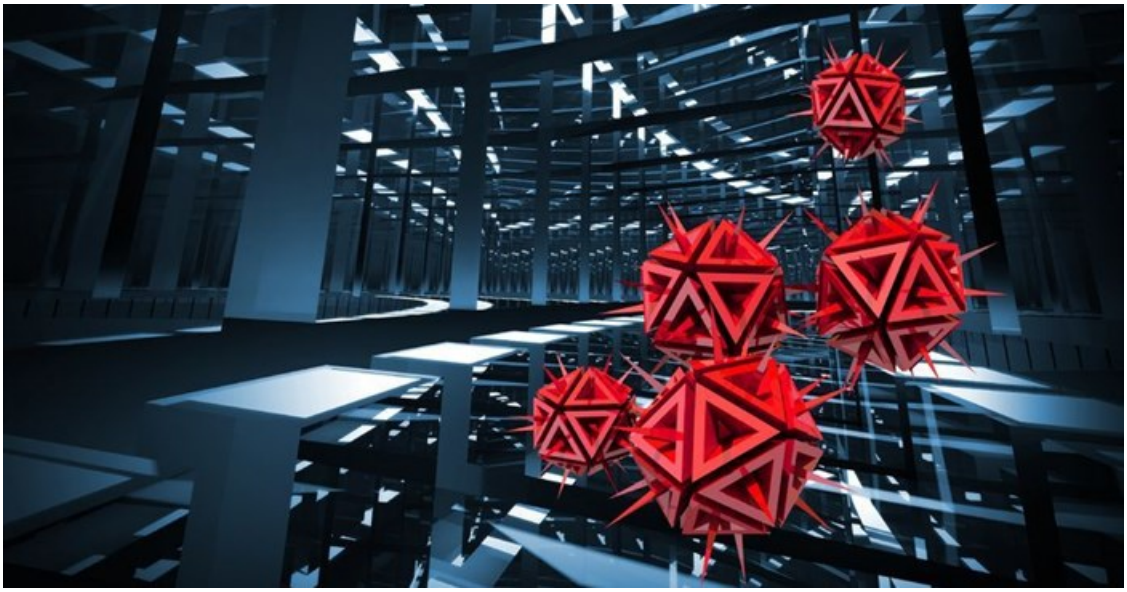
Ransomware is here to stay - can your data say the same?

By Mike Rees

23 Nov 2017

Ransomware looks set to stay, and more variants are emerging every week to wreak havoc on enterprises and individuals alike. As the vicious malware grows increasingly sophisticated and prevalent - even being offered as a service on the dark web - so, too, will organisations continue be attacked and their data will be at risk.



© Eugene Sergeev – 123RF.com

Ransomware, a form of malware that holds a business's or individual's data to ransom, can cost hundreds of thousands of rands in 'ransom' in order for the data to be made available again. In worse case scenarios - such as with NotPetya, where financial gain appeared to not be the primary objective - data is permanently lost, costing even more in terms of repetitional damage and loss of valuable information. Businesses can no longer afford to take a traditional approach to data security. They have to start developing creative ways to ensure the safety of their company, its data and its people.

How protected are you?

Many organisations assume that if they have network security tools, such as a firewall, in place, that they are adequately protected against ransomware. Unfortunately, this is not always the case. While it is necessary to have network and data security tools in place, these are not fully effective unless they are tested and updated frequently.

Updates ought to be implemented within a business as soon as they are released, and not only in reaction to the latest newsworthy ransomware outbreak. Understandably, installing patches and updates as they are made available isn't always practical as, typically, operations need to be ceased while these are installed. The concern with scheduling change control to install patches is that organisations are left vulnerable in the time between the patch release and its implementation. This can sometimes take as long as a week, or even more, depending on a business's change control frequency.

Businesses need to think creatively to install patches as quickly as possible with minimal disruption to daily business. Whether this means staggering the install across the business, scheduling more frequent change control sessions at the least disruptive times, or leveraging sophisticated technology which enables the automatic installation of patches while the business is fully operational, the fact remains that the faster that a business implements an update, the safer they will be.

Automated updates that run in parallel with an organisation's operations are ideal, but can be expensive. Businesses need to consider what they are willing to spend to keep their data safe, including weighing up what risks they are and are not willing to accept, and adapt their data protection strategy to this.

Why a data security policy matters

Even the most up-to-date systems, however, are rendered ineffective if they are not tested regularly to ensure that they work as they should. A proper data security policy needs to be implemented which enforces the regular testing of all security tools, measures, procedures and practices. Before compiling a policy, however, businesses need to understand the flow of their data.

Part of any good data security policy is the ability to carry out the necessary procedures when a threat occurs. This is a three-pronged approach. Firstly, the business needs to understand the business's data flow, to help identify precisely where data is located within a business and to isolate that data when a breach occurs.

Then, the business needs to be able to react quickly and reliably in response to any threat, in order to protect their data. There are tools available which help to identify threats and automatically isolate them, while also encrypting data and storing it centrally to achieve faster data restorations. Automatic multiple backups allow an organisation to go back to a specific point in time to retrieve any data lost, so as to achieve the best possible sameness as prior to the threat. Having a single tool which covers all of this reduces the complexity and helps to more easily manage data flow, data security and data restoration

Data is irreplacable

Lastly, everyone within the business needs to be aware of what steps to follow to protect their data proactively and reactively, and what the consequences are if they do not follow these protocols. When individuals understand the importance of their data, and the requirements for protecting that data, they are better able to do so. This, in fact, may be one of the most important aspects of creating a data security policy - if everyone follows the right steps to protect themselves and the company, risks are drastically reduced.

The reality is that data, today, is a business's most valuable asset. Boldly speaking, when it comes down to it, every other aspect of a business can be replaced, from the building to its infrastructure to its very staff. Data is irreplaceable, and cybercriminals are cashing in on this weak point. Businesses must be prepared.

ABOUT MIKE REES

Territory Account Manager: South Africa at Commvault
- Consolidating your backup and recovery makes sound business sense - 21 May 2019
- Optimising data storage has many business benefits - 22 Feb 2019
- Data governance is not just about compliance; it's good business - 10 Jan 2019
- What businesses need to know about business continuity, disaster recovery - 15 Nov 2018
- Ransomware is here to stay - can your data say the same? - 23 Nov 2017

View my profile and articles...