IT security is not secure if you aren't considering your data

By Bryan Balfe

23 Apr 2015

Security is one of the foremost concerns when it comes to IT infrastructure. However, protecting organisational data has become as important, if not more so, especially when one considers the critical nature of data to the majority of businesses today.

The reality is that IT is not secure if data is vulnerable at any point in its lifecycle. Security should not, therefore, be considered through a typically 'infrastructure out' approach, but from a perspective of the actual data itself. Organisations need to know what data they have, where it is being stored, and why, before they can ensure this data is adequately protected, and before they can consider their IT infrastructure fully secure.

One of the security trends that is beginning to emerge as a result of the need to protect data better is an increasing focus on edge devices, from desktops and laptops to tablets and even smartphones. This is the result of a growing awareness of the volumes of data that are now housed outside of the data centre environment, and is driven by theft, social engineering and a variety of other threats.

Confidential, sensitive or business-critical information is prone to being stolen or otherwise illicitly acquired off end points, which creates multiple risks, not least of which is non-compliance with the Protection of Personal Information (PoPI) Act. After all, it is far easier to steal a laptop or even download information onto a flash drive than to hack into a typically secure corporate network.

A loophole in networks

In addition to the issue of data going missing, these devices also often offer methods to access other corporate locations and data, creating a loophole in networks for those with malicious intent to exploit. End-point encryption is, thus, a growing requirement in order to ensure that even if these devices are stolen or fall into the wrong hands, they will be unable to read the contents of the hard drive or memory.

The challenge around this is to implement a solution that does not impact on users' experience or ability to do their jobs, and also to ensure data is encrypted not only 'on the wire' or during transmission, but also at rest, wherever it is stored. These trends further highlight the need to protect data wherever it resides, and to adopt a new, data-centric approach to IT security.

Understanding data is vital to securing it, and this requires a data audit to discover where data is stored, what data is stored where, and why. From there, a comprehensive threat and risk assessment can be conducted, so that organisations can begin to ascertain whether data is being stored in an inappropriate place. For example, confidential client information stored and shared over public cloud storage providers.

No policy

Many organisations, for example, do not have policies in place to prevent people from sharing information on these platforms, and the reality is that they are prone to being hacked. Collaborating and file sharing using such third-party public cloud systems simply is not secure. There is no way of knowing where the data actually resides, who can access it, and how secure it is. Organisations need to provide a secure alternative to ensure this does not occur.

The concept of securing IT does not usually include securing data, but this is a huge oversight. Organisations today need not only to understand where their data is, but also have policies in place to ensure that data at the edge makes its way back to the corporate network. Policies also need to be put into place for what happens to data when devices are lost, broken or stolen. Data also needs to be mapped according to its nature - if it is important, confidential or private, it is associated with risk should something happen to it. This is critical in building comprehensive security policies and processes.

Addressing this challenge requires that business be included on the risk assessment. After all, IT is least likely to be affected by a data breach first, and a data breach is ultimately a business problem. The proactive approach is to profile data extensively and accurately, so that an understanding is created of what is stored, what cannot be stored, and how this data can be defensibly deleted - particularly important in light of PoPI. It is also vital to identify all of the points where sensitive data exists and ensure this data is protected. Data needs to be secured where it is created, while it is being transmitted, and while it is at rest, throughout its lifecycle. Data management is, thus, an essential component of IT security, and without it any security policy will be incomplete.

ABOUT BRYAN BALFE

Channel Manager at CommVault in South Africa

- Understanding data sovereignty and its importance to your business - 22 Sep 2015
- Controlling data risk in the BYOD onslaught - 19 Aug 2015
- What enterprises can learn from the MSP revolution? - 13 Aug 2015
- Warning signs your archiving strategy is not geared for the future - 24 Jul 2015
- Driving forces behind cloud computing - 22 Jun 2015

View my profile and articles...