Visibility is key to successful security

By Saurabh Kumar

15 Jan 2016

The news lately has been full of reports of high-profile attacks on large organisations aimed at compromising or stealing sensitive customer information. Despite the increase in prevalence of data breaches, the majority of enterprises in South Africa are simply not doing enough to prevent these attacks. A prevailing attitude of 'it won't happen to us' typically results in less than adequate protection.

©Daniil Peshkov via 123RF

The reality is, however, that with increased connectivity, anyone can access data over the internet if it is not protected adequately. In order to protect themselves from the often-significant consequences of data breaches and data loss, organisations need to heed warnings and take data security far more earnestly. It is essential to ensure that identity and access management are in place. In addition, creating visibility is essential not only in preventing intrusions but also in detecting them as early as possible and mitigating negative effects.

Within any large enterprise, there are numerous ways that a security intrusion might take place, from a highly sophisticated attack right down to something as simple as human error. Visibility is, therefore, key to successful security, not only for preventing intrusion, but also to alleviate its negative effects.

Intrusion detection

Without visibility, organisations will have no way of knowing that a breach or other security event has occurred. As a result, lack of visibility results in breaches that go unnoticed for months, giving cyber criminals plenty of time to steal valuable and sensitive information. Intrusion detection is a critical element of any organisation's security protocol.

The flip side of the coin is intrusion prevention, which is a more proactive approach whereby various software solutions are implemented to detect breaches as they occur and effectively prevent them from infiltrating into an organisation. Identity and access management is a critical component of intrusion prevention, as with any large enterprise the majority of security threats originate from within.

Organisations need to have clear roles defined with regards to governing access to data as well as to track and audit any changes to data. This ensures that all access to all data is thoroughly documented, and it is possible to pinpoint where security threats originate in an organisation. This in turn also assists with improving visibility, which is the starting point for all other security initiatives such as the ability to disable infected devices and remove access permissions from compromised accounts.

While the majority of prominent cyber attacks have occurred within global organisations, this does not mean local companies are safe from the threat. The internet has resulted in the world as a whole becoming more connected and intertwined than ever before, and South African organisations are therefore at just as much risk as their international counterparts.

Matters are complicated

Furthering this challenge, trends such as the cloud, mobility and social media, which have all become integrated with internal IT, have complicated matters and made it more important than ever to monitor access, secure devices and ensure permissions are up to date and are removed when no longer required. These are all aspects of identity and access management, a vital tool in the cyber and data security landscape.

One sector in South Africa that is ahead of the curve when it comes to adoption of these solutions is financial services. The major banks utilise identity and access management solutions to develop role-based access to relevant applications. These solutions not only prevent unauthorised access but also create a complete audit trail of any access attempts, instantly alerting relevant parties if a breach is attempted or occurs. Other organisations need to take the example set by financial services and apply the correct solutions for their industry and requirements.

Packaged software systems

When it comes to security solutions, including identity and access management, there are packaged software systems that can be implemented so that enterprises do not have to develop solutions from the ground up. It is also possible to access managed services that can help to ensure a smooth roll-out and that organisations configure their security effectively.

In order to ensure the solution meets the organisation's expectations, it is essential to firstly understand existing security policies and processes, and then map them to the solutions that are available. The chosen solution must align with security and access policies which the organisation have already put into place.
Choosing between insourcing and outsourcing these services is a decision that depends entirely on the organisation's needs, requirements and infrastructure. A dynamic and experienced service provider can assist here to ensure the right balance is obtained for optimal protection given these criteria.

ABOUT SAURABH KUMAR

Managing Director at In2IT Technologies South Africa
- Digitisation and tech are key for businesses to thrive in 2021 - 8 Jan 2021
- The value blockchain can bring to business - 26 Jan 2017
- Digital change begins with business leadership - 14 Nov 2016
- ICT investment can help fuel SA's GDP growth - 3 May 2016
- Outsourcing vs insourcing: trust innovation to the experts - 25 Feb 2016

View my profile and articles...