BIZCOMMUNITY

Overcoming the 2019 cyber threat

By Ronald Ravel

1 Apr 2019

Over the last couple of years, the dramatic development of digital technologies has fuelled the growth and needs of the mobile workforce. Recent research by Microsoft found that only 11.4% of European employees feel highly productive at work, and, amidst the arrival of innovative technologies like 5G, mobile working is not only becoming increasingly prevalent but also more popular with offices no longer confined to four walls.

However, while it is important organisations give employees the flexibility of remote working, they must also be mindful that – in an age of mass data proliferation – the wider a network perimeter has to stretch, the more scope exists for security breaches.

The 2019 cyber-threat landscape

As organisations adapt to this rapidly changing environment, they must be cautious of technology's role as both enabler and inhibitor. With so much data now available and increasingly central to an organisation's day-to-day operations, the cost of any security breach is quickly increasing.

Ronald Ravel, Director B2B South Africa, Toshiba South Africa

An IBM and Ponemon Institute study, for example, showed the global average cost of a data breach rose by 6.4% year-on-year in 2018 to $3.86m.

Coupled with this is the growing intelligence of the cyber-criminals attacking this data, who are constantly evolving their methods to stay ahead of the game – as demonstrated by the 2018 SonicWall Cyber Threat Report, which reported a 101.2% increase in never-before-seen cyber attacks and malware variants. Cybercriminals are turning to highly effective weapons like ransomware, IoT malware and TLS/SSL-encrypted malware to target organisations around the world.

Devices and employee's – the first line of defence

Devices are often the first line of defence for organisations – instances of laptops being left on the train, stolen on a busy commute or connecting to a coffee shop's unsecure network, can leave sensitive data exposed. IBM and the Ponemon Institute found that almost half of security breaches involved a malicious or criminal attack, while a further 27% were due to the carelessness of negligent employees – and combining the two creates a potent concoction which IT managers need to

successfully manage.

Creating a GDPR Compliance Framework with security tech

Pieter Engelbrecht 26 Mar 2019

It is therefore important to ensure the security solutions are in place to protect business-sensitive information at both a hardware and network level. Organisations should look to devices such as Toshiba's X-Series, which boast biometric features alongside in-built smart data encryption tools.

Alongside these initial barriers, remote access and wiping tools are important in enabling IT teams to remove files and data from devices should they land in the wrong hands. Even within an organisation, it is important for individual departments to ensure security and confidentiality for sensitive documents. Central administration tools can grant access rights based on job type and job seniority – for example, restricting sensitive financial information from those sitting outside of that department.

Beyond digital technological solutions, organisations must also invest in training and education to ensure employees are taking the right methods to identify and mitigate potential security attacks, and prevent them from happening. According to Toshiba research, two thirds of organisations want to invest in engaging their staff in IT training, in turn ensuring correct and secure usage and ultimately reducing the chances of employee negligence.

The rise of IoT and the mobile edge

The rise and adoption of IoT is creating a growing need for even more stringent data protection policies. Security specialists such as Avast are specifically calling out IoT as a key battleground in 2019 as sophistication in this area increases, and as a result businesses will need to consider new and innovative security methods.

Source: pixabay.com

One such approach is to turn to mobile edge computing solutions, which not only pave the way for IoT to be used in the enterprise operationally, but ensure that it's also achieved in a secure manner. Such solutions enable data communication to be locally encrypted and translated to a communication protocol before being sent to the company's network core via the cloud.

As we see new IoT-driven solutions such as wearables enter the enterprise, the need to protect the ever-growing swathes of data created by this trend will result in organisations placing even more value on mobile edge computing.

New report: Bots, AI, wearables, VR to create billion-dollar savings in tourism

20 Mar 2019

Security remains the most important element of an organisation's IT strategy, with the current threat landscape more diverse and challenging than ever before. Solutions may only remain secure for a matter of months before cyber-criminals decipher ways to breach them, and so it is essential IT leaders constantly monitor and evolve to stay ahead of the game.

In the age of IoT, this means going beyond protecting the network at its core, but also using robust hardware and edge solutions to nullify the threat across the ever-expanding network perimeter.

ABOUT RONALD RAVEL

Ronald Ravel is Director B2B South Africa, Toshiba South Africa

- 2022 tech predictions: Smart glasses, drone delivery services, and more - 10 Dec 2021
- AI and edge computing is a match made in IT heaven - 24 Mar 2021
- The tech developments that will thrive in a post-Covid-19 era - 8 Dec 2020
- Unlocking employee engagement through enterprise technology - 6 Dec 2019
- CIOs need to ensure their workforce can catch up - 4 Jul 2019

View my profile and articles...