BIZCOMMUNITY

Your IT needs a wake-up call - maybe PoPI is it

By Pieter Engelbrecht

13 Oct 2017

When I read the warnings that fill our media, and the scramble for information, I'm reminded of the Y2K bug. Just like 1999, we are getting close to a full-scale panic about compliance, fines, and the potential loss of business if we don't make some pretty big changes.

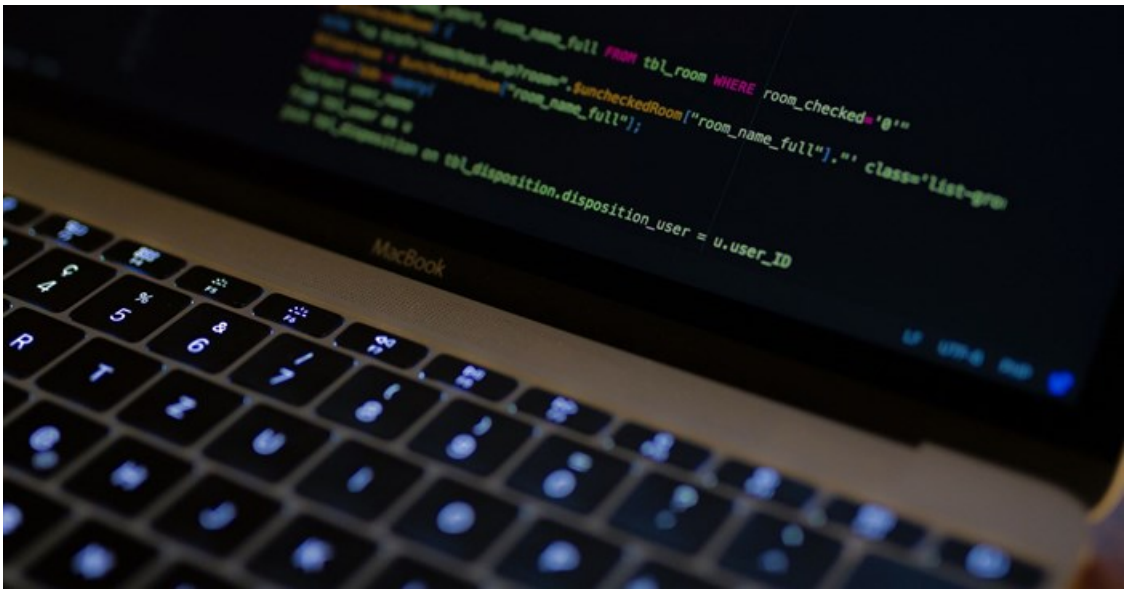

Photo by Caspar Rubin on Unsplash

While the eyes of every business are on your IT systems, there is a huge opportunity that you can take advantage of. The Protection of Personal Information (PoPI) Act and - if you conduct business in Europe - the General Data Protection Regulation (GDPR) are not just about privacy or incredible fines. They present an opportunity to take a holistic look at your security portfolio and underline the necessary steps you need to take to become compliant.

Security is a business problem, not an IT problem, and with the support of business leaders, you can build on PoPI and GDPR to create an end-to-end strategy for your IT systems. It’s an opportunity to gain much greater visibility of your network and prepares you for any future changes or possible attacks that may occur.

Getting ahead of growing networks through automation

In the event of a security attack, particularly if malware is involved, IT systems have to be taken offline. This can cost a company millions in lost revenue, and longer lasting damage to its reputation.

The potential sources for security breaches are huge, and that, to me, is the biggest catalyst for action. Every business is becoming more reliant on connected things, from old operational technology (like energy sensors) to GPS, to the latest connected lighting or locking systems. Your network is an enormous web of endpoints, from the core out to the millions of user devices at the edge, and customer data can travel through any one of them.

Without looking at this entire landscape, and applying some more rigorous security policies, the loss of customer data in the future is almost inevitable.

When I speak to CIOs, I hear a lot about the need to audit the entire network to understand every place that customer data can touch. This is key to PoPI and GDPR compliance of course, but if we stop there, we only tackle half the issue.

To achieve real end-to-end security, CIOs should work towards:

1. Segmenting the network so that each individual user and device can be reviewed separately
2. Automating the network configuration using machine learning

Using this combination, we will see machines become wise to individual devices and user behaviours, meaning they will act when a new behaviour is recognised. The subsequent actions could be network re-authentication, quarantining or blacklisting the user or device. All without the intervention of IT staff.

As the network continues to grow exponentially, IT systems are running to keep up.

> *“PoPI and GDPR are just the beginning of a bigger security concern that is never going to go away.”*

To effectively manage endpoint security, end users and user devices in a secure and sustainable way, we can no longer view the network as piecemeal.
The network of the future will represent a single ecosystem, with the ability to create unique policies at any time, in any location. It’s our best chance to get ahead of what’s coming.

ABOUT THE AUTHOR

Pieter Engelbrecht is the business unit manager for HPE Aruba.