How autonomous IT and security solutions will enable proactive IT departments

By Pieter Engelbrecht

11 Apr 2019

The cybersecurity of a business is still largely reliant on the people within each company's IT department. This is not sustainable long-term and organisations need to start looking to autonomous security measures to relieve some of the pressure felt by IT teams.

Pieter Engelbrecht, Business Unit Manager, Aruba HPE

The impact that cybercrime has on business alone signifies the importance of having robust and reliable cybersecurity measures in place. However, the rate by which cyber attacks are currently and will continue to take place, along with the increased sophistication thereof, has propelled the importance of cybersecurity to the forefront of critical operational needs.

Cybersecurity is not just reliant on deploying secure ICT systems but also on the people who create, monitor and update them, along with those who resolve security threats when alerted to them.

This has put a strain on the IT departments of numerous organisations rendering them largely reactive rather than proactive.

Reactive IT

A reactive IT team is unable to do any planning, they cannot see problems coming and therefore are only aware that issues have arisen as a result of the tangible effects they have on systems, networks and the overall business. This often leaves them scrambling to fix issues as they come up.

Investigating a single security alert can take a significant amount of time due to the scale and complexity of the data involved.

Without the time to make better decisions, this can result in increased downtime, loss of money and can leave the department feeling discouraged as they're not able to create, develop or improve on anything and are instead relegated to a task-oriented role rather than an innovative one.

A recent survey conducted by computer software company, Oracle, found that organisations received around 17,180 IT security and management related alerts every week, with 60% of IT executives lamenting the damage that the required amount of resources to manage and maintain infrastructure had on their organisation's competitiveness.

Autonomous IT and security solutions will take this pressure off of IT personnel through automated preventive and corrective actions, which will remove the cost and risk from IT operations and increase the rollout speed of other IT-related applications by freeing up the time of IT teams to serve the business better.

What this means is that IT departments will have the ability to move from being reactive to being proactive.

Proactive IT

Utilising proactive IT units will enable businesses to have control over their approach to and the future direction of their IT, and can thus make use of technology as a strategic tool to reduce the amount of time invested in operational tasks and increasing the time spent on tactical and strategic tasks.

This leaves them free to help prevent problems, instead of just fixing them, and thereafter business executives will be able to make strategic IT decisions that will positively impact on business operations and processes.

Not only are proactive IT solutions easier to integrate into a budget than unexpected and unaccounted for problem fixes, but utilising autonomous IT and security processes will ensure that there are systems in place to address emergencies that take place with little warning or time for preparation. The result of this is that many common issues will no longer even exist.

The skills gap

In addition to these benefits, autonomous systems could also help to alleviate the pressure of the cybersecurity skills gap which Cybersecurity Ventures predicts will widen exponentially by 2021.

Business leaders are starting to take cybersecurity concerns more seriously than ever before and in order to prioritise long-term defence structures, are increasingly looking for permanent IT security professionals to do so.

In fact, cybercrime is expected to triple the number of open cybersecurity positions over the next five years, and as every

IT position is currently also a cybersecurity position, this presents a massive problem – of which autonomous IT solutions could be the remedy.

The definition of autonomy is the capability of operating without human control. Being able to do this with security-related and other mundane IT tasks will allow these departments to improve operational efficiency and pursue tech-related strategies that can help the business stay competitive, differentiate themselves within the market they operate and undergo transformation at a faster pace.

And, the best thing is that autonomous IT and security solutions are no longer just a dream, but a concrete reality.

ABOUT PIETER ENGELBRECHT

Pieter Engelbrecht is the business unit manager at Aruba, a Hewlett Packard enterprise company.
- How autonomous IT and security solutions will enable proactive IT departments - 11 Apr 2019
- Creating a GDPR Compliance Framework with security tech - 26 Mar 2019
- Why are CIOs and CISOs positions becoming more challenging? - 31 Oct 2018
- Mitigate WAN complexity with SD Branch - 18 Sep 2018
- Securing the enterprise network with artificial intelligence - 21 Nov 2017

View my profile and articles...