BIZCOMMUNITY

The benefits and risks of BYOD

The trend of BYOD (bring your own device) is not going away. This is according to Arbor Network's territory manager for sub-Saharan Africa, Bryan Hamman, who says the rise of BYOD has been attributed to many factors, including the introduction of next-generation office workers who don't necessarily do their best work during traditional office hours, in traditional workspaces or even using traditional devices.

© huyquynh0 via pixabay.com

“Mobile devices, such as cell phones and tablets, being used for work, and therefore requiring a link to the company server, are increasingly prevalent. Salesmen not wanting to risk taking their laptops out of office are using tablets and phones to present at meetings. New technologies have changed the way we interact with businesses in very clear and beneficial ways," he says.

“But along with these advantages come risks – especially for companies that are not building BYOD into their security strategies. Firewalls and IPS devices protect the edge from incoming threats, but these attacks have advanced from exploit-based threats to targeted, hidden malware that stealthily steals private data and intellectual property.

What you should know about BYOD to work

26 May 2017

“With each new device that plugs into the network comes another portal for potential distributed denial of service (DDoS) attacks and another distribution line through which these attacks can extend their reach,” says Hamman.

Mark Campbell, consulting engineer for sub-Saharan Africa at Arbor Networks, has previously explained the intricacies of cyber and DDoS attacks.

Here, he notes that modern-day foes do things that can’t be stopped purely with technology. For instance, they do their reconnaissance in a human way to understand your technologies, processes, and people. They will use social media to understand your staff, affiliates, and partners. They watch for press announcements about your technology upgrades. They will then rent the equipment, online or physically, to craft and test their attacks against.

“This is incredibly sophisticated,” says Hamman. “Gone is the concept that cyber attackers are bored teens sitting on a LAN in their grandma’s garage trying to cause trouble. These attacks are planned and launched with intention. They are out to do as much damage to your infrastructure and access as much sensitive data as they can in as short a time as possible.”

First step in the BYOD journey

The first step in the BYOD journey, for companies that realise employee-owned devices on the intranet is non-negotiable, is to have a clear policy on what is and what is not allowed, as well as the expectations of the business in terms of security. These policies need to be clearly communicated to employees and security measures and practices must be detailed with training, where necessary.

Tips for C-level employees when managing IT security risks

Charl Ueckermann 2 Feb 2018

“Isolating BYOD devices from high-value systems is also recommended, but in a way they can be used for day-to-day activities while enforcing stricter permissions to use other, more business critical, resources,” says Hamman.

"You can't find what you can't see"

“The most important consideration of all, however, is knowing that you can’t find what you can’t see; solving business issues begins with network visibility,” he adds. “Rather than providing visibility and intelligence only at the vanishing enterprise perimeter, a BYOD empowered business must demand pervasive visibility throughout the enterprise and its linked devices.”

Hamman explains there are solutions available today that detect advanced malware and botnets, remove infected users, identify new users and devices, and more — not just at the enterprise perimeter.

“By seeing the threats throughout the network, enterprises can detect new threats and stop them using the right tools. It is an enterprise-wide belief that the days of just stopping the threat without context or analytics are over; visibility and security intelligence are key.

“Enterprises can protect the business with solutions that enable in-depth visibility into network, application and routing traffic while offering DDoS detection, mitigation and reporting capabilities.

“Lastly, the solution of choice should be extremely scalable, easily deployed and appropriate, whether the business is a small hosting provider with a single data centre or a large cloud services provider with multiple data centres and extensive network connectivity.”