BIZCOMMUNITY

Staying one step ahead of information security threats

By Brendan McAravey

18 Apr 2016

In the recent PricewaterhouseCoopers' Global State of Information Security Survey 2016, 41.44% of companies in South Africa and the Middle East reported that they had detected 50 or more cybersecurity incidents in the past 12 months. This was in comparison to the global total of 31.59%. A further 17.47% of South African and Middle Eastern companies had identified between 10 and 49 threats in the same time period.

Brendan McAravey

These statistics are indicative of a constantly evolving beast – today’s information security landscape. As attack vectors continue to grow, assaults become more frequent and attackers become even more sophisticated. The need to continually adapt to an increasingly hostile environment has resulted in a significant change from the familiar security measures that kept us 'comfortable' a mere five years ago. Although these measures are still valid, the reality is that they are nowhere near sufficient to combat the dangers of today’s increasingly complex threats.

Here are seven recommendations to help you keep up with the rapid pace of change in cybersecurity:

1. Say goodbye to generic 'best practices' security

Compliance is not a security programme – it’s a starting point. Any organisation that is still just ticking the boxes on their audit report is getting breached. Have this conversation in the boardroom and use it to drive the culture towards security that is specifically tailored to the business.

2. Patching is a daily event

Flaws in applications, services such as DNS and foundational software, including OpenSSL, mean that, unlike a few years ago, we can’t wait a month or more for patches. Ensure your organisation can respond with instant remediation across workstations, mobile, servers and clouds. Manage at the application level to respond without having to push new desktop images.

3. Security just got personal

Targeted attacks go after specific individuals with personalised messages and payloads from an apparently trusted source. It’s getting more and more difficult – even for security professionals – to differentiate the malignant from the benign. And the highly rare APT ups the ante when the attacker has found a truly valuable target. More education is necessary, but can only go so far. Hardening must reduce the default attack surface as much as possible, and containment strategies further sandbox attacks.

4. Breaches are to be expected

Formerly denied and only discussed in secret, breaches are now a reporting requirement for many organisations. A prescribed approach to incident management includes both technical and reputational responses. Containing breaches and their impact has been a deciding use case for app virtualisation across governments, healthcare and financial services. Virtualising all browser-based access is a leading practice for containing attacks against one of the most popular entry points for organisational breach.

5. End-to-end strong encryption is mandatory

Encryption is no longer just for networks and hard drives. Encryption must protect sensitive data within and between applications, from desktops to mobile. Criminals have also recognised the value of encryption, with ransomware leveraging encryption as a weapon. And, as the painful death of SSL has shown, outdated encryption can be as bad as no encryption at all. Ensure that you control encryption for endpoints through app and desktop virtualisation, on mobile devices with enterprise mobility management, and for cloud and web apps with an application delivery controller with embedded web app firewall.

6. Security begins with access

A deep knowledge of situational context is necessary to control identity, authentication, authorisation and access control. Focus on the 5Ws of Access for employees and non-employees – who needs access, what are they accessing and when, where do they need access from, and why do they require access. Use virtualisation to provide fine-grained access control for privileged users and to ensure that there is no direct access to sensitive data.

7. IT has competition

End users think they can do computing better themselves. And in some ways, they can. But not security. Ensure that Shadow IT, unsanctioned BYO and the use of consumer-grade apps, clouds and services for sensitive data are replaced with IT-controlled and sanctioned offerings. Simplify things for users by enabling single sign on, improving their access and automating a superior experience across devices.

This is by no means a prescriptive list. Information security teams should remain on guard at all times and aim to stay one step ahead of those who will take advantage of any negligence or ignorance. Nobody can afford to stand still. Attack vectors and exploitation methods will increase alarmingly, as more devices, people and locations become connected. And, as IoT becomes more of a reality, the need for sophisticated cybersecurity will increase exponentially. It’s time to keep watch, with both eyes open.

ABOUT BRENDAN MCARAVEY

Brendan McAravey is Country Manager at Citrix South Africa. McAravey is responsible for the growth and development of Citrix operations across the southern African development community, driving revenues, generating new business opportunities and cultivating the company's valued partner ecosystem.

- Technology developments outlook for 2020 - 3 Feb 2020
- Local enterprises need to think outside the cubicle - 3 Jul 2019
- 3 Things that make workspaces intelligent - 22 Mar 2019
- Boost employee productivity using technology - 24 Jan 2019
- Trends and technologies that will impact in 2019 - 17 Dec 2018

View my profile and articles...