datacentrix

Datacentrix takes on hacktivism and other vulnerabilities with new SOC services

The past two years have seen a veritable explosion of new cybersecurity vulnerabilities, including a steep increase in hacktivism, which Wikipedia describes as "the subversive use of computers and computer networks to promote a political agenda or a social change. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights or freedom of information movements."

Hacktivism came to a head in 2016 around the US elections, with numerous reported malicious cyber assaults being carried out against candidates (including Donald Trump, Hillary Clinton and Bernie Sanders), political parties and governmental IT networks.

Continuing into 2017, we saw WikiLeaks publish thousands of documents claiming the exposure of hacking secrets of the Central Intelligence Agency (CIA), which included the agency's (and presumably other hackers') abilities to break into mobile phones, smart TVs, and Microsoft, Mac and Linux operating systems.

A Wired.com article from August 2017 stated that: "Yesterday's WikiLeaks dump reiterated something we already knew: our devices are fundamentally unsafe. No matter what kind of encryption we use, no matter which secure messaging apps we take care to run, no matter how careful we are to sign up for two-factor authentication, the CIA can infiltrate our operating systems, take control of our cameras and microphones, and bend our phones to their will.

The same can be said of smart TVs, which could be made to surreptitiously record our living-room conversations, and internet-connected cars, which could potentially be commandeered and even crashed."

This year, a mere few weeks ago, a number of global technology companies began to roll out patches addressing design flaws in processors that were named 'Meltdown' and 'Spectre'. The chip vulnerabilities leave devices such as desktops, laptops and smartphones exposed to unauthorised access and information theft, as well as cloud and virtual environments.

"Looking at the course of events over the past two years alone, it is clear that organisations across the globe are grappling with a very real, ever growing data security issue – whether it be held on premise or within the cloud," states Wayne Olsen, security business unit manager at Datacentrix. "Businesses are under immense pressure to protect increasing volumes of data, prevent a myriad of attacks, and do it all faster and more effectively than ever before."

In order to support local companies looking to boost cybersecurity measures, Datacentrix is launching two new services within its industry-leading Security Operations Centre (SOC).

"Firstly, we have created the Datacentrix Cyber Threat Intelligence offering, which will allow local firms to monitor malware, phishing and hacking attacks, identify when information has been stolen, as well as check for malicious mobile attacks. We've increasingly found that applications are being launched using an organisation's name, without its knowledge or permission.

> **"We have created the Datacentrix Cyber Threat Intelligence offering, which will allow local firms to monitor malware, phishing and hacking attacks, identify when information has been stolen, as well as check for malicious mobile attacks. We've increasingly found that applications are being launched using an organisation's name, without its knowledge or permission."**

Wayne Olsen, security business unit manager at Datacentrix

"A recent example of this was a fake version of the WhatsApp app that was downloaded a million times from the Google Play Store before it was discovered to be fraudulent. The Cyber Threat Intelligence offering will help to protect against all of these vulnerabilities, as well as other brand abuse, such as bogus social media accounts created using companies' names."

The new service allows Datacentrix to find existing and potential attackers – even on the dark web – minute by minute in real time, and "take them down", Olsen explains.
"Secondly, Datacentrix is also introducing a Contextualised Vulnerability Management service, which will identify potential weak spots within a business' network topology, and put them at the top of the risk and vulnerability list," says Olsen. "This allows organisations to then remediate any problem areas.

"As a trusted security solution provider, it is Datacentrix' intention to monitor and defend customer ICT environments in real time against any potential security threats, but to do this in such a way that our clients are also able to reduce costs and leverage existing technology for improved insight. We believe that the new services added to our SOC offering will be a game-changer in the local market," he concludes.

For more information please contact Wayne Olsen: wolsen@datacentrix.co.za