Kind regards,
Salome

From: Heidi Swart [swart.heidi@gmail.com]
Sent: 19 May 2020 01:18 PM
To: Media@Telkom
Subject: Re: MEDIA Questions from the DAILY MAVERICK: HUAWEI CYBER SECURITY

[Quoted text hidden]
[Quoted text hidden]

Media@Telkom <Media-Telkom@telkom.co.za> Wed, May 20, 2020 at 8:22 AM
To: Heidi Swart <swart.heidi@gmail.com>

Good morning Heidi,

I hope you are well.

Please find the below response.

Telkom takes a holistic view of network security and management, for both internal and external threat management. Telkom is cognisant of the geo-political implications around using Huawei and is actively looking at its strategic approach regarding this going forward. We adhere to the King IV principles of good governance, including Principles 1, 11 and 12 which speak to the governing of risk, especially as it pertains to technology and information.

The Huawei Cyber Security Evaluation Centre's security findings relate mainly to software consistency, configuration management, third-party component support, lifecycle management, and LTE software improvement. These items are aggressively managed by Telkom in a systematic way to limit the ability of attackers to gain access to mobile network elements. We use a well-established type approval process before any new deployment of hardware and/or software through change advisory boards with strong control systems.

Telkom operationally manages and controls, amongst others, software testing, configuration testing, software version control, strict access management enforcement, segregation of duties, network element operating system and database hardening, perimeter security (excl. Firewalls and DDoS protection) and encryption of specific customer-sensitive data flows.

Intrusion prevention systems and egress firewalls are operated by Telkom/Openserve and are not supplied by Huawei. In addition, Telkom conducts annual internal and external audits to check for adherence, proof of closure of previous findings and identifying new findings in relation to operational management activities. This is in keeping with the finding of the UK's HCSEC that "…architectural controls in place in most UK operators limit the ability of attackers to engender communication with any network elements not explicitly exposed to the public which, with other measures in place, makes exploitation of vulnerabilities harder".

We work closely with the State Security Agency (SSA) to ensure that legal interception solutions (not supplied by Huawei) are used in accordance with South African law. We do not currently have any active projects with the SSA addressing Huawei-specific concerns. We believe establishing an evaluation centre such as the UK's HCSEC would be most effective as a cross-operator, supplier and government initiative.

Kind regards,

Salome.
