Gmail

Heidi Swart <swart.heidi@gmail.com>

MEDIA Questions from the DAILY MAVERICK: HUAWEI CYBER SECURITY

Willem Roos <willem@rain.co.za> Thu, May 21, 2020 at 10:06 PM
To: Heidi Swart <swart.heidi@gmail.com>

Dear Heidi,

Thank you for your question pertaining to the security of mobile networks in general, and rain's network in particular given the fact that Huawei equipment in used extensively in our network. It is certainly a very important issue that needs examination.

Before I answer your questions specifically, I would like to make a few general comments:

• rain takes users' privacy and security extremely seriously. We believe it is primarily the responsibility of the network operator to ensure that its network is secure, customer data is protected and compliance is in line with best-practice and the laws of the country.
• rain uses many vendors throughout our network, with Huawei and Nokia being our main suppliers.
• Huawei is a world leader in 5G technology, and a trusted partner from rain's point of view.

To answer your questions more specifically:

Q1. In light of the fact that South Africa does not have an equivalent to the UK's HCSEC, and given that Huawei equipment is used in core and non-core sections of South Africa's mobile networks, how can Rain assure the South African public that its networks are not at an increased risk because of Huawei equipment?

A1. rain has no reason to believe that Huawei equipment specifically carries increased security risks compared to other vendors. We have seen the findings of the HCSEC board report (published in March 2019) which Huawei has undertaken to correct, and have made significant progress in doing so.

Q2. Does Rain work with the State Security Agency (SSA) to mitigate the risks of Huawei's equipment? If so, could you please provide details of how this is done (for instance: Does it take place on Rain's premises, or at a separate premises? Does Rain invest any money in such efforts? Do you have joint cyber security teams with the SSA?)

A2. rain complies with all the pertinent laws and regulations in South Africa, and we work closely with all the relevant Government agencies involved (i.e. the Department of Communications and Digital Technologies as well as the SSA). rain has invested significant resources and money to ensure we are compliant and in line with international best-practice.

Q3. Is Rain at all planning on lobbying Huawei to establish an independent, transparent evaluation centre similar to the UK's HCSEC in South Africa? If so, is it possible to provide any detail, such as when it will be opened, or how it will be funded? If not, can you provide reasons?

A3. We believe the current regulatory framework in South Africa is sufficient to protect users' privacy.

Q4.1. Do you use Huawei-manufactured interception equipment? If so, how do you mediate associated risks?
Q4.2. Do you use ZTE - manufactured lawful interception equipment? If so, how do you mediate associated risks?
Q4.3. If you use neither of these brands, which brand do you use?

We currently do not use any Huawei or ZTE equipment specifically in our cybersecurity and lawful intercept area. We primarily make use of Utimaco (www.utimaco.com).

Kind regards

Willem
[Quoted text hidden]