Flaw in Vodacom software caused security leak

Faulty security software at cellphone network operator Vodacom allowed the distribution of the cellphone numbers of the company's subscribers to websites they browse on their phones.

Vodacom's Richard Boorman now admits that the company inadvertently supplied users cellphone numbers and IMEI numbers to some websites and blamed flawed security software for the distribution of these details. Image: IMC

The problem surfaced after Vodacom attempted to upgrade its security software. But instead of improving security the new software sent cellphone numbers and a unique identifier for mobile devices, the international mobile station equipment identity, to websites.

Networks use these identifiers to identify devices and blacklist or block stolen phones from accessing the network, rendering them useless.

Vodacom revealed this week that company engineers were urgently trying to fix the bug.

Spokesman Richard Boorman said: "On Wednesday (29 October), a bug, which in some cases was disseminating customers' cellphone numbers and IMEI details to websites, was identified. These details however were only sporadically visible on websites.

"As soon as we became aware of [the bug] we reversed the software update," he said.

Not known how many customers were affected

Asked how many customers had been affected, Boorman said the company was investigating but it might not be possible to determine the number. Vodacom has 32.5m South African subscribers.

Vodacom offered services that allow customers to charge purchases to their phone bill, such as apps downloaded from app stores. This was especially important for customers without credit cards.

"We support services to which customers opt in, such as our Look For Me emergency location service. In these instances, we provide the cellphone number to the app store or service provider so the store or provider can charge for the service," he said.

The flawed security software released by Vodacom meant some website received the IMEI numbers of users that logged onto their websites. Image: GizmoDirect

Such transactions were previously authenticated only by a cellphone number. The security upgrade would have authenticated both the cellphone number and the device's equipment identifier.

"This was done as an extra security check, so we could raise red flags if we saw a cellphone number being used with more than one device for a charge-to-bill service. We did it because we didn't want customers to be charged for something they had not bought," Boorman said.

"We are not trying to gloss over this, but Vodacom did not deliberately forward this type of information for [gain]," he added.

"Vodacom doesn't sell customer information to third parties and we don't disclose personal information, such as customer names or billing information. The only information that would have been passed on would have been cellphone and IMEI identification numbers," he said.

For more, visit: https://www.bizcommunity.com