Smart homes - easy prey for hackers

While the increasing use of home automation technology to create your version of a 'smart house' may be all the trend and seem practical, Richard Keymer, Head of Pre-sales at SecureData Africa, the largest security focused distributor in Africa, warns of the flipside in that once an automation system is established and can be operated remotely online, then chances are it can be hacked.

Image: www.freedigitalphotos.net

"A growing trend in electronics is to have them integrate with your home network in order to provide potentially useful features such as automatic updates or to extend the usefulness of existing technologies such as remotely controlling irrigation systems, pool pumps, garage doors, cameras and other devices. This allows their owners to turn these things on and off with a Smartphone app or via the Web.

"However, what living in this world of network-connected in fact means is that we run even greater risk of being compromised. Even more terrifying is that while in the past a compromise only meant your data was out of control, today it can enable control over the physical world," he comments.

Security concerns

Keymer explains that as we bring things in your homes onto the internet, we run into the same kind of security concerns we have for any connected device.

"Many of these devices have systems that have been made crawlable by search engines- meaning they show up in search results. And should they not require user names and passwords by default, you can click on the links, giving hackers the ability to control these devices in your home which could potentially result in covert audio/video surveillance, physical access or even personal harm," he says.

Keymer believes that part of the problem is that the companies manufacturing and installing home automation devices automatically assume that your home network is a fortress and has adequate network security measures in place, when in most cases it doesn't.

"Another problem is that some products don't have password protection by default which means that anyone who figures out the IP address for a particular device can hack into it. An additional issue is that once certain devices are connected to a Wi-Fi network they assume that whoever is using the network is the authorised user. So if you can manage to get on someone's Wi-Fi network, which is easy enough if they have no password on it, you could potentially take control of their home," he explains.

Ask security-related questions

For Keymer, asking the vendor the right questions around security is a must. "People opting to use home automation systems need to realise that in most instances the vendors are not network security experts and at best have limited knowledge of the potential risk of hacks to networks and Wi-Fi networks."

"And if you're doing it yourself, you need to do your homework and understand the reality of the risks and ensure the correct protocols and security measures are implemented in home environments," he advises.

Keymer also advises against using default username and passwords, and not leaving ports open or using port forwarding. "Users should make use of VPN systems whenever possible and using open hot-spots are a no-no," he adds. "However, that being said, it is also important that companies developing these types of devices and products implement proper security testing before releasing products."

And while in the past home automation enthusiasts were required to re-wire their homes, Keymer says that with today's smart TV functionality, devices are becoming increasingly easier to retro-fit.

"Five years ago, home automation wasn't a reality locally. However, as devices get smarter and increase in efficiency, we will no doubt see ever-expanding product lines when it comes to these devices and systems. Unfortunately the reality here is that we will also see them gaining more attention from hackers who will come to realise how insecure many of these systems actually are," he concludes.