Security a risk for 'Internet of Things'

By Thabiso Mochiko

28 Jul 2014

Not long ago cloud computing and "bring your own device" to work began to change the way businesses and individuals used technology. This is now expanding to include the concept of the "Internet of Things" (IoT).

SAPs Pfungwa Serima says the Internet of Things will have a major impact on consumers. Image: BizNis Africa

IoT is described as a network of devices, or "things", that have embedded technology to enable them to interact with each other. It includes objects or devices like security systems, thermostats, electronic appliances, lights in homes, medical devices, alarm clocks, cars and vending machines.

IoT can, for example, connect a machine that captures your blood pressure and sends it directly to your doctor's smartphone.

Vehicles and appliances will soon have the ability to monitor themselves and let their owners know when they require a service, says Pfungwa Serima, SAP Africa CEO, in a press release.

A Morgan Stanley report predicts that the number of devices connected to the IoT will reach 75bn by 2020.

In a report by New York-based network security firm Fortinet, two-thirds of respondents say a connected home, where household appliances and home electronics are seamlessly linked via the Internet, is "extremely likely" to become a reality within five years.

Chinese consumers are most convinced: 84% believe that is a likely outcome. In SA, this figure is 60%.

Security and privacy protection needed

A statement by Fortinet quotes Regional Director for Africa Perry Hutton as saying: "The ultimate winners of the IoT-connected home will come down to those vendors who can provide a balance of security and privacy compared with price and functionality."

Fortinet's Perry Hutton says business will drive the Internet of Things. Image: BizTech Africa

The IoT market is expected to hit $7trn by 2020, according to research firm International Data Corp.

IoT objects have the ability to change the state of the environment around them, or even their own state, Earl Perkins, Research Vice-President at tech firm Gartner, reports.

For example, it could raise the temperature of a room automatically once a sensor has determined it is too cold for you. Or it could adjust the flow of fluids to a patient in a hospital bed, based on information from the patient's medical records.

Fortinet's survey, which was completed in June, shows that price will affect usage, even though home owners say they are willing to pay more for a "connected" home.

Business drives adoption

Though IoT is still in its early stages, Hutton told the Financial Mail that business can drive its adoption.

"For example, some car insurance companies already offer free installation of a device to monitor driving behaviour and reward good driving," he said.

Security Analyst Jonas Thulin says that security is a fundamental requirement for the Internet of Things. IT Pro

Food retailers could provide a free Internet interface for a consumer's fridge, which can be used to order replacement supplier automatically when these are running low.

Fortinet security consultant Jonas Thulin confirmed in an interview that IoT is already happening. "The smartphone is a big driver. Look at the number of devices available now that will connecy your phone with appliances] in your home that relate to your weight, sound systems, electricity consumption, video camera, security, and so forth."

A"s with all new technology, the risk or inadequate security is a concern. Devices or equipment that can connect to the Internet can be hacked or controlled from a different location and changed accordingly," Thulin said

Security ignored in rush to get products to market

He warns that new measures are needed to protect the data that the devices create.

"IoT promises many benefits for end users, but also presents grave security and data privacy challenges", says Hutton.

He says crossing these hurdles will require the "clever" application of security technologies.

These include remote connection authentication, virtual private networks between end users and their connected homes, protection against malicious software as well as the application of security on premises, in the cloud and as an integrated solution by device manufacturers.

Jayson O'Reilly of DRS warns that security should be built-in rather than added as an afterthought. Image: LinkedIn

According to the report, consumers are aware of the risk. Most respondents to Fortinet's survey voiced their concern that a connected appliance could result in a data breach or exposure of sensitive, personal information. They also want control over who can access collected data.

Jayson O'Reilly, director of sales and innovation at security firm DRS, says in a statement that the technology industry has a long history of ignoring security in the rush to open new markets.

"We've already witnessed instances of hackers exploiting security holes in smart TVs and baby monitors, and more," Thulin says,

O'Reilly says companies that design and build IoT devices should apply security practices and protocols that will update and patch the security [systems] the devices use.

"There is no doubt that the IoT could have an enormous impact and radically alter our lives for the better.

"However, to ensure it doesn't become more of a hindrance than a help, security must be built in from the start, giving consideration to each component, how it will be used, and what sort of data it will contain.

"If nothing else, the last few years have shown us the hard way that security must be built in, not thrown in as an afterthought," O'Reilly says.

Source: Financial Mail via I-Net Bridge