50,000 affected by security camera privacy breach

by Andrew Ramadge via stan - SMH *Tuesday, Apr 10 2012, 1:40am*
international / mass media / other press

Watching 'Martha'

> Thousands of people all over the world could be watching 'Martha' [or you] get ready for bed right now. But Martha isn't an entertainer. She's an elderly woman, and she almost certainly doesn't know that the inside of her home is being broadcast on the web due to faulty video equipment.

Martha – or more likely, one of her carers – was one of up to 50,000 people who bought and installed a security camera made by the US company TRENDnet before it was discovered that the live footage they captured could be watched by anyone with an internet connection, without even having to guess a password.

Since the flaw was discovered in January, some TRENDnet customers have taken steps to fix it. But many haven't, and apparently remain unaware that the devices they installed to keep themselves safe could in fact be doing the exact opposite.

The reason they remain unaware is because very few customers registered their devices with the company, and TRENDnet is unable to fix the problem remotely. Users must download a software update from the company's website and install it manually.

The Australian distributor for TRENDnet took steps to contact local customers in February. But many others overseas – such as Martha – are unlikely to read tech stories like this one and are impossible to identify by their camera feed.

Even when it is possible to track down the owner of a webcam, the scale of the problem can be difficult to explain. One office worker at a university identified by Fairfax Media through its camera footage sounded suspicious when the problem was described over the phone, and did not answer emails offering advice on how to fix it.

Several days later, the university's camera was still active, showing workers and students visiting a teaching department, their faces clearly visible.

The TRENDnet case is an extreme example of what can go wrong when a security flaw is discovered

in a device connected to the internet. A similar problem would have never been technically possible for users of a CCTV, or “closed circuit” TV, system, which is kept offline.

But it's not just webcams that present a security risk. Our homes are increasingly full of all sorts of devices connected to the internet, such as phones, digital video recorders and TVs.

“There's no shortage of newly-connected devices entering our homes every day,” says Chris Gatford, the director of Australian security testing company HackLabs.

“And because now everything is connected in our homes, if one device does have a security problem, it's very likely to compromise the entire house.”

According to several estimates collected by the IT research company Gartner, there are about 10 billion gadgets connected to the internet today, and the figure is expected to double by 2015.

Mr Gatford says that means Australians will have to be vigilant when it comes to buying new devices and should put pressure on manufacturers to ensure a high level of security features.

In the case of TRENDnet, Mr Gatford says that many simple devices like security cameras are not currently equipped to receive automatic updates – but could be if consumers demanded it.

“Typically these devices are very 'dumb', in that they're not going out and looking for updates and they would struggle probably to manage [automatic] updates,” he says.

“As a consumer, maybe the new thing we'll be asking our local salesperson is, you know, 'Excuse me sir, does this product do automatic updates?'

“We need to be focusing on the vendors of these solutions and trying to put pressure on them to make sure that they're making products that are fit for use.”

Smart TVs and digital video recorders, often known as DVRs, are other types of internet-connected devices that Mr Gatford says could come with security risks.

“These are just computing devices. So the typical vulnerabilities that work on a PC, you know, probably could work just as well on these devices as well,” he says.

The advice Mr Gatford gives to friends and family who ask how to keep a home network of devices secure is to install any updates when a device alerts you, to look for devices with automatic updates built-in and, where possible, to stick to one brand with a reputation for taking security seriously.

http://tinyurl.com/c8fthkl
