The dangers of a connected world

By Lutz Blaeser

8 May 2015

While the Internet of Things (IoT) is a fairly new concept, it has arrived. Over and above PCs, smartphones and tablets, internet-connected devices such as speakers, baby monitors, fridges, cars, thermostats, fans, lights, and locks can connect to the internet, with new devices being connected every day.

The problem is that the IoT is connecting places that were never originally designed to be connected to the internet. Energy grids, critical infrastructure, air traffic control - all these systems can now connect to the Web, which means they can be hacked by a determined-enough threat actor.

Too easy for hackers

The IoT is now a de facto part of everyday life, and is integral to the way we do business too. Smart homes are commonplace now. Lighting, security, smart metres - just imagine the potential for abuse. The fact is, if it connects to the Web, it is only a matter of time before it will be hacked.

Unfortunately, security hasn't been built into these devices from the ground up, and has been seen as more of an afterthought. Businesses, driven by profits and wanting to be the first to market, rush to introduce new products, without having security through properly. This makes it child's play for hackers to compromise the vulnerabilities in these devices, as has been seen by hacks in the past few years of pacemakers, cars, smart fridges and similar.

Potential impact

The vast adoption of the IoT will take time, but it is never too early for executives across all organisations and industries to start really thinking about the potential impact and opportunities likely to emerge from this phenomenon.

Security needs to be top of mind, and built into IoT devices at the beginning. This will be expensive, but cheap at the price when you consider the potential impact and cost of the risks. The IoT could definitely revolutionise our lives, and shift the way we consume, the way we live and the way we do business. However, it also has the potential to be an enormous liability. Security must be a primary consideration, and not something to be tacked on willy-nilly at the end.

ABOUT LUTZ BLAESER

In 2011, Blaeser founded Intact Security, building on his knowledge and experience of the reseller market. His main focus at Intact Security is to continue building the Avira Antivirus market but also provide additional solutions into the offering. Since the company's inception, he has added additional antivirus and content security products such as Bitdefender, AVAST, G Data and Kaspersky as well as leading backup and disaster recovery solution StorageCraft.

- How to understand bad user behaviour - 12 Nov 2015
- The dangers of a connected world - 8 May 2015
- Mobile malvertising skyrockets - 9 Feb 2015
- Security is no longer a catch-up game - 30 May 2014

View my profile and articles...