BIZCOMMUNITY

Combatting the evil Internet of Things

By Peter Reid

15 Jun 2016

A recent survey of over 400 global IT security pros revealed that fears over the security of connected devices has risen sharply since last year. 86% of respondents to security analysts Pwnie Express' survey said they were worried about device threats - with 50% either 'very' or 'extremely' concerned. Many had even witnessed attacks first-hand.

Connected, smart devices are rapidly advancing into almost every area of our lives: our homes, our cars, our offices, and even our bodies. Most market commentators forecast tens of billions of connected devices by the end of the decade. However, while we remain in a state of enchantment over the possibilities of the Internet of Things (IoT), too few consumers and businesses are stopping to think about the critical security concerns the IoT revolution brings.

A fundamental adage of security is that the more devices you have connected to a network; the more vectors of attack are exposed. Although one of the biggest drivers of IoT adoption is sharply falling costs, the repercussion of this is that many connected sensors and devices are stripped down to the bare minimum – with insufficient consideration for encrypting and protecting those devices.

Not just a ‘dumb sensor’

As consumers we forget that even the most basic sensor is actually a small computer, a fully-fledged ‘Von Neumann device’ with its own processing and integration capabilities. By recognising this reality, we see that any connected object can potentially be hijacked and used for malicious purposes. Vulnerabilities abound wherever these devices are connected to wireless networks: whether that’s Bluetooth, NFC, WiFi, 3G, or any other form of wireless protocol.

Many ask what the real risk would be, if somebody, for example, was able to hack into my home thermostat or my connected toaster? While it's obviously unlikely that anyone would want to hack into your connected home infrastructure to change the temperature of your living room or burn your toast; that wouldn't necessarily be the attacker's end-goal.

Attacks often work in a progressive manner, where one small breach can open up opportunities to penetrate other areas of the network, and cause more damage. Attackers might compromise a printer on a corporate network, to sniff for passwords that would then enable them to configure their own admin-access.

So, the printer, or the thermostat, might just be the first step in a long chain of progressive breaches.

Remaining secure

To combat the threat of the 'evil Internet of Things', much needs to be done, at both an individual or company level, and at a broader industry level.

• Hard-wiring security into every device: IoT manufacturers and vendors need to consider the evolving nature of security in their product development from the outset. Achieving IoT security from the ground up involves ensuring the rigorous encryption is 'baked' into the devices themselves.

• Taking responsibility: Organisations embedding and allowing connected devices onto their networks must develop strong controls to ensure no weak links in the chain. This could include 'bring your own device' policies to manage mobile devices and wearables in the workplace, thorough analysis and testing of any IoT vendor they're using, and information security policies to manage the protection of sensitive data.

• Achieving standardisation: Many current machine-to-machine protocols were designed to be fast and efficient on local closed-loop networks. Now that we're connecting many of these devices to the open-loop IP standard, their vulnerabilities are becoming clear. In the modern, connected world, the devices need to comply with the established security protocols to ensure they can be safely patched into the global internet.

• Focus on the information that's being secured: As individuals, we're generally comfortable with vast amounts of personal data stored with ecosystems managed by the likes of Apple, Google and Facebook. As businesses, we need to adopt the same diligence as these digital leaders, in focusing on the protection of personal data from employees, customers, partners, and other stakeholders.

• Threat detection and early response: The threat landscape is in a never-ceasing state of evolution. So with all these other practices in place, attacks are still possible. It's essential for organisations to develop the instrumentation to quickly spot any attacks, and minimise the damage.

Think back to the way that online banking and e-commerce has taken off – supported by mature standards and huge emphasis on security. In a similar way, the incredible opportunities presented by a billions of connected devices will only be possible with a rigorous approach to security.

ABOUT PETER REID

Peter Reid is the Executive Head of Intervate, a T-Systems company
- Combatting the evil Internet of Things - 15 Jun 2016
- The journey to the cloud needs a practical, pragmatic approach - 20 Aug 2015

View my profile and articles...