Feature: Internet of Things Security - are you failing to prepare?

Submitted by: Nuvias
Wednesday, 24 May 2017

Internet of Things Security - are you failing to prepare?

By Ian Kilpatrick, Executive Vice-President Cyber Security at Nuvias (https://www.nuvias.com/) Group

Flickering lightbulbs, scary Barbie dolls, infected computer networks and cities out of action. Could this be the brave new world of the Internet of Things (IoT), if we neglect IoT security? Ian Kilpatrick, EVP Cyber Security for Nuvias Group, discusses the unstoppable growth of IoT and the necessity for organisations to take appropriate measures to protect their computer networks.

For several years, the IT industry has enthusiastically extolled the virtues of the Internet of Things (IoT), eager to enlighten us to the difference that living in a connected world will make to all our lives.
Now the IoT is here - in our homes and in the workplace.

Its uses range widely, from domestic time-savers like switching on the heating, to surveillance systems, to “intelligent” light bulbs, to the smart office dream.

This proliferation of devices and objects collect and share huge amounts of data. However proliferation also has the potential to create greater opportunities for vulnerabilities. Moreover, because these devices are connected to one another, if one device is compromised, a hacker has the potential opportunity to connect to multiple other devices on the network.

Indeed, there have been a number of high-profile cases where everyday items have been used to force websites offline. Recently, hackers harnessed the weak security of internet-connected devices, like DVRs and cameras, using botnets implanted on the devices, to take down sites such as Amazon, Netflix, Twitter, Spotify, Airbnb and PayPal.

More recently, security vulnerabilities in the new, Wi-Fi enabled Barbie doll were discovered, turning it into a surveillance device by joining the connected home network!
Elsewhere, researchers said they had developed a worm that could potentially travel through ‘smart’ connected lightbulbs city-wide, causing the web-connected bulbs to flick on and off.

These are just a few examples of the security failures in devices for the IOT. Unfortunately, they are not the exception. Manufacturers are rushing to make their devices internet-connected but, in many cases, with no thought (or indeed knowledge) around security.

The next step on IoT’s journey is connected or smart cities, where the consequences of an attack are enormous. It’s not just one lightbulb – a hacker can potentially plunge an entire city into darkness, or disable surveillance systems, causing chaos.

With IoT devices now moving into the workplace, organisations are increasingly vulnerable to attack. A survey (https://451research.com/images/Marketing/press_releases/VotE-IoT-Q2-Org-Dynamics-PR_FINAL.pdf) by

analyst group 451 Research predicts that enterprises will increase their IoT investment 33 percent over the next 12 months, but that security remains a concern with half of respondents citing it as the top impediment to IoT deployments.

Nevertheless, it says that organisations are forging ahead with IoT initiatives and opening their wallets to support IoT deployments.

There's no turning back the tide of any of these IoT applications – and in fact we shouldn't try to halt progress. However, checking the security capabilities before deployment isn't a bad strategy. Especially as it is important to ensure that the advance of IoT isn't providing hackers and criminals with another entry point for attack.

Securing the IoT

The IoT challenge is backfilling security onto IoT devices. Because these devices are not running on standard operating systems, they are often invisible to a large part of an organisation's defences. And if a device is compromised, and you end up with malware within your organisation, you must firstly spot the breach, and then find out where it's coming from – not an easy task.

Cleaning the device won't necessarily fix the problem, as you will have a compromised IoT device within your security perimeter, which will just continue to re-infect other devices.

There are many different types of solutions available. Kaspersky Labs, for example, has Kaspersky OS (https://os.kaspersky.com/), a secure environment for the IoT. Other suppliers, including Tenable Networks (https://www.wickhill.com/products/vendors/detail/117/Tenable) and Check Point (https://www.wickhill.com/products/vendors/category/30/Intrusion-Detection--Prevention), also provide solutions that are relevant here.

A key action for organisations is to pay close attention to the network settings for IoT devices and, where possible, separate them from access to the internet and to other devices.

Also IoT devices should be identified and managed alongside regular IT asset inventories; and basic security measures like changing default credentials and rotating strong Wi-Fi network passwords should be used.

As much as IoT manufacturers need to embed adequate levels of security into their devices, the ultimate responsibility for ensuring an organisation is secure is with the user. This is particularly true as Chief Information Security Officers (CISOs) are under more pressure than ever to maintain the integrity of their organisations, in the face of increasing legislation such as the General Data Protection Regulation (GDPR), which carries potentially crippling fines for data breaches.

Ultimately, IoT is here, and it isn't secure. It won't be secure until IoT device manufacturers make it secure, which will be many years in the future. In the meantime, it's down to organisations to make sure they are protected. User education should be a key element in defence around IoT deployment, partly because of the increased risks of shadow deployment in the workplace with IoT devices.

Business leaders need to ask their IT department or CISO for a strategic plan to deal with IoT vulnerabilities, rather than burying their head in the sand. As the saying goes, a failure to plan is planning to fail.

ENDS

Bio of author
Ian Kilpatrick, EVP (Executive Vice-President) Cyber Security for Nuvias (https://www.nuvias.com/) Group

A leading and influential figure in the IT channel, Ian now heads up the Nuvias Cyber Security Practice. He has overall responsibility for cyber security strategy, as well as being a Nuvias board member. Ian brings many years of channel experience, particularly in security, to Nuvias. He was a founder member of the award-winning Wick Hill Group in the 1970s and thanks to his enthusiasm, motivational abilities and drive, led the company through its successful growth and development, to become a leading, international, value-added distributor, focused on security. Wick Hill was acquired by Nuvias in July 2015.

Ian is a thought leader, with a strong vision of the future in IT, focussing on business needs and benefits, rather than just technology. He is a much published author and a regular speaker at IT events. Before Wick Hill, Ian qualified as an accountant, was financial controller for a Fortune 50 company, and was a partner in a management consultancy.

About Nuvias Group
Nuvias (https://www.nuvias.com/) Group is the pan-EMEA, high value distribution business, which is redefining international, specialist distribution in IT. The company has created a platform to deliver a consistent, high value, service-led and solution-rich proposition across EMEA. This allows partner and vendor communities to provide exceptional business support to customers and enables new standards of channel success.

The Group today consists of Wick Hill (https://www.wickhill.com/), an award-winning, value-added distributor with a strong specialisation in security; Zycko (http://www.zycko.com/), an award-winning, specialist EMEA distributor, with a focus on advanced networking; and SIPHON Networks (http://www.siphonnetworks.com/), an award-wining UC solutions and technology enabler for the channel. All three companies have proven experience at providing innovative technology solutions from world-class vendors, and delivering market growth for vendor partners and customers. The Group has 21 regional offices across EMEA, as well as serving additional countries through those offices. Turnover is in excess of US$ 350 million.

For further press information, or picture of Ian Kilpatrick, please contact Annabelle Brown on +44 (0)1326 318212, email pr@nuvias.com. Web www.nuvias.com