9 APR 2015 | NEWS

Internet of Things Day: Time to Consider IoT Threats, Say Experts

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil

Follow @philmuncaster

Today marks the fifth annual Internet of Things Day, but security experts have been using the occasion to warn organizations not to allow the IoT to become the ‘Internet of Threats’.

Internet of Things Day is comprised of events all around the world – from Singapore to Sweden and Bangalore to Barcelona – with a mission to promote, educate and share all things IoT.

But security flaws in the design of IoT devices have already set alarm bells ringing for enterprise IT leaders. A study of the 10 most common IoT devices by HP last July, for example, found 25 security flaws per device.

Then, a month later, Eurecom research found zero-day vulnerabilities, backdoors and other security holes in over 140,000 IoT devices, from routers to CCTV systems, which could allow them to be compromised.

Chris McIntosh, CEO of ViaSat UK, warned organizations that a major IoT cyber-attack on a nationwide scale was an “inevitability.”

“Organizations need to limit the scope of access from unauthorized parties as much as possible and assume that their networks have already been infected; this includes ensuring that, even if an attacker makes it into the system, the opportunity to do damage or steal data is limited,” he added.

“Next, organizations will need to take steps to cleanse the network from threats and ensure each node can be trusted to convey the right information.”

Piers Wilson, head of product management at security vendor Tier-3 Huntsman, argued that securing devices isn’t easy as they often can’t run traditional AV, while manufacturers don’t see it as their responsibility to produce kit with “security-by-design” in mind.

“When this *laissez faire* approach to IoT device security enters the enterprise, the risks magnify and go way beyond the traditional security implications of data loss, fraud, damaged reputations or privacy infringements,” Wilson argued.

“Far from being a dystopian security nightmare, there are a number of proactive steps that can be taken to ensure that effective security is maintained as IoT and device-based technologies spread through the enterprise.

The first step is to plan an “IoT-aware enterprise network” using techniques like network segmentation, access control and internal traffic management.

The second stage requires IT teams to work with vendor and business user communities to develop guidelines on how these technologies can benefit organizations.

Finally, firms need to gain visibility into IoT via network/system monitoring.

“This will enable them to ensure that if and when those technologies are attacked, exploited or malfunction, the resulting incident can be quickly detected, investigated and dealt with appropriately,” said Wilson.