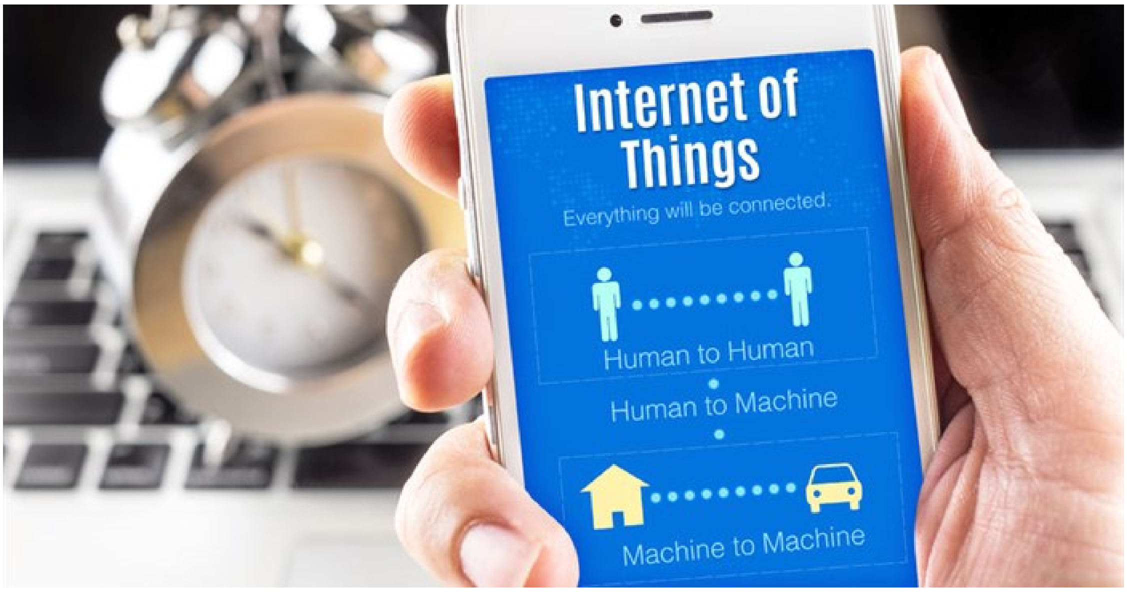
Internet of Things: big opportunities, bigger challenges

Much like cloud and mobility before it, the Internet of Things (IoT) is a topic on everyone's lips, and nowhere is this more true than in the security industry. "Although the IoT is partly a hype, it is definitely a topic that security practitioners need to familiarise themselves with, and add to the business strategy as a whole," says Lutz Blaeser, MD of Intact Security.



©weedezign via 123RF.com

In today's world, he says, all devices - products, sensors, wearables, mobiles - are connected to the internet and to each other. "Naturally this brings a ton of business opportunities, including better customer service, and products, and access to a previously undreamed of amount of information. However, hand in hand with these benefits, come a slew of security challenges and concerns. Anything that is connected to the internet is vulnerable to attack. Failure to secure this increasingly connected world could put company and individuals' data at risk."

Security spend

Blaeser says some recent research conducted by analysts at Gartner revealed that organisations are spending more on security related to the IoT. The study showed that worldwide IoT security spending will reach $348 million this year, a 24% increase from last year, and is expected to reach $547 million in the year 2018. Gartner says overall spending will be moderate at first, but predicts that IoT security spending will grow increasingly quickly after 2020, as improved skills, business change and more scalable service offerings improve on execution.

"The analysts also said they believe endpoint security spending will be focused on connected cars, as well as complex machines and vehicles such as heavy trucks, commercial aircraft and farming and construction equipment," Blaeser adds.

According to him, this focus on IoT security is good, as Gartner also believes that by 2020, one quarter of identified attacks in the enterprise will be linked to IoT in one way or another. "The challenge for security vendors will be to provide usable IoT security features in spite of the limited spend assigned to this area, and the often decentralised approached to the initial IoT implementations within businesses."

End-user threat

Blaeser says the survey revealed another alarming fact: "44% of businesses that admitted to being hacked could not pinpoint the source or type of attack or what the duration of the breach really was. Also, a mere 7% of technical departments allocate over 50% of their time to security. Moreover, more than half those who responded (56%), stated that the insider threat in the form of careless end-users constitutes the biggest security threat to their IoT networks.“

The IoT is growing in importance, and will most likely rise to among the top security priorities and concerns in the years to come. “As technology, and day-to-day devices become more and more interlinked, the consequences of security failure become more and more catastrophic. We have seen cars being hacked. Medical devices such as pacemakers and insulin pumps too. Home lighting systems, fridges, baby monitors. Since computers now control pretty much every device we use, little imagination is needed to picture the worst possible case scenario, should an adversary want to do us harm,” Blaeser says.

As the IoT embeds itself in every aspect of our lives, from industrial control systems to personal devices and the infrastructure we use for transport and power supply, these possible scenarios become more terrifying, he concludes. “It is for this reason that IoT security needs to be top of mind, and vendors and security practitioners need to work together to ensure the IoT wold is a safe one.”