

'IoT will make online devices less secure'

Lax safeguards, poor awareness will raise risk: security firm

JAY SHANKAR
BENGALURU

Devices used to build the Internet of Things (IoT), a network of devices capable of exchanging data, will be used by cyber criminals to 'liberate' attacks in the near future, said Sanjai Gangadharan, regional director, SAARC, AIO Networks, a cybersecurity firm.

"IoT will continue to be used to liberate attacks," Mr. Gangadharan said in an e-mail interview. "The attackers will take advantage of lax security standards in connected smart devices to build massive botnets that are able to deploy DDoS (Distributed Denial of Service) payloads."

"When you combine this with the lack of consumer and user awareness about the vulnerabilities of IoT devices – you have the perfect storm! We call it the DDoS of 'things,'" he said.

A DDoS attack will try to disrupt an online service, ranging from news websites to banks, unavailable by jamming it with traffic from multiple sources disabling the provider of such a service to publish or access information.

"The journey to combat the DDoS of things is two-fold," Mr. Gangadharan said. "First is the role of consumer and users to ensure the vulnerabilities in IoT devices are fixed. This means regular software updates to fix vulnerabilities is critical."

'Weaponised IoT'

"Second is the role of the respective businesses or enterprises who need to do their part to protect their data, resources and networks through the deployment of IT security solutions. Sophisticated application attack, led by weaponised IoT will grow in a big way."

By 2020, \$267 billion will be spent on IoT technologies, products and services, according to Boston Consult-



Weak defence: Critics of the national cybersecurity policy say that the implementation has been poor. ■ GETTY IMAGES/ISTOCK

ing Group. Spending on IoT applications is predicted to generate \$64.1 billion and IoT analytics spending is forecast to generate \$21.4 billion.

A spate of cybercrimes is driving the IoT security market, which is expected to touch \$29 billion by 2020, according to a report by Markets and Markets. The global IoT security market is slated to grow 55% until 2019, a report by research firm Technavio stated.

The global cyberinsurance market will be worth about \$7.5 billion in yearly sales by 2020, and is one of the fastest-growing segments in the insurance industry, according to a PwC report. AIO Networks, a New York Stock Exchange-listed firm headquartered in San Jose, intends to expand its research and development operations at its Bangalore facility for software security products, Mr. Gangadharan said.

"In the modern world, security is all about ensuring the right user has access to the right content on the network. Whatever measures are taken as far as security is concerned is to enforce this control and to ensure no compromise is made."

To protect Internet users India, framed a National Cyber Security Policy in 2013 to safeguard "informa-

tion such as personal information, financial and banking information and sovereign data." Critics of the policy say that the implementation has been poor.

'Law to keep pace'

"In our opinion, it is very difficult to have one single law preventing cybercrimes. The landscape of attacks keeps changing over a period of time. Accordingly, the law has to stay ahead of times," Mr. Gangadharan said.

A foolproof implementation of laws was the need of the hour, he said. But that alone was not sufficient to safeguard businesses against cyberattacks.

"Enterprises and businesses have to also take the responsibility of securing their networks with comprehensive security solutions. Decision makers should think ahead of problems making these laws proactive and not reactive. However, while laws bring regulations in place, enforcement is another key factor."

"Global initiatives may not always suit India... We have our freedom and we need to be able to customise certain initiatives according to our environment," he said referring to steps taken by the U.N, Internet Governance Forum, Council of Europe and Meridian process.