BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

APAC lists in Top 15 nations with higher cyber security risk on medical devices

13 September 2019 | News

Human-factor remains healthcare security's biggest loophole, says Kaspersky

More than two years after the infamous Wannacry ransomware crippled medical facilities and other organisations worldwide, the healthcare sector seems to be learning their lessons as Kaspersky reveals a decreased number of medical devices attacked in 2019.

Statistics from the global cyber security company showed that from 30% of hospital devices infected in 2017, medical organizations have witnessed only 28% of attacks in 2018, and almost one-third lesser for the current year at 19%.

Kaspersky, however, warns that the decline in number of attacks against devices in healthcare facilities is not observed everywhere. More than seven-in-10 medical machines in Venezuela (77%), the Philippines (76%), Libya (75), and Argentina (73%) are still being subjected to web attacks based on the company's freshest data.

Two more countries in the Asia Pacific region were in the Top 15 nations with the most number of detected infections. These include Bangladesh logging 58% of attacked devices and Thailand with 44%.

The numbers were derived after Kaspersky researchers divided the number of devices in medical organisations in the countries with Kaspersky solutions by the number of devices where malicious codes were detected. Medical devices include all servers, computers, mobiles and tablets, IoT gadgets, and hospital machines that are connected to the internet inside a healthcare facility.

"In as much as we want to believe that everybody was awakened by the damage brought about by the Wannacry attack, the reality is that some countries are still lagging behind securing their medical devices. One factor we observe is that the chances of being attacked really depend on how much money the government spends on cybersecurity in the public health sector. Another key reason is the low level of cybersecurity awareness the people inside medical facilities have," comments Yury Namestnikov, Head of Global Research and Analysis Team (GReAT) Russia at Kaspersky.

A Kaspersky survey in healthcare sector in US and Canada uncovered that nearly a third of all respondents (32%) said that they had never received any cybersecurity training from their workplace. There is also one-in-10 employees in management positions which admitted that they were not aware of a cybersecurity policy in their organisations.

In terms of the loopholes cybercriminals use to infect hospitals and medical facilities, Namestnikov noted that outdated Microsoft office accounts to 59% of all exploit attacks in 2019. It is followed by EternalBlue (32%), which is related to Wannacry, as well as Android devices (2%) which are gaining increased access in medical networks.

“Medical infrastructure has a lot of devices, some of them portable, most of them are becoming more and more connected to the internet. There’s even a technology being developed which will soon allow doctors to do surgeries remotely. We’re definitely entering the era of the ultra-connected medicine. And I have to say that, while we welcome these advancements, we cannot deny that these will open wider doors for cybercriminals. This is a truth the healthcare sector should take into consideration, seriously,” adds Namestnikov.

Acknowledging the serious threat cybercriminals can do against healthcare, Kaspersky suggests medical facilities to:

- Take cybersecurity seriously.
    - Cyberattack in this field should be addressed professionally as it is now a potential risk to someone’s life.
    - All individuals inside a hospital, a clinic, or a medical infrastructure should fully understand the latest cyberthreats and commit to beefing up their workforce, systems, and tools to combat these malicious attacks.
    - Services with threat data feeds and threat intelligence reports can help the healthcare sector understand and prevent potential cyberattacks.

- Verify the security capabilities of your third party suppliers.
    - Medical machines are usually costly and with warranties as long as 10 years. Makers of such healthcare devices should look into building a secure-by-design hardware which is ready for future vulnerabilities.
    - Vendors should also look at forming an incident response team in case of cyberattacks.

- Review access servers.
    - Hospitals and medical facilities are becoming more and more reliant to the internet, hence it is a must to check who has access to which servers and data.
    - Hospital is a public place. An ex-employee can do a lot damage, thus, removal of ex-employee credentials from systems should be taken care of.

- IT security regulation is a must.
    - Similar to the financial sector, relevant public and private should start drafting laws and regulations which aim to address the escalating threats against the healthcare sector.

- Security awareness training for all employees in clinics, hospitals, and other related facilities is more than necessary.