MUST READ US WARNING: NORTH KOREA'S TECH WORKERS POSING AS FREELANCE DEVELOPERS

Singapore sets up cybersecurity assessment, certification centre

Manufacturers and developers will be able to test and certify their products at the new SG$19.5 million ($13.99 million) facility, which is launched by Cyber Security Agency of Singapore and Nanyang Technological University.

Written by **Eileen Yu**,
Contributor

Posted in By The Way on May 18, 2022 | Topic: Security

Singapore has set up a facility to assess and certify systems for their cybersecurity robustness. Manufacturers and developers will be able to have their products tested and certified at the new centre, through which the government hopes to drive the testing, inspection, and certification (TIC) sector for cybersecurity.

The SG$19.5 million ($13.99 million) National Integrated Centre for Evaluation (NICE) will facilitate vulnerability assessment of software and hardware products, physical hardware attacks, and security measures, said Cyber Security Agency of Singapore (CSA) and Nanyang Technological University (NTU), which jointly launched the facility on Wednesday.

They noted that access to security evaluation facilities were difficult, due largely to high equipment cost and deep expertise typically required to carry out cybersecurity evaluation, at the highest assurance levels.

Located on NTU Smart Campus, NICE would provide this access to evaluators and developers as well as house a team of research and technical staff with the expertise to use the equipment.

NTU's deputy president and provost professor Ling San said: "The rising threat of cyberattacks makes it vital that institutions, companies, and agencies stay one step ahead of cyberthreats. Properly evaluating hardware to ensure they are designed with security in mind, rather than added on as an afterthought, is the first step in keeping our cyber-physical systems safe."

CSA's chief executive and commissioner of cybersecurity David Koh added that it was important to ensure new emerging technologies were securely designed, as Singapore moved towards a digital future.

Internet of Things (IoT) and increasing use of cyber-physical systems had led to the growth of devices and hardware components, such as communication points and sensors. Citing forecasts from Business Insider Intelligence, CSA said there would 64 billion IoT devices worldwide by 2025.

to rely on independent experts to perform such security evaluation."

It added that NICE would support Singapore's push for greater security evaluation by providing a central platform on which to test and certify products. The centre also would facilitate research and development in advanced security evaluation techniques.

In addition, Singapore Accreditation Council (SAC) would work closely with CSA and NiCE to develop relevant accreditation programmes. These would include SAC's IT testing programmes that enabled accredited TIC companies to assure the accuracy and consistency of their test reports and certificates that facilitated CSA's initiatives, such as the Cybersecurity Labelling Scheme (CLS).

As of end-April, more than 200 products had been submitted for labelling under this scheme.

To further streamline the labelling process, CSA on Wednesday also unveiled a new initiative, dubbed "CLS-Ready". This would enable security functionalities enabled by CLS-Ready hardware to bypass the need to be tested again at the end-device level.

For example, manufacturers could use a chip that was certified CLS-Ready in their end-user device, saving them time and cost when testing their device against CLS Level 4. By using a CLS-Ready chip, these devices would not need to go through another round of CLS Level 4 testing, as the core security mechanism in the chip already would have been assured as CLS-Ready, CSA explained.

Manufacturers applying for CLS-Ready labels would have to submit an application with supporting evidence and assessment report by an approved lab. These labels would remain valid as long as the devices were supported with security updates, up to a maximum of five years.

To encourage adoption, CSA said application fees for CLS-Ready labels would be waived until October 2022.

First introduced in October 2020, the labelling scheme was expanded in January last year to include all consumer IoT devices such as smart lights, smart door locks, smart printers, and IP cameras. The scheme, which initially applied only to Wi-Fi routers and smart home hubs, rates devices according to their level of cybersecurity features.

consumers to identify products with better security features, CSA said.

CLS assesses and rates smart devices into four levels based on the number of asterisks, each indicating an additional tier of testing and assessment the product has gone through. Level one, for instance, indicates a product has met basic security requirements such as ensuring unique default passwords and providing software updates, while a level four product has undergone structured penetration tests by approved third-party test labs and fulfilled level three requirements.

RELATED COVERAGE

- Singapore widens security labelling to include all consumer IoT devices
- Singapore begins licensing cybersecurity vendors
- Singapore must clamp down on security inertia before digital banking era can take off
- Singapore to introduce security label for smart home devices
- Singapore tightens security requirements for new home routers
- Singapore spotlights OT security, unveils security roadmap focusing on infrastructure

Singapore | Internet of Things