Publication: ZDNet
Date: 1 October 2013
Headline: Singapore aims to up cybersecurity with youth training, public awareness

Singapore aims to up cybersecurity with youth training, public awareness

By Eileen Yu | October 1, 2013 -- 09:10 GMT (17:10 SGT)

Summary**:** Singapore IT Security Authority will open an Advanced Cyber Security Training Facility with Temasek Polytechnic to provide youths with real-world hands-on training, and launch an interactive game to raise public awareness.

Proactive strategies and a sustainable national ecosystem needed to combat cybersecurity threats.

SINGAPORE--Youths in the country can soon tap a new facility to hone their cybersecurity skills under a new initiative from the government, which is also aiming to up public awareness about security threats.

Together with Temasek Polytechnic, the Singapore IT Security Authority (SITSA) will set up an Advanced Cyber Security Training Facility next year to provide students hands-on training based on real-world experience. "This presents a niche which is not easy to replicate, and an opportunity for our youths to become trained and competent cybersecurity professionals who can play a key role in safeguarding our cyberspace," said Masagos Zulkifli bin Masagos Muhammad, senior minister of state for Singapore's home affairs and foreign affairs.

Speaking at the opening of the GovernmentWare 2013 conference here Tuesday, Masagos stressed the need for effective strategies to combat evolving security threats. He noted that cybercriminals no longer worked in a random fashion, adding that targeted cyberattacks increased 42 percent in 2012 over the previous year.

With technology lifecycles short and dynamic, cyberdefense strategies need to move away from a reactive model to one that is proactive and driven by intelligence, he said. The minister underscored the need for early detection and analytics to help identify potential threats in real-time.

"In the event of a cyber incident, a robust monitoring and response structure can mitigate any damage caused. Such a forward-looking approach will allow us to strengthen detection capabilities, protect our assets, and respond to an attack more effectively," Masagos said.

Another speaker at the conference, Thomas J. Harrington, Citigroup's managing director and chief information security officer, also stressed the importance of data collection and analysis. This had enabled Citi to successfully identity potentially adversarial campaigns against the company which it would not have been able to do previously, said Harrington.

Publication: ZDNet
Date: 1 October 2013
Headline: Singapore aims to up cybersecurity with youth training, public awareness

The financial services company adopts the "intrusion kill chain" methodology, also known as the "cyber kill chain", which outlines the typical progression of a cyberattack and provides a structure for segmenting, analyzing, and mitigating an attack. It assumes malicious hackers must progress through each phase of the chain to achieve their objective. The targeted company then aims to disrupt the chain as early as possible to combat the attack.

Also key to Citi's cybersecurity strategy is three main components: talent, teamwork, and technology, Harrington said, pointing to talent as the most critical part of the equation. A company needs strong talent standing on its side thwart the attacks of equally strong talent that is launching the attacks, he said.

"There's a real fight for talent in this space," he added, noting the small pool of highly skilled cybersecurity professionals.

Recognizing the need for such skillsets, the Singapore government earlier this year unveiled its third cybersecurity roadmapwhich focuses on protecting critical infrastructure as well grooming homegrown talent.
In his speech, Masagos highlighted the need to build a "sustainable national ecosystem", including efforts to work with academic institutions and industry players to boost the country's cybersecurity talent pool with the necessary training. The new partnership with Temasek Polytechnic is part of the government's continuing efforts to nurture the next-generation of cybersecurity experts, he said, pointing to a similar partnership SITSA inked last year with the Singapore Management University.
The government today also announced a new interactive game, called CyberShock, that is part of a running campaign to raise public awareness that national security extends beyond terrorism and encompasses cybersecurity. The game simulates the effects of a cyberattack on five essential services such as power and public transport, and participants play their part in helping to defend against these attacks, Masagos explained.

The government also supports global efforts to exchange ideas and collaborate on research to address new threats, he added. Such efforts include the setting up of Interpol's digital crime center here, scheduled to begin operations next year, to support cybercrime investigations as well as research and development to beef up international policing.