Hackers expose Asia's weak cyber defences

SINGAPORE - A rash of website hackings in the Asia-Pacific has exposed weak cyber defences, which must be improved to help the region deal with more sophisticated and sinister threats, particularly from criminal organisations, analysts said.

Growing threat of cybercrime in Asia Pacific region.
Image: Information Security Buzz

Hackers claiming to be from the global activist group Anonymous compromised several government and commercial websites in Australia, the Philippines and Singapore recently, and vowed to mount wider attacks.

In the latest incident, Anonymous hackers hijacked a section of Singapore Prime Minister Lee Hsien Loong's official website, just a day after he vowed to "spare no effort" in hunting down anyone who attacks the regional financial centre's technological network.

"Cloud computing, the proliferation of mobile devices and the increasing use of social media have allowed an escalating volume of data to flow through multiple channels, giving hackers a wider field to ply their trade," analysts said.

They warned that Anonymous, which carries out attacks to highlight issues such as Internet freedom and corruption, is just one of the groups involved, and others with a more sinister agenda could inflict serious damage.

Large criminal organisations involved

"The more sophisticated group that government and business should fear are the cyber-criminal organisations, which have much greater resources at their disposal," said Tan Shong Ye, information technology risk and cyber security leader at global business consultancy PricewaterhouseCoopers (PwC).

"Their targets could be valuable intellectual property and critical infrastructure, including military and state secrets," Tan

said.

Shadowy hackers who have long targeted the West are turning their sights on Asia's fast-growing economies.

"As countries become wealthier, they have more assets and therefore are more likely to become targets," said Nina Laven, director for economics and country risk at consultancy group IHS. "We will likely see the region attracting more attacks," she said.

"South-east Asia and the wider Asia Pacific region are growing in significance in terms of cybersecurity issues as Internet usage becomes more pervasive," said Caitriona H. Heinl, a cyber security specialist at the S. Rajaratnam School of International Studies (RSIS) in Singapore.

Cross-border crimes

"These increasing levels of connectivity are raising the probabilities of cross-border cyber-related threats such as transnational cybercrime," she said.

Research firm Euromonitor said there were more than 389m smartphones and nearly 30m tablets and other portable computers in the Asia Pacific. It said mobile Internet subscriptions reached over 712m.

"While information security risks have evolved, security strategies have not kept pace," PwC said in its Global State of Information Security Survey released in September.

"In other words, most organisations are now defending yesterday while their adversaries are looking to exploit the vulnerabilities of tomorrow," Tan said.

"Most Asian countries have implemented some level of cybersecurity protection by having computer emergency response teams to deal with online attacks," Tan said.

He warned, however, that more needs to be done in the form of investments as well as attention, adding that PwC's survey showed that the number of security incidents detected worldwide in the past 12 months rose by 25% and average losses climbed 18% compared with the previous year.

Security issues not taken seriously

"Asian businesses in general are still not investing enough in cyber security," Tan said. He pointed out that companies only invest after they encounter a serious attack.

"China, the world's second biggest economy, and Russia are making solid progress in deploying cybersecurity safeguards while India is playing catch-up," Tan added.

"China's Internet infrastructure is more heavily guarded than others, thanks to the state's role in the 'Big firewall' of China," he said.

Laven of IHS stressed that international co-operation is key to fighting cyber attacks.

"Cybersecurity is a cross-border issue. Governments can invest in prediction, detection and recovery, but a lack of alignment between countries leads to security weaknesses that no one government can address," she said.

"Criminal groups could attack well-protected countries from overseas locations where there are weaker cyber safeguards," Laven said.

"Until governments can find ways to work together on preventing cyber crime, through penalties, incentives, or funding technical solutions that can be deployed across borders, international attackers will always be able to find weaknesses to exploit," she said.

Heinl of RSIS said that so far, national and regional efforts to adopt comprehensive cybersecurity strategies have been slow and fragmented.

Source: AFP via I-Net Bridge