Online Security Breaches

Sherman Tan

09 Jul 2011

Recent security breaches

Since Mar this year, we have witnessed several major cyberattacks on a number of commercial companies ("Security Compromised" dated 08 May 2011 by this author) but in recent months, the targets appeared to have shifted to government or government related websites including South Korea's presidential Blue House, the Turkish government official websites, the Spanish national Police website, Arizona Police website, the International Monetary Fund website in Jun last month. In response to the Malaysia's government move to block filesharing sites in Malaysia, the group, which called itself Anonymous, launched an attack codename "Operation Malaysia" on 16 Jun 2011 bringing down 41 government websites after it issued an early warning of its intention.

Besides government websites, banks were also not spared. For instance, in Apr 2011, Nonghyup, a large commercial bank in South Korea suffered a massive network failure that affected millions of bank users for more than a week when the bank's ATM network, credit authorization and electronic transfers were disabled. Citigroup also announced that computer hackers have breached the bank's network on 10 Jun 2011 and accessed data of some 200,000 bank card holders including names of customers, account number and contact information which contained email addresses.

Singapore banks making preparations

As banks around the world prepare themselves against such cyberattacks, major banks in Singapore are also doing likewise. At Singapore's DBS, besides putting up several layers of security to protect its customers, it was also the first and only bank in Singapore to offer a Money Safe guarantee to protect customers from unauthorized online transactions conducted via both internet and mobile channels. UOB on the other hand was reported recently to say that the bank would engage actively in assessing new technologies.

Mr Andrew Wong, head of information security at OCBC said that the bank would continue to strengthen its strategy to guard against evolving security threats. Besides these measures, sources familiar with the banking industry shared that the central bank is in the midst of issuing guidelines for banks to implement transaction signing for some of the critical online banking transactions sometime next year. In the meantime, security trading companies in Singapore have begun offering two-factor trading for their customers. For instance, DBS informed its customers that DBS Vickers Online will be implementing two-factor authentication from 1 Aug 2011 for trading transactions that are executed via DBS internet banking platform.

eGovernment Plan

As banks are fortifying their security measures, the Singapore government announced the opening of the Gov Global Exchange 2011 late last month. At the event unveiled by Deputy Prime Minister Teo Chee Hean, the government will invest about S$2 Billion to implement eGov2015. The plan calls for the government to use business analytics, which studies huge amount of data to identify trends that will help in decision making as well as social media and mobile services to engage citizens and businesses. As part of this plan, the government will be calling for a tender in the coming months for its private cloud, Central G-Cloud which is expected to be ready by the end of next year.

Part of the plan is to enhance the eCitizen Portal which is now 11 years old and offer 1,600 e-government related services.

The current eCitizen Portal provides a number of e-government services to both individuals and businesses. For instance, companies can make monthly Central Provident Fund (CPF) contributions for both employees and employers via the internet or through mobile phone applications. While the actual payment transactions are carried out via secured payment channels such as GIRO or MEPS; submission of staff salaries, CPF deductions are done via a single-factor authentication method; SingPass. Using this same SingPass, citizens can assess a host of government services including application for junior college, university studies, renewal of passport, etc. While there are counter-measures to prevent fraud; e.g. online passport renewal requires the applicant to present himself/herself in person to collect the passport, confidential information such as CPF contribution history, balances, email address, identification number, date of birth, etc could be exposed in the event the single-factor SingPass is compromised.

Besides enhancing the eCitizen portal, the eGov2015 plans to provide an e-mail inbox (OneInBox) for Singaporeans, permanent residents, employment pass holders and business owners who need to correspond with government agencies such as the HDB, CPF, Inland Revenue and Ministry of Manpower by next year. As such electronic mail box would contain some confidential information just by looking at the types of government agencies that are involved; a single-factor authentication is insufficient.

Assurity Trusted Solution Pte Ltd, the wholly owned subsidy of the Infocomm Development Authority of Singapore (IDA) which was set up in early this year with the charter to offer a super-token solution for second factor authentication would likely be part of the overall eGovernment game plan to bring the single-factor authentication to the next level.

Looking at the various online security breaches that have occurred as recent as Mar this year, user authentication is only one aspect of protecting consumer's confidential data. Denial of services attacks leading to disruption or non-available of critical data or services such as non-access to medical records, inability to make urgent payment services; delay in registration or submission of time-bound contractual obligations; etc could lead to major implications for various eGovernment services.

As the Singapore government plans to join the cloud computing bandwagon as part of its eGov2015 master plan, lowering the cost of buying computer resources should not be the only key consideration.

The writer is the Principal Consultant & Director at Innovar Pte Ltd (www.innovar.com.sg). He can be contacted at office@innovar.com.sg.