Tan Kin Lian, 9A Cactus Crescent, Singapore 809744
kinlian@gmail.com Mobile: 81685845

17 September 2018

Hacking of SingHealth Database

1. Introduction

My name is Tan Kin Lian. I wish to submit my views to the Commission of Inquiry into the hacking of the SingHealth database.

I worked as a programmer for three years during the period 1969 to 1972. While I headed NTUC Income from 1977 to 2007, I was actively involved in the oversight of the computer system used in that organization.

From 2008 to now, I managed a company involved in developing computer software. I am familiar with database systems and with the issues involved in retrieving data from databases.

I wish to give my views from the perspective of a person who sees the issue from a management angle and with a good working knowledge of database and security of access to the database

2 Hacking

The computer experts will identify various kinds of hacking that can occur and the different layers of the architecture that can be attacked. I do not wish to enter into the realm of these experts.

I read, from the information that is given to the public, that the hacking involved the unauthorised retrieval of 1.5 million patient records (but not the entire database) and the access to the visit records of certain VIPs.

It appears to me that the hacking concerns the access of the database and is not involved in other security issues.

3. Types of users

In accessing a database, the architect creates several roles and assigns certain functions to each role. For the purpose of simplifying the issue, I suggest that there are three user types:

a) Database administrator

b) Staff user

c) Doctor user

Each user is assigned to a certain type, and accesses the database using their credentials.

4. Nature of the hack

I read a report that the hacker was able to get the user credential from a front end workstation. I expect that this was a staff user who has access to the details of patients who visit the clinics on a selected day.

As there are a few dozen staff users and a few hundred doctor users, it would be impossible to prevent the credentials from being stolen.

Apart from using hacking to steal the credentials, the crook can bribe a user to release its credentials.

We have to prepare for the risk that the credentials will be stolen or sold, and to be able to respond when there is a large scale retrieval of the data.

5 How it might have happened

This is based on my speculation.

I suspect that the hacker was able to get the credential of a staff user who has access to the details of patients who make visits on a selected day.

With this credential, the hacker was able to access the details of patients who visited the records on a selected day. By doing the enquiry repeatedly, the hacker was able to retrieve the records of all the patients who visited the hospitals over the three year period.

I do not think that the hacker obtained the credentials of the database administrator as it would allow the hacker to download the entire database.

5. Audit trail of enquiry

Most database software automatically records changes to the database, i.e. when a record is added, deleted or changed.

In addition to this logging at the database software level, I suggest that the application system should also write a log of all enquiries that were made. I will refer to them as audit records and the process as an audit trail. The audit records could include the following:

a) The user ID who access a specific patient record and the timestamp

b) The user ID who access a certain page of information, such as all patients who visited the hospital on a specific date and the timestamp.

There should also be a daily analysis of the audit records to identify abnormal behaviour, e.g. a doctor user who makes more than 50 patient enquiries in a day, or a staff user who access more than 10 pages of patient visits in a day.

The abnormal access can be highlighted for the auditor to follow up and verify that the enquiries were legitimate.

This audit records can also be examined to identify access to the patient records of sensitive persons, such as VIPs.

It can identify the users who access these sensitive records so that the auditor can verify that the accesses are legitimate.

If this daily audit analysis was in place, the breach would have been detected at an early date, before so many patient records are retrieved.

6. Restrict access through the internet

I read that steps are now being taken to restrict access through the internet.

This is a useful step, but it does not totally control the risk. It is possible for the hacker to get access to an approved location and carry out the retrieval of data from that location.

The drawback is that many doctor users are not able to get access to the information that they need to carry out their work.

The audit trail would be a more comprehensive and better approach towards handling this risk.

7. Conclusion

I have speculated on how the hacking could have happened, based on the information that is published in the media. I might be wrong on this speculation.

Nevertheless, I hope that the system of audit trail be implemented as it is a desirable measure.

I hope that my suggestions are useful to the Commission of Inquiry.

Thank you.

Tan Kin Lian
9A Cactus Crescent, Singapore 809744
kinlian@gmail.com
Mobile: 81685845