Access Control Security

Access Control Security

Access control security is a mechanism that identifies the users of a computer system. It also verifies the users' access rights within the system, prevents intrusion made by unauthorised users and to ensure confidentiality, integrity and availability of the information handled by the system.

Data Access Right

Data access rights should be granted to users based on a "need-to-know" basis.

Logical Access Control

Logical access control is a security measure applying the AAA principle, i.e. Authentication, Authorisation and Accounting to ensure that information will not fall into the hands of improper users.

Authentication

The strength of an authentication system depends on the different security requirements of computer systems. Different methods may be used to authenticate users, such as password, digital certificate, etc. The purpose is to verify logon users' identities and record audit trails for auditing purpose.

Limiting the allowed number of failed logon attempts and lengthening the user account lockout time after repeated failed logon can minimise the risk of brute force attack by intruders who try password combinations for system logon.

Password Management

Password is one of the key components for logging on a computer system, so it is important to keep the password properly and not to disclose it to other people easily. Passwords should be encrypted when held in storage or transmitted over a network. Generally, the rule of thumb for setting a password is “difficult to guess but easy to remember”, for example, “1+Tw0Eq3”. Do not use a password that can be found directly from the dictionary. Change password regularly. An password policy can enhance the strength of password and make it difficult to crack.

Accounting

Accounting refers to the use of audit trails to record the events of daily operations of computer systems. System monitoring personnel or programs can then audit and review for any abnormal events happened. Nowadays, most application systems have included audit trail feature.

As the size of daily track records of computer systems can be enormous, the audit trail feature should be set to focus on recording abnormal system events for accounting purpose. Otherwise, the daily audit trails may take up most of the system resources and make it harder to identify abnormal system events.

The audit records should be accurate for use by auditors in regular review. Integrity is very important in accounting. Any incomplete records or improper behaviours discovered should be reported at once, followed by an investigation.

To learn more about information security, please visit the InfoSec website at:
http://www.infosec.gov.hk