Network and Communication Security (I)

Network and Communication Security (I)

Network and communication security mainly prevents damages and disturbances caused by malicious intrusion to a computer network. The aim is to protect information on the network.

Related security measures generally include Network Security Control, Internet Security, Email Security, Wireless Network Security, and Preventive Measure of Network Communication, etc.

Network Security Control

Network Security Control usually includes a few basic security measures such as Intrusion Prevention System (IPS), firewall and anti-virus software, etc.

When an intranet needs to be connected to any external network, the use of firewall or intrusion prevention system should be considered in order to monitor the data traffic, detect and prevent any improper action in the network.

If any attacking activity is detected, the prevention system should immediately trigger alerts and relevant protective responses to reduce harmful impacts on the network service.

Firewall is an individual system or a set of systems that implements control policy for data flow, separates internal and external networks, allows or denies data flow between networks, and prevents unauthorised access to the internal information system by outsiders.

Special caution should be exercised to protect sensitive information. Sensitive information must be encrypted before transmission. Appropriate security measures such as Secure Sockets Layer (SSL) or Virtual Private Network (VPN) should also be implemented.

Mutual authentication is required for communication between networks or computers.

Internet Security

Users should comply with the organisation’s established rules or related guidelines on proper use of Internet services. For example:

- Computer browsers should be configured properly to prevent malicious codes such as computer viruses from being downloaded to the computer.
- Avoid saving passwords by using password auto-complete / password remembering features of web pages.
- Do not browse or download any files from suspicious websites.
- Instant messaging or online chat room on the Internet must be used with caution in order to avoid computer virus invasion through these channels.

Email Security

Use email spam filtering software and anti-virus software to filter suspicious emails or emails containing computer viruses. Additional features such as authentication, encryption and digital signature can also be considered.

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