Content Filtering

Content filtering in general refers to the filtering of inappropriate content or messages, such as content containing objectionable materials, personal or sensitive information. In terms of information security, content filtering has different applications, for example, in browsing the Internet, receiving emails, generating search results with online search engines, accessing database, etc.

Use of Content Filtering

Using content filtering software, parents can compile and update a list of harmful websites to filter out websites containing content not suitable for children and teenagers. They can also set time limits for surfing the Internet. This can prevent children from browsing inappropriate online content or indulging in online activities.

Organisations can also use content filtering software to prevent staff from abusing resources, for example, downloading files in bulk from the Internet or browsing harmful websites. These activities consume bandwidth and waste resources.

Internet users can choose to take the security measures provided by Internet service providers. For example, they may use email filtering service to reduce the number of spam emails received.

If an organisation has its own email server, a content filtering system can be installed to filter spam and virus-infected emails before they are delivered to the inbox of individual staff. The content filtering system can also screen outgoing emails to check whether they contain sensitive data before sending them out via the Internet. This can reduce the risk of leaking sensitive information.

Operation of Content Filtering

Content filtering works in a number of ways. Following is a brief introduction to the different approaches, taking web page content filtering as an example.

1. Allow users to browse only websites on the White List. The White List is a database of approved websites. The Internet browser will first verify whether a website is on the White List before allowing it to be browsed by the user.

2. Prevent users from browsing websites on the Black List. These websites usually contain harmful information and are not suitable for browsing.

3. Some content filtering tools come with a database on categorisation of web pages. This database is periodically reviewed and updated by the supplier. It helps determine whether a web page is suitable for viewing by categorising and scoring the web content against pre-defined criteria.

4. Some tools combine different content filtering methods mentioned above to enhance accuracy and efficiency.

Other Corresponding Best Practices

Though content filtering provides certain protection, parents or organisations also have a role to play. Parents can spend more time with their children in browsing the Internet and teach them to behave online. Organisations should provide staff with regular training on information security to increase their awareness of data protection.

To learn more about information security, please visit the InfoSec website at:

http://www.infosec.gov.hk