Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

Elak diceroboh

KADANGKALA, persiapan peralatan keselamatan siber seperti tembok api dan lain-lain sudah ada tetapi masih berlaku pencerobohan keselamatan. Bolehkah dikongsi perkara yang menyebabkan perkara ini berlaku?
-Din, KL.

Seperti yang dibincangkan sebelum ini, aspek keselamatan siber merangkumi dan perlu berfungsi dalam tiga aspek atau 3P iaitu pendidikan, polisi dan *parameter* keselamatan. *Parameter* dan peralatan keselamatan siber ini adalah benteng terakhir pertahanan keselamatan siber. Dalam kes perbankan Internet tersebut, pihak bank hanya mempromosi penggunaan perbankan Internet tetapi tidak mendidik pemilik akaunnya menggunakan perkhidmatan perbankan Internet secara betul dan selamat. Seterusnya dibincangkan secara khusus antara masalah-masalah berlaku dalam *parameter* keselamatan siber ini.

1 Penggunaan perisian antivirus tidak dikemas kini atau tidak berupaya mengesani serangan virus atau *Malware* yang baharu. Boleh menggunakan lebih daripada satu perisian antivirus yang diyakini kebolehannya atau menggunakan aplikasi web *virustotal.com* yang meliputi hampir kesemua enjin carian virus atau *Malware*.

2 Perisian tembok api yang digunakan mempunyai tahap perlindungan keselamatan yang sangat minimum. Lihat dan fahami spesifikasi perisian tembok api yang digunakan dan fahami juga situasi rangkaian sesebuah organisasi. Konfigur perisian tembok api itu sesuai dengan kehendak keselamatan siber sesebuah organisasi. Sekiranya perlu, tukar kepada perisian yang lebih cekap.

3 Pengurusan tempelan perisian atau *patching* perlu dilakukan secara menyeluruh, terancang dan terkini. Pastikan jenis aplikasi dan sistem pengoperasian yang digunakan dalam organisasi dan sediakan kemudahan untuk membuat tempelan kepada setiapnya.

4 Penggunaan kata laluan yang mudah diceroboh dan dimanipulasikan oleh penggodam. Perlu ada polisi dan pendidikan kepada para pengguna berkenaan dengan penggunakan kata laluan yang selamat. Boleh menggunakan aplikasi pengesahan identiti yang lain jika perlu seperti biometrik, pengesahan dua faktor dan sebagainya.

5 Perisian IDS (*Intrusion Detection System*) tidak berupaya mengesani kandungan sesuatu fail sekiranya terdapat *Malware* dan sebagainya. Sama seperti perisian tembok api iaitu perlu dikonfigur dengan betul dan lengkap sesuai dengan prasarana rangkaian komputer yang ada.

6 Penggunaan teknik enkripsi dalam rangkaian telah berjaya dirungkaikan oleh pihak penceroboh. Oleh itu, pengurusan penggunaan teknik enkripsi ini perlu dilakukan dengan pelbagai jenis, terurus dan meliputi pelbagai teknik yang kental dan terkini.

7 Pendidikan keselamatan siber sangat perlu dan perlu pastikan ia berkesan mempengaruhi sesiapa terlibat menggunakan perkhidmatan teknologi maklumat dengan betul dan selamat.