Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

Bendung masalah *malware* e-mel

KEBANYAKAN virus atau *malware* disebarkan menerusi pembukaan e-mel. Apakah langkah-langkah keselamatan yang boleh diambil untuk membendung masalah ini?

- Abdullah, Bera.

E-mel merupakan satu alat komunikasi atau perantara digital yang banyak diguna pakai oleh pengguna Internet pada hari ini.

Selain digunakan sebagai alat komunikasi, kebanyakan dokumen penting akan dihantar menerusi medium ini terutama dalam sesebuah organisasi. Dokumen ini dihantar memenerusi sisipan fail bersama mesej yang hantar dalam bentuk pelbagai format seperti format gambar, PDF, teks, Excel dan Word.

Jadi, sifat perkhidmatan e-mel ini yang berupaya menembusi pengguna akhir dan agak sukar untuk perimeter keselamatan seperti perisian antivirus dan tembok api untuk mengesan kandungannya, menjadikan ia popular digunakan sebagai medium oleh pihak tidak bertanggungjawab untuk melakukan jenayah siber atau pencerobohan.

Teknik ancaman yang digunakan menerusi perkhidmatan e-mel adalah seperti sisipan fail, sambungan URL (*Uniform Resource Locator*) yang tidak selamat dan menerusi teknik-teknik penyamaran lain bagi pihak yang dipercayai oleh pengguna

Teknik penyamaran ini juga dikenali sebagai serangan *Phising* atau *E-mail Spoofing*.

Seterusnya, dibincangkan beberapa tindakan yang boleh diambil oleh individu atau organisasi dalam mengendalikan penggunaan e-mel ini dengan selamat.

1 Perlu disebarkan dan diajar ilmu mengendalikan penggunaan e-mel dengan betul dan selamat kepada pengguna e-mel menerusi kelas, poster, polisi dan panduan-panduan.

2 Bagi sesebuah organisasi, wujudkan polisi keselamatan khusus untuk penggunaan e-mel dalam organisasi termasuk alatan elektronik peribadi atau mudah alih yang digunakan atau budaya BYOD (*Bring Your Own Device*).

3 Penggunaan perisian keselamatan atau anti-*Malware* khusus untuk perkhidmatan e-mel dalam menapis kesalamatan sehingga kepada kandungan dan fail yang yang terdapat dalam sesebuah mesej e-mel.

4 Penggunaan perimeter keselamatan yang bersepadu antara perisian anti-*Malware*, tembok api dan lain-lain penting dalam menangani penyebaran *Malware* dalam sesebuah organisasi. Elakkan daripada pergantungan hanya pada sejenis parameter keselamatan sahaja.

5 Bagi sesebuah jabatan yang kritikal, boleh ditetapkan fail berformat tertentu dan fungsi fail tertentu yang perlu dikendalikan oleh pengguna atau staf tertentu sahaja dibenarkan.

6 Dokumen atau fail yang hendak disebarkan atau dikongsikan menerusi rangkaian komputer bagi sesebuah organisasi perlu disahtentukan terlebih dahulu oleh pihak bertanggungjawab sebelum disebarkan.