Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

Serangan *ransomeware*

APAKAH yang dikatakan dengan serangan *Ransomware* ini? - HAMBA ALLAH.

PADA masa ini, menjadi berita utama dunia berkenaan dengan serangan *Ransomeware* yang dikenali sebagai *WannaCry* atau *WannaCrypt* ke atas dunia siber termasuk negara-negara dan syarikat-syarikat gergasi dunia.

Dijangkakan oleh pakar keselamatan siber, gelombang serangan *Ransomware* jenis ini akan muncul kembali dalam masa terdekat.

Ransomware merupakan sejenis *Malware* atau perisian jahat yang akan mengunci sistem komputer mangsa yang dijangkiti dengan teknik enkripsi. Jadi, bagi membolehkan komputer mangsa digunakan semula, ia perlu dinyahenkripkan.

Untuk itu, si mangsa diperas ugut untuk membayar sejumlah nilai wang bagi mendapat kunci digital untuk menyahenkripkan komputer tersebut.

Penguncian sistem komputer melibatkan bahagian *Master Boot Record* (MBR) yang menyebabkan keseluruhan cakera keras terkunci dan terjejas.

Kebiasaannya, modus operandi penyebaran dan jangkitan serangan *Ransomware* ini adalah menerusi sisipan fail atau sambungan URL menerusi e-mel kepada pengguna akhir.

Apabila pengguna tersebut mengklik sisipan fail atau sambungan URL, serangan *Ransomware* ini akan berlaku.

Serangan *Ransomware* ini amat berkesan ke atas sistem komputer yang tidak dikemas kini terutama bagi sistem pengoperasian dan perisian keselamatan.

Seterusnya dibincangkan beberapa tindakan yang perlu diambil bagi mengurangkan berlakunya masalah serangan *Ransomware* ini dan kesannya.

1 Didik para pengguna yang terlibat dalam organisasi dengan penggunaan perkhidmatan teknologi maklumat seperti e-mel, pelayar web dan lain-lain dengan betul, selamat dan bertanggungjawab.

2 Sentiasa mengemas kini perisian yang digunakan terutama bagi sistem pengoperasian dan perisian keselamatan.

3 Pastikan aplikasi komputer yang digunakan boleh dipercayai dan selamat. Begitu juga tempat dapatannya boleh dipercayai.

4 Nyahaktifkan fungsi *macros* dalam perisian Microsoft Office, pastikan dinyatakan sambungan format yang yang tersembunyi dan dinyahaktifkan program *Remote Desktop Protocol*. Perkara ini boleh disetkan kepada setiap komputer menggunakan program *Local Group Policy Editor* atau *gpedit.msc* seperti terdapat dalam sistem Windows.

5 Sekiranya disedari terkena serangan ini, dengan segera putuskan segala sambungan rangkaian dan Internet bagi komputer tersebut.

6 Pastikan dibuat salinan pendua atau *back up* bagi sistem dan data yang penting.