Cabaran keselamatan siber 2016

APAKAH isu, cabaran dan ancaman dalam keselamatan siber pada tahun 2016 ini? -ARIFIN, Bohor.

BENTUK ancaman dan cabaran dalam keselamatan siber pada setiap masa akan mengikut kepada perkembangan terkini teknologi dalam teknologi maklumat dan tujuan kehendak manusia yang terlibat dalam serangan tersebut.

Sebagai contoh tujuan serangan pada masa lampau lebih bersifat untuk memusnahkan data atau sumber dalam dunia siber. Namun sejak semenjak mutakhir ini, serangan siber lebih kepada pencurian maklumat secara rahsia tanpa berlakunya pemusnahan. Begitu juga dengan perkembangan teknologi maya membolehkan serangan dibuat menerusi penggunaan ruang memori RAM seperti mana timbulnya masalah kelemahan seperti isu keselamatan *Heartbleed*.

Seterusnya dibincangkan beberapa isu, cabaran dan ancaman dalam keselamatan siber yang akan berkembang pada tahun 2016 ini berdasarkan kepada pemerhatian kepada berita, perkembangan teknologi dan laporan oleh pihak yang berautoriti.

1 Gaya serangan siber seperti *Ransomware* yang akan mengunci apa-apa sistem atau aplikasi yang diserang akan menjadi lebih popular. Seterusnya penggodam akan meminta tebusan sejumlah wang untuk membolehkan sistem atau aplikasi itu beroperasi secara normal semula.

2 Penggunaan banyak peralatan dalam capaian Internet menggunakan teknologi *Internet of things* (IoT) akan mendedahkan banyak bentuk serangan siber terhadapnya. Begitu juga perkembangan teknologi analitikal dalam data raya akan dipergunakan untuk tujuan jenayah siber.

3 Peningkatan kaedah serangan siber yang menggunakan pelantar orang lain untuk menyerang sesiapa sahaja dalam alam siber. Penggodam akan cuba masuk dalam sesebuah organisasi yang mempunyai sumber pengkomputeran yang banyak dan menggunakan segala kemudahan yang terdapat untuk membuat serangan kepada pihak yang lain.

4 Teknologi dan model kepercayaan dalam sistem pengkomputeran akan berkembangan naik bagi mengatasi masalah yang terhasil daripada serangan dan jenayah siber ini.

5 Risiko keselamatan siber dalam sesebuah organisasi perlu dibuat analisis terperinci untuk mengelakkan dipergunakan untuk tujuan jenayah siber.

6 Kaedah, teknologi dan metodologi pertahanan keselamatan siber yang lebih bersifat proaktif, analitikal dan automasi perlu dipertingkatkan dengan lebih baik.

7 Polisi, akta dan undang-undang keselamatan siber akan berkembang dengan lebih baik lagi bagi menuntut pada jenayah atau serangan siber yang lebih spesifik dan tuntas.