Persediaan ancaman Keselamatan Siber 2018

Tutorial ICT

Bersama **FIRKHAN**
firkhan.uthm@yahoo.com

PADA tahun lepas, ancaman keselamatan siber diserang di serata dunia oleh sejenis *malware* yang dikenali sebagai *Ransomware* dalam pelbagai jenis seperti *WannaCry* dan *NotPetya*. Seperti biasa ancaman keselamatan siber ini akan semakin canggih dan licik seiring dengan perkembangan teknologi siber semasa. Begitu juga dengan ancamam kecurian data yang melibatkan syarikat-syarikat dengan anggaran kerugian mencecah ratusan jutaan Ringgit.

Pada tahun ini, ancaman keselamatan siber seakan-akan sama seperti tahun lepas. Oleh itu, setiap organisasi dan individu perlu persediaan yang mencegah berlakunya ancaman keselamatan siber.

Oleh itu, beberapa teknologi keselamatan siber yang diperkenal penggunaannya secara meluas pada tahun lepas perlu diberi perhatian. Antaranya adalah seperti yang dibincangkan di bawah ini.

1 Keselamatan Kepercayaan Sifar atau *Zero Trust Security* (ZTS) untuk mencapai kebenaran masuk ke dalam akaun bagi sesebuah sistem komputer. Perkara ini diamalkan bagi memudahkan pengguna mencapai akaun sendiri ke dalam mana-mana sistem komputer. Namun begitu, ia boleh menjadi ancamam keselamatan siber sekiranya tidak diuruskan dengan baik. Oleh itu, beberapa protokol dan strategi keselamatan perlu ditingkatkan seperti keselamatan pengesahan identiti pengguna, set data yang spesifik, penggunaan status kelayakan banyak lapisan dan lain-lain.

2 Penggunaan kepintaran buatan (AI), pembelajaran mesin dan analisis kelakuan dalam tawaran penyelesaian keselamatan siber. Kebanyakan serangan siber berlaku secara tidak terus dengan manipulasi data, penyamaran dan kejuruteraan sosial secara teknikal, licik dan canggih. Oleh itu, keperluan kecerdasan buatan, pembelajaran mesin dan analisis kelakuan penting dalam menangani masalah-masalah tersebut.

Ia bukan sahaja berupaya mengesan dan bertindak ke atas ancaman tersebut tetapi berupaya membuat andaian dan jangkaan tindakan terhadap serangan siber yang berkemungkinan akan berlaku.

3 Sedia melengkapkan setiap kesemua prasarana teknologi maklumat (IT) dengan aspek keselamatan yang lebih ampuh. Penggunaan protokol keselamatan yang sentiasa dikemas kini perlu menjadi keutamaan bagi setiap prasarana IT yang ada. Kelemahan sistem dan keintegritian data boleh menjadi ancaman keselamatan utama pada prasarana teknologi maklumat. Begitu juga dengan penggunaan teknologi penyamaran daripada serangan seperti teknologi *Honey Net*.

4 Teknologi *Blockchain* mendepani ruang lingkup yang baru bagi keselamatan siber. Teknologi keselamatan transaksi kewangan digital ini boleh digunakan untuk menguatkan lagi enkripsi keselamatan siber terutama dalam dapatan kepercayaan untuk sistem pengesahan masuk akaun pengguna ke dalam sesuatu sistem terutama yang menggunakan kaedah ZTS.

Ancaman keselamatan siber berlaku berkadar kepada penggunaa teknologi baharu dalam komputer dan IT.

Justeru, persediaan yang rapi dan kental sangat diperlukan untuk pertahanan keselamatan siber bagi sesebuah organisasi atau individu untuk menghadapi ancaman daripada dalam atau luar.