Ancaman serangan kejuruteraan

BAGAIMANAKAH serangan kejuruteraan sosial memberi ancaman kepada keselamatan siber?
FAUZI, Kluang.

Terima kasih. Kejuruteraan sosial atau *social engineering* merupakan satu amalan penyamaran dan penipuan terhadap seseorang berkepentingan sehingga individu tersebut membuat sesuatu yang tidak sepatutnya dengan menggunakan cara tidak teknikal. Sasaran mangsa itu dihubungi

Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

untuk mendapatkan sesuatu maklumat berguna bagi tujuan pencerobohan siber ke atas sesebuah organisasi seperti kata laluan, maklumat rangkaian, akaun talian Internet dan sebagainya.

Sebelum serangan dibuat, penceroboh akan membuat kajian terperinci berkenaan maklumat mana-mana individu berkaitan bagi sesebuah organisasi yang hendak diceroboh. Maklumat ini boleh diperolehi menerusi Internet, media sosial, *Dark Web* atau dibeli di pasaran gelap

Seterusnya, penceroboh akan menggunakan maklumat yang diperolehi untuk mendapat kepercayaan dan mempengaruhi individu sasaran tersebut. Seperti mana proses penyamaran fizikal yang sering ditonton dalam filem aksi seperti dalam cerita *Mission Impossible*.

Terdapat tiga jenis taktik yang digunakan dalam serangan kejuruteraan sosial ini iaitu sama ada secara bertemu secara fizikal, menerusi telefon atau menerusi medium digital seperti laman web, media sosial dan e-mel. Serangan kejuruteraan sosial menerusi medium digital banyak penipuan dibuat menerusi satu taktik yang dikenali sebagai *Phising* sama ada menerusi web, media sosial atau e-mel.

Terdapat beberapa amalan yang boleh dipraktikan untuk menghindari daripada berlakunya serangan kejuruteraan sosial ini.

1 Bangunkan kumpulan yang akan menangani masalah keselamatan siber dalam organisasi yang dikenali sebagai *Incident Response Team*.

2 Penggunaan kaedah enkripsi menyeluruh dalam persekitaran digital organisasi.

3 Elemen serangan ini mesti dimasukkan ke dalam pengurusan kesinambungan perniagaan atau *Business Continuity Management* (BCM) dalam organisasi.

4 Latihan dan pendidikan kepada para perkerja pada semua peringkat dalam menangani ancaman keselamatan siber.

5 Keterlibatan sama oleh pihak pengurusan peringkat pertengahan dan tinggi dalam menangani isu ancaman serangan kejuruteraan sosial ini.

6 Sekiranya perlu, disediakan insurans perlindungan kerana kesan serangan ini kadangkala melibatkan kerugian sehingga nilaian jutaan ringgit.