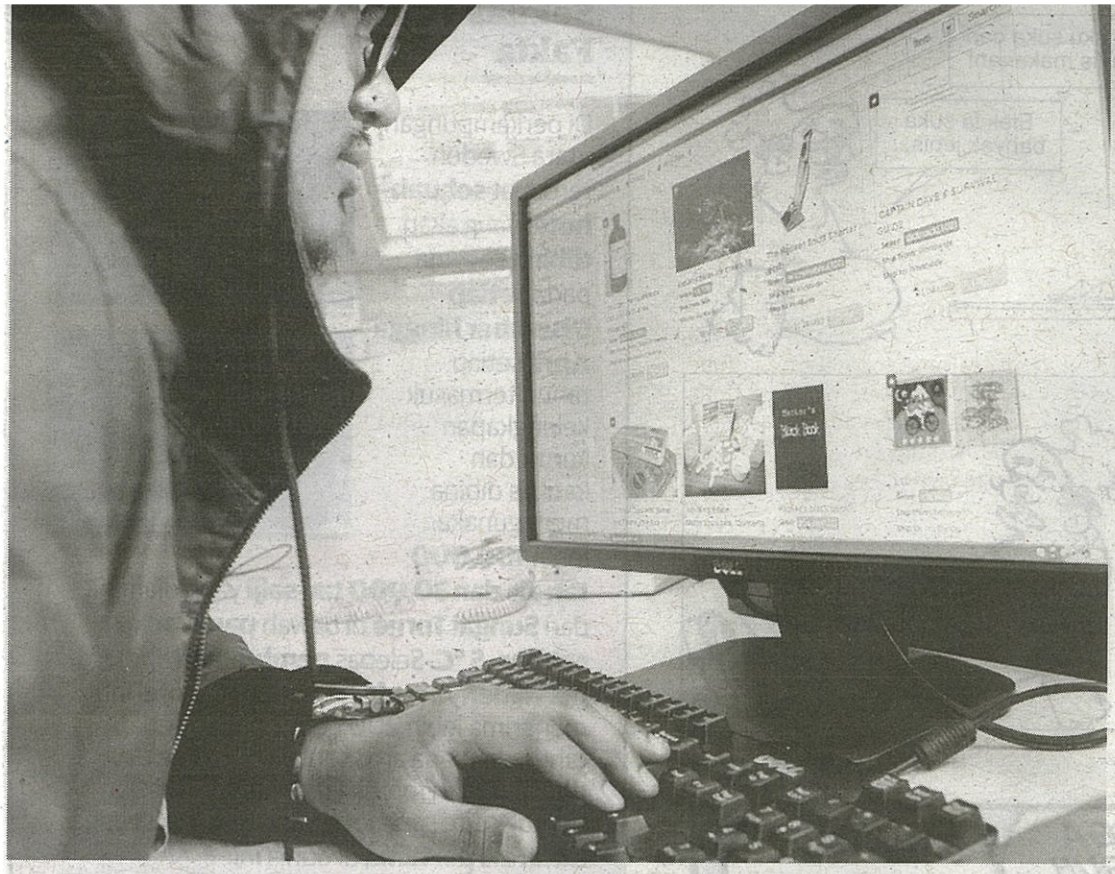

SERANGAN Penafian Perkhidmatan Teragih (DDoS) dilakukan oleh penggodam atau penyerang menggunakan beberapa peranti seperti telefon pintar dan komputer peribadi serta sambungan internet untuk menyesakkan kestabilan sebuah pelayan.

Bagaimana mahu kurangkan serangan DDoS?

SAUDARA PENGARANG,

KEBANYAKAN masyarakat adalah pengguna internet. Tetapi adakah anda sedar internet mempunyai ancaman yang dicipta oleh penggodam atau penyerang alam siber seperti Penafian Perkhidmatan Teragih (DDoS).

DDoS adalah sejenis serangan terhadap rangkaian komputer. Ia terjadi disebabkan sistem rangkaian komputer sesebuah organisasi atau syarikat dijangkiti Trojan. Secara tidak langsung, ia boleh mengganggu pengguna internet untuk mencapai sebuah sistem walaupun mereka adalah pengguna yang berdaftar dalam sistem itu.

Pengguna internet termasuklah pelajar, ahli perniagaan, guru, pensyarah dan pelanggan yang membeli belah secara dalam talian.

Biasanya, serangan DDoS dilakukan oleh penggodam atau penyerang menggunakan beberapa peranti seperti telefon pintar dan komputer peribadi serta sambungan internet untuk menyesakkan kestabilan sebuah pelayan *(server)*.

Sebelum ini, Ketua Pegawai Eksekutif CyberSecurity Malaysia, Datuk Dr. Amirudin Abdul Wahab berkata mendedahkan terdapat 33 laman web di Malaysia telah dirosakkan oleh penggodam melalui serangan DDoS.

Jadi, perkara pertama yang perlu dibuat jika anda seorang pentadbir rangkaian komputer atau pentadbir sistem adalah memastikan pelayan organisasi mempunyai kapasiti jalur lebar yang mencukupi. Jalur lebar yang mencukupi dapat membantu kelancaran trafik pada pelayan yang bertugas untuk melayani semua permintaan daripada pengguna.

Untuk memastikan kapasiti jalur lebar mencukupi, anda perlu membuat pengujian dengan menjana seberapa banyak trafik yang masuk ke dalam pelayan. Anda juga perlu memantau trafik secara berkala untuk menentukan ianya normal atau serangan DDoS. Biasanya, serangan DDoS adalah jumlah trafik yang terlalu tinggi diterima oleh pelayan secara konsisten.

Pelayan juga memerlukan perlindungan berlapis seperti memasang alatan keselamatan seperti *Wireshark, Firewall,* antispam, penapisan kandungan, *Snort* dan banyak lagi. Anda juga disarankan untuk menghentikan sementara alamat *broadcast* yang berfungsi sebagai penghantaran dan penerimaan data atau maklumat dalam rangkaian komputer sekiranya terdapat permintaan yang tinggi daripada seorang pengguna komputer. Itu mungkinserangan DDoS.

Selain itu, anda juga disarankan untuk membataskan capaian pengguna yang keluar masuk dari sistem rangkaian supaya trafik dapat disaring dengan baik selain melakukan kemaskini sistem pengoperasian komputer.

DR. MOHD AZAHARI MOHD YUSOF
Pensyarah Kanan Jabatan
Keselamatan Maklumat dan Teknologi Web
Fakulti Sains Komputer dan
Teknologi Maklumat UTHM