Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

Bezakan tiga aplikasi ancamam siber

APAKAH perbandingan antara IPS (*Intrusion Prevention System*), IDS (*Intrusion Detection System*) dan UTM (*Unified Threat Management*)?
- MUHAMMAD, Taiping.

KETIGA-TIGA perkara tersebut iaitu Sistem Perlindungan Pencerobohan (IPS), Sistem Pengesan Pencerobohan (IDS) dan Pengurusan Ancaman Bersepadu (UTM) merupakan aplikasi, perisian atau perkakasan yang digunakan untuk mengawal keselamatan siber bagi sesebuah rangkaian komputer dan Internet.

Oleh itu, apakah takrifan bagi ketiga-tiga jenis utiliti keselamatan siber ini?

IPS merupakan satu alat pemantauan keselamatan siber dalam rangkaian komputer yang akan bertindak serta-merta ketika mengesan sesuatu corak lalu lintas rangkaian komputer mencurigakan atau pelik yang dianggap berbahaya.

Antara tindakan yang dapat dijalankan oleh IPS ke atas paket atau corak yang dicurigai berbahaya ini adalah dengan sama ada memberhentikannya, menghalangnya atau tetapkannya semula.

Penggunaan IDS lebih popular terlebih dahulu sebelum adanya IPS. IDS juga merupakan satu alat pemantauan keselamatan siber dalam rangkaian komputer berfungsi untuk mengesan sesuatu corak lalu lintas rangkaian komputer mencurigakan atau pelik yang dianggap berbahaya.

Tiada tindakan secara formal atau praktikal dijalankan menerusi penggunaan IDS sekiranya wujud corak lalu lintas rangkaian yang pelik ini.

UTM pula merupakan satu pakej perisian pemantauan keselamatan siber secara bermodul yang berada dalam satu kotak peranti atau sistem. Di dalam perisian ini terdapat pelbagai jenis perisian keselamatan seperti tembok api, IDS, IPS, perisian *anti-malware* dan sebagainya.

Kesimpulannya, perbandingan antara ketiga-tiga alat keselamatan siber ini boleh dinyatakan seperti berikut.

1 Ketiga-tiganya membuat pemeriksaan secara pasif dan aktif kepada lalu lintas rangkaian siber secara menyeluruh.

2 Sekiranya terdapat hasil tapisan yang berbahaya, IPS akan membuat sebarang tindakan yang proaktif, IDS pula sekadar memberi maklumat kepada staf keselamatan siber dan kebiasaannya UTM akan ada tindakan yang diambil ke atas situasi berbahaya itu.

3 Kekerapan melakukan penalaan dan pelarasan kepada enjin tapisan keselamatan bagi sistem IDS dan IPS adalah tinggi tetapi bagi sistem UTM kebiasaannya tidak ada.

4 IDS akan membuat pemantauan secara pasif bagi segmen-segmen rangkaian siber yang lebih kecil manakala tidak bagi IPS dan UTM.