

Risiko keselamatan dalam IoT

APAKAH risiko keselamatan dalam capaian internet menggunakan teknologi *Internet of things (IoT)*?
- Pak Mus, Bentong.

KEDATANGAN sesuatu teknologi dalam kehidupan bukan sahaja mengundang manfaat tetapi sebaliknya datang bersama-sama dengan pelbagai risiko atau masalah yang perlu ditangani. Begitu juga dengan adanya teknologi IoT ini, membolehkan komunikasi berlaku dengan mudah dan cepat antara pelbagai peralatan elektronik menerusi internet. Namun begitu, kemudahan dan kelebihan ini boleh dimanipulasi oleh sesiapa sahaja yang tidak bertanggung jawab mengancam keselamatan teknologi maklumat.

1 Data dan maklumat yang ada dalam mana-mana aplikasi IoT ini akan disimpan dan digunakan secara meluas, rawak dan merata menerusi pelbagai peralatan elektronik mudah

Diskusi ICT



Bersama **FIRKHAN**
senbangict@yahoo.com

alih dan lain-lain. Keferredahan data dan maklumat ini terutama data peribadi akan digunakan secara salah dan tidak sah oleh orang-orang yang tidak bertanggung jawab seperti penggadam, penjenayah siber dan lain-lain.

2 Peralatan IoT ini juga akan berhubung dengan pelbagai peralatan elektronik seperti telefon pintar, komputer dan lain-lain menerusi pelbagai jenis capaian rangkaian seperti rangkaian Wi-Fi, rangkaian jalur lebar tanpa wayar

dan lain-lain. Pelbagai jenis capaian rangkaian yang digunakan ini akan membuka banyak peluang kepada penggadam untuk masuk ke dalam sistem komputer. Sekiranya penggadam ini berjaya meletakan apa-apa program seperti Malware ke dalam peralatan IoT ini, penggadam ini berupaya mengawal dan mengetahui apa sahaja yang mempunyai sambungan dengannya.

3 Kebanyakan peralatan IoT ini mempunyai fungsi atau kemampuan untuk membuat penjejakan dirinya sendiri seperti dari mana dan ke mana lokasi yang ia berada. Sekiranya tidak dijaga dengan selamat, fungsi ini juga boleh dimanipulasikan oleh penggadam untuk mengetahui lokasi semasa sasarannya.

4 Disebabkan peralatan IoT ini biasa dalam kuantiti yang banyak menyebabkan ia menjadi sasaran untuk dijadikan *Botnet* oleh penggadam. Peralatan-peralatan IoT ini digunakan oleh penggadam

sebagai tenteranya untuk menyerang mana-mana sasaran dalam dunia siber. Peralatan IoT yang mempunyai kelemahan dari segi keselamatan seperti kelemahan sistem enkripsi dan lain-lain menjadi popular untuk digunakan sebagai *Botnet* oleh penggadam.

5 Peralatan IoT juga terdedah dengan masalah keselamatan yang dikenali sebagai *Ransomware* iaitu satu jenis *Malware* yang menyebabkan peralatan IoT itu dikunci fungsinya sehingga pemunya membayar wang dalam sejumlah yang tertentu.

Peralatan IoT ini boleh berada dalam sebuah kereta, kapal terbang tanpa penumpang, televisyen dan sebagainya. Jadi, peralatan IoT dan mudah alih ini perlu sentiasa dikemas kini keselamatan perisian dan perisian tegar yang berada dalamnya dan perlu ada aplikasi keselamatan dalam mengendalikannya seperti perisian anti-virus, tembok api (*firewall*) dan lain-lain.