



KETUA SETIAUSAHA NEGARA,
MALAYSIA,
Jabatan Perdana Menteri,
Aras 4 Timur, Blok A, Bangunan Perdana
Putra,
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya

Telefon: 88881480
88883381
Faks: 88883382

UPTM(S) 159/338/8
JLD 30(84)

20 Oktober 2006

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua Ketua Pengurusan Badan Berkanun Persekutuan

Semua Y.B. Setiausaha Kerajaan Negeri

Semua Ketua Pengurusan Pihak Berkuasa Tempatan

LANGKAH-LANGKAH UNTUK MEMPERKUKUHKAN KESELAMATAN RANGKAIAN SETEMPAT TANPA WAYAR (*WIRELESS LOCAL AREA NETWORK*) DI AGENSI-AGENSI KERAJAAN

Sebagaimana sedia maklum, penggunaan *Wireless LAN* telah mula meningkat di kalangan agensi sektor awam kerana peralatan ini memudahkan sambungan terus komputer kepada sistem rangkaian komputer agensi tanpa menggunakan wayar.

2. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) telah membuat satu kajian mengenai penggunaan dan *vulnerabilities* rangkaian komputer setempat tanpa wayar (*wireless LAN*) dalam sektor awam, dan laporan kajian telah pun disediakan. Laporan ini telah dibentangkan di dalam mesyuarat Ketua-Ketua Jabatan Persekutuan Bilangan 3 Tahun 2006 pada hari Isnin, 9 Oktober 2006.

3. Hasil penemuan dalam laporan yang dibentangkan oleh MAMPU menunjukkan sebahagian besar peralatan *Wireless LAN* yang dipasang di agensi-agensi kerajaan mempunyai tahap

keselamatan yang rendah dan tidak memenuhi tahap keselamatan ICT seperti yang dinyatakan di dalam *Malaysian Public Sector Management of ICT Security Handbook (MyMIS)* yang dikeluarkan oleh MAMPU pada tahun 2001. Kegagalan mematuhi tahap keselamatan *Wireless LAN* boleh menjadi salah satu saluran oleh pihak yang tidak berkenaan atau yang berkepentingan untuk memasuki atau mencerooboh ke dalam sistem komputer agensi dengan mudah.

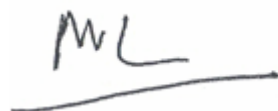
4. Sehubungan dengan itu, adalah perlu bagi agensi-agensi Kerajaan membuat kajian terperinci dan memberi pertimbangan khusus dari sudut keselamatan maklumat sebelum menggunakan *Wireless LAN* yang akan disambung kepada rangkaian atau sistem komputer yang digunakan untuk menyimpan, menghantar dan menerima maklumat terperinci. Agensi-agensi juga hendaklah memastikan langkah-langkah keselamatan seperti di Lampiran I diambil, sebelum melaksanakan *Wireless LAN*.

5. MAMPU akan menjalankan pemantauan dan pengauditan dari masa ke semasa ke atas rangkaian ICT agensi-agensi kerajaan yang menggunakan *Wireless LAN*. Pemantauan yang akan dilaksanakan menerusi kaedah "*ethical hacking*" bertujuan mendapatkan gambaran tahap pematuhan keselamatan ke atas rangkaian *Wireless LAN* agensi serta membolehkan agensi berkenaan menggunakan penemuan ini untuk melaksanakan langkah-langkah pengukuhan keselamatan.

6. Saya berharap perkara ini dapat diberi keutamaan dan diambil tindakan segera untuk melaksanakannya bagi memastikan keselamatan sistem komputer di agensi-agensi Kerajaan sentiasa terjamin.

Sekian. Terima kasih.

"BERKHIDMAT UNTUK NEGARA"



(TAN SRI MOHD SIDEK HASSAN)

Langkah-langkah Minimum Bagi Memperkukuh Kawalan Keselamatan Sistem Rangkaian Tanpa Wayar

1. Langkah-langkah pengukuhan sistem rangkaian tanpa wayar telah diperjelaskan dalam Arahan Keselamatan dan para 4.4.3.2 *Malaysian Public Sector Management of ICT Security Handbook (MyMIS)* yang dikeluarkan oleh MAMPU pada 2001.
2. Selain dari langkah-langkah tersebut, serta pelaksanaan enkripsi ke atas *wireless access point (AP)*, langkah-langkah pengukuhan lain ke atas sistem rangkaian tanpa wayar adalah seperti berikut:
 - (a) Meningkatkan keselamatan penggunaan *wireless access point (AP)* menerusi kaedah-kaedah berikut:
 - i. Menggunakan enkripsi dan *network key* yang kukuh dengan kombinasi pelbagai *character* seperti *alphabet*, aksara khas dan nombor;
 - ii. Kerap menukar kata laluan atau *network key*; dan
 - iii. Kawalan penggunaan *MAC Address*.
 - (b) Pengukuhan struktur rangkaian setempat boleh dilaksanakan seperti berikut:
 - i. Mereka bentuk sistem rangkaian setempat supaya akses menerusi *wireless access point (AP)* perlu melalui tapisan keselamatan yang sewajarnya; dan
 - ii. Mereka bentuk kawalan capaian menggunakan pengenalan pengguna (*user authentication*) melalui penggunaan *Radius Server*.

- (c) Pengukuhan keselamatan fizikal pula boleh dilaksanakan seperti berikut:
- i. Memasang alat *reflector* yang akan mengawal pancaran signal radio *wireless access point* (AP) dalam jarak yang dikehendaki;
 - ii. Menggunakan cat dinding yang khas yang dapat menghalang pancaran signal supaya dapat melampaui jarak yang dikehendaki seperti *Defend Air Radio Shield Paint*; dan
 - iii. Menggunakan *window shield* yang dapat menghalang signal daripada melepasi melalui tingkap