BAHAGIAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

POLISI KESELAMATAN RANGKAIAN UPNMNet

1.0 Tujuan Polisi

Polisi ini bertujuan untuk menerangkan perlaksanaan keselamatan rangkaian UPNMNet yang merupakan satu infrastruktur rangkaian setempat (LAN) untuk penyambungan di antara stesyen-stesyen kerja bagi tujuan komunikasi dan perkongsian maklumat / sumber.

2.0 Skop Polisi

2.1 Rekabentuk Keselamatan Rangkaian

Melibatkan rekabentuk keselamatan rangkaian yang mengambikira perkara-perkara berikut:

i. Matlamat, objektif dan skop keselamatan (sama ada meliputi *end-to-end security*, *inter-network security* atau keselamatan pada tahap sistem dalaman sahaja).

ii. Aset-aset yang perlu dilindungi termasuk jenis-jenis maklumat dan tahap keselamatan yang diperlukan.

iii. Potensi ancaman dan serangan (*vulnerabilities*) serta mewujudkan sistem pencegahan, polisi dan prosedur untuk melindungi maklumat serta integriti rangkaian.

2.2 Kawalan Keselamatan Rangkaian

Kawalan yang sewajarnya hendaklah diwujudkan untuk memastikan keselamatan data di dalam rangkaian daripada ancaman dalaman dan luaran serta melindunginya daripada capaian tanpa kebenaran.

3.0 Keselamatan Peralatan Rangkaian

3.1 Keselamatan Fizikal

i. Peralatan rangkaian ditempatkan di tempat yang bebas daripada risiko di luar jangkaan seperti banjir, gegaran, kekotoran dan sebagainya.

ii. Suhu hendaklah terkawal di dalam had suhu operasi peralatan rangkaian berkenaan.

iii. Memasang *Uninterruptible Power Supply* (UPS) dengan minimum 15 minit masa beroperasi tunggu sedia jika terputus bekalan elektrik dan perlindungan daripada *surge* dan *sag*.

3.2 Capaian Fizikal

a) Capaian Pengkabelan Rangkaian

Langkah-langkah yang perlu diambil untuk melindungi kabel rangkaian daripada di capai oleh orang yang tidak berkenaan :

i. Melindungi pengkabelan di dalam kawasan awam dengan cara memasang pembuluh (*conduit*) atau lain-lain mekanisma perlindungan; dan

ii. Pusat pendawaian terletak di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

b) Capaian Peralatan Rangkaian

i. Peralatan hendaklah ditempatkan di tempat yang selamat dan terkawal; dan

ii. Peralatan rangkaian hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

3.3 Capaian Logikal

i. ID dan kata laluan diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh kakitangan yang dibenarkan sahaja.

ii. Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan.

iii. Maklumat capaian ke router hendaklah direkodkan - pegawai, tarikh, masa dan aktiviti. Maklumat mestilah disimpan selama 90 hari.

iv. Rangkaian hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja. Semua perubahan konfigurasi suis rangkaian hendaklah dilogkan termasuk pengguna yang membuat perubahan, pengesahan, tarikh dan masa.

v. Perubahan perisian konfigurasi mestilah direkodkan – pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh.

vi. Perubahan konfigurasi hendaklah dikendalikan secara berpusat.

3.4 Penggunaan Peralatan Tanpa Kebenaran

Penggunaan peralatan rangkaian tanpa kebenaran boleh dikawal dengan :

i. Mengadakan kawalan capaian logikal seperti yang disebutkan di para

ii. Menempatkan peralatan di tempat yang selamat.

iii. Bilik pendawaian atau *wiring closet* hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

iv. Menyelenggara inventori peralatan dan membuat semakan secara berkala.

3.5 Konfigurasi Peralatan

Peralatan dikonfigurasi dengan betul dengan mengambil langkah-langkah berikut:

i. Mengaktifkan perkhidmatan yang diperlukan sahaja;

ii. Capaian untuk konfigurasi dihadkan melalui nod atau alamat IP yang dibenarkan sahaja;

iii. Menyahaktifkan siaran (*broadcast*);

iv. Menggunakan kata laluan yang selamat; dan

v. Dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja.

3.6 Penyelenggaraan Peralatan

i. Peralatan hendaklah dipasang, dioperasi dan diselenggarakan mengikut spesifikasi pengilang.

ii. Dibaiki dan diselenggara hanya oleh kakitangan yang terlatih dan dibenarkan sahaja.

iii. Mempunyai rekod penyelenggaraan.

4.0 Kebolehcapaian Pengguna (User Accessibility)

4.1 Rangkaian Setempat (Local Area Network)

i. Hanya staf dan pelajar UPNM dibenarkan membuat penyambungan ke rangkaian UPNM (rujuk Polisi Penggunaan Rangkaian dan Penyambungan).

ii. Hanya komputer kepunyaan UPNM yang dibenarkan untuk disambungkan ke rangkaian UPNM.

iii. Pengguna luar perlu mendapatkan kebenaran daripada Pusat Komputer sebelum membuat capaian ke rangkaian UPNM.

iv. Hanya pengguna yang disahkan sahaja dibenarkan membuat capaian kepada sistem pengkomputeran UPNM.

v. Setiap perkakasan atau peranti yang ingin berhubung ke dalam rangkaian UPNM perlu mematuhi perkara-perkara berikut:

1. Berhubung ke rangkaian menggunakan domain UPNM
2. Mengesahkan nama pengguna dan kata laluan
3. Memastikan peralatan tersebut menggunakan *virus pattern* yang terkini
4. Memastikan peralatan telah dilengkapi dengan *patches* sistem perasi yang terkini

vi. Perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyser*) tidak dibenar digunakan pada sebarang komputer kecuali setelah mendapat kebenaran bertulis daripada Pengarah Pusat Komputer. Status komputer tersebut hendaklah disemak setiap tahun.

vii. Perisian rangkaian hanya boleh dicapai melalui akaun ***root***.

5.0 Sambungan Dengan Lain-Lain Rangkaian

5.1 Capaian Yang Tidak Digalakkan

i. Kurangkan penggunaan protokol rangkaian seperti NetBEUI atau IPX, sebaliknya gunakan TCP/IP dan WINS Server.

ii. Elakkan penggunaan Workgroup. Ini adalah kerana workgroup menyokong *share-level security* dan bukan *user-level security*. Disyorkan menggunakan Domain NT dan NFS.

5.2 '*Firewall*'

i. Semua aliran trafik (multimedia dan data) daripada dalam ke luar UPNM dan sebaliknya mestilah melalui *firewall.*

ii. Hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya berasaskan kepada Dasar Keselamatan Rangkaian.

iii. Rekabentuk *firewall* hendaklah mengambilkira perkara-perkara berikut :

a. keperluan audit dan arkib;
b. kebolehsediaan;
c. kerahsiaan; dan melindungi maklumat