PERINTAH AM ANGKATAN TENTERA (PAAT) BIL 1/13

ARAHAN KESELAMATAN MAKLUMAT - PENCEGAHAN PENCEMARAN MAKLUMAT ATM MELALUI PLATFORM SIBER

Rujuk: JPP(M)2012/3 bertarikh 2 Apr 12

AM

1. Kebebasan akses di dalam platform siber sama ada melalui rangkaian mobil, *broadband internet* atau rangkaian statik seperti media komunikasi elektronik (telefon pintar, PDA, komputer riba, dsb) telah memberikan kesan yang mendalam terhadap pencemaran keselamatan maklumat di dalam ATM pada hari ini. Matlamat untuk mencapai Keunggulan Informasi di dalam ATM sukar diperolehi jika tindakan mempertahankan informasi tidak dilaksanakan dengan bersungguh-sungguh. Selain daripada menepis ancaman, eksploitasi dan serangan dari pihak luar, unsur dalaman iaitu anggota ATM sendiri merupakan penyumbang terbesar kepada kebocoran maklumat ATM kepada dunia luar.

TUJUAN

2. Arahan ini adalah untuk:

a. Mengukuhkan Arahan Keselamatan Angkatan Tentera Malaysia Tahun 1996.

b. Memberi panduan kepada warga ATM terhadap larangan-larangan dalam penggunaan internet dan intranet.

c. Memberi panduan kepada pemerintah-pemerintah untuk mengambil tindakan sewajarnya terhadap kesalahan penggunaan internet di kalangan warga ATM.

TAFSIRAN

3. **Ruang Siber**. Merupakan satu medium elektronik kepada rangkaian komputer sedia ada seperti internet yang mana perhubungan di atas talian menjadi platform kepada komunikasi ICT yang menawarkan perkhidmatan bersambungan secara maya, interaktif dan capaian tanpa mengira kedudukan geografi.

4. **Internet**. Perkhidmatan elektronik dan telekomunikasi di atas talian secara global yang menghubungkan pengguna rangkaian komputer di seluruh dunia melalui protokol yang sama.

5. **Intranet**. Perkhidmatan persendirian rangkaian komputer yang menggunakan teknologi protokol internet untuk berkongsi secara selamat, perkongsian mana-mana atau sebahagian maklumat organisasi dan rangkaian sistem operasi di dalam organisasi.

6. **Pengguna Internet**. Individu yang mempunyai akses dan menggunakan capaian terhadap sistem pengkomputeran, aplikasi dan sistem di atas talian yang telah dirangkaikan kepada internet.

7. **Muat Turun**. Aktiviti mendapatkan data, menerima data atau melaksanakan sesuatu perkara berkaitan perpindahan data melalui rangkaian komputer ke sistem persendirian (*local*) daripada sistem kawalan (*remote*). Sistem kawalan yang dimaksudkan adalah seperti pelayan web, pelayan FTP, pelayan email dan pelayan-pelayan lain yang menawarkan penyimpanan dan perkongsian data atau yang semaksud dengannya. Muat turun juga diklasifikasikan sebagai satu proses yang ditawarkan bagi mendapatkan sesuatu fail oleh mana-mana aplikasi di dalam sistem dan aplikasi.

8. **Muat Naik**. Aktiviti menghantar dan menyimpan data daripada sistem persendirian (*local*) kepada sistem kawalan (*remote*) seperti pelayan perkongsian data atau komputer lain dengan niat supaya sistem tersebut akan menyimpan salinan data dan fail yang dihantar atau mana-mana usaha berkaitan proses ini.

9. **Perisian**. Merujuk kepada semua aset-aset dan aplikasi digital ICT.

10. **Perkakasan**. Merujuk kepada semua aset-aset fizikal ICT.

11. **Sistem Informasi**. Merupakan aplikasi hasil daripada kombinasi teknologi maklumat dan aktiviti pengguna yang menggunakan teknologi untuk menyokong operasi, pengurusan dan proses membuat keputusan. Ia juga membawa maksud aplikasi yang terhasil melalui interaksi antara manusia, proses algoritma, data dan teknologi bagi menghasilkan sesuatu keperluan yang digunapakai oleh organisasi dan dimanfaatkan oleh pengguna untuk menyokong sesuatu proses kerja.

12. **Aplikasi**. Perisian komputer yang direkabentuk bagi membantu pengguna untuk melaksanakan tugasan tertentu secara persendirian ataupun berkumpulan.

13. **Pangkalan Data**. Merupakan koleksi data secara tersusun yang digunakan bertujuan untuk penghasilan maklumat yang kebiasaannya di dalam bentuk digital. Ia juga mempunyai ciri sebagai storan, penyimpanan kandungan, pengubahan, carian dan sebagainya. Ia boleh disimpan dalam bentuk bibliografi, teks dokumen dan statistik.

14. **Kod Perosak**. *Malicious software (malware)* dan *malicious code* adalah merupakan program (makro atau *script*) yang direkabentuk dan ditanam di dalam sistem komputer sasaran dengan tujuan untuk mengakses secara rahsia tanpa pengetahuan pemilik komputer. Ia juga dihasilkan oleh golongan profesional di dalam dunia pengkomputeran untuk pelbagai tujuan seperti membawa kerosakan, pencerobohan atau mengganggu kod perisian sedia ada.

15. **Spam**. Gangguan yang dilaksanakan dengan menggunakan sistem penyampaian elektronik (termasuk penyiaran media atau sistem penghantaran digital) dengan cara menghantar mesej yang tidak dikehendaki secara pukal dan berterusan.

16. **Blog**. Merupakan sejenis laman web atau sebahagian darinya yang menawarkan fungsi seperti catatan peribadi (diari), ulasan-ulasan, penerangan terhadap sesuatu peristiwa, atau penyampaian sesuatu material seperti grafik dan video yang digunakan secara meluas dan diselenggara mengikut selang masa tertentu

oleh individu yang mendaftar sebagai pemunya blog tersebut daripada penyedia perkhidmatan. Kemasukan (*entries*) merupakan aktiviti asas yang dilaksanakan bagi memastikan blog sentiasa terkini dengan tujuan menjadikanya interaktif dan ikutan kepada pengguna internet lain dengan meninggalkan pandangan dan komen-komen melalui platform yang disediakan.

17. **Laman Web**. Merupakan platform sumber maklumat mengandungi gabungan pelbagai bentuk dokumen, grafik, aplikasi dan sebagainya yang dibangunkan di dalam format HTML dan XHTML bersesuaian dengan kod dan capaian *World Wide Web* (WWW). Ia boleh dicapai melalui aplikasi pelayar web tertentu di komputer atau telefon pintar mudah alih untuk tujuan navigasi.

18. **Media Sosial**. Merupakan perkhidmatan atas talian (*online*), platform atau laman yang memfokuskan kepada pembangunan rangkaian sosial individu dan organisasi atau perhubungan sosial antara individu. Ia juga merupakan satu kaedah pengembangan rangkaian sosial individu atas talian dua hala berdasarkan kepada perkara yang dikongsi seperti minat ataupun aktiviti. Ia menawarkan profil pengguna sebagai wakil kepada data peribadi seseorang, rangkaian sosial sedia ada, dan platform komunikasi maya. Mempunyai ciri-ciri lain seperti mel elektronik, laman sembang (chatting), laman bersemuka dan sebagainya.

19. **Kata Nama**. Kod atau ganti nama (nick name) pengenalan individu yang digunakan sebagai wakil kepada individu tersebut bagi mengakses sesuatu sistem.

20. **Kata Laluan**. Kombinasi rahsia mana-mana perkataan, huruf, nombor, simbol atau aksara-aksara khas yang digunakan sebagai authentikasi setelah dipadankan dengan kata nama untuk mengakses sesuatu sistem dengan lebih selamat.

21. ***Online Chatting***. Merujuk kepada mana-mana komunikasi berasaskan teks atas talian maya seperti internet, intranet, telefon pintar yang melaksanakan perbualan *real time* antara individu kepada individu, individu kepada kumpulan dan kumpulan kepada individu.

22. ***Messenger***. Aplikasi sembang atas talian bagi tujuan komunikasi teks secara maya dan *real time*.

23. ***Web Hosting***. Merupakan perkhidmatan yang menyediakan ruang penyewaan kepada pelayan, kandungan dan format laman web ataupun *data center* mana-mana individu ataupun organisasi, oleh pembekal untuk tujuan mendapatkan *hosting* atau penyambungan kepada laman web kepada rangkaian internet supaya boleh diakses melalui *World Wide Web* (WWW).

24. **Pencemaran Maklumat**. Diklasifikasikan sebagai aktiviti sama ada sengaja atau tidak yang boleh membawa kepada kebocoran maklumat ketenteraan, mengkritik atau memberi pandangan secara terbuka terhadap dasar-dasar kerajaan, mengapi-apikan isu dan sentimen sensitif yang menimbulkan kebencian individu lain terhadap polisi atau dasar kerajaan serta perkara-perkara lain yang boleh menjejas kepada keselamatan negara.

KAEDAH PENCEMARAN MAKLUMAT

25. Diklasifikasikan sebagai perbuatan seperti berikut:

a. Memuat naik, memapar, mengemaskini atau memancarkan sebarang bentuk dokumen yang terperingkat atau berklasifikasi.

b. Memuat turun sebarang bentuk aplikasi atau dokumen yang tidak diketahui tahap keselamatannya.

c. Membincangkan dan mengambil bahagian dalam sebarang bentuk forum berkaitan isu-isu yang boleh menjejas keselamatan dan keharmonian negara.

d. Menghasut atau menawarkan sebarang bentuk provokasi.

e. Menggunakan *public email* bagi urusan rasmi.

f. Menggunakan kemudahan fasiliti awam bagi tujuan *hosting* kepada laman web rasmi pasukan.

g. Membenarkan pihak ketiga di luar organisasi ATM bagi menjalankan aktiviti ujian penembusan, audit ICT dan akses kepada sistem dalaman pasukan tanpa kebenaran BSPP.

h. Memasang dan menyediakan perkhidmatan WiFi tanpa enkripsi di dalam parameter dan kawasan tentera tanpa kebenaran BSPP.

i. Menggunakan perkhidmatan tanpa wayar yang tidak diketahui puncanya atau penyediaannya untuk tujuan rasmi dengan menggunakan komputer yang disediakan oleh pasukan atau komputer peribadi yang mengandungi dokumen berdarjah.

j. Menyimpan sebarang dokumen berkaitan tugas rasmi di dalam komputer peribadi.

k. Menyambungkan rangkaian dalaman (intranet) kepada rangkaian awam (internet) tanpa kebenaran pentadbir sistem atau BSPP.

BENTUK MAKLUMAT

26. Maklumat-maklumat dikategorikan seperti berikut:

a. Sebarang dokumen teks pelbagai format.

b. Sebarang bentuk gambar/imej dalam pelbagai format.

c. Sebarang bentuk audio visual.

d. Sebarang bentuk status kesiagaan atau aktiviti pasukan.

e. Sebarang lakaran dan simbol geografi/imajeri digital yang disediakan oleh pihak awam.

f. Sebarang bentuk ensiklopedia digital yang disediakan oleh pihak awam.

g. Maklumat peribadi seperti gambar, perlakuan atau aktiviti tidak bermoral yang boleh memberi imej negatif terhadap ATM.

APLIKASI DI RUANG SIBER

27. Aplikasi yang boleh menyumbang kepada pencemaran maklumat antaranya adalah seperti berikut:

a. E-mail Awam (Yahoo, Google, MSN dsb).

b. Perkongsian Dokumen (GoogleDocs, Zoho, Scribd dsb).

c. Perkongsian Storan (ZumoDrive, HostedFTP dsb).

d. Perkongsian Audio Visual (FotoFlexer, Youtube dsb).

e. Media Sosial (Facebook, Twitter, Myspace, Tagged, YahooGroup dsb).

f. Blog/Portal (Blogspot, Wordpress dsb).

g. Komunikasi Atas Talian (Google Talk, Skype, Yahoo Messenger, MSN dsb).

h. Komunikasi Mobil (SMS, MMS, Blackberry Messenger).

STRATEGI KAWALAN

28. Bagi memastikan pencemaran maklumat tidak berlaku, tindakan melalui pematuhan, pemantauan dan penguatkuasaan perlu dilaksanakan segera melalui:

a. **Tindakan Pematuhan (*Compliance Action*)**.

(1) **Dasar/Arahan Peraturan Sedia Ada**. Mematuhi dasar, arahan dan peraturan sedia ada yang dihebahkan dari semasa ke semasa mengikut kesesuaian. Arahan sedia ada adalah seperti:

(a) Akta Rahsia Rasmi 1972.

(b) Akta Angkatan Tentera 1972.

(c) Arahan Keselamatan ATM atau FAFSI.

(d) Arahan BSPP 1987.

(e) Dasar Keselamatan ICT KEMENTAH.

(2) Arahan/Garis Panduan yang dikeluarkan dari semasa ke semasa mengikut perubahan teknologi juga hendaklah dipatuhi.

b. **Tindakan Pemantauan (*Monitoring Action*)**.

(1) **Peringkat Strategik**. *Malaysia Defence Intelligence Organization* (MDIO)/BSPP adalah Agensi Pusat yang bertanggungjawab untuk mengkoordinasi, memantau dan merancang aktiviti pemantauan pencemaran maklumat di peringkat strategik.

(2) **Peringkat Operasional dan Taktikal**. Setiap Perkhidmatan/Formasi /Markas/Pasukan perlu bertanggungjawab untuk mengkoordinasi, memantau dan melaksana aktiviti pemantauan dan kempen kesedaran terhadap pencemaran maklumat di peringkat masing-masing.

c. **Tindakan Penguatkuasaan (*Enforcement Action*)**. Agensi-agensi yang dilantik perlu aktif melaksanakan penguatkuasaan dan sebarang pencemaran maklumat hendaklah diambil tindakan tatatertib yang sewajarnya.

29. **Larangan-Larangan Kepada Pengguna Ruang Siber**. Semua warga ATM dikehendaki mematuhi larangan-larangan apabila melayari ruang siber supaya mengelakkan daripada kejadian pencemaran maklumat. Ia merangkumi:

a. **Penggunaan Internet/Intranet**

(1) Dilarang memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen.

(2) Dilarang menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur sensitif, berdarjah, pornografi dan sebagainya.

(3) Dilarang menghantar dan memiliki bahan-bahan yang salah disisi undang-undang seperti bahan lucah, perjudian dan jenayah.

(4) Dilarang menyedia, memuat naik, memuat turun dan menyimpan maklumat berkaitan pasukan di internet.

(5) Dilarang menggunakan aplikasi yang melibatkan sebarang penyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej negara, pertubuhan dan individu.

(6) Dilarang menyedia, memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh melibatkan keadaan hura-hara dan menakutkan pengguna.

(7) Dilarang memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu di dalam sistem intranet.

(8) Dilarang menggunakan kemudahan internet yang disediakan oleh organisasi untuk kemudahan peribadi.

(9) Dilarang menjalankan dan menggunakan aplikasi untuk aktiviti-aktiviti komersial dan politik.

(10) Dilarang merancang dan melakukan aktiviti-aktiviti jenayah melibatkan platform siber seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas.

(11) Dilarang menggunakan kemudahan modem peribadi samada secara talian ataupun tanpa wayar yang bertujuan untuk membuat capaian terus ke internet dari kemudahan komputer pasukan.

(12) Dilarang menceroboh atau cuba menceroboh pangkalan data (*database*) dalam apa jua keadaan dan cara.

(13) Dilarang menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah.

(14) Dilarang membuka sistem dalaman (intranet) kepada internet tanpa kebenaran dan kelulusan BSPP.

(15) Dilarang membuka dan membenarkan akses kepada sistem dalaman (intranet) pasukan kepada pihak awam untuk tujuan pengauditan.

(16) Dilarang menyebarkan kod perosak seperti V*irus, Worm, Trojan horse dan trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain.

(17) Dilarang menggunakan aplikasi perkhidmatan tanpa wayar yang bukan disediakan oleh pasukan dengan menggunakan komputer peribadi atau komputer yang disediakan pasukan.

b. **Penggunaan Email**

(1) Dilarang menghantar maklumat berulang-ulang (*spam*) berupa gangguan.

(2) Dilarang menggunakan akaun milik orang lain, berkongsi akaun, memberi dan mendedahkan kata nama / kata laluan akaun kepada orang lain.

(3) Dilarang menghantar atau memajukan (*forward*) email layang.

(4) Dilarang membincang dan membahaskan isu-isu sensitif.

(5) Dilarang menggunakan email awam untuk tujuan rasmi dan mengepilkan fail yang mengandungi maklumat sensitif.

(6) Dimestikan untuk menggunakan email terselamat yang diperuntukkan dan disediakan oleh pasukan bagi urusan rasmi.

(7) Menggunakan kata laluan yang kukuh sekurang-kurangnya lapan aksara dengan kombinasi huruf, nombor atau aksara khas.

c. **Penggunaan Media Sosial/Forum/Blog/*Chatting*/*Mesengger***

(1) Dilarang memberi maklumat tentang status, kesiagaan dan aktiviti pasukan.

(2) Dilarang membincangkan isu-isu sensitif berkaitan dasar kerajaan.

(3) Dilarang memihak secara terbuka kepada mana-mana parti politik.

(4) Dilarang mengapi-apikan atau memprovokasi individu lain di dalam perbincangan isu-isu sensitif.

(5) Dilarang mewujudkan dan membangkitkan sebarang isu yang boleh mengakibatkan huru-hara dan kacau bilau kepada organisasi atau kumpulan tertentu.

(6) Dilarang memuat naik sebarang dokumen, imej atau audio visual berkaitan pasukan termasuk aset, keputusan mesyuarat, perancangan organisasi dan sebagainya.

(7) Dilarang membuat, menyebarkan penyataan fitnah atau hasutan yang memburuk dan menjatuhkan imej pasukan dan kerajaan.

(8) Dilarang memaparkan sebarang aktiviti peribadi yang tidak sihat yang boleh mencemarkan nama baik pasukan.

(9) Dilarang menggunakan lambang atau identiti pasukan untuk tujuan negatif.

d. **Penggunaan Web Hosting/Web/Portal**

(1) Dilarang menggunakan kemudahan *hosting* yang disediakan oleh pihak awam samada fizikal ataupun maya.

(2) Dilarang menempatkan peralatan seperti pelayan dan aplikasi server dan aplikasi atau melaksanakan sewaan kepada fasiliti luar.

(3) Perlu mendapatkan kelulusan pihak atasan/pasukan risik perkhidmatan bagi pembangunan sesuatu laman web yang melibatkan kandungan yang akan dipaparkan.

(4) Siaran atau muat naik maklumat rasmi berkaitan perkhidmatan hendaklah dilaksanakan oleh Unit Komunikasi (PR) masing-masing ataupun bagi pasukan yang mempunyai laman web dan portal adalah

dengan kelulusan Pegawai Memerintah/Pemerintah melalui pengurus laman web (*webmaster*).

30. **Tugas dan Tanggungjawab**. Tugas dan tanggungjawab yang perlu dimainkan bagi membendung pencemaran maklumat adalah seperti berikut:

a. **Tugas Agensi Pusat**. BSPP memainkan tanggungjawab dalam melaksanakan peranan seperti berikut:

(1) Menasihati Panglima Angkatan Tentera berkaitan ancaman dan keselamatan siber ATM.

(2) Melaksanakan audit keselamatan ICT dan Siber ATM termasuk semua perkhidmatan.

(3) Mengeluar dan mengemaskini dasar, polisi atau arahan berkaitan keselamatan siber dari semasa ke semasa.

(4) Mengkoordinasi aktiviti pemantauan keselamatan siber di peringkat strategik ATM.

(5) Memantau keseluruhan ancaman kepada rangkaian ATM.

(6) Mengesan kelemahan yang wujud dalam sistem, aplikasi dan rangkaian ATM.

(7) Mengkoordinasikan rancangan tindak balas cemas terhadap serangan dan ancaman siber.

(8) Mengkoordinasikan Pelan Kesinambungan Perkhidmatan.

(9) Melaksanakan Penilaian Postur Keselamatan Informasi terhadap mana-mana Perkhidmatan/Formasi/Markas/Pasukan dari masa ke semasa secara rambang.

b. **Tugas Penyedia Perkhidmatan**. Bahagian KOMLEK-MK ATM dan Cawangan ICT setiap perkhidmatan perlu mengkoordinasikan keperluan infrastruktur, aplikasi, sistem dan kemudahan platform berpusat bagi tujuan *hosting* web rasmi ,portal atau e-mel serta memastikan ia memenuhi ciri-ciri keselamatan informasi (*security features*).

c. **Tugas Pemantauan**. Setiap perkhidmatan perlu mewujudkan organisasi siber yang bertanggungjawab untuk mengkoordinasikan keperluan keselamatan maklumat.

d. **Tugas Pengesanan dan Pencegahan**. Cawangan Risik setiap perkhidmatan perlu:

(1) Membuat tindakan susulan untuk mengenalpasti sumber-sumber pencemaran dan kebocoran maklumat.

(2) Merekod dan meluluskan permohonan mewujudkan laman web rasmi pasukan.

e. **Tugas Siasatan**. Sebarang perbuatan yang telah dikenalpasti sebagai pencemaran maklumat perlu disiasat dengan sewajarnya oleh BSPP, Provos Marsyal ATM dan Provos Perkhidmatan mengikut mana yang berkenaan. Keupayaan yang perlu dibangunkan bagi menyokong siasatan kes termasuk kemahiran dalam Penyiasatan Komputer Forensik.

f. **Tugas Pendakwaan**. Kes-kes yang menpunyai bukti yang kukuh hendaklah dirujuk kepada Pegawai Memerintah bagi maksud dibicarakan setelah mendapat nasihat daripada Pegawai Undang-Undang di Formasi masing-masing.

31. **Program Peningkatan Kesedaran**. Setiap perkhidmatan perlu secara aktif meningkatkan tahap kefahaman dan kesedaran anggota berkaitan isu keselamatan maklumat di platform siber seperti menganjurkan kempen, bengkel, seminar dan ceramah. Pengenalan kepada keselamatan maklumat siber juga wajar dijadikan sebagai satu modul dalam kursus-kursus asas di semua peringkat ATM.

32. **Perlaksanaan Arahan**. Arahan Keselamatan Maklumat - Pencegahan Pencemaran Maklumat ATM Melalui Platform Siber yang dikeluarkan ini hendaklah dikuatkuasakan serta merta dan di isytiharkan melalui Perintah Bahagian Satu di setiap pasukan. Arahan ini berkuatkuasa serta-merta dari tarikh ia dikeluarkan dan semua peringkat anggota ATM adalah tertakluk kepada arahan ini. Sebarang perlanggaran arahan atau mana-mana bahagian darinya akan diambil tindakan mengikut peruntukan semasa.