KE ARAH IMPLEMENTASI
SISTEM POLISI KESELAMATAN ICT
KAJIAN KES : PUSAT TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

AZHARI BIN HJ AHMAD

Laporan projek ini dikemukakan
sebagai memenuhi sebahagian daripada syarat
penganugerahan Ijazah Sarjana Sains (Teknologi Maklumat – Pengurusan)

Fakulti Sains Komputer dan Sistem Maklumat
Universiti Teknologi Malaysia

OKTOBER 2008

ABSTRAK

Insiden keselamatan seringkali berlaku terhadap organisasi yang mempunyai kemudahan talian internet dan memberi kemudahan perkhidmatan terhadap orang ramai. Masalah ini juga berlaku kepada Pusat ICT umumnya dan UTM khususnya, dalam menyediakan pelbagai kemudahan komputer dan talian internet kepada pengguna. Mengikut kajian yang dilakukan, termasuk responden dari Pusat ICT masalah ini dapat dikurangkan dengan menyediakan satu panduan dokumen polisi ICT, memberi kesedaran dan menguatkuasa akan Polisi ICT yang lengkap dan menyeluruh. Keadaan ini menyebabkan fakulti atau jabatan di UTM terpaksa menggunakan inisiatif sendiri bagi menyediakan polisi keselamatan ICT yang bersesuaian dengan keperluan mereka seperti polisi penggunaan komputer di Perpustakaan Sultanah Zanariah. Tujuan projek ini adalah untuk membangunkan, menyediakan dan merekabentuk suatu sistem polisi keselamatan ICT agar dapat membantu pusat ICT sebagai sekretariat keselamatan ICT, UTM bagi menyediakan dokumen polisi keselamatan ICT yang baik, lengkap dan menyeluruh. Di samping itu, dokumen tersebut mestilah patuh kepada piawaian ISO 27001 dan Dasar Keselamatan Teknologi Maklumat dan Komunikasi untuk Sektor Awam oleh MAMPU. Sistem Polisi Keselamatan ICT ini berasaskan web serta boleh dicapai melalui rangkaian Internet, memberikan kemudahan kepada setiap peringkat pengurusan, pentadbir IT dan pengguna dalam memberikan dan menerima perkhidmatan ICT yang berkesan dan lebih baik.

ABSTRACT

Breach of safety incidence occurs frequently to organization that own internet connections especially if it is a public internet service facility. The problem exist to CICT-UTM as well as other goverment organization in preparing the internet connection to users. The study is based on questionaires of respondence at CICT that concluded that the internet security problem may be reduced by implementing an ICT policy, give an awareness to users globally and fully enforced the strict policy to users. Even though that on-shelf security and policy system are existed in the market, but mostly is about and focusing on the evaluation of the risk and managing the risk. This difficulty has made the IT management of the faculty and centres in UTM making their own initiatives by making and implementing the policy that only suit their own requirement. For example, PSZ-UTM is enforcing their own developed ICT policy and enforcing it by policing the user frequently. This projects is about developing, preparing and designing a system for ICT security policy that will assist the security implementer around the UTM-Campus. It will also assume that CICT will act as ICT security policy secretariat with the role of preparing the comprehensive safety policy documentations. The security policy document created in the thesis is in compliance with international standard organization of ISO27011 and Policy of Security of Information Technology and Communication for Public Sector produced by MAMPU. A web based ICT safety policy system develop in the projects will assist the internet administrator in providing a better and effective services in UTM.

KANDUNGAN

BAB 1

PENGENALAN

1.1 Pengenalan

Ledakan teknologi maklumat yang berkembang pesat di negara ini, memperlihatkan betapa beruntungnya generasi masa kini berikutan terdedah kepada dunia tanpa sempadan. Ia bukan saja berfungsi sebagai agen komunikasi, malah menjadi jambatan untuk pengguna memanfaatkannya sebagai sebahagian daripada rutin dan keperluan hidup. Keselamatan ICT berkait rapat dengan pelindungan maklumat dan aset ICT. Ini kerana komponen peralatan perkakasan dan perisian yang merupakan sebahagian daripada aset ICT organisasi kerajaan adalah pelaburan besar dan perlu dilindungi. Begitu juga dengan maklumat yang tersimpan di dalam sistem ICT, ia amat berharga kerana banyak sumber yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangkamasa yang singkat.

Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat. Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan negara. Sebarang penggunaan aset ICT kerajaan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan. Justeru itu satu tinjauan ISMS telah dibuat oleh NISER (National IC Security & Emergency Response Center) dalam bulan Oktober 2003 terhadap 100 organisasi, kebiasaannya jenis serangan adalah serangan virus (87%) dan *mail spamming* (83%). Lebih daripada 68% organisasi tersebut mempunyai sedikit pengetahuan mengenai ISMS.[1] Sementara lebih kurang 37% organisasi tidak mempunyai polisi keselamatan langsung.

Bagi menangani risiko ini dari semasa ke semasa, Dasar Keselamatan ICT Kerajaan akan diperjelaskan lagi melalui pengeluaran Piawaian Keselamatan ICT yang mengandungi garis panduan serta langkah-langkah keselamatan ICT. Kegunaan kesemua dokumen ini secara bersepadu adalah disarankan. Ini adalah kerana pembentukan dasar, piawaian, peraturan, garis panduan dan langkah-langkah keselamatan ini diorientasikan untuk melindungi kerahsiaan data, maklumat dan sebarang kesimpulan yang boleh dibuat daripadanya.

1.2 Latar Belakang Masalah

Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantungan antara satu dengan lain kerapkali mewujudkan pelbagai kelemahan.

Sesetengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenalpasti dan ditangani sewajarnya. Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Polisi dan Dasar Keselamatan ICT ini merangkumi perlindungan semua bentuk maklumat yang dimasuk, diwujud, dimusnah, disimpan, dijana, dicetak, dicapai, diedar, dalam penghantaran dan yang dibuat salinan keselamatan ke dalam semua aset ICT.

Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :

i) Data dan Maklumat - Semua data dan maklumat yang disimpan atau digunakan dipelbagai media atau peralatan ICT.
ii) Peralatan dan perkakasan ICT - Semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS), bekalan punca kuasa dan pendingin hawa.

iii) Media Storan - Semua alat berbentuk media storan dan peralatan yang berkaitan seperti disket, kartrij, CD-ROM, pita, cakera, pemacu cakera dan pemacu pita.

iv) Komunikasi dan Peralatan Rangkaian - Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router* dan peralatan PABX.

iv) Perisian - Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data.

v) Dokumentasi - Semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, transparensi, risalah dan slaid.

vi) Manusia - Semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT.

viii) Premis Komputer dan Komunikasi - semua kemudahan serta premis yang diguna untuk menempatkan perkara (i)-(vii) di atas.

Justeru itu, satu Unit Keselamatan ICT perlu ditubuhkan di Pusat ICT, UTM bagi memastikan perkhidmatan yang disediakan dan dilindungi dari serangan yang disengajakan atau tidak disengajakan (seperti serangan virus dan cecacing). Unit ini bertanggungjawab menyediakan pelayan dinding api dan proxy di laluan keluar masuk fakulti dan bahagian dan juga dinding api di laluan utama rangkaian universiti.

Disamping itu pemantauan terhadap keselamatan rangkaian dalaman ,sistem-sistem pelayan, komputer-komputer pengguna dengan menggunakan beberapa perisian seperti CISCO NAC (Network Access Control), OPMANAGER, Nagios, MRTG (Multi Router Traffic Generator) dan Host Monitoring digunakan. Dengan bantuan unit lain seperti Unit Rangkaian dan Bahagian Akademik kempen-kempen kesedaran keselamatan ICT kepada pengguna kampus turut dilakukan. Unit ini akan

melihat perlaksanaan Polisi Keselamatan ICT yang telah diluluskan oleh pihak universiti secara lebih terperinci .

Terdapat 5 pekeliling yang digariskan oleh agensi pusat (Malaysian Administrative Modernization and Management and Management Planning Unit(MAMPU) dan Jabatan Perdana Menteri) :

i) Pekeliling Am Bil. 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.
ii) Pekeliling Am Bil. 1 Tahun 2001 : Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dn Komunikasi(ICT).
iii) The Malaysian Public Sector ICT Management Security Handbook (MyMIS), January 2002.
iv) Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.
v) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

1.3 Pernyataan Masalah

i) Walaupun polisi keselamatan ICT telah diluluskan oleh Universiti pada tahun 2004 tetapi dokumen polisi keselamatan yang ada masih belum dikaji secara menyeluruh untuk diimplementasi di UTM.

ii) Tiada terdapat sistem Polisi Keselamatan dari Pusat ICT dalam membantu organisasi di UTM dalam menyediakan dokumen Keselamatan ICT.

1.4 Matlamat Projek

Matlamat projek ini adalah menyediakan sistem untuk mambantu UTM menyediakan polisi keselamatan ICT dengan berasakan piawaian ISO 27001 serta pekeliling dan garis panduan dari MAMPU.

1.5 Objektif Projek

Objektif projek ini adalah seperti berikut :

i) Untuk membuat kajian bagi membangunkan prototaip berdasarkan piawaian Keselamatan ICT yang sedia ada dari garispanduan yang dikeluarkan oleh MAMPU dan piawaian ISO 27001.

ii) Untuk mendapatkan maklumat dan cadangan polisi keselamatan ICT melalui sistem dari pegawai-pegawai terlibat dengan pengurusan ICT UTM.

iii) Menghasilkan dan mengeluarkan dokumen Polisi Keselamatan ICT untuk Pusat ICT umumnya dan UTM khususnya dengan menggunakan sistem Polisi Keselamatan ICT yang dibangunkan.

1.6 Skop Projek

i) Analisa dan kajian terhadap piawaian keselamatan ISO 27001 dan Dasar Keselamatan Teknologi Maklumat dan Komunikasi Untuk Sektor Awam dan pekeliling yang dikeluarkan oleh MAMPU.

ii) Kajian ini akan dilakukan terhadap Pusat Teknologi Maklumat dan Komunikasi, UTM yang bertindak sebagai sekretariat keselamatan ICT, UTM.

iii) Suatu sistem Polisi Keselamatan ICT akan dibangunkan bagi membantu Pusat ICT, UTM Skudai didalam membuat persediaan mendokumenkan Polisi Keselamatan ICT. Untuk membangunkan projek ini bahasa ASP dan Access sebagai pangkalan data akan digunakan.

iv) Pengguna-pengguna sistem yang terlibat secara langsung dalam perlaksanaan polisi keselamatan ICT adalah :

i. Pentadbir IT (Pusat Teknologi Maklumat dan Komunikasi)
ii. Pengurus IT
iii. Pegawai IT UTM (HEP,Canseleri, Bendahari, Pendaftar dan Perpustakaan Sultanah Zanariah).

1.7 Faedah Projek

1.7.1 Faedah Untuk Pusat ICT, UTM

i) Pusat ICT akan menggunakan sistem Polisi Keselamatan ICT yang dibangunkan bagi melahirkan Polisi Keselamatan ICT yang bersesuaian dengan keperluan Universiti.

ii) Penggunaan sistem peralatan Polisi Keselamatan ICT akan mengurangkan masa persediaan dan penyediaan dokumen.

iii) Semua input domain yang diperkenalkan oleh piawaian ISO 27001 pada bulan oktober 2005 boleh ditambah ke dalam pangkalan data. Dengan itu pembangunan Polisi ICT akan menepati seperti yang digariskan oleh MAMPU dan piawaian ISO 27001.

1.7.2 Faedah kepada Pusat ICT, IPTA Secara Umum

i) Pembangunan peralatan Polisi Keselamatan ini secara menyeluruh boleh melahirkan Polisi Keselamatan ICT untuk IPTA yang lainnya.

ii) Kawalan-kawalan yang lainnya terhadap 11 kawalan domain (Sila lihat di Lampiran A), dalam jenis piawaian yang berbeza boleh dimasukkan ke dalam pangkalan data bagi memenuhi keperluan organisasi.

1.8 Ringkasan Bab

Pembangunan Sistem Polisi Keselamatan ICT ini mengambil kira keperluan organisasi dan juga peningkatan kompetensi mereka yang terlibat dengan pengurusan polisi. Pihak pengurusan organisasi di Pusat Teknologi Maklumat dan Komunikasi (CICT) Universiti Teknologi Malaysia, ingin memastikan semua aset dan segala yang berkaitan ICT mempunyai polisi keselamatan bagi menjamin UTM mempunyai dasar polisi keselamatan ICT kepada warganya.

Pembangunan sistem ini mengambilkira penggunaan teknologi berasaskan web bagi memudahkan maklumat dicapai dimana-mana lokasi tanpa mengira pelantar operasi sistem komputer yang digunakan. Ia juga diharap boleh dikembangkan dengan menambah ciri-ciri kaedah capaian dan memperincikan lagi proses dan langkah-langkah yang dilaksanakan.

RUJUKAN

1. ISMS and A Level ICT Through Diagrams. (2003), NISER.
2. Keselamatan Organisasi di Malaysia (2003), NISER.
3. UTM Web Trafik, https://www.traffic.jaring.my (2008), Jaring.
4. ISO/IEC FDIS 17799:2005. Information Technology – Secutity Techniques – Information security management systems – Requirements.
5. IT Security Promotion Committee Japan. (Julai, 2000). *Guidelines for IT Security.*
6. Monitor and Review (Plans, events, quality). (18 Mei 2006). ENISA – Risk Strategy.
7. ICT Securis Security Policy. (January 2006). SECURIS.
8. Shahrizan Othman, Lizawati, Suraya Miskon dan Syed Norris.(2006). Pembangunan Aplikasi Berasaskan Web.
9. Boston B, Greenspan, J, Wall, D (2004), *MySQL/PHP Database Applications, 2nd Ed.*, Wiley Publishing, Inc., Indianapolis.
10. Digital Crime and Forensic Science in Cyberspace (2002), Prentice-Hall, Englewood Cliffs, New Jersey.
11. Dennis, A., Wixom, B.H., Tegarden, D. (2005), *System Analysis and Design with UML Version 2.0, 2nd Ed.*, John Wiley & Sons, Inc.
12. Integration of ICT in Smart Organisations, Istvan Mezgar. (2006), Wrox Press.
13. Dennis, A., Wixom, B.H., Tegarden, D. (2005), *System Analysis and Design with UML Version 2.0, 2nd Ed.*, John Wiley & Sons, Inc.
14. Introduction to ITIL. (2005), Stationery Office Books.
15. Information and Communication Technology for Peace. (2005), Daniel Stauffacher *3rd Ed.*, Prentice-Hall Inc., Englewood Cliffs, New Jersey.
16. Terrorism and the International Business Environment (2004), *Gabriele G.S. Suder American Foreign Policy*(31)
17. Reaves, C.C. (1992), *Quantitative Research of Behavioral Sciences*, John Wiley & Sons, New York.
18. Ridruejo, D.L. (2002), *SAMS Teach Yourself Apache 2 in 24 Hours*, Sams Publishing, Indianapolis, Indiana.

19. Pekeliling Am Bil. 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat, MAMPU 2000.
20. Pekeliling Am Bil. 1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT), MAMPU, 2001.
21. Garispanduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS), MAMPU, Januari 2002.
22. Dasar Keselamatan ICT Versi 4.0, MAMPU, 30 Mac 2006.
23. ISO/IEC FDIS 27001:2005. Information Technology – Secutity Techniques – Information security management systems – Requirements.
24. ISO/IEC TR 13335-1:1996. GMITS – Concepts and models for IT Security.
25. ISO/IEC TR 13335-2:1997. GMITS – Managing and planning IT Security.
26. ISO/IEC TR 13335-3:1998. GMITS – Techniques for the management of IT Security.
27. ISO/IEC TR 13335-4:2000. GMITS – Selection of safeguards.