BULETTIN B.PERJASA

BULETIN PERSATUAN JURUANALISA SISTEM SEKTOR AWAM

PERCUMA UNTUK AHLI

BIL 1/2019

Topik Menarik

PERJASA

PERSATUAN JURUANALISA SISTEM SEKTOR AWAM MALAYSIA

Muka surat ini sengaja dibiarkan kosong

Isi Kandungan

Perutusan Presiden

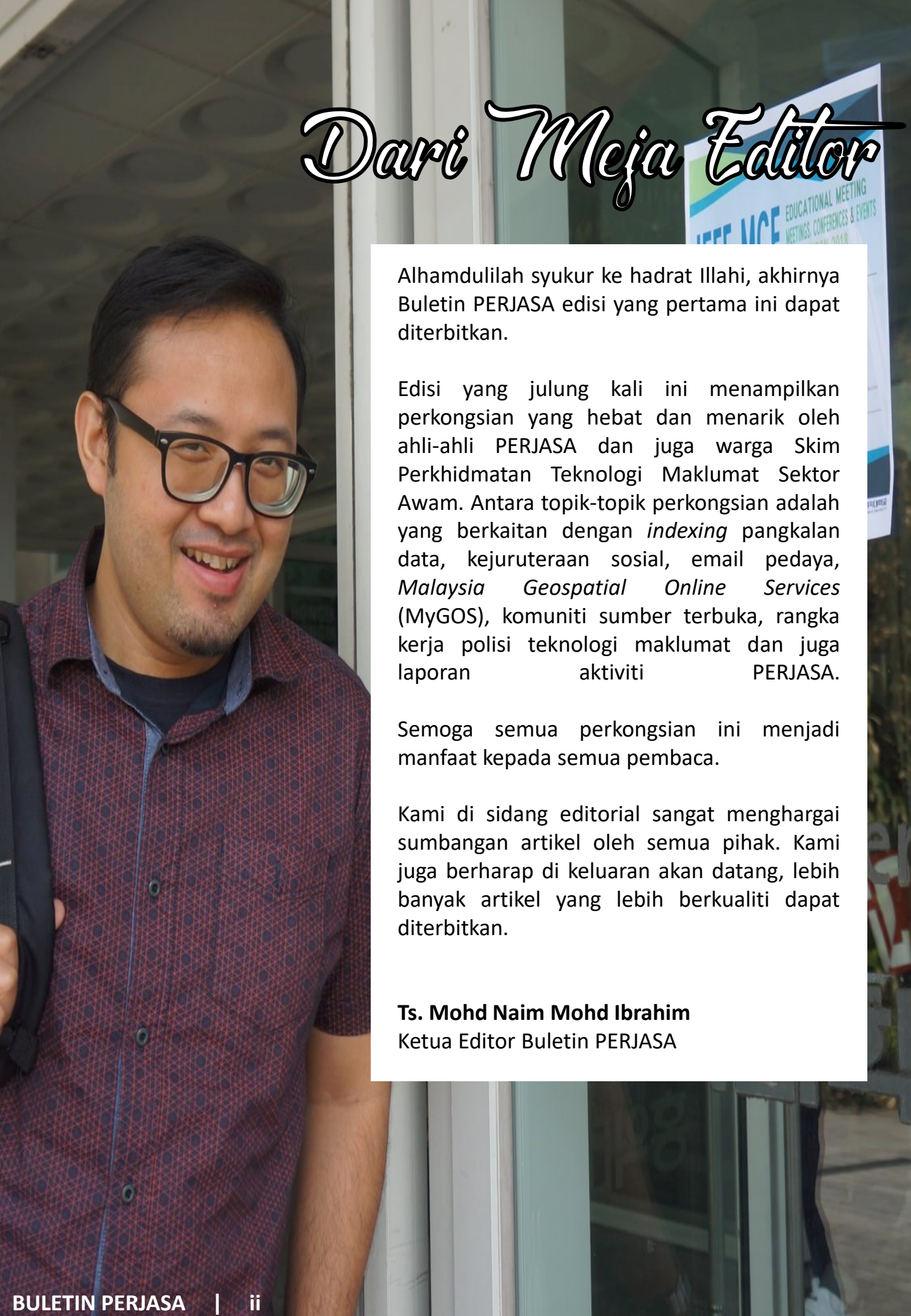
Dengan Nama Allah Yang Maha Pemurah Lagi Penyayang.

Saya bersyukur ke hadrat Ilahi di atas kelahiran semua Buletin PERJASA setelah kali terakhir PERJASA menerbitkan majalah adalah kira-kira 20 tahun yang lalu dengan nama JAS News.

Saya mengucapkan tahniah kepada barisan editorial dan juga ahli PERJASA yang sudi menyumbangkan artikel untuk B PERJASA ini. Saya berharap ia akan me wadah perkongsian ilmu dikalangan teknologi maklumat.

Di kesempatan ini juga, saya mengucapkan Selamat Menyambut Ramadan dan Selamat Menyambut Ai kepada semua umat Islam. Semoga beroleh kejayaan di dunia dan akhirat.

Ahmad bin Osman
Presiden PERJASA 2017-2019



Dari Meja Editor

Alhamdulilah syukur ke hadrat Illahi, akhirnya Buletin PERJASA edisi yang pertama ini dapat diterbitkan.

Edisi yang julung kali ini menampilkan perkongsian yang hebat dan menarik oleh ahli-ahli PERJASA dan juga warga Skim Perkhidmatan Teknologi Maklumat Sektor Awam. Antara topik-topik perkongsian adalah yang berkaitan dengan *indexing* pangkalan data, kejuruteraan sosial, email pedaya, *Malaysia Geospatial Online Services* (MyGOS), komuniti sumber terbuka, rangka kerja polisi teknologi maklumat dan juga laporan aktiviti PERJASA.

Semoga semua perkongsian ini menjadi manfaat kepada semua pembaca.

Kami di sidang editorial sangat menghargai sumbangan artikel oleh semua pihak. Kami juga berharap di keluaran akan datang, lebih banyak artikel yang lebih berkualiti dapat diterbitkan.

Ts. Mohd Naim Mohd Ibrahim
Ketua Editor Buletin PERJASA

Sidang Redaksi

Ketua Editor
Ts. Mohd Naim Mohd Ibrahim

Editor
Puan Felicia Chua Swee Suan
Puan Wan Amishah binti Wan Mahmud
Dr. Sheila Mahalingam
Ts. Adi Azlan bin Mohd Ali

Jawatankuasa PERJASA

Senarai AhliJawatankuasa Sesi 2017-2019
Pengerusi : Tuan Haji Ahmad bin Osman (MAMPU)
Timb Pengerusi : Dr. Nor'Ashikin binti Ujang (JPA)
Setiausaha : Puan Felicia Chua Swee Suan (MAMPU)
Penolong Setiausaha : Puan Razita binti Omar (JPA)
Bendahari : Cik Hazliana bt Talha (Bahagian Istiadat, JPM)
AJK :
Ts. Dr. Jayaletchumi T.S.Moorthy (INTAN)
Encik Luqman bin Subki (MKN)
Ts. Mohd Naim bin Mohd Ibrahim (KDN)
Ts. Adi Azlan bin Mohd Ali (JPA – Latihan)
Dr. Nur Azaliah binti Abu Bakar (MAMPU)
Ts. Mohamed Hairul bin Othman (JPA-Latihan)
Encik Razale bin Ibrahim (Jabatan Perangkaan)
Encik Mohd Safuan bin Elias (KPWKM)
Puan Wan Amishah binti Wan Mahmud (MAMPU)

Pemeriksa kira-kira:
Puan Mazilah binti Mohamad Amin (SWCorp)
Encik Hariadi bin Hinta (JPA)

Seminar PERJASA-Oracle: Unleashing Digital Transformation

Wan Amishah Binti Wan Mahmud
AJK PERJASA 2017-2019

Digital Transformation is no longer a question to Asia Pacific organizations. It has become a reality for all segments that are serious about staying relevant in the digital economy, including public sector. DX is a multiyear effort with specific goals and objectives, revenue growth, increase productivity and efficiency. Moreover DX involves a radical rethink of how to secure our data.

Not just about delighting customers with superior services and quality in real-time, governments agencies also need to become extremely agile and adaptable and ability to develop the right technological environment for continuous innovation.

PERJASA dengan kerjasama Oracle Malaysia telah mengadakan satu Seminar yang bertajuk Unleashing Digital Transformation. Objektif program adalah untuk berkongsi pengalaman pihak Oracle dalam perancangan dan melaksanakan transformasi digital.

Program telah dirasmikan oleh Presiden PERJASA iaitu Tuan Haji Ahmad bin Osman dan diadakan pada 22 November 2018 bermula dari 8.30 am hingga 4.00 pm, bertempat di Hotel Marriott, Putrajaya.

Seramai 104 ahli PERJASA telah menghadiri program berkenaan termasuk 8 orang wakil dari Kesatuan Penolong Pegawai Teknologi Maklumat dan Persatuan Juruteknik Komputer.

Dua (2) wakil PERJASA telah dijemput sebagai ahli Forum dan telah memberi pandangan mengenai transformasi digital dalam aspek modal insan dan ketersediaan struktur ICT Negara yang memerlukan anjakan paradigm semua pihak.

Seminar DevOps: Empowering Digital Services

Co-organized by PERJASA, KPPTM, CTSU & Microsoft Malaysia

Chua Swee Suan (Felicia),
PERJASA Secretary 2017-2019

Seminar DevOps: Empowering Digital Services has marked the first time ever successful collaborative event of The Association of Public Sector System Analysts (PERJASA), Assistant IT Officer Union (KPPTM) and Computer Technician Scheme Union (CTSU)! With the objective to upskill our members, we have invited our members and also Public Sector ICT personnel to join this seminar. Partnering as well with Microsoft Malaysia, this seminar was successfully held on 29 April 2019 at Pulse Grande Hotel Putrajaya with great support of 95 ICT personnel from various public sector agencies (75% attendance were the members of 3 association/union).

Time	Agenda
8.30am	Registration & Refreshments
9.00am	**Welcome Address** *By Encik Ahmad Osman, President, PERJASA*
9.15am	**Government Transformation Best Practice in Relation to IR4.0** *By Sherie Ng, Public Sector Lead, Microsoft APAC*
9.45am	**Microsoft DevOps Training Program** *By Christopher Lee, Business Group Lead, Cloud & Enterprise, Microsoft Malaysia*
10.15am	**Azure DevOps 101 + Case Study** *By Walter Wong, Founder of Gain Secure, Microsoft MVP*
12.00pm	Networking Lunch at Palm Hill Café
1.00pm	End of Event

Agenda of the seminar

What is DevOps?

DevOps (development and operations) is an enterprise software development phrase used to mean a type of agile relationship between development and IT operations.The DevOps ideals extend agile development practices by further streamlining the movement of software change thru the build, validate, and deploy and delivery stages, while empowering cross-functional teams with full ownership of software applications – from design thru production support.

Implementation of DevOps automation in the IT-organization is heavily dependent on tools, which are required to cover different areas of the systems development lifecycle (SDLC) such as Infrastructure as Code, Continuous Integration/ Deployment (CI/CD), Test Automation, Containerization, Orchestration, Software Deployment, Measurement and ChatOps.

Azure DevOps Bootcamps

Thus, while we had this seminar as the first step to introduce DevOps and now with Microsoft's enthusiasm to assist in our upskilling program, we are exciting to announce that there will be 3 Azure DevOps bootcamps to help accelerate your journey as DevOps practitioner coming soon in July – Sept 2019! Registration is open to PERJASA, KPPTM and CTSU members only. 50 members will be shortlisted and invited to the bootcamps and 3 commited participants will be chosen to attend 2 Microsoft Azure Developer training and certifications! Stay tuned for more update..

Pengenalan Kepada Indeks Pangkalan Data

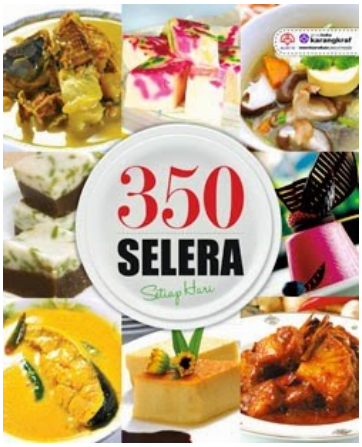
Ts. Mohd Naim Mohd Ibrahim
Kementerian Dalam Negeri

Saya telah beberapa kali dipanggil untuk membantu menyelesaikan masalah prestasi sistem aplikasi oleh Jabatan Pendaftaran Pertubuhan, Bahagian Pinjaman Perumahan Kementerian Kewangan, Jabatan Pertahanan Awam, Jabatan Sukarelawan (RELA) dan tempat saya berkhidmat sendiri. Kebanyakan masalah prestasi sistem yang saya temui adalah berpunca daripada masalah pangkalan data dan hampir 80% adalah berkaitan dengan indexing (okay, angka 80% tu saya main tembak je, tapi memang kebanyakkanya lah). Sebelum kita mempelajari bagaimana untuk membuat penalaan indeks (index tuning), mungkin ada baiknya kita mengenali dahulu apa itu indeks pangkalan data, kesan sekiranya tiada indeks dan apa pula natijahnya jika terlalu banyak indeks.

Mengikut Pusat Rujukan Persuratan Melayu @ DBP , indeks membawa maksud

Daftar kata penting menurut abjad berserta nombor halaman terdapatnya kata tersebut, biasanya diletakkan di bahagian akhir sesebuah buku; 2. senarai tajuk buku, nama pengarang dsb yg disusun secara sistematik pd kad di perpustakaan, faharasat, katalog;

Adakah anda pernah membaca buku ? Ya saya yakin anda tidak hanya membaca blog dan mukabuku (Facebook) sahaja, anda pastinya pernah membaca buku secara fizikal. Lazimnya buku (kecuali novel) mempunyai senarai isi kandungan di bahagian hadapan buku untuk menerangkan tajuk-tajuk utama. Itu boleh juga dianggap sebagai indeks. Indeks memudahkan kita untuk mencari tajuk yang kita ingin baca tanpa perlu membaca atau menyelak keseluruhan buku.



Dalam sesebuah buku resipi, pastinya ada banyak resipi masakan dimuatkan di dalamnya. Jika saya ingin memasak Ayam Masak Merah misalnya, saya perlu menyelak satu persatu helaian buku resipi tersebut sehingga saya jumpa Resipi Ayam Masak Merah sekiranya buku tersebut tidak mempunyai menu isi kandungan. Perbuatan menyelak satu persatu ini dalam pangkalan data dipanggil '*Full Table Scan*'. Ianya memakan masa yang lama dan sangat tidak efisian.

Sekiranya saya mempunyai pisang dan ingin menghasilkan suatu hidangan untuk minum petang, jika saya menyemak di ruangan isi kandungan sahaja, antara hidangan yang akan saya jumpa berdasarkan kata kunci 'pisang' adalah goreng pisang, pengat pisang, lepat pisang dan goreng pisang cheese. Tetapi saya pasti tertinggal cucur kodok yang juga boleh dihasilkan daripada pisang hanya kerana tiada perkataan 'pisang' dalam tajuk hidangan. Jadi untuk itu, saya perlu buat 'full table scan' semula kepada buku resipi saya untuk menyenaraikan semua hidangan yang boleh dihasilkan daripada pisang.

Alangkah mudahnya sekiranya saya mempunyai indeks hidangan berdasarkan bahan mentah. Sekiranya saya ingin memasak ayam, saya hanya perlu rujuk di indeks ini dibahagian ayam sahaja. Sekiranya saya ingin memasak hidangan yang berasaskan ikan, saya hanya perlu menyemak di ruangan ikan.

Tetapi bagaimana pula jika saya ingin melihat jenis hidangan sama ada ianya tradisional melayu, masakan cina, barat, india ataupun perancis ? Ya, mempunyai indeks jenis hidangan akan memudahkan kita mencari hidangan berdasarkan jenis atau negara asalnya seperti jadual dibawah.

Pendek kata, lebih banyak indeks, lebih mudah dan cepat carian kita, begitu jugalah dengan pangkalan data, mempunyai lebih banyak indeks, lebih mudah dan cepat carian dilakukan.

Bahan Mentah

Bahan Mentah	Masakan	Muka Surat
Ayam	Ayam Masak Merah	30
	Ayam Goreng Berempah	22
	Ayam Masak Tok	56
	Rendang Ayam	32
	Ayam Percik	12
	Ayam Bakar	64
	Sup Ayam	43
	Kari Ayam	52
Ikan	Ikan 3 Rasa	1
	Asam Pedas	6
	Ikan Bakar	65
	Rendang Ikan	32
	Laksa	65
Telur	Telur Dadar	2
	Telur Separuh Masak	9
	Kek	60

Jenis Masakan

Jenis Masakan	Masakan	Muka Surat
Tradisional Melayu	Ayam Masak Merah	34
	Asam Pedas	26
	Ayam Masak Tok	59
	Rendang Ayam	35
	Ayam Percik	15
	Ayam Bakar	67
	Rendang Ikan	46
	Laksa	55
Cina	Kek Bulan	4
	Yong Tau Foo	9
	Pau	68
	Kuetiaw Kungfu	35
	Mee Wantan	68
Barat	Spegeti	5
	Pizza	12
	Burger	63

> “Lebih banyak indeks, lebih mudah dan cepat carian kita, begitu jugalah dengan pangkalan data, mempunyai lebih banyak indeks, lebih mudah dan cepat carian dilakukan.”

Kesan Terlalu Banyak Indeks

Okay sekarang cuba bayangkan pula sekiranya kita mempunyai satu resipi yang baru yang kita ingin simpan dalam buku resipi kita. Selain daripada memasukkan resipi didalam buku, kita juga perlu mengemaskini isi kandungannya. Sekiranya saya mempunyai indeks bahan mentah, saya perlu mengemaskini indeks bahan mentah. Begitu juga dengan indeks jenis hidangan, negara asal, chef pencipta dan sebagainya.

Lebih banyak indeks, lebih leceh dan lama proses untuk memasukkan dan mengemaskini data baru. Begitulah halnya juga dengan pangkalan data, terlalu banyak indeks akan mempercepatkan carian, tetapi menyebabkan *insert* dan *update* menjadi perlahan.

Jadi bagaimana untuk membuat penalaan indeks ? Insyallah saya akan terangkan dalam edisi yang akan datang..

Apa Itu Kejuruteraan Sosial (*Social Engineering*)?

Muzamir bin Mokhtar
Kementerian Kewangan Malaysia

Kejuruteraan Sosial adalah kaedah memanipulasi psikologi serta tingkah laku manusia atau sekumpulan manusia dengan cara tertentu seperti kepercayaan dan emosi bagi membolehkan mereka memberikan maklumat sulit secara sukarela.

Contoh mudahnya, rakan sekerja kita minta kebenaran untuk akses PC sebab *Big Boss* minta hantarkan dokumen segera kepada dia. Kita pun memberikan kata laluan PC kita kepadanya. Secara automatik maklumat sulit kita sudah terdedah. Hati orang siapa yang tahu adakah rakan kita berniat baik atau sebaliknya. Kalau kata laluan itu boleh membuka akaun *online banking* kita juga? Bang! *Jackpot*!

Siapa yang popularkan istilah *social engineering*?

Kevin Mitnick ialah orang yang bertanggungjawab mempopularkan istilah Software Engineering ni melalui bukunya The Art Of Deception (2001).

Contoh kes berkaitan *social engineering*?

Berdasarkan sumber Ponemon Institute, Accenture pada tahun 2018, serangan siber yang paling banyak diterima oleh syarikat global adalah malware dan kedua sebanyak 68% adalah *Social Engineering*.

Pada tahun 2007, terdapat satu kes berlian bernilai 28 juta telah dicuri dari ABM AMRO Bank di Belgium oleh seorang lelaki dengan kaedah *Social Engineering* psikologi. Berbaik dengan staf bank dan seterusnya mengeluarkan berlian dari bilik kebal bank tersebut untuk tujuan mencuri.

Pada tahun 2013, akaun Twitter rasmi The Associated Press (AP) telah keluarkan tweet yang hampir menjatuhkan ekonomi dunia. Sekumpulan pengodam bernama Syrian Electronic Army telah mengambil alih akaun Twitter rasmi AP dan menghantar ciapan mengatakan White House di bom dan Presiden Barrack Obama cedera.
Pasaran Dow Jones terus menjunam. Kaedah ini menggunakan *Social Engineering* melalui *Phishing Email*.

Pada tahun 2016, hampir 20,000 data personel FBI dicuri melalui Department Of Justice (DOJ) US. Kaedahnya adalah godam e-mel staff DOJ, menyamar sebagai IT Helpdesk untuk akses Internal Portal. Seterusnya dapat akses kepada server berkenaan yang boleh akses server data personel FBI.

Adakah eknik social engineering perlukan *tools* yang hebat?

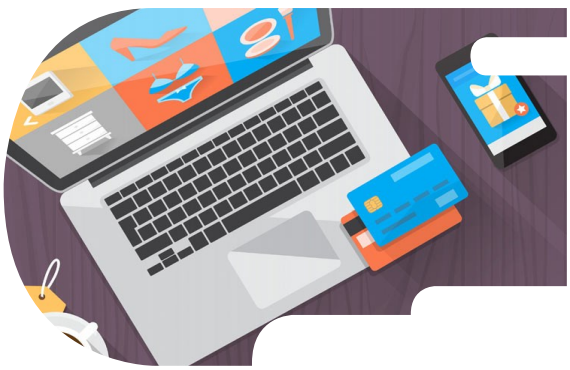
Teknik ini tidak memerlukan tools yang hebat, cukup sekadar seseorang pengodam itu pandai bermain emosi dan psikologi mangsa. Kira macam pandai jual minyak lah ibaratnya. Tak perlu berbelanja besar untuk menipu mangsa. Beli nombor telefon *prepaid*, pengodam menghubungi mangsa dengan samaran seterusnya mendapatkan apa yang diperlukan. Namun ia bukan boleh diperoleh dalam masa singkat jadi pengamal *Social Engineering* ni seorang yang sangat penyabar juga.

Teknik Social Engineering

1. In –Person : Contoh : Tinggalkan *Thumb Drive* di tempat terbuka di pejabat. Pasti sifat ingin tahu siapa punya dan apa didalamnya ada pada sesiapa yang jumpa. Apabila dia akses di PC Pejabat, mungkin *malware / trojan* dah ditanam dalam PC dan seterusnya maklumat sulit tersebar kepada pemilik Thumb Drive tersebut.

2. Phone : Contoh : Pemanggil hubungi Operator Telco dengan menyamar sebagai seorang isteri sedang dalam kesusahan dan perlu dapatkan akses akaun online nombor suaminya (mangsa). Buat bunyi anak menangis sebagai latar belakang untuk tunjukkan kesusahannya dan sifat kesian operator akan berikan maklumat tersebut.

3. Digital : Contoh : Daftar alamat domain yang hampiri domain popular. Domain maybank2u.com.my pada pandangan org mungkin sama dengan rnaybank2u.com.my.



Bagaimana untuk elakkan diri dari menjadi mangsa kejuruteraan sosial ?

1. Sentiasa bersifat ingin tahu dan waspada macam detektif conan;
2. Fikir panjang sebelum teruskan urusan bersifat peribadi atau sulit;
3. Kurangkan guna Free Survey dan Games di Media Sosial; dan
4. Hati-hatilah berkongsi maklumat peribadi di Media Sosial. Janganlah telanjangkan semuanya peribadi anda. Simpanlah sikit.

Bila bermulanya *Social Engineering* di Malaysia?

Cuba tengok semula filem P.Ramlee bertajuk Ali Baba Bujang tahun 1961. Sungguh bijak si Ali Baba (Aziz Sattar) menyamar sebagai wartawan untuk tagih kepercayaan secara bertanyakan pada Ketua Penyamun (P.Ramlee) untuk dapatkan kata laluan buka dan tutup pintu gua menyimpan harta rompakan si penyamun. Itu kes pertama di Malaysia agaknya.

.

Langkah Demi Langkah

Menyediakan Email Perdaya (Emails Spoofing) Menggunakan Kali Linux Distro

Nasir bin Ismail
Institut Tanah dan Ukur Negara (INSTUN)

Email Spoofing

"Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation." https://searchsecurity.techtarget.com/definition/email-spoofing

Langkah 1

Mendaftar Akaun SMTP2GO Secara Percuma dan Terhad

https://www.smtp2go.com/signup-ty/#

Contoh email address account yang akan digunakan untuk mendaftar secara percuma – FREE.

Full Name : Peserta Kursus TM
Work Email : pesertakursustm@yahoo.com
Password : ridzam@$12345TM!

Activate your SMTP2GO account melalui email yang didaftarkan.

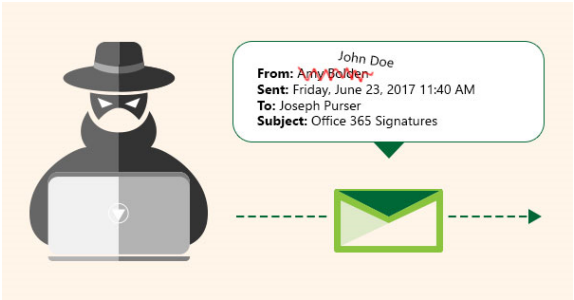
Pemeriksaan username, SMTP server port dan SMTP port number untuk kesahihah.

Contohnya:

SMTP Server: mail.smtp2go.com
Username: nasir@instun.gov.my
SMTP Port: 2525

Contoh :

Mendaftar tambahan akaun 'Mukhlis' dengan SMTP2GO – Free.



Langkah 2

Setup your SMTP Username

1. SMTP Username
2. SMTP Password

Simpan untuk rekod dan kegunaan semasa menjalankan kerja-kerja email spoofing.

SMTP Password : 9XYnGOfytN7aX8a

Pemeriksaan username, SMTP server port dan SMTP port number untuk kesahihah.

Contohnya:

SMTP Server: mail.smtp2go.com
Username: nasir@instun.gov.my
SMTP Port: 2525

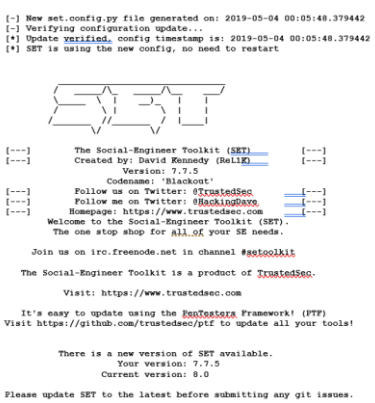
Contoh :

Mendaftar tambahan akaun 'Mukhlis' dengan SMTP2GO – Free.

Langkah 3

Menggunakan The Social-Engineering Toolkit (SET) Kali Linux untuk menjalankan kerja-kerja Email Perdaya / Email Samaran (Email Spoofing).

[-] New set.config.py file generated on: 2019-05-04 00:05:48.379442
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2019-05-04 00:05:48.379442
[*] SET is using the new config, no need to



Installasi SET Toolkit – GitHUB

#cd /root
#git clone https://github.com/trustedsec/social-engineer-toolkit.git

#cd /root/social-engineer-toolkit
#pip install –r requirements.txt

Langkah 4

Langkah demi langkah untuk menjalankan kerja-kerja Spoofed Email bagi tujuan pembelajaran dan pengajaran.

#setoolkit

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

Select from the menu:

1) Social-Engineering Attacks

Select from the menu:

5) Mass Mailer Attack

.

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address

set:phishing> Send email to:pesertakursustm@yahoo.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>

2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):info@duit.com
set:phishing> The FROM NAME the user will see:Syarikat TULUS IKHLAS Sdn Bhd
set:phishing> Username for open-relay [blank]:nasir@instun.gov.my
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):mail.smtp2go.com
set:phishing> Port number for the SMTP server [25]:2525
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
set:phishing> Email subject:Email Promosi Merdeka 2019
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Promosi Merdeka 2019 - Gadget Terkini
Next line of the body: END
[*] SET has finished sending the emails

Press <return> to continue

Langkah 5

Memeriksa DOMAIN yang hanya sah (valid) tersedia bagi digunakan sebagai pengantara.
https://instantdomainsearch.com/#search=dunia

Contohnya Domain Name yang boleh digunakan:
dunia.com, hayat.com, hayat.app, duit.com, duit.my

Langkah 6

Pemeriksaan Email Perdaya / Email Samaran / Email Palsu yang digunakan telah diterima oleh penerima didalam peti email mangsa masing-masing.
Contohnya : MS Exchange Server

Received: from INSTUN-MBX-01.instun.gov.my (10.137.81.72) by
INSTUN-MBX-01.instun.gov.my (10.137.81.72) with Microsoft SMTP Server (TLS)
id 15.0.712.22 via Mailbox Transport; Fri, 3 May 2019 15:34:39 +0800
Received: from mail.instun.gov.my (10.137.81.62) by
INSTUN-MBX-01.instun.gov.my (10.137.81.72) with Microsoft SMTP Server id
15.0.712.22; Fri, 3 May 2019 15:34:32 +0800
Authentication-Results: mail.instun.gov.my
header.from=tulus@kita.com; domainkeys=neutral (no sig)
Authentication-Results: mail.instun.gov.my
header.from=tulus; dkim=pass (Success)
Received: from a2i809.smtp2go.com (a2i809.smtp2go.com [103.47.207.41])

Langkah 6a

Contoh percubaan menyediakan Spoofed Email dengan menggunakan Domain: hayat.app kepada akaun pesertakursustm@yahoo.com

.

X-Apparently-To: pesertakursustm@yahoo.com; Fri, 03 May 2019 07:45:23 +0000
Return-Path: <kita@hayat.app>
Received-SPF: none (domain of hayat.app does not designate permitted sender hosts)
X-YMailISG: VJzIUK0WLDuYVxj3Yaa1i.gwS3pLTwVG9ug7Env1JPMRsbyT
bsCV.Csk0PvEWE5KwBab33QTZEfumB7kc_dzoZsPV.YPTREagr9S0vb_utbJ
GfYNClYqvOKTABoFsH3JA1CbV46gIi91Xqs_uNy995OVg3C62sbR3xB1gVLL

9UwFvj009yb5FH5SlT8jO4EFansMyNGCyFdZVvZ9matd1W9Vb90_R1F.GNY0
2HPMzgQcSRJKw0wnoqczUiQLlANkzQrMUSRscRqIZkwq7gNrLbJykss5Oveu
MbdTFbkftd_.4n9VDpTrKxN6Spp8uk4FrLy7PVLR2qqXTQ8sw7odlIlHJI1n
fo9y3XZkwmiu_1qqgnsIDf0KRwzAly4kwagK2Z1altdON.K7fJjQc5lcN0mB
R4Dr6IJtaOd9euLtUY0iLg4RLo42CNziuPnIyRXZ4glshKPfdpapSKPNbpf.
P75KnPnBFlhGk69uaTg8nXUKjoiYLdCgxXKeLNSfFolfIAZVjR5ctQxv.2bN
BaWW7XUdH6ljrHRrjQt8gG8tkBP.2fFX6VaUCJLYmGgnHcbtPeluxNpqxoxJ
w29r5t3jaGRaC.k0kLLYLJPH1SUbKH2584cLThNrclfvW01zHyidqicsY1wl
a2NtVzxV9uFsLqIBXlyvFKoi8Q19jTMRmkz8gl39J1Y.XHOE1CAfY1saDZPP
0MfJzh39pHx5GySCWyDj7pnpVhPKmb5bKi7DpdIF9vtkkMIl6IVQrCKmwAiR
9ispwSCiDiCpZpYXptXfO7VcSDiwNKTCvpUu6foYA2HxtNzVTktXw0f12F56
0Rwy.93i6is6obmeJ2V5t0ukcp5bnAMtIZLQ.eVmqGy_o7N6HT4fO8asXGxw
6aYSP0e.Yvapx845VOQw7JDClLzRzrjs9BmNw7aCLZUC.w6m2Htei1M35dEQ
8qqsF6RlhfUciVGqCtnPqpz8g3bjwhzNlSD87Ira98ecF.aLPJYyBtcaiE.Q
hM6toBuYNHwLSZs26R9jXVZWsXcEJ4c-
X-Originating-IP: [103.47.207.41]
Authentication-Results: mta4406.mail.gq1.yahoo.com
header.i=@smtpservice.net; header.s=me4k30.a1-4.dyn; dkim=pass (ok)
Received: from 10.253.33.220 (EHLO a2i809.smtp2go.com) (103.47.207.41)
by mta4406.mail.gq1.yahoo.com with SMTPS; Fri, 03 May 2019 07:45:22 +0000
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
d=smtpservice.net; s=me4k30.a1-4.dyn; x=1556870422; h=Feedback-ID:
X-Smtpcorp-Track:Date:Message-Id:Subject:To:From:Reply-To:Sender:
List-Unsubscribe;
bh=Oa8BqlRUITr1bn74jiX3TeGxkr/RKfIuNfQBPPJu2FA=; b=TngRZqIc
7Eim6SoU0XLyveYGoPUQSdecrzgePCg2YRO16GzFHNTA1LycNSwm85heorUtGj6nUu8pYgDW0z5yL
NxFaJZ09HReczKY4B3wKkHVbaeHPSH7yGLhU2aMUkoF3AhRKBtaBypwocGCfAPLNTQ3rmmvW8hJkl
hMpvURgy/LCgzPrRwGcvGb+eR/Q75saZ913H4a/fdVyef32YocrfQVWhrOyY9TAvZDcSevbzJ29Wo
yn1MptCRIqLob3/EtKbenud2re6kfDXr7wfi/5GSj70h2lU9FpB8aIDKaw93e7WhkGuGF2ShSwzl9
8y8ill+c0WkFCkYMDkeeb6/8fw==;
Received: from [10.139.162.187] (helo=SmtpCorp)
by smtpcorp.com with esmtpsa (TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256)
(Exim 4.91)
(envelope-from <kita@hayat.app>)
id 1hMSsj-SH4fR3-UL
for pesertakursustm@yahoo.com; Fri, 03 May 2019 07:45:21 +0000
Received: from [10.202.60.56] (helo=[10.127.0.1])
by smtpcorp.com with esmtpsa (TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256)
(Exim 4.91)
(envelope-from <kita@hayat.app>)
id 1hMSsi-4XaA9W-DB
for pesertakursustm@yahoo.com; Fri, 03 May 2019 07:45:20 +0000
Content-Type: multipart/mixed; boundary="===============4773641122462292029==“

Received-SPF: temperror (google.com: error in processing during lookup of guest@duit.my: DNS error) client-ip=103.47.207.41;
Authentication-Results: mx.google.com;

Langkah 7

Memeriksa sumber asal dan alamat email penghantar menggunakan beberapa laman web percuma.

https://infotracer.com

Uncover Hidden Information About Email Address

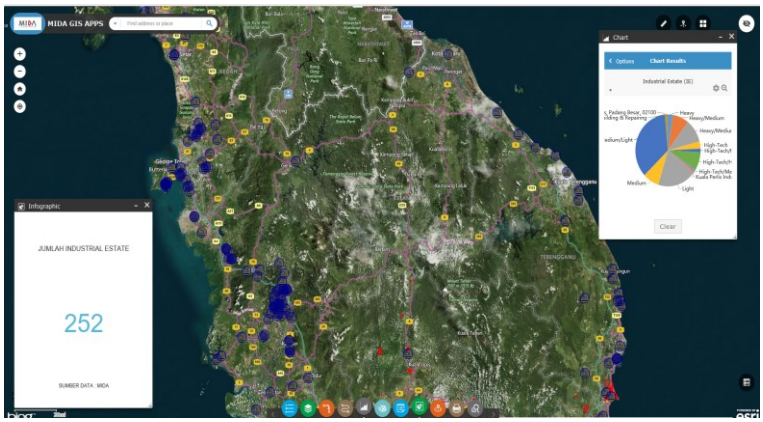
Domain: dunia.com

- Data Breaches: CLICK HERE
- IP Address: 74.125.141.27
- Social Profiles: CLICK HERE
- Email Service Provider: Google
- Report Update: 05/04/2019
- Full Report: CLICK HERE

Selamat mencuba bagi meningkatkan ilmu pengetahuan dan menambah kefahaman sediada. Wallahualam.

Perkongsian maklumat Geospatial Melalui Platform Malaysia Geospatial Online Services (MyGOS)

Nor Hayati Binti Abdullah
Pusat Infrastruktur Data Geospatial Negara (MaCGDI)



Aplikasi MIDA GIS

Pusat Infrastruktur Data Geospatial Negara / Malaysian Centre for Geospatial Data Infrastucture (MaCGDI), Kementerian Air, Tanah dan Sumber Asli (KATS) telah dipertanggungjawabkan dalam mengurus Program MyGDI. MyGDI merupakan program nasional inisiatif kerajaan bagi menyediakan infrastruktur perkongsian maklumat geospatial ke arah meningkatkan kesedaran mengenai kepentingan kegunaan data/maklumat geospatial dalam pembangunan negara. Melalui program MyGDI, MaCGDI telah mengambil inisiatif dalam membangunkan Geospatial Data Centre (GDC) bagi perkongsian data dan pelbagai aplikasi GIS.

Artikel ini akan menerangkan perkongsian maklumat geospatial melalui platform MyGOS yang berkonsepkan perkongsian map servis collect once use by many. Pengemaskinian data boleh dibuat secara atas talian dalam persekitaran yang selamat.

Pengenalan Malaysia Geospatial Online Services (MyGOS)

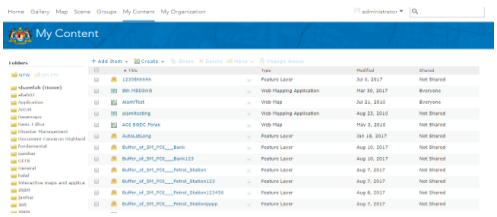
Portal Malaysia Geospatial Online Services (MyGOS) www.mygeoportal.gov.my/mygos merupakan satu platform perkongsian maklumat geospatial bagi Agensi Kerajaan secara atas talian yang membolehkan perkongsian maklumat dilakukan tanpa perpindahan data secara fizikal dalam persekitaran selamat.

Tujuan utama dibangunkan adalah :

- Platform perkongsian dan penggunaan maklumat geospatial antara sektor awam secara atas talian dalam persekitaran yang selamat.
- Membolehkan pengguna yang tiada pengetahuan Geospatial Information System (GIS) menggunakan maklumat geospatial dengan mudah tanpa memerlukan perisian Desktop GIS.
- Untuk membantu agensi kerajaan yang tiada kemudahan infrastruktur seperti perisian dan perkakasan GIS.
- Penjimatan kos perolehan perkakasan dan perisian GIS oleh agensi-agensi yang ingin membangunkan projek GIS.
- Penjimatan kos pembangunan aplikasi GIS.
- Penjimatan kos pengutipan data-data yang diperlukan dalam sesuatu projek pembangunan aplikasi.

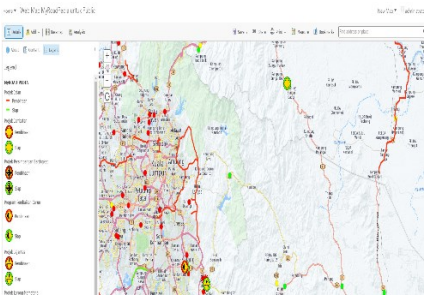
Kelebihan Fungsi-fungsi dalam MyGOS

Pengurusan Dokumen



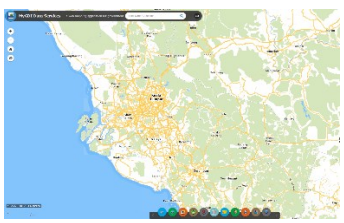
Pengguna boleh menguruskan dokumen terhad, sulit atau umum secara tersusun dengan menggunakan fungsi 'My Content'. Format dokumen yang boleh dimasukkan adalah seperti .pdf, .jpg dan lain - lain. Dengan fungsi ini, pengguna boleh berkongsi dokumen secara atas talian dan selamat

Web Map



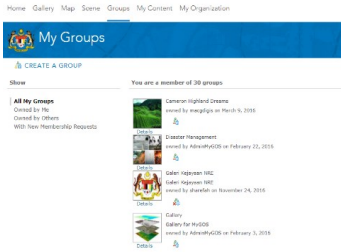
Memudahkan pengguna untuk membuat pemetaan dengan pantas secara atas talian. Pengguna turut boleh merekabentuk peta tersebut dengan kreativiti dan penampilan yang menarik seperti menukar saiz / icon symbology, membuat labels dan lain - lain

Pembangunan Aplikasi GIS



Pengguna yang tidak mempunyai latarbelakang GIS boleh membangunkan aplikasi GIS dengan cara yang mudah dimana terdapat pelbagai widget mengikut kesesuaian

Perkongsian Maklumat

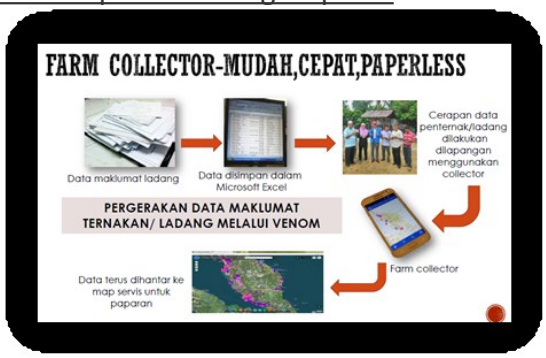


Maklumat yang hendak dikongsi boleh ditentukan menggunakan fungsi groups.

Storymap

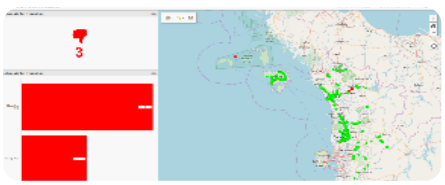
Pengguna dapat membangunkan storymap dengan membuat penceritaan mengenai sesuatu kronologi kejadian atau tempat / lokasi yang menarik. Storymap ini adalah paparan interaktif yang mempunyai peta serta maklumat asas mengenai penceritaan

Mencerap maklumat geospatial



Pengguna boleh mencerap maklumat geospatial melalui smartphones secara offline atau online dengan mengunakan fungsi 'Collector for ArcGIS

Dashboard



Pengguna dapat memaparkan hasil analisis yang interaktif untuk dibentangkan kepada pengurusan atasan.

Kolaborasi Bersama Agensi Kerajaan

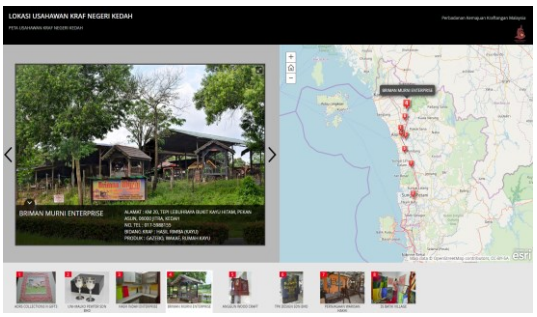
MaCGDI telah mula berkolaborasi dengan pelbagai Agensi Kerajaan melalui platform MyGOS sejak tahun 2013. Bagi kolaborasi ini, terlebih dahulu agensi perlu melalui proses khidmat runding bagi mengenalpasti keperluan agensi tersebut. Setelah persetujuan dicapai, proses seterusnya adalah menyediakan Dokumen Permulaan Projek bagi menentukan skop aplikasi dan data-data GIS yang diperlukan bagi pembangunan aplikasi. Skop membangunkan aplikasi dan data perlu disahkan oleh Pengurusan Atasan. Agensi akan diberi userid selepas penyerahan system bagi capaian kepada aplikasi MyGOS bagi tujuan persekitaran yang selamat.

Ini merupakan salah satu inisiatif dari MaCGDI dalam program transformasi awam untuk merealisasikan pelaksanaan dan perkongsian maklumat geospatial secara kolaborasi strategik. Sehingga kini, terdapat tujuh puluh lima (75) Agensi Kerajaan yang telah menggunakan perkhidmatan MyGOS dalam Pembangunan dan Pelaksanaan GIS di Agensi masing-masing. Jadual 1 menunjukkan status terkini maklumat projek Agensi Kerajaan yang telah menggunakan perkhidmatan MyGOS secara aktif

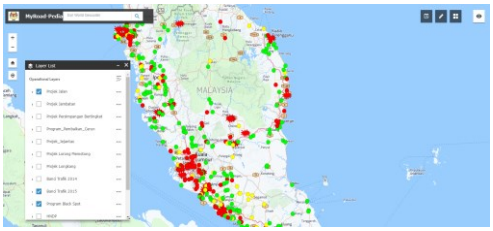
Melalui perkhidmatan MyGOS, Agensi telah dapat mengemaskini dan mengakses maklumat geospatial secara atas talian dan real – time serta membantu dalam membuat keputusan, merangka strategi serta menganalisis maklumat dengan cepat dan tepat. Perkongsian maklumat geospatial adalah gabungan strategik yang membawa faedah sinergi kepada semua agensi yang terlibat. Ini membolehkan integrasi data dilakukan untuk manfaat semua dan bukan terhad kepada kepentingan sesuatu agensi sahaja.

Jabatan/Agensi	Maklumat Projek
Kementerian Pendidikan Tinggi	Projek Pemetaan IPTA, IPTS
Kementerian Pembangunan Luar Bandar (KPLB)	Projek Maklumat Geospatial Luar Bandar
Kementerian Kerja Raya	MyRoad-Pedia
Kementerian Tenaga, Teknologi Hijau dan Air (KeTTHA)	Projek Maklumat Geospatial Loji Rawatan Air dan Empangan
Angkatan Pertahanan Awam Malaysia	Projek GIS APM
Agensi Penguatkuasaan Maritim Malaysia	Projek Maklumat Geospatial APMM
NADI, ICU	Projek Pemetaan Sekolah Dhaif
Pusat Zakat Melaka	Projek Pemetaan Lokasi Prospek Zakat Melaka
Pusat Hidrografi Nasional	Projek Maklumat Geospatial Marin SDI
Lembaga Getah Malaysia	Projek Maklumat Geospatial Ladang Getah
Halal Industry Development Corporation	Projek Pemetaan Halal Hab dan Restoran Halal
Jabatan Kerja Raya Malaysia Caw. Senggara Fasiliti Jalan	Projek Monitoring Potholes
Jabatan Kerja Raya Malaysia Caw. Kejuteraan Geoteknik	Projek Monitoring Boreholes
Jabatan Penilaian Dan Perkhidmatan Harta	Lokasi Rumah Mampu Milik
Lembaga Pembangunan Pelaburan Malaysia (MIDA)	Projek Lokasi Industri Estate
Lembaga Kemajuan wilayah Kedah (KEDA)	Projek GIS KEDA
Jabatan Perkhidmatan Awam	PesaraFindMe (Lokasi Pesara)
Perbadanan Kemajuan Kraftangan Malaysia	Lokasi Produk Kraftangan
Jabatan Warisan Negara	Lokasi tapak warisan dan warisan Kebangsaan
Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna (KPDNHEP)	Lokasi Stesen Minyak, Pasaraya ,
Majlis Bandaraya Alor Setar	Pemantauan Lokasi Pembayaran Cukai Pintu

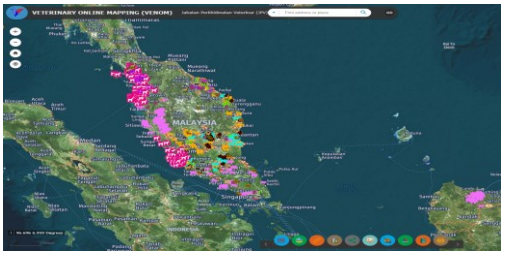
Pembangunan Aplikasi GIS di Agensi melalui platform MyGOS



Storymap Lokasi Usahawan Kraf



Storymap Lokasi Usahawan Kraf



Veterinary Online Mapping (VENOM)

Penjimatan Kos Kerajaan

Setiap agensi yang ingin membangunkan aplikasi dan memproses data GIS memerlukan kos perolehan yang tinggi seperti kos perkakasan, kos perisian dan sumber manusia. Bagi penggunaan MyGOS agensi hanya perlu berkolaborasi dengan MaCGDI dan tidak lagi perlu membuat perolehan yang mana menjimatkan kos kerajaan. Jadual 1 dan jadual 2 menunjukkan anggaran kos yang terlibat sekiranya Agensi ingin membangunkan projek GIS.

Activities	Frequency (kali setahun)	Cost/ Business (kos 1 agensi)	# of businesses (bil. Agensi)	Total (RM)
Perkakasan				
Application Server – MyGOS	-	30,000	8	240,000
Database server	-	35,000	8	280,000
Map service server - Federated MyGOS	-	40,000	8	320,000
Perisian				
ArcGIS Server Enterprise Advance 10.4 (4 core)	-	320,000	8	2,560,000
ArcGIS Desktop 10.5.1 Advance	-	120,000	8	960,000
Microsoft SQL Server Enterprise 2012	-	40,000	8	320,000
MyGOS				
Named User (3*RM5000)	-	15,000	8	120,000
	JUMLAH	600,000		4,800,000

Kos Perolehan Infrastruktur ICT oleh Agensi Secara *Outsource*

Activities	Hours needed	Cost per hour	Frequency (kali setahun)	Cost/ Business (kos 1 agensi)	# of businesses	Total (RM)
Kajian Keperluan Pengguna	240	60	1	14,400.00	8	115,200.00
Pemprosesan data	160	20	1	3,200.00	8	25,600.00
Pembangunan Aplikasi	640	80	1	51,200.00	8	409,600.00
Latihan	64	80	1	5,120.00	8	40,960.00
Pengujian (UAT, FAT & Stress Test)	120	60	1	7,200.00	8	57,600.00
Dokumentasi (URS, SRS, Manual, Laporan Pengujian)	160	60	1	9,600.00	8	76,800.00
Serahan	8	20	1	160.00	8	1,280.00
			JUMLAH	90,880.00		727,040.00

Kos Pembangunan Aplikasi yang Dibangunkan oleh Agensi Secara *Outsource*

Anggaran kos penjimatan hasil tidak dituntut bagi tahun 2014 hingga Mac 2019

mygos bersama KPDNHEP

Penutup

Impak dari projek kolaborasi ini adalah penjimatan kos kepada Kerajaan dimana Agensi hanya menggunakan infra yang dibekalkan oleh MaCGDI. Melalui penggunaan platform MyGOS, Agensi boleh membuat perkongsian data, menganalisa data secara spatial, tambah nilai data dari pelbagai Agensi serta dapat merancang dan membuat keputusan dengan cepat dan tepat.

Lawatan Inspektorat MyGOS ke Agensi Penguatkuasaan Maritim Malaysia (APMM)

Bengkel keperluan pengguna bersama Jabatan Warisan Negara

Hala Tuju Komuniti Sumber Terbuka Sektor Awam

Khairul Ashraf bin Basul Hak
Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)

Perisian sumber terbuka boleh ditakrifkan sebagai perisian yang mana kod sumbernya didedahkan kepada umum, dibenarkan untuk diubah, dikongsi dan diedarkan semula. Perisian ini biasanya dibangunkan dan disenggara oleh para penggiat dari kalangan individu atau organisasi yang dikenali sebagai komuniti sumber terbuka. Kebiasaannya pembangunan dan perubahan pada perisian ini adalah lebih pantas kerana melibatkan sumbangan dan kolaborasi banyak pihak.

Berbeza dengan perisian sumber tertutup atau proprietary, perisian jenis ini dimiliki oleh syarikat pengeluar yang melindungi hak cipta perisiannya, berorientasikan keuntungan dan disokong oleh kepakaran dalaman syarikat berkenaan. Pembangunan dan perubahan perisian proprietary biasanya lebih perlahan kerana melibatkan sumber dalaman yang mungkin terbatas dan wajib melalui siri jaminan kualiti sebelum diedarkan kepada pengguna umum.

Tidak kurang juga syarikat pembangun perisian yang menerajui produk perisian secara sumber terbuka kerana melihat kepada beberapa kelebihan utama iaitu sumber tenaga pengaturcara ramai dari kalangan komuniti dengan kos yang minima di samping tempoh pembangunan dan perubahan yang pantas. Produk seperti ini apabila telah matang akan diedarkan sebagai versi sumber terbuka dan syarikat pengasasnya mungkin menawarkan perkhidmatan sokongan berbayar dengan perisian pelengkap lain sebagai nilai tambah.

Kelebihan Komuniti Sumber Terbuka

Terlibat dalam komuniti sumber terbuka memberikan banyak kelebihan. Kelebihan yang paling ketara ialah peluang meningkatkan keupayaan dan kemahiran dalam teknologi berasaskan sumber terbuka.

. Teknologi baru yang diperkenalkan memerlukan sokongan daripada komuniti untuk membuat penilaian berterusan dan bersama-sama menyumbang dalam mengemaskini kekurangan atau pepijat yang ada. Kemahiran yang berbeza diperlukan dan individu yang memiliki kemahiran ini boleh mengaplikasikannya secara bebas dalam projek sumber terbuka.

Walaupun komuniti sumber terbuka kebiasaannya bekerja secara sukarela, manfaat yang diperolehi ialah kredibiliti penggiat komuniti akan meningkat apabila tersenarai dalam pasukan pembangunan produk-produk yang akhirnya digunakan di seluruh dunia. Ini merupakan satu bentuk pengiktirafan kepada kepakaran yang dimiliki dan akan menjadi aset kepada kemajuan kerjaya pada masa akan datang.

Selain itu, komuniti yang aktif dalam pembangunan dan pengemaskinian versi perisian sumber terbuka akan bebas untuk memasarkan perkhidmatan mereka kepada pengguna yang telah pun menggunapakai produk dan perisian berkenaan. Kelebihan ini lebih ketara apabila produk yang dibangunkan semakin matang dan semakin mendapat tempat dalam pasaran. Lebih daripada itu, produk berkenaan juga boleh dibangunkan secara berasingan dengan membentuk komuniti lain dengan hala tuju dan perancangan yang berbeza sehingga seterusnya memperkayakan pasaran dengan pilihan produk yang pelbagai.

Komuniti Sektor Awam

Melihat kepada kelebihan pembangunan perisian berasaskan sumber terbuka, timbul persoalan kepada kita iaitu bagaimana konsep sedemikian dapat diaplikasikan dalam pembangunan sistem aplikasi sektor awam. Berdasarkan realiti hari ini, setiap agensi menggunakan banyak sumber dari sudut tenaga kerja, masa dan kewangan dalam membangunan sesebuah aplikasi dalaman. Agensi pusat seperti MAMPU dan JPA dilihat semakin aktif membangunkan perisian generik yang boleh digunakan secara guna sama seperti aplikasi MyMesyuarat, DDMS, HRMIS dan lain-lain. Namun pembangunan secara berasingan ini memakan masa yang panjang di samping kos yang tinggi apabila melibatkan banyak tenaga kerja dalaman dan konsultasi pihak luar.

Adalah menjadi satu pencapaian yang besar kepada kakitangan awam jika pendekatan pembangunan sistem aplikasi dapat direvolusikan dengan menggembleng kepakaran dalaman yang ada dalam perkhidmatan awam merentas tanggungjawab hakiki kepada agensi masing-masing sebagai satu komuniti. Ini akan lebih bermakna jika impaknya kelak menjimatkan banyak sumber seperti masa dan kewangan serta dalam masa yang sama meningkatkan kepakaran dan keupayaan teknikal kakitangan awam. MAMPU sejak tahun 2004 telah memperkenalkan Pelan Induk Perisian Sumber Terbuka Sektor Awam dan sehingga kini usaha menggiatkan penggunaan perisian sumber terbuka ini diteruskan dalam Program Pembangunan Perisian Sumber Terbuka dan Kapabiliti Sektor Awam (OSDeC) melalui siri latihan, perkhidmatan coaching dan penyediaan prasarana.

Namun demikian, perkara yang lebih penting untuk membangunkan komuniti sumber terbuka sektor awam ialah tah dan kepakaran yang dimiliki ol awam umumnya dan khusus daripada skim perkhidmata maklumat. Sejauh mana k mencapai tahap yang boleh dige pendekatan kolaborasi dalam aplikasi dengan konsep kom terbuka.

Lebih daripada itu, apakah model pembangunan yang paling sesuai untuk diterapkan bagi memastikan pendekatan ini benar-benar mencapai hasrat yang diinginkan iaitu menghasilkan produk sistem aplikasi sumber terbuka yang matang. Dalam masa yang sama juga, pendekatan ini perlu mengekalkan prinsip sumber terbuka dari sudut keterbukaan kod sumber, kolaborasi komuniti dalam pembangunan serta jaminan kualiti, kebebasan untuk pembangunan berasingan dan pengemaskinian produk yang lebih pantas.

Peranan Ahli Komuniti

Komuniti yang kukuh memerlukan komitmen yang padu daripada ahlinya. Komuniti sumber terbuka sektor awam memerlukan peneraju yang mampu memberikan hala tuju yang jelas. Model tadbir urus komuniti seperti yang digariskan oleh The Linux Foundation melibatkan beberapa peranan penting seperti peneraju, penyelenggara, pelaksana, penyumbang dan pengguna.

Peneraju memainkan peranan dalam membuat keputusan akhir terhadap hasil, aktiviti dan hala tuju keseluruhan projek, manakala penyelenggara akan bertanggungjawab dalam pengagihan skop kerja di samping mengawal selia setiap komponen projek. Pelaksana pula adalah ahli yang memberikan komitmen dan tanggungjawab terhadap setiap tugasan projek manakala

Kita ingin melihat tadbir urus seperti ini mampu direalisasikan dalam komuniti sumber terbuka sektor awam dalam masa terdekat. Di sinilah peranan dan tanggungjawab daripada semua amat diperlukan untuk sama-sama membentuk komuniti dalam sektor awam yang boleh membentuk perspektif baharu terhadap keupayaan kakitangan awam, khususnya pegawai daripada skim teknologi maklumat.

Tiba masanya komuniti sektor awam diarusperdanakan dalam perkhidmatan awam dengan melibatkan kepakaran dari pelbagai bidang. Walaupun pendekatan komuniti sumber terbuka ini diterajui dengan fokus kepada pembangunan perisian, namun selaras dengan hala tuju pendigitalan sektor awam, komuniti ini memerlukan sumbangan daripada lebih daripada sekadar komuniti teknologi maklumat.

Sesebuah produk perisian yang matang memerlukan bukan hanya kod sumber yang bebas pepijat, tetapi memerlukan dokumentasi yang komprehensif, panduan pengguna, pelan pengurusan perubahan, siri-siri latihan dan selanjutnya input berterusan demi menjamin kelestarian produk berkenaan. Banyak aspek bukan teknikal boleh disumbangkan oleh ahli komuniti yang bukan daripada bidang teknikal.

Selain daripada pihak yang terlibat dalam pembangunan sesebuah aplikasi, jangan dilupakan bahawa golongan yang paling terkesan ialah pengguna aplikasi itu sendiri. Semua pengguna aplikasi sumber terbuka juga boleh turut menyumbang secara aktif sebagai ahli komuniti dalam memberikan maklumbalas dan seterusnya mungkin menentukan kelangsungan produk berkenaan sama ada akan terus berkembang dan lestari atau ditinggalkan kerana ketidakupayaan produk memenuhi jangkaan keperluan pengguna yang seiring dengan perubahan teknologi.

Program Pengurusan Perubahan @osdec @MAMPUJPM : Bengkel Bersama Komuniti Sumber Terbuka Bilangan 1 Tahun 2019 - Sesi Bergambar Bersama YBrs Encik Jaafar Ahmad, Pengarah Bahagian Pembangunan Aplikasi, MAMPU | Klana Beach Resort Port Dickson, Negeri Sembilan | 29 - 30 Januari 2019

A Framework for ICT Security Policy Compliance

Ts. Dr. Mohd Farizul Mat Ghani
Ministry of Education Malaysia

Najwa Hanis Abdul Samat
Department of Statistics Malaysia

ABSTRACT

Many organisations are beginning to realise the need to protect their IT assets both from accidental disasters and malicious or intentional attacks. ICT Security is a fundamental requirement. How organisations safeguard and protect their assets depends on the availability of resources and decision-making capability. The ICT Security Policy was established to ensure the smooth running of the organization and also to minimize the impact of ICT security incidents. In this study, four renowned Local Authorities (LAs) in Malaysia were the choosen in answering the research questions. Two modes of data collection were adopted in this study; interview and survey. Five major constructs of ICT Security Policy Framework (ISPF) unique to LAs were identified during preliminary investigation. The result provides valuable information on ISPF practices in establishing the components of the ISPF. A proposed ISPF specific for LAs was designed. Then a survey was conducted to investigate IT personnel perceptions on the existing ICT Security Policy practices at the various LAs. The result of the study contributes to the understanding of the status and LAs practices of ICT Security Policy in Malaysian government sector

INTRODUCTION

The rapid development of Information Technology in this country proves how fortunate our generation nowadays. As a result, we have a world without boudaries. Information, Communication and Technology (ICT) does not only serve as a communication agent, it also acts as a bridge for user to benefit as part of the routine and the necessities of life.

The security of ICT is closely related to ICT assets and information protection. This is because the hardware equipment and software components that are part of the ICT assets in government organisations are large investments and need to be protected. In addition, the information stored in the ICT system is valuable because a lot of resources are required to produce it and the information will be difficult to be re-generated in a short period of time. The demography within LAs in Malaysia took an evolutionary change since the introduction of Information Technology (IT) in Malaysian government sector.The significant achievement of IT in Malaysia can be traced from the early nineties after various adjustments of regulatory and commercial policies, both macroeconomic and within IT's converging sectors (Hancock, 2000). In pace with such adaptation, local authority in Malaysia are increasingly utilizing IT in all aspects of its organizational functions.

Furthermore, certain information that has been processed by the ICT system is deemed to be sensitive and classified. Unauthorized disclosure or information leakage could harm the national interest. Any usage of government's ICT assets apart from the outlined purpose and intention is considered as misuse of government's resources. ISMS survey which was conducted by CyberSecurity Malaysia in the month of October 2016 on 100 organizations had revealed that normal attacks are viruses (87%) and mail spamming (83%). In addition, more than 68% of the organizations have little knowledge on ISMS. Moreover, 37% of the organizations do not have any security policy at all [22].

Literature review

This section, firstly defines ICT Security Policy. Secondly, the various information security frameworks are examined and then discuss the four standard Framework ICT Security Policy commonly used. CyberSecurity Malaysia is the national cybersecurity specialist agency under the preview of Ministry of Science, Technology and Innovation (MOSTI). The establishment of CyberSecurity Malaysia is to provide technical specialised in cyber security services to protect the public, the economy and government services [22]. For the bigger national objective, CyberSecurity Malaysia also plays an important role in preventing or minimising disruptions to both critical national information infrastructures (CNII) and industries [24], [25]. Back in 2017, CyberSecurity Malaysia obtained full certification in Information Security Management System (ISMS) ISO/IEC27001 [20],[22].

MAMPU ICT security policy

Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) developed a method to assess the safety of an equipment called High-Level Risk Assessment (HiLRA) and produced Guidelines for Public Sector ICT Security Management Malaysia (MyMIS) for the Malaysian public security sector [24], [25]. MAMPU also provides ICT Security Consultancy to improve safety aspects and develop government ICT infrastructure. In addition, MAMPU also offers (a) consulting services on ICT security-related issues such as news, articles, advisories and tools, (b) findings and incident management, and (c) preparation of policy and ICT security management [26],[27].

The Public Sector Information Security Risk Assessment is intended to help public sector agencies measure and analyze the risks of their assets [19]. Once the risks have been analyzed, government agencies will take the necessary action in order to control the risks [18]. For this purpose, the government prepared General Circular Letter No. 6 Year 2005: Security Risk Assessment Guidelines for Public Sector to update on the importance of implementing information security risk assessment in the public sector [20], [21] .

Figures ICT security policy framework

Framework is define as an the outline action of the more thorough blueprint, which sets out the model to be followed in the creation of the design, selection and initial and ongoing implementation of all subsequent security control. It is also includes information security policies and procedures, security education training programs, and technological controls (Whitman and Mattord, 2010).

From the Information Security (InfoSec) policy perspective, a framework offers a possible starting point for understanding a security policy's impact to an organization, and is intended to guide organizations in developing, implementing, and maintaining security policy (Kasmiran, 2008). Policy should address both logical and physical security. In addition, privacy and confidentiality, integrity and availability, and legal compliance requirements (Computer Associates International Inc, 2015) also should be included.

A primary objective of InfoSec Policy is to define the user's rights and responsibilities in an organization and the effective InfoSec Policy will helps the users understand what acceptable and responsible behavior is in regards to information resources to ensure the safe environment (Hone and Eloff, 2012).

InfoSec Policy has attained an international awareness and several international standards have been built (Hong et al., 2016). The following section will explain the commonly used standards of Information Security Policy.

Existing information security standards framework

In this section, we discuss the existing standard information security frameworks such as MyMIS, ISO/IEC 27001, COBIT and COSO [8]. Due to the lack of information security framework specifically addressing higher education institutions, the four established framework (MyMIS, ISO/IEC 27001, COBIT and COSO) provided some guideline in developing the proposed information security framework [16], [17].

MyMIS

MAMPU has introduced a handbook called MyMIS. MyMIS basically provides a standard guideline especially for government sector. It comprises of management safeguards, basic operation, technical operation and legal matters (MAMPU, 2002).

ISO 27001

ISO 27001 is an auditable international standard which defines the requirements for the management of Information Security [20]. The standard is designed to ensure the selection of adequate and proportionate security controls. The focus on ISO 27001 as a basis for the policy development was to move towards a standard that could be externally measured. The council acknowledges that ISO27001 prefers to separate policy from procedure. However, for the sake of keeping each policy item 'holistic', the council will keep procedures and templates with each policy as far as possible. As the council becomes more mature in terms of policy management this can be reviewed. This means that each time a procedure is changed, the policy will need to be updated, but the council will accept this and include it in the policy review procedure.

COBIT

The Information Systems Audit and Control Association & Foundation (ISACAF) developed Control Objectives for Information and related Technology (COBIT) to provide management and business process owners with an IT governance model to help understand and manage the risks associated with IT. COBIT describes the processes and controls needed for implementing an information security policy, rather than focusing on the document itself. It contains a brief section on the Security and Internal Control Framework Policy, which gives various pointers on writing and maintaining such a document. COBIT consists of four main components namely, plan and organize, acquire and implement, deliver and support, and finally monitor and evaluate [15].

RESEARCH METHODOLOGY

In addressing the research questions, two phases of data collection were involved, namely, interview and survey. The interview is to determine the main component of ICT Security Policy for .

Having completed the interviews, a survey was embarked on in examining the IT personnel perceptions on the existing information ISPF at respective local authority in Malaysia.

Interview

The interview conducted involved four (4) LAs in Malaysia selected located in Selangor State. LAs chosen are all renowned local located in the most populous area of Malaysia's economic pulse. For anonymity and confidentiallity reasons, the selected local authoritys are referred as Alpa- A District Council (ADC) , Beta- B District Council (BDC) , Chi- District Council (CDC), and Delta- D District Council (DDC). The interviewees comprises of IT-expert staff and personnel in-charge of developing the ICT Security Policy Framework for each LAs . It was noted that most of the respondents are above 35 years of age; while the number of years in their respective organization and are in the current position recorded as more than six years. This implies that the interviewees are best candidates to provide information on an aggregated unit of analysis in relation to views of information security and its implementation and best practices. Each of the interview exercises lasted from 40 minutes to an hour. It was conducted between the months of April to May of 2018.

Results

Through the interviews, Table 1 summarizes the main components considered by the four LAs in this research.

LA	Component Considered	Standardadopted
ADC	Risk Assessment Physical and Environmental Security AccessControl Information Security Incident Management Compliance	COBIT & ISO 27001
BDC	Risk Assessment Security Policy Organization of Information Security Asset Management Human Resource Security Physical and Environmental Security Communication and Operation Management AccessControl Information Systems acquisition, development and maintenance InformationSecurity Incident Management Compliance	ISO27001
CDC	Management Safeguards Basic Operations Technical Operations	MyMIS
DDC	Management Safeguards Basic Operations	MyMIS

Table 1: Components of Main Components Considered by LAs.

As depicted in Table 1, various components were included by the respective LAs. BDC adopted all eleven domain of ISO 27001. Unlike ADC considered only five incorporated also those from COBIT. MyMIS is the standard adopted by CDC and DDC while CDC includes technical operations. Besides this, it is noteworthy to understand the current status of InfoSec policy practices.

Conceptual Framework

ISPF constructs identified for LAs was adopted from ISO 27001, MyMIS and COBIT. With the established guidelines, we developed the conceptual information security framework as illustrated in Figure 1. Based on the four (4) interviews, five main constructs were identified to be considered in the HEI ISPF. They are information security policy, risk management, access control, awareness program and training, and compliance. Figure 1 shows the conceptual components with their constructs considered for the proposed ISPF.

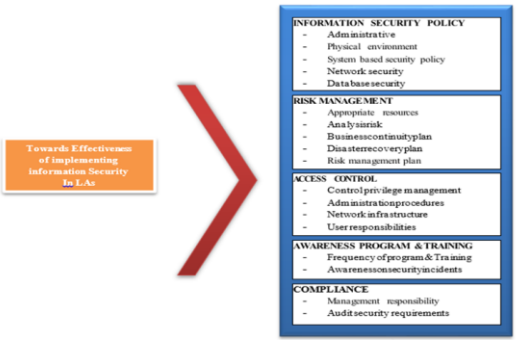


Figure 1 : Proposed Conceptual Information Security Framework for LA

Five security elements are used to enforce the ISPF. The security constructs are briefly described below:

Information Security Policy

This part explains about security policies. Security policies control address management support, commitment and direction in accomplishing information security goals including information security policy (Carlson, 2001).

Risk Management

Risk management is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed (Radack, 2004).

Access Control

Access control addresses an organization's ability to control access to assets based on business and security requirements including business requirement, user management, user responsibilities, network access control, host access control, application access control, access monitoring and mobile computing (Carlson, 2001).

Awareness Program & Training

Based on the awareness on the security issues, and is the single most effective means of ensuring information security. The most effective measures depend largely on the behavior of the people affected by those measures. For example, an access control system based on secret password is effective only if people do not share their password (Elliot et al., 1991).

Compliance

Compliance control addresses an organization ability to remain in compliance with regulatory, statutory and security requirement including legal, technical and system requirements and audits (Carlson, 2001). Nevertheless, from the four established framework (MyMIS, ISO 27001, COBIT, and COSO) indeed provided beneficial guidelines to the LAs which in turn form the basis in developing the proposed information security framework depicted in Figure 1.

Discussion and conclusion

This study has successfully answered both the research questions. Firstly, the main constructs of LAs ISPF were determined through interviews. Secondly, based on the IT personal responses through a survey, it establishes their perceptions on the existing information security policy practices. Through the interviews, it revealed that largely all the established government- supported LAs have some form of IT policies in place. Various establish information security standards were found to form the basis of their efforts towards the development of their very own policy.

This research further discovers that information security policy, risk management, access control, awareness program and training, and compliance are the major components or elements that fix upon the suggested framework for LAs. These components are in line with the objective of developing the framework which was to apply and cover all hardware, software, data, information, network, personal computing devices, support personnel, and users within LAs from intrusion, interception, interruption and denial of services.

This study does disclose top management concerns on the importance of adequate information security policy in the organizations. This is indicated by periodically reviewing and updating the policy based on significant changes due in relation to the risk identified by the organizations. Thus, the policy is consistently and readily made available for compliance by the administrator, faculties, staff, students and third party. Accordingly, the findings indicated the effectiveness of the policy the organizations have addressed all the five security constructs identified in the ISPF. Access control is found to be the most important security element. Additionally, policy also plays an important role in explaining to staff and students of their responsibility in the protection of the information resources, while stressing the importance of having secured information.

Awareness and compliance is the success key to the policy as implementation will take place after the policy had been endorsed. It was showed that the awareness training has been conducted to administrator and staff in the organization.

This study also indicated that LAs appoints specific person in-charge or committee set up in addressing ISPF and policy concerns. In furtherance of ensuring the compliance enforcement, information security policy department is actively in cooperation with other units of the organization and regular meetings and scheduled reporting are practiced.

Hence, thi effort would provide some clarification and insights into how ISPF is depicted in the academic setting. Further work is obviously necessary to look into the details of the framework. Thus, this research serves as an expansion of security and assurance in operational areas literature in the area of ISPF engagements.

Despite the study's limitations, we believe that our work makes significant contributions to practice and research.

Managerial perspective

i. It provides as an indicator to the status of ISPF implementation from IT personnel perspective;
ii. It identified the various standard adopted by LA or the lack of it;
iii. LAs can enjoy significant benefits from making right choices in terms of construct that are relevantnor set a priority- level to its ICT-related activities;
iv. Serves as preparatory guidelines for future planning and improvements to LAs ISPF; and
v. Better understanding of critical ISPF construct to ensure successful enforcement of information security.

Theoretical Contribution

i. Clarification and rearrangement of the available constructs: information security policy, risk management, access control, awareness program and training, and compliance are delineated in the proposed ISPF model;
ii. Identification of new constructs whereby the involvement of top management plays a significant role in sustaining a robust and effective. Notably, adequate implementation and improvement of the ISPF hinges on management's commitment.

In a nutshell, this study forms a basis in understanding the status and its practices of information security in Malaysian academic setting. This will further fulfill the LAs information security needs towards a more dynamic yet sustaining a secured academic environment.

References

[1] AS/NZ ISO/IEC 27002:2006 (2006),

[2] 'Information Technology – Security Techniques – Code of Practice for Information Security Management,' AS/NZ ISO/IEC 27002.

[3] Albrechtsen E, A qualitative study of user's view on information security. Computers & Security 2017; 26(4): 276–289.

[4] Bill and Morrow,. BYOD security challenges: control and protect your most sensitive data Network Security 2012; (12), pp.5-8.

[5] Burton-Jones, A. and Grange,. From use to effective use: a representation theory perspective. Information Systems Research 2015; 24(3), pp.632-658.

[6] Chan M, Woon I &Kankanhalli A,. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy & Security 2012; (3): 1841.

[7] Corpuz, M. and Barnes, P.H,. Integrating information security policy management with corporate risk management for strategic alignment. In Proceedings of the 14th World Multi-Conference on Systemics; 2010.

[8] Cybernetics and Informatics (WMSCI 2010).

[9] D'Arcy, J. and Herath, T,. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems 2011; 20(6), pp.643-658.

[10] Dickie,. Improving your organization;s attitude and commitment to security computer audit update;

October 1996.

[11] Gaunt,. Practical approaches to creating a security culture international journal of merical informatics 2012; no.49. (1998) pp 131-134

[12] Herath T &Rao HR,. Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. European Journal of Information Systems 2009; 18(2): 106–125.

[13] Hone, K and Eloff,. Information security policy-What do international security standard computers and security 2015; vol.21, no.5 pp.402-409.

[14] Humaidi, N. and Balakrishnan, V,. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In 2nd International Conference on Management and Artificial Intelligence IPEDR 2014; (Vol. 35, pp. 1-6).

[15] Ifinedo, P., 2011. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), pp.83-95.

[16] ISO/IEC TR 13335-1:1996,. GMITS -Concepts and models for IT Security 1996.

[17] ISO/IEC TR 13335-2:1997,. GMITS -Managing and planning IT Security 1997.

[18] ISO/IEC TR 13335-3:1998,. GMITS -Techniques for the management of IT Security 1998.

[19] ISO/IEC TR 13335-4:2000,. GMITS -Selection of safeguards 2000.

[20] ISOIlEC FDIS 27001:2005,. Information Technology –Secutity 2005.

[21] ISO/IEC FDIS 17799:2005,.Information Technology - security management systems Requirements 2005.

[22] ISMS and A LevellCT Through Diagrams, 2017, NISER.

[23] Kruger HA & Kearney WD,. A Prototype for Assessing Information Security Awareness. Computers and Security 2006; 25(4): 289–296.

[24] MAMPU,. The Malaysian Public Sector Management of Information Security 2002.

[25] MAMPU,. Techniques-Information security management systems – Requirements 2002.

[26] MDC., ICT Security Policy 2015; Version 2.

[27] MAMPU,. ICT Security Policy Julai, 2010; Version 5

[28] Venkatraman, S., A framework for ICT security policy management. Frameworks for ICT Policy: Government, Social and Legal Issues: Government, Social and Legal Issues 2010; p.1.

A Gentle Introduction to Sentiment Analysis Using Naïve Bayes

Meor Mohd Shahrulnizam bin Meor Sepli
Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)

Sentiment analysis is a common text classification technique that at its most basic function, identifies the polarity of a given topic through text mining. Polarity refers to the number of positive and negative terms inside a given document. In simpler terms, sentiment analysis is used to predict the category (could be positive or negative) of a given text in a document, like a piece of product review on Amazon, or the latest Marvel's movie reviews on IMDB's website.

One of the most common techniques for sentiment analysis is Multinomial Naïve Bayes (NB) text classification. Over the years, we saw advancement in the development of more advanced and complex algorithms such as Support Vector Machine (SVM), artificial neural network, etc. However, NB is still a preferable choice for researchers all over.

So why NB, you asked? Simply, because it is fast, reliable and fairly accurate. Don't take my words just yet. Read on.

How Does it Work?

The promise of NB is simplicity. It is based on Bayes' Theorem, a probability theory to predict the probability of an unknown event (posterior) based on previous occurrence of related events (a-priori).

I won't bore you with the exact formula, but the core principle is that each words in a sample text is counted and then a dictionary of frequent words and its count is built. So how does the categorization works? By counting how many times a word appears in a said category over the count of all the words with that category. In other words, supposed the word 'quality' is associated with negative more than positive samples, so it ends up being classified as negative, although we know that 'quality' is a semantically positive word. Hence the "naïve" in its name. This makes it a domain or topic-based algoritm.

Still scratching the back of your head? Don't turn to dust yet!

Practical Example

Let's take a look at a simplified example. The table below shows a training set, that is used by the classifier to learn unseen data. The source of inspiration for this data is taken from the Avengers: Endgame user reviews page at https://www.imdb.com/title/tt4154796/reviews?ref_=tt_urv.

Item	Text	Label
1	Thanos please snap this movie	Negative
2	Absolute perfection end game	Positive
3	This movie was awful	Negative
4	The movie was very boring	Negative
5	Good acting performance to all the characters	Positive

The probability for negative category, P(negative)=3/5. There are 3 negative samples over 5 total items.

The probability for positive category, P(positive)=2/5. There are only 2 positive samples over 5 total items.

To predict the category for Item #1: “Thanos please snap this movie”, we simply calculate the probability of each words’ occurences in its category.

The formula is,

$$\frac{Number\ of\ the\ word\ occurences\ +\ 1}{Number\ of\ words\ in\ category\ +\ Total\ number\ of\ words}$$

The results of the calculation are shown below.

Word	Negative	Positive
Thanos	$\frac{1+1}{14+25}$	$\frac{0+1}{11+25}$
please	$\frac{1+1}{14+25}$	$\frac{0+1}{11+25}$
snap	$\frac{1+1}{14+25}$	$\frac{0+1}{11+25}$
this	$\frac{2+1}{14+25}$	$\frac{0+1}{11+25}$
movie	$\frac{3+1}{14+25}$	$\frac{0+1}{11+25}$

Since it is labeled with a positive/negative category, it is called a supervised machine learning classification. So NB “learns” by using a set of previously labeled dataset.

So, to get the category for which “Thanos please snap this movie” belongs to, we just compare which value is bigger:

For P(“Thanos please snap this movie” | negative), read as, the probability of the sentence “Thanos please snap this movie” given negative category is,

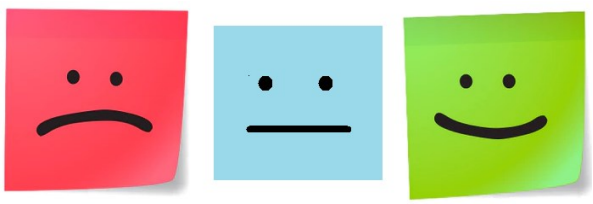
$$\begin{aligned} &P(Thanos \mid negative) \times P(please \mid negative) \times P(snap \mid negative) \\ &\quad \times P(this \mid negative) \times P(movie \mid negative) \times P(negative) \\ &= \frac{1+1}{14+25} \times \frac{1+1}{14+25} \times \frac{1+1}{14+25} \times \frac{2+1}{14+25} \times \frac{3+1}{14+25} \times \frac{3}{5} \\ &= 6.38 \times 10^{-7} \\ &= 0.000000638 \end{aligned}$$

Meanwhile, for the positive category,

$$\begin{aligned} &P(Thanos \mid positive) \times P(please \mid positive) \times P(snap \mid positive) \\ &\quad \times P(this \mid positive) \times P(movie \mid positive) \times P(positive) \\ &= \frac{0+1}{11+25} \times \frac{0+1}{11+25} \times \frac{0+1}{11+25} \times \frac{0+1}{11+25} \times \frac{0+1}{11+25} \times \frac{2}{5} \\ &= 6.6 \times 10^{-9} \\ &= 0.0000000066 \end{aligned}$$

Finally, obviously we have a winner here! Item #1: “Thanos please snap this movie" indeed belongs to a negative category. Please note, since it is a multiplication, word order (and common sense, ha!) are unimportant, so it doesn’t matter if “movie please snap this Thanos”.

Now, comes the boring part. In order to proceed further, a computer requires certain processing to convert the text into suitable formats the computer can understand. This processing or pre-processing is the most critical phase in machine learning classification as it cleans out uninteresting parts from the data, which may affect the accuracy of prediction. Only a handful of words are selected that influences the polarity orientation of the the text, so the exclusion of these noises should consequently improve and speed up classifier’s performance. In the sample codes, the first step of normalization is to fold all letters into lower case so that “LOVE” and “love” are not counted as different words. All whole digits are removed e.g. “95399”. All punctuations marks e.g. “,”, “:”, “&”, and “!” are removed. All characters except spaces, lower case letters (a-z) and digits (0-9), and consecutive white spaces are also removed. Stopwords like “a”, “is”, “the”, “on” are also removed. Stopwords are the most common elements in a language.



The End Game Prediction

Accuracy is one of the most common metrics in measuring supervised machine learning performance. In sentiment analysis context, it is a measure of how often a prediction is correct.

Using the Python code below, with only 46 items at 50% positive:negative data ratio and 3:4 training and testing ratio, I managed to obtain an accuracy of 83.3%, which is comparable with human concordance at 70-80%. This also shows that NB fares favourably with other sophisticated algorithms, even with a small dataset.

```
#---------------------
#test with one pos and neg document
pos="""avengers endgame review score avengers endgame could well described complicated storyline entire marvel histo
print('Predicted class:', classifier.classify(extract_features(pos.split())))
#print(extract_features(pos.split()))

neg="""thanos please snap movie bad script writing"""
print('Predicted class:', classifier.classify(extract_features(neg.split())))
#print(extract_features(neg.split()))
#---------------------

test_set = nltk.classify.apply_features(extract_features, testreviews)

#evaluation
classifier = nltk.NaiveBayesClassifier.train(training_set)
print ("accuracy:", nltk.classify.util.accuracy(classifier, test_set))
print(datetime.datetime.now())

classifier.show_most_informative_features(15)
```

```
train on 34 instances, test on 12 instances
2019-05-03 22:34:18.260559
Predicted class: 1
Predicted class: 0
accuracy: 0.8333333333333334
```

We can get better accuracy by applying more advanced pre-processing techniques using natural language processing tools such as stemming (crude removal of suffixes e.g. -ing, -er, -est), and lemmatization (dictionary-based root word reduction).

The full Jupyter Notebook code for this sample can be obtained at https://github.com/meornizam/perjasa052019.

Welcome to the world of Data Science!

Kejohanan Golf PERJASA 2019 - Piala GCIO

Ts. Adi Azlan bin Mohd Ali
AJK PERJASA 2017-2019

Pada 30hb Mac 2019 seramai 24 orang peserta terdiri daripada ahli PERJASA dan rakan strategik PERJASA telah menyertai Kejohanan Golf PERJASA 2019, bagi merebut piala GCIO yang telah dipertandingkan semenjak tahun 2010 lagi. Kejohanan kali ini yang dijalankan di Kelab Golf Perkhidmatan Awam dihadiri oleh tetamu kehormat YBhg. Datuk Zainal Abidin bin Abu Hassan, Timbalan Ketua Setiausaha (Keselamatan), Kementerian Dalam Negeri. Terdapat dua kategori yang telah disediakan untuk pemain iaitu Kategori Sektor Awam dan Kategori Korporat. Satu anugerah bagi keseluruhan pertandingan juga telah disediakan berupa piala pusingan GCIO yang menjadi rebutan semua peserta.

Keputusan pertandingan telah menyaksikan muka-muka baru dikalangan ahli perjasa menduduki kedua-dua kategori tersebut. Bagi Kategori Sektor Awam, En Johari bin Hashim telah dianugerahkan sebagai johan, En Turidi bin Mat menduduki tempat kedua dan tempat ketiga jatuh kepada En Mohd Iskandar Zulkarnain bin Mohd Noh. Manakala bagi Kategori Korporat, En Norhizam bin Mat Daud telah berjaya sebagai Johan, YBhg Dato' Azhar Ismail di tempat kedua dan akhir sekali En Wong Keng Hoe menduduki tempat ketiga. Juara keseluruhan yang membawa pulang piala pusingan GCIO telah dirangkul oleh En. Khairuddin bin Mohemed Nor.

Kejohanan golf ini dilihat sebagai satu cara untuk meningkatkan penyertaan ahli dalam bidang sukan dan menjadi acara santai bagi ahli-ahli perjasa bersama pihak industri menjalinkan hubungan erat dalam memajukan agenda transformasi pendigitalan sektor awam. Diharapkan pada masa akan datang, aktiviti ini dapat diteruskan seterusnya meningkatkan persepsi bahawa aktiviti golf adalah hanya untuk pengurusan tertinggi sahaja sedangkan ianya juga merupakan aktiviti sukan yang diceburi oleh pegawai-pegawai teknologi maklumat.

Sesi Perjumpaan Bersama Wakil PERJASA, KPPTM dan CTSU Bersama YBhg Ketua Pengarah MAMPU

Ts. Mohamed Hairul bin Othman
AJK PERJASA 2017-2019

Sesi Perjumpaan Bersama Wakil PERJASA, KPPTM dan CTSU Bersama YBhg Ketua Pengarah MAMPU pada 28 Januari 2019

PERJASA diwakili oleh Tn Hj Ahmad Bin Osman (Presiden) dan Ts. Mohamed Hairul Othman (AJK PERJASA).

Perjumpaan mengambil masa kira-kira 2 jam setengah yang turut disertai oleh YBhg Dr. Suhazimah Dzazali (TKP), YBhg Dato' Azlan Johar (Pengarah BKP), YBhg Dr. Mohd Zabri Yusoff (Pengarah Bhg Penyelidikan Pengurusan), Pn Susie Dorai Raj (Pengarah Bhg Perundingan ICT), En Ahmad bin Daud (Pengarah Bhg Strategi & Arkitektur) dan Pentadbiran MAMPU.

Objektif perjumpaan adalah bagi membincangkan cadangan penubuhan Agensi Digital Sektor Awam (PSDA). Selain daripada itu, banyak perkara turut diutarakan oleh wakil setiap persatuan meliputi isu berkaitan kebajikan, kompetensi, profesionalisma, kemajuan kerjaya, termasuk isu perjawatan di agensi negeri.

Bagi pihak YBhg Dato' Dr KP, semua cadangan diambil maklum dan akan diteliti dengan terpeinci. Selain daripada itu, YBhg Dato' Dr KP turut menjelaskan bahawa keputusan melibatkan beberapa perkara kritikal akan dibuat secara *quick win* selain daripada beberapa isu yang memerlukan penilitian lanjut untuk kajian dengan lebih komprehensif.

PERJASA menyambut baik keterbukaan YBhg Dato' Dr. KP untuk memberikan komitmen terhadap segala isu yang dibangitkan termasuk melibatkan PERJASA bagi membuat projection bagi keseluruhan Skim F. Disamping itu, beliau turut bersetuju perjumpaan secara berkala diadakan bagi memastikan segala isu dapat ditangani dengan sebaiknya. Rakan-rakan Skim F juga diharapkan agar dapat terus melengkapkan pengisian SPK bagi membantu proses perancangan kerjaya bagi memastikan bidang tugas seiring dengan kemahiran dan kepakaran masing-masing.

Keperluan Membina Tahap Ketersediaan Yang Tinggi (HA) Ke Atas Server Virtual

Mohd Rizal Kadis
Jabatan Kemajuan Islam Malaysia (JAKIM)

Keselamatan Maklumat terdiri daripada tiga ciri-ciri asas iaitu Kerahsiaan, Integriti dan Ketersediaan. Ini telah dinyatakan di dalam Dasar Keselamatan ICT setiap agensi Kerajaan dan Standard ISO/IEC 27001:2013 Information Security Management Sistem (ISMS). Artikel ini menyentuh tentang bagaimana "Ketersediaan" harus dikekalkan ke atas server kerana server merupakan tempat di mana data-data penting anda disimpan. Jika kita sudah melaksanakan Pensijilan ISMS, sudah tentu kita dapat melihat di antara salah satu kawalan standard adalah perkara A.17.2 Redundancies iaitu berkaitan dengan kemampuan kita untuk menyediakan fasiliti sekunder seperti server bagi menjamin tahap ketersediaan yang tinggi. Oleh kerana data disimpan di dalam server, maka perlindungan terhadap server mestilah mendapat keutamaan agensi berbanding perlindungan yang lain.

Sememangnya banyak elemen yang perlu dilihat untuk melindungi server daripada ancaman terutama serangan penggodam. Misalnya, di antara perlindungan yang biasa diambil adalah dengan memasang firewall atau Intrusion Detection Sistem (IDS) dan sebagainya. Namun, ancaman yang jarang diambil perhatian adalah datang daripada sistem pengoperasian itu sendiri iaitu "Pincang Tugas". Biasanya ancaman seperti ini akan mengakibatkan tempoh gendala (downtime) yang panjang dan sukar untuk dipulihkan.

Dengan kemunculan teknologi server hypervisor secara komersial hampir sedekad yang lalu, ianya telah banyak memberi manfaat dalam bidang ICT khususnya Pusat Data dimana keperluan terhadap server fizikal telah dapat dikurangkan secara mendadak dan sumber komputer dapat digunakan dengan lebih cekap dan berkesan dengan kebolehan mewujudkan server virtual di dalamnya mengikut permintaan. Ditambah pula dengan ciri-cirinya yang sofistikated dan maju seperti fungsi "Pindah Alih" secara automatik, ia mampu menyediakan keperluan server yang mempunyai tahap ketersediaan yang tinggi. Ini bermaksud, perkhidmatan server virtual tidak terganggu sekiranya berlaku kerosakan terhadap unit server fizikal kerana dengan adanya fungsi "Pindah Alih", kesemua server virtual yang berada dalam server fizikal yang rosak dapat dialihkan ke server fizikal yang masih berfungsi dengan baik secara automatik. Ini secara tidak langsung telah dapat memenuhi salah satu daripada komponen asas Keselamatan Maklumat iaitu Ketersediaan.

Kerajaan telah memanfaatkan teknologi ini sepenuhnya dengan menyediakan perkhidmatan Virtual Server Hosting di Pusat Data Sektor Awam (PDSA) dimana agensi-agensi Kerajaan hanya perlu memohon server virtual yang diperlukan tanpa mengeluarkan sebarang kos tambahan. Kemudahan yang disediakan oleh PDSA ini sedikit sebanyak telah berjaya mengurangkan kos perolehan server yang tinggi di agensi hanya untuk menempatkan sistem atau laman web yang tidak memerlukan sumber komputer yang tinggi.

Namun begitu, adakah dengan menyediakan satu unit server virtual bagi sistem kritikal agensi sudah mencukupi bagi mencapai tahap ketersediaan yang tinggi (High-Availability)? Sebagai contoh, sekiranya berlaku kerosakan terhadap sistem pengoperasian seperti Kernel Panic atau Blue Screen of Death (BSoD), sudah tentu fungsi "Pindah Alih" seperti yang dinyatakan di atas tidak akan dapat membantu. Mungkin juga terdapat kaedah alternatif lain yang boleh digunakan iaitu memulihkan semula server virtual daripada fail sandaran (backup) atau snapshot, namun kaedah ini pasti akan melibatkan tempoh gendala. Tempoh gendala mungkin akan menjadi lebih panjang sekiranya kerosakan tersebut berlaku diluar waktu bekerja seperti pada waktu tidur, cuti umum/perayaan, atau pemilik server virtual tersebut tidak dapat dihubungi untuk mendapatkan maklum balas dan persetujuan. Tidak kurang juga jika kerja-kerja penyelenggaraan server perlu dilaksanakan seperti menaik taraf perisian, mengemaskini patches, troubleshooting, reboot dan sebagainya pasti akan melibatkan waktu gendala. Ini belum lagi jika terdapat kegagalan pada server selepas kerja-kerja penyelenggaraan dilaksanakan.

Sekiranya perkara ini terjadi, sudah tentu ia akan mengakibatkan kekecewaan kepada pengguna yang sedang menggunakan sistem pada masa tersebut kerana komponen asas keselamatan iaitu ketersediaan tidak dapat dipenuhi.

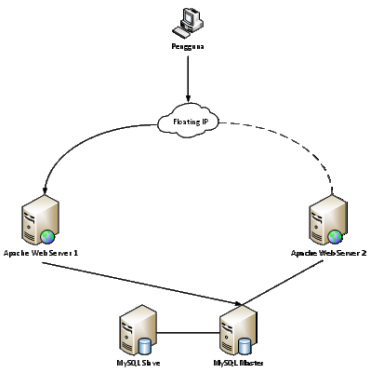
Ketersediaan Yang Tinggi (HA) boleh dibina kepada dua cara iaitu Active-Passive HA atau Active-Active HA bergantung kepada kesesuaian produk dan teknologi yang digunakan. Active-Passive HA terdiri daripada primary dan failover server dimana primary server adalah server yang aktif manakala failover server adalah sandaran kepada primary server tersebut. Sekiranya berlaku kerosakan kepada primary server, failover server akan mengambil alih peranan primary server tersebut sebagai aktif. Manakalan Active-Active HA pula, setiap server adalah aktif dan load-balancing boleh dimanfaatkan bagi mengimbangkan trafik rangkaian setiap server. Load balancing membolehkan setiap server mempunyai trafik yang sekata sekaligus mempercepatkan capaian sekiranya jumlah trafik adalah tinggi.

Adakah kos untuk membina HA tinggi? Sebenarnya kos untuk membina HA tidak tinggi dan boleh saja menggunakan teknologi sumber terbuka (open source) seperti Linux. Tambahan lagi, server virtual boleh dipohon secara percuma daripada PDSA. Cuma yang diperlukan adalah sedikit masa dan tenaga untuk membuatnya.

Untuk memahami konsep HA ini, konsep Active-Passive HA yang paling asas boleh dibina daripada teknologi yang biasa dan banyak digunakan oleh agensi kerajaan seperti berikut:-

1. Sistem dibangunkan menggunakan bahasa pengaturcaraan PHP.
2. Menggunakan perisian Apache Web Server.
3. Platform Linux.

Asas Infrastruktur Active-Passive HA



Gambarajah 1: Topologi Server berteraskan Active-Passive HA.

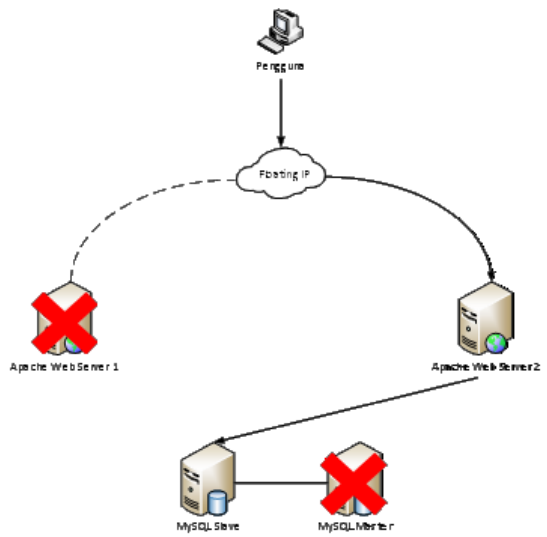
Gambarajah 1 adalah asas infrastruktur server virtual yang perlu dibangunkan bagi membentuk sekurang-kurangnya tahap ketersediaan server yang minimum. Fungsi bagi setiap server adalah seperti berikut:-

- Apache Web Server – Mengandungi perisian sumber terbuka HTTP server dan engine PHP. Ia juga mempunyai perisian HAProxy yang menggunakan Virtual Router Redundancy Protocol (VRRP) untuk mengawal floating IP.
- MySQL Master – Pangkalan data MySQL yang bertindak sebagai master.
- MySQL Slave – Pangkalan data MySQL yang bertindak sebagai slave.

Apakah Floating IP?

Floating IP adalah bersamaan dengan alamat IP fizikal yang ditetapkan secara kekal pada Network Interface Card (NIC) server bagi membolehkan server dikenal pasti dalam rangkaian. Perbezaan floating IP dengan alamat IP fizikal adalah ianya tidak akan kekal pada satu server sekiranya server yang menyimpan IP tersebut rosak. Sebaliknya, ia akan dipindahkan ke server lain yang masih baik keadaannya. Kerana itulah ia dinamakan floating IP. Sudah tentu Domain Name sistem perlu dilekapkan bersama dengan floating IP.

Daripada topologi yang ditunjukkan dalam Gambarajah 1, terdapat dua jenis server iaitu Apache Web Server dan MySQL yang masing-masing mempunyai lebih daripada satu server (redundancy) yang berfungsi secara Active-Passive HA. Di dalam persekitaran Active-Passive HA tersebut, Apache Web Server 1 dan MySQL Master berfungsi sebagai primary (active) manakala Apache Web Server 2 dan MySQL Slave berfungsi sebagai failover (passive). Server failover bertindak sebagai sandaran kepada server primary dimana server tersebut akan bertukar menjadi aktif sekiranya berlaku kerosakan kepada server primary.



Gambarajah 2: Kerosakan berlaku kepada Apache Web Server 1 dan MySQL Master.

Sekiranya kegagalan berlaku pada Apache Web Server 1, floating IP akan berpindah ke Apache Web Server 2 secara automatic. Ini membolehkan sistem masih boleh dicapai oleh pengguna tanpa gendala dan mereka langsung tidak menyedari kerosakan yang telah berlaku seperti pada Gambarajah 2.

Walau bagaimanapun, senibina yang ditunjukkan masih mempunyai beberapa kelemahan seperti berikut:-

1) Failover server tidak akan digunakan sehinggalah primary server rosak, ini akan menyebabkan pembaziran sumber.
2) Terdapat dua set kod sumber masing-masing dalam Apache Web Server 1 dan 2, ini menyebabkan Pentadbir Sistem perlu memuat naik kod sumber kepada dua lokasi berlainan.
3) Oleh kerana fail session disimpan di primary server sahaja, pengguna akan terkeluar daripada sistem secara tiba-tiba dan perlu login semula (bayangkan jika beliau sedang memasukkan data).
4) Connection ke pangkalan data MySQL perlu ditetapkan secara manual, ini bermakna pertukaran IP host perlu dibuat dalam kod sumber dan akan menyebabkan waktu gendala.
5) Pertukaran connection ke pangkalan data MySQL Slave mungkin menyebabkan sistem tidak berfungsi terutama jika melibatkan operasi Insert/Update/Delete.

Namun begitu, meskipun dengan kelemahan-kelemahan yang masih ada, ianya adalah lebih baik berbanding daripada menggunakan hanya satu server virtual tunggal sahaja.

Artikel seterusnya akan membincangkan penambahbaikan kepada senibina di atas.

PANGGILAN UN AR PERJASA

YBhg Dato'/Dr./Tuan/Puan dipelawa untuk menghantar artikel selewat-lewatnya pada 31 Julai 2019 (Rabu) untuk membolehkan sidang redaksi membaca dan membuat semakan terlebih dahulu sebelum diterbitkan.

Berikut adalah kreteria artikel :

- ✓ Format : Text file atau Microsoft Word (.doc / .docx) sahaja
- ✓ Panjang : Tidak kurang dari 200 patah perkataanSkop : Semua bidang dalam ICT
- ✓ Jenis artikel : Perkembangan teknologi terkini, amalan terbaik, step-by-step instruction, kajian kes, mengimbas sejarah jabatan/kerajaan dalam teknologi, jangkaan masa hadapan dll.
- ✓ Artikel yang di larang : Berunsurkan politik, mengkritik dasar kerajaan secara keras, berbaur lucah, menyentuh sensitiviti keagamaan dan perkauman, jauh menyimpang dari bidang ICT.
- ✓ Bahasa : Bahasa Melayu dan Bahasa Inggeris.

Artikel yang telah siap hendaklah dihantar ke
alamat email naim.ibrahim@gmail.com dan jawatankuasa@perjasa.org.my

Semua karya hendaklah **asli** dan dikarang sendiri oleh penghantar.