CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defence Begins with Knowledge

Vol 36 - (1/2014)

Geotagging / Location Sharing - Warrantless Surveillance

Hantu Internet

Job Scam

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. "

Bruce Schneier, Secrets and Lies

ISSN 1985-1995

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia, an agency under Malaysia's Ministry of Science, Technology and Innovation was set up to be the national cyber security specialist centre. Its role is to achieve a safe and secure cyberspace environment by reducing the vulnerability of ICT systems and networks while nurturing a culture of cyber security. Feel secure in cyberspace with **CyberSecurity Malaysia.**

www.cybersecurity.my

Cyber999 Help Centre | My CyberSecurity Clinic | Professional Development (Training & Certification) | Product Evaluation & Certification (MyCC) | Information Security Management System Audit and Certification (CSM27001) | Malaysia Trustmark | Security Assurance | Digital Forensic & Data Recovery | Malaysia Computer Emergency Response Team (MyCERT) | Security Management & Best Practices | Cyber Security Research | CyberSAFE (Cyber Security Awareness for Everyone)

CyberSecurity
MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

T: +603 8992 6888
F: +603 8992 6841
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

1Malaysia
People First,
Performance Now

An agency under
MOSTI
Ministry of Science,
Technology and Innovation

Best Brand
Internet Security
2008 & 2009

ISMS SIRIM
UKAS INFORMATION SECURITY MANAGEMENT 074
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

STANDARDS MALAYSIA ACCREDITED LABORATORY
MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA
Status Company

Best Child Online
Protection Website

A MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Greetings and thank you for reading the 36th Edition of the e-Security Bulletin. This July issue is the first of two editions for 2014, with the other one to be published in December.

The e-Security is a platform for internal staff to contribute to the cyber security community by sharing their knowledge in the form of literature. The articles contained in this bulletin cover a variety of topics about cyber security matters, whether technical or generic in nature. Hence, the bulletin is hoped to appeal to all members of cyber community, not only to those highly involved in the technical aspects of cyber security.

Furthermore, the e-Security bulletin is a bilingual publication. Several articles are in English while a few more are presented in the local language, Bahasa Malaysia.

I would like to thank and commend all contributors for their nobility of sharing invaluable knowledge with others and also for their continuous support. Keep writing and keep sharing!

We're proud of our contributors and their selfless act in sharing knowledge and information. This is because we believe in leading by example. It's hard to think of a better example we could set than that of a responsible global citizen.

We look forward to continuing to bring you latest opinions and articles on various issues as well as keeping you updated on industry news.

Thank you and warmest regards,

DR. AMIRUDIN ABDUL WAHAB
Chief Executive Officer, CyberSecurity Malaysia

EDITOR'S DESK

Greetings,

Hello and welcome to the eSecurity Bulletin 1/2014!

With great pleasure, the editorial team has gathered an interesting variety of articles for 'santapan minda', a Malay saying which means "food for thought".

This time around, we grouped the articles into four categories: General interests, Current trends, Special, and Experiential.

General interests (Informative), such as "Mengenali Apakah Itu APT" (What is Advanced Persistent Threats), "Pengenalan kepada Phishing" (Introduction to Phishing).

Current trends consist of articles on social media, cloud security, mobile security, critical infrastructure protection, web intrusion and defacement, as well as Job Scam Modus Operandi.

The Special section contains more technical articles, such as the forensic analysis on SMS Timestamp, Steganography Substitution System Methods, and Measuring Security Awareness.

Experiential – which, for me personally is the most interesting category, comprises articles written by staffs who are hands-on and practicing cyber security on a daily basis. They are not always from a technical background; hence, the articles would attract a large reader's base. For instance, we have the "The Personal Data Protection Act 2010: Challenges to Comply", which brings you behind the scenes of the challenges in implementing PDPA in CyberSecurity Malaysia within a tight deadline. The Human Resources Security is another experiential sharing article, which would be truly valuable not only to HR personnel but also to any employer and bosses who wish to ensure that their employees or subordinates comply with their organisation's security policy.

We had a great time putting all these articles together to feed your hungry minds, so to say.

Thank you for your continuous support to the eSecurity Bulletin. For further inquiries you can reach us via this email: info@cybersecurity.my

Last but not least, I would like to convey the editorial team's utmost appreciation to all our contributors. Your articles are not only invaluable knowledge sharing but the articles also imparts useful tips on how to stay safe online.

Safe surfing everyone……and happy reading!
Be Smart! Be Safe!

Best regards,
Lt Col Mustaffa Ahmad (Retired),
Editor

TABLE OF CONTENTS

READERS' ENQUIRY
Outreach and Corporate Communications, Level 5, Sapura@Mines, No.7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia,
Level 5, Sapura@Mines,
No. 7 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

MyCERT 1st Quarter 2014 Summary Report

By | Sharifah Roziah Mohd Kassim

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysia Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by MyCERT. This summary report highlights statistics of incidents handled by MyCERT in Quarter 1 (Q1) 2014 according to categories, security advisories and other activities carried out by MyCERT personnel. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of such incidents.

Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian constituency. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents and Trends Q1 2014

Reported incidents to MyCERT are from various parties within the constituency as well as foreign ones. These parties include home users, private sector bodies, government sector agencies, security teams from abroad, foreign CERTs, Special Interest Groups (SIG) including MyCERT's proactive monitoring on several cyber incidents.

From January to March 2014, MyCERT, via its Cyber999 service, handled a total of 1,922 incidents. This represents 7.1 percent decrease of the total incidents 2,069 compared to quarter 4 (Q4) 2013. The highest decrease in incidents is fraud with 239 incidents lesser than the previous quarter.

Figure 1 illustrates the number of incidents that are classified according to the Categories of Incidents for Q4 2013 and Q1 2014.

Categories of Incidents	Quarter		Incidents %
	Q4 2013	Q1 2014	
Content Related	9	9	0.5
Cyber Harassment	145	143	7.4
DoS	1	6	0.3
Fraud	1033	794	41.3
Intrusion	333	401	20.9
Intrusion Attempt	37	38	2.0
Malicious Codes	348	430	22.4
Spam	157	95	4.9
Vulnerabilities Report	6	6	0.3

***Figure 1:** : Comparison of Incidents between Q4 2013 and Q1 2014*

Figure 2 illustrates the number of incidents according to the Breakdown of Incidents by Classification for Q1 2014.

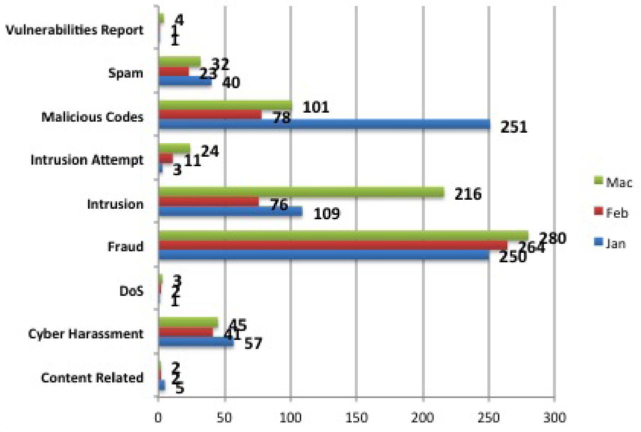


***Figure 2:** Breakdown of Incidents by Classification in Q1 2014*

Figure 3 illustrates the percentage of incidents handled according to categories in Q1 2014.

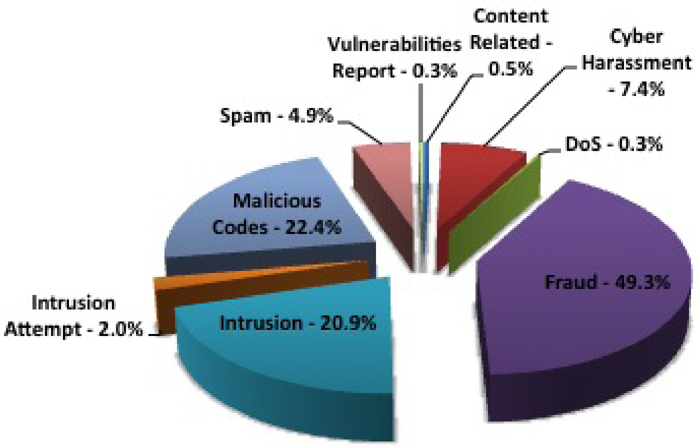


Figure 3: *Percentage of Incidents in Q12014*

In quarter 1 (Q1) 2014, the most number of incidents reported is fraud representing a 41.3 percent of the total number of incidents. Throughout the year 2013, fraud has been the most reported incident. A total of 794 fraud incidents were received in this quarter, from organisations and home users. Most of the fraud incidents reported involved phishing, job scams, fraud purchases and Nigerian scams.

MyCERT predict that fraud will continue to grow and always be among the most reported incident. Because of that, MyCERT advised Internet users to be precautious and always adhere to best practices when they purchase goods online. Users must ensure that the transaction is made with trusted parties and never simply transfer money to a seller without prior checking on the status of the seller.

The second highest incident reported is malicious code, which increased about 23.6 percent. The total malicious code incident reported for Quarter 1 2014 is 430. Throughout the year 2013 and including this quarter, malicious code is among the top three incidents reported to Cyber999. This is because MyCERT received continuous feeds from external parties about malicious code incidents that infected Malaysia. Upon receiving the feeds, MyCERT will respond by notifying the network and IP owner of the infected IPs.

The third highest incident reported to Cyber999 is intrusion with 401 incidents. Compared to the previous quarter, intrusion incidents increase by 68 or by 20.4 percent. As was in the previous quarters, web defacements or web vandalism that is part of intrusion incidents was still a continuous occurrence. Based on these findings, the majority of web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache. The majority of the defacement attacks were using SQL Injection and cross-site scripting (XSS) methods.

MyCERT observed for Q1 2014 a total of 175 .MY domains being defaced, representing a 60.1 percent of total defacement incident of .MY domains in Q1 belonging to various sectors such as private, educational and government. MyCERT responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations.

Figure 4 shows the breakdown of domains defaced in Q1 2014.

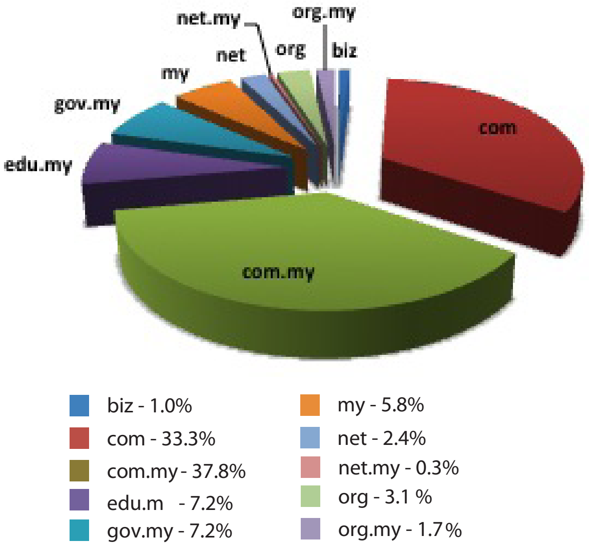


Figure 4: *: Percentage of Web Defacement by Domain in Q1 2014*

The situation related to MH370 had contributed to an increase in incidents reported in Q1 2014. The related incidents were defacements and malicious codes. The total defacement incidents related to MH370 was 61 but only one .gov site was involved. The most TLD that related to this incident was .com.my with 29 incident. Malicious code incidents that was connected with MH370 concerned Facebook Apps. When a user clicked on such apps, his/her computer will be infected with malicious codes.

Meanwhile, Cyber harassment incidents saw a slight decreased of 1.4 percent for this quarter, representing a total of 143 incidents. Harassment incidents generally involved cyber stalking, cyber bullying and threats. Social networking sites such as Facebook, Twitter, emails and chat programmes such as Yahoo Messenger, Skype have become popular avenues for cyber harassment as they are becoming popular communicating channels on the Internet. MyCERT warns users to be very precautious with whom they communicate on the net especially with unknown people and be ethical on the Internet.

Advisories and Alerts

In Q1 2014, MyCERT issued a total of 12 advisories and alerts with two alerts involving MH370, which was on Malware Related to Missing Malaysia Airlines MH370 Plane and Missing Malaysia Airlines MH370 Plane Found Hoax. The other alert and advisory was on Microsoft Ending Support for Windows XP and Office 2003, Critical Vulnerability in Microsoft Internet Explorer 9 and 10, Security Update for Adobe Flash Player and a New Zero-Day Exploit. The Alert and Advisory comes with descriptions, recommendations and references.

Readers can visit the following URL on advisories and alerts released by MyCERT:
http://www.mycert.org.my/en/services/advisories/mycert/2014/main/index.html

Other Activities

In Q1 2014, MyCERT personnel had conducted several talks, presentations and trainings at several locations. This included a talk at Agensi Nuklear Malaysia about WiFi security, training collaboration with UKM and a talk at APCERT AGM conference in Taiwan on 18-21 March 2014.

Besides the talks/presentations, MyCERT personnel had also conducted several Incident Handling training sessions for corporate and government organisations this quarter.

Conclusion

In conclusion, the number of computer security incidents reported to MyCERT this quarter had decreased by 7.1 percent as compared to the previous quarter. But there is an increase in several incidents like intrusion and malware. There is also an event related increase in the MH370 tragedy, especially on defacements. MyCERT advices users and organisations to be vigilant of the latest computer security threats and to take measures to protect their systems and networks from these threats.

Internet users and organisations may contact MyCERT for assistance. Our details are listed below:

Malaysia Computer Emergency Response Team (MyCERT)
E-Mail: cyber999@cybersecurity.my
Cyber999 Hotline: 1 300 88 2999
Fax: (603) 8945 3442
24x7 Mobile: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

Please refer to MyCERT's website for latest updates of this Quarterly Summary.■

Job Scam Modus Operandi

By | Juanita Abdullah Sani & Sarah Abdul Rauf

It's not hard to find someone who has been tempted by the offers. Especially among those who are struggling to make ends meet.

Introduction

An Internet user opened his email today and read an email that stated he successfully landed a job in a well-known company offering salary that was triple his current one. Without thinking twice and worried that the job offer would be given to someone else, he immediately replied to the email and gave his personal information. Without realising, he was actually duped by an online scammer. This type of scam is known as job scam.

Job scams or employment scams have been massively circulated since the year 2011 in Malaysia. There are various online scams but this type of scam is unique as it targets job seekers by posing as someone of authority from the recruitment department of selected companies. The industries that are most likely being targeted by job scams are Oil & Gas, Hotel and Hospitality activities.

Modus Operandi

Modus operandi refers to the usual ways that a particular criminal performs a crime. The modus operandi for a job scam is by emails, websites and phone numbers. The scammers will send emails to victims stating that they have been shortlisted for certain particular jobs and they need to provide their personal information to the scammer. The victims will communicate back and forth with the scammers using emails. To make the application more authentic the scammers will create websites that imitate the original companies that they claim they represent and provide phone numbers so that victims can call the numbers to verify the applications. Eventually some charges are imposed as processing fees to the wishful jobseekers to secure and obtain the jobs. Once the scammers have received the money, they will disappear and cannot be contacted. Based on MyCERT's experiences in dealing with job scams, several victims have even lost thousands of ringgit in value to these scammers.

As email is a major tool for this scam, MyCERT has gathered a few of these emails that have been used by the scammers. The email samples are shown in Table 1 below.

Gmail	Yahoo	Outlook
asstrecuitmentmanager	petronas.oilgasklmy300	workatpetronas2013
petronas.oilgasklmy2013	foreign.affairs_consultant	noorhamidassociates
petronas.oilgasklmy2002	petronas.oilgasklmy22	petronasoil.my
job.headhanter	petronas.oilgasklmy342	

petronas.oilgaskl20	petronas.oilgasklmy112	
petronasoilmalaysiajoboffers	petronas.oilgasklmy811	
petronas.oilgask12018		
petronas1petronas.oil		

Table 1: *List of emails used by job scamers*

The emails in Table 1 are just samples of the various emails used by these scammers. Other than Gmail, Yahoo and Outlook, these scammers also use other email services like Hotmail, MSN or spoofing emails of the companies they imitate. An example of these email services is an email from <officemail@petronascompanymy.com>.

Based on Table 1, MyCERT has observed that Gmail or Google Mail are amongst the favorite emails used by scammers. This is because when one uses the normal web interface for Gmail, the person is interacting with Gmail itself, not the Internet's email protocol. The first time the email enters the email protocol is when the email is sent from the Gmail server--so that is the first IP address that appears in the email header. IP address (Internet Protocol address) is a series of numbers that identifies a digital device such as our computers. IP address works likes a home address, it allows data to arrive at the correct Internet location.

Other email services like Yahoo will most likely reveal the IP address of the sender from the email's full headers. Due to that, the scammers' location can be detected by the technical assistance of an Internet Service Provider (ISP) together with Law Enforcement officers. On the other hand, Hotmail does not disclose the originating IP of a sender.

Similar to email addresses, scammers will repeatedly used the same phone number for their modus operandi. One distinct characteristic for the phone number is that the scammers will use mobile numbers instead of fixed line numbers so that their personal information and location is untraceable. Internet users who receive this kind of email, should know the emails are fake based on the phone numbers as most companies will not provide mobile numbers as their official contact points. Samples of phone numbers are shown in Table 2 below.

Contact Number		
60102145427	60162758426	60163949679
601126160959	60166752993	61116211192
60163148642	60163148642	61116211192
601126160958	61115586342	60143182568

Table 2: *List of mobile numbers used in Job Scams*

Finally, to make the job application email more authentic, the email will be sent by someone who appears to be the head of the human resource department or an attorney who manages the application or even someone from the Ministry of Foreign Affairs. In certain cases, the job application emails may appear to come from the Foreign Affairs Ministry, as these job scammers aim to target foreigners.

The above modus operandi (MO) of using emails, mobile numbers and websites are the common and popular methods for scammers to operate job scams. In several MyCERT investigations, we discovered that there is a new MO that is being circulated. The scammer will use instant messaging or IM for a job interview, amongst the reasons is that IM provides no valid contact information. The other new MO is texting, whereas in a real situation, a valid hiring manager will not be texting with any potential employee.

Statistics

Throughout the year 2013, MyCERT received a total of 151 incidents related to job scams. Figure 1 below shows the monthly distributions of job scam in 2013.

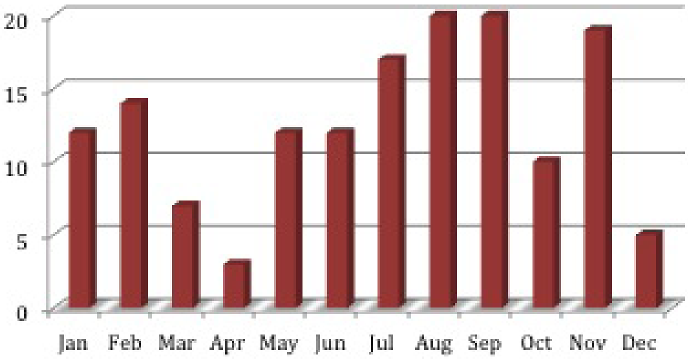


***Figure 1**: The graph depicting job scam incidents in 2013*

Figure 2 shows the comparison of job scam incidents between 2011 and 2013. The spike in job scam incidents was in 2012 where there were a total of 388 incidents. However, scammers will always find ways to improve the MO and Internet users should always stay alert to these changes. alert to these changes

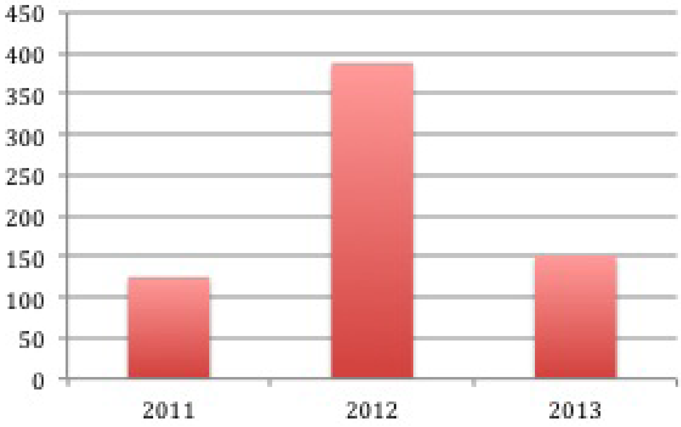


***Figure 2:** Job scam statistics for 2011 until 2013*

The most job scam impersonation revolves around a well-known company in the Oil & Gas industry based in Malaysia. MyCERT assumes that it is because the salary offered by that company is much higher as compared to any other small companies. Nevertheless, the MO for any job scam is almost the same no matter what the company appears to be. Figure2 below lists target industries by job scammers.

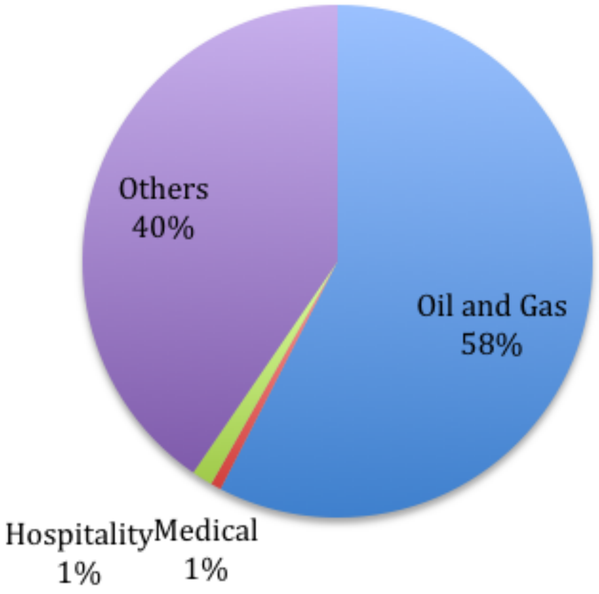


***Figure 2:** Job scam Target Industries in 2013*

Recommendation

MyCERT has released an alert regarding the job scam back in 2012 that can be referred to by Internet users. They may look out for the "red flags" listed below in suspicious emails that offers jobs, and once they identified these "red flags", they can just ignore such emails and never respond to them.

- Real companies will conduct an interview before offering a job and not just offer it via email.
- Look out for the scammer's email address. A contact email address being used is not a primary domain. For example, a Recruitment Department using a Yahoo! or Gmail email address.
- There may be inaccuracies and inconsistencies in the emails and the fake websites. For example spelling and grammatical errors.
- The fake websites will have inaccurate physical addresses and telephone numbers that belong to mobile numbers. Real websites will have correct physical addresses and will never use mobile numbers as their contact points.
- Fake job emails will also request users to bank in a certain amount of money to the fraudsters as processing fees for the jobs. A real job offer will never request for any processing fee.
- Look out for the web address. The web address may not reflect or bear the organisation's name.

Users who receive suspicios emails and need assistance, can report to Cyber999 at the contact details listed below:

E-Mail : mycert@mycert.org.my or cyber999@cybersecurity.my
Telephone: 1-300-88-2999 (monitored during business hours)
Facsimile: +603 89453442
Mobile: +60 19 2665850 (24x7 call incident reporting)
SMS: CYBER999 REPORT EMAIL COMPLAINT to 15888
Business Hours: Mon - Fri 08:30 -17:30 MYT
Web: http://www.mycert.org.my■

References:

1. *http://www.mycert.org.my/en/services/advisories/mycert/2012/main/detail/913/index.html*

2. *https://support.google.com/mail/answer/1198107?hl=en*

3. *https://productforums.google.com/forum/#!topic/gmail/L3dqotgK3Po*

4. *http://www.merriam-webster.com/dictionary/modus%20operandi*

5. *https://www.flexjobs.com/blog/post/new-job-scams-and-how-to-avoid-them/*

6. *MyCERT Definitions of Incidents http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/799/index.html*

7. *MyCERT Service Level Agreement (SLA) http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/800/index.html*

8. *http://cybersafe.my/guidelines.html*

Migrating to ISO/IEC 27001:2013 At Your Fingertips

By | Nooraida Aris

Digital environments have changed so much over the past years that some degree of obsolescence was inevitable.

1. Introduction

ISO/IEC 27001 Information Security Management System (hereinafter referred to as ISMS) is a management system standard for information security. The standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security for organisations. ISO/IEC 27001 is the backbone for the ISO/IEC 27000 series and it includes important clauses such as management commitment, risk management, training and awareness, and continuous improvements. By implementing ISMS and being an ISO/IEC 27001 certified organisation, an organisation may enjoy advantages such as improved organisational governance structure, better management of information security risks, compliance to business, legal and regulatory requirements and enhanced incident management.

Since ISO/IEC 27001 first became an international standard in 2005, there has been a very large increase in the number of ISO/IEC 27001 certified organisations in the world. According to statistics from the International Organisation for Standardization (ISO), ISO/IEC 27001 certificates issued in 2006 was 5,797 and the number of certificates exceeds 18,000 in 2012. In addition, the overall adoption by countries show an increase of 60 percent; showing 64 countries in 2006 to 103 countries in 2012.

Malaysia is one of the countries which have adopted the ISO/IEC 27001 ISMS certification. As of December 2012, there are 100 ISMS certified organisations in Malaysia (refer to Table 1).

Table 1: Number of ISO/IEC 27001 certified organisations in several countries (Source: www.iso.org/iso/home/standards/certification/iso-survey.htm)

Country	ISMS Cerifications as of 2012
Japan	7199
United Kingdom	1701
India	1600
China	1490
Romania	866
Chinese Taipei	855
Spain	805
Italy	495
Germany	488
USA	415
Hungary	199
Netherlands	190
Korea	181
Australia	113
Hong Kong	110
Malaysia	100
Thailand	96
Mexico	75
Philippines	66
Singapore	65
Canada	62
Vietnam	44
Indonesia	35

ISO/IEC 27001 was revised and only recently published on 1st October 2013. The revised version, known as ISO/IEC 27001:2013 Information Security Management System (ISMS) - Requirements, replaces the old ISO/ IEC 27001:2005 ISMS - Requirements which has been the main reference since 2005.

To ensure continuous compliance to ISO/IEC 27001, it is necessary for organisations with existing ISO/IEC 27001:2005 certification to migrate to the revised ISO/IEC 27001:2013. This article provides an overview of the changes in ISO/IEC 27001 since 2005, and guidance for organisations to migrate to ISO/IEC 27001:2013.

2. What's new in ISO/IEC 27001:2013?

The first major change is the structural change. This is to align the standard to other management system standards published by ISO. The new structure of ISO/IEC 27001:2013 mirrors the high level structure of the management system standards. Thus, the four mandatory clauses in ISO/IEC 27001:2005 have now been increased to eight clauses (refer Table 2). The new structure will make it easy for organisations that have achieved ISO/IEC 27001 certification to achieve other management system standard certifications such as ISO 9001, ISO 14001, etc.

Table 2: Mandatory clauses in ISO/IEC 27001

Mandatory clauses in ISO/IEC 27001:2005	Mandatory clauses in ISO/IEC 27001:2013
Clause 4 Information Security Management System	**Clause 4** Context of the organisation
Clause 5 Management responsibility	**Clause 5** Leadership
Clause 6 Internal ISMS audits	**Clause 6** Planning
Clause 7 Management review of ISMS	**Clause 7** Support
Clause 8 ISMS improvement	**Clause 8** Operation
	Clause 9 Performance evaluation
	Clause 10 Improvement

In addition, the risk assessment approach in this standard is more flexible as compared to the previous version. Requirement for risk assessment in ISO/ IEC 27001:2013 does not require that assets, threats and vulnerabilities to be identified. Thus, organisations are free to select whichever risk assessment methodology that suits them. As organisations may have an existing enterprise risk management approach, this will allow organisations to have a common risk assessment methodology even for information security risk assessment.

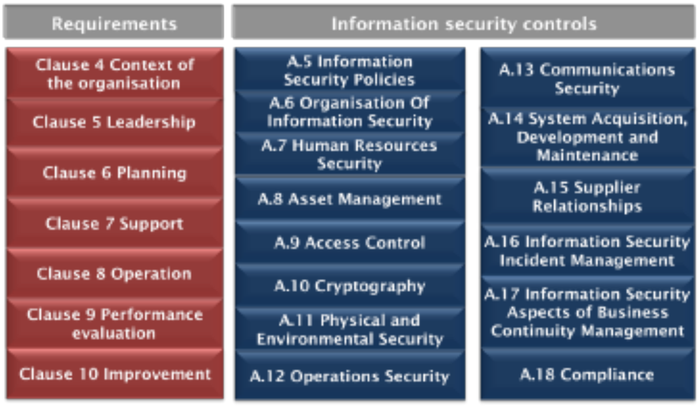
The other significant change to ISO/ IEC 2700:2013 is in Annex A. Annex A defines information security controls and the control objectives. This annex remains in ISO/IEC 27001 but the number of controls is reduced from 133 to 114 due to several controls being combined together. The number of control areas is now 14. They are:

A.5 Information security policies,
A.6 Organisation of information security,
A.7 Human resources security,
A.8 Asset management,
A.9 Access control,
A.10 Cryptography,
A.11 Physical and environmental security,

A.12 Operations security,
A.13 Communications security
A.14 System Acquisition, development and maintenance,
A.15 Supplier relationships,
A.16 Information security incident management,
A.17 Information security aspects of business continuity, and
A.18 Compliance.

Refer to Figure 1 for the overall view of the new ISMS requirements and information security controls in ISO/IEC 27001:2013.

Figure 1: Requirements and information security controls in ISO/IEC 27001:2013



Requirements

Clause 4 Context of the organisation
Clause 5 Leadership
Clause 6 Planning
Clause 7 Support
Clause 8 Operation
Clause 9 Performance evaluation
Clause 10 Improvement

Information security controls

A.5 Information Security Policies
A.6 Organisation Of Information Security
A.7 Human Resources Security
A.8 Asset Management
A.9 Access Control
A.10 Cryptography
A.11 Physical and Environmental Security
A.12 Operations Security
A.13 Communications Security
A.14 System Acquisition, Development and Maintenance
A.15 Supplier Relationships
A.16 Information Security Incident Management
A.17 Information Security Aspects of Business Continuity Management
A.18 Compliance

And lastly, the contents of standard has been revised and improved overall in the hope that it is better understood by organisations. For example, in ISO/IEC 27001:2005 version, the topics for conducting ISMS review were scattered in various clauses, but in this new standard, the topics were grouped together under Clause 9 Performance Evaluation.

3. How to migrate to the new ISO/IEC 27001:2013?

Firstly, organisations are recommended to send their relevant personnel for training sessions. Personnel who are in charge of ISMS should attend relevant training sessions to have a better understanding of these new requirements in ISO/IEC 27001:2013. Examples of the relevant training programmes are 'Introduction to ISO/IEC 27001:2013' and 'Migration to ISO/IEC 27001:2013'.

Next, organisations which have implemented ISO/IEC 27001:2005 are advised to conduct a thorough gap analysis. This is due to several requirements and controls that have been added, reviewed or deleted in the revised ISO/IEC 27002:2013. By conducting a thorough gap analysis, the organisation will be able to assess the gap between the current implemented ISMS and the new ISO/IEC 27001; and understand additional actions that are needed to be taken to comply with the new ISO/IEC 27001. They will also be able to develop a detailed plan with timeline for the ISO/IEC 27001:2013 migration.

Furthermore, organisations should review their current documents; as most probably they need to change and update their documents to suit to ISO/IEC 27001:2013. One document that must be updated is the Statement of Applicability (SOA). An SOA is a document describing the control objectives and controls that are relevant and applicable to the organisation's ISMS. SOA lists all information security controls that organisations have implemented and should be implementing. If there are new information security controls from ISO/IEC 27002:2013 that should be implemented, the SOA should be updated to reflect this change. Furthermore, there are also a possibility for organisations to develop new policy and procedure with regards to the new ISO/IEC 27001.

Finally, the necessity to conduct adequate awareness briefings to all relevant employees and external. The purpose is to educate employees on the changes and brief them on their additional roles and responsibilities (if any). Awareness to external parties should involve vendors and contractors.

4. What are guidelines that can help to migrate to ISO/IEC 27001:2013?

There is a document called Standing Document 3 (SD3), which was produced by the Working Group 1 (WG1) of Subcommittee 27 (SC27) that can provide guidelines to organisations intending to migrate to ISO/IEC 27001:2013. The purpose of SD3 is to show the corresponding relationship between the 2005 versions of ISO/IEC 27001 and ISO/IEC 27002 and the 2013 versions of ISO/IEC 27001 and ISO/IEC 27002.
This SD3 document contains three tables:

- **Table A:** Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005
- **Table B:** Comparison between ISO/IEC 27002:2005 and ISO/IEC 27002:2013
- **Table C:** Comparison between ISO/IEC 27002:2013 and ISO/IEC 27002:2005

The SD3 document is freely downloadable. Please refer to this URL http://www.jtc1sc27.din.de/sixcms_upload/media/3031/SD3.pdf. Organisations should be able to refer to these tables when trying to better understand the requirements and controls in the revised ISO/IEC 27001:2013.

5. When is the deadline to migrate to ISO/IEC 27001:2013?

Organisations which are currently certified with ISO/IEC 27001:2005 should not be worried as they will not need to migrate to the new ISO/IEC 27001:2013 immediately. There will be a transition period for migration to ISO/IEC 27001:2013 so that all tasks will be done in an orderly manner. According to International Accreditation Forum (IAF) 27th General Assembly (held in Seoul on 25 October 2013), a two year period from 1 October 2013 (which is the date of ISO/IEC 27001:2013 publication) is allowed for migration to ISO/IEC 27001:2013 (source : IAF Resolution 2013-13 – Endorsing a Normative Document). This means the last date for organisations to comply with ISO/IEC 27001:2013 is on 30 September 2015.

Conclusion

Organisations are advised to start their ISO/IEC 27001:2013 migration activities now and not wait until the last minute. Organisations are also advised to work closely with their certification body (CB) in order to ensure a smooth migration to ISO/IEC 27001:2013. Guidance provided in this article can be used as reference. By ensuring continuous compliance to ISO/IEC 27001, it is hoped that organisations will be able to continue managing information security in their organisations efficiently and effectively■

A Review on Steganography Substitution System Methods

The recent development of new robust techniques has now caught the eye of the privacy-craving public.

By | Nor Azeala binti Mohd Yusof, Abdul Alif Zakaria, Hazlin Abdul Rani, Nik Azura Nik Abdullah

1.0 Introduction

Nowadays, digital communication has become an essential part of our modern infrastructure. A lot of applications are Internet-based and this situation demands the security of data confidentiality and integrity so as to ensure that sensitive data and information on the Internet is protected against unauthorised access. There are various techniques that can be used to protect sensitive information. One of such technique is by using steganography. Unlike cryptography, steganography is the art of hiding and transmitting secret data. However, it is not intended to replace cryptography but to compliment it. The goal of steganography is to hide sensitive information in a cover so that no one can guess the existence of such information. The message will be inserted into the cover by modifying the nonessential pixels of the cover (Amirtharajan et. al., 2010).

2.0 Steganography Techniques, Characteristics, And Types

In order to obtain security, there are many suitable steganographic techniques that can be used. It depends on the type of the cover object (Hussain and Hussain, 2013). These known steganographic techniques are:

a. Image steganography: The image is used as the cover object and pixel intensities are used to hide the information.

b. Audio Steganography: The audio is used as the carrier. It has become very significant medium due to voice over IP (VOIP) popularity.

c. Network Steganography: The cover object is used as the network protocol and protocol is used as carrier.

d. Video Steganography: The video is used as carrier for hidden information.

e. Text Steganography: Using general technique, such as number of tabs, white spaces, capital letters, just like Morse code and etc.

Each technique embeds a message inside a cover. Various features characterise the method's strength and weaknesses. The importance of each feature depends on the application. Al-Ani et. al. (2010) classifies steganography systems into five characteristics which are capacity, robustness, undetectable, invisibility, and security.

Basically, there are three types of steganography (Al-Ani et. al., 2010).

a. Pure Steganography - does not require prior exchange of some secret information before a particular message is being sent. This type of steganography is more preferable for most application. Figure 1 shows how Pure Steganography works.

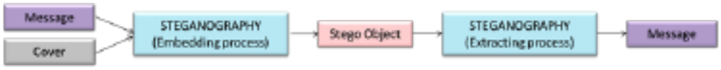

Message
Cover
STEGANOGRAPHY (Embedding process)
Stego Object
STEGANOGRAPHY (Extracting process)
Message

Figure 1: *Pure Steganography*

b. **Secret Key Steganography** - the sender chooses a cover and embeds the secret message into the cover using a secret key. It is similar to symmetric cipher in cryptography. Figure 2 shows how Secret Key Steganography works.

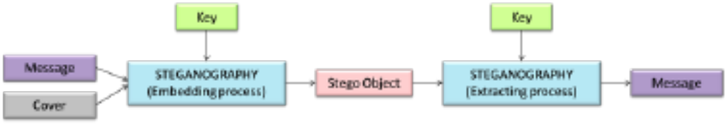

Key
Key
Message
Cover
STEGANOGRAPHY (Embedding process)
Stego Object
STEGANOGRAPHY (Extracting process)
Message

Figure 2: *Secret Key Steganography*

c. **Public Key Steganography** - requires two keys which are private key and public key. The public key is used in the embedding process and stored in a public database while the secret key is used to reconstruct the secret message.

There are several approaches to classify the steganography system. Al-Ani et. al., (2010) has classified steganography into six categories namely substitution systems, transform domains, spread spectrum techniques, statistical methods, distortion methods, and cover generating methods. However, only steganography substitution systems will be discussed further in this article.

Substitution System Methods

The basic idea of this substitution systems is to encode secret information by substituting insignificant parts of the cover with secret message bits. The information can be extracted if the receiver has knowledge of the positions where secret information has been embedded. By using this substitution system, the sender assumes that it will not be noticed by a passive attacker since only minor changes and modifications were made during the embedding process. Steganography substitution systems are divided into eight methods (Johnson et. al., 2000) shown in Figure 3. Each method will be discussed in the following subsections.

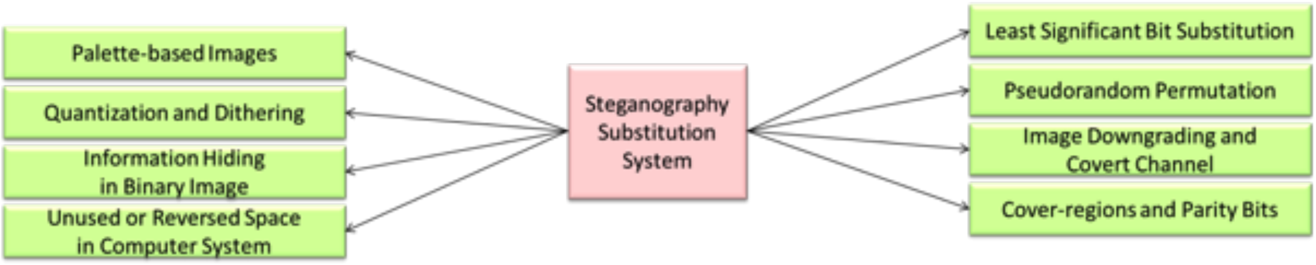

Palette-based Images
Quantization and Dithering
Information Hiding in Binary Image
Unused or Reversed Space in Computer System
Steganography Substitution System
Least Significant Bit Substitution
Pseudorandom Permutation
Image Downgrading and Covert Channel
Cover-regions and Parity Bits

Figure 3 : *Steganography Substitution System Methods*

A. Least significant bit substitution

Message and cover will be in binary form which only contains '0' and '1' bits. Figure 4 below shows the position of the most significant bit (MSB) and the least significant bit (LSB) in a binary representation.

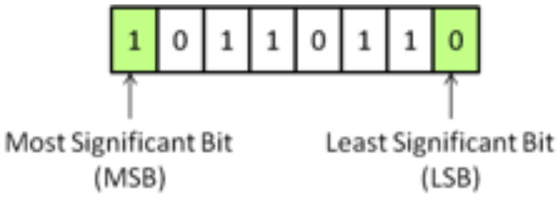


Figure 4 : *Binary Representation*

The embedding process starts by choosing the cover elements and performing the substitution operation on them. The least significant bits of the cover will be exchanged with the bit of message. This method allows more than one message bits to be stored in the two least significant bit of the cover. This process is illustrated in Figure 5. In this example, the cover contains all '0' bits, while the bit message contains all '1' bits.

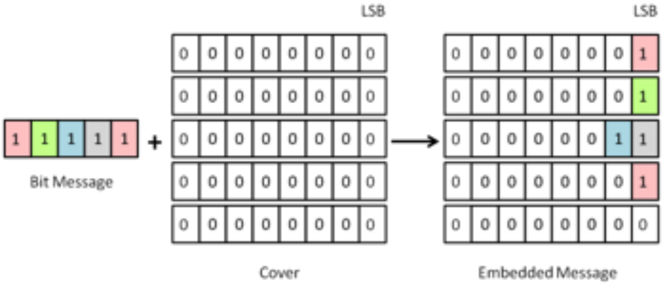


Figure 5 : *LSB Substitution*

In order to extract the secret message, the least significant bit of the selected cover-elements will be extracted and lined up. However, the sequence of element indices used in the embedding process must be accessible by the receiver. By using this method, information can be hidden with little impacts to the carriers. Because of the simplicity of applying it into image and audio, this method is now common to steganography.

B. Pseudorandom Permutation

In this method, a sequence of element indices will be generated by using a pseudorandom generator. Then the secret messages will be stored into the cover according to the bit position determined by the previous generated sequence. Therefore, the secret message bits can be distributed randomly over the whole cover if all cover bits can be accessed in the embedding process. Figure 6 below is an illustration of the pseudorandom permutation method.

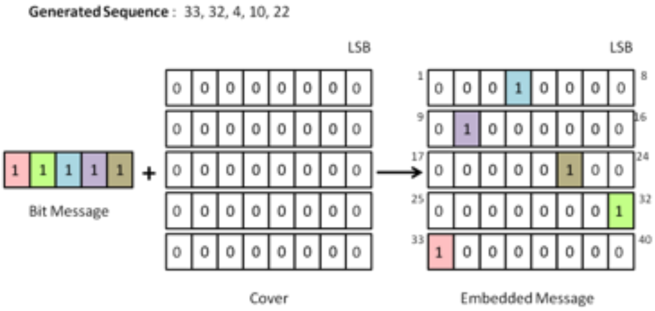


Figure 6 : *Pseudorandom Permutation*

C. Image Downgrading and Covert Channels

Image downgrading is a special case of a substitution system. It could be used to exchange images covertly. They are usually used for "leaking" information. Covert channels in operating systems allow processes to communicate "invisibly" and possibly across different security zones specified by a security policy. Images act both as secret messages and covers. In this method, a cover image and a secret image have an equal dimension. The sender exchanges the four least significant bits of the cover's grayscale values with the four most significant bits of the secret image. The receiver extracts the four least significant bits of the secret image. Four bits are sufficient to transmit a rough approximation of the secret image since the degradation of the cover is not visually noticeable in many cases. This process is illustrated in Figure 7 below.

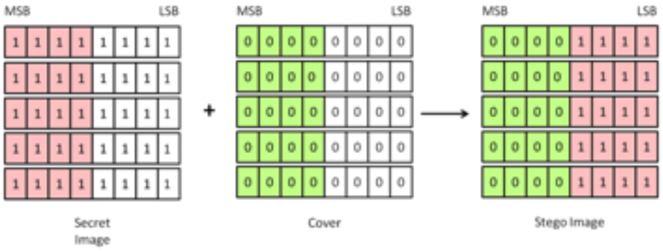


Figure 7 : *Image Downgrading and Covert Channels*

D. Cover-regions and Parity Bits

In this method, a pseudorandom sequence of disjoint cover-regions will be generated. A stego-key is used as the seed and only one bit of the secret message will be stored in a whole cover-region rather than a single element. During the embedding process, disjoint cover-regions are selected. Each encodes one secret bit in the parity bit. A parity bit of a region can be calculated by modulo the total numbers of '1' with 2. If the parity bit does not match with the secret bit to encode, one of the least significant bits in the cover region will be flipped. The parity bits of all the selected cover-regions are calculated and lined up to reconstruct the message at the receiver (Bandyopadhyay and Banik, 2012). This process is illustrated in Figure 8 below.

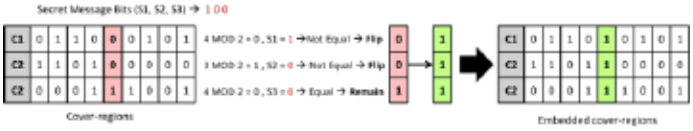

Secret Message Bits (S1, S2, S3) → 1 0 0
C1
C2
C2
4 MOD 2 = 0, S1 = 1 → Not Equal → Flip
3 MOD 2 = 1, S2 = 0 → Not Equal → Flip
4 MOD 2 = 0, S3 = 0 → Equal → Remain
Cover-regions
Embedded cover-regions

Figure 8 : *Cover Regions and Parity Bits*

E. Palette-based Images

This method emphasises the use of a subset of colours from a specific colour space that can be used to colorise the image as follows:-

a. A palette specifying N colours as a list of indexed pairs (i, ci), assigning a colour vector ci to every index i.

b. The actual image data which assign a palette index to every pixel rather than its colour value.

There are two techniques to be implemented; it's either manipulating the palette or the image data. The first technique encodes information in the palette. LSB of the colour vectors transfer information similar to the substitution methods previously presented. Information is encoded in the way the colours are stored in the palette because the palette does not need to be sorted in any way. There is sufficient capacity to encode a small message, since there are N! different ways to sort the palette. All techniques which use the order of a palette to store information are not robust. An attacker can destroy the secret message by simply sorting the entries in a different way.

The other technique encodes information in image data. Any approach of changing the LSB of some image data fails because neighbouring palette colour values need not be perceptually similar. Colours with similar luminance values may be relatively far from each other but it may generate very noticeable artefact (Wang et. al., 2005). However, colour values can, for instance, be stored according to their Euclidian distance in RGB space:

$$d = \sqrt(R^2+G^2+B^2)$$

Another approach would be sorting the palette entries according to their luminance components since the human visual system is more sensitive to change in the luminance (intensity) of a colour. The LSB of colour indices can safely be altered after the palette is sorted.

F. Quantisation and Dithering

Quantisation and dithering of digital images can be used for embedding secret information. Some steganographic systems operate on quantised images (Al-Ani et. al., 2010). Definition of quantisation is reviewed in the context of predictive coding. Prediction of the intensity of each pixel is based on values of the pixel in a specific neighbourhood. Outcome of the prediction may be a linear or nonlinear function of pixel values surrounding it. A discrete approximation of the difference signal is obtained by feeding calculated difference between adjacent pixels into a quantiser. Each quantisation step will introduce a quantisation error. Additional information in steganography is transmitted by adjusting the difference signal.

G. Information Hiding in Binary Images

It is difficult to implement this technique due to the fact that changing one bit in a binary image is easy to detect as it change the colour from black to white or the opposite (Al-Jaber and Sabri, 2003). This technique can be divided into two different techniques. The first hiding scheme encodes secret information using the number of black pixels in a specific region. The colour of some pixels is changed so that the desired relation holds. If neighbouring pixels have the opposite colour, modification will be carried out to those pixels. Modifications are carried out at the boundaries of black and white pixels in sharp contrasted binary images.

The other technique uses a combination of run length (RL) and Huffman encoding. The fact that in a binary image successive pixels have the same colour with high probability is utilized in RL techniques. Modification of the least significant bit of RL is carried out to ensure that information can be embedded into a binary, run-length encoded image.

H. Unused or Reserved Space in Computer Systems

Steganography implementation in these techniques takes advantage of unused or reserved space to hold covert information without perceptually degrading the carrier. Under Windows 95 operating system, 32Kb of minimum space is allocated to a file. For a file with the size of 1 Kb, an additional 31Kb is said to be “wasted” because it has been unused. Information can be hidden without being noticed in the directory.

Another technique is implemented by creating a hidden partition that is unnoticeable if the system is started normally (Viswam, 2010). Unused space exists in the packet headers of TCP/IP packets that are used to transport information across the Internet. There are six unused (reserved) bits in the TCP packet header and two reserved bits in the IP packet header. In each communication channel, thousands of packets that are transmitted provide an excellent covert communication channel if left unchecked.

4.0 Conclusion And Future Projects

Some of the substitution system methods are facing problems during the embedding process. The substitution system methods that are ridden with problems are listed in Table 1 below.

Method	Problem
Least Significant Bit	Which way should the cover sequence be chosen? If secret message is shorter than cover elements, sender can leave all other elements unchanged. It may cause different statistical properties in the first part (modified cover-elements) and second part (unchanged cover-elements) of the cover-elements.
	It changes far more elements than the transmission of the secret would require. Therefore the probability that an attacker will suspect secret communication increases.

Pseudorandom Permutation	One index could appear more than once in the sequence, since there is no output restriction of pseudorandom number generator. This event is called as “collision”. It will try to insert more than one secret message bit into one cover-element, thereby corrupting some of them.
Image Downgrading and Covert Channels	Information downgrading due to declassify or downgrade information by embedding classified information into objects with a substantially lower security classification.
Palette-based Images	All methods which use the order of a palette to store information are not robust since an attacker can simply sort the entries in a different way and destroy the secret message.

***Table 1**: Problems in some Substitution Methods*

Due to the listed problems, changes and improvements to the current techniques need to be done. The weaknesses of the current techniques give some ideas to develop better embedded techniques using steganography substitution system methods.

References

1. *Johnson N.F., and Katzenbeisser S.C. 2000. A survey of Steganographic techniques. Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.*

2. *Al-Ani Z.K., Zaidan A.A., Zaidan B.B., and Alanazi H.O. 2010 Overview: Main fundamentals for Steganography. Journal of Computer. 2(3): 158-165.*

3. *Amirtharajan R., Akila R., and Deepikachowdavarapu P. 2010. A Comparative Analysis of Image Steganography. International Journal of Computer Applications.2(3): 41-47.*

4. *Kaur R., Singh R., and Singh B., and Singh I. 2012. A Comparative Study of Combination of Different Bit Positions in Image Steganography. International Journal of Modern Engineering Research (IJMER). 2(5): 3835-3840.*

5. *Hussain M. and Hussain M. 2013. A Survey of Image Steganography Techniques. International Journal of Advanced Science and Technology. 54: 113-123*

6. *Yadav R., Saini R., and Kamaldeep. 2011. Cyclic Combination Method for Digital Image Steganography with Uniform Distribution of Message. Advanced Computing: An International Journal (ACIJ). 2(6): 29-43.*

7. *Sumathi C.P., Santanam T., and Umamaheswari G. 2013. A Study of Various Steganographic Techniques Used for Information Hiding. International Journal of Computer Science & Engineering Survey (IJSES). 4(6): 9-25.*

8. *Kayarkar H. and Sanyal S. 2012. A Survey on Various Data Hiding Techniques and Their Comparative Analysis. ACTA Technica Corviniensis. 5(3).*

9. *Wang H. and Wang S. 2004. Cyber Warfare: Steganography and Steganalysis. Communications of the ACM. 47(10)*

10. *Petricek V. (2001). Information Hiding and Covert Channels. Proceeding of 14th Annual Student Week of Doctoral Students, Prague.*

11. *Bandyopadadhayl S.K. and Banik B.G. (2012). International Journal of Emerging Trends & Technology in Computer Science (IFETTCS). 1(2): 71-74.*

12. *Wang X., Yao Z., and Li C. (2005). A Palette-Based Image Steganographic Method using Colour Quantisation. IEEE International Conference. 2.*

13. *Viswam D. 2010. Steganography. Seminar Report, School of Engineering, Cochin University of Science & Technology Kochi.*

Transition to ISO/IEC 27001:2013

By | Razana Md Salleh, Wan Nasra Wan Firuz, Nahzatulshima Zainudin, Rafidah Abdul Hamid, Sharifah Norwahidah Syed Norman

Introduction

The first revision on ISO/IEC 27001 was finally published in Quarter 4 of 2013. This has caused a stir in the older standard (2005 version) certified organisations as well as for organisations that are planning to be certified in the near future. Currently, there are 169 certified organisations from local certification bodies in Malaysia. As a certification body, CyberSecurity Malaysia (CSM) receives numerous questions pertaining to the transition period and the adoption of this new version. Therefore, this article provides a general overview regarding the transition to ISO/IEC 27001:2013 from the perspectives of a certification body. The information is summarised in a Q&A format based on frequent questions that were posed to CSM.

i. When was it published?

The new revised standard ISO/IEC 27001:2013 was published on the 1st of October 2013.

ii. Is the previous ISO/IEC 27001:2005 still valid after 1st October 2013?

No. The new version cancels and replaces the ISO/IEC 27001:2005 version. However, existing certified organisations are given two years to migrate from version 2005 to version 2013.

iii. When do I have to conform to the new 2013 revision?

For organisations that will be implementing ISMS after 1st of October 2013, it is encouraged to immediately conform to the new 2013 version. For existing certified organisations, the transition period given by the International Accreditation Forum (IAF) is two years from the release date. The deadline for conformance to the new standard is 1st of October 2015.

iv. What if my organisation is already certified with the old 2005 standard? Do I have to do it all over again?

The new 2013 revision is geared to focus more on the ability to measure the ISMS. A subsection focusing on measurement has been created to support this. It provides guidelines on how to evaluate information security performance. There are also a few new terms introduced such as “Risk Owner”, previously known as “Asset Owner”; “Stakeholders” is now named as “Interested Parties” and “Documents and Records” is now called “Documented Information”. A few additional documents may need to be developed to address the new requirements; whereas a few other documents could be dropped. **Table 1** will provide you with a minimum set of documents required to fulfil the 2013 version.

Organisations are also encouraged to prepare a transition plan and submit it to the relevant certification body. This will help the certification body to analyse the requirements and plan visits.

		ISO 27001:2013 clause
*Documents	Scope of the ISMS	4.3
	Information security policy and objectives	5.2, 6.2
	Risk assessment and risk treatment methodology	6.1.2

	Statement of Applicability	6.1.3 d)
*Documents	Risk treatment plan	6.1.3 e), 6.2
	Risk assessment report	8.2
	Definition of security roles and responsibilities	A.7.1.2, A.13.2.4
	Inventory of assets	A.8.1.1
	Acceptable use of assets	A.8.1.3
	Access control policy	A.9.1.1
	Operating procedures for IT management	A.12.1.1
	Secure system engineering principles	A.14.2.5
	Supplier security policy	A.15.1.1
	Incident management procedure	A.16.1.5
	Business continuity procedures	A.17.1.2
	Legal, regulatory, and contractual requirements	A.18.1.1
*Records	Records of training, skills, experience and qualifications	7.2
	Monitoring and measurement results	9.1
	Internal audit program	9.2
	Results of internal audits	9.2
	Results of the management review	9.3
	Results of corrective actions	10.1
	Logs of user activities, exceptions, and security events	A.12.4.1, A.12.4.3

***Table 1**: Minimum set of documents and records required by the new 2013 revision*

v. What are the documents and records that need to be produced for the new 2013 revision?

Many organisations used to complain about the amount of documents they had to produce for the 2005 version; however the new 2013 revision omits quite a number of those documents. For example, there is no requirement to develop an "ISMS Policy" but an "Information Security Policy" will suffice. See **Table 1** for the minimum set of documents and records required by the new 2013 revision. This is by no means a definitive list of documents and records – any other documents are to be added to improve the level of information security.

vi. I am currently implementing the 2005 version and will go through certification audits in the near future. What about my current implementation?

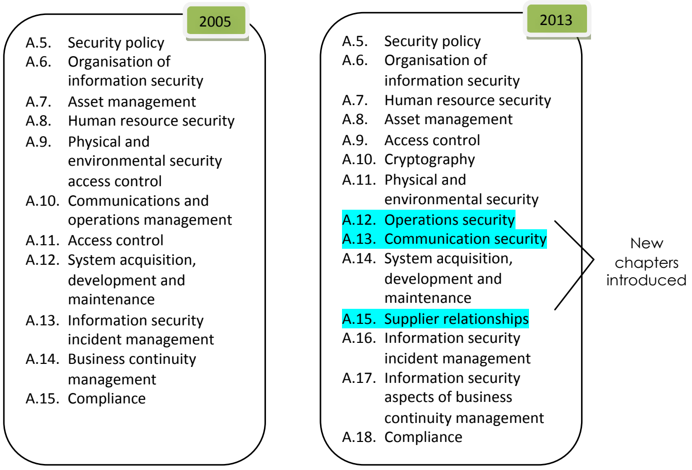
If you are at the early stages of implementing the 2005 version, and unlikely to go through the certification audits before 1st October 2014, it is better to pursue the new standard ISO/IEC 27001:2013.

vii. What are the other changes in the new 2013 revision?

- The new version of ISMS emphasises on business requirements and expectations of interested parties. It aims to add greater economic opportunities to the business community. To allow this to happen, the **PDCA model has been removed.**
- The revised version has **113 controls**, as opposed to the original 133 controls in the 2005 version. There is now **14 control domains** in the current version; compared to the previous 11

control domains (Figure 1).

- The risk has been aligned with ISO 31000:2009 (Risk Management—Principles and Guidelines), making the risk assessment requirement more general. It is **no longer necessary to identify assets, threats and vulnerabilities**. However, if the risk methodology uses an approach based on assets, threats and vulnerabilities, it is acceptable too.
- When implementing ISMS, the **controls must first be determined in the risk treatment process, before comparison is made with Annex A.**



2005

A.5. Security policy
A.6. Organisation of information security
A.7. Asset management
A.8. Human resource security
A.9. Physical and environmental security access control
A.10. Communications and operations management
A.11. Access control
A.12. System acquisition, development and maintenance
A.13. Information security incident management
A.14. Business continuity management
A.15. Compliance

2013

A.5. Security policy
A.6. Organisation of information security
A.7. Human resource security
A.8. Asset management
A.9. Access control
A.10. Cryptography
A.11. Physical and environmental security
A.12. Operations security
A.13. Communication security
A.14. System acquisition, development and maintenance
A.15. Supplier relationships
A.16. Information security incident management
A.17. Information security aspects of business continuity management
A.18. Compliance

Figure 1 : *The New Controls Added to ISO 27001:2013 Annex A as opposed to the old version*

*Controls from **Annex A** can be excluded if the organisation concludes there are no risks or other requirements which would demand the implementation of a control.

In the new 2013 version, controls must first be determined in the risk treatment process before comparison is made with Annex A. These controls can come from other best practices or sector specific standards. There would be three different situation where the controls from Annex A can be utilised as depicted in Figure 2. In the first situation, the there is a 100 percent overlap between the selected controls and Annex A. In the second situation, there is a partial overlap between the selected controls and Annex A. Finally, in the third situation, there is a 100 percent segregation between the selected controls and Annex A. As such, we look forward to see the new 2013 implementation.

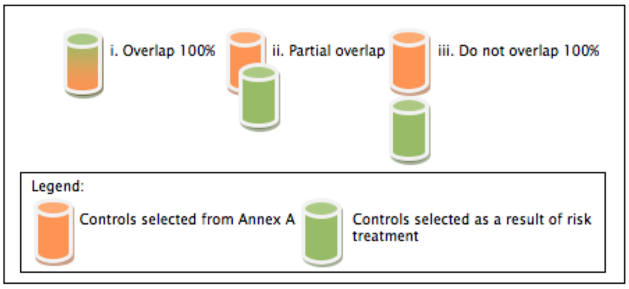

i. Overlap 100%
ii. Partial overlap
iii. Do not overlap 100%
Legend:
Controls selected from Annex A
Controls selected as a result of risk treatment

Figure 2 : *Different situations in utilizing controls from Annex A*

viii. What happens after the transition period ends?

On the 1st of October 2015, two years after publication of the new version, all certified organisations are expected to be in full compliance with ISO/IEC 27001:2013 and have new certificates issued. On the 2nd of October 2015, all certificates referring to ISO/IEC 27001:2005 or MS ISO/IEC 27001:2007 will become invalid and withdrawn.

Conclusion

Meeting the requirements of the new standard has never been easier. However, this new version has been revised through practical experiences from the older version, making it more flexible and giving more freedom on how to implement it. For further details, kindly contact csm27001@cybersecurity.my.■

Reference:

1. *The All New ISO 27001:2013 – Nothing Much to Worry, http://www.cyberintelligence.my/blog/*
2. *Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision), Information Security & Business Continuity Academy*
3. *Certified Organisation Register - http://csm27001.cybersecurity.my/org-cert.html*
4. *QMS Certification - http://www.malaysian-certified.my/*

Knowledge Hoarding versus Knowledge Sharing: A Transformation

It is essentially collaboration intelligence – giving us ideas and ways to optimise what we never had before.

By | Zaleha Abd Rahim

Introduction

We often hear someone proclaim, "Why should I share my knowledge? If I am the only one who knows how to do this, my position is secured and the management can never fire me". This is a fundamental and common problem that exists in a workplace because this type of person used knowledge as 'insurance' plan. However, this knowledge hoarding attitude is the most serious cost which may stifle an organisation especially when it involves innovation. Knowledge is essential for knowledge-based organisations and knowledge sharing is critical for these organisations to survive in the 21st century. Most organisations tend to rely on staffing and training in order to stay competitive. Therefore, organisations need to find ways on how to transfer expertise and knowledge from experts to novices who need to know. In other words, organisations must consider a transformation culture from knowledge hoarding to knowledge sharing.

Hoarding Knowledge

Knowledge hoarding exists when someone knows something but is either unwilling to share what they know or at least disclose the source of their knowledge. It can be considered as a disease within the information ecosystem of an organisation. Knowledge hoarding is an evil twin of knowledge sharing and is often considered as the result of bad knowledge management or an unhealthy informational environment. There are several reasons why people are reluctant to share knowledge such as:

- People perceive knowledge as power that makes them feel secure, safe and/or powerful. They hope to benefit in terms of dollars, power and credibility from having exclusive knowledge.

- There are no incentives or rewards for sharing knowledge. Most organisations reward staff for what they know and not what they share.

- Professionals are afraid to reveal or take any risks that they might not know something or be shown wrong and this will make them feel embarrassed.

- People perception that sharing knowledge will reduce his/her own value, prestige or recognition.

- Lack of understanding and appreciation on the value of sharing knowledge.

- Too busy and even with the best intentions do not develop a habit of knowledge sharing.

- Lack of clarity on issues of confidentiality which can lead to either withholding information that can be helpful or sharing it inappropriately.

What is Knowledge Sharing?

Knowledge sharing is an activity through which knowledge (i.e. information, skills, or expertise) is exchanged among people, friends, or family members, a community or an organisation. By knowledge sharing employees can contribute to knowledge application, innovation, and ultimately the competitive advantage of an organisation. Advancements in ICT and communications connectivity has multiplied the potential for knowledge sharing and wealth creation. Research has shown that knowledge sharing is positively related to cost reduction, speedier project completion, resolving critical issues just in time, spikes in team performance, innovation capabilities and increase performance in sales growth and revenue from new products or services.

Benefits of Knowledge Sharing

Knowledge sharing within a workplace is one of the most critical cultural values of an organisation. If we share knowledge and good practices with others, this may lead in increasing employees' productivity without increasing costs in the areas of time and training. Knowledge sharing is more than giving pertinent information to others within the organisation. It is sharing knowledge to enable positive cultural transformation to turn into successful business innovation and solving critical issues.

Listed below are several benefits in sharing knowledge:

- Cost effectiveness where new knowledge is developed and then re-used by many people
- Enhancement of effectiveness and efficiency by spreading good ideas and practices
- Time saving where we learn from our own mistakes and those of others
- When we share problems, our obtain emotional relief and this will decrease tension
- Solving problems brings people together and this will strengthen professional bonds and connections
- Increase in innovation and new discovery as well as excitement, engagement and motivation
- A feeling of satisfaction much like giving charity or making a contribution to society
- Respectful ways of using knowledge - with attribution and permission and this will benefit the person who generates the knowledge and the person who shares it

Environment for Constructive Knowledge Sharing

Trust is the key element in knowledge

sharing. Employees may not be willing to share their knowledge especially work-related knowledge if they believe that hoarding knowledge will assist them in furthering their careers or if they feel ill-treated at work. Therefore, organisations should create environment where ideas and assumptions can be challenged without fear and where diversity of opinion is valued and appreciated over commonality or compliance.

- Create habits or routines for sharing such as in meetings and informal gatherings such as 'Cafe Ilmu', Book Chat, Roundtable Discussions, etc.

- Move from a reactive to proactive sharing culture - change your mentality of knowledge sharing from a need to know to a need to share. Most of us would not care less about leaving a legacy behind the organisations when they leave. In fact, the concept of leaving a legacy behind is more rewarding when the knowledge you shared is reused by others, even when you are not there anymore.

- Create opportunities for serendipitous conversations especially in a very informal ways such as coffee corners, brown bags, 'Sembang Teh Tarik' or even designed for virtual serendipity.

Summary

Knowledge sharing is not about blindly sharing every bit of knowledge you have; or giving away your ideas; or being so naive and reveal absolutely everything. If you have a great idea, don't simply share the idea with your competitor either internal or external. On the other hand, don't try to develop the idea on your own and don't sit on it for fear of it being stolen from you. Identify a right mechanism and techniques to share the idea and get the recognition.

In today's digital world, hoarding knowledge ultimately erodes your power. If you know something that is very important or new knowledge discovery, the way to get power is actually by sharing it. As the old saying goes, the knowledge shared with the right intent can do wonders for any person or organisation.■

References:

1. *Sheng Wang and Raymond A. Noe, "Knowledge sharing: a review and directions for future research", Human Resource Management Review, Volume 20, pp. 115-131, 2010*

2. *http://copbibliography.wikispaces.com/file/detail/Barrier+and+Benefits+to+Knowledge+Sharing.doc*

3. *http://www.examiner.com/article/hoarding-knowledge-job-security-for-employees-or-bad-for-business*

4. *http://thepoint.gm/africa/gambia/article/effective-knowledge-sharing-and-its-benefits*

5. *http://www.citehr.com/367738-importance-knowledge-sharing-organizations.html*

6. *http://www.elsua.net/2010/09/06/why-is-knowledge-sharing-important-a-matter-of-survival/*

Securing Your Smartphone. Why It Is Important?

There is a need to bridge the gap between a user's choice of device and the demanding management and security they require.

By | Kamarul Baharin Khalid

Advances in communication technology have created an explosion on how we can reach and communicate with each other. Several years back, the only main function of a phone were to call and to send short text messages. However, nowadays, we have smartphones that functions similar to mini computers with functions that enables us to run our whole lives on it. These tools have become a necessity and increasingly useful. In fact, our digital life resides on and can be accessed via these devices that makes our smartphones a huge mine of data about us. No doubt, this is potentially sensitive and damaging. Therefore, securing our smartphones is not just necessary but a necessary practise.

Contact apps stores all your personal and business contact numbers and addresses. SMS apps stores all your text messages. Calendar apps stores all your appointments, birthdays, anniversaries and events. Reminder apps stores your daily to do list such as picking up the kids, taking pills, etc. Note apps stores all your personal notes like usernames, passwords, bank account numbers, etc. Camera/ Photo apps stores all your private, personal and family pictures and also locations where these pictures were taken. Social networking apps install applications such as Facebook, Twitter, Instagram, etc., which you can now access at your fingertips. These apps give you easy access for updating, reading and surfing websites. Email apps stores all your communications with others whether they are private or not. Not forgetting any document you store on the smartphone either copied from your computer or extracted from your emails. Your daily life events are stored on these apps in the smartphone.

With these information, anyone who have access to your smartphone, could have access to your daily private life information as well. One possible threat that can harm you if your private life information is exposed is identity theft. For example, if others can access your Facebook app, they can post on your Facebook wall or your friend's wall as if you are the one who is posting it. This act may well take place along with other apps like email, SMS, etc. Another possible threat is Blackmailing. For example, if your photo apps are accessible to others, they can use your private photos for their own benefits.

Therefore, it is advisable to switch on or enable the security features that are available in your smartphone just to prevent others from easily accessing your private information. Some security features are not built-in the smartphone itself but can be added by installing a 3rd party security app.

One of the basic security feature that comes with most smartphones is the lock screen pattern or passcode. This security feature, if enable, will lock the smartphone with a pattern or passcode when it is not in use. A few smartphones can even lock certain apps from running using this security feature. When enabled, your smartphone will be protected with the pattern or passcode and a user need to enter the right code correctly in order to unlock or run the locked apps. Without unlocking the smartphone or able to run apps, your private data will be protected.

Another security feature that you can enable on your smartphone is the tracking security system. This system can track where your smartphone is currently located and with its alarm sound, you can find where your smartphone is located if it is misplaced. But not all smartphones have this feature built-in. If it is not built-in, you can install it using a 3rd party anti-theft security app. Most security software for mobile comes with this feature. By default, this security system is off. You need to switch it on.

One more security feature that you can enable on your smartphone is remote wipe. This is your last security defence for your private data on the smartphone. This feature can wipe or erase your data remotely through SMS or Web access. If your smartphone is stolen and cannot be traced, activate this security feature so that all your private data will be erased automatically as if your phone is newly bought and you don't have to worry about your private data being access by others.

By enabling these security features does not mean that your data is 100 percent secure. However, these security features will at least delay the process by making it harder for others to access your private data inside your smartphone. A little security is better than none.■

Geotagging/Location Sharing-Warrantless Surveillance

By | Mohd Rizal bin Abu Bakar

Introduction

Have you ever felt like you are being watched online?

Without realising it, every user on the Internet, specifically on social networking sites, are being watched. In real time.

How long has it been since you sieved through your friends/followers list and thought, “Do I know this guy?”

Yes, those who carefully approve friend requests or followers have a lesser chance of getting an unknown profile on Facebook or Twitter looking at your every post, shares, likes and check-ins. But those who are in the dark need to re-evaluate these ‘friends/followers’ and take a good look at your social media account settings. Privacy in social networking, it seems, is not its best virtue.

In recent years, there have been multiple cases of cyber stalking. Although we rarely hear or see these in the news, it does not mean stalking individuals online is not a serious crime.

With more features developed for the Internet’s latest craze, social networking sites such as Facebook, Twitter and Instagram, many users have forgotten one of the dark side of socialising online-location sharing.

The trend of getting as many likes, friends and followers on social media accounts is a magnet in attracting unwanted attention. And with unwanted attention, comes dangerous consequences.

Many will think that without geotagging/location sharing features, social networking will not be able to function as it should; which is to share everything with your friends and followers.

So what is it about geotagging? And why is it dangerous?

Geotagging/Location Sharing

Location sharing is a feature developed to complement social networking sites. This feature allows users to share their GPS based locations from their smartphones and tablets via their favourite social networking apps, such as Facebook and Twitter.

In other words, it complements Facebook posts or Twitter tweets by providing friends and followers with a ‘shout out’ stating-I am here/I posted this photo from here.

Because the main feature of the technology is to complement social networking, developers of these apps always have the feature turned on by default. Which is not always a good thing.

Stalking Carrie Bugbee

Careless usage in using the technology can be highly dangerous, which was proved in the case of Carrie Bugbee (Seville, 2010), a social media-marketing strategist from BigDeal PR, a public relations company based in the United States.

As a social media expert in marketing services and products online, Bugbee is a regular user of geotagging. She has multiple social media accounts and many friends and followers-7,164 Twitter followers, 1,197 Facebook friends and more than 500 connections on LinkedIn to be exact and regularly shares her posts, tweets, and photos online.

Naturally, as a social media strategist, Carrie Bugbee jumped on the bandwagon of geotagging as a user. What happened next completely floored her view of professionalism in terms of social media marketing and as an individual/a common Internet user.

In February of 2010, Bugbee 'checked-in' (a geotagging term) using Foursquare on her phone to a local restaurant where she was having lunch with a friend. Now, here comes the scary part.

A waitress came over and told Bugbee she had a call on the restaurant telephone. Thinking it was an emergency, she answered the call and an unknown male voice was on the other line told her that she should not use Foursquare, as the app could reveal to the public where she lived.

Thinking it was a prank, Bugbee did not think much of it and laughed it off, but it was replied with a snarl and insults. In shock, Bugbee hung up the telephone.

Apparently, the stalker had used a website called PleaseRobMe.com (now defunct) a website which was created to do the opposite of what had happened to Carrie Bugbee-to warn Internet users of the dangers of geotagging/location sharing apps.

PleaseRobMe.com does this in the most peculiar way-the website publicised the location data from users of social networking sites. In Bugbee's case, the website had served its purpose; albeit the incident.

Because geotagging in smartphones and tablets is greatly assisted by the fact that these devices are mobile and most have data connections available all the time, unwary social media users are able to use their favourite apps to update their statuses anywhere and at anytime.

Consider this geotagging statistics conducted by Pew Research Center for 2011-2013 (ZICKUHR):

- 74 percent of adult smartphone users get directions or other information based on their current location.
- 12 percent of smartphone users use geosocial services such as Foursquare to check-in to certain locations and share that information.
- 30 percent of adult social media users use at least one of their accounts setup to include their location in posts.

The survey also found that the number of "check-in" services have declined from 18 percent to 12 percent since 2012 but is still widely used. Foursquare "check-in" services have declined compared to Facebook "Places".

There has not been a proper survey on why the use of Foursquare geosocial service declined. However, this is most probably due to the fact that Facebook has more features compared to Foursquare and triple the amount of users. Another possible reason is that Facebook has more concentration on general content compared to the singular focus of user location of Foursquare.

Geotagging-Look on the bright side

Despite the fact that the technology can be misused, geotagging can be a useful feature/tool for Law Enforcement.

While the stalkers and would be criminals are going through social media accounts of potential victims (they themselves as a user), law enforcement agencies are also using location based information to track them down.

Douglas Salane, a Director at the Center for Cyber Crime Studies (also former FBI and Manhattan District Attorney) stated "one of the most useful devices for law enforcement is a cell phone." (Seville, 2010).

However, the debate of the technology could be used to snoop on the privacy of Internet users and help curb criminal activities online is still in a gray area.

Conclusion

Ever since the stalking incident, Carrie Bugbee stopped using Foursquare, hired a babysitter and probably sleeps with her lights on.

The website PleaseRobMe.com was shut down months after the stalking of Carrie Bugbee. A few more similar incidents suggested that the website was more informative to stalkers and criminals instead of the average users.

Besides PleaseRobMe.com, another site called ICanStalkU.com was created in May of the same year. The web searches automatically for geotagged photos attached on Twitter tweets and generates a location message which is then published for public viewing.

The technology of geotagging is and will be the next big thing for social media web applications. As social media giants such as Facebook, Twitter and Google+ include the feature, many more will follow suit and as a result, will leave digital footprints of every user all over the web, which can be both good and bad.

In conclusion, geotagging is a love or hate technology. Indulging in social networking does not mean you have to share everything with everyone. If you decide to use it, use it wisely. Just a friendly reminder, if you get an anonymous call telling you to stop telling people where you are and what you are doing, that person is probably doing you a big favour.

If that happens, you should probably 'check-out' of social media, hire a babysitter and sleep with your lights on.■

Illicit Activities Gaining Ground In Web 2.0

The unregulated virtual world has arrived accompanied by contradictory powers and promises throwing out of balance our laws, public polices, economics and morality.

By | Zahri Yunos, Nurul Husna

A few years back, it would be hard to imagine the impact the Internet has had on our modern lives. Nowadays, advanced development in Information and Communication Technology (ICT) has opened up many opportunities for businesses, economics, inspired creativity, increased the quality of life and improved relationships. However, at the same time, it has also created opportunities for those with devious ambitions to cause havoc and harm. Cyberspace can be a powerful tool for perpetrators such as extremists and terrorist groups to promote extremist ideology and propaganda materials.

Extremists and terrorist groups use the Internet medium for illicit activities such as spreading of terrorism propaganda, fund raising, recruitment and mobilization, as well as planning and coordination. There have been numerous studies by researchers in analysing the illicit activities and terrorism in cyberspace.

What Is Illicit Activities?

Section 211 of the Communications and Multimedia Act prohibits content that is indecent, obscene, false, menacing or offensive in character with the intent to annoy, abuse, threaten or harass any person. Part 2, Section 5.0 of the Malaysian Communications And Multimedia Content Code interprets “menacing content” as content that causes annoyance, threatens harm or evil, encourages or incites crime, or leads to public disorder. Menacing content here also includes hate propaganda, which advocates or promotes genocide or hatred against an identifiable group or dissemination of information which may be a threat to national security or public health and safety. An example of menacing content would be bomb-making instructions and information and statements with regards to possible terrorist attacks.

Illicit Activities in Web 2.0

There have been numerous studies by researchers in Europe, the Middle East and North America analysing these illicit activities.

- Based on a study conducted at the Australian Federal Police [1], terrorists used the Internet to spread propaganda and promote extreme ideology. Analysis was done on the Al-Qaeda related websites such as Yahoo Groups, bulletin boards and forums. These groups normally manipulate cyber media to release their manifestos and propaganda statements, inter-group communication and inter-networked grouping.

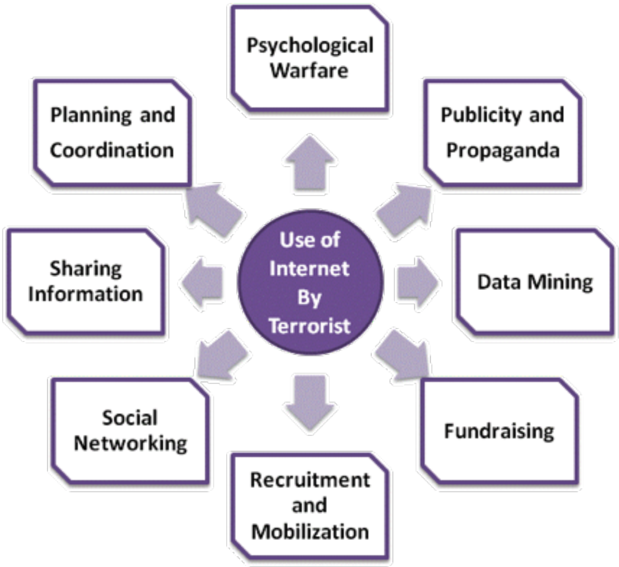
- With the introduction of YouTube and similar video-sharing sites, websites videos began playing an increasing role in distributing extremist and terrorist content. Conway [2] concluded that YouTube and similar video-sharing sites became an immediate repository for extremist video content and facilitates interaction between the administrators and viewers of the sites, thus opening radicalisation via the Internet.

- Salem [3] conducted a study of extremist groups' video on the Internet by using content analysis and a multimedia coding tool. They concluded that the web-hosted audio and video clips provided information platform and communication medium to convey messages to members, sympathisers and even be able to recruit new members via the Internet.

- Chen and his researchers group [4] conducted several experiments on cyber terrorism activities in major websites and blogs such as YouTube and Second Life. They also studied popular hosting service providers such as blogspot.com and wordpress.com. Their findings indicated that the virtual world was abused to promote cyber terrorism activities. Several of the videos published in YouTube were related to explosives, attacks, bombings and hostage taking. They also observed that the Web 2.0 media are used to promote ideas, share resources and communicate among each other.

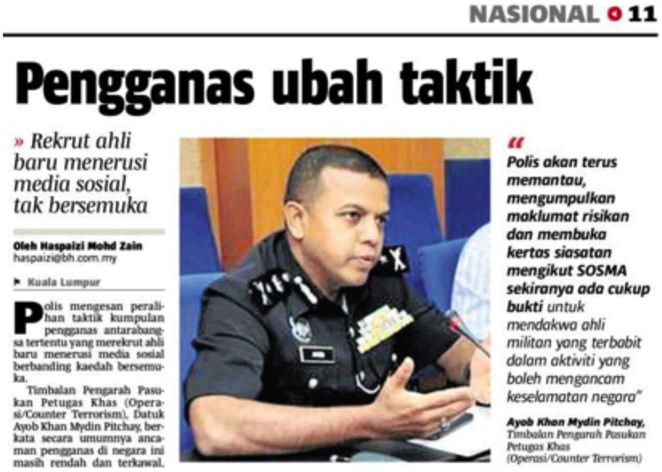
- A joint study by a group of researchers by the Singapore's S. Rajaratnam School of International Studies and the Australian Strategic Policy Institute [5] found that the Internet has contributed to radicalisation and will probably grow in regional significance. They also concluded that these websites and other social networking sites such as blogs and forums are evolving rapidly. They further clarified that their research work provided a better understanding on how terrorist organisations used the Internet and provides pathway for strategy and policy development to counter online radicalisation at the national and regional levels.

- Chau and Xu [6] conducted their research in the area of hate groups in blogs. They also found out that hatred and hate groups are a type of social movement which should not be ignored in today's environment. By disseminating hatred messages through web 2.0 media, the content can easily target anyone who has access to the Internet, including generation X. Youths are often easily influenced by these messages, eventually succumbing to the idea, and pose a threat to our society.



Local Case Studies

- Berita Harian, 9 January 2014 reported that the Royal Malaysian Police (RMP) have detected a change in international terrorist's tactic in recruiting new members. They are now utilising social media such as Facebook to get new members to join them. Previously, terrorist group such as Al-Qaeda would take years to recruit new members, communicate, strategies operation and launch attack but now it takes only few days or hours by using social media. According to the report, the RMP will continuously monitoring and an investigation paper, in accordance with The Security Offences (Special Measures) Act 2012 (SOSMA), can be initiated to charge those members involved in activities that can become a threat to national security.



NASIONAL 11

Pengganas ubah taktik

» Rekrut ahli baru menerusi media sosial, tak bersemuka

Oleh Haspaizi Mohd Zain
haspaizi@bh.com.my

Kuala Lumpur

Polis mengesan peralihan taktik kumpulan pengganas antarabangsa tertentu yang merekrut ahli baru menerusi media sosial berbanding kaedah bersemuka.

Timbalan Pengarah Pasukan Petugas Khas (Operasi/Counter Terrorism), Datuk Ayob Khan Mydin Pitchay, berkata secara umumnya ancaman pengganas di negara ini masih rendah dan terkawal.

"Polis akan terus memantau, mengumpulkan maklumat risikan dan membuka kertas siasatan mengikut SOSMA sekiranya ada cukup bukti untuk mendakwa ahli militan yang terbabit dalam aktiviti yang boleh mengancam keselamatan negara"

Ayob Khan Mydin Pitchay,
Timbalan Pengarah Pasukan Petugas Khas
(Operasi/Counter Terrorism)

- Berita Harian, 5 January 2014 reported that a 27 years old teacher has been arrested in Kelantan for selling “fake guns” via a social media website. It is interesting to note that the person used social media websites to promote his illicit activities. Based on the report, the person sells the "fake guns" online for his customer nationwide. Suspect is investigated under Section 36(1) Arms Act 1960 that could lead to 12 months in prison or a RM5000 fine, or both if found guilty.

- Berita Harian and The Star, 27 December 2013 reported that a 25 year old man has been detained over seditious postings on social media websites allegedly inciting people to join the “Himpunan Guling Kerajaan” (Rally to Topple the Government) on New Year’s Eve. He posted online and urged people to bring along necessary weapons including bombs. The man did not realise that by disseminating the message online, many can access to his postings, which posed a threat to public safety and national security. According to the report, the man would be investigated under Section 124C Penal Code which if found guilty can be imprisoned for up to 15 years. The man can also be charged under The Security Offences (Special Measures) Act 2012 (SOSMA).

Conclusion

It would be interesting to find out whether the people who use the Internet for illicit activities started off merely out of curiousity and later empathised with the plight of the extremists to the point of subscribing to the idea of invoking actual aggression. If more research can be done on this, it would help policy makers and stakeholders develop strategies to counter such threats. ■

Reference:

1. *L. Farrel, “Terrorism and the Internet. Speaker during Terrorism and the Internet Workshop, Jakarta Centre for Law Enforcement Cooperation (JCLEC - www.jclec.com).” 2007.*
2. *M. Conway, “Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures,” Centre for International Studies Dublin City University, pp. 1–38, 2008.*
3. *A. Salem, E. Reid, and H. Chen, “Content Analysis of Jihadi Extremist Groups ’ Videos,” Lect. Notes Comput. Sci. Vol 3975 @ Springer-Verlag, pp. 615 – 620, 2006.*
4. *H. Chen, S. Thoms, and T. J. Fu, “Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Groups,” IEEE Int. Conf. Intell. Secur. Informatics, pp. 98–103, 2008.*
5. *A. Bergin, S. Osman, C. Ungerer, and N. A. Mohamed Yasin, “Countering Internet Radicalisation in Southeast Asia.” An RSIS–ASPI Joint Report by S. Rajaratnam School of International Studies and Australian Strategic Policy Institute, 2009.*
6. *M. Chau and J. Xu, “Mining Communities And Their Relationships In Blogs: A Study Of Online Hate Groups,” Int. J. Hum. Comput. Stud., vol. 65, no. 1, pp. 57–70, Jan. 2007.*

Information sharing through social networking sites: Just how much is too much?

By | Syahrir Mat Ali

Introduction

A few years back, the Russian's CID and FSB agents successfully rescued the kidnapped son of world's renowned computer and Internet security mogul, Eugene Kaspersky – the founder of Kaspersky Lab. His son, a fourth-year student in Moscow, was kidnapped while walking back home from his internship at a nearby software company. As relieving as it must have been for all in hearing the news of a botched kidnapping, one crucial bit of detail as per stated in a report by the Russian news service, RIA Novosti, will definitely open most eyes to the risks that we have been putting ourselves into.

It so happened that the abductors had been stalking his routes for several months prior to the kidnapping and it paid off as they later discovered, among other things, that he did not have any security detail tailing him wherever he goes. It was later found that the kidnappers got all the information they needed for their stakeout from junior himself! Apparently, he had been posting detail information about himself on Vkontakte.ru, a Russian social networking site

Too much info?

A news report said that junior's Vkontakte's profile gave away vital information such as his real name, photos, school, his girlfriend, internship and even his previous apartment addresses – all of which any thinking kidnapper will need to understand their victims and plan out the best possible course of action or rather, abduction. Young Kaspersky's behaviour of divulging all those information on his profile page is really, nothing out of the ordinary.

That is actually how most people view their social networking sites – a place when they can share information with the people they know. Many will be asking, what is so wrong with that? Well, it is wrong when you start posting confidential information of yourself and your family for all to read. But then people will be asking, how are they to know what they posted can be detrimental to their security?

Now that is what this is all about. In the end, it boils down to the misperception people been having with regards to social networking sites.

We should really be asking ourselves, why is it okay for us or anybody to be exposing too much information over social networking sites? Are all those in our circle of social networking friends really our best of friends? Can and should they know everything that you have been doing? Ironically, we wouldn't even be sharing information of where we went for our holiday to all of our colleagues at the office, yet we seem to have no problem in announcing them through Facebook and uploaded tons of pictures as proof for all to see and download. What gives?

Are they any different?

Back when there was no Internet and folks still wrote mails and talked using public phones, people were already scamming other people through the various incarnation of pyramid schemes, lottery number predictions, *scratch and win* and many other types of scams. How is it any different, today? People still scam other people. Only this time, they use the Internet. It is faster and able to net more prey.

Also, during the pre-Facebook era, parents were known to tell their children that should anybody call and ask for them while they're away, they should say that mom and dad should be home anytime soon – when in fact they were outstation or working elsewhere for days. That was the measure of how careful people were back then out of fear that robbers or kidnappers might be looking for some form of intelligence over the phone. Whatever happened to that kind of awareness?

If anything, the Internet has made information gathering so much easier for kidnappers. They would just have to surf the most popular social networking sites and look up any name to scout, identify and understand their potential victims. In fact, perhaps it is more practical to get the vital information of anyone from social networking sites since those information are more likely to be most recent – especially if the would-be victims have been virtually living in there all day and night.

This may be surprising to those who are new to social networking sites, but it is not unusual to find very intimate and private information in form of workplace, names, age and number of children, addresses, telephone numbers and photos in social networking profiles. Even more surprising is how easy it is for some people to accept new "friendships" over the Internet. Just ask any of the hundreds of millions ofInternet users who have been spending many hours a day on Facebook and Twitter.

Today, there are even those who plan out their daily activities and conveniently announce them all in successive order through their favourite social networking sites. Indeed, those updates will keep you close to family and friends by letting them know what you have been up to these days, but you may have also been disseminating too much information to other prying eyes who may have other plans up their sleeves.

And, as if telling hundreds of people in Facebook what exactly you have been doing or where you are going is not enough, which may as well serve as a clear nod to criminals that you're not at home (go figure how useful will that be for them), now we even have Foursquare (https://foursquare.com) where you can officially declare where you are, physically!

Some may argue that only those in their circle of social network friends will be able to see and read their status updates. Really? How sure you are that all those "friends" in your lists are who they say they are? Do you really know all of them? Are all of your social networking friends vis-à-vis to the ones in your real life? Try to think back to the day you add them to your list of social networking friends.

These are some of the questions that users of social networking sites should be asking themselves. Nothing should have changed when it comes to being careful with information about yourself.

Safety measures

Technology such as social networking sites are there to connect people and there is nothing wrong with that. However, the minute people forget that these tools also possess the same information risks as any other form of communication; they can also be the most threatening.

Just keep all those personal and sensitive information to yourselves. Remember to treat exposing them to social networking sites as you would in real life to real people. You don't need to tell everybody what you're doing and where you're going. That kind of awareness should be consistently adhered to, even while socialising over the Internet.

Social networking site such as Facebook and other similar services, provides various security features that users can customise to control their information exposure. These settings are essentially tools, which users can use to decide what type or amount of information can be exposed to a particular group of people or "friends" in their social networking circle.

Users should pay extra attention to these security features and employ them in the best possible way so that only their select information is exposed to the right people. Information is power – so be sure it does not fall into the wrong hands.

Conclusion

This is why we say that the public must be made aware that the Internet is just another medium to communicate and the various social networking sites out there are merely the tools that facilitate that communication. Having said that, they must also be reminded that there has been not much of a change when it comes to crime and criminals. They will always be there wherever you are and in anything you do. Some of these crimes are pre-meditated and some are *crimes of opportunity*. Just make sure we do not become the victim of both and so lets start taking information sharing over the Internet more seriously. ■

References:

1. *Dangers of the Social Web. Internet Safety 101. Retrieved from http://www.internetsafety101.org/snsdangers.htm*

2. *Internet Social Networking Risks. Federal Bureau of Investigation. Retrieved from http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks*

3. *O'Donnell, A. (n.d.). The Dangers of Facebook Oversharing: Can too much sharing get you in trouble? About.com. Retrieved from http://netsecurity.about.com/od/securityadvisorie1/a/The-Dangers-Of-Facebook-Oversharing.htm*

4. *Online Social Networking Dangers and Benefits. University of the Pacific. Retrieved from http://www.pacific.edu/Campus-Life/Safety-and-Conduct/Online-Social-Networking-Dangers-and-Benefits-.html*

5. *RIA Novosti. (2011, April 21). Police free son of Russian software tycoon Kaspersky. RIA Novosti. Retrieved from http://en.ria.ru/russia/20110424/163679186.html*

6. *Stewart, S. (2011, April 28). The Kaspersky Kidnapping - Lessons Learned. Stratfor: Global Intelligence. Retrieved from http://www.stratfor.com/weekly/20110427-kaspersky-kidnapping-lessons-learned#axzz374kiho9R*

Human Resources Security

(In-compliance with ISO27001-Information Security Management System)

By | Hamidun Bin Katemin

Introduction

Employees are one of the most valuable resources for an organisation. No organisation can operate effectively without qualified, capable and competent employees. However, conversely, human resources can also pose or create some of the most serious risks to an organisation. This is because organisations provides their employees with **varying levels** of rights of access to their sensitive and/or critical information to carry out their day-to-day tasks.

According to Ponemon Institute's (2012) *The Human Factor in Data Protection*, at least 78 percent of respondents indicated that their company had experienced a data security breach as a result of human negligence or maliciousness.

The findings showed that employees are among the utmost threat to an organisation. There are a number of risks or ways employees can damage or threaten an organisation's system and reputation, including either planned and unplanned acts, human errors or mistakes.

So, what should we be doing about human threats in order to better-protect an organisation from security breaches or incidents?

Human Resource Security

The objective of human resources security is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

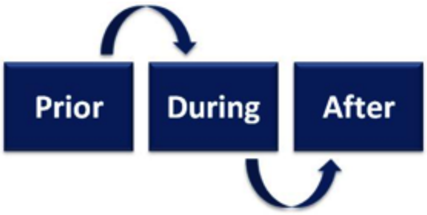
An organisation should develop a human resources security policy. The said policy should be published and communicated to all employees and relevant external parties.

The human resources security policy shall be reviewed regularly and if significant changes are initiated, there is a duty to ensure its continuing suitability, adequacy, and effectiveness.

> ***"Insider Threats Are Bad and Getting Worse: While the security community has focused its attention on advanced malware over the past few years, insider threats (i.e., threats posed by employees, third parties, or malicious software that uses legitimate access rights to networks, applications, and sensitive data as an attack vector) continue to present a number of challenges for many organisations. In fact, Enterprise Strategic Group research indicates that more than half (54 percent) of IT and security professionals believe that insider threats are more difficult to detect/ prevent today than they were in 2011" - The 2013 Vormetric Insider Threat Report by Enterprise Strategic Group***

Human Resource Policy Stages

The three stages of human resources security are:



Stage 1: Prior Employment

Objective: To ensure that employees understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Controls:

i. Roles and responsibilities

Security roles and responsibilities of employee shall be defined and documented in accordance with an organisation's information security policy during the pre-employment process.

ii. Screening

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Pre-employment background screening such as confirmation on academic qualifications, previous employments, or criminal records can minimise risk of employee theft, misappropriation, criminal activity or violence in the work place. Without prior screening, employers can be at risk of security breaches, regulatory violations and so on.

Pre-employment screening and background checks are vital to maintain workforce integrity and safety.

Background checks are considered the best solution in avoiding hiring the WRONG person! It can also minimise negligent hiring lawsuits. Once the "wrong" employee has been hired, the cost and pain of terminating that employee would be extremely considerable.

iii. Terms and conditions of employment

As part of their contractual obligation, employees shall agree and sign the terms and conditions of their employment contract, which shall state both parties' responsibilities for information security.

The terms and conditions of employment specify the particulars of the employment relationship between an employer and an employee.

The following basic information should be stated:

- The names of the employer and the employee.
- The salary, pay grade and/ or title for the job.
- A description of the functions of the job.
- An indication of where the employee is to work.
- An indication of arrangements relating to working hours.
- Important requirements in relation to responsibilities for information security.
- Non-disclosure agreement.

Stage 2: During Employment

Objective: To ensure that all employees are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human errors.

Controls:

i. Management responsibilities

Management shall require all employees to apply security in accordance with established policies and procedures of the organisation such as Access Control Policy, ICT Security Policy, Information Handling and Labelling Policy, and Password Policy.

Management should ensure that all employees are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or system. This could be done either by awareness programmes or training sessions.

ii. Job Description

Employee should have a written job description. A job description serves several purposes such as:

- Provides essential information for assigning the appropriate pay grade, and/ or title for the job.
- Identifies the essential functions of the job based on job specific competencies.
- Provides the incumbent an understanding of the primary accountabilities, duties and responsibilities they are expected to fulfil.
- Provides the incumbent on the importance of complying with the information security objectives and adhering to all relevant policies, procedures and guidelines.

iii. Non-Disclosure & Confidentiality

A non-disclosure & confidentiality agreement is a mechanism to protect sensitive technical or commercial information such as company data, know-how, prototypes, engineering drawings, computer software, test results, tools, systems and specifications from disclosure to others.

iv. Code of Conduct

The Code of Conduct defines the behaviour expected of employees. They are expected to adhere to a specified set of Code of Conduct:

- Strive towards a high standard of professionalism.
- Give undivided loyalty and devotion to the organisation at all times and on all occasions.
- Demonstrate strong esprit de corps.
- Display a high sense of co-operation and productivity in carrying out his/her duties.
- Take leadership/responsibility to generate new ways or approaches in the course of his/her work.

v. Training and Awareness

All employees of the organisation shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant to their job functions. This may include induction and awareness sessions to newly appointed employees, and ongoing security requirement training.

A consistent training programme throughout the entire process ensures employees are fully aware of their roles and responsibilities and understand the criticality of their actions in protecting and securing both information and facilities.

vi. Disciplinary Process

There should be a formal disciplinary process for an employee who commit security breach. This may include requirements for appropriate investigatory disciplinary processes such as verbal and written counselling; show cause, domestic inquiry proceedings and termination procedures.

The establishment of disciplinary process must ensure correct and fair treatment for employees who are suspected of committing breaches of security.

Stage 3: After, Termination or Change of Employment

Objective: To ensure that employees exit an organization or change employment in an orderly manner.

Procedures should be in place to ensure a employee exit from the organization or change of responsibilities and employments within an organization is managed. Human

Resource Department should ensure that the employee returns of all equipment in their possession and removes of all access rights granted to the employee.

Controls:

i. Employee Exit Checklist

The Human Resources function is generally responsible for the overall termination process and works together with the supervising manager of the employee leaving the organisation, employee going on long leave (with or without pay) for a significant period of time or retires, to manage the security aspects and help manage some of the risks.

The Employee Exit Checklist is designed to ease the task of terminating or change of responsibilities and should have the following actions:

- **Termination Responsibilities** - termination processes that ensure removal of access to all information resources.
- **Return Of Assets** - employees should return all of the organisation's assets in their possession upon termination of their employment. These include the return of all issued hardware and software, corporate documents, and other equipment such as mobile computing devices, access cards, manuals, and information stored on electronic media.
- **Removal Of Access Rights** - the access rights of all employees to information and information processing facilities should be removed upon termination of their employment. These include physical and logical access, keys, identification cards, subscriptions, and removal from any documentation that identifies them as a current member of the organisation.

ii. Job Handover

It is important for organisation to have a job handover guideline in place to help with a smooth job transition period.

The Job Handover Form should cover the list of all the important information for the incoming employee or successor will need to know such as ongoing projects or tasks, their current status, and expected completion dates.

Conclusion

A human resources security policy is needed to inform employees of the need and their responsibility to protect the organisations' technology and critical information.

To ensure the success of the said policy, it should start with the management. Without their commitment and support, the human resources security policy, might not take-off at all. ■

References

Department of Standards Malaysia (2005). Information Technology-Security Techniques – Code of Practice for Information Security Management (First Revision)(ISO/IEC 17799:2005,IDT).

The Human Factor in Data Protection. (January 2012). Ponemon Institute Research Report. Available: http://www.ponemon.org/library/the-human-factor-in-data-protection?s=The+Human+Factor+in+Data+Protection

Jon, Oltsik. (October 2013). The 2013 Vormetric Insider Threat Report. The Enterprise Strategy Group, Inc. Available: http://www.vormetric.com/sites/default/files/vormetric-insider-threat-report-oct-2013.pdf.

Charu, Pelnekar. Planning for and Implementing ISO 27001. ISACA Journal Volume 4, 2011. Available: http://www.isaca.org/journal/past-issues/2011/volume-4/documents/jpdf11v4-planning-for-and.pdf.

The Personal Data Protection Act 2010: Challenges to Comply

By | Nur Hannah M.Vilasmalar

The terrain of cyberspace creates unique legal dilemmas. Businesses that fail to adequately protect individuals' personal data risk losing their trust. This trust, particularly in the online environment, is essential to encourage people to use new products and services.

The Malaysian Government in May 2010 has enacted a legislation called as the Personal Data Protection Act (PDPA 2010) (the "Act") and received its Royal Assent on 2 June 2010. The Act effectively come into force on 15 November 2013 with the objective to protect personal data of individuals with respect to commercial transactions. Personal data is regarded as any information related to an individual's identity, characteristics, behaviour of the individual that is identified and identifiable from the information. It also includes any expression of opinion about an individual.

Under the Act, "commercial transactions" means any transaction of a commercial nature, whether contractual or otherwise which includes any matters relating to the supply or exchange of goods or services, agency, investment, financing, banking and insurance. In a literal meaning, all individuals or organisations that process or having control over the processing of the personal data in their business must comply with the Act. Basically, the seven principles outlined in the Act must be observed in order to ensure the compliance. These principles are general, notice and choice, disclosure, security, retention, data integrity and access principle.

Similar legislation has been enacted in other countries such as Singapore, Hong Kong, New Zealand, Canada and several European nations. However, in Malaysia the Act does not apply for application to the federal and state governments. Meanwhile, credit reporting companies are subjected to the Credit Reporting Agencies Act 2010 and personal data processed outside Malaysia is not subjected to the Act.

Challenges faced by an organisation

Being a new piece of legislation, coupled with criminal offenses for non-compliance of the Act, any breach of the Act by an organisation may give rise to the allegations that the management and officers are in breach of their legal duties. Therefore, it is very important for the whole organisation to be fully aware of the consequences of non-compliance with this new Act.

Besides having knowledge about the Act, an organisation is also required to review the existing processes in protecting collected data and also the manner or ways personal data are being safeguarded. Moreover, the introduction of the Act has in a way increased the level of awareness for both consumers and business owners about their rights provided for in the Act. Consumers are becoming more concerned about their data and the need for it to be protected. Therefore, if an organisation fails to protect their customers' personal data, they may alter their purchasing behaviour if they no longer trust an organisation in managing their personal information. Subsequently, this will affect an organisation's business affairs in many ways. In addition, management commitments are also crucial in materialising the acceptance of the Act by each member in the organisation.

Furthermore, having good corporate governance practices in an organisation will enable an organisation to respond to the needs and requirements of the Act. At the same time, these can also minimise the risk of the management and officers breaching their legal duties. For example, if a corporate body commits an offence under the Act, its directors, chief executive officer, chief operating officer, top management team or company secretary may be charged severally or jointly in the same proceeding. On the other hand, if the corporate body is found to have committed the offence the above personnel shall also be deemed to have committed the offence unless they can avail themselves to several of the defences available under the Act.

How to overcome these challenges?

Since it is a new piece of legislation, in order for an organisation to be equipped with the requirements and to have a better understanding of the Act, training is the best solution. Therefore, a series of training is to be conducted on various aspects in different stages. More importantly, these training sessions are needed to ensure that the members of the organisation (from top to bottom) are fully informed of what they can and cannot do with the personal data of employees, customers and third parties.

Alternatively, an organisation can also appoint personal data protection consultants to assist the organisation to assess the organisational systems, processes, contracts, data management and controls for compliance to the Act. This process may be costly and again the cost should be viewed against the benefits of having the Act. Therefore, it is worth to invest in such an engagement. Nevertheless, for those that already have in place adequate data protection measures, additional costs may not be a factor.

In conclusion, compliance with the Act is compulsory for an organisation processing personal data for commercial purposes which involves monetary transactions. This means that an organisation that collects and processes an individual's personal data, the seven principles mentioned above must be strictly followed to avoid breaching the Act. ■

Getting to Know Honeypot

By | Wira Zanoramy

Introduction

In the information age, getting connected to the Internet is a necessity. Various devices - smartphones, tablets, notebooks and desktops are connected to the Internet. Part of the causes in this phenomenon is the migration of the real-world activities like banking, retail, government and education onto the Internet.

With businesses and government sites running on the Internet, the cyber environment has become a new medium for cybercriminals. There are thousands of them connected to the Internet, breaking into production systems and exploiting their vulnerabilities for fun, fame and profit. Furthermore, some of them are sharing their tools and tactics with each other on the Internet [1, 2].

System administrators should always ask themselves these questions: What is the worst thing that could happen if an unauthorised person gained full access to their computer systems and network environment without any detection? Could this event compromise the whole organisation, its customers and the country? How much productivity will the organisation lose if all of its databases were completely compromised or erased? The most important question should be – how big is the impact towards the company's image and stakeholders? [3, 4].

Even though a lot of efforts have been made to secure IT resources from cyber-attacks, loopholes still exist as there is no perfect security. Due to this, a deception-based approach called as 'honeypot' is needed in order for the IT security administrators to detect malicious activities and at the same time to better understand the taxonomy of cyber-attacks [5, 6].

What is a Honeypot?

Honeypot is defined as an information system resource that is deployed inside the network and purposely configured to be scanned, attacked and compromised [7]. The term 'honeypot' is usually being used for representing 'a container filled with honey', which is often playing off the image of tempting sweetness that is being used as an attractive trap for bears. But in the case of network security, this term is used to represent a security technology that is based on deception. A honeypot is defined as a security resource whose value lies in being probed, attacked or compromised [6, 8]. When we look back into history, the idea behind the honeypot is based on the works of Sun Tzu and Clifford Stoll [9].

Honeypot plays an important role as it provides in-depth information about the techniques employed by attackers when they are compromising production systems and networks. This information is essential in giving us a deeper understanding about the motives of these attackers, their skills and tools being used to intrude and compromise networks. By identifying the capabilities and tactics of these attackers, network administrators could also discover vulnerabilities of their networks. By learning from the tactics used, necessary improvements can be done to increase the security posture of the network in order to prevent similar attacks taking place in the future [9, 10].

Honeypots are resources that are meant to have no authorised activity and production value on it. By default, honeypots should not be receiving any interactions. The reason is to make a clear assumption that: any interactions captured by honeypots are considered as malicious. Any detected activities on honeypots are assumed to be a probe, scan, or attack. The value of honeypots comes from their ability to capture such activities.

Usually, honeypots are covertly deployed inside the network like any other production hosts, but with an administrator's consent, they are fake hosts that are disguised as production hosts. This is to attract attackers into exploiting the honeypots instead of production hosts. Honeypots can be built in many forms, either in the form of physical machines, virtual machines (VM) or emulated virtual hosts.

Forms of Honeypot

A physical honeypot is a real computing platform that has its own valid IP address. For example, a computer installed with Fedora Linux or Windows 7 with running network services, like FTP, Telnet or SMTP [6].

A VM-based honeypot can be built by using virtualisation software like VMWare Workstation, Qemu-KVM, Virtualbox, Parallels Desktop or User Mode Linux (UML). By utilising either of these tools, a honeypot VM can be created with any type of operating system. This software is installed on a computing platform and a user can create one or multiple VM(s) running on the same platform. As for UML, the only drawback is that it can only simulate Linux systems (Provos & Holz, 2008).

Honeypot can also be built in the form of emulated virtual hosts. By using a tool called Honeyd, we can emulate up to thousands of virtual hosts running different types of operating systems on top of a single machine. Each of these virtual hosts is configured with a certain behaviour and personality, in which it defines how the virtual host will respond to the interactions of an attackers'. For example, a virtual host can be programmed to contain a Perl script that is emulating a DNS or FTP service.

Types of Honeypot

Honeypot is classified based on its level of interactions. The word 'interaction' here means - the degree of communications that are being allowed for the attacker to exploit the honeypot. At the same time, the 'level of interaction' also defines how deep the honeypot is allowed to be exploited by an attacker. The more an attacker can do to the honeypot, the more information can be collected by the honeypot from the attacker. However, here is where the honeypot will most likely suffer greater risk. There are two types of honeypots: low-interaction and high-interaction honeypots [5, 9, 10].

Low-interaction honeypots has the lowest interaction capabilities with an attacker and it is also the simplest honeypot to setup. This type of honeypot only provides minimal services and usually is in the form of a virtual host with emulated services. This virtual host or honeypot, can easily emulate the IP stack, OS and the applications of a real systems. Furthermore, it is also easy to set up right after being compromised [5, 8, 9, 10].

High-interaction honeypots are complex honeypot solutions because they require the setting up of real operating systems or a suite of real services to attackers in which nothing is emulated or restricted [11]. These high-interaction capabilities enables security practitioners to collect extensive amount of information from an attacker's malicious activities. This information can be used to study clearly the attacker’s behaviour, tools, motives and even his/her identity. The ability to gather huge amount of data is the main advantage of a high-interaction honeypot. Setting up this type of honeypot is time-consuming and it is also hard to maintain [6, 8, 10].

Conclusion

This article discussed the concept of honeypot, the possible forms of honeypot and the categories they fall into. Though it cannot solve all network security issues, honeypots are considered to be assistive technology and acts as a surveillance and forensic tool, for network security professionals and researchers to better understand cyber threats.■

References

1. *Nero, PJ, Wardman, B, Copes, H & Warner, G. (2011) Phishing: Crime That Pays eCrime Researchers Summit. eCrime Researchers Summit (eCrime), 2011 , vol., no., pp.1,10, 7-9 Nov.*

2. *Benjamin, V. & Hsinchun Chen (2012). "Securing cyberspace: Identifying key actors in hacker communities," Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on , vol., no., pp.24-29, 11-14 June 2012.*

3. *Zakaria WZA, Mat Kiah ML (2012) A review on artificial intelligence techniques for developing intelligent honeypot. In: Proceedings of 3rd International Conference on Next Generation Information Technology, Seoul, Korea, p696 – 701.*

4. *Zakaria WZA, Mat Kiah ML (2014). Implementing a CBR Recommender for Dynamic Honeypot using jCOLIBRI. 3rd International Conference on Computer Science & Computational Mathematics 2014, Langkawi, Malaysia.*

5. *Zakaria WZA, Mat Kiah ML (2013). A Review Dynamic and Intelligent Honeypot. ScienceAsia 39S, 1-5.*

6. *Zakaria WZA, Mat Kiah ML (2013). A Review for Developing an Adaptive Honeypot using Case-based Reasoning Approach. In: Proceedings of International Conference on Computer Science and Computational Mathematics 2013, 9 – 10 February, Kuala Lumpur, Malaysia.*

7. *Kumar, S., Sehgal, R., Bhatia, J. S., "Hybrid honeypot framework for malware collection and analysis." Industrial and Information Systems (ICIIS), 2012 7th IEEE International Conference on , vol., no., pp.1,5, 6-9 Aug. 2012.*

8. *Mokube, I. and Adams, M. (2007). Honeypots: concepts, approaches, and challenges. In Proceedings of the 45th annual southeast regional conference (ACM-SE 45). ACM, New York, NY, USA, 321-326.*

9. *Spitzner, L (2003). Honeypot: Tracking Hackers, Pearson Education, Boston.*

10. *Provos, N., & Holz, T. (2008). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Boston: Addison-Wesley.*

11. *Nicomette V, Kaaniche M, Alata E, Herrb M (2011). Set-up and deployment of a high-interaction honeypot: experiment and lessons learned. J Comput Virol 7, 143–57.*

Social Networking: Security and Privacy

By | Safairis Amat Noor, Adlil Ammal Mohd Kharul Apendi

Introduction

Social Networking is currently causing serious repercussions in our daily lives. By definition, the term, social networking comes from social network which means relationship that flows between people, groups, organisations, animals, computers and other information/ knowledge processing entities. In general, a social networking site is a platform that provides a virtual community for people with the same interest to share with each other or just to socialise together.[1]

As the importance and need towards Social Networking websites increases, the risks involved in protecting and securing our personal data and communicating devices and systems also increases. In this paper, we will concentrate on various possible risks; the impact of those risks; and security mechanisms need to be followed to protect ourselves and our devices in a social networking environment.

As there are a number of social networking sites available on the internet, we will only focus on the most widely accessed social networking websites which are Facebook and Twitter.

Security and Privacy Issues on Social Networking

Ignorant to security and privacy issues in social networks may lead to security incidents. Some of them are discussed below[3]:

- *Social applications provide easy access to attackers.*
  Almost all social applications are accessing users' privacy data. Attackers started inventing applications to deceive users for their own benefits. A user does not realise that he/she is exposed to the attackers while adding up their friends without proper filters. In fact, some of these friends' requests may come from spambots. Spambots have been programmed to send informal messages containing malicious links. When a user clicks on a malicious link, a Trojan will be silently downloaded to his/her computer.

- *Hoaxes in welfare*
  As social network sites becomes the latest platforms for users to communicate and interact with each other, it has been misused as intermediaries for collecting charities for disaster victims such as earthquakes and floods. There are many fake pages and groups being created by scammers with the intention of taking advantage of these disasters. These irresponsible scammers will send a link to a user to make a donation for the victims, but sadly all the money that has been donated will be credited to the scammer's bank account.

- *Phishing attacks on user credential*
  Phishing is a form of stealing data of user accounts such as usernames and passwords by presenting a fake login page to a particular user. In this case, after a user has login into the fake page, it will lead the information to the attacker. Once the attacker have access to the victim's account, they are in full control of the account. There are many effects of phishing which are identity theft,

preventing users from accessing their own accounts and excessive consumption of resources at the corporate level. There is also a new threat of phishing which can lead users into installing unused plug-ins containing malware. This malware will spread to other machines that are connected to the affected computer. In addition, pharming is a new form of phishing. This form will modify the domain name resolution system that redirects users to false web pages. Attackers will wait for users to visit the target site rather than produce them with links which make it more effective. There are various ways to evade these phishing attacks such as taking extra precautions with all emails received, verifying the resources of any application before filling in any personal data, avoiding opening suspicious links directly but using a new window and making sure that the visited page is a secure site.

- *Malware*

  In the last five years, a huge number of spam was widely dispersed through social networking sites. In an easy but effective way, attackers used phished social accounts posting inappropriate post messages that will link a user to the malware. All these types of messages were posted to a victim's friends' profile or account. This technique is being used to create confidence in a user to click it rather than being posted by spambots. This threat is known as "Koobface". Koobface is one of the most hugely spread malware that uses Facebook as a platform to spread. Figure 1 shows the lifecycle of Koobface. It shows that Koobface is invoked when a user's account starts to send the malicious link to their friends who directly open it without authenticating it first. Once the link is opened, it will lead the victims to a similar page like Tube. The page will then request them to download a plug-in in order to watch the video. Once a user downloads the plug-in, he/she will be affected by the malware that is being transferred from other infected machines. The new infected machines will act as hosts to store copies of the malware.

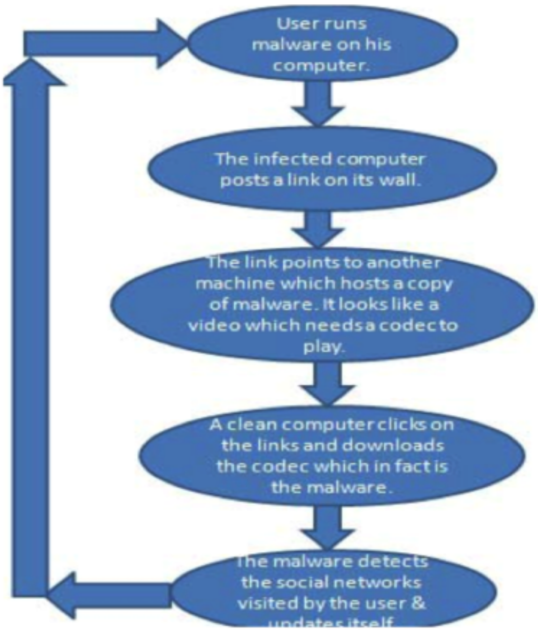

User runs malware on his computer.
The infected computer posts a link on its wall.
The link points to another machine which hosts a copy of malware. It looks like a video which needs a codec to play.
A clean computer clicks on the links and downloads the codec which in fact is the malware.
The malware detects the social networks visited by the user & updates itself

Figure 1: *Lifecycle of Koobface (a kind of Malware)[3]*

Social Networking Website-Facebook

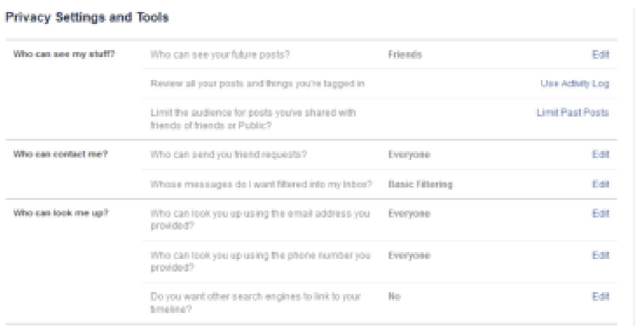
Facebook was developed by Mark Zuckerburg and his friends in 2003. Globally, Facebook is most widely used social networking website. Facebook is available with various languages [4]. According to research, Facebook has been ranked as the second widely accessed website after google. This shows how much people are addicted and dependent on this social networking website. Most widely used terms or indicates that it is the most probable location where data is shared/ exchanged/accessed by various people. So, potential attackers will concentrate on this website to get personal data of the people and any other information required for them to attack. Facebook also has so many applications and games where users can access freely. These applications are also potential risk areas.

Even though Facebook has provided Privacy and Security settings through which we can protect and secure our accounts and information, most of us are not even bothered about these. The Basic security recommendation is to apply all possible security settings to the applications and block access to all areas and then provide access to just the required areas of the application. Similarly, Facebook also needs to block access to all the possible areas or applications within it and let the user decide on what he/she wants to access.[5]

Security and Privacy concerns

- *User Profile*: Normally we provide actual or correct data in our Facebook profiles. That is not actually required unless we are sure that we will provide access to our profile to reliable friends. For all others, access should be barred.
- *Friends /Groups added*: Users need to be very careful in adding friends or joining groups. Only reliable friends / groups can be added or given access to your profile.
- *Shared Data:* The Data we are sharing represents our areas of interest and which indirectly helps in assessing our personal lives. So we need to be careful in sharing such data. We need to share our data only to the related or reliable friends and not everyone on Facebook.
- *Privacy/ Security Settings*: We need to change the Privacy settings to make our profiles and other actions secure. Facebook provides these settings to make our accounts and access more secure. As there is a provision, it is wise that we make our access and personal data more secure through these settings. These settings allow us to set who can contact us and who can have access to our profile.

The choices that Facebook provide for Privacy settings are:



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want other search engines to link to your timeline?	No	Edit

Figure 2: *Privacy Setting on Facebook*

i. Public
This setting will allow all information for that particular user account accessible and can be viewed by everyone on the Facebook network.

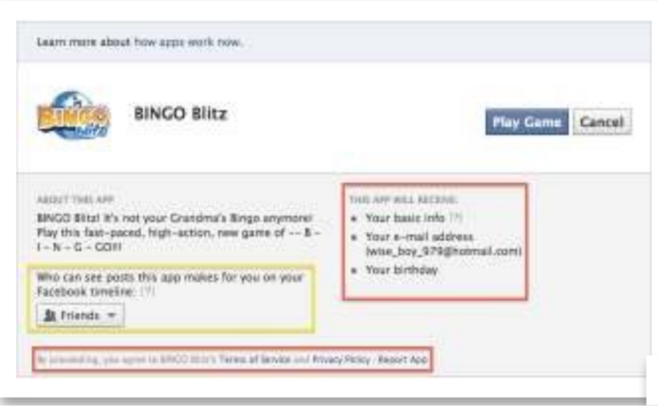
ii. Friends
Only friends of that particular user account can have access.

iii. Only me
This is 100% accessible and viewed by the owner of the account only.

iv. Custom
Can be customised by the account owner.

v. By group
User of an account will set the limit of view by group created.

- *Applications / Games* [5]: Facebook provides many applications and games for users. Each application has different terms of use and policies. Facebook has no control of those applications. Users need to really think the basic reason for accessing this website; it is for connecting to various known and reliable people and communicating with them, not for playing games and for accessing applications. Be secure by not accessing unwanted applications which are provided by third parties and follow the necessary security features.


Learn more about how apps work now.

BINGO Blitz

ABOUT THIS APP
BINGO Blitz! It's not your Grandma's Bingo anymore! Play this fast-paced, high-action, new game of -- B - I - N - G - GO!!!

Who can see posts this app makes for you on your Facebook timeline: [?]
Friends

THIS APP WILL RECEIVE:
- Your basic info [?]
- Your e-mail address (wise_boy_979@hotmail.com)
- Your birthday

By proceeding, you agree to BINGO Blitz's Terms of Service and Privacy Policy · Report App

Figure 3: *An example of a specific application that is asking for a permission. [5]*

- *Login Notifications:* Enable Login Notifications in the Facebook security settings, so that notifications will be sent to your mail or mobile. With this we can trace out and can take immediate action when an unauthorised user tries to get access to our account.

Facebook is really the most accessible and the most popular social networking website. This does not mean that it is the most secure application. Facebook provides many security and privacy features that provides better security to our accounts and access levels. It all depends on us whether to follow these security features and ethical concerns to make our lives peaceful and happy or else just go at it at our own risk and face the consequences.

Social Networking Website-Twitter

Twitter is the most widely used professional social networking website. Twitter is used to send and read short messages known as tweets. Only registered users can send messages and these messages can be read even by unregistered users. Twitter shares public information of its users to the remaining registered account holders for personal identification.

Twitter is not only the most widely used professional connectivity social network, it is also the most widely attacked social networking website. It became stable and more secure because of these attacks[6].

Security and Privacy concerns

- *User Information:* Don't share personal or critical information while tweeting with others. All tweets are public and you have an option to secure your tweets, by doing this, only the people who are following you can view your tweets. Even then, sharing critical information is not at all entertained for security purpose.
- *Following:* This really plays a critical and crucial role in protecting security and privacy of your account. Unless you know the person well do not follow or follow their tweets. Best way to attack is to follow the user and get some relevant information through their tweets. Don't follow anybody unless you know the person well enough and even then do not share any personal or critical information.
- *Location update:* Geo Tagging feature in Twitter will let a user know your current location. This is not safe at all. Unless it is really required, do not enable this service as there is no need for people to know your current location. This may alert attackers and burglars who are waiting for the right time to attack you and your assets.
- *Blocking:* If you feel some users in your follow list are not reliable block them immediately. By doing this, they will not

have any idea regarding your actions and location.

- *Monitor your Children:*
    - ◇ Children are not matured enough to use social networking websites. As it may have serious mental impact on them as well or else may result in physical attacks. Even then, if it is required, at least take note of some of the issues mentioned below for their safety.
    - ◇ Remove your child's personal information from twitter. Children are not matured enough to use this website. Even though they want to, make sure their personal information is kept hidden.
    - ◇ Turn off the tweeter location option. This helps in being safe. Or else it will open up opportunities for attackers to physically attack children or mentally disturb them through their tweets.
    - ◇ Frequently check their accounts. If they really want to use it, regularly monitor their accounts.
- *Login Information:* Always prefer to have complex passwords for your Twitter account. This makes it impossible to crack and misuse your account.

Even though Twitter is more secure compared to other social networking websites, it still depends on the way we handle it and how safe we make use of it or benefit from it.

Conclusion

Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as its large user base. Therefore, privacy and security issues in online social networks have become greater concerns. Privacy issue is one of the main concerns, since many social network users are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social network accounts to steal identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rates, which is more effective than the traditional email spam. The forth is the malware issue. Attackers use social networks as a channel to spread malware, since it can spread very fast through connectivity among users. Social networking sites are always facing new kinds of malware. Finally, physical threats, which are the most harmful of all. Since several social network features utilise location-based services, it is easier for criminals to track and approach victims.

Social networking sites try to implement different security mechanisms to prevent such issues, and to protect their users, but attackers will always find new methods to break through those defences. Therefore, social network users should be aware of all these threats, and be more careful when using them. ■

References

1. *E. Aïmeur, S. Gambs, and A. Ho, "Towards a Privacy-Enhanced Social Networking Site," 2010 Int. Conf. Availability, Reliab. Secur., no. 3, pp. 172–179, Feb. 2010.*
2. *D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," J. Comput. Commun., vol. 13, no. 1, pp. 210–230, Oct. 2007.*
3. *G. Bamnote, G. Patil, and a Shejole, "Social networking - Another breach in the wall," Int. Conf. Methods Model. Sci. Technol., vol. 1324, pp. 151–153, 2010.*
4. *L. Bilge, T. Strufe, D. Balzarotti, E. Kirda, and S. Antipolis, "All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks," Www 2009, pp. 551–560, 2009.*
5. *A. Albesher, "Privacy and Security Issues in Social Networks : An Evaluation of Facebook," pp. 7–10, 2013.*
6. *C. Perez, B. Birregah, R. Layton, M. Lemercier, and P. Watters, "REPLOT : REtrieving Profile Links On Twitter for suspicious networks detection," pp. 1307–1314, 2013.*

Developing the Nation's Competency Skill Sets for Forensic Document Examiners

By | Sarah Khadijah Taylor

Background

In March 2014, Department of Chemistry Malaysia had invited CyberSecurity Malaysia as a technical evaluator for the development of competency skill sets for Forensic Document Examiners (Level 2 and 3). The meeting was held in May 2014 of which I had the opportunity to represent CyberSecurity Malaysia and provide my technical inputs. Joining this meeting were representatives from Royal Malaysian Police (PDRM), Companies Commission of Malaysia (SSM), Department of Chemistry Malaysia, Malaysian Immigration Department and National Occupational Skills Standard (NOSS) as the facilitator.

BENGKEL PEMBANGUNAN NOSS BAGI BIDANG
1- Analisis Kimia Tahap 2-3 Fasa 3
2. Dokumen Examination

Who is a Forensic Document Examiner?

A Forensic Document Examiner is the one who analyses a document and determines the authenticity of a document. The examiner also conducts analysis on handwriting styles.

What is the motivation?

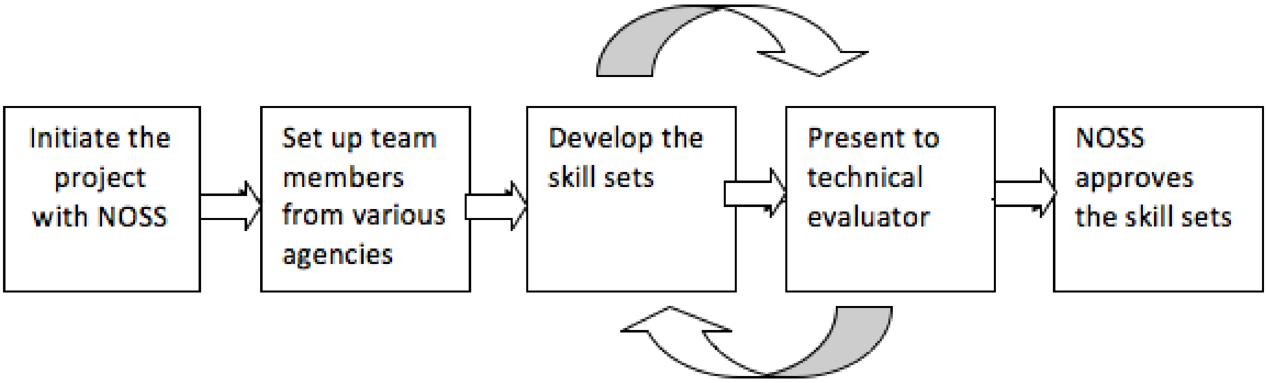
This project was initiated by Department of Chemistry Malaysia early this year although the initial discussion actually started last year. This project was initiated when most of the Forensic Document Examiners were being viewed as incompetent in Malaysia's court of law, causing their statements to be arguable in court. This issue was acknowledged by several agencies, including Department of Chemistry Malaysia and PDRM. Most of them were of the views that their existing training programmes did not have the proper structures specifying certain skill sets to be achieved by the various Forensic Document Examiners.

How?

This project was initiated and funded by Department of Chemistry Malaysia , under the purview of the NOSS. During the meetings, Department of Chemistry Malaysia served as the secretariat, while NOSS acted as the facilitator. When the skill sets are ready, it will be parked under NOSS for other agencies to refer and use.

Several workshops were conducted and attended by several agencies in order to develop these skill sets. The first workshop took five days, whereas the second one took another 5 days for the document containing the skill sets to be developed. The proposed document was presented to a panel of technical evaluators to get their comments and feedback. In general, the panel provided positive feedback with a few minor changes on the draft to enhance the skill sets. The document is yet be approved by NOSS in the next phase before it can be assigned as a national document.

It is observed that the process of developing the skill sets has taken a very short time. The duration between the first meeting and the third meeting was just two months! It was acknowledged by the participating agencies that the quick completion of the document was made possible as a result of their commitment and hard work. They were working from 8.30 am to 10.00 pm daily for the whole week, and in certain circumstances they had to stay up until 1.00 am.


Initiate the project with NOSS
Set up team members from various agencies
Develop the skill sets
Present to technical evaluator
NOSS approves the skill sets

What are the benefits?

This initiative to develop competency skill sets for the Forensic Document Examiners is to assist relevant agencies in their examination of various forensic documents. Amongst others, the skill sets can be used by agencies to hire new personnel and measure their performance. The skill sets can also be used by training providers to develop training programmes and assess a trainee's knowledge and skills. In addition, the skill sets can be used for human resource planning purposes namely to set a clear career path and progression for employees.

Summary

I personally think that the development of this skill sets for Forensic Document Examiners is a very good initiative. I would suggest that other agencies do the same to come up with skill sets that are related to their job functions. This project is highly beneficial and recommended when the various different agencies are saddled with the same job roles or functions, and there is a need at a national level for standardisation.

The document is very detailed, complete and thorough. Once it is complete, the document will contain the following items:

- Competency Unit; eg: Exhibit Comparison Activities.
- Work Activities (sub of Competency Unit); e.g.: 'Examine the features of the specimen exhibits' and 'Examine the features of the questioned exhibits'.
- Knowledge, Skill and Ability (KSA) for each Work Activities.
- Assessment of KSA
- Training hours
- Training delivery modes

The attractive part of this initiative is that it does not take a long time to complete. A typical cycle would be three months. However, a certain amount of money must be allocated to pursue this initiative as it involves the organisation of several activities.

The Importance of Cloud Computing

By | Syed Zulfauzi

Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. -NIST

Cloud computing is a synonym for distributed computing over a network and means the ability to run a programme on many connected computers at the same time. –Wiki

Service Models

Just as deployment models play an important role in cloud computing, service models are also an important consideration. The service model to which a cloud conforms dictates an organisation's scope and control over the computational environment, and characterises a level of abstraction for its use. A service model can be actualised as a public cloud or as any of the other deployment models. Three well-known and often-used service models are listed below:

Software-as-a-Service.

Software-as-a-Service (SaaS) is a model of service delivery whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud consumer does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

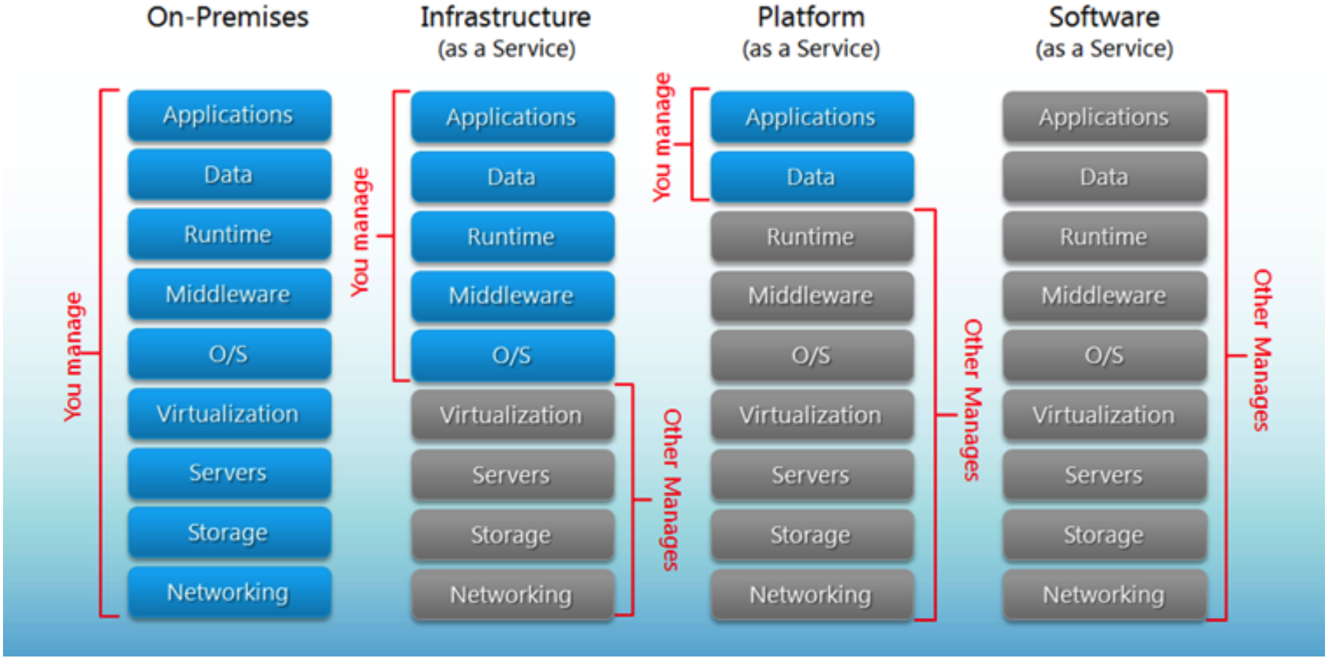


Figure 1: *Seperation of Responsibilities*

Platform-as-a-Service.

Platform-as-a-Service (PaaS) is a model of service delivery whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed programme and database development tools. The development environment is typically designed for a special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud consumer has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud consumer.

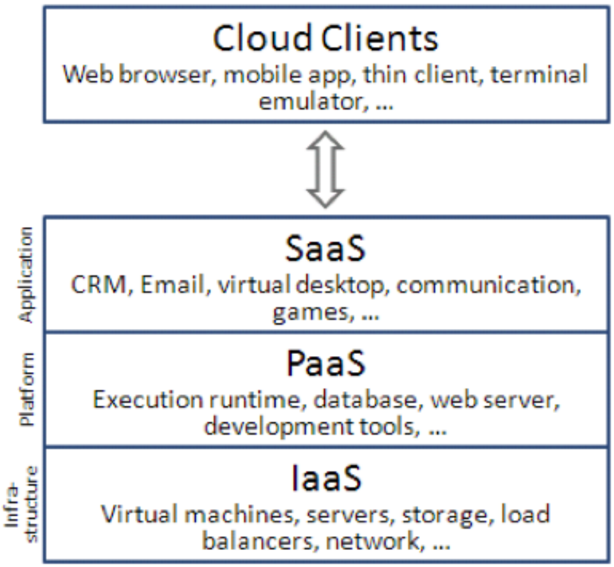

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Figure 2

Infrastructure-as-a-Service.

Infrastructure-as-a-Service (IaaS) is a model of service delivery whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualised objects controllable via a service interface. The cloud consumer generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud consumer.

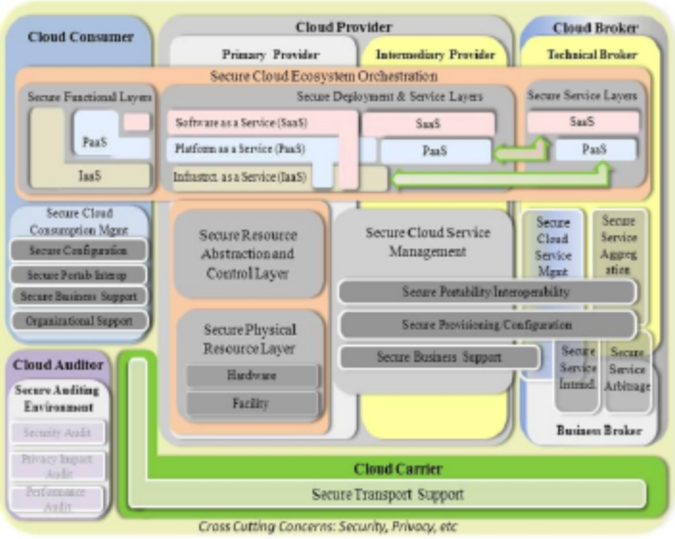

Cloud Consumer
Cloud Provider
Primary Provider
Intermediary Provider
Cloud Broker
Technical Broker
Secure Cloud Ecosystem Orchestration
Secure Functional Layers
Secure Deployment & Service Layers
Secure Service Layers
PaaS
IaaS
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastruct. as a Service (IaaS)
SaaS
PaaS
SaaS
PaaS
Secure Cloud Consumption Mgmt
Secure Configuration
Secure Portab Interop
Secure Business Support
Organizational Support
Secure Resource Abstraction and Control Layer
Secure Physical Resource Layer
Hardware
Facility
Secure Cloud Service Management
Secure Portability Interoperability
Secure Provisioning Configuration
Secure Business Support
Secure Cloud Service Mgmt
Secure Service Aggregation
Secure Service Intermed.
Secure Service Arbitrage
Business Broker
Cloud Auditor
Secure Auditing Environment
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Carrier
Secure Transport Support
Cross Cutting Concerns: Security, Privacy, etc

Figure 3

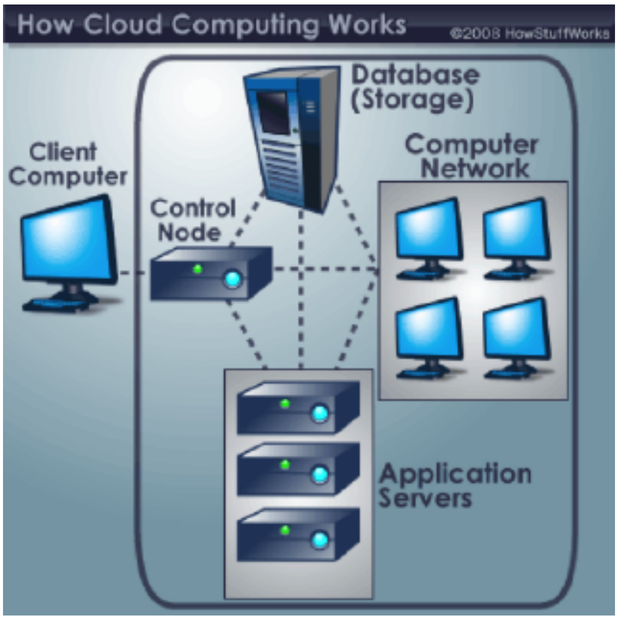


Figure 4

The importance of cloud computing and its advantages

1. **Help companies save money**
   Companies can save a lot of money in their investment into cloud

computing technologies. This can help organisations take the burden of acquisition of servers, software, and people that are needed to beef up enterprise services, shared technology solutions, and deployment of customised or custom off-the- shelf solutions.

2. **Help save the environment**
   Organisations that implement cloud computing technologies can have a significant impact on their ability to reduce their electricity bills dramatically. Cloud computing helps save the environment because it is shared infrastructure resources that a vendor provides to an organisation. Cloud computing vendors that specialise in infrastructure services have built up data centres around the country and offer their data centres to other companies. Companies do not need to have their own data centres, they can just have their applications hosted with these cloud computing providers to help save energy through sharing resources.

3. **Access to information anywhere at anytime**
   The Internet and cloud computing technology is a winning combination. These two technologies have allowed vendors to develop a product called "cloud drives"; which is an online storage medium that allows people to save their documents, videos, photos, and music over the Internet. The advantages of a cloud drive is that it provides the capability for people to access their information from any computer around the globe at their convenience. This type of simple technology allows people to become more productive by improving their access to information. There are a number of vendors that have entered the cloud computing market to offer cloud drives such as Google, Amazon, and Dropbox to name a few.

4. **Cloud computing solutions are easy to use**
   The reason why cloud computing is catching on is because of the simplicity that vendors have been integrating solutions to use this technology in the first place. People like simplicity, excellent customer service, and more sophistication in the services that they are receiving from companies. As long as vendors make it simple and enjoyable to access cloud technologies then it will become more integrated with other products.

5. **Integrate part of a disaster recovery solution**
   Organisations need to protect their critical data to ensure that they can provide services to their customers and that they are able to continue their daily operations to support their corporate mission. Most companies develop a disaster and recovery plan that discusses the necessary steps that they need to take for any type of events that a company may face. A company prepares for these events by having an alternative computing facility to save mission critical data for the organisation at some remote location away from the corporate headquarters. Companies also routinely take full and incremental backups on a daily and weekly basis that is stored on some type of storage device. Companies can now integrate cloud computing as a type of storage device that they can integrate with their disaster recovery plans in addition to the other methods that they are using to save their data. Having a cloud storage solution helps provide additional safeguard procedures to help ensure

that customer data will be safe and that your organisation will continue to operate based on any type of event.

6. **Will lead to new product and platform innovation**
   The need for new product ideas and innovation is critical to the success and growth of the global economy. These new product innovations can come from improving on older technologies or collaborating with existing technologies to form new ones. Cloud computing is positioned to be an important ingredient that companies can use to bundle with other services that can provide customers with new experiences. The number of possibilities that companies can combine with cloud computing is infinite and we are excited about the future innovations that may rise from this technology. We are already seeing innovations from companies such as Amazon, Google, Rackspace, IBM, and Microsoft. Cloud computing is new technology that has just begun to assemble the policies, technologies, disciplines and is not at a mature state yet. There is so much potential to grow this domain forward and it will be exciting to see what will happen in the next ten years in the evolution of the cloud. We expect to see more synergies from different technologies and possibly more collaborations from vendors in offering customers better solutions.

These are some example product exist in the market:

- amazon.com
- AT&T
- iCloud
- Dropbox
- Evernote
- Google Drive
- Skydrive
- 4shared
- Mediafire

Conclusion

The tight relationship between cloud computing, virtualisation, and shared storage naturally means that virtualisation and shared storage will increase in importance. The new utility model for IT services breaks the conventional technology, people, and process barriers that applications and information haven been confined to. Cloud computing is a new computing paradigm that is still emerging. Technology advances are expected to improve performance and other qualities of services from public clouds, including privacy and security. Many agency systems are long lived and, if transitioned to a public cloud, will likely experience technology and other changes over the course of their lifetime.

Cloud providers may decide to sell or merge their offerings with other companies; service offerings may be eclipsed by those of another cloud provider or fall into disfavour; and organisations may be required to re-compete an existing contract for cloud services, when all contractual obligations are exhausted. Eventually having to displace some systems to another public cloud is a distinct possibility that federal agencies and other organisations should not dismiss. ■

References

1. *http://www.nist.gov*
2. *www.Wikipedia.org*
3. *http://www.examiner.com/article/why-cloud-computing-is-important*
4. *www.crn.com*
5. *www.amazon.com*
6. *www.howstuffworks.com*

Measuring Security Awareness

By | Melisa Binti Muhamed

Introduction

Your organisation is ISMS certified. You have information security policies in place. Security awareness campaigns, trainings and talks have taken place. But how do you measure the effectiveness of the programmes and the awareness level of your organisation? What should you measure?

It's been said that security is hard to measure. That includes measuring the awareness level of an organisation. Although security has always been perceived as a dynamic process, it does not mean that it is left without any measurable aspects. The process needs to be improved in order to be measured.

According to John Schroeter, in an article from CSO [1], there are many benefits an organisation will enjoy when they make improvements to the process. Among those benefits are:-

a. Better budget justifications for creating the security awareness program/ training
b. Better ability to identify major data breached
c. Secure confidential information
d. Limit physical access to data storage devices
e. Achieve high compliance with legal and self- regulatory framework
f. In better position to attract and retain high-quality information security personnel
g. Effective enforcement of corporate information security policy
h. Protected company reputation which increase customer trust and loyalty

It is agreed among professionals that measuring security awareness effectiveness is not straightforward as in measuring manufacturing or quality processes. However with the use of right available tools and methods, getting real key indicators of an organisation's level of awareness is possible.

What should we measure?

To start with, there is no commonly agreed and understood standard measure of the effectiveness of a security awareness programme and the awareness level of an organisation. However, there are a number of qualitative and quantitative measures that can be used in order to obtain real insights and to show how much progress an organisation have achieved over a period of time.

In an article titled Measuring Information Security Awareness: A West Africa Gold Mining Environment Case Study[2], West Africa Gold Mining company used a methodology based on techniques borrowed from the field of social psychology to develop a measuring tool. The methodology proposed that learned predispositions to respond in a favourable or unfavourable manner to a particular object have three components: affect, behaviour and cognition.

Affect	One's positive and negative emotions about something
Behaviour	Intention to act in a particular manner
Cognition	The beliefs and thoughts one holds about an object

Figure 1: *Definition of the three component by Feldman, 1999; Michener and Delamater, 1994 [3]*

The three basic components were then used as a basis to create a model of equivalent dimensions as below:-

Knowledge	What a person knows; understanding of information security issues and requirements
Attitude	How do they feel about the topic; how learners feel about information security i.e. does it seem important. This determines their disposition to act
Behaviour	What do they do about it; the key to compliance. Employee behaviour is determined by their attitude and is a result of learners putting their knowledge into practice

***Figure 2:** Equivalent dimension developed to gather actual measurement for security awareness*

In a white paper by SAI Global [4], they believe that from a user perspective, information security lies in the overlap of attitudes, knowledge and behaviour. Addressing and measuring these three areas in an awareness programme will ensure the desired effect.

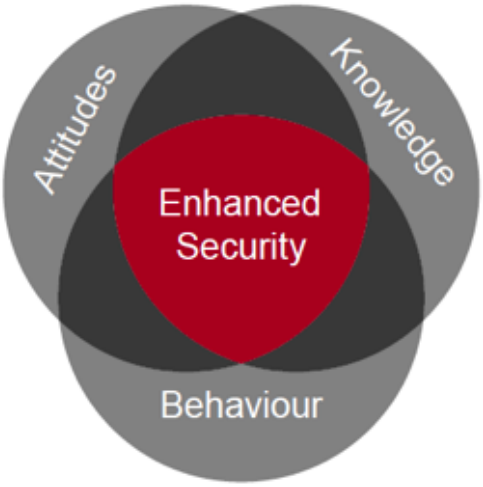


***Figure 3:** Overlap of attitudes, knowledge and behaviour*

From the model above, different measuring tools and methods have been developed over time in order to provide measurable results and indicators. In deciding what metrics to capture, it is important to consider the key determinants of security behaviour from a user perspective. The security position of an organisation can be improved when the attitudes, knowledge and behaviour of the users are aligned with the identified security objectives and requirements.

Attitude	Knowledge	Behaviours
Surveys	Assessment Tests	Behavioural Measures
Interviews		Surveys
Focus Group		Interviews
		Focus Group

***Figure 4:** Tools and methods for measuring attitudes, knowledge and behaviour*

Measuring Attitudes

All these tools are used to gather the performance measure. To measure and gauge attitudes, a number of options can be deployed to the target audience. Overall, the methods used should relate to how the target feels about information security. For example:-

- Does it help or hinder day-to-day work?
- Does the audience understand the connection between information security and the protection of the organisation’s reputation?

Methods	Attitudes that can be measured
Survey	Can be used for a large number of respondents. Useful to identify broad areas of trends and information security issues.
Focus Group	Small targeted audience from different backgrounds can be selected. This will provide the opportunity to drill down an issue and explore other key issues.
Interview	The target group should be the management, key stakeholders and influencers. This method will provide insights into key areas that matters to them.

***Figure 5:** Methods and target audience*

Measuring Knowledge

In measuring knowledge, a well-designed assessment test is very important. A poorly constructed assessment test will not measure the right knowledge of the target audience. The assessment test requires a clear and demonstrable link between required security behaviour that the organisation is trying to encourage and the knowledge that needs to be delivered and assessed.

The learning objectives should also be clearly addressed in the training content. This will help the organisation to focus on what they want the targeted audience to do and not dishing out excessive information for the audience to absorb. The questions in the assessment test should also be designed and relate directly to the behavioural learning objectives. This will become a valid test whether the user understand and will demonstrate the important security behaviours that the user need to exhibit. A good quality e-Learning system with a well-designed assessment test offer good opportunities in assessing security knowledge. Usually equipped with a large question bank, the system will ensure a learner will obtain different learning experiences each time he/she participate in the assessment and presented with different questions from their peers, thus, discouraging collusion.

Measuring Behaviour

Often, survey data that was captured is able to that provide a meaningful indication of users' behaviour or intended behaviour as it is self-reporting in nature. It also presents an opportunity to get the overall view of an organisation which gives a better indication of the organisation's culture. This can be achieved by not only asking questions about their behaviour but also by asking their perceptions about the organisation as a whole.

Apart from the survey data, incident reporting data is also a potential key indicator. The number of incidents reported and the number of disciplinary of security issues reported will be able to provide insights on the awareness level over a period of time.

Security Awareness Training and Assessment

With technological advancements, the use of manual methods such as surveys, interviews and focus group can be minimised or totally eliminated. Most organisations are now moving towards centralised, web based, video animated e-learning systems in providing security awareness training and assessment to their employees. These methods are able to provide more accurate and automated measurements to all the factors mentioned above.

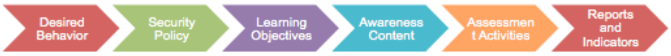


Figure 6: *Components of Security Awareness Training and Assessment*

With the e-learning systems in place, benchmarking of security awareness can easily be done. These e-learning systems can be used to gather operational measures or quantitative data. Quantitative data such as the number of employees trained, the frequency of training, pass and fail rates for assessment tests as well as profiling by department or geographical location can be produced by an e-learning system. This level of operational reporting can be particularly useful for regulatory compliance or internal or external auditing purposes. When collected over a year-on-year basis, these data provide a useful internal benchmark showing the growth of the awareness level of an organisation which makes this method the best way in measuring the level of security awareness.

In a research by Kenneth Knapp from University of Fairfax (Vienna, Virginia) in 2005 [5], an examination in the relationship of user awareness training components and perceived security effectiveness was carried out. From the study, they concluded that security awareness training alone will not secure an organisation. There were four main implications discovered from the study:-

- Training must be provided at least once a year
- Multiple training methods should be employed such as e-learning systems, newsletters, posters, brochures, etc
- Compliance should be ensured and non-compliance should come with consequences
- Train relevant topics and avoid excessive information

Conclusion

Looking at the future trends of security awareness training and assessment, CyberSecurity Malaysia has taken the step forward to fulfil the gap. *Continuous Readiness Information Security Management or CRISM* is an online e-learning programme developed to assist local organisations to assess and measure the security awareness level of their respective organisations. It is an engaging and behavioural-based learning approach developed to raise information security awareness. CRISM learning modules are moulded into real-life scenarios that makes learning more engaging and the intended learning objectives can easily be delivered across to the target audience.

The modules have also aroused positive, sustained behavioural changes to minimise the risk of security breaches due to human errors. As human is known as the weakest link in information security, teaching methods in the modules are carefully designed with layered approach that includes both technical and non-technical solutions in order to address this issue.

By using the tools and methods described above, it is possible for an organisation to measure the security awareness level of their organisation. Coupled with the right technical and non-technical strategy, an organisation will be able to evaluate whether or not a positive change in knowledge, attitudes and behaviour of employees has been achieved and to evaluate to the extend which activities that have been impacted the most. It is still a long way to go, but it is a possible journey in strengthening the weakest link in information security; human. ■

References

1. *Measuring the effectiveness of your security awareness program, by John Schroeter. (http://www.csoonline.com/article/2134334/metrics-budgets/measuring-the-effectiveness-of-your-security-awareness-program.html)*

2. *Measuring Information Security Awareness: A West Africa Gold Mining Environment Case Study, by HA Kruger and WD Kearney. (icsa.cs.up.ac.za/issa/2005/Proceedings/Full/018_Article.pdf)*

3. *Understanding Psychology. Fifth edition. McGraw-Hill College. Boston, River Ridge, IL by Feldman, R.S. 1999*

4. *Measuring the effectiveness of information security awareness training, by SAI Global. (http://www.saiglobal.com/Compliance/resources/WhitePapers/how-to-measure-information-security-training.htm)*

5. *Impact of Security Awareness Training Components on Perceived Security Effectiveness by Karen Quagliata (http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/JOnline-Impact-of-Security-Awareness-Training-Components-on-Perceived-Security-Effectiveness.aspx)*

The Trend of Intrusion Defacement

By | Farah Binti Ramlee

Abstract— Web defacement basically targets web hosting owners such as private or public blogs, corporate and government websites. This incident usually captures the interface of a website that displays unwanted, wrong information and different content form the actual presentation and creation of the website. Below is an example of website being defaced.

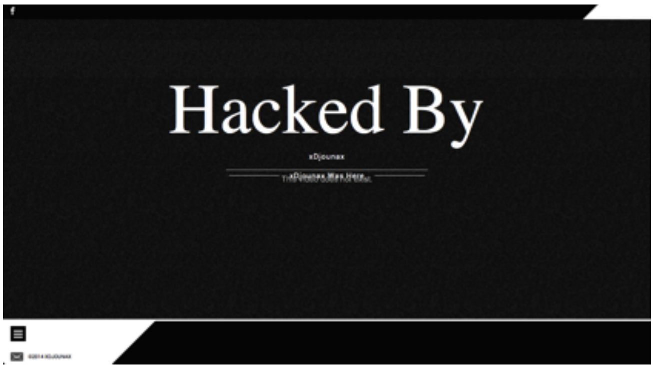
I. Introduction

Intrusion is referred to a successful unauthorised access or illegal access to a system or network. This could be the act of root compromise, web defacement, or installation of malicious programmes, i.e backdoor or trojan.

II. Intrusion Defacement

Intrusion defacement is also referred to as web defacement or website defacement, a form of malicious hacking in which a website is "vandalised." Often the malicious hacker will replace the site's normal content with a specific political or social message or will erase the content from the site entirely, relying on known security vulnerabilities for access to the site's content.

Web defacement basically targets web hosting owners such as private or public blogs, corporate and government websites. This type of incident usually captures the interface of a website that displays unwanted, wrong information and different content from the actual presentation and creation of the website. Below is an example of a website being defaced.



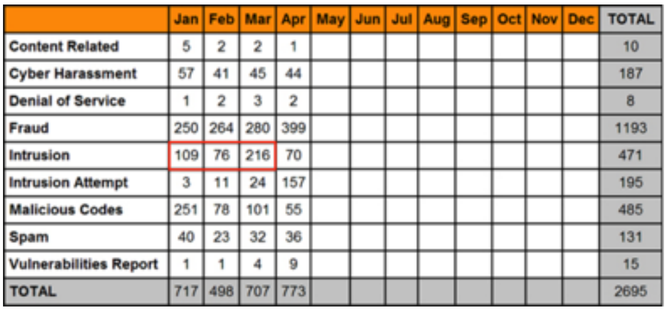
Hacked By

xDjounax

xDjounax Was Here

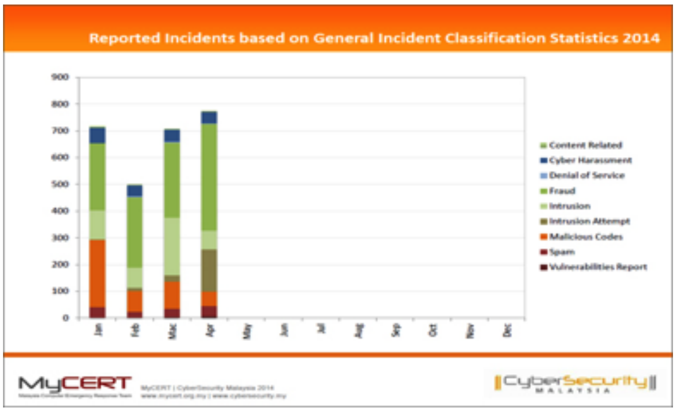
III. Intrusion Statistics for Quarter 1, 2014

In the 1st quarter of 2014, a total of 401 incidents were reported to CyberSecurity Malaysia under the Intrusion category as shown in *Table 1* and *Graph 1*.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Content Related	5	2	2	1									10
Cyber Harassment	57	41	45	44									187
Denial of Service	1	2	3	2									8
Fraud	250	264	280	399									1193
Intrusion	109	76	216	70									471
Intrusion Attempt	3	11	24	157									195
Malicious Codes	251	78	101	55									485
Spam	40	23	32	36									131
Vulnerabilities Report	1	1	4	9									15
TOTAL	717	498	707	773									2695

***Table 1** : Intrusion in Q1 (Jan - Mar) 2014*



***Graph 2:** Intrusion in Q1 (Jan - Mar) 2014*

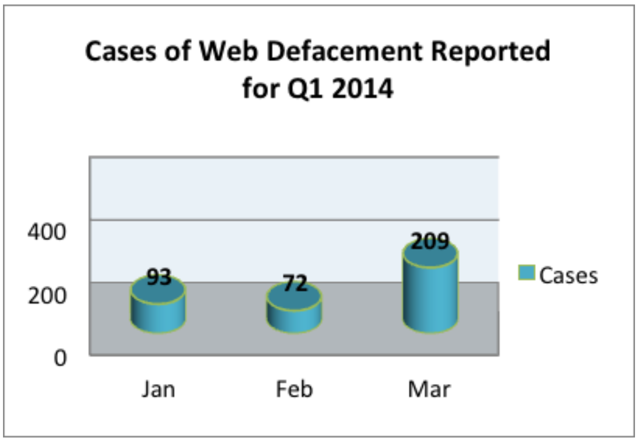
IV. Comparison Intrusion Defacement Analysis

In the 1st quarter of 2014, 374 out of 401 intrusion incidents were related to Intrusion Defacement as shown in *Table 2* and *Graph 2*.

Intrusion Defacement Report in Q1 (Jan-Mar) 2014

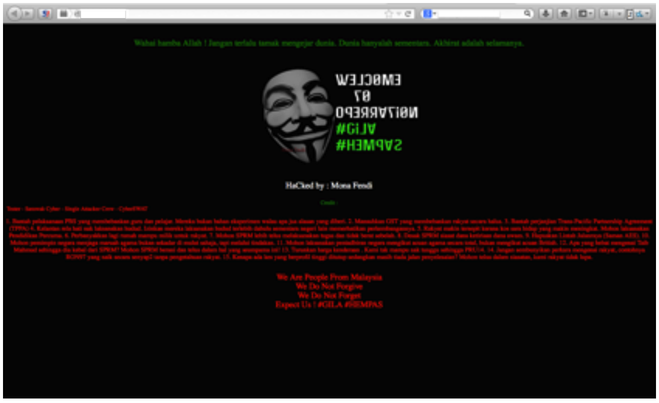
Month	No of Incidents
January	93
February	72
March	209
TOTAL	374

Table 2: *: Intrusion Defacement in Q1 (Jan - Mar) 2014*
Note: The statistics reflect number of tickets



Graph 2: *Intrusion Defacement Q1 (Jan - Mar) 2014*

A total number of 640 URLs recorded were defaced in the 1st quarter of 2014. Hacktivist groups mainly were responsible for the major types of intrusion defacement reported. In March 2014, Malaysia was shocked by the news on the missing airline MH370. According to MyCERT, these hacktivist groups had exploited this issue. From 209 incidents reported in March 2014, a total number of 61 URLs were defaced with hashtags of the operation as #Gila, #Hempas or #Gila_Hempas. Such defacements reflected the sentiment and protests by the attackers against the Malaysian Government regarding the MH370 incident and for several other reasons. Below is an example of a website that has been defaced by these hactivists.



Wahai hamba Allah ! Jangan terlalu tamak mengejar dunia. Dunia hanyalah sementara. Akhirat adalah selamanya.

HaCked by : Mona Fendi

[illegible]

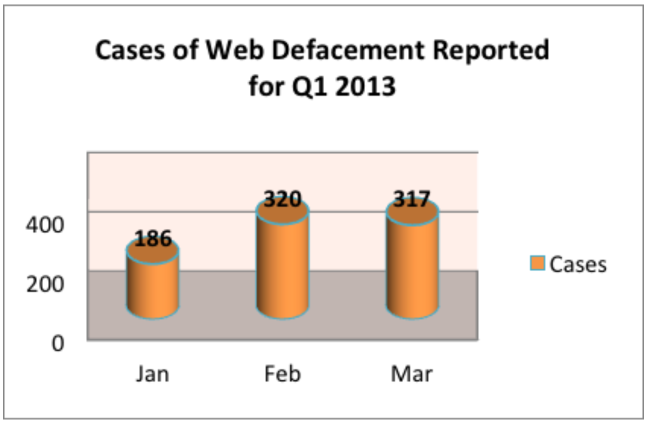
We Are People From Malaysia
We Do Not Forgive
We Do Not Forget
Expect Us ! #GILA #HEMPAS

In the 1st quarter of 2013, there were 823 incidents related to Intrusion Defacement reported to MyCERT as shown in *Table 3* and *Graph 3.*

Intrusion Defacement Report in Q1 (Jan-Mar) 2013

Month	No of Cases
January	186
February	320
March	317
TOTAL	823

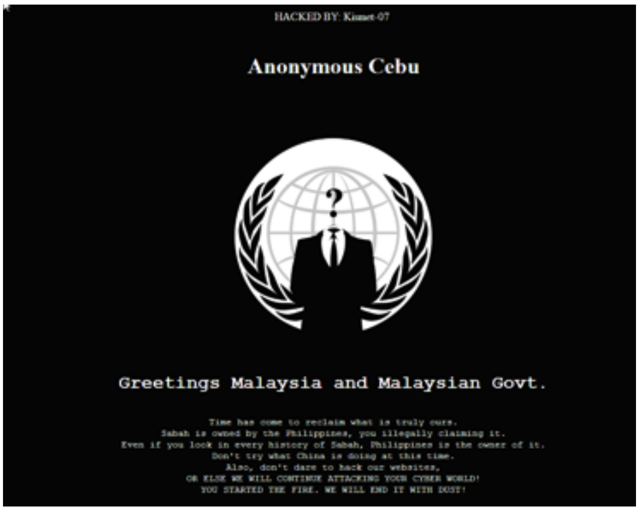
Table 3: *: Intrusion Defacement in Q1 (Jan - Mar) 2013*
Note: The statistics reflect number of tickets



Graph 3: *Intrusion Defacement Q1 (Jan - Mar) 2013*

A total number of 782 URLs were defaced in the 1st quarter of 2013. Similar to the

1st quarter in 2014, the websites were defaced by hacktivist groups. In February and March 2013, Malaysia was struck by the news of Sultanate of Sulu who claimed his ownership over the state of Sabah. The hacktivists, mainly from Malaysia and Philippines had exploited this issue to deface several websites including government websites belonging to the both countries for various political and personal agendas. These hacktivists had posted their thoughts and opinions on the defaced websites. Below is an example of a website that was defaced by these hacktivists.



HACKED BY: Kismet-07

Anonymous Cebu

Greetings Malaysia and Malaysian Govt.

Time has come to reclaim what is truly ours.
Sabah is owned by the Philippines, you illegally claiming it.
Even if you look in every history of Sabah, Philippines is the owner of it.
Don't try what China is doing at this time.
Also, don't dare to hack our websites,
OR ELSE WE WILL CONTINUE ATTACKING YOUR CYBER WORLD!
YOU STARTED THE FIRE. WE WILL END IT WITH DUST!

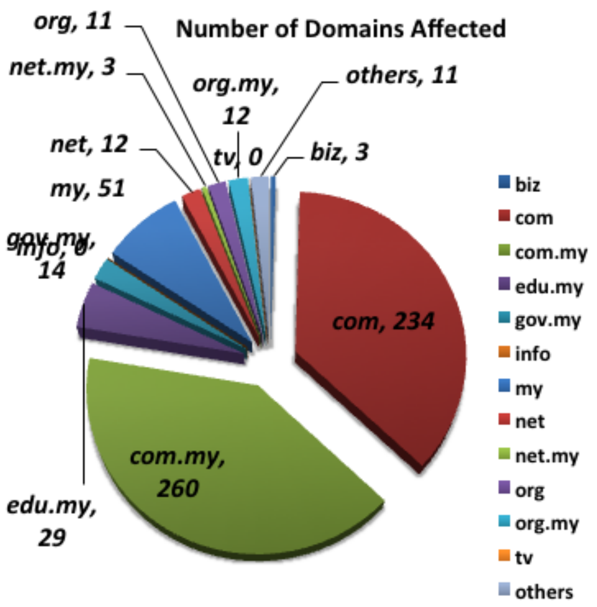
From the statistics above, it is observed that web defacement incidents from the 1st quarter 1 2013 to 2014 has decreased from 823 to 374 cases. However, the matter should not be taken lightly as the incident would definitely increase should there be issues or sentiments that can be exploited by hacktivists.

V. Indepth Analysis on Intrusion Defacement Quarter 1, 2004

The domains that were targeted by most of the intrusion defacement in the 1st quarter of 2014 are as shown in *Table 4* and *Graph 4*. The list was provided by MyCERT's web defacement crawler tool, MyLipas v0.7.2.

List of Domains	Number of Domains Affected
biz	3
com	234
com.my	260
edu.my	29
gov.my	14
info	0
my	51
net	12
net.my	3
org	11
org.my	12
tv	0
others	11
Total	640

Table 4: *Total targeted domains reported*



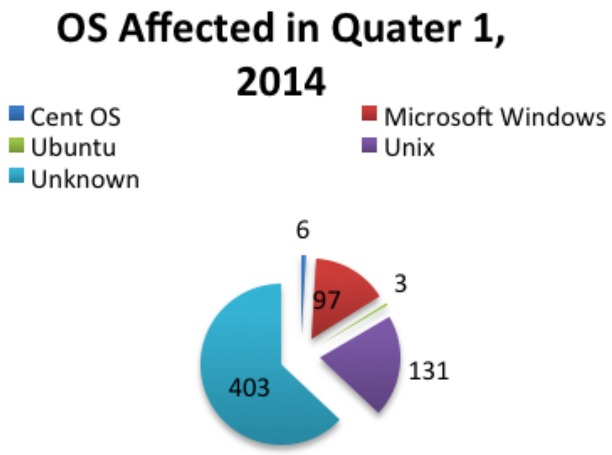
Graph 4: *Number of Domains targeted by defacement*

From the graph above, we can see that the top domains being defaced were com.my with 260 URLs followed by .com with 234 URLs and .my with 51 URLs.

Table 5 and *Graph 5* show the operating systems that were defaced in Quarter 1, 2014

OS	
Cent OS	6
Microsoft Windows	97
Ubuntu	3
Unix	131
Unknown	403
Total	640

Table 5: *Total affected Operating System domains reported*



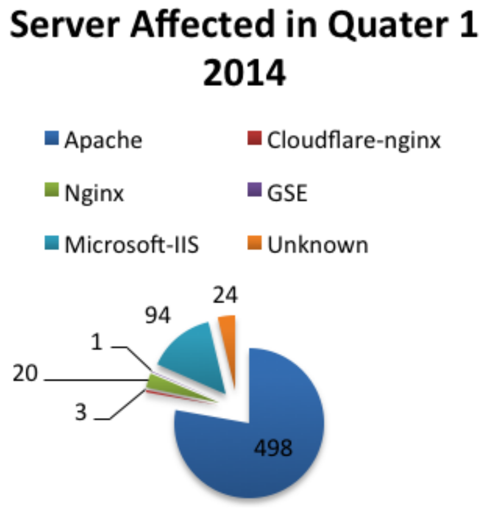
Graph 5: *Number of Operating Systems affected by defacement*

From the graph above, we can see that most websites using Unix operating system with 131 websites have been defaced. This is followed by Microsoft Windows with 97 websites and Ubuntu with six websites. The graph also indicates that 403 websites that were defaced were unable to be detected.

Table 6 and *Graph 6* below shows the servers that are affected by these incidents in Quarter 1, 2014.

Server	
Apache	498
Cloudflare-nginx	3
Nginx	20
GSE	1
Microsoft-IIS	94
Unknown	24
Total	640

Table 6: *Total affected Server reported*



Graph 6: *Number of Servers affected by defacement*

From the graph, we can see most websites using Apache server having 498 URLs were defaced followed by Microsoft Windows IIS with 94 URLs and Nginx with 20 URLS. The graph also indicates that the servers that housed 24 defaced URL were unable to be detected.

VI. Best Practices / Recommendation for Prevention

MyCERT has released an advisory pertaining to web security in order to protect various web owners against web defacement. The advisory can be referred in the following URL:

http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/945/index.html

The most common and immediate solution for handling a defaced website is by taking the website offline temporarily to contain further damage. The offline duration can be utilised to troubleshoot, analyse and rectify problems. However, the decision to take this common or immediate solution depends on the top management and organisational policy. The system administrator has to consult the top management as taking the website offline temporarily can be perceived as denial of service that affects the uptime of the compromised system. Links below are generic guidelines on how to act and handle web defacement incidents in an organisation. As this is the general guideline, most of the steps are relevant to most platforms. Your milestone may vary.

- Web Defacement - Incident Handling Steps (Unix/Linux/BSD)

  http://www.mycert.org.my/en/resources/incident_handling/main/main/detail/754/index.html

- Web Defacement - Incident Handling Steps (Windows)
  http://www.mycert.org.my/en/resources/incident_handling/main/main/detail/755/index.html

Conclusion

In conclusion, the numbers of incidents categorised under intrusion defacement during the 1st Quarter of 2014 were 640 URLs with 374 tickets. The numbers fluctuate, as in most cases web defacement attacks are merely the extension of physical crisis into cyberspace. It is also concluded that the motivation of web defacement attacks are no longer to detect vulnerabilities and inform system administrators about the security loopholes that exist in their systems but they are the means for hacktivist groups to express their feelings and protest against any organisation/government.

In this regard, all system owners need to be alert and take the necessary measures to secure their websites. Updating with the latest versions, patching systems, and conducting penetration testing are amongst the steps that can be taken by system administrators to ensure the security of their websites. System Administrator, Internet Service Provider (ISPs), Web Hosting and users must take note about intrusion defacement activities that may be present in their system logs. The repercussions from these activities can be of high impact namely on their websites availability and integrity, as well as their organisational image. ■

References

1. *http://www.mycert.org.my/en/services/statistic/mycert/2014/main/detail/949/index.html*

2. *http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/945/index.html*

Cloud Security Principles: What You Should Ask Your Cloud Service Provider

By | Ruhama bin Mohammed Zain

Cloud Security Principles

Cloud computing has become more and more acceptable to businesses today as some of the earlier reservations about the security of cloud services have given way to a more reality-based business requirement. This is also because of the move by some well-known companies and businesses that migrate some if not all of their applications to the cloud.

However, the ultimate responsibility for your data and especially your client's data rests with you, the business organisation and not with the cloud provider. Sure, you can put into the service level agreements what are the security responsibilities of the cloud provider but that will not absolve a businesses from being answerable to their clients for any data breaches in the cloud environment.

What then, are some of the cloud security principles against which you can measure the cloud provider's ability to ensure your data is secure as it should be? This article will describe some of them and explain some examples by which to measure whether the principles are adhered to by cloud service providers.

A principle is defined as "a basic truth or theory: an idea that forms the basis of something" according to the Merriam-Webster online dictionary. Security is taken to mean "the state of being protected or safe from harm" and cloud refers to "the computers and connections that support cloud computing" according to the same dictionary.

As we know the term cloud computing has been generally accepted to refer to either of the following types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These categorisations was derived from the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce. The principles described in this article should apply to all three.

The term "consumer" used in this article shall be taken to mean the subscriber of the cloud computing service.

1. Data in transit must be protected

This refers to the requirements that consumer data that travel across the networks must be sufficiently protected against eavesdropping and tampering, in order to protect their confidentiality and integrity. The way to do this is to apply a combination of encryption and network controls. Encryption will prevent an attacker from reading the data and network controls will prevent them from intercepting the data in the first place.

2. Asset must be made resilient and protected

Asset here refers to the computers and processing systems that either store or process consumer data. Both the asset and the consumer data itself must be protected from being tampered physically, stolen or damaged. Things like offsite backups, redundant servers, and physical security of the cloud data centres are some of the items that needs to be noted here.

3. Cloud tenants must be separated

Public cloud computing to a certain extent of the definition implies multi-tenancy. What this means is there exists more than one consumer utilising the same resources of the cloud service provider. It is therefore critical that separation between different consumers of the cloud service be established to eliminate the possibility of either malicious acts or compromised consumers adversely affecting the confidentiality, availability or integrity of another consumer of the service.

4. Availability of audit information to consumers

It is important that the consumers have available to them the audit information so that they may monitor things like access to their service and also access to the data that is contained within it. This is to allow them to take necessary actions in case of unexplained data access by potentially unauthorised parties.

5. Secure administration of the cloud service

The consumer should make sure that the methods used by the administrators of these service providers in managing the operational service are done in a manner designed to mitigate any risk of exploitation which could jeopardise the security of the service. Good practices like separation of duties between the service provisioners and the security administrators is one example.

6. Protection of External Interfaces

It is important to identify all external and any less trusted interfaces connected to the service so that proper protections are allocated to defend them against attacks. Since the networks that the cloud service runs on belong to the cloud provider, sometimes the consumer has no say whenever new connections are introduced into the network at a later stage. This becomes an important issue to be considered by the consumer.

7. Authentication and authorisation

Any and all access by both the consumer and the service provider to all interfaces into the service must follow strict authentication and authorisation processes. Nobody should be exempted from this requirement so that there is less chance for unauthorised individuals to do something harmful and also to ensure that actions taken by authorised individuals can later be traced back to them for accountability purposes.

8. Operational Security

There should be processes and procedures in place by the cloud service provider to ensure the operational security of the service is well-defined. The processes and procedures are important so that everybody is aware and can properly do their work during normal operating conditions as well as during security disasters.

9. Personnel security

The consumer should make sure that the cloud service provider performs adequate security screening of their personnel and ensure that those personnel undergo the correct security training for their role in the cloud provider's organisation.

10. Secure development of services

Consumers should evaluate and decide whether the cloud service provider implement secure development practices. One way this can be verified is to insist on the latest vulnerability and security assessment reports of the services that the consumer is interested in. This can help to show whether the cloud service provider consistently identify and mitigate threats to the security of the service.

Conclusion

Security is the responsibility of both the consumer and the cloud service provider. This article has attempted to describe some of the security principles that both the consumer and the provider should be concerned with. There are additional security principles that will add extra layers of confidence if they are implemented by the provider but the principles described above should be a good starting point in the right direction for the consumer. ■

References

1. *http://www.merriam-webster.com/dictionary/security*
2. *http://www.accountingcoach.com/blog/separation-of-duties-internal-control*
3. *http://www.safenet-inc.com/data-protection/virtualization-cloud-security/saas-security-cloud-access-control/*
4. *4. https://datatracker.ietf.org/documents/LIAISON/file1181.doc [Requirements for Service Protection Across External Interfaces Draft 0.34 January 2011]*
5. *https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles*

A Forensic Analysis on SMS Timestamp

By | Nor Zarina Zainal Abidin

I was once given a mobile phone to be analysed for a criminal case several years ago. The case objective was to extract SMS (text messages) from the phone and to correlate the timestamp of SMS from the sender's phone and the SMS from the receiver's phone.

What was supposed to be a simple analysis became complex as the timestamp correlation did not make sense at all. Further analysis on the timestamp found that there were actually three possibilities of how SMS timestamp were generated on the phone.

When a SMS is received, the timestamp displayed on the SMS could be:

- The timestamp of the sender's phone (device time)
- Timestamp of the telecommunication provider's server time (network time)
- Timestamp of the recipient's phone (device time)

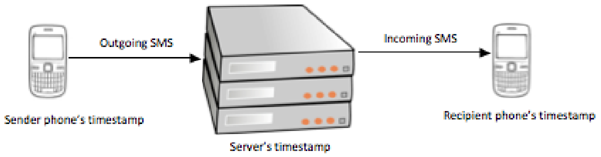
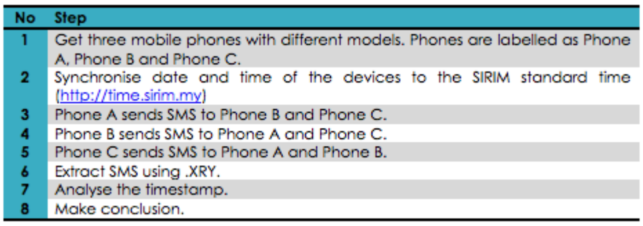


Figure 1: *Three (3) possibilities of timestamp generated for an SMS. Have you ever wondered which timestamp is displayed on your SMS?*

How do we determine which timestamp is generated on the SMS? In this article, I will present a simple analysis on three phone models and provide a conclusion from the analysis.

Methodology

The methodology of conducting this analysis is quite simple. The steps below show how the analysis is conducted:

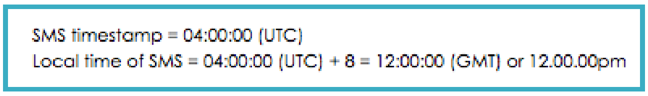


No	Step
1	Get three mobile phones with different models. Phones are labelled as Phone A, Phone B and Phone C.
2	Synchronise date and time of the devices to the SIRIM standard time (http://time.sirim.my)
3	Phone A sends SMS to Phone B and Phone C.
4	Phone B sends SMS to Phone A and Phone C.
5	Phone C sends SMS to Phone A and Phone B.
6	Extract SMS using .XRY.
7	Analyse the timestamp.
8	Make conclusion.

Preliminary Study on Timestamp

Before we proceed to the next section, it is important for an analyst to understand the timestamp system. Mobile phones, in general, uses the Coordinated Universal Time (UTC) format. It is also known as Zulu time' or 'Z time'. UTC is 24-hour time, which begins at 00:00 at midnight.

To obtain Malaysia's local time (known as GMT), we need to add 8 hours (+8) to the UTC. The example of UTC to GMT calculation is as below:



SMS timestamp = 04:00:00 (UTC)
Local time of SMS = 04:00:00 (UTC) + 8 = 12:00:00 (GMT) or 12.00.00pm

Figure 2: *Converting UTC time to GMT time*

Analysis & Finding

Three phone models were used for the purposes of this study. The phones have been synchronised to the SIRIM standard time. The details are as follows:

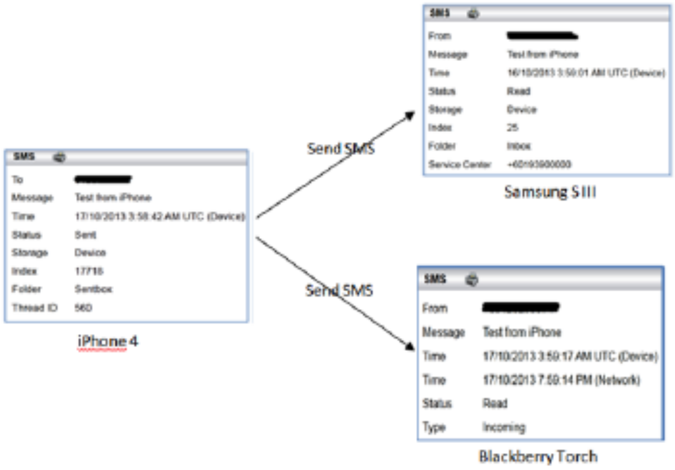
No	Model	Operating System	Telecommunication Provider (Telco)	Label
1	Apple iPhone 4 GSM	iOS	Telco X	Phone A
2	Samsung GT-i9305 Galaxy S III	Android	Telco Y	Phone B
3	BlackBerry 9800 Torch	Blackberry OS	Telco Z	Phone C

***Table 1:** Mobile Phone details*

The phones were then plugged into the .XRY and the SMS data was extracted from the phones.

Analysis on Apple iPhone 4 GSM

After synchronising the time to the standard time, SMS was sent from Phone A to Phone B and Phone C. The SMS timestamp shown in each phone is shown is the figures below:



SMS

To	[redacted]
Message	Test from iPhone
Time	17/10/2013 3:58:42 AM UTC (Device)
Status	Sent
Storage	Device
Index	17718
Folder	Sentbox
Thread ID	560

SMS

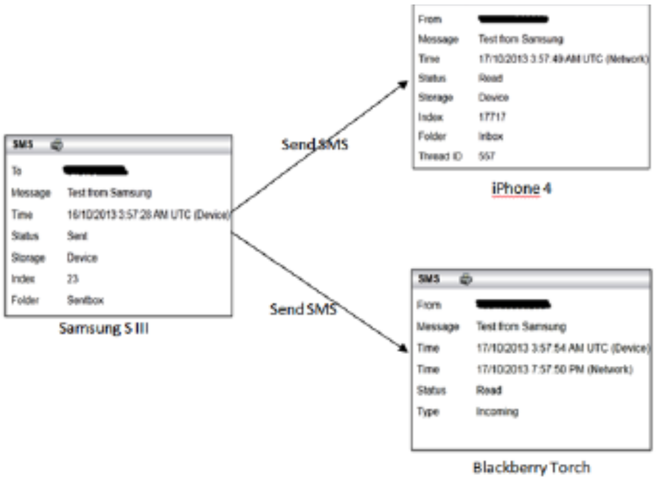
From	[redacted]
Message	Test from iPhone
Time	16/10/2013 3:50:01 AM UTC (Device)
Status	Read
Storage	Device
Index	25
Folder	Inbox
Service Center	+60193900000

SMS

From	[redacted]
Message	Test from iPhone
Time	17/10/2013 3:59:17 AM UTC (Device)
Time	17/10/2013 7:59:14 PM (Network)
Status	Read
Type	Incoming

Analysis on Samsung GT-i9305 Galaxy S III

In the next step, SMS was sent from Phone B to Phone A and Phone C. The SMS timestamps shown in each phone are displayed in the diagram below:



SMS

To	[redacted]
Message	Test from Samsung
Time	16/10/2013 3:57:28 AM UTC (Device)
Status	Sent
Storage	Device
Index	23
Folder	Sentbox

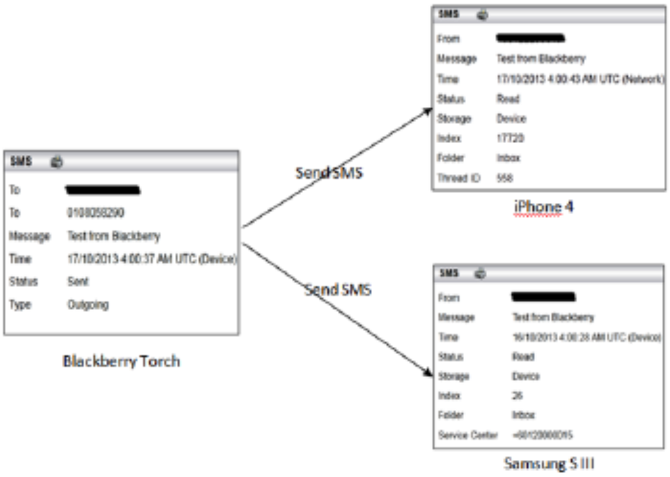
From	[redacted]
Message	Test from Samsung
Time	17/10/2013 3:57:49 AM UTC (Network)
Status	Read
Storage	Device
Index	17717
Folder	Inbox
Thread ID	557

SMS

From	[redacted]
Message	Test from Samsung
Time	17/10/2013 3:57:54 AM UTC (Device)
Time	17/10/2013 7:57:50 PM (Network)
Status	Read
Type	Incoming

Analysis on BlackBerry 9800 Torch

In the final step, SMS was sent from Phone C to Phone A and Phone B. The SMS timestamps shown in each phone are displayed in the diagram below :



SMS

To	[redacted]
To	0108058290
Message	Test from Blackberry
Time	17/10/2013 4:00:37 AM UTC (Device)
Status	Sent
Type	Outgoing

SMS

From	[redacted]
Message	Test from Blackberry
Time	17/10/2013 4:00:43 AM UTC (Network)
Status	Read
Storage	Device
Index	17720
Folder	Inbox
Thread ID	558

SMS

From	[redacted]
Message	Test from Blackberry
Time	16/10/2013 4:00:28 AM UTC (Device)
Status	Read
Storage	Device
Index	26
Folder	Inbox
Service Center	+60120000015

The following table provides a summarised view of the SMS timestamps for all the phones.

iPhone 4	Samsung S III	Blackberry Torch
Outgoing SMS Timestamp	Incoming SMS Timestamp	
17/10/2013 3:58:42 AM UTC (Device)	16/10/2013 3:59:01 AM UTC (Device)	▪ 17/10/2013 3:59:17 AM UTC (Device) ▪ 17/10/2013 7:59:14 PM (Network)

Table 2: *Summarised table of timestamp for outgoing text messages from iPhone 4*

Samsung S III	iPhone 4	Blackberry Torch
Outgoing SMS Timestamp	Incoming SMS Timestamp	
16/10/2013 3:57:28 AM UTC (Device)	17/10/2013 3:57:49 AM UTC (Network)	▪ 17/10/2013 3:57:54 AM UTC (Device) ▪ 17/10/2013 7:57:50 PM (Network)

Table 3: *Summarised table of timestamp for outgoing text messages from Samsung S III*

Blackberry Torch	iPhone 4	Samsung S III
Outgoing SMS Timestamp	Incoming SMS Timestamp	
17/10/2013 4:00:37 AM UTC (Device))	17/10/2013 4:00:43 AM UTC (Network)	16/10/2013 4:00:28 AM UTC (Device)

Table 4: *Summarized table of timestamp for outgoing text messages from Blackberry Torch*

Summary of Finding

The forensic analysis conducted on the SMS timestamps from the three different phone models shows that:

1. Apple iPhone 4 GSM generates network timestamp for incoming SMS and device time for outgoing SMS.

2. Samsung GT-i9305 Galaxy S III records the device time for both incoming and outgoing text messages.

3. BlackBerry 9800 Torch (Phone C) records the device and network times for incoming text messages but only device time for outgoing text messages.

No	Mobile Phone	Findings (Time)	
		Incoming text messages	Outgoing text messages
1.	Apple iPhone 4 GSM (Phone A)	Network	Device
2.	Samsung GT-i9305 Galaxy S III (Phone B)	Device	Device
3.	BlackBerry 9800 Torch (Phone C)	Network & Device	Device

Table 5: *Summary of findings*

Conclusion

Being a forensic analyst, one must be able to explain the meaning and significance what each data entails, especially the timestamp on a piece of data. This is important to ensure that data can be correctly correlated with each other, and at the end providing meaningful data to assist the investigation of a criminal case. ■

CRYPTOGRAPHY

In staying secure and safe, reliable encryption remains the foundation on which the trillion-dollar edifice of global e-commerce is built on.

By | Liyana Chew Nizam Chew

WHAT IS CRYPTOGRAPHY?	WHERE IS CRYPTOGRAPHY?
The science of making codes and encoding information and transforming private data into an unreadable format in preventing parties with hostile interests from obtaining them	▪ Government ▪ Spies ▪ Financial Institutions ▪ Security Agencies ▪ and YOU
WHY CRYPTOGRAPHY?	**WHO USES CRYPTOGRAPHY?**
Cryptography is an essential part of modern life. It allows users to protect the integrity of communications and the confidence of data without being held to ransom.	Any type of business that are using computers will surely have data to protect

Modern cryptography entails security and adheres to the following basic paradigms and principles:

1. Confidentiality – information that cannot be understood by anyone other than for whom it was intended for. Thus, protecting the information from disclosure to unauthorised parties.

2. Integrity – the information cannot be altered in storage or transit between sender and intended receiver with such alterations being detected.

3. Non-Repudiation- the creator/ sender of the information will not be able to deny at a later stage of his/her intentions in the creation or transmission of the information

4. Authentication – the sender and receiver can verify each other's identity and the origin/destination of the information. ■

Hantu Internet

By | Azira Abd Rahim

1.0 Pengenalan

Era globalisasi dan dunia tanpa sempadan yang diwar-warkan pada hari ni menjadikan setiap daripada kita berusaha untuk menjadi lebih maju seiring dengan pembangunan teknologi yang semakin canggih dan mendapat tempat dalam masyarakat. Hari ini, kita dapat melihat bagaimana teknologi moden memberi impak yang begitu besar terhadap kehidupan kita. Dunia Internet khususnya adalah salah satu daripada media canggih yang semakin mendapat perhatian segenap lapisan umur di mana ia turut memberi kesan dalam aktiviti kehidupan seharian yang meliputi urusan perhubungan, komunikasi, perbankan dan jual-beli, pembelajaran, keselamatan, hiburan dan lain-lain. Oleh demikian, dunia Internet telah banyak mengubah cara manusia berfikir, berhubung, berinteraksi di antara satu sama lain. Dalam erti kata lain, ia telah mewujudkan satu bentuk kehidupan yang unik namun ia tiada berbeza dari kehidupan di alam realiti.

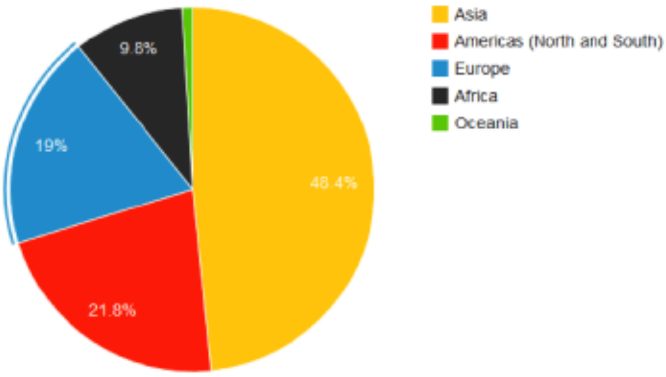
2.0 Statistik Kadar Pengguna Internet Di Seluruh Dunia

Berdasarkan data yang diperolehi dari 'Internet Live Stats' (penghuraian data oleh Kesatuan Telekomunikasi Antarabangsa (ITU) dan Bahagian Penduduk Bangsa-Bangsa Bersatu) pada tahun 2014, hampir 75 peratus atau 2.1 billion penduduk dunia terdiri daripada pengguna Internet. Negara China mempunyai kadar penduduk tertinggi dunia mewakili hampir 22 peratus daripada jumlah tersebut.

Ilustrasi 1: Jumlah pengguna Internet di seluruh dunia sehingga tahun 2014

Year (July 1)	Internet Users	Users Growth	World Population	Population Growth	Penetration (% of Pop. with Internet)
2014*	2,925,249,355	7.9%	7,243,784,121	1.14%	40.4%
2013	2,712,239,573	8.0%	7,162,119,430	1.16%	37.9%
2012	2,511,615,523	10.5%	7,080,072,420	1.17%	35.5%
2011	2,272,463,038	11.7%	6,997,998,760	1.18%	32.5%
2010	2,034,259,368	16.1%	6,916,183,480	1.19%	29.4%
2009	1,752,333,178	12.2%	6,834,721,930	1.20%	25.6%
2008	1,562,067,594	13.8%	6,753,649,230	1.21%	23.1%
2007	1,373,040,542	18.6%	6,673,105,940	1.21%	20.6%
2006	1,157,500,065	12.4%	6,593,227,980	1.21%	17.6%
2005	1,029,717,906	13.1%	6,514,094,610	1.22%	15.8%
2004	910,060,180	16.9%	6,435,705,600	1.22%	14.1%
2003	778,555,680	17.5%	6,357,991,750	1.23%	12.2%
2002	662,663,600	32.4%	6,280,853,820	1.24%	10.6%
2001	500,609,240	21.1%	6,204,147,030	1.25%	8.1%

* Source: Internet Live Stats (elaboration of data by International Telecommunication Union (ITU) and United Nations Population Division)



Sumber: ‘Internet Live Stats’ (penghuraian data oleh Kesatuan Telekomunikasi Antarabangsa (ITU) dan Bahagian Penduduk Bangsa-Bangsa Bersatu)

Berdasarkan gambar rajah di atas, kita dapat melihat bahawa penduduk dari negara-negara Asia merupakan peratusan pengguna Internet yang tertinggi berbanding penduduk di negara Eropah dan Amerika. Oleh itu, angka ini perlu dikaji untuk menilai sekiranya wujud masalah-masalah seperti ketagihan Internet di kalangan penduduk yang menggunakan Internet.

3.0 Kajian Berkenaan Dengan Ketagihan Internet Di Kalangan Pengguna

Seperti yang kita sedia maklum, Internet menyediakan pelbagai maklumat serta kemudahan yang boleh diakses dengan menggunakan telefon pintar, tablet dan juga komputer riba. Internet juga menghubungkan pengguna melalui e-mel, blog, rangkaian sosial dan perkhidmatan pesanan ringkas, di mana pengguna boleh berkomunikasi tentang pelbagai isu dan topik semasa tanpa perlu berada di sesuatu lokasi secara fizikal. Penyebaran penggunaan yang meluas ini memberi kesan terhadap hubungan *interpersonal (antara perorangan) dan intrapersonal (komunikasi dengan diri)* masyarakat samada secara positif mahupun negatif. Sesetengah masyarakat beranggapan bahawa penggunaan Internet telah mengurangkan interaksi secara bersemuka. Lebih banyak masa dihabiskan di Internet sehingga ianya menjejaskan kualiti waktu yang sepatutnya dihabiskan bersama keluarga dan rakan-rakan. Membeli belah dalam talian pula adalah sangat mudah dan menjimatkan masa. Namun kegunaannya juga telah menyebabkan orang ramai membeli barangan dan perkhidmatan tanpa berinteraksi secara fizikal. Peniaga yang menjalankan perniagaan atas talian pula dapat melakukan perniagaan mereka dengan mudah, namun mereka seolah-olah terkurung dari melihat dunia luar.

Menurut petikan dari laporan yang dikemukakan oleh Kementerian Kewangan 2013/2014 sempena Belanjawan 2014, jumlah bilangan pengguna Internet di Malaysia dijangka meningkat kepada 25 juta orang menjelang 2015 berbanding 18 juta orang pada 2012. Ianya merangkumi peningkatan kadar penembusan jalur lebar isi rumah kepada 66.8 peratus sehingga akhir Jun 2014. Manakala untuk kadar penembusan telefon mudah alih, ia melebihi 100 peratus dengan kadar sebanyak 42.6 juta langganan. Laporan ini merumuskan bahawa rakyat Malaysia semakin banyak memperuntukkan masa mereka melayari Internet berbanding rangkaian media lain seperti radio, televisyen, suratkhabar dan sebagainya. Menurut laporan ini lagi, sebanyak 11.8 juta rakyat Malaysia dianggarkan mempunyai akaun Facebook dengan lebih 80 peratus melayari Internet untuk mengakses Facebook.

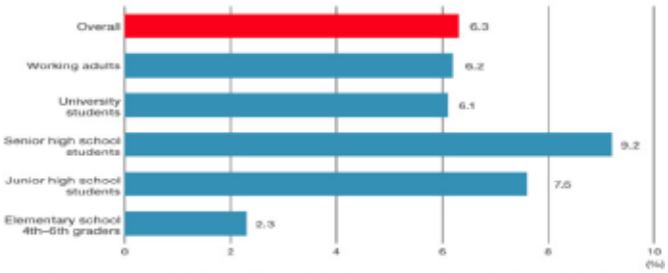
Melihat kepada cara hidup masyarakat hari ini, ianya kelihatan seolah-olah masyarakat lebih selesa memperuntukkan sebahagian besar waktu mereka dengan melayari laman serta aplikasi media sosial seperti ‘Facebook’,’ Instagram’, ‘Twitter’ dan sebagainya. Media sosial adalah salah satu aplikasi Internet terkini yang mempunyai daya penarik dan boleh digunakan oleh pelbagai lapisan masyarakat. Justeru, kita boleh katakan bahawa aspek teknologi Internet adalah penting untuk masyarakat digital masa kini. Namun perlu diingat bahawa Internet juga boleh menyumbang kepada kemudaratan seperti gejala penipuan, penggodaman, serangan virus, penyamaran, pembulian siber dan sebagainya yang boleh menyebabkan pengguna lain menjadi mangsa. Apa yang lebih membimbangkan adalah apabila kita turut mengalami gejala ketagihan akibat penggunaan Internet berikutan banyak masa yang telah diluangkan sehingga mengabaikan pelbagai perkara lain yang lebih penting dalam kehidupan seharian kita. Sekiranya masyarakat berkelakuan begini secara berterusan, ia akan menyebabkan kesan negatif yang lebih mendalam terhadap ekosistem interaksi dan komunikasi.

Bagaimana Seseorang Menjadi Ketagih Kepada Internet?

Ketagihan Internet telah menjadi satu masalah sosial yang sangat besar di negara-negara seperti Korea, China, Amerika Syarikat dan sebagainya. Kecenderungan peningkatan ketagihan Internet ini kebanyakannya didapati di kalangan remaja yang majoritinya adalah pelajar sekolah. Kebanyakan daripada mereka adalah pengguna telefon pintar, di mana terdapat pelbagai aplikasi yang mudah didapati selain dari penggunaan rangkaian sosial.

Mengikut kajian yang telah dilakukan oleh Institut Dasar Maklumat dan Komunikasi di Kementerian Hal Ehwal Dalaman dan Komunikasi pada Februari 2013, seramai 2,605 orang telah mengambil bahagian dalam kajiselidik ketagihan Internet mengikut peringkat umur, termasuk pelajar sekolah rendah dan dewasa. Analisis kajian telah mendedahkan bahawa peratusan tertinggi orang yang terdedah kepada ketagihan Internet adalah terdiri dari para pelajar sekolah menengah tinggi sebanyak 9.2 peratus diikuti oleh pelajar sekolah menengah rendah sebanyak 7.6 peratus. Melihat kepada peratusan ini, ianya cukup untuk membuatkan kita merasa bimbang akan kesan yang bakal dihadapi di masa akan datang apabila pelajar sekolah telah terjebak dengan ketagihan Internet ini.

Internet addiction rate by age group



Source: Survey conducted in February 2013 by the Hashimoto Laboratory and the Institute for Information and Communications Policy, Ministry of Internal Affairs and Communications

Sebagaimana penagih yang bergantung kepada dadah dan alkohol, begitulah juga dengan pengguna yang ketagihan Internet sehingga adakalanya mengganggu kesihatan fizikal dan mental. Merujuk kepada contoh-contoh yang dilaporkan di luar negara, ianya sudah cukup untuk membuka mata dan minda kita betapa bahayanya ketagihan Internet ini sekiranya tidak dibendung segera.

1. # 1- Chris Staniforth , Julai 2011

Chris Staniforth merupakan seorang pemuda berusia 20 tahun dari Sheffield, England telah mengalami ketagihan permainan video sehingga meninggal dunia secara tiba-tiba selepas bermain video selama 12 jam. Oleh kerana beliau memperuntukkan masa berlebihan tanpa berehat dan melakukan senaman mengakibatkan darah beku berpindah ke paru-paru beliau seterusnya tersumbat dan membawa maut.

2. # 2- Chen Shi, September 2010

Chen Shi , remaja berusia 16 telah terbunuh di Sekolah Beiteng di Changsha, China, di mana beliau telah dihantar untuk memulihkan dirinya daripada ketagihan Internet. Malangnya beliau telah dipukul sehingga meninggal dunia semasa mengikuti kelas pemulihan ketagihan Internet ini.

China adalah antara salah satu daripada negara-negara yang mengalami gejala ketagihan Internet; satu daripada setiap 10 pengguna Internet didakwa mengalami ketagihan.

3. # 3- Daniel Petric, Jun 2007

Daniel Petric berumur 16 tahun telah melakukan pembunuhan yang berniat jahat di rumah ibu bapanya di Wellington, Ohio akibat terlalu taksub dengan permainan video. Apabila ibu bapa Petric mula merasakan bahawa permainan ganas ini perlu dihentikan lantas Petric telah menembak kedua ibu bapanya menggunakan senjata bapa Petric dan telah dibicarakan di mahkamah dan telah dijatuhkan hukuman penjara selama 23 tahun untuk jenayah itu.

4. #4- Kes Kebuluran Kanak-Kanak, Mei 2010

Sepasang suami isteri dari Korea Selatan telah didakwa membunuh bayi perempuan mereka dengan hanya memberi makan sekali sehari sahaja akibat leka bermain permainan video di kafe Internet. Bayi itu juga dikatakan dipukul apabila menangis kelaparan. Kematian bayi ini adalah disebabkan nutrisi makanan yang tidak mencukupi. Akhirnya pasangan ini telah dipenjara selama 2 tahun atas kesalahan yang dilakukan.

Melihat pada kejadian tersebut membuatkan kita berfikir sejenak akan kesan dan impak disebalik ketagihan Internet ini sekiranya tiada alternatif yang ditawarkan untuk mengurangkan ketagihan ini. Ketagihan Internet boleh menjejaskan juga fungsi dan kehidupan masyarakat sekiranya dikaji dari sudut kesihatan mental dan memerlukan rawatan yang khusus. Ketidakmampuan untuk mengawal tindakan impulsif adalah salah satu sebab utama di sebalik ketagihan Internet ini. Mereka yang mengalami masalah emosi di mana sering tidak berpuas hati dengan kehidupan akan lebih cenderung menjadi seorang yang ketagihan Internet daripada seseorang yang mempunyai emosi positif dan gembira.

4.0 Penutup

Kesimpulannya, penggunaan Internet sememangnya memberikan kesan yang amat besar dalam kehidupan seharian kita. Sebagai pengguna Internet, kita seharusnya bijak dalam mewujudkan keseimbangan antara aktiviti Internet dan kehidupan sebenar untuk kebaikan sesama manusia. Untuk yang demikian, adalah penting kita perlu memastikan gejala ketagihan Internet ini dapat dibendung dari terus menular di kalangan masyarakat kini. Sekiranya anda mendapati gejala ini ada pada diri anda, lakukanlah sesuatu bagi mengelakkan diri anda dari terus terjerumus ke dalam masalah yang lebih besar, jangan segan untuk berjumpa kaunselor dan mulalah menggunakan Internet secara positif dan mengikut panduan. Ibu bapa juga berperanan menghadkan dan memantau anak-anak menggunakan komputer ketika melayari Internet. Ini adalah langkah yang bijak dan praktikal bagi mengurangkan gejala masalah ketagihan Internet. ■

Laman Rujukan

1. *http://www.internetinternetlivestats.com/internetInternet-users/*

2. *http://www.addictionrecov.org/Addictions/index.aspx?AID=43*

3. *http://www.netaddictionrecovery.com/the-problem/signs-and-symptoms.html*

4. *http://amanz.my/2012/12/secara-purata-pengguna-malaysia-menghabiskan-masa-sebanyak-20-jam-seminggu-di-internet/*

Mengenali Apakah Itu APT

Tidak ada "peluru perak" dalam mempertahankan aset terhadap APT. Yang nyata, ketersediaan penyelesaian keselamatan merentasi domain hari ini boleh membantu organisasi menangani masalah yang kian mencabar ini.

By | Mohd Fadzlan Mohamed Kamal

Pengenalan Kepada Dunia Siber

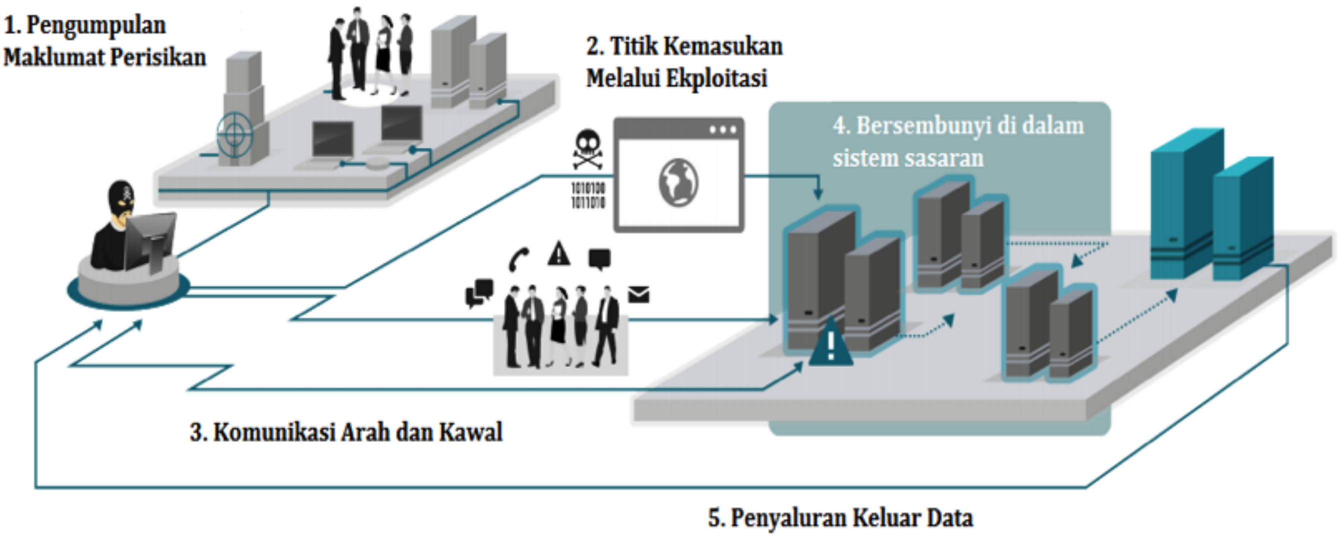
Perkembangan teknologi maklumat yang semakin canggih dan pantas pada hari ini bukan hanya memberi manfaat kepada segelintir pengguna sahaja bahkan melangkaui semua golongan dari seawal usia kanak-kanak sehinggalah kepada golongan berusia. Jika diteliti, kadar penembusan capaian dan penggunaan teknologi maklumat di Malaysia, ianya sangat mengagumkan dan meningkat hampir setiap hari. Tambahan pula, kerajaan telah memperkenalkan beberapa insentif dan inisiatif baru kepada golongan sasar seperti golongan belia, pelajar sekolah dan penduduk luar bandar dalam menyalurkan bantuan kemudahan IT. Secara tidak langsung, ini telah membolehkan bidang teknologi maklumat di Malaysia berkembang dengan pesatnya.

Walaupun terdapat banyak kebaikan yang diperolehi dalam bidang ini, namun pada sudut tertentu ia turut sama membuka ruang dan peluang kepada individu atau kumpulan yang cuba mengambil kesempatan dengan cara yang salah bagi meraih keuntungan atau bermotif jahat. Pihak yang cuba mengambil kesempatan atau digelar penjenayah siber ini, turut sama berkembang maju dan berevolusi seiring kecanggihan teknologi semasa malah mereka akan sentiasa cuba berada setapak di hadapan dalam kemajuan teknologi yang di kecapi. Oleh itu, semua pihak harus peka dan sentiasa berwaspada dengan taktik dan teknik terbaru yang diguna pakai bagi mengurangkan risiko menjadi mangsa sasaran penjenayah siber.

APT - Ancaman Kepada Dunia Siber

Advanced Persistent Threats atau lebih dikenali dengan nama singkatan APT merupakan antara ancaman berbahaya kepada dunia siber dewasa ini. Ia bukanlah sesuatu yang terlalu baru namun masih ramai yang belum mengetahui atau memahami apakah yang dimaksudkan dengan APT dan cara kerjanya. Terdapat pelbagai takrifan dan definisi yang berbeza mengenai APT ini mengikut sudut pandangan individu atau sesebuah organisasi, namun secara dasarnya APT merujuk kepada ancaman yang mempunyai tahap kebolehupayaan tinggi yang dicipta oleh individu pakar dalam bidang teknologi maklumat bertujuan untuk melakukan aktiviti jenayah terutamanya bermotifkan pengintipan.

Perkara menarik mengenai APT ialah, ia dicipta lebih khusus jika dibandingkan dengan perisian perosak (malware) yang wujud sebelum ini. Ini adalah disebabkan APT biasanya beroperasi untuk mencapai sasaran tertentu seperti pengintipan sesebuah negara, parti politik atau organisasi berbanding sasaran secara rawak. Oleh kerana APT dicipta secara khusus, mungkin ramai individu menyangka mereka tidak akan menjadi mangsa sasaran atau ancaman APT ini. Persepsi ini perlu difahami dan diperbetulkan, kerana pada asasnya kita bukanlah sasaran utama namun kita mungkin boleh menjadi salah satu agen pembawa APT tanpa kita sedari.


1. Pengumpulan Maklumat Perisikan
2. Titik Kemasukan Melalui Ekploitasi
4. Bersembunyi di dalam sistem sasaran
3. Komunikasi Arah dan Kawal
5. Penyaluran Keluar Data

Rajah 1 : *Peringkat Serangan APT*

Huraian Makna APT

Dalam menghuraikan makna di sebalik nama APT itu secara lebih mendalam, ia boleh diterjemahkan melalui 3 perkataan berdasarkan nama APT itu sendiri iaitu *Advanced* (canggih), *Persistent* (berterusan) dan *Threat* (ancaman).

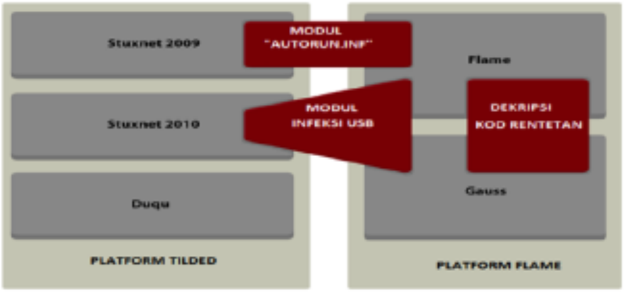
i. Perkataan *advance* merujuk kepada alat atau perisian yang mempunyai kebolehupayaan tinggi yang digunakan oleh penjenayah siber dalam melakukan serangan atau eksploitasi. Ia menggabungkan beberapa jenis teknik serangan dan eksploit ke dalam sesebuah APT. Teknik ini juga agak sukar dikesan oleh pengguna kerana ia tidak melakukan sebarang kerosakan, kemusnahan atau perubahan ketara di dalam sistem yang dihuni. Selain itu, APT juga dikawal untuk berinteraksi dengan pembuatnya iaitu penjenayah siber melalui arah dan kawal *(command and control)* dari pelayan *(server)* di luar rangkaian *(external network)* sesebuah organisasi. Kebiasaannya, APT mempunyai banyak pelayan untuk mengelirukan pihak yang cuba menjejaki, mengesan atau menyelidiki dalang di sebalik pembuat APT ini. *Advance* ini juga merujuk kepada perbezaan di antara APT dengan *malware* yang lain kerana teknik-teknik yang digunakan sangat berbeza serta lebih bijak dalam melakukan proses eksploitasi.

ii. Istilah *persistent* pula merujuk kepada ciri-ciri sesebuah APT yang mengekalkan kewujudan mereka secara tersembunyi di dalam sistem sasaran untuk mempertahankan diri daripada dikesan dan dihapuskan. Walaupun APT bersifat tersembunyi untuk mengelakkan daripada dikesan namun ia aktif berinteraksi dan sentiasa dikawal oleh penjenayah siber ini. Tempoh masa yang diambil oleh APT untuk mencapai objektifnya mungkin mengambil masa berbulan-bulan atau bertahun lamanya. Jangka masa yang panjang ini diambil supaya perancangan rapi dapat diatur untuk mendapatkan maklumat, melakukan pengintipan serta mengumpul sumber secukupnya mengenai sasaran selain cuba menembusi sistem sasaran dengan melakukan pelbagai jenis serangan secara berperingkat bagi mencapai tahap akses yang diinginkan.

iii. Threat atau ancaman pula merujuk kepada keseluruhan APT yang berniat jahat dan membawa impak buruk yang sangat besar kepada mangsa sasaran. Berdasarkan kepada bentuk dan corak serangan APT, ia tidak beroperasi secara sendirian tetapi merupakan jenayah terancang yang mungkin dibiayai oleh badan atau organisasi tertentu. Serangan APT ini cukup berbahaya kerana ia lebih menyasar kepada sesebuah badan atau organisasi yang berprofil tinggi, besar atau berkuasa yang kebiasaannya mempunyai maklumat penting serta kritikal dan perlu dijaga rapi seperti maklumat sistem pertahanan atau ketenteraan sesebuah negara. Maklumat yang dapat di salur keluar itu mungkin dijual kepada musuh atau yang lebih menjadi igauan ialah apabila ia dikongsi secara terbuka dengan orang awam yang mana dapat diakses dari seluruh pelusuk dunia. Jika sasaran mereka itu ialah badan keselamatan negara seperti polis, askar atau pemimpin negara itu sendiri, ini mungkin membawa kepada jatuhnya maruah, kepercayaan, keyakinan rakyat terhadap negara tersebut dan sebagainya.

APT Yang Dikenali

Terdapat banyak serangan APT yang telah dikesan sepanjang beberapa tahun kebelakangan ini. Keadaan ini menunjukkan bahawa APT bukanlah sesuatu yang boleh di ambil ringan. Antara beberapa kod nama APT yang berjaya dikesan ialah GhostNet, Operation Aurora, RSA Attack, Shady RAT, Red October dan lain-lain. Daripada kesemua APT yang dapat dikesan setakat ini, terdapat empat kod nama APT yang banyak diperkatakan dan mempunyai hubungan di antara satu sama lain iaitu Stuxnet, Duqu, Flame dan Gauss. Hubungan ini mungkin sekadar hasil kerjasama antara pembangun pada peringkat awalnya berdasarkan persamaan yang terdapat di dalam penggunaan kod infeksi yang diguna pakai dalam melakukan eksploitasi. Walau bagaimanapun, terdapat perbezaan jika dilihat melalui motif dan matlamat serangan di antara keempat-empat APT ini. Selain itu, keempat-empat APT ini juga dikategorikan antara malware yang mempunyai kod yang agak kompleks dan rumit untuk dirungkaikan.



Rajah 2 : *Hubungan di antara Stuxnet, Duqu, Flame dan Gauss*

Jika dilihat kebanyakan serangan APT lebih tertumpu kepada sistem operasi berasaskan Windows tetapi sebenarnya terdapat juga serangan APT yang lebih dahsyat yang mampu mengeksploitasi sistem operasi lain seperti Mac OS X dan Linux. Sistem operasi bagi alatan mobile seperti Android dan juga iOS tidak terkecuali menjadi sasaran serangan APT ini. APT yang dikenali sebagai Careto atau "The Mask" dikatakan mempunyai ciri-ciri seperti yang telah dinyatakan. Ini bermakna APT tidak terhad untuk melakukan eksploitasi terhadap pengguna yang menggunakan sistem operasi komputer sahaja tetapi juga mampu menjangkiti telefon pintar mahupun tablet. Perkara ini perlu dipandang serius dan diambil cakna oleh semua pengguna. Ini kerana boleh dikatakan semua golongan atau setiap lapisan masyarakat mempunyai peralatan mobile tersendiri yang boleh mengakses apa sahaja maklumat di hujung jari membuatkan APT lebih mudah untuk disebarkan tanpa mereka sedari.

Langkah Pencegahan

Berdasarkan kepada bahaya ancaman APT ini, semua pengguna perlu sentiasa berwaspada serta mengambil tahu mengenai langkah-langkah asas keselamatan komputer seperti memasang perisian *antivirus, firewall* dan perisian keselamatan seumpamanya supaya dapat menghalang APT ini di peringkat awal lagi. Setiap komputer peribadi dan telefon pintar juga disarankan agar melakukan proses kemas kini terbaru sistem operasi dan perisian keselamatan sekerap mungkin supaya ia sentiasa berada pada tahap terbaik untuk mempertahankan keselamatan data dan menutup ruang kelemahan dari terdedah kepada serangan dan ancaman siber terbaru yang berleluasa pada hari ini.

Tiada jalan mudah untuk mencegah serangan APT secara holistik. Walau bagaimanapun, semua pihak boleh menerapkan kaedah gabungan pelbagai jenis lapisan sistem pertahanan bagi keselamatan komputer, rangkaian mahupun pelayan. Selain saranan menggunakan *antivirus* dan *firewall*, antara langkah lain yang boleh diambil adalah penggunaan Teknologi Pencegahan Kehilangan Data *(Data Loss Prevention Technologies)*, menghadkan hak akses pada perkongsian fail dan penggunaan *USB drive*, mewujudkan polisi keselamatan komputer dan lain-lain. Sementara itu, sebagai lapisan tambahan untuk menghalang APT ini, pemasangan antispam dan tapisan web *(web filtering)* juga antara mekanisme yang baik untuk diguna pakai.

Kesimpulan

Sebagai kesimpulannya, segala bentuk kesedaran dalam usaha untuk mendedah dan memberi pengetahuan tentang keselamatan siber ini perlu dipergiatkan seiring dengan kemajuan yang dicapai dalam teknologi maklumat di negara kita hari ini. Pengetahuan mengenai amalan pertahanan dan keselamatan ini adalah perkara tunjang yang perlu diambil berat oleh semua pihak. Dengan meningkatnya jumlah penggunaan *e-mel*, akses laman sosial, perkongsian fail atas talian dan lain-lain lagi sebagai medium komunikasi dan perantaraan, adalah menjadi satu kemestian bagi setiap individu untuk sekurang-kurangnya memahami secara asas tentang ancaman dan langkah pencegahan yang perlu di ambil.

Langkah pencegahan dan pertahanan yang perlu diambil mungkin kelihatan remeh dan merumitkan, namun ia sangat membantu dan dapat menyukarkan penjenayah siber dalam melakukan aktiviti jahat serta tidak bertanggungjawab pada peringkat awalnya. Perkara yang perlu difahami ialah tiada jalan mudah dan singkat dalam membendung keseluruhan ancaman serangan APT ini. Samada terpaksa atau dipaksa, adalah perlu bagi semua pihak menitik-beratkan soal keselamatan komputer dan siber sebagai langkah persediaan awal untuk mengelakkan perkara tidak diingini yang mungkin atau bakal berlaku pada bila-bila masa. Oleh itu, adalah sangat disyorkan sebagai antara kaedah yang terbaik dalam menghalang APT ini dari terus merebak ialah dengan menggabungkan antara penggunaan perisian keselamatan, pengetahuan tentang ancaman, pendedahan terhadap taktik dan teknik serangan, dan polisi keselamatan komputer dan siber di dalam perlaksanaan bagi sesebuah organisasi ataupun untuk penggunaan individu sahaja. ■

Rujukan:

1. *Fortinet. (2013). Threats on the Horizon - The Rise of the Advanced Persistent Threat. Solution Brief. Retrieved from http://www.fortinet.com/sites/default/files/solutionbrief/threats-on-the-horizon-rise-of-advanced-persistent-threats.pdf*
2. *Global Research & Analysis Team (GReAT), (2012). Gauss: Nation-state cyber-surveillance meets banking Trojan. Retrieved from http://www.securelist.com/en/blog/208193767/*
3. *Gostev, A. (2012). 'Gadget' in the middle: Flame malware spreading vector identified. Retrieved from http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified*
4. *Kaspersky. (2014). Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyber-espionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers. Retrieved from http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers*
5. *Oltsik, J. (2013). Addressing APTs and Modern Malware with Security Intelligence. ESG Brief. Retrieved from http://www.webroot.com/shared/pdf/ESG-Brief-Webroot-Sept-2013.pdf*
6. *Trendmicro. (2013). How Do Threat Actors Move Deeper Into Your Network?. Retrieved from http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf*

Antivirus

Kini, terdapat pemahaman yang biasa dan meluas di kalangan pengguna-pengguna komputer tentang jenis kemudaratan yang virus komputer boleh lakukan dan bagaimana ia merebak.

By | Muhammad Arman, Mohd. Fadzlan

Pengenalan

Antivirus ialah perisian perlindung dan pertahanan komputer terhadap perisian yang berniat jahat. Perisian yang berniat jahat atau perisian perosak adalah termasuk *Virus, Trojans, Keyloggers, Hijacker, Dialers , Worm* dan kod-kod yang berupaya mencuri kandungan data dari komputer anda. Untuk menjadikan Antivirus sebagai satu pertahanan komputer yang berkesan, perisian antivirus perlu sentiasa berfungsi pada sepanjang masa, dan harus dikemaskini kerapkali untuk mengenal pasti versi perisian terbaru yang berniat jahat.

Terdapat beberapa perisian Antivirus yang diberikan secara percuma kepada pengguna. Antaranya ialah AVG (www.avg.com), Avast (www.avast.com) dan Avira (www.avira.com). Walau bagaimanapun, perisian percuma ini adalah tidak digalakkan untuk digunapakai oleh pengguna yang menggunakan komputer mereka di pejabat (pengguna komersil). Ini adalah kerana perisian Antivirus percuma lebih disasarkan kepada pengguna yang menggunakan komputer mereka di rumah dan mempunyai rangkaian jaringan berskala kecil.

Antara perisian Antivirus yang ada di pasaran

Apakah sebabnya pengguna di pejabat tidak digalakkan untuk menggunakan perisian Antivirus yang percuma? Salah satu sebab utama ialah kerana pengguna komersil banyak menggunakan aplikasi seperti *Intranet*, perkongsian direktori, perkongsian fail, penggunaan pemacu USB dan lain-lain. Melalui perkongsian ini, Virus amat mudah menjangkiti komputer di dalam rangkaian dan penyebarannya kadangkala tidak dapat ditahan oleh perisian Antivirus yang percuma. Keupayaan perisian Antivirus percuma juga tidak merangkumi semua aspek keselamatan siber.

Windows Defender

Apa pula Windows Defender?

Windows Defender adalah perisian dari Microsoft dan dikenali sebagai *Microsoft AntiSpyware* pada masa dahulu. Ia dibangunkan oleh *GIANT Company Software Inc.* dan telah diambilalih oleh Microsoft pada 16 Disember 2004. Versi percubaan perisian Microsoft AntiSpyware ini telah dikeluarkan pada 6 January 2005. Pada masa tersebut, pengguna yang menggunakan sistem pengoperasian Windows XP dan keatas sahaja yang boleh memuat turun dan menggunakannya. Perisian ini membantu pengguna komputer untuk memantau setiap fail yang ada di dalam komputer mereka sama ada berisiko dijangkiti virus ataupun tidak. Sehingga kini, Windows Defender masih lagi diguna pakai dan ianya telah ditukar nama kepada Microsoft Security Essentials.

Pentingnya Keperluan Untuk Sentiasa Mengemaskinikan Perisian Antivirus Anda

Antara persoalan yang sering timbul

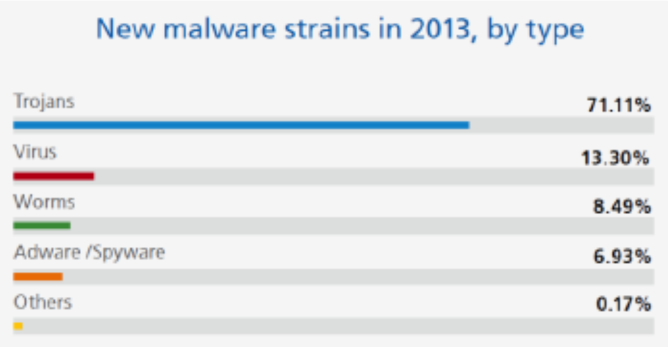
ialah mengapa perlunya perisian Antivirus dikemaskini selalu? Bagi sebilangan pengguna komputer, mereka berasa tidak selesa jika perisian Antivirus mengeluarkan arahan untuk dikemaskini secara kerap. Sebagai contoh jika arahan itu keluar setiap tiga hari atau dua hari sekali. Terdapat juga perisian Antivirus yang menyediakan servis kemaskini hampir setiap hari. Ianya tentu sangat mengjengkelkan bukan?

Untuk menjawab persoalan ini, kita harus memahami bagaimana Antivirus berfungsi. Sebenarnya Antivirus dicipta untuk mengesan sebarang jenis malware (sebarang program yang berniat jahat) berdasarkan *signature* (tandatangan) malware tersebut. Setiap malware mempunyai kod yang unik dan mempunyai *signature* yang tersendiri. Untuk memudahkan kefahaman, ianya boleh diumpamakan seperti kereta yang mempunyai nombor plat, enjin, chasis dan sebagainya. Sebelum ianya digunakan di jalan raya, nombor-nombor tersebut akan direkodkan oleh pihak yang berwajib untuk tujuan mengenalpasti dan memudahkan pencarian. Sekiranya kereta tersebut digunakan untuk tujuan membuat jenayah, maka kereta itu akan disenarai hitamkan dan nombor-nombor tadi akan diedarkan untuk dikenalpasti dan memudahkan pencarian.

Samalah juga halnya dengan Antivirus. Pengeluar-pengeluar Antivirus mempunyai makmal mereka yang tersendiri untuk mengesan dan menganalisa malware yang merebak di dunia maya. Apabila malware tersebut dikesan, *signature* itu akan disimpan di pangkalan data. Selepas itu, perisian Antivirus akan memuat turun *signature* malware yang baru dijumpai dari pangkalan data tersebut. Proses inilah yang berlaku ketika kita mengemaskini perisian Antivirus bersama dengan langkah-langkah pencegahan dan juga bagaimana untuk menghapuskan malware tersebut.

Jika *signature* sesuatu malware di kesan oleh Antivirus, fail yang dijangkiti itu akan terus dikuarantinkan dan akan ada notifikasi untuk memberitahu pengguna komputer bahawa komputer mereka telah dijangkiti virus atau malware.

Statistik di bawah menunjukkan peratusan jenis-jenis malware yang dikesan sepanjang tahun 2013.



Sumber: http://press.pandasecurity.com/

Tugas Antivirus seterusnya ialah mengesan dan menyekat sebarang program komputer yang sudah disenarai hitam sebagai merbahaya. Ia boleh diumpamakan seperti pihak polis yang melakukan sekatan jalan raya dan menahan kereta-kereta yang telah disenaraihitam.

Apa akan terjadi jika anda malas dan mengabaikan proses kemaskini perisian Antivirus? Risiko untuk komputer anda dijangkiti malware adalah lebih tinggi. Menurut statistik yang dikeluarkan oleh Kaspersky Lab pada tahun 2012, mereka telah berjaya mengesan lebih 200,000 malware baru setiap hari.

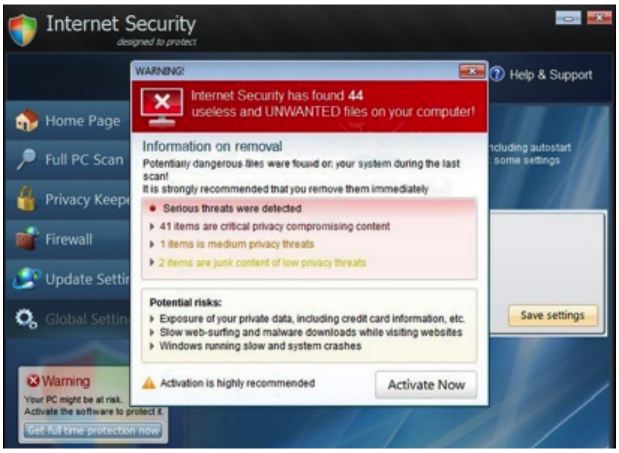
Perisian Antivirus Palsu

Apakah pula perisian Antivirus palsu?

Perisian Antivirus palsu adalah dikenali juga sebagai Scam Antivirus. Bagaimana ia menjangkiti komputer anda? Scam Antivirus adalah perisian yang anda muat turun dari laman sesawang yang mempunyai iklan percuma. Pernahkah bila anda melawati laman sesawang, secara tiba-tiba ada popup yang mengatakan komputer anda dijangkiti virus dan anda dikehendaki memuat turun perisian yang bernilai ratusan ringgit tetapi diberikan secara percuma kerana anda adalah pengunjung bertuah. Selesai sahaja anda memuat turun dan memasangnya, komputer anda secara mayanya adalah hak milik individu lain. Ini kerana pihak yang tidak bertanggungjawab itu telah memasang perisian untuk mengawal komputer anda dari jarak jauh.

Identiti anda dan semua fail di dalam komputer anda boleh diakses dengan sewenang-wenangnya oleh pihak yang tidak bertanggungjawab. Lebih berisiko lagi jika anda menyimpan nama pengguna dan kata laluan di dalam komputer anda.Sudah pasti ianya dapat diketahui oleh pihak yang tidak bertanggungjawab itu.

Gambarajah berikut adalah contoh perisian Antivirus palsu.



Internet Security has found 44 useless and UNWANTED files on your computer!

Information on removal

Potentially dangerous files were found on your system during the last scan!
It is strongly recommended that you remove them immediately

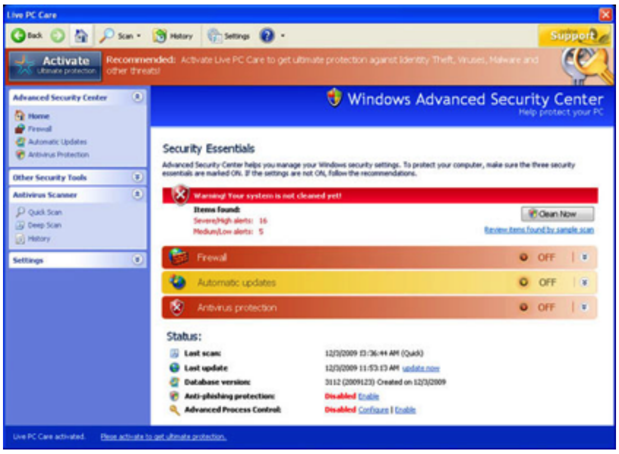
- Serious threats were detected
- 41 items are critical privacy compromising content
- 1 items is medium privacy threats
- 2 items are junk content of low privacy threats

Potential risks:

- Exposure of your private data, including credit card information, etc.
- Slow web-surfing and malware downloads while visiting websites
- Windows running slow and system crashes

Activation is highly recommended

Warning
Your PC might be at risk.
Activate the software to protect it.



Recommended: Activate Live PC Care to get ultimate protection against Identity Theft, Viruses, Malware and other threats!

Security Essentials

Advanced Security Center helps you manage your Windows security settings. To protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations.

Warning! Your system is not cleaned yet!

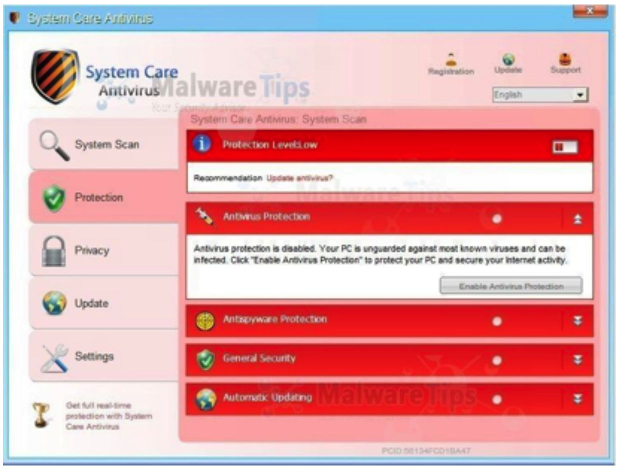
Items found:
Severe/High alerts: 16
Medium/Low alerts: 5

Firewall ● OFF
Automatic updates ● OFF
Antivirus protection ● OFF

Status:

Last scan:	12/3/2009 11:36:44 AM (Quick)
Last update	12/3/2009 11:53:13 AM update now
Database version:	3112 (2009123) Created on 12/3/2009
Anti-phishing protection:	Disabled Enable
Advanced Process Control:	Disabled Configure | Enable

Live PC Care activated. Plese activate to get ultimate protection.



System Care Antivirus: System Scan

Protection Level:Low

Recommendation Update antivirus?

Antivirus Protection

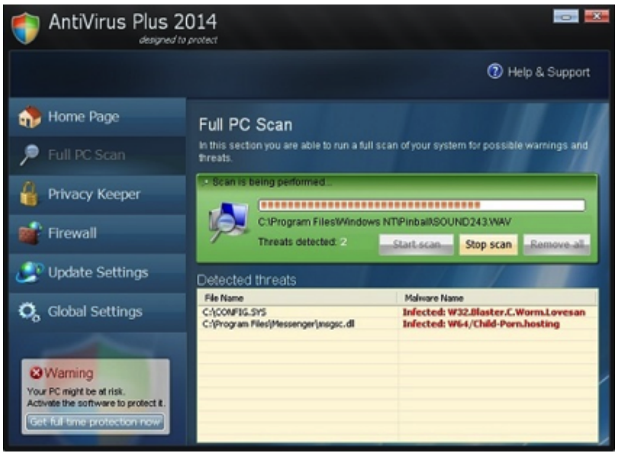
Antivirus protection is disabled. Your PC is unguarded against most known viruses and can be infected. Click "Enable Antivirus Protection" to protect your PC and secure your internet activity.

Antispyware Protection

General Security

Automatic Updating

Get full real-time protection with System Care Antivirus



Full PC Scan

In this section you are able to run a full scan of your system for possible warnings and threats.

Scan is being performed...

C:\Program Files\Windows NT\Pinball\SOUND243.WAV

Threats detected: 2

Detected threats

File Name	Malware Name
C:\CONFIG.SYS	Infected: W32.Blaster.C.Worm.Lovesan
C:\Program Files\Messenger\msgsc.dll	Infected: W64/Child-Porn.hosting

Warning
Your PC might be at risk.
Activate the software to protect it.

Penutup

Pengguna komputer amat digalakkan untuk memuat turun perisian Antivirus yang sah dan seterusnya menjadikan amalan mengemaskini signature Antivirus anda setiap hari atau sekerap mungkin sebagai amalan yang terbaik. Jangan sesekali terpedaya dengan perisian Antivirus percuma yang bukan dari laman sesawang pengeluar Antivirus yang asli. Jadilah pengguna yang bijak dengan cuba memahami fungsi dan cara kerja Antivirus dan jangan lagi merungut jika perisian Antivirus anda kerap mengeluarkan arahan untuk dikemaskini. Perkara sekecil ini haruslah dititikberatkan bagi menjamin keselamatan dan privasi anda sendiri. Anda juga boleh menggunakan fungsi kemaskini yang sedia ada secara otomatik untuk memastikan Antivirus pada komputer anda dikemaskini secara berkala.■

Rujukan

1. *http://en.wikipedia.org/wiki/Windows_Defender*
2. *http://en.wikipedia.org/wiki/GIANT_AntiSpyware*
3. *http://en.wikipedia.org/wiki/Microsoft_Security_Essentials*
4. *http://netforbeginners.about.com/od/a/g/antivirus.htm*
5. *https://sc1.checkpoint.com/documents/R76/CP_R76_AntiBotAntiVirus_AdminGuide/index.html*
6. *http://www.mdcomputing.com/introduction-to-antivirus-software-including-recommendations*

Mengenali Apa Itu Emel Phishing

By | Faiszatulnasro bt Mohd Maksom

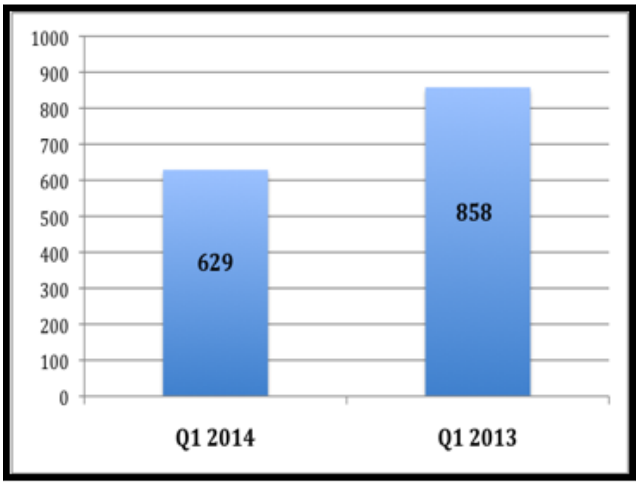
1.0 Pengenalan

Phishing walaupun secara umumnya dikategorikan sebagai jenayah penipuan siber, namun, masih terdapat pengguna Internet yang menjadi mangsanya. Mangsa phishing kebiasaannya tersedar yang mereka telah tertipu selepas kehilangan sejumlah wang akibat daripada tindakan mereka memasukkan katanama dan katalaluan di laman perbankan phishing. Kejadian seperti ini tidak sahaja berlaku kepada pengguna perbankan di atas talian, tetapi melibatkan juga pengguna laman sosial, akaun e-mel dan pelbagai akaun lain yang memerlukan pengguna memasukkan katanama dan katalaluan.

Justeru, sekiranya katalaluan dan katanama tersebut jatuh ke tangan penjenayah phishing, akaun terbabit dan maklumat peribadi mangsa boleh disalahguna bagi tujuan yang tidak sepatutnya, sekaligus boleh mencalarkan reputasi pemilik akaun tersebut. Lantas, mangsa akan berhadapan dengan situasi kecurian identiti sama ada disedari ataupun tidak.

Aktiviti phishing kebiasaannya dilakukan melalui e-mel, laman sesawang, panggilan telefon dan sebagainya. Menurut pemerhatian, phishing yang menggunakan e-mel sebagai medium adalah yang paling banyak digunakan kerana isi kandungan yang ringkas dan boleh dihantar kepada sesiapa sahaja tanpa mengira demografi penerima e-mel tersebut.

Merujuk kepada statistik yang direkodkan oleh MyCERT dalam tempoh suku pertama tahun 2013, sebanyak 629 insiden phishing telah dilaporkan melalui Pusat Bantuan Cyber999. Jika dibandingkan dengan suku pertama pada tahun 2014 pula, sebanyak 858 insiden yang telah dilaporkan, iaitu peningkatan lebih daripada 36 peratus. Peningkatan tersebut tidak menunjukkan lebih banyak kes phishing yang berlaku pada tahun 2014, sebaliknya berkemungkinan pengguna Internet mengetahui apa yang perlu dilakukan sekiranya mereka berhadapan dengan e-mel atau laman phishing. Iaitu, melaporkan kepada badan atau pihak yang boleh mengambil tindakan ke atas e-mel dan laman phishing yang diterima.



***Graf 1**: Perbandingan laporan kes phishing pada suku pertama tahun 2013 dan 2014*

2.0 Analisis Data Phishing

Data seterusnya merupakan data phishing yang menghoskan laman phishing jenama bank tempatan. Hasil daripada analisis yang dilakukan kepada data Pusat Bantuan MyCERT, maklumat yang diperoleh dikelaskan seperti jadual di bawah mengikut bulan pada suku pertama tahun 2014. Maklumat URL laman phishing yang dianalisis bertujuan mendapatkan maklumat domain, IP dan jenis jenama yang unik.

	Januari	Februari	Mac
Domain Unik	27	47	53
IP Unik	28	45	47
Jenama Unik	7	8	4

Jadual 1*: Data phishing*

Keseluruhan URL laman phishing yang menghoskan jenama bank tempatan yang telah dilaporkan adalah sebanyak 212. Domain unik yang tertinggi yang dilaporkan adalah pada bulan Mac iaitu sebanyak 53. Jumlah tersebut adalah yang tertinggi yang mana berkemungkinan domain yang telah dikompromi untuk menghoskan laman phishing telah dibaiki dan diperkukuhkan, menyebabkan pelaku jenayah phishing beralih mencari domain yang mempunyai keselamatan aplikasi yang ampuh. Statistik ini juga menunjukkan jumlah tertinggi bagi IP unik yang menghoskan laman phishing adalah pada bulan Mac, iaitu sebanyak 47 IP dan ianya selari dengan peningkatan domain unik yang dilaporkan.

3.0 Teknik Phishing

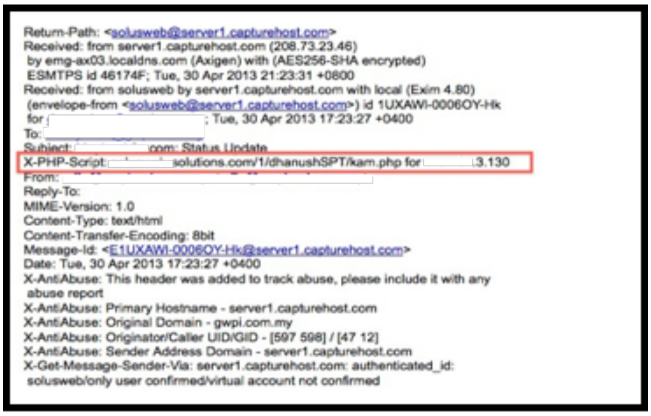
Penjenayah phishing sentiasa menggunakan kepelbagaian teknik untuk memerangkap pengguna Internet sehingga mereka menjadi mangsa penipuan phishing. Secara teknikalnya, penjenayah phishing ini menggunakan kaedah pengkodan untuk mengeksploit kelemahan pada aplikasi sesuatu sistem, terutamanya dari segi keselamatan. Kebiasaannya, kod akan diletakkan pada pelayan web yang mempunyai kerentanan. Kaedah ini bertujuan mengelakkan penjenayah phishing daripada dikesan.

3.1 PHPMAILER

Kepala e-mel mempunyai pelbagai maklumat berkaitan dengan alamat e-mel penerima dan penghantar, tarikh dan masa, subjek dan sebagainya. Maklumat-maklumat tersebut direkod oleh pelayan mel apabila e-mel tersebut dihantar dari satu pelayan ke pelayan yang lain sehingga sampai kepada penerima e-mel tersebut. Kepala e-mel dianalisis untuk mengesan daripada mana e-mel tersebut dihantar, rekod laluan pelayan ketika penghantaran e-mel berkenaan dan memastikan sama ada e-mel tersebut adalah e-mel penyamaran ataupun tidak.

PHPMailer ialah pengkodan untuk menghantar e-mail dengan lebih mudah dan menggunakan pengkodan PHP di pelayan web, lalu membenarkan penghantaran e-mel melalui laman web. Penggunaan PHPMailer lebih mudah untuk menghantar e-mel, antaranya boleh memasukkan lebih daripada satu penerima e-mel, penggunaan CC dan BCC; dan menyertakan lampiran. Penggunaan fungsi-fungsi tersebut adalah lebih fleksi iaitu boleh diubahsuai mengikut kehendak si penghantar e-mel.

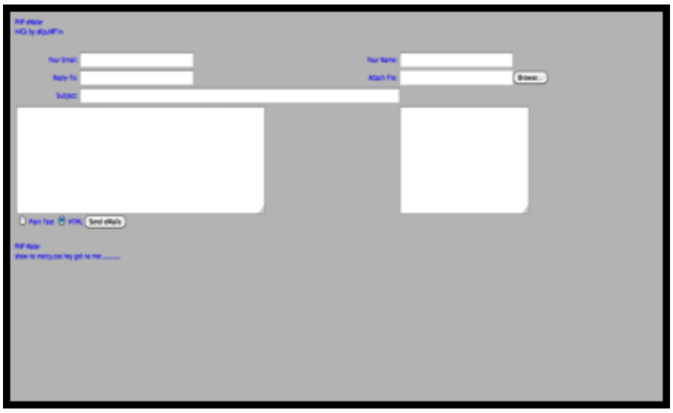
Dalam contoh kepala e-mel yang diperolehi, X-PHP-Script merekodkan e-mel yang dihantar menggunakan PHPMailer.



```
Return-Path: <solusweb@server1.capturehost.com>
Received: from server1.capturehost.com (208.73.23.46)
 by emg-ax03.localdns.com (Axigen) with (AES256-SHA encrypted)
 ESMTPS id 46174F; Tue, 30 Apr 2013 21:23:31 +0800
Received: from solusweb by server1.capturehost.com with local (Exim 4.80)
 (envelope-from <solusweb@server1.capturehost.com>) id 1UXAWI-0006OY-Hk
 for [redacted]; Tue, 30 Apr 2013 17:23:27 +0400
To: [redacted]
Subject: [redacted]com: Status Update
X-PHP-Script: [redacted]solutions.com/1/dhanushSPT/kam.php for [redacted].3.130
From: [redacted]
Reply-To:
MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
Message-Id: <E1UXAWI-0006OY-Hk@server1.capturehost.com>
Date: Tue, 30 Apr 2013 17:23:27 +0400
X-AntiAbuse: This header was added to track abuse, please include it with any
 abuse report
X-AntiAbuse: Primary Hostname - server1.capturehost.com
X-AntiAbuse: Original Domain - gwpi.com.my
X-AntiAbuse: Originator/Caller UID/GID - [597 598] / [47 12]
X-AntiAbuse: Sender Address Domain - server1.capturehost.com
X-Get-Message-Sender-Via: server1.capturehost.com: authenticated_id:
 solusweb/only user confirmed/virtual account not confirmed
```

Rajah 1*: Contoh kepala e-mel*

Sekiranya pautan di atas dibuka menggunakan pelayar sesawang, antara mukanya akan kelihatan seperti gambar rajah di bawah. Laman sesawang tersebut menunjukkan ianya telah dikompromi dan PHPMailer digunakan. Laman sesawang tersebut berfungsi sebagai satu proksi mel menggunakan skrip sesawang yang dieksploitasi untuk menghantar e-mel phishing mahupun e-mel spam.



***Rajah 2**: Antara muka PHPMailer*

3.2 Bouncer List

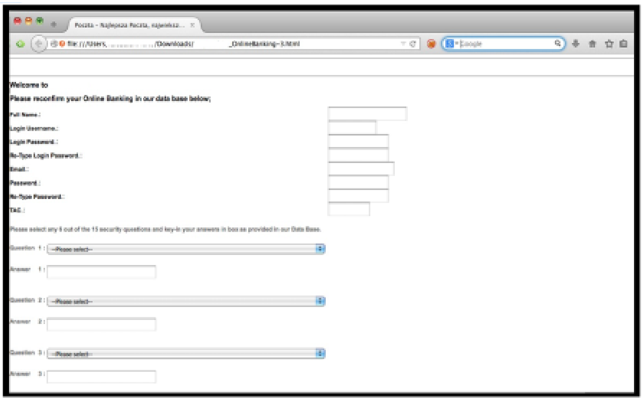
'Bouncer list' phishing merupakan teknik yang digunakan untuk menyasarkan phishing pada mangsa yang ditentukan, iaitu dengan membuat satu senarai ID. Mangsa yang menerima e-mel phishing akan cuba untuk mengakses ke laman phishing tersebut, IDnya akan disahkan terlebih dahulu sama ada ianya termasuk di dalam senarai sasaran ataupun tidak. Sekiranya ID mangsa tersenarai, mangsa akan dapat melihat laman phishing tersebut melalui pelayar sesawang. Jika mangsa memasukkan maklumat peribadi perbankan ke laman phishing tersebut, maklumat-maklumat peribadi tersebut akan dihantar kepada penjenayah phishing. Sebaliknya yang terjadi sekiranya ID mangsa tidak termasuk di dalam senarai 'bouncer'. Sekiranya mangsa tersebut cuba membuka laman sesawang phishing, pelayar sesawang mangsa akan dialihkan kepada laman '404 Page not found' atau '403 Forbidden' secara automatik.

4.0 Jenis Isi Kandungan E-mel Phising

Penyebaran jenayah phishing melalui e-mel adalah antara cara termudah bagi memerangkap mangsa. E-mel phishing kebanyakannya menggunakan teknik penyebaran e-mel *'blast'*, selain menghantar e-mel phishing kepada pengguna yang disasarkan. Isi kandungan e-mel phishing hampir kesemuanya mempunyai mesej yang berunsurkan amaran kepada pemilik akaun dan menjadikan ianya sebagai platform yang menghalakan penerima e-mel untuk melayari laman phishing. Seterusnya, ia akan mendorong mangsa memasukkan katanama dan katalaluan di laman sesawang yang kelihatan seolah-olah laman sesawang yang sah.

4.1 E-Mel Dengan Lampiran HTML

E-mel phishing yang dihantar memberi perintah kepada penerima e-mel supaya memuat turun lampiran yang disertakan. Apabila penerima e-mel membuka lampiran tersebut yang berbentuk borang, beberapa butiran peribadi yang berkaitan dengan maklumat perbankan perlu diisi. Setelah selesai mengisi borang dan bagi melengkapkan proses tersebut, butang 'submit' ditekan lalu tanpa disedari mangsa, maklumat-maklumat peribadi tersebut dihantar kepada penjenayah phishing. Teknik ini menggunakan kaedah POST yang menghantar maklumat-maklumat peribadi tersebut ke pelayan sesawang yang telah diaturkan bagi tujuan penyimpanan dan pemprosesan data. Sementara maklumat tersebut dihantar ke pelayan, mangsa akan mengalami keadaan di mana pelayar sesawang menjadi skrin putih dalam tempoh satu ke dua saat, lalu mangsa dialihkan ke laman perbankan yang sah secara automatik. Situasi ini membuatkan mangsa berfikir bahawa keseluruhan proses tersebut adalah transaksi yang sah. Namun, ianya adalah sebaliknya.


Welcome to

Please reconfirm your Online Banking in our data base below;

Full Name.:

Login Username.:

Login Password.:

Re-Type Login Password.:

Email.:

Password.:

Re-Type Password.:

TAC.:

Please select any 6 out of the 15 security questions and key-in your answers in box as provided in our Data Base.

Question 1 : --Please select--

Answer 1 :

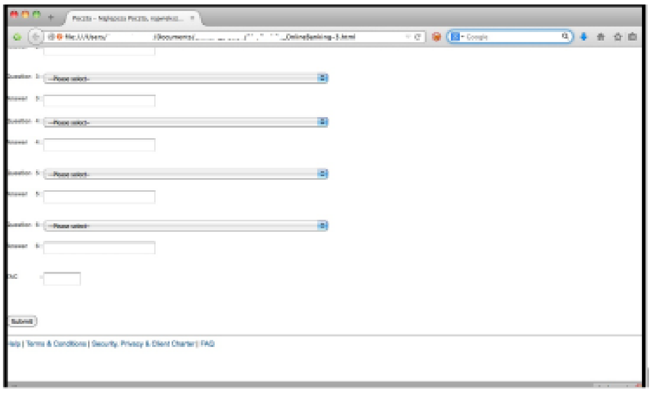
Question 2 : --Please select--

Answer 2 :

Question 3 : --Please select--

Answer 3 :

Rajah 1: *E-mel phishing dengan lampiran HTML (bahagian atas)*


Question 3: --Please select--

Answer 3:

Question 4: --Please select--

Answer 4:

Question 5: --Please select--

Answer 5:

Question 6: --Please select--

Answer 6:

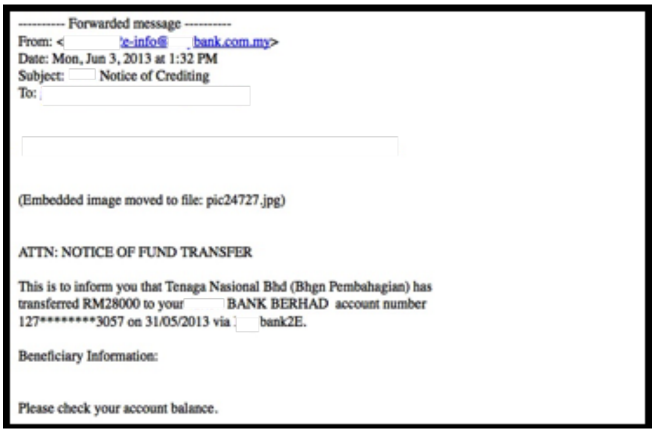
TAC :

Submit
Help | Terms & Conditions | Security, Privacy & Client Charter | FAQ

Rajah 2: *E-mel phishing dengan lampiran HTML (bahagian bawah)*

4.2 E-Mel Notifikasi Pemindahan Wang

Kebiasaannya jika ada pemindahan sejumlah wang melalui atas talian ke dalam akaun, e-mel notifikasi akan dihantar kepada pemilik akaun sebagai makluman. Kaedah ini dieksploitasi dengan menggunakan teknik kejuruteraan sosial agar penerima e-mel bertindak balas dengan maklumat yang diterima lalu mengklik pautan yang ada di dalam e-mel phishing tersebut.


---------- Forwarded message ----------
From: < e-info@ bank.com.my>
Date: Mon, Jun 3, 2013 at 1:32 PM
Subject: Notice of Crediting
To:

(Embedded image moved to file: pic24727.jpg)

ATTN: NOTICE OF FUND TRANSFER

This is to inform you that Tenaga Nasional Bhd (Bhgn Pembahagian) has transferred RM28000 to your BANK BERHAD account number 127********3057 on 31/05/2013 via bank2E.

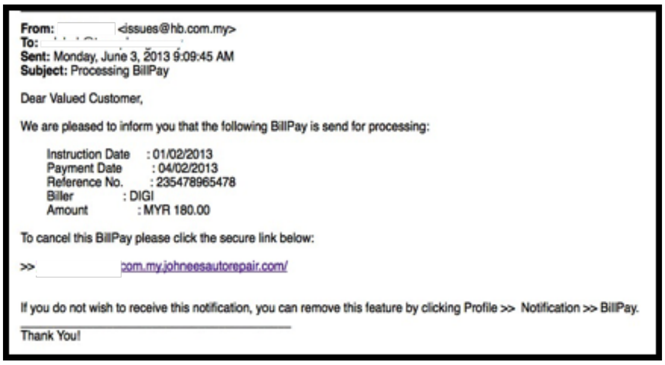
Beneficiary Information:

Please check your account balance.

Rajah 2: *E-mel notifikasi pemindahan wang*

4.3 E-Mel Notifikasi Pembayaran Bil

Reaksi manusia terhadap kewangan peribadi mereka adalah perkara yang sering diberi keutamaan. Sekiranya e-mel notifikasi berkaitan akaun peribadi yang menunjukkan seolah-olah ia telah digunakan oleh pihak lain bagi membuat transaksi yang tidak mendapat pengesahan atau pengetahuan pemilik akaun, sememangnya akan menimbulkan kebimbangan terhadap pemilik akaun tersebut. Kejadian seperti ini boleh berlaku dengan pantas di mana penerima e-mel akan mengklik pautan yang ada di dalam e-mel phishing bagi menyemak transaksi yang berlaku.



From: [redacted] <issues@hb.com.my>
To: [redacted]
Sent: Monday, June 3, 2013 9:09:45 AM
Subject: Processing BillPay

Dear Valued Customer,

We are pleased to inform you that the following BillPay is send for processing:

Instruction Date : 01/02/2013
Payment Date : 04/02/2013
Reference No. : 235478965478
Biller : DIGI
Amount : MYR 180.00

To cancel this BillPay please click the secure link below:

>> [redacted]com.my.johneesautorepair.com/

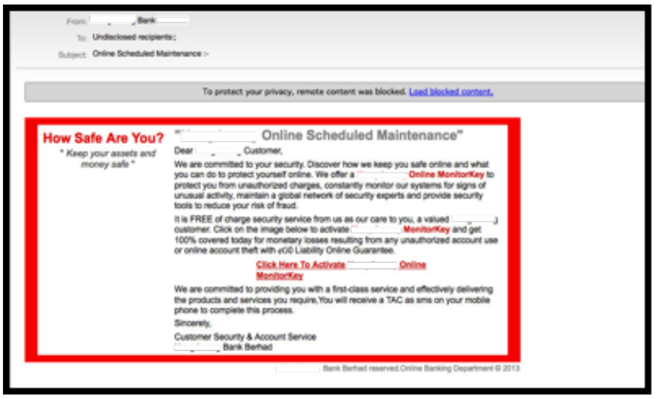
If you do not wish to receive this notification, you can remove this feature by clicking Profile >> Notification >> BillPay.

Thank You!

***Rajah 3**: E-mel notifikasi pembayaran bil*

4.5 E-Mel Penyelenggaraan di atas Talian

E-mel yang kelihatan lebih formal membuatkan penerima e-mel beranggapan bahawa ianya adalah e-mel yang sah daripada pihak bank. Penggunaan perkataan seperti 'free', 'security', 'safe', 'care' dan sebagainya secara psikologi memberikan jaminan keselamatan kepada pemilik akaun. Isi kandungan di dalam e-mel direka untuk mendapat kepercayaan dan keyakinan daripada pemilik akaun bahawa apa yang diarahkan adalah dijamin oleh pihak bank itu sendiri.



From: [redacted] Bank [redacted]
To: Undisclosed recipients:;
Subject: Online Scheduled Maintenance :-

To protect your privacy, remote content was blocked. Load blocked content.

How Safe Are You?
" Keep your assets and money safe "

"[redacted] Online Scheduled Maintenance"

Dear [redacted] Customer,

We are committed to your security. Discover how we keep you safe online and what you can do to protect yourself online. We offer a [redacted] Online MonitorKey to protect you from unauthorized charges, constantly monitor our systems for signs of unusual activity, maintain a global network of security experts and provide security tools to reduce your risk of fraud.

It is FREE of charge security service from us as our care to you, a valued [redacted] customer. Click on the image below to activate [redacted] MonitorKey and get 100% covered today for monetary losses resulting from any unauthorized account use or online account theft with ¢0 Liability Online Guarantee.

Click Here To Activate [redacted] Online MonitorKey

We are committed to providing you with a first-class service and effectively delivering the products and services you require,You will receive a TAC as sms on your mobile phone to complete this process.

Sincerely,

Customer Security & Account Service
[redacted] Bank Berhad

[redacted] Bank Berhad reserved.Online Banking Department © 2013

***Rajah 4**: E-mel jadual penyelenggaraan di atas talian*

5.0 Kesimpulan

Dengan kemajuan teknologi yang ada pada hari ini, pelbagai bentuk e-mel mahupun kaedah phishing digunakan untuk memerangkap mangsa. Isi kandungan di dalam e-mel phishing sentiasa diubah mengikut keadaan semasa dan mangsa yang lalai secara tidak langsung akan menyerahkan maklumat peribadi mereka kepada penjenayah phishing.

Justeru, pelbagai kaedah juga telah dan boleh dilakukan untuk menghindarkan diri daripada menjadi mangsa kepada penipuan phishing. Langkah pencegahan sentiasa berkaitan dengan tahap kesedaran dan cara pengguna Internet berhadapan dengan penipuan phishing. Jika diperhatikan, pendedahan maklumat berkaitan phishing terhadap pengguna Internet yang kurang berpengetahuan dari segi keselamatan komputer adalah masih di tahap yang agak rendah. Ini adalah kerana, mangsa penipuan phishing kurang ataupun mungkin tiada langsung didedahkan kepada maklumat berkaitan. Dengan adanya program kesedaran yang dilakukan dari peringkat sekolah rendah ke peringkat korporat, sedikit sebanyak membantu meningkatkan kesedaran orang ramai berkenaan keselamatan komputer secara umumnya.■

6.0 Rujukan

i. Pusat Bantuan MyCERT

ii. http://news.netcraft.com/archives/2012/11/13/phishing-attacks-using-html-attachments.html

iii. https://support.google.com/mail/answer/29436?hl=en

iv. https://code.google.com/a/apache-extras.org/p/phpmailer/wiki/UsefulTutorial

v. http://en.wikipedia.org/wiki/Phpmailer

vi. https://blogs.rsa.com/laser-precision-phishing-are-you-on-the-bouncers-list-today/

Pendayaan Sistem Nama Domain (DNS)

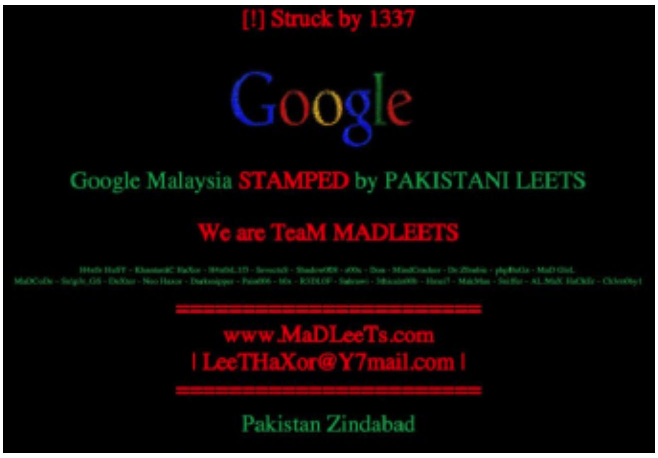
By | Nor Safwan Amirul

Pendahuluan

Manusia tidak mempunyai daya untuk menghafal sesempurna komputer kerana komputer mampu untuk mengingati beribu-ribu alamat nombor IP bagi mengecam atau mengenalpasti sesuatu laman *sesawang*. Tetapi sekiranya nombor alamat IP itu ditafsirkan kepada nama-nama yang mudah difahami, ia dapat memudahkan manusia untuk mengingatinya. Dan kerana itulah, DNS dicipta. DNS atau lebih dikenali sebagai Sistem Nama Domain merupakan satu analogi yang berfungsi sebagai buku telefon untuk *Internet* dengan menterjemahkan bahasa manusia kepada alamat IP. Sebagai contoh, nama domain www.contoh.com diterjemahkan kepada alamat 192.0.44.20. Dengan DNS, pengguna boleh mengakses laman sesawang dengan hanya mengingati nama laman sesawang atau alamat laman sesawang tanpa mengingati alamat IP laman sesawang tersebut. Namun disebabkan teknologi yang semakin tinggi dan pengetahuan yang makin meluas, telah memberi laluan kepada pihak yang tidak bertanggungjawab untuk menyalahgunakan kepakaran mereka dengan menggodam sesuatu laman sesawang bagi bertujuan memanipulasikan sesetengah informasi dengan hanya menggunakan DNS.

Pada 1 Julai 2013 yang lalu, samada disedari atau tidak, rakyat Malaysia di kejutkan dengan berita serangan penggodam yang menyerang laman-laman sesawang ternama di Malaysia. Antara laman sesawang yang terlibat adalah Google Malaysia , Microsoft Malaysia, Bing Malaysia, YouTube Malaysia, Dell Malaysia, Skype Malaysia, Kaspersky Malaysia dan lain-lain. Jika diperhatikan, laman sesawang yang terlibat bukanlah sebarangan dan majoritinya dimiliki oleh syarikat-syarikat yang besar dan berpengaruh.

Untuk pengetahuan anda, serangan yang digunakan oleh pihak yang tidak bertanggungjawab atau lebih dikenali sebagai penggodam (hackers) bagi menggodam laman-laman sesawang tersebut dikenali sebagai serangan pendayaan DNS.



[!] Struck by 1337

Google Malaysia STAMPED by PAKISTANI LEETS

We are TeaM MADLEETS

[illegible]

www.MaDLeeTs.com
| LeeTHaXor@Y7mail.com |

Pakistan Zindabad

Beberapa serangan dan isu keselamatan yang terjadi kepada Pelayan DNS adalah:

Serangan Protokol DNS

Serangan protokol DNS berlaku disebabkan oleh kelemahan pada protokolnya sendiri. Terdapat tiga perkara yang diperlukan untuk serangan protokol iaitu:

Peracunan Cache DNS (DNS Cache Poisoning)

Peracunan *cache* DNS ialah sejenis serangan penggodaman komputer, di mana data diberikan kepada pangkalan data cache bagi nama pelayan DNS yang mengakibatkan nama pelayan tersebut memberikan alamat IP yang salah dan terus mengalihkan trafik ke komputer lain (biasanya komputer si penggodam). Penggodam tersebut akan cuba menggantikan rekod alamat domain yang palsu ke dalam pelayan DNS. Sekiranya Pelayan DNS telah diubah dengan rekod yang palsu, maka terhasillah rekod cache yang telah diracuni. Setiap permintaan oleh pengguna yang menggunakan pelayan DNS tersebut akan diarahkan ke alamat yang telah ditentukan oleh penggodam.

DNS Spoofing

DNS *spoofing* merupakan aktiviti yang merujuk kepada aktiviti menjawab permintaan dari pengguna yang sepatutnya dituju kepada pelayan yang lain. Aktiviti ini melibatkan komunikasi di antara pengguna kepada pelayan DNS, dan kemudian, dari pelayan DNS kepada pelayan DNS yang lain. Melalui proses ini, penggodam akan cuba meniru struktur paket yang diminta oleh pengguna dan mengawalnya.

Serangan ID DNS

Setiap interaksi seperti identiti (ID) permintaan dan jawapan yang digunakan oleh pelayan DNS adalah dengan menggunakan nombor. Penggodam perlu mengetahui ID yang diperlukan oleh pengguna untuk menjalankan DNS ID hacking. Dengan menggunakan kaedah DNS spoofing, penggodam akan menyerupai data yang dihantar kepada pengguna untuk mengubah haluan kepada pelayan yang dikehendaki oleh penggodam .

Serangan Pelayan DNS (BIND)

Limpahan *Buffer (Buffer Overflow)* pada kod TSIG (transaksi tandatangan) berlaku pada BIND versi 8 semasa berlakunya proses TSIG, BIND (Berkeley Nama Domain Internet) akan memantau setiap proses TSIG yang memiliki kunci yang salah dan terus mengeluarkan kod yang menyatakan terdapat kesalahan atau masalah pada kod tersebut. Proses ini dipanggil *error handling* dimana ianya berlainan dengan proses yang biasa di gunakan. Setiap proses yang tidak sah akan memanggil semula fungsi yang memerlukan beberapa saiz permintaan buffer. Proses ini juga akan menyebabkan limpahan proses dimana ia akan menggantikan memori buffer yang dimiliki oleh andaian yang tidak sah kepada yang sah. Penggodam boleh menggunakan teknik limpahan *buffer* bagi mendapatkan hak untuk mengakses sistem tersebut.

Limpahan Buffer in nslookupComplain() berlaku pada BIND versi 4

Di dalam BIND , *vulnerable buffer* digunakan untuk mengeluarkan kesalahan mesej khas untuk *syslog* (catatan rekod aktiviti komputer). Penggodam akan menggunakan kelemahan yang ada pada BIND versi 4 dengan *DNS query* yang telah diselindungi dengan maklumat yang boleh mengancam BIND versi 4. Dengan memanipulasi data yang telah dieksploitasi, ia boleh mengganggu proses DNS dan menyebabkan berlakunya DDOS (Serangan penafian-perkhidmatan).

- SRV *bug (resource rekod)*
- NXT *bug (resource rekod)*

Pencegahan Serta Langkah Mengatasi Serangan Pendayaan DNS

Kebanyakan punca utama berlakunya pendayaan DNS adalah kerana kelemahan yang ada pada pelayan BIND itu sendiri. Oleh yang demikian di antara langkah pencegahan yang boleh di lakukan ialah dengan menggunakan versi BIND dan patch terbaru. Versi BIND memainkan peranan di dalam memberi peluang kepada penggodam untuk melakukan pendayaan DNS. Ini adalah kerana sebahagian besar daripada versi BIND yang lama mempunyai eksploitasi yang boleh digunakan oleh penggodam.

Sekiranya pengguna menggunakan versi BIND yang baru, ia dapat mengurangkan serangan kerana kelemahan yang ada pada versi BIND yang lama telah diperbaiki.
Berikut adalah beberapa langkah pencegahan untuk pendayaan DNS:

- Membataskan *zone-transfer*
  Bagi mengelakkan perkara ini berlaku, pengguna haruslah mengurangkan penggunaan pemindahan zon DNS kepada pelayan yang boleh dipercayai bagi mendapatkan maklumat atau *data zone* yang berkaitan. Selain itu, pengguna juga boleh menggunakan kaedah pengalihan identiti iaitu dengan menggunakan *Transaction SIGnature* (TSIG) di mana penggunaan kod TSIG yang sama digunakan oleh pelayan utama dan dengan ini *zone-transfer* tidak perlu lagi dilakukan oleh pelayan.

- Pengawalan *dynamic update*
  Sama seperti membataskan penggunaan *zone transfer,* pengguna juga perlu membataskan penggunaan *dynamic update* dengan hanya bergantung kepada pelayan-pelayan yang telah dipercayai.

- Pengawalan *query*
  Dengan pengawalan permintaan rekursif (proses berulang-ulang) pada pelayan DNS, ianya dapat mengurangkan ancaman DNS *spoofing/cache poisoning*. Permintaan rekursif dapat dikawal dengan memberi pilihan kepada pengguna untuk membenarkan rekursif.

```
Contoh:
options {
          ...
          allow-recursion
{192.168.3.0/24;};
          ...
};
```

- Menyembunyikan informasi versi BIND
  Pada asalnya , secara automatik konfigurasi yang ada pada BIND akan bertindak balas dengan memberi segala informasi berkaitan versinya kepada pengguna yang meminta identiti versi BIND tersebut. Informasi ini terletak di rekod .txt dibawah *chaosNET class.* Informasi ini selalunya digunakan oleh pentadbir sistem untuk melakukan kerja kerja penyenggaraan. Perlu diingati yang penggodam juga boleh mengambil kesempatan dengan menggunakan informasi versi BIND untuk mencari kelemahan yang ada pada versi BIND tersebut.

- Mengehadkan kawalan akses
  Dengan mengehadkan tindak balas oleh Pelayan DNS luar kepada pengguna IP nombor IP awam sahaja. Ia dapat mengelakkan Pelayan DNS luar daripada menerima permintaan dari pengguna nombor IP dalaman. Ini telah termaktub dalam RFC 1918. Berdasarkan Penguatkuasaan Nombor Teruntuk Internet (IANA) dibawah Akta RFC 1918, setiap nombor IP Internet telah dibahagikan kepada tiga bahagian .
  10.0.0.0 - 10.255.255.255 (10/8 prefix)
  172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  192.168.0.0 - 192.168.255.255 (192.168/16 prefix)8

Oleh kerana alamat nombor yang telah di bahagikan seperti diatas tidak di dedahkan di Internet , maka tindak balas daripada pelayan DNS luar dapat dihalang oleh *router Internet*, dengan ini kebarangkalian menerima serangan DDOS dapat dielakkan.

- Menutup laluan yang tidak diperlukan dan menganalisa lalu lintas data.
  Laluan yang tidak digunakan pada host yang nama-pelayan sebaiknya dimatikan. Laluan setiap data juga haruslah dianalisa dengan menapis segala laluan data yang meragukan. Laluan yang biasa digunakan seperti *port 53/tcp dan port 53/udp* boleh dibuka dan seharusnya dipantau. Salah satu langkah untuk menapis segala laluan adalah dengan menggunakan firewall.

- Mengambil tahu tentang isu-isu terkini tentang keselamatan BIND. Log sistem yang terdapat pada transaksi pelayan boleh dijadikan tempat rujukan untuk menganalisa segala laluan data transaksi pelayan. Selain itu, dengan mengikuti perkembangan isu-isu terkini tentang keselamatan DNS dan BIND dengan melanggan *mailing list* atau laman sesawang yang berkaitan dengan keselamatan BIND. Selain itu, ia dapat dijadikan bahan rujukan untuk mengetahui informasi dan kelemahan yang ada pada sistem pelayan.

- Penyalinan Data
  Penyalinan data amat penting untuk menghadapi perkara yang tidak diingini. Sekuat mana keselamatan yang digunakan , bukan bermakna kita dapat menepis 100 peratus daripada berlakunya serangan. Dengan itu, kita seharusnya melakukan penyalinan data bagi langkah berjaga-jaga.

Beberapa URL dan aplikasi yang boleh mengesan/menghalang pengguna daripada terkena serangan pendayaan DNS.

1. http://dnschanger.detect.my (by CyberSecurity Malaysia)
2. Hitman Pro
3. Kaspersky Labs TDSSKiller
4. McAfee Stinger
5. Malwarebytes
6. Microsoft Windows Defender Offline
7. Microsoft Safety Scanner
8. Norton Power Eraser

Kesimpulan

Keselamatan bukanlah bermaksud selamat dari segala ancaman tetapi ia merupakan satu langkah bagi mengurangkan atau menghindarkan diri dari segala ancaman yang bakal mendatang. Keselamatan boleh diandaikan seperti rangkaian rantai dimana kekuatan sesuatu keselamatan itu adalah bergantung kepada semua aspek yang bermula dari struktur kekuatan keselamatan itu sendiri sehinggalah ke penggunanya. Adalah diharapkan artikel ini dapat memberikan gambaran tentang betapa pentingnya isu keselamatan pelayan DNS dan memastikan perkhidmatan pelayan DNS sentiasa selamat dan kekal aktif di dalam jaringan. ■

Rujukan

- *http://www.thestar.com.my/Tech/Tech-News/2013/10/11/Google-Malaysia-page-redirect.aspx*
- *http://dawn.com/news/1048989/google-malaysia-hacked-by-pakistani-team*
- *http://www.theverge.com/2013/10/10/4825914/google-malaysia-taken-down-by-hackers*
- *http://www.cert.org/advisories/CA-2001-02.html*
- *http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf*
- *http://pl.duniasemu.org/network/bind_dns/bind_dns-4.html*

Training Programmes

CyberSecurity MALAYSIA

Professional Development Schedules in CyberSecurity Malaysia Calendar 2014

No.		Program Duration	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction														
1	Critical Infrastructure Protection	2 days		19-20					9-10					
2	Digital Forensics Essentials	3 days	20-22			1-3						8-10		
3	Malaysia Common Criteria (MyCC 1.0) - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day				2						21		
4	Introduction to ISO 27001 Information Security Management System	1 day	8		5		6		3		2		4	
5	Data Encryption for Beginners	1 day		12						4				
6	Cryptography for Beginners	1 day			12						2			
7	CSM Security Essential Training	2 days	28-29				28-29				10-11			22-23
8	Google-Fu Power Search Technique	2 days					20-21			19-20				
9	Wireless Security	2 days	9-10					19-20						8-9
10	Internet Banking Security	1 day						3				28		
11	Customize Training Package for groups and companies	1-5 days												
Intermediate														
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days				8-10						20-22		
2	Cryptography for Information Security Professional	3 days			25-27						9-10			
3	ISO 27001 Implementation	3 days		25-27		14-16				12-14		13-15		15-17
4	Incident Handling and Network Security Training (IHNS)	3 days				22-24			8-10				17-20	
5	Network Security Assessment Training	3 days					7-9					29-30		
6	Server and Desktop Security Assessment Training	2 days						4-5						3-4
7	Web Application Security Assessment Training	2 days						18				2		
8	Digital Forensics for First Responder	1 day				15-18						27-30		
9	Customize Training Package for groups and companies	4 days												
	(Intermdiate Courses Item 1-8)	1-5 days												
Specialization/Specific Domains														
1	Forensics on Internet Application	1 day						25					19	
2	Digital Forensics for Law Practioner	2 days					14-15				23-24			
3	Security Posture Compliance, Assessment and Penetration Testing	5 days			10-14						9-10		3-7	
4	ISMS Internal Auditor Course (ISO 27001)	3 days			18-19				30-31				26-27	
Professional Certification														
1	Business Continuity Management Professional Certification (BCLE2000)	5 days		24-28		21-25		16-20			22-26			1-5
2	ISO 27001 Lead Auditor (External Auditors)	5 days	20-24		3-7	7-11	19-23	30 - 4			22-26		3-7	

*Subject to change

Venue

CyberSecurity Malaysia, Training Centre, Level 4, Block C, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia. | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0844 (ISPD)

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

ISMS SIRIM CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

STANDARDS MALAYSIA ACCREDITED LABORATORY MS ISO/IEC 17025 TESTING SAMM NO. 456 (MyCEF LABORATORY)

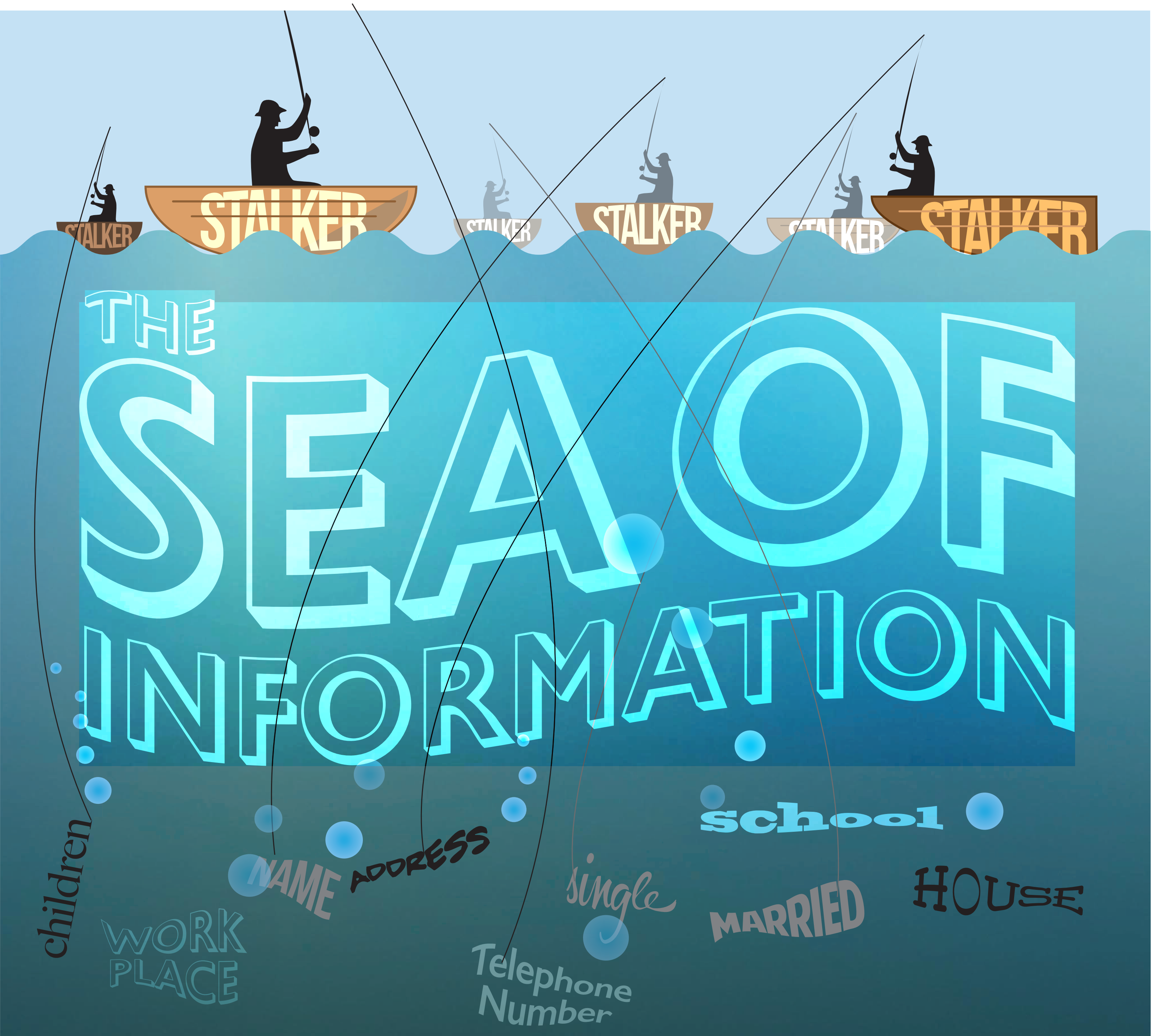
MSC MALAYSIA Status Company

CyberSecurity
MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

THE SEA OF INFORMATION



Information we put in on the Internet are out in the open sea.
Stalkers only need to phish them out.

Be smart. Be safe

logon to www. CyberSAFE . my to find out more   cybersafe.malaysia

CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan,
Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

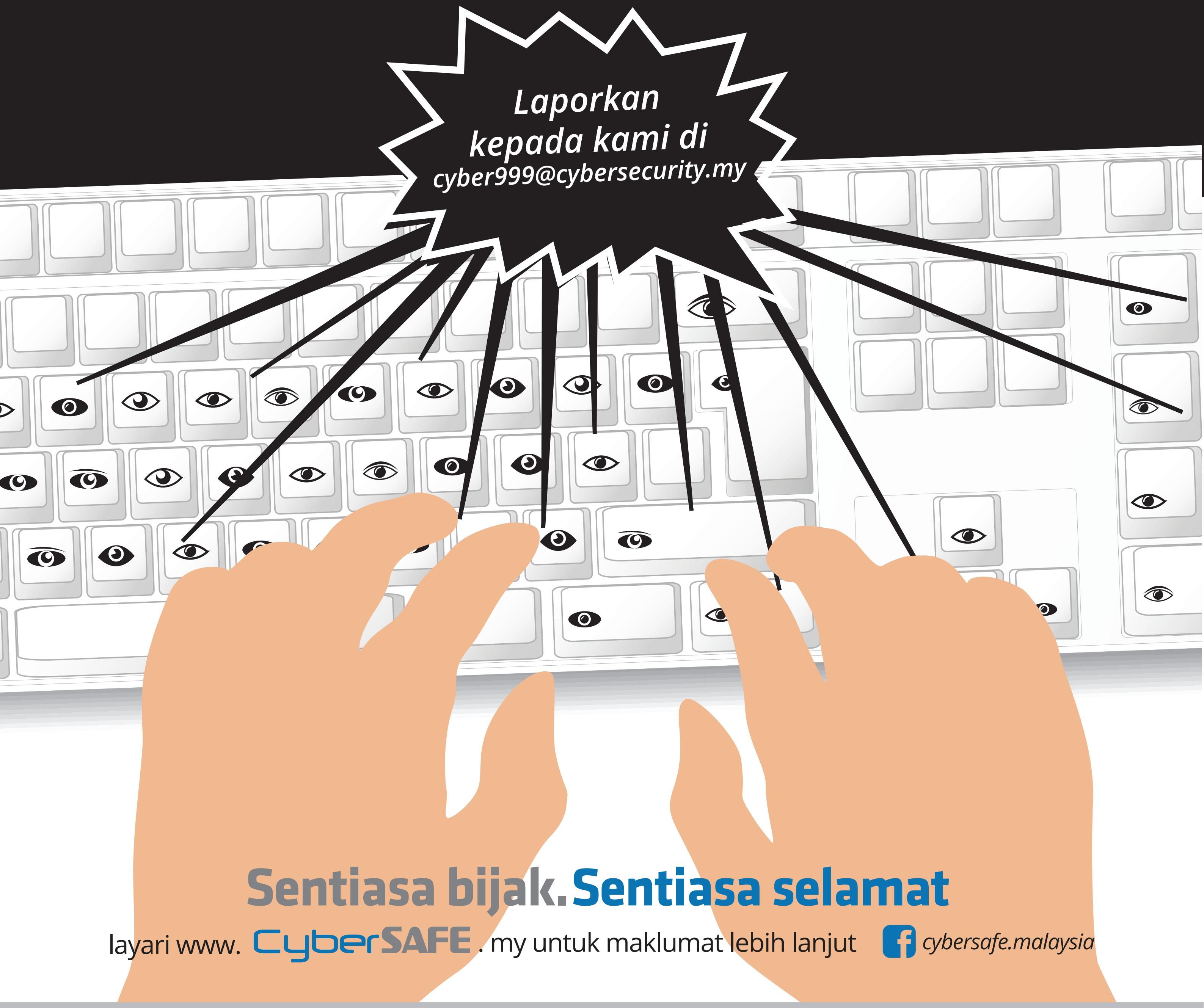
CyberSecurity MALAYSIA
Agensi di bawah MOSTI

Rakyat Didahulukan,
Pencapaian Diutamakan

MOSTI
Kementerian Sains,
Teknologi dan Inovasi

HENDAP SIBER:

Informasi anda sentiasa diperlukan dan
selalu diperhatikan **tanpa disedari**.



*Laporkan
kepada kami di
cyber999@cybersecurity.my*

Sentiasa bijak. Sentiasa selamat

layari www. CyberSAFE .my untuk maklumat lebih lanjut *cybersafe.malaysia*

Best Brand
Internet Security
2008 & 2009

ISMS SIRIM
UKAS INFORMATION SECURITY MANAGEMENT 074
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

STANDARDS MALAYSIA ACCREDITED LABORATORY
MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA
Status Company

Best Child Online
Protection Website

Pejabat Korporat:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan,
Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Talian Khidmat Pelanggan: 1300-88-2999 | www.cybersecurity.my

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

Private information on the Internet is public property

Be smart. Be safe

logon to www. CyberSAFE . my to find out more cybersafe.malaysia

Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan,
Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my