MALAYSIAN CYBER SECURITY AGENCY

e-Security

Volume 9 -(Q4/2006)

MOSTI

Contributors

MyCERT 4th Quarter Summary Report
Malaysian Cyber Security Agency

Forensics Investigations on SIM Card
By Razana Bt Md Salleh
Digital Forensics Analyst,
Malaysian Cyber Security Agency
zana@niser.org.my

Deployment Considerations: Comparing Converged and Dedicated Security Appliances
By CISCO

War Driving Analysis – Kuala Lumpur 2006
By Rozana Rusli
Head, Security Assurance,
Malaysian Cyber Security Agency
rozana@niser.org.my

Importance of Security Awareness
By Raj Kumar
Senior Training & Outreach Executive,
Malaysian Cyber Security Agency
raj@niser.org.my

Firewall & Malicious Attacks
By Abdirizak Omar Mahamoud
furso@streamyx.com

Regulating Cyber Café Operations
By Sivanathan Subramaniam
Digital Forensics Analyst,
Malaysian Cyber Security Agency
siva@niser.org.my

Combating Bots
By Adli Bin Abd Wahid
Senior Intrusion Analyst,
Malaysian Cyber Security Agency
adli@niser.org.my

Ethics in Information Security
By Yati Yassin & Zahri Yunos
Malaysian Cyber Security Centre
yati@niser.org.my
zahri@niser.org.my

What is Access Management?
By Anand Pon
Managing Director,
International Centre for Security Management
anandpon@gmail.com

Practical Strategies to Accelerate Business Applications
By Lim Pun Kok
Managing Director for Asean/ANZ
Blue Coat Systems

Business Continuity Planning for All
By Nazhalina Nazri
Security Management Analyst,
Malaysian Cyber Security Agency
nazhalina@niser.org.my

Mitigating On-Line Identity Theft
By Shaharudin Ismail & Zahri Yunos
Islamic University College of Malaysia
Malaysian Cyber Security Centre

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

- Bruce Schneier, Secret and Lies

Editor's Letter

vphilip@niser.org.my

Quarter 4 issue for the year ending 2006. Well, another end to a year and many more articles in this issue. First, I would like to thank all our contributors who have contributed to this issue. Some of the issues facing us today are highlighted in this issue such as botnets, malicious attacks, identity theft and business continuity planning.

As Internet Banking is growing is popularity and usage, we as users must also practice safe internet banking. Looking at that, the Malaysian Cyber Security Agency has produced 1-page quick guide to Safe Internet Banking which can be downloaded at **http://www.niser.org.my/resources/safe_online_banking.pdf.**

Recently concluded event was the APCERT AGM 2007 held at Sheraton Langkwai Beach Resort from the 7th – 10th February 2007. The event saw participants from the Asia Pacific regent and also invited guest from other regents attending, including Singapore, Australia, Thailand, Vietnam, Philippines, Cambodia, Indonesia, Pakistan, Tunisia, Netherlands, Korea, Japan and others. The Malaysian Computer Emergency Response Centre (MyCERT), Malaysian Cyber Security Agency was elected as Chair of APCERT for the new term. A proud moment for the Malaysian Cyber Security Agency in its vision to become the National Reference and Specialist Centre in Cyber Security.

The Malaysian Cyber Security Agency and (ISC)^2 will be launching another certification course this year, the Systems Security Certified Practitioner (SSCP). SSCP is aimed towards the technical community and like the CISSP; this certification has also obtained the ISO 17024.

Before I sign off, we would like to once again invite contributions to our newsletter and look out for our next INFOSEC.my Knowledge Sharing Session which will be held in April 2007. Do visit our website for regular updates.

Philip

Philip Victor
Editor

READER ENQUIRY

Training & Outreach
Malaysian Cyber Security Centre
(formerly known as NISER)
Ministry of Science, Technology and Innovation (MOSTI)
Email: training@niser.org.my

Table of Contents

MyCERT Quarterly Summary (Q) 2006
Original Issue Date: 17th Jan 2007

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during that quarter. This report highlights statistics of attacks or incidents reported to MyCERT, as well as other noteworthy incidents and new vulnerability information. MyCERT believes these statistics are only the tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order to enable us to assist those affected.

In addition, this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardenings.

Recent Activities

In this quarter, a total of 11008 incidents were received which is 96.96% increase compared to Q3. About 95% is contributed by spam reports. No major outbreak was observed this quarter but majority of incidents had slightly increased. However, we saw a tremendous increase in intrusion incidents mainly involving mass web defacements on virtual hosts running Cpanel applications. Other incidents that had increased are spam, harassment and denial of service. Other incidents showed slight decrease in this quarter.

	Q3 2006	Q4 2006	%
Intrusion	99	424	328.29
Denial of Service	2	4	100
Malicious Code	13	11	15.38
Hack Threat	20	14	30
Fraud	86	58	32.55
Harassment	13	25	92.31
Spam	5356	10472	95.52
Total	**5589**	**11008**	**96.96**

Mass Defacements of Websites Hosted on Virtual Hosting Server

As was in previous quarter, the fourth quarter of 2006 also saw increased number of mass defacements of websites hosted on virtual hosting servers. In this quarter we observed a host compromised resulting in about 203 websites defaced. Overall, there was increase in intrusion incidents with a total of 424 incidents compared to 99 incidents in previous quarter, more than three folds from previous quarter. Intrusions reported mainly involved web defacements of various domains belonging to our constituency and mass defacements of websites hosted on virtual hosting servers running Cpanel application. Most of these hosts are located at data centres by Internet service providers.

With the tremendous increase in intrusion, MyCERT would like to urge all system administrators and virtual host administrators to upgrade and patch systems, services and applications they are currently using as and when new security they are made available. In addition, it is also recommended to disable unnecessary or unneeded default services on the systems.

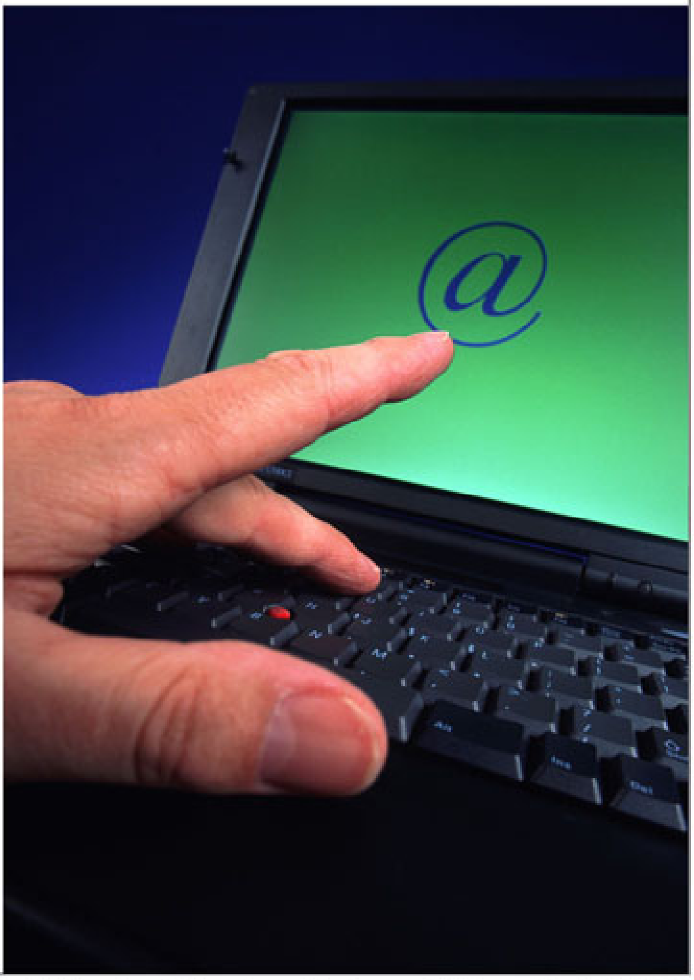
More detail steps in securing UNIX and Windows Servers are available at:

http://www.mycert.org.my/resource.html

Increase in Harassment Incidents

Number of incidents received on harassment increased to 25 compared to 13 incidents which represents 92.31%. Majority incidents involved email harrassment from disgruntled employees or former employees, expressing their dissatisfaction towards their employer. Most of the harassment cases were referred to the law enfrocement agencies.

Other types of harassments are sending of constant threatening or defamatory emails to victims with malicious intent.



Keylogger Trojan Activities

Malicious code incidents slightly decreased compared to previous quarter. A total of 11 incidents were reported compared to 13 in previous quarter, which represents a 15.38% decrease. In this quarter, we received two different reports from foreign organizations of keylogger Trojan called Goldun and Haxdoor. The trojan capture some details from end user computers which was sent and stored in a remote attacker's server.

The Haxdoor Trojan captures keystrokes from infected machines which includes usernames and passwords, and sends them to remote attacker's server.

The Goldrun Trojan specifically steals usernames, passwords and bank details from infected computers and sends the information to a remote malicious server.

Based on the report received, more then 50 online accounts such as usernames and passwords belonging to local customers were captured by the Trojan.

We advise users to safe-guard their PCs against Trojan, backdoor and worm infections. Users may refer to the below guidelines:

- Ensure computers are installed with anti-virus software and are frequently updated with the latest virus signatures. Users without anti-virus installed on their PCs may download an anti-virus from the following site:

  http://www.mycert.org.my/anti-virus.htm

- Ensure computers are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in computers.

- Enable personal/host-based firewalls on PCs.

Guidelines on safe Internet banking is available at:

http://www.niser.org.my/resources/safe_online_banking.pdf

Slight Decrease in Fraud Incidents

This quarter saw a slight drop in fraud incidents to 32.55%, which comprises of 58 reports compared to 86 reports in previous quarter. About 25.71% of fraud incidents reported were phishing incidents impersonating local financial institutions.

The respective ISPs, data centers and organizations have been alerted to remove the relevant websites and to investigate the affected machines and rectify them accordingly. In some cases, these hosts had been infected with bots and require thorough clean-up.

As was in previous quarter, MyCERT continues to receive reports from local users regarding Internet scams. These include the Nigerian Scam, Cheatings and Get Rich Scams. The mode of operations of the scams involves the use of spam to lure Internet users to visit specific websites and eventually request deposit of a certain amount of money to the fraudsters' accounts. Users are advised not to deposit or make payment to unknown third party's account.

User may refer to the following guide on safeguarding against fraudulent emails and phishing attempts:

http://www.mycert.org.my/other_resources/phishing.html

Other Activities

Spam

Spam incidents increased by one fold to a total of 10472 incidents in this quarter compared to 5356 in previous quarter. Spam has developed from a mere nuisance into an epidemic that threatens end users and organizations. There are no perfect techniques or tools to completely eradicate spams, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users' email clients. Users are also advised not to respond nor purchase products promoted via spams.

Denial of Service

During this quarter, four reports were received involving denial of service incidents compared to two in previous quarter. Reports on denial of service involved mailbombs and inaccessibility to certain sites due to traffic congestion. Main cause of the surge in traffic was identified to be due to unstable systems.

Hack Threat

Incidents involving hack threat decreased to about 30% in this quarter. A total of 14 reports were received on hack attempts for this quarter compared to 20 in the previous quarter. The threats involved unauthorized scanning of networks and systems.

MyCERT's findings for this quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21), HTTP (TCP/ 80), MS SQL (TCP/1433). Port scannings were actively done once a new bug or exploit is released publicly, using either automated or non -automated tools. Residue of worm traffics from infected hosts are still prevalent in the network.

Conclusion

Overall, the number of incidents reported to us had increased to about 96.96% compared to the previous quarter with incidents mainly contributed from spam incidents. Reports were the most for intrusion incidents. No crisis or outbreak was observed this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats.

We encourage users/organizations to report and seek assistance from MyCERT in the event of any security incidents.

Forensic Investigations on SIM CARD

Introduction

Mobile phone usage in the country has been increasing tremendously. According to MCMC, the penetration rate of mobile phone usage is 80.8% for the second quarter of 2006 as compared to 77.7% for the year 2005.

Almost everyone uses mobile phones, including criminals who use it to facilitate their law-breaking activities.

With vital information stored in mobile phones and SIM cards, it is important to perform forensic investigations on these storage devices that may contain evidences of the crime. It is also necessary to use correct investigation software or tools to extract evidence from SIM card.

Extracting Data from SIM

There are two ways of extracting data from SIM card. Firstly, by extracting data while the SIM is inserted in the phone. Secondly, the SIM must be removed from the phone and inserted in a reader for acquisition. However, it is better to extract data from mobile phone and SIM card separately. Why? Because by extracting data from mobile phone and SIM together at once, the tools usually communicates through mobile phone's operating system for data acquisition. This method may not be able to extract every data from SIM card. As an example, deleted text messages in SIM card may be recovered when the SIM is taken out from phone and read separately using a SIM card reader and appropriate tool.

Tools

There are many tools available in the market.
Listed below are some of them.

- **SIMCon (External SIM card support)**
- **.XRY (Internal and External SIM card support)**
- **MOBILedit! Forensic (Internal and External SIM card support)**
- **Oxygen Phone Manager (Internal SIM card support)**

What Is Stored in Your SIM card?

In mobile phone forensic investigation, data stored inside SIM card may help investigators find clues and evidence to solve criminal cases. Data that are crucial during investigations are:

- **IMSI**
- **MSISDN**
- **Location Area Code**
- **Last Number Dialed**
- **Phonebook**
- **SMS**

IMSI

IMSI or International Mobile Subscriber Identity is a 15 digit number to identify the SIM card and the subscriber within GSM network. It contains 3 digits Mobile Country Code (MCC), 2 digits Mobile Network Code (MNC) and 10 digits Mobile Subscriber Identity Number (MSIN). An example of IMSI number is 502130400796645; where 502 is for Malaysia (e.g. 525-Singapore. 13 is for TMTouch (e.g. 16-Digi, 12-Maxis), and the rest is the MSIN.

MSISDN

MSISDN or Mobile Subscriber ISDN is the telephone number of a GSM mobile phone. It contains unique 10 digit numbers that a caller uses to reach another mobile subscriber. You can have more than one MSISDN number associated, but by default you have three – voice, data and fax. Some SIM does not store MSISDN, thus making it harder for investigators to acquire the mobile phone number.

Location Area Code

Location Area Code is the number which refers to the current location of the SIM card. This code will remain in the SIM card even if the mobile phone is switched off, thus providing clues as in which area the criminal scene is. However, investigators may need help from the service provider to translate the code to get the exact location.

Last Number Dialed

Last number dialed is a list of numbers stored by SIM card when the subscriber makes calls to other subscribers. For a standard SIM card, 10 last number dialed are stored in the SIM card. This is indeed important information for investigators to trace the calls made by the suspected criminals. However, some mobile phones keep the last number dialed in the phone's memory instead of the SIM card, so investigators need to check both SIM and mobile phone for more accurate result.

Phonebook

Phonebook (name and contact number) is stored as "abbreviated dialing number" in SIM card. It stores up to 20 digits and 16 alphabet characters for each contact saved in SIM card. It may contain about 250 contact numbers in 2G SIM card or even up to 500 numbers in 3G USIM card. Phonebook may reside in phone's memory as well, so both SIM and phone's memory need to be checked for contact list.

SMS

SMS or Short Message Service is the text messages stored either in the SIM or in phone's memory. SMS contains among others are information such as the status (either received-read, received-to be read, originating message-sent, originating message-to be sent), the sender's number, the service centre time stamp and the text message itself. SIM card may store up to 40 or more SMS, depending on the SIM card storage size. The memory allocation for SMS on SIM card is fixed, so if the memory is not overwritten, investigator may be able to extract deleted SMS using software such as SIMCon.

Conclusion

SIM card holds important information that helps investigators find evidence and clues to solve criminal cases. With appropriate tools, data from SIM card can be extracted and analyzed to solve crimes. All the information discussed above can be placed and joined together to trail back and help investigators to simulate the crime scenes during investigations. What is important is to use various tools to extract as much data for evidence, because as always, crime leaves a trail.

Reference

[1] MCMC website:
http://www.cmc.gov.my/facts_figures/stats/index.asp

[2] SIMCon tool

[3] Forensics and the GSM mobile telephone system, S.Y. Willassen

[4] GSM Technical Specification 11.11, December 1995.

Deployment Considerations: Comparing Converged and Dedicated Security Appliances

CONVERGED VS. DEDICATED APPLIANCE DEPLOYMENT

WHEN TO DEPLOY ADAPTIVE SECURITY APPLIANCES, FIREWALL, INTRUSION PROTECTION SYSTEM OR VIRTUAL PRIVATE NETWORK CONCENTRATOR

With the introduction of the Adaptive Security Appliance, users have the option for an appliance-based solution for delivering converged, multifunction security and VPN services within a single platform. With its converged firewall, intrusion prevention system (IPS), and network antivirus services profile, customers may use the Adaptive Security Appliance to deploy a breadth of Adaptive Threat Defense services. For VPN services, the Adaptive Security Appliance offers flexible technologies that deliver tailored solutions to suit remote-access and site-to-site connectivity requirements.

The broad VPN and security services profile of the Adaptive Security Appliance makes it a single device for many uses. Deploy it as a converged threat prevention device at the central site by using its access control, application inspection, and worm, virus, and malware mitigation technologies. Use it as a dedicated remote-access device, taking advantage of its IP Security (IPSec) and Secure Sockets Layer (SSL) VPN capabilities. Move it into the network interior for interdepartmental access control and to guard against worms, viruses, and other malicious code that internal users may unwittingly bring into the network. In small business and branch office environments, the Adaptive Security Appliance serves as an "all-in-one" device, offering comprehensive threat prevention and VPN services while suiting the budgets and operational models of such deployments.

What are some of the deployment considerations associated with using a multifunction device like the Adaptive Security Appliance , versus traditional "dedicated" security appliances such as firewall security appliance, IPS sensor appliances, and VPN concentrators? This paper explores the functional, operational, and cost considerations of deploying a multifunction security appliance instead of dedicated appliances. Comparison of security/VPN appliance and router deployment considerations is out of scope for this paper, but is addressed in detail in the white paper "Positioning Integrated Router Security and Dedicated Security Appliances", available on .com.

SECURITY ARCHITECTURE AND IT ORGANIZATIONAL CONSIDERATIONS

The size, operational model, and segment of the network influence security and VPN platform decisions. There are scenarios where consolidating multiple security and VPN functions on a single device best meets requirements, as well as scenarios where dedicating devices to specific functions is more appropriate.

From a size perspective, the traffic volume and complexity of larger enterprise networks often results in deployment of more dedicated function devices. A security and VPN infrastructure built on devices performing focused or even single functions enables optimal scalability, simplifies software version selection and upgrade cycles, and allows for thorough configuration tuning and greater network segmentation. From an operations standpoint, deploying dedicated function devices also enables segmentation of network security responsibilities among different IT teams.

Typical examples of functional segmentation requiring dedicated security and VPN devices are:

- **Deployment of dedicated remote-access VPN devices**
- **Deployment of dedicated IPS devices for security policy auditing and regulatory compliance or to mesh with IT organizational responsibilities**
- **High-speed, data-center-specific deployments focused on protecting Web server farms and application servers**
- **Network-edge firewalls for resilient, high-speed traffic inspection and access control**

In smaller networks and organizations, the reverse tends to be true. Smaller networks, such as small businesses and remote offices, and smaller IT organizations tend to consolidate as many security and VPN functions on as few devices as possible. Having fewer devices reduces the complexity of the network and also reduces the breadth of knowledge that IT staff must possess to operate a network with multiple unique platforms. In essence, device consolidation generally simplifies operations for sites with smaller IT staffs that often have less specialized focus on security.

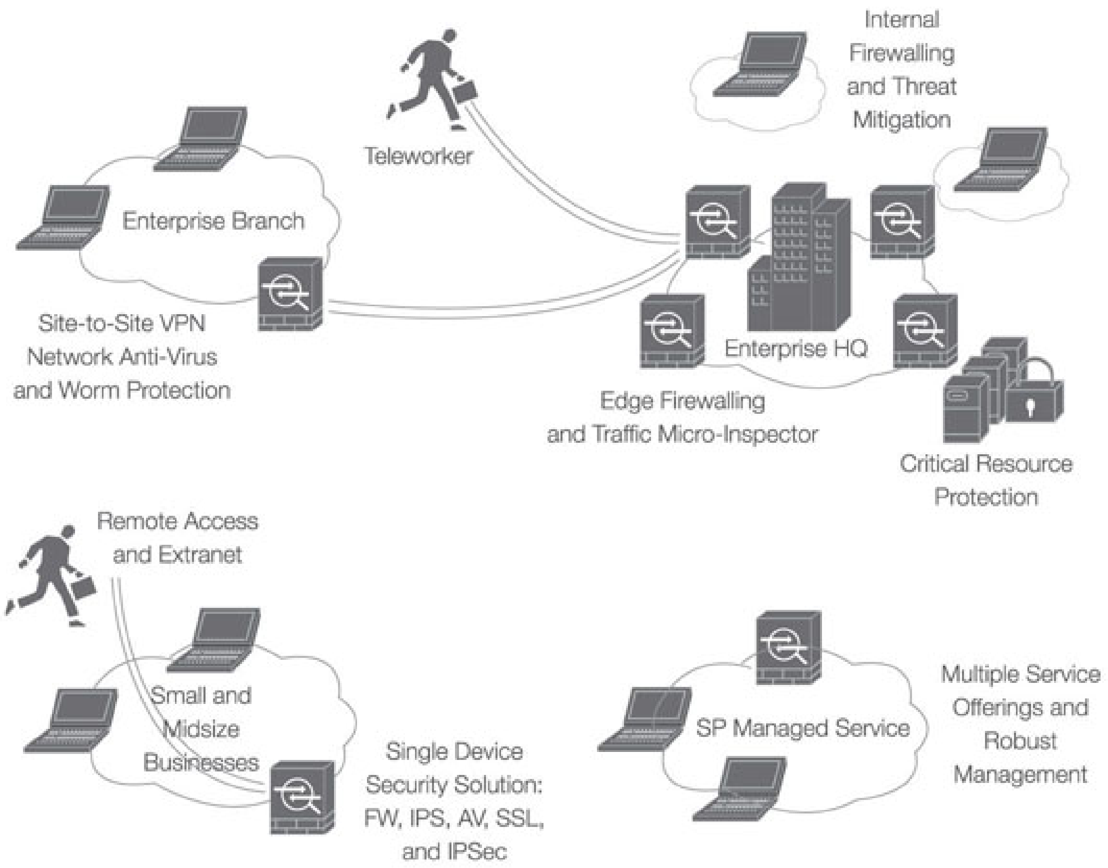


Figure 1. Single Device, Many Uses

In pure IPS deployments, IPS provides security policy auditing and regulatory compliance data. The audit infrastructure provides a "checks-and-balances" approach to securing and validating the posture of the network while layering rich attack, worm, virus, and spyware/adware protection on top of the policy enforcement devices. Furthermore, there is often separation of IT management teams for IPS and other security functions, like firewalls. Consequently, the organization managing the IPS infrastructure generally prefers to have devices dedicated to the service for which they are responsible.

Common deployment scenarios for which the Adaptive Security Appliance provides a single, standardized platform include:

- Converged access control, traffic and application inspection, and worm/virus/malware mitigation for the network edge and/or DMZ
- Converged access control, traffic and application inspection, and worm/virus/malware mitigation for the network interior
- Traditional firewall and application inspection for the network edge and/or DMZ
- Traditional firewall and application inspection for the network interior
- Remote-access VPN with converged traffic and application inspection and worm/virus/malware mitigation
- Traditional standalone remote access VPN termination
- Site-to-site VPN services
- "All-in one" access control, traffic and application inspection, worm/virus/malware mitigation, remote-access VPN, and site-to-site VPN for any location

Conclusion

Both converged and dedicated function security and VPN deployments have a role to play in securing today's networks. The decision is driven primarily by the size of the network, the resulting network architecture, location within the network, and the IT support model. The Adaptive Security Appliance, with its services breadth, is highly flexible and can be adapted for both converged and dedicated function security and VPN deployments.

War Driving Analysis

Introduction

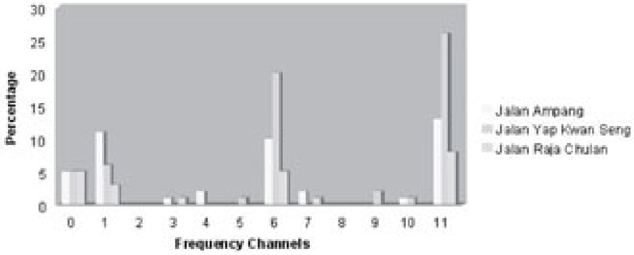
Wireless and broadband technology has contributed significantly to the increasing participation of the interconnected community. The world itself is becoming increasingly mobile, with a wide range of communication devices available. As a result of this mounting interconnectivity and interdependency, information systems and networks are now exposed to a growing number and variety of threats and vulnerabilities. With more and more organization going on the wireless network, it raises the need for a greater awareness and understanding of security issues relating to wireless networks and wireless protocols.

In view of this, on 28 -30 November 2006, Security Assurance of NISER conducted a war driving exercise in dense locations in Kuala Lumpur i.e. Jalan Ampang, Jalan Yap Kwang Seng and Jalan Raja Chulan with the aim to discover the Wireless LAN deployment along the business corridor in Kuala Lumpur and to focus on the users' attention to wireless security concerns.

This is the first phase of our study, to do information gathering and wireless network mapping and to be able to learn security implementation in these networks.

War driving is the act of searching for Wi-Fi wireless networks by moving vehicle as defined by Wikipedia. This exercise involves the use of Laptops with external wireless cards and wireless network discovery tools i.e. Kismet, Airopeek and Netstumbler (freely downloadable tools). A basic configuration for detecting the Wi-Fi wireless networks is used to learn the minimum requirement needed for anyone employing it. The exercise was conducted with no attempt to intercept or decrypt wireless network traffic.

Frequency Channel



The finding shows that channels [1,6,11] which are the default channels for 2.4 GHz band are the most commonly used giving an average of close to 20%. These are the non-overlapping channels. The Wi-fi networks are fairly distributed between these three channels at Jalan Ampang indicating a better network performance with less inter-access interferences as compared to the wireless networks in Jalan Yap Kwan Seng, where channel 11 is most commonly utilized.

Other channels like [3, 4, 5, 7, 9, and 10] were also detected in all three locations with each not exceeding 3%. Channels [2, 8] were not used in all three locations. Channel [0] is used mainly for ad-hoc network connections particularly a peer-to-peer connectivity.

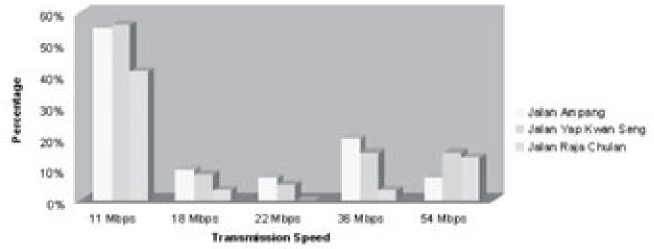
The frequency channels are considered as security parameters as they provide availability of network service and connectivity. Wireless networks use spread spectrum technology and the wireless signals bleed to other near-by channels. Therefore, multiple access points should be setup with the non-overlapping channels to maximize data throughput and to avoid interference and network noise that could result to unreliable wireless connectivity.

A total of 134 access points were detected at these locations,

- **Jalan Ampang (45)**
- **Jalan Yap Kwang Seng (66)**
- **Jalan Raja Chulan (23)**

in Kuala Lumpur 2006

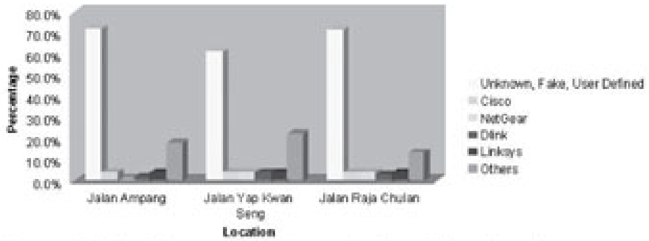
Transmission Speeds



The graph shows that the detected transmission speeds are 11Mbps, 18Mbps, 22Mbps, 36Mbps and 54Mbps. The data collected from all three locations are fairly similar. Networks with a transmission speed of 11 Mbps were the most common giving an average of close to 60%. Clearly, this indicates that majority are 802.11b wireless network of 2.4 GHz ISM Band. The newer versions of 802.11 which could give a maximum through put rate of 54 Mbps ie 802.11a and 802.11g were less common. Networks with transmission speed of 36 Mbps and 54Mbps did not exceed 20% whilst networks with transmission speed of 18 Mbps and 22 Mbps has an average below 10%.

Overall the data clearly indicates that the wireless networks in these areas have not advanced to the latest technology to enjoy new data transmission capabilities. This also goes to show that investment in new technology may not be of priority perhaps due to lack of awareness and lack of services using this infrastructure.

Equipment Vendors



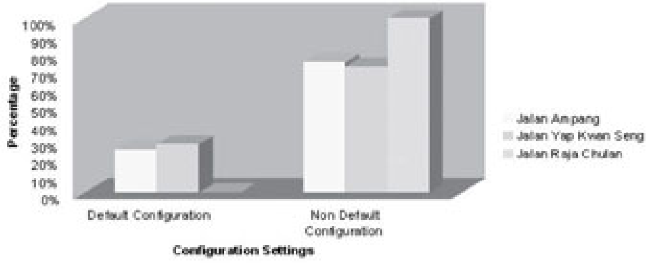
About ~70 % of the equipment vendors in all three locations were classified as unknown, fake and user defined. They were not recognized by the wireless discovery tools used. On the other hand, 17 different manufacturers were detected. Amongst the popular equipment vendors are Cisco, Netgear, DLink and Linksys while less popular includes 3COM, AboCom, Billion Electric, CC&C, Epigram, Nokia, Senoa, Vivato, CNET, Intel, Planet and ZCOM.

As this data shows, the unknown manufactures were fairly the same in all three locations. Making it difficult to guess the capability of the APs and the security functions they provide. Manufacturers' information is very useful to hackers as the Internet is full of information about well known product vulnerabilities, default setting configurations and default passwords.

Default vs. Non Default Configuration

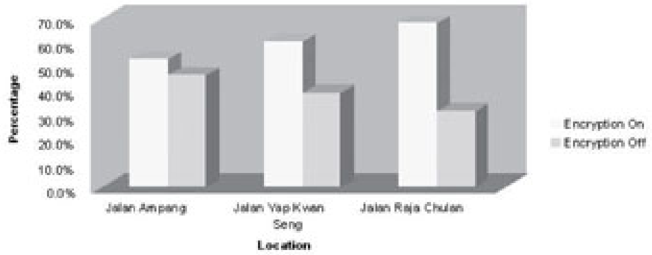
Networks with default configuration are a prime target for hackers. Default configuration is detected by default SSIDs (Service Set Identifier). It indicate that the network may still uses the "out-of-the-box setting with high chance of the administrator's account still uses the default password. Having known the information of the equipment vendors, the attacker may be able to use such information to gain complete control of a network.

The data shows that 25% of the detected access points were having default configuration while it's very encouraging to see that 75% of the detected access points were using user-defined configuration. This is expected as this is the business corridor of KL where protection of their business networks is of high concern.



From the data it shows that networks in Jalan Raja Chulan has the lowest percentage of default configuration indicating better protected networks in this area.

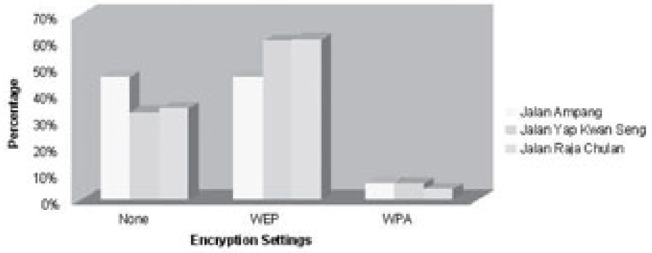
Encryption ON vs. Encryption OFF



The most encouraging about the WiFi networks detected was the ratio of protected to unprotected access points. Data collected by war-drivers around the world indicates that the number of access points with no encryption is approximately 70%. (source: Kapersky Lab). The ratio of encryption OFF to encryption ON is approximately 45% to 55%. Encryption OFF means an open wireless connection and encryption ON means WEP/WPA/TKIP (security scheme) is enabled. The ratio of protected to unprotected networks is almost balanced. The unprotected network percentage is clearly below the 70% global statistics. The findings indicate that the level of security awareness and concerns is fairly high which is very encouraging. Maybe this is expected as this is the business center. It is clear that businesses are concerned on wireless security issues and threats.

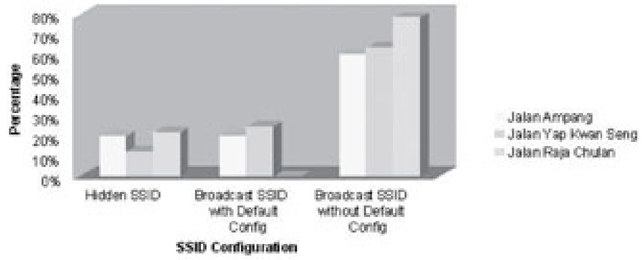
However this ratio of unprotected to protected network can still be reduced with continuous awareness on wireless security issues.

Types of Encryption Setting



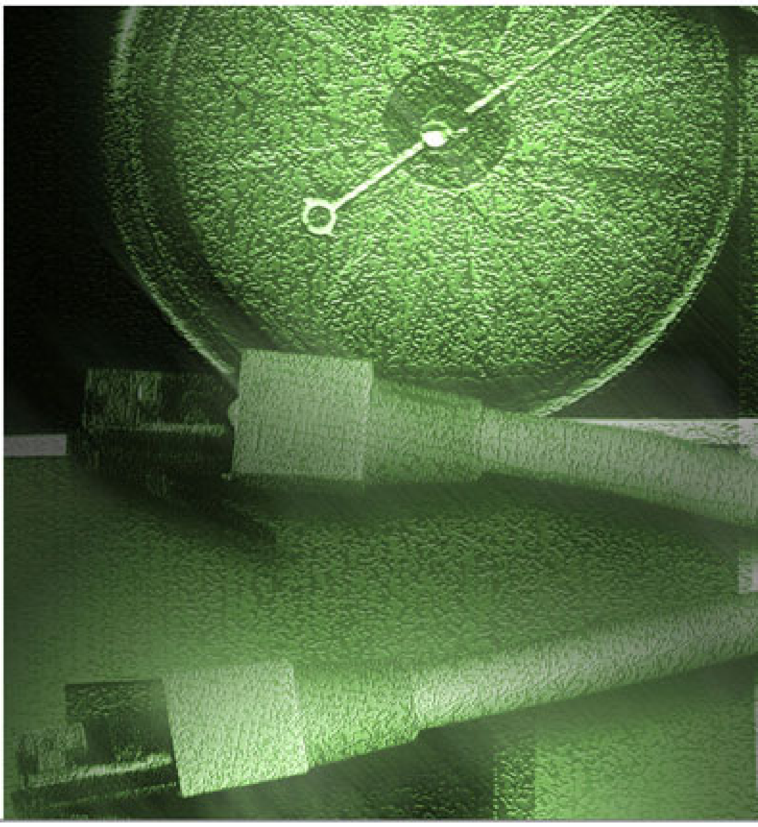
This is measuring the strength of the security implemented. The finding shows that 55% of the networks had WEP (Wired Equivalent protection) enabled and only 5% used WPA (WiFi Protected Access). The rest of the networks detected had not enabled encryption at all which expose them to network sniffing activities since traffic in the air is left in clear. Networks in Jalan Yap Kwan Seng are more susceptible to these attacks. WEP has proven to be a weak encryption scheme. WPA, the stronger encryption scheme, that uses 128 bit encryption key, was only used marginally. This indicates that many of the networks have not been upgraded to use WPA, the newer security standard. All WiFi compliant equipment should be able to support WPA as it is backward compatible. The purist may argue that anything less than the strongest security protection is equivalent to no security at all. Then this translates to that 95% of the networks detected have very weak security protection thus requiring more awareness to keep users informed on WiFi latest security technologies.

Service Set Identifier (SSID)



There are three types of WLAN deployment for SSIDs (Service set Identifier) i.e. hidden SSID), broadcast SSID with default configuration and broadcast SSID with non default configuration. SSID is a label like a network name that distinguishes a wireless LAN from another. Data shows that most networks, an average of 65% broadcasted their network names that disclosed the company and vendor names. SSIDs are the first thing that may attract a hacker. They offer direct information of a network that could entice hackers to try and gain access into these networks.

The finding shows that most common SSIDs are names of persons, companies, services and vendors. 25% of the networks are even more exposed to real threats for having their SSID broadcasted and in default configuration. Even though by hiding the SSIDs has little impact to the security of these networks, it acts as a first line of defense by avoiding it being noticed as potential targets by hackers.



Conclusion

These results does not truly reflect the actual overall picture of the WLAN in Kuala Lumpur, but rather it acts as a sampling data to learn and discover some common practices of WLAN deployment.

To summarize, the results of the war driving in Kuala Lumpur can be categorized into two areas:

1. WLAN deployment

- Most networks use non-overlapping channels which result to less interference and better performance
- Majority of the networks are 802.11b WLAN transmitting data at 11MB
- Most of the vendor equipments were not known
- Majority of the networks do not deploy default configuration

2. WLAN Security

- The unprotected networks are clearly below the 70% global statistics
- Majority of the networks have not advanced to using the newer encryption scheme, WPA
- Most networks reveal descriptive SSIDs or network names

Overall the WLAN deployments have not advanced to the latest WiFi technology to take advantage of the better performance and transmission capabilities and improved security technology such as stronger encryption scheme. .Awareness on WLAN security does exist as reflected by the high percentage of protected WLANs and considerate WLAN administration practices. However it needs to be continuous to keep users informed of latest WLAN security technology and issues.

References

Default Password Lists, URL:
http://www.phenoelit.de/dpl/dpl.html
(20 November 2006)

MAC Address Vendor List, URL:
http://standards.ieee.org/regauth/oui/oui.txt
(4 October 2006)

Wi-Fi Standard Compliance, URL:
http://certifications.wi-fi.org/wbcs_certified _products.php
(2 December 2006)

CWNA Certified Network Administrator Official Study Guide, Third Edition, McGraw Hill, 2005

Comparing 802.11 a,b, and g: Channels and Interference, September 2005, Que Publishings, URL:
http://www.quepublishing.com/articles/article.asp?p=413459&rl=1

Security Awareness

Programme Series

“The strongest factor in information security is not technology, it’s the people!”

The importance of Information Security Awareness Programme for Organisations

Security awareness is vital just as computer systems are vital for businesses and people today. Organisations, parents, teenager, kids and basically every computer user must understand the threats of using a networked computer.

There are many processes, procedures, rules and regulation for everything that we do or use today, e.g. driving a car, applying for a bank account, etc. In the past, computer systems were treated as a tool for creating documents, working with numbers, managing customer records, creating graphics, playing games and more. Then, when the computer network era emerged; people were able to share resources over distances.

The Internet era changed the way people work, play and communicate and also, the way businesses were conducted. Tech-savvy companies gave information to employees and customers via Web pages and e-mail systems. Businesses appended .com or .net to their names and many secured domain names and developed websites. These in turn became targets for hackers, who left their marks on thousands of Web pages, including websites belonging to critical national infrastructure and government organisations. Many new threats emerged such as identity theft, spam emails, phishing attacks, and virus attacks.

Today, to infect a large number of machines in the networked world takes a few seconds as compared to the past with standalone machines. The channels for attack are many, ranging from email systems, websites, instant messaging system, FTP and more. Many users use more than one web service regardless whether they are home users or office users.

There are numerous articles, talks, websites and campaigns on information security. There are hardware and software systems designed to protect data, people and businesses. But the question is, how you ensure that the users know and adopt the safe practices and proactively apply the methods described?

Users who are web-savvy probably have some knowledge about computer security and there are people who have security software installed, e.g. antivirus, anti-spyware and “assume” the system is secured. Having a technical security solution such as firewalls, antivirus and security systems are not sufficient enough, although it is primarily sold based on its “effectiveness”.

Time has come where throwing technology and big money at the problem is no longer effective at improving security. Instead of continually installing and patching the technology, and forever scrambling to deal with security incidents and emerging risks, it’s time to take a step back and find a better, more comprehensive approach. Security breaches will still be there and will grow by the day. It is important that people and organisations understand the severity of cyber threats and consider implementing security policies and best practices as a preventive mechanism.

The first and the foremost fundamental exercise should be to develop mechanisms that would ensure computer users are made aware of cyber threats and understand the implications.

In today’s organisations, it is vital that information assets are protected in terms of confidentiality, integrity and availability by parties involved. Personnel at managerial level need to know their roles and responsibilities related to the organization’s mission statement, understand the organization’s IT security policy (if available), procedures and practices. They have to understand the Management of Operational and Technical Controls in order to protect the IT resources as they are responsible for it.

In order to successfully implement a security awareness and training programme, a security policy must describe clearly the business needs and the threats that are related. Users must be informed of their security responsibility. Subsequently, the processes must be implemented for monitoring and reviewing the programme to ensure acceptable level of awareness is achieved.

Every employee in the organisation should be the target group for security awareness programme, with the ultimate goal of creating a security culture for all levels of staff and management.

The security awareness programme should include the following factors and activities to ensure successful implementation from inception:-

1. Selection of suitable topics for security awareness programme that is current and relevant.
2. Determining the sources for security awareness programme content development. The content should not drive vendor products but rather the concept of the threats, best practices and preventive measures.
3. Developing security awareness materials focusing on target audience and their needs. The language used for describing the concepts should be clear and not to be technical in nature.
4. Evaluate the effectiveness of the security awareness and training programme. Revisions should be made if the audience do not see the relevance or do not grasp the concept.
5. Provide updates and changes when technology or organisation priority changes. The security awareness programme must be designed to meet the organisation's mission and to maintain its well being. As new threats emerge and technology changes, there must be a platform where the users are communicated of such.

A security awareness programme is conducted to communicate security requirements and also to be used as a medium to disseminate information in order to share policies and processes. An organisation adopting a security awareness programme must define and understand their requirements and their roles and responsibilities. It is important within an organisation to identify who is to be involved and their responsibility in the security awareness programme.

It is said that learning is a continuous process and in information security, it can be divided into three levels of knowledge building exercise that is Awareness, Training and Education.Awareness programmes should be designed to create a general understanding of security concerns and to be used as a platform for sharing good security practices.

"Awareness is not training. The purpose of awareness presentation is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly" [1]

When an organisation has reached a level of security awareness, the next step, is to provide a more structured knowledge building activity i.e. training.

"Training strives to produce relevant and needed security skills and competencies"

Education is the last process in knowledge building and it is defined as:

"Education integrates all of security skills and competencies of the various functional specialties into common body of knowledge… and strives to produce IT security specialists and professionals capable of vision and pro-active response" [2] **.**

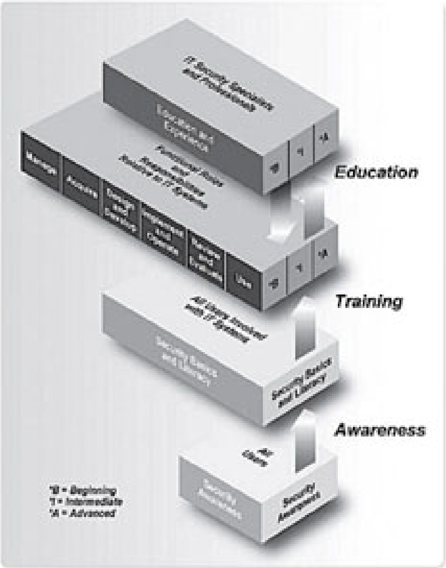

IT Security Specialists and Professionals
Education
Training
Use
All Users Involved with IT Systems
Security Basics and Literacy
Awareness
All Users
Security Awareness
"B" = Beginning
"I" = Intermediate
"A" = Advanced

Fig. 1: The IT Security Learning Continuum[3]

The benefit and the need for information security awareness helps to secure information assets by informing people about information security risks and controls, and to provide more specific information and guidance where necessary. Management support and commitment to information security enable successful implementation of the awareness programme and creating a security culture by means of adapting and implementing Security policies, standards, procedures and guidelines, cyber laws and rules and regulations. By informing and motivating people to behave in a more security-conscious manner, for example taking security risks into account in business decision making, would eventually lead to successful implementation of a security culture

References

Wilson, M., Hash, J., October 2003. Building an Information Technology Security Awareness Program
http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-506]
[Cited 18 December 2006]

Noticebored Newsletter. Why do client's need to address information security awareness? (Updated 1st January 2007)
http://www.noticebored.com/html/why_awareness_.html
[Cited 15 December 2006]

European Network and Information Security Agency (ENISA), June 2006, A User Guide: How to Raise Information Security Awareness: ENISA publication

Averick R., 2003. Marketing Security Awareness: Published by Institute of Internal Auditors
http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=544
[Cited 15 December 2006]

[1] NIST Special Publication 800-16

[2] NIST Special Publication 800-16

[3] Extracted from NIST-SP800-50 - Building an Information Technology Security Awareness and Training Program

FIREWALL AND MALICIOUS ATTACKS

It doesn't matter who you are or where you are; you could be a restaurateur dealing with credit card transactions or a government security advisor.
There should really only be one concern on your mind:

Is my data safe?

If you know the answer to this today, will it be true for tomorrow? New programs are being created and used 24/7. They are easier than ever to get hold of and use, they are being utilized by more and more people and they can run your company into the ground in a matter of minutes as connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Users who connect their computers to the Internet must be aware of these dangers, their implications and how to protect their data and their critical systems. It's undeniable that the Internet, like any other society, is plagued with a brand of malicious idiots who enjoy the electronic equivalent of writing on other people's walls with spray paint, tearing their mailboxes off, or just sitting in the street blowing their car horns. To simply ignore these realities is foolish and potentially dangerous to you, your business and your data. In previous articles, we addressed the issue of protecting yourself against external threats to your system, particularly as it relates to viruses.

In this article we are going to turn our attention essential defensive weapon in the armory

-- the firewall.

While just about everyone these days has an anti-virus program, they are not enough. There are other methods of attack or intrusion from the Internet against your network, hence your first line of defense should be a firewall. A firewall provides protection from port scanning and disables access to shared folders, files, and printers, which keeps the bad guys from copying files and programs to your computer that can cause serious problems when executed.

A firewall can also act as your corporate 'ambassador' to the Internet. Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug-fixes, and so forth. Several of these systems have become important parts of the Internet service structure and have reflected well on their organizational sponsors.

Sounds great, you say. But what exactly is a firewall?

FIREWALL FACTS

As mentioned above, a firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. A firewall can be either a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

You don't need to understand all of the technical details to use a firewall, but it is important that you understand how it works. A firewall examines all traffic routed between the two networks to see if it meets certain criteria.

There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria, and it denies if it does not. The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another.

Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependent upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state. They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through.

If the traffic meets the criteria, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.

WHO'S AT RISK?

DSL or a cable modem poses a greater risk to your computer than dial-up modems. Why? A dial-up modem uses a different network address every time it connects to the Web so it is a moving target. DSL or cable connections use a network address that doesn't change. A firewall helps obscure your network address, even though it always stays the same. If your computer is always connected to the Internet, your computer's network address is even more available to hackers. There is also a risk from "sharing the wire;" people in your neighborhood who have the same cable service could potentially trespass on your computer. A firewall can help protect your computer in such instances.

Many dial-up Internet users believe that anonymity will protect them. They feel that no malicious intruder would be motivated to break into their computer. It's a nice thought, but as the thousands of dial-up users who have been victims of malicious attacks losing days of work and having to reinstall their operating system can attest, this is only an illusion. Irresponsible pranksters can use automated robots to scan random IP addresses and attack whenever the opportunity presents itself.

Anyone who connects so much as a single computer to the Internet via modem should have a firewall. You should also use firewall protection on a computer that has a direct, dial-up connection to the Internet, a single computer connected to a cable modem, or a single computer connected to a DSL modem. If you're a broadband user with two or more ISP assigned IPs connected through a hub, you'll need to protect each computer individually. An easy rule of thumb-if a computer connects directly to the Internet, it needs protection.

If you have a Windows XP-based computer that is used for Internet Connection Sharing (ICS), you'll also want to enable a firewall on the host computer (and only the host computer).

WHO DOES NOT NEED A PERSONAL FIREWALL?

If a computer is a client computer to an ICS (Internet Connection Sharing) host, do not install a firewall, but be sure you do enable it on the host computer. If a computer is behind a NAT box or router, don't use a firewall, because the inherent properties of NAT will protect you. If you're in an enterprise/corporate environment, you likely don't need a personal firewall while logged into a domain at work because your IT staff will have proper commercial firewalls in place on the network.

MAINTAINING A FIREWALL

Simply installing a firewall is not enough. You need to establish and follow a maintenance program you will follow every month to keep your firewall in good condition:

1. Check for software updates. Go to your firewall vendor's Website, and sign up to be notified of updates. Note: If you are using Windows XP or Windows Me, you can install the Automatic Updates feature and get the software updates for Internet Connection Firewall (ICF) delivered automatically.
2. Review the logs. Ascertain how much probing traffic your firewall is repelling.
3. Turn off an "always on" connection. If you have a DSL or cable modem, turn off your connection when you don't need to be online.

FIREWALL LIMITATIONS

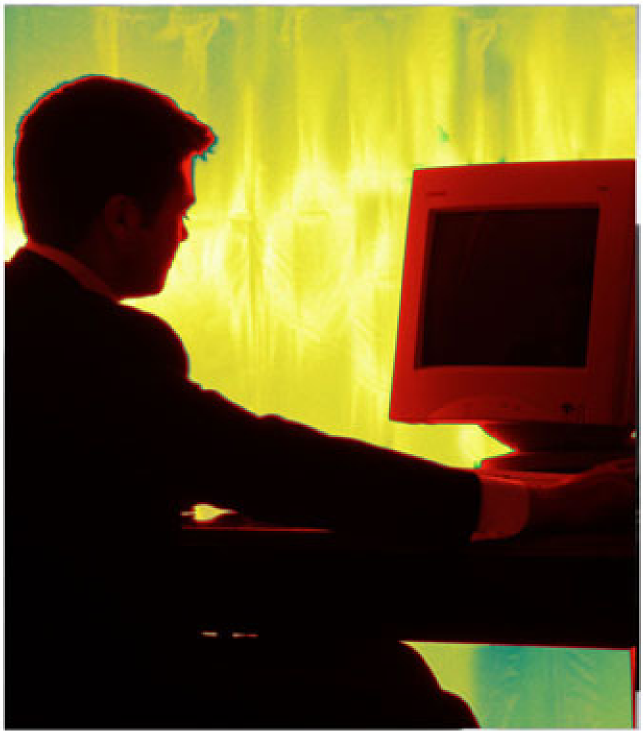
Despite their obvious values, firewalls do have their limitations as it is not a magic bullet. Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape can just as effectively be used to export data. Many organizations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected. While it is silly to build a 6-foot thick steel door when you live in a wooden house, I have encountered many corporations and individuals buying expensive firewalls and neglecting the numerous other back doors into their network. For a firewall to work, it must be a part of a consistent overall organizational security architecture. Firewall policies must be realistic and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network.

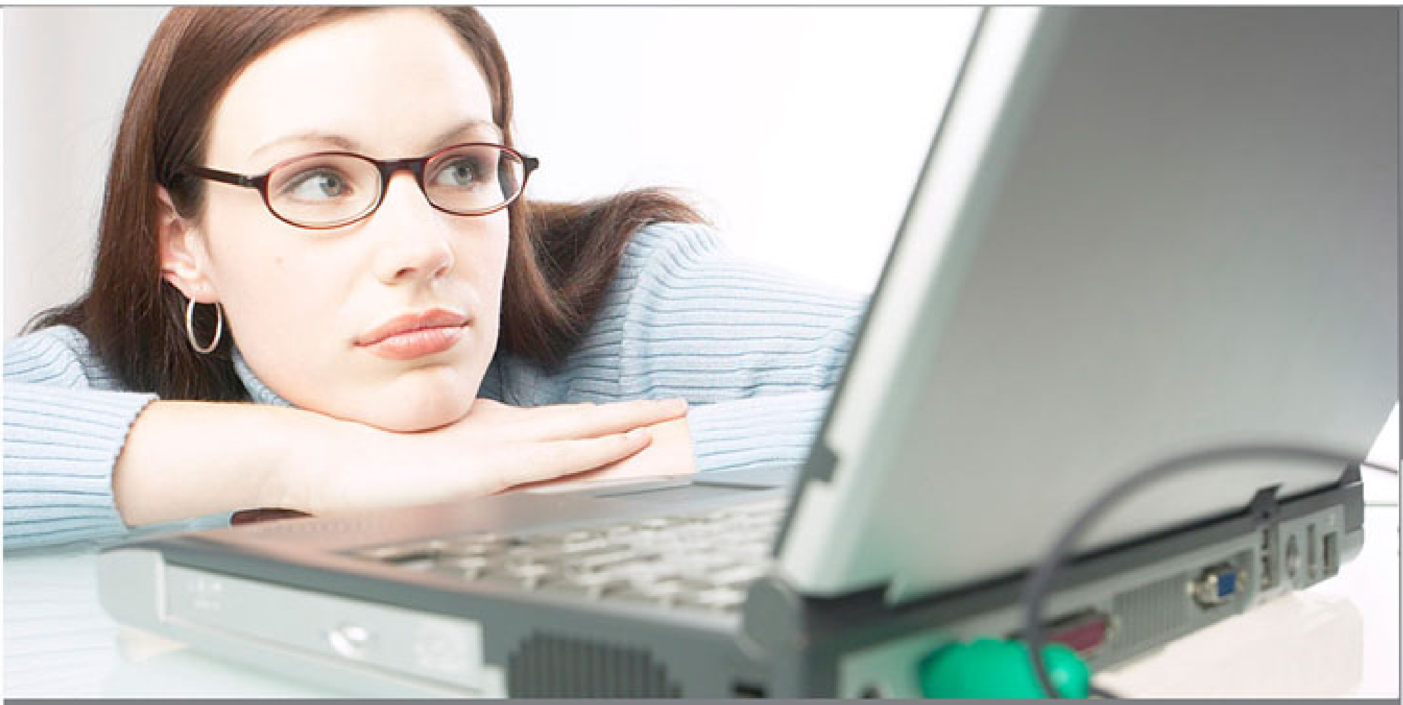
Another thing a firewall can't protect against is traitors inside your network. Floppy disks are a far more likely means for information to leak from your organization than through a firewall. Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall if he can find a 'helpful'' employee inside who can be fooled into giving away his password.

FIREWALL RELATED PROBLEMS

Firewalls introduce problems of their own. Information security involves constraints, and users don't like this. Firewalls restrict access to certain services. The vendors of information technology are constantly telling us "anything, anywhere, any time", and we believe them naively. Of course, they forget to tell us we need to log in and out, to memorize our 27 different passwords rather than writing them down on a sticky note on our computer screen and so on.

Firewalls can also constitute a traffic bottleneck. They concentrate security in one spot, aggravating the single point of failure phenomenon. The alternatives however are either no Internet access, or no security, neither of which are acceptable in most organizations or in your home computer.





Regulating Cybercafé Operations

Introduction

Besides serving tourists, teenagers and others without home computers, cybercafés are very attractive to terrorists and criminals. The wildly popular cybercafé outlets provide a good hide-out for these criminals to carry out their activities without being identified. Unlike accessing the Internet from a personal computer at home, cybercafés offer criminals multiple layers of protection against discovery. During the war in Afghanistan, US intelligence officials claimed that al-Qaeda members used Internet cafes in Pakistan to email each other in attempts to regroup after American air attacks. On another note, those responsible for kidnapping and killing journalist Daniel Pearl emailed ransom notes and threats also from Internet cafes.

But why Cybercafés?

[1] Internet cafes are regarded equivalent of public payphones. In other words, these cafes provide unmonitored and often anonymous access to the Internet. Much like public payphones, computers at Internet cafes are available for use by anyone, without registering a name or other identification information with any service provider. With hundreds or perhaps thousands of other visitors to cybercafés on any particular day, criminals can easily blend in with the crowd. Furthermore, practically anyone can setup a cybercafé with a number of computers and offer Internet access and this is done often with their own rules.

The Threats

The potential threats posed by cybercafés are tremendous and cannot be ignored. Among the threats, cyber-terrorism is seen to be the most dangerous and needs immediate attention.[2] As the Internet becomes more pervasive in all areas of human endeavours, individuals and groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e. members of an ethnic group or belief), communities and entire countries, without the inherent chance of capture, injury or death to the attacker. We cannot deny the possibility of a large attack making use of computer networks to sabotage critical infrastructures with the aim of putting human lives in jeopardy or causing disruption on a national scale either directly or by disruption of the national economy.

Business and prank attacks such as hacking and spreading of malicious software programs also take place at these cafes which includes spreading of emails containing inaccurate or false information about individuals, companies and governments with the intent of damaging their reputations.[3] The widespread of illegal e-gambling is a new trend in this country. Online gamblers are taking advantage of the loopholes and Malaysia's present laws are inadequate to cover this area. Electronic gambling is a form of gaming at cybercafés that allegedly operate as "online casinos" where a bet is placed for a wager, with payoffs at the end of the game.

[1] BBC News, 15th April 2002 by Paul Eng

[2] http://en.wikipedia.org/wiki/Cyberterrorism

[3] http://www.niser.org.my/news/2000_02_14_01.html

Another major issue which needs immediate attention is the unrestricted access to pornographic materials. Almost all, if not all cybercafés in the country do not have a filtering system to prohibit the access to pornographic sites. School children are the most frequent visitors to these cybercafés and this can be proven by a normal afternoon visit to any cybercafés in the country. These school children in school uniforms flock into the cafes as soon as the school sessions are over. They get hooked on to the Internet either to "meet" their cyber friends, get indulged with networked games or surfing prohibited porno websites.

Cybercafé users are also unaware of the personal security threats that they are exposed to. Personal information such as personal CVs, chat logs, photos and so on from previous users can be found in abundance. This information can be used to commit further frauds such as financial frauds (credit card, bank loans, EPF & etc).

Identity theft cases similar to [4] Syarizal's which rocked the country recently can also be seen as the result of personal information obtained from these cafes. On 5th October 2006, New Strait Times reported that more than 1,000 people have become the victims of identity theft costing millions of Ringgit since 2003.

Studies in US and Europe show that most of the computers in cybercafés are not clean and normally infected by various types of malicious software programs. Malicious programs like keystroke loggers are found in computers which can be used to capture passwords or encryption keys.

THE SOLUTIONS

A code of practice is necessary to regulate these cybercafés because these risks are clearly defined. New and unambiguous laws must be established to curb this alarming issue. Government should look at the bigger picture and analyze the overall impact to the national ICT security. Unlike public payphones, cybercafés are not necessarily completely anonymous. The very nature of Internet technology means suspicious users and activities can be monitored and tracked.

To start with, cybercafés must be mandated to enhance the premises' physical security by installing closed-circuit television system (CCTV). Some of the cybercafés are already equipped with this system but only to monitor their own staff and their cashier counter. CCTVs must be installed covering the entire premise to monitor visitors walking in and leaving the cybercafés. The quality of the captured video images must be reasonably high enough to identify the visitors' identity. The video footage must be backed-up and stored for at least a period of 6 months.

A strict access control must be imposed to identify and monitor visitors. Currently there is no such system in place merely due to the unavailability of proper law mandating the café proprietors to do so. MyKad can also be used to register visitors. Their identification information should be stored together with the information of the PC assigned to them such as the IP address and the workstation number.

Café owners should prohibit the use of the Internet facilities by unknown person, whose identity has not been established. This implementation will facilitate law enforcement officers to identify the whereabouts of suspect in the event of an incident. For foreign users, their passport information must be obtained and kept in a computerized log system.

Other physical elements such as partitions between PCs must also be considered. The partitions must be of a reasonable measurement such that the privacy of the users is protected. The activity server log must be preserved and kept for duration of at least 6 months or more and these logs must be readily accessible for law enforcers. The cybercafé owners must also play a vital role in combating this issue by immediately reporting to the police in the event they find activities of any visitor suspicious. Once reported the computer should not be used by other until clearance being issued by the police. Warnings, disclaimers and login messages should also be displayed on the desktop of the PCs and it is vital in reminding the users of the potential threats that they may be exposed to while using the PCs and the Internet. The café proprietors should also impose restrictions on downloading or installation of software programs which will automatically avoid the installation of malicious software programs.

The government must also mandate all the cybercafés to register their businesses with the relevant authority. The IP addresses assigned to these cafes must be identified and special licenses must be issued to operate Internet cafes. In the event of violation of the code of conduct, licenses should be revoked or a hefty fine should be imposed to the owners.

A web filtering system to restrict access to pornographic materials can also be implemented to all these IP addresses at the ISP level. The government should also run programs such as awarding the best operated cybercafés which comply with the laws. Logos with bronze / silver / gold style compliance certification scheme can also be introduced for the public to choose the best cybercafé to visit. Furthermore, the government should also focus on educating the public on the security threats and the precautions that must be taken when visiting cybercafés. Finally, cybercafés must be put under the scrutiny of the law enforcement agencies. Frequent spot-checks or security audits must be conducted to ensure that cybercafés comply with the ambits of the law.

CONCLUSION

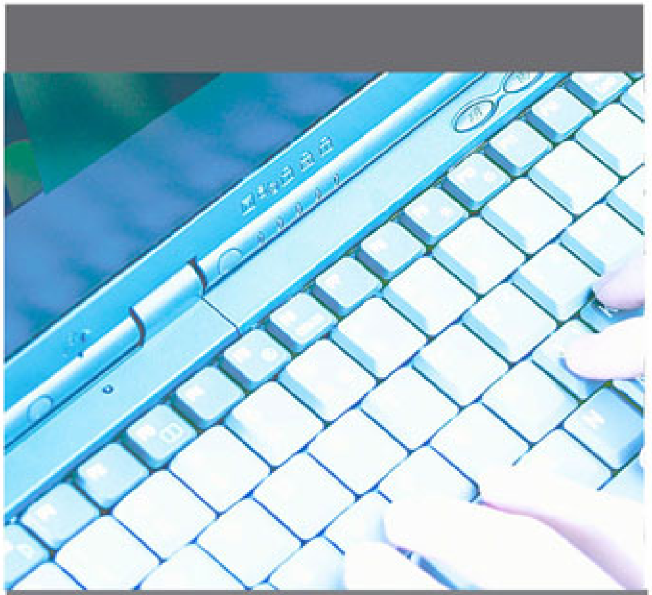
The key to the success of any protection program is effective governance and coordination. In response to industry demands, and in alignment with the ICT security needs of our country, a standard or a code of practice must be established to regulate the cybercafés without violating privacy rights. All cafes should be vetted regularly by the authorities to access its worthy of operations. Café owners should also be warned about any activities that would damage state security, disturb public order and interfere with the public's rights and interests.

REFERENCES

- http://en.wikipedia.org
- http://www.mailarchive.com/apple@lists.apnic.net/msg00007.html
- http://www.niser.org.my
- http://www.nst.com.my

[4] http://www.nst.com.my/Current_News/nst/Thursday/Frontpage/20061005075538/Article/index_html

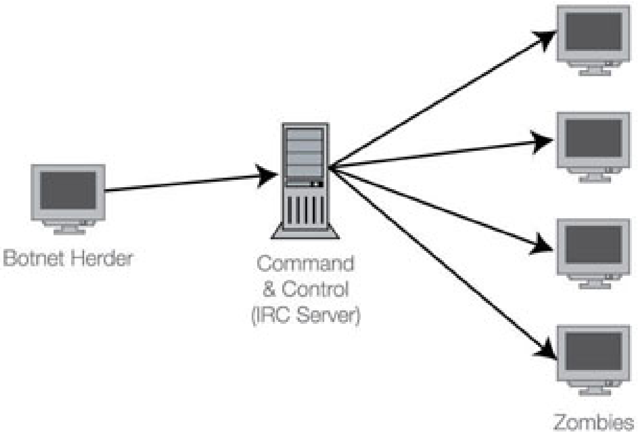
Combating Bots



What is a bot?

Bot is a term used to describe a piece of software that run automated tasks over the Internet. The advantage of using a bot for a repetitive task is obvious and therefore one can find its usage in web crawlers, internet gaming and online chatting. The usage of bots these days however has gone beyond its original (or legal) intention. Malicious use of bots includes co-coordinated and automated attacks on networked computers, such as a denial-of-service (dos) attack. In addition, bots are known to be used in a click fraud, where the bot imitates a web user in clicking on an advertisement, and for relaying unsolicited emails (spam) over the internet [1].

A botnet is a collection of computers that has been infected by a malicious bot (or zombies) and is being controlled remotely. This command and control (C&C) infrastructure allows the owner of the botnet, also known as the bot herder, to remotely send instructions which is then executed by computers where the bot is running.



The communication between the bot herder and the zombies occurs over the Internet, commonly using the inter-relay chat (irc) protocol (see diagram above). In this setup, the zombies connect to an irc server and wait for further instructions. Communication however is not limited to using IRC alone, peer-to-peer (p2p) protocol and http are known to be used by bot operators to maintain their botnet.

It is observed that home computers running an unpatched Windows based operating systems are popular targets for bot infection. However this does not mean that computers running Linux or Unix do not get infected by a bot. A bot typically attempts to infect another computer by exploiting known vulnerabilities.

What can a botnet do?

The botnet infrastructure makes it very convenient to serve different purposes:

1. Launch denial of service attacks
2. Relay unsolicited emails spam for spammers
3. Generate fake traffic to online advertising schemes (click fraud)
4. Harvest user id, passwords, credit card number, email addresses and other confidential information to conduct identity theft
5. Launch new worms, viruses, '0-day exploits'
6. Host spoofed sites of banks (Phishing)

From the above, one can see that botnet related services may generate a significant amount of income to botnet operators. This becomes the main reason for botnet operators to increase the size of their 'herd' so that bandwith, storage and processing capabilities becomes more attractive to potential customers.

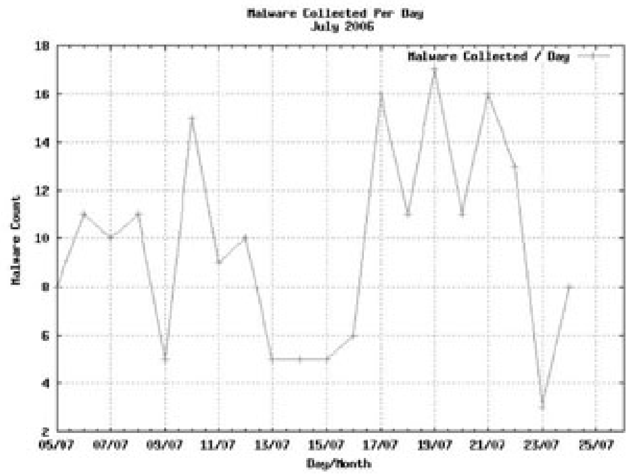
In October 2005, Dutch authorities arrested 3 men that was running a botnet that contain 1.5 million zombies. The trio was arrested after threatening to launch a dos attack against a firm in the US [2]

MyCERT's/Malaysia's experience with bots and botnets.

MyCERT has dealt with bots for quite sometime. In September 1999, 38 Malaysian servers were compromised and used to run bouncers or BNCs, a program that hides the original source of a user's connection, and bots (eggbots). These servers were used to launch attacks on other servers.

Due to the changing nature of threats involving botnets, NISER Honeynet Project deployed server for collecting malicious software (malware) on the Internet. The server emulates known Windows vulnerabilities and can be exploited by malware such as worms and bots, and also extract their payload for further analysis. It was observed that in a space of 21 days in the month of July 2006, the server were 'infected' on average from more than 1000 unique source IP addresses and that the first bot infection occurred less than 5 minutes after the server was connected to the internet.

The figure below shows the number of distinct malware collected on a daily basis in a space of 21 days in July 2006.



The majority of malware captured from the on the server is 'bot' related which in a way shows its prevalence. The following is the list of bots detected by Clam Anti-Virus [3]:

- Trojan.Poebot-32
- Trojan.Mybot-6586
- Worm.Gaobot.565
- Trojan.Mybot-2969
- Trojan.Mybot-5073
- Trojan.SdBot-2275
- Trojan.Mybot-6654
- Trojan.IRCBot-244
- Trojan.Mybot-7671
- Trojan.Codbot-18
- Trojan.Mybot-6648
- Trojan.Mybot-6648
- Trojan.SdBot-730
- Trojan.SdBot-2606
- Trojan.Spybot-200
- Trojan.Mybot-7671
- Trojan.Mybot-7631
- Trojan.SdBot-2500
- Trojan.Poebot-19
- Trojan.Mybot-6400

Detecting and Mitigating Botnets

Systematic patch management efforts on behalf of the user can ensure that a host is not compromised in the first place and it is also he most effective prevention technique. In our observation, most bots rely on exploitation of known vulnerabilities to infect other hosts. Infection is possible via vulnerabilities in the operating systems itself, or applications such as browsers, instant messaging software or media players. In fact, we even came across bots that spread via vulnerable web applications. Therefore timely updates definitely help to prevent the size of a botnet from growing larger.

'Suspicious' connection between the infected hosts and the C&C servers can be monitored and blocked upon detection. For instance, network administrator can look for outbound connection to an irc server such as the following:

```
10:15:47.564072 IP 10.1.1.5.3748 > 84.x.y.z.6667: S 2656374493:2656374493(0) win 57344 <mss 1460>
10:15:50.572609 IP 10.1.1.5.3749 > 84.x.y.z.6667: S 1844207723:1844207723(0) win 57344 <mss 1460>
10:15:53.772130 IP 10.1.1.5.3749 > 84.x.y.z.6667: S 1844207723:1844207723(0) win 57344 <mss 1460>
10:15:59.762218 IP 10.1.1.5.3748 > 84.x.y.z.6667: S 2656374493:2656374493(0) win 57344 <mss 1460>
10:15:59.971191 IP 10.1.1.5.3749 > 84.x.y.z.6667: S 1844207723:1844207723(0) win 57344 <mss 1460>
```

In the above example, 10.1.1.5 is a computer that has been infected by a bot and sending packets to a C&C server with IP address 84.x.y.z. However not all botnets use irc as the medium of communication as in the example above (port 6667) and therefore their communication may not be so obvious at first sight.

From some of the sample malware collected, it is observed that the IP address or the host name of the C&C server is hard-coded in the malware itself. This piece of information can then be used to identify the server and therefore shut it down (or block connection to it at the router or firewall). In the event where dns is used to point to the C&C, network administrator or operators can change dns entries to resolve to a different IP address.

Taking care of the C&C servers is only half of the story, communicating with owners whose computers have been infected by bots so that their computers will not be 'recruited' by another bot herder is another difficult task. On top of that, bots these days are designed with advanced features such as the use of encryption for hiding contents of communication. In addition, botnets operators have moved away from the client-server design to using peer-to-peer architecture where they no longer need to rely on a single C&C server.

Conclusion

Bots and botnets have certainly introduced a different challenge to network security practitioners. It is a global phenomenon and thus combating them require close collaboration between service providers, CERTs and industry across physical borders. Computer users or owners must also be aware of their role in this effort by ensuring that their computers are free from bots.

References

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

Dutch Botnet Suspects Ran 1.5 Million Machines -
http://www.techweb.com/wire/security/172303160

Clam Anti Virus
http://www.clamav.org

ETHICS
IN INFORMATION SECURITY

Ethics is a study of questions about what is morally right and wrong. An ethic of particular kind is an idea or moral belief that influences the behaviour, attitudes and philosophy of a group of people. How do we define "what is ethical"? Do we need a legal framework to bind us so as to be ethical?

Cases of security breaches across the globe

Bot is a term used to describe a piece of software that run automated tasks over the Internet. The advantage of using a bot for a repetitive task is obvious and therefore one can find its usage in web crawlers, internet gaming and online chatting. The usage of bots these days however has gone beyond its original (or legal) intention. Malicious use of bots includes co-coordinated and automated attacks on networked computers, such as a denial-of-service (dos) attack. In addition, bots are known to be used in a click fraud, where the bot imitates a web user in clicking on an advertisement, and for relaying unsolicited emails (spam) over the internet [1].

A botnet is a collection of computers that has been infected by a malicious bot (or zombies) and is being controlled remotely. This command and control (C&C) infrastructure allows the owner of the botnet, also known as the bot herder, to remotely send instructions which is then executed by computers where the bot is running.

The trend is also the same in other countries such as South Korea and China where the number of cases reported to their respective Computer Emergency Response Team (CERT) is increasing. In Korea in the year 2004, number of cases related to hacking, spam and worm incidents were 16,025, 3297 and 4993, respectively. Meanwhile, cyber security incidents reported to the China CERT (CNCERT/CC) in 2004 were phishing, DOS, web defacement and malicious code [3].

Malaysia is ranked 8 out of 10 top-infected countries in the Asia Pacific region as a target for cyber attackers. According to an Internet Security Threat Report by Symantec Corp, between 1 July and 31 December last year, cyber crime-related threats are gaining momentum, which is bad news for enterprises as their information assets and infrastructure becomes more vulnerable to cyber attacks. Symantec Corp in its ninth volume of Internet Security Threat Report anticipates an increase in malicious code activities that are designed specifically to generate profit over the next 12 to 18 months [4].

What contributes unethical?

With the advance of technology, the sophistication of tools and techniques are becoming more powerful. Furthermore, all of these tools are available on the Internet with more user-friendly, very minimal cost and in some instances free of charge. A personal computer and a simple connection to an Internet Service Provider (ISP) anywhere in the world is enough to cause a great deal of harm. Users are unaware the damage that will occur as a result of their action when using computers unethically.

Script Kiddies are people who use utilities and tools available freely from the Internet that can cause disruption or damage to the systems. These people merely lucked into the possession of harmful software programs called scripts. They eventually stumble across a site that is vulnerable, vandalize it and leave behind a message about how clever they are – despite the fact that they had no idea what they actually did or how they did it. This is because they usually do not know the full capability of the tools and use them without fully understanding the consequences and harm the tools can create especially if not used with care.

For example, Pentagon computer network was hacked by a 17 years old teenager from Austria, Markus Hirsch. He was reported to have successfully obtained information about the location of military nuclear missiles. He managed to get into Pentagon's computer networks after downloading certain software from the Internet and happily cruised in the network from his bedroom [5]. In another case, a Massachusetts teenager was charged with disabling the Aviation Authority control tower for six hours at Worcester Regional Airport [6].

Measures to overcome this problem

1

Creating ICT Security Culture amongst Users

Awareness is extremely important role in educating users on do's and don't in the cyberspace sphere. Lack of awareness from the person responsible will cause serious damages and loss. It is recommended that awareness should be inculcated to ensure good security practices. Having an ongoing security awareness program in place can greatly reduce the risks of security breaches.

2

Conform to the Code of Conduct

A code of conduct will serve as a guide and target for the standard of service expected from all users. The code is targeted to take care of the public interest, employers and clients without any compromise to professional competence and integrity. Users should pledge to the code and become ICT Security professionals just like other recognised professionals such as doctors, lawyers and architects. Among others, users should be aware and well versed in the policies and procedures that safeguard public security and safety.

3

Introducing subject on computer ethic in secondary school

As ethics is inculcate, computer ethics should be introduced early to students in secondary school. In the subject, they must be able to understand the importance of ethical computer usage. They must also make known to the Malaysian Cyberlaws to encourage them to abide to the law.

References

- http://news.com.com/Computer+crime+costs+67+billion%2C+FBI+says/ 2100-7349_3-6028946.html
- http://www.vnunet.com/2149507, January 31, 2006
- Rozana Sani (2006), Cybercrime Gains Momentum, New Straits Times, April 3, 2006
- APCERT Annual Report 2005
- Komputer Pentagon Diceroboh, Berita Harian, 16 Jun 2002
- www.fbi.gov/libref/historic/famcases/ames/ames.htm

Why Should We Use Access Control?

Few employers want to allow all of their employees access to all facilities all of the time. That's why more and more are using electronic access control to limit employees' access to their facilities. At a minimum, an electronic access control system can be used to allow only employees into a building after hours, and provide excellent documentation of when and where employees enter and exit. Access control is the only technology that proactively attempts to keep unauthorized individuals out of a building or areas within a facility, and is a perfect complement to video surveillance, burglar and fire systems in a comprehensive security solution proposal.

Replace the Key

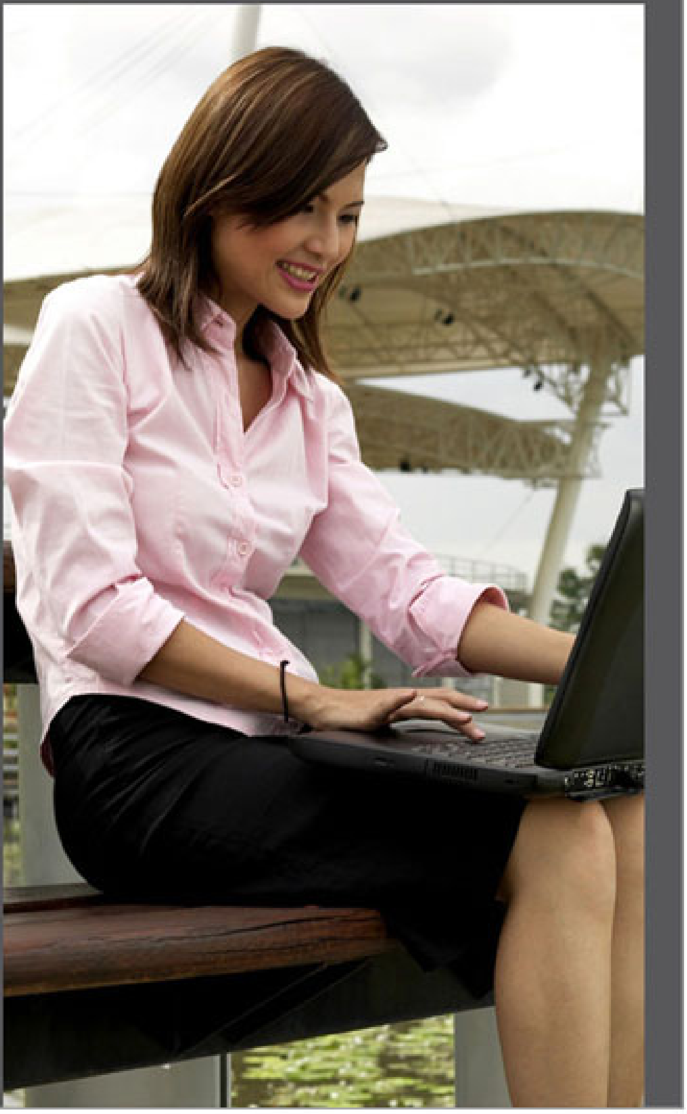
Managing keys is a nightmare for most companies. Some facilities use dozens of keys, making them cumbersome to carry and a liability while the holder stands at an entrance wading through the set for the right one. High employee turnover and multiple locations only compound the problem. Keys are easily lost or duplicated, and terminated employees often do not return keys. If however, an employee leaves the company without returning their access badge, the employer can easily delete that former employee's access. On a networked system, that access can even be changed remotely. In many cases the annual cost of re-keying a facility alone will justify the ROI of an electronic access control system.

Track and Deter Access

One of the advantages of an electronic access control system is the ability to document and report access activity. Most small single door applications have reporting available either through a printer or through web-based access that shows an audit trail of door access activity. Mid-range and large-scale systems can provide in depth, user-defined reporting of access activity. This is a critical component to the access system because it helps you to quickly understand who had access to critical areas of your business before and after an incident.

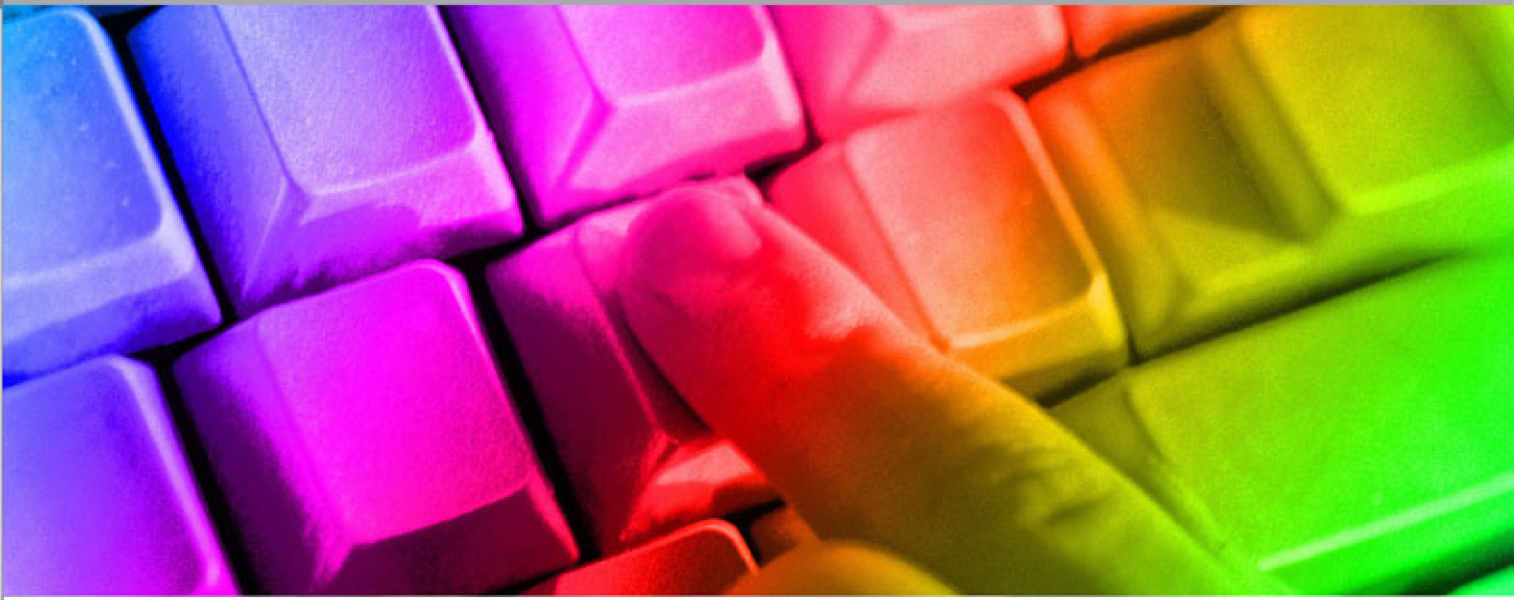
Visual Verification

Access systems are often designed so that visitors, temporary employees, contractors and regular full time employees wear different color badges. Additionally, badging systems frequently use a photo of the employee in conjunction with their access card. Photo I.D.s on an access card help building occupants know the card user is the person to whom it was issued. Policy then dictates that these cards are worn above the waist on all individuals for instant visual verification of everyone in the building.



What is Access Management?

Software Guards for Integrating Applications



Introduction

Access management is a simple concept. Every business has information that needs to be protected from unauthorized disclosure. To protect information, companies define policies that govern who can access specific classes of business and/or personal information. For example, if a manager seeks to access the salary of a subordinate, they should have authorization to do so, however, they should not be authorized to access the same information about a chief executive. That is, there is a policy that specifically governs the release of an employee's salary. Or is there? The answer is: "Probably not." What exists is a written policy related to disclosure of proprietary business information (and perhaps even a separate policy related to disclosure of employee personal information). Because human beings are skilled at generalizations, we expect someone in authority to be able to classify the request for salary information and make a decision. Access Management software has a simple goal. It allows the human who previously acted as a guardian of sensitive information to be removed from the process without loss of access control. This sounds simple, but most businesses are struggling with the implementation of access management as they integrate and extend their applications. This is because machines cannot classify information or make access decisions unless they are explicitly programmed with algorithms to accomplish this. When you take the responsibility for access decisions away from human beings, it becomes necessary to insert software guards into your applications.

A costly problem lurks: The access policy used by software guards is often coded directly into the business application (typically requiring new database tables and/or directory infrastructure). When access policy or audit requirements change, application software must be modified, tested and redeployed. Additionally, when access policy needs to be examined or applications audited for conformance a code review is required.

A service-oriented solution emerges: Access Management solutions, as defined by this paper, provide an alternative to the costly embedding of access policy. They allow application software guards to leverage services that enable access policy to be modified, tested and deployed dynamically without application code changes. This enables your developers to concentrate on providing business software. Access management solutions efficiently enable high performance access controls in distributed environments while allowing centralized management of access policy. An Access Management solution includes programming interfaces (APIs), policy management tools and auditing capabilities.

As part of your quest for an access management strategy, consider the following questions:

1. Who should be responsible for access policy?
2. What kind of access policy do you require?
3. What resources do you need to protect?
4. How do I plug in the access management solution?

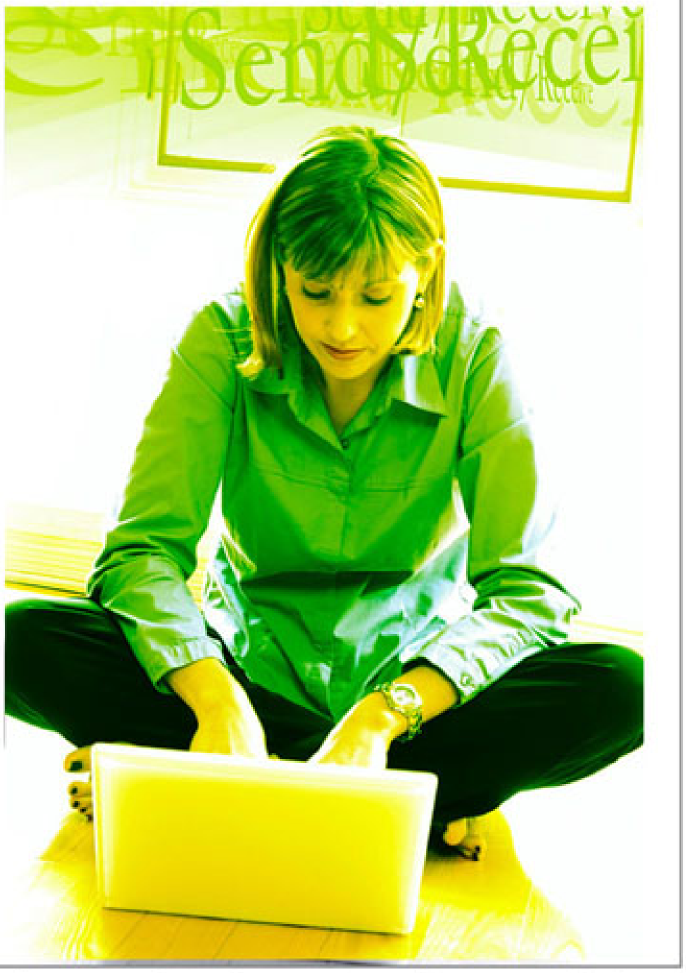
This paper describes a systematic approach to managing the complexity associated with software access management. It outlines a service-oriented architecture that maintains a clean separation of concerns between application domain functionality and access management. We hope this paper will help you define what access management means to your organization.

Why has Access Management become an Application Issue?

Often, individuals are granted access to business applications using operating system, database and/or network "access control" mechanisms. That is, the application has no responsibility for access management; application access is controlled by the runtime infrastructure. Increasingly, however, existing applications are being integrated and/or extended to an expanded base of end-users by leveraging technologies that bypass or tunnel through operating system and network security. These modernized applications not only steward business and personal information, they also span technology boundaries (e.g. the Web, J2EE, JMS, CORBA, RDBMS). It may be impossible for existing security infrastructure (not designed for multi-tier access) to maintain and communicate the identity of the user through each technical tier, making it impossible to leverage existing identity-based access control mechanisms. In fact, emerging identity management standards only address sharing identity in the e-business (i.e. "Web" technology) domain. Integrated business applications, however, are increasingly being held responsible for user and access management in service-oriented architectures that span technology boundaries to deliver functionality.

Unfortunately, when an application development group goes to their security organization for assistance (or advice) regarding the protection of business information or application features, they will likely be told: "Our security infrastructure will not help you with these issues – those are application business rules." This is because the focus of security infrastructure (and associated security organizations) has been on protecting networks and operating systems, not applications. This is understandable. Overwhelmed with attacks on their networks, corporate security groups have no resources available to assist with deployment of a security infrastructure for application-level security (often characterized as fine-grain access control).

Application security, therefore, must address any security-related requirements not provided by the runtime security infrastructure. In the areas of access management, any requirement to restrict the a) usage of application features or b) access to business and personal information is part of "application security."



Who should be responsible for access policy?

To implement an application access management solution, you must ensure that access policies exist and are unambiguous. Although access controls will be enforced by technology, defining access policy is the responsibility of the business. For this reason, access policy related to release of sensitive information and/or application features should be documented using business terminology. During the analysis of these business requirements, concise rules will be defined governing who has access to specific classes of business or personal information and under what circumstances (there may also be rules regarding who can access application features). This analysis often requires a significant classification effort in three areas: 1) information, 2) application features and 3) people. Many companies already have an information protection group tasked with ensuring that business policies are in place to ensure the protection of business and personal information. Such an organization can play an important role in ensuring that access policy is consistent across business applications. If each application group does this classification independently, inconsistencies in policy may occur.

But can an internal organization define access policy? Increasingly the answer is no. Legislation regarding confidentiality and privacy requires that individuals be allowed to define who (and under what circumstances) personal information is released. This adds new requirements for business applications in the area of access management. The users have become policy administrators with respect to access to personal information. While the application may restrict the policy choices, it must be able to dynamically change the policy in use.

It's obvious that this issue exists in healthcare, but other domains are seeing this trend toward individuals as access policy administrators. For example, in telecommunications, newer cell phones have a GPS embedded. This means that it is possible to very concisely locate the cell phone. This is a useful and desired feature in an emergency situation. It's easy to imagine parents wanting to be able to track their children using this feature, but what if a stalker has access to this information? It's clear that access management must be part of any application that supports location-based telecommunications products.

What kind of access policy do you need?

Access Policy can be very simple or very sophisticated. Once it has been determined that applications require access management features, they typically begin with very simple access control policy based on user identity. There are many applications, however, that require sophisticated access policy. To determine your requirements for access management solutions, you should determine the type of access policy that you require.

Access Policy can be classified as follows:

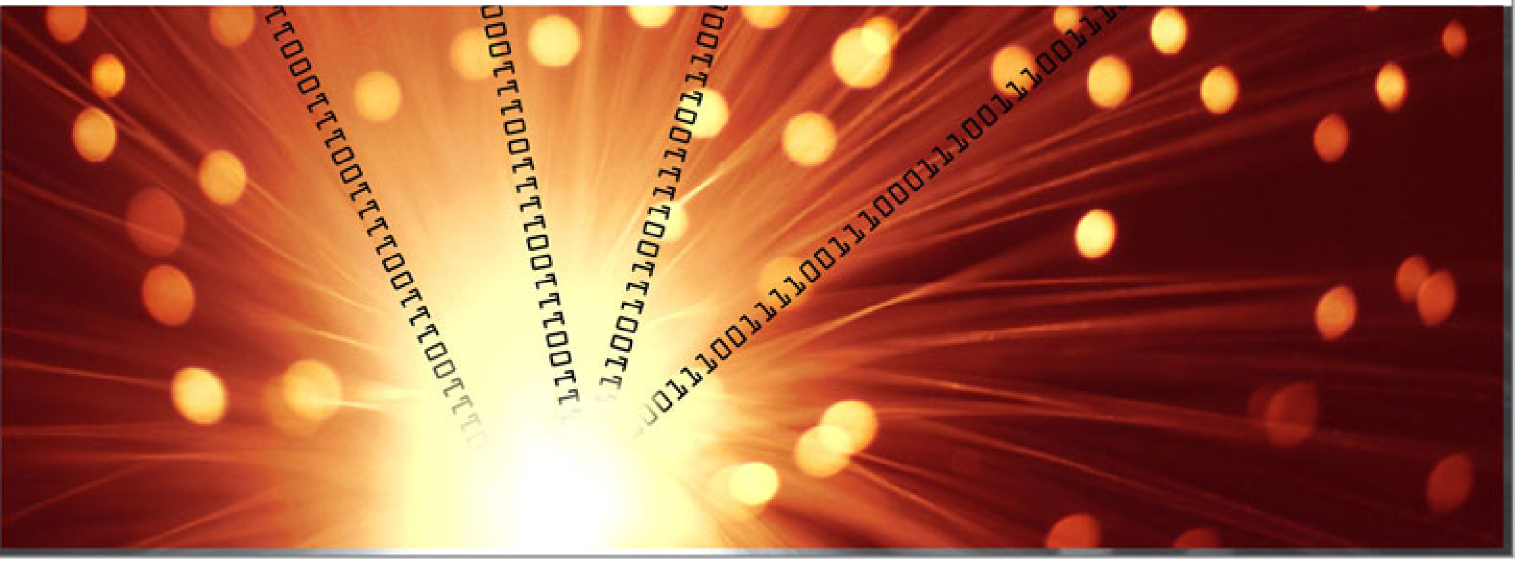
Policy Type	Question answered with regard to protected resource (information or application feature)	Example(s)
Identity-Based	Are you an individual that has been specifically granted access?	User ID / Password, Private Key, Electronic Token, Biometrics
Roled-Based	Are you currently in a role that has been specifically granted access?	Manager, Emergency Room Personnel
Group-Based	Are you part of a group that has been specifically granted access?	Accounting, Engineering
Context-Based	Is the context of the request such that access should be granted to this individual?	Time of Day, Location, Emergency, Account Balance
Entitlement-Based	Is this individual entitled to access this class of information?	Clearance Level
Relationship-Based	Is this individual entitled to access the personal/business information because of a relationship with the person or business?	Primary Care Physician, Manager of Employee, Account Representative, Parent
Rule-Based	Does the policy governing access to the resource allow this individual to access the resource?	Combination(s) of above

What do you need to protect?

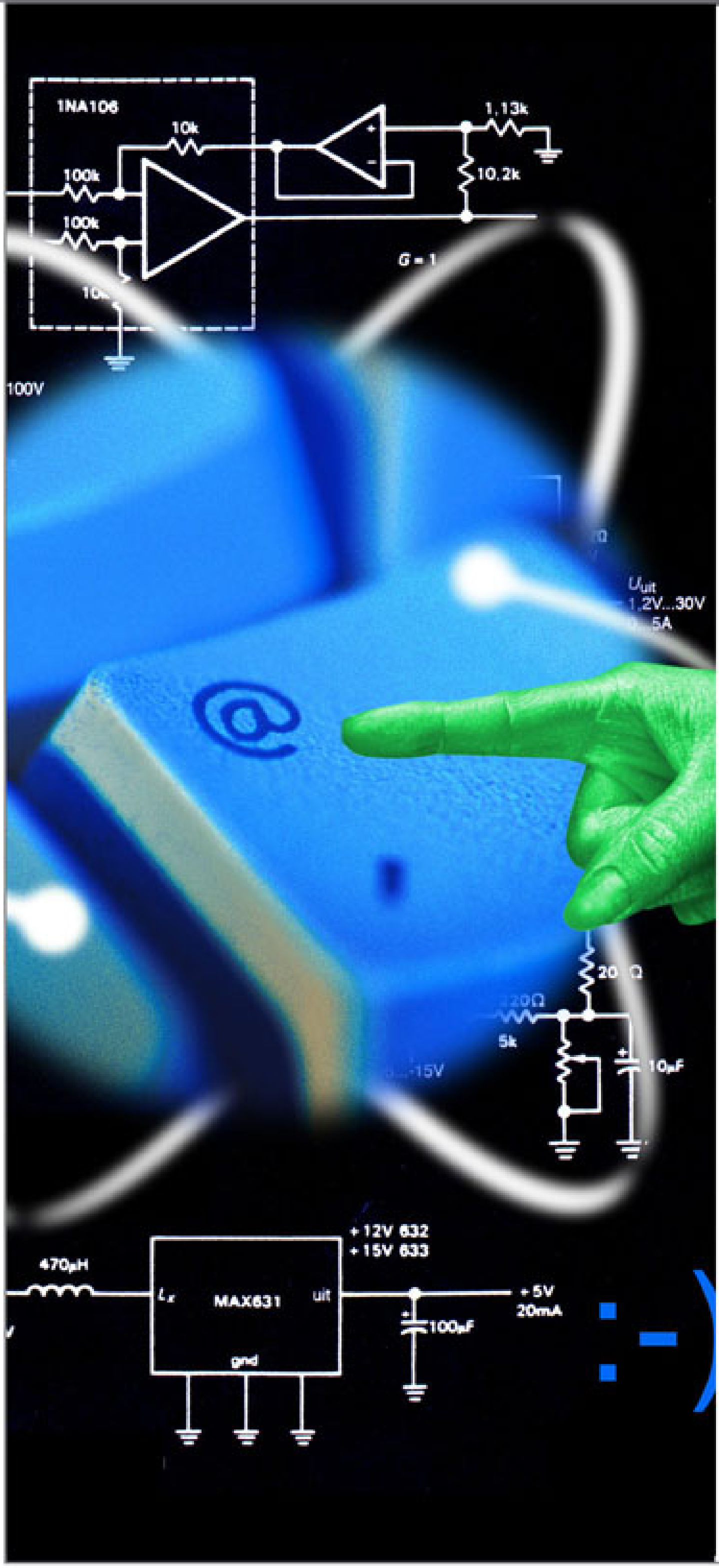
Traditionally, machines and networks have been the resources we protect. However, as we integrate our applications and expand the use of systems, we have seen that the application assumes the responsibilities for guarding access to business information and/or application functionality. The security community uses the generic term resource when discussing business information or concepts that need to be protected. Protected resources are typically given a unique name (or ID) that is used in communicating with an access manager to request an access decision. Deciding what resources should be protected and assigning them an ID sounds simple – and sometimes it is – but it can also become a time-consuming identification and data classification project not considered in the original application estimates.

For example, most companies deploying a human resources application would agree that an employee's salary should be protected. So far, so good. Now, let's assume that from a technical perspective, salary is a field in an employee record that resides in a database that exists on a server accessible via an application that supports remote client access via a network. Where do I insert the software guard, and what is the actual resource it must protect to ensure salary is not accessed improperly?

Granularity of Protected Resource	Access Policy that protects salary
Machine and/or network	Only people with the authority to run the HR application have User IDs on the machines where the HR application is installed.
Entire Application	Only people with the authority to view HR information are granted User IDs for the human resources application.
Speciic Application Feature (e.g. Screen, Menu, Button, or URL...)	Only people with the authority to view HR information will be allowed to request salary information from the HR application.
Entire Database	Only people with the authority to view HR information have User IDs in the human resources database. The database is accessed using requestors' ID.
Table (in a database)	Only managers can view employee records.
Row (in a table in a database)	Only the employee and people in the chain of mangement for an employee have the authority to view and employee's record.
Field (in a Row in a table in a database)	Only the employee and people in the chain of management for an employee have the authority to view an employee's salary.
Concept (information that contains multiple fields - potentially from different sources)	Only managers have access to employee's compensation information (compensation information is a classiication or concept that includes salary, commission and bonus).



Security Access Control Systems for Data Centre Applications



Data security and privacy are of primary concern not only to institutions such as the government, major banks, healthcare facilities and universities, but to companies of all sizes around the world. The growing popularity of physical and logical security convergence reinforce the adage that if a bad guy has unrestricted physical access to your computer, it's not your computer anymore. They also underscore the risks associated with a haphazard approach for enterprises joining both types of protection.

If physical access to a computer system can be achieved, gaining logical access to the information on that computer system is guaranteed. An attacker can use either electronic or physical means to gain access to information so the two disciplines must work together to help the organization manage risk.

Data center systems are protected by firewalls on the network, antivirus software on the servers, intrusion detection, etc. Therefore, the room should also physically secured from unauthorized access as well as being protected with fire suppression, climate control and power systems. Providing physical protection of computer systems has been the extent of the integration of physical and logical security. Completely separate reporting structures and a lack of overlapping knowledge for physical and IT security staff in many companies will take some effort to overcome.

The information nerve center of an organization should have high-end protection — using technologies such as biometrics and smart cards.

With information technology (IT) and related data practically controlling the way business is conducted today, protecting these systems and information is absolutely mission-critical. Any event, even a small one, can affect an entire operation, interrupt business and cost thousands, possibly millions, of dollars.
In general, most companies tend to focus on securing the perimeter, parking lot, lobby, loading dock or elevators on site before ever thinking about a core function within their organization — the data center and IT infrastructure.

Beyond security of the information systems themselves, the physical security of data centers and data closets is a serious function. Would the interruption of mission-critical systems be a cause for concern? The answer is most definitely "yes." Yet many companies still leave their data centers open to the general building population, thereby increasing their vulnerability.

Advertising should also be left to the main offices and branches. Large lighted letters of the organization's name along with the words "Data Center" on the side of a building are unacceptable. That's like painting a bull's eye on your organization. Making the data center as nondescript as possible with landscaping to shield perimeter fencing. Although keeping a low profile is a key checkpoint, always-manned guardhouses are located at each entryway through the fence. Inside any of the guarded entrances, digital surveillance cameras monitor all areas outside of the building. Video feeds can be monitored from both on-site and off-site locations. During non-business hours, infrared motion detectors for building entrances are enabled, and physical access is restricted to specific personnel.

Technologies To Consider

Biometric solutions are the technologies of choice for areas in need of the highest security. For a basic data center or data closet where network equipment or servers may be located, informed use and higher levels of protection are clearly needed.

Biometric systems use unique physical or behavioral characteristics to identify or authenticate one's identity. Biometric identification systems can range from several identifiers including:

→ Fingerprints

The most widespread biometric, fingerprint technology uses optical images or electronic field imaging to verify identity by pattern-matching, fringe patterns or ultrasonic methods.

→ Hand geometry

Looking at the length, thickness, bone structure, curves and distance between the joints of the hand, hand geometry readers compare and verify the data to an enrolled measurement.

→ Facial recognition

Using features of the face such as the location and position of the nose, outlines of the eyes, or areas of the cheekbones and mouth, facial recognition systems analyze the data and compare it to facial templates on a smart card or to database template files to achieve identification and verification.

→ Iris

Iris scanning uses the unique characteristics of the iris. An infrared imager illuminates the eye and captures a high-resolution picture. The data is converted to an algorithm, which maps the iris's distinct patterns and characteristics.

BEYOND BIOMETRICS

When creating a comprehensive, effective data center security plan, there are at least two other types of identification for authentication that should be considered:

- something you know — a PIN, password, or personal information (such as a user's mother's maiden name); and
- something you have — an ID card, smart card, driver's license, or company badge or credential

Biometrics may be insufficient as the sole form of identification when protecting a core security target. For data centers and technology infrastructures, pairing a biometric with another identification process ensures a better protected environment.

When considering options for a second acceptable form of identification, users should consider incorporating smart card technology. In general, a smart card is a plastic card embedded with a computer chip that stores data for transaction between users and systems. This data is associated with either value or information or both, and is stored and processed within the card's chip, either a memory or microprocessor chip. Smart cards come in a variety of formats and capabilities and include contact, contactless, or hybrid versions.

In the following case study, a hybrid card is used to demonstrate the versatility of the card, with its contactless capabilities for access control, and contact capabilities for secured computing.

THE GOAL: SECURE AND

For this example, a combination of a card, PIN and biometric is being used for both physical access and logical access to the data centers and server administration, and for access to mission-critical systems or information from the desktops.
To achieve positive identification, smart card readers with keypad and fingerprint technology for access control were incorporated in the data centers and data closets.

Next, all keyboards were replaced with security keyboards with smart card slots and fingerprint readers built-in for all servers and workstations with access to mission-critical systems and data. Because physical access control used contactless smart cards and the keyboards used contact smart chips, the users of these systems were upgraded to a hybrid card with increased memory to handle the biometric template stored on the card.

To achieve informed use and the ability to respond to both physical and logical violations, a middleware application was used to integrate the logical security application into an integrated security management system (ISMS) running in the access control platform. This set-up provides the capability to provide pop-up video associated with a data center or data closet entry/exit in the case of a denied access. It also generates an alarm for a denied logical access for a server or workstation, so security can respond accordingly. The ISMS also achieves a single reporting tool to see who accessed the data center and what data or information was accessed. In this way, security officers do not only respond to a physical security event, but they also can respond to logical violations. These capabilities give the organization peace-of-mind protection and total informed use of facility, data and information.

The combination engineering and using the latest design methodologies including zoned cooling, hot aisle / cold aisle enforcement, zoned fire suppression utilizing clean agents, and redundant power supply shall offer the most current best practices in data center design and management.

Recognizing the importance of physical security as well as network security, data center and office facilities designs are to be as secure as possible against unauthorized access, theft, fire and other physical threats. Monitoring the physical security of data centers and offices 24/7 via biometric technologies, CCTV and physical alarm systems.

Physical Security

Physical security is the first ring in the layered security approach. Without stringent physical security measures, additional network and data security is marginal at best. Data centers and office facilities are to be as secure as possible against unauthorized access, theft, fire and other physical threats. Monitoring the physical security of data centers and offices 24/7 via biometric technologies, CCTV and physical alarm systems;

Biometric Access Control

Biometric technology is used to restrict physical access not only to the datacenter but to offices, NOC, labs or staging areas that may be located in the vicinity. This insures that only authorized personnel are allowed into the building and each employee only has access to the areas they require.

At each security zone, a two stage authentication may be implemented, meaning not only a physical trait is required but also a known passcode. In this way a guarantee that the person entering the security zone is who they should be.

INFORMED USE

Reinforced Entry Points

At every datacenter and building entry point the most secured welded door frames, security glass and reinforced walls and ceilings should be used. This insures anyone entering the facility or accessing the server can not bypass physical security measures such as biometrics, passcodes, CCTV systems, and keyed entry.

After passing through all security access points that require biometrics and passcodes, a requirement should be incorporated that authorized personnel are to sign out keys required for each and every individually keyed steel cabinet and rack. All cabinets shall be fully secured and separate from each other.

CCTV Monitoring

The entire building and datacenter should be closely monitored by using the latest technology CCTV camera systems available today. These systems should incorporate a combination of fixed point and PTZ cameras so that all points are monitored and all areas are recorded. It is ideal that the cameras used are all low light or night vision cameras that capture all traffic that pass into and out of the building, datacenter and all other security zones.

This CCTV system must be isolated on a totally separate network that is backed up by a fully redundant power system. The data that these cameras record may be are stored for a minimum of three to twelve months.

Practical Strategies to *ACCELERATE* Business Applications

In Malaysia, more business than ever is done in local branch offices and remote sites, but fewer and fewer IT resources are hosted there. Applications are being consolidated--sometimes centralized, sometimes outsourced.

In many cases, a consolidated application translates to a poorly performing application. Long distances between users and applications, skinny/latency-prone network pipes, and applications and protocols stretched beyond their design limits mean poor application performance at remote sites.

These issues are exacerbated by the introduction of additional bandwidth-hungry, latency-sensitive applications such as voice-over-IP (VoIP) and video.

The industry response is predictable – accelerate the traffic. While appropriate at a high level, the rush to a solution has left out some important questions – e.g., should everything be accelerated? If not, which applications are key? What about encryption?

Acceleration technologies range from compression to caching, to bandwidth management and protocol optimization. All of these techniques have benefits, but for a given application, some improve performance more then others.

Enterprises need all of the techniques mentioned above for the array of applications deemed important to the business (file services, e-mail, web, secure web, video)– but what about the countless "applications" that run on the enterprise network that are not business-related, or worse – harmful to the business?

Given that 30% of enterprise network bandwidth is consumed by unauthorized applications (web advertisements, inappropriate web surfing, P2P, Skype, spyware, etc.), removing the undesirable can be as important as accelerating the desirable.

Enterprises Have Options

Organizations have several options to address these issues. First, they can upgrade their WAN circuits to higher-bandwidth links which is rather expensive or they can choose to ignore these performance issues – resulting in employee dissatisfaction, and more importantly, broken applications, impeded business processes.

There is another option: accelerate the traffic. Not surprisingly, this is the option many organizations are now examining. Acceleration techniques available include bandwidth management/traffic shaping, compression, protocol optimization, byte caching/dictionary compression, and object caching.

Bandwidth Management/ Traffic Shaping

This technique assigns a priority to a particular application's (or user's) traffic. This priority has an effect both on the order the traffic is sent in, and in the amount of bandwidth the traffic is afforded. While this technique doesn't make traffic go any faster on the network, it does ensure that the network is available first for the highest priority traffic.

Protocol Optimization

Protocol optimization takes protocols that are inefficient over the WAN (e.g., CIFS, MAPI, HTTP, TCP, HTTPS) and makes them more efficient – typically by parallelizing traditionally serialized communications. There are other optimizations, depending on the protocol (e.g., TCP session reuse) that can make starting up/tearing down flows faster. These optimizations do not reduce the amount of bandwidth an application consumes, but can greatly accelerate applications (i.e., reduce latency) – the longer the WAN link, the greater the improvement.

Byte Caching/Dictionary Compression

Byte caching is as it sounds – a low-level cache of small, sub-application-object pieces of information. Typically, byte caching/dictionary compression schemes observe repetitive patterns moving between two caches in application traffic, symbolize those patterns with a token, and send the token in lieu of the bulky traffic – tokens being typically a byte or two, symbolizing large blocks (e.g., 64KB). The cache on the far end matches the token with the original block of data, reconstitutes the traffic, and sends it on to the application or user (whichever is appropriate). Byte caching/dictionary compression is typically not application-specific, and operates at a lower level, reducing bandwidth of all TCP traffic.

Object Caching

Object caching is very different than byte caching – in that it is protocol/application specific, and is an all-or-nothing affair. If the cache contains the object, the user is served the object from a local store – extremely quickly. Object caching, on a "cache hit" (which is where the object has been through the cache and then stored) reduces greatly the bandwidth used, and the latency – both to almost zero. If the cache does not contain the object (or contains an outdated version of the object), then for that particular transaction, object caching does nothing (although the next time that object is requested, it will be fast).

Compression

Compression uses a common compression algorithm (e.g., gzip, lz compression) to remove extraneous/predictable information from the traffic before it is transmitted. The information is reconstituted at the destination based on that same algorithm. It is important to note that there is no synchronization between the two ends – and the first time something goes through is just as fast as the second. This technique reduces the data transmitted over the WAN link, but has limitations on how much bandwidth reduction it can achieve by itself – and has minimal impact on latency.

Enterprise Application Acceleration Evaluation Criteria

Organizations should have a strategy for evaluating different acceleration approaches and techniques. Overall, enterprises should first prioritize applications needing acceleration.

Second, organizations should examine each application (and its parent initiative) in detail, to assess the faults within that application, understand the best acceleration techniques for that application, and how to best bring those techniques to bear.

Third, organizations should examine the trends, both in the application mix (e.g., web, in-house vs. third party hosted, HTTPS), and in networking architecture.

Fourth, organizations should establish non-application specific overall solution criteria – deployability, manageability, reliability, and solution breadth/extensibility. Briefly, an enterprise set of criteria might look like this:

Enterprise Application-specific Criteria

- Application/protocol – File services, e-mail, e-learning/multimedia, web, secure/encrypted web, in-house or hosted – does it support the enterprise's key applications?
- Does the solution address the application(s) specific problem – network capacity and/or latency?
- Does the solution support all of the appropriate techniques for that application – bandwidth management, protocol optimization, object caching, byte caching, compression – and does it understand the application well enough to ignore inappropriate acceleration techniques?

Enterprise Solution Criteria

- Solution scalability – does the solution scale down (are there appropriate form factors for small sites) as well as up (are there form factors for very large sites)? What about centralized management?
- Solution breadth/adaptability – does the solution support all key applications? Does the solution require additional components be rolled out to remote sites?
- Solution Investment Protection – when the enterprise rolls out new applications, will the solution accelerate it? Prioritize and optimize it? When the network changes, is the solution still effective?

Conclusion

In summary, organizations must examine all of their key applications when evaluating application acceleration solutions- file services, e-mail, streaming/video, web, and secure web. Furthermore, organizations should look ahead – to what applications are coming, and how networks are evolving – given the large-scale nature of deploying remote office acceleration capabilities.

Business Continuity

Organizations in Malaysia are not altogether spared from natural catastrophic calamities which are capable of disrupting operations, resulting in loss of productivity, revenue, and potentially a loss of professional repute. The impact can be massive and severely damaging.

The recent earthquake in Taiwan is a case in point. It crippled internet connections in several Asian countries including Malaysia. Malaysians were puzzled as to the inability to access to the internet,

However, the eventual announcement by local ISPs and NISER confirmed that the earthquake off the Taiwan's Southern coast had damaged undersea cables, cutting off phones and Internet services on Wednesday to parts of China, South Korea, Japan, Southeast Asia and the United States.

When information exchanges are brought to a standstill, users are now made aware on how dependent their work and lives are to internet. We now realize how interdependent Malaysian internet connections are to the undersea cables in Taiwan. Although internet connection speed has gradually improved, the need for backup solutions to minimize impact of such events has to be in place to ensure business continuity.

Our dependencies to technologies are fast, turning them into our single point of failure.

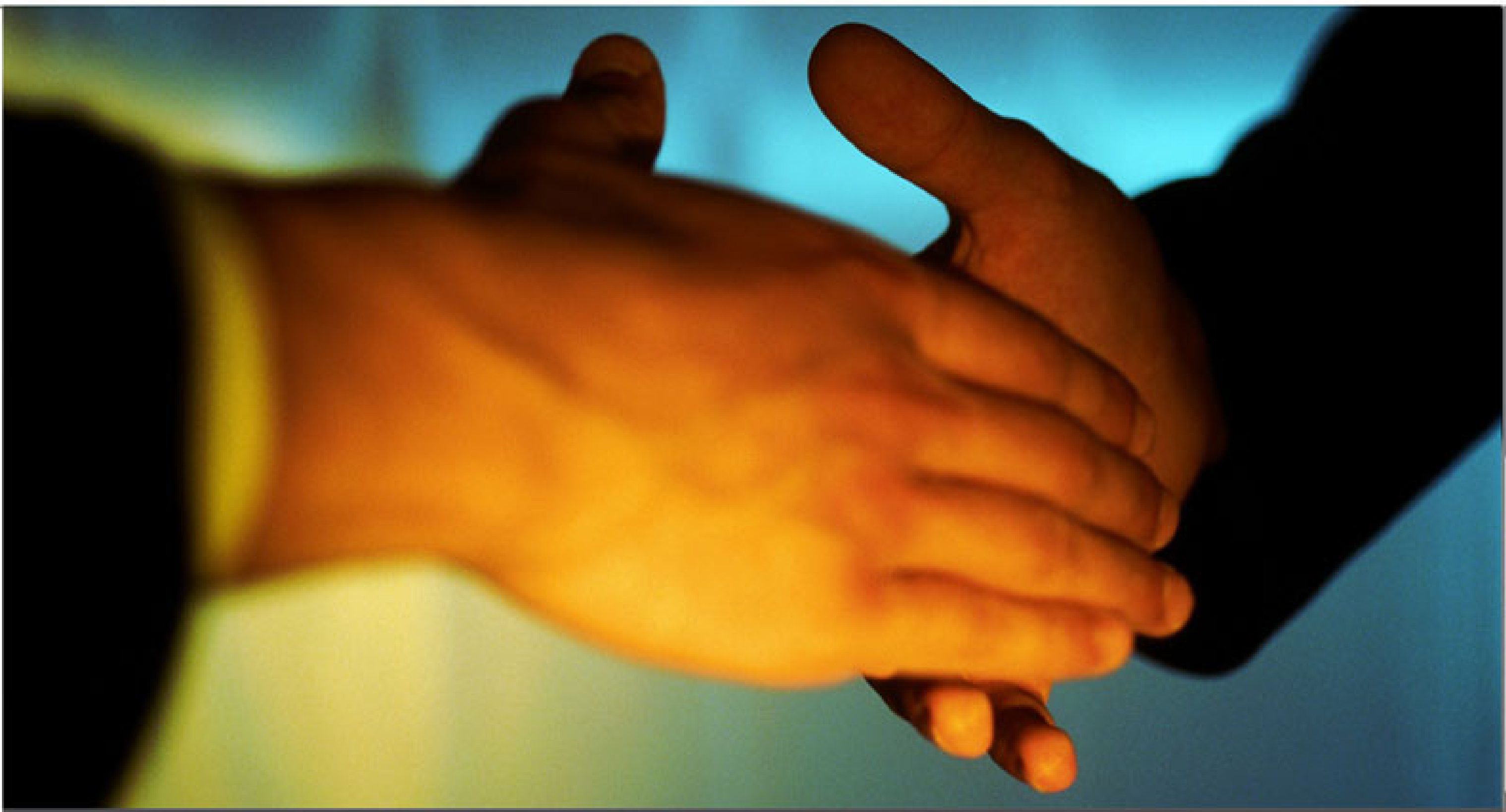
Without any proper and tested Business Continuity Plan we are putting our business and even lives at risks.

During Risk assessment exercise, all probable threats, vulnerabilities and risks should be taken into account. Threats either internal or external should be considered when drafting a Business Continuity Plan. No threat is far too big, small or outrageous to be included. Based on such assessments, can we then determine the magnitude of the impacts to be a mere disruption, or has it escalated into a full blown crisis?

Threats can be divided into 2 categories, namely: - natural threats and man made threats. Earthquake, tsunami, floods, hurricanes are all examples of natural threats. While terrorism, war, riots and threats induced by humans, are considered man made threats,

Business Continuity Plans are not just designed for service providers, by right; they should have already one installed. These plans are not just for larger companies but should be for every business entity. . From straightforward plans such as for evacuation during fire threats to more extensive which might include a recovery site involving SLAs with vendors.

Business Continuity Planning comprises, of several process, for it in order to be holistic. The most important part in Business Continuity Planning is first, having the support of the Top Management. Business Continuity



Planning for All

Planners must obtain the support by highlighting the importance and the risks that the organization will face, if there are no such plan is in place. This step is crucial in order to ensure that adequate resources are allocated for Business Continuity Planning activities. Next, a Business Continuity Policy must also be established in organizations and be made known of its existence to employees. The policy should cover the role and responsibility of employees with regards to business continuity.

Another factor is Risk Assessment and Analysis and Business Impact Analysis. These 2 activities will determine the importance of business functions, the risk and how it will affect the organizations if a main component of the business fails.

Developing Business Continuity Strategies is also an integral part of Business Continuity Plan. This is where Business Continuity Planners will select appropriate strategies for continuity and recovery of business processes, critical functions and operations. The strategies will cover steps that will be invoked in time of crisis and how to reduce and mitigate the risk. It will also outline the role and responsibilities of all employees within the strategy.

No strategies are of use unless being tested. Business Continuity Plan has to be tested in order to determine how effective these strategies are implemented. It brings along real life simulation exercise in order to access how employees react during crisis, and how well the continuity and recovery steps work.

In order to meet the dynamics of change in business, the Business Continuity Plan has to be constantly updated, tested and employee must be informed and made aware of such updates. Any new threat must be included along with their mitigation and recovery steps.

However, having successfully designed and implement a Business Continuity Plan is just half the work done. Besides, the duty of protecting stakeholders' interests, the BCP should be treated as an on-going program, a process to safe guard the workplace and the continuity of future business.

Mitigating On-line Identity Theft

Cases of identity theft were growing over the past few years. The Identity Theft New Survey and Trend Report conducted by the Privacy and American Business together with Harris Interactive reported that 38% or between 13-14 millions adults Americans were victims of identity theft between January 2001 until mid-May 2003 [1]. During the same period, the victims have lost approximately USD$3.8 billion to pay for the fraud cases resulting from the identity theft.

NISER (www.niser.org.my) through its arm, the Malaysian Computer Emergency Response Team (MyCERT) classifies the incidents on identity theft as part of forgery. MyCERT 2005 Annual Report showed a tremendous increase on identity theft, 106 cases in year 2004 compared to 149 cases in year 2005. The number of forgery cases in Malaysia was less than 30 for each year between 1998 and 2003 [2].

Even the number of identity theft cases is not serious compared to the US, Malaysians still need to take precaution action because identity theft is a crime that can have substantial financial impact. Techniques in identity theft

There are many techniques for the thieves to obtain and steal information of a person's identity even if he or she never uses a computer. The techniques can be in the form of conventional method such as shoulder surfing, dumpster diving (searching through your trash), overhearing a phone conversation and stealing credit card numbers in handbags. Computer or laptop theft is also one method of identity theft through conventional method where the thieves will copy information from the database in hard disk.

Advances in computer technology and the Internet have made it possible for detailed information about people to be compiled and shared more easily than ever. Personal information becomes more accessible and information about an individual can be obtained without knowledge. They may use sophisticated techniques such as hacking and copying database in servers, eavesdropping on the network, and phishing.

Trend Micro reported that the vast majority of threats in 2005 were inspired by financial gain [3]. "Spy-phishing" is a new kind of attack which adapts both the phishing scams and pharming along with some new tricks. Spy-phishing target online banking and financial institutions that use password-driven in their authentication processes. According to Trend Micro, a Trojan, or a link to download the Trojan is included in the email messages. Upon downloaded and executed the Trojan either manually or automatically through an exploited vulnerability, this malware monitors web traffic until it detects web access to the target page. When this happens, it sends any login or confidential data back to the attacker. Another way the spy-phishing works is fake the authentic online bank page. When the user are willingly to logs in and once they enter his information, the users will proceed to the intended site without interruption, so there is no unusual behavior that may alert them to a potential problem. The only difference is that the users' information has been diverted to a third party, who is now empowered to use the same to conduct illicit activities.

How to avoid being a victim?

Below are some suggestions on how to minimize risk from identity theft:

- Before providing any on-line personal information, make sure that you do your business transactions with a legitimate company. You should verify the legitimacy of the company you are dealing with before supplying any information. Some attackers may create a malicious website and appear to be legitimate.

- Take advantage of security features such as passwords and other security features to add layers of protection. Other layers of protection are using token such as smart card and biometrics recognition such as finger print and iris recognition.

- Please take extra precautions when providing information on-line by checking the privacy policy of the website you are dealing with. You need to check on how the company will use or distribute your information. There may be a hidden policy that allows the company to share your information with other companies.

- Protect yourself against viruses, worms, Trojan horses and malware by using license anti-virus software. The unlicensed anti-virus software is not able to keep updated your virus signatures. The consequence is that your computer maybe affected with malicious codes and they may steal or modify the data on your computer.

Conclusion

Creating a secure and safe environment that can promote online transactions is something that will bring benefits to society in general. Identity theft is one of the information security threats we need to look into seriously because it is a crime that can have substantial financial consequences, not only to the victim but also to the country.

References

- Privacy & American Business. 2003. Identity Theft New Survey & Trend Report.
<http://www.bbbonline.org/idtheft/IDTheftSrvyAug03.pdf>

- MyCERT. 2006. MyCERT 2005 Annual Report.
< http://www.mycert.org.my >

- Yaneza, J.L.J.A. & Sancho, D. 2006. The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast.
< http://www.trendmicro.com >