

Editor

Philip Victor
Training & Outreach Unit, NISER

Contributors :

- ~ **Worms and Trojans Go Mobile**
- By *Shaharudin Ismail & Zahri Yunos*
shahar@niser.org.my
zahri@niser.org.my 5
- ~ **Internet Content Filtering**
- By *Aswami Fadillah*
aswami@niser.org.my 7
- ~ **Guideline To Safe Web Browsing**
- By *Kamalrul Hasnooh & Sharifah Roziah*
kamalrul@niser.org.my
roziah@niser.org.my 10
- ~ **Protect Your Organisation - Adopt an Effective Risk Management Approach**
- By *Shamsuddin Abdul Jalil*
ssuddin@niser.org.my 15
- ~ **Keeping Kids Safe Online**
- By *Zahri Yunos & Sharifah Sajidah*
zahri@niser.org.my
sajidah@niser.org.my 16
- ~ **Tips on Protecting Your Personal Computer - Part 2**
- By *Nahzatulshima Zainuddin*
nahzatul@niser.org.my 17
- ~ **ISMS Implementation: Examining Roles and Responsibilities**
- By *Rafidah Abdul Hamid*
rafidah@niser.org.my 19
- ~ **Security Events** 20

From the Editor's Desk

Another great quarter has gone by and we bring you new exciting articles. The last quarter saw the e-Secure Malaysia 2005 Conference & Exhibition event held at PWTC from the 28th September – 1st October 2005 successfully ran.

During the event, concurrently running was the MyCrypt 2005 which had international participation and speakers. Malaysia hosted this event for the first time and it was successful.

Another event was the 1-day CISSP Boot Camp that was held on the last day of the conference. Conducted by Kang Meng Chow, an ISC² certified instructor, we had an astounding 25 participants attended. For those wanting to sit for the exam, our next CISSP exam is on the 3rd December 2005. For more details, please visit <http://www.niser.org.my/cissp>

All in all, being held for the very first time, the e-Secure Malaysia 2005 Conference & Exhibition was a great success and I guess we'll be looking forward for 2006 for an even bigger one.

Once again, I would like to thank all our contributors and welcome new contributors to our newsletter. Before signing off, on behalf of NISER, we would like to wish all our Hindu & Muslim readers a very Happy Deepavali & Selamat Hari Raya Aidil Fitri.

Philip Victor
vphilip@niser.org.my

Reader Enquiry

Training & Outreach Unit
National ICT Security & Emergency Response Centre
MIMOS Berhad
Technology Park Malaysia,
57000 Kuala Lumpur, Malaysia
Tel: 60 3 8657 7042
Fax : 60 3 8996 0827

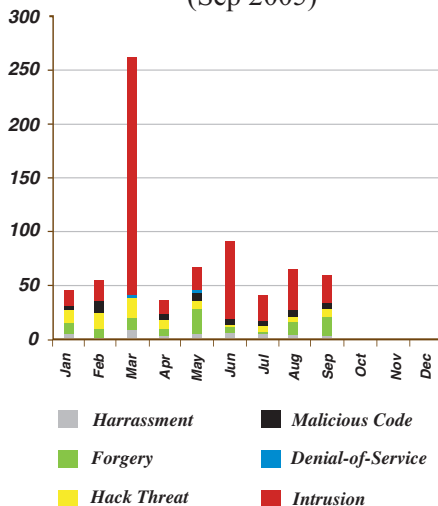
Email: training@niser.org.my

The MyCERT Quarterly Summary is a report, which includes some brief descriptions and analysis of major incidents observed during that period. This report also features highlights on the statistics of attacks and incidents reported, as well as other noteworthy incidents and new vulnerability information.

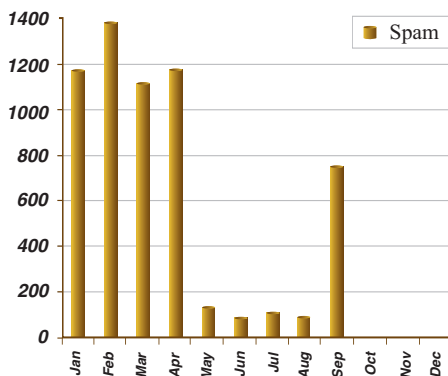
Additionally, this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardenings.

Complete figures and statistics graph on the Abuse Statistic released by MyCERT monthly is as below:

Incident Statistics
(Sep 2005)



Spam Incident Statistics
(Sep 2005)



Recent Activities

The Third Quarter 2005 is less hectic as compared to the previous quarter. There were no significant incidents or surge for this quarter, but we see a drop in all incidents. Generally, there is a 30.3% decrease in the number of incidents in this quarter as compared to the previous quarter. The number of incidents reported for this quarter is 1107 as compared to 1589 in the previous quarter.

Local Machines Compromised to Set Up Foreign Banking Phishing Sites

Forgery incidents continue on though this quarter shows a slight decrease on these activities, with a total of 35 incidents compared to 36 in the previous quarter, which represents a 2.8% decrease. Majority of forgery incidents are phishing activities involving foreign financial institutions. In this quarter, MyCERT received a series of reports from foreign financial organizations and CERTs regarding phishing sites hosted on Malaysian servers.

MyCERT responded to the reports by communicating with the server owners to remove the phishing sites and within 6 hours the sites were removed successfully. Upon analysis, we found that the affected servers were compromised and was used to set up phishing sites. In fact, we found a single server having more than 2 phishing sites belonging to foreign online banking, running on the server.

MyCERT strongly urges users who receive emails purportedly from a bank requesting to change their logon and password to ignore and delete such emails immediately. Users are also advised to refer and verify any such emails with their ISPs, CERTs or with the particular financial institutions mentioned.

In addition, MyCERT also advise organizations to secure and harden their servers to prevent the servers from being compromised and used for malicious purposes, such as running phishing sites.

Malicious Code Incidents on Continuous

The second quarter of 2005 indicates a slight decrease in virus or worm incidents with a total of 16 incidents, which is about 15.8% lower than the previous quarter. This number is relatively low considering that there are new worms and Trojans released to the net. Most of the worm incidents reported involved new variants of mass mailing worms such as the W32.Zotob and Trojan activities. However, this quarter remained peaceful with no significant worm outbreak or severe damages due to worm activities were reported.

MyCERT advise users to always take precaution against worm incidents, even though there are no worm outbreaks

observed within our constituency. Some of the precautions that can be taken are:

- Email Gateway Filtering
Sites are encouraged to apply filters at email gateways to block any attachments associated to the worm.
- System/Host
 - i. Users must make sure that their PCs are installed with anti-virus software and are updated continuously with the latest signature files. Users who do not have an anti-virus installed on their PCs may download an anti-virus from the following site: <http://www.mycert.org.my/anti-virus.htm>
 - ii. Users need to make sure that their PCs or machines are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in PCs or machines.
- Safe Email Practices

MyCERT has strongly advice users not to open any unknown attachments, which they have received via emails. Any suspicious emails shall be deleted or forwarded to the respective ISPs or CERTs for verification. Users may refer to the following guidelines on safe email practices:
http://www.mycert.org.my/faq-safe_email_practices.htm

More New .MY Sites Defaced

Incidents on Intrusion have dropped to 86 for this quarter from 103 in the previous quarter. It represents a 16.5% decrease. Web defacements still remain the top Intrusion incident compared to other Intrusions such as root compromise, with a total of 83 .my websites defaced for this quarter. However, no mass defacements were observed in this quarter.

Our finding indicates that majority of defaced websites for this quarter is from .com.my domains compared to other domains. As was in previous quarters with re-defacements, in this quarter we found more new .my sites being defaced. Thus, we would like to urge System Administrators and Web Administrators to take serious action on securing and hardening their server to prevent re-defacements.

MyCERT would like to advise all System Administrators and owners of systems and networks to upgrade and patch softwares, services and applications they are currently running. In addition, it is also recommended to disable unnecessary or unneeded default services supplied by vendors. Our analysis shows that majority of previous Intrusions such as web defacements were due to vulnerable

and unpatched services running on the server. Web defacements involving Linux machines are due to running of older versions of the Apache servers, PHP scripts and Open SSL. As for IIS web servers, web defacements were commonly due to Microsoft IIS extended Unicode directory traversal vulnerability, Microsoft Frontpage Server Extension vulnerability and WEBDAV vulnerability.

Details of the vulnerabilities and solutions are available at:

1. Apache Web Server Chunk Handling Vulnerability
<http://www.cert.org/advisories/CA-2002-17.html>
2. Vulnerabilities in PHP File upload
<http://www.cert.org/advisories/CA-2002-05.html>
3. Vulnerabilities in SSL/TLS Implementation
<http://www.cert.org/advisories/CA-2003-26.html>
4. WEBDAV Vulnerability
<http://www.cert.org/advisories/CA-2003-09.html>
5. Microsoft IIS extended Unicode directory traversal vulnerability
<http://www.mycert.org.my/advisory/MA-024.042001.html>

Web servers running Windows IIS servers, may use the IIS Lockdown tool to harden their server.

IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers.

The IIS Lockdown tool can be downloaded at:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en>

Web server running on Linux, may use the TCP filtering mechanism such as TCP Wrappers at the server or gateway level. TCP Wrappers is a tool commonly used on UNIX systems to monitor and filter connections to network services.

TCP Wrapper can be downloaded free at:
<http://www.cert.org/security-improvement/implementations/i041.07.html>

Slight Drop in Hack Attempts

Incidents on hack attempts showed a decrease of 5.9% in this quarter. A total of 16 reports were received on hack attempts for this quarter compared to 17 in the previous quarter, which targeted mainly, organizations' systems and networks. Home users PCs are also becoming the attackers target on port scannings. Most of reports on hack attempts were received from foreign complainants on hack attempts originating from Malaysia.

MyCERT's findings for this quarter showed that the top targeted ports for scanning are SMB (TCP/445), SSH (TCP/22), HTTP (TCP/80), MS SQL (TCP/1433), Netbios (TCP/137, TCP/138, TCP/139), which could be possibly due to newly discovered vulnerabilities on those services. Port scannings are actively carried out, using automated or non-automated tools once a new bug or exploit is released to the public. Besides scanning for open ports, scannings are also actively done to detect any machines running vulnerable programs and scripts, such as scanning for Unicode vulnerability on IIS web servers and scanning machines running vulnerable PHP scripts.

MyCERT recommends the following preventive measures:

- All ports or unneeded services should be closed except http services and other required ports or services should be filtered and patched accordingly.
- All machines or systems are properly patched and upgraded with latest patches, service packs and upgrades to fix any vulnerability that may present in the machines or systems.
- Organizations can install network based or host based IDS to alert scannings and other malicious attempts to their hosts.
- Home users are recommended to install personal firewalls in order to alert the owner of any unauthorized scanning to their machine, and to block any penetration into their system.

More information on home PC security is available at:
<http://www.mycert.org.my/homepcsecurity.html>

Significant Drop in Harassment Incidents

Incidents on harassment have decreased to 80%, with 2 reports received for this quarter compared to 10 reports in the previous quarter.

Majority of harassment incidents received, involved harassments committed via emails, chat forums and web forums, where majority of them were referred to the law enforcement agencies for further investigation. MyCERT has also assisted the Law Enforcement Agencies, such as the

police in investigating some harassment incidents.

We are not sure the reason for this significant drop but we advise users who are harassed via Internet or any individuals who observed any kind of harassments via web forums, which has religious, social, political or economic implications to report them to MyCERT for further analysis.

Other Activities

Spam

Spam incidents still remain on top with a total of 952 incidents for this quarter, despite the drop in the number of spam reports we received, with a 32% drop from the previous quarter. The main reason for this significant decrease is because more and more local ISPs are applying anti-spam filter at their gateways to prevent spam emails from dropping into end-users' mailbox. We see this as a positive measure in minimizing and eradicating spam activities in the country.

In addition, end users are also taking measures at their site, by applying appropriate filters at their PCs to minimize spam emails.

Denial of Service

In this quarter, we did not receive any reports on Denial of Service compared to 4 reports in the previous quarter.

Conclusion

Overall, the number of incidents reported to us has dropped more than a quarter compared to the previous quarter. In this quarter, we observed drop in all security incidents too. We hope the drop is due to proper security measures, which are being implemented to prevent incidents rather than saying the drop is due to less hacking activities in this quarter. Spam incidents have dropped more than 30% as a result of preventive measures taken by most ISPs through the application of spam filters at their gateways as well other measures by end users. Generally, no crisis or significant attack or incident was observed for this quarter that has caused severe impact to the constituency as was in the previous quarter. This scenario indicates a less hectic quarter compared to the previous quarter.

Complete figures and statistics graph on the Abuse Statistic released by MyCERT monthly is available at:

<http://www.mycert.org.my/abuse-stat/index.html>

WORMS AND TROJANS GO MOBILE

Nowadays, mobile phones are installed with advanced operating systems such as the Symbian OS, Microsoft Mobile OS and Palm OS. These kinds of mobile phones are also known as smart phones. Smart phones have many great features such as the phone camera for pictures and Quicktime videos, high resolution color screens, wireless data access for laptop, ability to play mp3 files, sending emails and even able to sync calendar and address book wirelessly with the desktop [1]. Smart phones are also equipped with the Bluetooth short-range wireless, WAP and mobile browsers features. These smart phones are considered as tiny computers.

Symbian OS is the advanced, open operating system licensed by the world's leading mobile phone manufacturers such as Nokia, Motorola and Sony Ericsson. It is designed for the specific requirements of advanced 2G, 2.5G and 3G mobile phones. Symbian OS combines the power of an integrated applications environment with mobile telephony, bringing advanced data services to the mass market [2]. Some of the smart phones are Nokia 6600 and 7610 models, Sony P900 and P910, Ericsson Mobile Communications AB and Motorola A925 and 1000.

With those features embedded, will the latest mobile phones or smart phones succumb to security threats like worms or Trojan horses? Security experts and antivirus companies have identified the emergence of new worms or Trojan horses in smart phones such as Cabir, Gavno.a, MetalGear and Skulls.D.

WORMS AND TROJAN HORSES IDENTIFIED

Cabir

Cabir was the first proof-of-concept worm identified. The worm uses the Bluetooth short-range wireless feature in smart phones to infect the phones and to transfer itself to the new host as a package file [3]. F-Secure researchers believe the author of the Cabir worm released the source code of the worm on the Internet as they discovered two more new versions of Cabir worms, namely Cabir.H and Cabir.I. The features in Cabir.H and Cabir.I have been updated and these worms are able to search for and find new targets. These worms are able to spread faster between mobile phones using a specially formatted Symbian Installation System (SIS) file. When infected, the mobile phone's screen displays the word "Caribe". In addition, the worms modify the Symbian OS of the phone so that Cabir is activated each time the phone is turned on [4]. Apart from that, the infected mobile phones will scan for vulnerable phones using the phone's Bluetooth wireless connection and send a file velasco.sis, which contains the worm to those phones. Cabir.H and Cabir.I do not destroy data on the phones they infect but block legitimate Bluetooth wireless connections and rapidly consume the phone's battery.

MetalGear

The smart phones are also vulnerable to Trojan horse threats. Simworks reported that the Trojan horse combines several malicious mobile phone programs that work to spread over Symbian-based phones. The program is a fake version of the game called "Metal Gear Solid", which disable antivirus programs as well as other programs. The program will also install the Cabir worms, which spreads through the Bluetooth short-range wireless protocol [5]. The program installer file, MetalGear.sis should not be opened and installed. If you run the program, it will install Cabir and another installer file, SEXXY.sis [6]. The Cabir worms will be activated and attempt to use Bluetooth to reach other phones. It will also render any already installed anti-virus code to become ineffective. This installer also adds code that disables the handset's Menu button. Figure 1 shows the MetalGear program in the smart phone's menu.



Figure 1 Disguised as a video game, the MetalGear program disables antivirus software on mobile phones and attempts to replicate.

Source: SimWorks

Skull.D

Skulls.D is another identified Trojan horse. Skulls.D has the capability to disable applications, drops the Cabir worm onto phones and informs users they have been infected by displaying a full-screen flashing skull [7]. The image is shown in Figure 2. The latest Skulls Trojan horse comes disguised as a new version of the Macromedia Flash player to fool users of mobile phones. Once users download and install this program, Cabir worm will be activated and overwrite all existing applications [8].



Figure 2 The Skulls Trojan horse changes system icons of the phone menu.

Source : F-Secure

Gavno.a and Gavno.b

The Trojan horse programs namely Gavno.a and Gavno.b, masquerade as patch files designed to trick users into downloading them. The Gavno Trojans were the first to aim at disrupting the telephony, a core function of mobile phones. These Trojan disrupt other applications such as text messaging, e-mail and address books. Gavno a., which has a size approximately 2KB, comes disguised in a SIS (Symbian Installation System) file, called patch.sis. Gavno.b, which is slightly larger, is tucked inside the SIS file patch_v2.sis^[9].

These Trojan programs are believed to be from Russia are proof-of-concept Trojan horses that expected to be spread from one mobile phone to another. Experts believe the Gavno Trojans could still cause a lot of damage even if they are not sophisticated programs^[9].

HOW TO MITIGATE THESE THREATS

What can we do to mitigate these threats now that we know there are security threats that could attack our smart phones? What is the best way to ease these worms from spreading?

To date, most of the smart phone worms and Trojan horses failed to spread. In a few cases, Cabir.a managed to spread from one phone to another phone by using Bluetooth. However, the spread of Cabir's viruses is severely curtailed by the need for users to accept and install the programs^[6]. Users could prevent the attack from disabling the Bluetooth wireless connection and decline to accept and install any new software from the networks.

In order to protect smart phones from being attacked by the Trojan horse, users should not download any new software from the networks especially pirated software. Users who are most likely to be hit by Trojan horse programs such as Skulls and MetalGear are typically users who like to download new software either from Symbian freeware Web sites or peer-to-peer networks^[7].

The infected users of the Trojan programs are unable to browse their file system or install new programs. The only way to get rid of the Trojan programs such as Skull is to reset the infected phone to its default factory conditions^[8]. But this means all the data and configuration will be gone.

CONCLUSION

The recent proof-of-concept mobile viruses would soon become real threats. The threat is expected to be very serious in the near future. The Bluetooth wireless is an example of technology that can distribute mobile viruses as proven by the Cabir worms. In the future, not only the worms' will pose as security threats to smart phones, but also to other types of equipment that install and use the Bluetooth and other wireless technologies.

REFERENCES

- [1] *Versi terbaru OS telefon pintar Symbian. 11 Feb 2005. Berita Harian – Komputer.*
- [2] <http://www.symbian.com/technology/symbos-ds.html>
- [3] *Lemos, R. Worm ready to wriggle into smart phones. http://news.zdnet.com/2100-1009_22-5233517.html*
- [4] *Roberts, P. New, virulent Cabir mobile phone worms spotted. 28 Dec 2004. http://www.infoworld.com/article/04/12/28/HNcabir_1.html*
- [5] *'Metal Gear' Trojan targets symbian phones. 22 Dec 2004. http://www.theregister.co.uk/2004/12/22/metal_gear_virus/print.html.*
- [6] *Lemos, R. Hybrid Trojan horse aims at Symbian phones. http://news.zdnet.com/2100-1099_22-5500229.html*
- [7] *Blau, J. Trojan disguised as Flash player targets cell phones. 07 Jan 2005. http://www.infoworld.com/article/05/01/07/HNflashtrojan_1.html*
- [8] *Lemos, R. Skulls program kills cell phone apps. http://news.zdnet.com/2102-1009_22-5460194.html*
- [9] *Blau, J. Mobile malware kills Symbian service. 24 January 2005. http://www.infoworld.com/article/05/01/24/HNmalwarekillssymbian_1.html*

Introduction

Internet Content Filtering (ICF) is a security mechanism to block or allow access based on preset filtering criteria. It can be in the form of software or hardware (appliance) that can be installed at the host (e.g. personal computer) and network Internet connectivity. It works by inspecting the Internet Protocol (IP) packet through monitoring, controlling and reporting it.

Mainly, its deployment purpose is to prevent connection to inappropriate websites and materials for viewing of a specific group (e.g. employees and children). The benefits of ICF are:

- blocking access to pornographic websites
- scanning HTTPS
- preventing online games and gambling
- disabling internet relay chats (e.g. Yahoo Messenger)
- prevents the download of huge mp3 files (song)
- prevents the download of huge mpeg files (movie)
- prevents audio or video streaming
- acts as another layer of protection to identify malicious Java and ActiveX executables

Demands

Nowadays, parents and employers are seeking ways to hinder their children and employees from accessing adult websites or other unproductive activities over the Internet. These activities will bring about negative implications such as social illness from addiction to Internet gambling or pornography should there be no preventive measures taken. For the employers, in order to curb such activities, they should impose an organization Internet usage policy that will enable them to take legal action should there be any breach on the policy. Here are some basis for ICF demands:

- to increase productivity by managing Internet resource
- to reduce unnecessary cost
- to improve Internet performance for efficient distribution of bandwidth
- to protect employees and children by filtering undesirable content
- to improve time management

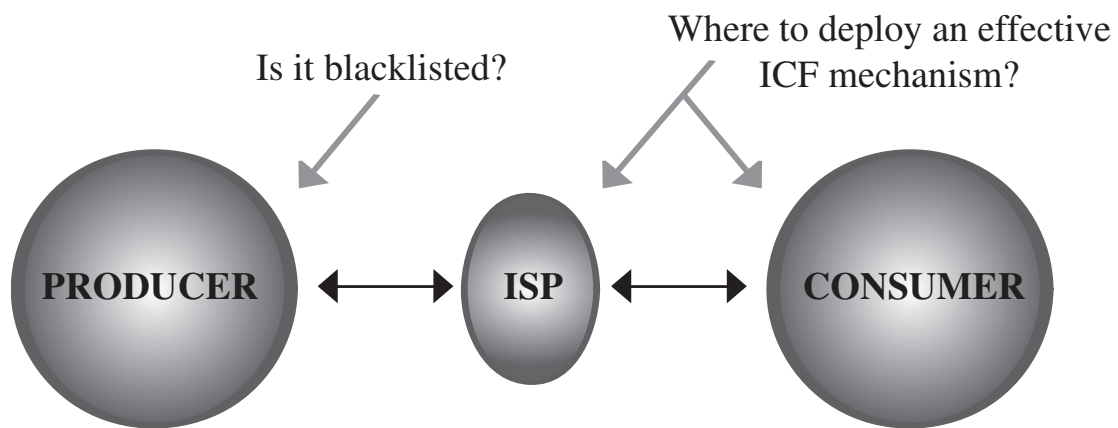
Deployment

Commonly, there are two ways to deploy the ICF mechanism at the host or network level. The choice is based on the number of host that needs to be protected. If it is for home user, software based is the best solution.

- Host - software based ICF is usually targeted for minimum number of host (e.g. home user). The software resides in the host itself, which needs the Internet access control.

- Network - hardware based that is an appliance suitable for an organization with larger number of hosts. It is placed at the network gateway where all transactions pass by the appliance and its computing power would be able to handle all processes.

The technology behind ICF software and hardware products is at application level blocking. It is a defragmentation of IP packets to analyze the content. It is more flexible compared to packet level blocking executed by a router Access Control List (ACL) feature. The diagram below shows the categorized groups that are involved in an Internet connection and ICF installation. This is important for a proper mitigation planning.



Typical Internet Connection Diagram

- Producer - a web content provider can be taken as an example. The website can be inspected to ascertain its classification of category. If the content contains pornographic elements, its Internet address is included in the ICF blacklist.
- Internet Service Provider (ISP) - is the main gateway, could be the most appropriate point for content filtering deployment and has minimal concern on the cost incurred. However, an Internet savvy user might be able to bypass the ISP using port forwarding technique or hiding the blocked IP address in another valid IP address of a proxy web server to request web pages.
- Consumer (e.g. employee or children) - a host based ICF can be installed by parents to avoid their children from accessing unwanted websites. Whilst for an organization, an appliance based ICF can be utilized to block their employee's certain Internet addresses access.

Issues

Host level ICF is mostly used in a home environment as it cost less and is easy to install on a personal computer. If there are many workstations such as in the office or organization, network level ICF is the most suitable for this type of environment. Therefore, it is important to identify the environment before deciding on the type of ICF before procurement.

Despite having these ICF guarding the host and network, they are not resistance proof as there are ways to circumvent them. A direct way is to exploit anonymous surfing. There are many free proxy web servers that can be used to hide the actual blocked IP address. The ICF would not be able to detect this. It only sees the initial part of the address.

Apart from using anonymous surfing, port forwarding is another way of bypassing ICF mechanism. By using tunnelling agent software (e.g. Putty) to tunnel a pre-configured local port such as port 121, to forward it using secure port 22 to the external proxy server connected to the Internet. The web browser must be set to send all data connection to port 121.

Every possible ICF issues have been discussed from introduction to deployment. Now, it is worthwhile to put an effort to discover the pros and cons of ICF to assist in the decision- making. Here are some known issues that should be taken into account when deciding on ICF solutions.

- Target group – this will provide the number of user. If the number is big an appliance based performs superior that host based.
- Cost – the cost of the product range from as low as USD\$40.00 up to about USD\$5000.00. As there is a big gap in the price range, the need to identify the target group is necessary.
- After sales service – is very important in the case of software maintenance.
- Host, proxy (gateway) or ISP – the point of deployment.
- Technology – only application level blocking is discussed, as it is the most favorable ICF technology.
- Effectiveness – the ICF product must operate as it claims. Some might encounter product bug. Therefore, evaluation is very important.
- Bypass – this is annoying. A computer savvy kid might use his expertise to exploit the digital parental guardian.

Conclusion

As a summary, network and host ICF are found to be ineffective after analysis, as non-technical and technical persons could circumvent both easily. This process could be done through anonymous surfing or tunneling (port forwarding) to free proxy server readily available from the Internet.

Nevertheless, it is better to have this ICF in place rather than have nothing to protect home and organization networks. The least it could do is to prohibit those that do not know how to bypass the ICF. Therefore, the conclusions that can be made for organizations, home users and ISPs are as follows.

- For an organization, a policy enforcement sponsored by the top management is very important as an official medium to educate employees and act as deterrence from misusing Internet facility by deploying ICF equipment at the gateways.
- Host based ICF is considered the best solution for home users to prohibit children from accessing inappropriate sites.
- Although ISPs has the financial strength, it is noted that packet level blocking is not a viable solution. Perhaps, application level blocking is adequate by connecting ICF appliance (processing power is required at ISP level).

Introduction

Security threats are not only targeting systems and networks but they are also affecting web browsers. Malicious hackers and virus writers can take advantage of low security settings in your web browsing software to infect and attack your computers. They can do this by enticing you to visit a malicious website and plant malicious codes into your browser even without your knowledge.

On June 24th 2004, a new Trojan was released to the net, the Download.Ject that affects customers using Microsoft Internet Explorer, a component of Microsoft Windows.

When a user visits a website hosted on a server that is infected with Download.Ject, the web page downloads a Trojan horse to the user's computer. This Trojan horse is called Backdoor: W32/Berbew, also known as Backdoor-AXJ, Webber, or Padodor. When this Trojan horse runs on the user's computer, it may perform several actions, including monitoring Internet access to capture sensitive information such as logon names and passwords, opening fake dialog boxes that prompts the user to enter confidential information such as ATM card codes, credit card numbers, or other confidential information. Microsoft has released a tool to help you remove Backdoor: W32/Berbew Trojan horse variants from your computer.

On October 2nd 2003, hackers found another way to exploit an unpatched hole in Internet Explorer Web browser, using a specially designed attack website to install a Trojan horse program on vulnerable Windows machines.

The Trojan program changes the Domain Name System (DNS) configuration on the Windows machine so that requests for popular Web search engines like Google and AltaVista brings the Web surfer to a website maintained by the hackers instead, according to the warnings from leading security companies.

The above scenario explains the threats and implications posed against web browsers. The trend in the threats may get more sophisticated in the near future. Though, you can arm your computers with a wide variety of commercial free tools or software, in actual fact you need a proper overall guideline on browser security.

Threats & consequences related to Web Browsing

Unauthenticated or fake sites

Phishing scam is an example of how users can be tricked into browsing an unauthenticated and fake website. Phishing scam is an activity where an attacker (phisher), fools or spoofs the original emails or websites, mainly Financial Institutions' websites and try to convince the recipients or customers of certain organizations (usually banks) to provide sensitive data such as credit card numbers, username and passwords, social security numbers, etc. According to a research done by the Antiphishing working group, nearly 5 percent of the total number of certain online bankings, online retailers and credit card companies' customers are being influenced by this attack.

Browser exploit or malicious code

An application that has a bug is a normal scenario, since the state of the art application that uses massive functionality and involves tremendous lines of code will accidentally invent a hole or bug. Lack of proper software engineering and line of code checking will certainly bring up the hole.

It will be a major problem for the developer of this software if an external party finds the bug. Usually as a culture of bug finding, the bug finder will normally report it to the developer of the particular software, and the developer will respond in a form of releasing certain patch for the bug.

If this is not the case and the finder is keeping the bug low, the bug itself will definitely create a high-level security bug. Usually, this is when the malicious code will take advantage of the bug or hole. For example, the buffer overflows in Internet Explorer CA-2002-04, is the buffer overflow vulnerability of Internet Explorer when handling embedded objects in HTML documents. This vulnerability could allow an attacker to execute arbitrary code on the victim's system when the victim visits a webpage or views a html email message.

Explicit Content

The world of the Internet is very broad and free .The meaning of free here does not only refer to its availability but also to the content of the web. Anyone can write or develop his own webpage regardless of the topics, languages, purposes and the content could be representing an individual or an organization. Apparently, the early idea of this freedom is to make the netizens more creative, independent, informative than the conservative media, and most importantly, able to share a variety of information. Thus, the content of the Internet is not filtered and can have a negative impact too.

Some negative information depicted in the Internet are, sexual nudity, inhumane culture, negative propaganda and etc. A newsflash from USA Today proves that most of the users of the Internet have abused the initial objective of the Internet. From a very useful technology that was derived from an educational culture, the Internet now, has turned into a field for income generating pornographic industries throughout the world.

For most cases, this so-called adult entertainment can easily become a very poisonous media for the young generation, as the access to such material is easy and efficient. Are we willing to have our next generation growing up with this kind of negative culture?

Man in the middle attack

Analogically, this type of attack is eavesdropping a conversation between two people. For example, person A talks to person B and person C acts as an eavesdropper who eavesdrops on what is being discussed by person A and B. In the computer world, eavesdropping is done thru a network device such as network interface cards (NIC). On a regular usage, the NIC is set to deliver data from the sender to the intended destination, without any third party involvement. For example, if I want to send a data to John Doe, only John Doe is the one who is eligible for this data.

However, in the "Man in the middle attack", data from the sender to John Doe is being intercepted by another party and the other party can read and probably reconstruct those data. In the network term, this behavior is also known as sniffing. If the data that travels to and from the network is low sensitive data, it should not be any problem but what if the data that flows are usernames and passwords of the CEO of a company. This attack is a major threat to organizations, since the activity is hard to detect and the sniffing activity is usually for network testing purposes. Again, a good intention of a technology has been turned into something which is unethical.

Countermeasures to These Threats

Patch your browser

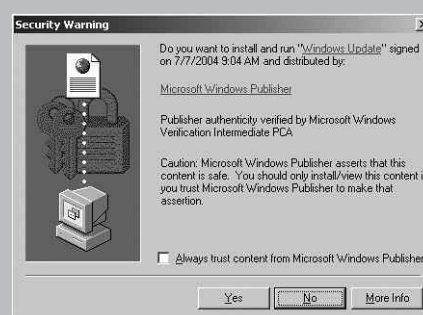
In order for us to overcome the bug, patching up software is the best move to implement. Usually, when a vulnerability is detected, the developer will create a patch for the hole as soon as possible. Each developer has his own way of patching up systems. Please refer to a specific vendor to patchup your system. However, this discussion will cover the wonders of how Microsoft deploys and releases their patch.

Before going in depth on how to retrieve a patch, it is pertinent to know where and how to notice a bug or vulnerability. Here are a set of urls, which are widely used by the users and customers.

- <http://www.us-cert.gov/>
- <http://www.microsoft.com/security/default.msp>
- <http://www.mycert.org.my>
- <http://www.incidents.org>
- <http://www.securityfocus.com/> (previously know as bugtraq)

For Microsoft users, the relevant sites where they can get patches are at:

<http://v5.windowsupdate.microsoft.com>



Picture 1

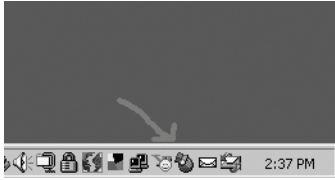
When browsing the site, the users will get a pop up window, requesting an input whether to continue to install the updates or otherwise. It is very important to click on the certificate link on the windows, to make sure the validity of the page. Once assured by the safety and validity of the page, proceed with the installation by following the guide on the web page.

After the installation you may check the history or what have been installed on your computer by entering the Add/Remove program menu Go to Start † Control Panel † Add/Remove programs. The lists of the installed patches are listed and you may remove if the patch does not suit your system. (Some patches will not work perfectly with some other third party program. Therefore, in certain situations, you will need to contact the vendor or the Microsoft representative to verify the patch before you deploy it.)

As a good practice, the industry always performs a testing period on non-operational machines before they can actually install the patches. This practice is to avoid any major glitches right after the patch is up. If you cannot afford such facility, it is good to find information about the latest patch via a mailing list or forum that discusses this type of patch. For example:

<http://communities.microsoft.com/newsgroups/default.asp?icp=xpsp2&slcid=us>

Or you can also find a small icon on the right of the desktop to reach the windows update.

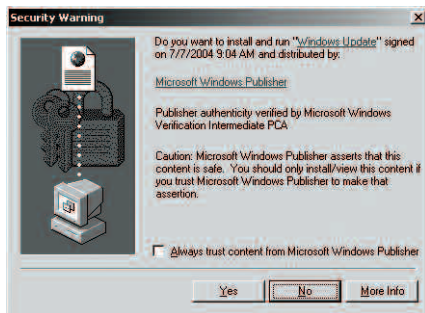


Picture 2

Verify the authenticity of the sites you are browsing

When you are browsing, it is hard to tell whether the site is actually the original site of the page that you have requested. Since there are lots of techniques out there to spoof a website, the technology of certificate is introduced. By default, the browser will always ask the user whether to accept the connection from a certain website or otherwise. But in most of the cases, people will just click OK and proceed to view the site of the URL that they have typed in.

In this case, the menu that keeps the users safe is:




Picture 3

If you click on the Microsoft Windows Publisher link, a certificate will pop up. Proceed whenever you see the certificate verification.

Verify Website's Security

Before browsing a website especially while making a purchase or sharing sensitive personal information over the Internet, make sure you verify the website using encryption to protect information you are submitting. Check for these security measures:

- Make sure you see <https://> in the web address (URL) of the website.
- Look for a lock image (example: ) in the lower right hand corner of your web browser, indicating that the

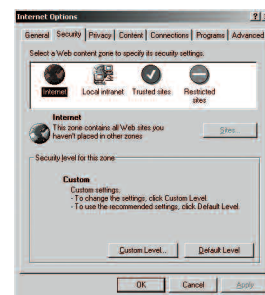
web page is using a security certificate to encrypt the information you are submitting.

- Click on the lock image in the browser, or on a "security certificate information" link, usually prominently displayed on secure websites. The link will verify the identity, validity, and security of the site, as well as providing the status of the security certificate. For example, on Ent Federal's online banking site, you will see the "Verisign Secure Site" image link at the bottom of every page. If you click on this image link, you can verify that Ent Federal's security certificate is current and in used throughout its online banking website.

Configure browser to High Security

Most of the current security breaches comes from ActiveX, Java and scripting. By default, all these scripting is accepted by the browser. However, due to high risk of security that comes from certain sites it is good to customize again the security level of your browser. Customizing the security level does not ensure full security, it could somehow provide mitigation against any threat. In addition, make sure other security mechanism such as antivirus, firewall and intrusion detection system are enabled.

In the case of Internet explorer, the menu for adjusting this level of security is within the Security tab inside the browser, Go to Tools → Internet Options → Security.



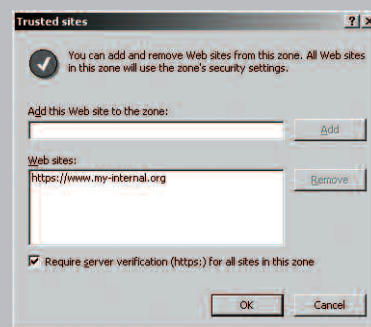
Picture 4

For Internet Connection security level, click the "world" icon. If you click default, the setting will be set to the current level. However, what you need to do is to disable the default setting. Therefore, go to custom and you will be presented with options regarding the features that you want to enable, disable or prompt. A prompt is a feature that pops up a menu, which, will wait for approval of whether the script could be executed or otherwise. While, disable and enable just give a way or not a certain feature without prompting any notices.

In Internet Explorer the default level value is medium. And the settings are as follow:

- ActiveX controls and plug-ins
 - Download signed ActiveX controls: Prompt
 - Run ActiveX controls and plug-ins: Enable
 - Script ActiveX controls marked safe for scripting: Enable
- Downloads
 - Font Download: Enable
- Microsoft VM
 - Java permissions: High safety
- Miscellaneous
 - Allow META REFRESH: Enable
 - Display mixed content: Prompt
 - Drag and drop or copy and paste files: Prompt
 - Installation of desktop items: Prompt
 - Launching programs and files in an IFRAME: Prompt
 - Navigate sub-frames across different domains: Enable
 - Software channel permissions: Medium Safety
 - User data persistence: Enable
- Scripting
 - Active scripting: Enable
 - Allow paste operations via script: Enable
 - Scripting of Java applets: Enable
- User Authentication: Automatic logon only in Intranet zone
- In order to add to the security level, just disable the features that are relevant to scripts as below:ActiveX controls and plug-ins
 - Download signed ActiveX controls: Disable
 - Run ActiveX controls and plug-ins: Disable
 - Script ActiveX controls marked safe for scripting: Disable
- Downloads
 - Font Download: Disable
- Microsoft VM
 - Java permissions: Disable Java
- Miscellaneous
 - Allow META REFRESH: Disable
 - Display mixed content: Disable
 - Drag and drop or copy and paste files: Disable
 - Installation of desktop items: Disable
 - Launching programs and files in an IFRAME: Disable
 - Navigate sub-frames across different domains: Disable
 - Software channel permissions: High Safety
 - User data persistence: Disable
- Scripting
 - Active scripting: Disable
 - Allow paste operations via script: Disable
 - Scripting of Java applets: Disable
- User Authentication: Automatic logon with current username and password

What about if you want to enable scripts for certain sites? For instance, your internal web based system requires scripts to be enabled; you can just add them into the trusted sites.



Picture 5

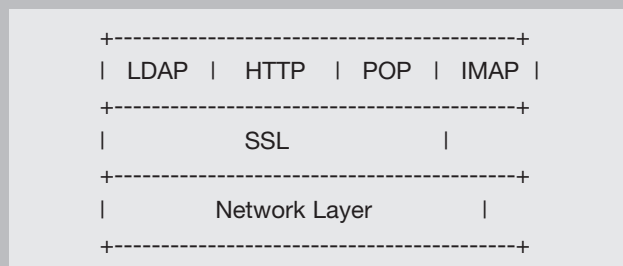
The script will be enabled only if you visit these trusted sites.

Use Secure Socket Layer (SSL) for secure transaction

Users of the Internet are always vulnerable to sniffing attack, since most of the protocols like http, imap, pops are in clear text transaction. This kind of attack is called “man in the middle attack “(which was explained earlier). In order for us to make it unreadable to human, computer scientists have invented encryption. This technology could mitigate the effort of sniffing data across the network. Previously, the clear text data can be seen only as a set of garbled (unreadable) data. The data is valid, once the correct recipient receives it.

SSL is a technology that adopts the advantage of encryption. It is a protocol layer that exists between the Network Layer and Application Layer. As the name suggests, SSL provides a mechanism for encrypting all kinds of traffic - LDAP, POP, IMAP and most importantly HTTP.

The following is an over-simplified structure of the layers involved in SSL.



Picture 6

SSL works by using a private key. For example, if John Doe (sender) wants to send data to Jenny (recipient), the sender will encrypt the data by using his private key. The result of this process is CipherText1. Secondly, the recipient will

encrypt it again with her public key and this will result to the CipherText2. Next, the SHA1 message digest of the "clear text" is created. Then, this SHA1 message digest is encrypted, using Sender's private key. The result of it is called, Digital Signature of the "Clear text". Finally, both Digital Signature and CipherText2 are sent to the recipient.

Once the recipient receives the data, Recipient's Private key will decrypt Cipher Text 2. This data is called CipherText1. Again, it will be decrypted and resulting Clear text data. Here, the SHA1 of the clear text message is created. The "Digital Signature" is decrypted using Sender's Public Key, resulting the "SHA 1 MSG Digest". The "SHA1 MsgDigest #1" is then compared against "SHA1 MsgDigest #2". If they are equal, the data will not be modified during transmission, and the integrity of the Original "Clear Text" is maintained.

Within this process, the data is not readable by the 3rd party if the data is being intercepted and the actual content of it will not be exposed. Furthermore, the use of this SSL technology ensures the integrity of the data.

Download relevant tools – To Block Pop up Windows

Hackers intercepting bank passwords, say experts

NEW YORK: Hackers have found a way to intercept passwords for banking websites by infecting pop-up ads with a program that can install itself on computers and record user keystrokes, security experts said Wednesday.

information before it gets encrypted," Sachs said. He said the latest threat is a variant of "spyware" which installs programs on computers of those interested in the... said.

Picture 7

The newspaper cutting above, talks about a malware that affects the users of sensitive websites through a pop up. The malware can install itself on computers and record all the keystrokes that users have typed in. Apart from that, pop ups are also considered as very annoying behavior and act as advertisements of products and brands.

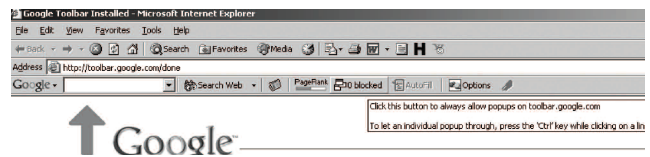
There are lots of software that fights this pop up ads. For example:

1. Pop up stopper by panicware
2. Pop up blocker by earthlink.net
3. Noadware by noadware.net
4. Google toolbar.

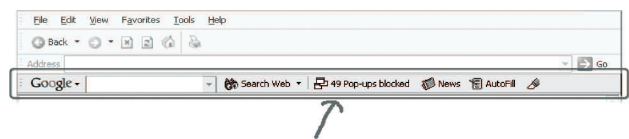
Since most of the users around the world use google as a search engine, we will take a look at google toolbars as our pop up blocker.

Download google toolbar for free at <http://toolbar.google.com/>

After getting thru with all the installation, a toolbar will appear right on top of your internet explorer bar. (See Picture 8)



To use the pop up blocker is simple. Once you click the button, the pop up blocker will understand it as allowing the pop ups. But when the button is unblocked, the toolbar will automatically block all pop ups that appear. The count of blocked pop ups will also appear on the button. (See picture 8)

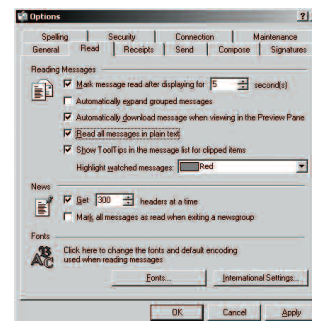


Picture 8

Use plain text to read emails

They are a few ways viruses; malicious codes and exploits can spread to the Internet users. Emails are hackers favorite way of spreading their notorious scripts and programs. The main idea here is to make the user execute the code that they have sent. Therefore, most of it is spread thru html- based emails. If you are using text- based emails like Pine, this kind of threat is not a problem. But the targets are at Microsoft based clients like Microsoft outlook, which has the feature of executable html. As a countermeasure, it is proposed that the html feature be disabled. Here is an example on how to disable html on Microsoft outlook. Other clients may vary and do consult respective vendors on how to do so.

1. In Microsoft outlook, go to Tools > Options > and tab Read.



Picture 9

2. Then tick option "Read all messages in plain text".

Now your Microsoft Outlook, will only read plain text email, and if an html email comes in, it will only show html tags (a non active html).

PROTECT YOUR ORGANIZATION - ADOPT AN EFFECTIVE RISK MANAGEMENT APPROACH!

Nowadays, with increasing number and variety of information security breaches around the world, organizations are facing a difficult time trying to ensure that their business remains secure and protected at all times. Losses suffered due to a successful security breach may impact the organizations not only financially, but also sometimes most importantly their image and reputation. With so much at stake, organizations cannot afford to take it easy when trying to avoid succumbing to the wrath of information security attacks.

Thus, to be able to prevent and reduce the impact of such breaches effectively, managing information security risks is vital and should be made a priority for organizations. However, implementing or adopting an effective information security risk management framework is easier said than done. The overall risk management programme will need to be conducted comprehensively and looked at meticulously to avoid unwanted incidents from happening. The following diagram depicts a comprehensive risk management framework that may be adopted in organizations:

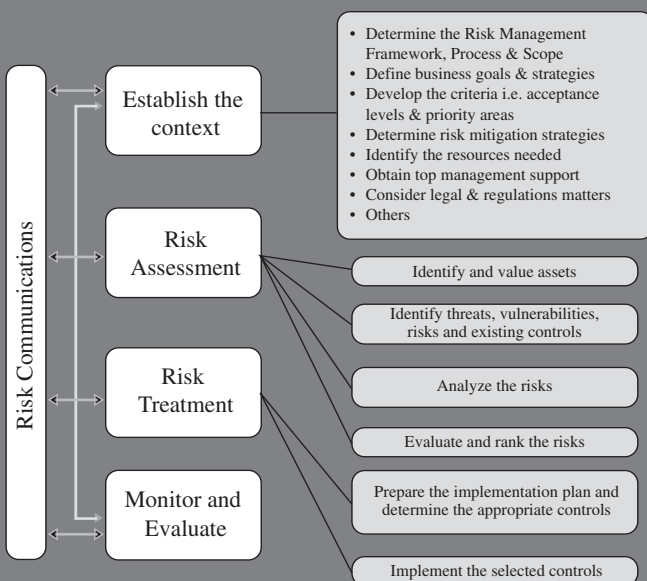


Figure 1: Risk Management Framework

As shown in the diagram, there are four main steps that should exist within a risk management programme: 1 establishing the context, 2 risk assessment, 3 risk treatment, and 4 monitoring and evaluating the risks. There is also another vital component that should exist in each of the steps, which is risk communication.

Establishing the context is essentially the first step that needs to be taken when initiating a risk management programme. This step is critical as it will set the entire tone of the risk management implementation in an organization. Among some of the important activities that need to be carried out during this step include determining and finalizing the risk management framework, processes and scope, defining business goals and strategies and determining risk mitigation strategies.

The second step is performing the risk assessment exercise. During this step, there are four main tasks that have to be completed successfully, which are identifying and valuing assets, identifying the various threats, vulnerabilities, risks and existing controls, analyzing the risks and finally evaluating and ranking the risks.

The risk treatment exercise is the third step, which plays a very critical role in this step, all the risks will be mitigated based on a risk treatment plan that has been approved by the management. There are two main activities that need to be done well here; preparing the implementation plan and determining the appropriate controls and once that is done, subsequently to implement the identified controls.

The final step, which is to monitor and evaluate the risk management programme, is also vital in ensuring the smooth running of the entire programme. Continual evaluation and analysis to the entire framework especially on any new changes that are affecting the organization such as the installation of new systems and introduction of new key personnel will ensure that the organization is well protected from new and emerging threats.

The area of risk communications will also need to be made a priority throughout the entire implementation process, as it will ensure that all employees in the organization will have the same level of understanding on risk management and the steps that are being taken to mitigate the various risks. This activity should exist in each of the four steps as it plays a huge role towards ensuring the overall success of the risk management programme.

The management team's involvement in each of the step of the risk management programme is critical and it has been proven time and time again that without sufficient participation from the management team, the programme will not be a success. To conclude, it would be beneficial for organizations to learn that if the risk management framework is implemented successfully, it will provide them with a secure base for which their business is to grow upon, especially in this day and age where unauthorized data manipulation is on the rise significantly.

KEEPING KIDS SAFE ONLINE

Children present additional challenges in terms of safety because of their natural characteristics: innocent, curious and adventurous, totally oblivious to the punishment. We need to consider these characteristics when determining how our children should be protected when they are online.

We may think that our children cannot cause any harm to us. What if they unintentionally visit pornographic websites? What if they unintentionally download computer viruses or worms?

Parents may monitor their children's surfing habits at home. In fact, some parents are unaware that their children have been accessing Internet at other places such as cybercafes and friends' home.

The Internet is used as a medium of child sexual and emotional abuse.¹ Due to unrestricted access, the tendency for young users to access pornographic materials is very high. Once these children are exposed to these images the probability of these images staying in their minds is very high.

In an article entitled One In Six Kids See Net Porn, Amanda Hodge claims that one in six children as young as eight years old has been exposed to online pornography, frequently through pop-up advertisements.²

Children often imitate what they have seen, read, or heard. Studies suggest that exposure to pornography can drive kids to act out sexually against younger, smaller, and more vulnerable kids.

Apart from that, exposure to pornography will result frequently in sexual illnesses and sexual addictions. According to a study, as more and more children are exposed to softcore pornography and explicit deviant sexual materials, they picked up extremely dangerous messages.³

According to a report issued by Internet watchdog agency Zone-H4, there were almost 400,000 attacks on Web sites around the world last year, a surge of 36 percent from 2003. One particular concern is the fact that the attacks on company and government websites spike during school holidays when the schoolchildren are spending time in front of their computers rather than on their studies.

Hacking is a growing problem among the teenage community. For sometime now, computer hacking, software cracking, and website defacement have gained

the interest of teenagers. They look for excitement and do not understand the real implications of their actions.

In 1993, the Milwaukee-based "414s" was one of the first teenage hacker groups whose members were arrested by the US Federal Bureau of Investigation and convicted of breaking into more than 60 systems.⁵

In 1997, a Massachusetts teenager was charged with disabling the US Aviation Authority control tower for six hours at Worcester Regional Airport.⁶ In June 2002, the Pentagon's computer networks were hacked by a 17-year-old teenager from Austria. He was reportedly successful in his attempt to obtain information on the location of military nuclear missiles.⁷

How can we make the Internet safe for young users and future generations?

Parents Roles Parents have to take an active interest in their children's activities as well as full responsibility in preventing children from accessing offensive materials on the Internet. Parents should implement responsible safeguards, to ensure that their children will have safe, educational and entertaining online experiences.

Parents should monitor their children's activities online closely by placing the PC in an area of the home where they can easily keep an eye on the children.

Parents may also try to establish online rules and an agreement with their children on the limitation of Internet use and of course with proper explanation.

Parents have to be alert on their child's behavioural changes. For example, a child who is secretive may indicate that he possesses inappropriate materials or may have done something wrong.

Service Providers Roles. It is essential for service providers or private organizations to offer assistance in disseminating information on safe Internet usage. They should also provide information on websites that are deemed unsuitable for children.

Service providers or private organizations should also conduct educational campaigns on Internet risks and safe surfing for children. As more and more sites offer offensive materials, service providers or private organizations should develop software to filter or block access to these sites. In addition, online safety tips and information on filtering software should be made known to users.

TIPS ON PROTECTING YOUR PERSONAL COMPUTER (PART 2)

Issue No 2: Email

The Internet provides one of the easiest communications tools known as electronic mail or email. It is a fundamental part of the Internet and its technology provides comprehensive communication, productivity and effectiveness. Undoubtedly, E-mail has revolutionized the way we conduct businesses and communication. However, as time passes by, electronic mail has been plagued with numerous security problems such as viruses, worms and spam (unsolicited commercial email), which have developed over time along with email use.

The three main principles of Information Security involves preserving the confidentiality, integrity, and availability of information resources. These three principles can be directly applied to the area of email security as well. Confidentiality of email refers to limiting information access and disclosure to authorized users. Integrity involves the assurance that information is authentic and complete. Where else, availability of email involves ensuring that mail servers remain online and able to service the user community. A weakness in any one of these three key areas will undermine the security posture of an email system and open the door to exploitation.

The Threats and Countermeasures

a. The Threats

Spam and Unwanted Email:

Spam is not just a nuisance anymore. It is a threat to every company regardless of its size. Hostile spam contains viruses such as Trojan horses and worms. The sheer quantity of Spam today decreases productivity and dramatically increases the cost of email use. Spam filtering also poses the potential loss of legitimate emails while attempts are made to weed out unwanted messages.

Viruses and Worms:

These malignant entities, though almost as prevalent as Spam, are infinitely worse. Viruses and worms can take over your computer, send your private information to attackers, destroy your hard drive, bring your computer to a stand still, or disrupt productivity in general. They are a threat to privacy and raise suspicion of legitimate email.

Email Bombs and Other Attacks:

"Email bombs" occur when you receive an immense number of email messages in a very short time. Dictionary attacks are generated by spammers trying to discover valid

Authorities Roles. Obviously, there is an urgent need to conduct educational programmes on the nature and use of the Internet, including its inherent dangers. With the advancement of information communication technology (ICT), it is necessary to ensure that our education system is tailored to educating our children on safe computing.

It is important for our children to know the dos and don'ts when they are online. Computer ethics should be introduced as a new subject in school. Ethics with regard to the use of ICT and data systems have to be addressed for primary and secondary schoolchildren.

Nowadays, youngsters are using cyber cafes to access undesirable sites and pursue activities such as Internet gambling and pornography viewing. Hence, it is recommended that the Government makes it mandatory for cybercafe operators to install software to block access to pornographic and other excessive websites.

Cyber security is a shared responsibility for all - Government, private and public sectors and the community. Within a relatively short period of time, the Internet has revolutionized communication and information sharing across the world, a revolution, which is embraced eagerly internationally.

Just as the Internet has become a source of significant positive change, it has also created new opportunities for the abuse or exploitation of children. With the growth of ICT and Internet usage in Malaysia, it is crucial that safeguards be put in place now, rather than when it is too late.

REFERENCES

1. Feather, M., "Internet and Child Victimization", *Children and Crime: Victims and Offenders Conference*, 17 - 18 June 1999. Brisbane: Australian Institute of Criminology.
(<http://www.aic.gov.au/conferences/children/feather>)
2. Amanda Hodge, "One In Six Kids See Net Porn", *The Australian IT*, 23 April 2005. (<http://australianit.news.com.au/australia>)
3. Donna Rice Hughes, "Protecting Your Children In Cyberspace", Fleming H. Revell Company, 1 August 1998. (www.protectkids.com)
4. Roberto Preatoni, "Main Web Site Hackers are Schoolboys", *Reuters.Know.How* 25 April 2005. (<http://www.zone-h.org>)
5. Dan Verton, "The Hackers Diaries: Interview and Insight Into Teenager Hacking", McGraw-Hill/Osborne, April 2002 (<http://www.osborne.com>)
6. Frank J. Cilluffo, "Cyber Attack: The National Protection Plan and its Privacy Implications", *Homeland Security @ GW*, 1 February 2001 (<http://homelandsecurity.gwu.edu/congress>)
7. "Komputer Pentagon Diceroboh", *Berita Harian*, 16 Jun 2002

email addresses at your organization by sending email to thousands of different addresses. Floods like these can bring your email service to its knees, filling up all your email storage space, and resulting in the loss of legitimate messages and businesses.

All of these threats can cause a great deal of damage to a business. These threats can use large quantities of disk space on email servers and in some cases run email servers out of space. They can saturate Internet connections by utilizing all available bandwidth. They can diminish employees' productivity by causing them to manage large amounts of irrelevant email. Finally, they can destroy data and cause costly cleanups.

b. The Tips

Turn off the preview pane

- Always know who an email is from before you open it
- To disable the Preview Pane in Outlook Express:
 - From the menu bar, click "View", and then click "Layout".
 - Uncheck the box labeled "Show Preview Pane".
 - Click "OK" to save the change.
- To disable the Preview Pane in MS Outlook:
 - Click on the Inbox folder.
 - Select "View", and uncheck "Preview Pane."
 - Repeat the procedure for other Outlook folders.
Disable Javascript
- HTML-based email is nice, but Javascript in an email message can be very dangerous
- To disable Javascript in Outlook and Outlook Express
 - Open Outlook Express.
 - From the menu bar, click Tools > Options > Security
 - Select Restricted sites zone
 - Click the Apply, then OK button and close the window
 - Go to Control Panel

- Double-click the Internet Options icon.
- Click Security tab > Custom Level button
- Scroll down until Active scripting is visible
- Select Disable
- Click the OK button

Go offline

- Email tracking (web bugs) do not work in offline mode.

Never open attachments that are programs

- Only open attachments that you are expecting
- Always scan attachments for viruses, even if you think your virus scanner is doing it automatically.

Never reply to spam, even to be "removed" from their mailing list

- Remember that secure web sites will never request you to change your password, enter your PIN, or answer other sensitive questions via email

Have firewall and anti virus in place

- The anti virus should have the capability of scanning emails in and out of your system
- Ensure that both firewall and anti virus are updated

Conclusion

The cost of ignoring email threats can be catastrophic and there is no such product that can safeguard your email perfectly. However, keep yourself updated with current security issues and applying the preventive measures could reduce the chance of being attacked.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) IMPLEMENTATION: EXAMINING ROLES AND RESPONSIBILITIES

“Security is everyone’s responsibility”.

Everyone has roles and responsibilities for maintaining security in an organization. The management, technical people, employees, vendors and contractors have different roles in developing and implementing an effective security process. This article will look at the roles and responsibilities of management, Information Security Department and users in implementing and maintaining information security management system (ISMS) in organizations.

Management's responsibilities

Management's responsibility goes beyond the basics of support. They must set the tone for the entire program. It is not enough just to bless the program. Management must own up to the program by becoming a part of the process.

Management is responsible for overseeing the development, implementation, and maintenance of ISMS. These responsibilities include defining the information security objectives of the organization, allocating a budget to invest in information security, and ensuring the compliance and enforcement of implementation.

Management has specific goals for the organization, and sometimes technical people are not in the position to understand these nuances. Both groups should understand that security is not something that can be wrapped in a package and bought off the shelf. It should be a goal that both parties strive to maintain. One of the ways to bridge the divide is by setting up an Information Security Management Committee. It is the responsibility of management to form this committee that will be responsible for reviewing changes in the business and determining how ISMS implementation should support those changes. To make this committee a success, it is good to distribute the responsibilities throughout the organization depending on the institution's size, complexities, cultures, nature of operations, and other factors. The distribution of duties should ensure an appropriate segregation of duties between individuals or organizational groups.

Management should also ensure integration of security controls throughout the organization by performing the following:

- Ensure the security process is governed by organizational policies and practices that are consistently applied,
- Require that information with similar criticality and sensitivity characteristics be protected consistently regardless of where in the organization it resides,
- Enforce compliance with the security program in a balanced and consistent manner across the organization, and
- Coordinate information security with physical security.

Information Security Department Responsibilities

The Information Security Department is responsible and accountable for security administration. At a minimum, they should directly manage or oversee risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. Security officers should have the authority to respond to a security event by ordering emergency actions to protect the organization from an imminent loss of information or value. They should have sufficient knowledge, background, and training, as well as an organizational position, to enable them to perform their assigned tasks.

Users Responsibilities

Users should know, understand, and be held accountable for fulfilling their security responsibilities. The means of ensuring users understanding and/or recognition of their responsibilities varies. User security awareness training is one of the most common means available to achieve recognition of responsibility and computing asset worth. Some organizations require personnel to sign an agreement that includes the protection of computing assets as a condition of employment, while others sign agreements as a condition of allowing their connection to the organizations network.

One way to ensure that every current and future user knows that security is part of his job function is to make it part of the job description. Spelling out the security function or expectations within the job description demonstrates the commitment to information security, as well as emphasizes that it is part of the job. After it is made part of the job description, it becomes something that can be considered in performance evaluations.

Conclusion

Information security is the responsibility of everyone in the organization. Management support is crucial for a successful ISMS implementation. Along with its support is a responsibility to the ongoing maintenance of this program. To have a successful ISMS implementation; management, Information Security Department and users must have a good understanding of their roles and responsibilities and be willing to take actions.

SECURITY EVENTS 2005

No	Event	Venue	Date
1.	RSA® Conference 2005	Austria Center Vienna	17 - 19 Oct 2005
2.	Information Security Decisions	New York City, USA	19 - 21 Oct 2005
3.	The 10th Nordic Workshop on Secure IT-systems	Tartu, Estonia	20 - 21 Oct 2005
4.	SANS Network Security 2005	Los Angeles, CA	24 - 30 Oct 2005
5.	12th ACM Conference on Computer and Communication Security	Alexandria, USA	07 - 11 Nov 2005
6.	CSI 32nd Annual Computer Security Conference & Exhibition	Marriott Wardman Park Washington, D.C.	14 -16 Nov 2005
7.	The IASTED International Conference on Communication, Network And Information Security (CNIS 2005)	Phoenix, USA	14 - 16 Nov 2005
8.	Information Security Management Conference	Amsterdam, The Netherlands	14 - 16 Nov 2005
9.	Network Security Conference	Amsterdam, The Netherlands	14 - 16 Nov 2005
10.	The Conference and Expo on Mobile & Wireless Security	Orlando, FL	15 - 17 Nov 2005
11.	The 8th Annual International Conference on Information Security and Cryptography	Seoul, Korea	01 - 02 Dec 2005
12.	AsiaCrypt 2005	Chennai, India	04 - 08 Dec 2005
13.	Annual Computer Security Applications Conference	Arizona, USA	05 - 09 Dec 2005
14.	InfoSecurity Conference	New York, USA	06 - 08 Dec 2005
15.	6th International Conference on Cryptography	Bangalore, India	10 - 12 Dec 2005
16.	7th International Conference on Information and Communications Security	Beijing, China	10 - 13 Dec 2005