April 2010

www.infosecawareness.in

Information Security Awareness

Program by
Information Security Education and Awareness (ISEA)
Department of Information Technology
Ministry of Communications and Information Technology
Government of India

InfoSec Tip

Lock your Desktop before you leave your desk

If you walk away from your desk, even for a brief moment, and your PC is left unlocked, someone will walk in, and send mail to a broad distribution list with something silly. Like "I Love You", or worse things, some downright embarrassing. **For some reason this is called "Goating".**

If you are running Windows NT, Windows 2000, or Windows XP Professional , Type **Ctrl-Alt-Del** and then selecting **"Lock Computer"** to lock your computer. To unlock your computer, hit Ctrl-Alt-Del again and enter in your password

You can also set your screen saver to require a password to return to your computer.

InfoSec Quote

"If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees." - Kahlil Gibran

InfoSec Cartoon

Be careful about shoulder surfing

SOME MORE TIPS

- ✔ Install Anti Key Loggers
- ✔ Always scan Attachments with latest anti virus
- ✔ Always logout or lock desktops while in breaks
- ✔ Keep Password more secure
- ✔ Use Single disposal credit cards numbers as some larger banks are offering the same
- ✔ Always use two way authentication or three way authentication methods to participate online
- ✔ Use separate credit card for online transaction.

Executed by :
Centre for Development of Advanced Computing
Hyderabad

InfoSec Quiz

1) The following is the program your personal computer's microprocessor uses to get the computer system started after you turn it on

(a) Boot
(b) source code
(c) initialization
(d) BIOS

2) A person that will talk people in to revealing passwords or information that will compromise his personal or company data

(a) Social Networker
(b) Social Engineer
(c) Social Manager
(d) Social Sciences Teacher

3) Junk e-mail, as in mass mailings, is annoying but harmless

(a) True
(b) False

4) The following is an attempt to trick an audience into believing that something false is real

(a) Hoax
(b) Baiting
(c) Logic Bomb
(d) Virus

5) Which of the following is the most important to install and keep up to date on your personal computer?

(a) Anti Virus and Anti spyware
(b) Desktop Firewall
(c) Operating System Updates
(d) All of the above

Jan '10 Mar '10 Contest Answers

InfoSec Quiz

1) D 2) B 3) C 4) B 5) A

InfoSec Crossword

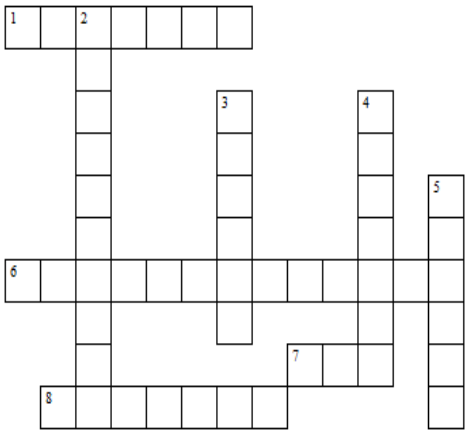
Logon to
www.infosecawareness.in
to participate in the
InfoSec Contest

Congratulations
Last Edition Contest Winners

InfoSec Crossword
Mr. Rahul Maheshwari
Madhya Pradesh

InfoSec Quiz
Mr. RamaSubramanian
Chennai

InfoSec Crossword



ACROSS

1. Person employed to verify, independently, the quality and integrity of the work that has been undertaken within a particular area, with reference to accepted procedures

6. The process whereby a person approves a specific event or action

7. An fault in a computer system

8. Its a program which captures and analyses packets of data as it passes across a network.

DOWN

2. The process by which encrypted data is restored to its original form in order to be understood or usable by another computer or person

3. A small identifier file placed on a user's computer by a Web site

4. The process of recording events at the time that they occur

5. A mechanical device used by software developers to prevent unlicensed use of their product.

InfoSec Virus Alert

Trojan:Win32/Spyeye

Original issue date: March 26, 2010

It has been observed that Trojan Win32/Spyeye is in the wild. It is a family of password-stealing and backdoor Trojans and is downloaded unknowingly by a user when visiting a malicious Web site. It can also be dropped by other malware. (TrojanDropperWin32/Spyeye)

The trojan is able to download files, log user keystrokes, depicts rootkit behavior, performs bot related functionality etc. The Trojan then upload captured account credentials to Web sites specified by the attacker.

It also provides certain rootkit capabilities thereby hide its own process on injected processes, hide and prevent access to its own binary code, Hide and prevent access to its startup registry entry.

Aliases:

Win-Trojan/Pincav.125952.B (AhnLab) Win32/SpyEye.B (CA), Trojan.Win32.Pincav.rvy (Kaspersky), BackDoor-Spyeye (McAfee), Mal/Spyeye-A (Sophos), Trojan.SpyEYE (Symantec), TSPY_EYEBOT.SMA (Trend Micro)

For more details: **http://www.cert-in.org.in/virus/Win32_Spyeye.htm**

InfoSec News

New malware overwrites software updaters, It's the first time researchers have seen malware overwrite rather than mask itself as an update

For the first time security researchers have spotted a type of malicious software that overwrites update functions for other applications, which could pose additional long-term risks for users.

The malware, which infects Windows computers, masks itself as an updater for Adobe Systems' products and other software such as Java, wrote Nguyen Cong Cuong, an analyst with Bach Khoa Internetwork Security (BKIS), a Vietnamese security company, on its .

BKIS showed screen shots of a variant of the malware that imitates Adobe Reader version 9 and overwrites the AdobeUpdater.exe, which regularly checks in with Adobe to see if a new version of the software is available.

Users can inadvertently install malware on computers if they open malicious email attachments or visit websites that target specific software vulnerabilities. Adobe's products are one of the most targeted by hackers due to their wide installation base.

After this particular kind of malware gets onto a machine, it opens a DHCP (Dynamic Host Configuration Protocol) client, a DNS (Domain Name System) client, a network share and a port in order to received commands, BKIS said.

Malware that poses as an updater or installer for applications such as Adobe's Acrobat or Flash are nothing new, said Rik Ferguson, senior security advisor for Trend Micro

http://computerworld.co.nz/news.nsf/security/new-malware-overwrites-software-updaters?opendocur

InfoSec News (Contd...)

2 New Twitter feature looks for malicious URLs

Twitter has added a new service that detects malicious URLs in an effort to quell the rise in spam and phishing on the microblogging social network.

The new security feature ultimately will scan all URLs before they hit the Twitter feed, but initially is only doing so for URLs sent via Twitter direct messages [DMs] and email notifications about DMs. Twitter is using its own URL shortener for these links: "For the most part, you will not notice this feature because it works behind the scenes but you may notice links shortened to twt.tl in Direct Messages and email notifications," said Del Harvey, Twitter's director of trust and safety, in a recent blog post.

Twitter's security feature comes amid new data revealing the level of abuse on the social network: One in eight Twitter accounts last year was malicious, suspicious, or suspended, according to a report issued more recently by Barracuda Networks. The surge in celebrities joining Twitter in 2009 resulted in a major jump in spam, phishing, and other abuse on the site, according to the report.

And those numbers have remained steady to date. "We are still seeing Twitter identify 3 to 4 percent of Twitter accounts as malicious. And, meanwhile, 9 to 10 percent of accounts on Twitter are actively engaging in malicious activity," says Paul Judge, chief research officer at Barracuda.

Twitter's abuse rate increased 66 percent during what Barracuda calls the "Twitter Red Carpet Era," the period during November 2008 to April 2009 when a wave of celebrities joined the social network

3 Zeus malware now has Windows-like piracy protection

The newest version of Zeus, a do-it-yourself crimeware kit responsible for millions of dollars in losses by consumers and businesses, comes with anti-piracy provisions similar to those used by Microsoft's Windows, a researcher said today. Like Windows, Zeus 1.3 ties itself to a specific computer using a key code based in part on the machine's hardware configuration, said Kevin Stevens, a security researcher with Atlanta-based SecureWorks, and a co-author of a report on Zeus published last week.

Know More at: http://news.hackerjournals.com/?p=10366

Hi Friends, I share my personal details with the Internet world only if necessary. with the confirmation that its not visible to public. DO YOU ?

Visit www.infosecawareness.in for more details

InfoSec Concept - I

SOCIAL ENGINEERING

What is Social Engineering?

Social Engineering is a collection of techniques used to manipulate people into perform actions or divulging confidential information. While similar to a confidence trick or a simple fraud, the term typically applies to trickery for information gathering or computer system access. In most of the cases the attacker never comes to face-to-face with the victims and later seldom realizes that they have
been manipulated.

In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal or Help Desk and may ask for user security procedures.

Why Social Engineering?

Social Engineering uses human error or weakness (i.e. cognitive biases) to gain access to any system despite the layers of defensive security controls that have been implemented.

An Attacker may have to invest a lot of time and effort in breaking an access control system, but he or she will find it much easier in persuading a person to allow admittance to a secure area or even to disclose confidential information.

Due to no replacement of human interface in automated systems and networks today, Human interfaces will always be there to provide information and perform maintenance of the system.

Reasons for Social Engineering

- Careless talking is one of the reason for social engineering
- Careless talking about business, the office, home, personal and the people and discussing with those who not authorized to talk, and also gives the sensitive information indirectly to someone who may use it for a specific reason such as breaking into your computer, your organization details etc

Who is affected

- Any Individual
- Members of an Organization
- Children
- Women etc

HOW DO THEY DO?

- A Social Engineer may meet you outside of your work place or organization and may ask you about your work or how your organization does the things.
- A Social Engineer may approach you either a telephone or e-mail and pose as a person from your In-formation Technology Department or Help Desk and may ask for user id, password and other details like systems and network information.
- A Social Engineer may come to your organization to pres-ent business needs and may ask for network connectivity to know about network informa-tion or any sensitive information.
- A Social Engineer may ask your identity card to know aboutyour personal information about your school, organization etc.
- A Social Engineer may approach you to join as friend in your so-cial networking site and may send applications through links to your ID and may do trick-ing to get your personal details.

Types of Social Engineering

Non-Technical

Hoaxing

A Hoax is an attempt to trick an audience into believing that something false is real. Unlike a fraud, A hoax is often perpetrated as a practical joke, to cause embarrassment, or to provoke social change by making people aware of something

Tip: Hoaxes are often sent as “send this to everyone you know” requests, frequently include technical jargon and may sometimes appear to come from a credible-sounding source (like Microsoft, Adobe etc). Do not bother forwarding these warnings to anyone

Pretexting

Pretexting is the act of creating and using an invented scenario (the pre-text) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances

Tip: The above technique can be used to trick a business or personal into disclosing sensi-tive information by attackers to obtain Credit card details, Telephone Bills, Banking Records and other information directly from your or your Children

Dumpster Diving

Dumpster Diving, also known as Trashing, is another popular method of Social Engineering. A huge amount of information can be collected through company dumpsters or wastage from home.

Tip: Never dump any confidential papers into trash, before dumping make sure you don’t have any important information in it

Technical

Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Tip: Never respond to requests for personal information via e-mail.

Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.

Tip: If you receive a call for asking personal details, do not respond.

Popups

Pop-up ads or pop-ups are a form of online advertising on the World Wide Web intended to attract web traffic or capture email addresses or hidden under another window. It works when certain web sites open a new web browser window to display advertisements

Tip: Always block POPUPs

Cyber Acts

InfoSec Concept - II

Creating fake profiles in Social Networking sites

A fake profile of somebody is created on Social Networking Sites such as Orkut, Facebook etc. The profile displays her/ his original name and contact information (Home Address, Mobile Numbers,Photographs etc) by describing her/ his as " loose character " or containing defamatory information (Sexually weakness, immoral character) about victim so that all users of that social networking site see that profile and may start calling and disturbing them.

The motive of doing such activity is for taking revenge or jealousy about those people or The School Children may hatred about their teachers.

As per Indian IT ACT 2000/2008 Amendment, Section 67, and Indian Penel Code (IPC) 500, 509, the following are liable

*** Director (s) of Social Networking Sites**
*** All those who created such fake profiles**

Online Hate Community

An online hate community is created sp that the community displays objectionable information against a particular country, religious or ethnic group or even against national leaders and historical figures.

The motive of doing such activity is desire to cause racial hatred such as community creating anti-India or Anti America online communities

As per IPC Section 153A, 154A, The following are liable

*** Director (s) of Social Networking Sites**
*** All those who created such fake profiles**

If you are the victim of a cyber crime

Report it immediately. To know where to report

VISIT

www.infosecawareness.in/report-abuse

Virus Attacks

A highly skilled programmer creates a new type or strain of virus and releases it on the Internet so that it can spread all over the world. Being a new virus, it goes undetected by many Antivirus software and hence is able to spread all over the world and cause a lot of damage. Antivirus companies are usu-ally able to find a solution within 12 to 48 hours

The virus spreading all over the world and is not targeted at any specific person or organisation

The Creator of the virus is liable for such actions under IT ACT 2000/2008 sections 43 and 66, and IPC Section 426.

The motivation is simply getting thrill and pleasure in destroying the data or to make himself as popular

A highly skilled programmer creates a new type or strain of virus. He does not release it on the Internet. Instead he sells it for a huge amount of money. The buyer uses the virus to target his rival company. Be-ing a new virus, it may be undetected by the victim company's Antivirus software and hence would be able to cause a lot of damage. Antivirus companies may never get to know about the existence of the virus

The virus targets a particular organisation. This type of a virus is not known to antivirus companies as it is a new virus created specifically to target a particular organisation

The motivation is Illegal financial gain, revenge, business rivalry

The Creator of the virus is liable for such actions under IT ACT 2000/2008 sections 43 and 66, and IPC Section 426.

Guidelines to Prevent Virus

- Keep you Antivirus software up to date and make sure that it is working properly.
- Scan the files with anti-virus software before you download it from the Internet and execute it.
- Be careful while exchanging the files between the systems through disks or through network.
- While using the disk make sure that it is write protected .

SOME SECURITY TOOLS

Virus Protection & Cleaner Tools

- ***Windows based***
  - Mcafee Virus Scan
  - Comodo Antivirus
  - Clamav (open source)
  - Winpooch (open source)

Assessment of OS Security Levels

- Microsoft security assessment tool (MSAT)-(Windows)
- Nessus ($, Linux, Windows)
- Retina ($, Windows)
- IBM internet scanner
- Patch link vulnerability assessment tool
- Qualys guard ($, Linux, windows)
- GFI LAN guard ($, windows)

Assessment of Database Security Levels

- IP Locks
- App Detective

Guess the tip which suits the above cartoon picture & win prizes.

Logon to www.infosecawareness.in *to send the tip.*

InfoSec Tools

PARENTAL CONTROL BAR

Parental Control Bar is a simple, powerful tool to help shield your children from explicit websites. Simply activate Child-Mode while your children surf the internet, and the toolbar will block access to adult-oriented websites.

An important aspect of ensuring that your child is safe while using the Internet is the installation of parental control software.

Parental controls will provide you with the advantage of being able to

- ✔ Enforce time limits to child Internet activity set by parents
- ✔ Block access to materials (pictures) identified as inappropriate for kids
- ✔ Monitor your child's activity on the Internet by storing names of sites and/or snapshots of material seen by your child on the computer for you to view later
- ✔ Set different restrictions for each family member
- ✔ Limit results of an Internet search to content appropriate for kids

For more details Visit :
http://infosecawareness.in/parents/parental-control-bars

InfoSec Workshops – Mar '10 / Apr '10

Information Security Trainers Training

@ Hyderabad
@ Patiala
@ Mohali

→ **220 Members Participated**

Information Security Awareness to Students

@ Hyderabad
@ Mohali
@ Chandigarh

→ **850 Members Participated**

Information Security Awareness to Others

(NGO's / CSI Operators, Air Force, Govt. Employees)

@ Hyderabad
@ Rourkela
@ Mohali

→ **261 Members Participated**

InfoSec Workshop Participants Comments

The program was very good and it created awareness for us to access the net with safety

- Sangita Rajan
KV, Picket

Very useful information is shared. Keep up the good services C-DAC

M.Vijaya Padma, Teacher
Sreenidhi International School,
Moinabad, Hyderabad.

I like it very much because it is very much interested and given knowledge very much.

B. Rathik , Student

KV, Picket

This workshop is really good. I came to know about the features of PC.

D. Swapna, Parent

The seminar was wonderful and we would like to practipate in may more seminars

-Harshad Reddy,
Student KV, Picket
Hyderabad

This seminar is useful for everyone, gives us a clear picture how we can get trapped into the hands of hackers or attackers.

M. Malathi,Teacher
Sreenidhi International School

Thanking you to spend time with us and telling about new things

M. Sreekanth,
Student, KV Picket

www.infosecawareness.in

Interested to organize InfoSec Workshop at Your Location ?

for more details visit ....
www.infosecawareness.in/isea-pi

DOWNLOAD

- ✔ Cartoon Videos
- ✔ Brochures
- ✔ Posters
- ✔ Handbooks

from
http://www.infosecawareness.in/downloads

Users Views on the Cartoon – Guess Tip Contest

Beware of unknown websites

Rajasekhar

Protect your PC from virus which may come from e-mail attachments etc.

Aditya

Do not open unknown mails that could be dangerous

Rohit Bodla

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-Learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain management and Wireless Sensor Networks

For Information Security Awareness Workshops at your place

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115
Fax: 040-2315 0117.