Information Security Hand Book 2015

Your First Aid Box for IT Security

Presented by

Public Relations Society of India-Kolkata Chapter
www.prsikolkata.org
&
Indian School Of Ethical Hacking
www.isoeh.in

PRSI

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

Public Relations Society of India, Kolkata Chapter

Public Relations Society of India is the national association of public relations practitioners and communication specialists in India. It functions primarily for professional development. It seeks to formulate and interpret the objectives and potential of public relations as a socially useful function and uphold its value as an integral part of management. It also maintains close links with the academic bodies for promotion of public relations as a subject of management studies.

Promotion of professionalism has been high on the agenda of the Kolkata Chapter right from its inception. To provide an academic foundation to the profession, it has brought out a number of monographs on various subjects in the field of public relations and communication by distinguished practitioners.

Public Relations Society of India Kolkata Chapter
67 Suhasini Ganguly Sarani
Kolkata 700025
info@prsikolkata.org
www.prsikolkata.org

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of
Ethical Hacking

What is the current status of Cyber Security in India?

"In India, we went straight from no telephones to the latest in mobile technology. And the same with internet-connected computers. They came in all of a sudden and no one was taught even the basic facts about cyber security," said Cherian Samuel of IDSA why India is the 5th most cyber - crime affected country as per report "Cyber Security: The Vexed Question of Global Rules" from SDA & McAfee.

Link of Original Report from McAfee:
http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf
(check page - 67 of 108)

"The national cyber security policy sees India needing as many as 500,000 professionals in the field in five years. Currently, there are only about 37,000 cyber security professionals in India and there is a big gap between demand and supply. We want private sector participation in training people in this field."
~Gulshan Rai, Director General, CERT-India(http://www.cert-in.org.in)

[Source: Hindustan Times, 24.05.2013]
http://www.hindustantimes.com/business-news/CorporateNews/Jobs-boom-ahead-in-cyber-security/Article1-1065518.aspx

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

Why is IT Security KNOW-HOW a "COMPULSORY" for EVERYONE in this Digital Age?

Globally, with a tremendous rise in cyber crime, there is a rapid growing demand for both skilled & unskilled professionals to have basic to high level of IT Security knowledge, so that one can safeguard the Internet and corporate networks and data.

- **Banking Sector / Non- IT Corporate**: Their data and network is constantly under attack. More and more organizations are hiring security experts to protect themselves from Industrial espionage. Company HR is giving more priority to the Software and Network Engineers who are familiar with the IT security basics.

- **Software Developers / DBA / Network Engineers**: With websites defaced, database hacked, network penetrated, the future computer Engineers need to have in depth IT Security Knowledge to get a job.

- **Govt. / Military / Police / Investigation Bureau**: Organized crime shifting modulus operandi to cyber base, Police & other investigation bureau are recruiting Engineers with IT Security knowledge. Computer Engineers with knowledge of Digital Forensics will be the top recruited in coming days.

- **Common Man / kids**: With increased use of Online Bill Payment, staying connected via Social Network sites & mobile usage, one needs to know how to stay protected. With the kids introduced to the Internet quite early in age, IT Security education is a must among the elders so that they can guide their children to stay protected.

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

BASIC Security

Basic threats: Virus, Worms, Trojans, Key loggers, Adware, Spyware, **Root-kit, Ransomware**. The last two are the most hard to detect. Rootkit possess as normal OS process and are usually not detected by Anti-virus. Use an anti-rootkit to detect. Ransomware will come as attachment (pdf, MS-word, etc), which when opened, will encrypt all your data (files) on hard disk, deleting the original file. The hacker will ask you for money to get back your data.

Sources: P2P - Kazaa / torrent, Email attachments, Social Network Allow Access API, Online Games, Freeware, Open Bluetooth, Illegal websites, etc.

Symptoms of Trojan attack:

- CDROM drives opens and closes itself
- Antivirus is disabled or don't work properly Ctrl+Alt+Del stops working; taskbar can not be opened
- Computers shuts down or powers up by itself
- Mouse pointer disappears or move by itself.
- Screensaver setting changes automatically.
- Windows Start button disappears
- Pop up ads keep coming
- Your password gets leaked, credit card information gets stolen

Virus and Worms: Countermeasures:

- Install a good Antivirus like Nod32, Kaspersky, Norton, etc.
- Install a firewall like Zone Alarm
- Install a Antispyware
- Scan every attachment in email before downloading it
- Update the antivirus regularly so that it can detect new viruses
- Possibility of Virus infection may corrupt all your data, thus maintain regular data back up

Trojan countermeasures:-

- Trojans uses unused ports in your computer to connect back to Trojan handler.
- Install free port monitoring tool Curr Ports, Source: http://www.nirsoft.net/utils/cports.html
- Suspicious ports should be closed.
- Install process monitoring tools such as *"Whats Running"* to scan suspicious process. http://www.whatsrunning.net
- Install good antivirus and a firewall.
- Don't download and install applications from unknown senders

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

Online virus scanner

- www.virustotal.com
- http://virusscan.jotti.org
- www.onlinescan.avast.com
- https://www.metascan-online.com :- it uses 39 different antivirus engine

How to protect your PC fromRansomware?

1) Install anti malware software like Malware bytes in your PC.
2) Scan your every e mail attachment with Malware bytes.
3) Install Crypto Prevent in your machine.
4) If you can't restore your file do a system restore of your machine.
5) Always backup your important data in an external drive.

How to Protect Your Privacy on Your Mobile Devices

Mobile Devices will be attacked more than laptop or desktop in coming days. Most of the people will use smart phone to access websites & make payments online. Hackers know that too.

- Use a Passcode. This may sound obvious, but according to a Consumer Reports survey, 64% of us don't use our passcodes.
- Be Selective With Your Apps. Install Apps that are available in Apps store.
- Don't Click on unknown Links.
- Enable Remote Wiping. In case of your mobile gets stolen remotely wipe out your data. It comes default in every mobile. Check Security section of your settings. Alternately, you may use a free tool called "lookout" utility.https://www.lookout.com
- Keep Software Up to Date, be it Android or iPhone keep your data backed up on cloud or local drive using data cable - contacts, emails, calendar, SMS, whatsapp& other files.
- Install a good antivirus into your mobile and regularly update that.
- Stay Off of Open Wi-Fi Networks. Don't connect to free wifi. It is a hackers' paradise. Someone can sniff your data.
- Lock your memory card with password in case it contains sensitive data.
- Write Down Your IMEI of your phone.
- Do not exchange your mobile at mobile store or classified site like OLX. Your confidential data can be recovered if not over written using professional tools.
- Never give your password if you do not see HTTPS:// (secured site)
- Always enable 2 factor authentication for login. It will send you SMS in your mobile.

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

How they hack your website?

Hacking is a growing threat for every business both large and small. Whether it's stealing private data, taking control of your computer, or shutting down your website, hackers can seriously impact any business, at any time. Hackers can attack in so many ways here are few of them.

1) SQL Injection Attack- Attacker can take control of your admin panel and database.
2) Cross Site Scripting (XSS) attack- Attacker can hijack the user's session.
3) Broken Authentication and Session Management Attack - allows attackers to compromise passwords, keys, session tokens.
4) Security Misconfiguration attack - it can lead to the whole system being compromised.
5) DDOS Attack - Website does not respond to users' request.
6) Invalidated Redirects and Forwards attack - can lead a user to redirect phishing and malware websites.
7) Insufficient Transport Layer Protection Attack - attackers can attack a https secure site.
8) Insecure Cryptography Storage Attack - Attacker attacks unencrypted files.
9) Directory traversal attack- Allows attackers to access restricted directories.
10) SSH brutforce Attack - Attackers tries to break SSH login credentials.

How you will protect your site from attackers?

1) Do not allow users to input single quote ' =<> symbols in any input on website.
2) Use Stored Procedures.
3) Patch your database and Operating System Regularly
4) Use Prepared Statements (Parameterized Queries).
5) Use strong encryption algorithm to store sensitive information like password etc.
6) Vulnerability scanning and penetration testing should be done every six months.
7) Disable any other DB functionality you don't need.
8) Never Insert Untrusted Data Except in Allowed Locations.
9) Block all unnecessary ports,ICMP traffics,NETBIOS and SMB.
10) Remove all unused modules, backup files and scripts from Webserver.
11) Use strong password policies and don't use default passwords.
12) Run processes using least privileged account.
13) Use error handlers that do not display debugging or stack trace information.
14) Protect server-side source-code from being downloaded by a user.
15) Implement encryption for the transmission of all sensitive information. This should include TLS for protecting the connection and may be supplemented by discrete encryption of sensitive files or non-HTTP based connections

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

How hackers get into your network?

1) Email Social Engineering/Spear Phishing attack- Attacker get into your network by sending an email attachment.
2) Sniffing attack- Attacker sniffs username/password/credit card number, etc. from the network
3) DDOS Attack - attacker clogs your network for a long time.
4) Scanning attack - Attackers can remotely scan your network to find vulnerabilities in your system.
5) Firewall/IDS evasion attack - Attacker bypasses the firewall/antivirus/IDS.
6) Outdated wireless encryption Attack.
7) Wireless jamming attack- attackers forcefully disconnects all connected users and stop others so that they can't connect to the network.
8) MAC spoofing Attack - Attackers spoof someone's MAC id and enters in your network.

How to protect your network from attackers?

1) Vulnerability scanning and network penetration testing should be done at least twice a year.
2) Take measures from MAC spoofing.
3) Use strong firewall and Intrusion Detection system (IDS). Make sure they can't be bypasses.
4) All network communication should be encrypted.
5) Use VPN, SSh for remote communication.
6) Use ingress filtering and load balancer to protect network from DDOS attack.
7) Permanently add the MAC address of the gateway to the ARP cache.
8) Use IPv6 instead of IPv4.
9) Use IP Security(IPSec) in your network.
10) Use tools to check whether any machine running in promiscuous mode.
11) Use DHCP snooping binding tables.
12) Use Dynamic ARP inspection.
13) Use appropriate security to switches so that they can not be flooded.
14) Use a strong Intrusion Prevention system.
15) Use a good antivirus and antimalware in network and regularly update those.

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of Ethical Hacking

Are our kids safe?

On Social Media:

- 73% of under 13 age are from metro cities
- 85% of under 16 age are from metro cities

Impact:

- Cyber Bulling
- Sextortion by paedophiles
- Revenge Porn uploading morphed nude image on social media with real phone number, with source IP masked using TOR
- Reveal private information

Mitigations:

- Resources: http://stopcyberbullying.org/index2.html
- Wiki guide - http://en.wikipedia.org/wiki/Internet_safety
- Facebook report page: https://www.facebook.com/help/263149623790594

Various Cyber Scams

- Nigerian Scam / 419 Scam - Offers your money
- Money Mule Scam / Job Scam - Offers you job
- Lottery Scam - Offers your money
- Phishing Scam - Ask you to put password on fake website
- Smishing (SMS) - Contact you via SMS or whatsapp (sometimes call you spoofing your friend's number)
- Advance Scam (Friend abroad / Romance Angle)

In all cases, they will ask you to send some minor processing fees of US$100 for you to get $100,000 or a job or a Russian girlfriend. You lose whatever you pay.

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of
Ethical Hacking

In coming days, we wish to fill up the void of well trained IT Security professional in India. As per Nasscom survey, India needs 500,000 IT security professionals in coming 5 years, while we currently have only 37,000 working in the industry.

We wish to make Kolkata the IT SECURITY HUB OF INDIA.

********** ● **********

ISOEH
Indian School Of Ethical Hacking

Indian School of Ethical Hacking

ISOEH (www.isoeh.com & www.isoeh.in) with offices at India and Singapore has 15 years of experience in IT Security Industry working with Governments, Military and Corporates as clients; is trying best to promote IT security awareness among the mass. Promoters of ISOEH are certified ISO / IEC 27001: 2013 Auditors, CEH (Certified Ethical Hacker) and CHFI.(Forensic Experts)

We have reached out to colleges, corporates, PSU, law enforcement depts. to provide all support.

ISOEH is into 1st party audit, penetration testing, research, full-disclosure, corporate training in Information Security & Cyber Security; providing anti hacking services to companies who has got hacked or may face the threat of being hacked.

In coming days, we wish to fill up the void of well trained IT Security professionals in India. As per Nasscom survey, India needs 500,000 IT security professionals in coming 5 years, while we currently have only 37,000 working in the industry. ISOEH currently trains around 500 professionals per year. **We wish to make Kolkata the IT SECURITY HUB OF INDIA**.

Infinity Benchmark Building
18th Floor
Saltlake Electronics Complex
Sector - V, Kolkata 700091

D/24, Katju Nagar
1st Floor, Kolkata-32
(Beside South City Mall)

17 Phillip Street
Room #06-00
Grand Building
Singapore - 048695

Web: www.isoeh.com&www.isoeh.in , Facebook: www.facebook.com/isoeh.in,

Twitter: https://twitter.com/isoeh Email: sandeep@isoeh.com, abir@isoeh.com ,

Mob: +91 9830310550, +91 9434243285

Public Relations Society of India
Kolkata Chapter

ISOEH
Indian School Of
Ethical Hacking