Data Security : An Analysis

Dr.S.B.Thorat
Director,
Institute of Technology and Management,
Nanded, (Maharashtra), India
suryakant_thorat@yahoo.com

S.K.Nayak
Head,
Department of Computer Science
Bahirji Smarak Mahavidyalaya,
Basmathnagar, Dist- Hingoli
(Maharashtra), India
sunilnayak1234@yahoo.com

M.M.Bokhare
Head,
Institute of Technology and Management,
Nanded, (Maharashtra), India
bokaremadhav@yahoo.com

Abstract— There is intense of cyber attach through electronic media, so it calls for data security practice. Internet technology becomes very pervasive to exchange data through online. Various Government and private sectors mostly depends on Information Technology and facing problem of security breach. The precious thing on internet is the data. This data need to be protected from any damage and errors. The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them. There are many way to protect from the cyber space. The data can be protected using various techniques such as Anti-viruses, anti-malware, spyware, encryption, access control, physical security, keep backup of data regularly, and good security habit.

Keywords-*Encryption,Access control, Physical security, Backup*.

I. INTRODUCTION

Most people only aware pocket theft, bank robbery, kidnapping etc. In this cracking world, personal information is of vital importance. Security is breached by unauthorized persons called intruder in cyber world. In this case, Data security is important in vision of government as well as private sector and lot of money has been spent in the IT market. Numerous high-profile cyber-attacks or scams have occurred at database companies like ChoicePoint and LexisNexis, as well as at universities, banks, and other firms. All of these instances have aided in putting cyber security on the national agenda. Later Government made legacy against cyber crime. There are many organizations which are taking care of data security at international level. Cyber Emergency Response Team (CERT) is one of great organization which provides free solution to any attack in the world.

Data security is a major concern of both the government and the private sector. The risks are hackers, attackers, viruses, worms, botnet, rootkit, spyware, adware, Trojan horses, keylogger, and vulnerabilities. **Virus**: Program that copies itself into other programs could be transferred through infected disks, rate dependent on human use. **Worm**: A virus that uses the network to copy itself onto other computers. **Rootkits**: Imposter OS tools used by attacker to hide his tracks. **Botnets**: Network of software robots attacker uses to control many machines at once to launch attacks (e.g. DDoS through packet flooding, click fraud). **Spyware**: Software that monitors activity of a system or its users without their consent. **Keylogger**: Spyware that monitor's user keyboard or mouse input, used to steal usernames, passwords, credit card #s, etc. **Trojan Horses**: Software performs additional or different functions than advertised. **Adware**: Shows ads to users without their consent. **Clickbot**: Bot that clicks on ads, leads to click fraud (against cost-per-click or CPC ad models).

II. WHICH ARE THE RISKS

A. Hacker, Attacker, Intruder

These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting.

B. Social Engeeniring attack

To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

C. Fishing attack

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

D. Malicious code

Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the following characteristics: It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page. Some forms propagate without user intervention and typically start by exploiting software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate

via email, websites, or network-based software. Some malicious code claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder. Viruses and worms are examples of malicious code.

E. Vulnerability

In most cases, vulnerabilities are caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities (Understanding Patches).

F. Denial of service attack

Denial-of-service attacks can be difficult to distinguish from common network activity, but there are some indications that an attack is in progress. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular web site into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

G. Distributed Denial of Service (DDoS) attack

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including ours, to launch the denial-of-service attack.

III. GOOD SECURITY HABBITS

A. Minimize the access of other people

You may be able to easily identify people who could, legitimately or not, gain physical access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe others. Identifying the people who could gain remote access to your computer becomes much more difficult. As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information; however, you can develop habits that make it more difficult.

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information. Disconnect your computer from the internet when you aren't using it.

The developments of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled.

B. Firewall

When anyone or anything can access your computer at any time, your computer is more susceptible to being attacked. You can restrict outside access to your computer and the information on it with a firewall.

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary internet traffic. Firewalls can be configured to block data from certain locations while allowing the relevant and necessary data through (see Understanding Denial-of-Service Attacks and Understanding Hidden Threats: Rootkits and Botnets for more information). They are especially important for users who rely on "always on" connections such as cable or DSL modems.

C. Anoid being a victim

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send sensitive information over the Internet before checking a web site's security. Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available

online from groups such as the Anti-Phishing Working Group (APWG). Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. Don't use cyber cafes, there is risk of viruses and keylogger.

Keylogger is an application which keep log of your key in a file. Someone can steal information you typed on keypad. Use the virtual keypad without using physical keypad. Don't directly access unknown links of sites through email links. It may be scam and don't response it.

D. Responding to attack

1) Avoid being part of problem

There are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers: Install and maintain anti-virus software .Install a firewall, and configure it to restrict traffic coming into and leaving your computer. Follow good security practices for distributing your email address applying email filters may help you manage unwanted traffic.

2) Knowing attach happening

Not every attack is denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack: unusually slow network performance (opening files or accessing web sites) unavailability of a particular web site inability to access any web site dramatic increase in the amount of spam you receive in your account.

3) Avoid being part of problem

Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack. Contact the appropriate technical professionals for assistance. If you notice that you cannot access your own files or reach any external web sites from your work computer, contact your network administrators.

4) Avoid being part of problem

If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity. If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account. Consider reporting the attack to the police, and file a report with the Federal Trade Commission (FTC).

IV. CONCLUSION

Government should not assert authority in ways that would make private sector assumption of security responsibility impossible in the future as technology advances or conditions changes. Data security is important in vision of government as well as private sector and lot of money has been spending in the electronic market. Identity theft, data security breaches, viruses, and other online insults are spawning intense calls for government intervention.

ACKNOWLEDGMENT

We are thankful to Hon. Ashok Chavan (Chief Minister, Maharashtra) India, Society members of Shri. Sharada Bhawan Education Society, Nanded. Also thankful to Shri. Jaiprakash Dandegaonkar (Ex-State Minister, Maharashtra), Society members of Bahirji Smarak Vidyalya Education Society, Wapti for encouraging our work and giving us support.

Also thankful to our family members and our students.

REFERENCES

[1] J.P. "Information security in a multi-user computer environment," in Advance in computers, Vol. 12, Morris Rubinoff (Ed.), Academic Press, New York.
[2] Internet Security Alliance, Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices, July 2002. http://www.isalliance.org/news/BestPractices.pdf.
[3] Preventing Identity Theft and Data Security Breaches: The Problem with Regulation by Clyde Wayne Crews Jr. and Brooke Oberwetter.
[4] Fred Avolio, "Securing Cyberspace—Comments On the National Strategy, Net Sec Letter #21, October 2, 2002 http://www.avolio.com/columns/21-SecuringCyberspace.HTML.
[5] http://www.antiphishing.org/phishing_archive.html
[6] http://www.ftc.gov/
[7] http://www.wikipedia.com
[8] http://www.pfgeni.com
[9] http://www.pdf-search-engine.com

AUTHORS PROFILE

Authors Profile …

Dr.S.B.Thorat completed his M.Sc. (ECN) degree in 1986 from Pune University, India and his M.E. degree in Computer science and Engineering in 1996 from TTTI Chandigarh and Ph.D. in 2009 from India. He is now working as a Director at the Institute of Technology and Management Nanded (Maharashtra), India from last 10 years. He is having total 24 years teaching experience. He is having 09 international publications. Presently he is acting as a Dean of faculty of Computer studies at Swami Ramanand Teerth Marathwada University, Nanded.

S.K.Nayak
M.Sc. (Computer Science), D.B.M, B.Ed.
He completed M.Sc. (Computer Science) from S.R.T.M.U, Nanded. In 2000 he joined as lecturer in Computer Science at Bahirji Smarak Mahavidyalaya, Basmathnagar. From 2002 he is acting as a Head of Computer Science department. He is doing Ph.D. He attended many national and international conferences, workshops and seminars. He is having 10 international publications. His interested areas are ICT, HCI, Green Computing,tec.

Bokhare M.M. completed his B.E. (CSE) from M.G.M. College, Nanded in 2001. He appeared for M.E. (CSE) in the same college. He completed his M.B.A. from Y.C.M.O.U, Nashik. He is now working as a Head of the department in Institute of Technology and Management, Nanded from last 05 years. He is having 05 national and 05 international publications.