International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A REVIEW PAPER ON CYBER SECURITY

[1]Akshat Jain, [2]Rohini Sharma
[1]Student
Department of CSE
Chandigarh University, Gharuan
[2]Assistant Professor
Department of CSE
Chandigarh University, Gharuan
[1]19bcs1003@gmail.com, [2]rohinie7721@cumail.in

Abstract: *This paper is aimed particularly at readers concerned with major systems employed in medium to large commercial or industrial enterprises. It examines the nature and significance of the various potential attacks, and surveys the defense options available. It concludes that IT owners need to think of the threat in more global terms, and to give a new focus and priority to their defense. Prompt action can ensure a major improvement in IT flexible at a modest marginal cost, both in terms of finance and in terms of normal IT operation. Cyber Security plays an important role in the development of information technology as well as Internet services. Our attention is usually drawn on "Cyber Security" when we hear about "Cyber Crimes". Our first thought on "National Cyber Security" therefore starts on how good is our infrastructure for handling "Cyber Crimes".*

Keywords: Security, Dependability, Cryptography, Networked Systems, Crime, Protection, cyber safety, e-commerce.

I. INTRODUCTION

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized. Cybercrime bounds any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet. A major part of Cyber Security is to fix broken software, a major attack aim of Cyber Crime is to exploit broken software. Software security accountability are caused by defective specification, design, and implementation. The commonly accepted definition of cyber security is the protection of any computer system, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether accidental or intentional. Cyber attacks can come from internal networks, the Internet, or other private or public systems. Businesses cannot afford to be indifferent of this problem because those who don't respect address, and counter this threat will surely become victims. Unfortunately, common development practices leave software with many vulnerabilities or accountability.

Figure 1: Cyber security

To have a secure US cyber infrastructure, the supporting software must contain few, if any, vulnerabilities. The trend involves exploiting vulnerabilities that go as far back as 2009 in Office documents. Other cross-platform, third-party technologies favored by hackers include Java, Adobe PDF and Adobe Flash. Cyber security depends on the care that people take and the decisions they make when they set up, maintain, and use computers and the Internet. Cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. The problem of End-User mistakes cannot be solved by adding more technology; it has to be solved with a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management .The potential seriousness of cybercrime is even greater if it affects critical IT systems of telecommunications, power distribution, banking or transport, i.e. of the infrastructure on which virtually all individual companies depend . Such concerns led the US President to set up a Commission on Critical Infrastructures. However, in this paper we deal only with the defense of corporate IT systems. Such cybercrimes cannot be considered separately for individual systems, because of the rapidly growing interconnectivity between IT systems, via Intra-nets, Extra-nets and the Internet itself, as well as by direct physical interconnection, or exchangeable storage media such as diskettes or magnetic disks. Such interconnectivity (often unintended, rarely appropriately planned) turns separate IT systems into components of what is in effect a single large super system that might suffer an overall failure, or whose data or software may be seriously polluted as a result of a single malicious act (or accident).

II. CYBER SECURITY AND CYBER CRIME

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one Major challenge. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. 37 Enhancing cyber security and protecting critical information infrastructures are essential to each nation’s security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.

The legal, technical and institutional challenges posed by the issue of cyber security are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

III.ADVANTAGES AND RISKS

However, the growth of the information society is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs.23 Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Attacks against information infrastructure and Internet services have already taken place. Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. the financial damage caused by cybercrime is reported to be enormous. On the other hand, most of our industrial IT infrastructure is still sufficiently fragmented that there remains a window of opportunity to guide its evolution towards improved security through the progressive introduction of components, such as interface controllers, that provide more effective defenses in the face of hostile attack. When properly implemented and managed, such interface controllers (guards, gateways and firewalls) can greatly enhance the security of systems involving the following classes of data flow - particularly where these do not already benefit from end-to-end encryption.

IV.THREATS TO CYBER SECURITY

Threats to cyber security can be roughly divided into two general categories: actions aimed at and intended to damage or destroy cyber systems and actions that seek to exploit the cyber infrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure―cyber exploitation. While some intrusions may not result in an immediate impact on the operation of a cyber-systems, as for example when a ―Trojan Horse infiltrates and establishes itself in a computer, such intrusions are considered cyber-attacks when they can thereafter permit actions that destroy or degrade the computer’s capacities. Cyber exploitation includes using the Internet and other cyber systems to commit fraud, to steal, to recruit and train terrorists, to violate copyright and other rules limiting distribution of information, to convey controversial messages (including political and ―hate‖ speech), and to sell child pornography or other banned materials. Following are some new threats to cyberspace. With the proliferation of free hacking tools and cheap electronic devices such as key loggers and RF Scanners, if you use e-mail or your company’s systems are connected to the Internet, you’re being scanned, probed, and attacked constantly. This is also true for your vendors and supply chain partners, including payment processors. E-mail and the web are the two main attack vectors used by hackers to infiltrate corporate networks. So, clearly, every company is vulnerable because every company needs to have these functions. Conversely every company needs to guard its systems against unauthorized access through these openings because supposed firewalls offer no protection whatsoever once a hacker has entered.

V. DEVELOPMENT OF SOFTWARE TOOLS THAT AUTOMATE THE ATTACKS

Recently, software tools are being used to automate attacks. With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers – e.g. through a botnet – he/she can increase the scale still further. Since most of these software tools use preset methods of attacks, not all attacks prove successful. Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad- based attacks, as the companies developing protection software examine attack tools and prepare for the standardized hacking attacks. High-profile attacks are often based on individually-designed attacks.

VI. ILLEGAL ACCESS

The offence described as ―hacking refers to unlawful access to a computer system191, one of oldest Computer related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government. Examples of hacking offences include breaking the password of password-protected websites and Circumventing password protection on a computer system. But acts related to the term ―hacking‖ also Include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system, setting up ―spoofing‖ websites to make users disclose their Passwords and installing hardware and software-based key logging methods (e.g. ―key loggers‖) that Record every keystroke – and consequently any passwords used on the computer and/or device. Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone. Three main factors have supported the increasing number of hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks. Interception of communications is normally undetectable and, in the absence of suitable countermeasures, offers a tempting target to attackers. In appropriate computer systems, unofficial access to data-bases, etc., can be monitored and, where this has been done, it has produced ample evidence that probing attacks are indeed taking place on a substantial and increasing scale. In the present context we regard all attacks which solely seek to gain information, from communications or computers, as ―passive.

VII. MOBILE DEVICES AND APPLICATIONS

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber-attack as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

VIII. SOCIAL MEDIA NETWORKING

Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

IX. CLOUD COMPUTING

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

X. PROTECT SYSTEM RATHER THAN INFORMATION

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

XI. NEW PLATFORMS AND DEVICES

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. But the proliferation of new platforms and new devices - the iPhone, the I Pad, Android, for example - will likely create new threats. The Android phone saw its first Trojan this summer, and reports continue with malicious apps and spyware, and not just on Android.

XII. WHAT COULD HAPPEN

Lots of things: all of them bad. Accordingly, a company (particularly franchise businesses and other licensors) must evaluate its risk to determine and implement appropriate policies and procedures. We have formulated a ―Chan Scale of Cyber In-Security‖, based on the potential harm that can be caused: 1 Chan – Low risk. Hacker has gained entry to system but minimally.

Minor risk of business disruption, but access can aid attackers in information gathering and planning future attacks. 2 Chans – Medium Risk. Malware has been implanted in the company's network, which could cause malfunctions and mischief. There is a significant risk of a business disruption that could result in financial loss and/or damage of goodwill. 3 Chans – Medium-to- High Risk. Using sniffers or other equipment, hackers have obtained personally identifiable information (PII) from point of sale (POS) systems. There is a significant risk of a business disruption that could create financial loss and/or damage of goodwill. 4 Chans – High Risk. Inside job: data stolen by disgruntled employee. There is a potential risk of business disruption, resulting in financial loss and damage of goodwill. PII may be taken, as well as company's confidential information and financial information. 5 Chan's – Critical Risk. Hackers have gotten into the system and can access PII as well as the company's financial information and confidential information. There is a severe risk of business disruption, financial loss, damage of goodwill. System, application, and database have been compromised.

XIII. NECESSITY OF CYBER SECURITY

Information is the most valuable asset with respect to an individual, cooperate sector, state and country. With respect to an individual the concerned areas are: 1) Protecting unauthorized access, disclosure, modification of the resources of the system.

2) Security during on-line transactions regarding shopping, banking, railway reservations and share markets.

3) Security of accounts while using social-networking sites against hijacking.

4) One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defenses.

5) Need of separate unit handling security of the organization.

6) Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness

7) In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered with respect to state and country.

8) Securing the information containing various essential surveys and their reports.

9) Securing the data basis maintaining the details of all the rights of the organizations at state level.

XIV. SECURITY TRAINING AND AWARENESS

The human factor is the weakest link in any information security program. Communicating the importance of information security and promoting safe computing are key in securing a company against cyber-crime because any enterprises cannot protect the confidentiality and availability of information in today's networked environment.

Learning is a continuum; it starts with awareness, builds to training, and evolves into education.

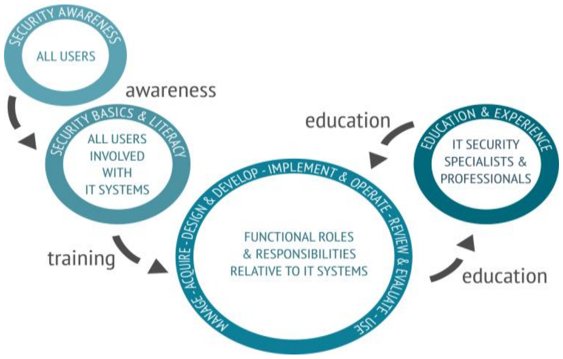
SECURITY AWARENESS
ALL USERS
awareness
SECURITY BASICS & LITERACY
ALL USERS INVOLVED WITH IT SYSTEMS
training
education
EDUCATION & EXPERIENCE
IT SECURITY SPECIALISTS & PROFESSIONALS
MANAGE - ACQUIRE - DESIGN & DEVELOP - IMPLEMENT & OPERATE - REVIEW & EVALUATE - USE
FUNCTIONAL ROLES & RESPONSIBILITIES RELATIVE TO IT SYSTEMS
education

Figure 2: Security training and awareness

Below are a few best practices:

1. Use a ―passphrase‖ that is easy to remember — E@tUrVegg1e$ (Eat your veggies) and make sure to use a combination of upper and lower case letters, numbers, and symbols to make it less susceptible to brute force attacks. Try not to use simple dictionary words as they are subject to dictionary attacks – a type of brute force attack.

2. Do not share or write down any ―passphrases. ‖

Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.

3. Do not click on links or attachments in e-mail from untrusted sources.

4. Do not send sensitive business files to personal email addresses.

5. Have suspicious/malicious activity reported to security personnel immediately. Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation. 6. Educate employees about phishing attacks and how to report fraudulent activity.

XV. CONCLUSION

This paper has examined the significance of privacy for individuals as a fundamental human right. Violations of human rights arise from the unlawful collection and storage of personal data, the problems associated with inaccurate personal data, or the abuse, or un-authorized disclosure of such data. In this paper we also includes the current threats, issues, challenges and measures of IT sector in our society. With the increasing incidents of cyber-attacks, building an effective intrusion detection model with good accuracy and real-time performance are essential. The cyber-crime as a whole refers to Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harms the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding this type of crime has become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. A computer can be a source of evidence. Even when a computer is not directly used for criminal purposes, may contain records of value to criminal investigators. So the network must be secure as no one can access the information of the computer. The risks of cyber-crime are very real and too ominous to be ignored. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thought out cyber policy, including crisis management in the event of a worst case scenario.

References

[1]. I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," J. Inf.Secur. Appl., vol. 34, pp. 183–196, 2017.

[2]. W. Wang and Z. Lu, "Cybersecurity in the Smart Grid: Survey and challenges," Comput. Networks, vol. 57, no. 5, pp. 1344–1371, 2013.

[3]. C. W. Ten, G. Manimaran, and C. C. Liu,"Cybersecurity for critical infrastructures: Attack and defense modeling," IEEE Trans. Syst. Man,Cybern. Part ASystems Humans, vol. 40, no. 4, pp. 853–865, 2010.

[4]. J. Walker, B. J. Williams, and G.skelton,"Cybersecurity for emergency management," Technol. Homel. Secur. HS2010 IEEE Int. Conf., pp. 476–480, 2010.

[5]. J. J. Walker, T. Jones, M. Mortazavi, and R. Blount, "CyberSecurity Concerns for Ubiquitous/Pervasive Computing Environments," 2011 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov., pp. 274–278, 2011.

Author Profile

Akshat Jain is pursuing B.E in Computer Science Engineering (2019-2023) from Chandigarh University. He is first year student and having deep interest in "Cyber Security".

Rohini Sharma received the B.tech and M.tech degrees in Computer Science & Engineering from Punjab Technical University in 2008 and 2015, respectively. She is having teaching experience of 11 years as an Assistant Professor. Her research area is Networking and published nine papers in this field earlier.