ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Review of Today's Important Security Mechanism: Cyber Security

Roshan G. Uke

Itrons Technologies, Amravati, Maharashtra, India

ABSTRACT: Security is paramount important in almost all the areas of information Technology. And today's world of IT is becoming completely digitalized, with the growing use of computer and internet. Along with this, the number of mobile users, digital applications and data networks increase, at the same time and amount it increases the opportunities for exploitation. Security of most valuable information is crucial for all type of businesses and application. Customer and client information, payment and transaction information, personal files, bank details, etc. all of this information is often impossible replace if lost and dangerous if gets in hands of criminals. Network outages, data compromised by hackers, computer viruses and other incidents affect our lives in many ways that range from inconvenient to life-threatening. So, to tackle with this and to live without providing any threat to our important applications and data, in this paper we are going to study the most important technique of security i.e. Cyber security. It is the most important security in information technology that focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. This paper performs the brief study of cyber security mechanism and techniques to apply security to our important digital assets.

KEYWORDS: Attacks, Cyber Security, vulnerability, Disaster recovery plan (DRP), information security (infosec).

I. INTRODUCTION

With the sophistication of our modern community becomes a source of vulnerability in itself. While rapid technological developments have provided vast areas of new opportunity and potential sources of efficiency for most of all organizations. These new technologies have also brought unprecedented threats with them. Now a days we are becoming highly dependent on computer, information technology and internet. This drives most of the critical industries such as aviation, electricity and water supply, banking and finance and telecommunications networks, etc. And this dependency on information technology makes us potentially vulnerable to cyber-attacks that serves to disrupt the most useful information. This will lubricates our economy as well as system of government [1].

Data is most valuable assets of today's world of Information Technology. But, the Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. To tackle with this the most important concept, Cyber Security, also known as Computer Security or IT security is arrived. Cyber Security is the protection of information systems from theft or damage to the hardware, software, and to the information on them as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, One another parameter is due to malpractice by operators, whether it may be intentional, accidental, or any other being tricked into deviating from secure procedures. The field of security in terms of cyber security is growing on increasing due to the increasing reliance on computer systems in most of all societies. Along with this the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things – and of the Internet and wireless network such as Bluetooth and Wi-Fi are also getting more useful by all.

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks. Traditionally it has been to focus most resources on the most crucial system components that protect against the biggest known threats. This tried to necessitate leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. To deal with this current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments [2].

There are lots of variations is going on continuously from traditional days to current needs, few of them are studied in section II of this paper under literature survey. Many of all the businesses from large to small need to do more to protect against growing cyber threats. As larger companies take steps to secure their systems, less secure small businesses are easier targets for cyber criminals. So, section III contains different elements of cyber security along with different security mechanisms to be followed. As said earlier world is moving towards completely digitalized and that will increases the application areas of cyber security. In this paper, section IV gives the brief overview of different applications of cyber security. Now, as we come to know the cyber security is of paramount important in almost all sectors, of normally all individuals to all corporate users. So it is necessary to define certain strategies to perform more secure computing task. Section V, in this paper defines some strategies that should be followed by mostly government of every country. One another interesting thing mentioned in section VI of this paper, is the Glossary of term in the alphabetic order, explaining different important terms related to cyber security. In this way, the complete paper is organized and finally in the last section VI, I have concluded the paper.

II. LITERATURE SURVEY

The Internet has undergone astounding growth, by nearly any measure, in recent years. The number of Internet users increased from roughly 360 million in 2000 to nearly two billion at the end of 2010. The number of hosts connected to the Internet increased from fewer than 30 million at the beginning of 1998 to nearly 770 million in mid-2010. According to industry estimates, this global network helps facilitate $10 trillion in online transactions every single year [3].

With the growing use of internet and digitalized users, Cyber-attacks on Internet commerce, vital business sectors and government agencies have grown exponentially. Some estimates suggest that, in the first quarter of this year, security experts were seeing almost 67,000 new malware threats on the Internet every day. This means more than 45 new viruses, worms, spyware and other threats were being created every minute – more than double the number from January 2009. As these threats grow, security policy, technology and procedures need to evolve even faster to stay ahead of the threats.

According to a December 2010 analysis of U.S. spending plans, the federal government has allotted over $13 billion annually to cybersecurity over the next five years.

During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber-attacks and digital spying are the top threat to national security, eclipsing terrorism [4].

Adam Vincent, CTO-public sector at Layer 7 Technologies which is a security services provider to federal agencies including Defense Department organizations, describes the problem as,

- The threat is advancing quicker than we can keep up with it.
- The threat changes faster than our idea of the risk.
- It's no longer possible to write a large white paper about the risk to a particular system.
- You would be rewriting the white paper constantly

III. ELEMENTS OF CYBERSECURITY

As we all knows that security is paramount important in all the sectors of information technology that consist of different elements. For that, it is necessary to ensure cybersecurity, requiring coordinated efforts throughout an information system. Most of the time this information system security is done by different elements of cyber security [5]. The below section give brief description about different elements of cybersecurity and the action to be taken for applying these security measures. These elements includes:

A. Application Security:

As the word suggest, Application that is the use of software, hardware, and procedural methods that performs certain type of useful computing task. And now its security that is application security encompasses the field to protect these applications from external threats that makes use of our software, hardware to provide intentional or unintentional harm to that application. These application areas encompasses, different websites, emails, mobile application, etc. all need different kinds of security in itself. Once an afterthought in software design, security is becoming an increasingly important concern during development as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats [6]. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Security Mechanisms:

- Actions taken to ensure application security are sometimes called countermeasures. The most basic software countermeasure is an ‘application firewall’ that limits the execution of files or the handling of data by specific installed programs.
- The most common hardware countermeasure is a ‘router’ that can prevent the IP address of an individual computer from being directly visible on the Internet.
- Other countermeasures include conventional firewalls, encryption/decryption programs, anti-virus programs, spyware detection/removal programs and biometric authentication systems.
- Carefully plan and address the security aspects of the deployment of a public web server in the contest of different websites [7].
- Ensure appropriate steps are taken to protect web content from unauthorized access or modification.

Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application, identifying and prioritizing potential threats and documenting adverse events and the actions taken in each case. This process is known as threat modeling. In this context, a threat is any potential or actual adverse event that can compromise the assets of an enterprise, including both malicious events, such as a denial-of-service (DoS) attack, and unplanned events, such as the failure of a storage device.

B. Information Security:

The Information is the most important and useful assets overall IT Sector, therefore it is necessary to protect them from any unauthorized access. Information security abbreviated as ‘infosec’, is the set of business processes that protects information assets regardless of how the information is formatted or whether it is being processed, is in transit or is being stored. The management of information security is at something of a crossroads, as the aptitude of hackers seems to be increasing as well, with threats seemingly coming from different devices that may be latest tablet or smartphone, your newest Internet of Things-connected device, or a good old-fashioned, easily crack able password. Information security is not a single technology; rather it a strategy comprised of the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Processes and policies typically involve both physical and digital security measures to protect data from unauthorized access, use, replication or destruction.

Infosec management can include everything from mantraps to encryption key management and malware detection. Infosec programs are important for maintaining the confidentiality, integrity and availability of IT systems and business data [8]. Many large enterprises employ a dedicated security group to implement and maintain the organization's infosec program. Typically, this group is led by a chief information security officer (CISO).

Security Mechanisms:

- Conduct an inventory to know that which type of data do you have, how to handle it and which users are accessing this data and for what.
- Once you've identified your data, keep a record of its location and move it to more appropriate locations as needed [7].
- Develop some privacy and security mechanism
- Protect data collected on the Internet
- Create layers of security according to levels of security should be provided to the data as confidential, sensitive or any other, etc.
- Back – up your data and Plan for data loss or theft

C. Network security:

The Network security is applicable to the use of network to access any remote important things in secure manner without providing any harm to them. Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, and network-accessible resources [9]. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks in both public and private sector. Most of us make use of them in everyday jobs for conducting transactions and communications among businesses, government agencies and individuals. Networks are subject to attacks from malicious sources. These Attacks can be of two categories: "Passive" that is when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal going operations.

With network security, your company will experience many business benefits, protected against business disruption, which helps keep employees productive. Network security helps your company meet mandatory regulatory compliance [10]. Because network security helps protect your customers' data, it reduces the risk of legal action from data theft.

Security Mechanisms:

- Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats.
- Secure internal network and cloud services
- Develop strong password policies
- Secure and encrypt your company’s Wi-Fi
- Encrypt sensitive company data
- Regularly update all applications
- If remote access is enabled, make sure it is secure [7].

A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security [10].

Network security components often include:

- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats,
- Virtual Private Networks (VPNs), to provide secure remote access

D. Disaster recovery plan (DRP):

Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized and the organization will be able to either maintain or quickly resume mission-critical functions. Disaster recovery plan is referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) that describes how an organization is to deal with potential disasters [11]. Typically, this recovery planning involves an analysis of business processes and its continuity need; mostly includes a significant focus on disaster prevention. Disaster recovery is becoming an increasingly important aspect of enterprise computing. As a consequence, recovery plans have also become more complex. Current enterprise systems tend to be too large and complicated for such simple and hands-on approaches, however, and interruption of service or loss of data can have serious financial impact, whether directly or through loss of customer confidence.

Appropriate plans vary from one enterprise to another, depending on variables such as the type of business, the processes involved, and the level of security needed. Disaster recovery planning may be developed within an organization or purchased as a software application or a service from another source. It is normal case, for an enterprise to spend 25% of its information technology budget on disaster recovery [12].

IV. APPLICATIONS OF CYBERSECURITY

The application of cyber security is the vast and always going with the today’s digitalized world of computer and information technology. The application area encompasses from Governments, military, corporations, financial institutions, and healthcare ecosystems. It also consist of other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. This suggest us that cybersecurity is paramount important in most of all the application in todays digitalized world.

V. STRATEGIES TO APPLY

To achieve our objectives related to cyber security any Government should applies the following strategic priorities [13]:

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest.
- Educate and empower all users with the information, confidence and practical tools to protect themselves online.
- Partner with business to promote security and resilience in infrastructure, networks, products and services.
- Model best practice in the protection of government ICT systems, including the systems of those transacting with government online.
- Promote a secure, resilient and trusted global electronic operating environment that supports complete national interests.
- Maintain an effective legal framework and enforcement capabilities to target and prosecute cybercrime.
- Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

VI. IMPORTANT GLOSSARY OF TERMS

The cybersecurity is an important terms for all computer users and all the people that’s comes directly or indirectly in contact with today’s world of information technology. So, here in this section I am giving, an interesting but important alphabetic glossary of terms related to cybersecurity. There are lots of terms available related to cyber security in our alphabetic order but here I am giving, just a single but more important term to know about cybersecurity [15].

Adware
Adware’s are any software application that displays advertising banners while the program is running. They often includes code that tracks a user’s personal information and passes it on to third parties without the user’s authorization or knowledge. And if you gather enough of it, adware slows down your computer significantly. Over time, performance can be so degraded that you are unable to work properly.

Blended Threat
It is called as a computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods—for example, using characteristics of both viruses and worms. This will create one of the type of infection to our working system.

Cyber Security
Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Cyber exercise
A planned event perform during which an organization simulates a cyber-disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from any type of disruption.

Computer Network Defense Analysis
It is the defensive measures uses and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Cyberbullying
It is the sending or posting of harmful, cruel, rude or threatening messages, or slanderous information, text or images using the Internet or other digital communication devices.

Dumpster Diving
It is the recovering of files, letters, memos, photographs, IDs, passwords, checks, account statements, credit card that offers and more from garbage cans and recycling bins. This information can then be used to commit identity theft.

Evil Twins
These are the fake wireless Internet hot spot that looks like a legitimate service. When victims connect to the wireless network, a hacker can launch a spying attack on their transactions on the Internet, or just ask for credit card information in the standard pay-for-access deal.

Firewall
It can be said as A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized. It is a capability or mechanism for limiting the network traffic between networks and/or information systems

Grooming
It is the Use of internet to manipulate and gain trust of a minor as a first step towards the future sexual abuse, production or exposure of that minor. Sometimes involves developing the child’s sexual awareness and may take days, weeks, months or in some cases years to manipulate the minor.

Hazard
It is the most important term that threaten our computer, storage or network system. It is a natural or man-made source or cause of harm or difficulty.

Information system resilience
The ability of an information system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and whenever important recover it properly and effectively in a timely manner.

Key
The numerical value used mostly for providing security to important information or software application. It is used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Legal Advice and Advocacy
Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. It advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Malicious logic
Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Network resilience
The ability of a network to provide continuous operation i.e., highly resistant to disruption and able to operate in a degraded mode if damaged or recover effectively if failure does occur and also scale to meet rapid or unpredictable demands.

Outsider threat
A person or group of persons external to an organization who are not authorized to access its assets and pose a potential risk to the organization and its assets.

Patch
A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and/or operating system may be configured to check automatically for patches, or you may need to periodically visit the manufacturers' websites to see if there have been any updates.

Risk
The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences. It is also called as a structured approach to managing risks to data and information by which an organization selects and applies appropriate security controls in compliance with policy and commensurate with the sensitivity and value of the data.

Skimming
It is the high-tech method by which thieves capture your personal or account information from your credit card, driver's license or even passport using an electronic device called a "skimmer." Such devices can be purchased online for under $50. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the device or an attached computer. Skimming is predominantly a tactic used to perpetuate credit card fraud, but is also gaining in popularity amongst identity thieves.

Tailored trustworthy space
A cyberspace environment that provides a user with confidence in its security, using automated mechanisms to ascertain security conditions and adjust the level of security based on the user's context and in the face of an evolving range of threats.

URL Obfuscation

Taking advantage of human error, some scammers use phishing emails to guide recipients to fraudulent sites with names very similar to established sites. They use a slight misspelling or other subtle difference in the URL, for example "monneybank.com" instead of "moneybank.com" to redirect users to share their personal information unknowingly.

Vishing
Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official looking message in an email or a pop-up advertisement that urges them to act immediately, but in a vishing scam, they are urged to call the phone number provided rather than clicking on a link.

Whitelist
It is the list of entities that are considered trustworthy and are granted access or privileges to perform their task.

Zombie Computer
A remote-access Trojan horse installs hidden code that allows your computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks. Authorities have a harder time tracing criminals when they go through zombie computers.

VII. CONCLUSION

Here, we have seen that in the today's advance world the pace of technological change and broader developments is growing on increasing. This will also give rise to online threat environment and that is necessary to undertake ongoing evaluation and regular reviews of the appropriateness by applying proper security mechanism. And this would be possible by the most important security mechanism that we have seen in this paper that is Cyber Security activities. The process of evaluating the effectiveness of the cyber security policy is possible by different elements of cyber security mention in earlier section. With the rapid escalation in the intensity and sophistication of cyber crime and other cyber security threats, it is imperative that government, business and the community should have to be aware of this cyber security policies. So, it becomes today's need to apply the cyber security mechanism in the world of computer and information technology to secure variety of applications and data.

REFERENCES

[1] Cyber Security Strategy [Online] available: www.ag.gov.au/cybersecurity
[2] What is Cyber Security? [Online] available: http://www.itgovernance.co.uk/what-is-cybersecurity.aspx
[3]Cyber SeCurity Strategy [Online] available: https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf
[4] National Cyber Security Framework Manual [Online] available: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
[5] Cybersecurity and Its Ten Domains [Online] available:https://www.coursera.org/learn/cyber-security-domain
[6] http://searchsoftwarequality.techtarget.com/definition/application-security
[7]Cyber Security Planning Guide [Online] available: https://transition.fcc.gov/cyber/cyberplanner.pdf
[8] http://searchsecurity.techtarget.com/definition/information-security-infosec
[9] https://en.wikipedia.org/wiki/Network_security
[10] http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/What_is_network_security/index.html
[11] http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan
[12] http://searchdisasterrecovery.techtarget.com/definition/business-continuity-action-plan
[13]Cyber SeCurity Strategy [Online] available: https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf
[14] Cybersecurity, Innovation and The Internet Economy [Online] available: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf
[15] Explore Terms: A Glossary of Common Cybersecurity Terminology [Online] available: https://niccs.us-cert.gov/glossary