International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Security Intelligence

M. Swetha, L. Prabha, S. Rajadharani

Sri Krishna Adthiya College of Arts and Science College, Coimbatore, Tamil Nadu, India

ABSTRACT

Governments, military, organizations, financial institutions, universities and other businesses collected, process and store a large amount of confidential information and data on computers and transmit that data over networks to other computers. With the continuous rapid growth of volume and sophistication of cyberattacks, quick attempts are required to secure sensitive business and personal information, as well as to protect national security. The paper details about the nature of cyberspace and shows how the internet is unsecure to transmit the confidential and financial information. We demonstrate that hacking is now common and harmful for global economy and security and presented the various methods of cyber attacks in India and worldwide.

How to cite this paper: M. Swetha | L. Prabha | S. Rajadharani "Cyber Security Intelligence" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.894-897, URL: https://www.ijtsrd.com/papers/ijtsrd29261.pdf

IJTSRD29261

INTRODUCTION:

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network.[1] The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming.

CYBER SECURITY TECHNOLOGIES:

Cyber security is defined as technologies and processes constructed to protect computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through Internet by cyber criminals, terrorist groups and hackers. Cyber security is related to protecting your internet and network based digital equipment and information from unauthorized access and alteration. Internet is now not only the source of information but also has established as a medium through which we do business, to advertise and sell our products in various forms, communicate with our customers and retailers and do our financial transactions. The internet offers lots of benefits and provides us opportunity to advertise our business across the globe in minimum charges and in less human efforts in very short span of time. As internet was never constructed to track and trace the behaviour of users. The Internet was actually constructed to link autonomous computers for resource sharing and to provide a common platform to community of researchers. As internet offers on the one hand huge number of benefits and on the other hand it also provides equal opportunities for cyber-terrorists and hacker. In today's Internet-connected world where technologies underpin almost every facet of our society, cyber security and forensic specialists are increasingly dealing with wide ranging cyber threats in almost real-time conditions. The capability to detect, analysis, and defend against such threats in near real-time conditions is not possible without employment of threat intelligence, big data, and machine learning techniques. For example, when a significant amount of data is collected from or generated by different security monitoring solutions, intelligent and next-generation big-data analytical techniques are necessary to mine, interpret, and extract knowledge of these unstructured/ structured data. Thus, this gives rise to cyber threat intelligence and analytic solutions, such as big data, artificial intelligence, and machine learning, to perceive, reason, learn, and act against cyber adversary tactics, techniques, and procedures.

INFORMATION OF CYBER SECURITY

In the article entitled "Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection authored" by Pierre Parrend, Julio Navarro, Fabio Guigou, Aline Deruyver, and Pierre Collet [3], another

analysis of multi-step attack is presented. In this paper, the authors provide a review of the two main approaches for tracking hard-to-find cyberattacks: statistical analysis and machine learning, which are the two domains of data analysis. The authors propose a comprehensive framework for the study of complex attacks and related analysis strategies through statistical tools, on the one side, and machine learning tools, one the other side. It puts these complex attacks in perspective with their core applications in the security domain: detection and investigation. Transaction traces analysis is a key utility for marketing, trend monitoring, and fraud detection purposes. A good source of such traces are Points-of-Sale (POS) which are devices representing the transactions' checkout processes.

ISSUES OF CYBER SECURITY:

The management of risk to information systems is considered fundamental to effective cyber security. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). Most cyber attacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Reducing such risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts. The federal role in cyber security involves both securing federal systems and assisting in protecting non federal systems. Under current law, all federal agencies have cyber security responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. On average, federal agencies spend more than 10% of their annual ICT budgets on cyber security. More than 50 statutes address various aspects of cyber security. Five bills enacted in the 113th Congress and another in the 114th address the security of federal ICT and U.S. CI, the federal cyber security workforce, cyber security research and development, information sharing in both the public and private sectors, and international aspects of cyber security. Other bills considered by Congress have addressed a range of additional issues, including data

CYBER DEFAMATION LAW:

Cyber defamation is not a specific criminal offense or tort, but rather defamation or slander conducted via digital media, usually through the Internet. Penalties for "cyber defamation" vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights. Stopping or addressing defamation can be difficult. If the person has no serious grudge, then a cease and desist letter may stop the behaviour and get the statements removed from the Internet. On the other hand, if the person is acting out of spite, it may be necessary to file a report with the police depending on local law.

FROM INFORMATION SECURITY TO CYBER SECURITY:

All security is about the protection of assets from the various threats posed by certain inherent vulnerabilities. Security processes usually deal with the selection and implementation of security controls (also called countermeasures) which help to reduce the risk posed by these vulnerabilities (ISO/IEC 27002, 2005; Farn et al., 2004; Gerber and Von Solms, 2005). In the case of ICT security, the asset(s) that need to be protected are the underlying information technology infrastructure. Information security, on the other hand, extends this definition of the assets to be protected to include all aspects of the information itself. It thus includes the protection of the underlying ICT assets, and then goes beyond just the technology to include information that is not stored or communicated directly using ICT . However, as demonstrated in the scenarios above, in cyber security the assets that need to be protected can range from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure, such as. In fact sets include absolutely anyone or anything that can be reached via cyberspace. It is thus the assertion of this paper that the term cyber security is related, but not analogous, to the term information security. In cyber security, information and ICT are the underlying cause of the vulnerability. and communication infrastructure. However, the single most defining characteristic of cyber security is the fact that all assets that should be protected need to be protected because of the vulnerabilities that exist as a result of the use of the ICT that forms the basis It is still possible for the assets dealt with in security to include information itself, or even information of cyberspace.

CYBER CRIME IN INDIA:

In 2013, total 4,356 cases were reported under IT Act while this figure was 2,876 in 2012. In other words, there was rapid growth about 51.5% from 2012 to 2013. 681 cases about 15.6% were registered from Maharashtra. In Andhra Pradesh 635 cases were registered under same Act, followed by Karnataka (513 cases) and Uttar Pradesh with 372 cases. About 45.1% (1,966 cases) were related to hacking of websites and damage of computer resources. There were 1,337 cases related to cybercrime, registered under different sections of IPC during 2013 while this figure was around 601 in 2012. This shows a rapid increase, around 122.5% in a year. Only in Uttar Pradesh 310 cases were registered from 1,337 cases. Maharashtra holds second positions with 226 cases followed by Haryana with 211 cases. Most of the cases, out of total 1,337 cases were related to forgery and financial fraud. From the 1,337 cases, 747 cases were registered under forgery category while 518 cases fall in fraud. Cyber Crime Growth in India Year Cases Registered Under IT Act Person Arrested 2010 966 799 2011 1,791 1,184 2012 2,876 1,522 2013 4,356 2098 Although, All these (1,337) offences were put in traditional IPC crimes but somewhere these were related to cyber crime wherein computer systems and internet were used to conduct such offences . Uttar Pradesh was the state with the highest number (219) of cyber forgery followed by Maharashtra with 215. Statistics depicted in the table 1.show that cyber crimes are rapidly growing in numbers and sophistication as well. We still require a technique or procedure to control cyber crimes. As the statistics of the arrested people show that there is a huge gap between cases registered and the person arrested. It means we are not reaching and arresting all the criminals who commit such types of cyber crimes. Note: the data of table 1 has been taken from A Report on, Crime in India 2013 compendium, National Crime records Bureau, Ministry of Home affairs, Govt. of India. 8. CONCLUSION In this paper, we have detailed about the nature of cyberspace

AND THE WEAKEST LINK IS….

Humans are inherently complex and multi-faceted creatures with our own agendas, influences, faults, beliefs, and

priorities. Sometimes we're also simply just too trusting. Even the most hardened system can be breached through social engineering – the 'hacking' of people. No amount of secure network topologies and firewalls or security software can withstand a user innocently clicking on an email link, or being convinced to give up login details over the phone by someone pretending to be from the IT department In fact a recent study by researchers at the Friedrich-Alexander University of Erlangen-Nuremberg, Germany, revealed that just over 50% of people click on links in emails from strangers, even when they were aware of the risks. 4 And so, as a result, cyber security isn't just about technological defences: it's also about people. From the home user through to industry and government, everyone needs a basic understanding of cyber threats and how to recognise them – something which comes under the umbrella of digital literacy

CHALLENGES OF CYBER SECURITY:

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning
- End-user education

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

FIVE TYPES OF CYBER SECURITY:

- Critical infrastructure security: Critical infrastructure security consists of the cyber-physical systems that modern societies rely on. ...
- Application security: ...
- Network security: ...
- Cloud security: ...
- Internet of things (IOT) security…

BENEFITS OF MANAGING CYBER SECURITY:

- Protect networks and data from unauthorized access.
- Improved information security and business continuity management.
- Improved stakeholder confidence in your information security arrangements.
- Improved company credentials with the correct security controls in place.

WHY CYBER SECURITY IS IMPORTANT?

The average unprotected computer (i.e. does not have proper security controls in place) connected to the Internet can be compromised in moments. Thousands of infected web pages are being discovered every day. Hundreds of millions of records have been involved in data breaches. New attack methods are launched continuously. These are just a few examples of the threats facing us, and they highlight the importance of information security as a necessary approach to protecting data and systems.

INDIAN CYBER SITUTATION:

India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%.

- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA
- India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm "Symantec Corp"

VARIOUS TYPES OF HARDWARE ATTACK IN CYBER SECURITY:

Manufacture backdoor may be created for malware or other penetrative purposes. Backdoors may be embedded in radiofrequency identification (RFID) chips and memories.

- Unauthorized access of protected memory
- Inclusion of faults for causing the interruption in the normal behaviour of the equipment.
- Hardware tampering by performing various invasive operations
- Through insertion of hidden methods, the normal authentication mechanism of the systems may be bypassed.

EVOLUTION OF CYBER SECRITY:

1. viruses (1990s) Anti-Virus, Firewalls
2. Worms (2000s) Intrusion Detection & Prevention
3. Botnets (late 2000s to Current) DLP, Application-aware Firewalls, SIM
4. APT, Insiders (Current) Network Flow Analysis

HARDWARE CYBER SECURITY CONCERN:

Above hardware attacks may pertain to various devices or systems like:

- Network systems
- Authentication tokens and systems
- Banking systems
- Surveillance systems
- Industrial control systems
- Communication infrastructure devices

CYBER SECURITY INTIATIVES IN INDIA:

1. National Counter Terrorism center (NCTC):

After 26/11 attack in 2008, suddenly the Indian government realized the importance of Counter terrorism initiatives and

proposed National Counter Terrorism center(NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities. The NCTC is supposed to coordinate between various State and Central govt. agencies and serve as a single and 48 effective point of control and coordination of all counter terrorism measures. It is model on the American NCTC and Britain Joint Terrorism Analysis Centre and will derive its powers from the Unlawful Activities Prevention Act, 1967 (Mrunal, 2012).

2. National Information Security Assurance Programme (NISAP):

To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP), to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. CERT-in has established the facility for Computer Forensics for investigation of cyber crimes and to provide hands on training to the law enforcement agencies and judiciary. This infrastructure is being augmented to include network forensics and mobile forensics investigation facility. CERT-In is cooperating with defence, banks, judiciary and law enforcement agencies in training their officials as well as extending the support in investigation of cyber crimes (Srinath, 2006).

THREATS TO CYBER SECURITY:

Threats to cyber security can be generally divided into two general categories that include actions aimed at to damage or destroy cyber systems that is cyber attacks and actions that try to exploit the cyber infrastructure for illegal or damaging purposes without destructive or compromising that infrastructure that is cyber exploitation. While some intrusions may not result in an instant impact on the operation of a cyber-systems, such as when a Trojan Horuse penetrates and establishes itself in a computer, such intrusions are considered cyber-attacks when they can subsequently permit actions that obliterate or corrupt 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 breach copyright and other rules limiting distribution of information, to convey controversial messages that comprises of political and hate speech and to put up for sale child pornography or other banned materials.

CONCLUSION:

As technology continues to integrate computing, networking, and control elements in new cyber- physical systems, we also need to train a new generation of engineers, computer scientists and social scientists to be able to cover the multidisciplinary nature of CPS security, such as transduction attacks. In addition, as the technologies behind CPS security mature, some of them will become industry-accepted best-practices and will transition to industry, while others might be forgotten. In 2018, one of the areas with the greatest momentum was the industry for network security monitoring in cyber-physical networks.

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cyber security threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting and remediation, and finally the planning of the appropriate responses. It has explained the importance of each step in the vulnerability management phase and how each should be carried out.

REFERENCE:

[1] Subodh Asthana “Cyber defamation law”

[2] Eric A. Fischer “cyber security issues”

[3] Theresa Payton ”cybercrime”

[4] https://digitalguardian.com

[5] https://www.kaspersky.com

[6] https://academic.oup.com

[7] https://clutejournals.com