Investigation into cyber security countermeasures

Investigation into cyber security countermeasures

Introduction

Data security and morals has been seen as one of the chief regions of concern and enthusiasm by scholastic analysts and industry specialists. Data security and morals is defined as a comprehensive term that alludes to all exercises expected to verify data and frameworks that help it so as to encourage its moral use. In this starting section, this significant field of study is presented and the principal ideas and hypotheses are talked about. A wide exchange of devices and advancements used to accomplish the objectives of data security and morals is trailed by a dialog of rules for the structure and improvement of such instruments and innovations. Administrative, authoritative and cultural ramifications of data security and morals are then assessed. The section finishes up after an evaluation of various future advancements and exercises seemingly within easy reach that will affect this field.

The rise of the general public dependent on data flag a change toward another general public dependent on the creation and trade of data instead of physical merchandise. Basically, it has guided another scope of rising PC intervened exercise that have altered the manner in which we live and communicate with each other.

ULO2.

Crucial cyber security issues that must be addressed immediately

Issues regarding the cyber security are no matter of joke nowadays. General activities can attract new threats in the process. Issues involve SOE problems, security software using no anti-virus problems, ransom ware-infection problems and no policy-backupproblems.

SOE problems

First of all, SOE problems arises when two different systems are working in same framework. It is hard to maintain the process and multiple systems in one frame cannot standardize that creates window for attackers to breach(Yang, et al, 2017).

As example using Linux and Windows in a same computer will make the hard disk less stable and it will create data allocation problem. The Linux will try to improve itself by taking up more space where as windows will try to install the continuous updates and these two will collide with each other. The system will crash in no time. Now in the caser of an organization using different types of system software will create problems too. Both of them use different code and process and that will create mishap(Sha, et al, 2018). The gap that has been created by using these is severe and needs to be solved immediately so the threat can be prevented or at least minimized.

Security software using no anti-virus problems

Using security software’s that has no antivirus protection enabled is the main target of malware.

The main function of the malware is to damage the device from every possible way. The malware contains virus, Trojan applications, spyware, and adware application.

Ransom ware-infection problems

Mostrecently, the attack of ransomware is coming up constantly, the role it plays is unique, it makes its way into a system them locks it down entirely. The user becomes unable to open the computer and access the files and threatens to erase everything of the computer unless the source of the ransomware is paid.

The degree of threat it contains is extreme in nature. It should be addressed immediately or any organization of the world can be a target of this(Borgohain, Kumar &Sanyal, 2015).

No policy-backup problems

No policy-backup problems mainly refer that the data is not backed up properly.

This can cause the loss of data, money and time. Back up of data is done mainly because people can lose their official or personal data anytime, the backup will come handy then. It should be addressed immediately because the problem will cause someone or an organization a great problem.

Effective proposition of the addressed issues

The problem involving SOE is severe and solution of it may not be critical but the process to solve this is critical and expensive. The entire systems in the

organization should be changed into one system. There should not be a different system in the office so the error of the systems does not increase.

A computer that is being used for the organization should be protected by anti-virus software and it should be updated in regular routine basis. Updating the anti-virus software will provide the software with the information of newly released virus and that will help the user of it to create a firewall so the malware or viruses cannot enter(Alrawais, et al, 2017).

The ransomware problem is very crucial and to defeat it the system that is already attacked by it should be separated from the main server so others can not be infected. After that report to the authority should be made and explain what has really happened.

Creating backup is the only way to recover the lost data. There must be an instruction in the workplace about how to create backup so those who do not the process or importance will understand the gravity of it.

Comparison and `contrasting current solution and alternative approaches towards the addressed issues

The SOE problem can be solved by other ways too, few experts state that, there should be some stuffs allocated to translate and solve the errors. However, the solution is time consuming and resource too. On the other hand, changing the entire system software will bring everyone under one system and that is more efficient from the economic point of view(Mendez, Papapanagiotou& Yang, 2017).

The alternative way to solve the virus problem is to check the system files daily to see if there is some unwanted file has entered or troubleshoot every time any problem occurs. This process is time consuming and labor intensive because a software expert has to come on a daily basis to check the entire system. Where as updating and enabling the virus-protection will guide the computer on its own. Moreover, the system will be completely automatic(Sadeghi, Wachsmann&Waidner, 2015).

Isolating the infected node or computer is more efficient when the whole organization are at stake. Trying to identify the source or running another program to remove the system will create loss of existing data along with other computers(Cook, et al, 2018).

If the device containing important file of an individual or an organization is stolen the backup will help to restore the data. There are few other ways to recover the lost or stolen data such as taking snapshot, or imaged based backup but they are not efficient enough. Whenever the process or use of the data is done, the user will be able to take the snapshot then and most importantly he has to do it repeatedly. However, backing up data by using CDP method will be automatic and it will keep backing up after a certain period of time. The user does not have to do it physically.

Cost breakdown structure of the chosen issues

Aspects	Cost breakdown

An organization has minimum 20 computers in every sector	The change of the system software to windows 10 (say) will cost $60 each. The amount reaches $1200
Norton Antivirus software	The price of Norton Antivirus software $69. 99 for the basic version each and total

	amount will be $1399. 8.
Installation charge	It can go up to $15 per hour. If a group of 4 people come to install and each computer takes one hour to change into a different system software then the total time taken will be 20

	hours (4 people setting up 5 computers for 5 hours). The amount will be $300 for installation.
Total cost	The total cost will be $2899. 8. Although the cost is a rough sketch it may differ from

company

to

products.

Table. 1: Cost breakdown structure of the chosen issues

(Source: Created by the learner)

ULO3

Law and Ethics in Information Security

Information’s are not effectively and promptly accessible as far back as the PCs and web were presented. A lot of numerous network PC framework offer and pass information, data documents all around the world however not very long it was known that a solitary escape clause in a PC framework presented by disappointed clients would make delinquent commotion in the lives of individuals influencing them socially and expertly (Tankard, 2015). Violations, for example, hacking, robbery, unauthori6ed access to data, password robberies, and malware are planned to disfigure basic information and hinder the PC framework morals is significant in basic leadership procedure of an organi6ation in securing the information. morals and its set of principles give rules to a client to play out the correct activities and be simply to every last one (Granjal, Monteiro & Silva, 2015). It gives a way route to the correct obligation one ought to perform while at work, home or anyplace. so also if individuals comprehended the PC morals and applied it in their reality, life would be so a lot simpler. here are a large number of

individuals who are compelled to leave organizations since they were being unreliable and act dishonestly .

The quick improvement of information advancement empowers various affiliations, governments and conventional individuals to trade significant information in a reliable way. In this manner, security issues emerge when sharing information. Right now, the relationship of the affiliations depends on PCs and information outlines, numerous affiliations are worried about information security, as they use progressions, for example, private Internet organizations, workstations and virtual private frameworks. With the development of the commitment of these advances, the different risks to the significant assets of an affiliation likewise increment. Information security ensures the grouping, unwavering quality and openness of information assets against different perils. Specific protection measures are not adequate to ensure information security (Kouicem, Bouabdallah&Lakhlef, 2018). There must be various measures. Make an inexhaustible and astounding information security; regardless of the particular measures; usable, good, sociological and authentic appraisals must be thought about (Vashi & Patel, 2017). Organizations depend on methodology, advancement and people. Notwithstanding whether we have top notch information and security systems, there are individuals who work with these information outlines. There is no specific information security ensure as individuals are incorporated. A survey prompted reported instances of deceptive lead in an affiliation (Conti, et al, 2018).

FUNDAMENTAL CONCEPTS AND THEORIES ON SECURITY AND ETHICS OF INFORMATION

Information security concerns the ID of the electronic information assets of an affiliation and the advancement and utilization of devices, strategies, arrangements, standards, procedures and principles to ensure secrecy, unwavering quality and openness of these advantages. Notwithstanding the way that data security can be characterized in various manners, the US organization has accomplished the most noteworthy thing (Bhabad, & Bagade, 2015). The National Institute of Standards and Technology (NIST) characterizes data security that expresses that data security shields information and information outlines from unapproved get to, use, exposure, interference, change or showering to give unwavering quality, privacy and availability . Data characterized as those made to perceive and address the vulnerabilities of the PC system or the PC association (Mendez Mena, Papapanagiotou& Yang, 2018).

Characterizes three goals of sweeping information security, classification, uprightness and accessibility (Ammar, Russello&Crispo, 2018). This trio of goals is once in a while alluded to as the planned security exertion to set up the authenticity of a transmission, a message or a source or a technique to check an individual’s endorsement so as to acquire explicit kinds of information (Deep, Zheng &Hamey, 2019). The basic procedures for customer approval are: acquiring passwords, getting tokens, something the client possesses and which can be founded on a blend of programming or hardware that enables affirmed access to that system (eg Smart Cards and clients of brilliant papers), utilization of biometric information (something that the client is, for instance, unique mark, palm print or voice print), arrive at the zone (for instance a particular workstation), client profile (for instance,

direct expected or acceptable) and confirmation data, to check that the trustworthiness of the data has not been undermined(Laeeq, & Shamsi, 2015)..

Conclusion

We are the first age of people where the capacities of the advancements that help our in-arrangement handling exercises are genuinely progressive and far surpass those of our progenitors. In spite of the fact that this mechanical unrest has brought us closer and has made our lives simpler and progressively profitable, incomprehensibly, it has additionally made us increasingly fit for hurting each other and increasingly helpless against be hurt by one another. Our vulnerabilities are the result of our abilities

A Framework For Global Electronic Commerce that we are very nearly an upset that is similarly as significant as the adjustment in the economy that accompanied the mechanical transformation. Before long electronic systems will enable individuals to rise above the boundaries the electronic system transformation has changed our lives in way incomprehensible just 10 years back. However, we are just at the edge of this insurgency. The bewildering pace of advances in data innovation vows to change our lives significantly more radically. With the end goal for us to exploit the conceivable outcomes offered by this new interconnectedness, associations, legislative organizations, and people must find approaches to address the related security and moral ramifications.

Reference List

- Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing* , *21* (2), 34-42.
- Ammar, M., Russello, G., &Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications* , *38* , 8-27.
- Bhabad, M. A., & Bagade, S. T. (2015). Internet of things: architecture, security issues and countermeasures. *International Journal of Computer Applications* , *125* (14).
- Borgohain, T., Kumar, U., &Sanyal, S. (2015). Survey of security and privacy issues of internet of things. *arXiv preprint arXiv: 1501. 02211* .
- Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.
- Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., &Janicke, H. (2018). Internet of cloud: Security and privacy issues. In *Cloud Computing for Optimization: Foundations, Applications, and Challenges* (pp. 271-301). Springer, Cham.
- Deep, S., Zheng, X., &Hamey, L. (2019). A survey of security and privacy issues in the Internet of Things from the layered context. *arXiv preprint arXiv: 1903. 00846* .
- Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials* , *17* (3), 1294-1312.
- Kouicem, D. E., Bouabdallah, A., &Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks* , *141* , 199-221.

- Laeeq, K., & Shamsi, J. A. (2015). A study of security issues, vulnerabilities and challenges in internet of things. *Securing Cyber-Physical Systems* , *10* .
- Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective* , *27* (3), 162-182.
- Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv: 1707. 01879* .
- Sadeghi, A. R., Wachsmann, C., &Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). IEEE.
- Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems* , *83* , 326-337.
- Tankard, C. (2015). The security issues of the Internet of Things. *Computer Fraud & Security* , *2015* (9), 11-14.
- Vashi, D., & Patel, V. (2017). Security, privacy and trust issues in internet of things. *International Journal of Innovations & Advancement in Computer Science* .
- Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal* , *4* (5), 1250-1258.