International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

An Empirical Study on Information Security

Bhavya Verma[1], Purva Choudhary[1], Dr. Deepak Chahal[2]

[1]MCA Student, [2]Professor,

[1,2]Department of IT, Jagan Institute of Management Studies, Rohini, New Delhi, India

ABSTRACT

Information security or Infosec worries with protecting information from unauthorized access. Its a part of information risk management and it therefore involves preventing or reducing the probability of unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspect or recording. In this article we will talk about the IT security, various threads to information security, different obstacles of information security and the various ways in which internet can be lucrative.

KEYWORDS: *Information, Security, Virus, Authentication*

How to cite this paper: Bhavya Verma | Purva Choudhary | Dr. Deepak Chahal "An Empirical Study on Information Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.186-189, URL: www.ijtsrd.com/papers/ijtsrd30888.pdf

IJTSRD30888

INTRODUCTION

Information security is also called as InfoSec. It is not all about security information from illicit access, rather it's the practice of preventing illicit access, disclosure, inspection, recording, etc of information. The preeminent of information security is the balanced protection of the Confidentiality, Integrity and Availability (also known as CIA). Security is looked in terms of how data is stored, coded, transmitted, encrypted and deleted. Various statistics has shown that companies take security of the data of an individual with very high priority [1].

IT Security

IT security is also known as computer science, which talks about security to technology. Computer security are not just needed at homes these days, hackers worldwide are smart enough to penetrate through huge servers leaking all the required information, thus in these cases, IT security is needed. This scenario may be expensive, a significant breach costs an organization far more. Big breaches almost jeopardize small businesses leading to huge fall out of these small businesses.

Even though information security and IT security sounds familiar, but the difference that lies between them is that in infosec, various set of tools are designed which helps in providing sensitivity in business sector, where as computer science talks about security to data which becomes limited within the digital world.

Threads to information security may encompass following:-

1. Computer viruses

Computer virus was introduced by Ran Weber in 1999, which is a vile software which crosses the threshold into our computers without consent. It creates a replica of itself heading to activate its malicious activities and thus continue to spread all over the system.

2. Theft

Any theft on the hardware, software or the data of any organization leads to huge loss to the organization

3. Sabotage

Sabotage, as the name suggest, means deliberately destroying anything. Hackers worldwide have an in-depth knowledge of how they could sabotage information of the organization which could cause maximum vandalism to the system.

4. Vandalism

Vandalism affects hardware, software and the data of an organization wilfully leading to its effect in the entire system. ISO 27002:2005 defines information security for prevising into three major elements:-

I. Confidentiality

Any unintended source if hinders inside the organization had to be put to a stop. This is done through confidentiality. All sorts of secrete, sensitive and protection prone data needs to be kept away from all the malicious invaders. Confidentiality

can only be accessed depending upon the availability and accessibility by the trusted users only. Protection can be done with the help of encryption, access control structure, file permission, etc

II. Integrity

When we need to secure our data, it is not just limited to the security of data, it involves various other factors also like maintaining the consistency, accuracy, trustworthiness, etc of data. It is very important in data security that it does not just provide the access to ensure that the data cannot be changed or alter by malicious officials. Integrity to data security can only be ensured by implementing the concept of file permission and user access controls in addition to these two vital concepts, it is very important to place some means for detecting any changes in data that might occur as a result of non-human caused events. All sorts of backups or redundancies which has to take place must be available to restore the affected data and secure it strictly for further use. As all the existing technologies somehow have a loop hole that cannot be removed or is being improved to remove the potential threat loop hole [2].

III. Availability

Availability is best ensured by tightly storing all Hardware, performing hardware repairs as soon as needed and maintaining an efficient packet space freed from software conflicts. It is also important to stay current with all the program upgrades required. Providing adequate communication bandwidth and preventing the emergence of bottles is very important. Backtracking, poor performance, RAID and even high availability teams can reduce the adverse effects when hardware issues arise. Rapid and harmonious disaster preparedness is essential in cases of serious crime; that authority depends on the existence of a comprehensive disaster recovery plan (DRP). Protecting protection against data loss or interruption in connection should include unexpected events such as natural disasters and fire. to prevent data loss from such occurrences, a backup copy may be stored at a location-based location, or perhaps while fireproof, not securely waterproof. Today, networks are complex arrangements that cannot be left to chance. Each design must be researched, assembled, proven, and then implemented [3]. Additional security tools or software such as firewalls and proxy services may monitor downtime and inaccessible data due to malicious actions such as service-Do-service (DoS) attacks and network attacks.

Obstacles to information security:-

I. Financial Services Workers Fooled by CD Scam

Studies conducted in the financial district of London have shown what years of security experts say: employees - even those who work with the most sensitive financial data - don't know or don't care about basic security measures.

In this study, CDs were given to passengers as they entered the city. Recipients were told that the discs contained a special Valentine's Day promotion. In fact, the CDs contain something other than the code that informs the company that was doing the work on how many recipients tried to open the CD. Among the deportees were employees of the world's largest retail bank and two insurers.

Employees, by installing the CD in their offices and installing it directly on their PCs, go far beyond the security of their company. Experts say employees need to understand that they are the first and easiest way in their company's network.

II. Security Incident Investigations Within Banks

The method of bank security investigations is receiving a lot of attention these days. In the past, standard procedures and procedures for responding to an incident were acceptable. However, due to security practices and regulations that directly affect banks, these institutions require very different approaches to their security investigations to account for these new regulations and security measures.

Security incident investigations are activities aimed at answering questions (when, where, what, to whom, how and why) regarding a specific event that affected an organization's information or infrastructure in an unwanted, anonymous and / or illegal manner.

In comparison with many other types of security checks, security incident investigations are more environmentally-friendly (e.g. an incident has already been identified), and this puts additional pressure and time / resources compared to other security activities.

However, security incident investigations are not entirely independent of other data security operations. Other functions may provide useful input before / during an investigation, may be started as a result of an investigation or accept as input of a search result.

III. Trouble In Authentication

Bank fraud and identity theft are a shock to both the banker and the consumer. The number of consumers involved in widespread credit card fraud would be great. The impact on people's bank accounts is likely to increase acceptance of "disruptive technologies", e.g., hardware tokens. This could be a storm suitable for banks. You have the customer's permission to tell them what to do.

Large banks have been working for many years in ensuring the integrity and are ready to take on this challenge. What concerns me most about community banks and credit unions. They are currently having a difficult time competing with online banks and payment of taxes.

What's wrong with multitasking? The problem with customer authentication information is that it is provided to the customer. Someone asks as you might have your social security number, your mother's maiden name, and you know the name of your first pet, first-born, and your favourite food.

If I have your laptop, your fob, your wallet and everything else in your wallet, you're out of luck. If I use a thumb print gun, I only have one print name for it.

Anything that can be contained in a database can be extracted from a database. Everything in your home, car, office, hotel room and Starbucks can be stolen. We need to come up with something stolen. The difference between two things and a lot of things is just the number of things I need from you.

Enter the authentication at risk. The risk analysis engine will look at your banking performance, analyse it, and the differences in the flag. This is similar to how access control systems work. If there seems to be something very unusual about the online banking area of the work, or the number of transactions, or the number of transactions, the sale is significant.

While banks pursue dual-user authentication, website authentication is still a problem to be solved. With user authentication, the user is authorized by the bank. But what about verification of the bank's website to the user? How does a user know that he or she has come to the right website rather than the phishing site?

The authentication vendor of your choice must be able to demonstrate not only the strict user authentication method, the online risk management method, but also the website authentication method. Electronic signatures are one way of looking at website verification.

IV. Phishing: An Insidious Threat to Financial Institutions

Illegal hacking using illegal emails to get people out of their account numbers and passwords is on the rise. Hijacking product names of banks, merchants and credit card companies, chefs often make recipients accountable. Under-hacking techniques instil fraud on PCs to steal information directly, sometimes using the Trojan keylogger software.

Fortunately, a combination of technological solutions exists to detect and reduce cybercrime attacks. The long-term solution is the use of law and industry resources to quickly identify and deter hackers, as well as government intervention in Asian and Eastern European countries where organized crime is rampant. However there are a number of steps that individual organizations can take and which should take a different approach.

The first thing to understand is that identity theft culminates in a social engineering revolution, where victims are misled into transmitting information that can be used to hijack accounts or create other mayhem.

In addition to stealing sensitive data, the FDIC said, attackers can resort to other means to steal information, such as hacking, retrieving hard-copied documents or staring at someone, using the contents, and uploading malicious software to a consumer-owned computer.

There are two main reasons why phishing and other types of attacks have been used more often and with increasing success. They should cause identity theft, and some account theft: User authentication by the financial services industry for remote customer access is weak, and the Internet has no E-mail and Web site verification.

V. Online Activities at Work

Buyers in the U.S. They are responding to the increasing fear of online identity theft. Businesses - especially those in the financial services sector - must counter this trend by emphasizing their efforts to deploy acquisition-based applications.

A new survey (see below) shows the first evidence that fear of identity theft is starting to take online usage statistics. Internet usage rates are very important for banks and other financial services institutions. The sector is characterized by high competition, small differences between institutions, and low levels of customer loyalty.

Two key strategies have emerged in the struggle to grow the size and scale of the current customer base:

- Maximize Internet Bank usage. By increasing the percentage of customers who use online services, banks can increase their customer revenue, reduce transaction costs, and increase long-term reliability.
- Lower the churn. By reducing the percentage of customers converting their business to another institution, banks can maintain market share in a competitive market otherwise.

Although there are fears about a Consumer Reports survey, the need for Internet-based banks continues to grow. The Pew Internet & American Life Project reports that more than 50 million adults are now banking online. This figure has increased 47% since 2002.

Info-Tech sees the online market as a symbol of the great competitiveness of the banking sector. Despite the growing demand for the market, the perception of risk is seen as a threat to the ongoing access to online services. Building better software and lead to some good reproducible research as compared to virtual machines [4].

Institutions that redirect their contributions to addressing security concerns and meeting the need to explode will receive a competitive advantage over those who choose to take a conservative approach. Banks can pay for this practice.

Ways to Make the Most of Internet Use:

1. Address security forward. Issues of identity theft have become a major concern for consumers. Online marketing efforts should focus specifically on the steps the bank takes to protect all usage and personal data. Create a program to communicate the following key issues:

Messages are sent to the home business page detailing specific steps the bank is known to have taken.

A direct product of the bank's security efforts. Include this product in all customer publications.

The FAQs outline steps that customers can take to increase their online safety. This includes using 128-bit-encrypted browsers, never responding to e-mail from any bank, and warning signs of URL URLs. To maximize purchases, focus on cost and time savings for consumers.

2. Track current usage. Understand how current services are used by using Web analytics to get end-user information. Research customers to better understand why they use online resources. Include inspections of branch services and telephone services and ensure that all points of contact are made.

Describe the first answers to this data. If the key performance indicators are violated, have a plan to explain who is doing it and who is funding it to address the issue.

3. Educate the customer. Do not assume that all customers are automatically ready to go online. Late immigrants may need more supervision and training before they can be free. Add FAQs and other training content to the centre's website to make sure they get the help they need.

4. Look to leaders. The Canadian banking market is leading the world in online banking penetration. According to a recent report by comScore Media Metrix Canada, 40% of Canadians use online banking services.

Conclusion

Information security as we can understand is a key instrument in IT security when we have to talk about. It can never be taken lightly while considering the reverberation of its failure and the corresponding after effects which can affect the entire system. It becomes escalating important as the level of safety and the responsibility that is required to ensure business continuity and safety for the information that is derived from the data used in the system. A look at top threats was identified as computer virus, theft, sabotage and vandalism. Thus, ISO27002:2005 has defined the need of preserving information security with three major elements : Confidentiality, Integrity and availability.

References:

[1] Bhutani S. et al, Data privacy and security issues in India: An empirical study, International Journal of Research in Engineering, Volume 1; Issue 4; October 2019; Page No. 15-17.

[2] Chahal D. et al. Cyber Securence Affected by Big Data and Artificial Intelligence, International Journal Of Innovative Research In Technology, Volume 6 Issue 6, November 2019.

[3] Bhatnagar A. et al. Juniper Networks: An Overview of the Concept, IJSRD - International Journal for Scientific Research & Development| Vol. 6, Issue 10, 2018.

[4] Kharb L, Automated Deployment of Software Containers Using Dockers, International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 4, Issue 10, October (2016).