



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCC5003 Network Operating Systems and Security

Alexandru Balasa

1814696

Lecture: Terry Walcott

Table of Contents

Introduction.....	3
Body.....	Error! Bookmark not defined.
Some recommendation that can help in preventing Data Hacking Issue:	9
Conclusion	10
References.....	11

Introduction

The purpose of the Assignment is to find a way by which we can prevent Data Breach. Companies should make sure that information is satisfactorily protected to forestall loss or thieving. wherever a breach has taken place, firms may have to advise people similarly to face a negative impact on the company's complete and client loyalty. Steps required to be taken to reduce information breach

- **Up-to-date Security package**

Ensure the package is updated and patched often to avoid weak spots for hackers to use.

- **Regular Risk Management**

Access and review any changes or new risks in information protection.

- **Encryption and information backup**

Personal information sought to a minimum of being encrypted, as well as on work laptops issued to employees [1]. (Talesh, 2018).

- **Staff coaching and awareness**

Train employees to follow best practices, bear in mind the importance of knowledge security, and the way to avoid mistakes.

- **Ensure vendors and partners providing protection standards**

When operating with alternative firms that handle customers' information, need to have a check that they have proper security process in place

- **Third-party information Security Evaluations**

Having a 3rd party perform a risk analysis and take precaution to prevent any kind of data breach

The 3 Principles of knowledge Security

According to Steichen, there square measure 3 basic principles of knowledge security which are confidentiality, integrity, and availableness. This can be additionally referred to as the core principles of knowledge security for the past twenty years.

1. Confidentiality

It is the term wont to stop the revelation of knowledge to unauthorized people or systems. Breaches of confidentiality take several forms. allowing somebody to appear over your shoulder at your monitor whereas you have got confidential knowledge displayed on that may be a breach of confidentiality. If a laptop personal computer containing sensitive info a couple of company's workers is taken or sold-out, it might lead to a breach of confidentiality. Giving out hint over the phone could be a breach of confidentiality if the caller isn't approved to own the knowledge. samples of confidentiality of electronic knowledge being compromised embrace portable computer thievery, word thievery, or sensitive emails being sent to the inaccurate people [4].(Herrera-Cubides *et.al*,2019).

2. Integrity

In info security, integrity implies that knowledge can't be changed while not authorization. this can be not a constant factor as denotative integrity in databases. Integrity is desecrated once any worker accidentally or with malicious intent deletes necessary knowledge files, once a worm infects a computer system, once an employee changes his remuneration in payroll info, once any unauthorized user vandalizes an online website, once somebody is ready to solid a sizable amount of votes in an internet poll, and so on. info security systems usually give message integrity aboard confidentiality [3].(Yasin *et.al*,2019).

3. Availability

For any system to serve its purpose, the knowledge should be obtainable once it's required. this implies that the computing systems want to store and method the knowledge, the {protection} controls wont to protect it, and therefore the communication channels want to access it should be functioning properly. Highly available systems aimed to stay obtainable quite a bit of time, preventing any service disruptions because of power outages, hardware failures, and system upgrades. Creating some certain availableness may additionally involve creating a preventing or denial mode of service attacks.

In the realm of knowledge security, availableness will typically be viewed as united of the foremost necessary elements of an eminent info security program. Ultimately end-users ought to be able to perform job functions; by making certain availableness a corporation is ready to perform to the standards that the organization's stakeholders expect. This may involve topics like proxy configurations, outside net access, the power to access shared drives, and therefore the ability to send emails. Most of the times executive don't perceive the technical facet of knowledge security and appearance at availableness as a simple fix, however, this typically needs collaboration from many alternative structure groups, like development operations, network operations, incident response, and policy/change management. An eminent info security team involves many alternative key roles to mesh and align for the United States intelligence agency triad to be provided effectively [2].(Sieber *et.al*,2017).

In Broad, the risk is that the probability some or the other day thing unhealthy or bad may happen that can cause or hurt to an informational quality (or the loss of the asset). A vulnerability could be a weakness that would be wont to endanger or cause hurt to any informational quality. A threat is something that has the potential to cause hurt. The probability that a threat can use a vulnerability to cause hurt creates a risk. Once a threat will use a vulnerability to intercommunicate hurt it in any way or it's away. Within the context of knowledge security, the impact could be a loss of availableness, integrity, and confidentiality, and presumably different losses (lost financial gain, loss of life, loss of real property)

Critique the previous hacking problem and steps to prevent it

Major Hacking Problems :

1. DDoS Attacks

Distributed denial of provider (DDoS) assaults have become certainly considered one of all the most distinguished varieties of cybercrime over the last few years. While there's no doubt they've improved in frequency A DDoS assault aims to overload a server with getting the right of entry to requests till it in the long run crashes. These assaults are normally facilitated through "botnets," a fleet of computer systems inflamed through malicious software program and directed through a hacker to ship get right of entry to requests to 1 target [5].(Guri, Mirsky and Elovici,2017).

2. Malware

In a conventional fashion of cyberattacks, a malicious software program is regularly delivered right into a device via a range of methods. Email attachments, software program downloads, and software program vulnerabilities are the most not unusual place assets of malware. Once installed, malware disguises itself by attaching to valid code and spreading to different structures. The aim of malware is normally to furnish unauthorized get right of entry to to a laptop or device. Ransomware, which denies the person get right of entry to important information through encryption till a ransom is paid to liberate it, has been chargeable for numerous fame cyberattacks in latest years. But new sorts of malware, which include Trojans, viruses, and worms, are constantly rising to threaten groups and people alike.

3. Phishing Scams

A virtual model of an age-antique scam, phishing assaults contains email messages that use numerous varieties of mental manipulation and deception to persuade customers to click on a hyperlink that units them on a course to sharing their private statistics. Modern phishing messages are exceedingly sophisticated, regularly posing as emails from valid, relied on groups. And whilst maximum net customers understand to be particularly cautious of such requests, a 2016 Verizon document located that oldsters had been sixfold much more likely to click on on a phishing email than a regular advertising email [7].(Yuan *et.al*,2020).

4. Internal Misuse

Even the only cybersecurity measures can show useless while personnel set up to misuse their get right of entry to privileges. While humans leaking steady information to public assets can

also be the most newsworthy instance of such abuses, it's manner extra not unusual place for employees to without difficulty take essential information and know-how while not having any precise plan for what to attempt to do with it. Recent studies located that eighty-five percentage of personnel took files or statistics they'd for my part created and 30 percent took the information they hadn't created. These statistics protected approach files, purchaser information, or even proprietary ASCII textual content files.

Solutions :

- Predictive Analytics

To successfully counter cyberattacks, IT employees should understand what an assault seems if while it's probably to occur, and in which it's coming from. Predictive analytics software program pushed through system mastering can accumulate big quantities of information on recognized cyberattacks and observe the outcomes to present protection protocols. this will be regularly particularly beneficial for energetic DDoS mitigation as it permits cybersecurity structures to discover threats and take proactive measures to redirect site visitors earlier than the device is overwhelmed. Rapid reaction instances are important for keeping off the worst results of cyberattacks. The longer a breach is going undetected, as an instance, the extra information is traveling be compromised, which may be steeply-priced to groups of all sizes [6].(Hoyt *et.al*, 2016).

- Back-Up Critical Data

In the case of DDoS and ransomware assaults, groups should own a know-how again-up plan in location. Having to get right of entry to mission-important information can imply the distinction between getting structures and offerings again online speedy with minimum downtime and struggling with a catastrophic server outage. With an intensive again-up approach in a location that regularly shops essential information and property for the duration of a separate and ideally off-web web page device, groups can keep away from the "all or nothing" hazard of a cyberattack inflicting extended downtime.

- SLA Assurances

Many groups outsource quantities in their IT infrastructure or information operations to 1/3-birthday birthday celebration groups. While this will lessen prices and logistical burdens, it additionally introduces the capacity hazard of statistics publicity if the 1/3 birthday celebration doesn't have a comparable stage of cybersecurity measures in location to protect towards threats. To keep away from this problem, groups need to make use of provider stage agreements (SLAs) to outline the safety duties of all events concerned withinside the relationship.

- Cyber Insurance

With hacking turning into a widespread hazard throughout more than one industry, many groups have spoken back through buying coverage plans to shield them towards capacity monetary losses. For industries like healthcare, which has problem enforcing sturdy safety features because of compliance laws, coverage is rapidly turning into a need to shield groups financially from cyberattacks on their structures or the ones in their providers and partners [8].(Marotta *et.al*,2017).

- Bug Bounties

Identifying vulnerabilities in software program code are regularly a tedious and time-ingesting process. Many groups without a doubt don't have the sources to problem their packages to the rigorous scrutiny important to discover each unmarried worm or loophole that is probably exploited through hackers. In the latest years, however, groups have determined to outsource this mission via "worm bounty" packages. These packages inspire well-intentioned hackers to scour web-primarily based software programs for vulnerabilities and errors, handing over a coin payout while showed insects are identified.

Some recommendation that can help in preventing Data Hacking Issue:

- **Using public Wifi doesn't access any personal or financial data**

Turn off anything you don't need – Hackers use features like location or GPS to hack the data. So use it when it is required.

- **Choose your apps wisely – Get rid of the apps that are not used.**

Use a password, lock code, or encryption – Try to use a strong password with more than 8 characters having a combination of Uppercase, lowercase, numbers, and special character.

- **Be skeptical about links and attachments.**

Trace or erase – Make sure the data is secured and not lost [9].(Alsayed and Bilgrami, 2017).

Conclusion

It's difficult to forget 2020 in hurry. The Coronavirus pandemic has utterly reworked our lives and created a perfect atmosphere for cyber-attacks and security breaches. Since the beginning of the year, there are as several as 726 million cyberattacks, exposing Associate in Nursing eye-watering sixteen billion records. Any hopes that cyber-attacks would have taken a back seat throughout the crisis are broken, and it's become more and more apparent that cybercriminals can still exploit the pandemic for gain. Data could be a valuable artifact and cybercriminals square measure keen to take advantage of this information to form cash and commit fallacious activities. in keeping with the 2020 Verizon information breach investigations report, eighty-six of this year's breaches were driven by gain, up by 15 percent from 2019. The report conjointly completes that phishing and purloined passwords stay the highest ways in which cybercriminals square measure accessing company networks and systems. This year is by no suggests that over nevertheless thus we will expect to ascertain additional cyber-attacks and information breaches within the weeks and months to return. Thus, it's solely by awareness we can act on that and stop the Data Information Breach.

References

- [1] .Talesh, S.A., 2018. Data breach, privacy, and cyber insurance: How insurance companies act as “compliance managers” for businesses. *Law & Social Inquiry*, 43(2), pp.417-440.
- [2] .Sieber, S., Graef, F., Amjath-Babu, T.S., Mutabazi, K.D., Tumbo, S.D., Faße, A., Paloma, S.G.Y., Rybak, C., Lana, M., Ndah, T.H. and Uckert, G., 2017. Trans-SEC’s food security research in Tanzania: Principles, research models and assumptions. *Food Security*, 9(6), pp.1147-1155.
- [3] .Yasin, A., Liu, L., Li, T., Fatima, R. and Jianmin, W., 2019. Improving software security awareness using a serious game. *IET Software*, 13(2), pp.159-169.
- [4] .Herrera-Cubides, J.F., Gaona-García, P.A., Montenegro-Marín, C., Cataño, D. and González-Crespo, R., 2019. Security Aspects in Web of Data Based on Trust Principles. A brief of Literature Review. *International Journal of Communication Networks and Information Security*, 11(3), pp.365-379.
- [5] .Guri, M., Mirsky, Y. and Elovici, Y., 2017, April. 9-1-1 DDoS: attacks, analysis and mitigation. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 218-232). IEEE.
- [6] .Hoyt, R.E., Snider, D.H., Thompson, C.J. and Mantravadi, S., 2016. IBM Watson analytics: automating visualization, descriptive, and predictive statistics. *JMIR public health and surveillance*, 2(2), p.e157.
- [7] .Yuan, Q., Huang, B., Zhang, J., Wu, J., Zhang, H. and Zhang, X., 2020, October. Detecting Phishing Scams on Ethereum Based on Transaction Records. In *2020 IEEE International Symposium on Circuits and Systems (ISCAS)* (pp. 1-5). IEEE.
- [8] .Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A., 2017. Cyber-insurance survey. *Computer Science Review*, 24, pp.35-61.
- [9] .Alsayed, A. and Bilgrami, A., 2017. E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *Int. J. Of Emerg. Techn. and Adv. Activ*, 7(1), pp.109-115.