Some Cyber Security Topics: Review Study

PRAMOD KUMAR
Establishment and Administration, Indian Institute of Management, Udaipur
email :pramod.kumar@iimu.ac.in

Abstract: **Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cloud computing has emerged from the legacy data centres. Consequently, threats applicable in legacy system are equally applicable to cloud computing along with emerging new threats that plague only the cloud systems. Traditionally the data centres were hosted on-premises. Hence, control over the data was comparatively easier than handling a cloud system which is borderless and ubiquitous. Threats due to multi-tenancy, access from anywhere, control of cloud, etc. are some examples of why cloud security becomes important. Considering the significance of cloud security, this work is an attempt to understand the existing cloud service and deployment models, and the major threat factors to cloud security that may be critical in cloud environment.**

Key words: **Cloud Computing; Multi Tenancy; Control of Cloud; Cloud Security; Deployment Models;**

INTRODUCTION

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems. **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware. **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed. **Information security** protects the integrity and privacy of data, both in storage and in transit. **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella. For various types of attacks, one may refer to the articles listed under references. Risk Management Regime: Embed an appropriate risk management regime across the organisation. Secure configuration: Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information. Network security: The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it. Managing user privileges: If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

User education and awareness

Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture. Incident management: All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise. Malware prevention: Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach. Monitoring: System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements. Removable media controls: Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use. Home and mobile working: Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

The Importance of Cyber security

The world relies on technology more than ever before. As a result, digital data creation has surged. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization . A data breach can have a range of devastating consequences for any business. It can unravel a company’s reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Going further, a data breach can impact corporate revenues due to non-compliance with data protection regulations. It’s estimated that, on average, a data breach costs an affected organization $3.6 million. With high-profile data breaches making media headlines, it’s essential that organizations adopt and implement a strong cybersecurity approach.

Computer forensics (also known as **Computer Forensic Science**)

It is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is accepted as reliable within U.S. and European court systems.

Forensic process

A portable Tableau write blocker attached to a Hard Drive

Computer forensic investigations usually follow the standard digital forensic process or phases which are acquisition, examination, analysis and reporting. Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

Computer Forensics Lab

The computer forensic lab is a safe and protected zone where electronic data can be managed, preserved, and accessed in a controlled environment. There, there is a very much reduced risk of damage or modification to the evidence. Computer forensic examiners have the resources needed to elicit meaningful data from the devices that they are examining.

Techniques

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular.

Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.

Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

Stochastic forensics

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

Steganography

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the images appear identical upon visual inspection, the hash changes as the data changes.

Mobile Devices Forensics

Phone Logs: Phone companies usually keep logs of calls received, which can be helpful when creating timelines and gathering the locations of persons when the crime occurred.

Contacts: Contact lists help narrow down the suspect pool due to their connections with the victim or suspect.

Text messages: Messages contain timestamps and remain in company servers indefinitely, even if deleted on the original device. Because of this, messages act as crucial records of communication that can be used to convict suspects.

Photos: Photos can be critical in either supporting or disproving alibis by displaying a location or scene along with a timestamp of when the photo was taken.

Audio Recordings: Some victims might have been able to record pivotal moments of the struggle, like the voice of their attacker or extensive context of the situation.

Volatile data

Volatile data is any **data** that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. **Volatile data** resides in registries, cache, and random access memory (RAM). The investigation of this **volatile data** is called "live forensics". When seizing evidence, if the machine is still active, any information stored solely in RAM that is not recovered before powering down may be lost. One application of "live analysis" is to recover RAM data (for example, using Microsoft's COFEE tool, WinDD, WindowsSCOPE) prior to removing an exhibit. CaptureGUARD Gateway bypasses Windows login for locked computers, allowing for the analysis and acquisition of physical memory on a locked computer.

RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate, an effect exploited by the cold boot attack. The length of time that data is recoverable is increased by low temperatures and higher cell voltages. Holding unpowered RAM below −60 °C helps preserve residual data by an order of magnitude, improving the chances of successful recovery. However, it can be impractical to do this during a field examination. Some of the tools needed to extract volatile data, however, require that a computer be in a forensic lab, both to maintain a legitimate chain of evidence, and to facilitate work on the machine. If necessary, law enforcement applies techniques to move a live, running desktop computer. These include a mouse jiggler, which moves the mouse rapidly in small movements and prevents the computer from going to sleep accidentally. Usually, an uninterruptible power supply (UPS) provides power during transit.

However, one of the easiest ways to capture data is by actually saving the RAM data to disk. Various file systems that have journaling features such as NTFS and ReiserFS keep a large portion of the RAM data on the main storage media during operation, and these page files can be reassembled to reconstruct what was in RAM at that time.

Analysis tools

A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review. Autopsy (software), Belkasoft Evidence Center, COFEE, EnCase are the some of tools used in Digital forensics.

Hack computer

The **Hack Computer** is a theoretical computer design created by Noam Nisan and Shimon Schocken and described in their book, *The Elements of Computing Systems: Building a Modern Computer from First Principles.* In using the term "modern", the authors refer to a digital, binary machine that is patterned according to the von Neumann architecture model. The Hack computer is intended for hands-on virtual construction in a hardware simulator application as a part of a basic, but comprehensive, course in computer organization and architecture. One such course, created by the authors and delivered in two parts, is freely available as a massive open online course (MOOC) called Build a Modern Computer From First Principles: From Nand to Tetris. In the twelve projects included in the course, learners start with a two input Nand gate and end up with a fully operational virtual computer, including both hardware (memory and CPU) and software (assembler, VM, Java-like programming language, and OS). In addition to the hardware simulator used for initial implementation of the computer hardware, a complete Hack computer emulator program and assembler that supports the projects described in the book and the on-line course is also available at the author's web site.

Cyber Security

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Risk Management Regime: Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries. Secure configuration: Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

Network security: The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it. Managing user privileges: If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

User education and awareness: Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture. Incident management: All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise. Malware prevention: Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

Monitoring: System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements. Removable media controls: Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use. Home and mobile working: Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

The Importance of Cybersecurity

The world relies on technology more than ever before. As a result, digital data creation has surged. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization.

A data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Going further, a data breach can impact corporate revenues due to non-compliance with data protection regulations. It's estimated that, on average, a data breach costs an affected organization $3.6 million. With high-profile data breaches making media headlines, it's essential that organizations adopt and implement a strong cybersecurity approach.

Challenges and solutions

In addition to established competitors, fintech companies often face doubts from financial regulators like issuing banks and the Federal Government. In July 2018, the Trump Administration issued a policy statement that allowed FinTech companies to apply for special purpose national bank charters from the federal Office of the Comptroller of the Currency. Federal preemption applies to state law regarding federally chartered banks. Data security is another issue regulators are concerned about because of the threat of hacking as well as the need to protect sensitive consumer and corporate financial data. Leading global fintech companies are proactively turning to cloud technology to meet increasingly stringent compliance regulations. The Federal Trade Commission provides free resources for corporations of all sizes to meet their legal obligations of protecting sensitive data. Several private initiatives suggest that multiple layers of defense can help isolate and secure financial data.

ACKNOWLEDGEMENTS

Author hereby thanks Dr,S,Sridhar, Ex Vice Chancellor, Technical Chair of this Web Conference and his comments while reviewing this paper for publication are highly appreciable and well taken to modify this final version .

REFERENCES

[1]. "#Cybercrime— what are the costs to victims - North Denver News". North Denver News. 17 January 2015. Retrieved 16 May 2015.

[2]. "Bitcoin not a currency says Japan government". BBC News. 7 March 2014. Retrieved 25 January 2022.

[3]. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress". www.everycrsreport.com. Retrieved 5 September 2021.

[4]. "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Retrieved 17 May 2021.

[5]. "Chapter 3: Computer Forensic Fundamentals - Investigative Computer Forensics: The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives [Book]". www.oreilly.com. Retrieved 2022-03-04.

[6]. "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2020.

[7]. "computer security | Definition & Facts | Britannica". www.britannica.com. Retrieved 12 July 2022.

[8]. "Computer Security and Mobile Security Challenges". researchgate.net. 3 December 2015. Archived from the original on 12 October 2016. Retrieved 4 August 2016.

[9]. "Cryptocurrencies: What Are They?". Schwab Brokerage.

[10]. "Cyber crime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.

[11]. "cybercrime | Definition". Encyclopedia Britannica. Retrieved 25 May 2021.

[12]. "cybercrime | Definition, Statistics, & Examples | Britannica". www.britannica.com. Retrieved 14 December 2021.

[13]. "Email Security | Trellix". www.trellix.com. Retrieved 24 October 2022.

[14]. "EXP-SA: Prediction and Detection of Network Membership through Automated Hard Drive Analysis".

[15]. "Ghidra". Archived from the original on 15 August 2020. Retrieved 17 August 2020.

[16]. "How To Make A Mint: The Cryptography of Anonymous Electronic Cash". groups.csail.mit.edu. Archived from the original on 26 October 2017. Retrieved 11 January 2018.

[17]. "Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015. Retrieved 4 July 2016.

[18]. "Insurtech startups are leveraging rapid growth to raise big money". TechCrunch. April 20, 2021. Retrieved October 13, 2021.

[19]. "Is it a currency? A commodity? Bitcoin has an identity crisis". Reuters. 3 March 2020. Retrieved 25 January 2022.

[20]. "KPMG Pulse of Fintech H1 2021 - Global". KPMG. 2021. Retrieved December 28, 2021.

[21]. "KPMG Pulse of Fintech H1 2021 - Global". KPMG. 2021. Retrieved December 28, 2021.

[22]. "KPMG Pulse of Fintech H1 2021 - Global". KPMG. Retrieved December 28, 2021.

[23]. "KPMG Pulse of FinTech H1 2021 Global". KPMG. 2021. Retrieved December 28, 2021.

[24]. "Reliance spells end of road for ICT amateurs". The Australian. 7 May 2013.

[25]. "The Global Risk Report 2020" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020.