Data Security Measures

Sangita G. Utekar* **Kalpana R. Tathare****

* **Librarian**
D. G. Tatkare Mahavidyalay, Mangaon, Maharashtra, India

* **MLISc Student,**
Bharati Vidyapith, Mumbai, Maharashtra, India

QR Code

Abstract: - *Data Security is in the form of digital privacy measures that are applied to avoid this unauthorized access to websites, networks and databases. There are many ways of protecting or securing data which is important and some of them include encryption, strong user authentication, backup solutions and data erasure. There are many international laws and standards that govern data security measures. Data Protection procedures must be implemented to ensure that personal data is accessible to those whom it may concern.*

Keywords: Data management, Data Securing Technologies, Data Protection, System Security Measures

Introduction

Introduction: Data Security is the process of keeping data secure and protected from not only unauthorized access but also corrupted access. The main focus of data security is to make sure that data is safe and away from any destructive forces. While some data may not be that secretive, other might be of private value and importance. But unauthorized access to such private information or data can cause many problems such as corruption, leakage of confidential information and violation of privacy.

Data management: Besides securing and protecting data, it is also important to properly manage and monitor it. Data management is the development as well as the execution of the processes, procedures, architectures and policies which administer the complete data lifecycle requirements of a company. Data management is important because, without proper management of data, it would be difficult to monitor and protect it.

Data Security: Data security is important for most companies and businesses. Information like client details, bank details, account details, personal files, etc. must be well protected because if it gets into wrong hands, it can be misused easily. Such information can be hard to replace

and potentially dangerous. By securing such data or information, one can protect the files and avoid facing any difficulties.

The following are some of the reasons why data security is important:
The organization's reputation may be affected –
Threats are on an increase because of the emergence of mobile devices, internet, and cloud computing, etc.

Data Securing Technologies:

Disk Encryption: This is a technology through which encryption of data on a hard disk drive takes place. This technology takes place in two major ways – software or hardware. In disk encryption, data is converted into unreadable codes that cannot be accessed or deciphered by anyone who is unauthorized. There are several ways and tools to carry out disk encryption, and these tools may vary in the security offered and features used.

Software and hardware based ways to protect data: Besides disk encryption, both software and hardware based ways can also be used to protect data. On one hand, software-based security solutions encrypt the data to protect it from theft, on the other, hardware-based solutions can prevent read and write access to data. Hardware based security solutions offer very strong protection against unauthorized access and tampering. But in the case of software-based solutions, a hacker or a malicious program can easily corrupt the data files and make the system unusable and files unreadable. This is why, hardware-based solutions are mostly preferred over software based ones. The hardware-based systems are more secure due to the physical access required to compromise them. This system is much more effective in the situation where an operating system is more vulnerable to threats from viruses and hackers.

Backups: One of the easiest yet most effective ways to avoid data loss or to lose important and crucial files is by taking a backup of your data regularly. There are many ways to take backup and it is up to you how many copies of your data you wish to keep. While external hard disks are a common way to take backup, these days cloud computing too proves to be a cheap and easy way to maintain a backup of all files at a safe location. A backup will not prevent data loss but would at least ensure that you don't lose any information of importance.

Data masking: Data masking is another data securing technology that can be brought into use by those who wish to secure their data. Another term that is used to refer to data masking is data obfuscation and is the process through which one can hide original data with random characters, data or codes. This method is especially very useful for situations where you wish to protect classified data and do not want anyone to access it or read it. This is a good way to let the data be

usable to you but not to the unauthorized hacker or user.

Data erasure: Data erasure, which is only known as data wiping and data clearing is a software-based method of overwriting information or data and aims to totally destroy all data which may be present on a hard disk or any other media location. This method removes all data or information but keeps the disk operable.

Data Protection Principles:

Personal Data must be processed lawfully and fairly.

Personal data should be relevant, adequate and not excessive in relation to the purpose or purposes due to which they have been processed.

Personal data must be obtained just for one or more than one specified and lawful reasons and must not be processed in any way that is not compatible with those reason/reasons.

Personal data should be accurate and should be kept up to date wherever it is necessary to keep it up to date.

Personal data which is processed for any reason or reasons should not be kept for any time longer than required for that reason or reasons.

Personal data should not be processed according to the rights of data subjects under this Act.

The suitable technical, as well as organizational measures, must be taken against any unauthorized processing or unlawful processing of personal data and also against any accidental destruction or loss of or damage of personal data.

Description of these Measures: The following sections describe the Basic System Security Measures, the Intermediate System Security Measures, the Advanced System Security Measures, and the Data Security Measures.

Basic System Security Measures:

Password Protection: All accounts and resources must be protected by passwords which meet the following requirements, which must be automatically enforced by the system:

Must be at least eight characters long

Must NOT be dictionary or common slang words in any language, or be readily guessable

Must include at least three of the following four characteristics in any order:upper case letters, lower case letters, numbers, and special characters, such as*!@#$%^&*.

Must be changed at least once per year.

Software Updates: Systems must be configured to automatically update operating system software, server applications (webserver, mailserver, database server, etc), client software (web-browsers, mail-clients, office suites, etc), and malware protection software (anti-virus, anti-spyware, etc). For Medium or High Availability systems, a plan to manually apply new updates within a documented time period is an acceptable alternative.

Firewall: Systems must be protected by a firewall which allows only those incoming connections necessary to fulfill the business need of that system. Client systems which have no business need to provide network services must deny all

incoming connections. Systems that provide network services must limit access those services to the smallest reasonably manageable group of hosts that need to reach them.

Malware Protection: Systems running Microsoft or Apple operating systems must have anti-virus software installed and it must be configured to automatically scan and update.

B. Intermediate System Security Measures: The Intermediate System Security Measures define the Security Measures that must be applied to medium criticality and high criticality systems. Note that except under special circumstances, they do not apply to desktop and laptop computers. The requirements are:

1. Authentication and Authorization:

Remove or disable accounts upon loss of eligibility: Accounts which are no longer needed must be disabled in a timely fashion using an automated or documented procedure.

Separate user and administrator accounts: Administrator accounts must not be used for non-administrative purposes. System administrators must be provisioned with non-administrator accounts for end-user activities, and a separate administrator account that is used only for system-administration purposes.

Use unique passwords for administrator accounts: Privileged accounts must use unique passwords that are not shared among multiple systems. Credentials which are managed centrally, such as the NetID/password combination, are considered a single account, regardless of how many systems they provide access to.

Throttle repeated unsuccessful login-attempts: A maximum rate for unsuccessful login attempts must be enforced. Account lockout is not required, but the rate of unsuccessful logins must be limited.

Enable session timeout: Sessions must be locked or closed after some reasonable period.

Enforce least privilege: Non-administrative accounts must be used whenever possible. User accounts and server processes must be granted the least-possible level of privilege that allows them to perform their function.

2.Audit and Accountability:

Synchronize system clock: The system clock must be synchronized to an authoritative time server at least once per day.

Enable system logging and auditing: The facilities required to automatically generate, retain, and expire system logs must be enabled.

Follow an appropriate log retention schedule: System logs must be retained for 30-90 days and then destroyed unless further retention is necessary due to legal, regulatory, or contractual requirements.

Audit successful logins: Generate a log message whenever a user successfully logs on.

Audit failed login attempts: Generate a log message whenever a user attempts to log on without success.

Audit when a system service is started or stopped: Generate a log message when a system service is started or stopped.

Audit serious or unusual errors: Generate a log message when a serious or unusual error occurs, such as crashes.

Audit resource exhaustion errors: Generate a log message when a resource exhaustion error occurs, such as an out-of-memory error or an out-of-disk error.

Audit failed access attempts: Generate a log message when an attempt to access a file or resource is denied due to insufficient privilege.

Audit permissions changes: Generate a log message when the permissions of a user or group are changed.

Include appropriate correlation data in audit events: For each audit event logged be sure to include sufficient information to investigate the event, including related IP address, timestamp, hostname, username, application name and/or other details as appropriate.

3.Configuration and Maintenance:

1.Security Partitioning: Systems may share hardware and resources only with other systems that have similar security requirements, regardless of their criticality classification. Systems which share similar security requirements have user communities of similar size and character, similar firewall profiles, and similar technical requirements. For example:

* Multiple systems of the same criticality may be aggregated together to share hardware and resources provided they have similar security requirements.

* Medium criticality systems may share hardware and resources with low criticality systems provided that all systems meet the intermediate systems Security Measures, and share similar security requirements.

Follow vendor hardening guidelines: This document cannot be comprehensive for all systems available. Follow basic vendor recommendations to harden and secure systems.

Disable vendor default accounts and passwords: Many systems come with default accounts which are publicly known. These accounts should be disabled.

Disable all unnecessary network services: Processes and services which are not necessary to complete the function of a system must be disabled.

C. Advanced System Security Measures: The Advance system security measures define the Security Measures that must be applied to high criticality systems. The requirements are:

Audit and Accountability:

Enable process auditing or accounting: Enable process auditing or accounting, which generates logs information about the creation of new processes and their system activity.

Audit privilege escalation or change in privilege: Generate a log message whenever a user changes their level of privilege.

Audit firewall denial: Generate a log message when the host-based firewall denies a network connection.

Audit all significant application events: Log all significant application events.

Write audit events to a separate system: System logs must be written to a remote system in such a way that they cannot be altered by any user on the system being logged.

Configuration and Maintenance:

Follow advanced vendor security recommendations: This document cannot be comprehensive for all systems and applications available. Conform to best practices and recommendations outlined in vendor security whitepapers and documentation.

Host-based and network-based firewalls: Systems must be protected by both a host-based and a network-based firewall that allows only those incoming connections necessary to fulfill the business need of that system.

Configuration management process: Configuration changes must be regulated by a documented configuration and change management process.

Partitioning: Systems may share hardware and resources only with other systems that have similar security requirements, regardless of their criticality classification. Systems which share similar security requirements have user communities of similar size and character, similar firewall profiles, and similar technical requirements. For example:

Multiple systems of the same criticality may be aggregated together to share hardware and resources provided they have similar security requirements.

High criticality systems may share hardware and resources with medium and low criticality systems provided that all systems meet the advanced systems Security Measures, and share similar security requirements.

Additional Requirements:

Physical access: The system must reside in a secured, managed data-center.

D. Data Handling Security Measures:

The Data Security Measures define the minimum security requirements that must be applied and must be recorded in a manual.

Requirements for Handling Confidential Data:

Access control: Access to Confidential data must be provided on a least-privilege basis. Sharing: Confidential data may be shared only among authorized persons, and with permission.

Retention: Confidential data should only be stored for as long as is necessary to accomplish the documented business process.

Incident Notification: If there is a potential security incident that may place protected data at risk of unauthorized access, the office must be notified.

Requirements for Handling Restricted Data:

1.Collection: Restricted data should only be collected when all of the following conditions are met:

The data is not available from another authoritative source, and

The data is required by business process, and

You have permission to collect the data from the appropriate data steward or

If the data is requested by the Office of General Counsel in response to litigation.

2.Access control: Individuals must be granted access to restricted data on a least-privilege basis. No person or system may access the data unless required by a documented business process. In such cases where access is required, permission to use the data must be granted by the data steward.

Devices which can be used to access restricted data must automatically lock after some period of inactivity, through the use of screensaver passwords, automatic logout, or similar controls.

Restricted data must be encrypted during transmission with a suitable method.

Restricted data should only be stored for as long as is necessary to accomplish the documented business process.

When restricted data is no longer needed it should be destroyed in accordance with applicable policies, using methods that are resistant to data-recovery attempts such as cryptographic data destruction utilities, on-site physical device destruction, or NAID certified data destruction service.

3.Incident Notification: If there is a potential security incident which may place restricted data at risk of unauthorized access, the authorities must be notified.

Conclusion:

Security measures are important to protect computers and data from any security threats. Security measure must be update to avoid any latest security threats. Countermeasures and controls can be applied to the data, the programs, the system, the physical devices, the communications links, the environment, and the personnel. Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems and their components.

Bibliography:

1. A Complete Guide to Data Security. (2015, April 30). Retrieved January 3, 2018, from https://www.cleverism.com/complete-guide-data-security/
2. Tonsager, L. (2018). 5 Privacy and Data Security Measures That Can Protect Your Company Against Trade Secret Theft. Retrieved January 3, 2018, from https://www.insideprivacy.com/data-security/5-privacy-and-data-security-measures-that-can-protect-your-company-against-trade-secret-theft/
3. What is Database Security? - Definition from Techopedia. (2018). Retrieved January 3, 2018, from https://www.techopedia.com/definition/29841/database-security