Part 5: Backup and Encrypt Data

Introduction

For organizations, data backup and recovery is crucial for day-to-day operations. It is vital to prepare ahead of time and set up data backup procedures in case the worst-case scenario occurs, such as employing an offsite server or external drives to store large amounts of information. Without these methods, data recovery might be difficult, resulting in the permanent loss of information.

Backup

- It is important that all systems containing essential business information are identified to ensure adequate assurance be taken of them when backing up its information.

- Essential systems will have both onsite and offsite backup. It is vital to determine what type of backup is to be used for what information; it being either a full, incremental or differential backup. Non-essential systems may also be backed up. Essential systems should have offline backups.

- Essential systems shall be restorable within **2** business days. Non-essential systems should be restorable within **6** business days.

- All backups and recovery processes are tested and verified weekly.

- Access is restricted solely to the individuals responsible for backup, testing, and restoration.

Encryption

Introduction

A crucial component of thorough data protection is encryption. Whether the data is on a device, in transit, or in the cloud, encryption maximizes data security. It can be extremely helpful in the fight against sophisticated attacks, in preventing breaches made possible by IoT, and in preserving regulatory compliance.

- All backups, whether onsite, offsite, or offline are stored in an encrypted state, preferably in AES 256 as it's impossible to crack using brute force, and the computing power required to crack it in a different way is still not available.

- It is the responsibility of the organization to ensure the requirements outlined above are implemented. They are the sole personnel permitted to access, restore, test, and manage company backups.

- Identify and list business data and information systems essential to the organization. Use the table below if preferred.

- Identify non-essential systems, information and data repositories which should be included in your backup schedule and plan.

- Determine backup locations and frequency, verify against minimum requirements as outlined in the policy section.

Event Recovery Process

Introduction

The Cybersecurity Framework (CSF) defines the lifespan of the enterprise risk management process with five components: identify, protect, detect, respond, and recover. The recover function has a tremendous impact on the business, with two recovery stages: immediate tactical and long-term strategic. This section offers advice on how to plan and prepare for a cyber event, as well as how to recover from it and incorporate the processes and procedures into enterprise risk management strategies.

There are two parts to this section, it is crucial that all actions be done before and after the cyber event occurs, respectfully. The first part will include tactical recovery efforts for cyber incident recovery, which rely on the activities completed during the enterprise risk management lifecycle process's protection, detection, and reaction capabilities. The second part is more strategic and focuses on the ongoing enhancement of the organization's lifecycle of risk management processes.

Part 1

• Make a list of all the resources, people, processes, and technology that the organisation has access to in order to fulfill its goal. Include any dependencies between these resources, along with any dependencies.

- A designated person or role to coordinate with the response team and any consultants to provide access to offline and online backups as needed.

• All assets should be categorised and kept up to date according to their interdependencies and relative importance so that recovery efforts may be safely prioritised.

• Document the circumstances under which the recovery plan will be activated, who has the ability to activate it, and how recovery personnel will be alerted. Also, define key milestones, intermediate recovery goals, and criteria for concluding active recovery procedures.

• Ensure that initial restoration planning considers the necessity for tactical recovery operations in order to prevent recovery from significantly impacting incident response.

• Create a thorough recovery communications plan that clearly defines recovery communication goals, objectives, and scope, as well as information sharing rules and techniques.

• With realistic goals and roles, organizations should conduct cyber incident recovery exercises and testing within an acceptable timeframe according to the organization. To strengthen the organization's cybersecurity posture and ensure that they can fulfill their mission, they should update plans, policies, and processes.

• Document issues regularly during recovery so that there is enough information later in the recovery process or immediately after recovery to expand on documentation and enhance capabilities.

• Implement event, signature, and other monitoring types to inform the organization about known malicious activity. Keep track of any artifacts or evidence discovered during detection and response.

Part 2

• Based on the tactical phase results, create and implement an improvement strategy for the organization's overall security standing.

• Communicate with internal and external stakeholders to keep them updated on the recovery effort's progress. Any improvements should be communicated to internal stakeholders, while any impact should be expressed to external stakeholders.

• Review the objectives, evaluations, and benchmarks that were established during the tactical phase. This data can be used to measure the success of the recovery effort and point out areas that require improvement.

References

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016, December 1). *SP 800-184, Guide for Cybersecurity Event Recovery | CSRC*. SP 800-184, Guide for Cybersecurity Event Recovery | CSRC. https://doi.org/10.6028/NIST.SP.800-184