Jamia Millia Islamia

Dept. Of Computer Science

Big Data Assignment-#2

Submitted By: Wasit Shafi

Roll no: 18MCA054

Submitted To: Dr.Mansaf Alam

Q1. What is data security. Explain security policy.

Sol.

Data Security : Data Security is a process of protecting files, databases, and accounts on a network by adopting a set of controls, applications, and techniques that identify the relative importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.

Security policy

1. Ensuring Data Security Accountability: A company needs to ensure that its IT staff, workforce and management are aware of their responsibilities and what is expected of them. The various types of data should be classified so that both workers and management understand the differences. By categorizing data, employees are aware of how to handle each type and which types they are allowed to distribute. Important classes to include in the policy are:

- Confidential data
- Data that is meant to be sent internally within the company
- General data
- Data that is meant to be sent outside the company

2. Policies that Govern Network Services : This section of the data security policy dictates how the company should handle issues such as remote access and the management and configuration of IP addresses. It also covers the security of components like routers and switches.

3. Scanning for Vulnerabilities: It is important to find any vulnerabilities in a company's IT infrastructure before hackers do. Since hackers will scan for vulnerabilities the minute they are discovered, a company should have a routine in place for checking its own networks regularly.

4. **Managing Patches :** Implementing code to eliminate vulnerabilities can help to protect against threats. How and when patches are to be implemented in the system should be a part of the data security policy.

5. Monitoring Compliance: The use of audits is a good way to ensure that the company's staff and management are complying with the various elements of a data security policy. These audits should be performed on a regular schedule.

Q2.Explain tools to monitor secure data, document data security.

Sol.

1. FireHost Compliance as a Service (FireHost Inc.)

If your business is in an industry that has strict data compliance requirements but lacks the staff or skills to deploy a solution, Texas-based FireHost offers what it describes as a cloud-based Compliance as a Service (CaaS). The service entrusts FireHost experts with securing your data and ensuring you're meeting such requirements as PCI and HIPAA. The service also aims to reduce the need for multiple security products.

2. StorageGRID Webscale (NetApp Inc.)

In order to keep data secure, organizations must know where their data is stored. NetApp Storage-GRID, Webscale provides monitoring tools that lets IT track the physical movement of data. This storage management tool tracks large amounts of uncategorized data and keep it constant with the same security levels extended to confidential enterprise data.

It supports the Amazon Web Services Simple Storage Service (S3) and implements automatic encryption and access control capabilities & aims to limit the threat of an unauthorized access or data leak.

3. Keyless SSL (CloudFlare Inc.)

CloudFlare has made a name for itself over the past few years giving Web sites hosted in its service protection from distributed denial-of-service (DDoS) attacks. Recently, the

company has come up with a solution for those enterprises not wanting to hand over SSL encryption keys to cloud providers in its Keyless SSL solution.

4. Share Plan for Enterprises (Code 42 Software Inc.)

Whether you're keeping your enterprise files in a public cloud, an on-premises private cloud or in a hybrid deployment, the service you choose can make a difference when it comes to ensuring your organization's data is secure. Share Plan for Enterprises from Code 42 looks to keep your documents secure and encrypted while allowing for easy employee access to data, whether they're on-premises or in the cloud.

Q3.What is host security Discuss Disaster recovery?

Sol.

Host Security: Host security describes how your server is set up for the following tasks: Preventing attacks. Minimizing the impact of a successful attack on the overall system. Responding to attacks when they occur.

Cloud disaster recovery is a service that enables the backup and recovery of remote machines on a cloud-based platform. Cloud disaster recovery is primarily an infrastructure as a service (IaaS) solution that backs up designated system data on a remote offsite cloud server.

Q4.What is Disaster in cloud? Discuss scaling a cloud infrastructure: Capacity Planning and Cloud Scale.

Sol.

A disaster is any type of unexpected event that disrupts your business's IT workloads. A disaster could be caused by the failure of a cloud provider's hardware, such as the data center fire that disrupted service to some Azure customers in 2017.

Scaling a Cloud : Scalability is the capability of a process, network, software or appliance to grow and manage increased demands. This is one of the most valuable and

predominant feature of cloud computing. Through scalability you can scale up your data storage capacity or scale it down to meet the demands of your growing business.

Capacity planning seeks a heavy demand. It determines whether the systems are working properly, used to measure their performance, determine the usage of patterns and predict future demand of cloud-capacity. This also adds an expertise planning for improvement and optimizes performance.

Cloud-scale is a cloud-based service, application, system or platform that can be scaled without any technical limitations. Without technical limitations, such cloud technologies are only limited by financial resources, contractual limitations and physical resources such as data centers.