USER INFORMATION PROTECTION TECHNOLOGIES IN THE GOOGLE CLOUD

Abdusamatova Shahodat Khojiakbar's daughter
Informatics and information technology teacher at the academic lyceum named after Islam Karimov at the Almalyk branch of TDTU
Mannonov Asliddin Akbar's son
Student of cyber security faculty of TATU named after Al Khorazimi, phone:

Abstract: *This article presents technologies for protecting user information in the Google cloud, which has the largest data warehouse*

Keywords: *cloud technologies. Google Drive, user information, cloud computing, cloud infrastructure.*

Like all major cloud vendors, Google Cloud Platform (GCP) practices cloud security under a shared responsibility model that requires both the cloud provider and the customer to implement security measures. GCP is required to protect its infrastructure, while cloud users need to protect their cloud resources, workloads, and data. To help users protect their cloud assets, GCP provides many security tools natively integrated with GCP services, including key management, identity and permission management, logging, monitoring, security scanners, asset management, and compliance.

Google uses various measures to protect its infrastructure. For example, the following basic security services are available to ensure security:

Cryptographic authentication and authorization - applied at the application level for all inter-service communications. This feature allows for granular access control. In this security technology, if the user wants to use Google's services or data stored in the cloud on different devices and places, he must go through authentication and authorization processes, which is done remotely based on Google's special software tool.

Service Account ID - Any service running on Google's cloud infrastructure is associated with cloud technology. A service must use cryptographic credentials to make remote procedure calls (RPCs) to other services or to identify itself to clients. For example, a user who wants to use such services on Google's server or the information or service of a site on another server can verify his identity through a Google account and use it remotely.

Segmentation and firewalls - Google's cloud infrastructure is protected by firewalls and uses ingress and egress filters on important network connections to prevent IP spoofing, that is, Google users can see who accessed their account and from which device and from where. Or if a Google account is opened for parents to monitor their child, they can monitor it.

Protection against privileged access attacks - Google designs its infrastructure with security in mind. This includes measures to protect against privileged access attacks originating from the hypervisor, operating system (OS) image, or bootloader. For example,

Google uses a variety of components from different vendors that are carefully selected in its infrastructure to ensure security.

Data destruction features - Google provides data disposal that performs frequent logical cleaning of permanent drives and other storage devices. After the discs are erased, the inspection is usually done by an authorized person. All processes are recorded and stored with relevant results. At the end of the process, all usable deleted drives are sent for reuse and damaged disks are deleted. In addition, data destruction facilities are audited weekly.

Data encryption – Google provides encryption for data at rest and in transit. This process is automated and does not require user intervention. For example, AES-256 is a process that encrypts persistent disks using persistent keys and master keys. Google manages all the keys and rotation of this process.

Secure Internet Connection - Google Front End (GFE) is an infrastructure service that protects services available on the Internet. GFE ensures that TLS connections use the correct certificates and follow best practices, and also protects against Denial of Service (DoS) attacks.

Operational Security – Several operational security measures implemented and implemented by Google:

Data Sources - Combines network signals from host-based signals from monitoring, infrastructure services, and personal devices.

Machine Learning Analytics – Analyzes data and provides Google teams with alerts about potential incidents.

Investigation - Google's incident responders are responsible for alert prioritization, incident investigation and response to potential incidents. They operate 24/365 and conduct Blue Team/Red Team exercises to improve operational practices.

REFERENCES:

1. Michael Cobb "7 Best Practices for GDPR Compliance"

2. "Cyber security against cybercrime" Abdurasul IMINOV, head of the Department of Information Technologies of the Ministry of Internal Affairs, lieutenant colonel

3. "Guide to security technologies and trends in 2022" e-guide