Google's trusted infrastructure

So far, you've learned about the cloud's underlying infrastructure, and how it compares to an on-premises framework. In this reading, you'll learn how a cloud service provider's (CSP's) many layers work together to secure infrastructure. Using Google's infrastructure as a model, you'll learn about the many aspects of keeping cloud infrastructure safe.

You'll also gain insight into how Google secures their physical infrastructure, service deployments, data storage, internet connectivity, and operations. An understanding of these layers will broaden your awareness of security concerns specific to the cloud.

Google's trusted infrastructure

Google implements security in five progressive layers, and each layer adds security measures to different aspects of their infrastructure.

Secure low-level infrastructure

Google's low-level infrastructure is the physical aspect of the data center's infrastructure, which includes the security of data centers, servers, and the software run on those devices. Access to data centers is very restricted. Employees, vendors, and contractors entering the premises are subject to camera surveillance, metal detectors, and biometric identification.

Servers must also meet specific requirements. For example, each server has its own unique identity that authenticates data flowing in and out. Google uses automation to check for software updates, detect hardware or software problems, and authenticate credentials that communicate with servers. Automation helps bolster infrastructural security because it reduces human and manual effort to perform common and repetitive tasks.

Secure service deployment

Google's infrastructure uses a zero-trust security model. In this model, all users, devices, and systems must be authenticated and authorized before gaining access to the network. This protocol is a crucial part of keeping service deployments secure.

The zero-trust security model is especially important in a multi-tenant environment where data is spread across the shared public infrastructure. With zero trust in place, customer data is isolated from other customers sharing the same server machines. This means that although different customers share the same infrastructure, they're unable to access each other's data.

Also, applications use cryptographic authentication and authorization to provide access control across services. This means a person's or application's credentials are encrypted in a non-human readable format, keeping login information secure.

Secure data storage

Another security measure Google uses is to protect user data is to enforce encryption at rest. This practice encrypts stored data that's not actively in use, so malicious actors can't view sensitive information.

Google also uses an approach where data is scheduled for deletion. The scheduling approach protects stored data from unintentional deletion, like user error or malicious activity.

Secure internet communication

Securing cloud infrastructure requires a range of layers. Since the cloud's services rely on communication through the internet, the cloud's network must have strong security. For example, Google's infrastructure is isolated from the public internet through the use of a private IP address space, meaning communication is only possible within the private network. Isolating infrastructure helps defend against cyber-related attacks, like denial of service attacks.

Another measure of securing communication with Google's services and network involves using credentials to access cloud services. Users must input their username and password to log in to their account.

Operational security

Google takes several measures to keep their operations and employee information secure, like:

- Using verified code libraries that prevent security bugs
- Integrating manual security reviews performed by security experts to test software
- Safeguarding employee devices and credentials
- Monitoring for threats

Developers use specific code libraries to create applications, which help prevent the introduction of bugs and cross-site scripting. Before becoming the foundation for applications, the libraries' source code is reviewed and tested. Once developers create applications using the verified code samples, experts in web and operating system security test the applications to check for security vulnerabilities.

Google also has several security protocols for their employees and devices. Employees use multi-factor authentication to log in to devices, and devices are regularly updated with security patches and monitored for suspicious activity. Monitoring devices helps reduce

insider risk, where employees could misuse their access to the network. Also, employees are only provided access to data and resources that they require to fulfill their job responsibilities, provisioned by identity and access management.

Finally, Google has a dedicated group of security experts who monitor for the latest security threats. They research techniques like social engineering that threat actors use to carry out ransomware, spyware, and watering hole attacks.

Key takeaways

Google's infrastructure serves as one model for securing cloud infrastructure. These measures can be adopted by a cloud service provider to increase their defenses against cybercrime. As a cloud security professional, it's important for you to understand the many components to securing cloud infrastructure.

Resources for more information

- Review Google's whitepaper for their Infrastructure Security Design Overview