

You Can't Secure the Cloud, Right?

• Security in the Cloud

a. Lima lapisan perlindungan yang meliputi operational security, internet communication, storage services, service deployment, hardware infrastructure

b. Hardware infrastructure layer

- Hardware design and provenance: papan server serta perangkat jaringan di pusat data Google dirancang khusus oleh Google sendiri
- Secure boot task: memastikan sistem melakukan booting dengan software stack yang benar
- Premises security: Google merancang dan membangun pusat datanya sendiri

c. Service deployment layer

- Encryption of inter-service communication = layanan Google berkomunikasi menggunakan remote procedure calls (RPC). Menyediakan privasi dan integritas kriptografi
- User identity = secara cerdas meminta informasi tambahan dari pengguna berdasarkan faktor-faktor risiko tertentu

d. Storage services layer

- Encryption at rest = sebagian besar aplikasi Google mengakses penyimpanan file secara tidak langsung melalui layanan penyimpanan dan enkripsi. Enkripsi diterapkan pada lapisan layanan penyimpanan ini

e. Internet communication layer

- Google front end (GFE) = memastikan semua layanan terdaftar menggunakan koneksi TLS
- Denial of service (DoS) protection = mengurangi risiko dampak DoS pada layanan yang berjalan di belakang GFE

f. Operational security layer

- Intrusion detection

- Reducing insider risk
- Employee universal second factor (U2F) use
- Software development practices

• **The Shared Security Model**

- Tanggung jawab keamanan dibagi antara pelanggan dan Google Cloud
- Ketika pelanggan mendeploy aplikasi ke infrastruktur on-premises mereka, mereka bertanggung jawab atas keamanan seluruh stack
- Ketika mereka memindahkan aplikasi ke Google Cloud, Google menangani banyak lapisan keamanan
- Google Cloud menyediakan tools untuk membantu mengontrol akses ini, yaitu Identity and Access Management (IAM)

• **Encryption Options**

a. Customer-managed encryption keys (CMEK)

- Mengelola kunci dalam solusi yang di-hosting di cloud
- Enkripsi dan dekripsi melalui API
- Rotasi kunci otomatis dan sesuai keinginan
- Dukungan kunci simetris dan asimetris

b. Customer-supplied encryption keys (CSEK)

- Kontrol lebih besar, kompleksitas manajemen keamanan yang lebih tinggi
- Bertanggung jawab menyimpan kunci

c. Persistent disk encryption with CSEK

- Data dienkripsi sebelum meninggalkan instance
- Kunci yang ditentukan sistem atau disediakan pelanggan

d. Client-side encryption = mengenkripsi data secara lokal sebelum menyimpannya di cloud

• **Authentication and Authorization with IAM**

- Memungkinkan administrator mendefinisikan siapa yang dapat mengakses dan menerapkan kebijakan
- Role types = basic, predefined, custom
- Cloud identity = menyederhanakan manajemen pengguna, dan akun layanan memungkinkan autentikasi aplikasi secara aman
- Kebijakan IAM diterapkan secara hierarkis, sehingga memudahkan pengelolaan keamanan pada resources

• Lab: User Authentication: Identity-Aware Proxy

- IAP adalah resource yang digunakan untuk mengatur autentikasi pada aplikasi berbasis HTTP
- Hanya pengguna dan grup tertentu yang dapat mengakses aplikasi dan resource yang dilindungi oleh IAP
- IAP melakukan autentikasi dan otorisasi

Pada lab ini, saya diajarkan cara mendeploy app dan memproteksi menggunakan IAP (restrict access). Diajarkan juga cara menggunakan cryptographic verification.

• Lab: Cloud IAM: Qwik Start

Pada lab ini, saya diajarkan cara assign role pada second user dan remove assigned roles, membuat Cloud Storage bucket, dan remove project access

• Quiz

1. When a customer moves an application to Google Cloud, which one of the following does the customer remain responsible for? Data security
2. Which IAM role is the most broad in scope? Basic
3. At which level of Google Cloud's infrastructure security will you find intrusion detection? The operational security system
4. With which encryption option does a customer encrypt data before sending it to Google Cloud? Client-side encryption

Congratulations!

You've completed Google Cloud Computing Foundations: Infrastructure in Google Cloud!

