Ikhtisar

Tak terasa ya sudah sejauh ini kita melangkah pada materi keamanan. Baiklah, sekarang saatnya mengurai apa yang telah kita pelajari.

- Pertama, AWS menyajikan *shared responsibility model* alias model tanggung jawab bersama. AWS bertanggung jawab atas keamanan dari cloud sementara Anda bertanggung jawab untuk keamanan di cloud.
- Kemudian, AWS IAM memungkinkan Anda untuk memiliki users, groups, roles, dan policies.
    - *Users* dapat Anda pakai untuk *login* atau masuk ke AWS dengan menggunakan nama pengguna dan kata sandi. Ia juga secara default tidak memiliki *permission* (izin) sama sekali.
    - *Groups* merupakan kumpulan dari beberapa pengguna.
    - *Roles* adalah identitas yang berguna untuk memberikan akses kredensial sementara dan permission untuk jangka waktu tertentu.
    - *Policies* berfungsi untuk memberikan permission ke sebuah identitas secara eksplisit, baik *allow* (mengizinkan) atau *deny* (menolak) suatu tindakan tertentu di AWS.
    - IAM juga menghadirkan *identity federation* (federasi identitas). Jika suatu perusahaan telah memiliki penyimpanan identitasnya sendiri, maka user di perusahaan tersebut dapat terkoneksi ke AWS menggunakan *role based access* (akses berbasis peran). Hal itu memungkinkan user melakukan sekali *login* untuk sistem perusahaan tersebut dan sekaligus juga lingkungan AWS.
    - Satu hal terakhir yang perlu diingat tentang IAM adalah *multi-factor authentication* (MFA). Pastikan Anda mengaktifkan MFA untuk setiap user, terutama *root user* yang memiliki semua permission secara default dan tak dapat direstriksi.

- Selanjutnya, kita juga telah membahas AWS Organizations. Saat menggunakan AWS, kemungkinan Anda akan memiliki beberapa akun. Biasanya, akun digunakan untuk mengisolasi beban kerja, lingkungan, tim, atau aplikasi. Nah, AWS Organizations dapat membantu Anda untuk mengelola beberapa akun secara hierarkis.
- Tak luput kita juga telah belajar mengenai *compliance*(kepatuhan). AWS menggunakan auditor pihak ketiga untuk membuktikan compliance-nya terhadap beragam program compliance. Anda dapat menggunakan:
    - AWS Compliance Center untuk menemukan informasi lebih lanjut tentang compliance.
    - AWS Artifact untuk mendapatkan akses ke dokumen compliance.

  Persyaratan compliance yang Anda miliki mungkin dapat bervariasi untuk setiap aplikasinya.

- Lalu, kita telah menelaah tentang serangan distributed denial-of-service (DDoS) dan cara menanganinya dengan menggunakan layanan seperti ELB, security group, AWS Shield, dan AWS WAF.
- Kemudian, kita juga telah mempelajari materi enkripsi. Di AWS, Anda sebagai pemilik data bertanggung jawab atas keamanannya. Itu berarti Anda perlu menerapkan enkripsi untuk data yang Anda miliki, baik *in-transit* (ketika dikirim) maupun *at rest* (saat disimpan).

Keamanan adalah prioritas utama AWS, dan akan terus demikian. Ada banyak pertimbangan saat menangani keamanan di AWS. Oleh sebab itu, pastikan Anda membaca dokumentasi tentang cara mengamankan sumber daya AWS Anda karena akan berbeda setiap layanannya.

Ingat! Gunakan *least privilege principle* (prinsip privilese paling rendah) saat memberikan *permission* (izin) kepada user dan role di IAM; enkripsi data di setiap lapisan; dan pastikan Anda menggunakan layanan AWS untuk melindungi lingkungan cloud Anda.

Materi Pendukung

Silakan review tautan berikut untuk mempelajari lebih lanjut tentang konsep yang telah kita bahas di modul ini:

- Security, Identity, and Compliance on AWS
- Whitepaper: Introduction to AWS Security
- Whitepaper: Amazon Web Services - Overview of Security Processes
- AWS Security Blog
- Kepatuhan Cloud
- Studi Kasus

Sebelumnya

Selanjutnya