Rakamin Academy

Cloud Computing

Cloud Security and Governance

Raih Mimpi #TanpaBatas

Outline Pembelajaran

Rakamin Academy

Security & Governance

- [ ] Pendahuluan Security & Governance
- [ ] Identity Access Management (IAM)
- [ ] Perlindungan Data dan Enkripsi
- [ ] Compliance & Risk Management
- [ ] Studi Kasus dan Diskusi

Objektif sesi

- Mengenalkan konsep dasar dari Cloud Security dan Governance
- Mengenalkan konsep *Identity and Access Management* (IAM)
- Mempelajari konsep Data Protection and Encryption di Cloud
- Memahami kepentingan Compliance dan Risk Management dalam konteks cloud

Expected output

- Peserta dapat memahami dan menerapkan prinsip-prinsip dasar Cloud Security and Governance.
- Peserta mampu merancang dan menerapkan strategi IAM efektif.
- Peserta memahami dan dapat melaksanakan teknik Data Protection dan Encryption di cloud.
- Peserta mampu menjalankan program Compliance dan Risk Management dalam lingkungan cloud.
- Peserta memiliki keterampilan praktis dalam menerapkan konsep-konsep yang dipelajari ke dalam kasus nyata.

Cloud Security & Governance

Cloud Security adalah perlindungan data, aplikasi, dan infrastruktur yang ada dalam teknologi cloud. Sedangkan Governance adalah kerangka kerja yang menentukan bagaimana teknologi cloud dikelola dan digunakan secara efisien, efektif, dan aman.

Tujuan

Mengelola dan melindungi informasi dan operasi yang terjadi di lingkungan cloud.

Manfaat

Melindungi data dan sistem dari risiko keamanan cyber, menjaga privasi data, memastikan kepatuhan terhadap regulasi industri dan pemerintah, memaksimalkan efisiensi operasional.

Peran dalam Industri Modern

Dengan meningkatnya penggunaan teknologi cloud, keamanan dan tata kelola cloud menjadi sangat penting. Ini membantu organisasi untuk melindungi aset mereka, memastikan kelancaran operasi, dan mematuhi standar keamanan dan privasi yang ditetapkan.

Standard and Best Practices

Beberapa standar industri yang umum untuk keamanan dan tata kelola cloud termasuk ISO/IEC 27001, NIST SP 800-53, dan CIS Critical Security Controls.

Best Practices Keamanan

- Mendefinisikan dan mengimplementasikan kebijakan keamanan yang kuat
- Menggunakan otentikasi dua faktor
- Menerapkan kontrol akses yang ketat
- Melakukan audit keamanan secara berkala

Best Practices Governance

- Mendefinisikan dan mengimplementasikan kebijakan dan prosedur tata kelola
- Menyediakan pelatihan dan sumber daya yang tepat untuk staf
- Mengintegrasikan tata kelola cloud dengan tata kelola TI secara keseluruhan

Identity and Access Management

IAM adalah kerangka kerja yang digunakan untuk mengelola identitas digital dan hak akses pengguna dalam suatu sistem

Manfaat :

1. Memperkuat keamanan data dengan memastikan hanya pengguna yang berwenang yang dapat mengakses sistem dan data
2. Meningkatkan produktivitas dan efisiensi operasional dengan memberikan akses yang tepat dan cepat ke sistem dan data.
3. Membantu memenuhi persyaratan kepatuhan dengan melacak dan melaporkan aktivitas pengguna.

Best Practices :

1. Menggunakan otentikasi dua faktor untuk meningkatkan keamanan
2. Menerapkan principle of least privilege (POLP), yaitu memberikan hak akses minimal yang diperlukan untuk melakukan tugas
3. Mengatur proses untuk manajemen lifecycle akun pengguna (pembuatan, pembaruan, dan penghapusan akun)

Studi Kasus : Implementasi IAM dalam sektor Perbankan

Dalam sektor perbankan, kerahasiaan dan integritas data adalah hal yang sangat penting. Oleh karena itu, penggunaan IAM menjadi sangat penting.

IMPLEMENTASI:

Bank biasanya menggunakan otentikasi multi-faktor untuk memastikan identitas pengguna. Mereka juga menerapkan POLP untuk membatasi akses hanya kepada mereka yang membutuhkannya.

HASIL YANG DIHARAPKAN:

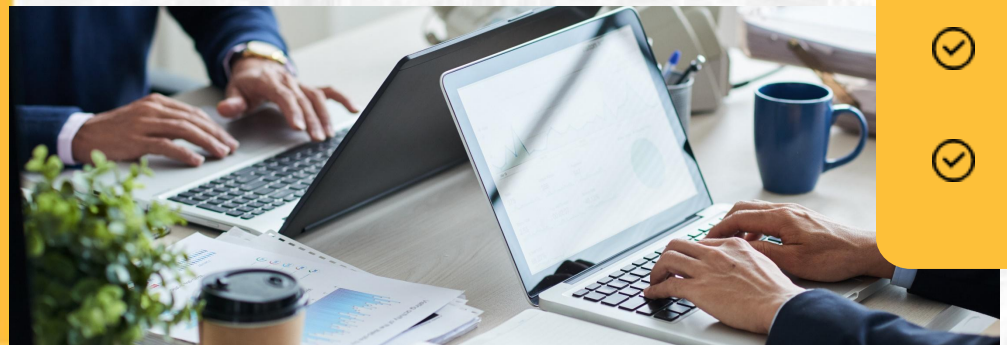
Dengan implementasi IAM yang tepat, bank dapat melindungi data pelanggan dan transaksi mereka dari ancaman keamanan, serta memastikan mereka mematuhi regulasi perbankan

DISKUSI PERTANYAAN TERBUKA:

Apa pelajaran yang bisa kita ambil dari implementasi IAM di sektor perbankan? Bagaimana ini dapat diterapkan di industri lain?

Perlindungan Data Dan Enkripsi

Data Protection adalah serangkaian strategi dan teknologi yang digunakan untuk memastikan bahwa data tetap aman, tersedia, dan rahasia. Encryption adalah proses mengubah informasi atau data menjadi kode rahasia untuk mencegah akses yang tidak sah.



Strategi Data Protection di Cloud:

- Backup dan Disaster Recovery: Menyimpan salinan data di lokasi yang berbeda untuk memastikan data dapat dipulihkan jika terjadi kegagalan sistem atau data loss
- Data Masking: Menggunakan metode untuk menyembunyikan data asli dengan data palsu atau modifikasi yang tidak dapat diidentifikasi.

Metode Enkripsi di Cloud

- Data-at-rest Encryption: Mengenkripsi data saat tidak sedang digunakan atau disimpan.
- Data-in-transit Encryption: Mengenkripsi data saat sedang ditransfer antara sistem atau jaringan

Studi Kasus : Proteksi dan Enkripsi Data dalam Sektor Perbankan

Data adalah aset paling berharga bagi perbankan. Oleh karena itu, proteksi dan enkripsi data sangat penting untuk menjaga kerahasiaan dan integritas data.

IMPLEMENTASI:

Bank biasanya memiliki solusi backup dan disaster recovery untuk memastikan data dapat dipulihkan jika terjadi data loss. Mereka juga menggunakan enkripsi baik untuk data-at-rest maupun data-in-transit untuk memastikan data aman dari akses yang tidak sah.

HASIL YANG DIHARAPKAN:

Dengan proteksi dan enkripsi data yang tepat, bank dapat melindungi data pelanggan dan transaksi mereka dari ancaman keamanan, serta memastikan mereka mematuhi regulasi perbankan.

DISKUSI PERTANYAAN TERBUKA:

Apa pelajaran yang bisa kita ambil dari strategi proteksi dan enkripsi data di sektor perbankan? Bagaimana ini dapat diterapkan di industri lain?

Compliance & Risk Management

Compliance adalah penerapan standar, regulasi, dan hukum yang berlaku. Risk Management adalah proses identifikasi, penilaian, dan kontrol terhadap risiko yang dapat mengancam tujuan organisasi.

Kedua konsep ini sangat penting dalam Cloud Security. Compliance membantu perusahaan mematuhi hukum dan regulasi yang berlaku, sementara Risk Management membantu perusahaan menangani dan memitigasi risiko yang dapat mempengaruhi keamanan dan operasi perusahaan

Best Practices :

01 Mengimplementasikan framework Compliance dan Risk Management seperti ISO 27001 atau NIST SP 800-53

02 Melakukan penilaian risiko secara berkala untuk mengidentifikasi dan mengatasi risiko baru.

03 Melakukan audit internal dan eksternal untuk memastikan kepatuhan dan efektivitas manajemen risiko.

Diskusi


Rakamin
Academy
Thank you
Raih Mimpi #TanpaBatas