**Rangkuman Webinar “Cloud and IoT Security :**

**The Trend of Cloud Security”**



Nama : Dzikri Mutawakkil Al Hamdika

NRP : 3121600041

**Sarjana Terapan Teknik Informatika**

**Politeknik Elektronika Negeri Surabaya**

**2022**

**Pengantar**

Komputasi awan adalah model yang menawarkan layanan komputasi instan tanpa menanggung biaya. Namun demikian, seperti teknologi lainnya, ia membawa kekurangannya. Salah satu masalah utama adalah masalah keamanan dan privasi termasuk kebocoran data karena infrastruktur sumber daya komputasi bersama untuk memproses informasi bisnis rahasia - seperti kekayaan intelektual, rahasia dagang, dan informasi rahasia pelanggan, yang dapat menyebabkan aktor yang tidak berwenang dapat mengaksesnya.

1. **Ancaman**
   1. Kehilangan data dan kebocoran data

Sebagian besar fitur perlindungan data cloud untuk perusahaan ditawarkan secara terpisah sebagai layanan opsional dan tambahan, mis. penyimpanan tambahan untuk retensi snapshot dan anti ransomware karena sumber dayanya luas dan mahal

* 1. Penyalahgunaan dan Penggunaan Jahat

Karena komputasi awan adalah ekosistem multi layanan, interaksi, dan saling ketergantungan, telah menjadi lebih umum. Eksploitasi (PagS) untuk "Peretasan sebagai Layanan" dapat lebih menantang untuk dikurangi karena tersembunyi di infrastruktur yang sama.

* 1. Antarmuka dan API yang tidak aman

Memanfaatkan API yang tidak aman di lingkungan multitenancy dapat meningkatkan risiko spionase bisnis, yang berpotensi mengakibatkan kompromi atau pencurian data sensitif dan pribadi.

* 1. Masalah Teknologi Bersama

Penyedia layanan cloud menggunakan infrastruktur yang dapat diskalakan untuk mendukung banyak penyewa yang berbagi infrastruktur yang mendasarinya. Pada lapisan terendah, di mana hypervisor dapat dieksploitasi dari mesin virtual yang disusupi di sewa lain untuk mendapatkan akses ke semua VM di lingkungan bersama yang sama.

1. **Serangan**
   1. Serangan Tingkat Mesin Virtual

Serangan pada platform Cloud yang sama dapat mempengaruhi penyewa lainnya. Wajib bagi penyebaran Cloud apa pun untuk mengeraskan lapisan virtualisasi untuk mencegah serangan VM ke VM.

* 1. Pembajakan Layanan dan Sesi

Dalam serangan pembajakan sesi, penyerang mencoba untuk mengambil alih sesi atau koneksi yang sedang berlangsung antara pengguna dan layanan, dan kemudian menggunakan koneksi tersebut untuk memperoleh akses ke informasi pribadi atau sistem yang terhubung ke layanan tersebut. Penyerang dapat mencuri informasi otentikasi seperti username, password, token akses, atau cookie sesi yang digunakan oleh pengguna saat mengakses layanan. Setelah informasi ini dicuri, penyerang dapat menggunakan akses tersebut untuk mengakses akun pengguna dan melakukan aktivitas yang tidak sah, seperti mengubah informasi pribadi, mencuri data sensitif, atau melakukan transaksi keuangan.

* 1. Manusia di Awan dan DDoS

Serangan DDoS dilakukan dengan cara menggunakan banyak komputer yang terhubung ke internet dan dikendalikan oleh penyerang untuk mengirimkan lalu lintas ke sistem target secara bersamaan. Seiring dengan meningkatnya adopsi teknologi cloud, serangan DDoS pada layanan cloud semakin sering terjadi karena layanan cloud dapat diakses melalui internet.

1. **Keamanan**
   1. Lapisan Kontrol Awan

Gunakan lapisan kontrol tambahan dalam manajemen Cloud dari 3% penyedia solusi pihak, terutama untuk penyebaran multi-cloud.

* 1. Tanggung Jawab Bersama

Gunakan "perjanjian back-to-back" dengan Penyedia Cloud Anda untuk memastikan kepatuhan standar keamanan penuh.

1. **Alat-Alat**
2. Keamanan yang Ditetapkan Perangkat Lunak yakinkan kembali solusi Keamanan Cloud tertinggi yang tersedia.
3. Otentikasi Multifaktor; Kemajuan AAA untuk setiap Lapisan Cloud misalnya kombinasi biometrik wajib.
4. Inspeksi dan Pemantauan; penilaian pendapat kedua.

1. **Pengetesan**
2. Isolasi Sumber Daya Cloud : Mencegah serangan pivot VM ke VM.
3. Periksa Masalah Penguncian : Mencegah terjebak dalam produk yang rentan.
4. Periksa Masalah Tata Kelola : Meyakinkan kembali standar praktik terbaik.
5. Periksa Masalah Kepatuhan : Hindari sanksi dan hukuman.
6. Periksa Integritas Data, Retensi, dan Pembuangan: Mencegah kebocoran dan kerugian.

**Ringkasan**

Diskusi ini menyampaikan masalah keamanan yang terkait dengan layanan cloud. Tercatat bahwa penjahat dunia maya telah mengambil keuntungan dari kerentanan dalam ekosistem bersama dan kurangnya kontrol keamanan yang efektif, yang menyebabkan penyalahgunaan platform. Peretas dapat secara ilegal mengakses informasi rahasia penyewa lain yang berada di infrastruktur cloud yang sama. Oleh karena itu, bisnis disarankan untuk melakukan penilaian risiko berkelanjutan untuk mengurangi potensi ancaman terhadap data sensitif mereka.

Selanjutnya, penyedia keamanan cloud harus meningkatkan perlindungan keamanan melalui penerapan langkah-langkah keamanan proaktif yang lebih canggih dan canggih untuk mengatasi tantangan ini.