Keamanan Jaringan

(Resume Webinar)

Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

The Trend of cloud security

Cloud computing adalah salah satu model yang menawarkan layanan komputasi instan tanpa menanggung biaya. Namun demikian, seperti teknologi lainnya membawa kekurangannya. Salah satu masalah utama adalah masalah keamanan dan privasi termasuk data teokoge karena sumber daya komputasi Infrastruktur bersama untuk memproses informasi bisnis rahasia seperti kekayaan intelektual, rahasia dagang, dan informasi rahasia pelanggan, yang dapat menyebabkan pelaku yang tidak sah dapat mengaksesnya.

Ancaman dalam decade terakhir

- **Data Loss dan Data Leakage**

Sebagian besar fitur Perlindungan Data Cloud untuk Perusahaan ditawarkan secara terpisah sebagai layanan opsional dan diperpanjang, mis. penyimpanan tambahan untuk retensi snapshot dan anti-ransomware karena sumber dayanya banyak dan mahal.

- **Abuse and Neforious use**

Karena Cloud Computing adalah ekosistem berbagai layanan, interaksi, dan saling ketergantungan, menjadi lebih lazim. Eksploitasi (PaaS) untuk "Peretasan sebagai Layanan" dapat lebih menantang untuk dimitigasi karena tersembunyi di beberapa infrastruktur.

Misalnya, perlindungan lain dibutuhkan di dalam permukaan Cloud untuk melindungi data, dan itu adalah permukaan tambahan. Sebagian besar adalah solusi pencegahan kehilangan data. Layanan ini biasanya dikombinasikan dengan solusi pihak ketiga. Jadi ini tidak disediakan oleh layanan cloud-nya.

- **Insecure Interface and API**

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

- **Shared Tecgnology Issues**

Penyedia layanan cloud menggunakan infrastruktur yang dapat diskalakan untuk mendukung banyak penyewa yang menopang infrastruktur yang mendasarinya. Di lapisan paling bawah, di mana hypervisor dapat dieksploitasi dari mesin virtual yang dikompromikan di penyewa lain untuk mendapatkan akses ke semua VM di beberapa lingkungan bersama.

- Virtualisasi adalah teknologi yang memungkinkan satu infrastruktur fisik berfungsi sebafau infrastruktur adalah teknologi yang memungkinkan satu infrastruktur fisik berfungsi sebagai berbagai infrastruktur logis atau sumber daya, mengurangi jumlah besar yang diinvestasikan untuk membeli sumber daya tambahan adalah teknik, yang memungkinkan berbagi instant fisik tunggal atau multi sumber daya tambahan penyewa.
- Virtualisasi Perangkat Keras adalah abstraksi sumber daya komputer dari perangkat lunak yang menggunakan sumberdaya tersebut, virtualisasi perangkat keras juga disebut virtualisasi server virtuauzasi perangkat keras menginstal hypervisor atau

virtual machine manager (vmml yang menciptakan lapisan abstraksi antara perangkat lunak dan perangkat keras.

- Lingkungan virtualisasi dikelola oleh software atau firmware, dikenal sebagai hyperviso
- Hypervisor rentan terhadap semua jenis serangan untuk infrastruktur normal

- **Hyper Jacking**

Digunakan untuk menginfeksi sistem berbasis cloud computing dengan hypervisor dos, penyerang harus memiliki kontrol hypervisor. Penyerang menggunakan rootkit yang diinstal pada vm (mesin virtual) untuk menyerang untuk mendapatkan pengendalian atas hypervisor, usaha tersebut oleh penyerang cyber didefinisikan sebagai hyper-jacking. Jika penyerang berhasil hyper jack kekuatan hypervisor, dia dapat mengendalikan seluruh hosting. Hasilnya, penyerang dapat mengubah perilaku dan menyebabkan kerusakan pada mesin virtual.

- **Virtual Machine Level Attack**

Serangan pada platform Cloud yang sama dapat memengaruhi penyewa lainnya. Penerapan Cloud apa pun wajib untuk mengeraskan lapisan virtualisasi guna mencegah serangan VM ke VM.

- **Service and Session Hijacking**
- **Man in the cloud and DDOS**

DDoS dapat diartikan sebagai Penolakan Layanan secara Terdistribusi. DDoS adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapa komputer host penyerang sampai dengan komputer target tidak bisa diakses.

- **Cloud Control Layers**

Terapkan lapisan kontrol tambahan dalam manajemen Cloud dari penyedia solusi pihak 3", terutama untuk penerapan multi-cloud.

- **Shared Responbilities**

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

Iot Security Concern Terhadap Transformasi Digital & Kasus Penggunaan Keamanan Smartphone

IoT telah merevolusi cara hidup, bekerja, dan berinteraksi dengan teknologi. Dengan semakin banyaknya perangkat yang terhubung, potensi pelanggaran keamanan dan pencurian data pun meningkat. Transformasi digital dan munculnya rumah pintar di Indonesia telah memperkuat kebutuhan akan praktik keamanan IoT yang kuat.

Menurut data jumlah device yang digunakan di Indonesia adalah 128% dari populasi penduduk Indonesia, sedangkan pengguna internet di Indonesia sebanyak 77% dari penduduk Indonesia dengan 60% diantaranya adalah pengguna media sosial.

Keamanan siber terus berkembang, baik perilaku maupun praktiknya. Apakah itu keadaan darurat kesehatan global, perubahan iklim, populasi yang menua, atau tantangan masa depan lainnya, teknologi digital menawarkan alat yang menarik untuk membantu memajukan dunia. Ketika tujuan pembangunan berkelanjutan (SDGs) mencapai kematangannya pada tahun 2030, 90% dari proyeksi populasi dunia, atau 7,5 miliar orang, diproyeksikan akan online dengan sekitar 24,1 miliar perangkat Iot yang terhubung.

Terdapat 5 bagian dalam IOT Security Concern

1. Autentication
   - Mechanism
   - Credential
   - Process
2. Firmware & Software Updates
   - Vulnerbilities
   - Exploitation
   - Methods
3. Standardization
   - Based on Manufacturer
   - Based on Different Protocols
   - Interoperability
4. Privacy & Personal Data protection
   - Collection & Storage
   - Access Methods
   - Processing Mechanism
5. Physical Security
   - Access
   - Location
   - Vandalism Protection

Terdapat 3 Challenges Baru Security

- **Network** (untuk Network Security)

- Ultra-high throughput
- Latency < 1 ms
- Availiability 99.999%
- Connections aggregation
- High security(Private Network)

➢ **Data Storage** (untuk Data & Platform Security)
- Local Edge Computing
- Local Data Storage
- On Cloude Data Storage
- High Security Hybrid Data Storage
- Blockchain

➢ **System Integrator** (untuk Device & Application Security)
- Migration & Integration
- Installation & Delivery
- Optimization
- Operastion & maintenance

Terdapat 3 bagian dalam managing IOT Security, yaitu **management**, **operation**, and **technology.**

Dalam Smarthome, terdapat beberapa **Threat & Challenges dalam IOT Security** diantaranya:

➢ **Devices Vulnerability**
- Hacking.
- Data Breaches.
- Malware Attacks.

➢ **Hackers**
- Exploit vulnerability.
- Gain access to home network.
- Steal data and take control of device.

➢ **Data Breaches**
- Leaking of personal information.
- Password, email, credit card details stolen.
- Device storage data collection.

➢ **Malware Attacks**
- Virus.
- Trojan.

Tedapat 5 bagian best practices untuk smarthome IOT Security

1. Password
   - Not By Default
   - Strong & Unique

- Periodically Changes

2. Firmware & Soveware Updates
   - Regilar Update
   - Latest Patch
   - Avoid Vulnerabilities
3. Network
   - Implement Segregation
   - Strengthening Firewalls in Gateway
   - Uses redudancy
4. Encryptio
   - Access
   - Location
   - Vandalism Protection
5. Audit & Assessment
   - Regularly
   - People-Process-Tecnology
   - Proactive Risk Mitigation

Perangkat dan solusi IOT akan memiliki penetrasi yang signifikan di masa depan menghadapi solusi digital yang berpusat pada manusia untuk mengembangkan jaringan dengan permintaan yang sangat besar di segmen vertikal khususnya untuk memenuhi kebutuhan masyarakat.

Siklus hidup untuk teknologi baru semakin pendek sehingga kolaborasi, penggunaan infrastruktur bersama, teregulasi & inovatif menjadi kunci keberhasilan keamanan IOT.