# TUGAS 3 MANAJEMEN JARINGAN

**BRAMANTIO RIZKI NUGROHO**

**NIM 09121001044**

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

**Keeping Up With The Revolution of IT Security**

Keamanan teknologi Informasi dan komunikasi semakin berkembang bersama dengan kemajuan teknologi. Video ini membahas beberapa tren dalam keamanan TI yang dapat membentuk masa depan IT.

Keamanan telah berkembang sejak awal komputasi. Gelombang pertama adalah keamanan endpoint dengan perusahaan seperti Symantec, McAfee, dan lainya. Gelombang besar kedua inovasi dalam keamanan IT adalah keamanan jaringan dengan perusahaan seperti Checkpoint, Cisco, Palo Alto Networks. Pada gelombang ketiga adalah perusahaan yang ingin melindungi aplikasi dengan memeriksa lalu lintas HTTP. Ini mencakup perusahaan seperti Imperva, Akamai, F5,dan lainnya.

Yang pertama dibahas adalah API pendekatan Centric untuk pengembangan aplikasi. Banyak aplikasi modern lebih seperti shell atau lapisan UI yang konten disalurkan melalui API.Mereka juga menggunakan berat API untuk terhubung ke solusi eksternal untuk otomatisasi. Keamanan API harus menjadi bagian dari strategi keamanan setiap korporasi. Hal ini dapat mencegah beberapa masalah keamanan dan kinerja utama.

Pada Solusi keamanan tradisional (FW, IPS, WAF, dll) biasanya tidak memiliki visibilitas klien yang tepat diperlukan untuk secara efektif mengidentifikasi bots canggih. Mengidentifikasi bots maju dan peramban,otomatisasi memerlukan teknik khusus. keamanan tradisional tidak dirancang untuk menangani masalah ini. Kebanyakan Wafs dirancang khusus untuk melindungi terhadap ancaman seperti OWASP atas 10 dan melakukannya dengan aturan pendekatan berbasis. Bots lanjutan di sisi lain, terbang di bawah radar dari alat-alat ini karena mereka muncul untuk menjadi manusia dan tidak melakukan serangan yang memicu Web serangan aplikasi mengetahui aturan.Mengidentifikasi bot ini memerlukan menggunakan berbagai pendekatan, yang menjadi lebih maju sebagai bot menjadi lebih canggih.

Sedangkan pada aplikasi modern secara geografis didistribusikan dengan pusat data di mana pun basis pelanggan terkonsentrasi. Penyebaran pengaruh beberapa infrastruktur jenis (*clouds, on-prem, hybrid, multi-cloud,)*

Pilihan penyebaran fleksibel memungkinkan cakupan yang lengkap dari perkebunan web beragam.Tindakan pencegahan keamanan harus dapat saling berhubungan untuk berbagi data, tidak siled atau terisolasi.Karena sifat terdistribusi penyebaran aplikasi, ada persyaratan tambahan yang dimasukkan di vendor keamanan untuk menjadi efektif. Mereka harus fleksibel untuk menutupi jenis penyebaran pelanggan mungkin memiliki, sehingga semua penyebaran atau contoh dapat berbagi manfaat keamanan yang sama. Selain itu, keamanan ini perlu berkomunikasi antara dirinya, bukannya siled di setiap penyebaran atau instalasi situs.

Dengan mengetahui banyak tentang keamanan yang ada pada IT maka kita harus lebih teliti dalam menyimpan data. Hindari menyimpan data sensitif yang berlebihan di could,memahami bagaimana layanan cloud Anda vendor kerja, gunakan password yang kuat,dan jangan biarkan bot mengikis database.

Source : https://www.brighttalk.com/webcast/288/181839?utm_campaign=webcasts-search-results-feed&utm_content=network+management&utm_source=brighttalk-portal&utm_medium=web&utm_term=