Konsep Keamanan, Kepatuhan dan Identitas

Modul 3

Muhammad Ogin Hasanuddin

KK Teknik Komputer
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

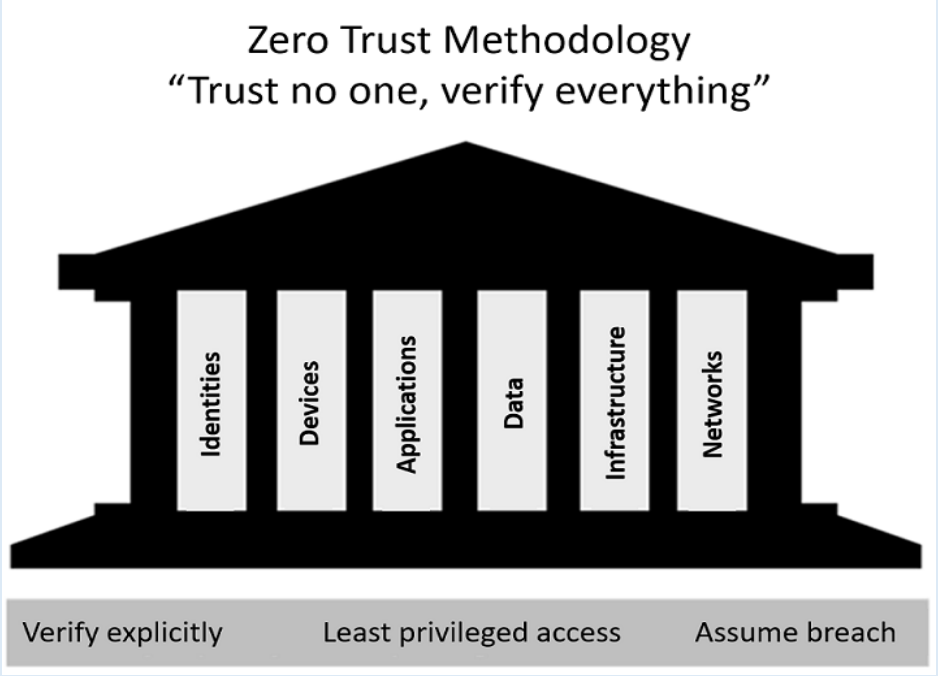

Konsep Dasar Keamanan, Kepatuhan dan Identitas
Kepatuhan dan Identitas di Bidang Kesehatan

Konsep Dasar Keamanan, Kepatuhan dan Identitas

Sebuah organisasi perlu memahami bagaimana tindakan yang paling tepat untuk melindungi data yang dimiliki, bukan hanya sekedar berpikir bagaimana agar data yang ada dapat di proses, diakses, keberadaan data apakah di komputasi awan ataukah bukan.

1. Metodologi Zero – Trust

   Semua komponen yang tersedia berada dalam sebuah jaringan yang terbuka dan beroperasi berdasarkan prinsip “tidak percaya siapapun, namun memverifikasi semuanya”. Pendekatan tanpa kepercayaan yang digunakan untuk memverifikasi permintaan secara eksplisit menggunakan semua sinyal yang tersedia berfungsi sebagai filosofi keamanan yang terintegrasi pada enam pilar dasar yaitu identitas, perangkat, aplikasi, jaringan, infrastruktur, dan data.

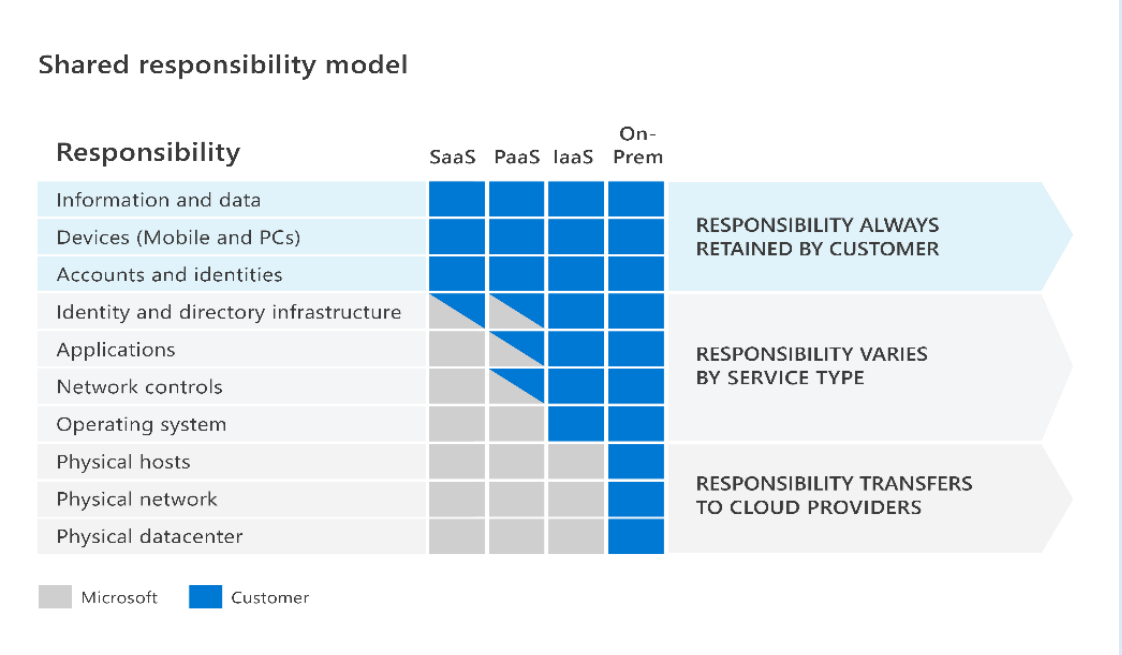


Konsep Dasar Keamanan, Kepatuhan dan Identitas

2. Model Tanggung Jawab Bersama

Model ini dapat melakukan pengidentifikasian tugas keamanan yang dikerjakan oleh penyedia komputasi awan dan para pengguna. Ketika sebuah organisasi menggunakan perangkat keras dan lunak maka organisasi tersebut perlu bertanggung jawab untuk menerapkan keamanan dan kepatuhan secara 100% penuh. Tanggung jawab itu sangat bervariasi bentuknya dan dapat di spesifikasikan berdasarkan beban kerjanya seperti perangkat lunak sebagai layanan, platform sebagai layanan, infrastruktur sebagai layanan, serta pusat data lokalnya.

Tanggung jawab yang selalu dipegang oleh sebuah organisasi pelanggan meliputi informasi dan data, perangkat, serta akun dan identitas. Sehingga manfaat dari model tersebut yaitu menyatakan bahwa model tersebut bertanggung jawab bersama dalam pengorganisasian tanggung jawab sebagai pengguna pengorganisaan schedule.

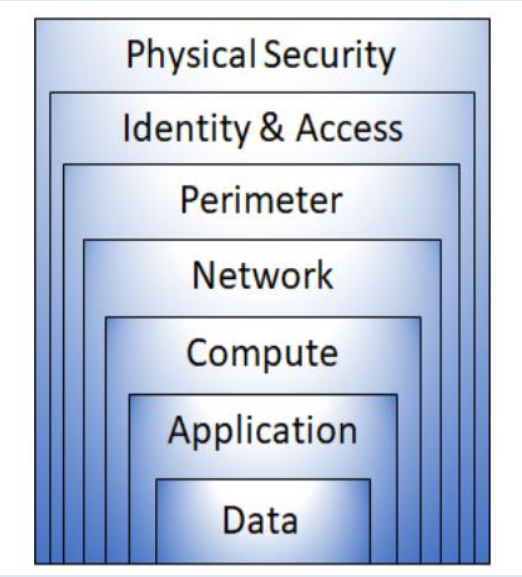


Konsep Dasar Keamanan, Kepatuhan dan Identitas

3. Proses Pertahanan yang Mendalam

Beberapa contoh lapisan keamanan seperti berikut:

a. Keamanan fisik, membatasi akses ke pusat data karena hanya untuk personel yang berwenang.
b. Kontrol keamanan identitas dan juga akses, mengotentifikasi multi – faktor atau mengontrol akses ke infrastruktur juga kontrol perubahan.
c. Keamanan perimeter, melakukan perlindungan penolakan layanan yang terdistribusi agar dapat memfilter serangan berskala besar sebelum menyebabkan penolakan layanan bagi pengguna.
d. Keamanan jaringan, melakukan segmentasi jaringan serta kontrol akses jaringan untuk membatasi komunikasi antar sumber daya yang digunakan.
e. Menghitung keamanan lapisan, mengamankan akses ke mesin virtual yang ada di penyimpanan komputer atau di komputasi awal agar dapat menutup port tertentu lainnya.
f. Keamanan lapisan aplikasi, memastikan bahwa aplikasi yang digunakan aman dan bebas dari kerentanan keamanan.
g. Keamanan lapisan data termasuk kontrol untuk mengelola akses ke data bisnis untuk mengelola akses ke data bisnis dan pelanggan juga melakukan enkripsi dalam melindungi setiap data.



Konsep Dasar Keamanan, Kepatuhan dan Identitas

4. Ancaman Secara Umum
   a. Pelanggaran data

      Melakukan pencurian data pribadi seseorang artinya setiap informasi yang terkait dengan individu dan digunakan dalam melakukan pengidentifikasian secara langsung maupun tidak langsung.

   b. Dictionary Attack

      Serangan terhadap identitas berupa mencuri identitas dengan mencoba sejumlah besar kata sandi yang diketahui atau secara acak ke salah satu tempat mengakses akun tertentu.

   c. Ransomware

      Salah satu jenis malware yang mengenkripsi sebuah file dan folder dalam mencegah pengaksesan ke beberapa file yang penting. Penyerang yang mendistribusikan malware sering kali dimotivasi oleh uang dan akan menggunakan komputer yang terinfeksi untuk melancarkan serangan seperti mengumpulkan informasi yang dapat dijual, menjual akses ke sumber daya komputasi serta memeras pembayaran dari korban.

   d. Serangan yang Mengganggu

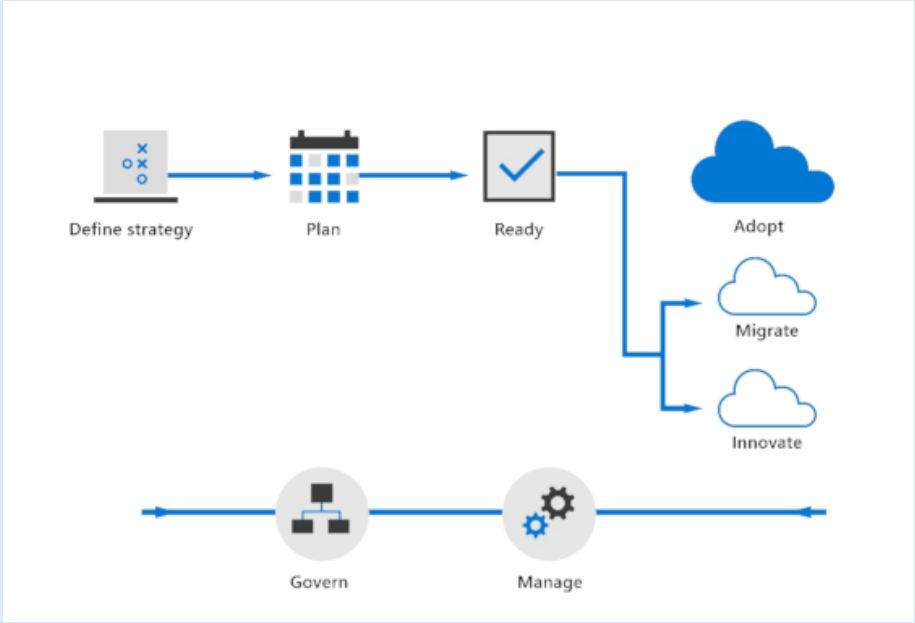
      Serangan ini lebih disebut serangan Distributed Denial of Service (DDoS) yang dapat menargetkan titik akhir yang dapat dijangkau oleh publik melalui internet.

Konsep Dasar Keamanan, Kepatuhan dan Identitas

5. Kerangka Kerja Adopsi Komputasi Awan

Microsoft Cloud Adoption Framework for Azure terdiri dari panduan implementasi, dokumen, praktik yang terbaik, dan juga alat yang dapat dirancang untuk membantu penerapan strategi bisnis di komputasi awan.Terdapat siklus dalam prosesnya sebagai berikut :

a. Strategi
b. Rencana
c. Persiapan
d. Pengadopsian
e. Mengatur lingkungan dan beban kerja
f. Mengelola manajemen



Kepatuhan dan Identitas di Bidang Kesehatan

HHS (Health and Human Services), HIT “Melibatkan pertukaran informasi kesehatan dalam lingkungan elektronik. Penggunaan IT kesehatan secara luas dalam industri perawatan akan meningkatkan kualitasnya, mencegah kesalahan medis, mengurangi biaya perawatan kesehatan, meningkatkan efisiensi administrasi, mengurangi dokumen dan memperluas akses ke perawatan kesehatan yang terjangkau.”

1. Kebijakan, dokumen yang sifatnya formal tingkat tinggi yang secara singkat dapat menyatakan sebuah perspektif organisasi tentang topik tertentu.
2. Prosedur, langkah – langkah berurutan terperinci yang didokumentasikan dan menginformasikan karyawan rumah sakit tentang cara melakukan tindakan tertentu.
3. Standar, seperangkat spesifikasi yang harus diikuti oleh karyawan layanan kesehatan atau organisasi dan biasanya membahas sistem atau konfigurasi teknis.
4. Pedoman, rekomendasi atau saran terdokumentasi yang menawarkan panduan khusus topik berdasarkan praktik terbaik industri.

Microsoft Cloud for Healthcare

Cloud for healthcare membantu organisasi layar kesehatan, meningkatkan pengalaman pasien, mengoordinasikan perawatan, dan mendorong efisiensi operasional, membantu mendukung keamanan, kepatuhan dan interoperabilitas data kesehatan.

a. Kesehatan virtual, banyak pasien yang mencari peluang baru untuk menggunakan teknologi saat mengelola kesehatan mereka.
b. Interoperabiltas, meningkatkan keterlibatan pasien jarak jauh membutuhkan pertukaran data yang terintegrasi.
c. Hasil kesehatan, dengan volume data yang besar namun tidak terstruktur maka penyedia harus menghabiskan banyak waktu untuk mencoba mengumpulkan wawasan dari data tersebut
d. Tekanan keamanan, apabila organisasi perawatan kesehatan tidak dapat menggunakan data mereka secara efisien.

Microsoft Cloud for Healthcare

Kemampuan ini mendukung tiga skenario prioritas yang disorot oleh Microsoft Cloud for Healthcare dengan cara yaitu :

1. Meningkatkan keterlibatan pasien, memungkinkan data pasien mengalir dengan aman di seluruh rangkaian perawatan.
2. Memberdayakan kolaborasi tim kesehatan, mempercepat kemampuan tim kesehatan.
3. Meningkatkan wawasan klinis dan operasional, menyatukan data dan menerapkan analitik canggih dan kecerdasan buatan.

Dibangun untuk melindungi informasi kesehatan dalam mendukung keamanan dan privasi menyeluruh, mengelola peraturan kepatuhan yang terus berkembang dan meningkatkan tata kelola serta kepercayaan data.

Kemampuan Layanan Kesehatan Unggulan

Terdapat sembilan kemampuan yang diaktifkan melalui tiga skenario yang dijelaskan di pembahasan sebelumnya dan berpusat pada penyedia. Kesembilan kemampuan tersebut yaitu :

1. Perawatan yang dipersonalisasi, membangun hubungan melalui peningkatan pengalaman yang dipersonalisasi untuk setiap pasien.
2. Wawasan pasien, mengubah data menjadi wawasan preskriptif.
3. Kesehatan virtual, menyediakan cara baru untuk pemeliharaan melalui teks bot, suara, video dan obrolan.
4. Kolaborasi tim perawatan, mengoptimalkan sumber daya dan menyelesaikan masalah secara kolektif.
5. Koordinasi perawatan, mengembangkan sistem keterlibatan dengan alur kerja yang cerdas.
6. Pemantauan pasien berkelanjutan, menggabungkan Internet of Medical Things (IoMT) dan analitik untuk mengoptimalkan perawatan.
7. Interoperabilitas, membuat sistem keterlibatan layanan kesehatan baru dengan menghubungkan data dari beberapa kumpulan data.
8. Analisis operasional, mendapatkan wawasan yang dapat ditindaklanjuti untuk mengoptimalkan operasi.
9. Analisis klinis, mengakses dan membantu pembagian data yang dapat ditindaklanjuti dengan aman untuk membantu meningkatkan perawatan pasien.


Thank You
See You Next
Chapter