Konfigurasi Kebijakan Keamanan untuk Mengelola Data

Oleh: Dimas Agung Prasetyo

Setelah mengikuti kelas ini anda akan bisa

- Menjelaskan konsep keamanan informasi
- Menjelaskan klasifikasikan dan pelabelan data
- Menjelaskan persyaratan retensi data
- Menjelaskan konsep kepemilikan dan kedaulatan data
- Menjelaskan implementasi konsep tersebut menggunakan beberapa produk Microsoft

Pengetahuan Dasar yang diharapkan

- Konsep Keamanan dasar (Security Fundamental)
- Pengalaman dasar pengoperasian O365 dan layanannya
- Pengalaman dasar pengoperasian Azure dan Layanannnya

Apa itu data dan informasi?

Data

- Data kurang lebih adalah sekumpulan fakta yang kada bisa bersifat sangat sederhana, random, abstrak dan tidak memiliki manfaat langsung jika tidak dikelola dan diolah lebih lanjut
- Contoh Nilai mahasiswa, Angka penjualan

Informasi

- Ketika sekumpulan data di proses, diolah dan diberi konteks yang tepat yang kemudian bermanfaat bagi organisasi dapat disebut Informasi
- Contoh: Grafik tren nilai mahasiswa dalam periode tertentu, Grafik tren penjualan produk pada musim panas

Mengapa Informasi Penting dan Perlu Dikelola Bagi Organisasi

Mengapa Informasi Penting?

- Informasi adalah inti operasi organisasi
- Bagi organisasi, Informasi adalah asset yang menjawab
  - “Siapa kami?",
    “Untuk siapa kita ada"
    “Bagaimana kami melakukan sesuatu"
    “Kapan kita melakukannya",
    “Di mana kami mengembangkan kegiatan kami"
    “Mengapa kami melakukan seperti yang kami lakukan"

Mengapa Informasi Perlu Dikelola?

- Meningkatkan efesiensi proses bisnis
- Mendukung pengembangan strategic
- Menjaga akuntabilitas
- Mengelola Resiko
- Memastikan operasi organisasi yang berkesinambungan

Informasi perlu dikelola aspek keamanannya

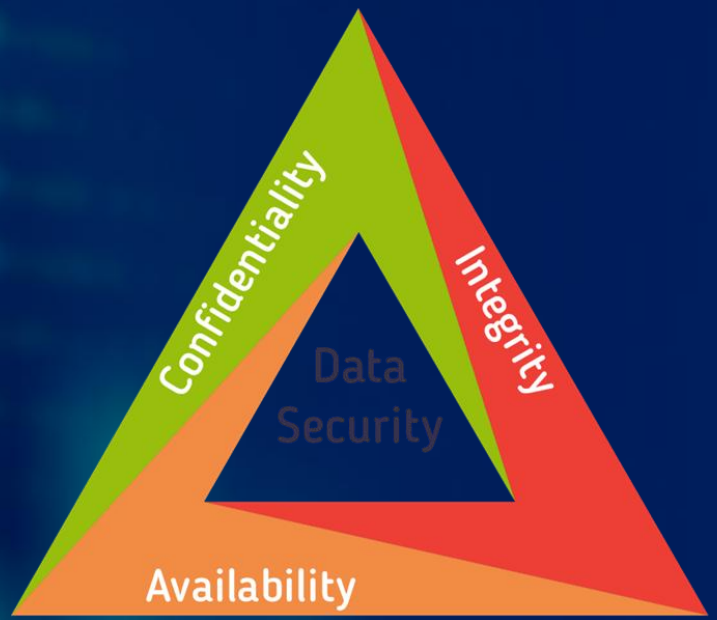
- Melindungi Pelanggan
- Melindungi Informasi Hak Milik
- Melindungi Aset
- Menjaga Reputasi
- Melindungi Income
- Memberi Jaminan Kompetitif
- Memberikan Ketenangan

Prinsip Keamanan Informasi

- Confidentiality. Aktivitas atau upaya yang dilakukan untuk memberikan perlindungan agar Informasi tidak diakses oleh pihak tidak berwenang

- Integrity. Aktivitas atau upaya yang dilakukan untuk memastikan infromasi / data yang disimpan utuh (tidak dimanipulasi, diubah, diedit) oleh pihak tidak berwenang

- Availibility. Aktivitas atau upaya yang dilakukanuntuk memastikan data atau infromasi selalu tersedia saat dibutuhkan oleh organisasi untuk mendukung kegiatan operasional



Klasifikasi Data

Klasifikasi data adalah istilah khusus yang digunakan di bidang keamanan siber dan tata kelola informasi untuk menggambarkan proses identifikasi, pengkategorian, dan perlindungan konten sesuai dengan sensitivitas atau tingkat dampaknya. Dalam bentuknya yang paling dasar, klasifikasi data adalah sarana untuk melindungi data Anda dari pengungkapan, perubahan, atau penghancuran yang tidak sah berdasarkan seberapa sensitif atau berdampaknya data tersebut

Bagaimana Implementasinya?

- Beberapa produk Microsoft seperti Office365 dan Azure bisa membantu anda dalam mengamankan ases infromasi yang ada di organisasi

- Pendekatan Keamanan Produk Microsoft:
  - kontrol pelanggan
  - transparansi
  - keamanan
  - perlindungan hukum yang kuat untuk privasi,
  - tidak ada penargetan berbasis konten,
  - dan manfaat bagi pelanggan dari data apa pun yang kami kumpulkan

- Informasi lebih detil
- Security Development Lifecycle (SDL)
- Privacy Statement

Bagaimana Azure dan O365 menjamin data organisasi

Azure

External audits	Section	Latest report date
ISO 27018 Statement of Applicability Certificate	A-2.1: Public cloud PII processor's purpose	December 3, 2021
SOC 1	DS-15: Customer subscription termination/expiration SDL-1: Security Development Lifecycle (SDL) methodology LA-4: Protection of confidential customer data	September 30, 2021
SOC 2 SOC 3	DS-15: Customer subscription termination/expiration SDL-1: Security Development Lifecycle (SDL) methodology LA-4: Protection of confidential customer data SOC2-1: Asset classification SOC2-7: Published confidentiality and security obligations	November 12, 2021

Office 365

External audits	Section	Latest report date
ISO 27018 Statement of Applicability Certificate	A-2.1: Public cloud PII processor's purpose	March 2022
SOC 2	CA-12: Service level agreements (SLAs) CA-17: Microsoft security policy CA-25: Control framework updates	September 30, 2021

Framework Klasifikasi Data

- Organisasi perlu membuat klasifikasi data
- Terdiri dari beberapa tingkat (3-5) yang memuat beberapa parameter seperti nama, deskripsi, dan contoh dunia nyata.
- Microsoft merekomendasikan tidak lebih dari lima label
- Contoh Level (Tips Klasifikasi Dokumen Elektronik Perusahaan Agar Aman dari Jerat UU ITE (hukumonline.com))
  - Publik,
  - Internal,
  - Rahasia,
  - dan Sangat Rahasia.
- Penggunaan nama label harus jelas tidak menimbulkan keraguan contoh:
  - Rahasia & Terbatas
  - Rahasia dan Sangat rahasia

Aspek Lain Klasifikasi Data (i)

- Label hanyalah sebuah nama yang memberikan Info nilai dari suatu informasi yang diberi label
- Selain pendefinisian label perlu juga disiapkan instrumen kontrol yang melekat pada label tersebut
- Kontrol memberikan parameter infromasi tambahan terhadap label untuk memproteksi Informasi tersebut
- Kontrol dapat berupa tambahan informasi berikut:
  - Jenis dan lokasi penyimpanan
  - Enkripsi
  - Kontrol akses
  - Penghancuran data
  - Pencegahan kehilangan data
  - Pengungkapan publik
  - Akses logging dan pelacakan

  Dan lain lain

Aspek Lain Klasifikasi Data (ii)

- Kontrol keamanan akan bervariasi menurut tingkat klasifikasi
- Semakin tinggi klasifikasi data tingkat perlindungan biasanya akan semakin kompleks
- Sebagai contoh dibawah: Perlakuan data yang disimpan pada removable disk (usb misal) untuk klasifikasi data tertentu.

Storage type	Confidential	Internal	Unrestricted
Removable Storage	Prohibited	Prohibited unless encrypted	No control required

Implementasi Klasifikasi Data (i)

- Mengembangkan dan Mengpalikasikan klasifikasi data tidak mudah pada situasi nyata
- Begitu kebijakan atau standar ditetapkan, user perlu dibimbing agar kebijakan dan standar diterapkan
- Bimbingan ini diterjemahkan dalam bentuk guidelines atau petunjuk kerja

Implementasi Klasifikasi Data (ii)

Perlu diingat!

- Proses yang berkelanjutan bukan sekali jadi langsung sempurna
- Kebijakan harus menyentuh pengguna level dasar
- Klasifikasi Data dibuat untuk diimplementasikan
- Level disesuaikan kebutuhan
- Libatkan orang yang tepat
- Keamanan VS kenyamanan

Titik kritikal yang perlu diperhatikan

- Merancang kerangka kerja klasifikasi data yang kuat dan mudah dipahami, termasuk menentukan tingkat klasifikasi dan kontrol keamanan terkait.
- Mengembangkan rencana implementasi yang mencakup konfirmasi solusi teknologi tepat guna, menyelaraskan rencana tersebut dengan proses bisnis yang ada, dan mengidentifikasi dampaknya terhadap tenaga kerja.
- Menyiapkan kerangka kerja klasifikasi data dalam solusi teknologi yang dipilih dan mengatasi kesenjangan antara kemampuan teknologi alat dan kerangka kerja itu sendiri.
- Menetapkan struktur tata kelola yang mengawasi pemeliharaan dan kesehatan yang sedang berlangsung dari upaya klasifikasi data.
- Mengidentifikasi indikator kinerja utama (KPI) tertentu untuk memantau dan mengukur kemajuan.
- Meningkatkan kesadaran dan pemahaman tentang kebijakan klasifikasi data, mengapa kebijakan tersebut penting, dan bagaimana mematuhinya.
- Mematuhi tinjauan audit internal yang menargetkan kehilangan data dan kontrol keamanan siber.
- Melatih dan melibatkan pengguna sehingga mereka menjadi sadar akan perlunya klasifikasi yang benar dalam pekerjaan sehari-hari mereka dan menerapkan langkah-langkah klasifikasi yang tepat.

Kepemilikan dan Kedaulatan Data

Kepemilikan Data

- Karena Informasi adalah core,Kepemilikan adalah aspek yang perlu dilindungi
- Organisasi harus memegang Kontrol terhadap data
- Termasuk ketika data dan informasi disimpan oleh pihak ketiga
- Untuk kebutuhan online, Microsoft dan layanannya mengelompokkan data:
  - Data Pelanggan
  - Data Pribadi
  - Data Layanan Profesional
  - Data Administrastor
  - Data Pembayaran
- Microsoft menjamin data tersebut tidak dibagi untuk iklan (cloud privacy / ISO-IEC 27018)
- Pelanggan layanan cloud Microsoft tahu di mana data mereka disimpan.
  Data pelanggan tidak akan digunakan untuk pemasaran atau iklan tanpa persetujuan eksplisit.
  Pelanggan Microsoft tahu apa yang terjadi dengan data mereka.

Kedaulatan Data

- Kedaulatan data berfokus pada tempat data disimpan (data home). Dan ini menyiratkan bahwa data yang disimpan tunduk pada hukum dan struktur pemerintahan yang bertanggung jawab atas wilayah tempat data dikumpulkan.
- Organisasi harus memperhatikan lokasi data akan disimpan Ketika data tersebut didistribusikan untuk mempertimbangkan aspek legal dan hukum.
- Contoh: undang-undang perlindungan data terbaru dari Uni Eropa, GDPR, telah menerapkan aturan ketat tentang bagaimana organisasi menangani informasi pribadi warganya, bahkan ketika perusahaan memproses data di luar wilayah tersebut.

Kedaulatan Data vs Residensi Data

Residensi Data

- Residensi data adalah ketika bisnis atau pemerintah menentukan lokasi geografis tempat datanya harus disimpan.
- Persyaratan residensi data seringkali merupakan hasil dari alasan terkait kebijakan atau peraturan.

Kedaulatan Data

- Di sisi lain, kedaulatan data mengacu pada penunjukan lokasi geografis di mana data disimpan secara fisik dan menjadi subjek hukum negara tersebut.
- Sementara residensi data memastikan bahwa data tetap berada di lokasi geografis yang ditentukan, kedaulatan data memastikan bahwa informasi tersebut tunduk pada hukuman hukum dan perlindungan negara tempat data disimpan secara fisik.

Kedaulatan Data, Residensi Data di Azure

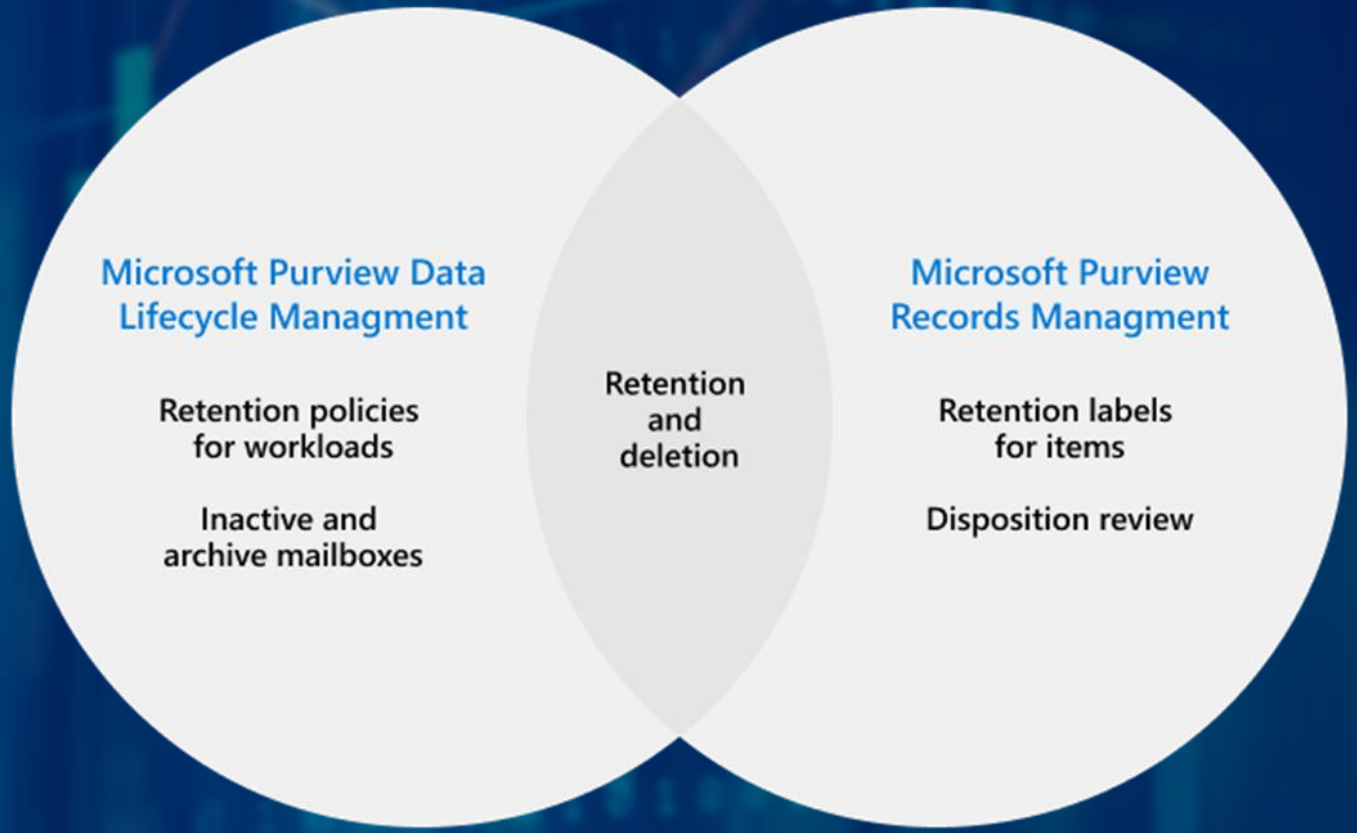
- Microsoft menjamin anda sebagai pelanggan, Anda mempertahankan kepemilikan data pelanggan—konten, data pribadi, dan data lain yang Anda berikan untuk disimpan dan dihosting di layanan Azure. Anda juga memegang kendali atas geografi tambahan di mana Anda memutuskan untuk menyebarkan solusi atau mereplikasi data Anda.
- Microsoft mengamankan data Anda menggunakan beberapa lapisan protokol keamanan dan enkripsi.
- Microsoft compliant dengan GPDR yang secara umum memberikan perlindungan hukum terhadap data pelanggan

Retensi Data

- Kebijakan penyimpanan data menyangkut data apa yang harus disimpan atau diarsipkan, di mana itu harus terjadi, dan untuk berapa lama. Setelah periode waktu retensi untuk kumpulan data tertentu berakhir, periode tersebut dapat dihapus atau dipindahkan sebagai data historis ke penyimpanan sekunder atau tersier, tergantung pada persyaratannya. Dengan cara ini, penyimpanan utama tetap bersih dan organisasi tetap patuh pada standar yang ditetapkan
- Aspek yang perlu diperhatikan dalam menentukan retensi data
  - Persyaratan Hukum
  - Persyaratan bisnis
  - Jenis daya
- Manfaaat Retensi Data
  - meningkatkan konsistensi untuk proses aplikasi data otomatis
  - mengurangi biaya penyimpanan data
  - meningkatkan efisiensi dan efektivitas operasional
  - mendukung kewajiban perusahaan untuk *compliance*
  - membuat klasifikasi informasi berdasarkan data pengguna menjadi lebih mudah

Bagaimana Microsoft Membantu Retensi Data

Govern your data



Keep what you need and delete what you don't

Use tools and capabilities to retain the content that you need to keep, delete the content that you don't.

1. Understand how retention and deletion works for Microsoft 365 services.
2. Create retention policies and if needed, retention labels for exceptions.
3. Manage mailboxes.
4. Import PST files to online mailboxes.

Manage high-value items

Configure advanced retention, deletion, and data management options for business, legal, or regulatory record-keeping requirements.

1. Understand the records management solution.
2. Use file plan to manage your retention schedules.
3. Apply your retention labels.
4. Manage the permanent deletion of data.

Penutup

- Information adalah salah satu aspek penting dalam organisasi
- Informasi perlu dikelola dan dijaga untuk menjamin operasi dan sustainibilitas organisasi
- Organisasi perlu menetapkan standar dan kebijakan dalam pengelolaan Informasi
- Layanan Microsoft seperti O365 dan Azure membantu organisasi dalam pengelolaan informasi
- Microsoft secara internal telah mengimplementasikan standar pengamanan Informasi dan diaudit secara berkala
- Organisasi bisa memanfaatkan layanan layanan yanga da pada Microsoft untuk membantu pengelolaan informasi

Thank You.